Transparency

Feature Description

UPDATED: 07 December 2020

Copyright Notices

Copyright © 2002-2020 Kemp Technologies, Inc. All rights reserved. Kemp Technologies and the Kemp Technologies logo are registered trademarks of Kemp Technologies, Inc.

Kemp Technologies, Inc. reserves all ownership rights for the LoadMaster and Kemp 360 product line including software and documentation.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933

Table of Contents

1 Introduction **5**

1.1 Document Purpose 5

1.2 Intended Audience 5

1.3 Related Firmware Version 5

2 Transparency **6**

2.1 Implications of Network Transparency 6

2.2 Layer 4 and Layer 7 6

2.3 Direct Server Return 7

2.4 Transparency Requirements 7

2.5 Enable Layer 7 Transparency 9

2.6 Layer 7 Issues 10

2.7 Transparency, SNAT, and Single-Arm Networks 10

2.8 Cloud Transparency 11

3 Non-Transparency **13**

3.1 Subnet Originating Requests 13

4 Additional L7 HTTP Header **15**

4.1 Configure the Log Files to Record X-Forwarded-For 16

4.1.1 Record the X-Forwarded-For Header in IIS 7 16

4.1.2 Record the X-Forwarded-For Header in Apache 20

5 Alternate Source Addresses **21**

6 Transparency vs. Non-Transparency Browsing **22**

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

6.1 Why is it not possible to browse from the same subnet with transparency? 22

6.2 Why is it possible to browse from the same subnet with non-transparency? 24

7 Troubleshooting 25

7.1 Unable to Connect to Real Servers using Remote Desktop Protocol (RDP) 25

7.1.1 One-Arm Setup 25

7.1.2 Two-Arm Setup 25

References 27

Last Updated Date 28

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

1 Introduction

To place a load balancer in a network effectively and utilize Layer 7 functionality, two things need to happen:

- Traffic needs to flow through the load balancer on the way in
- Return/response traffic needs to flow through the load balancer on the way out

To meet the requirements above there are two options; Layer 7 (L7) Transparency or L7 Non-Transparency. When a packet arrives at the LoadMaster, the source IP address of the packet is that of the client and the destination IP address is that of the Virtual Service. When L7 Transparency is enabled the packet is passed to the Real Server with the same source IP address of the packet but with the destination IP address changed to be the that of the Real Server.

With L7 Non-Transparency when the packet is being sent to the Real Server the LoadMaster will change the destination IP address of the packet to be the Real Server (as it does in L7 Transparent Mode) but it will also change the source IP address from the original client IP address to the IP address of the Virtual Service.

1.1 Document Purpose

This document serves as an explanation of network transparency, its implications and other related concepts.

1.2 Intended Audience

This document is intended to be used by anyone who is interested in learning more about transparency and the Kemp LoadMaster.

1.3 Related Firmware Version

Published with LMOS version 7.2.48.3 LTS. This document has not required changes since 7.2.48.3 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

2 Transparency

2.1 Implications of Network Transparency

To decide whether or not network transparency is needed, ask this question: does the IP address of the client requests need to appear in the logs?

If the answer is yes, then network transparency is required. That means the LoadMaster will need to be configured and the network will need to be designed in a certain way, which this document will describe.

If the answer is no, then there is a little more flexibility in how the network can be configured.

The table below shows a matrix of the advantages and disadvantages of transparency.

Pro/Con	Transparent	Non-Transparent
Pro	Preserves the source IP address	Can browse from the same subnet as the Real Server
Pro	Works with Layer 4 (L4) and L7	No need to change the default gateway
Con	Cannot browse from the same subnet as the Real Servers	The source IP address is not preserved (but X-Forwarded-For header can be used)
Con	The default gateway must be the LoadMaster	Only available for L7
Con	Cannot have non-local Real Servers	
Con	Cannot use with SSL re-encryption	

The transparency settings are based on making sure that traffic moves from the Real Server back to the client through the LoadMaster. This type of symmetric routing, that is, going in and out of the LoadMaster, is an inherent requirement of all load balancers (with the exception of employing direct server return, a feature which the LoadMaster supports, which has its own set of limitations).

2.2 Layer 4 and Layer 7

The LoadMaster makes a differentiation between L4 and L7 handling. This refers to Layer 4 and Layer 7 of the OSI model. Layer 4 involves TCP/UDP ports, and Layer 7 refers to the higher-level awareness

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

of the LoadMaster, such as with HTTP cookies, SSL acceleration, and content switching. For all Layer 4 Virtual Services, the only behaviour available is transparent networking.

Layer 4 is any load balanced traffic that does not involve cookie persistence, SSL acceleration, content switching or content switching rules. Layer 4 does include SRC (source IP) address persistence.

Virtual IP Address	Prot	Name	Layer
10.154.11.71:80	tcp	Example L7	L7
10.154.11.73:80	udp	Example L4	L4

It is possible to tell if a Virtual Service is using L4 or L7 handling by looking at the Virtual Service in **Virtual Services** and **View/Modify Services** in the main menu of the LoadMaster Web User Interface (WUI). It will indicate what layer it is operating on in the **Layer** column.

Any time any cookie persistence, SSL acceleration, or content switching options are used, the traffic automatically becomes L7.

2.3 Direct Server Return

Direct Server Return (DSR) is a method whereby the LoadMaster only handles the inbound traffic flow. The servers respond directly to the clients, bypassing the LoadMaster on the way out.

For further information on Direct Server Return, refer to the **Configuring DSR, Technical Note** on the Kemp Documentation Page.

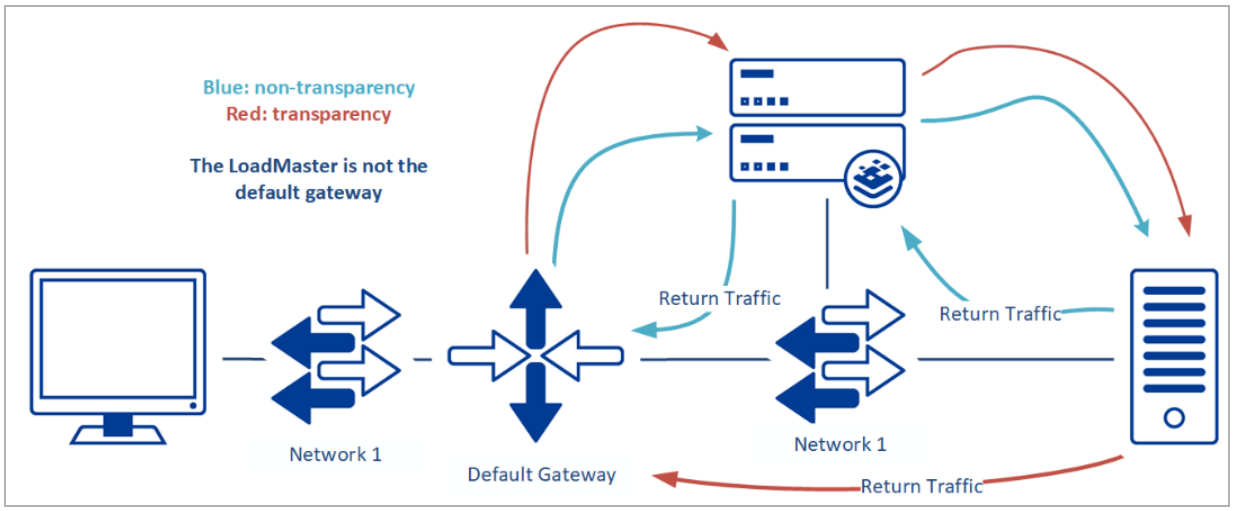
2.4 Transparency Requirements

When using **Transparency**, there are two requirements that must be met:

