FORTINET
High Performance Network Security

FortiADC™ Basic Deployment Link Load Balance

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

October 2, 2018

FortiADC Deployment Guide: Basic Deployment Link Load Balancing

TABLE OF CONTENTS

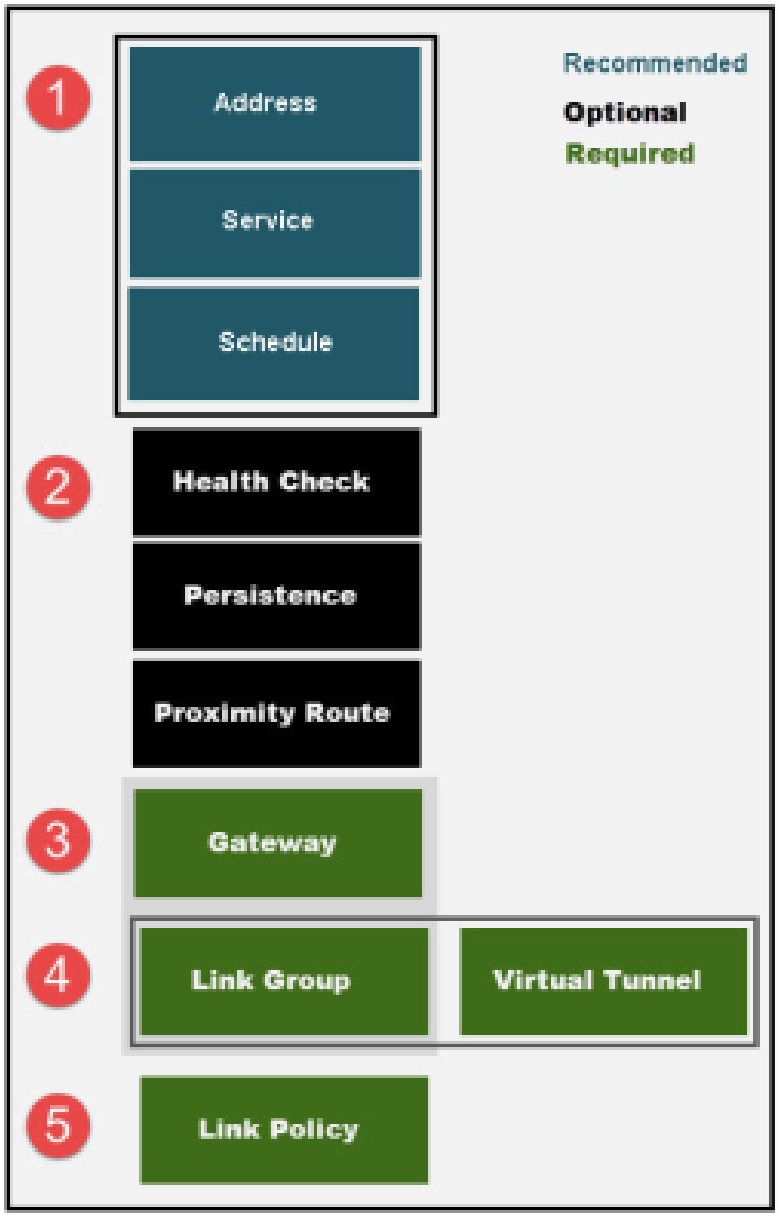
Introduction

The link load balancing (LLB) features are designed to manage traffic over multiple internet service provider (ISP) or wide area network (WAN) links. This enables you to subscribe to or provision multiple links, resulting in reduced risk of outages, additional bandwidth for peak events, and potential cost savings if your ISP uses billing tiers based on bandwidth rate or peak/off-peak hours.

In most cases, you configure link load balancing for outgoing traffic. Outbound traffic might be user or server traffic that is routed from your local network through your ISP transit links, leased lines, or other WAN links to destinations on the Internet or WAN. You configure link policies that select the gateway for outbound traffic. When the FortiADC system receives outbound traffic that matches a source/destination/service tuple that you configure, it forwards it to an outbound gateway link according to system logic and policy rules that you specify.

Configuration Overview

The configuration objects used in the LLB configuration and the order in which you create them are shown as below:



1. Add address, address group, isp, service, service group, and schedule group configuration objects that can be used to match traffic to link policy rules. This step is recommended. If your policy does not use match criteria, it will not have granularity.

2. Configure optional features. If you want to use health check rules, configure them before you configure the gateway links. If you want to use persistence rules or proximity routes, configure them before you configure a link group.

3. Configure gateway links.

4. Configure link groups or virtual tunnels.

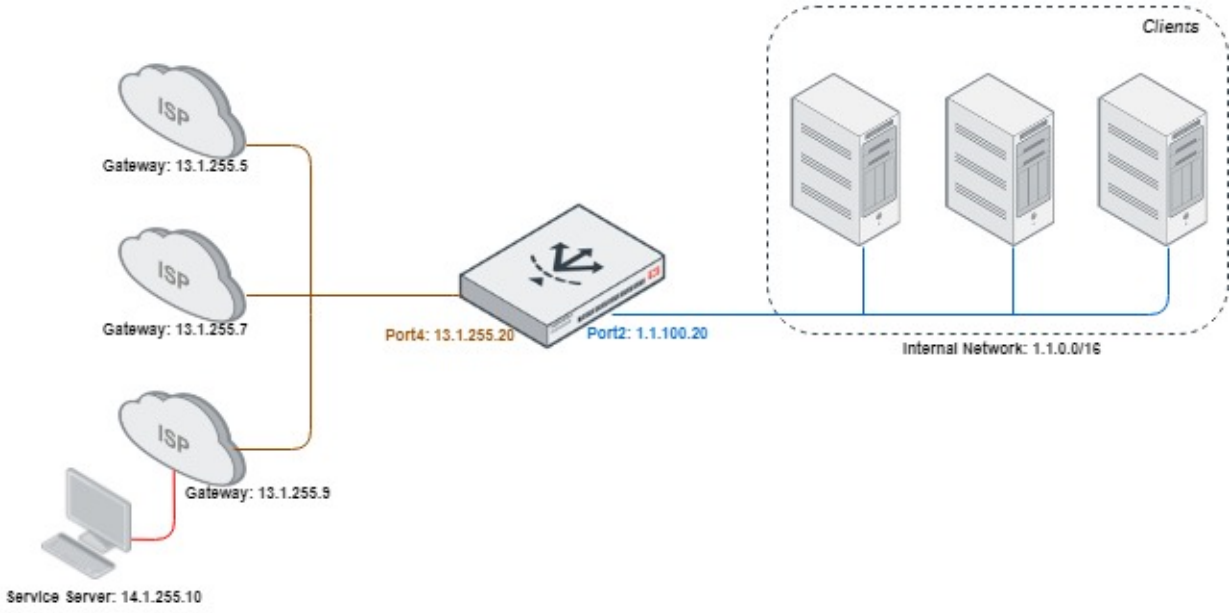
5. Configure the link policy. When you configure a link policy, you set the source/destination/service matching tuple for your link groups or virtual tunnels.

The LLB feature supports load balancing among link groups or among virtual tunnel groups. Deployment examples are introduced in the following pages.

Deployment - with Link Group

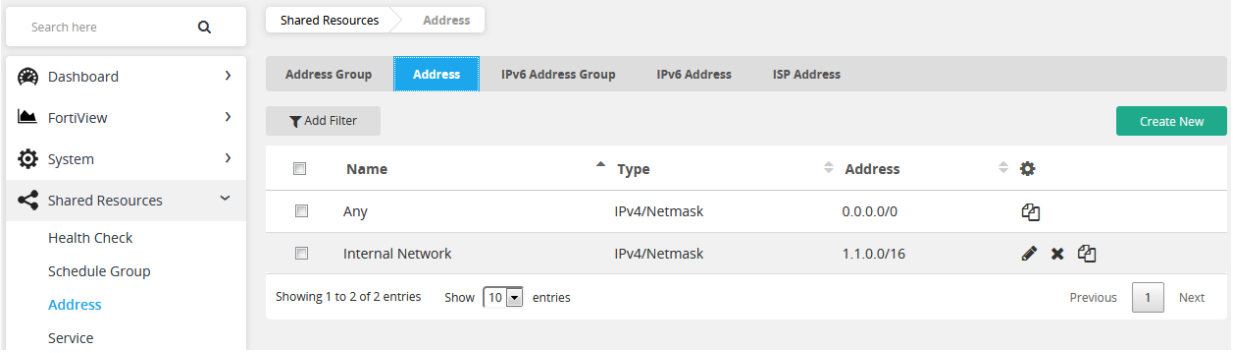
The link group option is useful for ISP links. It enables you to configure multiple ISP links that are possible routes for the traffic. The LLB picks the best route based on health checks, LLB algorithms, bandwidth rate thresholds, and other factors you specify, including a schedule.

Topology



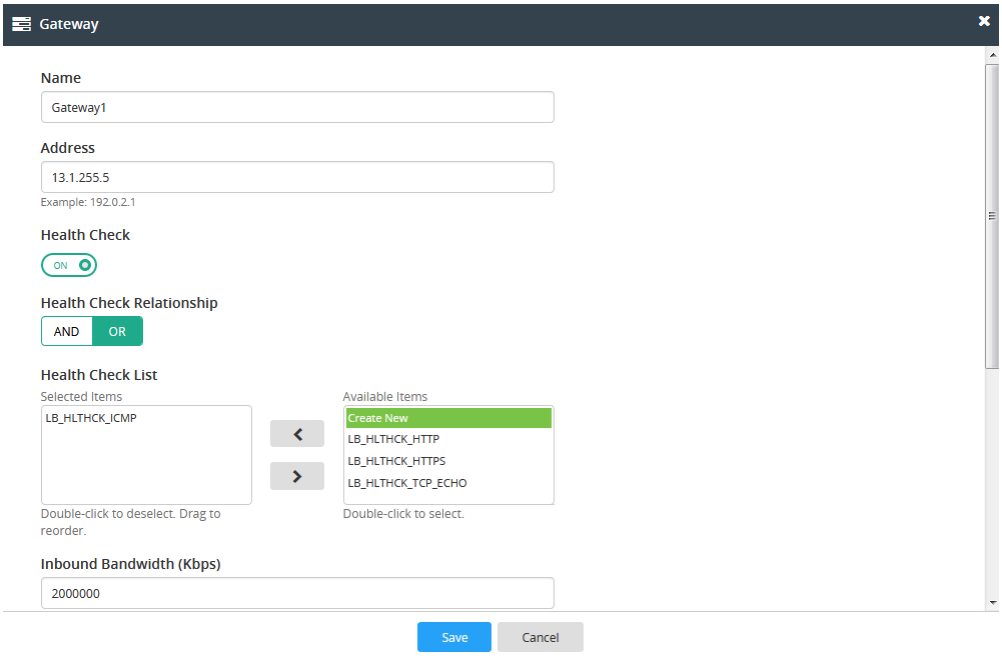
Configure Address For Link Policy

1. Click **Shared Resources > Address.**
2. Click the **Address** tab.
3. Click '**Create New**' to display the configuration editor.
4. Fill in the **Name** as “Internal Network”.
5. Select **Type** as **IPV4**/**Netmask**.
6. Fill in the IPV4/Netmask of internal servers which are going to send traffic out. In this case use IP 1.1.0.0/16.
7. Click **Save** to save the configuration.

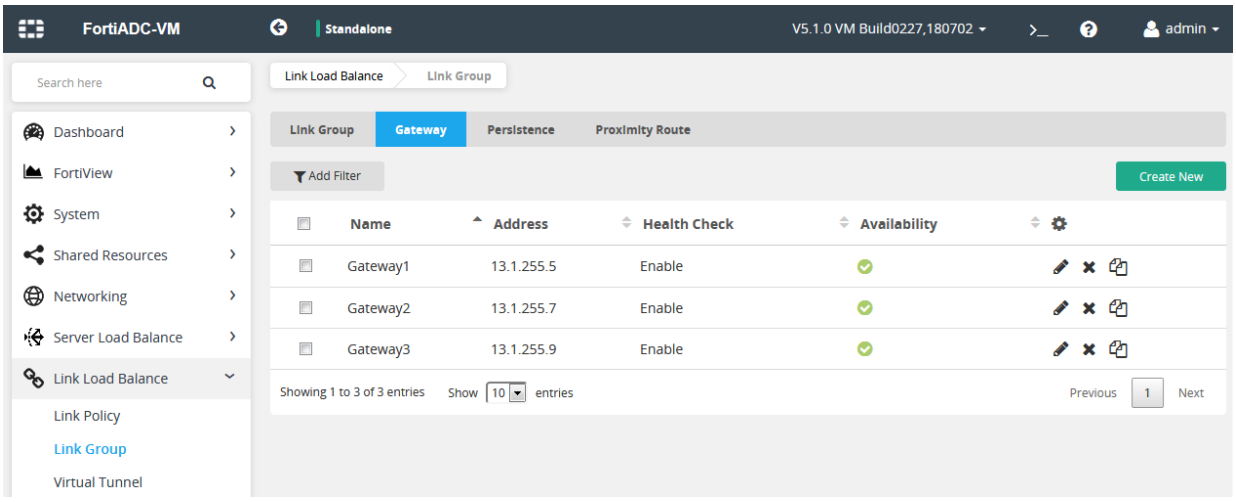


Configure Gateway Links

1. Click **Link Load Balance** > **Link Group.**
2. Click **Gateway** tab.
3. Click '**Create New**' to display the configuration editor.
4. Fill in the **Name** as “Gateway1”
5. Fill in the **Address** as 13.1.255.5.
6. Enable the check the box for **Health Check.**
7. Decided between Health Check Relationship **And/Or**. (Default is Or).
8. In **Health Check List**, select “LB_HLTHCK_ICMP” from the Available Items and move it to the Selected Items column.
9. Click **Save** to save the configuration



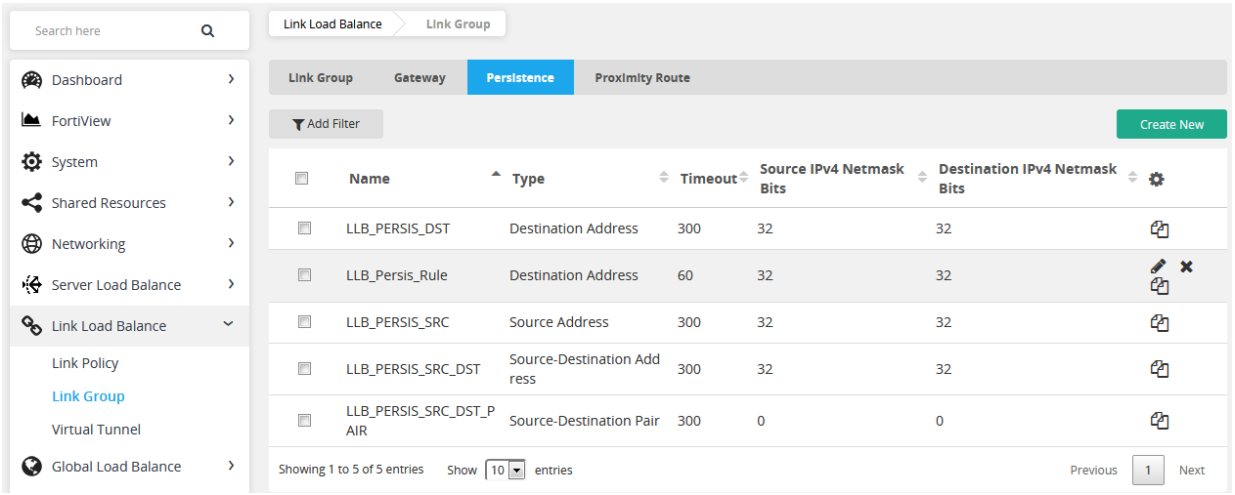
10. Repeat the same process for adding other gateways.



Configure a Persistence Rule

This step is optional as there are a few default rules available. In case you need create additional, follow steps below.

1. Click **Link Load Balance > Link Group.**
2. Click the **Persistence** tab.
3. Click '**Create New**' to display the configuration editor.
4. Complete the configuration
5. Click **Save** to save the configuration.

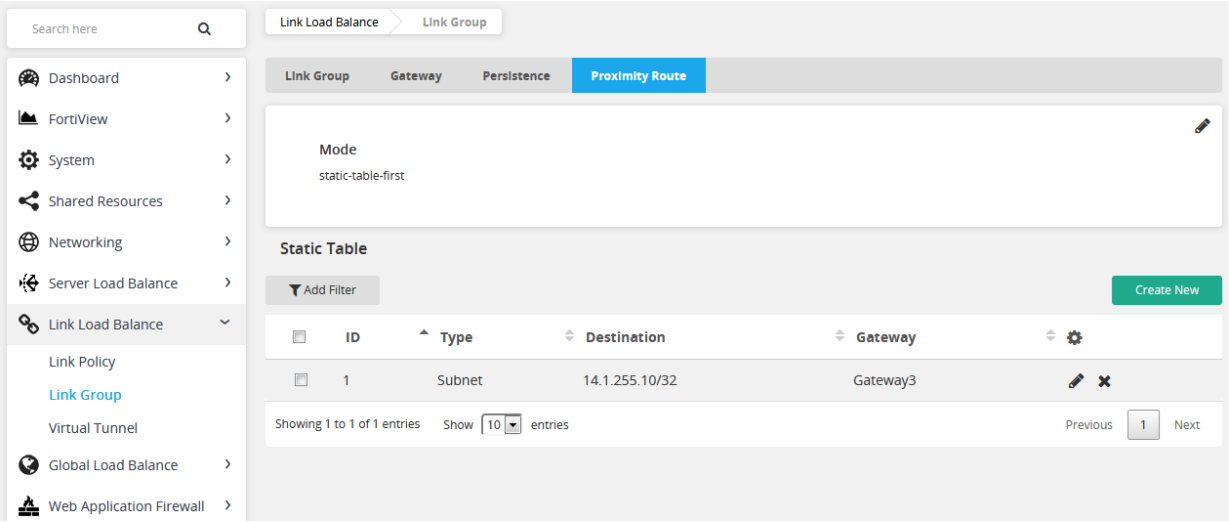


Configure a Proximity Route Setting

This step is optional as there are multiple routes for traffic. This feature enables users to associate link groups with efficient routes

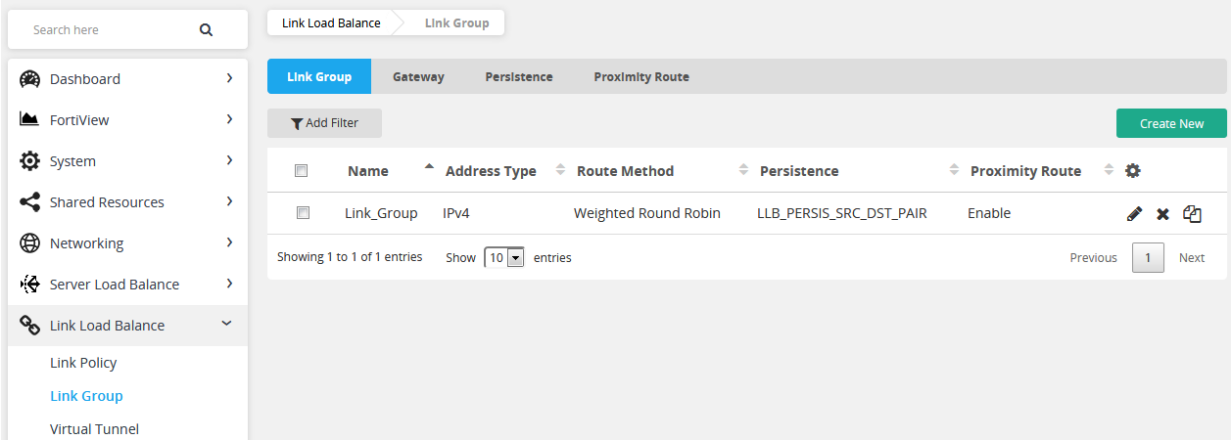
1. Click **Link Load Balance > Link Group**.
2. Click the **Proximity Route** tab.

3. Click edit icon of **Mode** on the right side and complete the configuration as required.
4. Click **Save** to save the configuration.
5. If static table is used, click '**Create New**' to add static routes in table.
6. Fill in the **IP/Netmask** as 14.1.255.10/32 as the topology for this example.
7. In **Gateway**, select “Gateway3” from the available items.
8. Click **Save** to save the configuration.

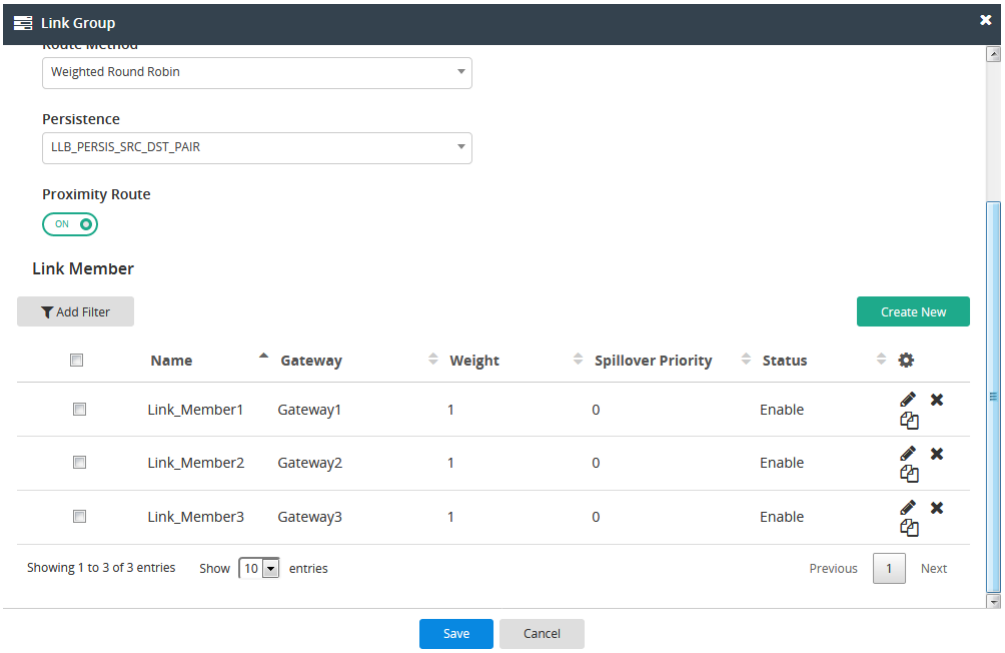


Configure a Link Group

1. Click **Link Load Balance > Link Group**.
2. The configuration page displays the **Link Group** tab.
3. Click '**Create New**' to display the configuration editor.
4. Fill in the **Name** of the group “Link_Group”.
5. For **Route Method** select “Weighted Round Robin”.
6. For **Persistence** select “LLB_PERSIS_ SRC_DST_PAIR”.
7. Click to enable **Proximity Route**.
8. Click **Save** to save the configuration.



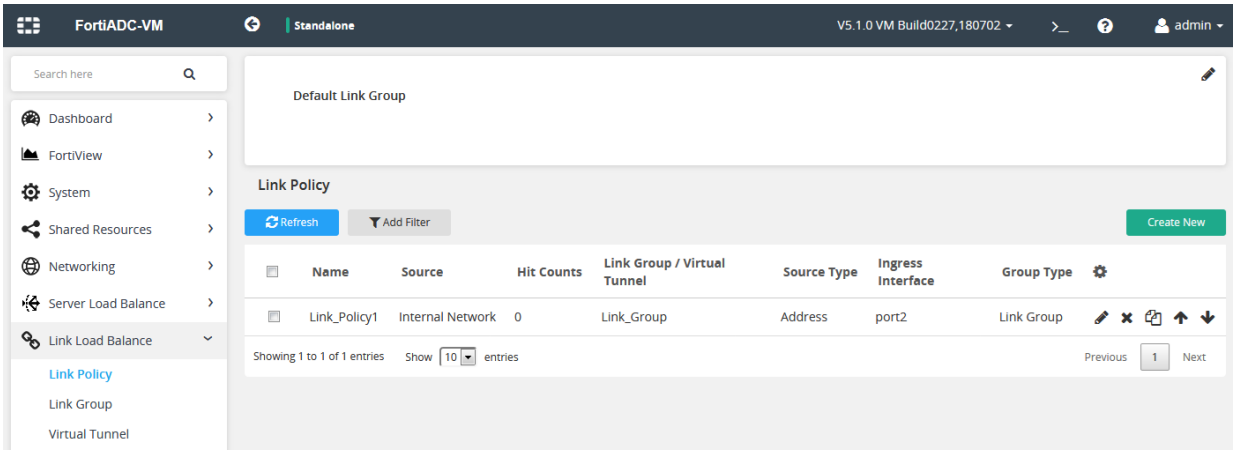
9. Edit the **Link Group** you just created for adding link members.
10. Go to the Link Member section and Click '**Create New**'.
11. Fill in the **Name** of the member “Link_Member1” .
12. Select the **Gateway** “Gateway1” from the dropdown list .
13. Check 'ON' for **Status**.
14. Click **Save** to save the configuration.
15. Repeat the same process from Step10~14 for adding other gateways.



Configure Link Policies

1. Go to **Link Load Balance > Link Policy**.
2. Click '**Create New**' to display the configuration editor.
3. Fill in the **Name** as “Link_Policy1” .

4. Select **Ingress Interface** as “port2” .
5. Enabled **Source Type** as **Address**.
6. Select “Internal Network” for **Source** .
7. Select **Group Type** as “Link Group” .
8. Select “Link_Group” as **Link Group .**
9. Click **Save** to save the configuration.

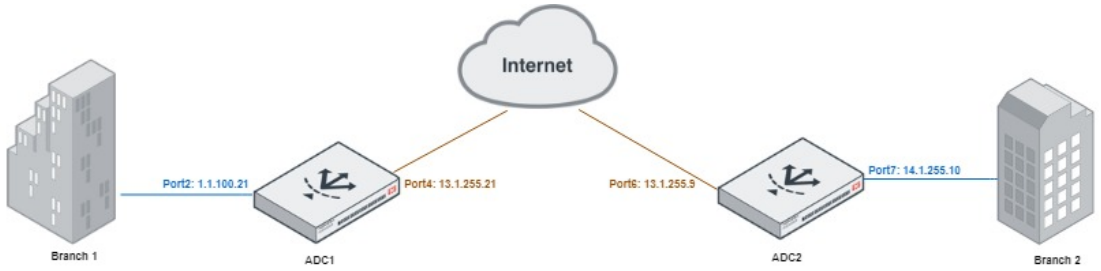


Now the Link Load Balance configuration with Link Group is completed.

Deployment - with Virtual Tunnel

Virtual tunnels enable reliable, site-to-site connectivity using Generic Routing Encapsulation (GRE) to tunnel traffic between pairs of FortiADC appliances. When you add members to a virtual tunnel configuration, you need to specify a local and remote IP address. These addresses are IP addresses assigned to a network interface on the local and remote FortiADC appliance.

Topology

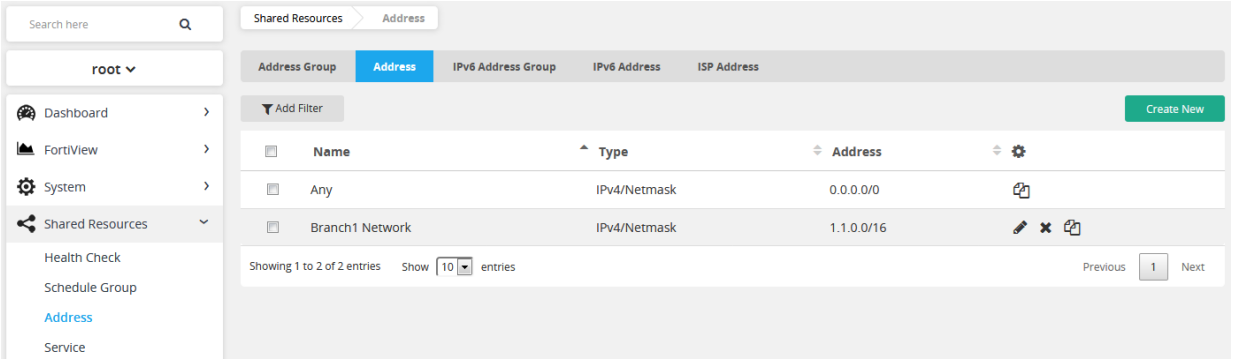


For Virtual Tunnel connection, LLB configurations are binomial between pairs of FortiADC appliances. Both ADC1 and ADC2 should have similar LLB configurations.

Configure Address For Link Policy

To configure address on ADC1:

1. Click **Shared Resources > Address**.
2. Click the **Address** tab.
3. Click '**Create New**' to display the configuration editor.
4. Fill in the **Name** as “Branch1 Network”.
5. Select **Type** as **IPV4/Netmask**.
6. Fill in the IPV4/Netmask of internal servers which are going to send traffic out. In this case use IP 1.1.0.0/16.
7. Click **Save** to save the configuration.

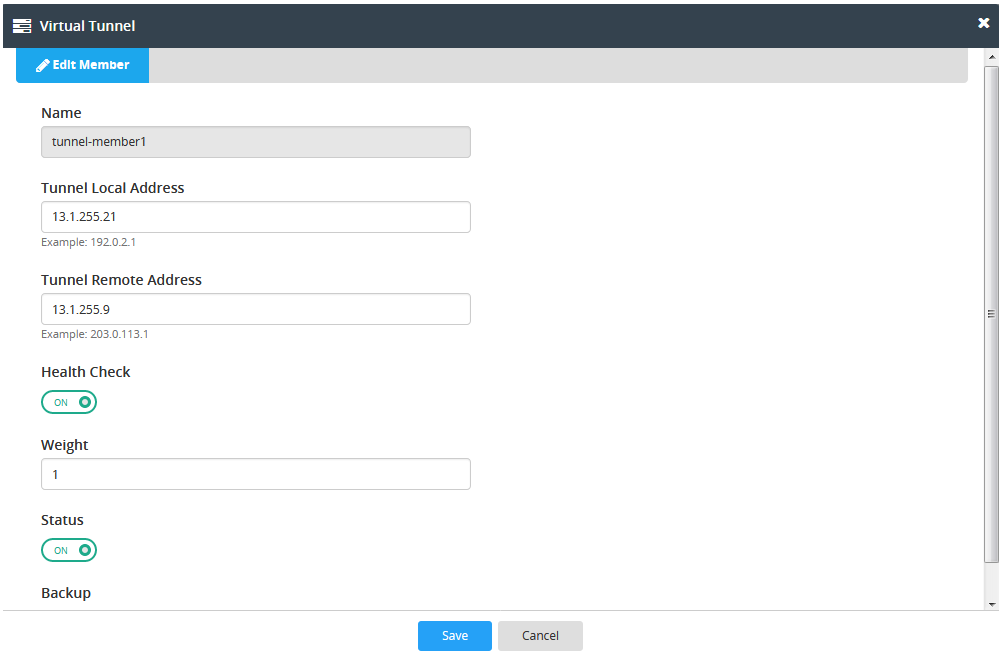


Repeat the same process to configure address for "Branch2 Network" with IP 14.1.255.0/24 on ADC2.

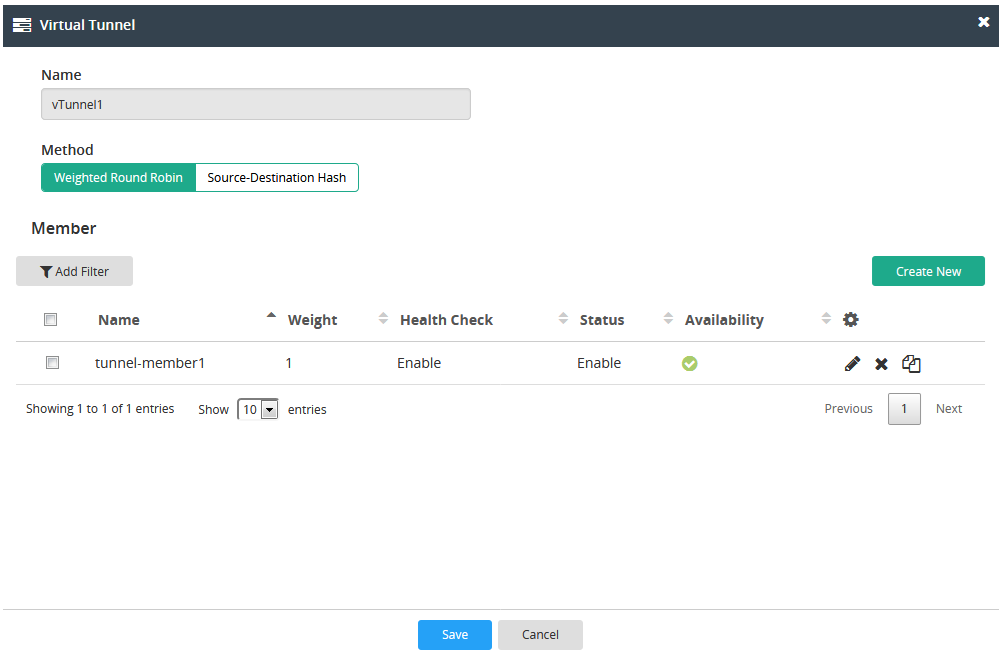
Configure Virtual Tunnel

To configure virtual tunnel on ADC1:

1. Click L**ink Load Balance > Virtual Tunnel**.
2. Click '**Create New**' to display the configuration editor.
3. Fill in the **Name** as “vTunnel1”
4. For **Method** select “Weighted Round Robin”.
5. Click **Save** to save the configuration.
6. Edit the **Virtual Tunnel** you just created for adding members.
7. Go to the **Member** section and Click 'Create New'.
8. Fill in the **Name** as “tunnel-member1”
9. Fill in the **Tunnel Local Address** as 13.1.255.21.
10. Fill in the **Tunnel Remote Address** as 13.1.255.9.
11. Check 'ON' for **Health Check Status.**



12. Click **Save** to save the configuration

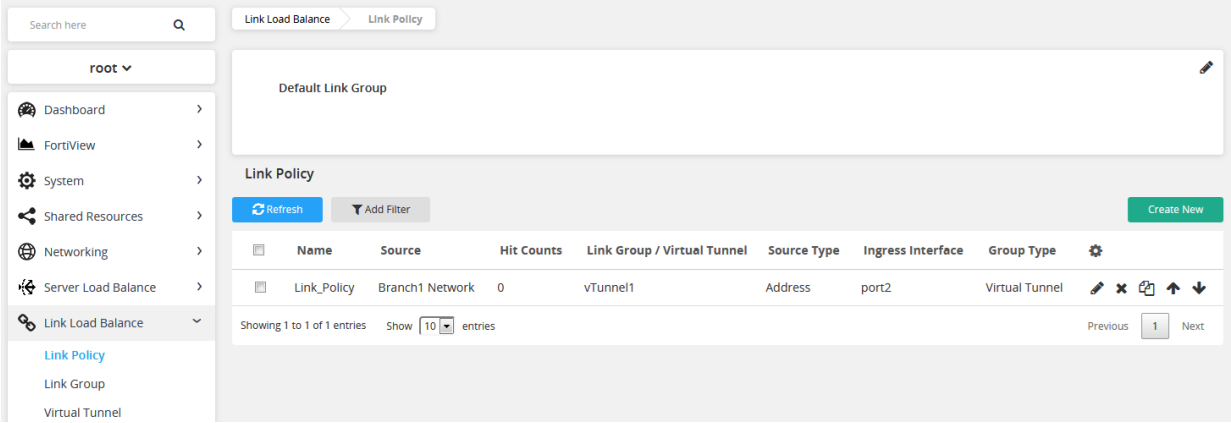


Repeat the same process to configure virtual tunnel with opposite Tunnel Local/Remote Address on ADC2.

Configure Link Policies

To configure link policy on ADC1:

1. Go to **Link Load Balance > Link Policy**.
2. Click '**Create New**' to display the configuration editor.
3. Fill in the **Name** as “Link_Policy” .
4. Select **Ingress Interface** as “port2” .
5. Enabled **Source Type** as **Address**.
6. Select “Branch1 Network” for **Source** .
7. Select **Group Type** as “Virtual Tunnel” .
8. Select “vTunnel1” as **Virtual Tunnel** .
9. Click **Save** to save the configuration.



Repeat the same process to configure link policy with Ingress Interface as “port7” on ADC2.

After Virtual Tunnel configurations are completed on ADC1 and ADC2, the flows go through this link policy can be encapsulated by GRE.

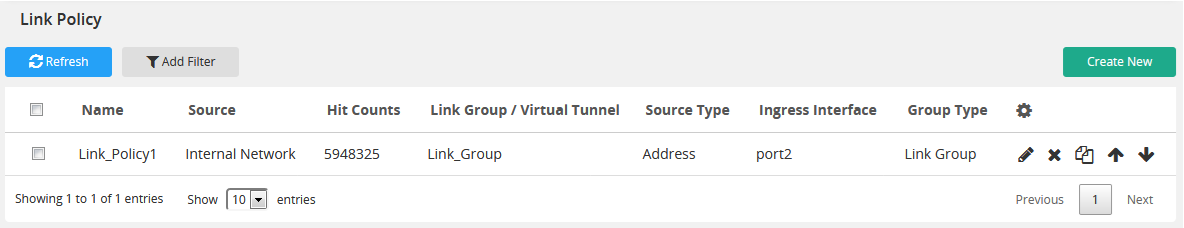
Monitor LLB Traffic

There are several ways to observe LLB Traffic on FortiADC. By the information delivered time, it can be divided into " Real Time Monitor" and " Historical Statistics".

Real Time Monitor

Hit Counts

Hit Counts shows how many times the link policy has been used. It can be found in **Link Load Balance > Link Policy.**



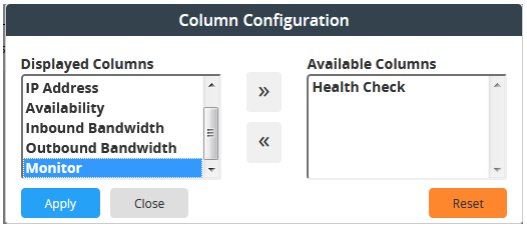
FortiView

To display LLB traffic going through a gateway using charts by selecting the corresponding check box in the

Monitor column.

1. Go to **FortiView > Link Load Balance > Gatewa**y.

2. Edit Column Configuration and select “Monitor” from the **Available Columns** and move it to the **Display Columns**.



3. Click **Apply** to save the configuration.

4. Check the box for **Monitor** for the gateway.

5. A graph will appear in the window show throughput and connections for the link.

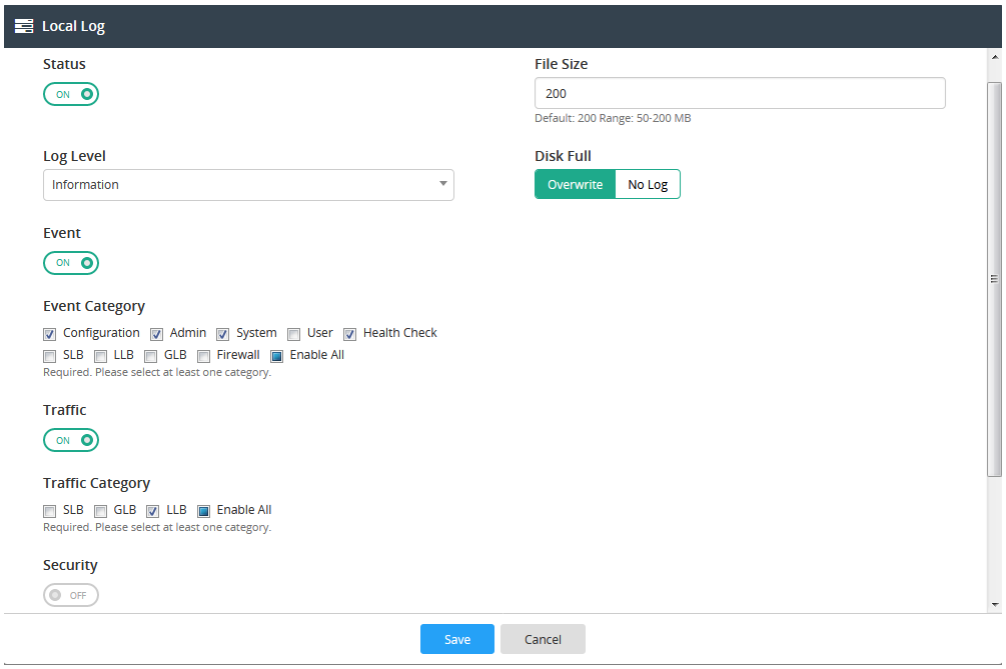
Historical Statistics

Traffic Logs

When the session went through by LLB policy and has been closed, the session information such as source/ destination IP and port, protocol and received/sent bytes is recorded in traffic logs.

