



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	4
Introduction	5
Server load balance layer 4	6
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.

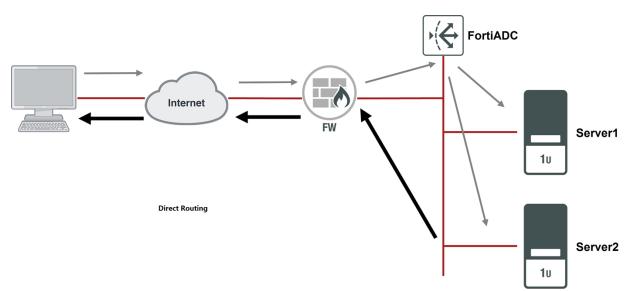
For layer 4 virtual server, it has five packet forwarding methods—Direct Routing, DNAT, Full NAT, Tunneling, NAT46.

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:

⇔	FortiADC-VM		G Standalone		V5.1.3 VM Build0245,181128 -	>	0 🎍	admin 👻
	arch here Q		Server Load Balance Vin	tual Server				
	example 🗸		Virtual Server Conten	Virtual Server				
	Dashboard	>	▼ Add Filter	Basic General Monitoring			Create	New 🛩
	FortiView	>	Name Name	Name Type L4-0R Layer 7 Layer 4 Layer 2	© Availability		• •	
۵	System	>		Status Address type				
4	Shared Resources	>	Showing 0 to 0 of 0 entries	Disable Enable Maintain			Previous	Next
		>		Traffic Group				
*	Server Load Balance	~		default *				
	Virtual Server Application Resources			Specifics				
	Application Optimization			Schedule Pool				
	Real Server Pool			(m)				
	Scripting			Content Routing				
	SSL-FP Resources			() on				
8	Link Load Balance	>		Packet Forwarding Method				
Ø	Global Load Balance	>	L	Direct Routing *				
▲	Web Application Firewall	>		Save Cancel				
1	User Authentication	>						
۲	Network Security	>						

- 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

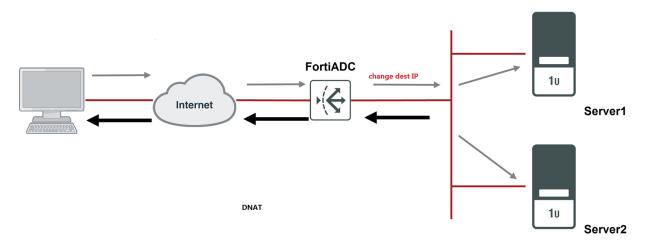
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled

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:

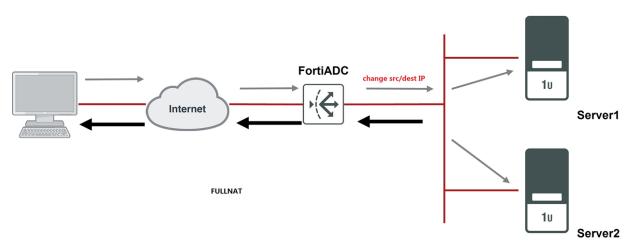
FortiADC-VM	G Standalone		V5.1.3 VM Build0245,181128 - >_	🚱 🔮 admin 🗸
Search here Q	Server Load Balance Vir	ual Server		
example 🗸	Virtual Server Conter	I Virtual Server		
(a) Dashboard >	¥ Add Filter	Basic General Monitoring		Create New 🛩
FortiView >	8 Name	Name Type L40NAT Layer 2 Layer 2	Availability	• •
🐼 System >		Status Address Type		
Shared Resources	Showing 0 to 0 of 0 entries	Disable Enable Maintain IPv6		Previous Next
Networking		Traffic Group		
🛠 Server Load Balance 🛛 👻		defauit. •		
Virtual Server		Specifics		
Application Resources Application Optimization		Schedule Pool		
Real Server Pool				
Scripting		Content Routing		
SSL-FP Resources		0 01		
℃ Link Load Balance		Packet Forwarding Method		
Global Load Balance		DNAT *		
🚣 Web Application Firewall >		Sive Cancel		
LUSER Authentication				
Network Security				
Log & Report				

