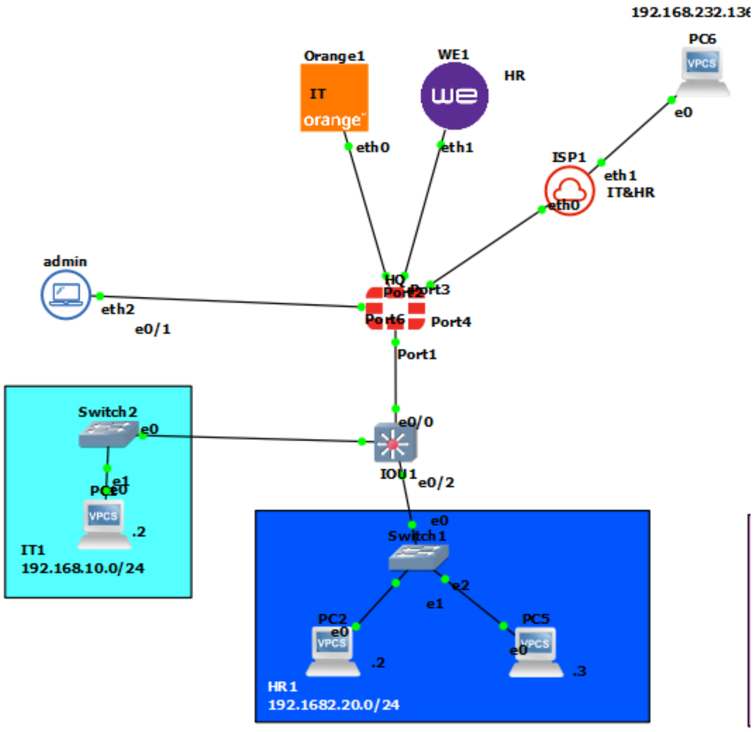
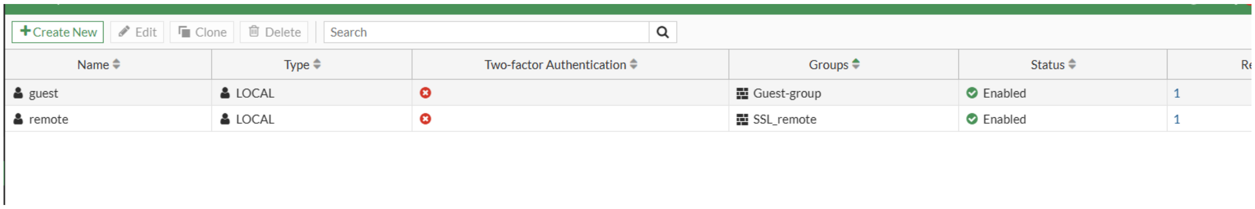
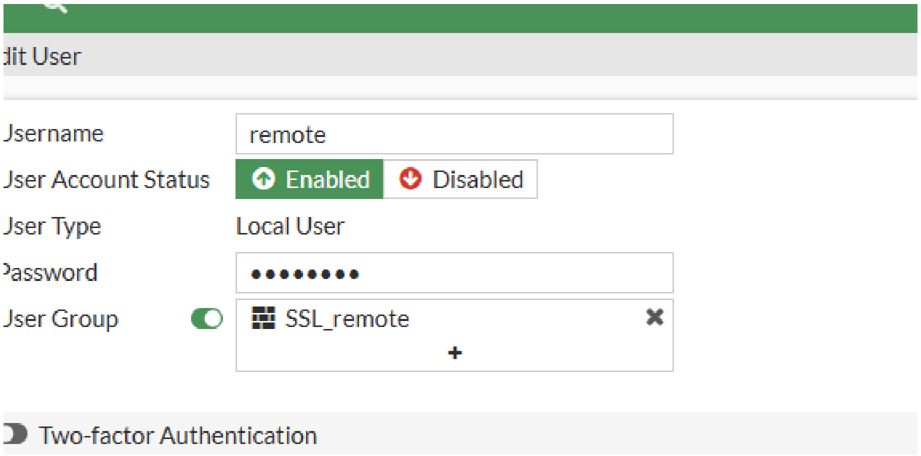
Study SSL_VPN_CONF



