



How To Guide:

IPSec VPN Tunnels for Load Balancing

Introduction

In the past, IPSec VPN tunnels destined for the same remote network could only establish over a single interface, yet it is now possible to form and send traffic over IPSec VPN tunnels on multiple interfaces with the Q-Balancer appliances at both ends, which significantly increases the flexibility of traffic path and routing decisions in VPN deployments.

Diagram Example

Branch:

Port 1:

WAN 1: example_1

IP: 203.67.222.40, Subnet: 203.67.222.40/30,
GW:203.67.222.1

Port 2:

WAN 2: example_2

IP: 100.100.100.6, Subnet:100.100.100.0/29,
GW:100.100.100.1

Port 4:

Branch LAN: 10.168.1.0/24, Interface:
10.168.1.254

HQ:

Port 1:

WAN 1: hq_1

IP: 103.67.222.47, Subnet: 103.67.222.40/29,
GW:103.67.222.41

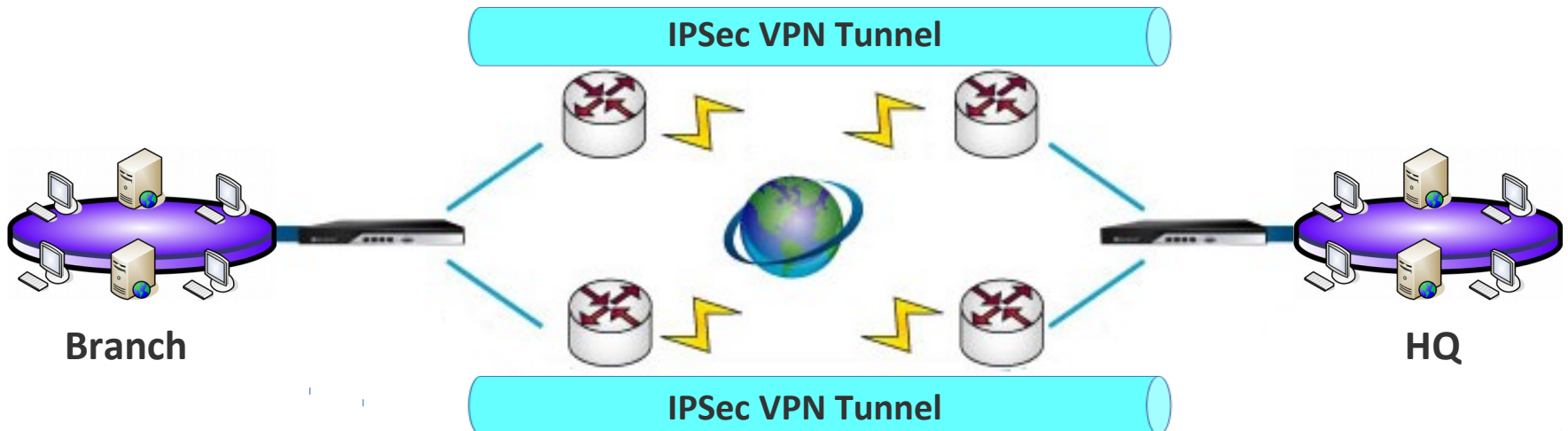
Port 2:

WAN 2: hq_2

IP: 118.169.192.20, Subnet:
118.169.192.20/30, GW:118.169.192.21

Port 4:

HQ LAN: 20.20.20.0/24, Interface:
20.20.20.254



Requirement

In this case, the solution is required to:

- > Failover LAN-to-LAN access between two IPSec tunnels.
- > Find the optimal path for critical network services.

Follow the steps below to configure IPSec VPN Tunnels for load balancing on the branch appliance with the IP details given:

- 1. WAN > ADD*
- 2. LAN > ADD*
- 3. VPN > IPSec > ADD*
- 4. Object > DPS > ADD*
- 5. Policy Routing > ADD*

WAN > ADD > Static

Name

example_1

Port

Port 1



Path Monitoring

dns_ipv4

Subnet

203.67.222.40/30

IP

203.67.222.40

Gateway

203.67.222.1

OK

CANCEL

WAN > ADD > Static

Name

example_2

Port

Port 2 ▼

Path Monitoring

dns_ipv4 ▼

Subnet

100.100.100.0/29

IP

100.100.100.6

Gateway

100.100.100.1

OK

CANCEL

WAN configuration on the branch appliance is done as follows:

WAN

ADD ▾

DELETE

Status	Type	↕	Name	↕	Port	↕	Interface	↕	Subnet	↕	IP	↕	Gateway	↕
✓	Static		example_1		Port 1		eth0_6		203.67.222.40/30		203.67.222.40		203.67.222.1	
✓	Static		example_2		Port 2		eth1_2		100.100.100.0/29		100.100.100.6		100.100.100.1	

LAN > ADD

Name

branch_LAN

Related ISP

Auto



Port

Port 4



Subnet

10.168.1.0/24

Route

Interface Gateway

IP

10.168.1.254

DHCP

Enabled



OK

CANCEL

LAN configuration on the branch appliance is done as follows:

LAN

ADD

DELETE

Name	↑↓	Port	↑↓	Interface	↑↓	Subnet	↑↓	Route	↑↓	IP	↑↓
branch_LAN		Port 4		eth3_3		10.168.1.0/24		Interface		10.168.1.254	

VPN > IPSec > ADD

In the Q-Balancer there are two types of *IPSec VPN Tunnels*, **General** and **QB2QB**. **General** is to establish IPSec VPN with third-party VPN solution, while **QB2QB** is to establish IPSec VPN between the Q-Balancer appliances. In this case, we will use **QB2QB** to build IPSec tunnels. Adding *IPSec Tunnels* on the branch appliance is done as follows:

VPN > IPSec > ADD

Enabled

Name

IPSec_tun_1

Type

General QB2QB

Tunnel ID

1

Pre-Shared Key

qbalancer

Down/Up Speed

15.3 / 2.9 Mbps

VPN > IPSec > ADD

Local

Local

203.67.222.40



Select the local IP to be the endpoint of the IPSec tunnel.

IKE ID

203.67.222.40

Network

Choose your option

Ignored



VPN > IPSec > ADD

Remote

Select the IP address to be the remote peer

Remote

103.67.222.47

IKE ID

103.67.222.47

Network

IP or Subnet

Ignored



VPN > IPSec > ADD

Leave rest of parameters default.

Phase 1

Exchange Mode

Main Aggressive

Encryption Algorithm

AES-256

Authentication Algorithm

SHA-256

DH Group

2 (1024-bits)

Lifetime

14400 Secs

Phase 2

Encryption Algorithm

AES-256

Authentication Algorithm

SHA-256

DH Group

2 (1024-bits)

Lifetime

14400 Secs

Dead Peer Detection

Enabled

Delay

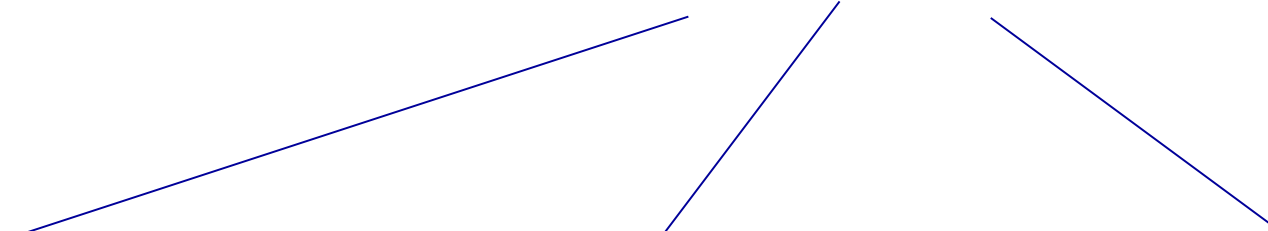
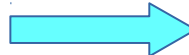
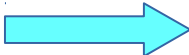
30 Secs

Timeout

180 Secs

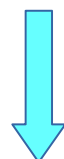
OK

CANCEL



The procedure of adding second IPSec Tunnel is same as the first one, and so is skipped in this guide. The IPSec tunnels on the branch appliance is done as follows:

Name ↑↓	Type ↑↓	Tunnel ID ↑↓	Interface ↑↓	Local ↑↓	Local IKE ID ↑↓	Local Network ↑↓
IPSec_tun_1	QB2QB	1	ipsec0	203.67.222.40	203.67.222.40	-
IPSec_tun_2	QB2QB	2	ipsec1	100.100.100.6	100.100.100.6	-



Remote ↑↓	Remote IKE ID ↑↓	Remote Network ↑↓	Pre-Shared Key ↑↓	Exchange Mode ↑↓	Other
103.67.222.47	103.67.222.47	-	qbalancer	Main	▼
118.169.192.20	118.169.192.20	-	qbalancer	Main	▼

Objects > DPS > ADD

Adding a **DPS** object for **IPSec VPN** tunnels on the branch appliance:

Name
branch_IPSec_balance

Backup Pool
None

Algorithm
Weighted Round Robin by Connection

Links
IPSec_tun_1, IPSec_tun_2

Weight

IPSec_tun_1 1 IPSec_tun_2 1

Proxy

OK CANCEL

Note: All algorithms are applicable for VPN load balancing.

Policy Routing > ADD

Priority 7

Highest Lowest

Source
branch_LAN +

Destination
hq_LAN +

Services
 Any Services Applications

Schedules
 Always Custom

Choose your option +

Pool
branch_IPSec_balance ▼

NAT
 Smart Manual No

Choose your option ▼

QoS
Enabled

Comments

Add HQ subnet here for policy routing.

Choose the DPS newly created for IPSec VPN.

Policy Routing

Policy Routing for IPSec VPN Tunnels on the branch appliance is done as follows:

Source	↑↓	Destination	↑↓	Services	↑↓	Schedules	↑↓	Pool	↑↓	NAT	↑↓
branch_LAN	↔	hq_LAN		Any		Always		branch_IPSec_balance		No	

Follow the steps below to configure IPSec VPN Tunnels for load balancing on the HQ appliance with the IP details given:

- 1. WAN > ADD*
- 2. LAN > ADD*
- 3. VPN > IPSec > ADD*
- 4. Object > DPS > ADD*
- 5. Policy Routing > ADD*

WAN > ADD > Static

Name

hq_1

Port

Port 1 ▼

Path Monitoring

dns_ipv4

Subnet

103.67.222.40/29

IP

103.67.222.47

Gateway

103.67.222.41

OK

CANCEL

WAN > ADD > Static

Name

hq_2

Port

Port 2 ▼

Path Monitoring

dns_ipv4

Subnet

118.169.192.20/30

IP

118.169.192.20

Gateway

118.169.192.21









OK

CANCEL

WAN configuration on the HQ appliance is done as follows:

WAN

[ADD](#) [DELETE](#)

Status	Type 	Name	Port 	Interface 	Subnet 	IP 	Gateway 
	Static	hq_1	Port 1	eth0_9	103.67.222.40/29	103.67.222.47	103.67.222.41
	Static	hq_2	Port 2	eth1_10	118.169.192.20/30	118.169.192.20	118.169.192.21

LAN > ADD

Name

hq_LAN

Related ISP

Auto

Port

Port 4

Subnet

20.20.20.0/24

Route

Interface Gateway

IP

20.20.20.254

DHCP

Enabled



OK

CANCEL

LAN configuration on the HQ appliance is done as follows:

LAN

ADD

DELETE

Name	↑↓	Port	↑↓	Interface	↑↓	Subnet	↑↓	Route	↑↓	IP	↑↓
hq_LAN		Port 4		eth3_11		20.20.20.0/24		Interface		20.20.20.254	

VPN > IPSec > ADD

Enabled



Name

IPSec_tun_1

Type



General



QB2QB

Tunnel ID

1

Pre-Shared Key

qbalancer

Down/Up Speed

15.3

/ 2.9

Mbps

VPN > IPSec > ADD

Select the local IP to be the endpoint of the IPSec tunnel.

Local

Local

103.67.222.47



IKE ID

103.67.222.47

Network

Choose your option

Ignored



VPN > IPSec > ADD

Select the IP address to be the remote peer.

Remote

Remote

203.67.222.40

IKE ID

203.67.222.40

Network

IP or Subnet

.....

Ignored



VPN > IPSec > ADD

Leave rest of parameters default.

Phase 1

Exchange Mode

Main Aggressive

Encryption Algorithm

AES-256

Authentication Algorithm

SHA-256

DH Group

2 (1024-bits)

Lifetime

14400 Secs

Phase 2

Encryption Algorithm

AES-256

Authentication Algorithm

SHA-256

DH Group

2 (1024-bits)

Lifetime

14400 Secs

Dead Peer Detection

Enabled

Delay

30 Secs

Timeout

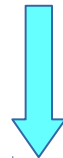
180 Secs

OK

CANCEL

The procedure of adding second IPSec Tunnel is same as the first one, and so is skipped in this guide. The IPSec tunnels on the HQ appliance is done as follows:

Name ↑↓	Type ↑↓	Tunnel ID ↑↓	Interface ↑↓	Local ↑↓	Local IKE ID ↑↓	Local Network ↑↓
IPSec_tun_1	QB2QB	1	ipsec0	103.67.222.47	103.67.222.47	-
IPSec_tun_2	QB2QB	2	ipsec1	118.169.192.20	118.169.192.20	-



Remote ↑↓	Remote IKE ID ↑↓	Remote Network ↑↓	Pre-Shared Key ↑↓	Exchange Mode ↑↓	Other
203.67.222.40	203.67.222.40	-	qbalancer	Main	▼
100.100.100.6	100.100.100.6	-	qbalancer	Main	▼

Objects > DPS > ADD

Adding a **DPS** object for **IPSec VPN** tunnels on the HQ appliance:

Name

hq_IPSec_balance

Backup Pool

None

Algorithm

Weighted Round Robin by Connection

Links

IPSec_tun_1, IPSec_tun_2

Weight

IPSec_tun_1



1

IPSec_tun_2



1

Proxy

OK

CANCEL

Policy Routing > ADD

Priority 7

Highest Lowest

Source

hq_LAN ▼ +

Destination

branch_LAN ▼ +

Services

Any Services Applications

Schedules

Always Custom

Choose your option ▼ +

Pool

hq_IPSec_balance ▼

NAT

Smart Manual No

Choose your option ▼

QoS

Enabled

Comments

OK CANCEL

Add branch subnet here for policy routing.

Policy Routing

Policy Routing for IPSec VPN on the **HQ** appliance is done as follows:

Source	↕	Destination	↕	Services	↕	Schedules	↕	Pool	↕	NAT	↕
hq_LAN	↔	branch_LAN		Any		Always		hq_IPSec_balance		No	

For reference, the following is the counterpart setting on the **branch** appliance:

Source	↕	Destination	↕	Services	↕	Schedules	↕	Pool	↕	NAT	↕
branch_LAN	↔	hq_LAN		Any		Always		branch_IPSec_balance		No	

Done!

Check if the LAN hosts at the branch are able to ping hosts at the HQ now.