# Table of Contents

About this Guide................................................................................................................. 4
Loadbalancer.org Appliances Supported.............................................................................. 4
Loadbalancer.org Software Versions Supported................................................................... 4
Microsoft Windows Versions Supported............................................................................... 4
Microsoft Terminal Services.................................................................................................. 5
Load Balancing Terminal Services.......................................................................................... 5
The Basics............................................................................................................................. 5
   Session Load Balancing..................................................................................................... 5
   Session Persistence (aka Server Affinity)......................................................................... 5
Port Requirements................................................................................................................... 5
Deployment Overview........................................................................................................... 6
Load Balancer Deployment Methods..................................................................................... 7
Layer 4..................................................................................................................................... 7
   Direct Server Return (DR Mode)......................................................................................... 7
   Network Address Translation (NAT Mode)......................................................................... 8
Layer 4 Persistence Methods................................................................................................ 9
   Source IP Persistence......................................................................................................... 9
Layer 7 (SNAT Mode)............................................................................................................. 9
Layer 7 Persistence Methods................................................................................................ 10
   Source IP Persistence......................................................................................................... 10
   Microsoft Session Directory Persistence........................................................................ 10
   RDP Cookie Persistence................................................................................................... 10
Our Recommendation.......................................................................................................... 11
Loadbalancer.org Appliance – the Basics............................................................................ 12
Initial Network Configuration............................................................................................... 12
Accessing the Web User Interface (WUI)........................................................................... 13
Clustered Pair Configuration.............................................................................................. 14
Load Balancing Terminal Servers........................................................................................ 15
EXAMPLE 1 – Layer 4 DR Mode (Using Source IP Persistence)........................................... 15
   Overview......................................................................................................................... 15
   Load Balancer Configuration.......................................................................................... 15
      Configure the Network Interface............................................................................. 15
      Configure the Virtual Service.................................................................................. 15
      Define the Real Servers............................................................................................ 16
   Terminal Server Configuration....................................................................................... 17
      Solve the ‘ARP Problem’............................................................................................. 17
   Accessing the Load balanced Servers........................................................................... 17
EXAMPLE 2 – Layer 4 NAT Mode (Using Source IP Persistence)......................................... 18
   Overview......................................................................................................................... 18
   Load Balancer Configuration.......................................................................................... 18
      Configure the Network Interfaces............................................................................. 18
      Configure the Virtual Service.................................................................................. 19
      Configure the Real Servers....................................................................................... 19
   Terminal Server Configuration....................................................................................... 20
      Default Gateway......................................................................................................... 20
   Accessing the Load balanced Servers........................................................................... 21
EXAMPLE 3 – Layer 7 SNAT Mode (Using Source IP Persistence)......................................... 22
   Overview......................................................................................................................... 22
   Load Balancer Configuration (single–arm example)....................................................... 22
      Configure the Network Interface............................................................................. 22
      Configure the Virtual Service (VIP)....................................................................... 22
      Configure the Real Servers (RIPs).......................................................................... 23
   Accessing the Load balanced Servers........................................................................... 23
EXAMPLE 4 – Layer 7 SNAT Mode (Using RDP Cookie Persistence)...................................... 24
   Overview......................................................................................................................... 24
About this Guide

This guide details the configuration of Loadbalancer.org appliances for deployment with Microsoft Terminal Services.

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 Terminal Services. 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](http://www.loadbalancer.org/products)

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

**Loadbalancer.org Software Versions Supported**

- v7.3.2 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 Windows Versions Supported**

- Windows 2000 to Windows 2008 R1
Microsoft Terminal Services
Terminal Services is one of the components of Microsoft Windows that allows a user to access applications and data on a remote computer over a network. Terminal services is Microsoft's implementation of thin–client terminal server computing, where Windows applications, or even the entire desktop of the computer running terminal services, are made accessible to a remote client machine.

Load Balancing Terminal Services

The Basics

Session Load Balancing
The fundamental purpose of deploying a load balancer is to share the load from multiple clients between two or more back–end Terminal Servers. Typically, all Terminal Servers within the cluster / farm have the same applications installed to ensure all clients get the same applications irrespective of which server they are connected to.

Session Persistence (aka Server Affinity)
A critical aspect of load balancing terminal services is session persistence. Within a terminal server environment, this relates to the ability to reconnect to disconnected sessions that occur when a client session is closed rather than logged off. If this reconnection process is not handled correctly, users may not be able to return to their previous sessions.

