

FortiADC - High Performance VPN Load-Balancing with FortiADC and FortiGate

Version 1.0.0

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 25, 2020

FortiADC 1.0.0 High Performance VPN Load-Balancing with FortiADC and FortiGate

01-100-600000-20200325

TABLE OF CONTENTS

Change Log	4
Introduction	5
Solution with FortiADC	6
Solution 1: Layer4 SLB One-Arm Deployment for SSL VPN Load-Balancing	7
Solution 2: Layer4 SLB In-Line Deployment for both IPsec and SSL VPN Load-Balancing	8
Solution 3: FortiGSLB for both IPsec and SSL VPN Load-Balancing	9
Appendix A: GUI Reference	11
Solution 1 Example Configuration	11
Solution 2 Example Configuration	15
Solution 3 Example Configuration	23
Appendix B: CLI Reference	25
Solution 1 Example Configuration	25
Solution 2 Example Configuration	27

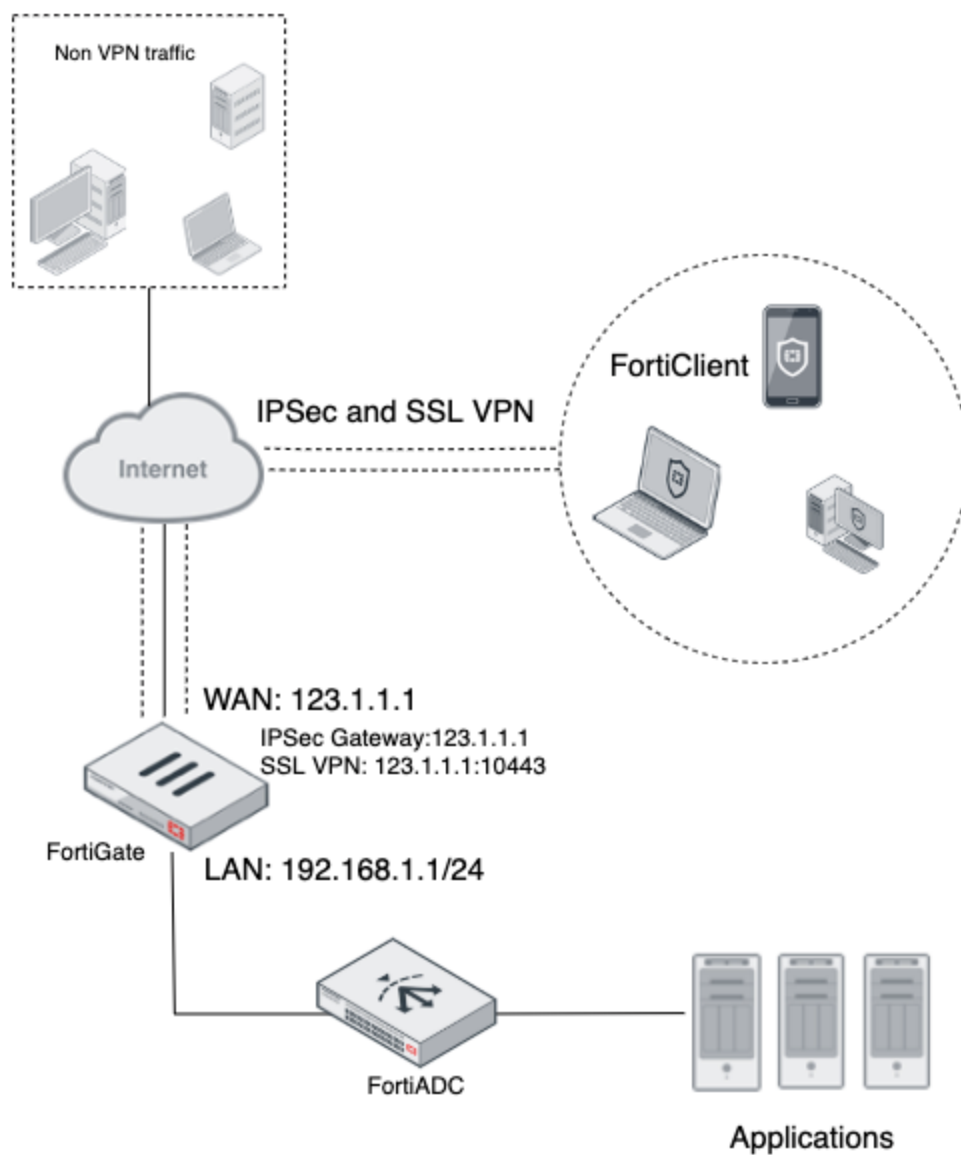
Change Log

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 topology without VPN Load Balancing



