# Table of Contents

1. About this Guide ................................................................. 4
2. Loadbalancer.org Appliances Supported .......................... 4
3. Loadbalancer.org Software Versions Supported .................. 4
4. Microsoft Lync Software Versions Supported .................. 4
5. Microsoft Lync ........................................................................ 5
   - Microsoft Lync Editions ..................................................... 5
   - Standard Edition .......................................................... 5
   - Enterprise Edition ....................................................... 5
6. Microsoft Lync & Loadbalancer.org ..................................... 5
7. Microsoft Lync Server Roles .................................................. 5
8. Load Balancing Lync ............................................................. 7
   - Load Balancing Methods Supported ................................. 7
   - DNS Load Balancing .................................................... 7
   - Hardware Load Balancing (HLB) ................................. 8
   - Load Balanced Roles .................................................. 8
   - Loadbalancer.org Appliance Considerations .................... 8
   - Load Balancer Deployment Mode .................................. 8
   - Persistence (aka Server Affinity) ................................... 9
   - TCP Timeout Settings ............................................... 9
   - Reverse Proxy Server ............................................. 9
   - Additional Details .................................................. 9
9. Load Balanced Ports/Protocols ........................................... 10
   - Front End Servers .................................................. 10
   - Required .................................................................. 10
   - Optional .................................................................. 10
   - Director Servers ................................................... 11
   - Required .................................................................. 11
   - Optional .................................................................. 11
   - Edge Servers (Internal Access) .................................... 11
   - Edge Servers (External Access) .................................. 11
10. Deployment Architecture .................................................. 12
    - Loadbalancer.org test Environment ............................... 12
    - One-arm Vs Two-arm ............................................. 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
11. Loadbalancer.org Appliance – the Basics ........................... 19
    - Virtual Appliance Download & Deployment .................. 19
    - Initial Network Configuration .................................... 19
    - Accessing the Web User Interface (WebUI) ................... 20
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12. Appliance Configuration for Lync</td>
<td>STEP 1 – Configure Layer 7 Global Settings</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>STEP 2 – Configuring the Load Balanced Front End Services</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Virtual Service (VIP) List</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Configuring the FrontEndPool VIP</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Configuring the FePoolExtWebSvcs8080 VIP</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Configuring the FePoolExtWebSvcs4443 VIP</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>STEP 3 – Configuring the Load Balanced Director Services</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Virtual Service (VIP) List</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Configuring the DirectorPool VIP</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Configuring the DirPoolExtWebSvcs8080 VIP</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Configuring the DirPoolExtWebSvcs4443 VIP</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>STEP 4 – Configuring the Load Balanced Edge Pool Services (Internal)</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Virtual Service (VIP) List</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Virtual Service (VIP) Configuration</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Real Server (RIP) Configuration</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>STEP 5 – Configuring the Load Balanced Edge Pool Services (External)</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Virtual Service (VIP) List</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Virtual Service (VIP) Configuration</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Real Server (RIP) Configuration</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>STEP 6 – Finalizing the Configuration</td>
<td>38</td>
</tr>
<tr>
<td>13. Testing &amp; Validation</td>
<td>Client connections bypass the load balancer</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Taking Servers Offline</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Microsoft Lync Testing Tool</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Lync Diagnostics Tools</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Wireshark Protocol Analyzer</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Other Useful Resources</td>
<td>40</td>
</tr>
<tr>
<td>14. Technical Support</td>
<td></td>
<td>40</td>
</tr>
<tr>
<td>15. Further Documentation</td>
<td></td>
<td>40</td>
</tr>
<tr>
<td>16. Conclusion</td>
<td></td>
<td>40</td>
</tr>
<tr>
<td>17. Appendix</td>
<td>1 – Clustered Pair Configuration – Adding a Slave Unit</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>2 – Configure Reverse Proxy VIPs</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>3 - Company Contact Information</td>
<td>46</td>
</tr>
</tbody>
</table>
1. About this Guide

This guide details the steps required to configure a load balanced Microsoft Lync 2010 / 2013 environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft Lync 2010 / 2013 configuration changes that are required to enable load balancing. For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the relevant Administration Manual:

- v7.Administration Manual
- v8.Administration Manual

2. Loadbalancer.org Appliances Supported

Due to the number of Virtual Services (VIPs) required for Lync, the Enterprise R16 & R20 are not supported. All other models can be used with Lync as listed below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise VA</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products/hardware](http://www.loadbalancer.org/products/hardware)

3. Loadbalancer.org Software Versions Supported

- V7.6.4 and later

4. Microsoft Lync Software Versions Supported

- Microsoft Lync 2010 – all versions
- Microsoft Lync 2013 – all versions
5. Microsoft Lync

Microsoft Lync 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 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, 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 Enterprise Edition is required. Load balancing is required to load balance the Front End pools, Director pools and Edge Server pools.

