FortiADC - Server Load Balance Layer 4 Deployment Guide

Version 5.3.0

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

November 26, 2019
FortiADC 5.3.0 Server Load Balance Layer 4 Deployment Guide

TABLE OF CONTENTS

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.

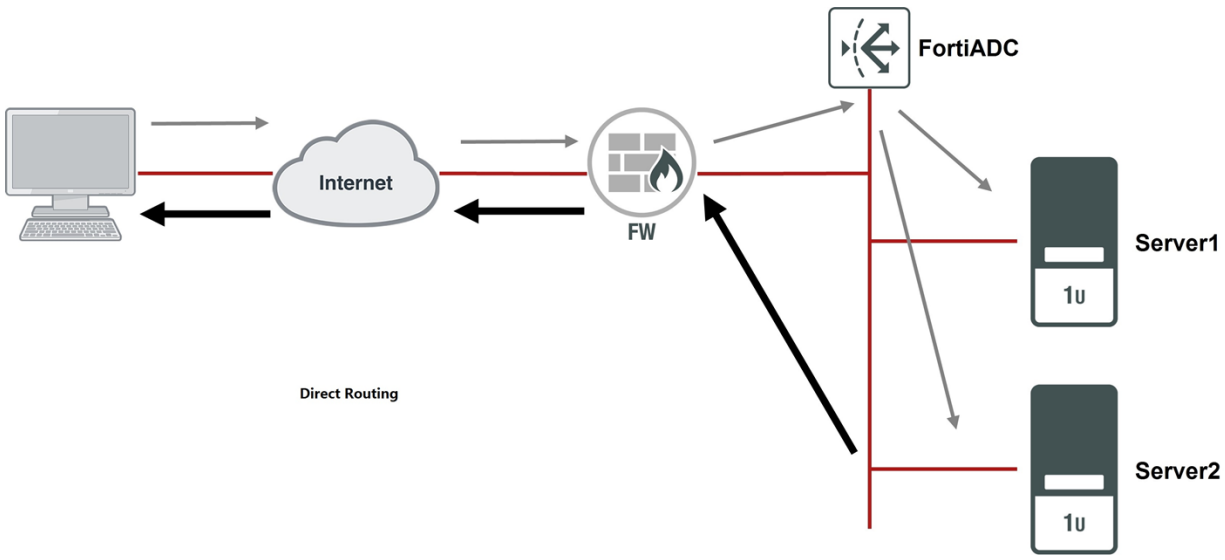
For layer 4 virtual server, it has five packet forwarding methods—Direct Routing, DNAT, Full NAT, Tunneling, NAT46.

Server Load Balance Layer-4 VS

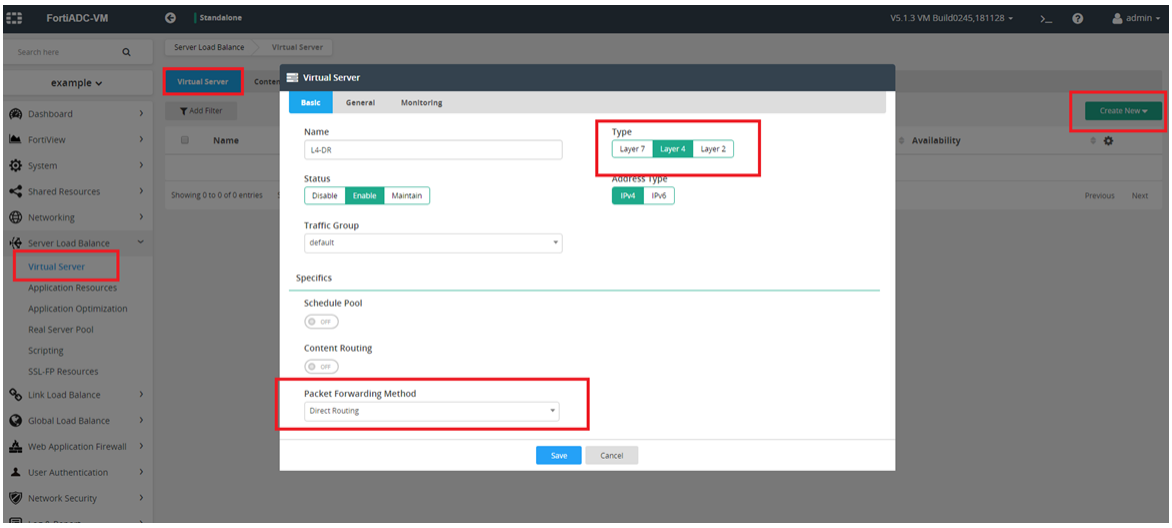
Direct Routing mode

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

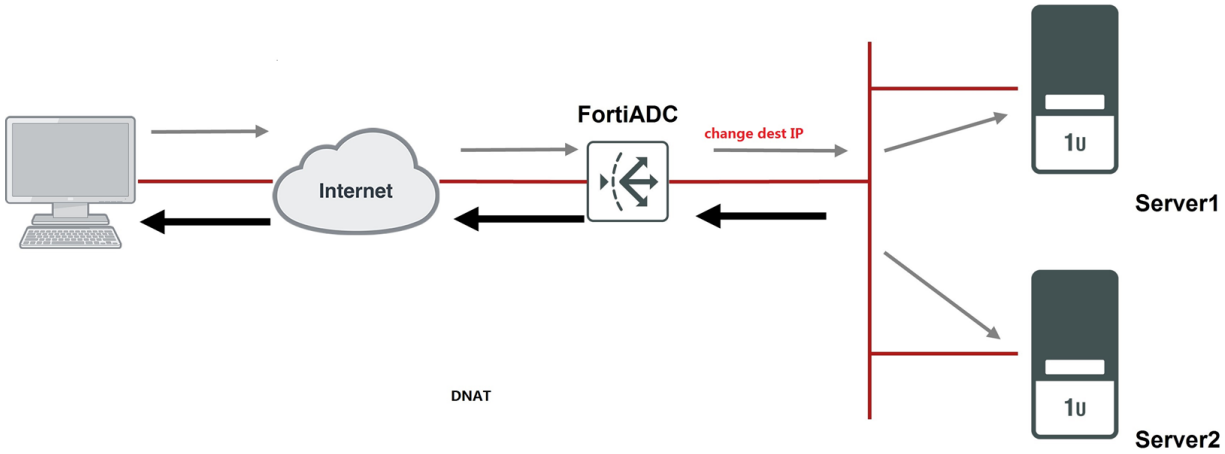
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled

netsh interface ipv4 set interface "loopback" weakhostsend=enabled

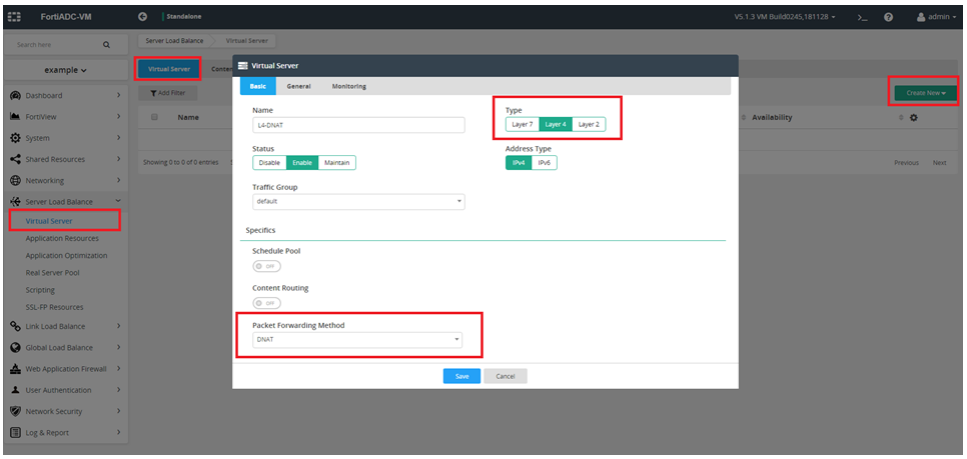
DNAT mode

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:

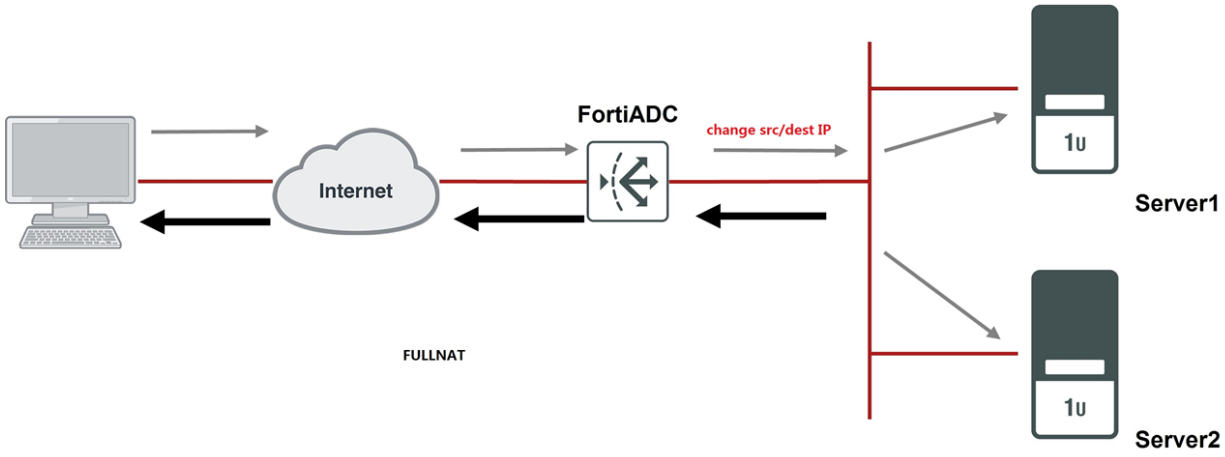


- Use DNAT as the packet forwarding method and set the default gateway on each server to FortiADC's IP address on the same subnet/VLAN (or, use static routes to send responses to FortiADC's IP address)

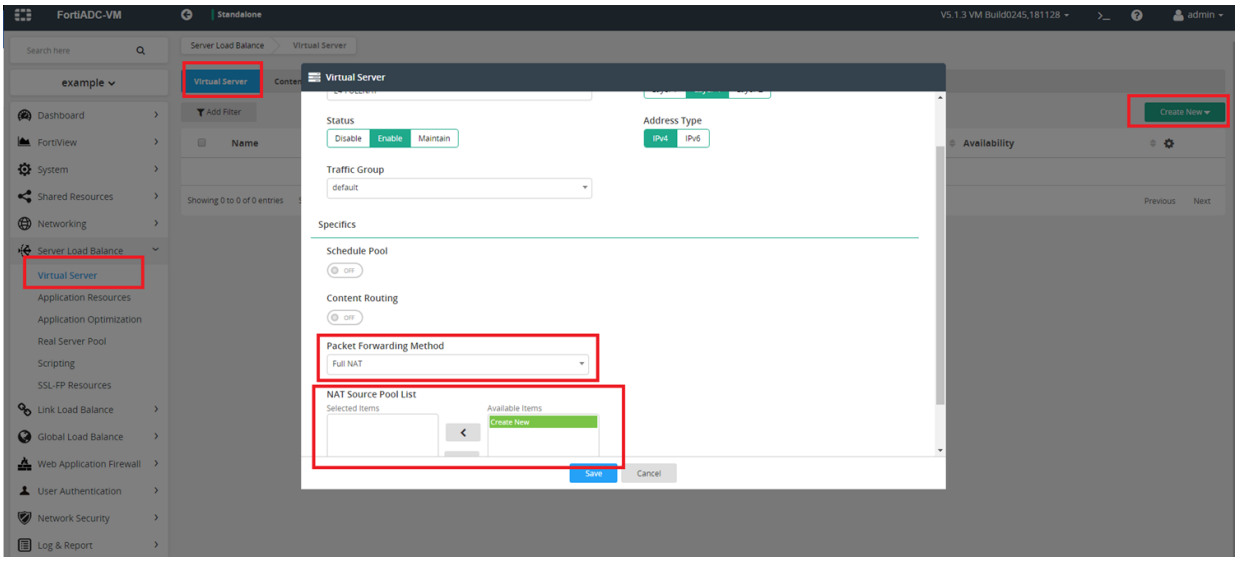
FULLNAT mode

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:



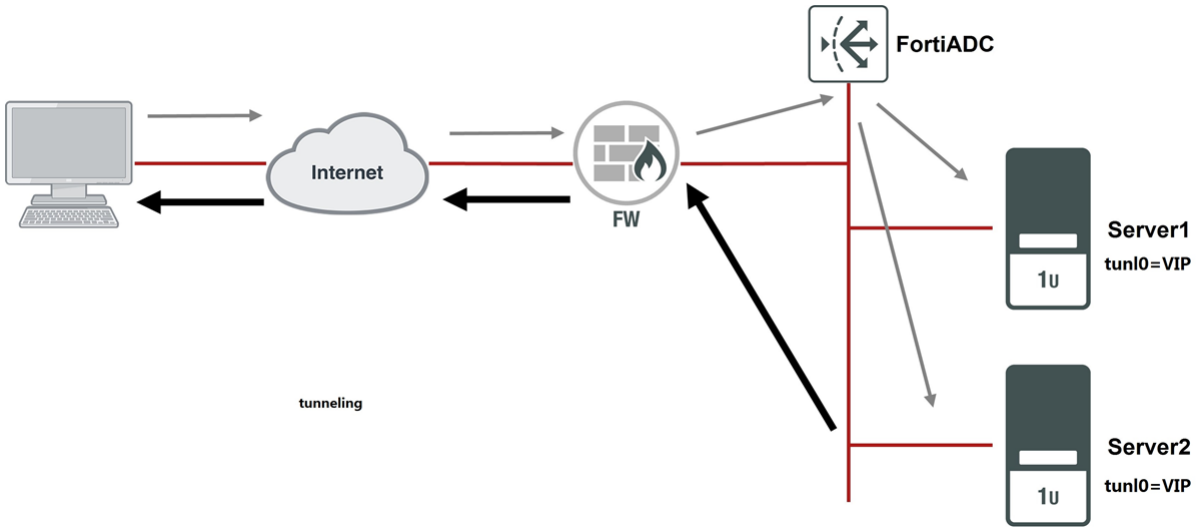
GUI:



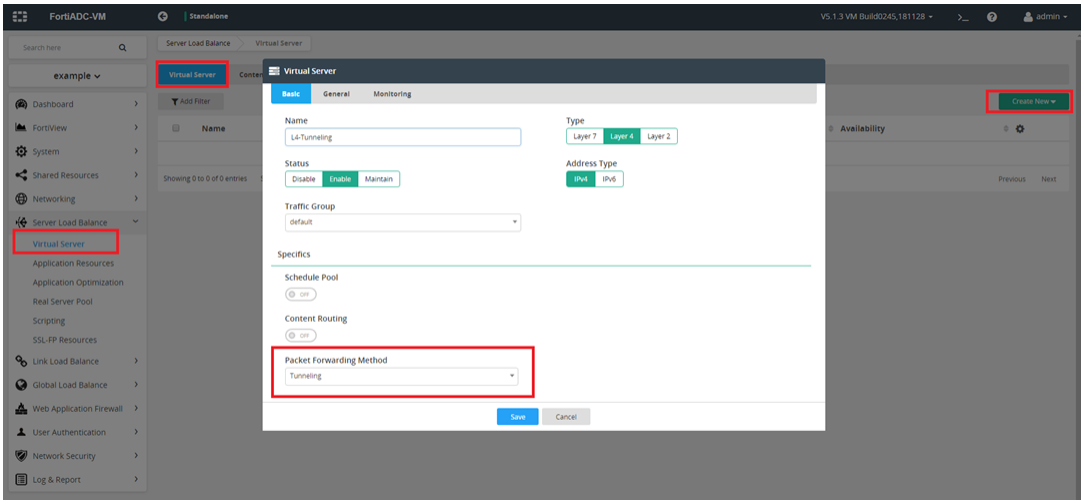
Tunneling mode

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:



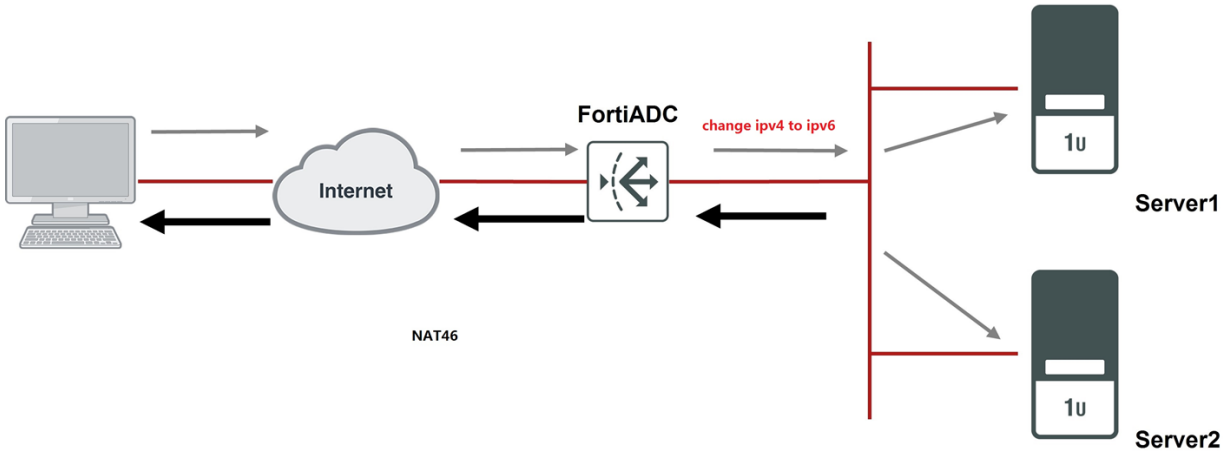
GUI:



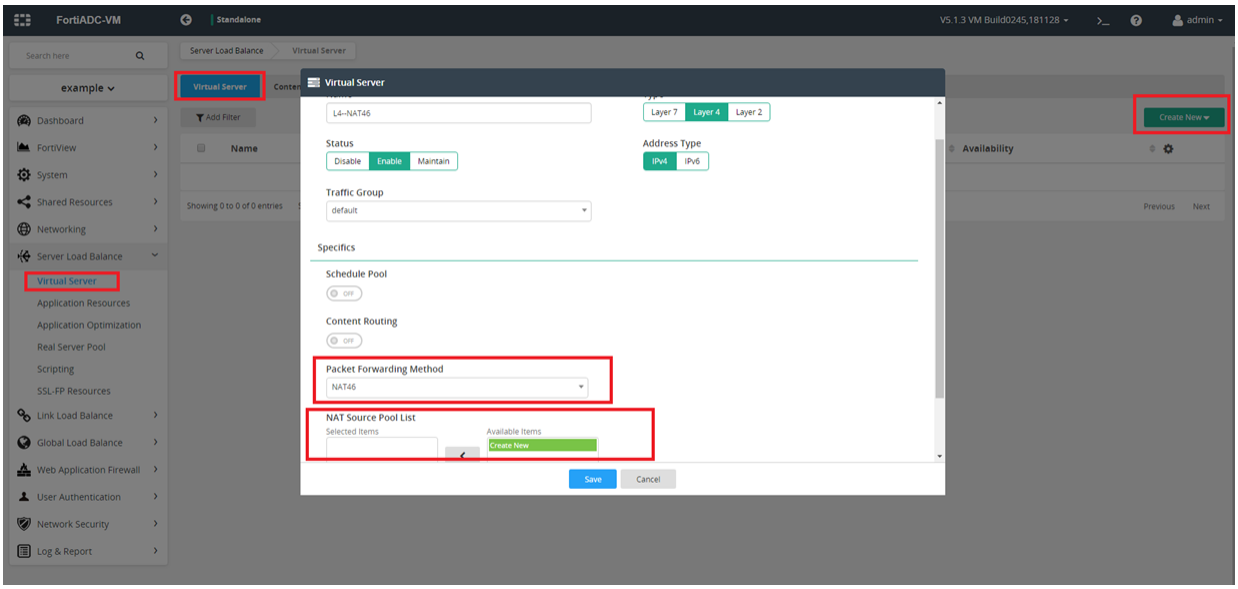
NAT46 mode

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:

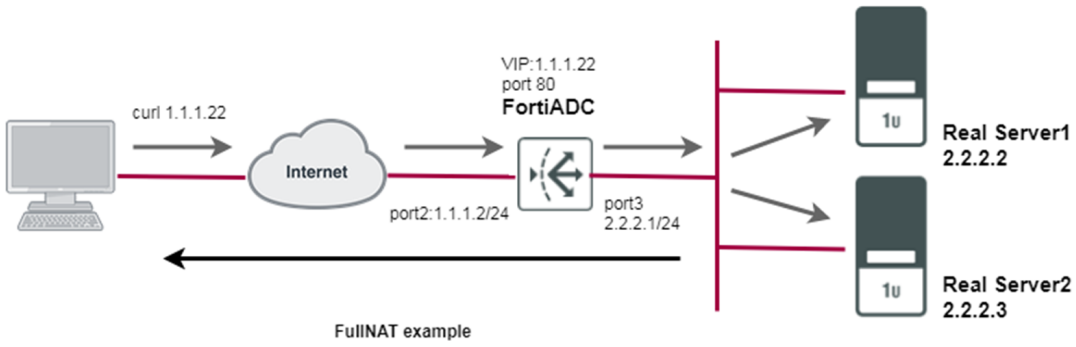


GUI:



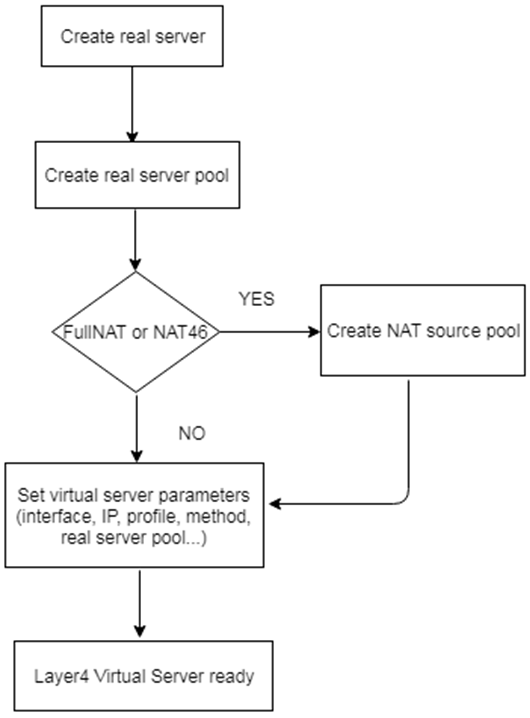
FortiADC SLB4 Deployment with FullNAT mode and TCP profile and WRR method

SLB4 FullNAT Example Topology



FullNAT example

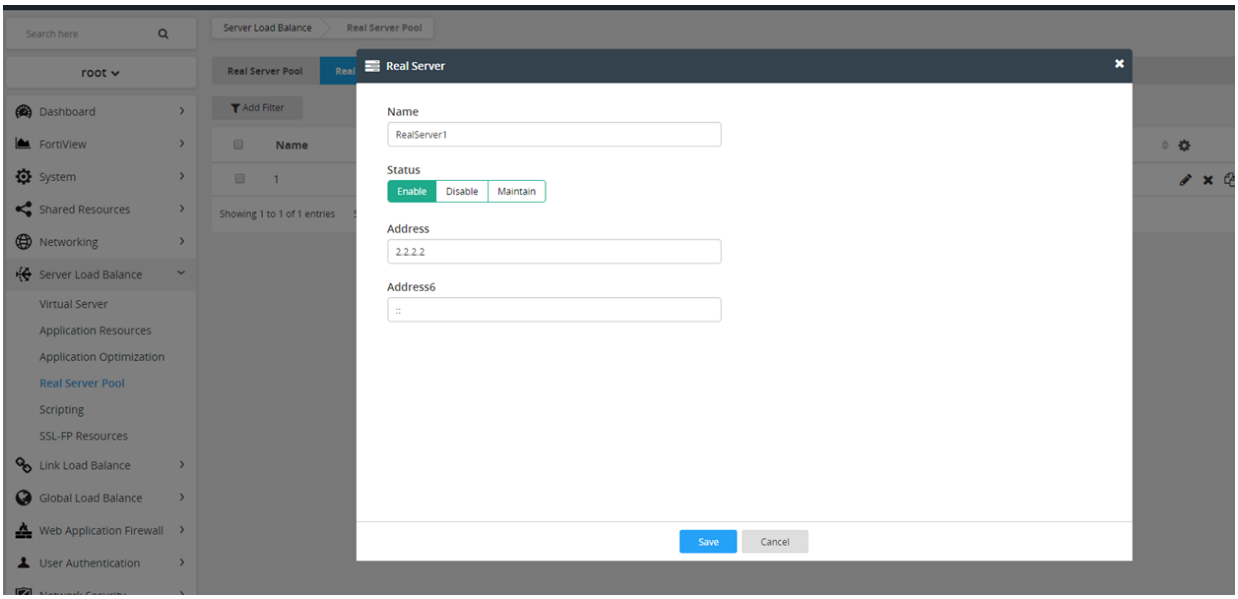
SLB4 FullNAT, TCP profile, WRR method steps



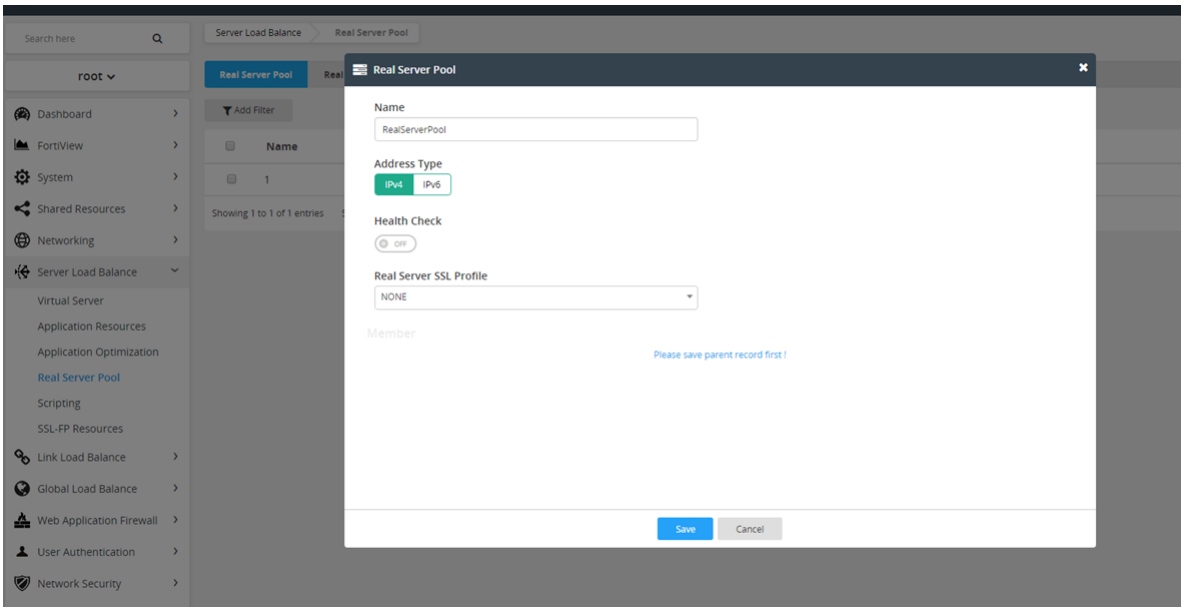
basic Layer4 VS steps

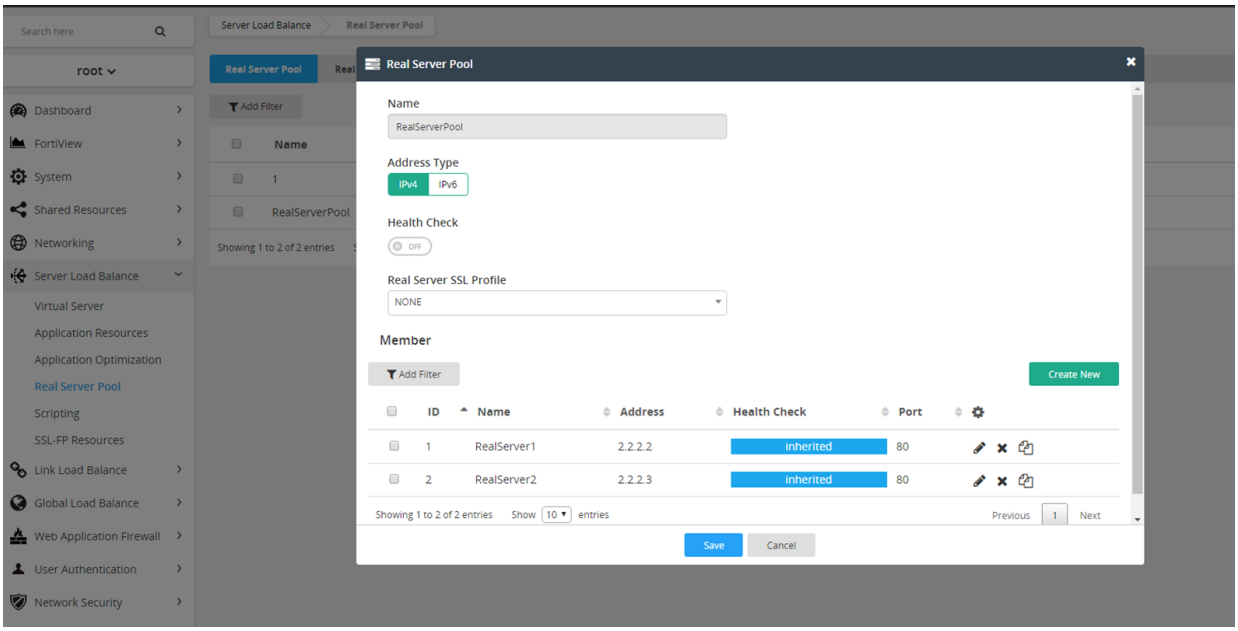
To deploy a SLB Layer 4 server:

Step 1: Create new Real Server

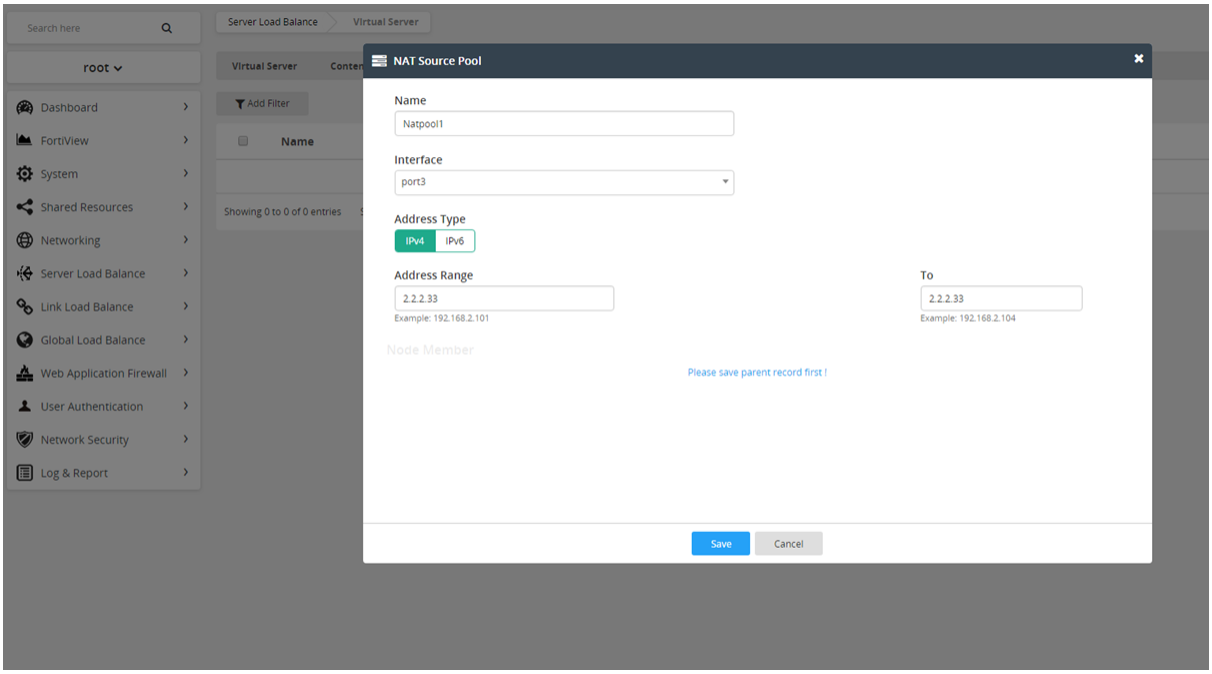


Step 2: Create new Real Server Pool and add real servers into it.