- The Real Server needs to have the LoadMaster as the default gateway
- The clients cannot be on the same subnet as the Real Server

The diagrams and text below explain why these requirements must be met.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved



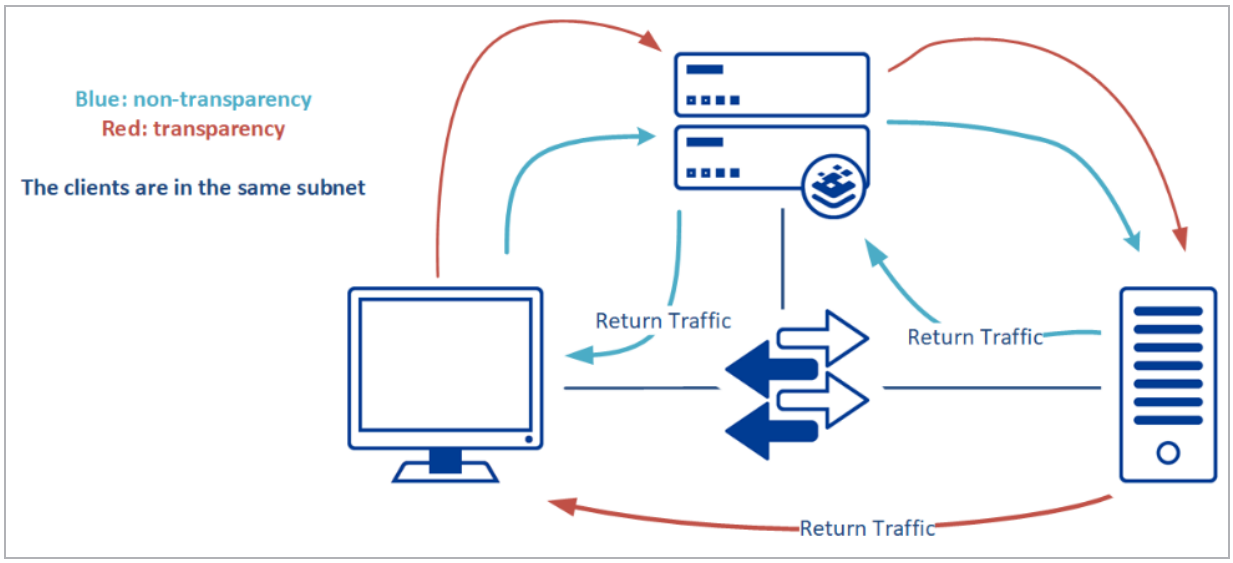
In the diagram above, neither of the flows have the LoadMaster as the default gateway. In order to be transparent, the default gateway of the Real Servers must be the LoadMaster. This is true whether the network configuration is one-armed or two-armed. If the LoadMaster is not the default gateway, there is no way to ensure that traffic passes through the LoadMaster on the way from the server to the client, and the LoadMaster cannot do its job.

Here is the flow of traffic if transparency is enabled and the LoadMaster is not the default gateway:

1. Client to Virtual Service
2. Virtual Service to Real Server
3. Real Server to network default gateway
4. Network default gateway to client

The connection will fail between the Real Server and network default gateway.

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved



Another requirement of transparency is that you must be browsing from a subnet other than that of the Real Servers. Again, it is to ensure that traffic passes in and out of the LoadMaster. If you are on the same subnet as the Real Server, the return traffic will simply go directly to the client, instead of through the LoadMaster. As a result, the client is expecting to see traffic come from the IP address of the Virtual Service, but instead will see traffic coming from the IP address of the Real Server. When that happens, the client system ignores the traffic. For a more detailed explanation, refer to the **Transparency vs. Non-Transparency Browsing** section.

Here is the flow of traffic if transparency is enabled and the clients are in the same subnet as the Real Server:

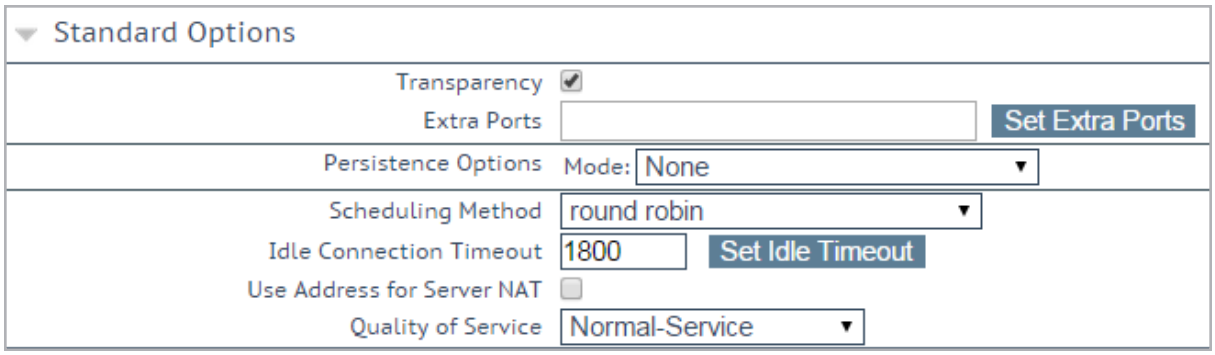
1. Client to Virtual Service
2. Virtual Service to Real Server
3. Return traffic from Real Server direct to client

The connection will fail between the Real Server and the client due to the fact that the clients are in the same subnet as the Real Server.

2.5 Enable Layer 7 Transparency

Each L7 Virtual Service has the capability of being transparent or non-transparent. If the service is an L7 service, whether it is using some of the L7 handling features, or if it is forced, the following check box will appear in the **Standard Options** section of the Virtual Service modify screen.

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved



This check box governs the transparency setting for the specific Virtual Service. When it is ticked, transparency is enabled.

2.6 Layer 7 Issues

When load balancing without any Layer 7 functionality, for example when there is no cookie persistence and no SSL acceleration, then the only option is for transparency to be enabled.

