



# FortiADC - Server Load Balance Layer 4 Deployment Guide

Version 5.4.0

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



February 19, 2020

FortiADC 5.4.0 Server Load Balance Layer 4 Deployment Guide

01-540-600000-20200219

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Server load balance layer 4</b> .....	<b>6</b>
Server Load Balance overview .....	6
Server Load Balance Layer-4 VS .....	6
FortiADC SLB4 Deployment with FullNAT mode and TCP profile and WRR method .....	12

## Change Log

Date	Change Description
11/25/2019	Second release.
6/5/2019	First release.

# Introduction

This guide details the steps required to configure a layer 4 load balance server in FortiADC. It covers the configuration of different mode layer 4 server. For more information, please also refer to the relevant Administration Manual.

# Server load balance layer 4

## Server Load Balance overview

FortiADC is like an advanced server load balancer. It can balance traffic to available destination servers based on health checks and load-balancing algorithms.

The physical distance between clients and the servers in your backend server—and other factors, like the number of simultaneous connections that the servers can handle, or load distribution among the servers -- are important contributing factors to server performance. So the purpose of FortiADC is to give user multiple methods for optimizing server response times and server capacity. Traffic is routed to the FortiADC virtual server instead of the destination real servers.

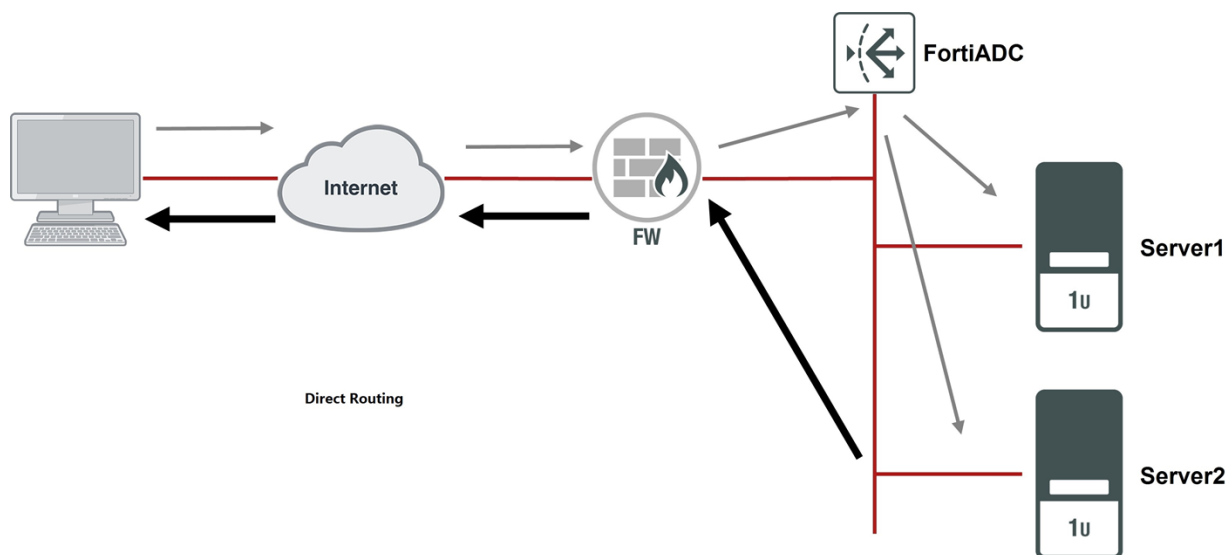
For layer 4 virtual server, it has five packet forwarding methods—Direct Routing, DNAT, Full NAT, Tunneling, NAT46.

## Server Load Balance Layer-4 VS

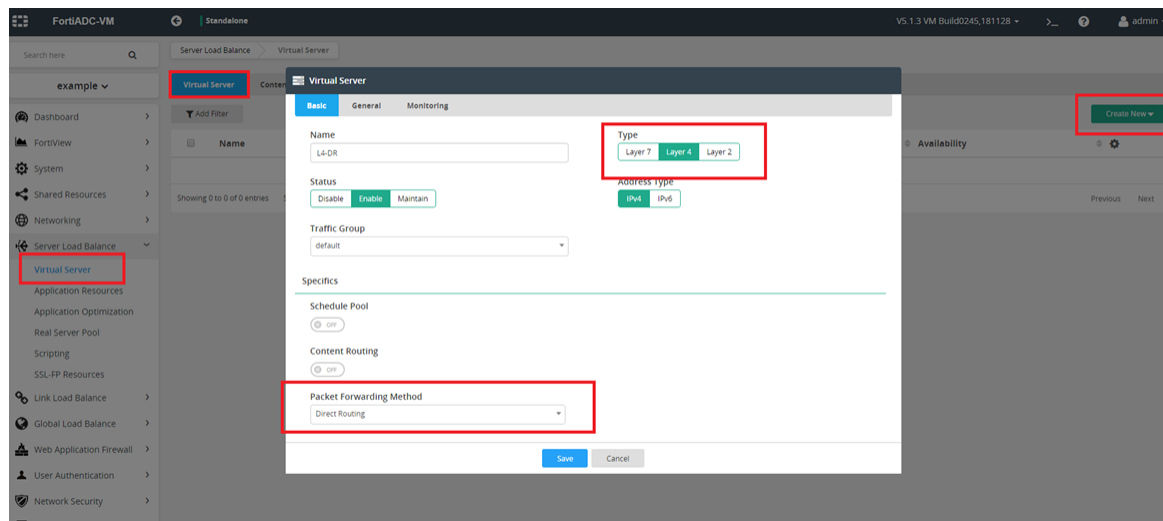
### Direct Routing mode

Direct Routing mode works by changing the destination MAC address of the incoming packet to match the selected Real Server. DR mode is transparent. The Real Server will see the source IP address of the client.

#### Topology:



## GUI:



- When the packet reaches the Real Server, it expects the Real Server to own the VS IP. This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Servers own IP address and the VS IP.
- FortiADC must have an interface in the same subnet as the Real Servers to ensure layer2 connectivity required for DR mode to work.
- The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet
- Port translation is not possible in DR mode i.e. having a different RIP port than the VIP port

## DR mode for Windows server

Add a loopback adapter, set the virtual-server IP to the loopback adapter.

1. Click **Start**, then type cmd in the search box.
2. When cmd.exe appears, right-click it and choose **Run** as administrator.
3. In the command prompt, type `hdwwiz.exe` and press **Enter**.
4. Click **Next**.
5. Select **Install the hardware** that is manually selected from a list (Advanced), then click **Next**.
6. Select **Network adapters**, then click **Next**.
7. Select **Microsoft** as the manufacturer, select **Microsoft KM-TEST Loopback Adapter** as the adapter for Windows 10, then click **Next**.
8. Select **Next** to confirm the installation.
9. Select **Finish** to complete the installation.
10. Find the new added loopback adapter, then set the virtual-server IP to the loopback adapter.