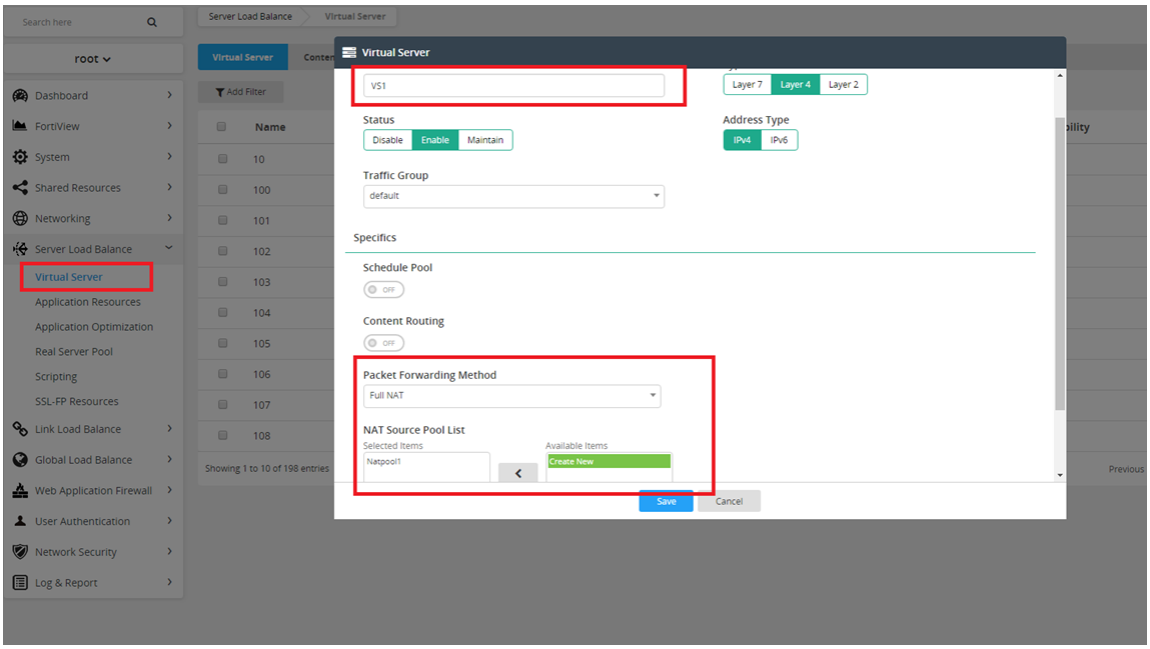


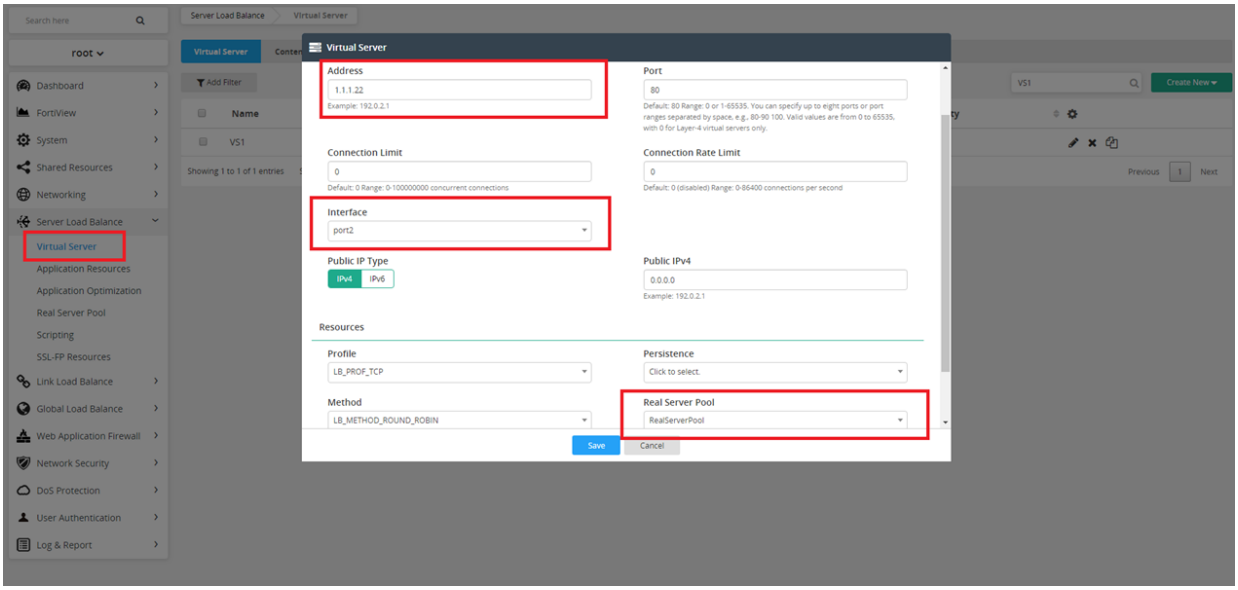


Step 3: Create a NAT source Pool

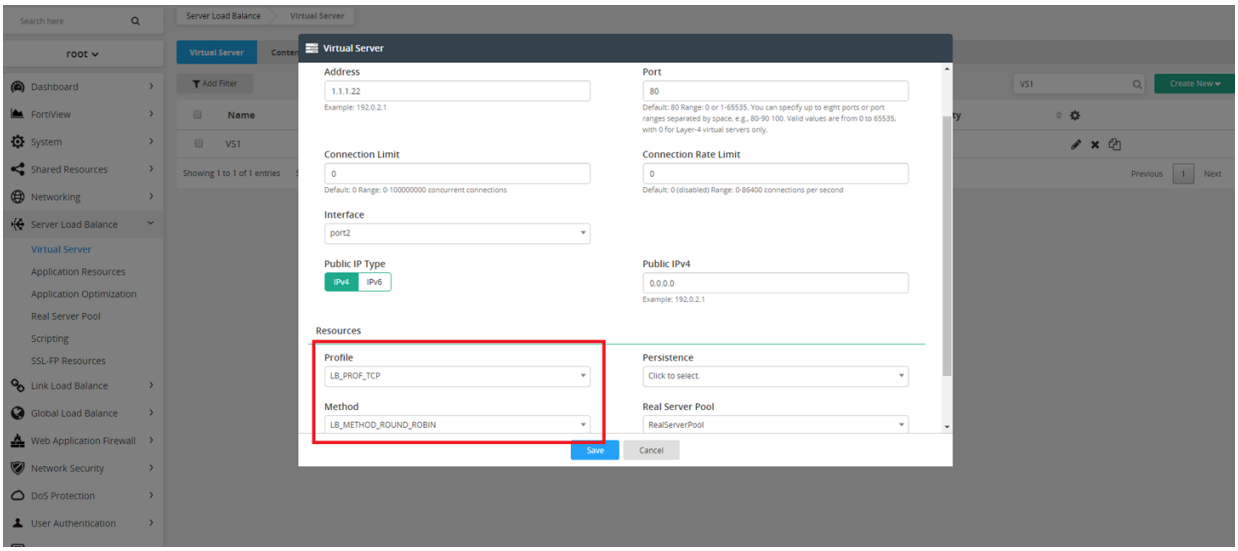


Step 4: Create FullNAT Virtual Server and choose Real Server Pool





Step 5: Choose Profile TCP and Method LB_METHOD_ROUND_ROBIN

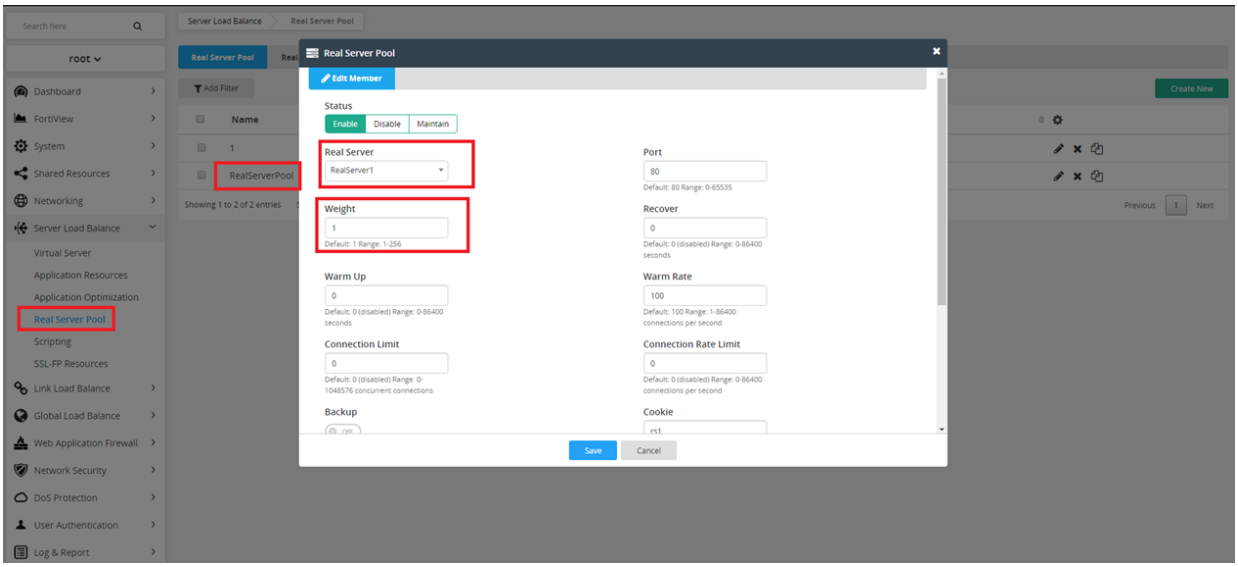


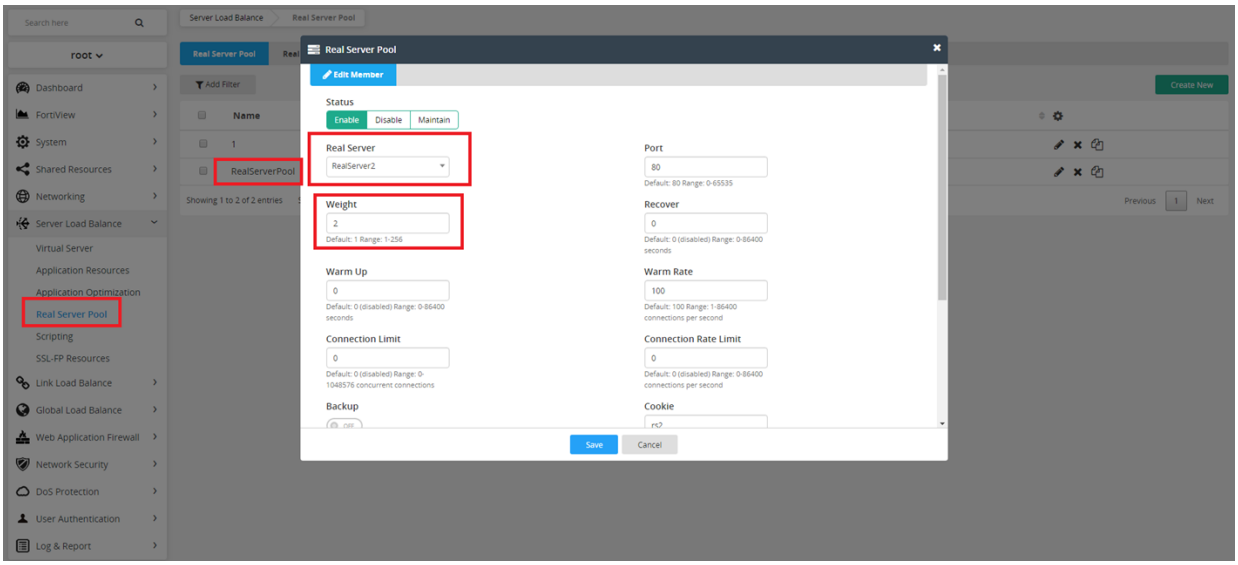
Set real server's weight (optional)

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.