This part implements SSL VPN remote access on a FortiGate firewall for secure connectivity to the internal management network. Remote users authenticate with a local user account and are assigned a virtual IP from a dedicated SSL VPN address. After authentication, the firewall applies a security policy that allows secure access to only the required internal subnet (remote device).



Name	Type	Two-factor Authentication	Groups	Status	Re
guest	LOCAL	✗	Guest-group	✓ Enabled	1
remote	LOCAL	✗	SSL_remote	✓ Enabled	1



dit User

Jsername: remote

Jser Account Status: Enabled | Disabled

Jser Type: Local User

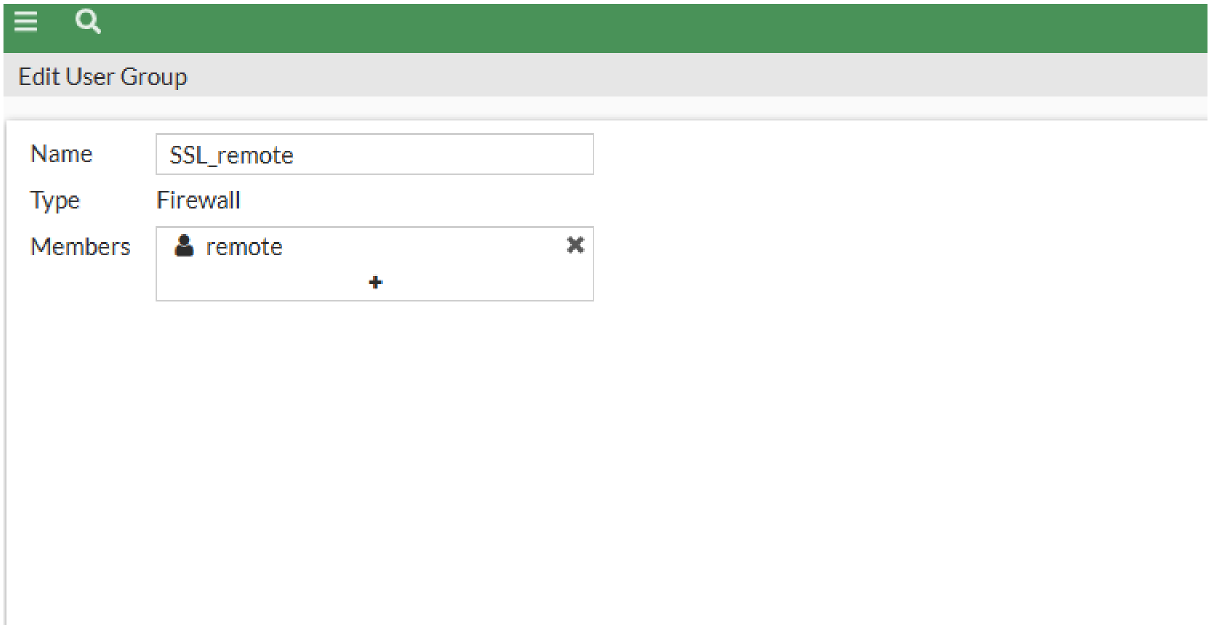
assword: •••••••••

Jser Group: SSL_remote

Two-factor Authentication

Local User

- **Username: remote**
- **Type:** Local User
- **Two-Factor Authentication:** Disabled
- **Status:** Enabled



