

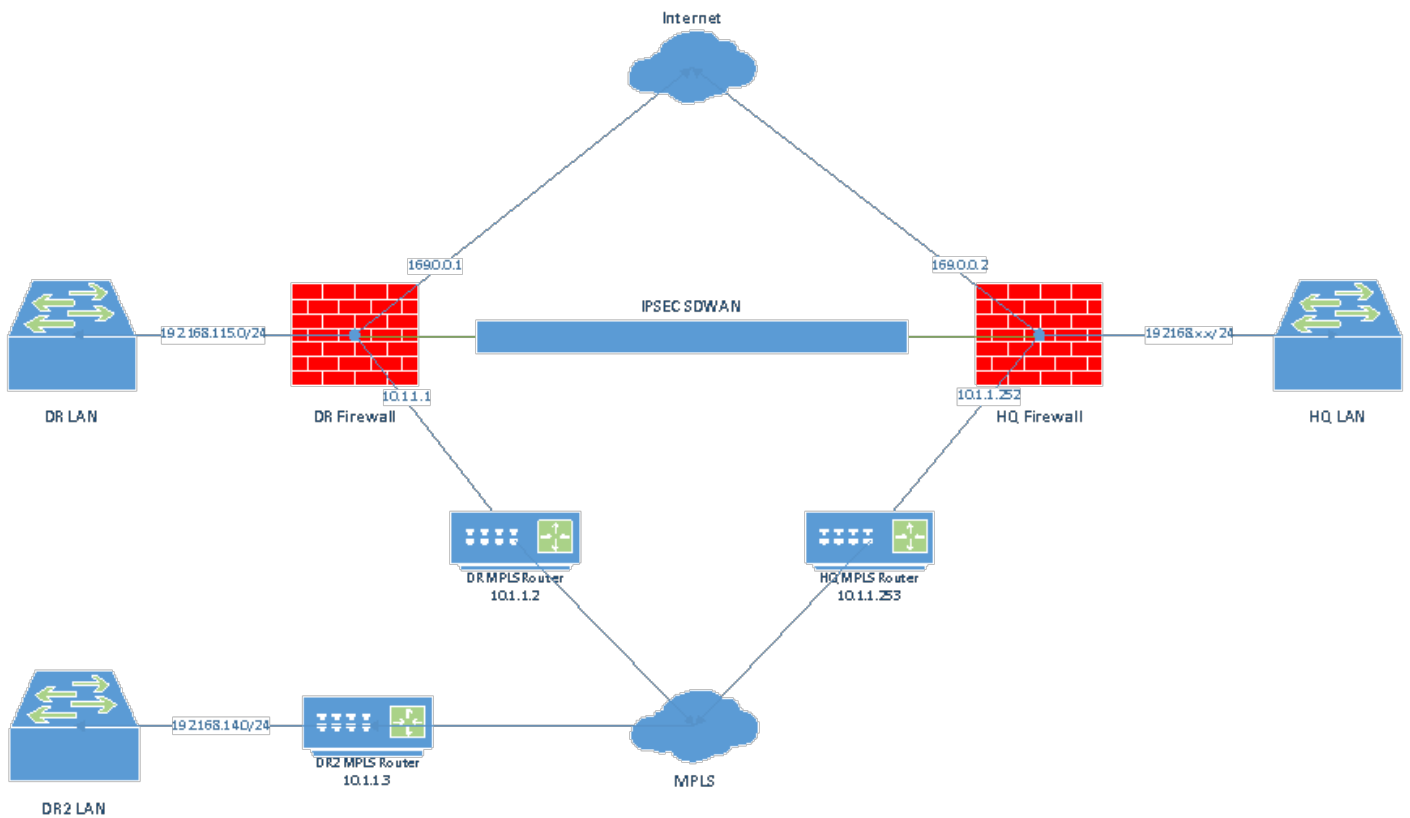
MPLS + Internet IPSEC SDWAN

SDWAN



HQ MPLS MPLS+Internet

?????