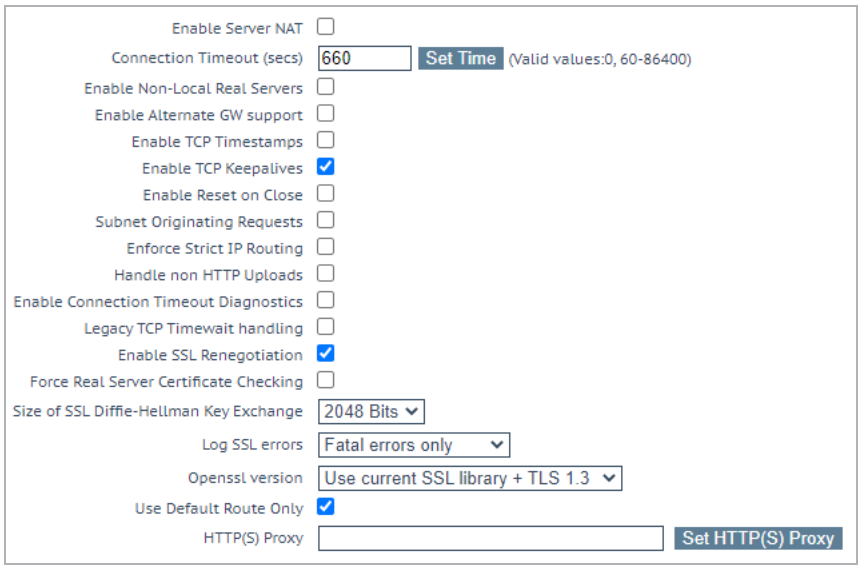
> Even if transparency is disabled in the LoadMaster configuration, Layer 4 traffic is always transparent.

2.7 Transparency, SNAT, and Single-Arm Networks

If using a single-armed configuration (that is when the Virtual Services and the Real Servers are on the same subnet) and employing transparency, SNAT (Source NAT) should be disabled. SNAT is the mechanism that allows servers behind the LoadMaster to make outbound connections in a two-armed configuration. It acts much like an office firewall, by “masquerading” the outbound connections as coming from a public IP address. In a single-armed configuration, SNAT is not necessary, although it normally does not interfere with regular operations.

There is an exception - when using transparency, the LoadMaster is the default gateway for the Real Servers, and you want to access the Real Servers directly. SNAT will “break” connections directly to the servers by attempting to masquerade those connections, so SNAT should be disabled.

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved



To disable SNAT, go to **System Configuration > Miscellaneous Options > Network Options** in the WUI. Simply uncheck the **Enable Server NAT** box, and SNAT is disabled. Servers will now be directly accessible.

2.8 Cloud Transparency

If you can set the Real Server to route return traffic to the LoadMaster interface, transparency can be set for the Virtual Service. Using routing tables may be required to prevent asymmetric routing.

> Transparency currently cannot be used in conjunction with cloud High Availability (HA) because there is no shared IP address.

If you are seeing the following scenario:

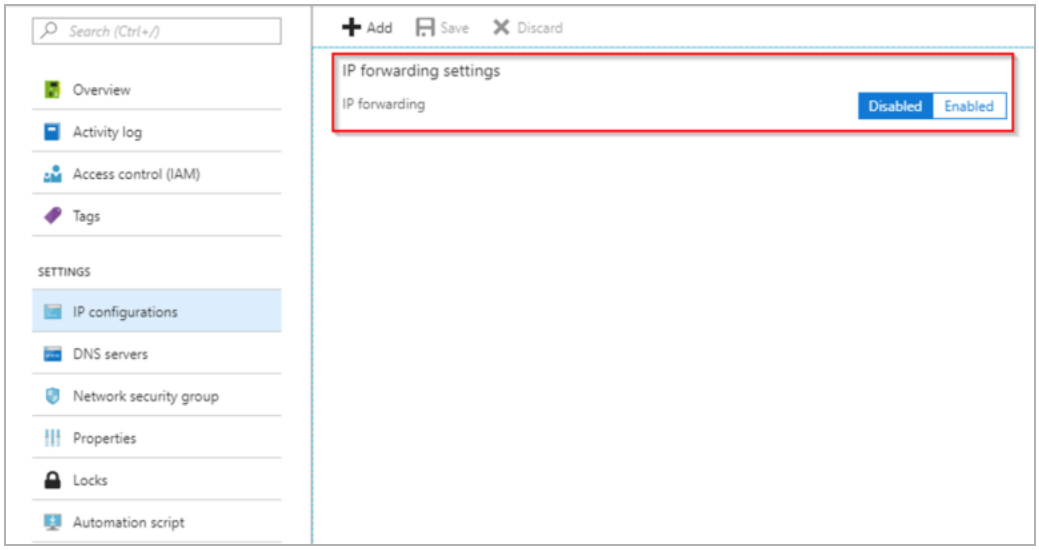
- With transparency disabled, the LoadMaster sends traffic to a healthy Real Server as normal and the Real Server responds.
- With transparency enabled, the LoadMaster sends traffic to a healthy Real Server as normal. However, no traffic is seen on the Real Server.

This is due to IP forwarding in Azure or source/destination checks in Amazon Web Services (AWS).

For further information on IP forwarding in Azure, refer to the following Microsoft content: Enable or disable IP forwarding.

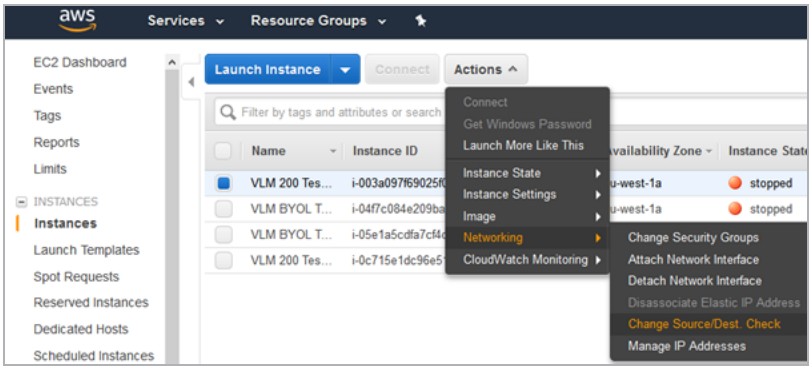
 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

You can find this in the Azure portal by going to: **Home > <*Virtual LoadMaster (VLM)*> > Networking > <*VLM NIC/Interface*> > IP configurations**.



Set **IP forwarding** to **Enabled**.

For further information on **Source/Destination Checks** in AWS, refer to the following AWS content: Disabling Source/Destination Checks.

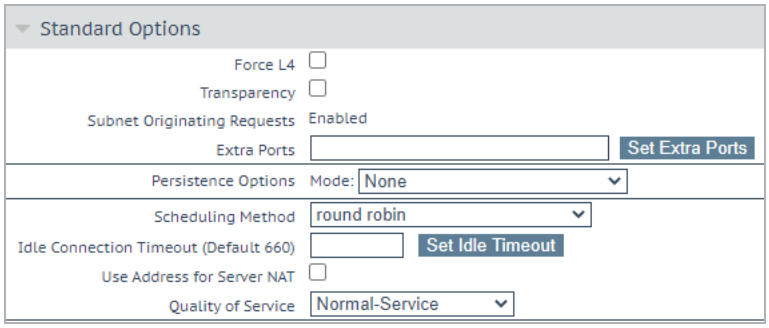


You can find this in the AWS portal by selecting the EC2 instance (the LoadMaster) and going to: **Actions > Networking > Change Source/Dest. Check**. This must be disabled.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

3 Non-Transparency

There are two main benefits to using non-transparency. The first benefit is that it allows you to browse your Virtual Service when the client is on the same subnet. The other advantage is that the LoadMaster does not need to be the default route in a one-armed configuration. Traffic is forced through the LoadMaster on the way out by making the request appear as if it came from the LoadMaster itself (which is why the IP address is hidden).



