



Load Balancing Trend Micro InterScan Web Security Gateway

v1.4.2

Deployment Guide

NOTE: This guide has been archived and is no longer being maintained. While the content is still valid for the particular software versions mentioned, it may refer to outdated software that has now reached end-of-life.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

Contents

1. About this Guide.....	4
2. Loadbalancer.org Appliances Supported.....	4
3. Loadbalancer.org Software Versions Supported.....	4
4. Trend Micro Web InterScan Web Gateway Appliances Supported.....	4
5. Benefits of Implementing a Load Balancer.....	5
6. Load Balancer Configuration Options.....	5
<i>Deployment Modes</i>	5
Layer 4 (Recommended).....	5
Layer 7.....	6
<i>Persistence / Server Affinity</i>	6
Source IP Address (Recommended).....	6
Destination Hash.....	6
7. Web Gateway Deployment Modes.....	6
1 – Explicit Proxy Mode (Recommended).....	6
2 – Transparent Routed Proxy Mode.....	6
8. Summary of Deployment Options.....	7
9. Loadbalancer.org Appliance – the Basics.....	8
<i>Virtual Appliance Download & Deployment</i>	8
<i>Initial Network Configuration</i>	8
<i>Accessing the Web User Interface (WebUI)</i>	8
<i>HA Clustered Pair Configuration</i>	10
10. Option 1 – Explicit Proxy Mode (Recommended).....	11
<i>Option 1A – Using DR (Direct Return) Mode (Recommended)</i>	11
Deployment Architecture.....	11
Load Balancer Configuration.....	12
Web Gateway Configuration.....	13
Finalize Settings.....	15
<i>Option 1B – Using NAT Mode</i>	16
Deployment Architecture.....	16
Load Balancer Configuration.....	17
Web Gateway Configuration.....	19
Finalize Settings.....	20
<i>Option 1C – Using NAT Mode (Preferred NAT Topology)</i>	21
Deployment Architecture.....	21
Load Balancer Configuration.....	22
Web Gateway Configuration.....	24
Finalize Settings.....	24
<i>Configuration Settings Common to Options 1A, 1B & 1C</i>	25
Web Gateway Operating Mode.....	25
Proxy Port Configuration.....	25
Client Configuration.....	26
11. Option 2 – Transparent Routed Proxy Mode.....	27
Deployment Architecture.....	27

<i>Load Balancer Configuration</i>	28
Create the Virtual Service (VIP).....	28
Add the Floating IP.....	29
Configure Firewall Rules.....	29
Define the Real Servers (RIPs).....	30
<i>Web Gateway Configuration</i>	31
Web Gateway Operating Mode.....	31
<i>Router/Default Gateway Configuration</i>	32
<i>Client Configuration</i>	33
12. Testing & Validation.....	33
Layer 4 – Current Connections.....	33
13. Technical Support.....	34
14. Further Documentation.....	35
15. Conclusion.....	35
16. Appendix.....	35
1 – Clustered Pair Configuration – Adding a Slave Unit.....	35
2 – Modified Transparent Mode Firewall Rules.....	37
17. Document Revision History.....	39

1. About this Guide

This guide details the steps required to configure a load balanced Trend Micro InterScan Web Gateway environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Trend Micro InterScan Web Gateway configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the relevant Administration Manual:

- [v7 Administration Manual](#)
- [v8 Administration Manual](#)

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Trend Micro InterScan Web Gateways. The complete list of models is shown below:

Discontinued Models	Current Models *
Enterprise R16	Enterprise R20
Enterprise VA R16	Enterprise MAX
Enterprise VA	Enterprise 10G
Enterprise R320	Enterprise 40G
	Enterprise Ultra
	Enterprise VA R20
	Enterprise VA MAX
	Enterprise AWS **
	Enterprise AZURE **
	Enterprise GCP **

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

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

3. Loadbalancer.org Software Versions Supported

- v7.6.4 and later

4. Trend Micro Web InterScan Web Gateway Appliances Supported

- All versions

Note that the Trend Micro InterScan Web Security Virtual Appliance (v6.5) was used in the lab environment for this guide

5. Benefits of Implementing a Load Balancer

Implementing Loadbalancer.org appliances enables multiple Trend Micro InterScan Web Gateways to be deployed in a cluster. This provides the following key benefits:

- **High-Availability** – If a Web Gateway fails, service is not interrupted
- **Maintenance** – Web Gateways can easily be taken out of the cluster for maintenance
- **Performance** – For additional performance simply add more Web Gateways to the cluster

6. Load Balancer Configuration Options

The following sections describe the various load balancer deployment modes and persistence options that are used when load balancing Web Gateways.

Deployment Modes

Layer 4 (Recommended)

DR Mode - Direct Server Return Mode (Recommended)

In this mode, traffic from the client to the Web Gateway passes via the load balancer, return traffic passes directly back to the client which maximizes performance. Direct routing works by changing the destination MAC address of the incoming packet on the fly which is very fast. This mode is transparent by default meaning that the Web Gateway sees the real client IP address and not the IP address of the load balancer.

Due to its speed, overall simplicity and effectiveness, Direct Routing (DR) mode with source IP persistence is our recommended method and can be used in both Explicit Proxy Mode & Transparent Routed Proxy Mode.

NAT Mode - Network Address Translation Mode

This mode requires the implementation of a two-arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works). Return traffic MUST pass back via the load balancer. This can be achieved by either setting the default gateway on the Web Gateways to be the load balancer or by configuring a static route on the Web Gateways that forces client return traffic to pass back via the load balancer. This mode offers high performance and like DR mode is transparent by default.

Layer 7

SNAT Mode - Source Network Address Translation

Using HAProxy in SNAT mode means that the load balancer is acting as a full proxy and therefore it doesn't have the same raw throughput as the layer 4 methods. Also, this method is not transparent by default so the real servers (i.e. the Web Gateways) will see the source address of each request as the load balancers IP address. This is generally not desirable, although this can be resolved in two ways: either by reading the X-Forwarded-For header that's included by default when using HAProxy, or by enabling TProxy on the load balancer. The issue with using TProxy is that the default gateway on the real servers must be changed to be the load balancer and it also requires a two-arm infrastructure with two subnets which complicates the deployment. The same requirements apply when using layer 4 NAT mode as mentioned above. SNAT mode does not have the raw throughput of the layer 4 solutions and is therefore not normally used for Web Gateway load balancing deployments.

Persistence / Server Affinity

Persistence may or may not be required and depends on the specific Web Gateway being used. Two possible methods are described in the following sections.

Source IP Address (Recommended)

Source IP persistence is the default option for Layer 4 services and can easily be selected for Layer 7 services. When set, clients connecting from the same source IP address within the persistence timeout period (the default is 5 minutes) will always be sent to the same Web Gateway.

Destination Hash

Another option at Layer 4 is to change the load balancing algorithm (i.e. the "scheduler") to destination hash (DH). This causes the load balancer to select the Web Gateway based on a hash of the destination IP address. This causes session requests to be directed at the same server based solely on the destination IP address of a packet which therefore makes client connections persistent for a particular Internet host.

Since this setting is a scheduler, the way connections are load balanced will also change. However it should still provide a well balanced distribution of client sessions between Web Gateways.

7. Web Gateway Deployment Modes

There are two implementation methods that are typically used when deploying with a load balancer – these are Explicit Proxy Mode & Transparent Routed Proxy Mode.

1 – Explicit Proxy Mode (Recommended)

This mode requires the load balancers VIP address to be defined in users browsers. This means that the load balancer will receive client requests and distribute these requests between the back-end Web Gateways. Trend Micro refer to this mode as **Forward Proxy Mode**. Please refer to the section starting on page [11](#) for configuration details.

2 – Transparent Routed Proxy Mode

With this mode, client requests must be routed to the load balancer/Web Gateway cluster. This can be achieved by adding rules to the default gateway device. Rules are configured for HTTP & HTTPS traffic on ports 80 and 443. Please refer to the section starting on page [27](#) for configuration details.