 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:



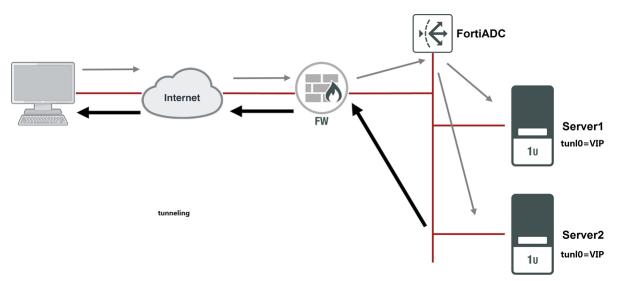
GUI:

0	FortiADC-VM		G Standalone		V5.1.3 VM Build0245,181128 -	>_ 🕜 💄 admin 🗸
s	earch here C	2	Server Load Balance Virt	ual Server		
	example 🗸		Virtual Server Conten	Virtual Server		
	Dashboard	>	T Add Filter	Status Address Type		Create New 🗸
	FortiView	>	Name	Disable Enable Maintain IPv4 IPv6	Availability	• •
¢	System	>		Traffic Group		
4	Shared Resources	>	Showing 0 to 0 of 0 entries	default *		Previous Next
۲	Networking	>		Specifics		
• (Server Load Balance	ř		Schedule Pool		
L	Virtual Server			() or		
	Application Resources Application Optimization			Content Routing		
	Real Server Pool			Packet Forwarding Method		
	Scripting			Full NAT *		
	SSL-FP Resources			NAT Source Pool List		
8	Link Load Balance	>		Selected Items Available Items Create New		
Ø	Global Load Balance	>		<		
4	Web Application Firewall	>		Save Cancel		
1	User Authentication	>				
1	Network Security	>				
	Log & Report	>				

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:



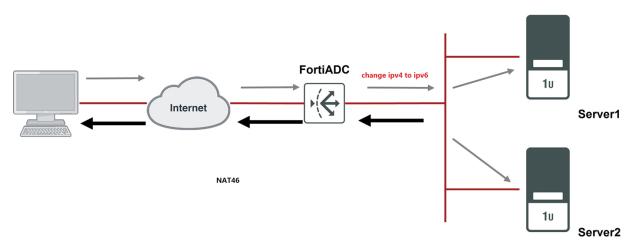
GUI:

===	FortiADC-VM		G Standalone		V5.1.3 VM Build0245,181128 -	- 0	🚢 a	dmin +
Search	here Q		Server Load Balance Vir	tual Server				Î
	example 🗸		Virtual Server Conten	Tirtual Server				
(a) Das	shboard	>	¥ Add Filter	Basic General Monitoring			Create N	ew 🕶
E Fort	tīView	>	Name	Name Type L4-Tunneling Layer 7 Layer 4 Layer 2	Availability		• •	
🚯 Syst		>		Status Address Type				
		>	Showing 0 to 0 of 0 entries 5	Disable Enable Maintain			revious	Next
	tworking	>		Traffic Group				
	ver Load Balance	ř		default *				
	plication Resources			Specifics				
	plication Optimization			Schedule Pool				
	ipting			Content Routing				
	-FP Resources			() on				
		>		Packet Forwarding Method Tunneling *				
-	bal Load Balance b Application Firewall							
_	o Application Firewall			Save Cancel				
		>						
🔳 Log	ş & Report	>						

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:

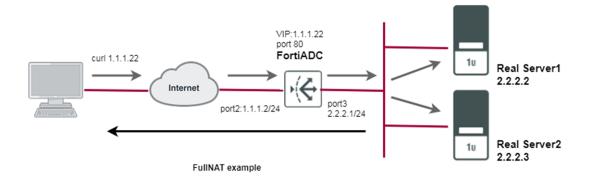


GUI:

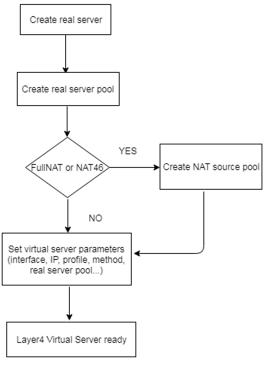
FortiADC-VM	C Standalone	V5.1.3 VM Build0245,181128 - >_	😧 🔒 admin 🗸
Search here Q	Server Load Balance Virtual Server		
example 🗸	Virtual Server Conten 🗮 Virtual Server		
Dashboard >	Y Add Ricer Layer 7 Layer 7 Layer 2	·	Create New 🗸
FortiView >	Name Status Address Type Disable Enable Maintain IPv4 IPv6	Availability	• •
System >	Traffic Group		
Shared Resources	Showing 0 to 0 of 0 entries default v		Previous Next
Networking >	Specifics		
Virtual Server	Schedule Pool		
Application Resources	() on		
Application Optimization	Content Routing		
Scripting	Packet Forwarding Method		
SSL-FP Resources	NAT46 *		
Selection Content of C	NAT Source Pool List Selected Items Available Items		
Web Application Firewall	Create New		
▲ User Authentication >	Save Cancel		
Network Security			
Log & Report			

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

Search here Q	Server Load Balance	Real Server Pool	
root 🗸	Real Server Pool	Real Server X	
Dashboard	> TAdd Filter	Name	
FortiView	> 📄 Name	RealServer1	• \$
🔅 System	> 1	Status Enable Disable Maintain	din a
Shared Resources	> Showing 1 to 1 of 1 entr		
Networking	>	2222	
A server cour submer	~	Address6	
Virtual Server		и	
Application Resources Application Optimization			
Real Server Pool			
Scripting			
SSL-FP Resources			
S Link Load Balance	>		
Global Load Balance	>		
Web Application Firewall	>	Save Cancel	
Luser Authentication	>		

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

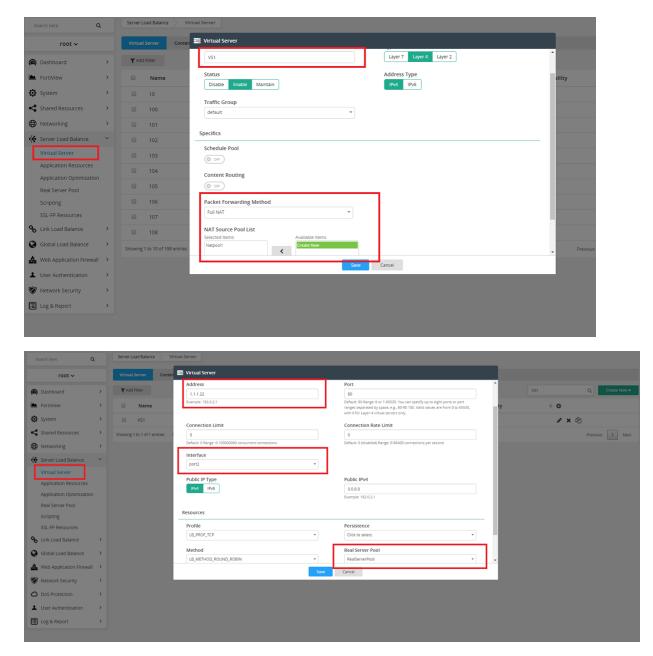
Search here Q	Server Load Balance Real Server Pool
root 🗸	Real Server Pool Real Server Pool X
Dashboard	T Add Riter Name RealServerPool
FortiView	Name State
System	Address Type
Shared Resources	Showing I to 1 of 1 entries 5 Health Check
Networking	
Server Load Balance	Real Server SSL Profile
Virtual Server	NONE *
Application Resources	Member
Application Optimization	Please save parent record first !
Real Server Pool	
Scripting	
SSL-FP Resources	
S Link Load Balance	
Global Load Balance	
Web Application Firewall	Save Cancel
Luser Authentication	
Network Security	

Search here Q	Server Load Balance Re	Real Server Pool	
root 🗸	Real Server Pool Real	Real Server Pool X	
Dashboard >	▼ Add Filter	Name	
E FortiView	Name	RealServerPool	
System >	8 1	Address Type IPv4 IPv6	
Shared Resources	RealServerPool	Health Check	
Networking	Showing 1 to 2 of 2 entries	() OF	
Server Load Balance		Real Server SSL Profile	
Virtual Server		NONE	
Application Resources		Member	
Application Optimization		T Add Filter	
Real Server Pool			
Scripting		🗐 ID 🔦 Name 🗢 Address 🗢 Health Check 🗢 Port 🗢 🏠	
SSL-FP Resources		🗆 1 RealServer1 2.2.2.2 inherited 80 🖋 🗶	
S Link Load Balance		2 RealServer2 2.2.2.3 inherited 80 🖋 🗶 🖓	
Global Load Balance		Showing 1 to 2 of 2 entries Show 10 T entries Previous 1 Next	
Web Application Firewall		Save Cancel	
Luser Authentication			
♥ Network Security >			

Step 3: Create a NAT source Pool

Search here Q	Server Load B	alance Virtual Server					
root 🗸	Virtual Serve	er Conten 🔜 NAT So	ource Pool				×
🖗 Dashboard	> TAdd Filter	Name Natpo					
FortiView	> 🗆 N	lame					
🔅 System	>	Interfa port3		•			
	> Showing 0 to 0	of 0 entries SAddres	ss Type				
Networking	>	IPv4	IPv6				
🕀 Server Load Balance	>	Addres	ss Range			То	
🗞 Link Load Balance	>	2.2.2.3 Example:	33			2.2.2.33 Example: 192.168.2.104	
Global Load Balance	>	Node M					
📥 Web Application Firewall	>			Please save parent re	cord first !		
Luser Authentication	>						
🗑 Network Security	>						
Log & Report	>						
				Save C	ancel		

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



Step 5: Choose Profile TCP and Method LB_METHOD_ROUND_ROBIN

Search here Q		Server Load Balance Virt	ual Server	
root 🗸		Virtual Server Conten	🚔 Virtual Server	
			Address	Port
Dashboard	>	T Add Filter	1.1.1.22	80 VSI Q Create New -
FortiView	>	Name	Example: 192.0.2.1	Default 20 Range: 0 or 1-5555. You can specify up to eight ports or port ranges separated by space. e.g. 80-90 OL Valid values are from 0 to 5555. with 0 for Lange-4 virtual servers only.
System	>	VS1	Connection Limit	Connection Rate Limit
Shared Resources	>	Showing 1 to 1 of 1 entries	0	0 Previous 1 Next
Networking	>		Default: 0 Range: 0-10000000 concurrent connections	Default: 0 (disabled) Range: 0-86400 connections per second
			Interface	
K Server Load Balance	ř		port2 *	
Virtual Server				
Application Resources			Public IP Type	Public IPv4
Application Optimization			IPv4 IPv6	0.0.0
Real Server Pool				Example: 192.0.2.1
			Resources	
Scripting				
SSL-FP Resources			Profile	Persistence
S Link Load Balance	>		LB_PROF_TCP *	Click to select.
Global Load Balance	>		Method	Real Server Pool
-			LB_METHOD_ROUND_ROBIN *	RealServerPool 👻 🗸
Web Application Firewall	>		Sa	Save Cancel
😻 Network Security	>			
O DoS Protection	>			
LUSER Authentication	>			

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.

Search here Q		Server Load Balance Ree	I Server Pool		
root 🗸		Real Server Pool Real	Real Server Pool		
Dashboard	>	T Add Filter	🖋 Edit Member		Create New
FortiView	>	Name	Status Enable Disable Maintain		• •
System	>	0 1	Real Server	Port	1 × 2
Shared Resources	>	RealServerPool	RealServer1 👻	80 Default: 80 Range: 0-65535	1 × C
Networking	>	Showing 1 to 2 of 2 entries	Weight	Recover	Previous 1 Next
K Server Load Balance	ř		1 Default: 1 Range: 1-256	O Default: 0 (disabled) Range: 0-86400	
Virtual Server Application Resources			Warm Up	seconds Warm Rate	
Application Optimization			0	100	
Real Server Pool			Default: 0 (disabiled) Range: 0-86400 seconds	Default: 100 Range: 1-86400 connections per second	-
Scripting			Connection Limit	Connection Rate Limit	
SSL-FP Resources	>		0 Default: 0 (disabled) Range: 0-	O Default: 0 (disabled) Range: 0-86400	
•			1048576 concurrent connections Backup	connections per second	
Global Load Balance				ret	
Web Application Firewall	>		Save	Cancel	
DoS Protection	>				
	, ,				
Log & Report	>				

Search here Q	Server Load Balance R	eal Server Pool		
root 🗸	Real Server Pool Rea	📑 Real Server Pool	×	
Dashboard >	T Add Filter	🖋 Edit Member		Create New
FortiView >	Name	Status Enable Disable Maintain	• 4	5
System >	8 1	Real Server	Port	* × @
Shared Resources	RealServerPool	RealServer2 v	80 Default: 80 Range: 0-65535	r × 4
Networking	Showing 1 to 2 of 2 entries	Weight	Recover	Previous 1 Next
Server Load Balance 👻		2 Default: 1 Range: 1-256	0 Default: 0 (disabled) Range: 0-86400	
Virtual Server Application Resources		Warm Up	seconds Warm Rate	
Application Optimization		0	100	
Real Server Pool		Default: 0 (disabled) Range: 0-86400 seconds	Default: 100 Range: 1-86400 connections per second	
Scripting SSL-FP Resources		Connection Limit	Connection Rate Limit	
Clink Load Balance		Default: 0 (disabled) Range: 0- 1048576 concurrent connections	Defaut: 0 (disabled) Range: 0-86400 connections per second	
Global Load Balance		Backup	Cookie	
Web Application Firewall		(@_0#)	rc3 ×	
Vetwork Security				
O DoS Protection				
LUSER Authentication				
Log & Report				

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

root@ubuntu:~# wget http://l.l.l. 2018-12-31 09:58:47 http://l Connecting to l.l.l.22:80 conn HTTP request sent, awaiting respo Length: 869269504 (829M) [applica Saving to: 'big.iso'	.1.1.22/big.iso ected. nse 200 OK
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.

			Luyer 4	22.1.1.01		CO_INCOI_ICI	LINDIC	
Search here	۹	82	Layer 4	22.1.1.82	80	LB_PROF_TCP	Enable	0
root 🗸		83	📑 Virtual Server		,			
🙀 Dashboard	>	84	Basic Genera	I Monitoring				
FortiView	>	85	Traffic Log			FortiView		
System	>	86		be used mainly for debugging		O OFF		
Shared Resources	>	87	 extensive memory an debugging is complete	d CPU reso <mark>r</mark> ces. Please disabl e.	e traffic logging after			
Networking	>	88	Comments					
Server Load Balance	~	89	Please input comr	ments				
Virtual Server		9						
Application Resources		90						
Application Optimizatio	n	91						- 1
Real Server Pool								
Scripting		92						
SSL-FP Resources		93						
🗞 Link Load Balance	>	94						
Global Load Balance	>	95						
Web Application Firewa	all >	96			Save	Cancel		
Luser Authentication	>	97	Layer 4	22.1.1.97	80	LB_PROF_ICP	Епаріе	
📎 Network Security	>	98	Layer 4	22.1.1.98	80	LB_PROF_TCP	Enable	0
Log & Report	>	99	Layer 4	22.1.1.99	80	LB_PROF_TCP	Enable	0

root 🗸		Local Log	Syslog Server	🚍 Local Log
Dashboard	>	Statu		Log Level Disk Full
FortiView	>	enable		
System	>	Log L		Event
Shared Resources	>	inform		Event Category
Networking	>	Event		Configuration @ Admin @ System User @ Health Check SLB LB GLB Frewall B Enable All
Server Load Balance	>	Event	t Category	Required. Please select at least one category.
🗞 Link Load Balance	>		uration,admin,health_che	
Global Load Balance	>	Traffi disable		Con O Traffic logging should be used mainly for debugging traffic logging will consume extensive memory and CPU resources. Please disable traffic logging after
Web Application Firewall	>		c Category	debugging is complete.
LUSER Authentication	>	sib		Traffic Category SLB GLB Enable All Enable All
💓 Network Security	>	disable		Required. Please select at least one category.
Log & Report	~	Script		Security (D or)
Log Browsing		disable	e	Scrint .
Log Setting Report Email		Debu		Save Cancel
Report Config				
Report				

root 🗸		Event Log	Security Log	Traffic Log	Script Log Aggregat	Log							
Dashboard	>	SLB Layer 4	SLB HTTP	LB TCPS 🔍 SLB F	ADIUS 🔍 GLB 🔍 SLB SIP	SLB RDP SLB DNS	S SLB RTSP	SLB SMTP	LB RTMP SLB DIAMETER	⊖ SLB MySQL			
FortiView	>	Tilter Settir	ig 🕹 Down	load CR	fresh								
System	>	(mar seta	5 2 00m										
Shared Resources	,	Date	Time	Source	Received Bytes	Destination	Sent Bytes	Service	Virtual Server	Duration (s)	Trans Destination	Real Server Name	
Networking	>	2018-12-31	02:02:27	1.1.1.90	1645562	1.1.1.22	894320609	tcp	VS1	8	2.2.2.2	RealServer1	
Server Load Balance	,	Da	ate		2018-12-31				Time	02:02:27			_
Link Load Balance	>		g ID		0100008000 741736				Log Level	information	n		
			essage ID ceived Bytes		1645562				Duration (s) Sent Bytes	8 894320609			
Global Load Balance	>		otocol		6				Service	tcp			
Web Application Firewall	>		urce		1.1.1.90				Source Port	47936			
User Authentication	,	De	estination		1.1.1.22				Destination Port	80			
user Authentication	<i>_</i>	Tr	ans Source		2.2.2.33				Trans Source Port	5022			
Network Security	>	Tr	ans Destination		2222				Trans Destination Port	80			
.og & Report	~	Vi	rtual Server		VS1				Action	none			
		So	urce Country		Australia				Destination Country	Australia			
Log Browsing		ту	pe		traffic				Sub Type	slb_layer4			
Log Setting		Vo	lom		root				Real Server Name	RealServer	1		
Report Email		2018-12-31	02:02:22	🔛 1.1.1.90	120	1.1.1.22	176	tcp	VS1	6	2.2.2.3	RealServer2	
Report Config Report		Showing 1 to 2 of	of 2 entries Show	10 entries								Previous 1) N

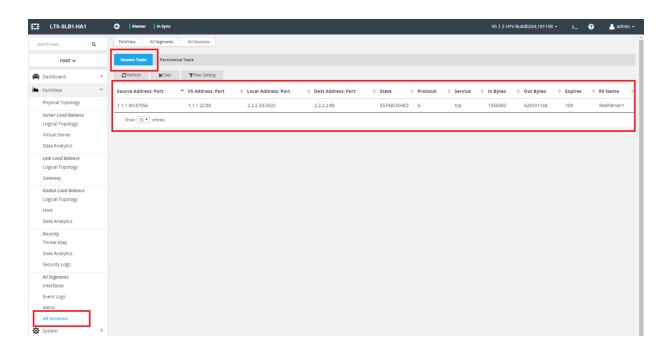
Check if WRR method works as expected from the traffic log:

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

Search here Q		Log & Report	Log Browsing											
root 🗸		Event Log	Security Log	Traffic Log	Script Log									
Dashboard	>	🖲 SLB Layer 4 🛛 🔅	® SLB Layer 4 © SLB HTTP © SLB FLOS © SLB FLP © GLB © SLB SLP © SLB SLP © SLB BLNS © SLB FLTS © SLB SMITP © SLB DIAMETER © SLB MJSQL © LLB											
FortiView	>	▼ Filter Setting ▲ Download ⑦ Refresh 18/08/14/08:46:49 - 19/11/25 04:21:29 *												
System	>	Date	Time	Source	Received Bytes	Destination	Sent Bytes	Service	Virtual Server	Duration (s)	Trans Destination	Real Server Name	0	
Shared Resources	>	2019-11-25	04:31:39	21 1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2		
Networking	>	2019-11-25	04:29:14	1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2		
🛠 Server Load Balance	>	2019-11-25	04:29:14	21 1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.2	RealServer1		
🗞 Link Load Balance	>	2019-11-25	04:29:13	21 1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2	Ð	
Global Load Balance	>	2019-11-25	04:29:11	21 1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2	ľ	
Web Application Firewall	>	2019-11-25	04:29:11	21 1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.2	RealServer1	Ē	
Network Security	>	2019-11-25	04:29:11	1.1.1.90	332	31 1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2	Ð	
DoS Protection	>	2019-11-25	04:29:10	21 1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2	Ð	
User Authentication	>	2019-11-25	04:29:10	21 1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.2	RealServer1		
🔲 Log & Report	~	2019-11-25	04:29:09	21 1.1.1.90	332	1.1.1.22	423	tcp	VS1	3	2.2.2.3	RealServer2		
Log Browsing		Show 10 *	entries								Previ	ous 1 2 3 4 5	Next	
Report Email														
·····														

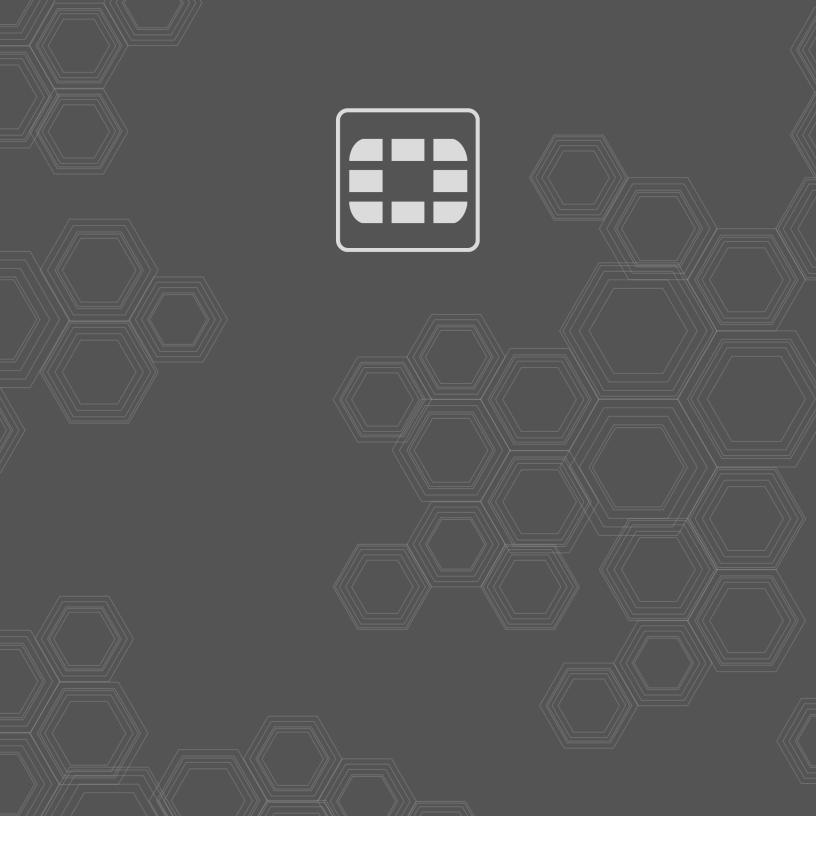
• Check the session table:

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





Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGare® 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.