# Table of Contents

1. About this Guide..................................................................................................................4
2. Loadbalancer.org Appliances Supported........................................................................4
3. Loadbalancer.org Software Versions Supported.............................................................4
4. Microsoft IIS Software Versions Supported.....................................................................4
5. Microsoft Internet Information Services (IIS)....................................................................5
6. Load Balancing IIS..............................................................................................................5
   The Basics............................................................................................................................5
   IIS Server Health-checks....................................................................................................5
   Providing Resilience ..........................................................................................................5
   Ports & Protocols...............................................................................................................5
   SSL & Certificates.............................................................................................................5
   Persistence (aka Server Affinity)......................................................................................6
7. Deployment Concept...........................................................................................................6
8. Load Balancer Deployment Methods..................................................................................7
   Layer 4 DR Mode...............................................................................................................7
   Layer 4 NAT Mode............................................................................................................8
   Layer 7 SNAT Mode..........................................................................................................9
   Loadbalancer.org Recommended Mode...........................................................................10
   Helping you Choose.........................................................................................................10
9. Loadbalancer.org Appliance – the Basics........................................................................11
   Initial Network Configuration............................................................................................11
   Accessing the Web User Interface (WebUI).......................................................................11
   HA Clustered Pair Configuration.......................................................................................12
10. Appliance & Server Configuration - Layer 4 DR Mode......................................................13
    Overview..........................................................................................................................13
    Load Balancer Configuration............................................................................................13
    Configure the Network Interface..................................................................................13
    Configure the Virtual Service (VIP)..............................................................................13
    Configure the Real Servers (RIPs)................................................................................14
    IIS Server Configuration..................................................................................................14
    Solve the ‘ARP Problem’...............................................................................................14
    Configure IIS Bindings.....................................................................................................14
    DR Mode – Key Points.....................................................................................................15
11. Appliance & Server Configuration - Layer 4 NAT Mode....................................................16
    Overview..........................................................................................................................16
    Load Balancer Configuration............................................................................................16
    Configure the Network Interfaces..................................................................................16
    Configure the Virtual Service (VIP)..............................................................................17
    Configure the Real Servers (RIPs)................................................................................17
    IIS Server Configuration..................................................................................................18
    Default Gateway.............................................................................................................18
    NAT Mode – Key Points.................................................................................................19
12. Appliance & Server Configuration - Layer 7 SNAT Mode..................................................19
1. About this Guide

This guide details the configuration of Loadbalancer.org appliances for deployment with Microsoft Internet Information Services (IIS).

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to our Administration Manuals which are available here:

- v7. Administration Manual
- v8. Administration Manual

2. Loadbalancer.org Appliances Supported

All our products can be used with IIS. 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>Enterprise R320</td>
<td>Enterprise Ultra</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/hardware](http://www.loadbalancer.org/products/hardware)

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

3. Loadbalancer.org Software Versions Supported

- v7.6.4 and later

4. Microsoft IIS Software Versions Supported

- Microsoft IIS – all versions
5. Microsoft Internet Information Services (IIS)

IIS is one of the components of Microsoft Windows and is Microsoft’s implementation of a web server. The protocols supported include HTTP, HTTPS, FTP, FTPS, SMTP & NNTP. The latest versions of IIS are built on an open and modular architecture that allows users to customize and add new features through various IIS Extensions. It’s estimated that around 25% of all websites utilize IIS.

6. Load Balancing IIS

Note:
It’s highly recommended that you have a working IIS environment first before implementing the load balancer.

THE BASICS

The primary function of the load balancer is to distribute inbound requests across multiple IIS servers. This allows administrators to configure multiple servers and easily share the load between them. Adding additional capacity as demand grows then becomes straight forward and can be achieved by simply adding additional IIS servers to the cluster.

IIS SERVER HEALTH-CHECKS

Regular IIS server monitoring ensures that failed servers are marked as down and client requests are only directed to functional servers. Health checks can range from a simple ICMP PING to a full negotiate check where content on a certain page is read and verified. Please refer to page 31 for more details.

PROVIDING RESILIENCE

Typically, two appliances are deployed as an active/passive pair. This ensures that a single point of failure is not introduced. A heartbeat signal between the two units is used to ensure that should the active unit fail, the passive unit takes over. Please refer to page 45 for more details.

PORTS & PROTOCOLS

The following table shows the ports that are normally used with IIS for web based applications:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP/HTTP</td>
<td>HTTP web traffic</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>HTTPS web traffic</td>
</tr>
</tbody>
</table>

SSL & CERTIFICATES

For secure websites & web pages, SSL/TLS is used. This ensures that data is encrypted between client and server. SSL certificates can either be installed on the load balancer (aka SSL off-loading) or on the IIS (aka SSL pass-through). When installed on the load balancer, it’s also possible to enable re-encryption so that the connection from the load balancer to the IIS servers is protected (aka SSL bridging). Please refer to page 21 onward for more information.
Note:
SSL termination on the load balancer can be very CPU intensive. In most cases, for a scalable solution, terminating SSL on the IIS servers is the best option. implementing the load balancer.

PERSISTENCE (AKA SERVER AFFINITY)
Ideally, persistence should be considered at the start of any IIS project. A database is typically used to maintain session information. This information is then available to all IIS servers so that whenever a user connects, any previous session details can be accessed. If this structure is not in place, persistence can be implemented on the load balancer. For HTTP, this can be based on source IP address, application/load balancer generated cookies or SSL session ID. These methods ensure that repeated connections from a particular client within a session are always sent to the same back-end IIS server.

7. Deployment Concept
The following diagram provides a simply illustration to indicate how the load balancer is deployed with multiple IIS servers.
Clients connect to the Virtual Service (VIP) on the load balancer rather than connecting directly to one of the IIS servers. These connections are then load balanced across the IIS servers to distribute the load according to the load balancing algorithm selected.

VIPs = Virtual IP Addresses

Note:
The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to section 2 in the appendix on page 45 for more details on configuring a clustered pair.
8. 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

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

Note:
Kemp, Brocade, Barracuda & A10 Networks call this Direct Server Return and F5 call it N-Path.

- DR 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 the Real Server 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
**LAYERS 4 NAT MODE**

Layer 4 NAT mode is also a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode.

- 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 WebUI 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 7 SNAT MODE**

Layer 7 SNAT mode 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 typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.

This mode can be deployed in a one-arm or two-arm configuration and does not require any changes to the Real 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 load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way
- Because SNAT mode is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
- SNAT mode 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 own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address), this can be configured per layer 7 VIP. If required, the clients IP address can be passed through either by 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
LOADBALANCER.ORG RECOMMENDED MODE

Where possible we recommend that Layer 4 Direct Routing (DR) mode is used. This mode offers the best possible performance since replies go directly from the Real Servers to the client, not via the load balancer. It’s also relatively simple to implement. Ultimately, the final choice does depend on your specific requirements and infrastructure.

HELPING YOU CHOOSE

The flow chart below is intended as a simple guide to help determine which deployment mode is most appropriate. Please also refer to section describing each deployment mode.

START

Do you require enhanced options such as SSL termination, cookie based persistence, HTTP mode URL rewriting, header insertion/deletion, etc.?  

No

Can the load balanced application bind to the real servers own IP address and the VIP at the same time?  

Yes

Use layer 4 DR Mode

AND are the load balancer and the real servers part of the same Layer 2 network?  

No

Do you want to retain the clients source IP address when packets reach the real servers (transparent)?  

Yes

Use layer 4 NAT Mode

No

Use layer 7 SNAT Mode
INITIAL NETWORK CONFIGURATION

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

**Method 1 - Using the Network Setup Wizard at the console**
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

**Method 2 - Using the WebUI**
Using a browser, connect to the WebUI on the default IP address/port: **http://192.168.2.21:9080**
To set the IP address & subnet mask, use: **Local Configuration > Network Interface Configuration**
To set the default gateway, use: **Local Configuration > Routing**
To configure DNS settings, use: **Local Configuration > Hostname & DNS**

**Method 3 - Using Linux commands**
At the console, set the initial IP address using the following command:
```
ip addr add <IP address>/<mask> dev eth0
```
At the console, set the initial default gateway using the following command:
```
rout add default gw <IP address> <interface>
```
At the console, set the DNS server using the following command:
```
echo nameserver <IP address> >> /etc/resolv.conf
```

*Note:*
If method 3 is used, you must also configure these settings using the WebUI, otherwise the settings will be lost after a reboot.

ACCESSING THE WEB USER INTERFACE (WEBUI)
The WebUI can be accessed via HTTP at the following URL: **http://192.168.2.21:9080/lbadmin**
*Note the port number → 9080*

The WebUI can be accessed via HTTPS at the following URL: **https://192.168.2.21:9443/lbadmin**
*Note the port number → 9443*

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

Login using the following credentials:

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

Once logged in, the WebUI will be displayed as shown below:
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 2 of the Appendix on page 45.

**HA CLUSTERED PAIR CONFIGURATION**

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 2 of the Appendix on page 45.
10. Appliance & Server Configuration - Layer 4 DR Mode

Note:
It’s highly recommended that you have a working IIS environment first before implementing the load balancer.

OVERVIEW

1. **Configure the Network Interface** – A single Interface is needed, eth0 is normally used
2. **Configure the Virtual Service (VIP)** – All IIS servers are accessed via this IP address
3. **Configure the Real Servers (RIPs)** – Define the servers that make up the IIS cluster
4. **Configure the IIS Servers** – In DR mode, the ‘ARP Problem’ must be solved on each IIS server

LOAD BALANCER CONFIGURATION

CONFIGURE THE NETWORK INTERFACE

1. One interface is required. Page 11 covers the various methods available to configure network settings.

CONFIGURE THE VIRTUAL SERVICE (VIP)

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

   ![Virtual Service Configuration](image)

   3. Enter an appropriate name (Label) for the VIP, e.g. **IIS-Cluster**
   4. Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.2.180**
   5. Set the **Virtual Service Ports** field to **80**
   6. Leave **Protocol** set to **TCP**
   7. Ensure that **Forwarding Method** is set to **Direct Routing**
   8. Click **Update**
   9. Now click **Modify** next to the newly created Virtual Service
10. Set *Balance Mode* (the load balancing algorithm) according to your needs
11. Click **Update**

**CONFIGURE THE REAL SERVERS (RIPS)**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>IIS-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.2.190</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

3. Enter an appropriate name (Label) for the first IIS server, e.g. **IIS1**
4. Change the *Real Server IP Address* field to the required IP address (e.g. **192.168.2.190**)
5. Leave other settings at their default values
6. Click **Update**
7. Repeat the above steps for your other IIS server(s)

**IIS SERVER CONFIGURATION**

**SOLVE THE ‘ARP PROBLEM’**

As mentioned previously, DR mode works by changing the MAC address of the incoming packet. Therefore the load balancer and the IIS servers must both be configured to accept traffic for the same IP address. However, only the load balancer should respond to ARP requests. To achieve this, a loopback adapter is added to the IIS servers. The IP address is then set to be the same as the Virtual Service and is also configured so that it does not respond to ARP requests. Please refer to section 1 in the appendix on page **40** for more information.

**CONFIGURE IIS BINDINGS**

By default, IIS listens on all configured IP addresses as shown below:
If the default configuration is left, no further IIS configuration is required. If you do change the IP address in the bindings from “All Unassigned” to a specific IP address, then you need to make sure that you also add a binding for the Virtual Service IP address (VIP) as shown below:

In this example, 192.168.2.180 is the main NIC interface for the IIS server and 192.168.2.190 is the Virtual Service’s IP address (assigned to the loopback Interface). This ensures that IIS responds to both the RIP and the VIP.

**DR MODE – KEY POINTS**

- You **must** solve the ‘ARP Problem’ on all IIS servers in the cluster (please refer to page 40 for more information)
- Virtual Services & Real Servers (i.e. the IIS servers) must be within the same switch fabric. They can be on different subnets but this cannot be across a router – this is due to the way DR mode works, i.e. by changing MAC addresses to match the destination server
- Port translation is not possible, e.g. VIP:80 → IIS:82 is not allowed. The port used for the VIP & RIP must be the same
- IIS bindings must include the Virtual Service IP (VIP) address – this is the default for IIS when ‘All Unassigned’ is selected
11. Appliance & Server Configuration - Layer 4 NAT Mode

Note:
It’s highly recommended that you have a working IIS environment first before implementing the load balancer.

OVERVIEW

1. **Configure the Network Interfaces** – Two interfaces must be used located on different subnets. This can either be two physical interfaces such as eth0 and eth1, or one physical interface such as eth0 and an additional alias/secondary interface
2. **Configure the Virtual Service (VIP)** – All IIS servers are accessed via this IP address
3. **Configure the Real Servers (RIPs)** – Define the servers that make up the IIS cluster
4. **Configure the IIS Servers** – In NAT mode, the IIS servers default gateway must be configured to be an IP address on the load balancer

LOAD BALANCER CONFIGURATION

CONFIGURE THE NETWORK INTERFACES

1. Set the first IP address using one of the methods listed on Page 11
2. Using the WebUI, navigate to: Local Configuration > Network Interface Configuration
3. 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:
Using a single interface with multiple IPs:

```
eth0
192.168.2.170/24
192.168.23.170/24
```

**CONFIGURE THE VIRTUAL SERVICE (VIP)**

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

<table>
<thead>
<tr>
<th>Label</th>
<th>IIS-Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td>192.168.2.180</td>
</tr>
<tr>
<td>Ports</td>
<td>80</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>NAT</td>
</tr>
</tbody>
</table>

3. Enter an appropriate name (Label) for the VIP, e.g. **IIS-Cluster**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.180**
5. Set the *Virtual Service Ports* field to **80**
6. Leave Protocol set to **TCP**
7. Set the *Forwarding Method* is to **NAT**
8. Click **Update**
9. Now click **Modify** next to the newly created Virtual Service
10. Set *Balance Mode* (the load balancing algorithm) mode according to your needs
11. Click **Update**

**CONFIGURE THE REAL SERVERS (RIPS)**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:
3. Enter an appropriate name (Label) for the first IIS server, e.g. IIS-1
4. Change the Real Server IP Address field to the required IP address, e.g. 192.168.23.190
5. Set the Real Server Port field to 80
6. Leave other settings at their default values
7. Click Update
8. Repeat the above steps for your other IIS server(s)

IIS SERVER CONFIGURATION

DEFAULT GATEWAY
The default gateway on each IIS server must be configured to be an IP address on the load balancer. It’s 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. In this scenario if the master unit fails, the floating IP will be brought up on the slave.

To create a floating IP address on the load balancer:

1. Using the WebUI, navigate to: Cluster Configuration > Floating IPs
2. Enter the required IP address to be used for the default gateway and click Update.
3. 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:

<table>
<thead>
<tr>
<th>Floating IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.180</td>
</tr>
<tr>
<td>192.168.23.254</td>
</tr>
<tr>
<td>New Floating IP</td>
</tr>
<tr>
<td>Delete</td>
</tr>
</tbody>
</table>

4. Now configure your IIS Servers to use this additional IP address as their default gateway
NAT MODE – KEY POINTS

- Virtual Services & Real Servers (i.e. the IIS servers) must be on different subnets
- The default gateway on the IIS servers should be an IP address on the load balancer
- Port translation is possible, e.g. VIP:80 → RIP:8080 is allowed

12. Appliance & Server Configuration - Layer 7
SNAT Mode

Note:
It’s highly recommended that you have a working IIS environment first before implementing the load balancer.

OVERVIEW

1. **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
2. **Configure the Virtual Service (VIP)** – All IIS servers are accessed via this IP address
3. **Configure the Real Servers (RIPs)** – Define the IIS servers that make up the IIS cluster
4. **Configure the IIS Servers** – No Real Server changes are required

LOAD BALANCER CONFIGURATION (SINGLE-ARM EXAMPLE)

CONFIGURE THE NETWORK INTERFACE

1. One interface is required. Page 11 covers the various methods available to configure network settings.

CONFIGURE THE VIRTUAL SERVICE (VIP)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Services and click Add a New Virtual Service
2. Enter the following details:
3. Enter an appropriate name (Label) for the Virtual Service, e.g. IIS-Cluster
4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.2.180
5. Set the Virtual Service Ports field to 80
6. Leave Layer 7 Protocol set to HTTP Mode
7. Click Update
8. Now click Modify next to the newly created Virtual Service
9. Set Balance mode (the load balancing algorithm) mode according to your needs
10. Click Update

CONFIGURE THE REAL SERVERS (RIPS)

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

3. Enter an appropriate name (Label) for the first IIS server, e.g. IIS-1
4. Change the Real Server IP Address field to the required IP address (e.g. 192.168.2.190)
5. Set the Real Server Port field to 80
6. Click Update
7. Repeat the above steps for your other IIS server(s)

IIS SERVER CONFIGURATION

In SNAT (HAProxy) mode, no IIS server configuration changes are required.
SNAT MODE – KEY POINTS

- Virtual Services & Real Servers (the IIS servers) can be on the same or different subnets
- Port translation is possible, e.g. VIP:80 → RIP:8080 is allowed
- No configuration changes are required to the IIS servers
- Not as fast as Layer 4 DR mode or NAT mode

13. Additional Configuration Options & Settings

SSL TERMINATION

SSL termination can be handled in the following ways:

1. On the IIS Servers (recommended) – aka SSL Pass-through
2. On the load balancer – aka SSL Offloading
3. On the load balancer with re-encryption to the IIS Servers – aka SSL Bridging

1 – CERTIFICATES INSTALLED ON THE IIS SERVERS (AKA SSL PASS-THROUGH)

Notes:

- It's not possible to use HTTP cookie persistence since packets are encrypted and therefore the cookie cannot be read. If persistence via the load balancer is required, IP persistence must be used
- Data is encrypted from client to server. This provides full end-to-end data encryption as shown in the diagram below:

Creating a CSR (Steps shown are for Windows 2008 R2)

To generate a certificate for IIS the first step is to create a Certificate Signing Request (CSR)

1. Select the IIS server in IIS Manager then double-click Server Certificates
2. In the actions section on the right hand side of the screen, select *Create Certificate Request*, fill in the relevant details as per the example below, then click **Next**.

3. Leave the default settings and click **Next**.
4. Where prompted on the following screen enter a suitable filename, e.g. c:\csr.txt and click **Finish**
5. Use this saved CSR with your chosen Certificate Authority to obtain your certificate
6. Once you’ve received your certificate from the CA, save it as a text file
7. To install the certificate on the IIS server select **Complete Certificate Request** in the action section of Server Certificates in IIS Manager, then specify the filename and a friendly name and click **OK**

8. At this point depending on your specific version of Windows, you may receive the message shown below. This is a known issue that occurs because the friendly certificate name entered in step 7 above in not being read correctly
For more details please refer to [http://support.microsoft.com/kb/959216](http://support.microsoft.com/kb/959216). Note that the certificate has been installed and can be seen in IIS Manager under Server Certificates.

9. Now amend the site bindings to include HTTPS and the newly installed certificate.

### 2 – CERTIFICATES INSTALLED ON THE LOAD BALANCER (AKA SSL OFF-LOADING)

#### Notes:

- Since SSL is terminated on the load balancer, data from the load balancer to the IIS servers is not encrypted as shown in the diagram below. This may or may not be an issue depending on the network structure between the load balancer and IIS servers and your security requirements.

#### Note:
Re-encryption is possible between the load balancer and the IIS Servers (aka. SSL bridging). To use this, enable the ‘Re-encrypt to Backend’ option for each RIP and click Update. Each server must be correctly configured for HTTPS for this to work and an appropriate certificate must also be installed (this can be a self signed server certificate). Please see page 29 for more details.

- A Pound or STunnel SSL VIP can be used to terminate SSL. The backend for this VIP can be either a Layer 4 NAT mode Virtual Service or a Layer 7 HAProxy Virtual Service. The following diagram shows this:

![Diagram of SSL termination on load balancer]

**Note:** It's not possible to use a layer 4 DR mode Virtual Service in this scenario.

#### Note:
SSL termination on the load balancer can be very CPU intensive. In most cases, for a scalable solution, terminating SSL on the IIS servers is the best option.
1) Export the certificate from Windows

It's often easiest to get the certificate working on the IIS server first, then export the certificate and import this to the load balancer. The steps for Windows 2008 R2 for this process are as follows:

(Steps shown for Windows 2008 R2)

1. Once the certificate is working correctly on your Windows server, run **mmc**, and add the certificates snap-in. Expand the Personal folder and click on **Certificates** – your certificate should be here. Right-click the certificate and select **All Tasks > Export**. This will start the Certificate Export Wizard as shown below:

   ![Certificate Export Wizard](image1)

2. Click **Yes** to export the private key and click **Next**

   ![Certificate Export Wizard](image2)
3. Check *Include all Certificates in the certification path if possible* and click **Next**

4. Enter a password to secure the private key and click **Next**

5. Enter a folder & filename for the exported certificate and click **Next**
6. Now click Finish to complete the wizard, the following confirmation should be shown:

```
Certificate Export Wizard

The export was successful.
```

2) Import the certificate to the load balancer

1. Using the WebUI, navigate to: Cluster Configuration > SSL Certificate and click Add a new SSL Certificate
2. Select the Upload prepared PEM/PFX file option
3. Enter an appropriate label (name), e.g. IIScert1

4. Browse to and select the relevant .pfx file

5. Enter the relevant password if the certificate file is password protected

6. Click Add Certificate

3) configure SSL termination

Now configure SSL termination using either Pound or STunnel (STunnel is the default). For the VIP you can use the same IP address as your HAProxy or NAT VIP created earlier with port 443 for HTTPS. The IP address & port for the Backend Cluster should be set the same as your HAProxy or NAT mode VIP as detailed below:

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

2. Enter the following details (shows STunnel example which is the default terminator)

<table>
<thead>
<tr>
<th>Label</th>
<th>IIS-SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Certificate</td>
<td>IIScert1</td>
</tr>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.2.100</td>
</tr>
<tr>
<td>Virtual Service Port</td>
<td>443</td>
</tr>
<tr>
<td>Backend Virtual Service IP Address</td>
<td>192.168.2.100</td>
</tr>
<tr>
<td>Backend Virtual Service Port</td>
<td>80</td>
</tr>
<tr>
<td>Ciphers to use</td>
<td>ECDHE-RSA-AES256-SHA384 ECDHE</td>
</tr>
<tr>
<td>SSL Terminator</td>
<td>STunnel</td>
</tr>
<tr>
<td>Do not insert empty fragments</td>
<td>✔️</td>
</tr>
<tr>
<td>Delay DNS Lookups</td>
<td>✔️</td>
</tr>
<tr>
<td>Disable SSLv2 Ciphers</td>
<td>✔️</td>
</tr>
<tr>
<td>Disable SSLv3 Ciphers</td>
<td>✔️</td>
</tr>
<tr>
<td>Disable TLSv1 Ciphers</td>
<td>✔️</td>
</tr>
<tr>
<td>Client Cipher Renegotiation</td>
<td>✔️</td>
</tr>
<tr>
<td>Disable SSL Renegotiation</td>
<td>✔️</td>
</tr>
<tr>
<td>Time To Close</td>
<td>0</td>
</tr>
<tr>
<td>Set Source Address</td>
<td></td>
</tr>
<tr>
<td>Enable Proxy Protocol</td>
<td></td>
</tr>
</tbody>
</table>

3. Enter an appropriate name (Label) for the VIP, e.g. IIS-SSL
4. Select the SSL certificate just uploaded
5. Change the Virtual Service IP address field to the required value, e.g. **192.168.2.180**
6. Change the Virtual Service Port field to the required value, e.g. **443**
7. Change the Backend Virtual Service IP Address field to the required value, e.g. **192.168.2.180**
8. Change the Backend Virtual Service Port field to the required value, e.g. **80**
9. The remaining options can be left at their default values
10. Click **Update**

**4) Restart Services**

1. Now restart/reload services as directed in the blue box at the top of the screen

   *Once restarted your secure website should be accessible at: https://<Virtual IP Address>*

**3 – CERTIFICATES INSTALLED ON THE LOAD BALANCER WITH RE-ENCRYPTION TO IIS (AKA SSL BRIDGING)**

**Notes:**

- This is similar to SSL Offload, the only difference is that the connection from the load balancer to the IIS Server is encrypted using the certificate located on the IIS Server, this could be a self-signed certificate since no client connections are terminated here
- This mode can be enabled for each Real Servers using the option **Re-Encrypt to Backend**

### To enable re-encryption:

1. For each IIS Server use the WebUI option: **Cluster Configuration > Layer 7 – Real Servers > Modify**
2. Set **Real Server Port** to **443**
3. Enable the option **Re-Encrypt to Backend**
4. Click **Update**

**Note:**

This can also be configured at the Virtual Server level in v8.2.1 and later and applies to all Real Servers subsequently added.
MULTIPLE PORTS ON A SINGLE VIRTUAL SERVICE (VIP)

It may be desirable to combine multiple ports in a single Virtual Service. For example, if your IIS server has both HTTP and HTTPS content, you may want clients to connect to the same IIS server for both. This is especially useful if you need persistence as clients move from HTTP to HTTPS, e.g. an e-commerce web site without a proper back end database for session state.

LAYER 4

The concept is to create a firewall rule that matches incoming packets to a particular IP and port, and mark them with an arbitrary integer. A Virtual Service is then configured or modified, specifying the firewall mark instead of an IP and port.

Firewall Marks are configured automatically when multiple ports are defined for a Layer 4 VIP. For example, to configure an HTTP/HTTPS Virtual Service, simply specify port 80 & 443 separated by a comma in the 'Virtual Service Ports' field as shown below:

![Layer 4 Configuration](image)

**Note:**
Firewall marks can also be configured manually if needed, for details on this please refer to the Administration Manual.

LAYER 7

For Layer 7 VIPs, multiple ports can be defined. Simply specify all the required ports in the Virtual Service Ports field separated by commas as shown below:

![Layer 7 Configuration](image)
**REAL SERVER (IIS) HEALTH CHECKS**

The load balancer performs regular health checks to ensure that each server in the cluster is healthy and able to accept client connections. The health check options depend on whether the VIP is defined at layer 4 or layer 7 as outlined below.

**LAYER 4**

By default, a TCP connect health check is used for newly created layer 4 Virtual Services. The following tables lists all options available:

<table>
<thead>
<tr>
<th>Check Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negotiate</td>
<td>Sends a request and looks for a specific response (see Negotiate Check Service below)</td>
</tr>
<tr>
<td>Connect to port</td>
<td>Just do a simple connect to the specified port/service &amp; verify that it’s able to accept a connection</td>
</tr>
<tr>
<td>Ping server</td>
<td>Sends an ICMP echo request packet to the Real Server</td>
</tr>
<tr>
<td>External check</td>
<td>Use a custom file for the health check. Specify the file path in the ‘Check Command’ field.</td>
</tr>
<tr>
<td>No checks, always Off</td>
<td>All Real Servers are off</td>
</tr>
<tr>
<td>No checks, always On</td>
<td>All Real Servers are on (no checking)</td>
</tr>
<tr>
<td>5 Connects, 1 Negotiate</td>
<td>Do 5 connect checks and then 1 negotiate check</td>
</tr>
<tr>
<td>10 Connects, 1 Negotiate</td>
<td>Do 10 connect checks and then 1 negotiate check</td>
</tr>
</tbody>
</table>

**LAYER 7**

By default, a TCP connect health check is used for newly created layer 7 Virtual Services. The following tables lists all options available:

<table>
<thead>
<tr>
<th>Check Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negotiate HTTP</td>
<td>Sends an HTTP request and looks for a specific response. Also set the Request to Send &amp; Response Expected fields</td>
</tr>
<tr>
<td>Negotiate HTTPS</td>
<td>Sends an HTTPS request and looks for a specific response. Also set the Request to Send &amp; Response Expected fields</td>
</tr>
<tr>
<td>Connect to port</td>
<td>Just do a simple TCP connect to the specified port/service &amp; verify that it’s able to accept a connection</td>
</tr>
<tr>
<td>External Script</td>
<td>use a custom file for the health check. Specify the script path in the Check Script field</td>
</tr>
<tr>
<td>MySQL</td>
<td>The check consists of sending two MySQL packets, one Client Authentication packet, and one QUIT packet, to correctly close the MySQL session. It then parses the MySQL Handshake Initialization packet and/or Error packet</td>
</tr>
</tbody>
</table>
**Additional Configuration Options & Settings**

| No checks, always On | All Real Servers are assumed on (i.e. no checking) |

**Note:**
For full details on the options available, please refer to Chapter 8 – *Real Server Health Monitoring & Control* in the *Administration Manual*.

**URL REWRITING / CONTENT SWITCHING**

The load balancer is able to rewrite requests sent by the clients before they are forwarded to the server. HTTP rewriting rules can be configured either using the *Edit ACL Rules* option or the *Manual configuration* option for more detailed custom rules.

**Edit ACL Rules:**
This option can be accessed using the WebUI option: *Cluster Configuration > Layer 7 – Virtual Services > Modify > Edit ACL Rules*

![HAProxy ACL List](image)

In the example above, requests are redirected to the URL location `http://www.example.com` if the path begins with `/example`

E.g. if the requested URL is: `http://www.domain.com/example`
the request is redirected to: `http://www.example.com`

**Manual Configuration:**
This option can be enabled using the WebUI option: *Cluster Configuration > Layer 7 – Virtual Services > Modify > Manual Configuration*

Once enabled, the WebUI option: *Cluster Configuration > Layer 7 - Manual Configuration* can be used to defined the custom layer 7 service.

**Note:**
For full details on these options, please refer to Chapter 6 – *Configuring Load Balanced Services* in the *Administration Manual*.

**HTTP HEADER MANIPULATION**

The load balancer is able to add and delete HTTP headers. This can be configured using the WebUI option:
Cluster Configuration > Layer 7 – Virtual Services > Modify > Edit HTTP Headers.

In the example above, a header will be added called X-Client-IP with the value set to the client’s IP address.

The options available are:

**Add** - Allows you to append a HTTP header who’s name is controlled by the ‘Header Name’ input box. The value of the header is controlled by the ‘Header Value’ Box.

**Set** - Does the same as add but the header is removed/replaced if it already exists.

**Delete** - Removes all HTTP header fields that match the header name specified in the Header Name Box.

**SERVER FEEDBACK AGENT**

The load balancer can modify the weight (amount of traffic) of each server by gathering data from either a custom agent or an HTTP server. For layer 4 VIPs the feedback method can be set to either agent or HTTP, for Layer 7 VIPs, only the agent method is supported.

A telnet to port 3333 on an IIS Server with the agent installed will return the current 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 C:\ProgramData\LoadBalancer.org\LoadBalancer).

The load balancer typically expects a 0-99 integer response from the agent which by default relates to the current CPU idle state, e.g. a response of 92 would imply that the IIS Servers CPU is 92% idle. The load balancer will then use the formula \((92/100 * \text{requested weight})\) to find the new optimized weight. Using this method an idle IIS Server will get 10 times as many new connections as an overloaded server.

**Note:**

The ‘Requested Weight’ is the weight set in the WebUI for each Real Server added, the default is 100. For more information please also refer to the following blog article:


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 server

Click **Next**

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

**Note:**
The agent should be installed on all IIS Servers in the cluster.

**Starting the Agent**
Once the installation has completed, you'll need to start the service on the IIS Servers. 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'.

- To start the service, click **Start**
- To stop the service, click **Stop**
To Configure the Virtual Service to use the Agent
As mentioned, both layer 4 and layer 7 VIPs can be configured to use the feedback agent. To Configure Virtual Services to use Agent/HTTP Feedback follow the steps below:

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 - Virtual Services or Layer 7 - Virtual Services
2. Click Modify next to the Virtual Service
3. Set the Feedback Method to Agent
4. Click Update
5. Reload/restart services as prompted

LOAD BALANCER TRANSPARENCY

LAYER 4 – DR & NAT MODE
By default both Layer 4 modes are transparent. This means that IIS will log the actual IP address of the client rather than the IP address of the load balancer.

LAYER 7 – TPROXY
When using HAProxy, the load balancer is not transparent by default. This means that the IP address of the load balancer will be captured and stored in the IIS logs. If you want the client IP address to be logged, TProxy can be enabled. TProxy enables the IIS servers behind a layer 7 HAProxy configuration to see the client source IP address. In this mode, the IIS servers must be in a different subnet to the VIP and the default gateway on all IIS servers must be the load balancer.

LAYER 7 – X-FORWARDED-FOR HEADERS
Since the load balancer must be in a NAT configuration (i.e. VIPs & RIPv in different subnets and default gateway on the IIS Servers set as an IP on the load balancer) to utilize TProxy, it’s not always an appropriate solution. In situations such as this, the X-forwarded-for header can be enabled for the layer 7 Virtual Service using the WebUI. The IIS servers can then be configured to record this data in the log file. For more details about configuring the various versions of IIS, please refer to the following blog article:
http://www.loadbalancer.co.uk/blog/iis-and-x-forwarded-for-header

14. Testing & Validation

TESTING LOAD BALANCED SERVICES
To test a web server based configuration, add a page to each web servers root directory e.g. test.html and put the server name on this page for easy identification during the tests.

Use two or more clients to do the testing. Open up a web browser on each test clients and enter the URL for the VIP e.g. http://192.168.110.10
Testing & Validation

Each client should see a different server name because of the load balancing algorithm in use i.e. they are being load balanced across the cluster.

**Why test using two clients?** If you use a single client it will most likely keep on hitting the same server for multiple requests. This is to do with the way that the load balancing algorithms are optimized.

**DIAGNOSING VIP CONNECTION PROBLEMS**

1. **Make sure that the device is active** - this can be checked in the WebUI. For a single appliance, the status bar should report **Master & Active** as shown below:

<table>
<thead>
<tr>
<th>Master</th>
<th>Slave</th>
<th>Active</th>
<th>Passive</th>
<th>Link</th>
</tr>
</thead>
</table>

2. **Check that the VIP/floating IP is up** - Using View Configuration > Network Configuration verify that the VIP is active on the load balancer, if not check Logs > Heartbeat for errors.

   ```
   2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qdisc 8000
   link/ether 00:6c:29:cf:80:03 brd ff:ff:ff:ff:ff:ff
   inet 192.168.110.85/18 brd 192.168.127.255 scope global eth0
   valid_lft forever preferred_lft forever
   inet 192.168.110.90/18 brd 192.168.127.255 scope global secondary eth0
   valid_lft forever preferred_lft forever
   ```

   The above example shows that the interface address (192.168.110.85) and the VIP address (192.168.110.90) are both up.

3. **Check that the IIS Servers are up** - Using System Overview make sure that none of your VIPs are colored red. If they are, the entire cluster is down (i.e. all IIS Servers). Green indicates a healthy cluster, yellow indicates that your cluster may need attention (one or more of the IIS Servers may be down), and blue indicates all IIS Server have been deliberately taken offline (by using either Halt or Drain).

4. **Check the connection state** -

   For Layer 4 DR mode VIPs check Reports > Layer 4 Current Connections to view the current traffic in detail. Any packets with state **SYN_RECV** imply that the 'ARP Problem' has not been correctly solved on the IIS Servers. See page 40 for more details on solving the ARP problem.

   For layer 4 NAT mode VIPs check Reports > Layer 4 Current Connections to view the current traffic in detail. Any packets with state **SYN_RECV** often imply that the default gateway on the IIS Servers has not been set to be an IP address on the load balancer.

   For Layer 7 VIPs check Reports > Layer 7 Status. The default credentials required are:
Testing & Validation

**Username:** loadbalancer

**Password:** loadbalancer

This will open a second tab in the browser and display a statistics/status report as shown in the example below:

### Statistics Report for pid 3261

#### General process information

<table>
<thead>
<tr>
<th>pid</th>
<th>3261 (process #1 - heap #1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>options</td>
<td>-65536-65535</td>
</tr>
<tr>
<td>system stats</td>
<td>total_memory = 14848000 bytes, minimum = 55096 bytes, maximum = 148472768 bytes, current = 11372840 bytes, connected = 320, conn_time = 2000, running_time = 1.11, init = 100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Time</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>UP</td>
<td>going up</td>
</tr>
<tr>
<td>active</td>
<td>DOWN</td>
<td>going up</td>
</tr>
<tr>
<td>active</td>
<td>UP</td>
<td>going down</td>
</tr>
<tr>
<td>active</td>
<td>DOWN</td>
<td>going down</td>
</tr>
<tr>
<td>active or backup</td>
<td>DOWN</td>
<td>for maintenance (N/A)</td>
</tr>
</tbody>
</table>

#### Display options

- Host: DOWN servers
- Switch: on
- GUI: export

#### External resources:

- Primary site
- Secondary site
- Online manual

<table>
<thead>
<tr>
<th>Server</th>
<th>Processor</th>
<th>RAM</th>
<th>Memory</th>
<th>Disk</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ON</td>
</tr>
<tr>
<td>Backend</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>OFF</td>
</tr>
</tbody>
</table>

#### In this example:

**Microsoft IIS Deployment Guide**

Page

In this example:
Testing & Validation

*RIP1* is green, this indicates that it’s operating normally.

*RIP2* is blue, this indicates that it has been either Halted or Drained. In this example Halt has been used as indicated by *Online (Halt)* being displayed. If it had been drained it would show as *Online (Drain)*.

*RIP3* is red, this indicates that it has failed a health check.

**USING REPORTS & LOG FILES**

The appliance includes several logs and reports that are very useful when diagnosing issues. Both are available as main menu options in the WebUI. Details of both can be found in chapter 13 in the Administration Manual.

15. Technical Support

For more details about configuring the appliance and assistance with designing your deployment please don’t hesitate to contact the support team using the following email address: support@loadbalancer.org

16. Further Documentation


17. Conclusion

Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Microsoft IIS environments.
18. Appendix

1 - SOLVING THE ARP PROBLEM
When using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each Real Server to be able to receive traffic destined for the VIP, and ensuring that each Real Server does not respond to ARP requests for the VIP address – only the load balancer should do this.

The steps below are for Windows 2012 / 2016, for other versions of Windows please refer to chapter 6 in the Administration Manual.

Step 1: Install the Microsoft Loopback Adapter

1. Click Start, then run hdwwiz to start the Hardware Installation Wizard
2. When the Wizard has started, click Next
3. Select Install the hardware that I manually select from a list (Advanced), click Next
4. Select Network adapters, click Next
5. Select Microsoft & Microsoft KM-Test Loopback Adapter, click Next
6. Click Next to start the installation, when complete click Finish

Step 2: Configure the Loopback Adapter

1. Open Control Panel and click Network and Sharing Center
2. Click Change adapter settings
3. Right-click the new Loopback Adapter and select Properties
4. Un-check all items except Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) as shown below:
Note:
Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

5. If configuring IPv4 addresses select **Internet Protocol Version (TCP/IPv4)**, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255, e.g. 192.168.2.20/255.255.255.255 as shown below:
6. If configuring IPv6 addresses select **Internet Protocol Version (TCP/IPv6)**, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) and set the **Subnet Prefix Length** to be the same as your network setting, e.g. 2001:470:1f09:e72::15/64 as shown below:

7. Click **OK** on TCP/IP Properties, then click **Close** on Ethernet Properties to save and apply the new settings.

8. Now repeat the above process on the other Windows 2012/2016 Real Servers.

**Step 3: Configure the strong/weak host behavior**

Windows Server 2000 and Windows Server 2003 use the weak host model for sending and receiving for all IPv4 interfaces and the strong host model for sending and receiving for all IPv6 interfaces. You cannot configure this behavior. The Next Generation TCP/IP stack in Windows 2008 and later supports strong host sends and receives for both IPv4 and IPv6 by default. To ensure that Windows 2012/2016 is running in the correct mode to be able to respond to the VIP, the following commands must be run on each Real Server:

For IPv4 addresses:

- `netsh interface ipv4 set interface "net" weakhostreceive=enabled`
- `netsh interface ipv4 set interface "loopback" weakhostreceive=enabled`
- `netsh interface ipv4 set interface "loopback" weakhostsend=enabled`

For these commands to work, the LAN connection NIC must be named “net” and the loopback NIC must be named “loopback” as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named “LAN” and “LOOPBACK”, the commands required would be:

- `netsh interface ipv4 set interface "LAN" weakhostreceive=enabled`
- `netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled`
- `netsh interface ipv4 set interface "LOOPBACK" weakhostsend=enabled`
For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmists=0
```

For these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```
netsh interface ipv6 set interface "LAN" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostsend=enabled
netsh interface ipv6 set interface "LOOPBACK" dadtransmists=0
```

Note:
The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.

1. Start Powershell or use a command window to run the appropriate netsh commands as shown in the example below:

```
C:\Users\administrator.ROBUST\> netsh interface ipv6 set interface "net" weakhostreceive=enabled
C:\Users\administrator.ROBUST\> netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
C:\Users\administrator.ROBUST\> netsh interface ipv6 set interface "loopback" weakhostsend=enabled
C:\Users\administrator.ROBUST\> netsh interface ipv6 set interface "loopback" dadtransmists=0
```

Note:
This shows an IPv6 example, use the IPv4 commands if you’re using IPv4 addresses.

2. Now repeat these 4 commands on the other Windows 2012 Real Servers
Configuring IIS to Respond to both the RIP and VIP

For DR mode, it’s also important to make sure that IIS responds to both the VIP and RIP. By default, IIS listens on all configured IP addresses, this is shown in the example below (shows Windows 2008 example). As can be seen the IP address field is set to “All Unassigned”.

If the default configuration is left, no further IIS configuration is required. If you do change the IP address in the bindings from “All Unassigned” to a specific IP address, then you need to make sure that you also add a binding for the Virtual Service IP address (VIP).

Note:
Solving the ARP problem for other version of Windows is similar. For full details, please refer to the Administration Manual.
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 section below for more details:

**Note:**

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

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

**Version 7:**

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

**Version 8:**

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

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration

![Create a Clustered Pair](image)
• Specify the IP address and the loadbalancer users password (the default is ‘loadbalancer’) for the slave (peer) appliance as shown above
• Click Add new node
• The pairing process now commences as shown below:

![Create a Clustered Pair](image)

• Once complete, the following will be displayed:

![High Availability Configuration - Master](image)

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

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

**Note:**
Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
# 3 - COMPANY CONTACT INFORMATION

<table>
<thead>
<tr>
<th>Region</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Website</strong></td>
<td>URL: <a href="http://www.loadbalancer.org">www.loadbalancer.org</a></td>
</tr>
</tbody>
</table>
| **North America (US)**  | Loadbalancer.org, Inc.  
                         4250 Lancaster Pike, Suite 120  
                         Wilmington  
                         DE 19805  
                         USA  
                         Tel: +1 888.867.9504  
                         Fax: +1 302.213.0122  
                         Email (sales): [sales@loadbalancer.org](mailto:sales@loadbalancer.org)  
                         Email (support): [support@loadbalancer.org](mailto:support@loadbalancer.org) |
| **North America (Canada)** | Loadbalancer.org Ltd  
                           300-422 Richards Street  
                           Vancouver, BC  
                           V6B 2Z4  
                           Canada  
                           Tel: +1 866.998.0508  
                           Fax: +1 302.213.0122  
                           Email (sales): [sales@loadbalancer.org](mailto:sales@loadbalancer.org)  
                           Email (support): [support@loadbalancer.org](mailto:support@loadbalancer.org) |
| **Europe (UK)**         | Loadbalancer.org Ltd.  
                           Compass House  
                           North Harbour Business Park  
                           Portsmouth, PO6 4PS  
                           UK  
                           Tel: +44 (0)330 3801064  
                           Fax: +44 (0)870 4327672  
                           Email (sales): [sales@loadbalancer.org](mailto:sales@loadbalancer.org)  
                           Email (support): [support@loadbalancer.org](mailto:support@loadbalancer.org) |
| **Europe (Germany)**    | Loadbalancer.org GmbH  
                           Tengstraße 27  
                           D-80798  
                           München  
                           Germany  
                           Tel: +49 (0)89 2000 2179  
                           Fax: +49 (0)30 920 383 6495  
                           Email (sales): [vertrieb@loadbalancer.org](mailto:vertrieb@loadbalancer.org)  
                           Email (support): [support@loadbalancer.org](mailto:support@loadbalancer.org) |