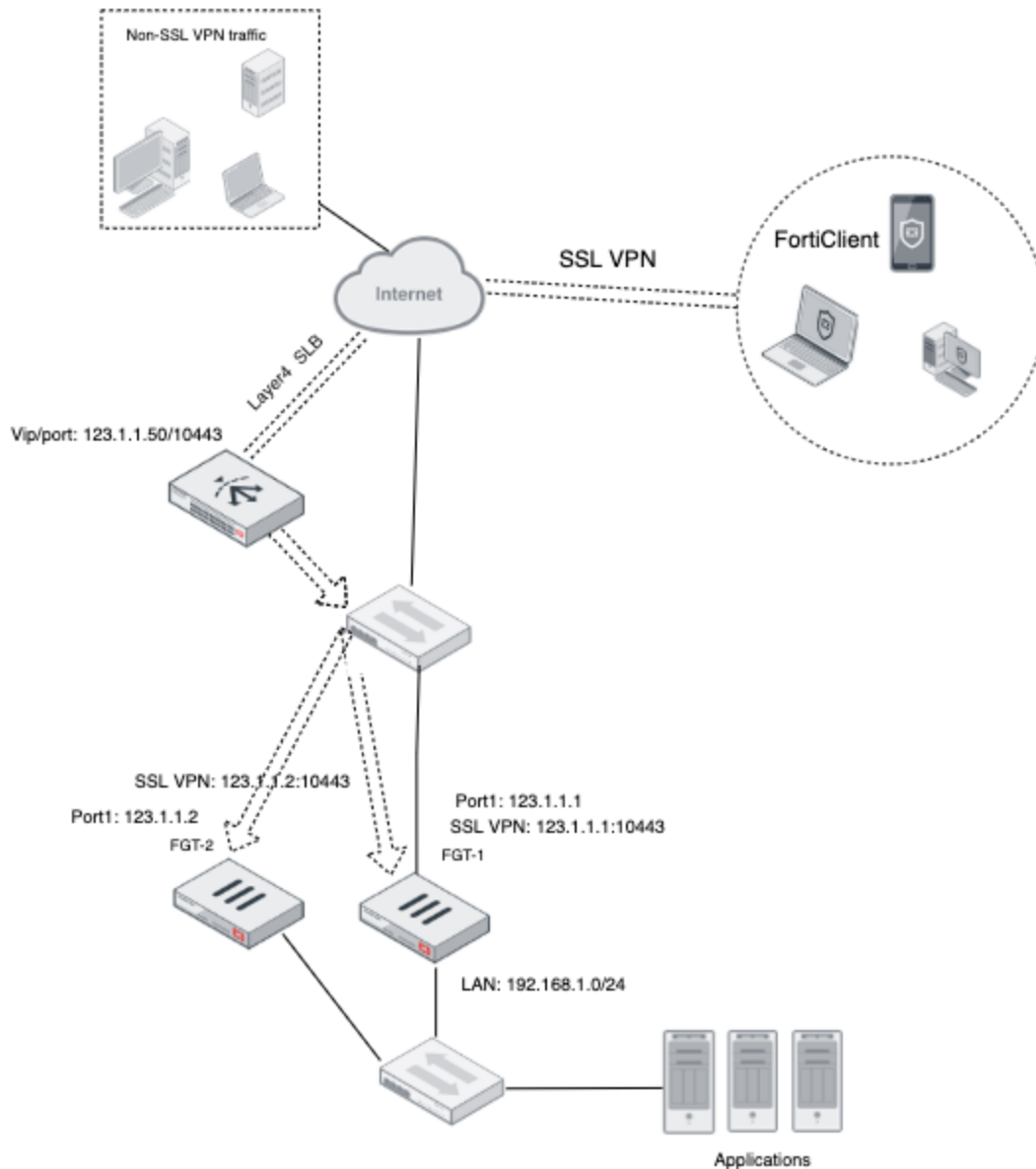
Solution with FortiADC

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

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



Key configurations:

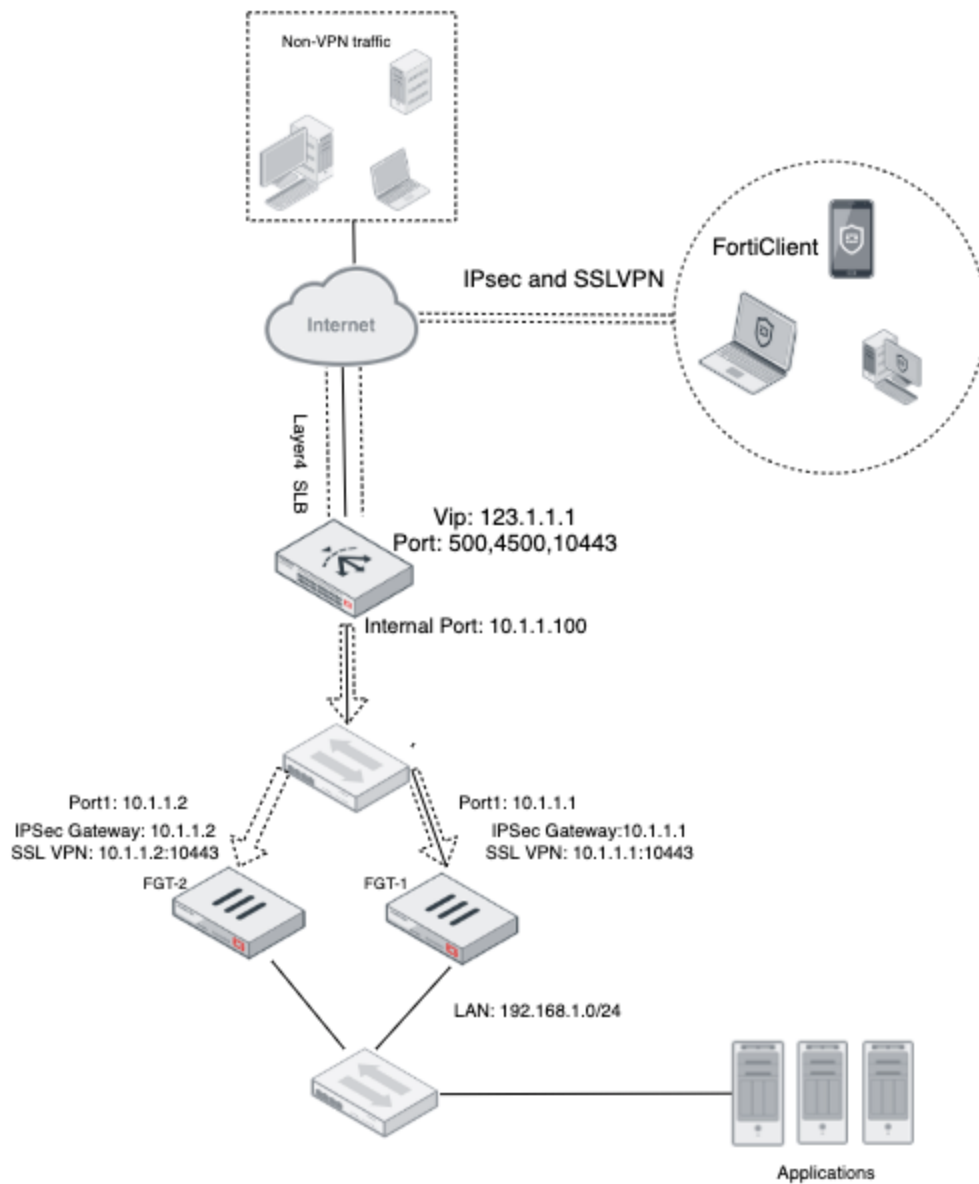
- Assign another public IP for FortiADC interface address.
- Configure Layer4 SLB and publish the VIP and its listening port as the SSL VPN site for all FortiClient users (Example: `https://123.1.1.50:10443`). You will need to configure **Full-NAT** in VS configuration profile.
- FortiADC is able to load balance the SSL VPN traffic across FortiGate pool. None-SSL VPN traffic will be routed to the original FortiGates.

