

FINAL PROJECT (DEPI)



INTRODUCTION TO THE PROJECT

This project implements and tests three VPN solutions on FortiGate : SSL VPN for remote access, IPsec VPN for site-to-site connectivity, and SD-WAN for link optimization. Each solution was configured and verified through functional test results.



TEAM MEMBERS

<< HOSSAM MOHAMED >>

<< AHMED MAHMOUD >>

PROJECT PHASES

01.

configuring ssl vbn with
test results (HOSSAM)

02.

Establish an IPsec VPN
tunnel between two
FortiGate devices
(AHMED)



03.

Configure SD-WAN to
optimize VPN traffic
(HOSSAM)

04.

Create final report
detailing VPN
configurations (AHMED)

05.

Create a presentation
(HOSSAM)

01.

**configuring ssl vbn with
test results (HOSSAM)**

- 1- create user group and add local user to it**
- 2-configure SSL-VPN settings**
- 3- configure SSL-VPN Portal**
- 4- create firewall policy**
- 5- configure FortiClient**

TEST RESULTS FOR SSL VPN

Local-FortiGate

Dashboard Network Policy & Objects Security Profiles VPN User & Authentication WiFi Controller System Security Fabric Log & Report Forward Traffic Local Traffic Sniffer Traffic System Events Security Events Reports Log Settings

FORTINET v7.4.1

Logs

Date/Time 2025-08-05 10:59:49 -> 2025-08-05 11:04:... Search VPN Events Disk custom Details

Date/Time	Level	Action	Status	Message	VPN Tunnel
2025/08/05 11:04:09	Information	ssl-new-con		SSL new connection	
2025/08/05 11:04:09	Error	ssl-alert		SSL alerts	
2025/08/05 11:04:09	Information	tunnel-down		SSL tunnel shutdown	
2025/08/05 11:04:08	Information	tunnel-down		SSL tunnel shutdown	
2025/08/05 11:02:47	Error	ssl-alert		SSL alerts	
2025/08/05 11:02:27	Information	tunnel-up		SSL tunnel established	
2025/08/05 11:02:26	Information	ssl-new-con		SSL new connection	
2025/08/05 11:02:26	Information	tunnel-up		SSL tunnel established	
2025/08/05 11:02:26	Information	ssl-new-con		SSL new connection	