Transparency is disabled by default in the LoadMaster.

If cookie persistence, content switching or SSL acceleration is employed for a given Virtual Service, the **Force L4** option disappears. As mentioned previously, the chief disadvantage is that the source IP address of the client is hidden, although it is forwarded in a separate HTTP header.

> If the client is local to the Virtual Service, transparency is automatically disabled. If using two VLANs and the netmasks of the two VLANs do not differentiate between them, the LoadMaster decides the client is local and disables transparency. This is not only the case with VLANs - it can also happen when using the same networks on multiple interfaces.

3.1 Subnet Originating Requests

There is a check box called **Subnet Originating Requests** in **System Configuration > Miscellaneous Options > Network Options**. When transparency is turned off for a Virtual Service, the source IP address of the connections to the Real Servers is the Virtual Service. When the **Subnet Originating Requests** check box is selected, the source IP address will look like the local interface address on the Real Server's subnet.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

Depending on transparency and SOR, the Real Server may see traffic originating from a different IP address.

Transparency	Subnet Originating Requests	Real Server sees
Disabled	Disabled	VS address
Disabled	Enabled	LoadMaster Real Server-side interface address
Enabled	Disabled	Client IP address
Enabled	Enabled	Client IP address

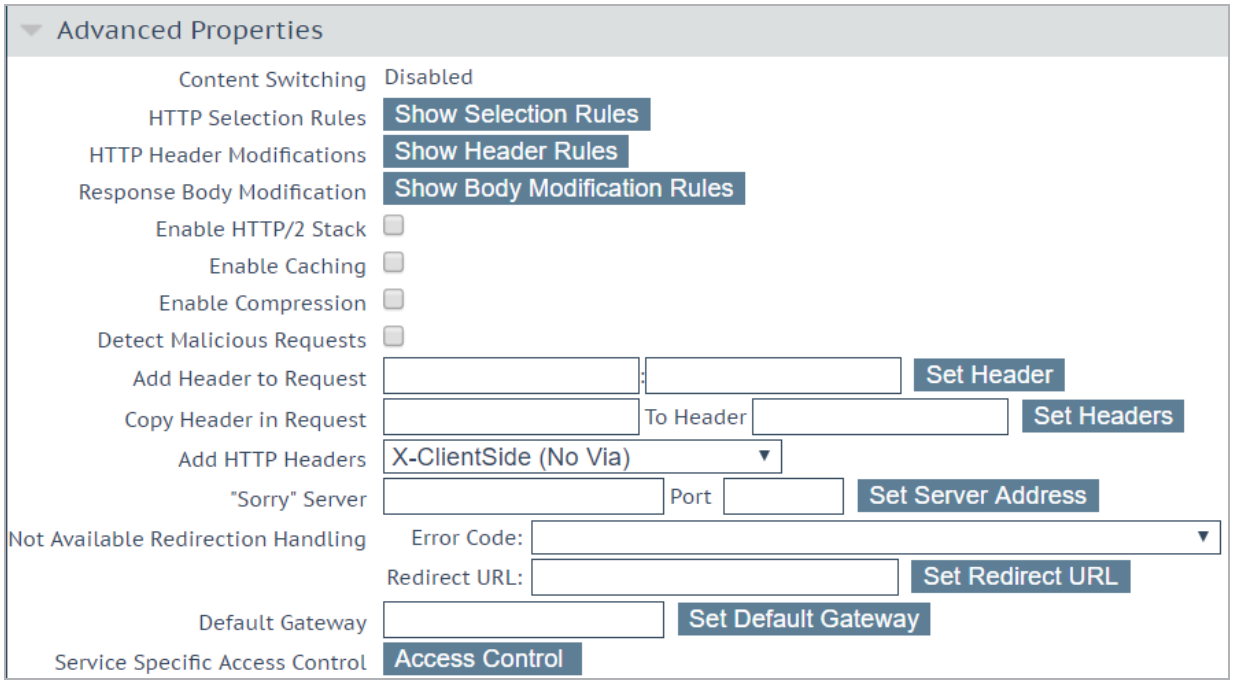
If transparency is enabled, SOR does not have any effect on the routing of traffic.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

4 Additional L7 HTTP Header

> This section only applies to Virtual Services with the **HTTP/HTTPS Service Type**.

While the source IP address is not preserved in the regular sense with non-transparency, the LoadMaster does provide a method to retrieve the actual source IP address through an HTTP header.



For HTTP GET requests the LoadMaster inserts an additional HTTP header, called X-Forwarded-For, when L7 is used with non-transparency.

In order for these headers to be sent by the LoadMaster, the following conditions must be met:

- The Virtual Service must be operating L7 and be non-transparent
- The Add HTTP Headers drop-down in the Advanced Properties section must be set to something other than Legacy Operation(X-Forwarded-For)

What this means is that the Virtual Service must be operating at L7 because it is using either some L7 persistence mode (that is, not **Source IP Address**), content switching or SSL acceleration for it to send these headers.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

4.1 Configure the Log Files to Record X-Forwarded-For

Depending on the web server or application infrastructure the X-Forwarded-For value can be configured to be logged. Refer to the relevant section below to find out how to do this.

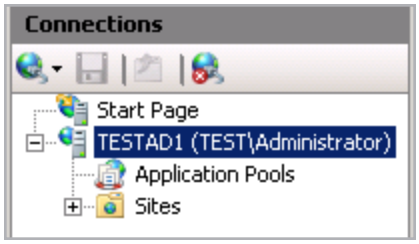
> These steps were correct at time of writing. Please refer to the relevant vendor documentation for up-to-date steps.