Port Requirements
The following table shows the ports that must be load balanced.

| 3389  | RDP Protocol |

N.B. It is possible to change the port used, but the default is 3389
Deployment Overview

The load balancer is deployed in front of the terminal servers to provide load balancing and fail-over functionality.

Once deployed, clients then connect to the Virtual Service (VIP) on the load balancer rather than connecting directly to one of the Terminal servers. These connections are then load balanced across the Terminal 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.
Load Balancer Deployment Methods

Layer 4

Two Layer 4 methods are available – ‘DR Mode’ and ‘NAT Mode’. These are described in the sections below. These methods only support source IP address based persistence (affinity) for reconnecting user sessions to the same backend server. This works very well in many situations, but in cases where clients connect via some form of NAT device, then these methods may not be appropriate because the source IP address for all clients would be the same. If this is the case, layer 7 methods can be used instead (see page 9).

Direct Server Return (DR Mode)

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
Network Address Translation (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:
  
  **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-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
  
  **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 4 Persistence Methods

Source IP Persistence
At layer 4 the only persistence option is source IP persistence.

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

Layer 7 Persistence Methods

Three persistence methods are supported to ensure that clients can reconnect to their sessions. These are 'Source IP Persistence', 'Microsoft Session Directory Persistence' and 'RDP Cookie Persistence' and are described in the following sections.

Source IP Persistence

As at Layer 4, this method is appropriate when client PC's have unique IP addresses. This method is very straightforward to configure and requires no changes to the terminal servers.

Microsoft Session Directory Persistence

Session Directory provides functionality that allows a group of terminal servers to coordinate the reconnection of disconnected sessions. All sessions are stored as records in a central database. This database is updated and queried by the terminal servers whenever users log on, log off, or disconnect their session, while leaving their applications active.

The load balancer is able to interact with Session Directory by enabling Routing Token Redirection mode. This mode allows the reconnection of disconnected sessions by utilizing a routing token to enable the load balancer to re-connect the client to the correct terminal server.

Session Directory

WIN 2000 / 2003 / 2008 R1 – For these versions of Windows clustering must be used to provide HA for the session database. If this is not done the session database is vulnerable to failure and therefore data loss resulting in the inability for disconnected sessions to reconnected correctly.

RDP Cookie Persistence

This method utilizes the cookie sent from the client in the Connection Request PDU. This cookie is created when the username is entered at the first client login prompt (mstsc.exe). If the username is not entered here, the cookie is not created.

In older versions of the product (pre v6.16), the rdp-cookie persistence method worked by hashing the login name, then distributing to the back-end terminal servers based on this hash. This method was not ideal as distribution of user connections was often not equally balanced across the back-end servers.

In later versions, these cookies are used on the load balancer to create a 'stick-table' which is used to keep track of which terminal server each user is associated with. Initial connections are load balanced by the selected load balancing algorithm (round robin or least connection) and an entry is created in the stick table. The table is then used by the load balancer to ensure that reconnected sessions are sent to the same back-end (terminal) server.
NOTE: In certain scenarios depending on client version as well as the specific client & server settings, the RDP cookie (mstshash) is not consistently sent.

Please also refer to our blog post on this topic: http://blog.loadbalancer.org/microsoft-drops-support-for-mstshash-cookies/

Update (October 2015) – with the latest versions of the various Windows clients, this problem appears to have been resolved.

Our Recommendation

One-arm layer 4 DR mode with source IP persistence is the fastest option so where possible this is recommended. If this is not feasible for any reason – e.g. the terminal 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 NAT mode is not feasible – e.g. all inbound requests are NAT’ed causing all clients to have the same source IP address, or its not possible to configure the load balancer as the gateway, layer 7 SNAT mode (either one-arm or two-arm) is suggested since the terminal servers can be positioned on any routeable network and no configuration changes are required.