Note: When configuring the Web Gateways, **Simple Transparency Mode** should be selected. Please refer to page [31](#) for more details.

In this mode it's not possible to filter HTTPS traffic. This is because SSL cannot be proxied transparently. SSL authenticates both sides of the connection and if a proxy is in the middle, then both sides try to authenticate to the proxy which is incorrect and therefore the connection fails. We recommend using Explicit Proxy Mode rather than Transparent Routed Proxy Mode when possible due to this limitation.

8. Summary of Deployment Options

Option	Web Gateway Mode	Load Balancer Mode	Notes
Option 1A (Recommended)	Forward Proxy Mode	DR Mode	The Web Gateways must be configured to accept traffic for the VIP. Please refer to page 11 for configuration details.
Option 1B	Forward Proxy Mode	NAT Mode	The load balancer must be set as the default gateway for the Web Gateways. Please refer to page 16 for configuration details.
Option 1C	Forward Proxy Mode	NAT Mode	A static route must be configured on the Web Gateways to send client return traffic back via the load balancer. Please refer to page 21 for configuration details.
Option 2	Simple Transparency Mode	DR Mode	Firewall rules must be added to the load balancer to transparently send traffic to the Web Gateways. Please refer to page 27 for configuration details.

9. Loadbalancer.org Appliance – the Basics

Virtual Appliance Download & Deployment

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk. The Virtual Appliance can be downloaded [here](#).

Note: The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

Note: Please refer to the [Administration Manual](#) and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Initial Network Configuration

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

Method 1 - Using the Network Setup Wizard at the console

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Method 2 - Using the WebUI

Using a browser, connect to the WebUI on the default IP address/port: **https://192.168.2.21:9443**

To set the IP address & subnet mask, use: *Local Configuration > Network Interface Configuration*

To set the default gateway, use: *Local Configuration > Routing*

To configure DNS settings, use: *Local Configuration > Hostname & DNS*

Accessing the Web User Interface (WebUI)

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

2. Login to the WebUI:

Username: loadbalancer

Password: loadbalancer

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

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

SYSTEM OVERVIEW ?

2015-06-18 14:21:20 UTC

Would you like to run the Setup Wizard?

Accept

Dismiss

VIRTUAL SERVICE

IP

PORTS

CONN
S

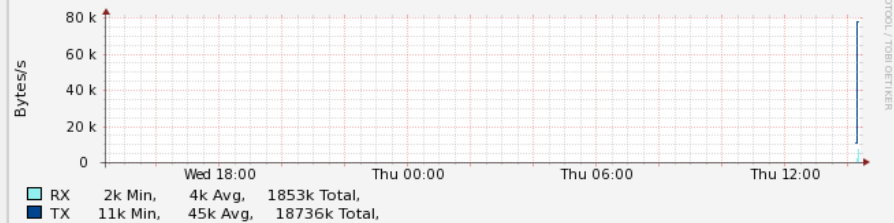
PROTOCOL

METHOD

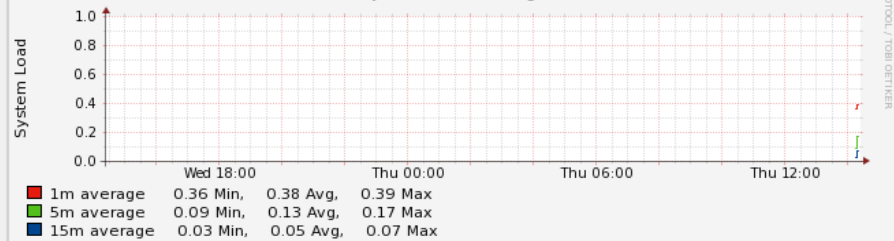
MODE

No Virtual Services configured.

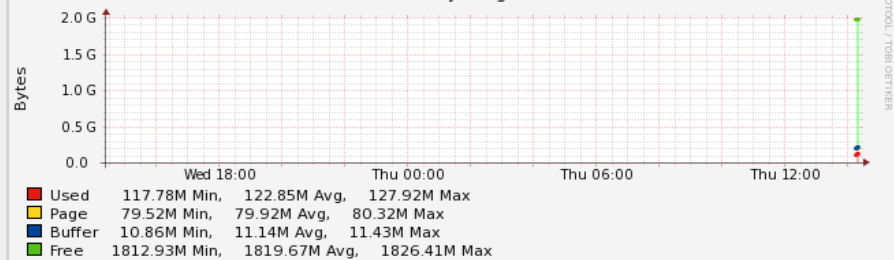
Network Bandwidth



System Load Average



Memory Usage



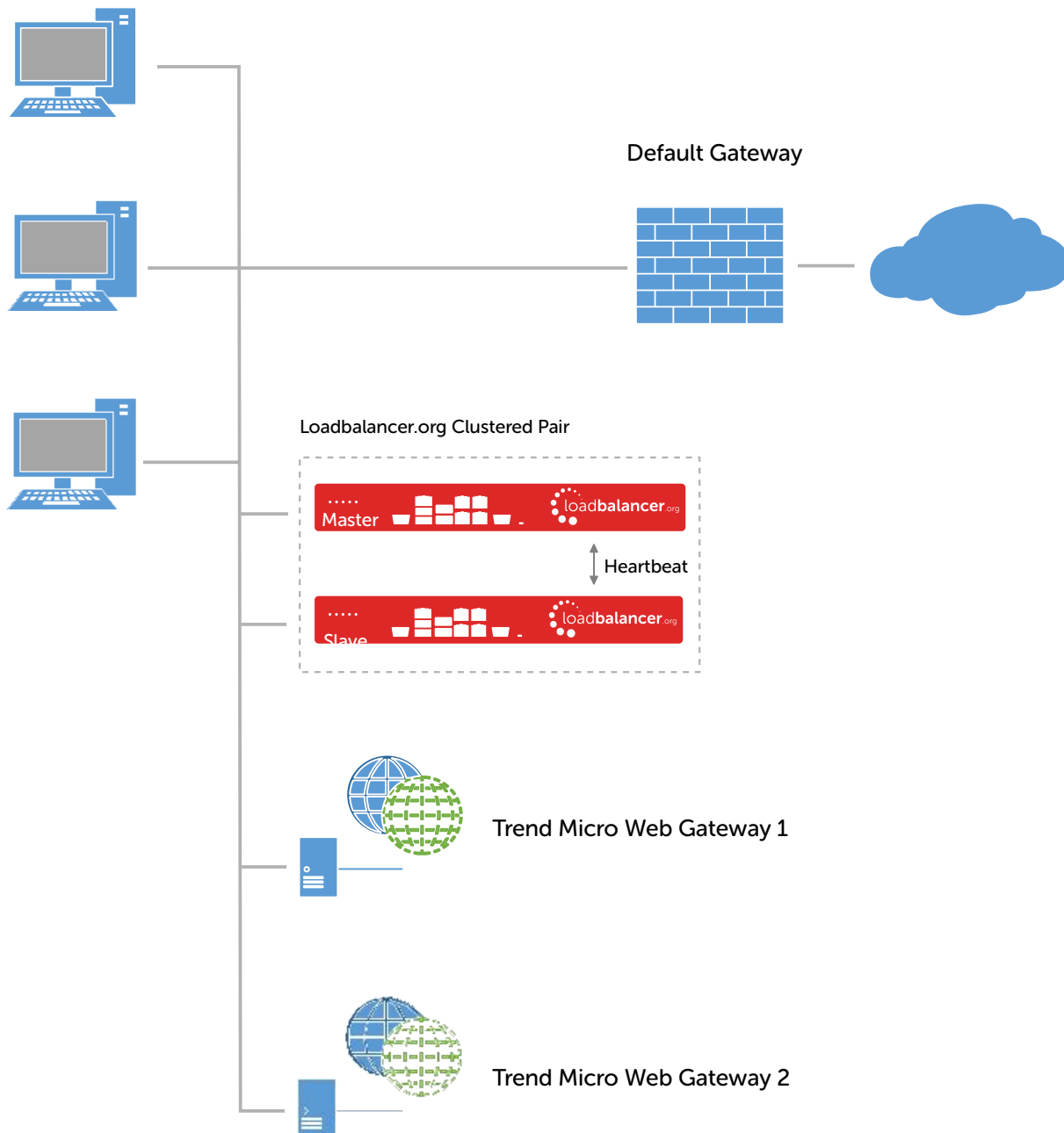
HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page [35](#).