4.1.1 Record the X-Forwarded-For Header in IIS 7

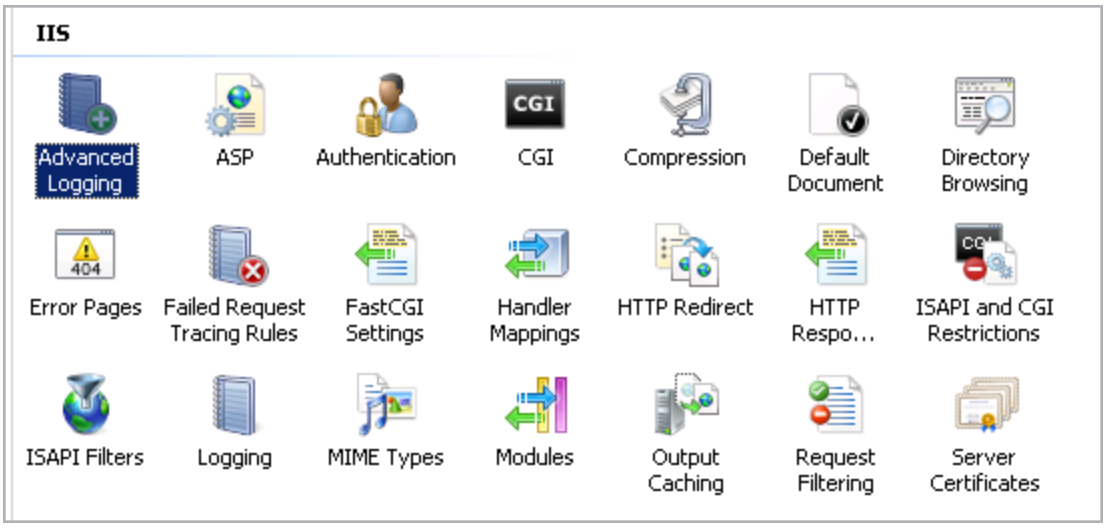
To record the X-Forwarded-For header in IIS 7, follow the steps below:

1. First, IIS Advanced Logging will need to be installed. This can be downloaded from the Microsoft website: IIS Advanced Logging. After this has been installed, an extra option called **Advanced Logging** will appear for the sites in IIS.

2. Open the IIS Manager.

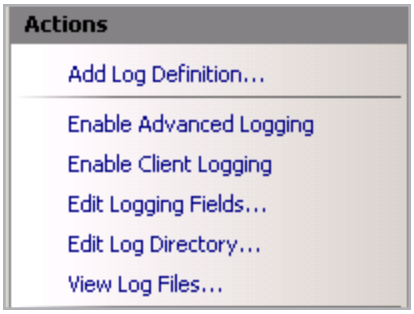


3. In the **Connections** section on the left, select the relevant directory, server or website to configure the **Advanced Logging** on.