Log Details

Reason: tunnel established

Security

Level: Information

Event

Remote IP: 10.200.3.1

Tunnel ID: 1,752,213,590

Tunnel IP: 10.212.134.200

Tunnel Type: ssl-tunnel

Message: SSL tunnel established

Other

Log event original timestamp: 1754416947577007600

Timezone: -0700

Log ID: 0101039947

Type: event

Sub Type: vpn

Duration

Connected < 10 Mi... 1

Connection Mode

Tunnel 1 Total

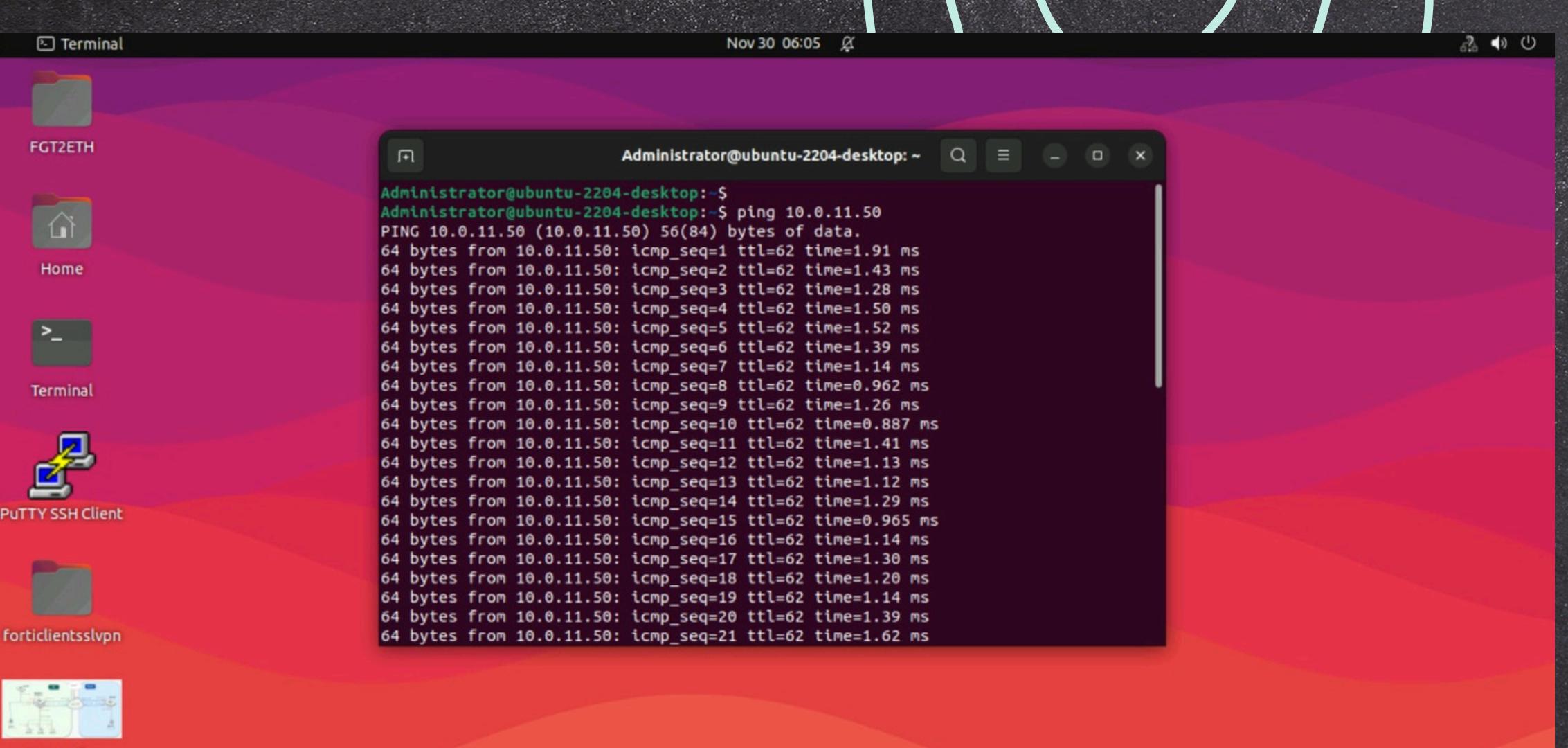
Locate on VPN Map View Connection Details Search

User Group	Remote Host	Duration	Connections	Bytes
SSL_VPN_USERS	10.200.3.1	1m 27s	1 Tunnel Connections	2.99 kB