Edit User Group

Name: SSL_remote

Type: Firewall

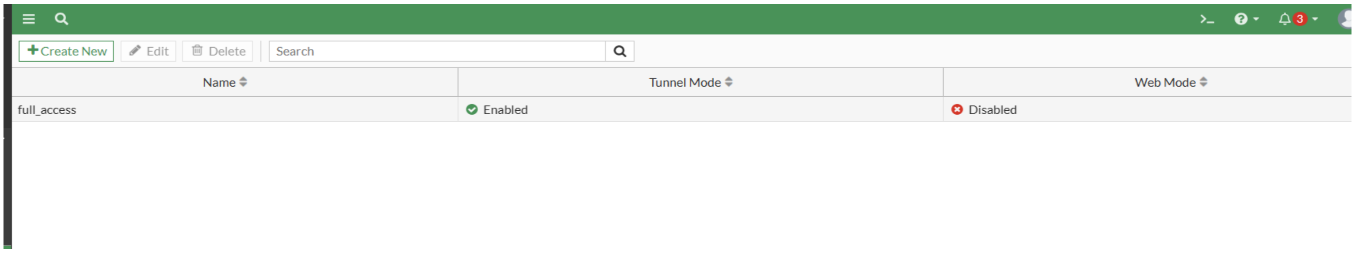
Members: remote

User Group

- **Group Name:** ssl_remote
- **Group Type:** Firewall group
- **Members:** remote