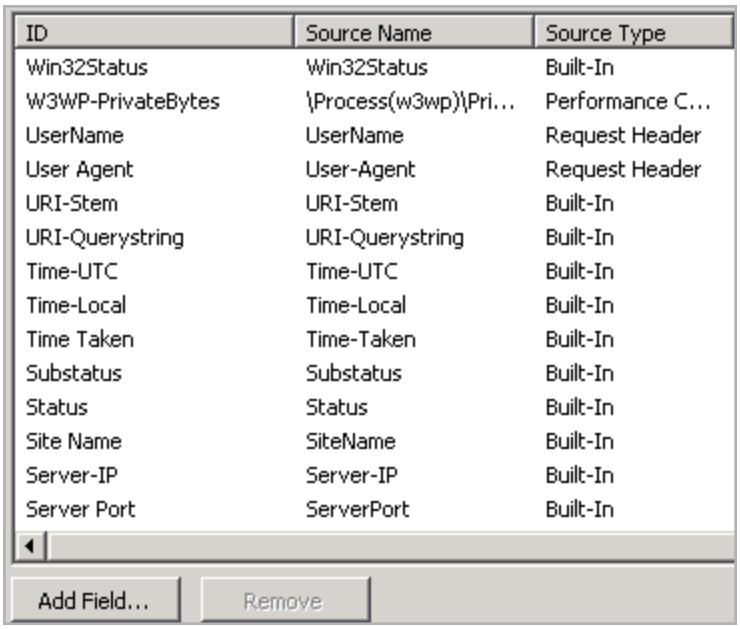


Copyright 2002-2020, Kemp Technologies, All Rights Reserved

4. In the **Home** section, under **IIS**, double-click **Advanced Logging**.

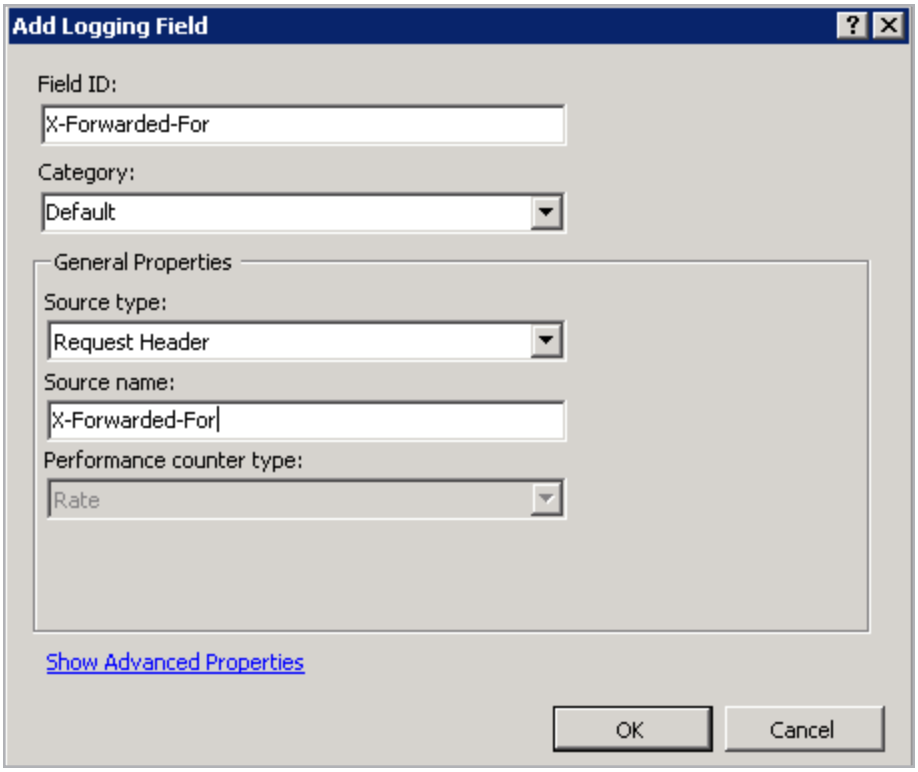


5. On the right, click **Edit Logging Fields**.

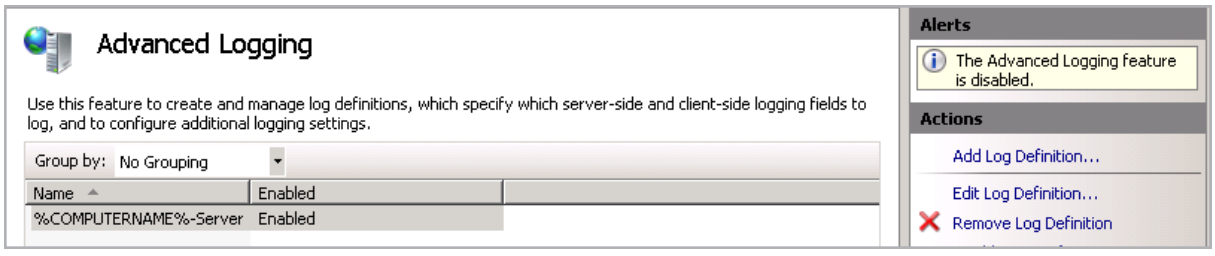


6. Click **Add Field**.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

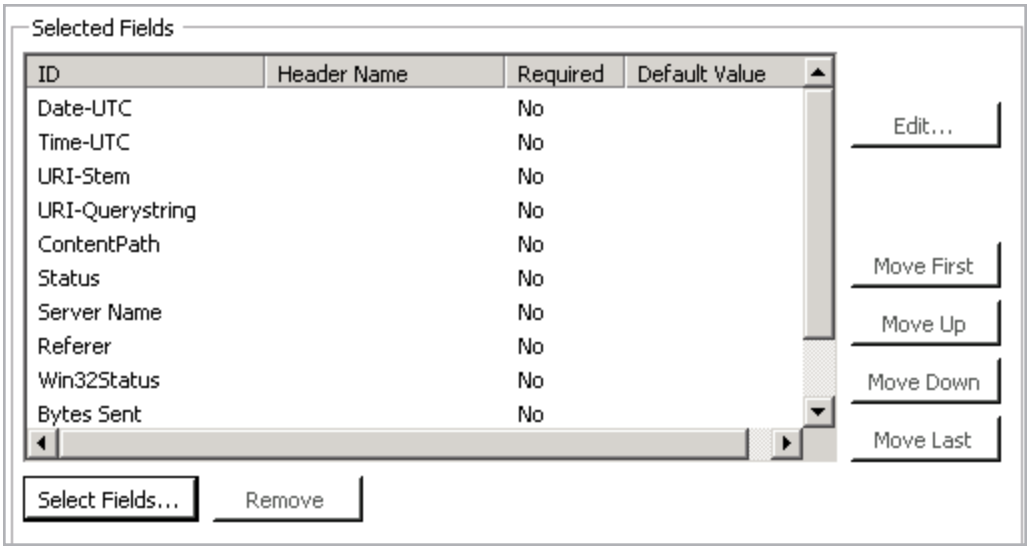


7. Enter **X-Forwarded-For** in the **Field ID** text box.
8. Select **Default** as the **Category**.
9. Select **Request Header** as the **Source Type**.
10. Enter **X-Forwarded-For** in the **Source Name** text box.
11. Click **OK**.
12. Click **OK** again.

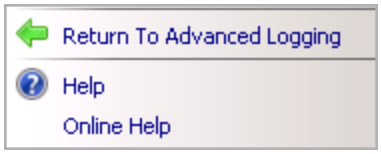


13. Select a log definition. By default, there is only one: **%COMPUTERNAME%-Server**. The log definition selected must be **Enabled**.
14. Click **Edit Log Definition**.

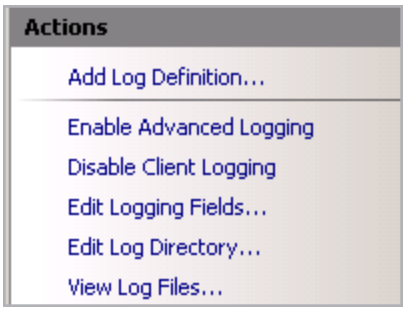
Copyright 2002-2020, Kemp Technologies, All Rights Reserved



15. Scroll down and click **Select Fields**.
16. Select the **X-Forwarded-For** logging check box.
17. Click **OK**.
18. Click **Apply**.



19. Click **Return to Advanced Logging**.



20. Click **Enable Advanced Logging**.

After completing these steps, the client IP address is included in the logs.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

4.1.2 Record the X-Forwarded-For Header in Apache

For Apache, the combined format in the HTTPD configuration file is as follows:

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"\"%{forensic-id}n\"" combined

Add the client side field by adding **%{X-Forwarded-For}**.

LogFormat "%{X-Forwarded-For}i %l %u %t "%r" %>s %b "%{Referer}i""%{User-Agent}i"" combined

Another available option in the **Add HTTP Headers** drop-down list is **X-Client-Side** header. This is just an alternative to the **X-Forwaded-For** header.

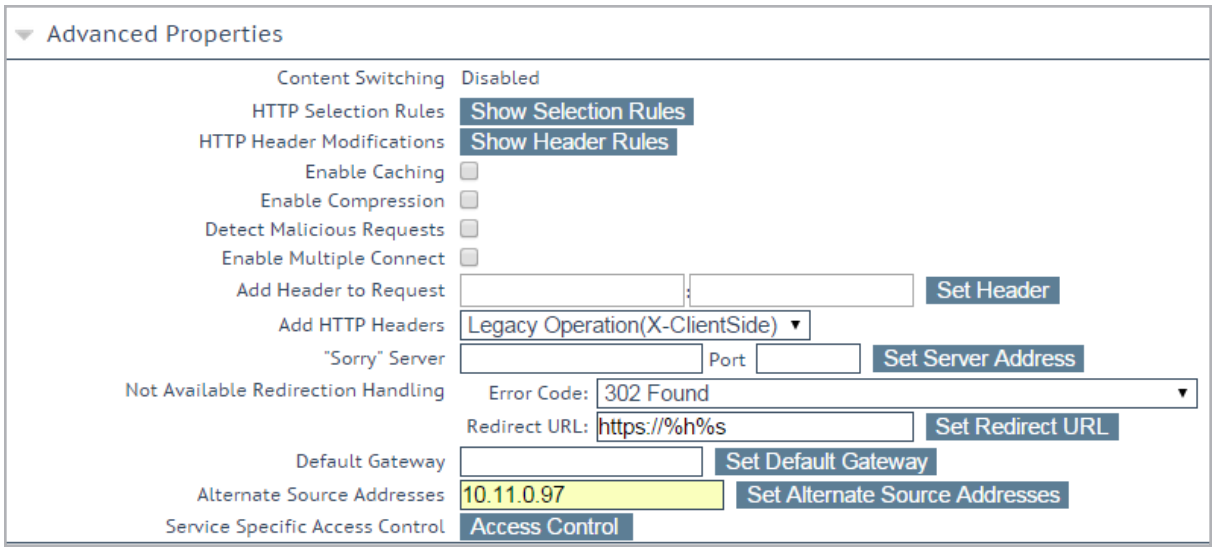
To log these in Apache, use the following code:

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"\"%{forensic-id}n\" \”%{X-ClientSide}" combined-ClientSide

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

5 Alternate Source Addresses

If required, alternate source addresses can be specified per Virtual Service.



This field is available in the **Advanced Properties** section of the Virtual Service modify screen.

> This option is only available if the **Allow connection scaling over 64K Connections** option is enabled in the **System Configuration > Miscellaneous Options > L7 Configuration** screen.