Notes:

- 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 taking 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 port 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. FortiADC. None-SSL VPN traffic will be routed to the original FortiGate.

Notes:

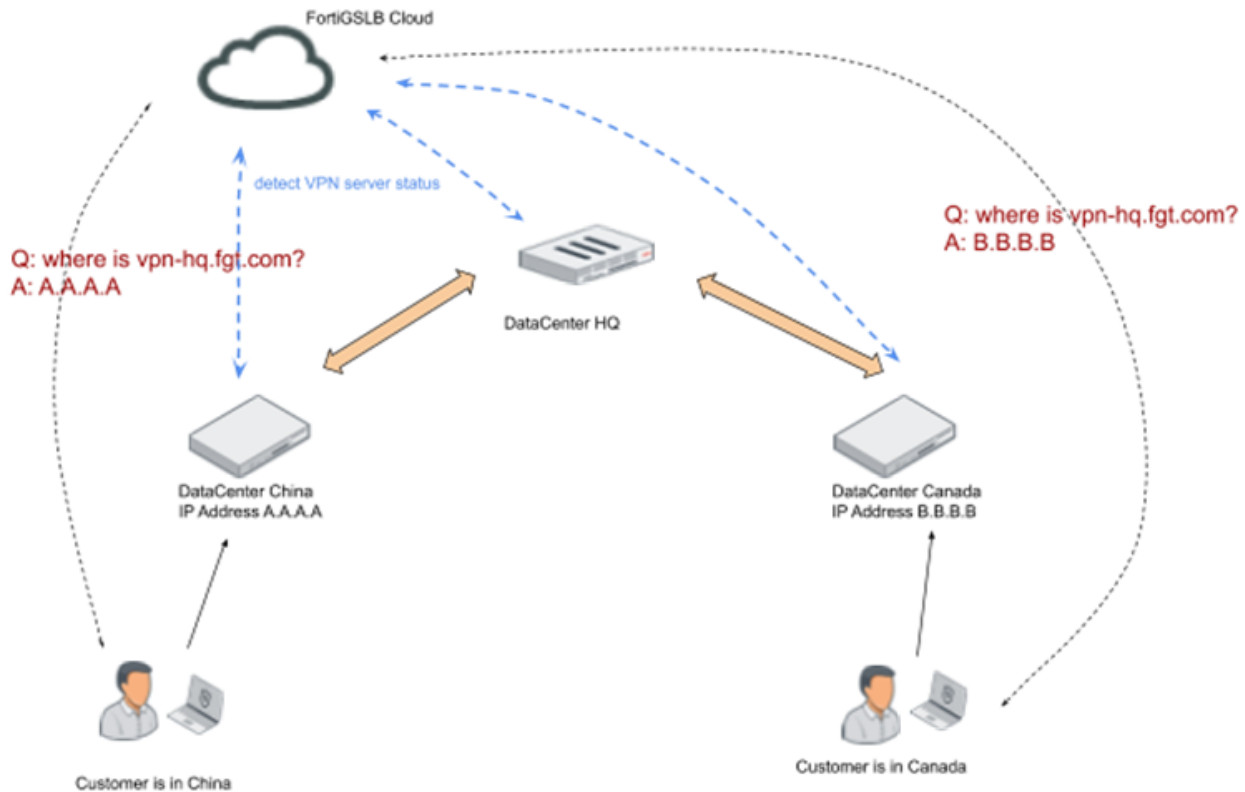
- Must change FortiGate network settings and move the original WAN to internal subnet.