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
```

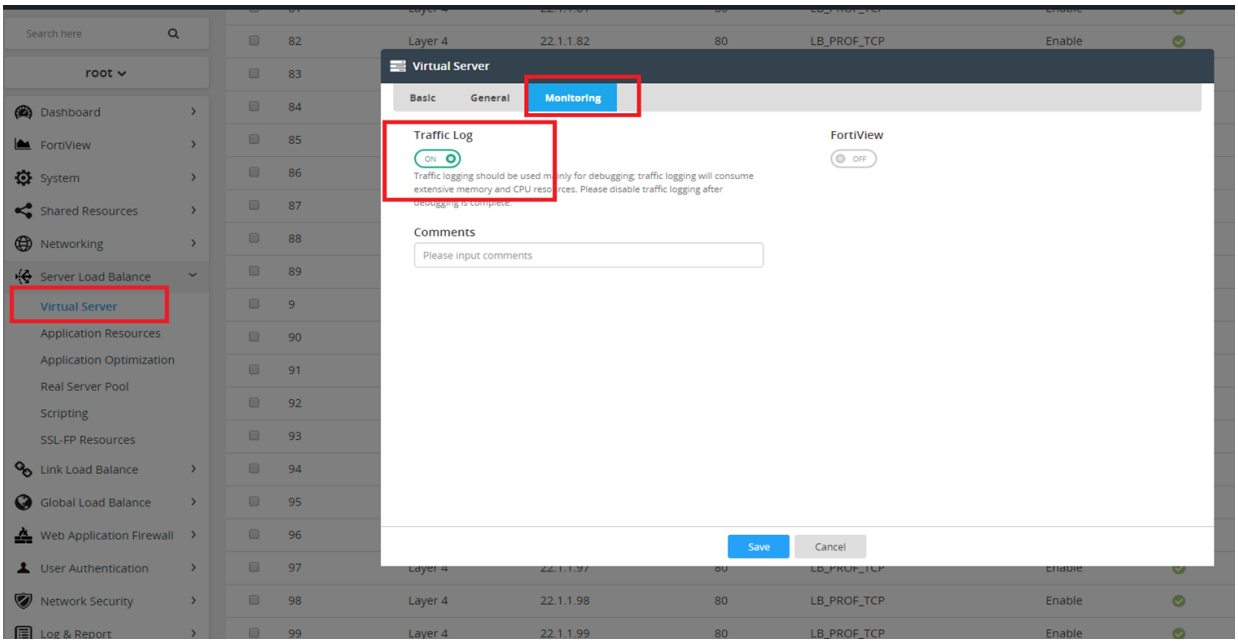
Check if the WRR method works. If you send three requests to the virtual server, you should receive two responses for real server 2, and one response for real server 1.

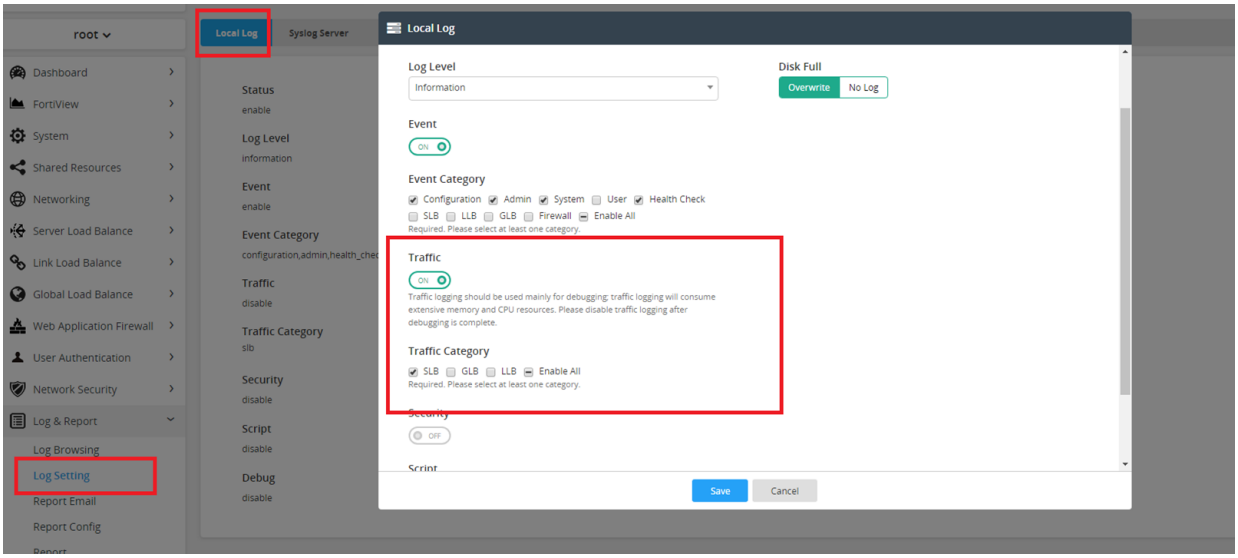
```
root@ubuntu:~# curl 1.1.1.22
server1
root@ubuntu:~# curl 1.1.1.22
server2
root@ubuntu:~# curl 1.1.1.22
server2
```

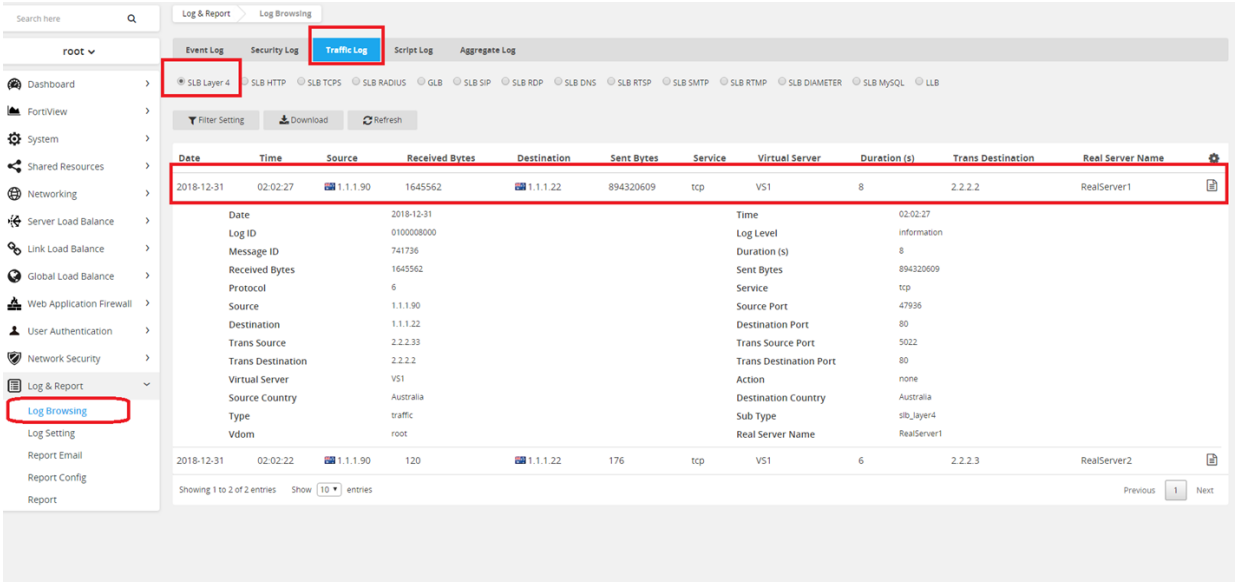
Check traffic log and session table information

• Check the traffic log:

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

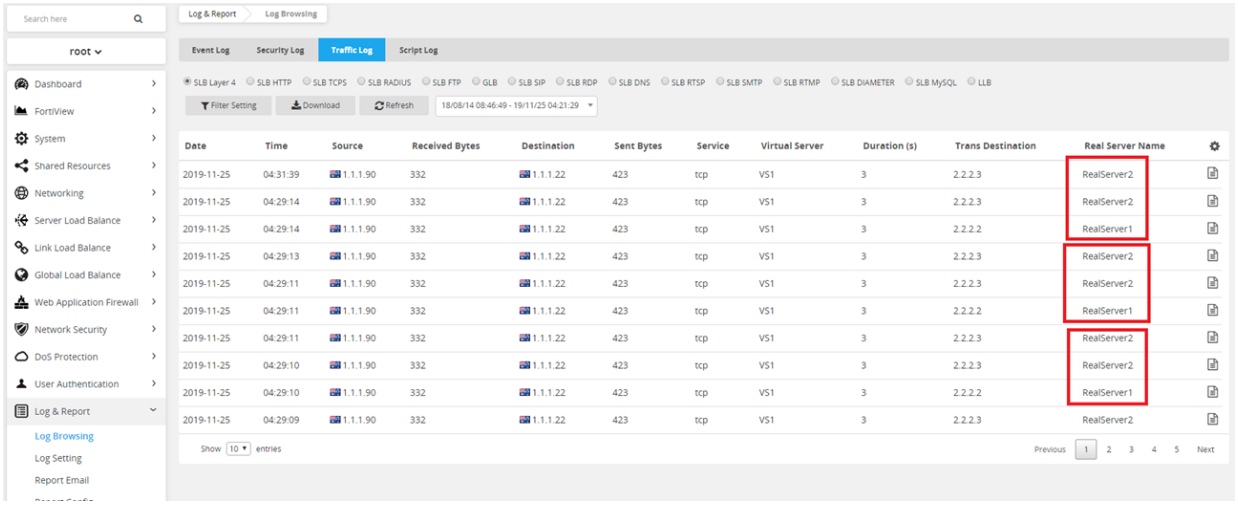

Search here
root
Dashboard
FortiView
System
Shared Resources
Networking
Server Load Balance
Virtual Server
Application Resources
Application Optimization
Real Server Pool
Scripting
SSL-FP Resources
Link Load Balance
Global Load Balance
Web Application Firewall
User Authentication
Network Security
Log & Report
Virtual Server
Basic
General
Monitoring
Traffic Log
ON
Traffic logging should be used mainly for debugging; traffic logging will consume extensive memory and CPU resources. Please disable traffic logging after debugging is complete.
FortiView
OFF
Comments
Please input comments
Save
