



FortiOS - Zscaler Internet Access and Fortinet SD-WAN Deployment Guide

Version 6.2.4

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



September 8, 2020

FortiOS 6.2.4 Zscaler Internet Access and Fortinet SD-WAN Deployment Guide

01-624-660292-20200908

TABLE OF CONTENTS

Change Log	4
Zscaler Internet Access and Fortinet SD-WAN	5
Configuring IPsec or GRE tunnels on Zscaler Internet Access	6
Configuring IPsec or GRE tunnels on FortiOS	7
Configuring SD-WAN interfaces	12
Configuring firewall policies	15
Configuring Performance SLA test	19
Configuring SD-WAN rules	21
Verifying configuration with Zscaler test page	23
Results	24
Interface usage	24
IPsec status	25
Performance SLA	26
Routing table	27
Firewall policy	27
Top sources	27

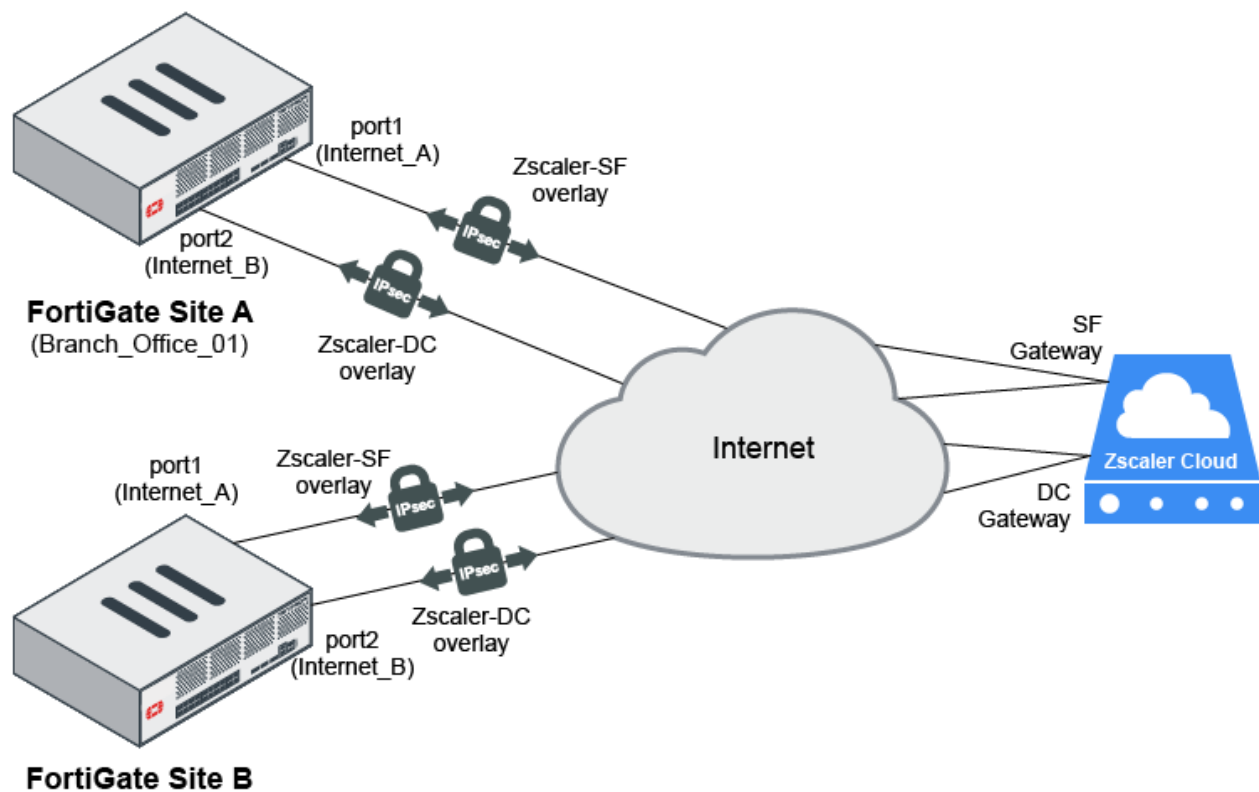
Change Log

Date	Change Description
2020-07-07	Initial release.
2020-07-27	Updated Configuring IPsec or GRE tunnels on FortiOS on page 7 , Configuring SD-WAN interfaces on page 12 , Configuring firewall policies on page 15 , Configuring Performance SLA test on page 19 , and Configuring SD-WAN rules on page 21 .
2020-09-08	Updated Configuring IPsec or GRE tunnels on Zscaler Internet Access on page 6 and Configuring IPsec or GRE tunnels on FortiOS on page 7 .

Zscaler Internet Access and Fortinet SD-WAN

This document demonstrates the interoperability of Zscaler Internet Access (ZIA) and Fortinet secure SD-WAN. You can use this guide as an example to deploy ZIA and Fortinet secure SD-WAN.

In this example, we have two FortiGate sites, Site A and Site B. Each site has two underlay connections `port1 (Internet_A)` and `port2 (Internet_B)` that have two overlay connections `Zscaler_SF` and `Zscaler_DC` to Zscaler SF Gateway and Zscaler DC Gateway respectively. Web traffic will be routed to Zscaler where it will be scanned, while non-web traffic passes over the underlays and is scanned by FortiGate.



This section contains the following topics:

- [Configuring IPsec or GRE tunnels on Zscaler Internet Access on page 6](#)
- [Configuring IPsec or GRE tunnels on FortiOS on page 7](#)
- [Configuring SD-WAN interfaces on page 12](#)
- [Configuring firewall policies on page 15](#)
- [Configuring Performance SLA test on page 19](#)
- [Configuring SD-WAN rules on page 21](#)
- [Verifying configuration with Zscaler test page on page 23](#)
- [Results on page 24](#)

Configuring IPsec or GRE tunnels on Zscaler Internet Access

IPsec and GRE are similar in the sense that both provide tunneling across the public Internet. However, IPsec also provides encryption and GRE does not. Also, Zscaler Internet Access supports a greater throughput over GRE tunnels while throughput over an IPsec tunnel is capped.

In this case, you will configure either IPsec tunnels or GRE tunnels, and not both.

To configure IPsec tunnels on ZIA:

1. Locate the available data-centers and the hostname/IP address of the VIP to which you will establish a tunnel; go to [Locating the Hostnames and IP Addresses of Zscaler Enforcement Nodes \(ZENs\)](#).
2. Add the VPN credentials for IPsec tunnel on ZIA; go to [Adding VPN Credentials](#).
3. Configure the VPN credentials to a location; go to [Configuring Locations](#).

Repeat the above procedure to configure a second IPsec tunnel to another Zscaler ZEN.



You may configure GRE tunnels, though Fortinet recommends configuring IPsec tunnels.

To configure GRE tunnels on ZIA:

1. Locate the available data-centers and the hostname/IP address of the VIP to which you will establish a tunnel; go to [Locating the Hostnames and IP Addresses of Zscaler Enforcement Nodes \(ZENs\)](#).
2. Configure the GRE tunnel on ZIA; go to [Configuring GRE tunnels](#).
3. Configure a location by choosing a static IP address; go to [Configuring Locations](#).

Repeat the above procedure to configure a second GRE tunnel to another Zscaler ZEN.

If you have any problems, contact Zscaler by submitting a support ticket at <https://help.zscaler.com/submit-ticket>.

Configuring IPsec or GRE tunnels on FortiOS

In this case, you will configure either IPsec tunnels or GRE tunnels, and not both.

To configure an IPsec tunnel:

1. Go to *VPN > IPsec Wizard*. The *VPN Creation Wizard* displays.
2. Enter a *Name* for the tunnel and select the *Template type* to be *Custom*.

VPN Creation Wizard

1 VPN Setup

Name

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

< Back **Next >** Cancel

3. Click *Next*. The *New VPN Tunnel* settings are displayed.
4. Configure the *Network* settings as indicated in the table below. The *Dynamic DNS* field should be the Zscaler ZEN hostname that you will use.

IP Version	IPv4
Remote Gateway	Dynamic DNS
Dynamic DNS	<Zscaler SF Host>
Interface	Internet_A(port1)

Network ✓ ↺

IP Version IPv4

Remote Gateway Dynamic DNS ▼

Dynamic DNS <Zscaler SF Host>

Interface Internet_A (port1) ▼

Local Gateway ☐

Mode Config ☐

NAT Traversal Enable Disable Forced

Dead Peer Detection Disable On Idle On Demand

Forward Error Correction Egress ☐ Ingress ☐

+ Advanced...

5. Configure the *Authentication* settings with the *Method* to be *Pre-shared Key* and entering the pre-shared key (PSK). The PSK should be unique per site, and the *IKE Version* should be selected to be 2.

Authentication ✓ ↺

Method Pre-shared Key ▼

Pre-shared Key ●●●●●●●●

IKE

Version 1 2

6. Configure the *Phase 1 Proposal* settings as indicated in the table below. The *Local ID* field should be set to the FQDN you configured in the previous steps.

Encryption	AES256
Authentication	SHA1
Diffie-Hellman Group	2
Key Lifetime (seconds)	86400

Local ID <Zscaler SF Host>

Phase 1 Proposal ➕ Add ✓ ↺

Encryption AES256 ▼

Authentication SHA1 ▼

Diffie-Hellman Group

☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27

☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16

☐ 15 ☐ 14 ☐ 5 ☒ 2 ☐ 1

Key Lifetime (seconds)

86400

Local ID

<Zscaler SF Host>

7. Configure the *Phase 2 Selectors* settings as indicated in the table below. Leave all other settings to their default values.

Local Address (Subnet)	0.0.0.0/0.0.0.0
Remote Address (Subnet)	0.0.0.0/0.0.0.0
Encryption	NULL
Authentication	MD5
Enable Perfect Forward Secrecy (PFS)	Unchecked.
Key Lifetime (Seconds)	28800

Local Address

Subnet ▼ 0.0.0.0/0.0.0.0

Remote Address

Subnet ▼ 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal ⊕ Add

Encryption NULL ▼

Authentication MD5 ▼

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☐

Local Port All ☒

Remote Port All ☒

Protocol All ☒

Auto-negotiate ☐

Autokey Keep Alive ☒

Key Lifetime

Seconds ▼

Seconds

28800

8. Click OK.

Similarly, configure another IPsec tunnel Zscaler-DC over the Internet_B(port2) interface.

Verify your IPsec tunnels by navigating to *VPN > IPsec tunnels* from the tree menu on the left side of the FortiGate GUI.

<div>+ Create New</div>		<div>Edit</div>	<div>Delete</div>	<div>Search</div>
Tunnel		Interface Binding		
<div>3 2</div>				
Zscaler-DC		Internet_B (port2)		
Zscaler-SF		Internet_A (port1)		
<div>5 1</div>				



You may configure GRE tunnels, though Fortinet recommends configuring IPsec tunnels.

To configure a GRE tunnel from the CLI:

1. Create a GRE tunnel and add it as an interface:

```
config system gre-tunnel
  edit "Zscaler-SF"
    set interface "port1"
    set remote-gw <Zscaler SF Host>
    set local-gw <Internet_A>
  next
end
```

2. Configure the GRE tunnel interfaces:

```
config system interface
  edit "Zscaler-SF"
    set ip <ip address in a /30 subnet provided by Zscaler> 255.255.255.255
    set allowaccess ping
    set type tunnel
    set interface "port1"
  next
end
```

Similarly, configure another GRE tunnel `Zscaler-DC` over the `Internet_B (port2)` interface.

Configuring SD-WAN interfaces


To use the secure SD-WAN capability, we need to configure the primary and secondary Zscaler ZENs as SD-WAN interface members.

In this example, the SF ZEN is closer, so we will choose the Lowest Cost (SLA) SD-WAN algorithm to prefer the SF ZEN over the DC ZEN, and configure the Zscaler-SF interface with a lower cost.

To configure the primary ZEN as an SD-WAN interface member:

1. Go to *Network > SD-WAN*, and click *Create New* from the *SD-WAN Interface Members* section. The *New SD-WAN Member* modal slides on screen.
2. Configure the *Interface* to be *Zscaler-SF* from the drop-down list.
3. Configure the *Cost* to be 5. A lower *Cost* value indicates that this member is the primary interface member, and is preferred more than a member with a higher *Cost* value when using the *Lowest Cost (SLA)* strategy.

New SD-WAN Member

Interface	<div> Zscaler-SF ▼</div>
Gateway	<input type="text" value="10.0.10.1"/>
IPv6 Gateway	<input type="text" value="::"/>
Cost	<input type="text" value="5"/>
Status	<div><input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable</div>

OK

Cancel


4. Click *OK*.

To configure the secondary ZEN as an SD-WAN interface member:

1. Go to *Network > SD-WAN Zones*, and click *Create New > SD-WAN Member*. The *New SD-WAN Member* screen displays.
2. Configure the *Interface* to be *Zscaler-DC* from the drop-down list.

- Configure the *Cost* to be 10. A higher *Cost* value indicates that this member is the secondary interface member, and is preferred less than a member with a lower *Cost* value when using the *Lowest Cost (SLA)* strategy.

New SD-WAN Member

Interface	 Zscaler-DC
Gateway	10.10.11.1
IPv6 Gateway	::
Cost	10
Status	<input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/>

OK


Cancel

- Click **OK**.





Similarly, repeat the above procedure to configure the *Internet_A* and *Internet_B* interfaces with *Costs* of 5 and 10 respectively.

After all the SD-WAN interface members are configured as required, verify the configurations on the *Network > SD-WAN* screen.

SD-WAN

Name SD-WAN
 Type SD-WAN Interface
 Status 

SD-WAN Interface Members

<input checked="" type="button" value="+ Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	
Interfaces	Cost
 Zscaler-SF	5
 Zscaler-DC	10
 Internet_A (port1)	5
 Internet_B (port2)	10

After configuring SD-WAN interface members, we need to configure a static route that points to the *SD-WAN* interface.

To configure the static route:

- Go to *Network > Static Routes*, and click *Create New > IPv4 Static Route*. The *New Static Route* screen displays.
- Select *Subnet* for the *Destination* setting and enter 0.0.0.0/0.0.0.0 in the associated text input field.

3. Select *SD-WAN* as the *Interface* from the drop-down list.
4. Click *OK*.

New Static Route


Dynamic Gateway ⓘ ☐

Destination ⓘ

SubnetInternet Service

0.0.0.0/0.0.0.0

Interface


 SD-WAN


Comments

Write a comment...

0/255

Status

 Enabled

 Disabled

OK

Cancel














Configuring firewall policies

Configure firewall policies for both the overlay and underlay traffic as indicated below.

In this example, the overlay traffic does not require scanning, and the underlay traffic requires scanning. The firewall policies are configured accordingly.

To configure a firewall policy for the overlay traffic:

1. Go to *Policy & Objects > IPv4 Policy*, and click *Create New*. The *New Policy* screen displays.
2. Configure the fields as follows:
 - a. Enter a name in the *Name* field, like *Out Overlay Traffic* in this case.
 - b. Select the appropriate interface from the *Incoming Interface* field. In this case, it is `port3`.
 - c. Make sure the *Outgoing Interface* field is set to the *Zscaler-SF* and *Zscaler-DC* interfaces.

Name ⓘ	Out Overlay Traffic
Incoming Interface	 B01_LAN (port3)  +
Outgoing Interface	 Zscaler-DC   Zscaler-SF  +
Source	 B01_LAN  +
Destination	 all  +
Schedule	 always ▼
Service	 ALL  +
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

- d. Since the overlay traffic does not require scanning, all the *Security Profiles* will remain turned off.

Firewall / Network Options

NAT ☒

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options PROT default

Security Profiles

AntiVirus ☐

Web Filter ☐

DNS Filter ☐

Application Control ☐

IPS ☐

File Filter ☐

SSL Inspection SSL no-inspection

Logging Options

Log Allowed Traffic ☒ Security Events All Sessions

Comments 0/1023














Enable this policy ☒

3. Click OK.

To configure a firewall policy for the underlay traffic:

1. Go to *Policy & Objects > IPv4 Policy*, and click *Create New*. The *New Policy* screen displays.
2. Configure the fields as follows:
 - a. Enter a name in the *Name* field, like *Out Underlay Traffic* in this case.
 - b. Select the appropriate interface from the *Incoming Interface* field. In this case, it is `port3`.

- c. Make sure the *Outgoing Interface* field is set to the *Internet_A* and *Internet_B* interfaces.

Name ⓘ	Out Underlay Traffic	
Incoming Interface	 B01_LAN (port3) 	
	+	
Outgoing Interface	<div> Internet_A (port1)   Internet_B (port2) </div>	
	+	
Source	 B01_LAN 	
	+	
Destination	 all 	
	+	
Schedule	 always ▼	
Service	 ALL 	
	+	
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY	
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based	

- d. Since the underlay traffic requires to be scanned, set the *Security Profiles* of *AntiVirus*, *DNS Filter*, *Application Control*, *IPS*, and *SSL Inspection* as turned on to scan the traffic.

Firewall / Network Options

NAT ☒

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options PROT default

Security Profiles

AntiVirus ☒ AV default

Web Filter ☐

DNS Filter ☒ DNS default

Application Control ☒ APP default

IPS ☒ IPS default

File Filter ☐

SSL Inspection SSL certificate-inspection

Logging Options

Log Allowed Traffic ☒ Security Events All Sessions

Comments 0/1023

Enable this policy ☒

3. Click OK.

Once created, verify the firewall policies by navigating to *Policy & Objects > IPv4 Policy*. The *Security Profiles* column indicates that the *Out Overlay Traffic* IPv4 policy is set up to not scan any traffic, while the *Out Underlay Traffic* IPv4 policy is set to scan all traffic as *SSL Inspection*, *IPS*, *Application Control*, *DNS Filter*, and *AntiVirus* profiles are all active.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
1	Out Overlay Traffic	B01_LAN (port3)	Zscaler-DC Zscaler-SF	B01_LAN	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	All
2	Out Underlay Traffic	B01_LAN (port3)	Internet_A (port1) Internet_B (port2)	B01_LAN	all	always	ALL	✓ ACCEPT	✓ Enabled	AV default DNS default APP default IPS default SSL certificate-inspection	All
0	Implicit Deny	any	any	all	all	always	ALL	✗ DENY			All

Configuring Performance SLA test

Configure a performance SLA test that will be tied to the SD-WAN interface members for the Zscaler ZENs.

To configure a Performance SLA test:

1. Go to *Network > Performance SLA*, and click *Create New*. The *New Performance SLA* screen displays.
2. Enter a name for the *Name* field like `Zscaler_VPNTEST` in this case.
3. Select *IPv4* from the *IP Version* field.
4. Select the *Protocol* to be *HTTP*.
5. The *Server* field is set to the URL `http://gateway.<zscaler-cloud>.net/vpntest` test page, where `<zscaler-cloud>` is to be replaced with your Zscaler cloud name.
6. In the *Participants* fields, add `Zscaler-DC` and `Zscaler-SF` SD-WAN interface members as participants.

New Performance SLA

Name:

IP Version: ☒ IPv4 ☐ IPv6

Protocol: ☐ Ping ☒ HTTP

Server:

Participants:

Zscaler-DC

Zscaler-SF

Enable probe packets: ☒

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 ☒

OK **Cancel**

7. Click **OK**.



When configuring the Performance SLA test using the GUI, you cannot configure the HTTP GET request. The *Server* field only accepts a valid FQDN. Use the CLI to configure the HTTP GET request.

To configure a Performance SLA test using the CLI:

```
config system virtual-wan-link
  config health-check
    edit "Zscaler_VPNTEST"
      set server "gateway.<zscaler-cloud>.net"
      set protocol http
      set http-get "/vpntest"
      set interval 10000
      set failtime 10
      set members 2 3
      config sla
        edit 1
          set latency-threshold 250
          set jitter-threshold 100
          set packetloss-threshold 5
        next
      end
    next
  end
end
end
```

Configuring SD-WAN rules

Configure SD-WAN rules that will tie the Performance SLA probe (Zscaler_VPNTEST) to each of the SD-WAN members with the *Lowest Cost (SLA)* strategy selected to determine which ZEN will be the active-primary and which one will be the standby-secondary.

To configure an SD-WAN rule:

1. Go to *Network > SD-WAN Rules*, and click *Create New*. The *Priority Rule* screen displays.
2. Enter a name in the *Name* field, like `HTTPS-Zscaler-Out` in this case.
3. Select the *IP Version* to be *IPv4*.
4. Select the *Source* and *Destination* addresses to be `all`.
5. Select the *Protocol* to be *TCP*, and the *Port Range* to be `443-443`.

Priority Rule

Name:

IP Version: ☒ IPv4 ☐ IPv6

Source

Source address: + ×

User group: +

Destination

Address: + ×

Protocol number: ☒ TCP ☐ UDP ☐ ANY

Port range: -

Internet Service i: +

Application i: +

6. Select the *Lowest Cost (SLA)* strategy for the outgoing interfaces. It determines which ZEN will be the active-primary and which one will be the standby-secondary.
7. Specify the preference for the outgoing interfaces in the *Interface preference* field by adding `Zscaler-SF` and `Zscaler-DC` in the preferred order.

8. Specify the *Required SLA target* by adding the `Zscaler_VPNTEST` performance SLA test we created earlier.

Outgoing Interfaces

Strategy

Manual

Best Quality

Lowest Cost (SLA)

Maximize Bandwidth (SLA)

Interface preference

Zscaler-SF

Zscaler-DC

+

Required SLA target

Zscaler_VPNTEST

+

Status

Enable

Disable

OK

Cancel

9. Click **OK**.

Configure similar SD-WAN rules for HTTP, and non-web traffic. In our example, the non-web traffic is steered to the underlays using the *Best Quality* strategy.

Once configured, verify your SD-WAN rules by navigating to *Network > SD-WAN Rules*:

+ Create New

Edit

Delete

Search

Q

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	HTTPS_Zscaler_Out	all	all	SLA	Zscaler-SF Zscaler-DC
2	HTTP_Zscaler_Out	all	all	SLA	Zscaler-SF Zscaler-DC
3	Non-Web_Traffic	all	all	Latency	Internet_A (port1) Internet_B (port2)
Implicit 1					
	sd-wan	all all	all all	Source IP	any

Verifying configuration with Zscaler test page

To verify your configuration with Zscaler, request a verification page via the URL <https://ip.zscaler.com>.

If you are routing traffic via a Zscaler proxy service, the URL <https://ip.zscaler.com> will respond with a message confirming it.

You are accessing this host via a Zscaler proxy hosted at Los Angeles in the zscalertwo.net cloud.

Your request is arriving at this server from the IP address 104.129.198.69

The Zscaler proxy virtual IP is 104.129.198.34.

The Zscaler hostname for this proxy appears to be zs2-qla1a1.

If not, it will respond with an appropriate message.

The request received from you did not have an XFF header, so you are quite likely not going through the Zscaler proxy service.

Your request is arriving at this server from the IP address 209.37.255.2

Your Gateway IP Address is most likely 209.37.255.2

Results

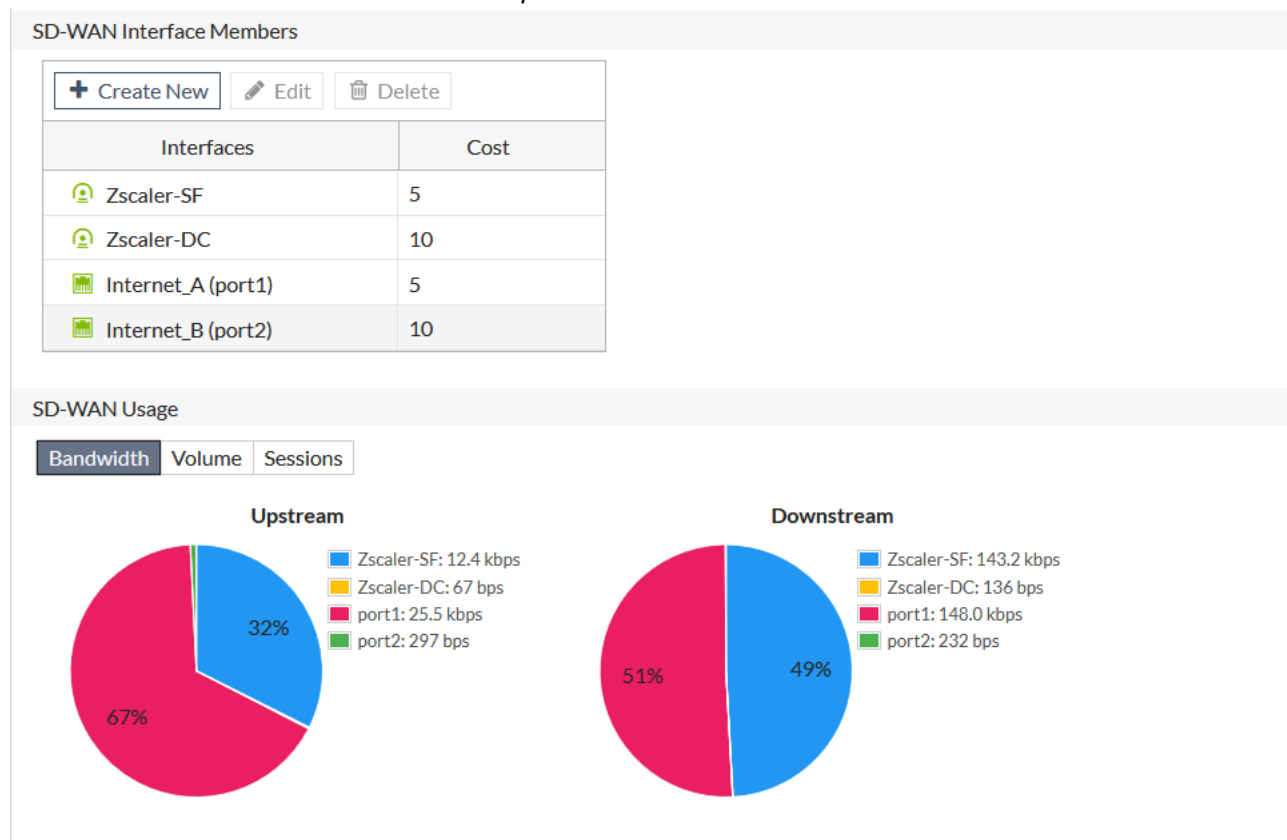
The following GUI pages show the function of the Fortinet secure SD-WAN deployed with Zscaler Internet Access (ZIA) and can be used to confirm that it is setup and running correctly:

- [Interface usage on page 24](#)
- [IPsec status on page 25](#)
- [Performance SLA on page 26](#)
- [Routing table on page 27](#)
- [Firewall policy on page 27](#)
- [Top sources on page 27](#)

Interface usage

Go to *Network > SD-WAN* to review the SD-WAN interface usage.

Select *Bandwidth* to see donut charts of the *Upstream* and *Downstream* bandwidth for each interface.



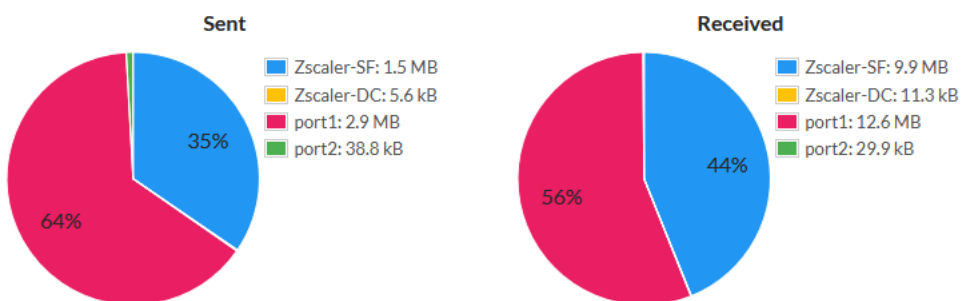
Select *Volume* to see donut charts of the received and sent bytes over the interfaces.

SD-WAN Usage

Bandwidth

Volume

Sessions



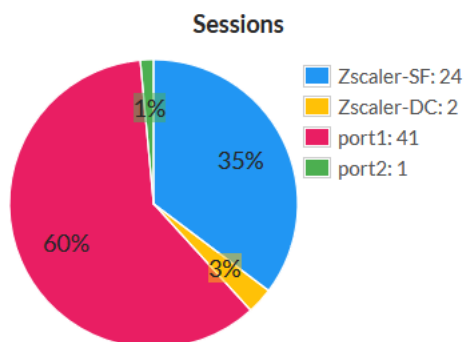
Select *Sessions* to see a donut chart of the number of active sessions on each interface.

SD-WAN Usage

Bandwidth

Volume

Sessions



IPsec status

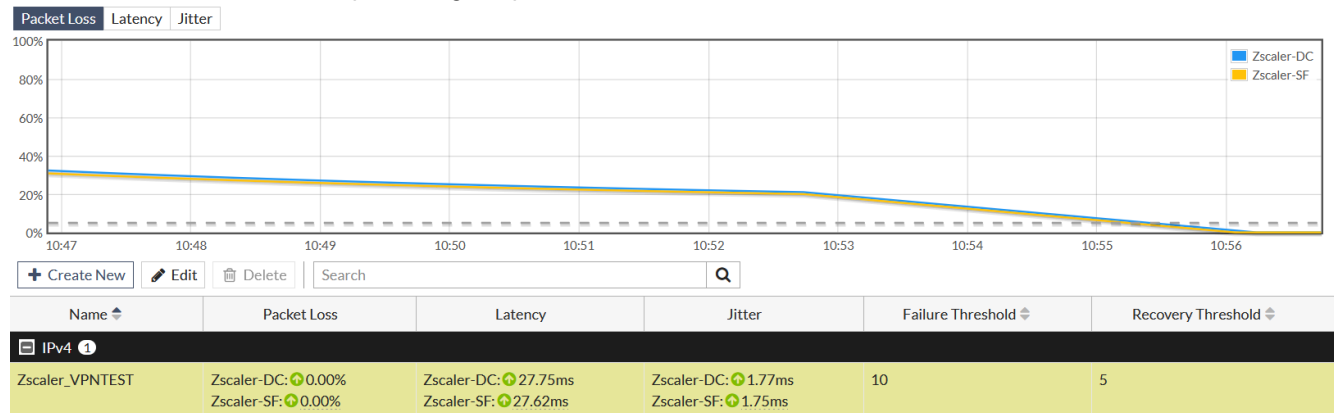
Go to *Monitor > IPsec Monitor* to review all IPsec tunnels.

Reset Statistics		Bring Up		Bring Down		Locate on VPN Map							
Name		Remote Gateway		Peer ID		Incoming Data		Outgoing Data		Phase 1		Phase 2 Selectors	
Custom 3													
To-HQ-MPLS		192.168.0.1				341.22 kB		150.97 kB		To-HQ-MPLS		To-HQ-MPLS	
Zscaler-DC		10.100.65.101				53.87 MB		12.35 MB		Zscaler-DC		Zscaler-DC	
Zscaler-SF		10.100.64.101				807.08 MB		49.97 MB		Zscaler-SF		Zscaler-SF	

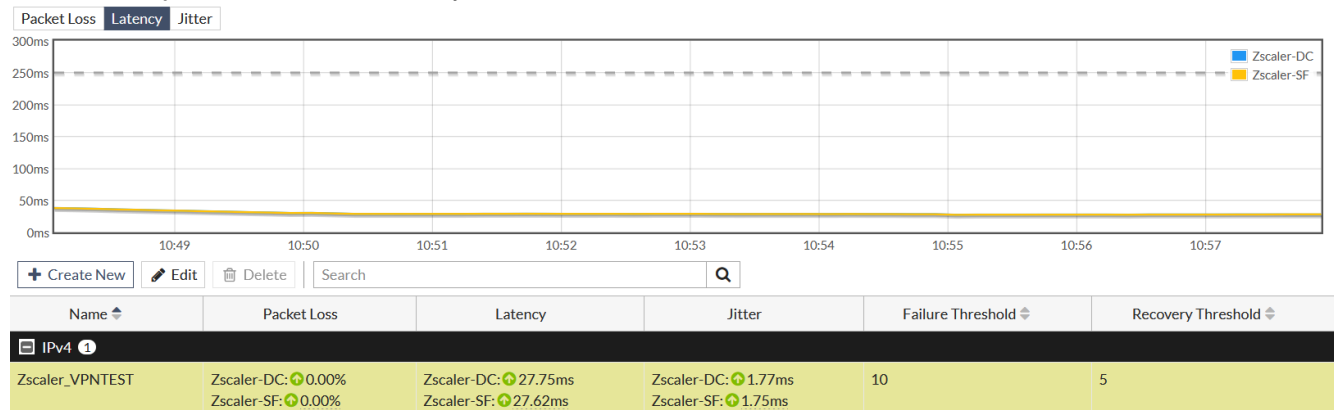
Performance SLA

Go to **Network > Performance SLA** and select the SLA from the table (Zscaler_VPNTTEST in this example) to view the packet loss, latency, and jitter on each SD-WAN member in the health check server.

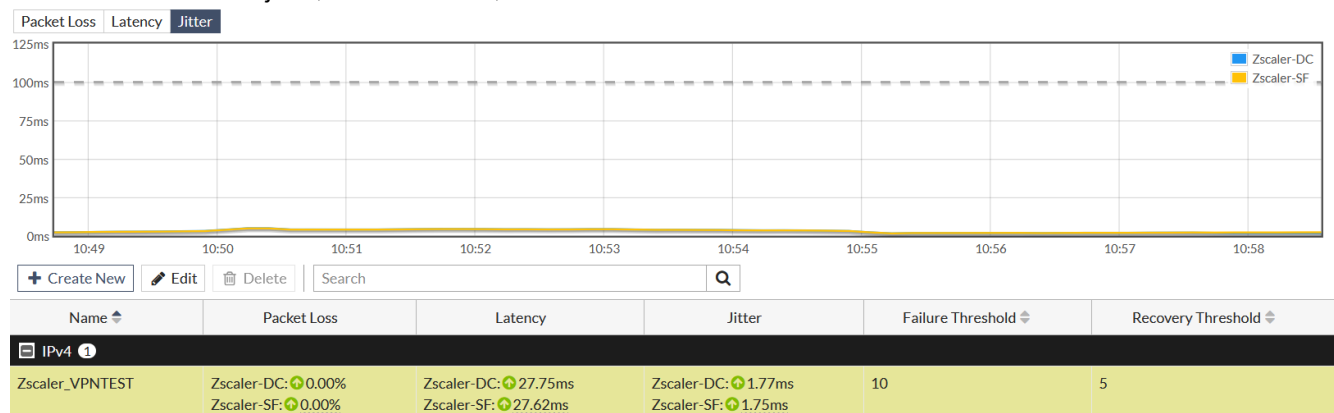
Select **Packet Loss** to see the percentage of packets lost for each member.



Select **Latency** to see the current latency, in milliseconds, for each member.



Select **Jitter** to see the jitter, in milliseconds, for each member.



Routing table

Go to *Monitor > Routing Monitor* and select *Static & Dynamic* to review all static and dynamic routes.

Refresh

Route Lookup

View

Create Address

Search

Static & Dynamic

Policy

Branch_Office_01

Type	Network	Gateway IP	Interfaces	Distance
IPv4 49				
Static	0.0.0.0/0	10.0.10.1	Zscaler-SF	1
Static	0.0.0.0/0	10.10.11.1	Zscaler-DC	1
Static	0.0.0.0/0	10.100.67.1	Internet_A (port1)	1
Static	0.0.0.0/0	10.100.67.9	Internet_B (port2)	1
Connected	10.0.10.0/24	0.0.0.0	Zscaler-SF	0
Connected	10.0.10.2/32	0.0.0.0	Zscaler-SF	0
Connected	10.0.11.0/24	0.0.0.0	Zscaler-DC	0
Connected	10.0.11.2/32	0.0.0.0	Zscaler-DC	0
Connected	10.1.0.0/24	0.0.0.0	B01_LAN (port3)	0
Connected	10.1.0.2/32	0.0.0.0	B01_LAN (port3)	0
Connected	10.1.0.3/32	0.0.0.0	B01_LAN (port3)	0
Connected	10.1.100.0/24	0.0.0.0	Guest Network (vsw.port6)	0
BGP	10.2.0.0/24	10.0.10.3	Zscaler-SF	200
BGP	10.2.0.0/24	10.0.11.3	Zscaler-DC	200
Connected	10.100.7.0/24	0.0.0.0	port7	0
Connected	10.100.55.0/24	0.0.0.0	Management (port4)	0
Static	10.100.64.0/24	10.100.67.1	Internet_A (port1)	10
Static	10.100.65.0/24	10.100.67.9	Internet_B (port2)	10

Firewall policy

Go to *Policy & Objects > IPv4 Policy* to review the firewall policy.

<div><div>+ Create New</div><div> Edit</div><div> Delete</div><div><div><div> Policy Lookup</div><div>Search</div><div></div></div></div></div>		Interface Pair View		By Sequence							
ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
1	Out Overlay Traffic	B01_LAN (port3)	Zscaler-DC Zscaler-SF	B01_LAN	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All
2	Out Underlay Traffic	B01_LAN (port3)	Internet_A (port1) Internet_B (port2)	B01_LAN	all	always	ALL	ACCEPT	Enabled	<div><div> AV default</div><div> DNS default</div><div> APP default</div><div> IPS default</div><div> SSL certificate-inspection</div></div>	All
0	Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	DENY			All

Top sources

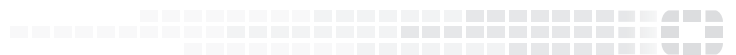
Go to *FortiView > All Sessions* to confirm that web traffic (ports 443 and 80) flows through the right overlay interface member, and non-web traffic flows through the right underlay interface member.

Results

FortiGate: Branch_Office_01 ✕ 📄										
Add Filter										
Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	Packets	Duration (seconds)	Destination Interface
10.1.0.102	JOHNLOCUS	100.21.29.17	SSH	TCP	62077	22	10.72 kB	85	1m 42s	Internet_A (port1)
10.1.0.102	JOHNLOCUS	212.13.197.231	HTTPS.BROWSER	TCP	62088	443	985 B	9	5s	Zscaler-SF
10.1.0.102	JOHNLOCUS	212.13.197.231	HTTPS.BROWSER	TCP	62087	443	43.76 kB	46	5s	Zscaler-SF
10.1.0.102	JOHNLOCUS	10.100.88.5	TCP/8013	TCP	62086	8013	104 B	2	8s	Internet_A (port1)



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.