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:

- Create new VPN** in FortiGate (VPN) or use the existing VPN.
- Create FQDN** in **FQDN services** > choose **DNS-Query-Origin Virtual Server Pool Selection Method**.
- Create FQDN member** > **Create new Virtual Server Pool**.
- Create pool member** > **Create generic server** > **Create new data center** > **Create new Server member** (add FortiGate VPN server IP).
- Create new Location List** for Virtual Server Pool
- Perform steps c.-e. for another Virtual Server Pool with a 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 servers, with the address as the IP of the listening FortiGate interface.

Real Server

Name

sslvpn1

Status

Enable

Disable

Maintain

Type

IP

FQDN

Address

123.1.1.1

Address6

::

Save

Cancel

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

Real Server Pool

Name

sslvpn_pool

Address Type

IPv4

IPv6

Health Check

ON

Health Check Relationship

AND

OR

Health Check List

Selected Items

Available Items

Double-click to deselect. Drag to reorder.

Create New

LB_HLTHCK_ICMP

LB_HLTHCK_HTTP

LB_HLTHCK_HTTPS

LB_HLTHCK_TCP_ECHO

Double-click to select.

Real Server SSL Profile

NONE

Member

Add Filter

Create New

ID	Name	Address	Health Check	Port	
1	sslvpn1	123.1.1.1	inherited	10443	
2	sslvpn2	123.1.1.2	inherited	10443	

Showing 1 to 2 of 2 entries

Show 10 entries

Previous 1 Next

Save

Cancel

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

NAT Source Pool

Name: nat1

Interface: port1

Address Type: IPv4 IPv6

Address Range: 123.1.1.51
Example: 192.168.2.101

To: 123.1.1.60
Example: 192.168.2.104

Node Member

Please save parent record first!

Save Cancel

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 server pool.

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

Virtual Server

Basic **General** Security Monitoring

Configuration

Address
123.1.1.50
Example: 192.0.2.1

Port
10443
Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit
0
Default: 0 Range: 0-100000000 concurrent connections

Connection Rate Limit
0
Default: 0 (disabled) Range: 0-86400 connections per second

Interface
port1

Resources

Profile
LB_PROF_TCP

Persistence
LB_PERSIS_SRC_ADDR

Method
LB_METHOD_ROUND_ROBIN

Real Server Pool
sslvpn_pool

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 enabled 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 servers, with the address as the IP of the listening FortiGate interface.

 Real Server

Name

Status

Enable Disable Maintain

Type

IP FQDN

Address

10.1.1.1

Address6

Save

Cancel

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.

Real Server Pool

Name

ipsecvpn_pool

Address Type

IPv4 IPv6

Health Check

ON

Health Check Relationship

AND OR

Health Check List

Selected Items

LB_HLTHCK_ICMP

Double-click to deselect. Drag to reorder.

Available Items

Create New

LB_HLTHCK_HTTP

LB_HLTHCK_HTTPS

LB_HLTHCK_TCP_ECHO

fr1784

Double-click to select.







Real Server SSL Profile

NONE

Member

Add Filter

Create New

ID	Name	Address	Health Check	Port	
1	vpn1	10.1.1.1	inherited	0	  
2	vpn2	10.1.1.2	inherited	0	  

Showing 1 to 2 of 2 entries

Show 10 entries

Previous 1 Next

Save

Cancel

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

Real Server Pool

Name

sslvpn_pool

Address Type

IPv4 IPv6

Health Check

ON

Health Check Relationship

AND OR

Health Check List

Selected Items

Double-click to deselect. Drag to reorder.

Available Items

Create New

LB_HLTHCK_ICMP

LB_HLTHCK_HTTP

LB_HLTHCK_HTTPS

LB_HLTHCK_TCP_ECHO

Double-click to select.

Real Server SSL Profile

NONE

Member

Add Filter

Create New

ID	Name	Address	Health Check	Port	
1	vpn1	10.1.1.1	inherited	10443	
2	vpn2	10.1.1.2	inherited	10443	

Showing 1 to 2 of 2 entries

Show 10 entries

Previous 1 Next

Save

Cancel

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.

Virtual Server

Basic

General

Security

Monitoring

Name

IPSecVPN_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

DNAT

Save

Cancel

Virtual Server

Basic

General

Security

Monitoring

Configuration

Address

123.1.1.1

Example: 192.0.2.1

Port

500 4500

Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit

0

Default: 0 Range: 0-100000000 concurrent connections

Connection Rate Limit

0

Default: 0 (disabled) Range: 0-86400 connections per second

Interface

port1

Resources

Profile

LB_PROF_UDP

Persistence

LB_PERSIS_HASH_SRC_ADDR

Method

LB_METHOD_ROUND_ROBIN

Real Server Pool

ipsecvpn_pool

Save

Cancel

- 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.

Virtual Server

BasicGeneralSecurityMonitoring

Name

SSLVPN_L4

Type

Layer 7Layer 4Layer 2

Status

DisableEnableMaintain

Address Type

IPv4IPv6

Traffic Group

default

Comments

Specify the comments

Specifics

Schedule Pool

OFF

Content Routing

OFF

Packet Forwarding Method

DNAT

Save

Cancel

Virtual Server

BasicGeneralSecurityMonitoring

Configuration

Address

123.1.1.1

Example: 192.0.2.1

Port

10443

Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit

0

Default: 0 Range: 0-100000000 concurrent connections

Connection Rate Limit

0

Default: 0 (disabled) Range: 0-86400 connections per second

Interface

port1

Resources

Profile

LB_PROF_TCP

Persistence

LB_PERSIS_SRC_ADDR

Method

LB_METHOD_ROUND_ROBIN

Real Server Pool

sslvpn_pool

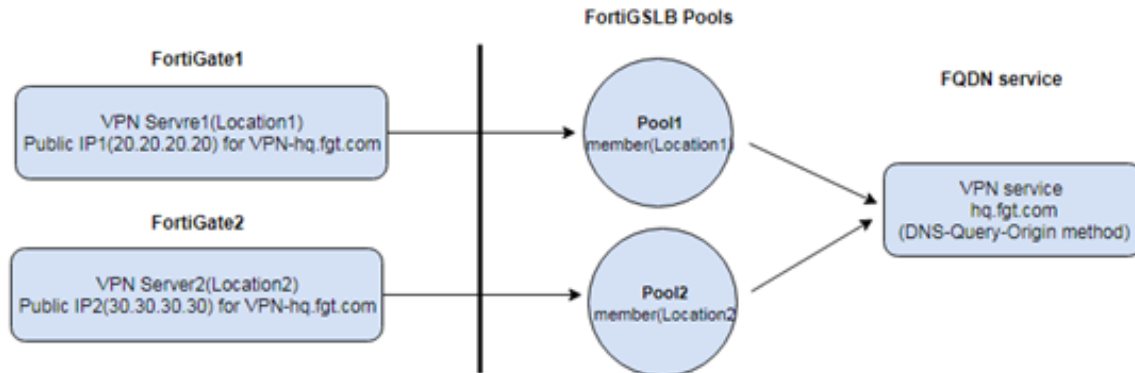
Save

Cancel

5. To view the result, do the following:
 - a. Open the FortiClient Console and go to **Remote Access**.
 - b. Make sure **Auto-connect** is enabled 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 have FortiGate VPN servers in two locations.
- 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.

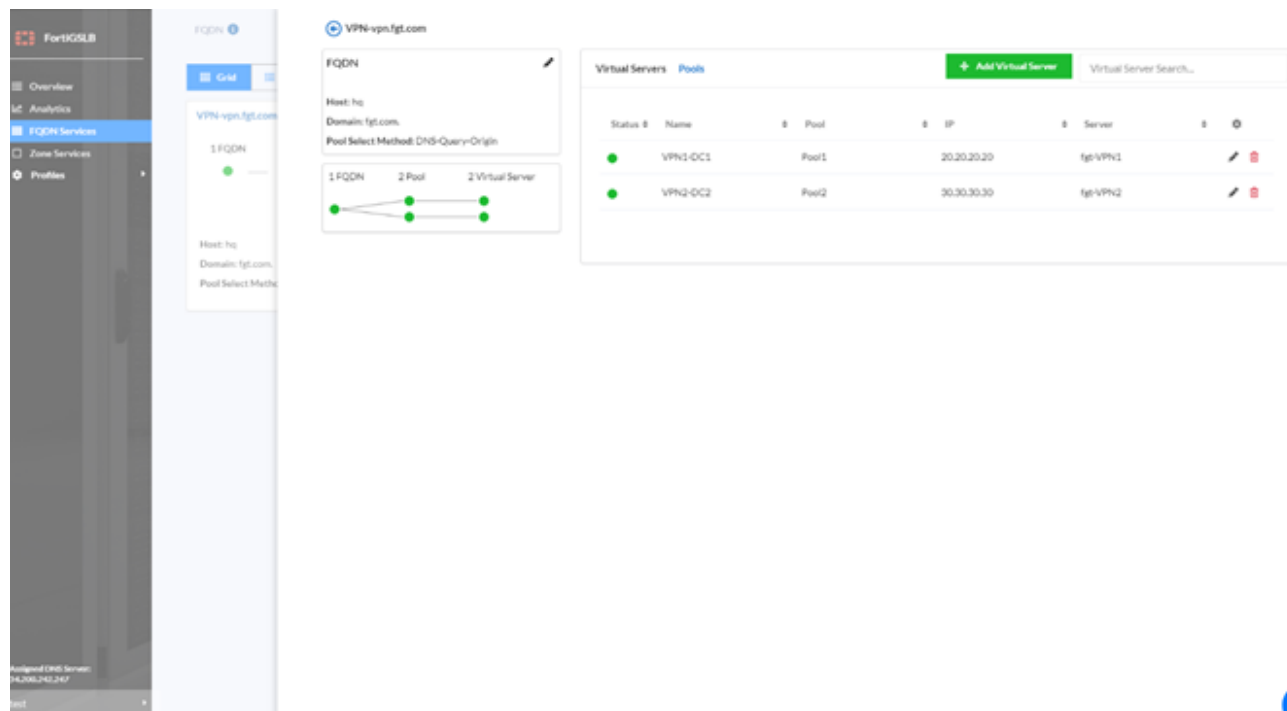
Steps

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 other types.
5. **Create new Location** List1 for Virtual 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 other types.
8. **Create new Location** List2 for Virtual 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
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 server pool.

```
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 servers 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 rsl
set real-server vpn1
next
edit 2
set pool_member_service_port 0
set pool_member_cookie rsl
set real-server vpn2
next
end
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 rsl
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
```

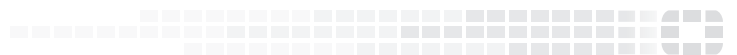
b. SSL VPN Virtual Server settings:

- 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
```



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.