????? MPLS?Internet Interface????

HQ Interface:

	MPLS (VLAN101)		VLAN	10.1.1.252/255.255.255.248
--	----------------	--	------	----------------------------

	port1		Physical Interface	169.0.0.2/255.255.255.0
--	-------	--	--------------------	-------------------------

HQ :

Destination <input type="checkbox"/>	Gateway IP <input type="checkbox"/>	Interface <input type="checkbox"/>
10.1.1.0/29	10.1.1.253	MPLS (VLAN101)

Internet Interface MPLS DR

MPLS Static Route

????MPLS?Internet?DR?IPSEC VPN??????????

MPLS IPSEC Internet IPSEC

VPN Creation Wizard

1 VPN Setup

Name

Template type Site to Site Hub-and-Spoke Remote Access Custom

New VPN Tunnel

Name

MPLS_IPSEC

Comments

Comments

0/255

Network

IP Version

IPv4 IPv6

Remote Gateway

Static IP Address

IP Address

10.1.1.2

Interface

MPLS (VLAN101)

Local Gateway



Mode Config



NAT Traversal

Enable Disable Forced

Keepalive Frequency

10

Dead Peer Detection

Disable On Idle On Demand

DPD retry count

3


DPD retry interval

20

s

Forward Error Correction

Egress Ingress

 Advanced...

Authentication

Method

Pre-shared Key

Pre-shared Key

••••••



IKE

Version

1 2

Mode

Aggressive Main (ID protection)

Phase 1 Proposal ⊕ Add

Encryption	AES128	Authentication	SHA256	✕
Encryption	AES256	Authentication	SHA256	✕
Encryption	AES128	Authentication	SHA1	✕
Encryption	AES256	Authentication	SHA1	✕

Diffie-Hellman Groups

<input type="checkbox"/>	32	<input type="checkbox"/>	31	<input type="checkbox"/>	30	<input type="checkbox"/>	29	<input type="checkbox"/>	28	<input type="checkbox"/>	27
<input type="checkbox"/>	21	<input type="checkbox"/>	20	<input type="checkbox"/>	19	<input type="checkbox"/>	18	<input type="checkbox"/>	17	<input type="checkbox"/>	16
<input type="checkbox"/>	15	<input checked="" type="checkbox"/>	14	<input checked="" type="checkbox"/>	5	<input type="checkbox"/>	2	<input type="checkbox"/>	1		

Key Lifetime (seconds)

Local ID

XAUTH

Type

Phase 2 Selectors

Name	Local Address	Remote Address	
MPLS_IPSEC	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	

New Phase 2 ✓ ↺

Name

Comments

Local Address

Remote Address

⊕ Advanced...

IPSEC

Tunnel	Interface Binding	Status
Custom		
IPSEC_BOO	port1	Inactive
MPLS_IPSEC_BOO	MPLS (VLAN101)	Inactive

??Interface?VPN????IP??????????

MPLS_IPSEC_BOO	Tunnel Interface	10.1.1.10/255.255.255.255	PING
----------------	------------------	---------------------------	------

Name	MPLS_IPSEC_B00
Alias	<input type="text"/>
Type	Tunnel Interface
Interface	MPLS (VLAN101)
VRF ID	<input type="text" value="0"/>
Virtual domain	HQ_Core
Role	<input type="text" value="Undefined"/>

Address

Addressing mode	Manual
IP	<input type="text" value="10.1.1.10"/>
Netmask	255.255.255.255
Remote IP/Netmask	<input type="text" value="10.1.1.9 255.255.255.252"/>

Administrative Access

IPv4	<input type="checkbox"/> HTTPS	<input type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
	<input type="checkbox"/> FMG-Access	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP
	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection
	<input type="checkbox"/> Speed Test		

FortiOS 7.0?????????CLI??

```

FortiGate-1800F (MPLS_IPSEC_B00) # show
config system interface
  edit "MPLS_IPSEC_B00"
    set vdom "HQ_Core"
    set ip 10.1.1.10 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 10.1.1.9 255.255.255.252
    set snmp-index 81
    set interface "VLAN101"
  next
end

```

```

FortiGate-1800F (IPSEC_B00) # show
config system interface
  edit "IPSEC_B00"
    set vdom "HQ_Core"
    set ip 10.1.1.14 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 10.1.1.13 255.255.255.252
    set snmp-index 82
    set interface "port1"
  next
end

```

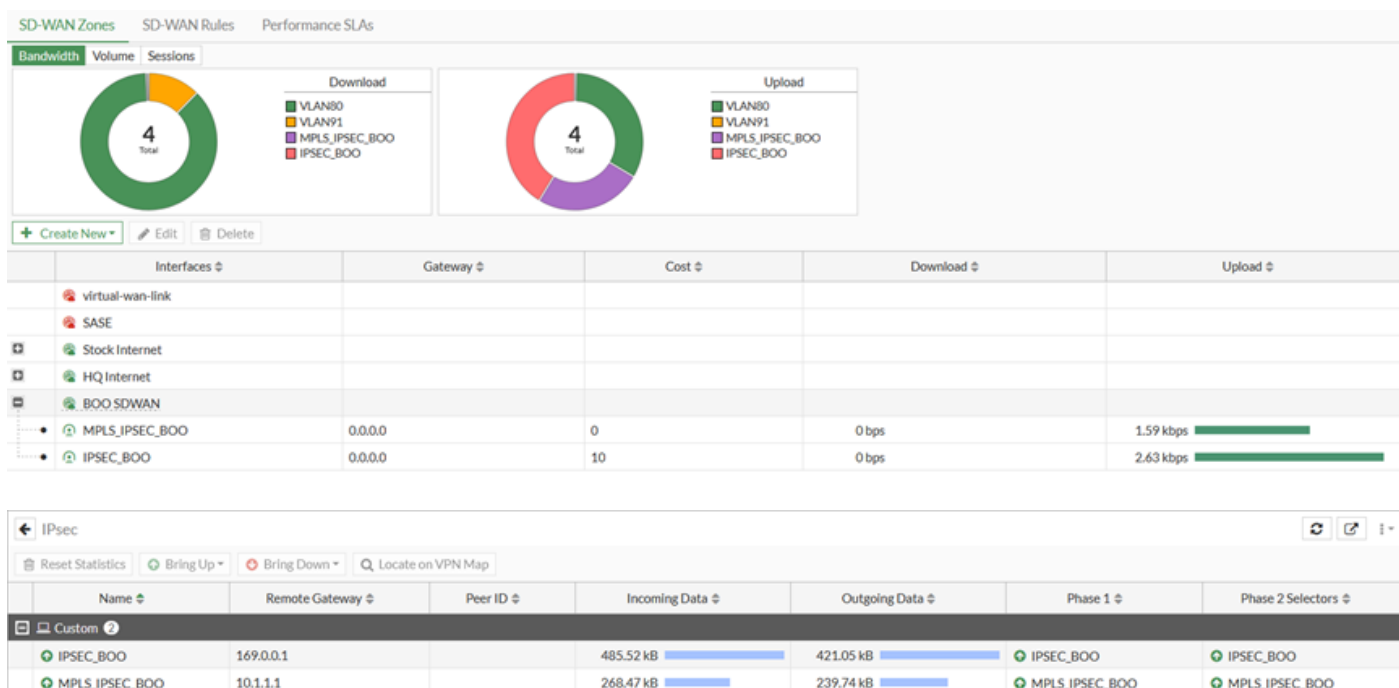
IPSEC VPN Interface IP HQ DR

HQ Internet IPSEC VPN Interface 10.1.1.14 DR Internet IPSEC VPN Interface 10.1.1.13

HQ MPLS IPSEC VPN Interface 10.1.1.10 DR MPLS IPSEC VPN Interface 10.1.1.9

SDWAN Zone IPSEC VPN Interface Member

HQ DR IPSEC VPN Tunnel Ping IPSEC VPN Interface IP



```
FortiGate-1800F (HQ_Core) # execute ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1): 56 data bytes
64 bytes from 10.1.1.1: icmp_seq=0 ttl=254 time=0.5 ms
64 bytes from 10.1.1.1: icmp_seq=1 ttl=254 time=0.3 ms
^C
--- 10.1.1.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.4/0.5 ms

FortiGate-1800F (HQ_Core) # execute ping 169.0.0.1
PING 169.0.0.1 (169.0.0.1): 56 data bytes
64 bytes from 169.0.0.1: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 169.0.0.1: icmp_seq=1 ttl=255 time=0.1 ms
^C
--- 169.0.0.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms

FortiGate-1800F (HQ_Core) # █
```

????SDWAN Rule

???HQ?SDWAN Rule?DR????????

Priority Rule

Name

Source

Source address

User group

Destination

Address

Protocol number

Internet Service

Application

Outgoing Interfaces

Select a strategy for how outgoing interfaces will be chosen.

- Manual**
Manually assign outgoing interfaces.
- Best Quality**
The interface with the best measured performance is selected.
- Lowest Cost (SLA)**
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.
- Maximize Bandwidth (SLA)**
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

Zone preference

Forward DSCP

Reverse DSCP

????Firewall Policy?Static Route

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
BOO SDWAN → HQ Internet	all	all	always	ALL	ACCEPT	Enabled	g-default g-default g-default certificate-inspection	UTM	3.63 MB
BOO SDWAN → LAN	all	all	always	ALL	ACCEPT	Disabled	g-default g-default g-default certificate-inspection	UTM	129.95 kB
BOO SDWAN → Server_Farm	all	all	always	ALL	ACCEPT	Disabled	g-default g-default g-default certificate-inspection	UTM	40.83 MB

Server_Farm → BOO SDWAN

all all always ALL ACCEPT Disabled

AV g-default
 APP g-default
 IPS g-default
 SSL certificate-inspection

UTM 26.30 MB

VOIP → BOO SDWAN

all all always ALL ACCEPT Disabled

AV g-default
 APP g-default
 IPS g-default
 SSL certificate-inspection

UTM 0 B

Destination	Gateway IP	Interface	Status
192.168.115.0/24		BOO.SDWAN	Enabled

????Ping DR LAN Interface???????

```
FortiGate-1800F (HQ_Core) # execute ping 192.168.115.254
PING 192.168.115.254 (192.168.115.254): 56 data bytes
64 bytes from 192.168.115.254: icmp_seq=0 ttl=255 time=0.7 ms
64 bytes from 192.168.115.254: icmp_seq=1 ttl=255 time=0.6 ms
^C
--- 192.168.115.254 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.6/0.6/0.7 ms

FortiGate-1800F (HQ_Core) #
```


! HQ DR

????SDWAN????????????LAN Interface???

????????LAN Interface?Health Check??Check????????????????????

Edit Performance SLA



Name **Check_BOO**

Probe mode  **Active** Passive Prefer Passive

Protocol **Ping** HTTP DNS

Server

Participants **All SD-WAN Members** **Specify**

 IPSEC_BOO	<input data-bbox="933 604 965 649" type="button" value="x"/>
 MPLS_IPSEC_BOO	<input data-bbox="933 649 965 694" type="button" value="x"/>
<input data-bbox="662 694 694 739" type="button" value="+"/>	

SLA Target


Latency threshold ms


Jitter threshold ms

Packet Loss threshold %


Link Status

Check interval ms

Failures before inactive 

Restore link after  check(s)

Actions when Inactive

Update static route 

Revision #11

Created 11 June 2024 01:48:10 by []

Updated 2 August 2024 14:32:55 by []