Cancel
Layer 4
22.1.1.82
80
LB_PROF_TCP
Enable
22.1.1.98
22.1.1.99


root
Dashboard
FortiView
System
Shared Resources
Networking
Server Load Balance
Link Load Balance
Global Load Balance
Web Application Firewall
User Authentication
Network Security
Log & Report
Log Browsing
Log Setting
Report Email
Report Config
Local Log
Syslog Server
Status
enable
Log Level
information
Event
enable
Event Category
Traffic
disable
Traffic Category
slb
Security
disable
Script
disable
Debug
disable
Local Log
Log Level
Information
Disk Full
Overwrite
No Log
Event
ON
Event Category
Configuration
Admin
System
User
Health Check
SLB
LLB
GLB
Firewall
Enable All
Required. Please select at least one category.
Traffic
ON
Traffic logging should be used mainly for debugging; traffic logging will consume extensive memory and CPU resources. Please disable traffic logging after debugging is complete.
Traffic Category
SLB
GLB
LLB
Enable All
Required. Please select at least one category.
OFF
Save
Cancel



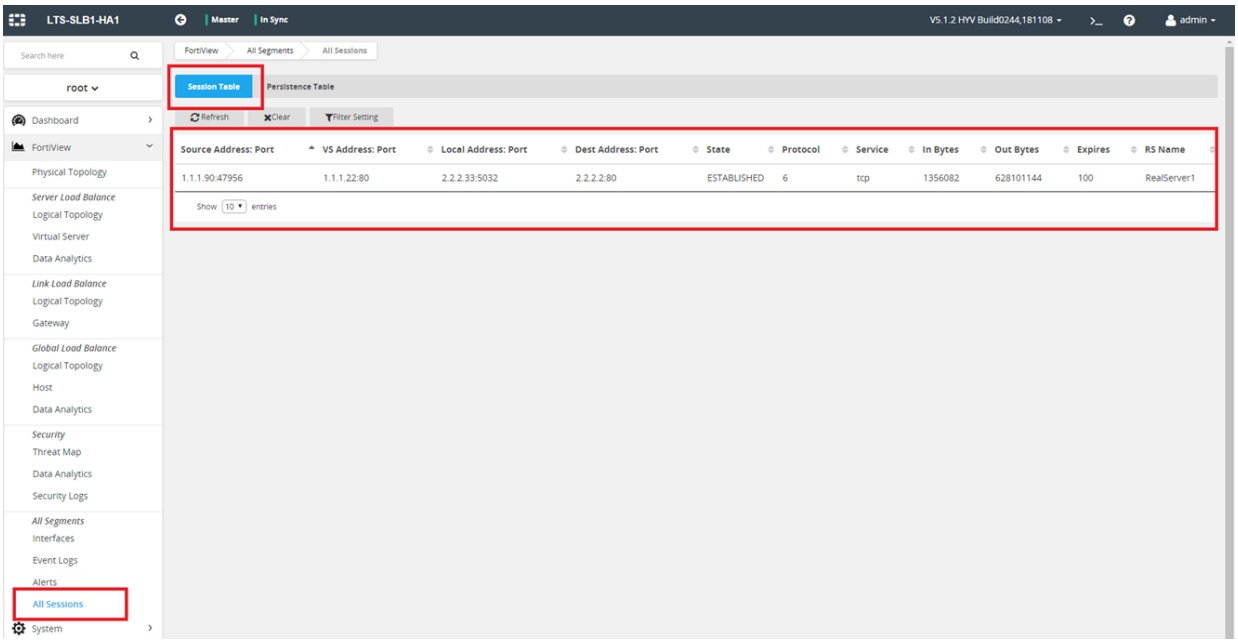
Check if WRR method works as expected from the traffic log:

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



• Check the session table:

Fortiview



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
```