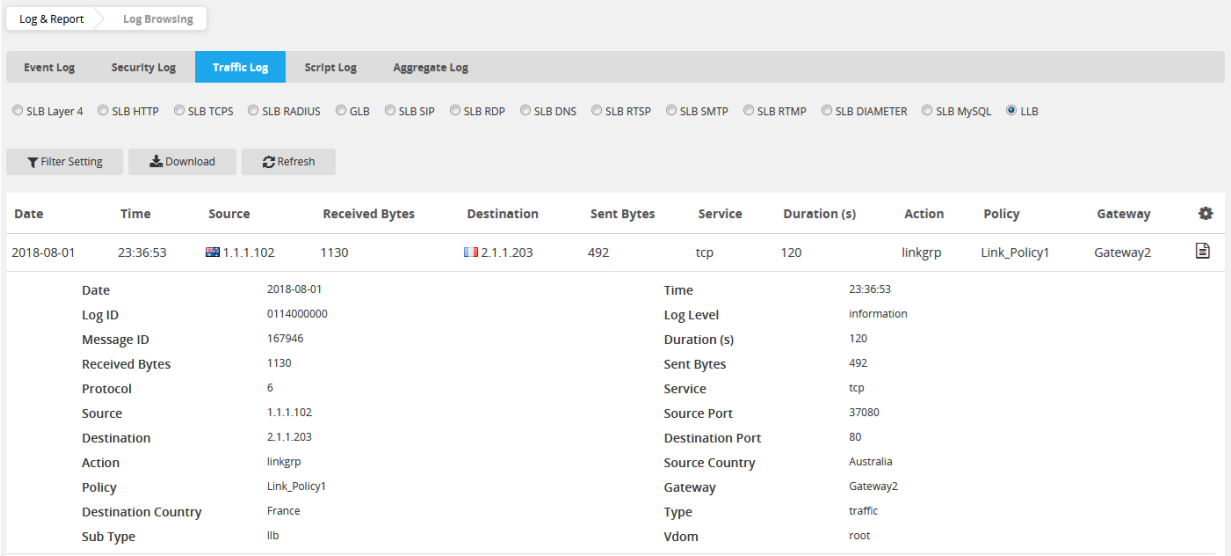
To enable **LLB Traffic Logs**:

1. Go to **Log & Report > Log Setting.**
2. The configuration page displays the **Local Log** tab.
3. Click edit button.
4. Click to enable **Traffic**.
5. Check 'LLB' in the **Traffic Category.**
6. Click **Save** to save the configuration.



To view the LLB traffic logs:

1. Go to **Log & Report > Log Browsing**.
2. Click the **Traffic Log** tab and then select **LLB**.

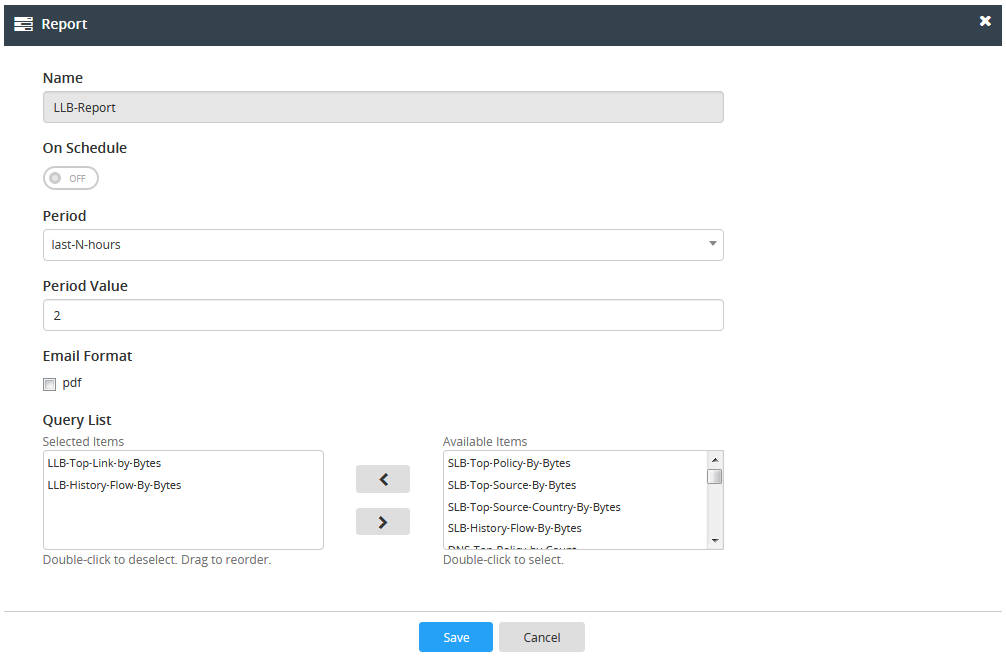


Report

FortiADC provides to query 'top link' and 'history flow' in sessions or bytes of **Link Load Balance** in **Report**.

Create Report configuration for LLB Report:

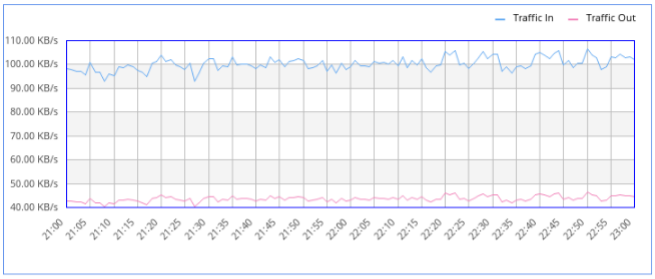
1. Go to **Log & Report > Report Config.**
2. Click '**Create New**' to display the configuration editor.
3. In Query List, select “LLB-Top-Link-by-Bytes” and "LLB-History-Flow-By-Bytes" from the **Available** Items and move it to the Selected Items column.
4. Fill in **Name**, **Period** and complete the configuration as required.
5. Click **Save** to save the configuration.



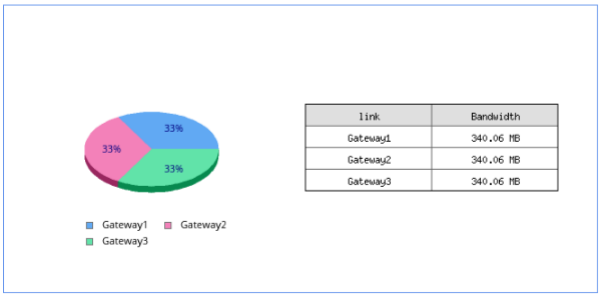
After **Report** is generated, check the report in **Log & Report > Report**. Link Load Balancer statistics charts are shown .

Link Load Balancer

LLB-History-Flow-By-Bytes



LLB-Top-Link-by-Bytes



link	Bandwidth
Gateway1	340.06 MB
Gateway2	340.06 MB
Gateway3	340.06 MB