Rename the name of NIC connecting to FortiADC to new name, such as "nic\_to\_adc", rename the new added loopback NIC to "loopback", then execute the following command:

```
netsh interface ipv4 set interface "nic_to_adc" weakhostreceive=enabled
```

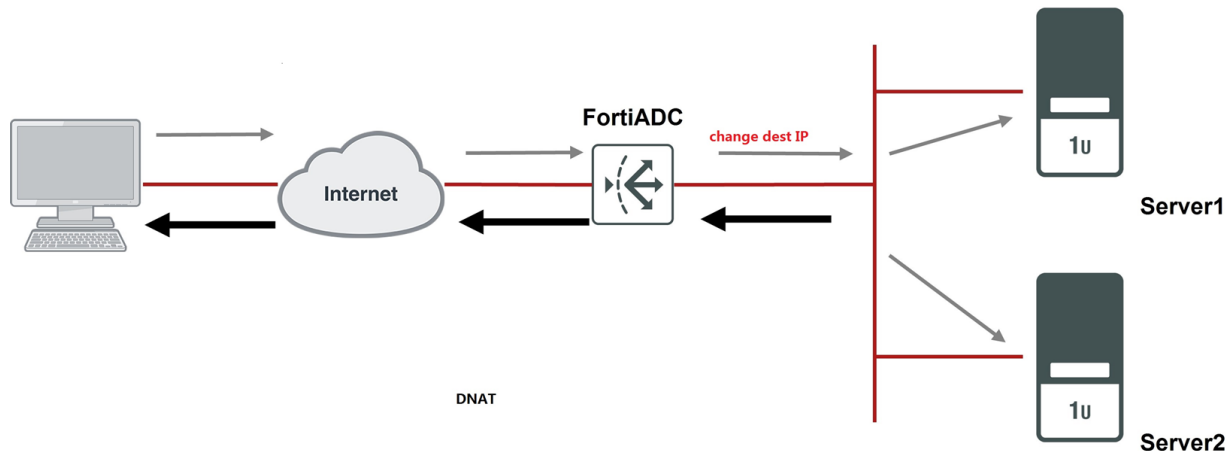
```
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
```

```
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

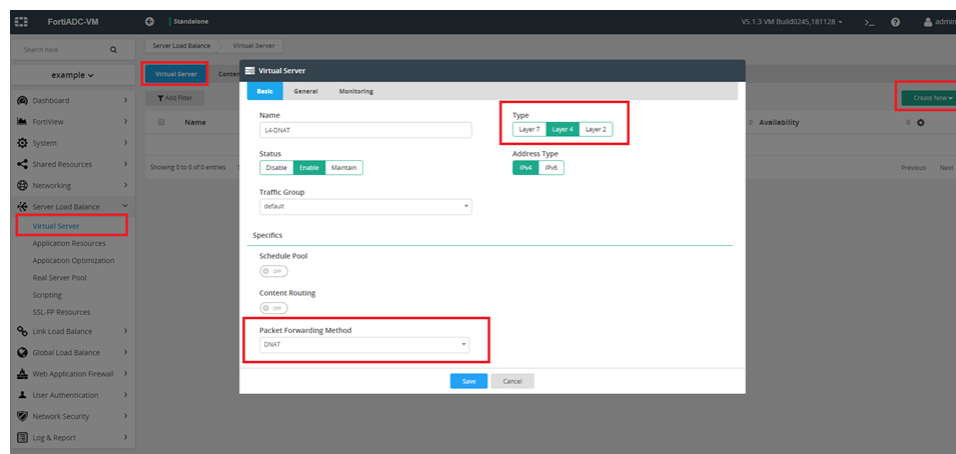
## DNAT mode

Typically, Layer 4 DNAT uses two interfaces connecting to client and real servers. The packet's destination IP will be changed after going through the FortiADC VS.

### Topology:



### GUI:



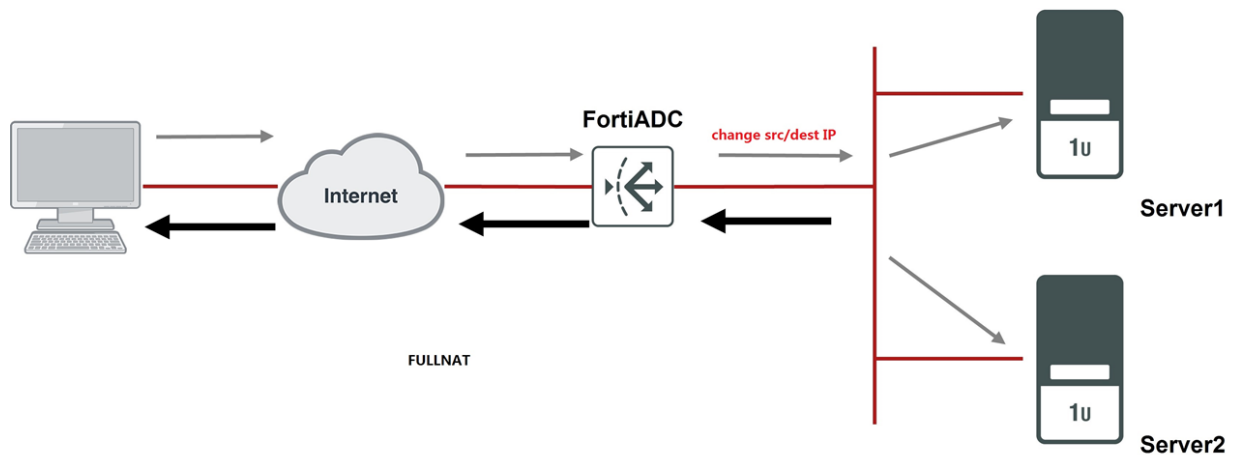
- Use DNAT as the packet forwarding method and set the default gateway on each server to FortiADC's IP address on the same subnet/VLAN (or, use static routes to send responses to FortiADC's IP address)

## FULLNAT mode

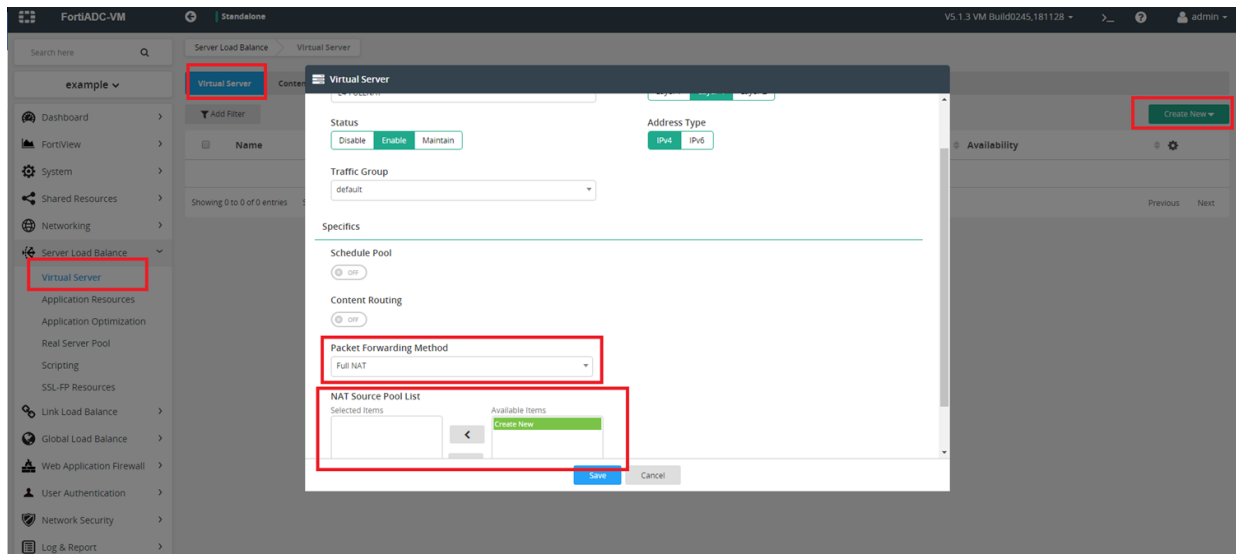
Layer 4 FULLNAT VS changes the packet's source and destination address before sending the packet to real servers. User can self-define the pool IP address range in the NAT source pool, and select it in Pool List. Normally, the NAT source pool's address range is in the same network subnet with real server.



## Topology:



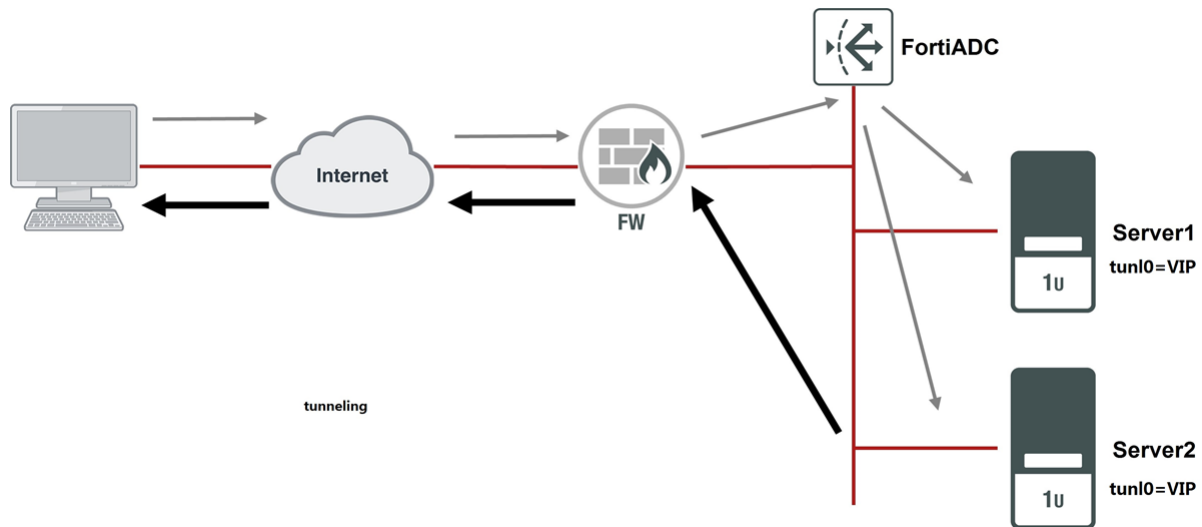
## GUI:



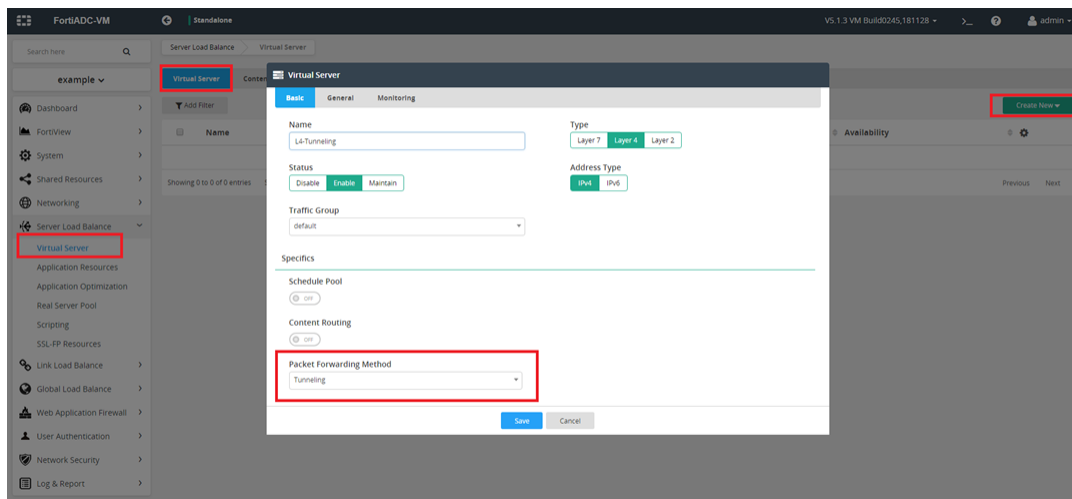
## Tunneling mode

Tunneling mode VS is based on direct routing mode. The FortiADC VS encapsulates the original packet (client IP to Virtual Server IP) inside an ipip packet of ADC IP to real server IP, which is put into an output chain and is routed to the real server. The real server receives the packet on a tunl0 device and decapsulates the ipip packet, revealing the original packet (client IP to Virtual Server IP). Then it sends the packet to client.

## Topology:



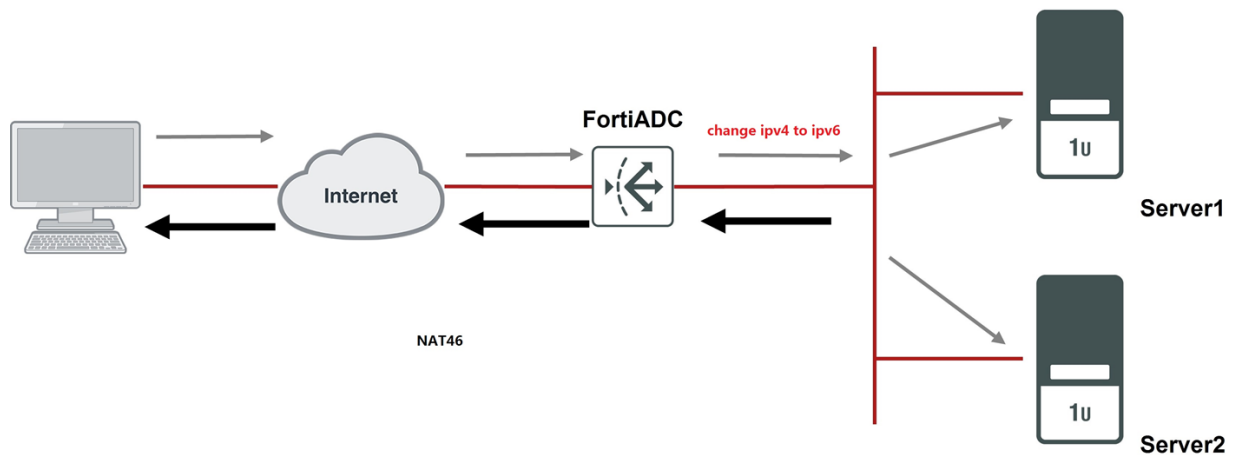
## GUI:



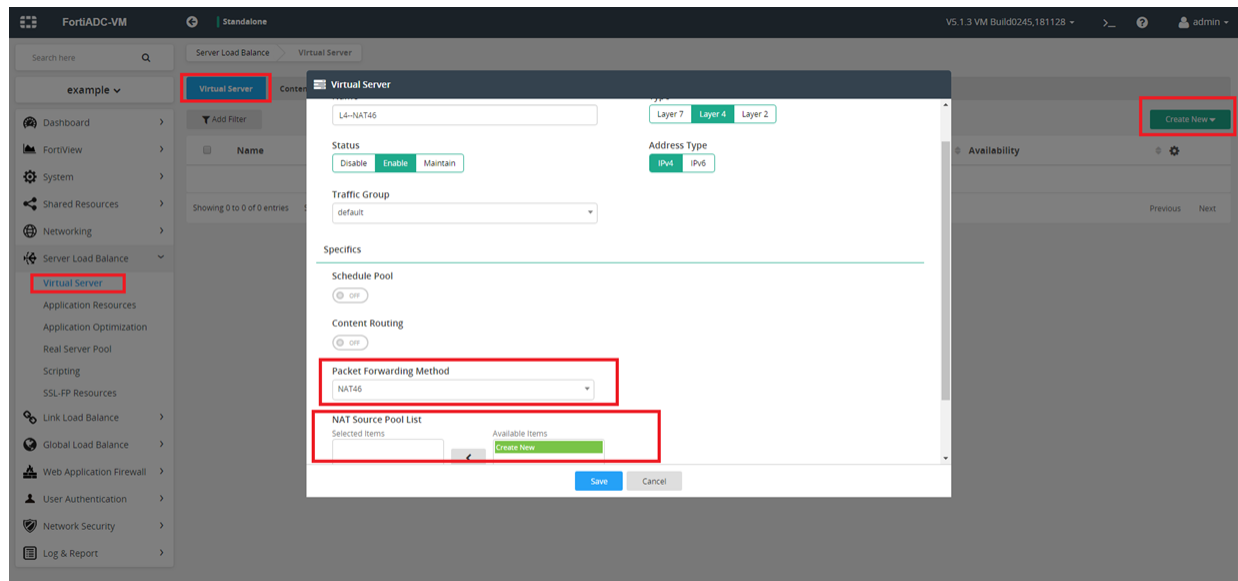
## NAT46 mode

NAT46 mode VS converts the packet's source address from ipv4 to ipv6, which were set in NAT source pool. Then it sends them to ipv6 real server.

## Topology:

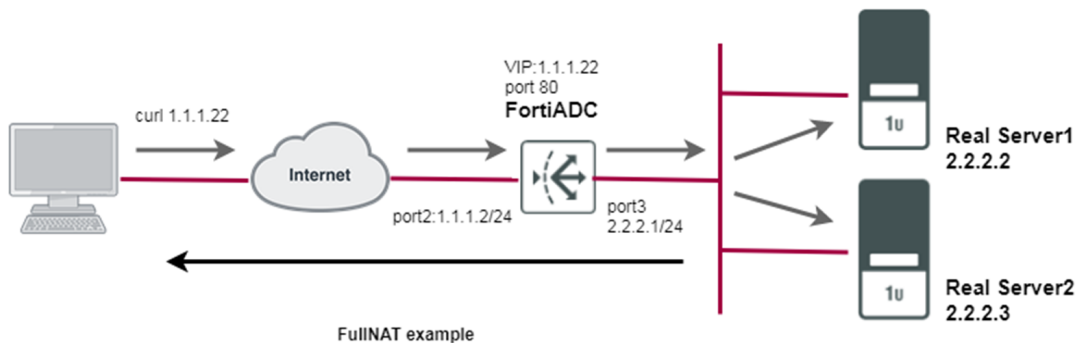