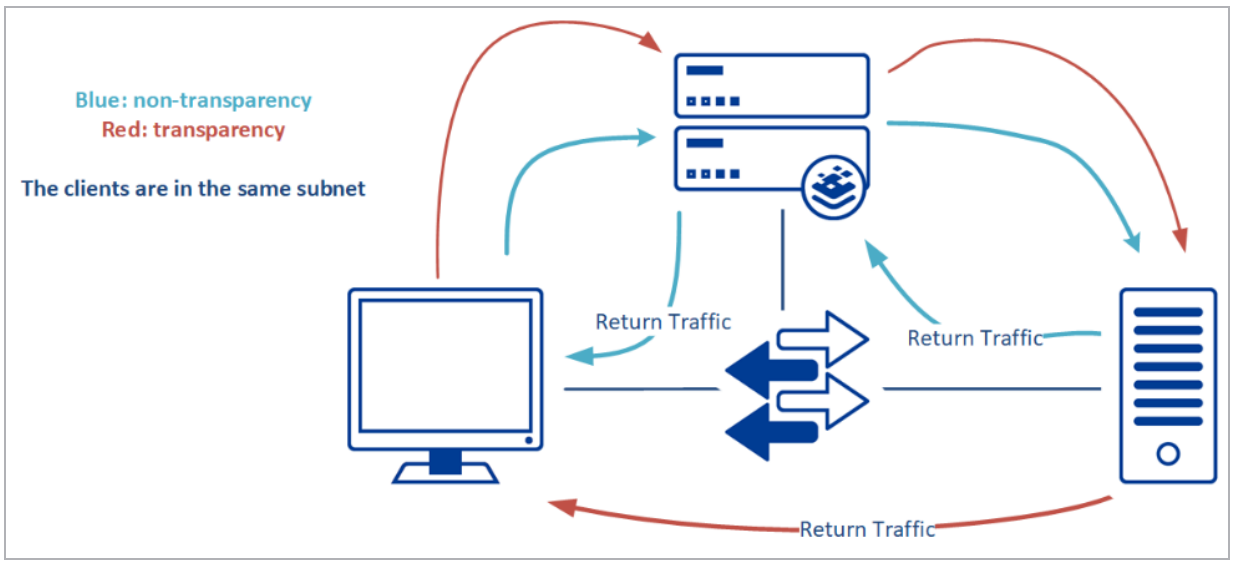
If no list is specified, the LoadMaster will use the IP address of the Virtual Service as its local address. Specifying a list of **Alternate Source Addresses** ensures that the LoadMaster will use these addresses instead.

Using an **Alternate Source Address** will allow more source ports to be used. With one IP address we are limited to 64,000. In order to use more, at least two additional IP addresses must be added in this field. One of the IP addresses can be the Virtual Service address.

Another benefit to using an **Alternate Source Address** is to change the source address that the Real Server is going to see. This is helpful in the case where the Real Server and the Virtual Service are on separate subnets and the Real Server does not have a route back. Adding an alternate source IP address on the Real Server subnet will allow symmetrical routing without having to add static routes on the Real Server.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

6 Transparency vs. Non-Transparency Browsing



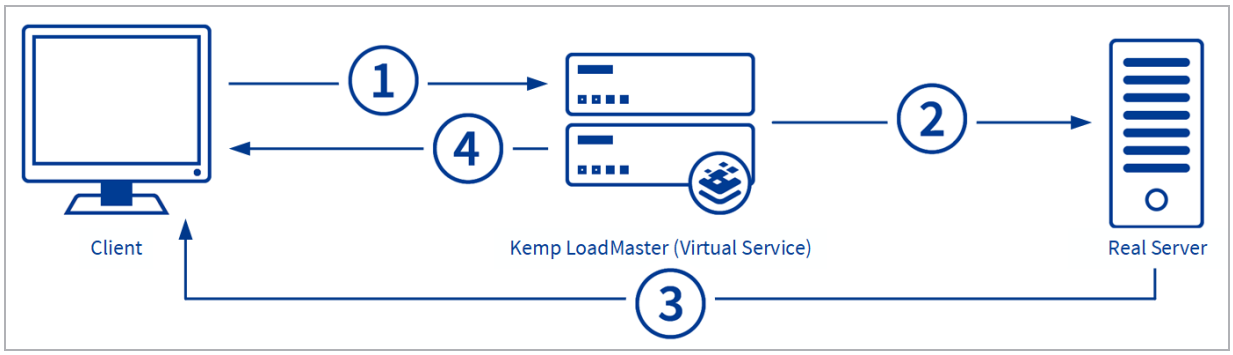
6.1 Why is it not possible to browse from the same subnet with transparency?

In a network configuration with transparency enabled, the reason why you cannot browse from the local network is because of the path that the traffic flows. As stated, in order for a load balancer to do its job, the load balancer must be in the path of both inbound and outbound traffic. Load balancing typically happens in four steps. Traffic flows from the:

1. Client to the Virtual Service on the LoadMaster
2. LoadMaster to the Real Server
3. Real Server to the LoadMaster
4. LoadMaster to the client

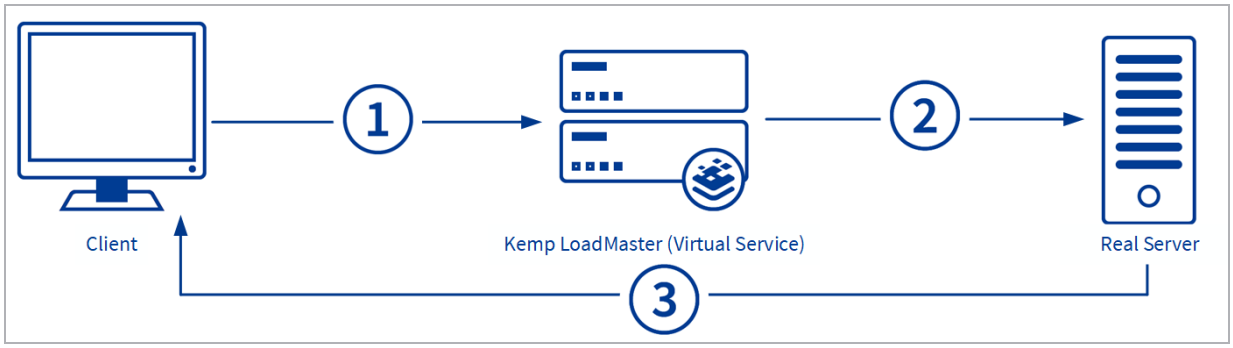
Take the example of a simple one-armed configuration, where the client IP address is 64.254.1.12, the Virtual Service address is 192.168.1.200, and the Real Server is 192.168.1.100. The diagram and table below shows what happens in a regular connection:

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved



Step	Path	Source IP	Destination IP
1	Client to Virtual Service	64.254.1.12	192.168.1.200
2	Virtual Service to Real Server	64.254.1.12	192.168.1.100
3	Real Server to Client (before LoadMaster)	192.168.1.100	64.254.1.12
4	Virtual Service to Client (after LoadMaster)	192.168.1.200	64.254.1.12

Now, take the same example except this time the client will have the IP address of 192.168.0.10, which is on the same subnet as the Real Server.