10. Option 1 – Explicit Proxy Mode (Recommended)

Option 1A – Using DR (Direct Return) Mode (Recommended)

Deployment Architecture



Notes:

- Browser settings on client PC's must be changed to point at the Virtual Service (VIP) on the load balancer (see page [26](#))

- The load balancer is configured in one-arm Layer 4 DR mode
- The Trend Micro Web Gateways must be configured to accept traffic for the VIP (see page [13](#))
- Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page [35](#)
- For more information on Trend Micro Web Gateway deployment options please refer to [this URL](#)

Load Balancer Configuration

Create the Virtual Service (VIP)

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

Label	<input type="text" value="Proxy"/>	?
Virtual Service	IP Address	<input type="text" value="192.168.2.202"/>
	Ports	<input type="text" value="8080"/>
Protocol	<input type="text" value="TCP"/>	?
Forwarding Method	<input type="text" value="Direct Routing"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

4. Enter an appropriate label (name) for the VIP, e.g. **Proxy**
5. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.202**
6. Set the *Virtual Service Ports* field to the required port, e.g. **8080**
7. Ensure that *Protocol* is set to **TCP**
8. Ensure that *Forwarding Method* is set to **Direct Routing**
9. Click **Update**
10. Now click **Modify** next to the newly created VIP
11. Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour)
12. Click **Update**

Define the Real Servers (RIPs)

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

Label	<input type="text" value="Proxy1"/>	?
Real Server IP Address	<input type="text" value="192.168.2.210"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

4. Enter an appropriate label (name) for the first Web Gateway, e.g. **Proxy1**
5. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.210**
6. Click **Update**
7. Repeat the above steps to add your other Web Gateway(s)

Web Gateway Configuration

Note: By default the password for admin, root, and enable accounts is **adminIWSS85**. This can also be set during the installation process when IWSVA is deployed from the ISO file.

Modify the Web Gateways to accept traffic for the VIP

Concept

As mentioned previously, DR mode is our recommended load balancer operating mode. To use this mode, changes are required to the real servers, i.e. the Web Gateways. The real servers must accept traffic for the VIP, but they must not respond to any ARP requests for that IP, only the VIP should do this.

To configure a Linux based Web Gateway to accept traffic for the VIP, the iptables command below must be added to an appropriate startup script such as **/etc/rc.local** so that it is automatically executed each time the Web Gateway boots. It can also be executed immediately by running the command at the command prompt, but the setting will be lost after a reboot unless the command has been added to a startup script.

```
iptables -t nat -A PREROUTING -p tcp -d <VIP address> -j REDIRECT
```

e.g.

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.2.202 -j REDIRECT
```

i.e. Redirect any incoming packets destined for the VIP to the local address

Note: For more information please refer to the [Administration Manual](#) and search for 'ARP Problem'.

Configuring the Trend Micro Appliance

Note: These steps must be followed on all Gateways.

1. Login as root either at the console or using a remote SSH session
2. Edit the file **/etc/rc.local** using **vi**, **vim** or a remote editor such as the one included in WinSCP
3. Then add the following additional line to this file, setting the VIP address as required, as shown below:

```
iptables -t nat -A PREROUTING -p tcp -d <VIP address> -j REDIRECT
```

```

#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local

F_check_ipmiDevice()
{
    rm -f /var/iwss/ipmi/.sensor_valid.txt
    if [ -e /tmp/ipmi0 -o -e /tmp/ipmi/0 -o -e /tmp/ipmidev/0 ] ;then
        return 0
    fi

    /sbin/modprobe ipmi_msghandler >/dev/null 2>&1
    if [ $? -ne 0 ];then
        return 1
    fi
    /sbin/modprobe ipmi_si >/dev/null 2>&1
    if [ $? -ne 0 ];then
        return 1
    fi
    /sbin/modprobe ipmi_devintf >/dev/null 2>&1
    if [ $? -ne 0 ];then
        return 1
    fi

    return 0
}
F_check_ipmiDevice

iwss_cfg="/etc/iscan/intscan.ini"
F_log_offload_import_init()
{
    log_offload_mount_cmd=`grep mount_device $iwss_cfg | cut -d = -f 2`
    if [ "$log_offload_mount_cmd" != "" ];then
        $log_offload_mount_cmd
        chown iscan:iscan /var/offload
    fi
}
F_log_offload_import_init

