SSL VPN Configuration Documentation

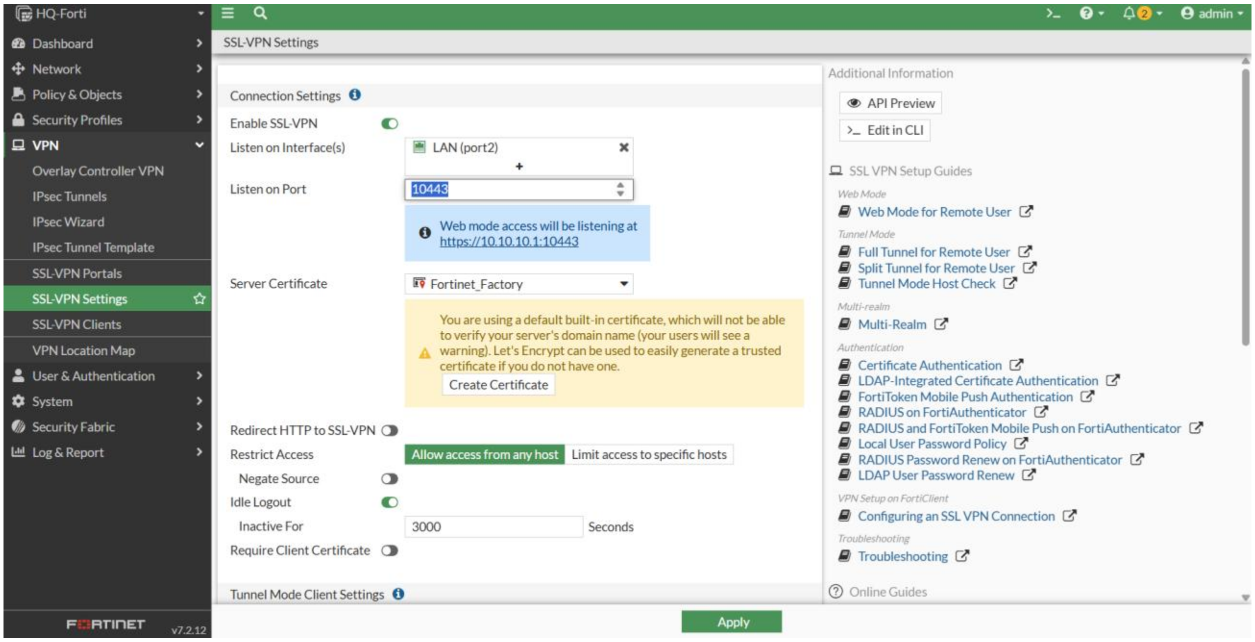
3. HQ FortiGate SSL VPN Configuration

Step 1: SSL VPN Settings

Navigate to **VPN → SSL-VPN Settings**

Configuration:

- **Listen on Interface:** port2 (LAN)
- **Listen on Port:** 10443 (HTTPS)
- **Server Certificate:** Fortinet_Factory
- **Idle Timeout:** 3000 seconds
- **Tunnel Mode IP Pools:** SSLVPN_TUNNEL_ADDR1 (10.212.134.200 - 10.212.134.210)
- **IPv6 Pools:** SSLVPN_TUNNEL_IPv6_ADDR1 (fdff:ffff::/120)
- **Default Portal:** full-access



SSL-VPN Settings

Connection Settings

Enable SSL-VPN ●

Listen on Interface(s): LAN (port2)

Listen on Port: 10443

Web mode access will be listening at https://10.10.10.1:10443

Server Certificate: Fortinet_Factory

You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one.

Create Certificate

Redirect HTTP to SSL-VPN ○

Restrict Access: [✓ Allow access from any host] Limit access to specific hosts

Negate Source ○

Idle Logout ●

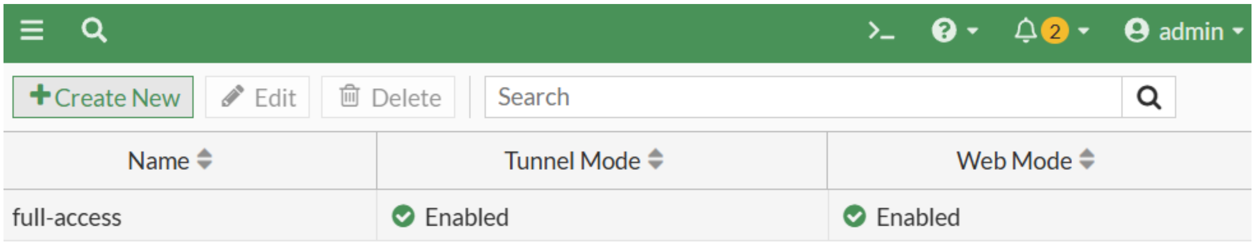
Inactive For: 3000 Seconds

Require Client Certificate ○

Tunnel Mode Client Settings

Portal Settings (full-access):

- Tunnel Mode: Enabled
- IPv6 Tunnel Mode: Enabled
- Web Mode: Enabled
- **IP Pools:** SSLVPN_TUNNEL_ADDR1
- **IPv6 Pools:** SSLVPN_TUNNEL_IPv6_ADDR1



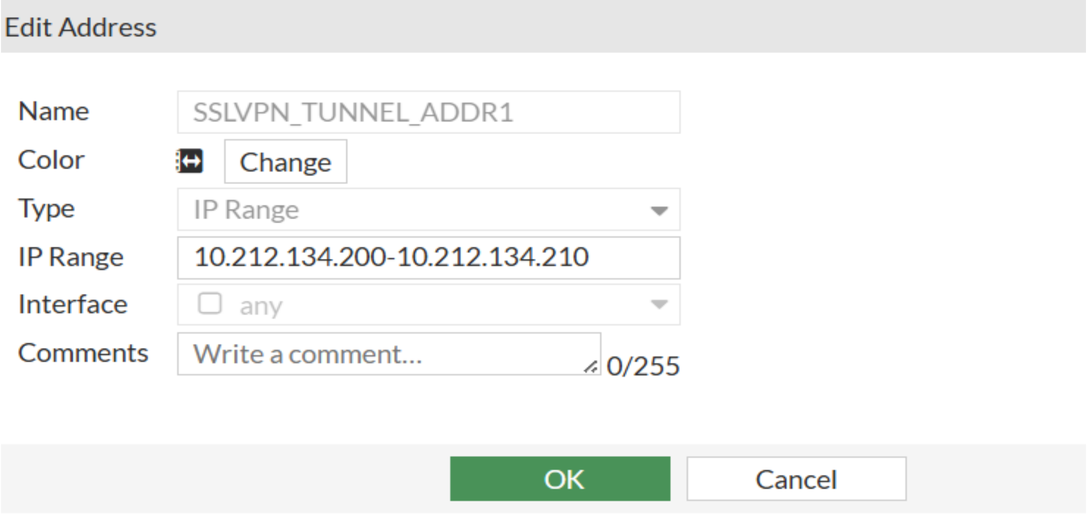
Name	Tunnel Mode	Web Mode
full-access	✓ Enabled	✓ Enabled

Step 2: Create IP Pool for SSL VPN Users

Navigate to **Policy & Objects → Addresses**

Create New IP Pool:

- **Name:** SSLVPN_TUNNEL_ADDR1
- **Type:** IP Range
- **Start IP:** 10.212.134.200
- **End IP:** 10.212.134.210


Edit Address

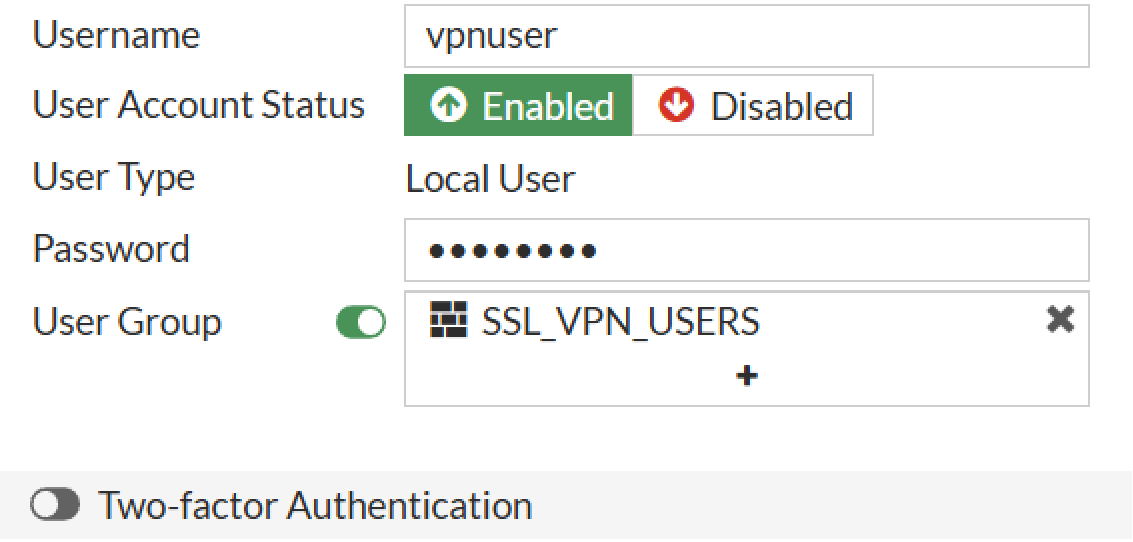
Name	SSLVPN_TUNNEL_ADDR1
Color	Change
Type	IP Range
IP Range	10.212.134.200-10.212.134.210
Interface	□ any
Comments	Write a comment... 0/255

Step 3: Create User Account

Navigate to **User & Authentication → User Definition**

Create New User:

- **Username:** vpnuser
- **Type:** Local User
- **Password:** (Set secure password)
- **Status:** Enabled



Username	vpnuser
User Account Status	Enabled / Disabled
User Type	Local User
Password	••••••••
User Group	SSL_VPN_USERS

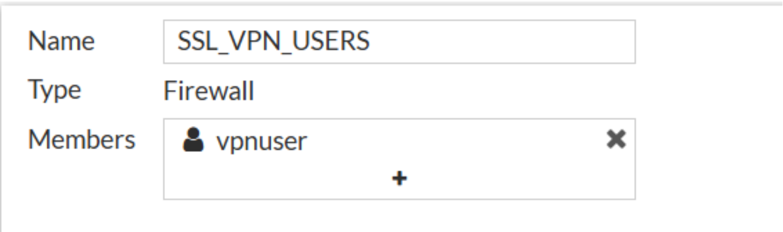
Two-factor Authentication

Step 4: Create User Group

Navigate to **User & Authentication → User Groups**

Create New Group:

- **Name:** SSL_VPN_USERS
- **Type:** Firewall
- **Members:** vpnuser



Name	SSL_VPN_USERS
Type	Firewall
Members	vpnuser

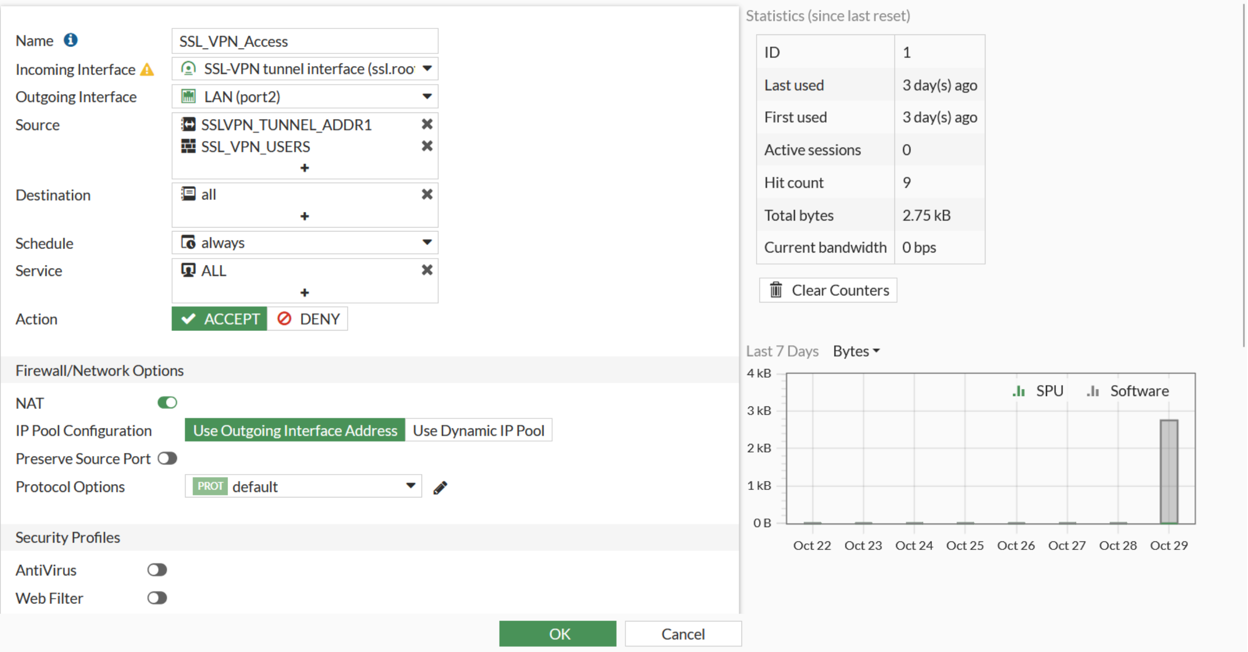
Step 5: Firewall Policy Configuration

SSL VPN Access Policy

Navigate to **Policy & Objects → Firewall Policy**

Policy Details:

- **Name:** SSL_VPN_Access
- **Incoming Interface:** SSL_VPN tunnel interface (ssl.root)
- **Outgoing Interface:** LAN (port2)
- **Source:** SSLVPN_TUNNEL_ADDR1
- **Destination:** all
- **Schedule:** always
- **Service:** ALL
- **Action:** ACCEPT
- **NAT:** Enabled (Use Outgoing Interface Address)
- **Security Profiles:** AntiVirus, Web Filter enabled



Name	SSL_VPN_Access
Incoming Interface	SSL-VPN tunnel interface (ssl.roo
Outgoing Interface	LAN (port2)
Source	SSLVPN_TUNNEL_ADDR1 SSL_VPN_USERS
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT / DENY

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	○

Statistics (since last reset)

ID	1
Last used	3 day(s) ago
First used	3 day(s) ago
Active sessions	0
Hit count	9
Total bytes	2.75 kB
Current bandwidth	0 bps

Step 6: Web-Based Mode Testing

Test 5.1: SSL VPN Portal Access Test

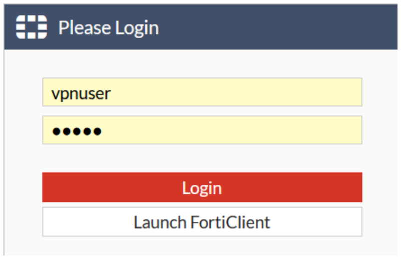
Verify web portal accessibility and authentication

- SSL-VPN portal accessible at https://192.168.32.135:10443 or <ip:port>
- Portal shows: "The SSL-VPN portal has been enabled for tunnel mode use only"
- FortiClient launch and download options available
- Connection history visible with previous sessions

Test 5.2: Web Portal Services Test

Test web-accessible services through portal

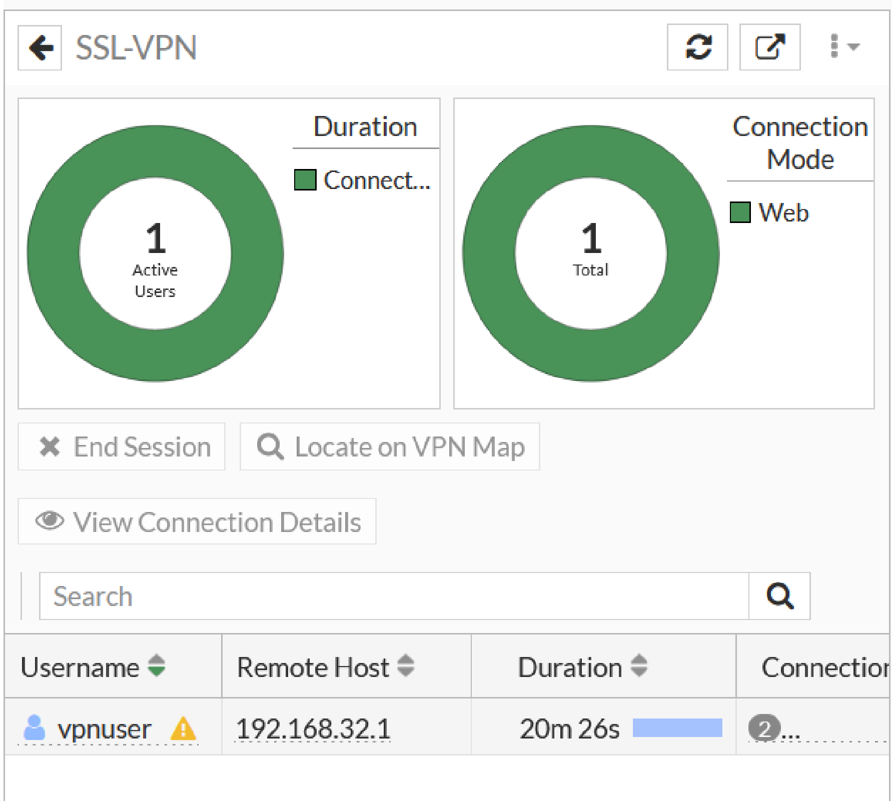
- Access to the VPN target
- Then login as a vpnuser
- View the details
- Verify login from the fortigate firewall GUI (Dashboard → Network)



Please Login

vpnuser

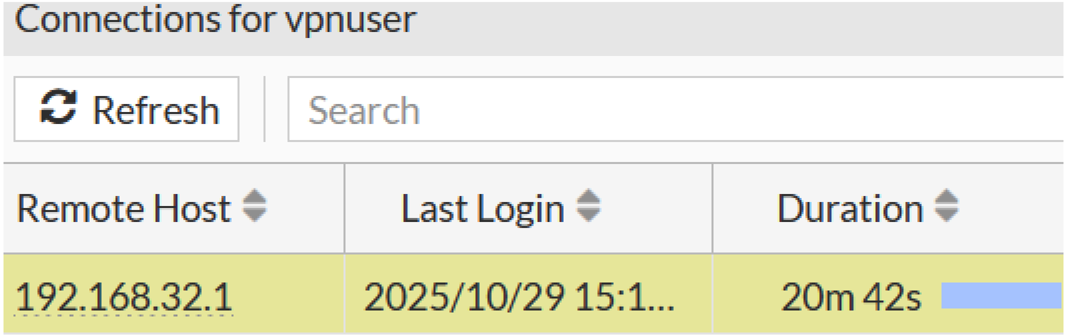
•••••



SSL-VPN

Username	Remote Host	Duration	Connectio
vpnuser ⚠	192.168.32.1	20m 26s	2...

- See the details to view that its web mode access on the SSL VPN



Connections for vpnuser

Remote Host	Last Login	Duration
192.168.32.1	2025/10/29 15:1...	20m 42s

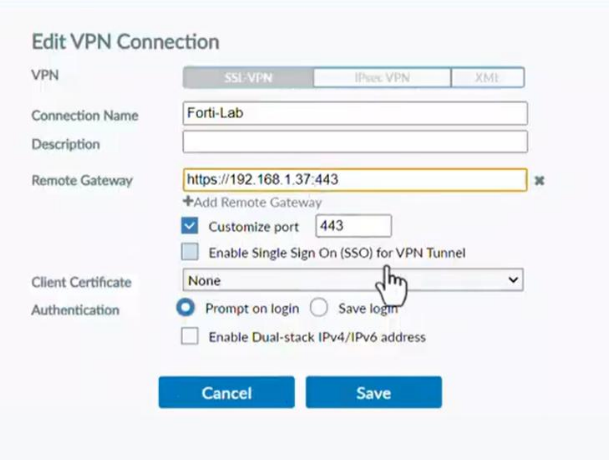
Step 7: FortiGate SSL VPN tunnel mode test

FortiClient Connection configuration

VPN Connection Settings

Connection Parameters:

- **VPN Name:**
- **Connection Type:** SSL-VPN
- **Remote Gateway:** https://<IP>:10443
- **Custom Port:** 10443
- **Authentication:** Username/Password
- **Username:** vpnuser
- **Single Sign-On:** Disabled
- **Client Certificate:** None
- **Dual-stack IPv4/IPv6:** Enabled



Edit VPN Connection

VPN: SSL-VPN | IPsec VPN | XML

Connection Name: Forti-Lab

Description:

Remote Gateway: https://192.168.1.37:443

+Add Remote Gateway

☑ Customize port 443

□ Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: None

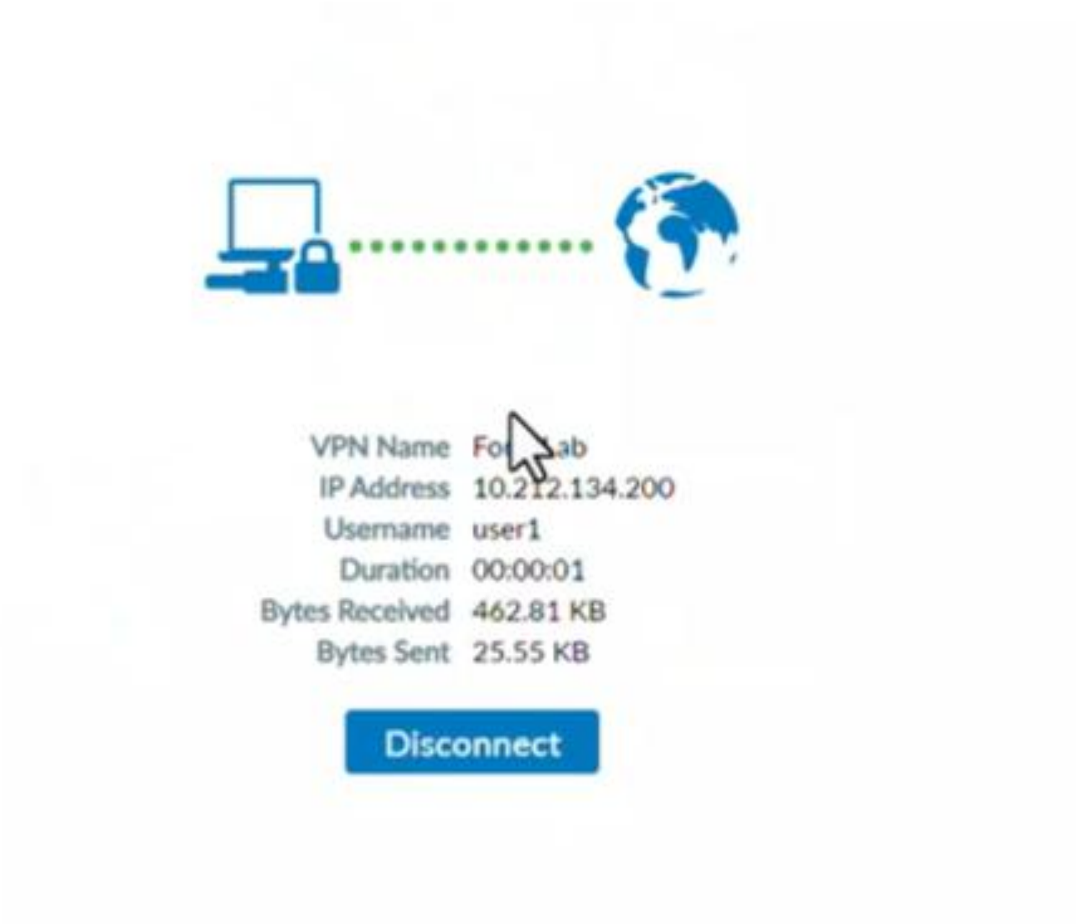
Authentication: ● Prompt on login ○ Save login

□ Enable Dual-stack IPv4/IPv6 address

Step 8: connection and monitoring

In this step, after establishing the connection using **tunnel mode**, I selected **Forti-Lab** and tested the setup using the **VPN user** I had previously created.
As shown in the image, the monitoring interface displays several key details for each connected user:

1. **Username** – identifies the authenticated VPN user.
2. **IP Address** – shows the assigned IP for the VPN session.
3. **Connection Duration** – indicates how long the user has been connected.
4. **Bytes Sent and Received** – displays the amount of data transmitted during the session.



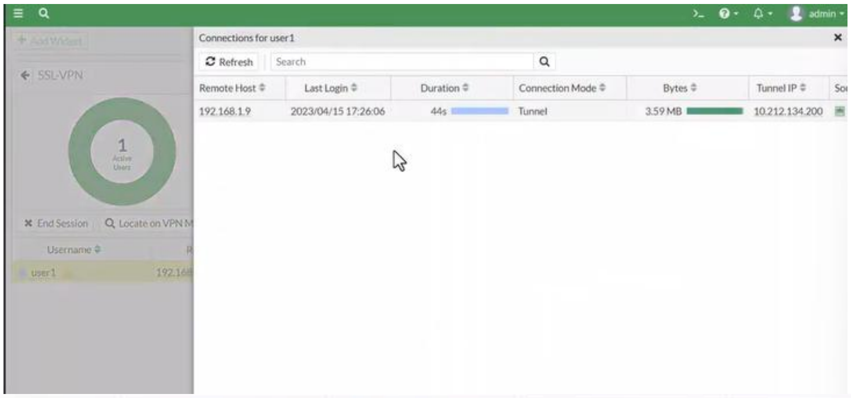
VPN Name	FortiLab
IP Address	10.212.134.200
Username	user1
Duration	00:00:01
Bytes Received	462.81 KB
Bytes Sent	25.55 KB

Step 9: Monitoring and Troubleshooting

Active Connections Monitoring

SSL-VPN Dashboard Shows:

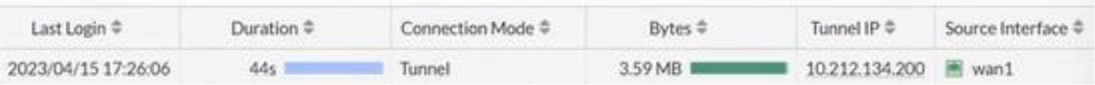
- Active Users: 1
- Connection Mode: Web
- Username: vpnuser
- Remote Host: 192.168.1.9
- Tunnel Ip: 10.212.134.200
- Duration: 44s
- Source interface: Wan1
- Tunnel IP: Assigned from SSLVPN_TUNNEL_ADDR1 pool



Connections for user1

Remote Host	Last Login	Duration	Connection Mode	Bytes	Tunnel IP	So
192.168.1.9	2023/04/15 17:26:06	44s	Tunnel	3.59 MB	10.212.134.200	

Username	R
user1	192.168



Last Login	Duration	Connection Mode	Bytes	Tunnel IP	Source Interface
2023/04/15 17:26:06	44s	Tunnel	3.59 MB	10.212.134.200	wan1

Document Version: 1.0
Last Updated: October 28, 2025
FortiGate Version: 7.2.12
Tested With: FortiClient 7.2.12