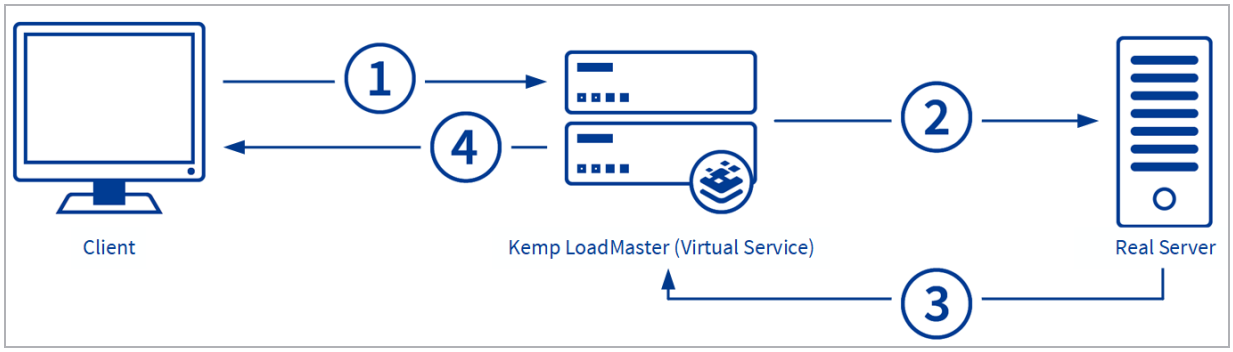
Step	Path	Source IP	Destination IP
1	Client to Virtual Service	192.168.0.10	192.168.1.200
2	Virtual Service to Real Server	192.168.0.10	192.168.1.100
3	Real Server to Client (before LoadMaster)	192.168.1.100	192.168.0.10

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

The response comes back from a different IP address than the client was expecting, so the client drops the traffic entirely and the page never loads.

6.2 Why is it possible to browse from the same subnet with non-transparency?

Non-transparency replaces the IP address of the client with the IP address of the LoadMaster itself, thereby forcing traffic back through the LoadMaster on the way out. When the Real Server responds to the request, it responds to the LoadMaster. The LoadMaster then forwards the traffic along to the client.



Step	Path	Source IP	Destination IP
1	Client to Virtual Service	192.168.0.10	192.168.1.200
2	Virtual Service to Real Server	192.168.1.200	192.168.1.100
3	Real Server to Virtual Service (before LoadMaster)	192.168.1.100	192.168.1.200
4	Virtual Service to Client (after LoadMaster)	192.168.1.200	192.168.0.10

Notice that in the first transparency table (in the **Why is it not possible to browse from the same subnet with transparency?** section) either the source IP or the destination IP was rewritten, but not both. In the non-transparency table above (in the **Why is it possible to browse from the same subnet with non-transparency?** section) both the source IP and destination IP were re-written. This is why the logs of the web server will only see the IP address of the LoadMaster for all incoming connections when transparency is disabled (as it is by default).

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

7 Troubleshooting

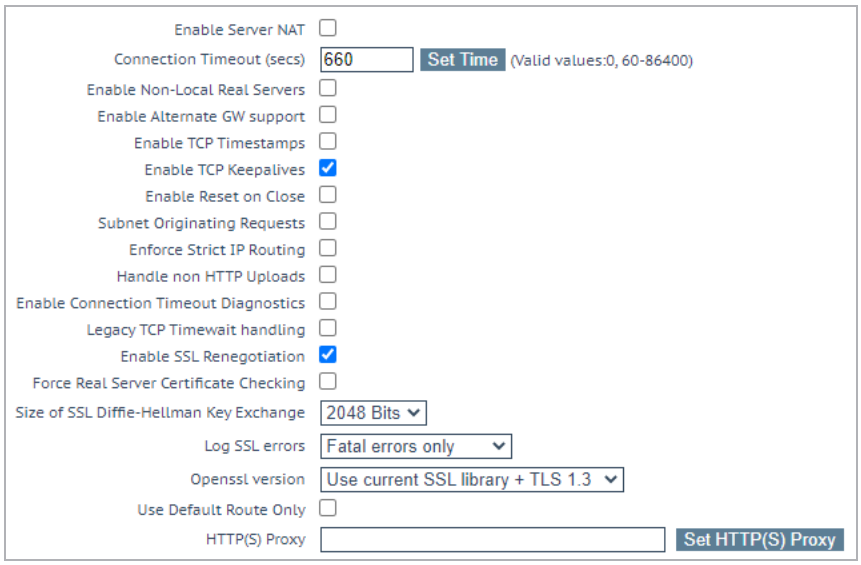
7.1 Unable to Connect to Real Servers using Remote Desktop Protocol (RDP)

After enabling transparency, RDP connections may not work. To resolve this problem, refer to the relevant section below depending on your setup.

7.1.1 One-Arm Setup

If you have a one-arm setup – disable Server Network Address Translation (SNAT). This will allow access to Real Servers using RDP. To do this, follow the steps below in the LoadMaster:

1. In the main menu of the LoadMaster WUI, select **System Configuration > Miscellaneous Options > Network Options**.



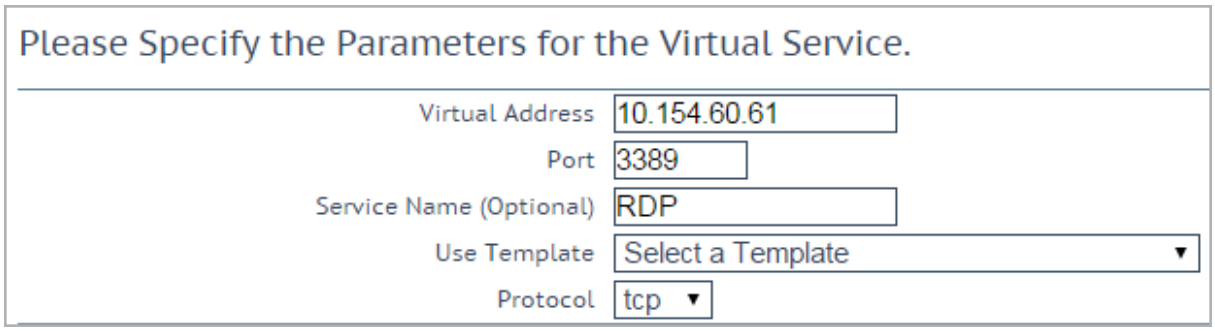
2. Remove the tick from the **Enable Server NAT** check box.

7.1.2 Two-Arm Setup

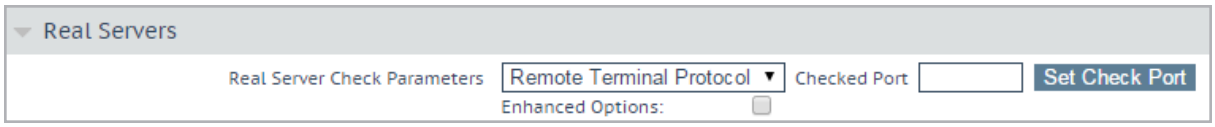
If you have a two-arm setup – create an RDP Virtual Service by following the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services > Add New**.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved



2. Create a Virtual Service on port **3389**.



3. Expand the **Real Servers** section and add the Real Server to be accessed.

After this Virtual Service has been created, the Real Server is accessible using RDP.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

Web User Interface (WUI), Configuration Guide

Configuring DSR, Technical Note

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

Last Updated Date

This document was last updated on 07 December 2020.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved