High Performance VPN Load balancing with FortiADC and FortiGate

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

March 19, 2020
FortiADC 5.4.0 High Performance VPN Load-Balancing with FortiADC and FortiGate
01-540-600000-20200319

TABLE OF CONTENTS

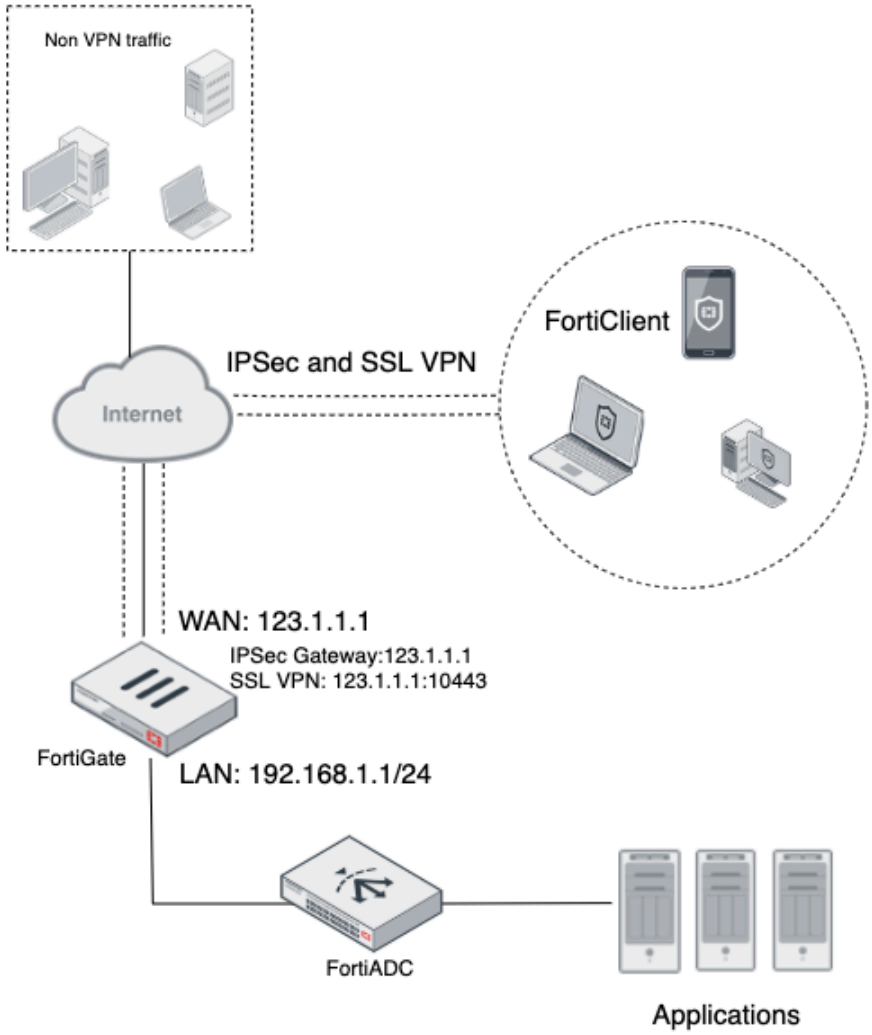
Change Log

Date	Change Description
2020-03-19	Initial release.

Introduction

This guide details the solutions to scale up FortiGate VPN capacity. In this guide, we will provide an overview on FortiGate VPN Load-Balancing with FortiADC.

Original Topology: Customer origin topology without VPN LB



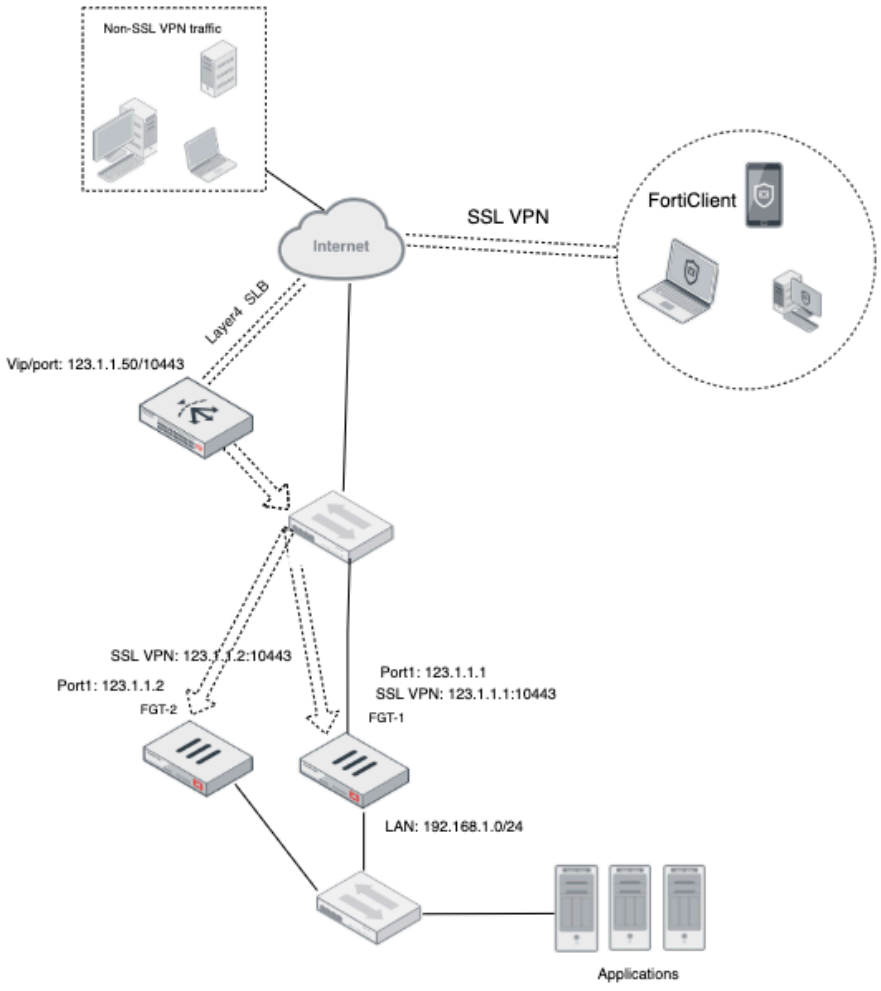
Solution with FortiADC

FortiADC provides three solutions to scale up the VPN capacity with FortiGates.

1. Layer-4 SLB One-Arm Deployment for SSL VPN Load-Balancing
2. Layer-4 SLB In-Line Deployment for both IPsec and SSL VPN Load-Balancing
3. FortiGSLB for both IPsec and SSL VPN Load-Balancing

Solution 1: Layer4 SLB One-Arm Deployment for SSL VPN Load-Balancing

Topology 1: FortiADC into network without any changes on FortiGate



Key configurations:

a. Assign another public IP for FortiADC interface address.

b. Configure **NAT-Source-Pool**

c. Configure Layer4 SLB and publish the VIP and its listening port as the SSL VPN site for all FortiClient users (Example: https://123.1.1.50:10443). Need to configure **Full-NAT** in VS configuration profile.

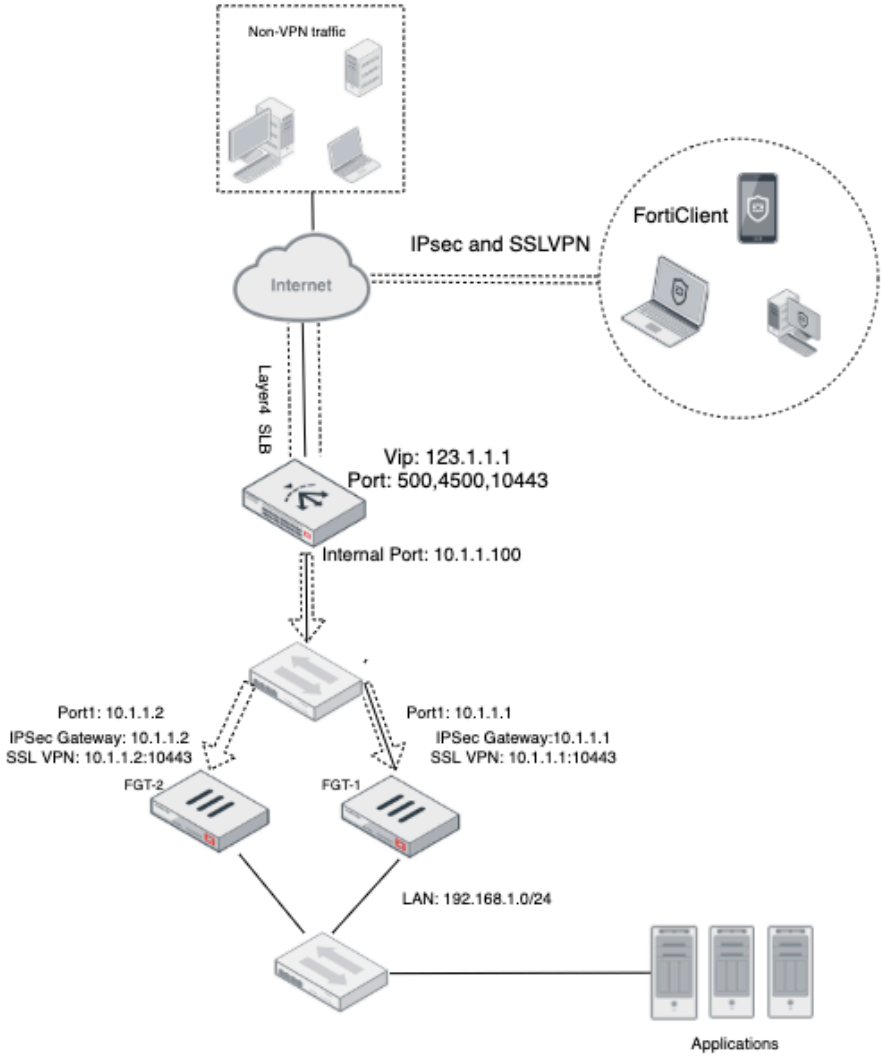
d. FortiADC is able to load balance the SSL VPN traffic across FortiGate pool. None-SSL VPN traffic will be routed to the original FortiGates.

Notes:

- In case you already have FortiADC, you can use VDOMs.
    - One VDOM for SSL/IPsec LB
    - One VDOM for Application LB
- Only supports SSL VPN
- The source IP address cannot be recorded on FortiGate due to FortiADC's Full-NAT settings.

Solution 2: Layer4 SLB In-Line Deployment for both IPsec and SSL VPN Load-Balancing

Topology 2: FortiADC in front of FortiGates and take over original FortiGate WAN settings.



Key configurations:

1. Move the WAN IP to FortiADC, and change the original FortiGate WAN IP to the internal IP address
2. Configure Layer4 SLB and publish the VIPs and its listening ports for FortiClient users
   a. Create separate virtual servers for IPsec VPN and SSL VPN
   b. You must use DNAT method in SLB VS configuration profile.
   c. Other settings:
      a. **IPsec VPN load-balancing**: specify the ports 500, 4500, and select **UDP profile** and SRV_ADDR **persistence**.
      b. **SSL VPN load-balancing**: specify the one configured on FortiGate (example: 10443). Select **TCP profile** and SRC_ADDR **persistence**.
3. Configure route policy on FortiADC, and add 1-to-1 NAT according to the FortiGate settings to take over the FortiGate network functions if needed.
4. FortiADC is able to load balance both IPsec and SSL VPN traffic across FortiGate pool. None VPN traffic will be routed to the original FortiGate.

Note:

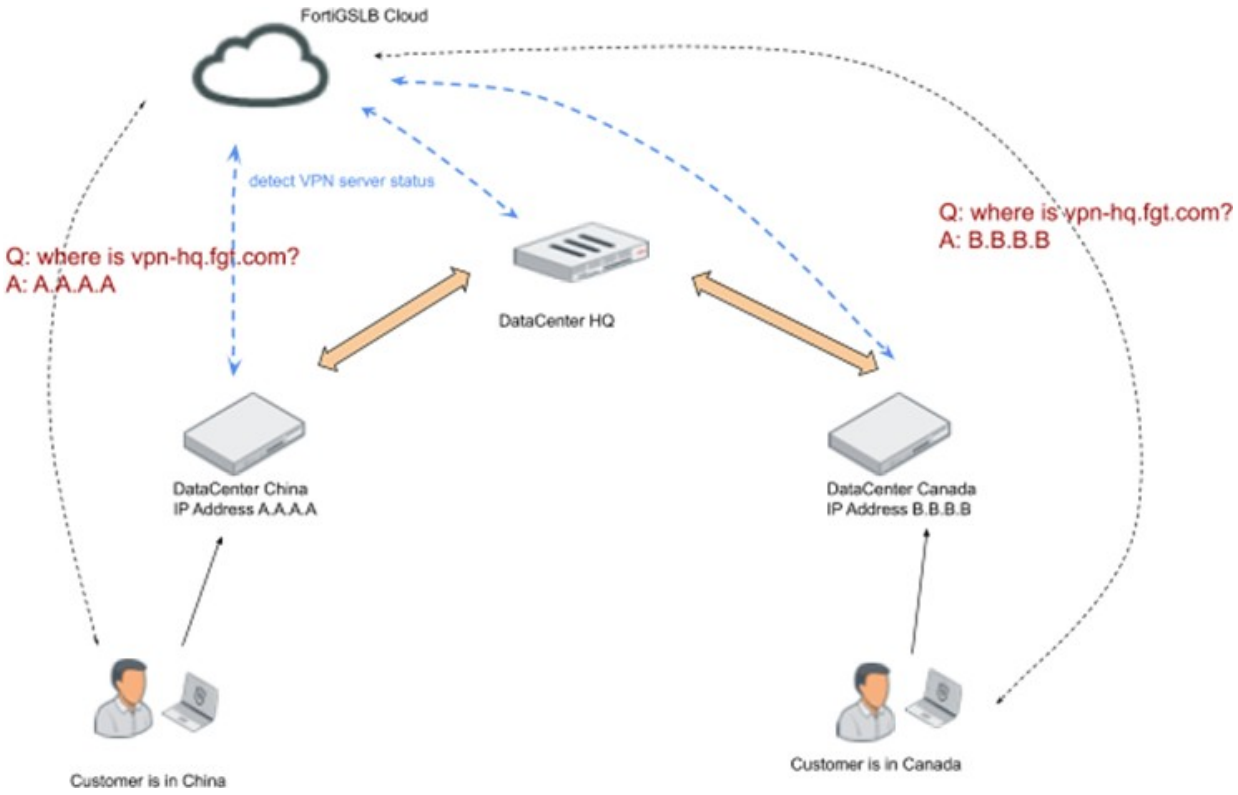
- In case you already have FortiADC, you can use VDOMs.
  - One VDOM for SSL/IPsec LB
  - One VDOM for Application LB
- Must change FortiGate network settings and move the original WAN to internal subnet.

Solution 3: FortiGSLB for both IPSec and SSL VPN Load-Balancing

This is a solution for SSL-VPN with FortiGSLB Cloud. It is also supported with FortiADC (GSLB module).

For remote clients who want to connect to the company HQ via VPN, FortiGSLB allows clients to automatically connect to the FortiGate VPN server that is geographically closest to their current location. This can also be specified according to FortiGate VPN server availability. In cases when the VPN server is down, FortiGSLB can redirect users to the next available FortiGate VPN server in another location.

Topology 3: GSLB Service for SSL/IPSec VPN Load Balancing



Key configurations:

a. **Create new VPN** in FortiGate (VPN) or use the existing VPN.
b. **Create FQDN** in FQDN services > **choose DNS-Query-Origin Virtual Server Pool Selection Method**.
c. Create FQDN member > Create new Virtual Server Pool.
d. **Create pool member > Create generic server > Create new data center > Create new Server member** (add FortiGate VPN server IP).
e. **Create new Location List** for Virtual ServerPool
f. Perform steps c.-e. for another Virtual Server Pool with different location.

Note:

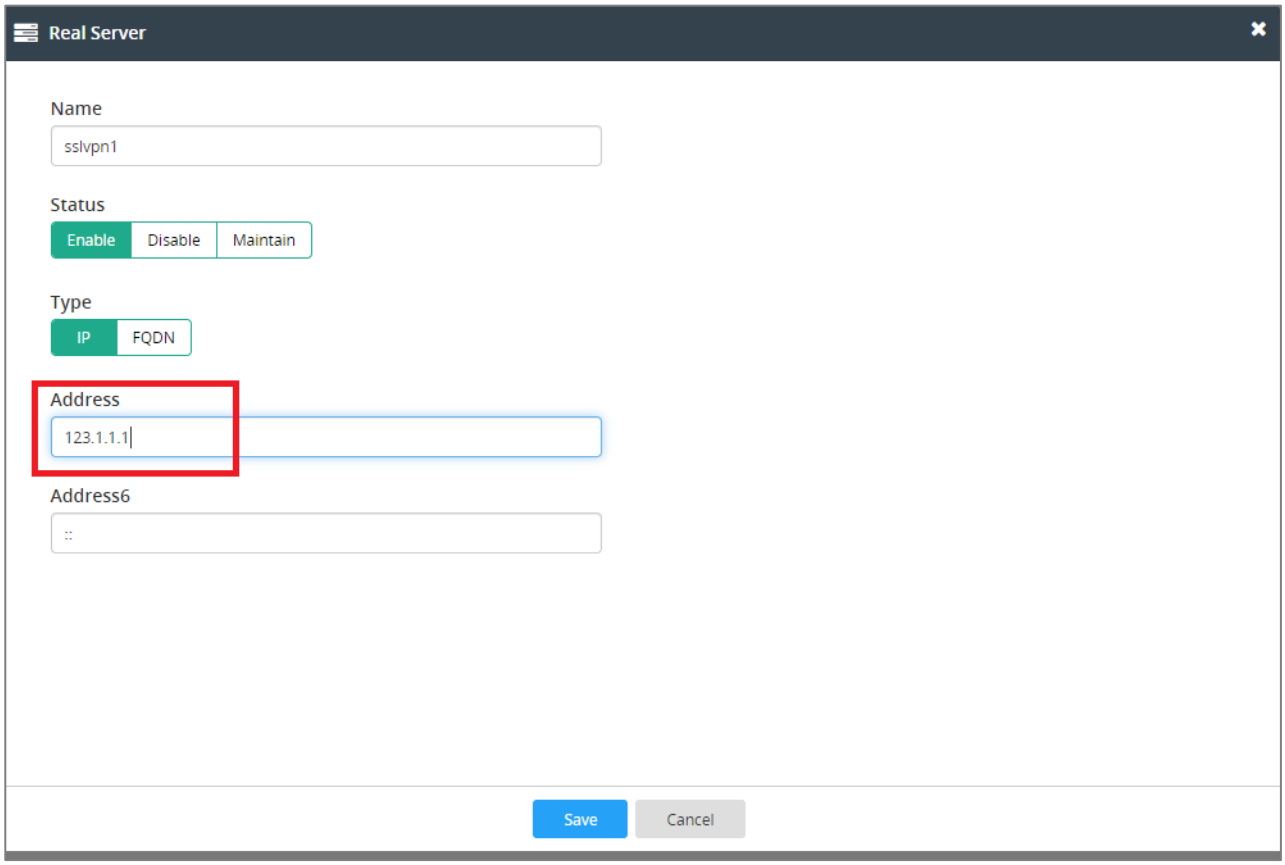
The virtual servers from the generic servers (FortiGate) will be added into Pool and Server directly and will work in FQDN services.

Appendix A: GUI Reference

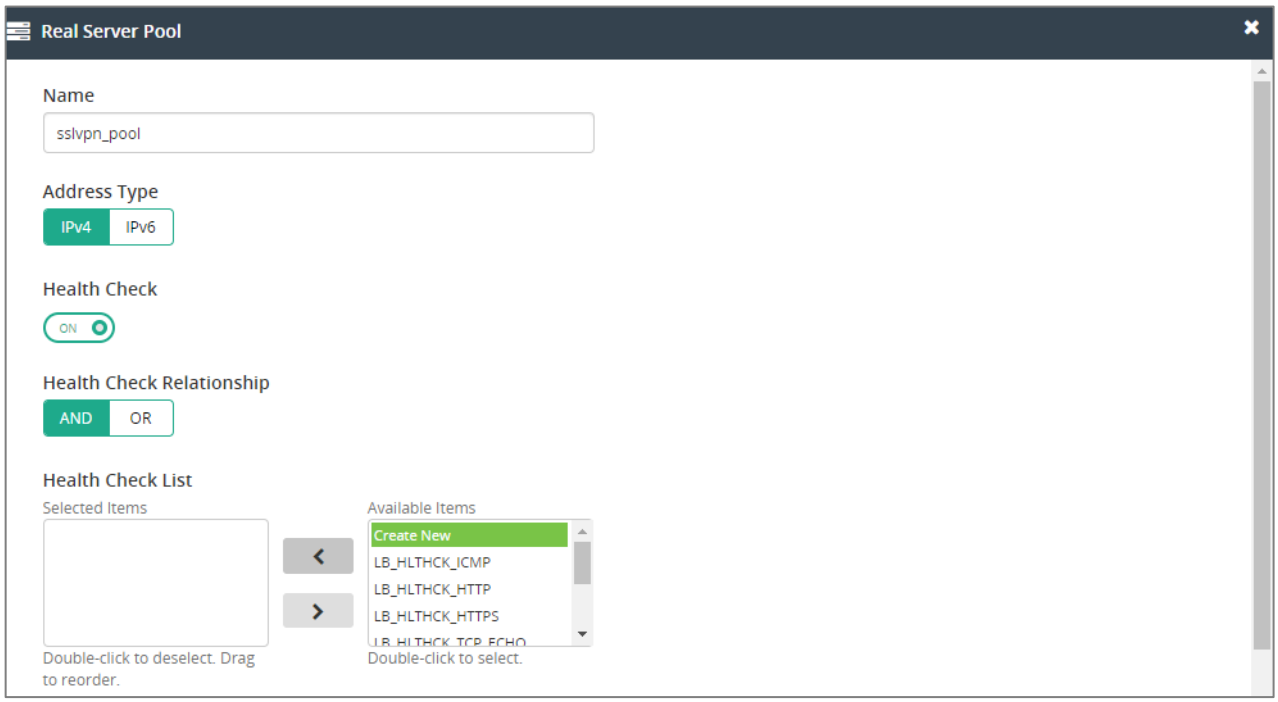
Solution 1: Example Configuration

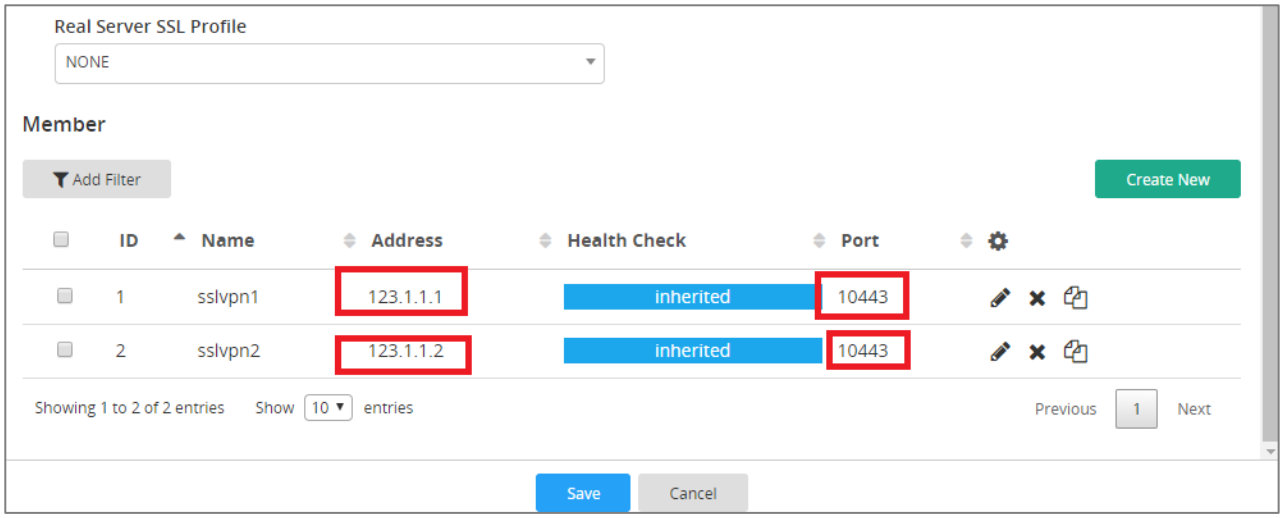
Steps

1. Configure basic networking settings like interface IP (example: 123.1.1.50) and routing.
2. To deploy the Layer4 SLB, first create new real severs, with the address as the IP of the listening FortiGate interface.