02. Establish an IPsec VPN tunnel between two FortiGate devices (AHMED)

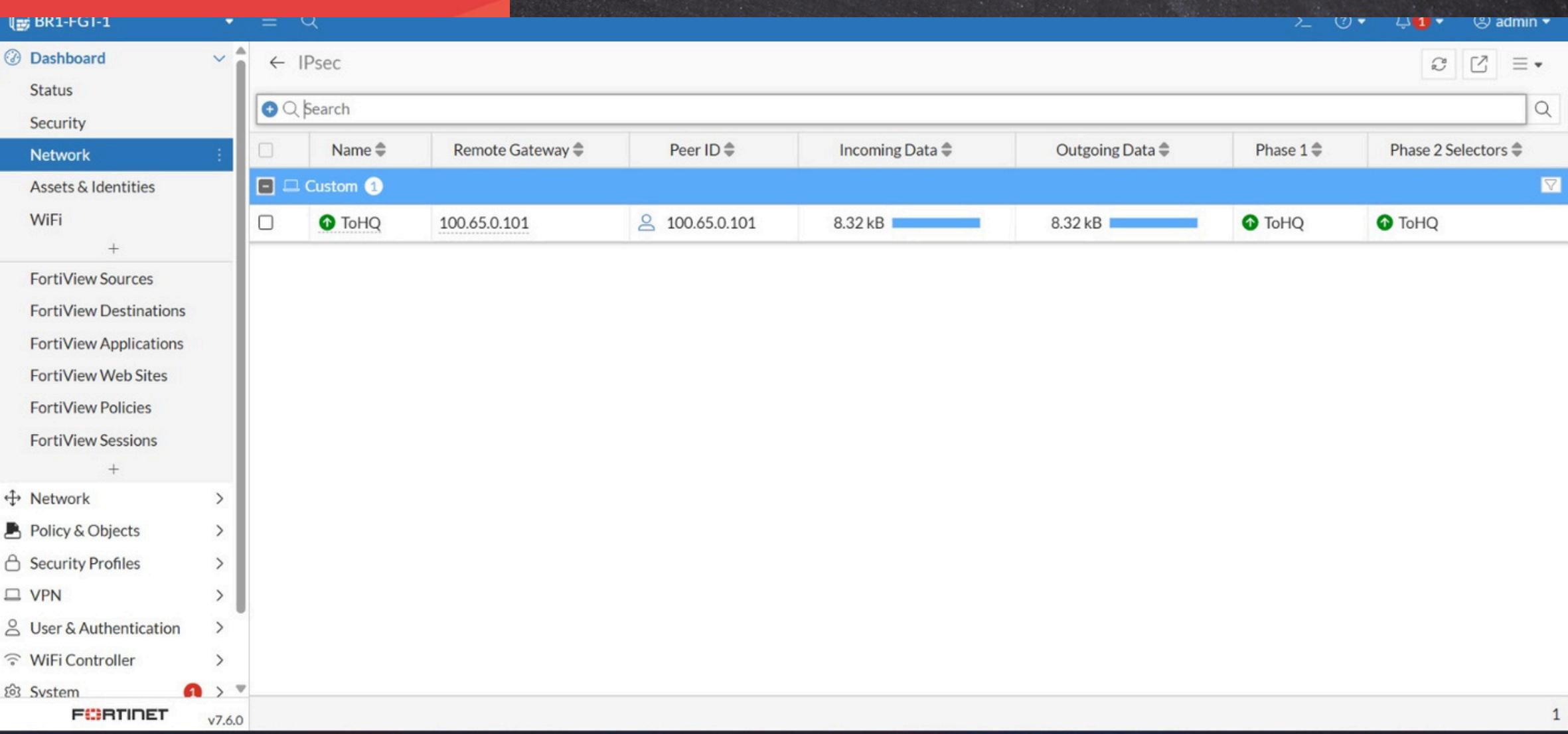
- 1- Configure Phase 1 & Phase 2 Settings**
- 2-Create Firewall Policies for VPN Traffic**
- 3- Add a Static Route for VPN Traffic**
- 4- Configure Phase 1 & Phase 2 on the Second FortiGate**
- 5- Bring Up and Monitor the VPN Tunnel**
- 6- Test Connectivity Between Sites**

TEST RESULTS FOR IPSEC



A screenshot of a Ubuntu desktop environment. A terminal window titled "Administrator@ubuntu-2204-desktop: ~" is open, displaying the output of a "ping" command to 10.0.11.50. The terminal shows 21 ICMP echo requests sent, all with a ttl of 62 and times ranging from 0.887 ms to 1.91 ms.

```
Administrator@ubuntu-2204-desktop:~$ ping 10.0.11.50
PING 10.0.11.50 (10.0.11.50) 56(84) bytes of data.
64 bytes from 10.0.11.50: icmp_seq=1 ttl=62 time=1.91 ms
64 bytes from 10.0.11.50: icmp_seq=2 ttl=62 time=1.43 ms
64 bytes from 10.0.11.50: icmp_seq=3 ttl=62 time=1.28 ms
64 bytes from 10.0.11.50: icmp_seq=4 ttl=62 time=1.50 ms
64 bytes from 10.0.11.50: icmp_seq=5 ttl=62 time=1.52 ms
64 bytes from 10.0.11.50: icmp_seq=6 ttl=62 time=1.39 ms
64 bytes from 10.0.11.50: icmp_seq=7 ttl=62 time=1.14 ms
64 bytes from 10.0.11.50: icmp_seq=8 ttl=62 time=0.962 ms
64 bytes from 10.0.11.50: icmp_seq=9 ttl=62 time=1.26 ms
64 bytes from 10.0.11.50: icmp_seq=10 ttl=62 time=0.887 ms
64 bytes from 10.0.11.50: icmp_seq=11 ttl=62 time=1.41 ms
64 bytes from 10.0.11.50: icmp_seq=12 ttl=62 time=1.13 ms
64 bytes from 10.0.11.50: icmp_seq=13 ttl=62 time=1.12 ms
64 bytes from 10.0.11.50: icmp_seq=14 ttl=62 time=1.29 ms
64 bytes from 10.0.11.50: icmp_seq=15 ttl=62 time=0.965 ms
64 bytes from 10.0.11.50: icmp_seq=16 ttl=62 time=1.14 ms
64 bytes from 10.0.11.50: icmp_seq=17 ttl=62 time=1.30 ms
64 bytes from 10.0.11.50: icmp_seq=18 ttl=62 time=1.20 ms
64 bytes from 10.0.11.50: icmp_seq=19 ttl=62 time=1.14 ms
64 bytes from 10.0.11.50: icmp_seq=20 ttl=62 time=1.39 ms
64 bytes from 10.0.11.50: icmp_seq=21 ttl=62 time=1.62 ms
```