Layer 7 must be used when integration with Session Broker is required to enable the load balancer to interpret the routing token.
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](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:

```bash
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:

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

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

```bash
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:  \texttt{http://192.168.2.21:9080/lbadmin}

* Note the port number → 9080

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

\begin{itemize}
  \item \textbf{Username}: loadbalancer
  \item \textbf{Password}: loadbalancer
\end{itemize}

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

EXAMPLE 1 – Layer 4 DR Mode (Using Source IP Persistence)

Overview

• **Configure the network interface** – A single Interface is required, eth0 is normally used in one-arm deployments, however this is not mandatory

• **Configure the Virtual Service (VIP)** – This is created on the load balancer and is the cluster address through which all back-end terminal servers are accessed

• **Configure the Real Servers (RIPs)** – Define the terminal servers that make up the cluster

• **Configure the Terminal Servers** – In DR mode, the ARP issue must be solved on each terminal server

Load Balancer Configuration

Configure the Network Interface

• One interface is required. Page 12 of this guide cover the various methods available to configure network settings.

Configure the Virtual Service

• Go to *Cluster Configuration > Layer 4 – Virtual Services* and click **[Add a New Virtual Service]**

• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>TS-Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.2.180</td>
</tr>
<tr>
<td>Ports</td>
<td>3389</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 name (label) for the VIP, e.g. **TS–Cluster**

• Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.180**

• Set the *Virtual Service Ports* field to **3389**
• Ensure that Protocol is set to TCP
• Ensure that Forwarding Method is set to Direct Routing
• Click Update
• Now click [Modify] next to the newly created Virtual Service
• Ensure Persistent is enabled
• Set Persistence Timeout to an appropriate value, e.g. 3600 (i.e. 1 hour)

_N.B. This is the time that the load balancer tracks the client IP to terminal server mapping and should typically be set to be the same as the RDP idle session timeout configured on the servers_

• Click Update

**Define the Real Servers**

• Go to Cluster Configuration > Layer 4 – Real Servers and click [Add a New Real Server] next to the newly created Virtual Service

• Enter the following details:

  - **Label**: TS1
  - **Real Server IP Address**: 192.168.2.190
  - **Weight**: 100
  - **Minimum Connections**: 0
  - **Maximum Connections**: 0

  - Click Update

• Enter an appropriate label (name) for the RIP, e.g. **TS1**
• Change the Real Server IP Address field to the required IP address, e.g. **192.168.2.190**
• Click **Update**
• Repeat for your remaining terminal server(s)
Terminal Server Configuration

Solve the 'ARP Problem'
For Windows 2000, 2003, 2008 & 2012 a Loopback adapter must be added to each connection server to enable them to accept traffic destined for the VIP. Also, for Windows 2008 a series of 3 netsh commands must also be run to configure the strong / weak host behaviour.

For detailed steps on solving the ARP problem, please search for 'The ARP Problem' in the administration manual.

Accessing the Load balanced Servers
The load balanced terminal servers should now be accessible via the VIP address.
EXAMPLE 2 – Layer 4 NAT Mode (Using Source IP Persistence)

Overview

- **Configure the Network Interfaces** – Two Interfaces are needed, this can be either two physical interfaces such as eth0 and eth1, or one physical interface and an alias/secondary interface such as eth0:0
- **Configure the Virtual Service (VIP)** – This is created on the load balancer and is the cluster address through which all back-end terminal servers are accessed
- **Configure the Real Servers (RIPs)** – Define the terminal servers that make up the cluster
- **Configure the Terminal Servers** – In NAT mode, the terminal servers default gateway must be the load balancer

Load Balancer Configuration

Configure the Network Interfaces

- Set the first IP address using one of the methods listed on page 12 of this guide
- Using the WUI, define an additional IP address in a different subnet – either by using 2 separate interfaces or a single interface with an additional alias (secondary) address as shown below:

**Using Separate Interfaces**

```
+----------------+-----------------+--------+
| IP Address     | MTU 1500 bytes |
| Assignment     | bytes           |
| eth0            | 192.168.2.170/24|
| eth1            | 192.168.23.170/24|
```

**Using a Single Interfaces with an Alias**

```
+----------------+-----------------+--------+
| IP Address     | MTU 1500 bytes |
| Assignment     | bytes           |
| eth0            | 192.168.2.170/24|
| eth0:0          | 192.168.23.170/24|
```
Configure the Virtual Service