## GUI:

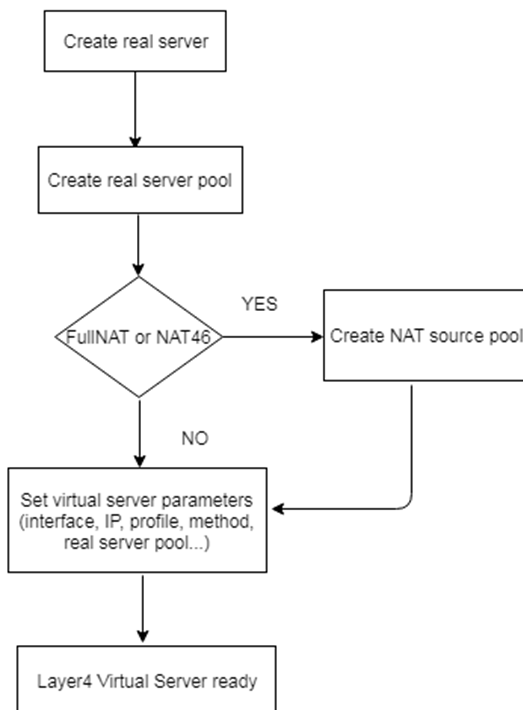


## FortiADC SLB4 Deployment with FullNAT mode and TCP profile and WRR method

### SLB4 FullNAT Example Topology



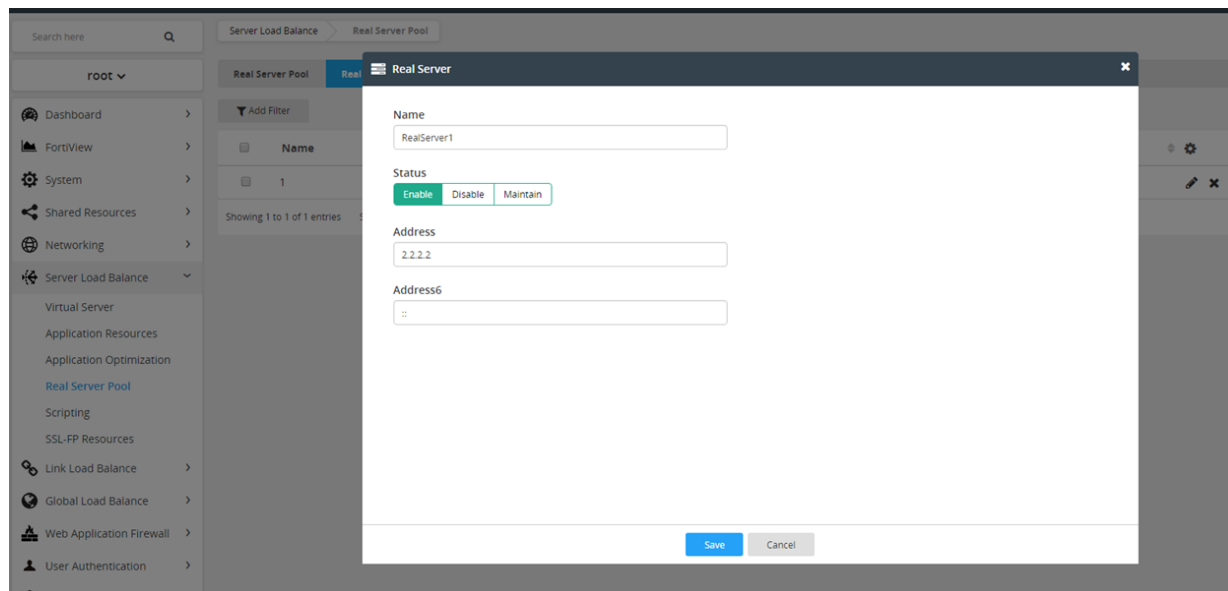
### SLB4 FullNAT, TCP profile, WRR method steps



basic Layer4 VS steps

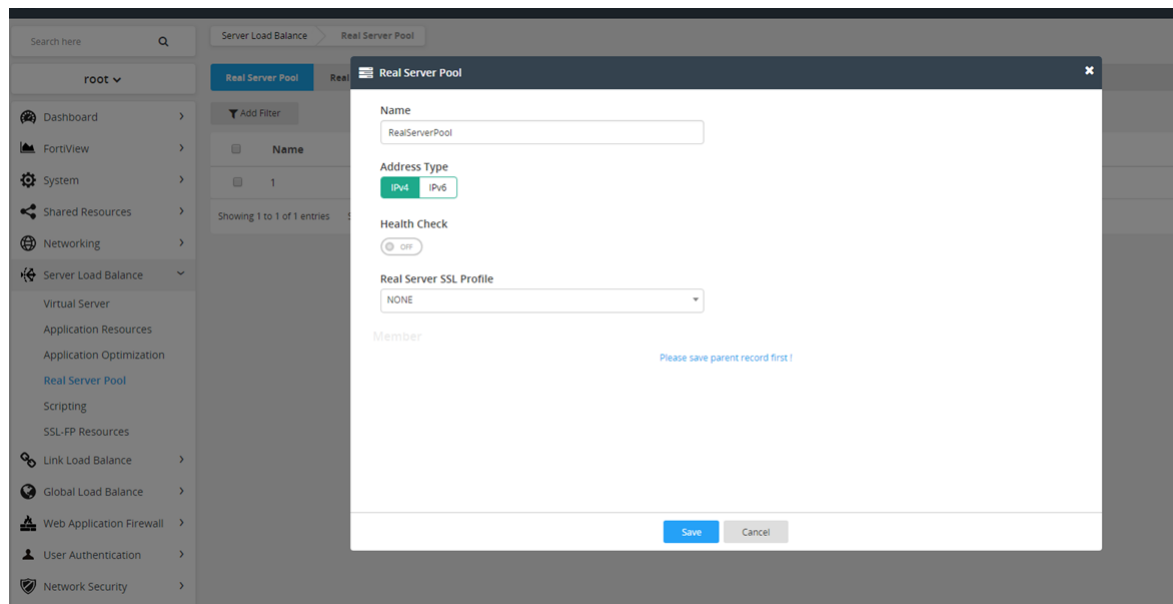
### To deploy a SLB Layer 4 server:

#### Step 1: Create new Real Server

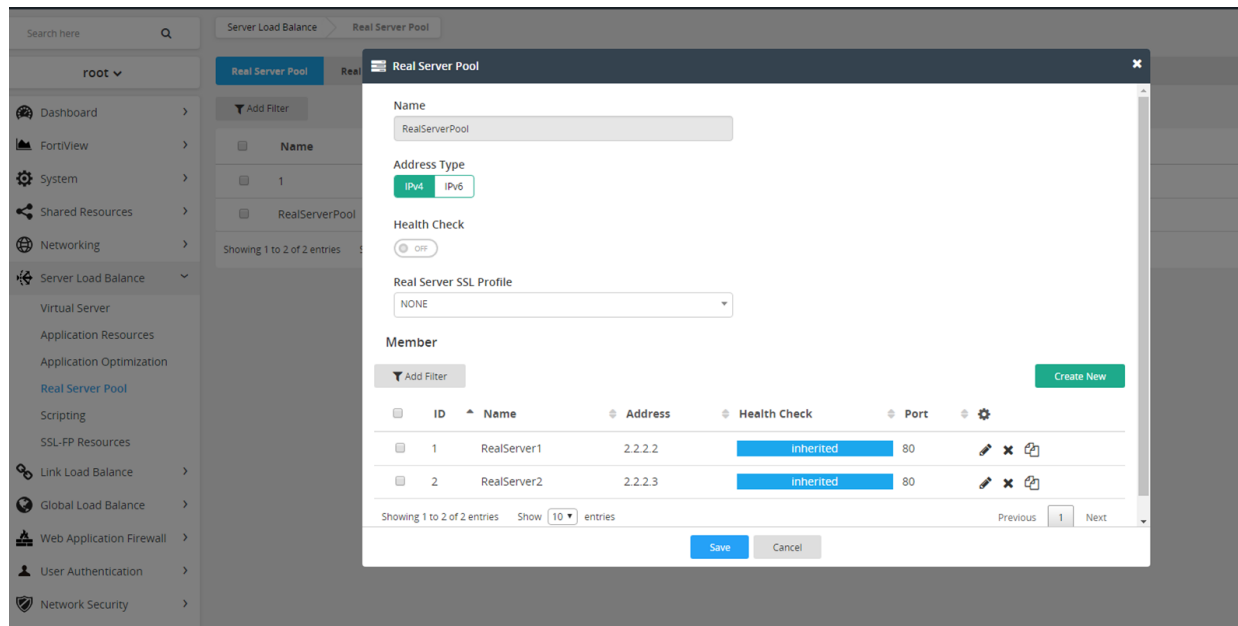


The screenshot shows the FortiADC web interface. On the left is a navigation menu with categories like Dashboard, FortiView, System, Shared Resources, Networking, and Server Load Balance. The 'Server Load Balance' menu is expanded, showing options like Virtual Server, Application Resources, Application Optimization, Real Server Pool, Scripting, SSL-FP Resources, Link Load Balance, Global Load Balance, Web Application Firewall, and User Authentication. The main panel displays the 'Real Server Pool' configuration page. A modal window titled 'Real Server' is open, showing the following fields: 'Name' (RealServer1), 'Status' (Enable, Disable, Maintain), 'Address' (2.2.2.2), and 'Address6' (::). At the bottom of the modal are 'Save' and 'Cancel' buttons.

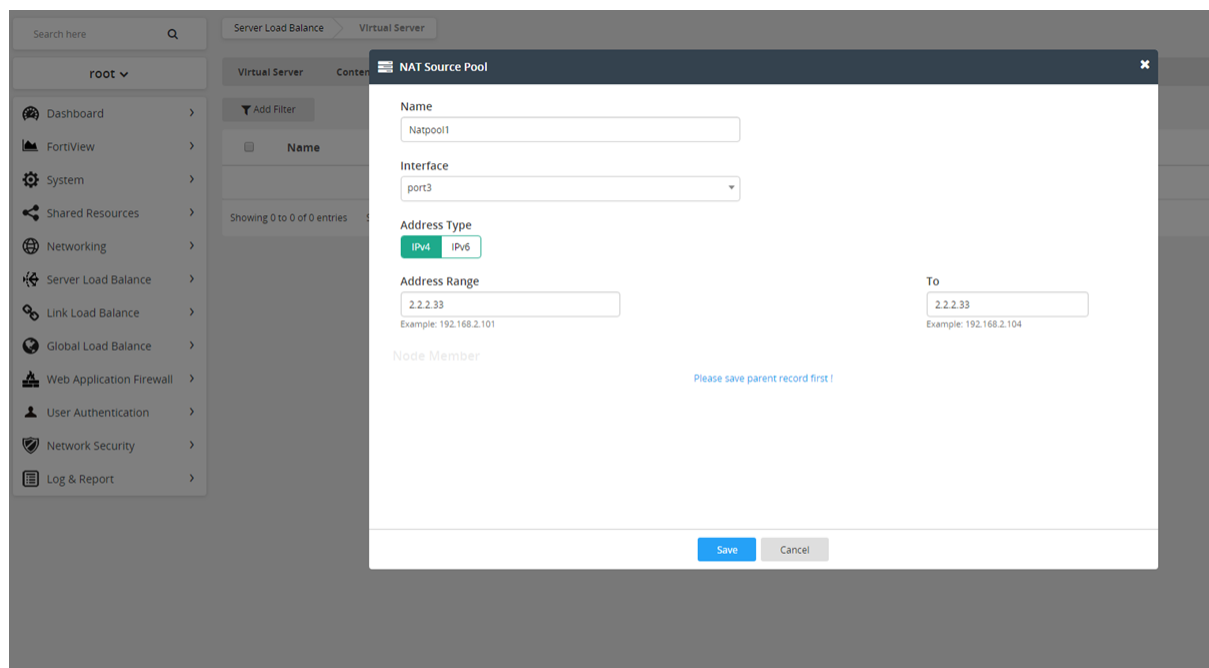
#### Step 2: Create new Real Server Pool and add real servers into it.



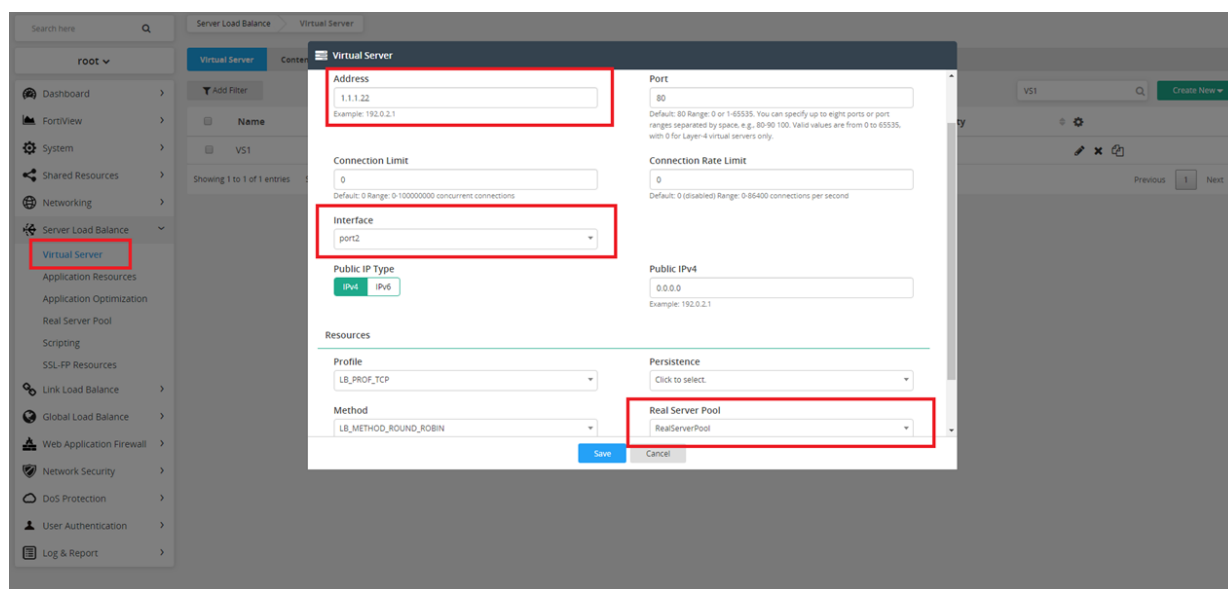
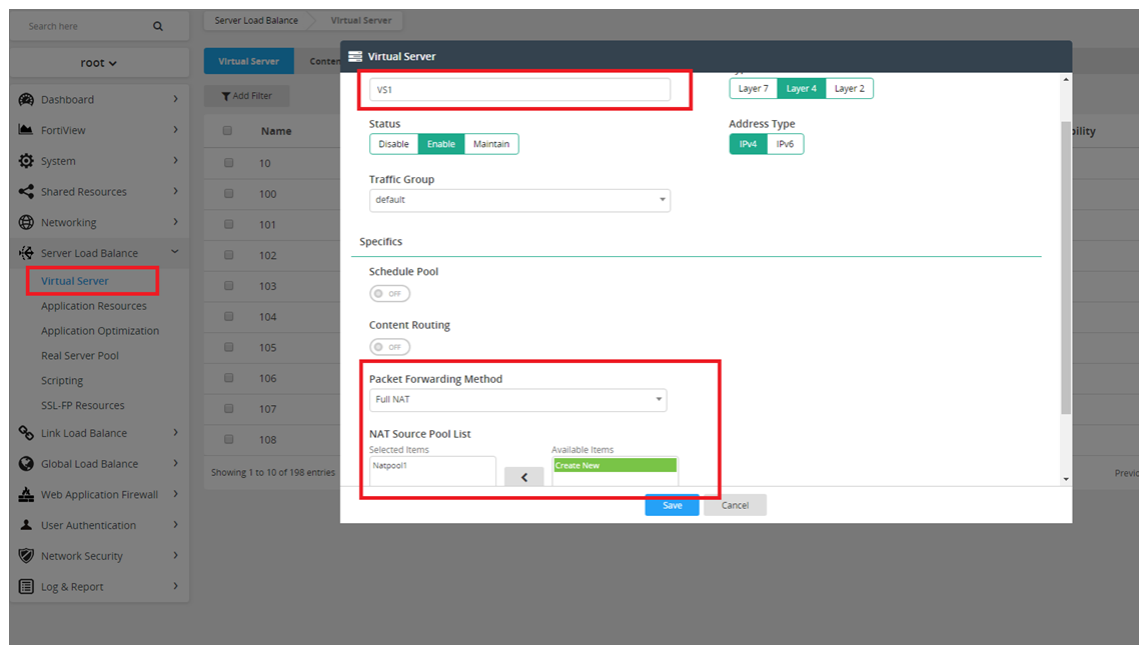
The screenshot shows the FortiADC web interface with the 'Real Server Pool' configuration modal open. The modal contains the following fields: 'Name' (RealServerPool), 'Address Type' (IPv4, IPv6), 'Health Check' (OFF), 'Real Server SSL Profile' (NONE), and a 'Member' section with a blue link that says 'Please save parent record first!'. At the bottom of the modal are 'Save' and 'Cancel' buttons.



### Step 3: Create a NAT source Pool



### Step 4: Create FullNAT Virtual Server and choose Real Server Pool



Step 5: Choose Profile TCP and Method LB\_METHOD\_ROUND\_ROBIN

The screenshot shows the 'Virtual Server' configuration window in the FortiADC interface. The 'Resources' section is highlighted with a red box, indicating the 'Profile' is set to 'LB\_PROF\_TCP' and the 'Method' is set to 'LB\_METHOD\_ROUND\_ROBIN'. Other visible fields include 'Address' (1.1.1.22), 'Port' (80), 'Connection Limit' (0), 'Interface' (port2), 'Public IP Type' (IPv4), and 'Public IPv4' (0.0.0.0).

### Set real server's weight (optional)



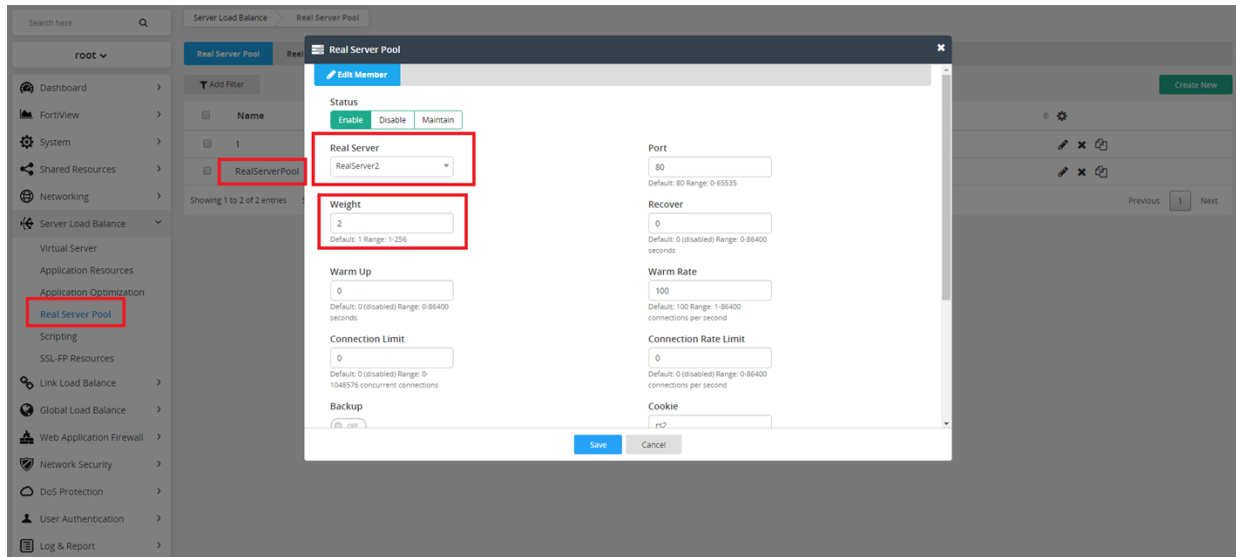
If you want to set different weights to the real server, please change the weight in Real Server Pool.

For example:

RealServer1's weight is 1, RealServer2's weight is 2. The total connections are 30, in this condition, 10 connections go to RealServer1, and another 20 connections go to RealServer2.

The screenshot shows the 'Real Server Pool' configuration window in the FortiADC interface. The 'Real Server' dropdown is set to 'RealServer1' and the 'Weight' is set to '1', both highlighted with red boxes. Other visible fields include 'Status' (Enable), 'Port' (80), 'Recover' (0), 'Warm Up' (0), 'Warm Rate' (100), 'Connection Limit' (0), 'Backup' (rs1), and 'Cookie' (rs1).





Step 6: Send traffic from client using tools like “curl” or “wget”

```
root@ubuntu:~# wget http://1.1.1.22/big.iso
--2018-12-31 09:58:47-- http://1.1.1.22/big.iso
Connecting to 1.1.1.22:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 869269504 (829M) [application/octet-stream]
Saving to: 'big.iso'

big.iso          100%[=====>] 829.00M  73.0MB/s   in 9.2s
2018-12-31 09:58:57 (90.3 MB/s) - 'big.iso' saved [869269504/869269504]
```

```
root@ubuntu:~# curl 1.1.1.22
server1
```

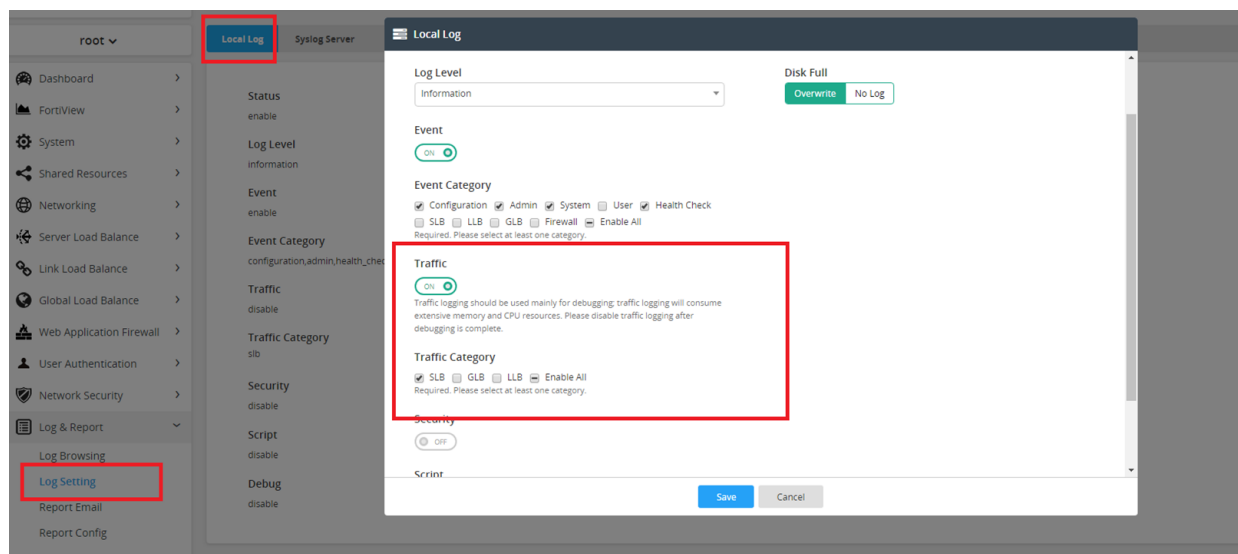
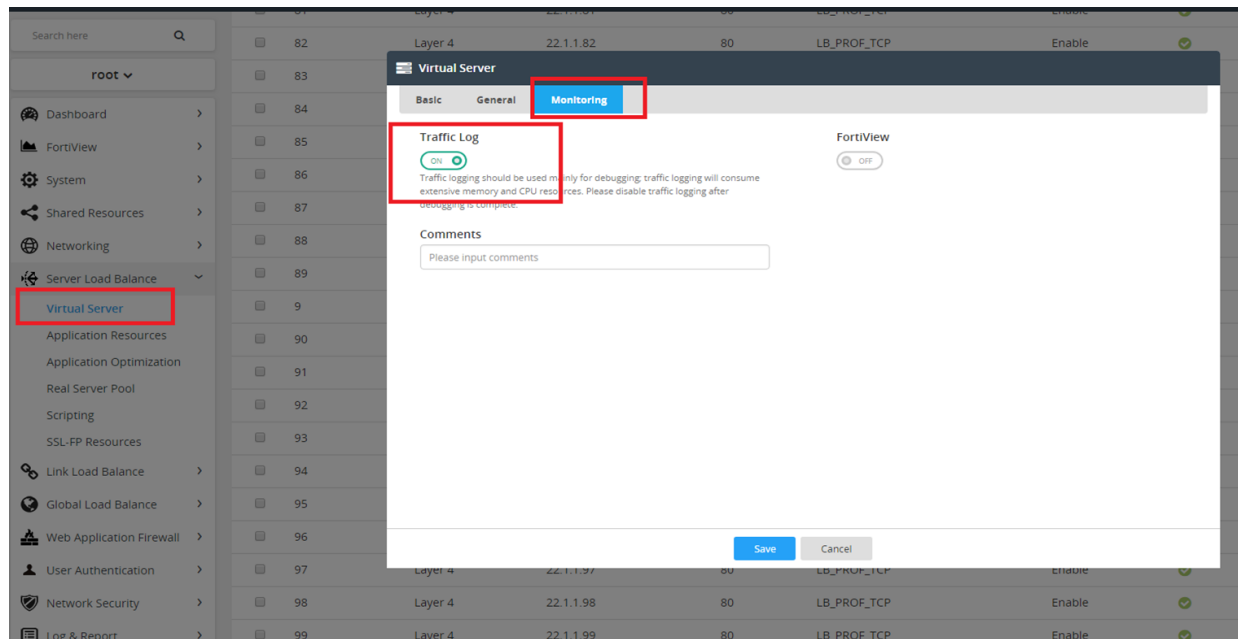
Check if the WRR method works. If you send three requests to the virtual server, you should receive two responses for real server 2, and one response for real server 1.