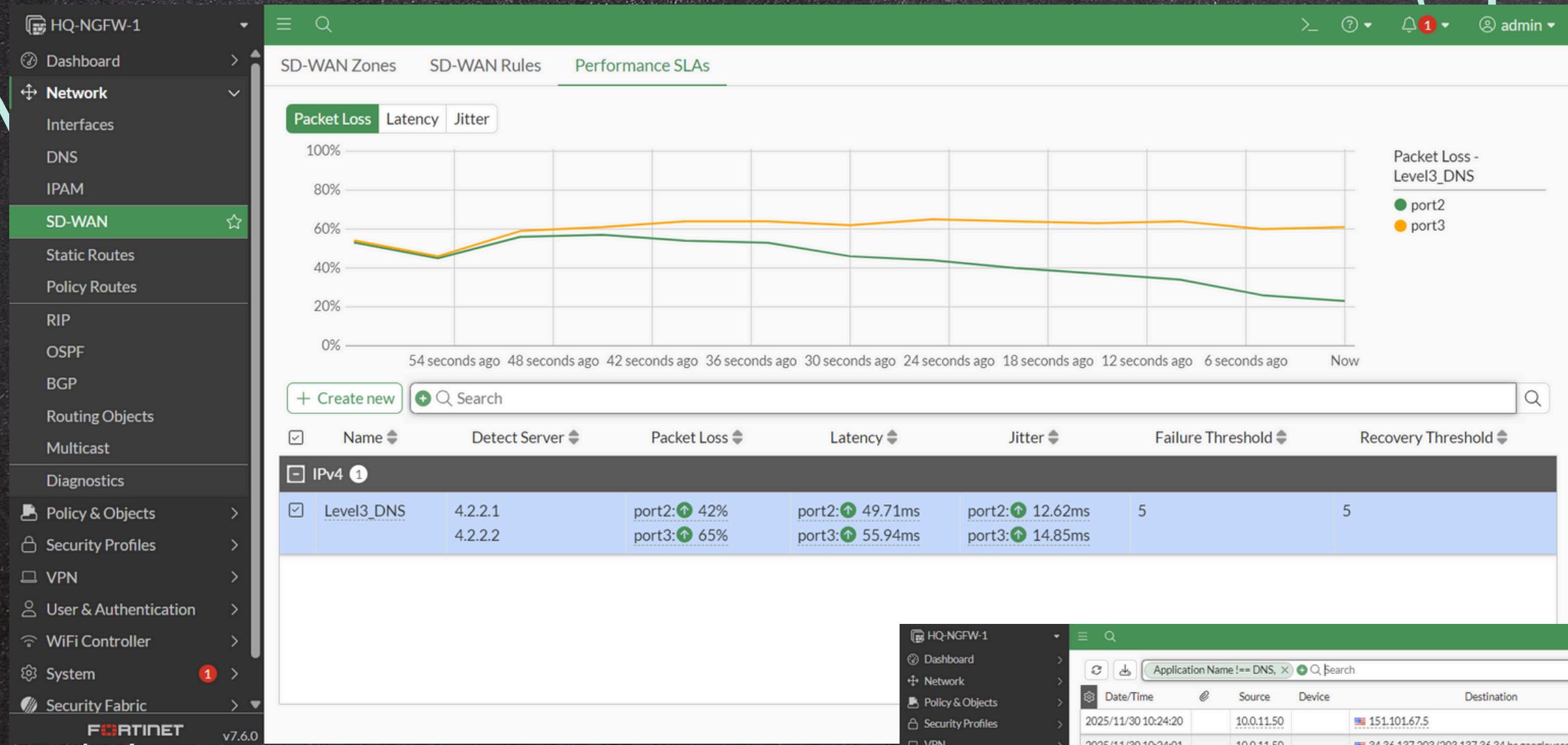
A screenshot of the Fortinet FortiView interface. The left sidebar shows the navigation menu under "BR1-FGT-1". The "Network" section is selected, showing sub-options like "Assets & Identities", "WiFi", and "FortiView Sources". The main content area is titled "IPsec" and displays a table of sessions. One session is listed: "Custom 1" with "Name" set to "ToHQ", "Remote Gateway" to "100.65.0.101", "Peer ID" to "100.65.0.101", "Incoming Data" at 8.32 kB, and "Outgoing Data" at 8.32 kB. Both "Phase 1" and "Phase 2 Selectors" are set to "ToHQ".

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
ToHQ	100.65.0.101	100.65.0.101	8.32 kB	8.32 kB	ToHQ	ToHQ

03. Configure SD-WAN to optimize VPN traffic (HOSSAM)

- 1- Deleting all policies related to wan ports**
- 2-configure SD-WAN members and zone**
- 3- create performance SLA**
- 4- create SD-WAN Rules**
- 5- configure static route for SD-WAN**
- 6- create firewall policy for SD-WAN**

TEST RESULTS FOR SD-WAN



HQ-NGFW-1

Application Name != DNS

Date/Time Source Device Destination Application Name Result Policy ID Destination Interface SD-WAN Quality SD-WAN Rule Name

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
2025/11/30 10:24:20	10.0.11.50		151.101.67.5	SSL	✓ Accept (134.19 kB / 16.11 MB)	DIA(1)	port2	Seq_num(1 port2 Underlay), alive, selected	Critical-DIA
2025/11/30 10:24:01	10.0.11.50		34.36.137.203 (203.137.36.34.bc.googleusercontent.com)	SSL	✓ Accept (UTM Allowed)	DIA(1)	port2		
2025/11/30 10:23:26	10.0.11.50		185.125.190.56 (prod-ntp-3.ntp4.ps5.canonical.com)	NTP	✓ Accept (UTM Allowed)	DIA(1)	port2		
2025/11/30 10:23:04	10.0.11.50		34.107.243.93 (93.243.107.34.bc.googleusercontent.com)	SSL	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:22:20	10.0.11.50		151.101.67.5	SSL	✓ Accept (133.06 kB / 16.11 MB)	DIA(1)	port2	Seq_num(1 port2 Underlay), alive, selected	Critical-DIA
2025/11/30 10:22:08	10.0.11.50		142.250.200.98 (mad41s13-in-f2.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:22:04	10.0.11.50		142.250.200.98 (mad41s13-in-f2.1e100.net)	HTTPS.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:22:03	10.0.11.50		142.250.200.98 (mad41s13-in-f2.1e100.net)	HTTPS.BROWSER	✓ Accept (2.65 kB / 29.71 kB)	DIA(1)	port3		
2025/11/30 10:21:57	10.0.11.50		142.250.200.142 (mad41s14-in-f14.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:51	10.0.11.50		34.160.90.233 (233.90.160.34.bc.googleusercontent.com)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:49	10.0.11.50		151.101.1.91	HTTPS.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:49	10.0.11.50		35.190.72.216 (216.72.190.35.bc.googleusercontent.com)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:47	10.0.11.50		142.250.200.67 (mad07s24-in-f3.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:46	10.0.11.50		142.250.200.67 (mad07s24-in-f3.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:45	10.0.11.50		57.144.252.128 (xx-fbcndn-shv-01-atl3.fbcndn.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port2		
2025/11/30 10:21:44	10.0.11.50		142.251.140.227 (lcmafa-ab-in-f3.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port2		
2025/11/30 10:21:44	10.0.11.50		142.250.184.162 (mad07s23-in-f2.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:44	10.0.11.50		13.33.243.10 (server-13-33-243-10.mad53.r.cloudfront.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:44	10.0.11.50		142.251.140.225 (dia01s03-in-f1.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port2		
2025/11/30 10:21:43	10.0.11.50		142.250.200.98 (mad41s13-in-f2.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:41	10.0.11.50		151.101.65.229	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:41	10.0.11.50		173.194.76.95 (ws-in-f95.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port2		
2025/11/30 10:21:39	10.0.11.50		57.144.252.1 (edge-star-mini-shv-01-atl3.facebook.com)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port3		
2025/11/30 10:21:39	10.0.11.50		151.101.131.5	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port2	Seq_num(1 port2 Underlay), alive, selected	Critical-DIA
2025/11/30 10:21:38	10.0.11.50		173.194.76.84 (ws-in-f84.1e100.net)	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port2		
2025/11/30 10:21:38	10.0.11.50		151.101.67.5	HTTP.BROWSER	✓ Accept (UTM Allowed)	DIA(1)	port2	Seq_num(1 port2 Underlay), alive, selected	Critical-DIA

THANK YOU!