



# Load Balancing Microsoft Lync 2010/2013

v1.8.1

*Deployment Guide*

**NOTE:** This guide has been archived and is no longer being maintained. While the content is still valid for the particular software versions mentioned, it may refer to outdated software that has now reached end-of-life. For more information please contact [support@loadbalancer.org](mailto:support@loadbalancer.org).



---

## Contents

1. About this Guide.....	3
2. Loadbalancer.org Appliances Supported.....	4
3. Loadbalancer.org Software Versions Supported.....	4
4. Microsoft Lync Software Versions Supported.....	4
5. Microsoft Lync.....	4
<i>Microsoft Lync Editions.....</i>	<i>4</i>
Standard Edition.....	5
Enterprise Edition.....	5
6. Microsoft Lync & Loadbalancer.org.....	5
7. Microsoft Lync Server Roles.....	5
8. Load Balancing Lync.....	8
<i>Load Balancing Methods Supported.....</i>	<i>8</i>
DNS Load Balancing.....	8
Hardware Load Balancing (HLB).....	8
<i>Load Balanced Roles.....</i>	<i>8</i>
<i>Loadbalancer.org Appliance Considerations.....</i>	<i>9</i>
Load Balancer Deployment Mode.....	9
Persistence (aka Server Affinity).....	9
TCP Timeout Settings.....	10
Reverse Proxy Server.....	10
<i>Additional Details.....</i>	<i>10</i>
9. Load Balanced Ports/Protocols.....	11
<i>Front End Servers.....</i>	<i>11</i>
Required.....	11
Optional.....	11
<i>Director Servers.....</i>	<i>12</i>
Required.....	12
Optional.....	12
<i>Edge Servers (Internal Access).....</i>	<i>12</i>
<i>Edge Servers (External Access).....</i>	<i>12</i>
10. Deployment Architecture.....	13
<i>Loadbalancer.org test Environment.....</i>	<i>13</i>
<i>One-arm Vs Two-arm.....</i>	<i>14</i>
<i>Front End Pool – the Details.....</i>	<i>15</i>
<i>Director Pool – the Details.....</i>	<i>16</i>
<i>Internal Edge – the Details.....</i>	<i>17</i>
<i>External Edge – the Details.....</i>	<i>18</i>
<i>Lync Topology Builder.....</i>	<i>19</i>
<i>DNS Configuration.....</i>	<i>19</i>
11. Loadbalancer.org Appliance – the Basics.....	21
<i>Virtual Appliance Download &amp; Deployment.....</i>	<i>21</i>
<i>Initial Network Configuration.....</i>	<i>21</i>
<i>Accessing the Web User Interface (WebUI).....</i>	<i>21</i>

---

HA Clustered Pair Configuration.....	23
12. Appliance Configuration for Lync.....	24
STEP 1 – Configure Layer 7 Global Settings.....	24
STEP 2 – Configuring the Load Balanced Front End Services.....	24
Virtual Service (VIP) List.....	24
Configuring the FrontEndPool VIP.....	25
Configuring the FePoolExtWebSvcs8080 VIP.....	26
Configuring the FePoolExtWebSvcs4443 VIP.....	27
STEP 3 – Configuring the Load Balanced Director Services.....	31
Virtual Service (VIP) List.....	31
Configuring the DirectorPool VIP.....	31
Configuring the DirPoolExtWebSvcs8080 VIP.....	33
Configuring the DirPoolExtWebSvcs4443 VIP.....	34
STEP 4 – Configuring the Load Balanced Edge Pool Services (Internal).....	38
Virtual Service (VIP) List.....	38
Virtual Service (VIP) Configuration.....	38
Real Server (RIP) Configuration.....	39
STEP 5 – Configuring the Load Balanced Edge Pool Services (External).....	40
Virtual Service (VIP) List.....	40
Virtual Service (VIP) Configuration.....	40
Real Server (RIP) Configuration.....	41
STEP 6 – Finalizing the Configuration.....	42
13. Testing & Validation.....	43
Client connections bypass the load balancer.....	43
Taking Servers Offline.....	43
Microsoft Lync Testing Tool.....	43
Lync Diagnostics Tools.....	43
Wireshark Protocol Analyzer.....	44
Other Useful Resources.....	44
14. Technical Support.....	44
15. Further Documentation.....	44
16. Conclusion.....	45
17. Appendix.....	46
1 – Clustered Pair Configuration – Adding a Slave Unit.....	46
2 – Configure Reverse Proxy VIPs.....	48
18. Document Revision History.....	51

## 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:

Discontinued Models	Current Models *
Enterprise VA	Enterprise MAX
Enterprise R320	Enterprise 10G
	Enterprise 40G
	Enterprise Ultra
	Enterprise VA MAX
	Enterprise AWS **
	Enterprise AZURE **
	Enterprise GCP **

\* For full specifications of these models please refer to: <http://www.loadbalancer.org/products/hardware>

\*\* Some features may not be supported, please check with Loadbalancer.org support

## 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.

Role	Details
Front End Server	<p><b>Purpose:</b> 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.</p> <p><b>Scalability:</b> Each front end server can support up to 10,000 users. When configured in a pool, up to 80,000 users are supported.</p> <p><b>High Availability:</b> Use a pool of servers with a load balancer.</p>
Back End Server	<p><b>Purpose:</b> The back-end SQL Server hosts various databases to keep track of Lync's configuration and state information.</p> <p><b>Scalability:</b> Microsoft recommends using an SQL cluster for high availability.</p> <p><b>High Availability:</b> Use clustering/Mirroring techniques.</p>
A/V Conferencing Server	<p><b>Purpose:</b> Provides Audio/Visual conferencing functionality to Lync clients.</p>

	<p><b>Scalability:</b> Microsoft recommends a separate dedicated server for more than 10,000 users. Each dedicated A/V server supports up to 20,000 users.</p> <p><b>High Availability:</b> Use a pool of servers (no load balancer is required).</p> <p><b>Co-location:</b> By default this role is co-located with the Front End Server, but can also be deployed separately.</p>
Edge Server	<p><b>Purpose:</b> 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!.</p> <p><b>Scalability:</b> 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.</p> <p><b>High Availability:</b> Use a pool of servers with a load balancer.</p>
Mediation Server	<p><b>Purpose:</b> 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.</p> <p><b>Scalability:</b> A dedicated Mediation Server supports up to 1200 users. Co-located with a Front End Server, it supports up to 226 users.</p> <p><b>High Availability:</b> Use a pool of servers with a load balancer.</p> <p><b>Co-location:</b> 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.</p>
Monitoring Server	<p><b>Purpose:</b> 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.</p> <p><b>Scalability:</b> 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.</p> <p><b>High Availability:</b> Use a standby server (messages are queued on the Front-End servers if a failure occurs).</p>

	<p><b>Co-location:</b> Can be co-located with Archiving Server.</p>
Archiving Server	<p><b>Purpose:</b> 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.</p> <p><b>Scalability:</b> 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.</p> <p><b>High Availability:</b> Use a standby server (messages are queued on the Front-End servers if a failure occurs).</p> <p><b>Co-location:</b> Can be co-located with Monitoring Server.</p>
Director Server	<p><b>Purpose:</b> 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.</p> <p><b>Scalability:</b> One Director for every 15,000 users who will access a site remotely. As a minimum, Microsoft recommend two Directors for high availability.</p> <p><b>High Availability:</b> Use a pool of servers with a load balancer.</p>



---

## 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 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.



---

## 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:

Load Balanced Pools	Supported Modes	Notes
Enterprise Pools	Full-NAT	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.
Edge Pools	Full-NAT & Half-NAT	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).