```
root@ubuntu:~# curl 1.1.1.22
server1
root@ubuntu:~# curl 1.1.1.22
server2
root@ubuntu:~# curl 1.1.1.22
server2
```

### Check traffic log and session table information

- Check the traffic log:

We need to enable traffic log in virtual server and Log&Report.



Search here

Log & Report

Log Browsing

root

Event Log

Security Log

Traffic Log

Script Log

Aggregate Log

SLB Layer 4

SLB HTTP

SLB TCPS

SLB RADIUS

GLB

SLB SIP

SLB RDP

SLB DNS

SLB RTSP

SLB SMTP

SLB RTMP

SLB DIAMETER

SLB MySQL

LLB

Filter Setting

Download

Refresh

Date	Time	Source	Received Bytes	Destination	Sent Bytes	Service	Virtual Server	Duration (s)	Trans Destination	Real Server Name
2018-12-31	02:02:27	1.1.1.90	1645562	1.1.1.22	894320609	tcp	VS1	8	2.2.2.2	RealServer1
Date	2018-12-31		2018-12-31				Time	02:02:27		
Log ID	0100008000						Log Level	information		
Message ID	741736						Duration (s)	8		
Received Bytes	1645562						Sent Bytes	894320609		
Protocol	6						Service	tcp		
Source	1.1.1.90						Source Port	47936		
Destination	1.1.1.22						Destination Port	80		
Trans Source	2.2.2.33						Trans Source Port	5022		
Trans Destination	2.2.2.2						Trans Destination Port	80		
Virtual Server	VS1						Action	none		
Source Country	Australia						Destination Country	Australia		
Type	traffic						Sub Type	slb_layer4		
Vdom	root						Real Server Name	RealServer1		
2018-12-31	02:02:22	1.1.1.90	120	1.1.1.22	176	tcp	VS1	6	2.2.2.3	RealServer2

Showing 1 to 2 of 2 entries

Show

10

entries

Previous

1

Next

Check if WRR method works as expected from the traffic log:

From the traffic log, we can see the traffic go to the real server according to their weight (RS1:RS2=1:2).

Search here

Log & Report Log Browsing

Event Log Security Log **Traffic Log** Script Log

SLB Layer 4 SLB HTTP SLB TCPS SLB RADIUS GLB SLB SIP SLB RDP SLB DNS SLB RTSP SLB SMTP SLB RTMP SLB DIAMETER SLB MySQL LLB

Filter Setting Download Refresh 18/08/14 08:46:49 - 19/11/25 04:21:29

Date	Time	Source	Received Bytes	Destination	Sent Bytes	Service	Virtual Server	Duration (s)	Trans Destination	Real Server Name
2019-11-25	04:31:39	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2
2019-11-25	04:29:14	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2
2019-11-25	04:29:14	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.2	RealServer1
2019-11-25	04:29:13	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2
2019-11-25	04:29:11	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2
2019-11-25	04:29:11	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.2	RealServer1
2019-11-25	04:29:11	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2
2019-11-25	04:29:10	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2
2019-11-25	04:29:10	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.2	RealServer1
2019-11-25	04:29:09	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2

Show 10 entries Previous 1 2 3 4 5 Next

• Check the session table:

**FortiView**

The screenshot shows the FortiADC GUI for device LTS-SLB1-HA1. The 'Session Table' is selected, showing a table with session details. The table has columns for Source Address: Port, VS Address: Port, Local Address: Port, Dest Address: Port, State, Protocol, Service, In Bytes, Out Bytes, Expires, and RS Name. A single session is listed with the following details:

Source Address: Port	VS Address: Port	Local Address: Port	Dest Address: Port	State	Protocol	Service	In Bytes	Out Bytes	Expires	RS Name
1.1.1.90:47956	1.1.1.22:80	2.2.2.33:5032	2.2.2.2:80	ESTABLISHED	6	tcp	1356082	628101144	100	RealServer1

The table also includes a 'Show 10 entries' link.

## CLI

```
tM) LTS-SLB1-HA1 (root) # diagnose server-load-balance session lis
client-ip/port virtual-server-ip/port local-ip/port real-server-ip/port protocol service state in-bytes out-bytes expire virtual-ser
ver-name real-server-name
1.1.1.90 47964 1.1.1.22 80 2.2.2.33 5036 2.2.2.2 80 6 tcp ESTABLISHED 1490474 792525392 100 VS1 RealServer1
```



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.