iptables -t nat -A PREROUTING -p tcp -d 192.168.2.202 -j REDIRECT

```

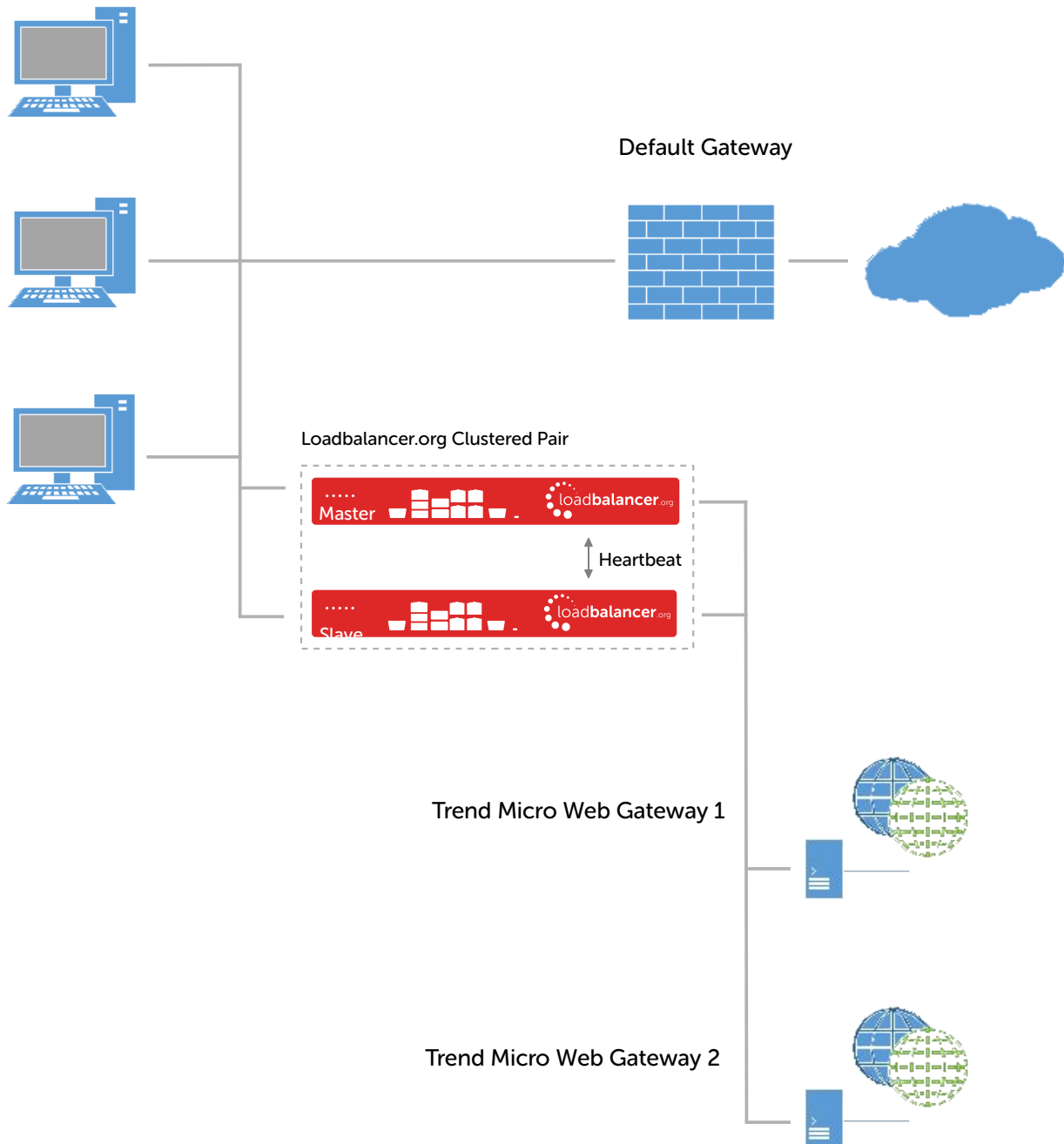
4. Reboot the Web Gateway to apply the new setting

Finalize Settings

Now refer to the section "*Configuration Settings Common to Options 1A, 1B & 1C*" on page [25](#) to finalize Web Gateway settings and configure client browser settings.

Option 1B – Using NAT Mode

Deployment Architecture



Notes:

- Browser settings on client PC's must be changed to point at the Virtual Service (VIP) on the load balancer (see page [26](#))
- The load balancer is configured in two-arm Layer 4 NAT mode
- Return traffic MUST pass back via the load balancer. To enable this, the default gateway for the Web Gateways

is configured to be the load balancer. For an HA pair, a floating IP address must be configured to allow the gateway to move between master and slave in the event of a failover (see page [17](#))

- Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page [35](#)
- For more information on Trend Micro Web Gateway deployment options please refer to [this URL](#)

Load Balancer Configuration

Configure Network Settings

Two interfaces are required. Typically eth0 is used for the internal (Web Gateway) subnet and eth1 is used for the external (client & VIP) subnet, although this is not mandatory since interfaces can be used as required / preferred.

To configure network settings on the load balancer:

1. Ensure that the required cables are plugged in (hardware) or virtual NICs are connected (virtual)
2. Using the WebUI, navigate to: *Local Configuration > Network Interface Configuration*
3. Define the required IP addresses and subnet mask:

The screenshot shows the 'IP Address Assignment' configuration page. At the top, there are four network interface icons: eth0 (10 GB/s), eth1 (10 GB/s), eth2 (disabled with a red X), and eth3 (disabled with a red X). Below the icons, the configuration for eth0 and eth1 is shown. For eth0, the IP address is 192.168.4.200/24 and the MTU is 1500 bytes. For eth1, the IP address is 192.168.2.200/24 and the MTU is 1500 bytes.

4. Configure the required IP address for eth0, e.g. **192.168.4.200/24**
5. Configure the required IP address for eth1, e.g. **192.168.2.200/24**
6. Click **Configure Interfaces**

Define a Floating IP to be used as the Default Gateway for the Web Gateways

As mentioned, when using a clustered pair of load balancers for HA (our recommended configuration), a floating IP must be used as the default gateway for the Web Gateways. This will 'float' between the master and slave units in the event of a failover or failback. This ensures that the Web Gateways always have a consistent return path via the load balancer – whether the master or slave is active.

To configure a Floating IP:

1. Using the WebUI, navigate to: *Cluster Configuration > Floating IP's*

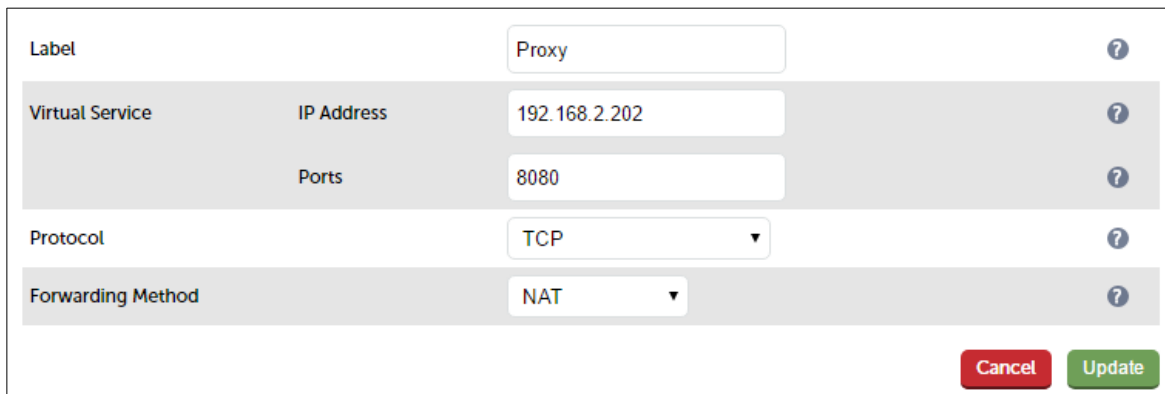


New Floating IP	<input type="text" value="192.168.4.205"/>	<button>Add Floating IP</button>
-----------------	--	----------------------------------

2. Define a suitable IP address for the default gateway , e.g. **192.168.4.205**
3. Click **Add Floating IP**

Create the Virtual Service (VIP)

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



Label	<input type="text" value="Proxy"/>	?	
Virtual Service	IP Address	<input type="text" value="192.168.2.202"/>	?
	Ports	<input type="text" value="8080"/>	?
Protocol	<input type="text" value="TCP"/>	▼	?
Forwarding Method	<input type="text" value="NAT"/>	▼	?
			<button>Cancel</button> <button>Update</button>

4. Enter an appropriate label (name) for the VIP, e.g. **Proxy**
5. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.202**
6. Set the *Virtual Service Ports* field to the required port, e.g. **8080**
7. Ensure that *Protocol* is set to **TCP**
8. Ensure that *Forwarding Method* is set to **NAT**
9. Click **Update**
10. Now click **Modify** next to the newly created VIP
11. Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour)
12. Click **Update**

Define the Real Servers (RIPs)

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

Label	<input type="text" value="Proxy1"/>	?
Real Server IP Address	<input type="text" value="192.168.4.210"/>	?
Real Server Port	<input type="text" value="8080"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

4. Enter an appropriate label (name) for the first Web Gateway, e.g. **Proxy1**
5. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.4.210**
6. Set the *Real Server Port* field to the required port, e.g. **8080**
7. Click **Update**
8. Repeat the above steps to add your other Web Gateway(s)

Enable Auto-NAT

By default, servers behind the load balancer in a NAT configuration will not have access to the outside network. By enabling Auto-NAT, servers (i.e. the Web Gateways) will have their requests automatically mapped to the load balancer's external IP address. The default configuration is to map all requests originating from internal network eth0 to the external IP on eth1. A different interface can be selected if required.

To enable Auto-NAT on the load balancer:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Advanced configuration*

Email Alert Destination Address	<input type="text"/>	?
Auto-NAT	<input type="text" value="eth1 (Default)"/>	?
Multi-threaded	<input type="text" value="yes"/>	?
		<input type="button" value="Update"/>

2. Set the Auto-NAT field to the external interface. As mentioned the default configuration is to use eth1 and the external interface and eth1 as the internal interface, but can be set to suit your needs.
3. Click **Update**

Web Gateway Configuration

Note: By default the password for admin, root, and enable accounts is **adminIWS85**. This can also be set during the installation process when IWSVA is deployed from the ISO file.

Configure the Default Gateway

As mentioned, Option 1B requires the default gateway on the Web Gateways to be the load balancer. When using an HA pair of load balancers, the gateway on the load balancer must be a Floating IP to provide a consistent return path via the load balancer – whether the master or slave is active. Page [17](#) details how to create the Floating IP.

To set the default gateway using the WebUI (repeat for all Web Gateways) :

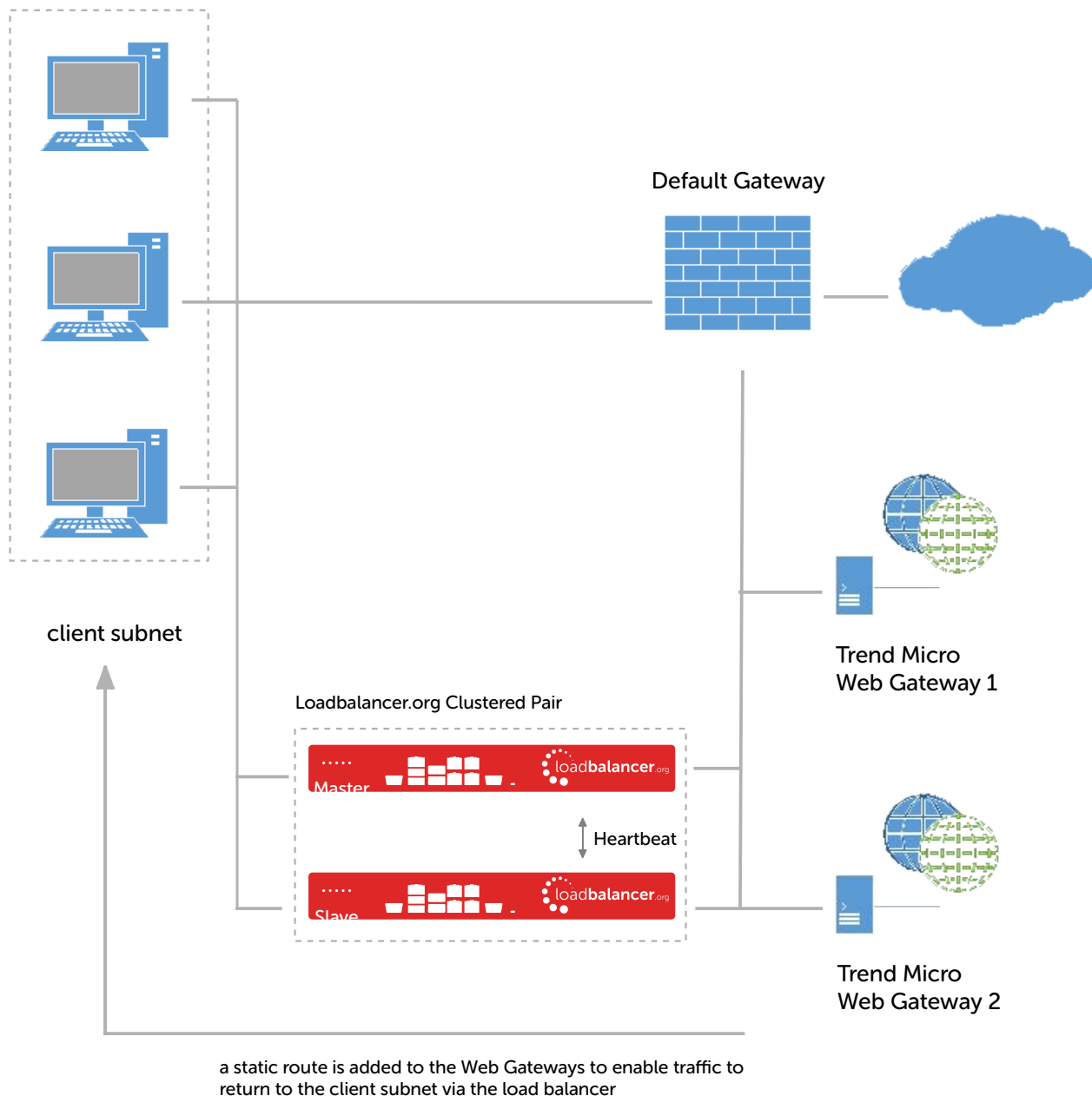
1. Login to the WebUI of the Web Gateway
2. Navigate to: *Administration > Network Configuration > Network Interface*
3. Define the required Gateway address, e.g. **192.168.4.205**
4. Click **Save**

Finalize Settings

Now refer to the section "*Configuration Settings Common to Options 1A, 1B & 1C*" on page [25](#) to finalize Web Gateway settings and configure client browser settings.

Option 1C – Using NAT Mode (Preferred NAT Topology)

Deployment Architecture



Notes:

- Browser settings on client PC's must be changed to point at the Virtual Service (VIP) on the load balancer (see page [26](#))
- The load balancer is configured in two-arm Layer 4 NAT mode
- Return traffic MUST pass back via the load balancer. To enable this, a static route is configured on the Web Gateways to send return traffic back via the load balancer. For an HA pair, a floating IP address must be configured to allow the gateway to move between master and slave in the event of a failover (see page [22](#))

- This method is more efficient & faster than Option 1B since the Web Gateways can access the Internet directly rather than going via the load balancer
- Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page [35](#)
- For more information on Trend Micro Web Gateway deployment options please refer to [this URL](#)

Load Balancer Configuration

Configure Network Settings

Two interfaces are required. Typically eth0 is used for the internal (Web Gateway) subnet and eth1 is used for the external (client & VIP) subnet, although this is not mandatory since interfaces can be used as required / preferred.

To configure network settings on the load balancer:

13. Ensure that the required cables are plugged in (hardware) or virtual NICs are connected (virtual)
14. Using the WebUI, navigate to: *Local Configuration > Network Interface Configuration*
15. Define the required IP addresses and subnet mask:

The screenshot displays the 'IP Address Assignment' configuration window. At the top, there are four network interface icons labeled eth0, eth1, eth2, and eth3. eth0 and eth1 are active (10 GB/s), while eth2 and eth3 are disabled (indicated by a red X). Below the icons, there are two configuration sections. The first section for eth0 shows the IP address '192.168.4.200/24' and an MTU of '1500 bytes'. The second section for eth1 shows the IP address '192.168.2.200/24' and an MTU of '1500 bytes'.

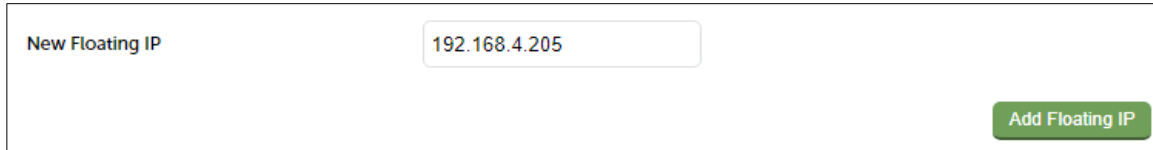
16. Configure the required IP address for eth0, e.g. **192.168.4.200/24**
17. Configure the required IP address for eth1, e.g. **192.168.2.200/24**
18. Click **Configure Interfaces**

Define a Floating IP to be used as the gateway for the Static Route on the Web Gateways

As mentioned, when using a clustered pair of load balancers for HA (our recommended configuration), a floating IP must be used as the gateway for the static route on the Web Gateways. This will 'float' between the master and slave units in the event of a failover or failback. This ensures that the Web Gateways always have a consistent return path via the load balancer – whether the master or slave is active.

To configure a Floating IP:

1. Using the WebUI, navigate to: *Cluster Configuration > Floating IP's*

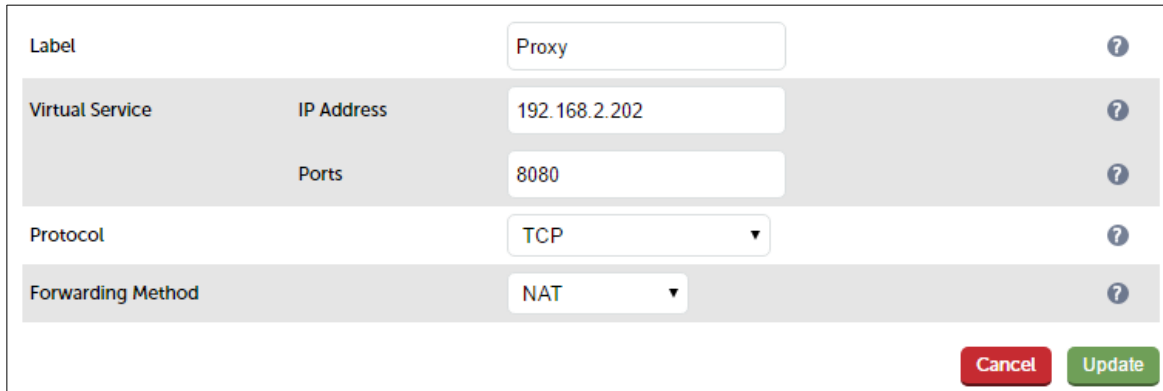


New Floating IP	<input type="text" value="192.168.4.205"/>	<button>Add Floating IP</button>
-----------------	--	----------------------------------

2. Define a suitable IP address for the default gateway , e.g. **192.168.4.205**
3. Click **Add Floating IP**

Create the Virtual Service (VIP)

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



Label	<input type="text" value="Proxy"/>	?	
Virtual Service	IP Address	<input type="text" value="192.168.2.202"/>	?
	Ports	<input type="text" value="8080"/>	?
Protocol	<input type="text" value="TCP"/>	▼	?
Forwarding Method	<input type="text" value="NAT"/>	▼	?
<div><button>Cancel</button><button>Update</button></div>			

4. Enter an appropriate label (name) for the VIP, e.g. **Proxy**
5. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.202**
6. Set the *Virtual Service Ports* field to the required port, e.g. **8080**
7. Ensure that *Protocol* is set to **TCP**
8. Ensure that *Forwarding Method* is set to **NAT**
9. Click **Update**
10. Now click **Modify** next to the newly created VIP
11. Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour)
12. Click **Update**

Define the Real Servers (RIPs)

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

Label	<input type="text" value="Proxy1"/>	?
Real Server IP Address	<input type="text" value="192.168.4.210"/>	?
Real Server Port	<input type="text" value="8080"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

4. Enter an appropriate label (name) for the first Web Gateway, e.g. **Proxy1**
5. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.4.210**
6. Set the *Real Server Port* field to the required port, e.g. **8080**
7. Click **Update**
8. Repeat the above steps to add your other Web Gateway(s)

Web Gateway Configuration

Configure a Static Route

As mentioned, Option 1C requires a Static Route to be defined on the Web Gateways that forces client return traffic to pass back via the load balancer. When using an HA pair of load balancers, the gateway for the static route must be a Floating IP to provide a consistent return path via the load balancer – whether the master or slave is active. Page [22](#) details how to create the Floating IP.

To define a Static Route using the WebUI (repeat for all Web Gateways) :

1. Login to the WebUI of the Web Gateway
2. Navigate to: *Administration > IP Address Settings*
3. Click **Add**, the *Add Static Route* screen appears
4. Enter a value for the *Network ID*, e.g. **192.168.2.0**
5. Enter a value for the *Netmask*, e.g. **255.255.255.0**
6. Enter a value for the *Router*, e.g. **192.168.4.205**
7. Click **Save**

Finalize Settings


Now refer to the section "*Configuration Settings Common to Options 1A, 1B & 1C*" below to finalize Web Gateway and client browser settings.

Configuration Settings Common to Options 1A, 1B & 1C

The steps in the following 3 sub sections must be followed for options 1A, 1B & 1C.

Web Gateway Operating Mode

The Trend Micro Web Gateway can easily be configured for Proxy Mode using the deployment wizard as shown below:



Deployment Wizard

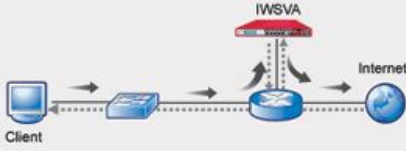
Deployment Mode

IWSVA operates in different modes that affect how IWSVA fits into your network and scans traffic. IWSVA operates as a single unit or a cluster. In a cluster, two or more IWSVAs work together to provide fail-tolerance ability.

Mode Selection

- ☐ Transparent bridge mode *(This mode requires a minimum of two NICs.)*
- ☐ Transparent bridge mode - high availability *(Requires a minimum of four NICs.)*
- ☒ Forward proxy mode
- ☐ Reverse proxy mode
- ☐ ICAP mode
- ☐ Simple transparency mode
- ☐ Web cache coordination protocol mode(WCCP)

Forward proxy mode In this mode, IWSVA acts as an intermediary for requests from clients accessing the Internet. A client connects to IWSVA, requesting URLs available from a different server. IWSVA evaluates the request according to its policy. If the request is valid, IWSVA scans and provides the specified Web page by connecting to the relevant server and requesting the page on behalf of the client.



