# Table of Contents

About this Guide .................................................................................................................. 4
Loadbalancer.org Appliances Supported .............................................................................. 4
Loadbalancer.org Software Versions Supported .................................................................. 4
Microsoft Exchange Software Versions Supported ............................................................... 4
Exchange Server 2013 ........................................................................................................... 5
Exchange 2013 Server Roles ............................................................................................... 5
Load Balancing Exchange 2013 ........................................................................................... 6
  Load Balancing & HA Requirements .................................................................................. 6
    Client Access Array ........................................................................................................ 6
    Database Availability Group (DAG) .................................................................................. 6
  Persistence (aka Server Affinity) ...................................................................................... 6
  Port Requirements ........................................................................................................... 6
  SSL Termination ............................................................................................................... 6
  HTTPS Namespaces & IP addresses .................................................................................. 7
  Health-Checks ................................................................................................................ 7
Deployment Overview ........................................................................................................ 8
  Virtual Service (VIP) Requirements .................................................................................. 8
Clustered Pair Configuration for HA ................................................................................... 9
Load Balancer Deployment Methods .................................................................................... 9
  Layer 4 DR Mode (aka Direct Server Return) ................................................................. 9
  Layer 4 NAT Mode ......................................................................................................... 10
  Layer 7 SNAT Mode ....................................................................................................... 11
Our Recommendation ......................................................................................................... 12
  Helping you Choose ...................................................................................................... 12
Exchange 2013 Configuration for Load Balancing ................................................................. 14
  1) External Access Domain ............................................................................................. 14
  2) Virtual Directories ..................................................................................................... 14
  3) Outlook Anywhere ..................................................................................................... 15
  4) Autodiscover ............................................................................................................. 15
  5) Certificates ................................................................................................................ 17
  6) Send & Receive Connectors ....................................................................................... 17
    Adding Connectors ....................................................................................................... 17
  7) DNS Configuration .................................................................................................... 18
  8) Additional Configuration Steps (depends on Load balancing method) ...................... 18
    DR Mode .................................................................................................................... 18
    NAT Mode ................................................................................................................ 18
    SNAT Mode ............................................................................................................... 18
  9) IIS Restart (** Important **) ....................................................................................... 18
Loadbalancer.org Appliance – the Basics ............................................................................ 19
  Initial Network Configuration ......................................................................................... 19
Accessing the Web User Interface (WUI) ............................................................................ 20
Appliance Configuration for Exchange 2013 – Using DR Mode .......................................... 21
  Configure VIP1 – CAS Role HTTPS Services ............................................................... 21
    a) Setting up the Virtual Service ................................................................................. 21
    b) Setting up the Real Servers .................................................................................... 22
  Configure VIP2 – CAS Role IMAP4 / POP3 Services .................................................... 23
    a) Setting up the Virtual Service ................................................................................. 23
    b) Setting up the Real Servers .................................................................................... 24
  Configure VIP3 – CAS Role SMTP Services .................................................................. 25
    a) Setting up the Virtual Service ................................................................................. 25
    b) Setting up the Real Servers .................................................................................... 26
Appliance Configuring for Exchange 2013 – Using NAT Mode

Appliance Configuring for Exchange 2013 – Using SNAT mode

Testing & Verification

Useful Exchange 2013 & Other Microsoft Tools

Testing Server state using Set-ServerComponentState

Testing Mailflow

Testing SMTP using Telnet

Microsoft Testing Tool

Useful Appliance based Tools & Features

Using System Overview

Layer 4 Status Report

Layer 7 Statistics Report

Appliance Logs

Technical Support

Conclusion

Appendix

1 – Enabling full Transparency using Tproxy (applies to Layer 7 SNAT mode)

2 – Limiting inbound SMTP Connections using Firewall Rules (applies to Layer 7 SNAT mode)

3 – Using a Layer 4 Virtual Service for SMTP

4 – Configuring an HTTP to HTTPS redirect for OWA

5 – Clustered Pair Configuration – Adding a Slave Unit

6 – Company Contact Information
About this Guide
This guide details the configuration of Loadbalancer.org appliances for deployment with Microsoft Exchange 2013. It includes details of ports/services that must be load balanced, topology considerations for the various Exchange 2013 server roles and also steps on how to configure the appliances.

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

**Version 7 Documentation**

**Version 8 Documentation**

Loadbalancer.org Appliances Supported
All our products can be used with Exchange 2013. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td></td>
<td>Enterprise R320</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
</tbody>
</table>

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

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

Loadbalancer.org Software Versions Supported

- v7.5 and later
  
  *N.B. this guide includes configuration steps for v7.6 & later. For older versions of the appliance please contact Loadbalancer.org sales or support*

Microsoft Exchange Software Versions Supported

- Microsoft Exchange 2013 CU2 (15.0.712.24) and later
Exchange Server 2013

Exchange 2013 is Microsoft’s latest enterprise level messaging and collaboration server. Exchange 2013 has been designed for simplicity of scale, hardware utilization, and failure isolation. This has greatly simplified both the deployment process and the implementation of a load balancer.

Exchange 2013 Server Roles

Exchange 2013 has been consolidated into two roles, these are: the **Client Access Server** role and the **Mailbox Server** role.

The functionality of the Hub Transport server role has split between the CAS role (the **Front End Transport Service**) and the Mailbox Server role (the **Transport Service** and the **Mailbox Transport Service**).

The Edge Transport server role has been removed.

<table>
<thead>
<tr>
<th>Role</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Client Access Server | The Client Access Server role is comprised of three components, client protocols, SMTP, and a UM Call Router. The CAS role is a thin, protocol session stateless server that is organized into a load balanced configuration. Unlike previous versions, session affinity is not required at the load balancer. This is because logic now exists in CAS to authenticate the request, and then route the request to the Mailbox server that hosts the active copy of the mailbox database.  
  *N.B. A number of issues have been seen with IOS-7 on the iPhone when used with ActiveSync. Upgrading to IOS-8 resolved these issues.* |
| Mailbox Server    | The Mailbox Server role now hosts all the components and/or protocols that process, render and store the data. No clients will ever connect directly to the Mailbox server role; all client connections are handled by the Client Access Server role. Mailbox Servers can be added to a Database Availability Group, thereby forming a high available unit that can be deployed in one or more datacenters. |

**CAS Array Object**

This concept has been removed and there is no longer any need to define a CAS array object.

**Client Access Protocols**

Outlook clients no longer use RPC to access their mailbox. This is now handled only by RPC over HTTPS (aka Outlook Anywhere). Native RPC is only used for server to sever communication. POP3 and IMAP4 continue to be supported as with previous versions.

**External SMTP Mail flow**

External SMTP communication is now handled by the **Front End Transport Service** on the CAS role.

**Exchange Administration**

The Exchange Admin Center (EAC) is the new web-based management console in Microsoft Exchange Server 2013. The EAC replaces the Exchange Management Console (EMC) and the Exchange Control Panel (ECP), which were the two interfaces used to manage Exchange Server 2010. Note that “ECP” is still the name of the virtual directory used by the EAC.
Load Balancing Exchange 2013

Load Balancing & HA Requirements

In Exchange Server 2013, there are two basic building blocks – the Client Access Array and the Database Availability Group (DAG). Each provides a unit of high availability and fault tolerance that are decoupled from one another. Multiple Client Access Servers make up the Client Access Array, while multiple Mailbox Servers form the DAG.

Client Access Array

As mentioned earlier, the 2010 concept of a CAS Array no longer exists. In 2013, a Client Access Array is simply a group of two or more Client Access Servers. The load balancer then enables resilience and HA.

Database Availability Group (DAG)

A DAG is a group of up to 16 Mailbox Servers that hosts a set of databases and provides automatic database-level recovery from failures that affect individual servers or databases.

**NOTE:** DAG's utilize Microsoft Clustering Services which cannot be enabled on the same server as Microsoft Network Load Balancing (NLB). Therefore, using Microsoft NLB is not an option in this case. Using a Loadbalancer.org hardware or virtual appliance provides an ideal solution.

Persistence (aka Server Affinity)

Due to Exchange 2013’s new architecture, all sessions to the CAS servers are stateless and therefore persistence/affinity is no longer required on the load balancer.

Port Requirements

The following table shows the port list that must be load balanced. Some services such as IMAP4 or POP3 may not be used in your environment.

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Role(s)</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>CAS</td>
<td>Inbound SMTP</td>
</tr>
<tr>
<td>110</td>
<td>CAS</td>
<td>POP3 clients</td>
</tr>
<tr>
<td>143</td>
<td>CAS</td>
<td>IMAP4 clients</td>
</tr>
<tr>
<td>443</td>
<td>CAS</td>
<td>HTTPS (Outlook Web App, AutoDiscovery, Web Services, ActiveSync, Outlook Anywhere, Offline Address Book, Exchange Administration Center)</td>
</tr>
<tr>
<td>993</td>
<td>CAS</td>
<td>Secure IMAP4 clients</td>
</tr>
<tr>
<td>995</td>
<td>CAS</td>
<td>Secure POP3 clients</td>
</tr>
</tbody>
</table>

SSL Termination

SSL offloading for Exchange 2013 is supported from SP1 as detailed in this Microsoft article. However, for scalability and effective load sharing we recommend terminating SSL on the Exchange Servers rather than on the load balancer.
HTTPS Namespaces & IP addresses

The following examples show 2 different approaches to HTTPS namespace configuration and the related load balancing considerations for each.

Example 1 – simple namespace configuration

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.robtest.com</td>
<td>Outlook Web App, ActiveSync, Outlook Anywhere, Offline Address Book, Exchange Web Services</td>
</tr>
<tr>
<td>autodiscover.robtest.com</td>
<td>Auto Discover</td>
</tr>
</tbody>
</table>

Notes:
• In this case a single VIP is used for all HTTPS namespaces / services
• Both DNS entries should then point at the same VIP
• This method is simple to setup, but only permits a single Exchange URL to be health checked. However, a successful full HTTPS service check on the OWA virtual directory is a good indication that the other Virtual Directories & applications are also functioning correctly

Example 2 – expanded namespace configuration

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>owa.robtest.com</td>
<td>Outlook Web Access</td>
</tr>
<tr>
<td>outlook.robtest.com</td>
<td>Outlook Anywhere</td>
</tr>
<tr>
<td>ews.outlook.com</td>
<td>Exchange Web Services</td>
</tr>
<tr>
<td>autodiscover.robtest.com</td>
<td>Autodiscover</td>
</tr>
<tr>
<td>activesync.robtest.com</td>
<td>ActiveSync</td>
</tr>
<tr>
<td>oab.robtest.com</td>
<td>Offline Address Book</td>
</tr>
</tbody>
</table>

Notes:
• In this case multiple VIPs are used – one for each HTTPS namespace / service
• Each related DNS entry should then point at the corresponding VIP
• This method is more complex to setup, but does enable more granular health checks to be configured
• This guide uses the config of example 1 above, i.e. a single IP address for all services.

Health-Checks

In this guide, the health check for HTTPS services accesses owa/healthcheck.htm on each server and checks for a ‘200 OK’ response. A different virtual directory (e.g. ECP, EWS etc.) can be chosen if preferred or more appropriate. Note that healthcheck.htm is generated in-memory based on the component state of the protocol in question and does not physically exist on disk.
**Deployment Overview**

There are multiple ways to deploy Exchange, but in this example two servers are used. Each server hosts the CAS & Mailbox roles in a DAG configuration. This provides high availability and uses a minimum number of Exchange Servers.

Clients then connect to the Virtual Services (VIPs) on the load balancer rather than connecting directly to one of the Exchange servers. These connections are then load balanced across the Exchange servers to distribute the load according to the load balancing algorithm selected.

The load balancer can be deployed as a single unit, although Loadbalancer.org strongly recommends a clustered pair for resilience & high availability.

**Virtual Service (VIP) Requirements**

To provide load balancing and HA for Exchange 2013, the following VIPs are required:

- HTTPS (for all HTTPS based services)
- SMTP

Optionally, additional VIPs may be required as follows:

- HTTP (required for redirecting to HTTPS, see page 48 in the appendix for more details)
- IMAP4
- POP3

*N.B. IMAP4 and POP3 are not typically used. Therefore these VIPs are not generally required.*
Clustered Pair Configuration for HA

In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 5 of the Appendix.

Load Balancer Deployment Methods

The load balancer can be deployed in one of 3 fundamental ways; Layer 4 DR mode, Layer 4 NAT mode or Layer 7 SNAT mode. These are described below.

Layer 4 DR Mode (aka Direct Server Return)

One-arm Direct Routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

- Direct Routing mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast
- When the packet reaches the Real Server it expects it to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Servers own IP address and the VIP
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as Solving the ARP Problem. please refer to chapter 6 in the administration manual for more information
- On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP
- The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work
- The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet
- Port translation is not possible in DR mode i.e. having a different RIP port than the VIP port
- DR mode is transparent, i.e. the Real Server will see the source IP address of the client
Layer 4 NAT Mode

Sometimes it's not possible to use DR mode. The two most common reasons being: if the application cannot bind to the RIP & VIP at the same time; or if the host operating system cannot be modified to handle the ARP problem. The second choice is Network Address Translation (NAT) mode. This is also a high performance solution but it requires the implementation of a two arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works).

- The load balancer translates all requests from the external Virtual Service to the internal Real Servers
- Normally eth0 is used for the internal network and eth1 is used for the external network although this is not mandatory. If the Real Servers require Internet access, Autonat should be enabled using the WUI option: Cluster Configuration > Layer 4 – Advanced Configuration, the external interface should be selected
- NAT mode can be deployed in the following ways:
  1. **2-arm (using 2 Interfaces), 2 subnets** (as shown above) - One interface on the load balancer is connected to subnet1 and the second interface and Real Servers are connected to subnet2. The VIP is brought up in subnet1. The default gateway on the Real Servers is set to be an IP address in subnet2 on the load balancer. Clients can be located in subnet1 or any remote subnet provided they can route to the VIP
  2. **2-arm (using 1 Interface), 2 subnets** - same as above except that a single interface on the load balancer is allocated 2 IP addresses, one in each subnet
  3. **1-arm (using 1 Interface), 1 subnet** - Here, the VIP is brought up in the same subnet as the Real Servers. For clients located in remote networks the default gateway on the Real Servers must be set to be an IP address on the load balancer. For clients located on the same subnet, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer - for more details on ‘One-Arm NAT Mode’ please refer to chapter 6 in the administration manual
- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. SMTP or RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this - please refer to chapter 6 in the administration manual
- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client
- Port translation is possible in NAT mode, i.e. VIP:80 → RIP8080 is possible
Layer 7 SNAT Mode

Layer 7 load balancing uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer, and HAProxy generates a new request to the chosen real server. As a result, Layer 7 is a slower technique than DR or NAT mode at Layer 4. Layer 7 is generally chosen when the network topology prohibits the use of the layer 4 methods.

Single-arm and two-arm configurations are supported as shown below. In both cases return traffic passes via the load balancer. Since layer 7 works as a proxy, there is not need to set the appliance as the gateway.

This mode has the advantage of a one arm configuration and does not require any changes to the application servers. However, since the load balancer is acting as a full proxy it doesn’t have the same raw throughput as the layer 4 methods.

The network diagram for the Layer 7 HAProxy SNAT mode is very similar to the Direct Routing example except that no re-configuration of the Real Servers is required. The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- SNAT is a full proxy and therefore load balanced Real Servers do not need to be changed in any way
- Because SNAT is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
- SNAT is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancers IP address. If required, this can be solved by either enabling TProxy on the load balancer, or for HTTP, using X-forwarded-For headers. Please refer to chapter 6 in the administration manual for more details.
- SNAT mode can be deployed using either a 1-arm or 2-arm configuration
Our Recommendation

One-arm layer 4 DR mode is the fastest option so where possible this is recommended. If this is not feasible for any reason – e.g. the Exchange Servers are located on a different subnet to the VIP, then two-arm layer 4 NAT mode is suggested as this also offers high performance.

In situations where the network topology does not allow DR mode to be used (e.g. because VIPs & RIPs not located in different subnets) or NAT mode (e.g. because its not feasible to set the Exchange Servers default gateway to be the load balancer), layer 7 SNAT mode is suggested since the Exchange Servers can be positioned on any routeable network and no Exchange Server configuration changes are required.

Helping you Choose

```
START

Will the VIP and the Exchange Servers be located in the same subnet and within the same switch fabric?

YES

Use layer 4 DR Mode

NO

Is it possible to set the default gateway on the Exchange Servers to be the load balancer?

YES

Use layer 4 NAT Mode

NO

Use layer 7 SNAT Mode
```
NOTE: SNAT Mode Source IP Address Transparency

It's important to remember that when using SNAT mode (HAProxy), the source IP address of packets reaching the Exchange Servers will be the IP address of the load balancer and not the source IP address of the client.

If this is an issue, please refer to section 4 in the Appendix for details on using Tproxy. Tproxy enables the original source IP address to be maintained, but requires that separate subnets are used, and also requires that the load balancer becomes the default gateway for the Exchange Servers. Enabling Tproxy is a global setting and therefore effects all Virtual Services configured on the load balancer which may not always be desirable.

Transparency is normally only an issue for SMTP traffic at the receive connector. System Administrators typically want to lock down receive connectors to accept SMTP connections only from a controlled set of devices such as external smart mail hosts, printers, networked photocopiers etc.

If transparency for SMTP is the only issue, there are a number of options available to address this:

**Option 1** – Enable full layer 7 transparency using Tproxy. This is covered in section 1 of the Appendix.

**Option 2** – Use the load balancers on-board firewall to lock down inbound SMTP connections rather than doing this at the receive connector. This is covered in section 2 of the Appendix.

**Option 3** – Configure a layer 4 Virtual Service for SMTP rather than a layer 7 (HAProxy) based Virtual Service. Layer 4 is transparent by default so the source IP address is maintained. This is covered in section 3 of the Appendix.
Exchange 2013 Configuration for Load Balancing

1) External Access Domain
This can be configured using the EAC. Select servers > virtual directories and then click the spanner icon. This will open the form shown below. All CAS servers should be configured with a valid external name, e.g. mail.robtest.com

![Configure External Access Domain](image)

2) Virtual Directories
The Internal and External URL's for the various virtual directories need to be configured to suit your environment. The External URL's are automatically set to be the same as the external access domain when this is configured, but can be changed if needed. The Internal URL's must be set individually by clicking the Edit (pen) icon for each virtual directory. All settings can be configured using the EAC option: servers > virtual directories as shown below:

![Virtual Directories Configuration](image)
3) Outlook Anywhere

This is configured using the EAC. Select servers > servers and then click the edit (pen) icon next to each server, click the Outlook Anywhere option as shown below to change the setting. The external and internal names for each server should be configured as required, e.g. mail.robtest.com

![Outlook Anywhere Setting](image)

4) Autodiscover

Internal

A new Active Directory object named the service connection point (SCP) is created on the server where you install the Client Access Server role. The SCP object contains the authoritative list of Autodiscover service URLs for the forest. The Set-ClientAccessServer cmdlet is used to update the SCP object as shown in the following example:

```
Set-ClientAccessServer -Identity "EXCH01" -AutoDiscoverServiceInternalUri "https://autodiscover.robtest.com/autodiscover/autodiscover.xml"
```

Once configured, the Test Email AutoConfiguration option available when <CTRL> right-clicking the Outlook icon in the taskbar can be used to view these settings as shown below:

![Test Email AutoConfiguration](image)

*N.B. The minimum Outlook client for Exchange 2013 is Outlook 2007, 2003 is NOT supported.*
When Outlook 2007/2010 is started on a client that is not domain-connected, it first tries to locate the Autodiscover service by looking up the SCP object in Active Directory. Because the client is unable to contact Active Directory, it tries to locate the Autodiscover service by using Domain Name System (DNS). In this scenario, the client will determine domain of the user's e-mail address, and then check DNS by using two predefined URLs. For the SMTP domain robtest.com, Outlook will try the following two URLs to try to connect to the Autodiscover service:

https://robtest.com/autodiscover/autodiscover.xml

https://autodiscover.robtest.com/autodiscover/autodiscover.xml

Again, this can be seen using the Test Email AutoConfiguration option as shown below:
5) Certificates

The recommended approach is to use SAN certificates and specify all required namespaces. It's also possible to use wildcard certs if preferred. Certificate requests can be generated using either the graphical based Exchange Admin Center or the command based Exchange Management Shell.

The EAC can also be used to import/export certificates using the `server > certificates > More option`.

** IMPORTANT!! - the same certificate and private key must be deployed on all Exchange Servers **

NOTE: SSL offloading for Exchange 2013 is supported from SP1 as detailed in this Microsoft article. However, for scalability and effective load sharing we recommend terminating SSL on the Exchange Servers rather than on the load balancer.

6) Send & Receive Connectors

By default no send connectors are created when Exchange 2013 is installed. A send connector must be created manually that either sends outbound email messages to a smart host or directly to their recipient using DNS.

For a dual role server that has both the CAS and Mailbox roles, five receive connectors are automatically created by default. The table below lists these connectors:

<table>
<thead>
<tr>
<th>Receive Connector</th>
<th>Role</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default &lt;server name&gt;</td>
<td>Mailbox</td>
<td>Accepts connections from Mailbox servers running the Transport service and from Edge servers</td>
</tr>
<tr>
<td>Client Proxy &lt;server name&gt;</td>
<td>Mailbox</td>
<td>Accepts connections from front-end servers. Typically, messages are sent to a front-end server over SMTP</td>
</tr>
<tr>
<td>Default FrontEnd &lt;server name&gt;</td>
<td>CAS</td>
<td>Accepts connections from SMTP senders over port 25. This is the common messaging entry point into your organization</td>
</tr>
<tr>
<td>Outbound Proxy Frontend &lt;server name&gt;</td>
<td>CAS</td>
<td>Accepts messages from a Send Connector on a back-end server, with front-end proxy enabled</td>
</tr>
<tr>
<td>Client Frontend &lt;server name&gt;</td>
<td>CAS</td>
<td>Accepts secure connections, with Transport Layer Security (TLS) applied</td>
</tr>
</tbody>
</table>

For more information on mail connectors please refer to the following Technet article:

**Adding Connectors**

Connectors can be created using the Exchange Administration Center (EAC) or the Exchange Management Shell. Receive connectors must use a unique combination of IP address bindings, port number assignments, and remote IP address ranges from which mail is accepted. Multiple send connectors can created, this is typically done to enables multiple outbound email routes to specified that have different costs.

The exact connector configuration depends on your specific environment and requirements.
7) DNS Configuration

Configure appropriate internal and external DNS entries for the various Internal and External URL's that have been defined in steps 1) to 4). The DNS entries should point at the HTTPS VIP on the load balancer - assuming a simple namespace design as shown below:

<table>
<thead>
<tr>
<th>DNS record</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.robtest.com</td>
<td>Points at the VIP used for all HTTPS based services</td>
</tr>
<tr>
<td>autodiscover.robtest.com</td>
<td>Points at the VIP used for all HTTPS based services</td>
</tr>
</tbody>
</table>

_N.B. If multiple VIPs are defined for the various Virtual Directories, DNS should be configured accordingly_

8) Additional Configuration Steps (depends on Load balancing method)

The steps required depend on the load balancing mode used as described below.

**DR Mode**

The ‘ARP problem’ must be solved on each Exchange Server for DR mode to work. For detailed steps on solving the ARP problem, please refer to the quick start guide available at the following link:


Search this document for “Solving the ARP problem for Windows Servers”

**NAT Mode**

When using Layer 4 NAT mode, the default gateway on each Exchange Server MUST be set to be the loadbalancer. It’s recommended that a floating IP address is used rather than the interface IP address. This makes it possible for the load balancer to failover to a slave unit and successfully bring up the gateway address.

**SNAT Mode**

When using SNAT mode, no configuration changes to the Exchange Servers are required.

9) IIS Restart (**Important **)

Once all Exchange configuration is complete restart IIS on each server (or reboot the server) to ensure all changes are applied. This can be done using the following command in a command or Powershell Window:

```
iisreset /restart
```
Loadbalancer.org Appliance – the Basics

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 WUI:
Using a browser, connect to the WUI on the default IP address/port: http://192.168.2.21:9080
To set the IP address & 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
e.g.
ip addr add 192.168.2.10/24 dev eth0
```

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

```
route add default gw <IP address> <interface>
e.g.
routing add default gw 192.168.2.254 eth0
```

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

```
echo nameserver <IP address> >> /etc/resolv.conf
e.g.
echo nameserver 192.168.2.250 >> /etc/resolv.conf
```

N.B. If method 3 is used, you must also configure these settings using the WUI, otherwise the settings will be lost after a reboot.
Accessing the Web User Interface (WUI)

The WUI can be accessed from a browser at:  

http://192.168.2.21:9080/lbadmin

* Note the port number → 9080

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

**Username:** loadbalancer  
**Password:** loadbalancer

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

The screen shot below shows the v7.6 WUI once logged in:
Appliance Configuration for Exchange 2013 – Using DR Mode

NOTE: It's highly recommended that you have a working Exchange 2013 environment first before implementing the load balancer.

Configure VIP1 – CAS Role HTTPS Services

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:
  - Enter an appropriate label for the VIP, e.g. CAS-HTTPS
  - Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
  - Set the Virtual Service Ports field to 443
  - Leave Protocol set to TCP
  - Leave Forwarding Method set to Direct Routing
  - Click Update
  - Now click [Modify] next to the newly created VIP
  - Set Balance mode to Weighted Round Robin

NOTE: Microsoft recommends that 'Round Robin' rather than 'Least Connection' should be used to help prevent over loading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real servers and therefore send all new requests to the new server. The trade off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

- Un-check the Persistence option
- Set Check Type to Negotiate
Set Protocol to HTTPS
Set Request to send to owa/healthcheck.htm

As mentioned earlier, any other Exchange virtual directory (e.g. ECP, EWS etc.) can be used if preferred or more appropriate. All have an associated healthcheck.htm that can be used in the same way. Note that healthcheck.htm is generated in-memory based on the component state of the protocol in question and does not physically exist on disk.

Set Response expected to 200 OK
Click Update

b) Setting up the Real Servers

Using the WUI, go to Cluster Configuration > Layer 4 – Real Servers and click [Add a new Real Server] next to the newly created VIP
Enter the following details:

- Enter an appropriate label for the RIP, e.g. CAS1
- Change the Real Server IP Address field to the required IP address, e.g. 192.168.30.20
- Click Update
- Repeat the above steps to add your other CAS Server(s)
Configure VIP2 – CAS Role IMAP4 / POP3 Services

a) Setting up the Virtual Service

N.B. these steps show IMAP4 settings, for POP3 change the port numbers from 143 & 993 to 110 & 995

- Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-IMAP4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>143,993</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. CAS-IMAP4
- Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
- Set the Virtual Service Ports field to 143,993
- Leave Protocol set to TCP
- Leave Forwarding Method set to Direct Routing
- Click Update
- Now click [Modify] next to the newly created VIP
- Set Balance mode to Weighted Round Robin

NOTE: Microsoft recommends that 'Round Robin' rather than 'Least Connection' should be used to help prevent over loading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real servers and therefore send all new requests to the new server. The trade off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

- Un-check the Persistence option
- Click Update
b) Setting up the Real Servers

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

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</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>

- Enter an appropriate label for the RIP, e.g. **CAS1**
- Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.30.20**
- Click **Update**
- Repeat the above steps to add your other CAS Server(s)
Configure VIP3 – CAS Role SMTP Services

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>25</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. **CAS-SMTP**
- Set the Virtual Service IP address field to the required IP address, e.g. **192.168.30.10**
- Set the Virtual Service Ports field to **25**
- Leave Protocol set to **TCP**
- Leave Forwarding Method set to **Direct Routing**
- Click **Update**
- Now click [Modify] next to the newly created VIP
- Un-check the Persistence option
- Click **Update**
b) Setting up the Real Servers

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

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</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>

- Enter an appropriate label for the RIP, e.g. **CAS1**
- Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.30.20**
- Click **Update**
- Repeat the above steps to add your other CAS Server(s)

**Configure HTTP to HTTPS OWA Redirect**

If required, the load balancer can be configured to automatically redirect users who attempt to connect to http://<URL to access OWA> to https://<URL to access OWA>. For details on configuring this, please refer to section 4 in the Appendix.
Appliance Configuring for Exchange 2013 – Using NAT Mode

NOTE: It's highly recommended that you have a working Exchange 2013 environment first before implementing the load balancer.

Configure VIP1 – CAS Role HTTPS Services

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:
  - Enter an appropriate label for the VIP, e.g. CAS-HTTPS
  - Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
  - Set the Virtual Service Ports field to 443
  - Leave Protocol set to TCP
  - Set the Forwarding Method to NAT
  - Click Update
  - Now click [Modify] next to the newly created VIP
  - Set Balance mode to Weighted Round Robin

NOTE: Microsoft recommends that 'Round Robin' rather than 'Least Connection' should be used to help prevent over loading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real servers and therefore send all new requests to the new server. The trade off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

- Un-check the Persistence option
- Set Check Type to Negotiate
• Set Protocol to HTTPS
• Set Request to send to owa/healthcheck.htm

As mentioned earlier, any other Exchange virtual directory (e.g. ECP, EWS etc.) can be used if preferred or more appropriate. All have an associated healthcheck.htm that can be used in the same way. Note that healthcheck.htm is generated in-memory based on the component state of the protocol in question and does not physically exist on disk.

• Set Response expected to 200 OK
• Click Update

b) Setting up the Real Servers

• Using the WUI, go to Cluster Configuration > Layer 4 – Real Servers and click [Add a new Real Server] next to the newly created VIP
• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</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>
• Enter an appropriate label for the RIP, e.g. CAS1
• Set the Real Server IP Address field to the required IP address, e.g. 192.168.30.20
• Set the Real Server Port field to 443
• Click Update
• Repeat the above steps to add your other CAS Server(s)
Configure VIP2 – CAS Role IMAP4 / POP3 Services

a) Setting up the Virtual Service

N.B. these steps show IMAP4 settings, for POP3 change the port numbers from 143 & 993 to 110 & 995

- Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-IMAP4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>143,993</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>NAT</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. **CAS-IMAP4**
- Set the Virtual Service IP address field to the required IP address, e.g. **192.168.30.10**
- Set the Virtual Service Ports field to **143,993**
- Leave Protocol set to **TCP**
- set Forwarding Method to **NAT**
- Click **Update**
- Now click [Modify] next to the newly created VIP
- Set Balance mode to **Weighted Round Robin**

**NOTE:** Microsoft recommends that ‘Round Robin’ rather than ‘Least Connection’ should be used to help prevent over loading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real servers and therefore send all new requests to the new server. The trade off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

- Un-check the Persistence option
- Click **Update**
b) Setting up the Real Servers

- Using the WUI, go to Cluster Configuration > Layer 4 – Real Servers and click [Add a new Real Server] next to the newly created VIP
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></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>

- Enter an appropriate label for the RIP, e.g. **CAS1**
- Change the Real Server IP Address field to the required IP address, e.g. **192.168.30.20**
- Leave the Real Server Port field blank
- Click **Update**
- Repeat the above steps to add your other CAS Server(s)
Configure VIP3 – CAS Role SMTP Services

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>25</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>NAT</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. CAS-SMTP
- Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
- Set the Virtual Service Ports field to 25
- Leave Protocol set to TCP
- Set Forwarding Method to NAT
- Click Update
- Now click [Modify] next to the newly created VIP
- Un-check the Persistence option
- Click Update
b) Setting up the Real Servers

- Using the WUI, go to Cluster Configuration > Layer 4 – Real Servers and click [Add a new Real Server] next to the newly created VIP
- Enter the following details:

  - Enter an appropriate label for the RIP, e.g. **CAS1**
  - Change the Real Server IP Address field to the required IP address, e.g. **192.168.30.20**
  - Change the Real Server Port field to **25**
  - Click **Update**
  - Repeat the above steps to add your other CAS Server(s)

Configure HTTP to HTTPS OWA Redirect

If required, the load balancer can be configured to automatically redirect users who attempt to connect to **http://<URL to access OWA>** to **https://<URL to access OWA>**. For details on configuring this, please refer to section 4 in the Appendix.
Configure Layer 7 Global Settings

To ensure that client connections remain open during periods of inactivity, the Client and Real Server Timeout values must be changed from their default values of 43 seconds and 45 seconds respectively to 5 minutes. To do this follow the steps below:

- Go to Cluster Configuration > Layer 7 – Advanced Configuration

![Configuration settings](image)

- Change Client Timeout to **1800000** as shown above (i.e. 1800000 ms which is 30 minutes)
  
  *N.B. 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)
  
  *N.B. You can also enter 30m rather than 1800000*

- Click the **Update** button to save the settings
Configure VIP1 – CAS Role HTTPS Services

a) Setting up the Virtual Service

• Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]
• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-HTTPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>443</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

• Enter an appropriate label for the VIP, e.g. CAS-HTTPS
• Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
• Set the Virtual Service Ports field to 443
• Set Layer 7 Protocol set to TCP Mode
• Click Update
• Now click [Modify] next to the newly created VIP
• Set Balance mode to Weighted Round Robin

NOTE: Microsoft recommends that 'Round Robin' rather than 'Least Connection' should be used to help prevent overloading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real servers and therefore send all new requests to the new server. The trade-off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

• Set Health Checks to Negotiate HTTPS
• Set Request to send to owa/healthcheck.htm

As mentioned earlier, any other Exchange virtual directory (e.g. ECP, EWS etc.) can be used if preferred or more appropriate. All have an associated healthcheck.htm that can be used in the same way. Note that healthcheck.htm is generated in-memory based on the component state of the protocol in question and does not physically exist on disk.

• Leave Response expected blank, this will configure the load balancer to look for a '200 OK' response
• Click Update
b) Setting up the Real Servers

- Using the WUI, go to *Cluster Configuration > Layer 7 – Real Servers* and click [Add a new Real Server] next to the newly created VIP
- Enter the following details:
  - Enter an appropriate label for the RIP, e.g. **CAS1**
  - Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.30.20**
  - Change the **Real Server Port** field to **443**
  - Click **Update**
  - Repeat the above steps to add your other CAS Server(s)
Configure VIP2 – CAS Role IMAP4 / POP3 Services

a) Setting up the Virtual Service

N.B. these steps show IMAP4 settings, for POP3 change the port numbers from 143 & 993 to 110 & 995

- Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-IMAP4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>143,993</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. CAS-IMAP4
- Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
- Set the Virtual Service Ports field to 143,993
- Set Layer 7 Protocol to TCP Mode
- Click Update
- Now click [Modify] next to the newly created VIP
- Set Balance mode to Weighted Round Robin

NOTE: Microsoft recommends that 'Round Robin' rather than 'Least Connection' should be used to help prevent over loading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real servers and therefore send all new requests to the new server. The trade off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

- Ensure Persistence Mode is set to None
- Click Update
b) Setting up the Real Servers

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

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

  - Enter an appropriate label for the RIP, e.g. **CAS1**
  - Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.30.20**
  - Leave the *Real Server Port* field blank
  - Click **Update**
  - Repeat the above steps to add your other CAS Server(s)
Configure VIP3 – CAS Role SMTP Services

NOTE: Source IP Address Transparency

It's important to remember that when using SNAT mode (HAProxy), the source IP address of packets reaching the Exchange Servers will be the IP address of the load balancer and not the source IP address of the client.

If this is an issue, please refer to section 4 in the Appendix for details on using Tproxy. Tproxy enables the original source IP address to be maintained, but requires that separate subnets are used, and also requires that the load balancer becomes the default gateway for the Exchange Servers. Enabling Tproxy is a global setting and therefore effects all Virtual Services configured on the load balancer which may not always be desirable.

Transparency is normally only an issue for SMTP traffic at the receive connector. System Administrators typically want to lock down receive connectors to accept SMTP connections only from a controlled set of devices such as external smart mail hosts, printers, networked photocopiers etc.

If transparency for SMTP is the only issue, there are a couple of options available to address this:

Option 1 – Enable full layer 7 transparency using Tproxy. This is covered in section 1 of the Appendix.

Option 2 – Enable the load balancers on-board firewall to lock down inbound SMTP connections rather than doing this at the receive connector. This is covered in section 2 of the Appendix.

Option 3 – Configure a layer 4 Virtual Service for SMTP rather than a layer 7 (HAProxy) based Virtual Service. Layer 4 is transparent by default so the source IP address is maintained. This is covered in section 3 of the Appendix.

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>25</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. CAS-SMTP
- Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
- Set the Virtual Service Ports field to 25
- Set Layer 7 Protocol to TCP Mode
- Click Update
• Now click [Modify] next to the newly created VIP
• Ensure Persistence Mode is set to None
• Click Update

b) Setting up the Real Servers

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

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>25</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

• Enter an appropriate label for the RIP, e.g. CAS1
• Change the Real Server IP Address field to the required IP address, e.g. 192.168.30.20
• Change the Real Server Port field to 25
• Click Update
• Repeat the above steps to add your other CAS Server(s)

Configure HTTP to HTTPS OWA Redirect
If required, the load balancer can be configured to automatically redirect users who attempt to connect to http://<URL to access OWA> to https://<URL to access OWA>. For details on configuring this, please refer to section 4 in the Appendix.

Finalizing the Configuration
To apply the new settings, HAProxy must be restarted as follows:

• Go to Maintenance > Restart Services and click Restart HAProxy
Testing & Verification

Useful Exchange 2013 & Other Microsoft Tools

**Testing Server state using Set-ServerComponentState**

The Exchange Management shell command Set-ServerComponentState can be used to verify that the load balancer is correctly health-checking the servers.

To take down OwaProxy, use the following command:

```
Set-ServerComponentState EXCH2013-2 -Component OwaProxy -Requester Maintainence -State Inactive
```

*The server should now be marked down (shown red) in the system overview.*

To bring it back online, use the following command:

```
Set-ServerComponentState EXCH2013-2 -Component OwaProxy -Requester Maintainence -State Inactive
```

*The server should now be marked up (shown green) in the system overview.*

**Testing Mailflow**

The **Test-Mailflow** cmdlet can be used to diagnose whether mail can be successfully sent from and delivered to the system mailbox on a computer that has the Mailbox server role installed. You can also use this cmdlet to verify that e-mail is sent between Mailbox servers within a defined latency threshold.

The following screenshot shows an example of using this cmdlet:
If everything is working correctly, a new message will appear in the test users mailbox:

```
From:      SystemMailbox{d97cc0-d860-47cf-bb13-d4c24bf6bd}  Sent:  Tue 18/06/2013 14:03
To:        rob
CC:
Subject:   Test-Mailflow b908b1c55-8428-475a-866f-db67e3c76ce1 65c200a-6860-44b2-983a-327e3c9cfe

This is a Test-Mailflow probe message.
```

**Testing SMTP using Telnet**

SMTP can be tested using telnet to connect to port 25, then by issuing various commands to simulate an email being sent. Using System Overview in the WUI, each CAS server can be tested by 'Halting' all others then running through the tests.

e.g. `telnet 192.168.111.240 25`

The following screenshot shows an example of using telnet to verify SMTP operation:
If everything is working correctly, a new message will appear in the test users mailbox:

```
From: test@test.com
To: test@test.com
Sent: Wed 05/06/2013 15:18
CC: 
Subject: This is a test!

This is a test message!
```

To do the same test via the load balancer, connect to the VIP, e.g.: `telnet mail.robtest.com 25`

**Microsoft Testing Tool**

The Exchange Remote Connectivity Analyzer tool, available at [https://www.testexchangeconnectivity.com/](https://www.testexchangeconnectivity.com/) is a useful Web-based Microsoft tool designed to help IT Administrators troubleshoot connectivity issues with their Exchange Server deployments. The tool simulates several client logon and mail flow scenarios. When a test fails, many of the errors have troubleshooting tips to assist the IT Administrator in correcting the problem.
Useful Appliance based Tools & Features

Using System Overview

The System Overview is accessed using the WUI. It shows a graphical view of all VIPs & RIPs (i.e. the Exchange Servers) and shows the state/health of each server as well as the state of the each cluster as a whole. The example below shows that both CAS servers are healthy and available to accept connections.

Layer 4 Status Report

The Layer 4 Status report gives a summary of layer 4 configuration and running stats as shown below. This can be accessed in the WUI using the option: Reports > Layer 4 Status.
Layer 7 Statistics Report

The Layer 7 Statistics report gives a summary of all layer 7 configuration and running stats as shown below. This can be accessed in the WUI using the option: Reports > Layer 7 Status.

Appliance Logs

Logs are available for both layer 4 and layer 7 services and can be very useful when trying to diagnose issues. Layer 4 logs are active by default and can be accessed using the WUI option: Logs > Layer 4. Layer 7 logging is not enabled by default (because it's extremely verbose) and can be enabled using the WUI option: Cluster Configuration > Layer 7 – Advanced Configuration, and then viewed using the option: Logs > Layer 7.
Technical Support

For more details or assistance with your deployment please don’t hesitate to contact the support team at the following email address: support@loadbalancer.org

Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Exchange 2013 environments.
Appendix

1 – Enabling full Transparency using Tproxy (applies to Layer 7 SNAT mode)

As mentioned previously, Layer 7 SNAT mode is non-transparent by default. If a fully transparent configuration is required, Tproxy can be used. The main points to note are that two subnets must be used and the default gateway on the Exchange Servers must be set to be the load balancer.

Key points to consider:

- The Exchange Servers must be on a different subnet to the VIP – this can be achieved by using 2 IP addresses assigned to a single interface, or two separate interfaces (eth0 & eth1)
- The default gateway on the Exchange Servers must be configured to be an IP address on the load balancer. For a clustered pair of load balancers, it’s best to add an additional floating IP for this to allow failover to the slave
- Tproxy must be enabled using the WUI:
  Go to Cluster Configuration > Layer 7 – Advanced Configuration and set Transparent Proxy to ‘On’ and click Update

N.B. If the load balancer has been deployed in Layer 4 DR or NAT mode, both are transparent by default so no additional steps are required. This section only applies when using Layer 7 SNAT mode.
2 – Limiting inbound SMTP Connections using Firewall Rules (applies to Layer 7 SNAT mode)

Since layer 7 is not transparent by default, it’s not possible to filter inbound SMTP connections by IP address at the receive connector on the Hub Transport Server. One way to address this is to add firewall rules to the load balancer to limit which hosts can connect inbound on port 25.

Rules can be added using the WUI option: Maintenance > Firewall Script. Simply copy/paste/edit the examples below into the firewall script then click Update.

**EXAMPLES:**

1) to limit inbound SMTP connections to a specific smart host:

VIP1="192.168.30.10"
SRC1="192.168.30.50"

```bash
iptables -A INPUT -p tcp --src $SRC1 --dst $VIP1 --destination-port 25 -j ACCEPT
iptables -A INPUT -p tcp --dport 25 -j DROP
```

*These rules will only allow SMTP traffic from the host 192.168.30.50 to reach the 192.168.30.10 VIP.*

2) to limit inbound SMTP connections to a range of smart hosts:

VIP1="192.168.30.10"
SRC1="192.168.30.50-60"

```bash
iptables -A INPUT -p tcp -m iprange --src-range $SRC1 --destination $VIP1 --destination-port 25 -j ACCEPT
iptables -A INPUT -p tcp --dport 25 -j DROP
```

*These rules will only allow SMTP traffic from hosts in the range 192.168.30.50 through 192.168.30.60 to reach the 192.168.30.10 VIP.*

N.B. *If the load balancer has been deployed in Layer 4 DR or NAT mode, both are transparent by default so no additional steps are required. This section only applies when using Layer 7 SNAT mode.*
3 – Using a Layer 4 Virtual Service for SMTP

This guide uses Layer 7 HAProxy based Virtual Services for all load balanced services. Layer 7 Virtual Services are not transparent by default which can be an issue for SMTP. In these cases a Layer 4 VIP can be used instead for SMTP. There are two possibilities: DR (Direct Return) mode and NAT (Network Address Translation) mode. Layer 4 DR mode is covered on page 9 of this guide, Layer 4 NAT mode is covered on page 10.

N.B. If the load balancer has been deployed in Layer 4 DR or NAT mode, both are transparent by default so no additional steps are required. This section only applies when using Layer 7 SNAT mode.

4 – Configuring an HTTP to HTTPS redirect for OWA

An additional layer 7 VIP is required that listens on HTTP port 80 on the same IP address. The VIP is then configured to redirect connections to HTTPS port 443.

e.g. http://mail.robstest.com/owa should be redirected to https://mail.robstest.com/owa

The steps:

1) Create another Layer 7 VIP with the following settings:

   • **Label**: HTTP-redirect
   
   • **Virtual Service IP Address**: <same as the VIP that’s listening on port 443>
   
   • **Virtual Service Ports**: 80
   
   • **Layer 7 Protocol**: HTTP Mode
   
   • **Persistence Mode**: None
   
   • **Force to HTTPS**: Yes

   N.B. In v7.6.4 and later, this additional VIP will be shown purple/green to indicate that it’s being used for HTTP to HTTPS redirection. In earlier versions, the VIP will be shown red since there are no associated real servers.

2) **Apply the new settings** – to apply the new settings, HAProxy must be restarted:

   • Using the WUI, go to: **Maintenance > Restart Services** and click **Restart HAProxy**
5 – 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 document referenced below for more details:

**Version 7**
Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

**Version 8**
Please refer to Chapter 9 – Appliance Clustering for HA in the v8 Administration Manual.

Don't hesitate to contact our support team if you need further assistance: support@loadbalancer.org
## 6 – 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.  
270 Presidential Drive  
Wilmington,  
DE 19807  
USA  
Tel : +1 888.867.9504 (24x7)  
Fax : +1 302.213.0122  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |
| **North America (Canada)** | Loadbalancer.org Ltd.  
300–422 Richards Street  
Vancouver, BC  
V6B 2Z4  
Canada  
Tel : +1 855.681.6017 (24x7)  
Fax : +1 302.213.0122  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |
| **Europe (UK)** | Loadbalancer.org Ltd.  
Portsmouth Technopole  
Kingston Crescent  
Portsmouth  
PO2 8FA  
England, UK  
Tel : +44 (0)330 3801064 (24x7)  
Fax : +44 (0)870 4327672  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |
| **Europe (Germany)** | Loadbalancer.org GmbH  
Alt Pempelfort 2  
40211 Düsseldorf  
Germany  
Tel : +49 (0)30 920 383 6494  
Fax : +49 (0)30 920 383 6495  
Email (sales) : vertrieb@loadbalancer.org  
Email (support) : support@loadbalancer.org |