Load Balancing Censornet USS Gateway

v1.1.1
Contents

1. About this Guide .................................................................................................................. 3
2. LoadBalancer.org Appliances Supported ........................................................................... 3
3. LoadBalancer.org Software Versions Supported ................................................................. 3
4. Censornet USS Gateway Versions Supported ................................................................. 3
5. Benefits of Implementing a Load Balancer .......................................................................... 3
6. Load Balancer Configuration ............................................................................................... 4
   Deployment Mode .................................................................................................................... 4
   Persistence/Server Affinity ...................................................................................................... 4
7. LoadBalancer.org Appliance – the Basics......................................................................... 4
   Virtual Appliance Download & Deployment ........................................................................ 4
   Initial Network Configuration ............................................................................................ 4
   Accessing the Web User Interface (WebUI) ......................................................................... 5
   HA Clustered Pair Configuration ....................................................................................... 6
8. Load Balancer & USS Gateway Configuration .................................................................. 6
   Deployment Architecture ................................................................................................... 7
   USS Gateway Configuration ............................................................................................... 8
   Configuring the Primary Gateway ...................................................................................... 8
   Configure Remaining Gateways ......................................................................................... 10
   Modify the USS Gateways to accept traffic for the VIP ................................................... 11
   Load Balancer Configuration ............................................................................................ 12
   Configure the IP Address and Hostname .......................................................................... 12
   Create the Virtual Service (VIP) ....................................................................................... 13
9. Client Configuration ............................................................................................................. 14
10. Testing & Validation ........................................................................................................... 14
11. Technical Support ............................................................................................................... 14
12. Further Documentation ...................................................................................................... 14
13. Conclusion .......................................................................................................................... 14
14. Appendix ............................................................................................................................ 15
   1 - Clustered Pair Configuration – Adding a Slave Unit ....................................................... 15
15. Document Revision History .............................................................................................. 17
1. About this Guide

This guide details the steps required to configure a load balanced Censornet USS Gateway environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any USS 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

The following table shows which Loadbalancer.org Appliances (hardware and virtual) can be used to load balance Censornet USS Gateway.

<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 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</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)

3. Loadbalancer.org Software Versions Supported

- v76.4 and later

4. Censornet USS Gateway Versions Supported

- All versions

5. Benefits of Implementing a Load Balancer

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

- **High-Availability** – If a Gateway fails, service is not interrupted
6. Load Balancer Configuration

Deployment Mode
Layer 4 DR mode is used. In this mode, traffic from the client to the USS Gateway passes via the load balancer, return traffic passes directly back to the client which maximizes performance. Direct Routing mode 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 USS Gateways see the real client IP address and not the IP address of the load balancer.

Persistence/Server Affinity
Source IP persistence is used. When enabled (the default setting for new layer 4 VIPs), 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 USS Gateway.

7. Loadbalancer.org Appliance – the Basics

Virtual Appliance Download & 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.

Note: The Virtual Appliance can be downloaded [here](#).

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:
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 15.

8. Load Balancer & USS Gateway Configuration
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 14)
- The load balancer is configured in one-arm Layer 4 DR mode
- The Censornet USS Gateways must be configured to accept traffic for the VIP (see page 11)
• 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 16.

USS Gateway Configuration

Configuring The Primary Gateway

1. Choose one of the Gateways to act as the primary gateway for the purposes of configuration
2. Decide on the hostname and IP address that you want the load balanced proxy service to use, e.g. filter and 172.24.11.160
3. Using the Network Interfaces and Settings sections in the WebUI temporarily configure the primary Gateway to have that hostname and IP address as shown in the example below:

![Network Interfaces and Settings](image)

This will form part of the FQDN that will eventually be used by end user devices to reference the proxy

4. Reboot the Gateway to ensure the new changes have fully taken effect
5. Now join the Gateway to your Active Directory domain. This can be done by following these instructions to add a domain, join the domain and finally create the DNS entry. In this example, the DNS entry filter.uss.local must correctly resolve to 172.24.11.160. The result should be a successfully joined domain configuration entry as
shown in the example below:

![Gateway Configuration Example]

The important parts to check here are:

1. Joined is in green and says YES
2. Keys is in green and says YES

6. Test that the gateway is working as expected by configuring a domain computer with the proxy filter.uss.local and port 8080. You will also need to install the SSL Certificate from the gateway. This can be done by pointing the browser at http://filter.uss.local/ussgw.der and installing the certificate in the browsers Trusted Root Authority section.

Note: If you’re unable to browse, ensure that the DNS entry for the FQDN has been set up and correctly propagated on the network.