```
graph LR; Client[Client] --> IWSVA[IWSVA]; IWSVA --> Internet[Internet];
```

Steps

1. Deployment Mode
2. Proxy Settings
3. Network Interface
4. Static Routes
5. Product Activation
6. System Time
7. Summary
8. Results


< Back

Next >


Cancel

Proxy Port Configuration

The required proxy port (8080 is the default) can also be set using the deployment wizard as shown below:


TREND MICRO™

Deployment Wizard

Proxy Settings 

Please specify the relevant proxy settings.

HTTP Listening Port

Port number:

Forward Proxy Mode

☐ Enable upstream proxy (dependent mode)

Proxy server:

Port number:

Anonymous FTP over HTTP

Email address:

Steps

1. Deployment Mode
2. **Proxy Settings**
3. Network Interface
4. Static Routes
5. Product Activation
6. System Time
7. Summary
8. Results

< Back

Next >

Cancel

Client Configuration

Client browser settings must be set so that browsers connect via the VIP. In a Microsoft based LAN environment, this is typically achieved using AD group policy.

Note: Depending on your requirements, it may be necessary to use an FQDN rather than an IP address for the Proxy server address. If you use an FQDN, make sure you have a valid DNS configuration that correctly resolves the hostname.

Browser Network Settings:

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

☒ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address:

Port:

Advanced

☒ Bypass proxy server for local addresses

OK

Cancel

Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	<input type="text" value="192.168.2.202"/>	<input type="text" value="8080"/>
Secure:	<input type="text" value="192.168.2.202"/>	<input type="text" value="8080"/>
FTP:	<input type="text" value="192.168.2.202"/>	<input type="text" value="8080"/>
Socks:	<input type="text"/>	<input type="text"/>

☒ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

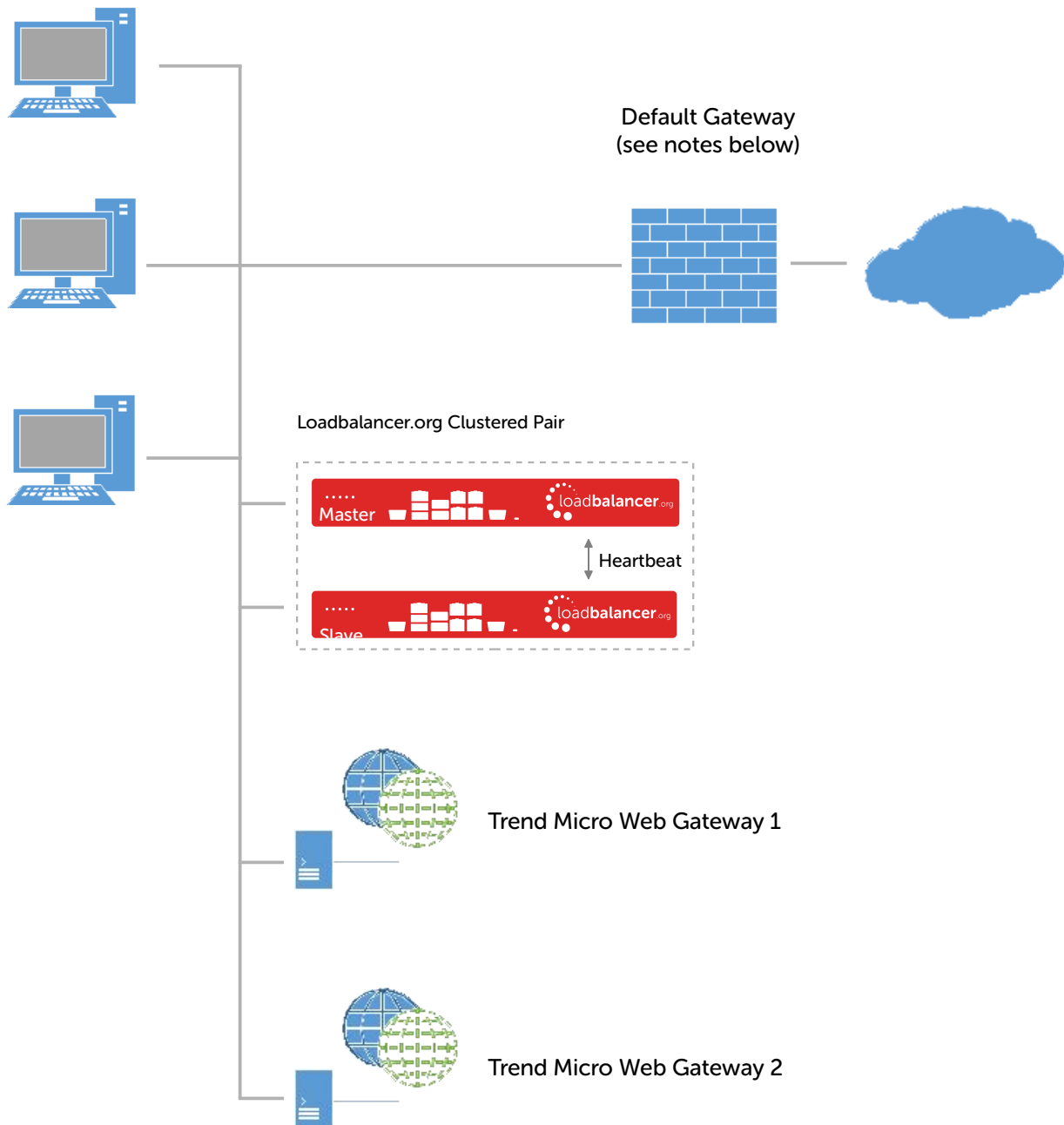
Use semicolons (;) to separate entries.

OK

Cancel

11. Option 2 – Transparent Routed Proxy Mode

Deployment Architecture



Notes:

- Rules must be added to the router/firewall so that the required traffic (typically HTTP & HTTPS on port 80 & 443) is sent transparently to the load balancer, please see page [32](#) for example rules for a Linux router
- As with Explicit Proxy Mode, the load balancer is configured in Layer 4 DR mode
- Firewall rules must be added to the load balancer to transparently send traffic to the Web Gateways (see page

29)

- Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page [35](#)
- For more information on Trend Micro Web Gateway deployment options please refer to [this URL](#)

Load Balancer Configuration

Create The Virtual Service (VIP)

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

Label	<input type="text" value="Proxy"/>	?	
Virtual Service	IP Address	<input type="text" value="1"/>	?
	Ports	<input type="text"/>	?
Protocol	<input type="text" value="Firewall Marks"/>	▼	?
Forwarding Method	<input type="text" value="Direct Routing"/>	▼	?
		<input type="button" value="Cancel"/>	<input type="button" value="Update"/>

4. Enter an appropriate label (name) for the VIP, e.g. **Proxy**
5. Change the *Virtual Service IP address* field to **1**

Note: This is the reference number for the 'Firewall Mark' . The same reference number is used when configuring the firewall rules – please see page [29](#) for more details.

6. Clear the *Virtual Service Ports* field, the ports are defined in the firewall rules on page [29](#)
7. Ensure that *Protocol* is set to **Firewall Marks**

Note: The ports field will be disabled when this is done.

8. Ensure that *Forwarding Method* is set to **Direct Routing**

9. Click **Update**
10. Now click **Modify** next to the newly created VIP
11. Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour)
12. Under the *Health Checks* section change *Check Type* to **Ping Server**
13. Click **Update**

Add The Floating IP

1. Using the WebUI, navigate to: *Cluster Configuration > Floating IPs*



New Floating IP

192.168.2.202

Add Floating IP

2. Enter an appropriate IP address for the Virtual Service, e.g. **192.168.2.202**
3. Click **Add Floating IP**

Configure Firewall Rules

Note: The *Firewall Script* page is locked by default on newer Loadbalancer.org appliances as part of "Secure Mode", which makes applying the changes described below impossible. To enable editing of the firewall script, navigate to *Local Configuration > Security*, set *Appliance Security Mode* to **Custom**, and click the **Update** button to apply the change. Editing the *Firewall Script* page will then be possible.

1. Using the WebUI, navigate to: *Maintenance > Firewall Script*
2. Scroll down to the Firewall Marks section
3. Add the following lines to this section as shown in the screen shot below:

```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp --dport 443 -j MARK --set-mark 1
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100
```

Note: Please see section 2 in the Appendix if you intend to forward ALL traffic to the Web Gateways.

MAINTENANCE > FIREWALL SCRIPT

```

##### Manual Firewall Marks #####

iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp --dport 443 -j MARK --set-mark 1
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100

# Example: Associate HTTP and HTTPS with Firewall Mark 1:
#VIP1="10.0.0.66"
#iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
#iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1

# A Virtual Service may then be created in the web interface, using 1 as the
# service address.

##### Packet Filtering #####

# You should always use a network perimeter firewall to lock down all
# external access to the load balancer except the required Virtual Services
# and the required services from your admin machine / network (SSH & HTTPS)

# Allow unlimited traffic on the loopback interface:
#iptables -A INPUT -i lo -j ACCEPT
#iptables -A OUTPUT -o lo -j ACCEPT

```

Update

- Click **Update**

Define The Real Servers (RIPs)

- Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers*
- Click **Add a New Real Server** next to the newly created VIP
- Enter the following details:

Label	<input type="text" value="Proxy1"/>	?
Real Server IP Address	<input type="text" value="192.168.2.210"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

Cancel
Update

- Enter an appropriate label (name) for the first Web Gateway, e.g. **Proxy1**
- Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.210**
- Click **Update**

7. Repeat the above steps to add your other Web Gateway(s)

Web Gateway Configuration

Note: By default the password for admin, root, and enable accounts is **adminIWSS85**. This can also be set during the installation process when IWSVA is deployed from the ISO file.

Web Gateway Operating Mode

The Trend Micro Web Gateway can easily be configured for Transparent Mode by following the steps below:

Note: These steps must be followed on all Gateways.

Step 1

Use the Deployment Wizard to configure the appliance in *Simple Transparency Mode* as shown below:

Deployment Mode

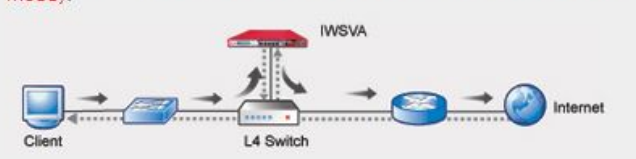
IWSVA operates in different modes that affect how IWSVA fits into your network and scans traffic. IWSVA operates as a single unit or a cluster. In a cluster, two or more IWSVAs work together to provide fail-tolerance ability.

Mode Selection

- ☐ Transparent bridge mode (This mode requires a minimum of two NICs.)
- ☐ Transparent bridge mode - high availability (Requires a minimum of four NICs.)
- ☐ Forward proxy mode
- ☐ Reverse proxy mode
- ☐ ICAP mode
- ☒ Simple transparency mode
- ☐ Web cache coordination protocol mode(WCCP)

Warning: The HTTPS decryption feature will be disabled in this mode.

Simple transparent mode In this mode, an L4 switch is set up to direct HTTP/FTP traffic to IWSVA(NOTE: IPv6 support is not currently provided in this deployment mode).



The diagram illustrates the network topology for Simple transparent mode. A Client (represented by a computer icon) sends traffic to an L4 Switch (represented by a switch icon). The L4 Switch directs traffic to the IWSVA (represented by a server icon with a red top). The IWSVA then forwards the traffic to the Internet (represented by a globe icon).

Steps

1. Deployment Mode
2. Transparency settings
3. Network Interface
4. Static Routes
5. Product Activation
6. System Time
7. Summary
8. Results

< Back

Next >

Cancel

Step 2

- Login as root either at the console or using a remote ssh session
- Edit the file `/etc/rc.local` using `vi`, `vim` or a remote editor such as the one included in WinSCP
- Then add the following additional lines to this file as shown below:

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080
```

```
iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 8443
```

```
F_check_ipmiDevice

iwss_cfg="/etc/iscan/intscan.ini"
F_log_offload_import_init()
{
    log_offload_mount_cmd=`grep mount_device $iwss_cfg | cut -d = -f 2`
    if [ "$log_offload_mount_cmd" != "" ];then
        $log_offload_mount_cmd
        chown iscan:iscan /var/offload
    fi
}
F_log_offload_import_init

iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080
iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 8443
```

Note: When using transparent routed mode, it's not necessary to modify the Web Gateway to accept traffic destined for the VIP, this is only required when using Explicit Proxy Mode.

Router/Default Gateway Configuration

Depending on your network configuration, rules must be added to the router/default gateway so that all required traffic (typically HTTP & HTTPS on port 80 & 443) is sent to the floating IP address on the load balancer. The load balancer then distributes this traffic between the Web Gateways. The example shown below is for a Linux based router:

Example iptables rules for a Linux based router:

```
SUBNET="192.168.2.0/24"
FWMARK="5"
TABLE="10"
LOADBALANCER="192.168.2.202"
iptables -t mangle -A PREROUTING -s $SUBNET -p tcp -m tcp --dport 80 -
-j MARK --set-mark $FWMARK
iptables -t mangle -A PREROUTING -s $SUBNET -p tcp -m tcp --dport 443
-j MARK --set-mark $FWMARK
```

```
ip route add default via $LOADBALANCER dev eth3 table $TABLE
ip rule add fwmark $FWMARK table $TABLE
```

This example uses policy routing via firewall marks. This works by first selecting and marking the packets we want to be sent to the Web Gateway, i.e. all packets on port 80 & 443. Then, when the kernel goes to make a routing decision, the marked packets aren't routed using the normal routing table, instead via table 10 in this case. Table 10 has only one entry: route packets to the Web Gateway.

Note: This is required when no changes have been made to the clients default gateway settings.

Client Configuration

If rules are configured on the router as described in the section above, no client change are required. If such rules are not configured, then the default gateway on the client PCs must be modified to be the load balancer.

12. Testing & Validation

To verify that the traffic is passing through the load balancer correctly the following reporting options can be used:

System Overview

Reports > Layer 4 Status

Reports > Layer 4 Current Connections

Many reporting and dashboard options are also available in the Trend Micro user interface. For more details please refer to the appropriate Trend Micro documentation

Layer 4 – Current Connections

Explicit Proxy Mode

The example screen shot below illustrates that the test client (192.168.64.7) sends requests to the VIP (192.168.111.88), the load balancer then forwards the request onto the Gateway (192.168.64.60).

LAYER 4 CURRENT CONNECTIONS

Check Status

IPVS connection entries

pro	expire	state	source	virtual	destination
TCP	13:07	ESTABLISHED	192.168.64.7:3565	192.168.111.88:8080	192.168.64.60:8080
TCP	13:05	ESTABLISHED	192.168.64.7:3563	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3541	192.168.111.88:8080	192.168.64.60:8080
TCP	13:05	ESTABLISHED	192.168.64.7:3570	192.168.111.88:8080	192.168.64.60:8080
TCP	13:07	ESTABLISHED	192.168.64.7:3567	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3572	192.168.111.88:8080	192.168.64.60:8080
TCP	13:05	ESTABLISHED	192.168.64.7:3560	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3561	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3571	192.168.111.88:8080	192.168.64.60:8080
TCP	13:07	ESTABLISHED	192.168.64.7:3566	192.168.111.88:8080	192.168.64.60:8080
TCP	02:58	NONE	192.168.64.7:0	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3564	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3568	192.168.111.88:8080	192.168.64.60:8080

Transparent Mode

The example screen shot below illustrates the difference when running in transparent mode.

LAYER 4 CURRENT CONNECTIONS

Check Status

IPVS connection entries

pro	expire	state	source	virtual	destination
TCP	00:41	FIN_WAIT	192.168.64.7:5774	70.42.56.98:80	192.168.64.60:80
TCP	00:15	FIN_WAIT	192.168.64.7:5758	74.208.104.65:80	192.168.64.60:80
TCP	14:19	ESTABLISHED	192.168.64.7:5681	93.188.129.145:80	192.168.64.60:80
TCP	00:50	FIN_WAIT	192.168.64.7:5779	70.42.56.98:80	192.168.64.60:80
TCP	00:47	FIN_WAIT	192.168.64.7:5778	70.42.56.98:80	192.168.64.60:80
TCP	14:35	ESTABLISHED	192.168.64.7:5679	176.34.178.134:80	192.168.64.60:80
TCP	14:35	ESTABLISHED	192.168.64.7:5691	178.236.5.70:80	192.168.64.60:80

Many reporting and dashboard options are also available in the Trend Micro Web Gateway user interface. For more details please refer to the appropriate Trend Micro documentation.

13. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don't hesitate to contact our support team: support@loadbalancer.org.

14. Further Documentation

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

15. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Trend Micro InterScan Web Gateway environments.

16. Appendix

1 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

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

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


Version 7:

Please refer to **Chapter 8 – Appliance Clustering for HA** in the [v7 Administration Manual](#).

Version 8:

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

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



loadbalancer.org

Local IP address

192.168.1.20

IP address of new peer


192.168.1.21

Password for *loadbalancer* user on peer

.....

Add new node


- Specify the IP address and the *loadbalancer* users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above
- Click **Add new node**
- The pairing process now commences as shown below:



192.168.1.20

loadbalancer.org

Attempting to pair..



192.168.1.21

loadbalancer.org

Local IP address

192.168.1.20

IP address of new peer


192.168.1.21

Password for *loadbalancer* user on peer

.....


configuring

- Once complete, the following will be displayed:



192.168.1.20

loadbalancer.org



192.168.1.21

loadbalancer.org

Break Clustered Pair

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

36

© Copyright Loadbalancer.org • www.loadbalancer.org • sales@loadbalancer.org

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.

2 – Modified Transparent Mode Firewall Rules

If ALL traffic is to be forwarded to the Web Gateways, the firewall rules below should be used rather than the rules on page [29](#), i.e.:

Replace:

```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp --dport 443 -j MARK --set-mark 1
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100
```

With:

```
iptables -t mangle -A PREROUTING -p tcp -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p udp -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp -d <LB-IP> -j MARK --set-mark 2
iptables -t mangle -A PREROUTING -p udp -d <LB-IP> -j MARK --set-mark 2
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100
```

Notes:

- <LB-IP> should be replaced with the base IP address of the load balancer (typically eth0), this is the address used by heartbeat and for administration purpose

-
- If these modified firewall rules are used, then either the default gateway for client PC's should be changed to be the load balancer, or the rules on the router should be changed to forward all traffic to the load balancer
 - This will only work for TCP and UDP traffic. So for example, ICMP and some VPN technologies will not work because the load balancer only supports TCP and UDP.

Don't hesitate to contact our support team if you need further assistance: support@loadbalancer.org

17. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.4.0	6 August 2019	Styling and layout	General styling updates	RJC
1.4.1	17 January 2020	Added note explaining how to disable "Secure Mode" to unlock the firewall script page	Required update	RJC
1.4.2	13 August 2020	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH

About Loadbalancer.org

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



United Kingdom

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

United States

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

Canada

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

Germany

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