6. Microsoft Lync & Loadbalancer.org

Deploying Microsoft Lync 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 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.

7. Microsoft Lync 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. |
<table>
<thead>
<tr>
<th>Role</th>
<th>Purpose</th>
<th>Scalability</th>
<th>High Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Back End Server</strong></td>
<td>The back-end SQL Server hosts various databases to keep track of Lync’s configuration and state information.</td>
<td>Microsoft recommends using an SQL cluster for high availability.</td>
<td>Use clustering/Mirroring techniques.</td>
</tr>
<tr>
<td><strong>A/V Conferencing Server</strong></td>
<td>Provides Audio/Visual conferencing functionality to Lync clients.</td>
<td>Microsoft recommends a separate dedicated server for more than 10,000 users. Each dedicated A/V server supports up to 20,000 users.</td>
<td>Use a pool of servers (no load balancer is required).</td>
</tr>
<tr>
<td><strong>Edge Server</strong></td>
<td>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!.</td>
<td>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.</td>
<td>Use a pool of servers with a load balancer.</td>
</tr>
<tr>
<td><strong>Mediation Server</strong></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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Co-location: 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><strong>Monitoring Server</strong></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 Load Balancer).</td>
</tr>
</tbody>
</table>
Archiving Server

**Purpose:** 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.

**Scalability:** 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.

**High Availability:** Use a standby server (messages are queued on the Front-End servers if a failure occurs).

**Co-location:** Can be co-located with Archiving Server.

Director Server

**Purpose:** 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.

**Scalability:** One Director for every 15,000 users who will access a site remotely. As a minimum, Microsoft recommend two Directors for high availability.

**High Availability:** Use a pool of servers with a load balancer.

8. Load Balancing Lync

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

**LOAD BALANCING METHODS SUPPORTED**
Microsoft Lync supports two types of load balancing solutions: Domain Name System (DNS) load balancing and Hardware Load Balancing (HLB).

**DNS LOAD BALANCING**
Lync DNS load balancing is typically implemented at the application level. When the application (for example, a Lync 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 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.

Note:
The configuration presented in this manual uses hardware load balancing for all load balanced services.

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 recommended 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.

LOADBALANCER.ORG APPLIANCE CONSIDERATIONS

LOAD BALANCER DEPLOYMENT MODE
Direct Return (DR) mode aka Direct Server Return (DSR) mode is not supported for Lync. 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.

  Note:
  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.

  Note:
  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>

**PERSISTENCE (AKA SERVER AFFINITY)**

Most Lync protocols are configured using source IP address persistence.

For Lync Web Services, if only Lync 2013 front-end/director servers are used, no persistence is required. If the mobility features available in Lync Server 2010 CU4 & later are used, then cookie persistence is required. In this case, 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.

**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 Web Services**

A Reverse Proxy server in the perimeter network is required in to enable external access to the Lync Server Web Services. 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.

**Reverse Proxy Options**

The options for the Reverse Proxy include:

- Microsoft TMG 2010 (now discontinued), for configuration details click [here](#).
- Microsoft IIS with AAR (Application Request Routing), for configuration details click [here](#).
- Defining additional VIPs on the load balancer pair located in the DMZ, please refer to section 2 in the Appendix for more details

**ADDITIONAL DETAILS**

For additional details please refer to the following Microsoft Technet article:
Load Balancing Lync

Reverse Proxy Servers:


Lync Load Balancing Requirements:


Components Required for External User Access:


9. Load Balanced Ports/Protocols

FRONT END SERVERS

REQUAED

<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 Attendant (dial in conferencing</td>
</tr>
</tbody>
</table>
### Load Balanced Ports/Protocols

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>5269</td>
<td>TCP/XMPP</td>
<td>XMPP Proxy service <em>(Lync 2013 only)</em></td>
</tr>
</tbody>
</table>
10. Deployment Architecture

LOADBALANCER.ORG TEST ENVIRONMENT

**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

**Note:**

N.B. this Reverse Proxy functionality can also be achieved using additional VIPs defined on clustered pair 2 as shown on page 43 in the Appendix.

For further details on server port requirements please also refer to the following Microsoft links:
Deployment Architecture

- 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

Notes:

- The load balancers are deployed in two-arm mode, but this can changed if desired depending on your network topology – see page 13 for more details

ONE-ARM VS TWO-ARM

The options available depend on the load balancing method used and the network topology. In this guide services are deployed using both layer 7 SNAT mode and layer 4 NAT mode.

Layer 7 SNAT Mode

For layer 7 services, both one-arm and two-arm can be used without any problem. This is because layer 7 works as a reverse proxy and client requests are always comprised of 2 connections, i.e.:

Client <----- Load Balancer
and
Load Balancer <----- Back-end Server

Therefore, clients can be located on the same subnet as the Load balancer or on a different subnet or network without any issue, provided that network routing is configured correctly.

Layer 4 NAT Mode

For Layer 4 NAT mode, unlike layer 7 SNAT mode, the client source IP address is maintained right through to the servers (i.e. it’s transparent). This means that the client location must be considered to ensure that NAT mode works correctly. The main point to consider is that return traffic from server to client must pass via the load balancer.

For a two-arm configuration where clients are located in the same subnet as one arm of the load balancer, and the load balanced servers are located on the same subnet as the other arm of the load balancer, the load balanced servers default gateway must be set to be the load balancer and everything will work.

For a one-arm configuration, it depends where the clients are located in relation to the load balanced servers. One-arm layer 4 NAT mode for Lync will only work if the clients are located in remote subnets/networks, and the default gateway on the load balanced servers is set to be the load balancer. If clients are located on the same subnet as the load balanced servers, this will not work.

This Deployment Guide

In this guide, both load balancer pairs are deployed in two-arm mode.
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 page 25 for details on setting up SSL Offload, cookie insertion and SSL re-encryption
DIRECTOR 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 page 31 for details on setting up SSL Offload, cookie insertion and SSL re-encryption
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: 192.168.10.0/24 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
  ◦ and to the router/firewall: 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
**EXTERNAL EDGE – THE DETAILS**

**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
- Microsoft recommend that 3 Public IP’s are used for the external edge services. Please refer to the following URL: [http://technet.microsoft.com/en-us/library/jj205025.aspx](http://technet.microsoft.com/en-us/library/jj205025.aspx)
**LYNC TOPOLOGY BUILDER**

The image below shows the topology layout of the test environment.

---

**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 Service (VIP) created on the load balancer. Additional internal records are also manually added:

- `sipinternaltls._tcp.robtest.com` → `pool1.robtest.com`
- `pool1.robtest.com` → `Enterprise Pool VIP on the load balancer`

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

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

VIRTUAL APPLIANCE DOWNLOAD & DEPLOYMENT

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk. The Virtual Appliance can be downloaded [here](#).

**Note:**
The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance’s WebUI.

**Note:**
Please refer to the [Administration Manual](#) and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

INITIAL NETWORK CONFIGURATION

The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

**Method 1 - Using the Network Setup Wizard at the console**

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

**Method 2 - Using the WebUI**

Using a browser, connect to the WebUI on the default IP address/port: [http://192.168.221:9080](http://192.168.221:9080)

To set the IP address & subnet mask, use: **Local Configuration** > **Network Interface Configuration**

To set the default gateway, use: **Local Configuration** > **Routing**

To configure DNS settings, use: **Local Configuration** > **Hostname & DNS**

**Method 3 - Using Linux commands**

At the console, set the initial IP address using the following command:

```
ip addr add <IP address>/<mask> dev eth0
```

At the console, set the initial default gateway using the following command:

```
route add default gw <IP address> <interface>
```

At the console, set the DNS server using the following command:

```
echo nameserver <IP address> >> /etc/resolv.conf
```

**Note:**
If method 3 is used, you must also configure these settings using the WebUI, otherwise the settings will be lost after a reboot.
ACCESSING THE WEB USER INTERFACE (WEBUI)

The WebUI can be accessed via HTTP at the following URL: \texttt{http://192.168.2.21:9080/lbadmin}

\textit{* Note the port number \texttt{\rightarrow 9080}}

The WebUI can be accessed via HTTPS at the following URL: \texttt{https://192.168.2.21:9443/lbadmin}

\textit{* Note the port number \texttt{\rightarrow 9443}}

\textit{(replace 192.168.2.21 with the IP address of your load balancer if it's been changed from the default)}

Login using the following credentials:

\textbf{Username}: loadbalancer
\textbf{Password}: loadbalancer

\textbf{Note:}
To change the password, use the WebUI menu option: \textit{Maintenance \textgreater Passwords}.

Once logged in, the WebUI will be displayed as shown on the following page:
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page 41.
12. Appliance Configuration for Lync

STEP 1 – CONFIGURE LAYER 7 GLOBAL SETTINGS
To configure the TCP timeouts required by Lync, HAProxy’s client and server timeouts must be changed from their default values of 43 seconds and 45 seconds respectively to 30 minutes. To do this follow the steps below:

1. Using the WebUI, navigate to: Configuration > Layer 7 – Advanced Configuration

   ![Configuration UI](image)

   - Change **Client Timeout** to 1800000 as shown above (i.e. 1800000 ms which is 30 minutes)
     - Note: You can also enter **30m** rather than 1800000
   - Change **Real Server Timeout** to 1800000 as shown above (i.e. 1800000 ms which is 30 minutes)
     - Note: You can also enter **30m** rather than 1800000
   - Click the **Update** button to save the settings

STEP 2 – CONFIGURING THE LOAD BALANCED FRONT END SERVICES

VIRTUAL 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 Protocol</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>None or cookie *</td>
</tr>
<tr>
<td>FePoolExtWebSvcs4443</td>
<td>192.168.20.30</td>
<td>4443</td>
<td>7</td>
<td>Other TCP</td>
<td>None or cookie *</td>
</tr>
</tbody>
</table>

* If only Lync 2013 front-end servers are used, no persistence is required. If 2010 front-end servers are used, then cookie persistence is required. Please refer to the relevant section below.
CONFIGURING THE FRONTENDPOOL VIP

Create the VIP:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Service and click Add a New Virtual Service
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>FrontEndPool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.10.30</td>
</tr>
<tr>
<td>Ports</td>
<td>135,443,444,5061,5065,5069</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
<tr>
<td>Manual Configuration</td>
<td>checkbox checked</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the VIP, e.g. FrontEndPool
4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.10.30
5. Set the Virtual Service Ports field to 135,443,444,5061,5065,5069
6. Set Layer 7 Protocol to TCP Mode
7. Click Update
8. Now click Modify next to the newly created VIP
9. Set the Check Port field to 5061
10. Click Update

Define the Real Servers for the VIP just created:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP
2. 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></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>checkbox unchecked</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

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

CONFIGURING THE FEPOOLEXTWEBSVCS8080 VIP

Note:
Persistence is not required for external web services when only using Lync 2013 Front-end Servers, it is only required when the mobility features available in Lync Server 2010 CU4 & later are used. However, for simplicity the VIP configuration below has this enabled. As mentioned here, this has no negative impact. If you only have Lync 2013 servers, you can disable this if preferred by modifying the VIP and setting persistence to ‘none’.

Create the VIP:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Service and click Add a New Virtual Service
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>FePoolExtWebSvcs8080</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.20.30</td>
</tr>
<tr>
<td>Ports</td>
<td>8080</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>HTTP Mode</td>
</tr>
<tr>
<td>Manual Configuration</td>
<td></td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the VIP, e.g. FePoolExtWebSvcs8080
4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.20.30
5. Set the Virtual Service Ports field to 8080
6. Set Layer 7 Protocol to HTTP Mode
7. Click Update

Define the Real Servers for the VIP just created:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP
2. Enter the following details:
Appliance Configuration for Lync

3. Enter an appropriate label for the RIP, e.g. **FE-1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.10.31**
5. Set the **Real Server Port** field to **8080**
6. Click **Update**
7. Repeat the above steps to add your other Front End Server(s)

**CONFIGURING THE FEPOOLEXTWEBSVCS4443 VIP**

**Note:**
Persistence is not required for external web services when only using Lync 2013 Front-end Servers, it is only required when the mobility features available in Lync Server 2010 CU4 & later are used.

**Lync 2013**
Follow this procedure if you have only Lync 2013 front-end servers in your deployment.

**Create the VIP:**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Service* and click **Add a New Virtual Service**
2. Enter the following details:

   ![Virtual Service Configuration](image)

   3. Enter an appropriate label for the VIP, e.g. **FePoolExtWebSvcs4443**
   4. Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.20.30**
5. Set the Virtual Service Ports field to **4443**
6. Set Layer 7 Protocol to **TCP Mode**
7. Click **Update**

**Define the Real Servers for the VIP just created:**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP
2. 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>4443</td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>unchecked</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. **FE-1**
4. Change the Real Server IP Address field to the required IP address, e.g. **192.168.10.31**
5. Set the Real Server Port field to **4443**
6. Click **Update**
7. Repeat the above steps to add your other Front End Server(s)

**Lync 2010**

Follow this procedure if you have any Lync 2010 front-end servers in your deployment.

**Export the Certificate from a Front-End Server & Upload to the load balancer:**

1. Export the SSL Certificate from one of the Front-end Servers in .pfx format
   - Make sure that the private key is included
   - Tick the option ‘Include all certificates in the certification path if possible’
2. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**
3. Select the Upload prepared PEM/PFX file option and enter the required details
4. Click Upload PEM/PFX file

Configure SSL Termination:

1. Using the WebUI, navigate to: Cluster Configuration > SSL Termination and click Add a New Virtual Service
2. Ensure SSL terminator is set to STunnel and enter the following details:

3. Enter an appropriate label for the VIP, e.g. FePoolExtWebSvcs4443
4. Select the required SSL certificate
5. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.20.30
6. Set the Virtual Service Port field to 4443
7. Set the Backend Virtual Service IP Address field to the required IP address, e.g. 192.168.20.30
8. Set the Backend Virtual Service Port field to 8081 (the same port will be used for the layer 7 VIP created below)
9. Other fields can be left at their default values
10. Click Update

Create the VIP:
1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Virtual Service** and click **Add a New Virtual Service**

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>FePoolExtWebSvcs8081</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.20.30</td>
</tr>
<tr>
<td>Ports</td>
<td>8081</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>HTTP Mode</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the VIP, e.g. **FePoolExtWebSvcs8081**
4. Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.20.30**
5. Set the **Virtual Service Ports** field to **8081**
6. Set **Layer 7 Protocol** to **HTTP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created VIP
9. Ensure **Persistence Mode** is set to **HTTP Cookie**
10. Change **HTTP Cookie Name** from **SERVERID** to **MS-WSMAN**
11. Click **Update**

**Define the Real Servers for the VIP just created:**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Real Servers** and click **Add a new Real Server** next to the newly created VIP
2. 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>4443</td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>✔</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. **FE-1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.10.31**
5. Set the **Real Server Port** field to **4443**
6. Click **Update**
7. Click **Modify** next to the new RIP
8. Ensure that **Re-Encrypt to Backend** is enabled (checked)
9. Click Update
10. Repeat the above steps to add your other Front End Server(s)

STEP 3 – CONFIGURING THE LOAD BALANCED DIRECTOR SERVICES

VIRTUAL 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>None or cookie *</td>
</tr>
<tr>
<td>DirPoolExtWebSvcs4443</td>
<td>192.168.20.20</td>
<td>4443</td>
<td>7</td>
<td>Other TCP</td>
<td>None or cookie *</td>
</tr>
</tbody>
</table>

* If only Lync 2013 director servers are used, no persistence is required. If 2010 director servers are used, then cookie persistence is required. Please refer to the relevant section below.

CONFIGURING THE DIRECTORPOOL VIP

Create the VIP:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Services and click Add a New Virtual Service
2. Enter the following details:

![Virtual Service Form]

3. Enter an appropriate label for the VIP, e.g. DirectorPool
4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.10.20
5. Set the Virtual Service Ports field to 5061
6. Change Layer 7 Protocol to TCP Mode
7. Click Update

Define the Real Servers for the VIP just created:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP
2. Enter the following details:
3. Enter an appropriate label for the RIP, e.g. **DIR-1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.10.21**
5. Set the **Real Server Port** field to **5061**
6. Click **Update**
7. Repeat the above steps to add your other Director Server(s)

**CONFIGURING THE DIRPOOLEXTWEBSVCS8080 VIP**

**Note:**
Persistence is not required for external web services when only using Lync 2013 Director Servers, it is only required when the mobility features available in Lync Server 2010 CU4 & later are used. However, for simplicity the VIP configuration below has this enabled. As mentioned here, this has no negative impact. If you only have Lync 2013 servers, you can disable this if preferred by modifying the VIP and setting persistence to ‘none’.

**Create the VIP:**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Virtual Service** and click **Add a New Virtual Service**
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>DirPoolExtWebSvcs8080</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.20.30</td>
</tr>
<tr>
<td>Ports</td>
<td>8080</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>HTTP Mode ▼</td>
</tr>
<tr>
<td>Manual Configuration</td>
<td>□</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the VIP, e.g. **DirPoolExtWebSvcs8080**
4. Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.20.30**
5. Set the **Virtual Service Ports** field to **8080**
6. Set *Layer 7 Protocol* to **HTTP Mode**
7. Click **Update**

**Define the Real Servers for the VIP just created:**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP
2. 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>8080</td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>False</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. **DIR-1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.10.21**
5. Set the *Real Server Port* field to **8080**
6. Click **Update**
7. Repeat the above steps to add your other Director Server(s)

**CONFIGURING THE DIRPOOLEXTWEBSVCS4443 VIP**

**Note:**
Persistence is not required for external web services when only using Lync 2013 Director Servers, it is only required when the mobility features available in Lync Server 2010 CU4 & later are used.

**Lync 2013**
Follow this procedure if you have only Lync 2013 director servers in your deployment.

**Create the VIP:**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Service* and click **Add a New Virtual Service**
2. Enter the following details:
3. Enter an appropriate label for the VIP, e.g. `DirPoolExtWebSvcs4443`
4. Set the `Virtual Service IP address` field to the required IP address, e.g. `192.168.20.30`
5. Set the `Virtual Service Ports` field to `4443`
6. Set `Layer 7 Protocol` to TCP Mode
7. Click Update

**Define the Real Servers for the VIP just created:**

1. Using the WebUI, navigate to: `Cluster Configuration > Layer 7 – Real Servers` and click **Add a new Real Server** next to the newly created VIP
2. Enter the following details:

   ![Real Server 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 `4443`
   - Click Update
   - Repeat the above steps to add your other director Server(s)
**Lync 2010**  
Follow this procedure if you have any Lync 2010 director servers in your deployment.

*Export the Certificate from a Front-End Server & Upload to the load balancer:*

1. Export the SSL Certificate from one of the Front-end Servers in .pfx format
   - Make sure that the private key is included
   - Tick the option 'Include all certificates in the certification path if possible'

2. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificate* and click *Add a new SSL Certificate*

   ![Add a new SSL Certificate](image)

   3. Select the Upload prepared PEM/PFX file option and enter the required details
   4. Click *Upload PEM/PFX file*

*Configure SSL Termination:*

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Termination* and click *Add a New Virtual Service*

2. Ensure SSL terminator is set to STunnel and enter the following details:

   ![SSL Termination Configuration](image)
### Appliance Configuration for Lync

3. Enter an appropriate label for the VIP, e.g. `DirPoolExtWebSvcs4443`
4. Select the required SSL certificate
5. Set the Virtual Service IP Address field to the required IP address, e.g. `192.168.20.20`
6. Set the Virtual Service Port field to `4443`
7. Set the Backend Virtual Service IP Address field to the required IP address, e.g. `192.168.20.20`
8. Set the Backend Virtual Service Port field to `8081` (the same port will be used for the layer 7 VIP created below)
9. Other fields can be left at their default values
10. Click Update

### Create the VIP:

1. Using the WebUI, navigate to: `Cluster Configuration > Layer 7 – Virtual Service` and click **Add a New Virtual Service**
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>FePoolExtWebSvcs8081</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.20.30</td>
</tr>
<tr>
<td>Ports</td>
<td>8081</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>HTTP Mode</td>
</tr>
<tr>
<td>Manual Configuration</td>
<td>No</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the VIP, e.g. `FePoolExtWebSvcs8081`
4. Set the Virtual Service IP address field to the required IP address, e.g. `192.168.20.30`
5. Set the Virtual Service Ports field to `8081`
6. Set Layer 7 Protocol to **HTTP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created VIP
9. Ensure Persistence Mode is set to **HTTP Cookie**
10. Change HTTP Cookie Name from **SERVERID** to **MS-WSMAN**
11. Click **Update**

### Define the Real Servers for the VIP just created:

1. Using the WebUI, navigate to: `Cluster Configuration > Layer 7 – Real Servers` and click **Add a new Real Server** next to the newly created VIP
2. Enter the following details:
3. Enter an appropriate label for the RIP, e.g. **FE-1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.10.31**
5. Set the **Real Server Port** field to **4443**
6. Click **Update**
7. Click **Modify** next to the new RIP
8. Ensure that **Re-Encrypt to Backend** is enabled (checked)
9. Click **Update**
10. Repeat the above steps to add your other Director Server(s)

**STEP 4 – CONFIGURING THE LOAD BALANCED EDGE POOL SERVICES (INTERNAL)**

**VIRTUAL 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>

**VIRTUAL 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:**

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

**Create the VIP:**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 4 – Virtual Services** and click **Add a New Virtual Service**
2. Enter the following details:

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

3. Enter an appropriate label for the VIP, e.g. **IntEdgeAccess5061**
4. Change the **Virtual Service IP address** field to the required IP address, e.g. **192.168.10.10**
5. Set the **Virtual Service Ports** field to **5061**
6. Leave **Protocol** set to **TCP**
7. Change the **Forwarding Method** to **NAT**
8. Click **Update**
9. Now click **Modify** next to the newly created VIP
10. Change **Persistence Timeout** to **1800**
11. Click **Update**

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

**REAL SERVER (RIP) CONFIGURATION**

Real Servers (RIPs) must now be defined for each VIP created.

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created VIP
2. 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>192.168.10.10</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>5061</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. **EDGE-1**
4. Change the **Real Server IP Address** to the required IP address, e.g. **192.168.100.10**
5. Set the **Real Server Port** field to **5061**
6. Click **Update**
7. Repeat the above steps to add your other Edge Server(s)

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

**STEP 5 – CONFIGURING THE LOAD BALANCED EDGE POOL SERVICES (EXTERNAL)**

**VIRTUAL 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>ExtEdgeAccess5269 (Lync 2013 only)</td>
<td>10.25.1.10</td>
<td>5269</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 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.*

**Note:**
Make sure that you change the protocol for the Audio Visual VIP ‘IntEdgeAv3478’ from the default setting ‘TCP’ to ‘UDP’.

**Create the VIP:**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:
3. Enter an appropriate label for the VIP, e.g. **ExtEdgeAccess443**
4. Change the **Virtual Service IP address** field to the required IP address, e.g. **10.25.1.10**
5. Set the **Virtual Service Ports** field to **443**
6. Leave **Protocol** set to **TCP**
7. Change the **Forwarding Method** to **NAT**

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

### REAL SERVER (RIP) CONFIGURATION

Real Servers (RIPS) must now be defined for each VIP created.

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 4 – Real Servers** and click **Add a new Real Server** next to the newly created VIP
2. 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>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

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

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

### STEP 6 – FINALIZING THE CONFIGURATION

To apply the new settings for the Layer 7 based VIPs and SSL termination VIPs, HAProxy and Stunnel must be restarted as follows:

- Go to **Maintenance > Restart Services** and click **Restart HAProxy**
- Go to **Maintenance > Restart Services** and click **Restart Stunnel**
13. 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 user’s 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 WebUI** – 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/OCS Server Remote Connectivity Analyzer tool is a very useful Web-based Microsoft tool designed to help IT Administrators troubleshoot their Lync deployments. It’s available at the following link: https://testconnectivity.microsoft.com/

LYNC DIAGNOSTICS TOOLS

Microsoft’s Lync Server 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 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:

Note:
To be able to analyze the logs, download and install the Microsoft Lync Server 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 Documentation Hub
http://blogs.technet.com/b/nexthop/

Testing & verifying Lync Edge Server:

Reverse Proxy Concepts & Testing Web Services:

Using ISS ARR as a Reverse Proxy for Lync:

14. Technical Support
If you have any questions regarding the appliance or would like assistance designing your deployment, please don’t hesitate to contact our support team: support@loadbalancer.org.

15. Further Documentation

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

1 – CLUSTERED PAIR CONFIGURATION – ADDING A SLAVE UNIT

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

**Note:**

A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
- Software updates

**Version 7:**

Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

**Version 8:**

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration
• Specify the IP address and the loadbalancer users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above

• Click Add new node

• The pairing process now commences as shown below:

![Create a Clustered Pair](image)

• Once complete, the following will be displayed:

![High Availability Configuration - Master](image)

• To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen

Note:
Clicking the Restart Heartbeat button on the master appliance will also automatically restart heartbeat on the slave appliance.

Note:
Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
2 – CONFIGURE REVERSE PROXY VIPs

If required, additional VIPs can be defined on the load balancer pair in the DMZ which can be used in place of a full Reverse Proxy such as TMG. The VIPs are used to translate ports from 80/443 to 8080/4443.

Front-end Server Reverse Proxy HTTP VIP

Create the VIP:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Service and click Add a New Virtual Service
2. Enter the following details:

   - Enter an appropriate label for the VIP, e.g. ReverseProxyFE-http
   - Set the Virtual Service IP address field to the required IP address, e.g. 10.12.1.150
   - Set the Virtual Service Ports field to 80
   - Leave Layer 7 Protocol set to HTTP Mode
   - Click Update

Define the Real Servers for the VIP just created:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP
2. Enter the following details:

   - 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 Re-Encrypt to Backend set to 8080
   - Weight: 100
   - Click Update
5. Set the **Real Server Port** field to **8080**
6. Click **Update**
7. Repeat the above steps to add your other Front End Server(s)

**Front-end Server Reverse Proxy HTTPS VIP**

**Create the VIP:**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Virtual Service** and click **Add a New Virtual Service**
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>ReverseProxyFE-https</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>10.12.1.150</td>
</tr>
<tr>
<td>Ports</td>
<td>443</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
<tr>
<td>Manual Configuration</td>
<td></td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the VIP, e.g. **ReverseProxyFE-https**
4. Set the **Virtual Service IP address** field to the required IP address, e.g. **10.12.1.150**
5. Set the **Virtual Service Ports** field to **443**
6. Set **Layer 7 Protocol** to **TCP Mode**
7. Click **Update**

**Define the Real Servers for the VIP just created:**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Real Servers** and click **Add a new Real Server** next to the newly created VIP
2. 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>4443</td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. **FE-1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.10.31**
5. Set the *Real Server Port* field to **443**
6. Click **Update**
7. Repeat the above steps to add your other Front End Server(s)

**Director Server Reverse Proxy HTTP & HTTPS VIPs**
Repeat the steps above to create similar VIPs/RIPs for the Director Server Web Services.
## 3 - COMPANY CONTACT INFORMATION

<table>
<thead>
<tr>
<th>Website</th>
<th>URL: <a href="http://www.loadbalancer.org">www.loadbalancer.org</a></th>
</tr>
</thead>
</table>

### North America (US)
- **Loadbalancer.org, Inc.**
  - 4550 Linden Hill Road, Suite 201
  - Wilmington, DE 19808
  - USA
- **Tel:** +1 833.274.2566
- **Email (sales):** [sales@loadbalancer.org](mailto:sales@loadbalancer.org)
- **Email (support):** [support@loadbalancer.org](mailto:support@loadbalancer.org)

### North America (Canada)
- **Loadbalancer.org Appliances Ltd.**
  - 300-422 Richards Street
  - Vancouver, BC
  - V6B 2Z4
  - Canada
- **Tel:** +1 302.213.0122
- **Email (sales):** [sales@loadbalancer.org](mailto:sales@loadbalancer.org)
- **Email (support):** [support@loadbalancer.org](mailto:support@loadbalancer.org)

### Europe (UK)
- **Loadbalancer.org Ltd.**
  - Compass House
  - North Harbour Business Park
  - Portsmouth, PO6 4PS
  - UK
- **Tel:** +44 (0)330 380 1064
- **Email (sales):** [sales@loadbalancer.org](mailto:sales@loadbalancer.org)
- **Email (support):** [support@loadbalancer.org](mailto:support@loadbalancer.org)

### Europe (Germany)
- **Loadbalancer.org GmbH**
  - Tengstraße 27
  - 80798 München
  - Germany
- **Tel:** +49 (0)89 2000 2179
- **Email (sales):** [vertrieb@loadbalancer.org](mailto:vertrieb@loadbalancer.org)
- **Email (support):** [support@loadbalancer.org](mailto:support@loadbalancer.org)