Address Objects

SSL VPN IP Pool



Name	Tunnel Mode	Web Mode
full_access	✓ Enabled	✗ Disabled

SSL VPN Portal Configuration

Portal Name: full-access

Mode: Tunnel Mode Only

- Tunnel mode: **Enabled**
- Web mode: **Disabled**

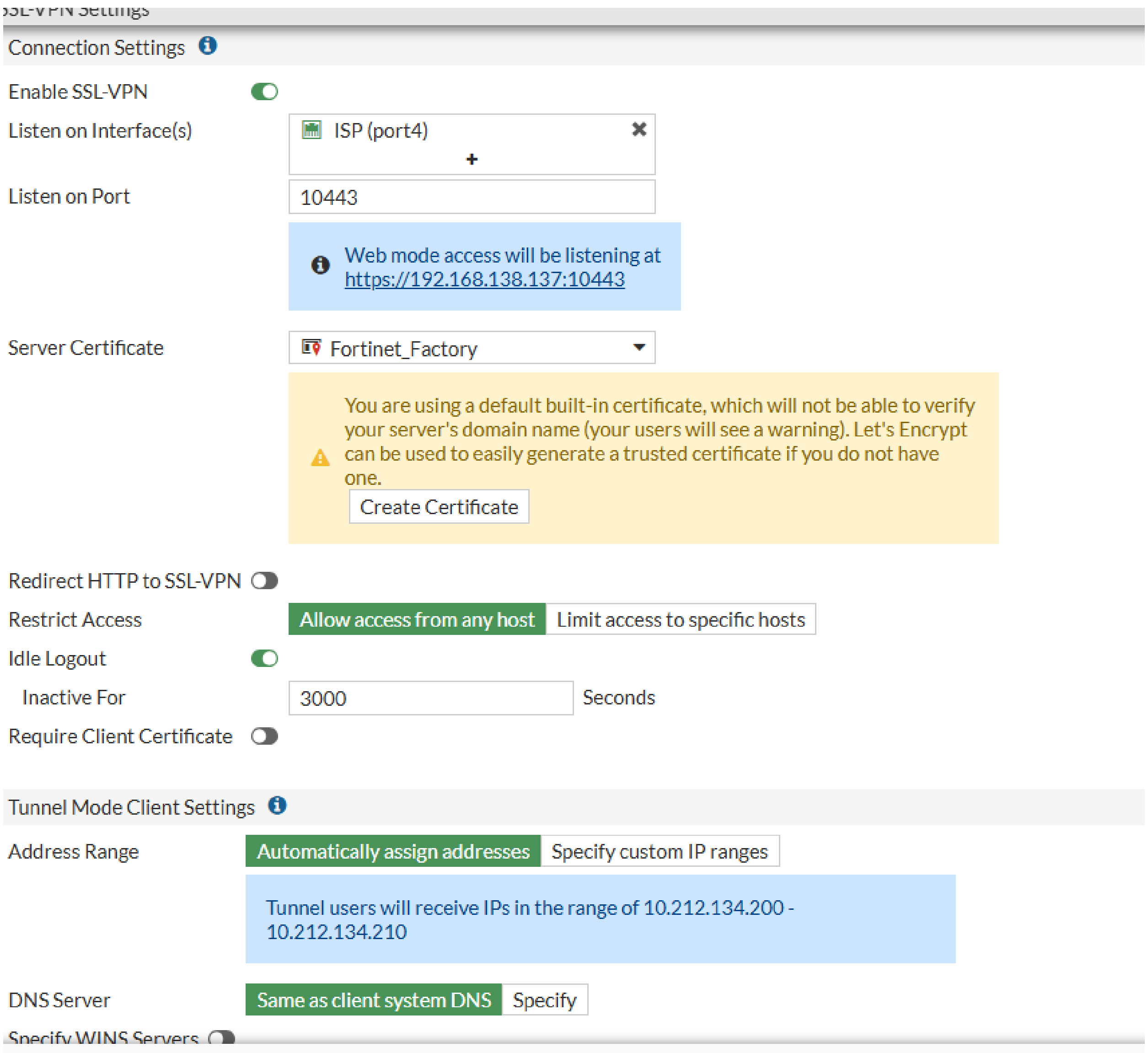
Split Tunneling: Enabled

- Split tunneling based on destination
- Traffic to the internal network goes through VPN
- Internet traffic goes out through the user’s local connection

Routing Address Override: port of remote

(VPN users receive a route to the management subnet.)

Source IP Pool: sslvpn_tunnel_addr1



SSL-VPN Settings

Connection Settings

Enable SSL-VPN ☑

Listen on Interface(s): ISP (port4)

Listen on Port: 10443

Web mode access will be listening at https://192.168.138.137:10443

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.

Redirect HTTP to SSL-VPN ☐

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

Idle Logout ☑

Inactive For: 3000 Seconds

Require Client Certificate ☐

Tunnel Mode Client Settings

Address Range: [✓ Automatically assign addresses] Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server: [✓ Same as client system DNS] Specify

Specify WINS Servers ☐

SSL VPN Settings

Listen on Interface: port4

Listen on Port: 10443

(Chosen to avoid conflict with Admin HTTPS port 443.)