Note: Also ensure that the date/time on the Gateway is within 5 minutes of the time on the Active Directory domain controller that the Gateway has joined. This is important for the Kerberos protocol.

Assuming this works as expected, the next step is to export the Kerberos Keyfile and SSL certificate from this Gateway to use on the other Gateways that will be part of the load balanced cluster.

7. To export the Keytab file, navigate to the Configure > Authentication section, select the Server menu and click Export Keyfile.

![Key File Export Diagram]

Ensure that you save the Keyfile somewhere safe on your PC

8. To export the SSL certificate, go to the System section, click the SSL Certificates menu and click Export CA.

© Copyright Loadbalancer.org - www.loadbalancer.org - sales@loadbalancer.org
Ensure that you save the CA file somewhere safe on your PC

9. Finally, repeat the first steps from this section to reconfigure this Gateway with a unique hostname and IP that it will use as part of the cluster. For example, set its hostname to `gateway1` and its IP address to 172.24.11.165. This frees up the filter hostname and 172.24.11.160 IP address for the load balancer’s Virtual Service to use.

**Configure Remaining Gateways**

On the remaining gateways complete the following steps:

1. Navigate to the Network Interfaces section and Settings section to set the desired hostname and IP address.

2. Next, navigate to the Configure > Authentication section and add the same domain as you did in the primary Gateway configuration. Also join the domain but do not create the keys.

3. Click the Server option and then the Import Keytab option.
4. Click **Browse** and navigate to the Keytab file that was downloaded as part of the section *Configuring the Primary Gateway on page 8.*

5. Click **Upload.**

6. Navigate to the **System** section, click the **SSL Certificates** menu and then click **Import CA.**

Click **Browse** and navigate to the CA file that was downloaded as part of the section *Configuring the Primary Gateway on page 8.*

**Modify The USS Gateways To Accept Traffic For The VIP**

- Note: This final step must be followed on all Gateways.

**Concept**

To enable DR mode to function, changes are required to the real servers, i.e. the USS 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.
Configuring the Censornet USS Gateway Appliances

1. Using the USS Gateway's WebUI, navigate to: Configure > Advanced
2. Enter the IP address of the VIP created on the load balancer, e.g. 172.24.11.100
3. Click the Save button

Load Balancer Configuration

Configure The IP Address And Hostname

1. Using one of the methods described on page 8, configure an appropriate IP address for the appliance's eth0 network interface, e.g. 172.24.11.25/24

   Note: Based on the example values used in this guide, do not use 172.24.11.160 – this is reserved for the Virtual Service (VIP). This IP was used when configuring the Primary Gateway as described on page 8.

2. Using the WebUI, navigate to: Local Configuration > Hostname & DNS
3. Set the hostname to an appropriate value, e.g. filter

   Note: The hostname 'filter' was used when configuring the Primary Gateway as described on page 8.

4. Click Update
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**: Enter an appropriate label (name) for the VIP, e.g. **Proxy-VIP**
   - **Virtual Service IP address**: Set to the required IP address, e.g. **172.24.11.160**
   - **Virtual Service Ports**: Set to the required port, e.g. **8080**
   - **Protocol**: Ensure it is set to **TCP**
   - **Forwarding Method**: Ensure it is set to **Direct Routing**
4. **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**: Enter an appropriate label (name) for the first USS Gateway, e.g. **USS-Gateway1**
   - **Real Server IP Address**: Change to the required IP address, e.g. **172.24.11.165**
4. **Click Update**
6. Click **Update**
7. Repeat the above steps to add your other USS Gateway(s)

9. **Client Configuration**
Client Web browser settings must be configured to connect via the VIP on the load balancer. In a Microsoft based LAN environment, this is typically achieved using AD Group Policy. Please refer to [this Censornet URL](#) for details on configuring client Web browsers.

10. **Testing & Validation**
To verify that traffic is passing correctly through the load balancer, the following WebUI reporting options can be used on the load balancer:

   **System Overview**
   - Reports > Layer 4 Status
   - Reports > Layer 4 Current Connections

Various reporting options are also available in the Censornet USS Gateway user interface. For more details please refer to the appropriate Censornet documentation.

11. **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.

12. **Further Documentation**

13. **Conclusion**
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Censortnet USS Gateway environments.
14. 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
• 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.
15. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.0</td>
<td>6 September 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>RJC</td>
</tr>
<tr>
<td>1.1.1</td>
<td>21 August 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
</tbody>
</table>
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 personalised 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

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

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

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

© Copyright Loadbalancer.org • www.loadbalancer.org