- Go to Cluster Configuration > Layer 4 – Virtual Services and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>TS-Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.2.180</td>
</tr>
<tr>
<td>Ports</td>
<td>3389</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 (name) for the VIP, e.g. **TS-Cluster**
- Set the Virtual Service IP address field to the required IP address, e.g. **192.168.2.180**
- Set the Virtual Service Ports field to **3389**
- Ensure that Protocol is set to **TCP**
- Ensure that Forwarding Method is set to **NAT**
- Click Update
- Now click [Modify] next to the newly created Virtual Service
- Ensure Persistent is enabled
- Set Persistence Timeout to an appropriate value, e.g. **3600** (i.e. 1 hour)

*N.B. This is the time that the load balancer tracks the client IP to terminal server mapping and should typically be set to be the same as the RDP idle session timeout configured on the servers*

- Click Update

Configure the Real Servers

- Go to Cluster Configuration > Layer 4 – Real Servers and click [Add a New Real Server] next to the newly created Virtual Service
- Enter the following details:
Enter an appropriate label (name) for the RIP, e.g. **TS1**

- Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.23.190**
- Change the **Real Server Port** to **3389**
- Click **Update**
- Repeat for your remaining terminal server(s)

**Terminal Server Configuration**

**Default Gateway**

It is possible to use the internal IP address on eth0 for the default gateway, although it’s recommended that an additional floating IP is created for this purpose. This is required if two load balancers (our recommended configuration) are used. If the master unit fails, this will enable the floating IP to be brought up on the slave. To create a floating IP address on the load balancer:

- Go to **Cluster Configuration > Floating IP(s)**
- Enter the required IP address to be used for the default gateway and click **Add Floating IP**
- Once added, there will be two floating IP’s, one for the Virtual Service (**192.168.2.180**) and one for the default gateway (e.g. **192.168.23.254**) as shown below:
Accessing the Load balanced Servers

The load balanced terminal servers should now be accessible via the VIP address.
EXAMPLE 3 – Layer 7 SNAT Mode (Using Source IP Persistence)

Overview

- **Configure the Network Interface(s)** – HAProxy can be deployed in single-arm or two-arm mode. As with layer 4 NAT mode, with a two-arm Layer 7 configuration, this can be either two physical interfaces such as eth0 and eth1, or one physical interface such as eth0 and an alias/secondary interface such as eth0:0
- **Configure the Virtual Service (VIP)** – This is created on the load balancer and is the cluster address through which all back-end terminal servers are accessed
- **Configure the Real Servers (RIPs)** – Define the terminal servers that make up the cluster
- **Configure the Terminal Servers** – No terminal server changes are required for SNAT mode

Load Balancer Configuration (single-arm example)

Configure the Network Interface

- One interface is required. Page 12 of this guide covers the various methods available to configure network settings.

Configure the Virtual Service (VIP)

- Go to *Cluster Configuration > Layer 7 – Virtual Services* and click **[Add a New Virtual Service]**
- Enter the following details:
  - Enter an appropriate name (Label) for the Virtual Service, e.g. **TS–Cluster**
  - Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.2.180**
  - Set the **Virtual Service Ports** field to **3389**
  - Click **Update**
  - Now click **[Modify]** next to the newly created Virtual Service
  - Ensure **Persistence Mode** is set to **Source IP**
  - Set **Persistence Timeout** to an appropriate value, e.g. **3600** (i.e. 1 hour)
**N.B.** This is the time that the load balancer tracks the client IP to terminal server mapping and should typically be set to be the same as the RDP idle session timeout configured on the servers

- Click **Update**

**Configure the Real Servers (RIPs)**

- Go to **Cluster Configuration > Layer 7 – Real Servers** and click [Add a New Real Server] next to the newly created Virtual Service

- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>TS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.2.190</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>3389</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

- Enter an appropriate name (Label) for the first terminal server, e.g. **TS1**
- Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.2.190**
- Set the **Real Server Port** field to **3389**
- Click **Update**
- Now repeat for your remaining terminal server(s)

**Accessing the Load balanced Servers**

The load balanced terminal servers should now be accessible via the VIP address.
EXAMPLE 4 – Layer 7 SNAT Mode (Using RDP Cookie Persistence)

N.B. As mentioned earlier on page 11, this method is not generally recommended due the issues noted.

Overview

• **Configure the Network Interface(s)** – HAProxy can be deployed in single-arm or two-arm mode. As with layer 4 NAT mode, with a two-arm Layer 7 configuration, this can be either two physical interfaces such as eth0 and eth1, or one physical interface such as eth0 and an alias/secondary interface such as eth0:0

• **Configure the Virtual Service (VIP)** – This is created on the load balancer and is the cluster address through which all back-end terminal servers are accessed

• **Configure the Real Servers (RIPs)** – Define the terminal servers that make up the cluster

• **Configure the Terminal Servers** – No terminal server changes are required to support SNAT mode

Load Balancer Configuration (single-arm example)

**Configure the Network Interface**

Please refer to the previous example.

**Configure HAProxy Timeouts**

Please refer to the previous example.

**Configure the Virtual Service (VIP)**

Please refer to the previous example. N.B. When configuring persistence, choose *RDP Client Cookie* rather than *Source IP*.

**Configure the Real Servers (RIPs)**

Please refer to the previous example.

Terminal Server Configuration

No changes are required to the terminal servers.

Accessing the Load balanced Servers

The load balanced terminal servers should now be accessible via the VIP address.
EXAMPLE 5 – Layer 7 SNAT Mode (Using Connection Broker Persistence)
(In Windows 2008 R1 this is known as Session Broker, in Windows 2003 and earlier as Session Directory)

Overview

- **Configure the Network Interface(s)** – HAProxy can be deployed in single-arm or two-arm mode. As with layer 4 NAT mode, with a two-arm Layer 7 configuration, this can be either two physical interfaces such as eth0 and eth1, or one physical interface such as eth0 and an alias/secondary interface such as eth0:0
- **Configure the Virtual Service (VIP)** – This is created on the load balancer and is the cluster address through which all back-end terminal servers are accessed
- **Configure the Real Servers (RIPs)** – Define the terminal servers that make up the cluster
- **Configure the Terminal Servers** – No terminal server changes are required to support SNAT mode although the back-end servers must be configured to use session broker in Routing token re-direction mode

Load Balancer Configuration (single-arm example)

Configure the Network Interface

- One interface is required. Page 12 of this guide covers the various methods available to configure the network settings.

Configure the Virtual Service (VIP)

- Go to *Cluster Configuration > Layer 7 – Virtual Services* and click [Add a New Virtual Service]
- Enter the following details:
  
  ![Virtual Service Configuration](image)

  - Enter an appropriate name (Label) for the Virtual Service, e.g. **TS–Cluster**
  - Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.2.180**
  - Set the **Virtual Service Ports** field to **3389**
  - Click **Update**
  - Now click **[Modify]** next to the newly created Virtual Service
  - Change **Persistence Mode** to **MS Session Broker**
  - Click **Update**
Configure the Real Servers (RIPs)

- Go to Cluster Configuration > Layer 7 – Real Servers and click [Add a New Real Server] next to the newly created Virtual Service

- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>TS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.2.190</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>3389</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

- Enter an appropriate name (Label) for the first terminal server, e.g. **TS1**
- Change the **Real Server IP Address** field to the required IP address (e.g. **192.168.2.190**)
- Set the **Real Server Port** field to **3389**
- Click **Update**
- Now repeat for your remaining terminal server(s)
Terminal Server Configuration

Windows 2003
The Terminal Services Session Directory service should be started on the server designated for this purpose. (Note that Windows 2003 Enterprise Edition is required to support Session Directory)

Then on each terminal server to be included in the cluster / Farm:
- Open Terminal Services Configuration
- Click Server Settings
- Right–click Session Directory and select Properties
- Tick the check box to Join Session Directory
- Enter a name for the Terminal Server Cluster (Farm), e.g. FARM1 (all servers within the same farm require the same name to be specified)
- Enter the DNS name or IP address for the server running the Session Directory service
- Un–select the IP Address Redirection check–box.

N.B. This is a critical step which enables Routing Token Redirection Mode. In this mode the load balancer is able to interact with routing tokens from the client to determine which real server is running a previously disconnected session

- Click OK

Session Directory Settings:

![Session Directory Settings GUI](image)
Install Session Broker on the server designated to hold the Session Broker role.

Then on each terminal server to be included in the cluster / Farm:

- Open Terminal Services Configuration
- Right-click ‘Member of farm in TS Session Broker’ and select Properties
- Tick the check box to Join a farm in TS Session Broker
- Enter the DNS name or IP address for the server running the Session Broker Role Service
- Enter a name for the Terminal Server Cluster (Farm), e.g. FARM1 (all servers within the same farm require the same name to be specified)
- Un-select the **Use IP Address Redirection** check-box.

**N.B. This is a critical step which enables Routing Token Redirection Mode. In this mode the load balancer is able to interact with routing tokens from the client to determine which real server is running a previously disconnected session**

- Click **OK**

**Session Broker Settings:**

![Session Broker Settings](image-url)
Accessing the Load balanced Servers

The load balanced terminal servers should now be accessible via the VIP address.
Load Balancing TS Gateway Servers

Terminal Services Gateway (TS Gateway) enables authorized remote users to connect to resources on an internal corporate or private network, from any Internet-connected device. The network resources can be terminal servers, terminal servers running RemoteApp programs, or computers with Remote Desktop enabled.

TS Gateway uses Remote Desktop Protocol (RDP) over HTTPS to establish a secure, encrypted connection between remote users on the Internet and the internal network resources on which their productivity applications run.
To load balance multiple Gateway servers, simply create a VIP that listens on port 443 (HTTPS) with no persistence. Then define the TS gateway servers as related real servers. A layer 4 DR mode VIP is recommended for optimum performance although a layer 4 NAT mode or layer 7 SNAT mode VIP can also be used.

For more details of these operating modes please refer to pages 7 – 10.

For each TS client connection, two SSL connection are made. If the second of these 2 SSL connections gets load balanced to a different server it will get automatically redirected to the server that received the 1st connection provided that all the Gateway servers are all correctly configured as farm / collection members.

A second load balancer can then be used with Connection Broker / Session Broker to load balance the Terminal Servers / Remote Data Servers as described in the previous section of this guide.

For further information on deploying TS Gateway, please refer to the following Microsoft Technet article: http://technet.microsoft.com/en-us/library/cc304366.aspx
Technical Support
For more details or assistance with your deployment please don’t hesitate to contact the support team:
support@loadbalancer.org

Conclusion
Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Terminal Server environments.
Appendix

1 - Server Feedback Agent

The load balancer can dynamically modify the weight (amount of traffic) of each server by gathering data from a custom agent. Once installed and running, the agent listens on TCP port 3333. When the load balancer connects to this port, the agent responds with the idle stats as an integer value in the range 0–100. The figure returned can be related to CPU utilization, RAM usage or a combination of both. This can be configured using the XML configuration file located in the agents installation folder (by default this is located in C:\ProgramData\LoadBalancer.org\LoadBalancer).

This functionality enables intelligent load balancing based on the real time resource usage statistics of each terminal server. This is especially useful for session hosts where running client programs can easily saturate the servers resources.

For more information please also refer to the following blog article:

http://blog.loadbalancer.org/open-source-windows-service-for-reporting-server-load-back-to-haproxy-load-balancer-feedback-agent/

Windows Agent Download

The latest Windows feedback agent can be downloaded from:

http://downloads.loadbalancer.org/agent/loadbalanceragent.msi

To install the agent, run loadbalanceragent.msi on each terminal server

Click Next
Select the installation folder and click **Next**

Click **Next** to start the installation

*N.B. .NET Framework v3.5 is required by the agent and .NET Framework v4.0 is required by the Monitor*

*N.B. The agent should be installed on each terminal server*
**Starting the Agent**

Once the installation has completed, you'll need to start the service on the terminal server. The service is controlled by the Feedback Agent Monitor program that is also installed along with the Agent. The monitor can be accessed on the Windows server using: *All Programs > Loadbalancer.org > Monitor.* It's also possible to start the service using the services snap-in – the service is called 'Loadbalancer CPU monitor'.

![Feedback Agent Monitor](image)

- To start the service, click **Start**
- To stop the service, click **Stop**

**Configuration**

To Configure Virtual Services to use the feedback agent, follow the steps below:

- Go to *Cluster Configuration > Layer 4 - Virtual Services or Layer 7 - Virtual Services*
- Click **[Modify]** next to the Virtual Service

![Virtual Services Configuration](image)

- Change the Feedback Method to **Agent**
- Click **Update**
- For layer 7 VIPs, restart HAProxy using the WUI option: *Maintenance > Restart Services*
2 – 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
## 3 – Company Contact Information

<table>
<thead>
<tr>
<th>Website</th>
<th>URL: <a href="http://www.loadbalancer.org">www.loadbalancer.org</a></th>
</tr>
</thead>
</table>
| **North America (US)** | Loadbalancer.org, Inc.  
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 Dusseldorf  
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 |