### 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:

#### *Reverse Proxy Servers:*

2010: [https://technet.microsoft.com/en-us/library/gg398069\(v=ocs.14\).aspx](https://technet.microsoft.com/en-us/library/gg398069(v=ocs.14).aspx)

2013: [https://technet.microsoft.com/en-us/library/gg398069\(v=ocs.15\).aspx](https://technet.microsoft.com/en-us/library/gg398069(v=ocs.15).aspx)

#### *Lync Load Balancing Requirements:*

2010: [https://technet.microsoft.com/en-us/library/gg615011\(v=ocs.14\).aspx](https://technet.microsoft.com/en-us/library/gg615011(v=ocs.14).aspx)

2013: [https://technet.microsoft.com/en-us/library/gg615011\(v=ocs.15\).aspx](https://technet.microsoft.com/en-us/library/gg615011(v=ocs.15).aspx)

---

### Components Required for External User Access:

2010: [https://technet.microsoft.com/en-us/library/gg425779\(v=ocs.14\).aspx](https://technet.microsoft.com/en-us/library/gg425779(v=ocs.14).aspx)

2013: [https://technet.microsoft.com/en-us/library/gg425779\(v=ocs.15\).aspx](https://technet.microsoft.com/en-us/library/gg425779(v=ocs.15).aspx)

## 9. Load Balanced Ports/Protocols

### Front End Servers

#### Required

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

#### Optional

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

		TURN traffic
--	--	--------------

## Director Servers

### Required

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

### Optional

Port	Protocols	Use
5060	TCP/SIP	Unsecured SIP Traffic

## Edge Servers (Internal Access)

Port	Protocols	Use
443	TCP/STUN	Audio/Visual service
3478	UDP/STUN	Audio/Visual service
5061	TCP/MTLS/SIP	Access (SIP proxy) service
5062	TCP/MTLS/SIP	Audio/Visual authentication service
8057	TCP/MTLS	Web Conferencing

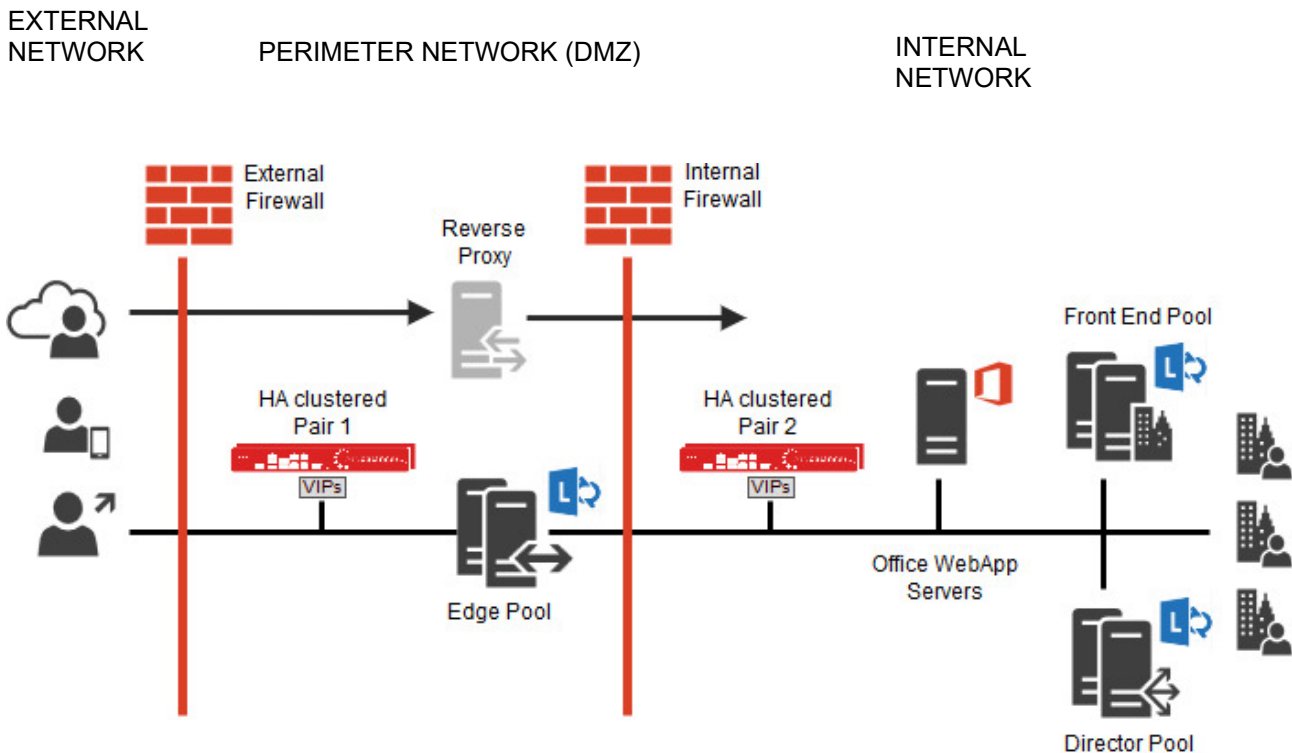
## Edge Servers (External Access)

Port	Protocols	Use
443	TCP/TLS/STUN/SIP	Access (SIP proxy), Web Conferencing, Audio/Visual services
3478	UDP/STUN	Audio/Visual service
5061	TCP/MTLS/SIP	Access (SIP proxy) service
5269	TCP/XMPP	XMPP Proxy service ( <i>Lync 2013 only</i> )

Note: For further details on server port requirements please also refer to the following Microsoft links:  
 For Front End & Director Servers: <http://technet.microsoft.com/en-us/library/gg398833.aspx>  
 For Edge Servers: <http://technet.microsoft.com/en-us/library/gg398739.aspx>

## 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: this Reverse Proxy functionality can also be achieved using additional VIPs defined on clustered pair 2 as shown on page [48](#) in the Appendix.

- 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 be changed if desired depending on your network topology – see page [14](#) 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.

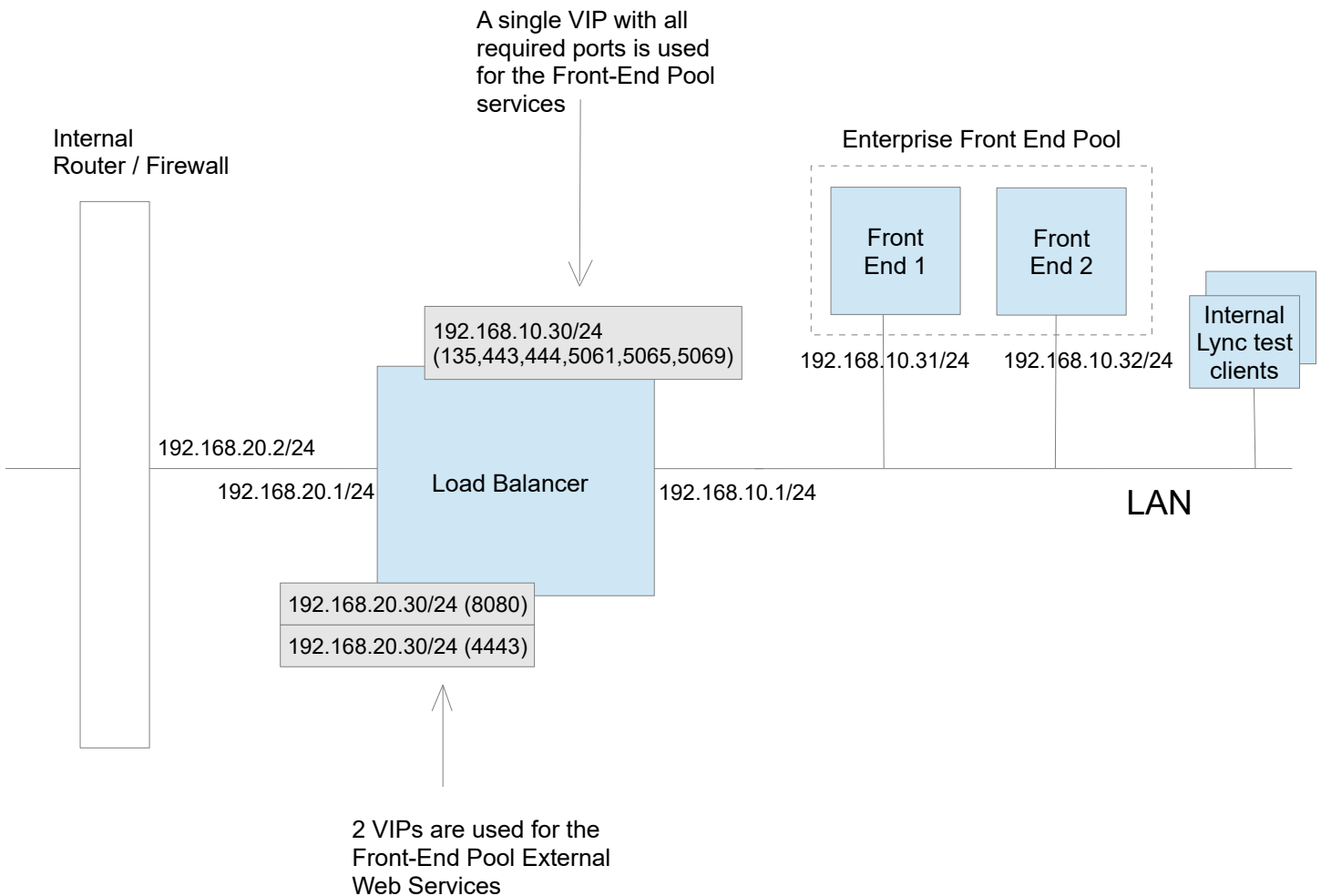
For a two-arm configuration where clients are located in the same subnet as one arm of the load balancer, and the load balanced servers are located on the same subnet as the other arm of the load balancer, the load balanced servers default gateway must be set to be the load balancer and everything will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

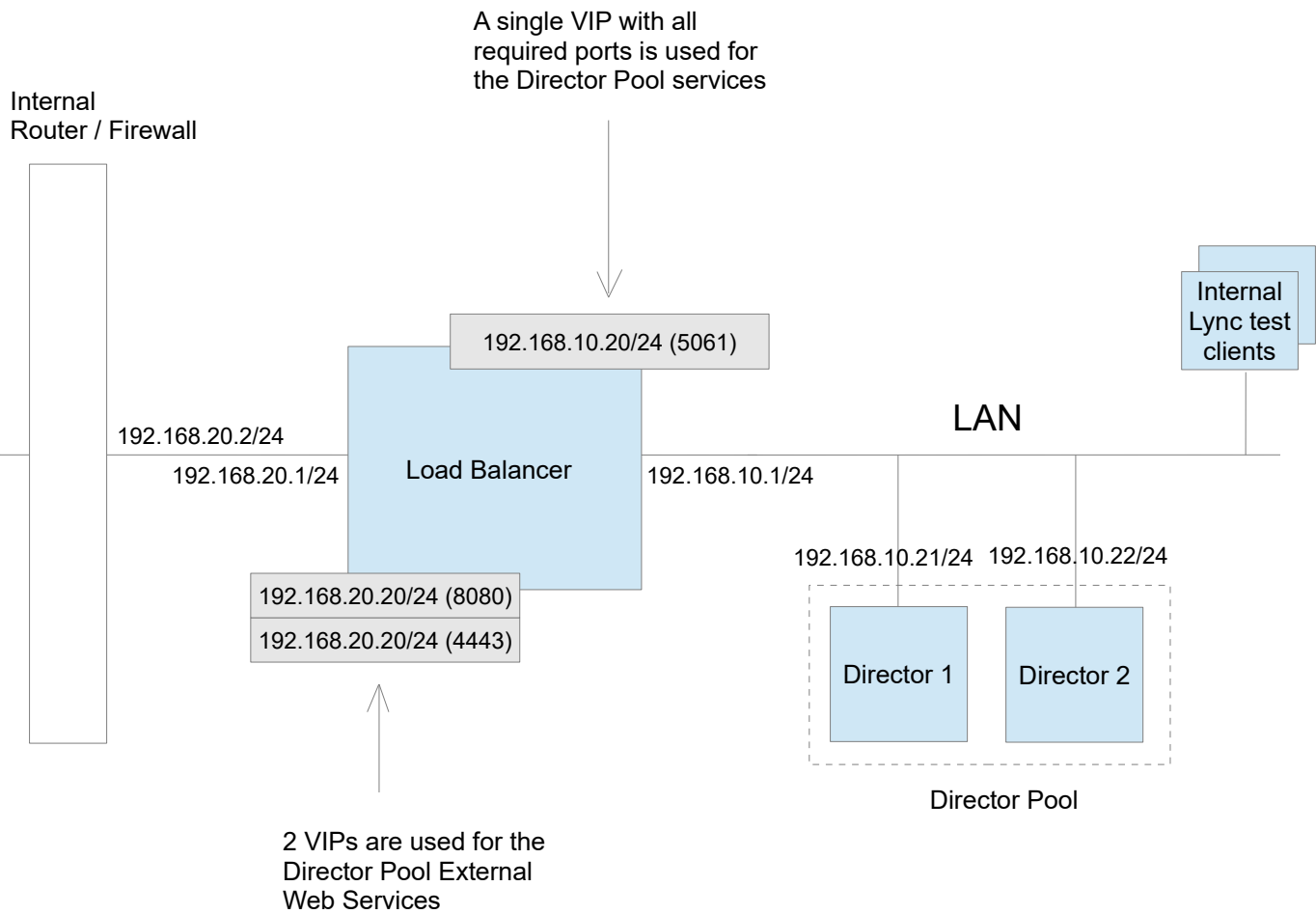


#### NOTES:

- 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 [27](#) for details on setting up SSL Offload, cookie insertion and SSL re-encryption



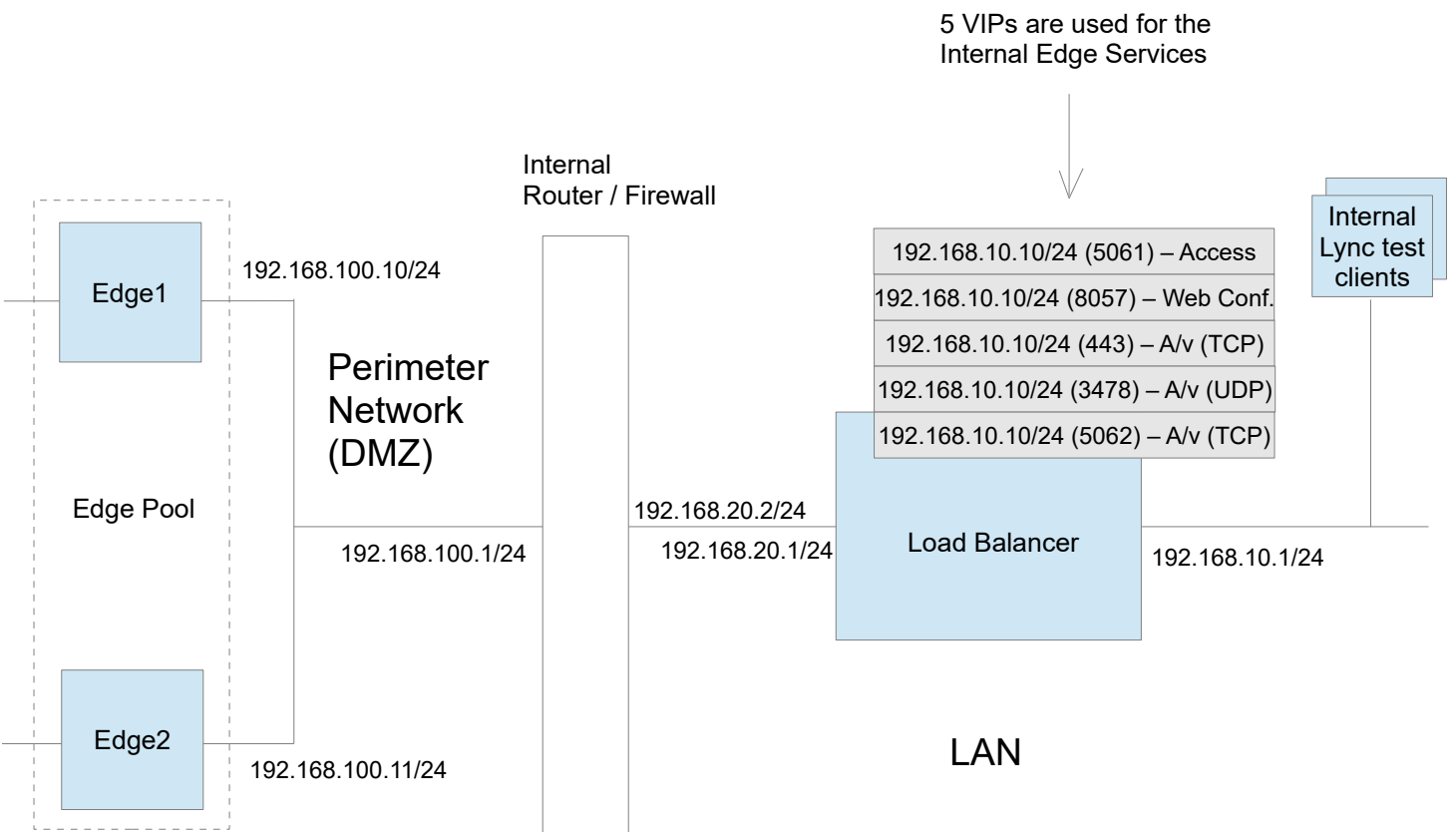
## Director Pool – the Details



### 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 [34](#) for details on setting up SSL Offload, cookie insertion and SSL re-encryption

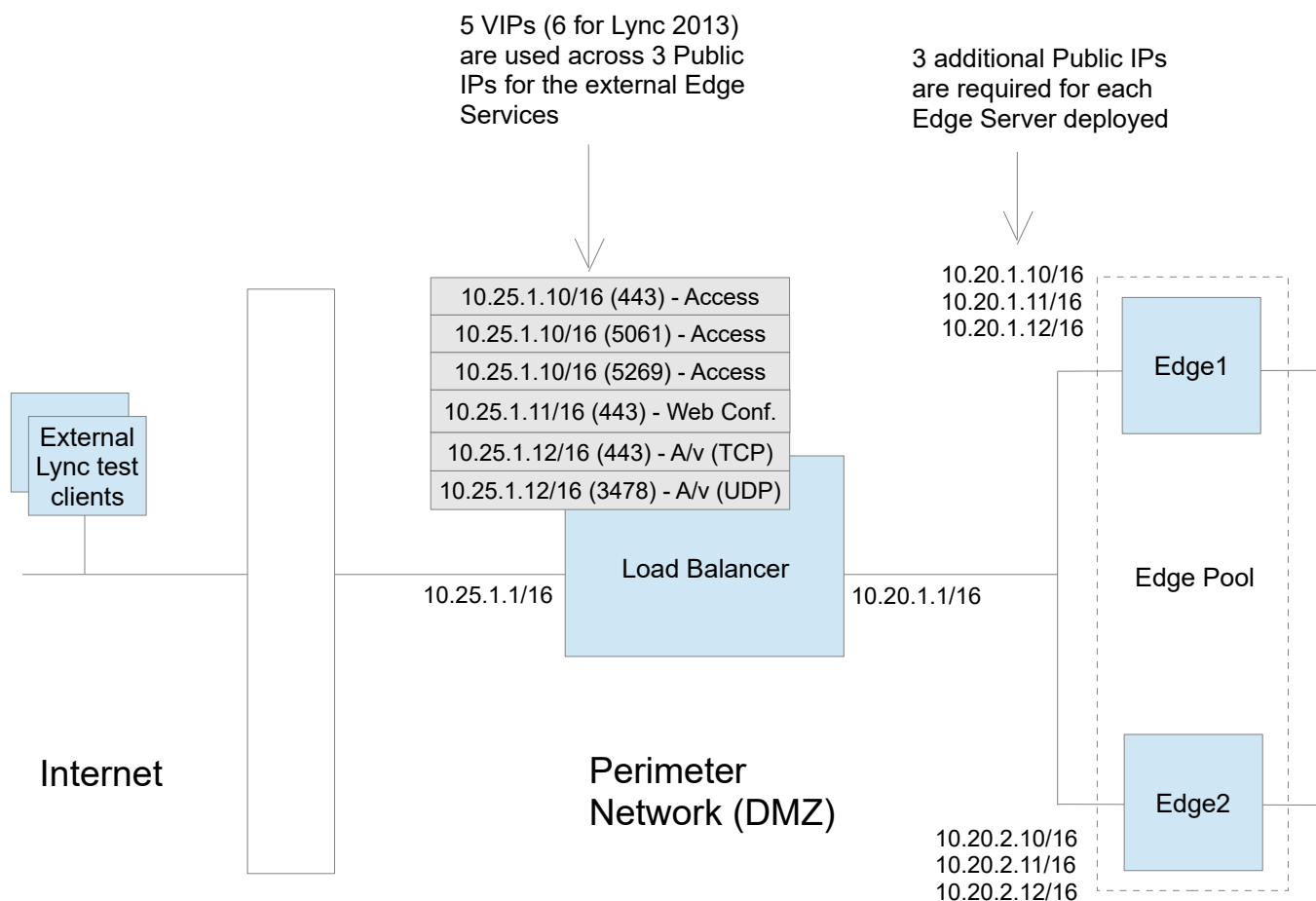
## Internal Edge – the Details



### 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:
      - 192.168.100.0/24 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
  - 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

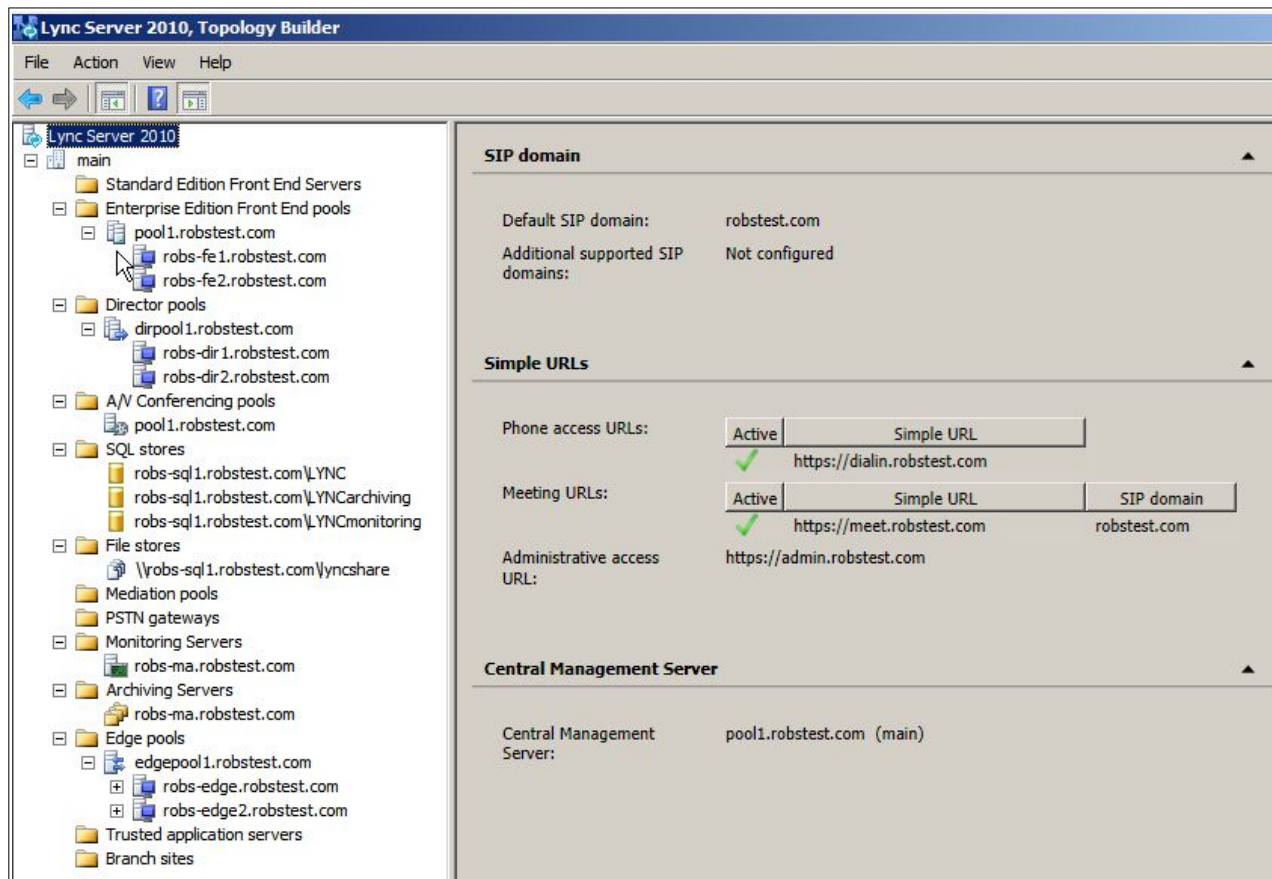


### NOTES:

- 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>

## 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.robstest.com	→	points to the reverse-proxy (Director Pool)
admin.robstest.com	→	points to the reverse-proxy (Front End Pool)
pool1.robstest.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://192.168.2.21:9443**

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*

### Accessing the Web User Interface (WebUI)

1. Browse to the following URL: **https://192.168.2.21:9443/lbadmin/**  
(replace with your IP address if it's been changed)  
\* Note the port number → **9443**

2. Login to the WebUI:

**Username:** loadbalancer

---

**Password:** loadbalancer

Note: To change the password , use the WebUI menu option: *Maintenance > Passwords*.

Once logged in, the WebUI will be displayed as shown below:




## SYSTEM OVERVIEW

2015-06-18 14:21:20 UTC

Would you like to run the Setup Wizard?

Accept


Dismiss

VIRTUAL SERVICE 

IP 

PORTS 

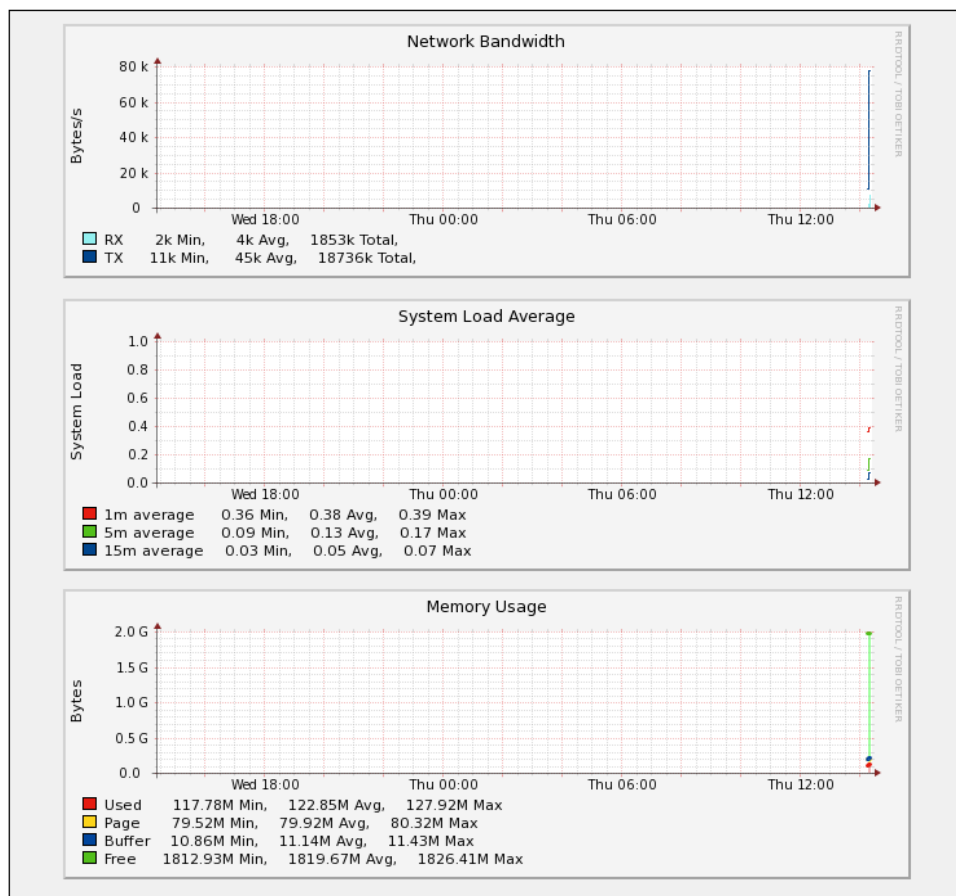
CONNS 

PROTOCOL 

METHOD 

MODE 

No Virtual Services configured.



## HA Clustered Pair Configuration

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 [46](#).

## 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*

Lock HAProxy Configuration (Deprecated)	<input type="checkbox"/>	?
Logging	<input type="checkbox"/>	?
Log Only Errors	<input type="checkbox"/>	?
Redispatch	<input checked="" type="checkbox"/>	?
Connection Timeout	4000 ms	?
Client Timeout	1800000 ms	?
Real Server Timeout	1800000 ms	?

2. 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*
3. 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*
4. 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:

VIP Name (Label)	IP Address	Port(s)	Layer	Layer 7 Protocol	Persistence Method
FrontEndPool	192.168.10.30	135, 443, 444, 5061, 5065, 5069	7	Other TCP	Source IP address
FePoolExtWebSvcs8080	192.168.20.30	8080	7	Other TCP	None or cookie *
FePoolExtWebSvcs4443	192.168.20.30	4443	7	Other TCP	None or cookie *

\* 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:

Label	FrontEndPool	?	
Virtual Service	IP Address	192.168.10.30	?
	Ports	135,443,444,5061,5065,5069	?
Layer 7 Protocol	TCP Mode	▼	?
Manual Configuration	<input type="checkbox"/>		?
		Cancel	Update

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. Under the *Health Checks* section click **Advanced** to expand the section
10. Set the *Check Port* field to **5061**
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:

Label	<input type="text" value="FE-1"/>	?
Real Server IP Address	<input type="text" value="192.168.10.31"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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:

Label	<input type="text" value="FePoolExtWebSvcs8080"/>		?
Virtual Service	IP Address	<input type="text" value="192.168.20.30"/>	?
	Ports	<input type="text" value="8080"/>	?
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>		?
Manual Configuration	<input type="checkbox"/>		?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

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:

Label	<input type="text" value="FE-1"/>	?
Real Server IP Address	<input type="text" value="192.168.10.31"/>	?
Real Server Port	<input type="text" value="8080"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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:

**Layer 7 - Add a new Virtual Service**

**Virtual Service**

Manual Configuration ☐ ?

Label  ?

IP Address  ?

Ports  ?

**Protocol**

Layer 7 Protocol  ?

**Cancel** **Update**

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:

Label  ?

Real Server IP Address  ?

Real Server Port  ?

Re-Encrypt to Backend ☐ ?

Weight  ?

**Cancel** **Update**

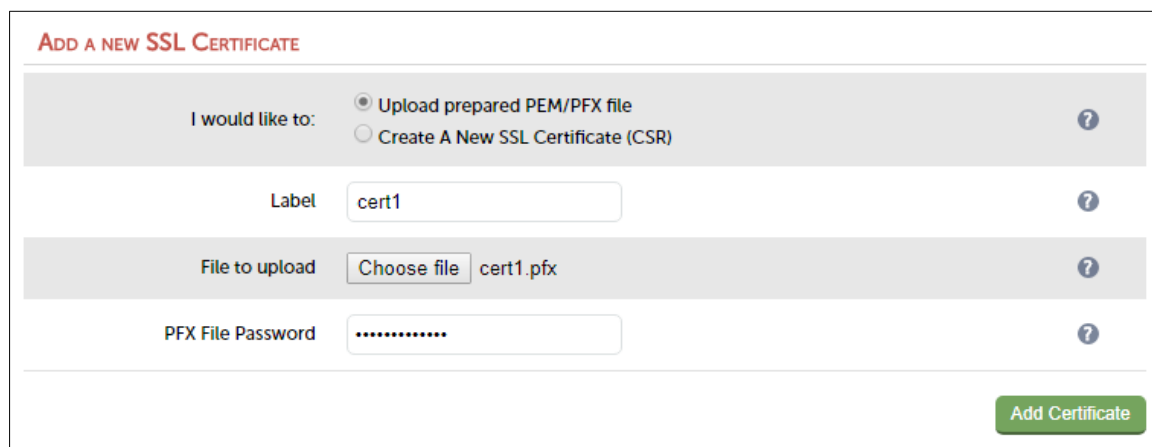
3. Enter an appropriate label for the RIP, e.g. **FE-1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.10.31**
5. Set the *Real Server Port* field to **4443**
6. Click **Update**
7. Repeat the above steps to add your other Front End Server(s)

## 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**



The screenshot shows a web form titled "ADD A NEW SSL CERTIFICATE". It contains the following fields and options:

- I would like to:** Two radio button options: "Upload prepared PEM/PFX file" (selected) and "Create A New SSL Certificate (CSR)".
- Label:** A text input field containing "cert1".
- File to upload:** A "Choose file" button followed by the filename "cert1.pfx".
- PFX File Password:** A password input field with masked characters (dots).
- Add Certificate:** A green button at the bottom right of the form.

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. Select the appropriate VIP from the *Associated Virtual Service* drop-down menu, e.g. **FePoolExtWebSvcs4443**
3. Set the *Virtual Service Port* field to **4443**
4. Select the required SSL certificate
5. Click **Update**



### SSL Termination - Add a new Virtual Service

Label	SSL-FePoolExtWebSvcs4443	?
Associated Virtual Service	FePoolExtWebSvcs4443	?
Virtual Service Port	4443	?
SSL Operation Mode	High Security	?
SSL Certificate	Default Self Signed Certificate	?

Cancel
Update

Create the VIP:

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

Label	FePoolExtWebSvcs8081	?
Virtual Service	IP Address	192.168.20.30
	Ports	8081
Layer 7 Protocol	HTTP Mode	?
Manual Configuration	<input type="checkbox"/>	?

Cancel
Update

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

Label	<input type="text" value="FE-1"/>	?
Real Server IP Address	<input type="text" value="192.168.10.31"/>	?
Real Server Port	<input type="text" value="4443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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:

VIP Name (Label)	IP Address	Port(s)	Layer	Layer 7 Protocol	Persistence Method
DirectorPool	192.168.10.20	5061	7	Other TCP	Source IP address
DirPoolExtWebSvcs8080	192.168.20.20	8080	7	Other TCP	None or cookie *
DirPoolExtWebSvcs4443	192.168.20.20	4443	7	Other TCP	None or cookie *

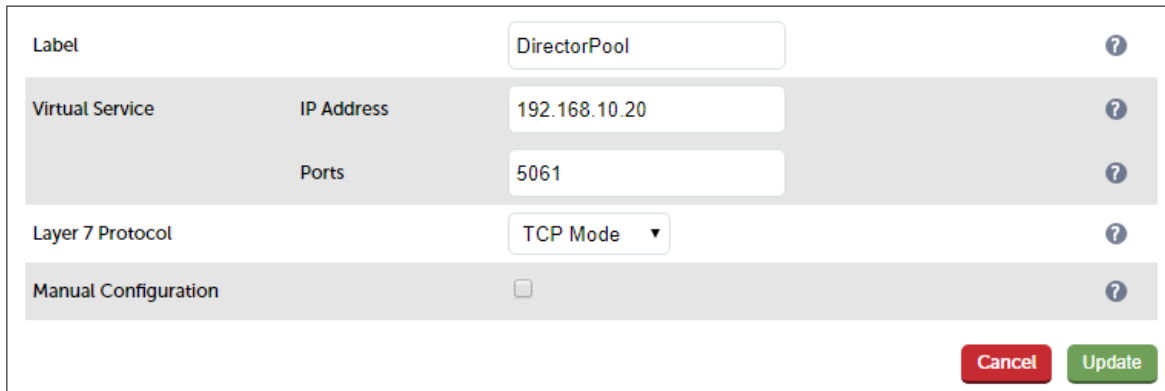
\* If only Lync 2013 director servers are used, no persistence is required. If 2010 director servers are used, then cookie persistence is required. Please refer to the relevant section below.

### 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:



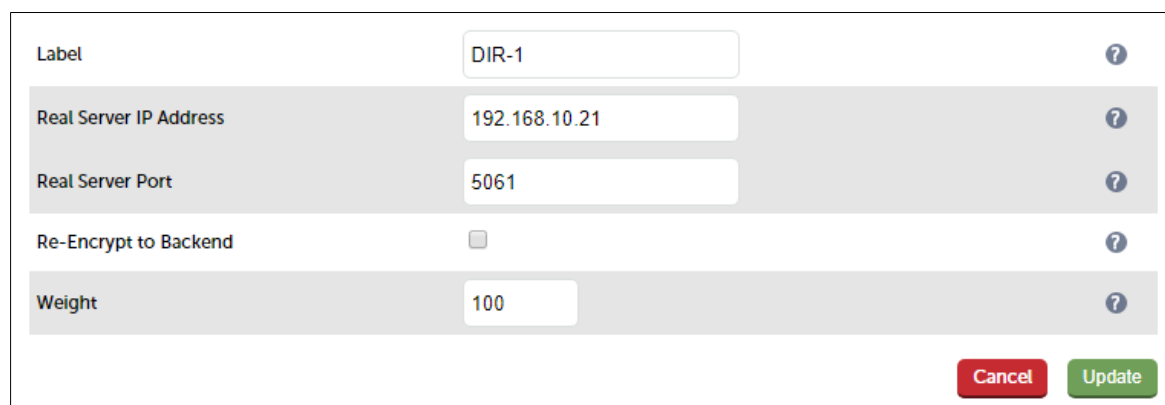
Label	DirectorPool	?	
Virtual Service	IP Address	192.168.10.20	?
	Ports	5061	?
Layer 7 Protocol	TCP Mode	?	
Manual Configuration	<input type="checkbox"/>	?	

Cancel Update

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:



Label	DIR-1	?
Real Server IP Address	192.168.10.21	?
Real Server Port	5061	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	100	?

Cancel Update

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:

Label	DirPoolExtWebSvcs8080		?
Virtual Service	IP Address	192.168.20.30	?
	Ports	8080	?
Layer 7 Protocol	HTTP Mode ▼		?
Manual Configuration	<input type="checkbox"/>		?
			<b>Cancel</b> <b>Update</b>

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:

---

Label	<input type="text" value="DIR-1"/>	?
Real Server IP Address	<input type="text" value="192.168.10.21"/>	?
Real Server Port	<input type="text" value="8080"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

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:

Layer 7 - Add a new Virtual Service

Virtual Service

Manual Configuration
☐
?

Label
?

IP Address
?

Ports
?

Protocol

Layer 7 Protocol
?

Cancel
Update

- Enter an appropriate label for the VIP, e.g. **DirPoolExtWebSvcs4443**
- Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.20.30**
- Set the *Virtual Service Ports* field to **4443**
- Set *Layer 7 Protocol* to **TCP Mode**
- Click **Update**

Define the Real Servers for the VIP just created:

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

Label

?

Real Server IP Address

?

Real Server Port

?

Re-Encrypt to Backend

☐
?

Weight

?

Cancel
Update

- 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)

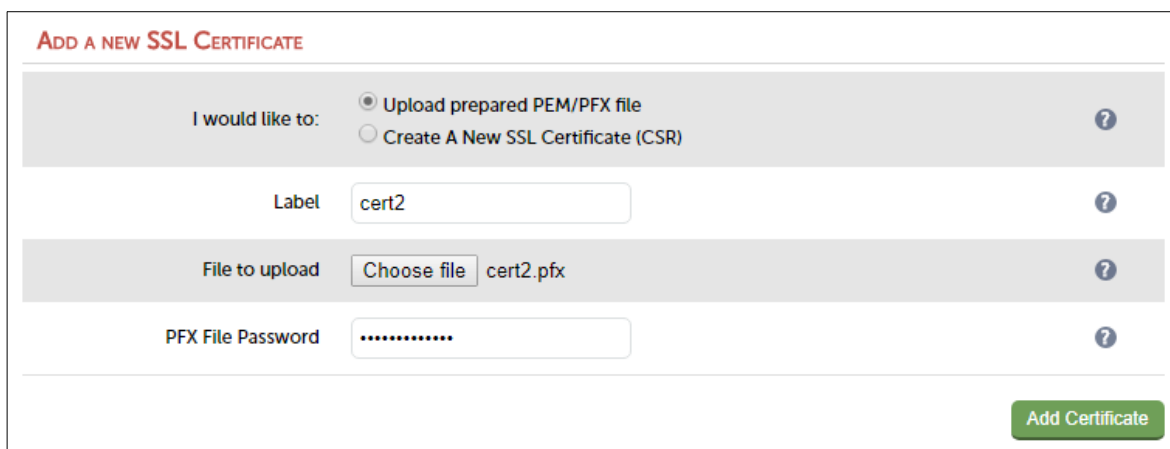
---

## 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**



The screenshot shows a web form titled "ADD A NEW SSL CERTIFICATE". It contains the following fields and options:

- I would like to:** Two radio button options: "Upload prepared PEM/PFX file" (selected) and "Create A New SSL Certificate (CSR)".
- Label:** A text input field containing "cert2".
- File to upload:** A section with a "Choose file" button and the filename "cert2.pfx".
- PFX File Password:** A password input field with masked characters ".....".
- Buttons:** A green "Add Certificate" button at the bottom right.

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

*Configure SSL Termination:*

6. Using the WebUI, navigate to: *Cluster Configuration > SSL Termination* and click **Add a New Virtual Service**
7. Select the appropriate VIP from the *Associated Virtual Service* drop-down menu, e.g. **DirPoolExtWebSvcs4443**
8. Set the *Virtual Service Port* field to **4443**
9. Select the required SSL certificate
10. Click **Update**



SSL Termination - Add a new Virtual Service

Label	SSL-DirPoolExtWebSvcs4443	?
Associated Virtual Service	DirPoolExtWebSvcs4443	?
Virtual Service Port	4443	?
SSL Operation Mode	High Security	?
SSL Certificate	cert2	?

Cancel
Update

Create the VIP:

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

Label	FePoolExtWebSvcs8081		?
Virtual Service	IP Address	192.168.20.30	?
	Ports	8081	?
Layer 7 Protocol	HTTP Mode		?
Manual Configuration	<input type="checkbox"/>		?

Cancel
Update

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

Label	<input type="text" value="FE-1"/>	?
Real Server IP Address	<input type="text" value="192.168.10.31"/>	?
Real Server Port	<input type="text" value="4443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

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:

VIP Name (Label)	IP Address	Port	Protocol	Layer	Persistence Method
IntEdgeAccess5061	192.168.10.10	5061	TCP	4	Source IP address
IntEdgeWebConf8057	192.168.10.10	8057	TCP	4	Source IP address
IntEdgeAv443	192.168.10.10	443	TCP	4	Source IP address
IntEdgeAv3478	192.168.10.10	3478	UDP	4	Source IP address
IntEdgeAv5062	192.168.10.10	5062	TCP	4	Source IP address

### 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:

Label	<input type="text" value="IntEdgeAccess5061"/>		?
Virtual Service	IP Address	<input type="text" value="192.168.10.10"/>	?
	Ports	<input type="text" value="5061"/>	?
Protocol	<input type="text" value="TCP"/>		?
Forwarding Method	<input type="text" value="NAT"/>		?
		<input type="button" value="Cancel"/>	<input type="button" value="Update"/>

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:

Label	<input type="text" value="EDGE-1"/>	?
Real Server IP Address	<input type="text" value="192.168.100.10"/>	?
Real Server Port	<input type="text" value="5061"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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:

VIP Name (Label)	IP Address	Port	Protocol	Layer	Persistence Method
ExtEdgeAccess443	10.25.1.10	443	TCP	4	Source IP address
ExtEdgeAccess5061	10.25.1.10	5061	TCP	4	Source IP address
ExtEdgeAccess5269 (Lync 2013 only)	10.25.1.10	5269	TCP	4	Source IP address
ExtEdgeWeb443	10.25.1.11	443	TCP	4	Source IP address
ExtEdgeAv443	10.25.1.12	443	TCP	4	Source IP address
ExtEdgeAv3478	10.25.1.12	3478	UDP	4	Source IP address

### 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 'ExtEdgeAv3478' 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:

Label	ExtEdgeAccess443	?	
Virtual Service	IP Address	10.25.1.10	?
	Ports	443	?
Protocol	TCP	▼	?
Forwarding Method	NAT	▼	?
		Cancel	Update

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:

---

Label	<input type="text" value="EDGE-1"/>	?
Real Server IP Address	<input type="text" value="10.20.1.10"/>	?
Real Server Port	<input type="text" value="443"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

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 users *home server* if available). This is normal and expected behavior and is explained in the 'Client Registration' section of the following technet article:

<http://blogs.technet.com/b/nexthop/archive/2011/05/25/dns-load-balancing-in-lync-server-2010.aspx>

### 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

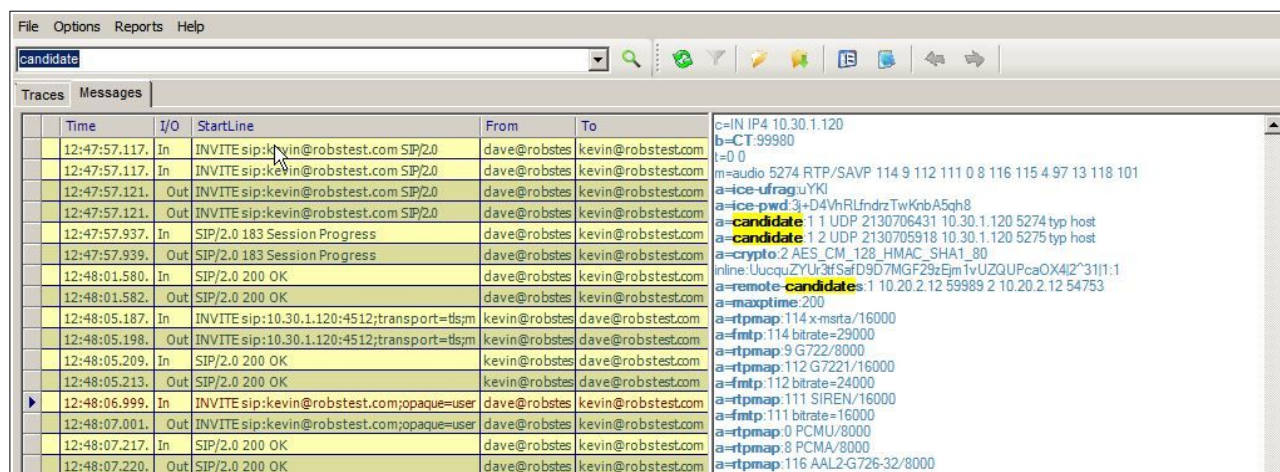
The Microsoft Lync/OCS Server Remote Connectivity Analyzer tool is a very useful Web-based Microsoft tool designed to help IT Administrators troubleshoot their Lync deployments. It's available at the following link:

<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.



Time	I/O	StartLine	From	To	Details
12:47:57.117	In	INVITE sip:kevin@robstest.com SIP/2.0	dave@robstest	kevin@robstest.com	c=IN IP4 10.30.1.120 b=CT:99980 t=0 0 m=audio 5274 RTP/SAVP 114 9 112 111 0 8 116 115 4 97 13 118 101 a=ice-ufrag:YKl a=ice-pwd:3+D4VhRLfndrzTwKnBAsqh8
12:47:57.117	In	INVITE sip:kevin@robstest.com SIP/2.0	dave@robstest	kevin@robstest.com	a=candidate:1 1 UDP 2130706431 10.30.1.120 5274 typ host
12:47:57.121	Out	INVITE sip:kevin@robstest.com SIP/2.0	dave@robstest	kevin@robstest.com	a=candidate:1 2 UDP 2130705918 10.30.1.120 5275 typ host
12:47:57.121	Out	INVITE sip:kevin@robstest.com SIP/2.0	dave@robstest	kevin@robstest.com	a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:UucquZYUrf3fSafD9D7MGf29zEjmTvUZQUPcaOX4I2*3111:1
12:47:57.937	In	SIP/2.0 183 Session Progress	dave@robstest	kevin@robstest.com	a=remote-candidate:1 10.20.2.12 59989 2 10.20.2.12 54753 a=maxtime:200
12:47:57.939	Out	SIP/2.0 183 Session Progress	dave@robstest	kevin@robstest.com	a=rtmap:114 x-msita/16000 a=fmtp:114 bitrate=29000
12:48:01.580	In	SIP/2.0 200 OK	dave@robstest	kevin@robstest.com	a=rtmap:9 G722/8000 a=rtmap:112 G7221/16000
12:48:01.582	Out	SIP/2.0 200 OK	dave@robstest	kevin@robstest.com	a=fmtp:112 bitrate=24000 a=rtmap:111 SIREN/16000
12:48:05.187	In	INVITE sip:10.30.1.120:4512;transport=tls;m	kevin@robstest	dave@robstest.com	a=fmtp:111 bitrate=16000 a=rtmap:0 PCMU/8000
12:48:05.198	Out	INVITE sip:10.30.1.120:4512;transport=tls;m	kevin@robstest	dave@robstest.com	a=rtmap:8 PCMA/8000 a=rtmap:116 AAL2-G726-32/8000
12:48:05.209	In	SIP/2.0 200 OK	kevin@robstest	dave@robstest.com	
12:48:05.213	Out	SIP/2.0 200 OK	kevin@robstest	dave@robstest.com	
12:48:06.999	In	INVITE sip:kevin@robstest.com;opaque=user	dave@robstest	kevin@robstest.com	
12:48:07.001	Out	INVITE sip:kevin@robstest.com;opaque=user	dave@robstest	kevin@robstest.com	
12:48:07.217	In	SIP/2.0 200 OK	dave@robstest	kevin@robstest.com	
12:48:07.220	Out	SIP/2.0 200 OK	dave@robstest	kevin@robstest.com	

---

For additional guidelines on using the logging tool refer to the following link:

<http://msdn.microsoft.com/en-us/library/lync/hh347311.aspx>

Note: To be able to analyze the logs, download and install the Microsoft Lync Server Resource Kit Tools from the following link:

2010: <http://www.microsoft.com/en-us/download/details.aspx?id=21165>

2013: <http://www.microsoft.com/en-us/download/details.aspx?id=36821>

## 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:*

<http://blogs.technet.com/b/nexthop/archive/2011/12/07/useful-tips-for-testing-your-lync-edge-server.aspx>

### *Reverse Proxy Concepts & Testing Web Services:*

<http://social.technet.microsoft.com/wiki/contents/articles/9807.configuring-forefront-tmg-2010-as-reverse-proxy-for-lync-server-2010.aspx>

### *Using ISS ARR as a Reverse Proxy for Lync:*

<http://blogs.technet.com/b/nexthop/archive/2013/02/19/using-iis-arr-as-a-reverse-proxy-for-lync-server-2013.aspx>

## 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](mailto:support@loadbalancer.org).

## 15. Further Documentation

The Administration Manual contains much more information about configuring and deploying the appliance. It's available here: <http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf>



---

## 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

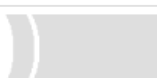
#### Version 7:

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*



Local IP address

192.168.1.20

IP address of new peer

192.168.1.21

Password for *loadbalancer* user on peer

.....

Add new node

- 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

M

192.168.120

loadbalancer.org

Attempting to pair..

S

192.168.121

loadbalancer.org

Local IP address

192.168.120

IP address of new peer

192.168.121

Password for *loadbalancer* user on peer

.....

configuring

- Once complete, the following will be displayed:

**HIGH AVAILABILITY CONFIGURATION - MASTER**

Node	IP Address	Target
M	192.168.1.20	loadbalancer.org
S	192.168.1.21	loadbalancer.org

**Break Clustered Pair**

- 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.

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:

Label	ReverseProxyFE-http		?
Virtual Service	IP Address	10.12.1.150	?
	Ports	80	?
Layer 7 Protocol	HTTP Mode ▼		?
Manual Configuration	<input type="checkbox"/>		?
			Cancel Update

3. Enter an appropriate label for the VIP, e.g. **ReverseProxyFE-http**
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 **80**
6. Leave *Layer 7 Protocol* set 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:

Label	<input type="text" value="FE-1"/>	?
Real Server IP Address	<input type="text" value="192.168.10.31"/>	?
Real Server Port	<input type="text" value="8080"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
<input type="button" value="Cancel"/> <input type="button" value="Update"/>		

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)

## 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:

Label	<input type="text" value="ReverseProxyFE-https"/>		?
Virtual Service	IP Address	<input type="text" value="10.12.1.150"/>	?
	Ports	<input type="text" value="443"/>	?
Layer 7 Protocol	<input type="text" value="TCP Mode"/>		?
Manual Configuration	<input type="checkbox"/>		?
<input type="button" value="Cancel"/> <input type="button" value="Update"/>			

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:

Label	<input type="text" value="FE-1"/>	?
Real Server IP Address	<input type="text" value="192.168.10.31"/>	?
Real Server Port	<input type="text" value="4443"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

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)

### Director Server Reverse Proxy HTTP & HTTPS VIPs

Repeat the steps above to create similar VIPs/RIPs for the Director Server Web Services.

---

## 18. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.8.0	18 October 2019	Styling and layout	General styling updates	RJC
1.8.1	12 June 2020	New title page Updated Canadian contact details Changed the instructions for adding a TLS/SSL termination	Branding update Change to Canadian contact details Changes to the appliance WebUI	AH

## About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.



### United Kingdom

Loadbalancer.org Ltd.  
Compass House, North Harbour  
Business Park, Portsmouth, PO6 4PS  
UK: +44 (0) 330 380 1064  
sales@loadbalancer.org  
support@loadbalancer.org

### Canada

Loadbalancer.org Appliances Ltd.  
300-422 Richards Street, Vancouver,  
BC, V6B 2Z4, Canada  
TEL: +1 866 998 0508  
sales@loadbalancer.org  
support@loadbalancer.org

### United States

Loadbalancer.org, Inc.  
4550 Linden Hill Road, Suite 201  
Wilmington, DE 19808, USA  
TEL: +1 833.274.2566  
sales@loadbalancer.org  
support@loadbalancer.org

### Germany

Loadbalancer.org GmbH  
Tengstraße 2780798,  
München, Germany  
TEL: +49 (0)89 2000 2179  
sales@loadbalancer.org  
support@loadbalancer.org