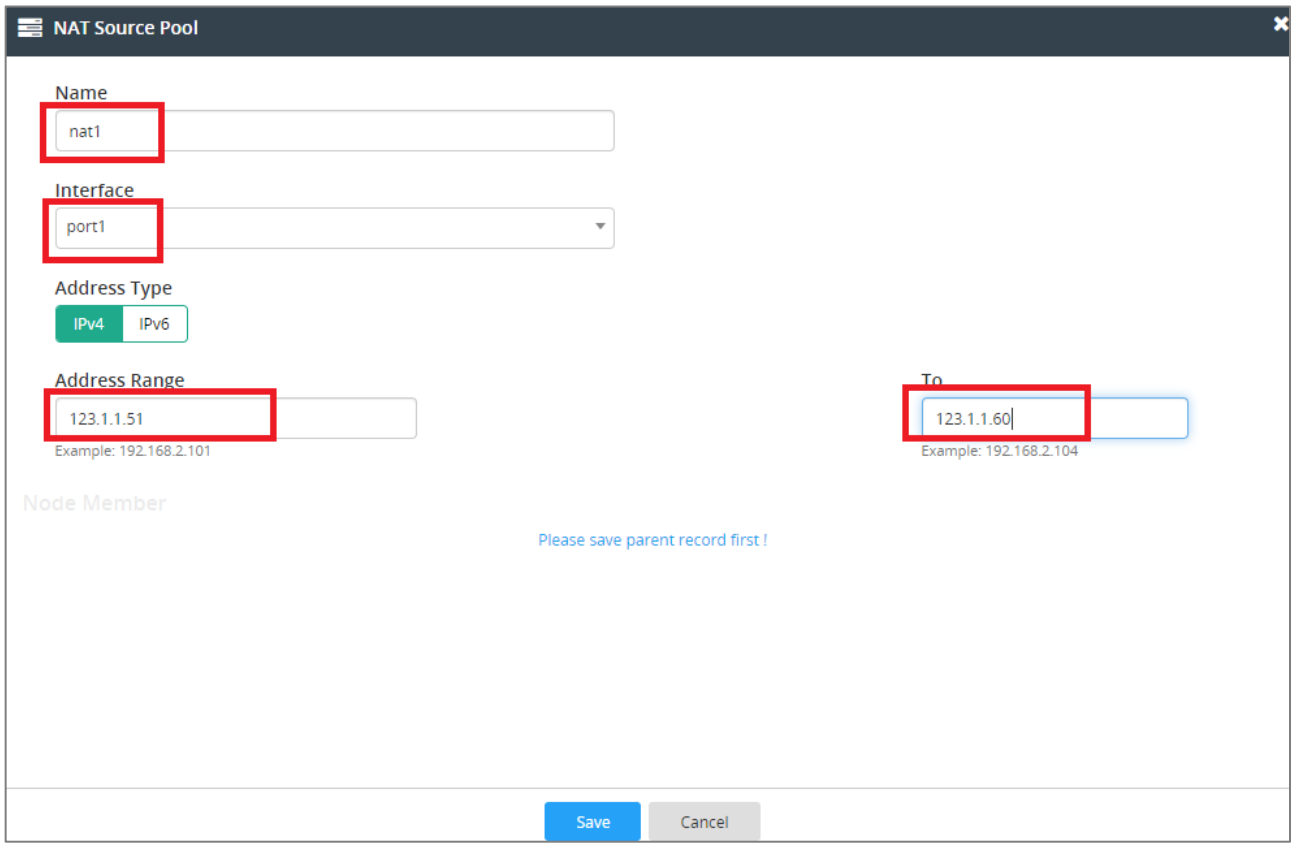


3. Create a new Real Server Pool and add real servers into it.

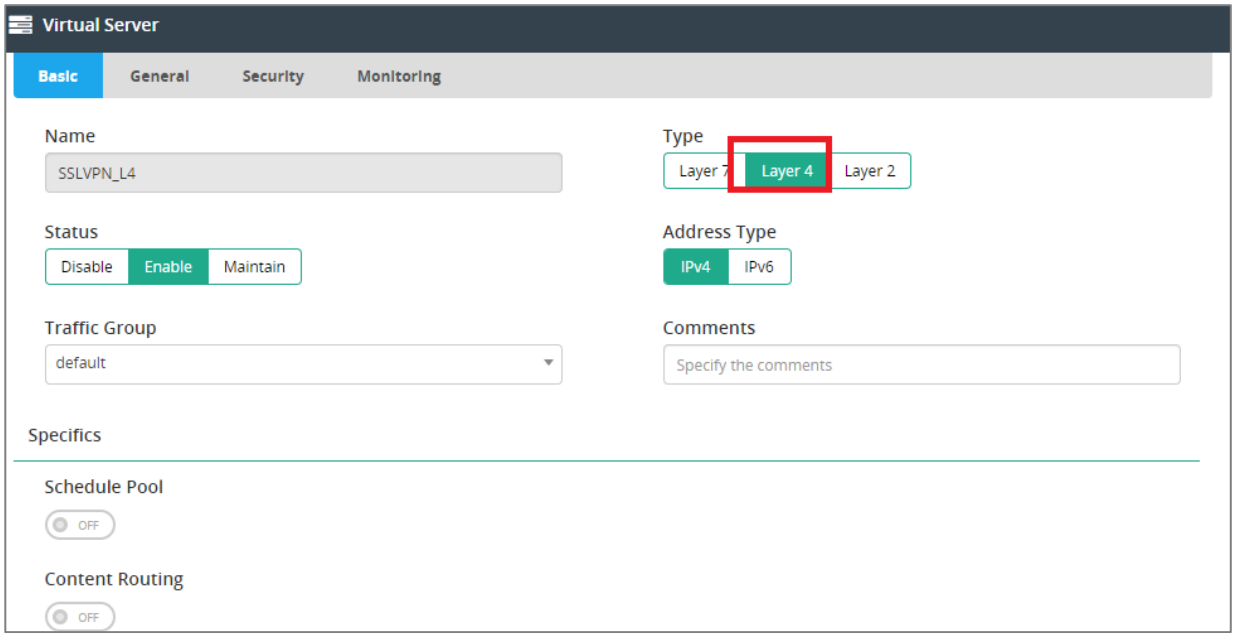


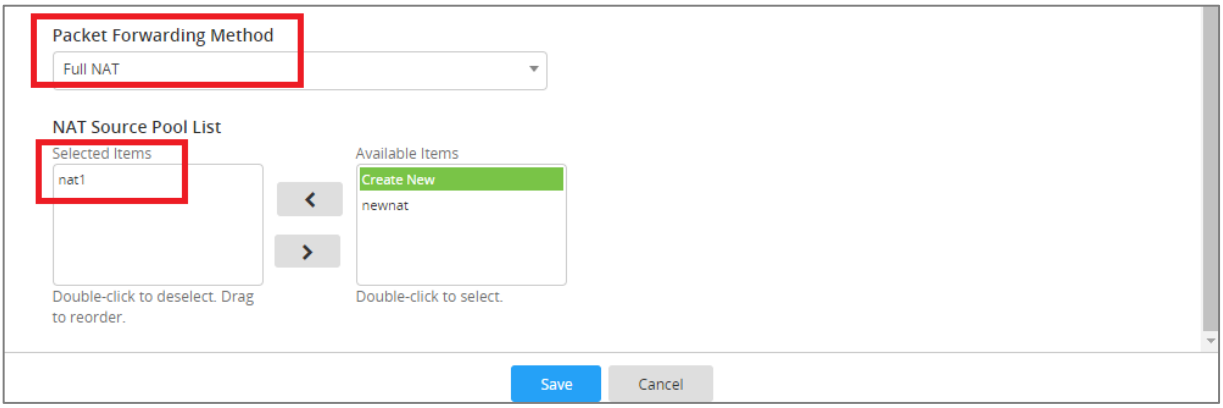


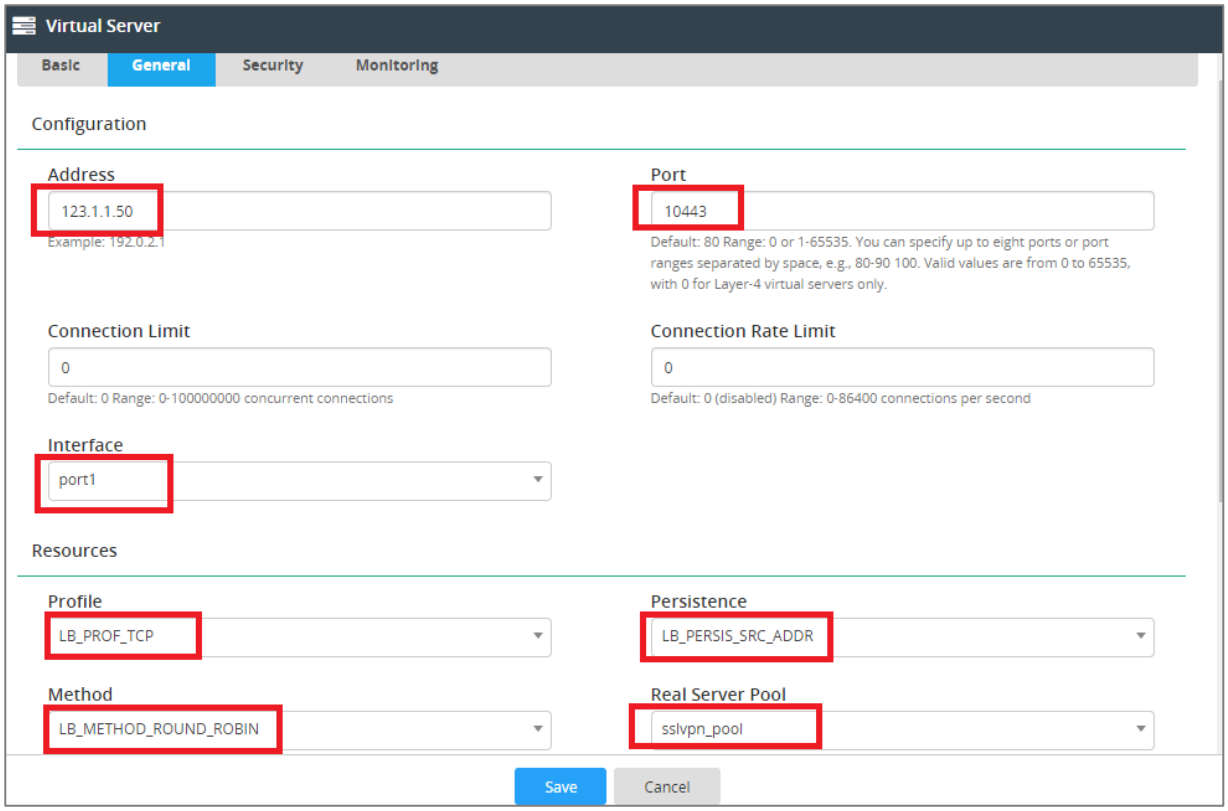
4. Create a NAT source Pool in **Server Load Balance > Virtual Server > NAT Source Pool**.



5. Finish the Basic and General configurations for the Virtual Server settings, including:
   a. Select Layer 4 type.
   b. Select Full NAT Packet FORWARDING Method and specify the net source pool.
   c. Specify address, port, and interface in general configuration.
   d. Select TCP Profile and ROUND_ROBIN method and make sure to specify the persistence method (e.g. SRC_ADDR, HASH_SRC_ADDR), then select the configured real serverpool.


Virtual Server
Basic
General
Security
Monitoring
Name
SSLVPN_L4
Type
Layer 7
Layer 4
Layer 2
Status
Disable
Enable
Maintain
Address Type
IPv4
IPv6
Traffic Group
default
Comments
Specify the comments
Specifics
Schedule Pool
OFF
Content Routing
OFF


Packet Forwarding Method
Full NAT
NAT Source Pool List
Selected Items
nat1
Available Items
Create New
newnat
Double-click to deselect. Drag to reorder.
Double-click to select.
Save
Cancel



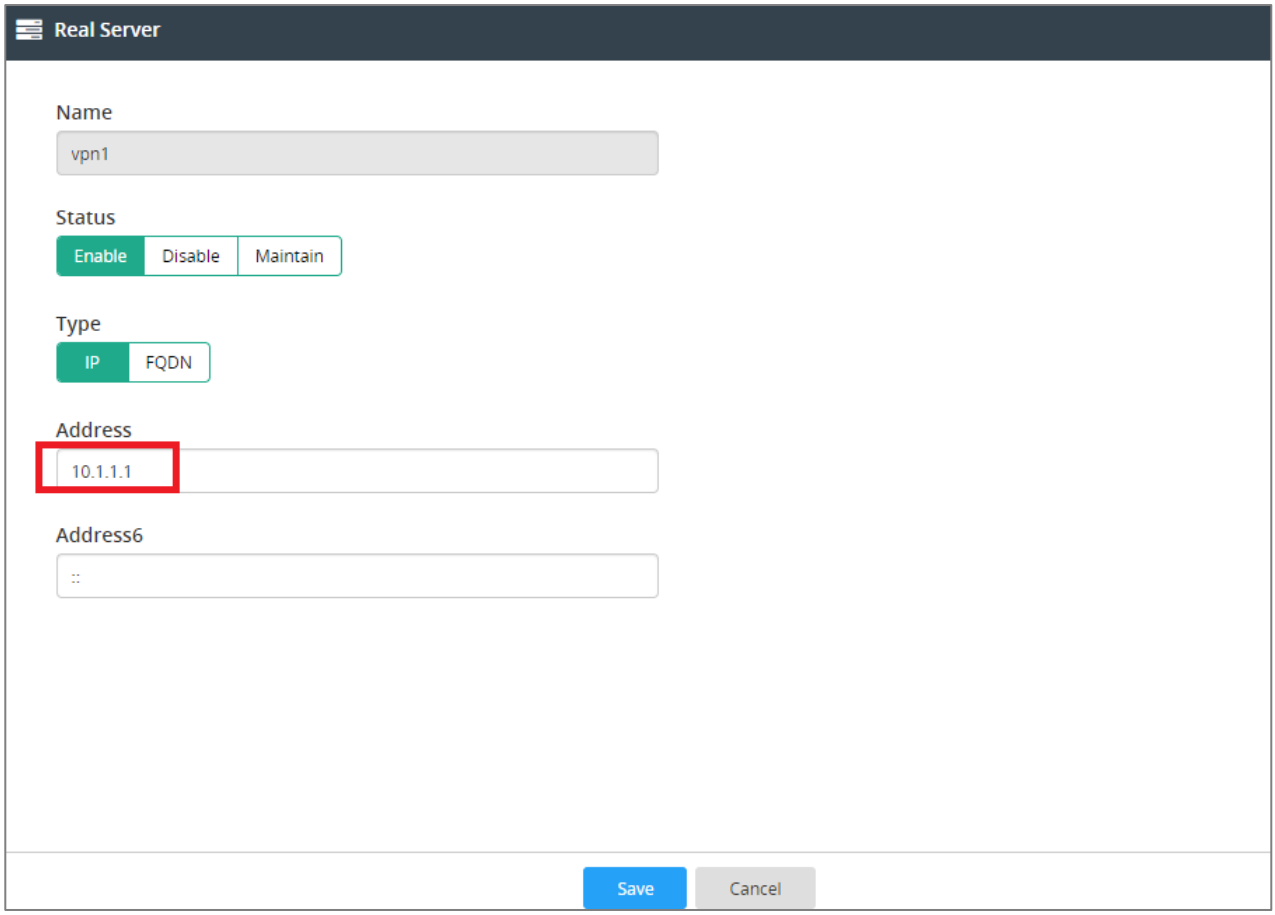
6. To view the result, do the following:
   a. Open the FortiClient Console and go to **Remote Access**.
   b. Make sure **Auto-connect** is enable on FortiGate
   c. Add a new connection.
      i. Set VPN Type to SSL VPN.
      ii. Set Remote Gateway to the IP of the FortiADC VIP (example: 123.1.1.50).
   d. Select Customize Port and set it (example: 10443).
   e. Save your settings.
   f. Use the credentials you've set up to connect to the SSL VPN tunnel.

Solution 2: Example Configuration

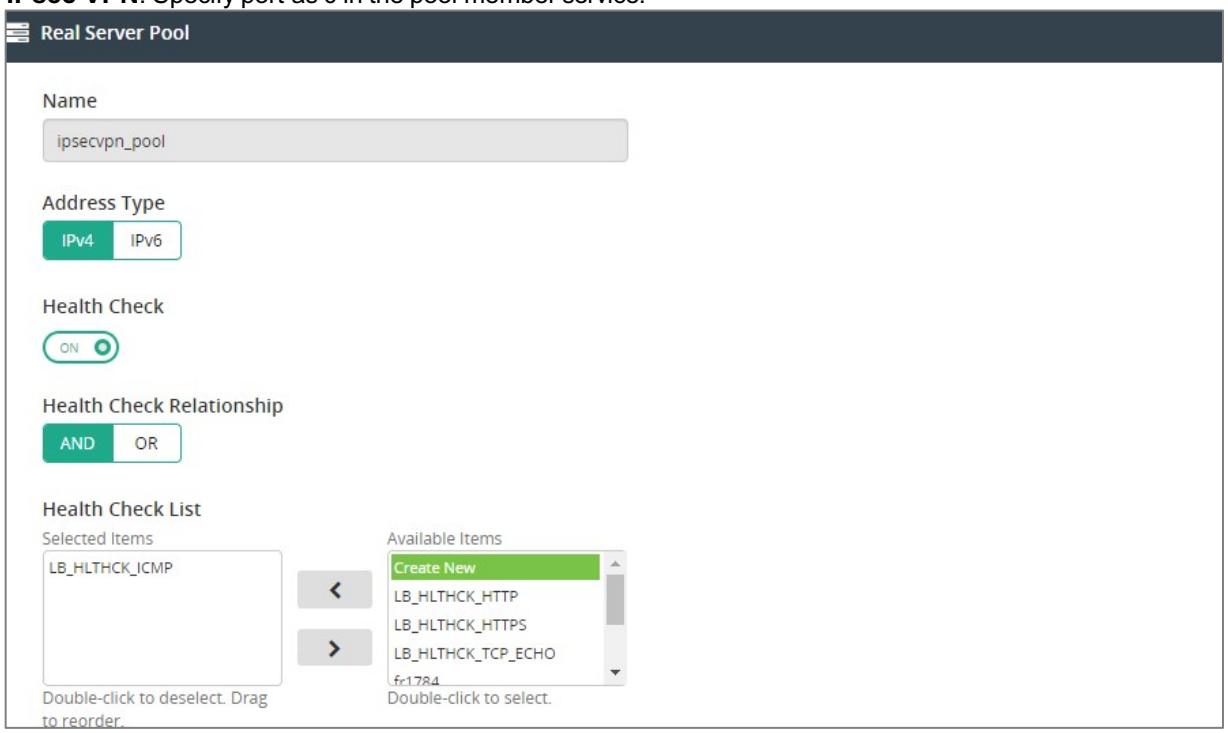
Steps

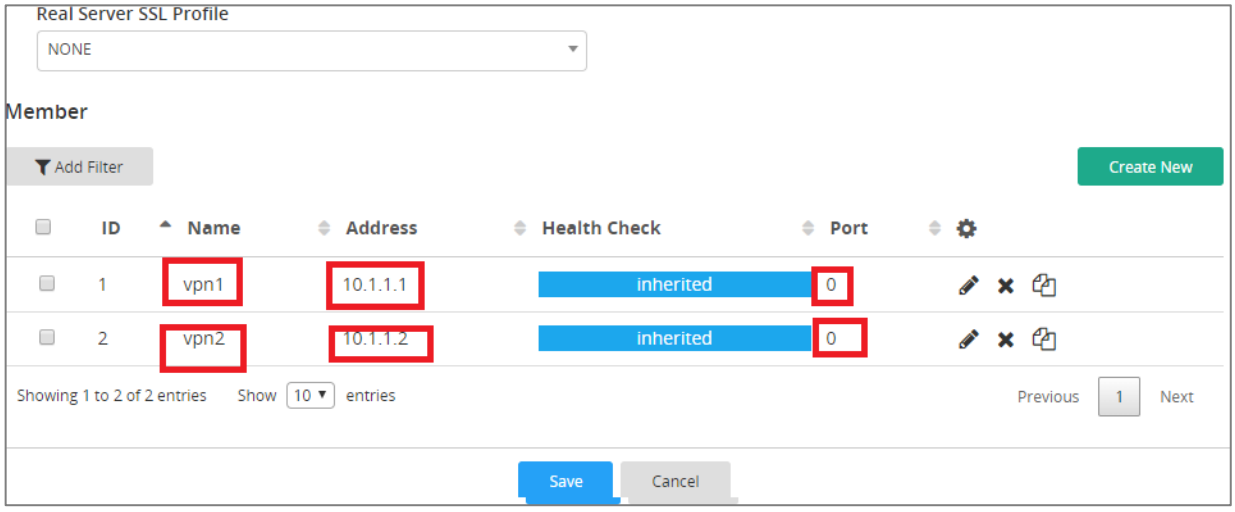
1. Change the network settings to match the topology in the in-line example, including:
   a. FortiGate network settings modification and related configurations that might also need to be modified.
   b. Set the gateway to ADC for the outbound traffic.
   c. Configure basic networking settings like WAN interface IP (example: 123.1.1.1), LAN interface IP and route to take over the original FortiGate WAN related function.

2. To deploy the Layer 4 SLB, first create new real severs, with the address as the IP of the listening FortiGate interface.

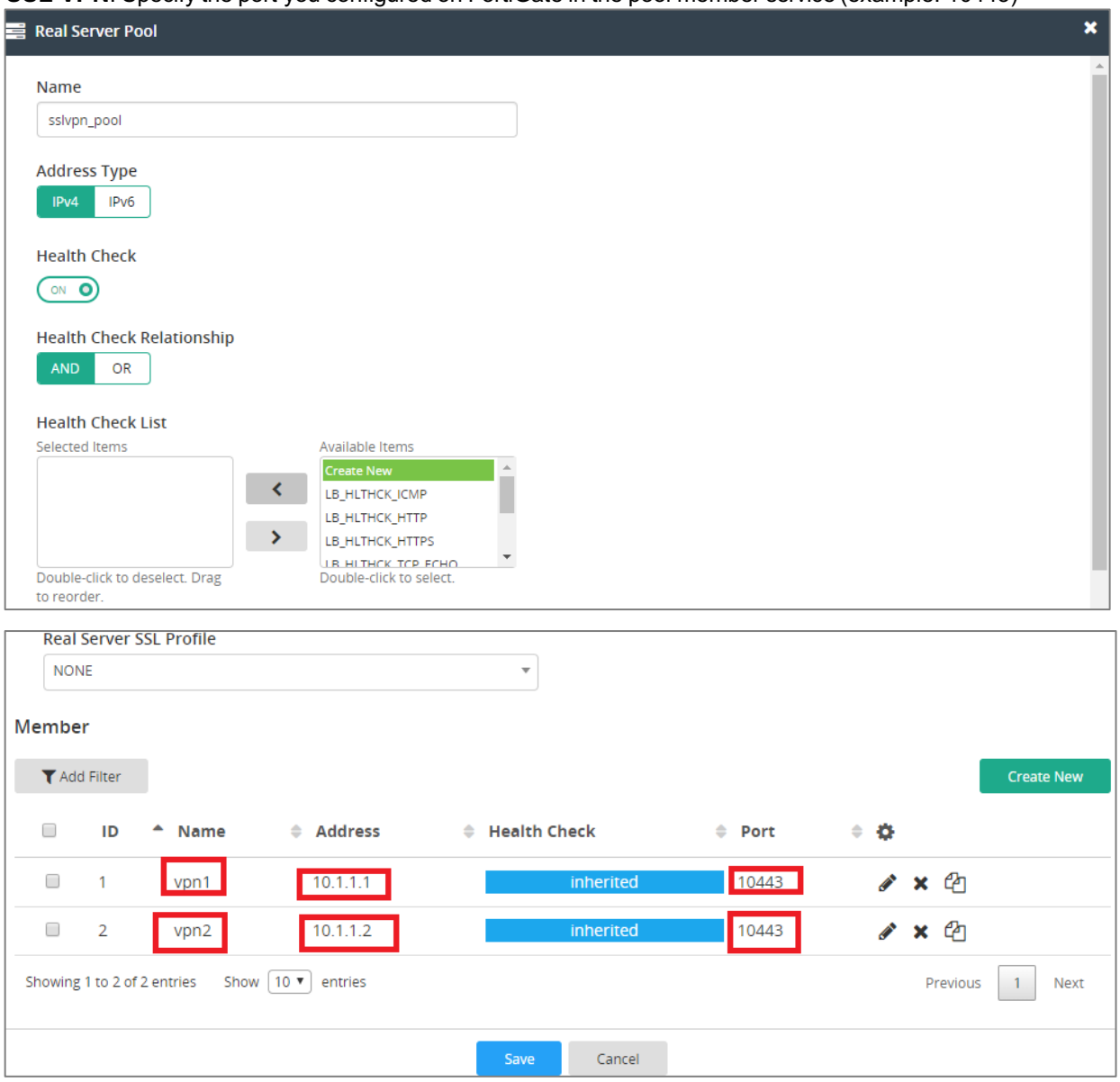


3. Create separate Real Server Pools for IPsec and SSL VPN balancing and then add real servers into them.
   a. **IPsec VPN**: Specify port as 0 in the pool member service.





b. **SSL VPN**: Specify the port you configured on FortiGate in the pool member service (example: 10443)



4. Finish the Basic and General configurations

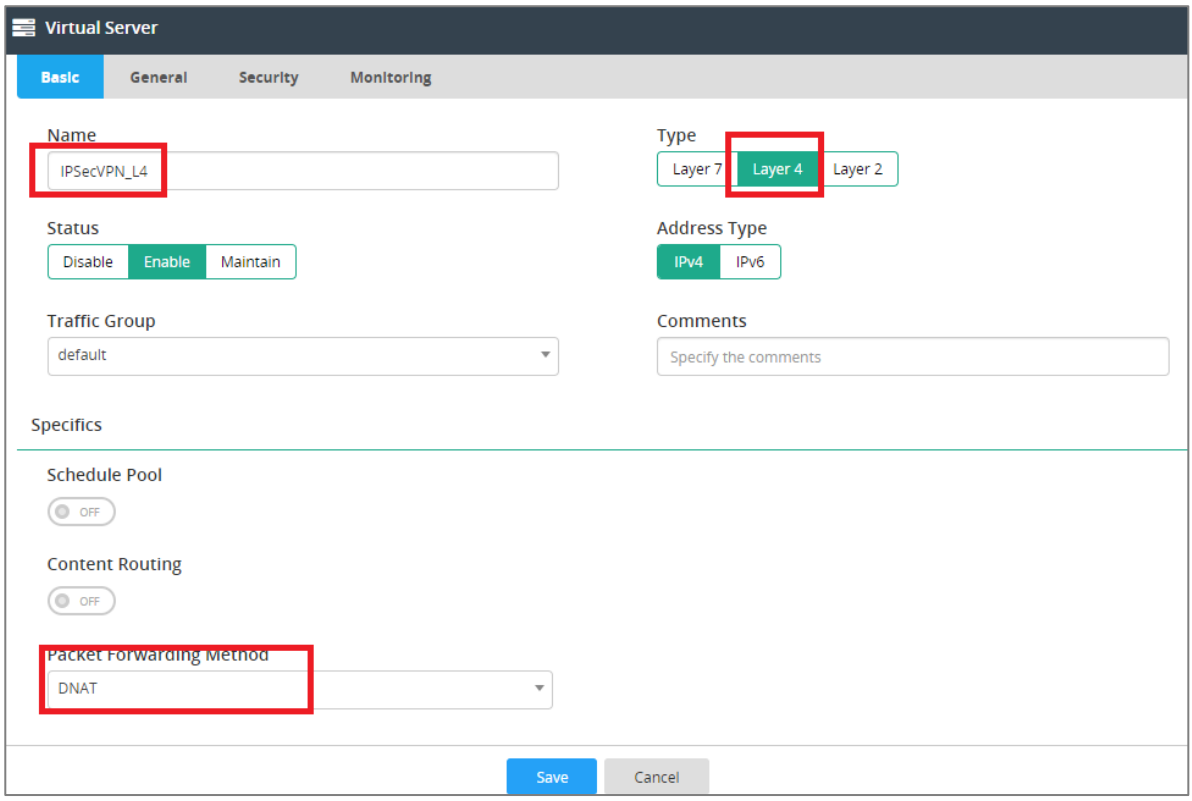
a. IPsec VPN Virtual Serversettings:

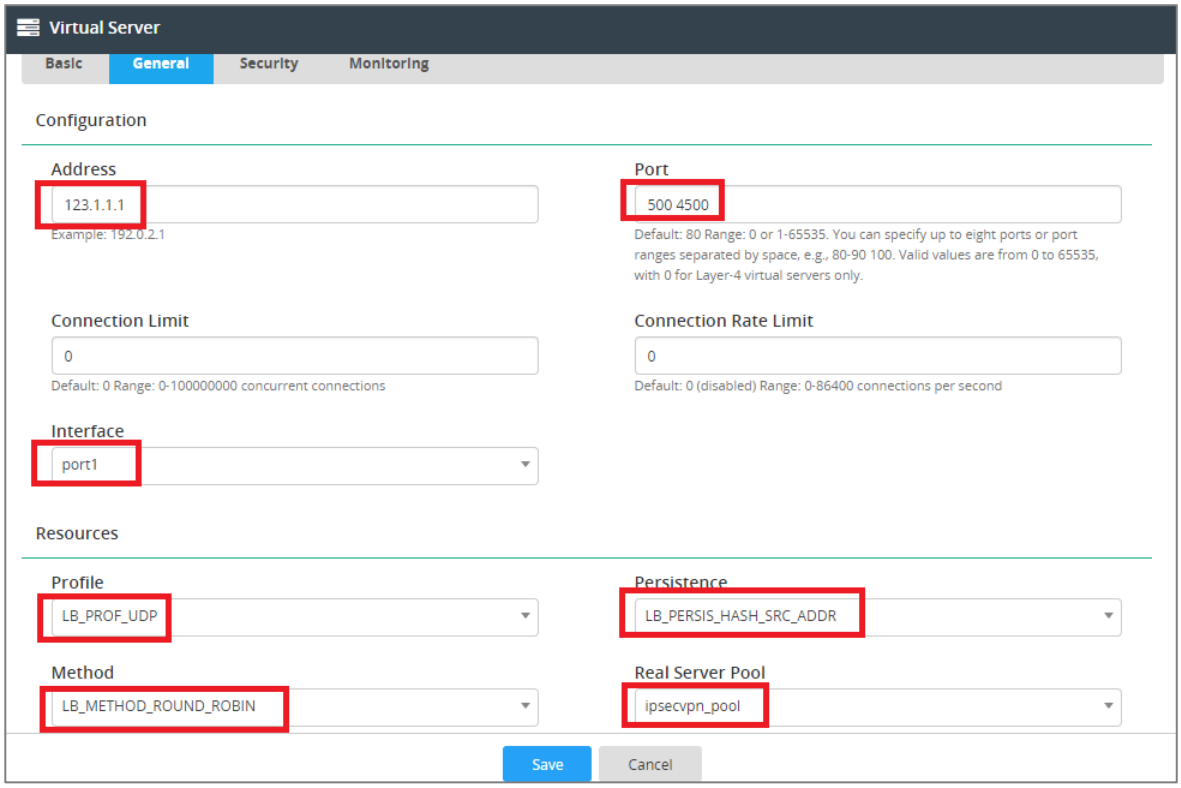
i. Select Layer 4 type.

ii. Use the default DNAT Packet FOWARDING Method.

iii. Specify address, port (500, 4500), and interface in general configuration.

iv. Select UDP Profile and ROUND_ROBIN method and make sure to specify the persistence method (e.g. SRC_ADDR, HASH_SRC_ADDR), then select the configured real serverpool.





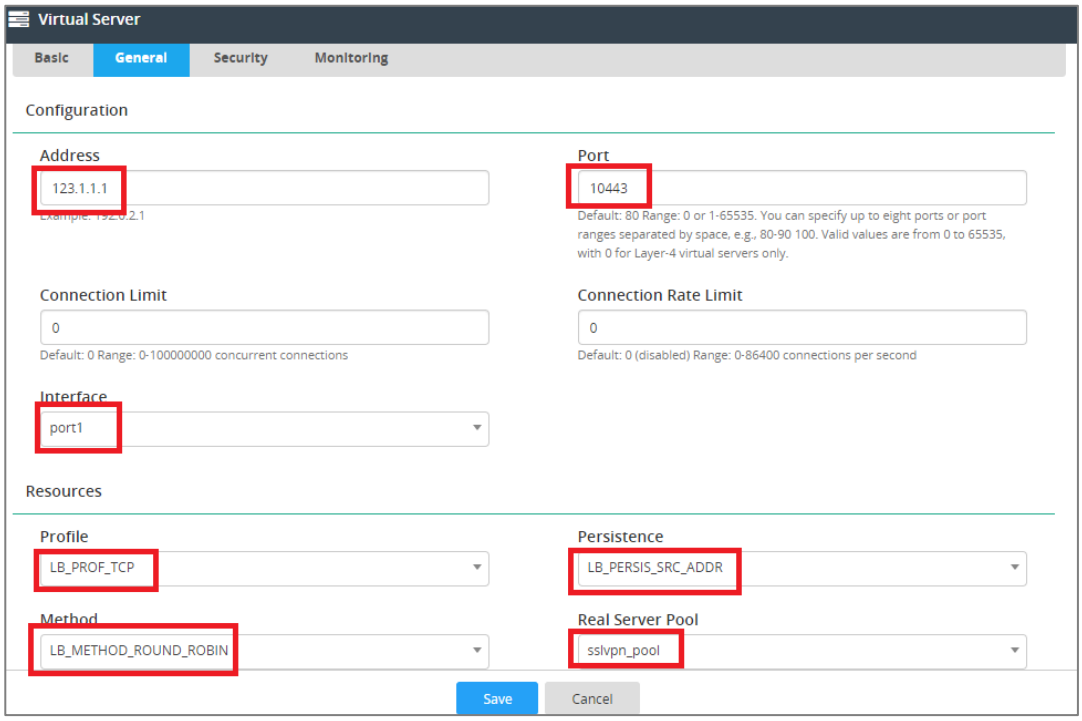
b. SSL VPN Virtual Server settings:

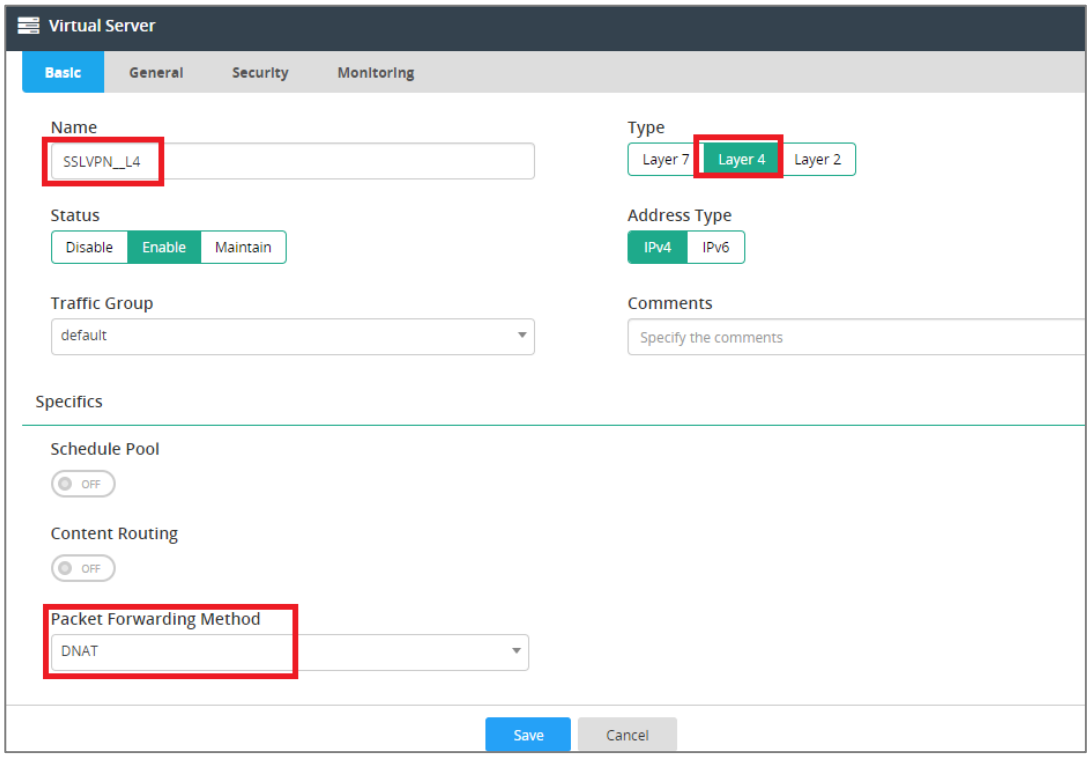
i. Select Layer 4 type.

ii. Use the default DNAT Packet FOWARDING Method.

iii. Specify address, port, and interface in general configuration.

iv. Select TCP Profile and ROUND_ROBIN method and make sure to specify the persistence method (e.g. SRC_ADDR, HASH_SRC_ADDR), then select the configured real server pool.

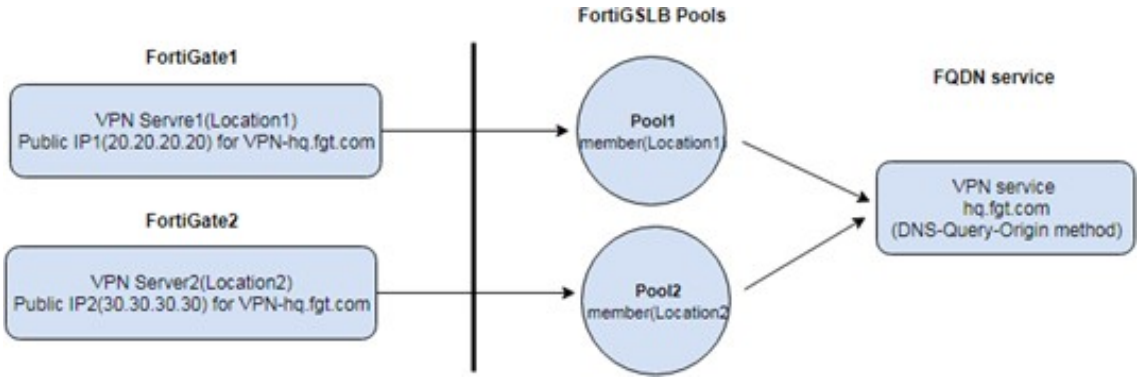




5. To view the result, do the following:
   a. Open the FortiClient Console and go to **Remote Access**.
   b. Make sure **Auto-connect** is enable on FortiGate
   c. Add a new connection.
      i. Set VPN Type to SSL VPN.
      ii. Set Remote Gateway to the IP of the FortiADC VIP (example: 123.1.1.1).
   d. Select Customize Port and set it for the SSL VPN users (example: 10443).
   e. Save your settings.
   f. Use the credentials you've set up to connect to the VPN tunnel.

Solution 3: Example Configuration

This example illustrates the solution for when all the client's incoming traffic comes from one location.



This example assumes the following:

- You need FortiGate VPN in two locations or different A record for each FortiGate
- Every FortiGate VPN server supports a VPN service that can connect to the company HQ.

The FortiGSLB has one pool with these two FortiGate VPN servers and it can load balance the incoming traffic geographically and monitor all VPN servers' status at any time.

If the traffic comes from one location, the FortiGSLB can load balance the traffic to the nearest available server and redirect it to another VPN server once that VPN server becomes unavailable. Clients from all places can enjoy the best performance of VPN server and fast connection to company HQ even while travelling.

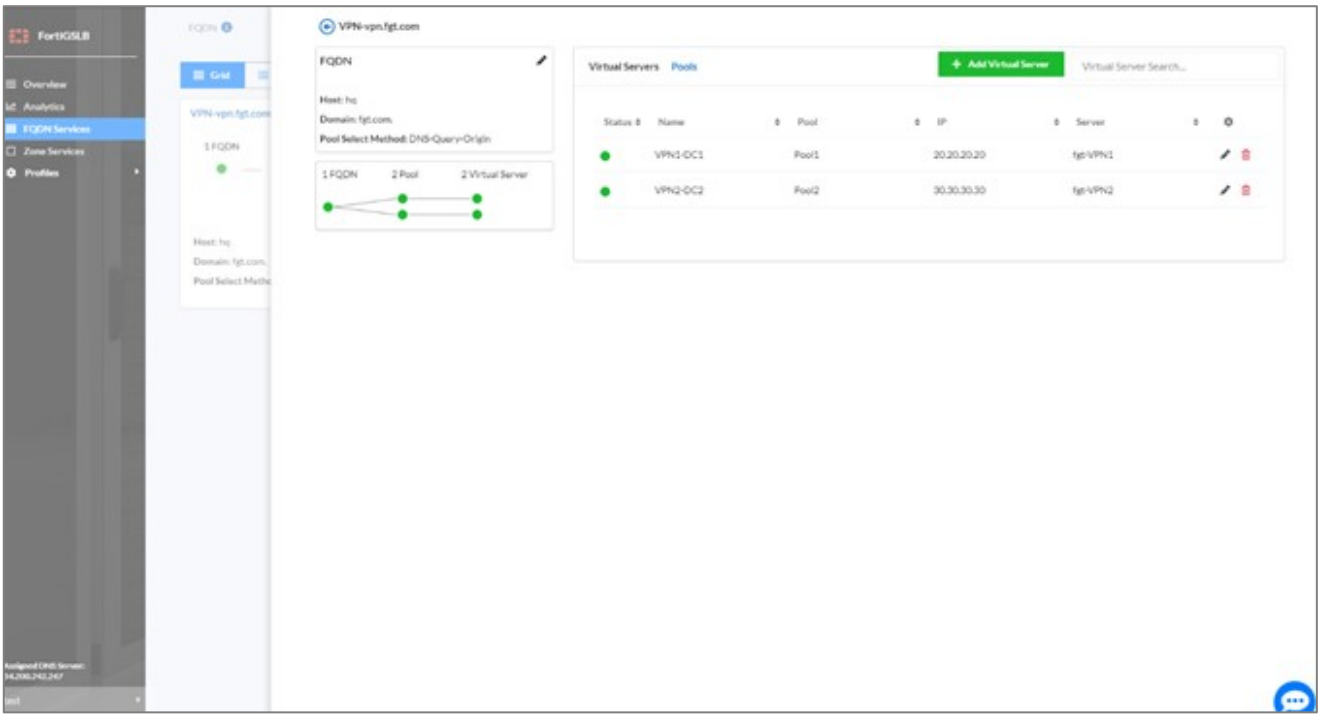
Steps

1. **Create New VPN** in FortiGate (VPN) or use the existing VPN.
2. **Create FQDN** VPN-hq.fgt.com in FQDN services > **choose DNS-Query-Origin Virtual Server Pool Selection Method**
3. Create FQDN member > Create new Virtual Server Pool1
4. **Create pool member** > **Create new generic server** fgt-VPN1 > **Create new Data Center** DC1 > **Create new Server member** VPN1-DC1. **Add FortiGate** VPN IP VPN1-DC1 Public IP and **enable health check** Default_ HLTHCK_ICMP or othertypes.
5. **Create new Location** List1 forVirtual Server Pool1
6. Create FQDN member > Create new Virtual Server Pool2
7. **Create pool member** > **Create new generic server** fgt-VPN2 > **Create new Data Center** DC2 > **Create new Server member** VPN2-DC2. **Add FortiGate VPN IP** VPN2-DC2 Public IP and **enable health check** Default_ HLTHCK_ICMP or othertypes.
8. **Create new Location** List2 forVirtual Server Pool2

Note: The virtual server from the generic servers (FortiGate) will be added into Pool and Server directly and will work in FQDN services.

Sample topology view at FortiGSLB

We have added each FortiGate VPN server into the FortiGSLB pool. GSLB will load balance client traffic geographically using pool locations.



After completing these steps, the customer can monitor the VPN service status from both Location1 and Location2 on the FQDN service detail page. The FortiGSLB will load balance the traffic to the server that have the nearest location. If the nearest location VPN server is down, the FortiGSLB will direct the traffic to other available location. If both VPN service servers are not available, the FortiGSLB will direct traffic to the default VPN server.

Appendix B: CLI Reference

Solution 1: Example Configuration

Steps

1. Configure basic networking settings like interface IP (example: 123.1.1.50) and routing.
2. To deploy the Layer4 SLB, first create new real servers with the address as the IP of the listening FortiGate interface.

```
config load-balance real-server edit "sslvpn1"
set ip 123.1.1.1
next
edit "sslvpn2"
set ip 123.1.1.2
next
end
```

3. Create a new Real Server Pool and add real servers into it.

```
config load-balance pool
edit "sslvpn_pool"
set health-check-ctrl enable
set health-check-list LB_HLTHCK_ICMP
set real-server-ssl-profile NONE
config pool_member
edit 1
set pool_member_service_port 10443
set pool_member_cookie rs1
set real-server sslvpn1
next
edit 2
set pool_member_service_port 10443
set pool_member_cookie rs1
set real-server sslvpn2
next
end
```

4. Create a NAT source Pool in **Server Load Balance > Virtual Server > NAT Source Pool**.

```
config load-balance ippool
edit "nat1"
set interface port1
set ip-min 123.1.1.51
set ip-max 123.1.1.60
next
end
```

5. Finish the Basic and General configurations for the Virtual Server settings, including:
   a. Select Layer 4 type.
   b. Select Full NAT Packet FORWARDING Method and specify the net source pool.
   c. Specify address, port, and interface in general configuration

d. Select TCP Profile and ROUND_ROBIN method and make sure to specify the persistence method (e.g. SRC_ADDR, HASH_SRC_ADDR), then select the configured real serverpool.

```
config load-balance virtual-server
edit "SSLVPN_L4"
set packet-forwarding-method FullNAT
set interface port1
set ip 123.1.1.50
set port 10443
set load-balance-profile LB_PROF_TCP
set load-balance-persistence LB_PERSIS_SRC_ADDR
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool sslvpn_pool
set ippool-list nat1 next
end
```

Solution 2: Example Configuration

Steps

1. Change the network settings to match the topology in the in-line example, including:
   a. FortiGate network settings modification and related configurations that might also need to be modified.
   b. Set the gateway to FortiADC for the outbound traffic.
   c. Configure basic networking settings like WAN interface IP (example: 123.1.1.1), LAN interface IP and route to take over the original FortiGate WAN related function.
2. To deploy the Layer 4 SLB, first create new real severs with the address as the IP of the listening FortiGate interface.

```
config load-balance real-server edit "vpn1"
set ip 10.1.1.1
next
edit “vpn2"
set ip 10.1.1.2
next
end
```

3. Create separate Real Server Pools for IPsec and SSL VPN balancing and then add real servers into them.
   a. **IPsec VPN**: Specify port as 0 in the pool member service.

```
config load-balance pool
edit "ipsecvpn_pool"
set health-check-ctrl enable
set health-check-list LB_HLTHCK_ICMP
set real-server-ssl-profile NONE
config pool_member
edit 1
set pool_member_service_port 0
set pool_member_cookie  rs1
set real-server vpn1
next
edit 2
set pool_member_service_port 0
set pool_member_cookie  rs1
set real-server vpn2
next
end
```

   b. **SSL VPN**: Specify the port you configured on FortiGate in the pool member service (example: 10443)

```
config load-balance pool
edit "sslvpn_pool"
set health-check-ctrl enable
set health-check-list LB_HLTHCK_ICMP
set real-server-ssl-profile NONE
config pool_member
edit 1
set pool_member_service_port 10443
set pool_member_cookie rs1
set real-server vpn1
next
```

```
edit 2
set pool_member_service_port 10443
set pool_member_cookie rs1
set real-server vpn2 next
end
next
end
```

4. Finish the Basic and General configurations
   a. IPsec VPN Virtual Server settings:
      i. Select Layer 4 type.
      ii. Use the default DNAT Packet FOWARDING Method.
      iii. Specify address, port (500, 4500), and interface in general configuration.
      iv. Select UDP Profile and ROUND_ROBIN method and make sure to specify the persistence method (e.g. SRC_ADDR, HASH_SRC_ADDR), then select the configured real server pool.

```
config load-balance virtual-server
edit "IPSecVPN_L4"
set interface port1
set ip 123.1.1.1
set port 500 4500
set load-balance-profile LB_PROF_UDP
set load-balance-persistence LB_PERSIS_HASH_SRC_ADDR
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool ipsecvpn_pool
next
end
```

   b. SSL VPN Virtual Server settings:
      i. Select Layer 4 type.
      ii. Use the default DNAT Packet FOWARDING Method.
      iii. Specify address, port, and interface in general configuration.
      iv. Select TCP Profile and ROUND_ROBIN method and make sure to specify the persistence method (e.g. SRC_ADDR, HASH_SRC_ADDR), then select the configured real server pool.

```
config load-balance virtual-server
edit "SSLVPN_L4"
set interface port1
set ip 123.1.1.1
set port 10443
set load-balance-profile LB_PROF_TCP
set load-balance-persistence LB_PERSIS_SRC_ADDR
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool sslvpn_pool
next
end
```