Server Certificate: Fortinet_Factory

Idle Timeout: 3000 seconds

Restrict Access: Allow from any host

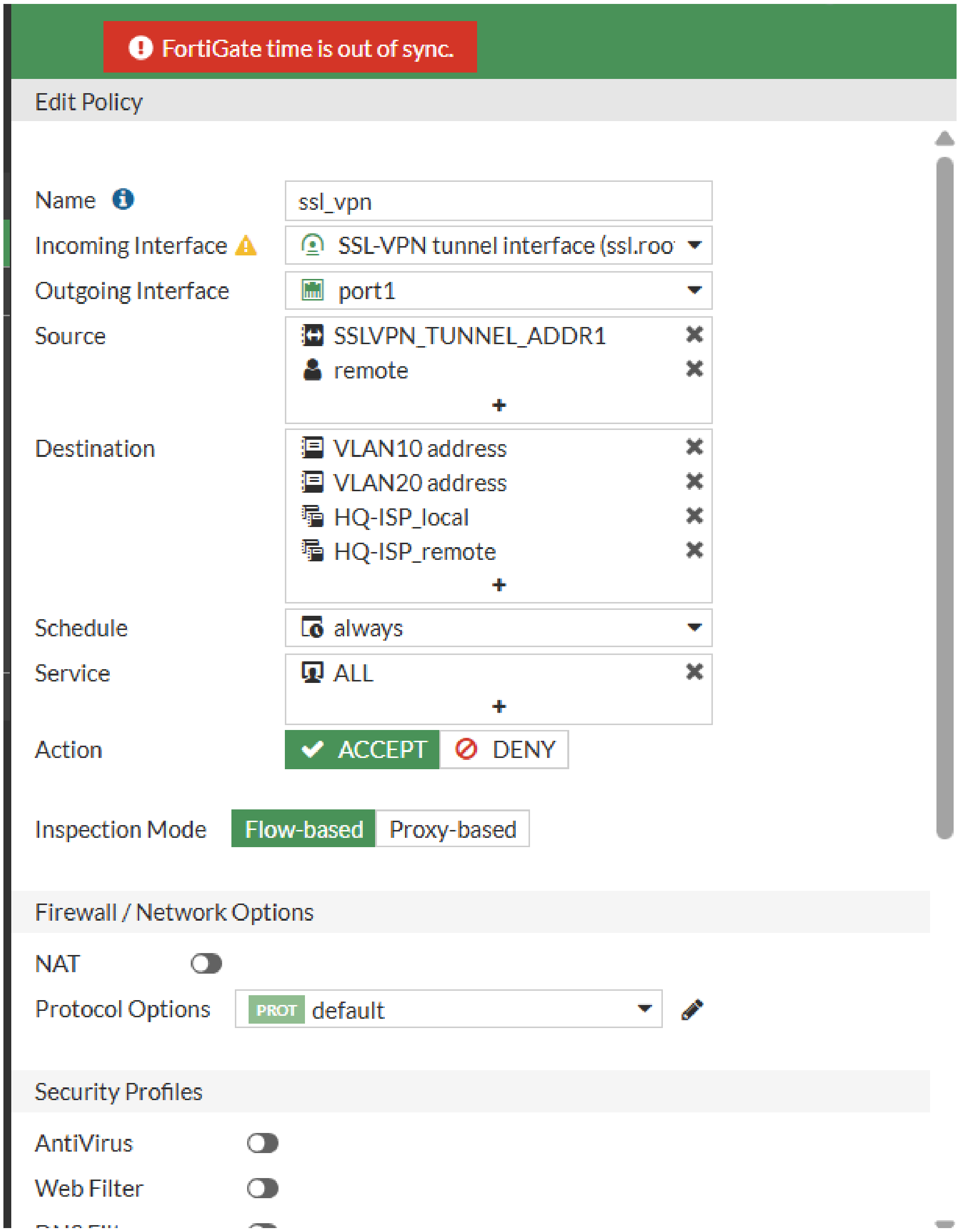
Address Range: Automatically assign from IP pool

Authentication / Portal Mapping

- **All Other Users/Groups → tunnel-access**

This ensures all users in ssl_vpn get the correct portal.

Policy



FortiGate time is out of sync.

Edit Policy

Name: ssl_vpn

Incoming Interface: SSL-VPN tunnel interface (ssl.roo

Outgoing Interface: port1

Source: SSLVPN_TUNNEL_ADDR1
remote

Destination: VLAN10 address
VLAN20 address
HQ-ISP_local
HQ-ISP_remote

Schedule: always

Service: ALL

Action: [✓ ACCEPT] DENY

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT: ○

Protocol Options: PROT default

Security Profiles

AntiVirus: ○

Web Filter: ○

SSL VPN Firewall Policy

A single firewall policy allows VPN traffic to reach the management network.

The Policy Name: ssl_vpn Incoming Interface: ssl.root (SSL VPN Tunnel Interface)

Outgoing Interface: port

Notes / Pending Fix

SSL VPN Testing Steps (Precise & Clear)

1. Connect using FortiClient

Open FortiClient.

Select Remote Access → SSL VPN.

Enter the FortiGate public IP / domain.

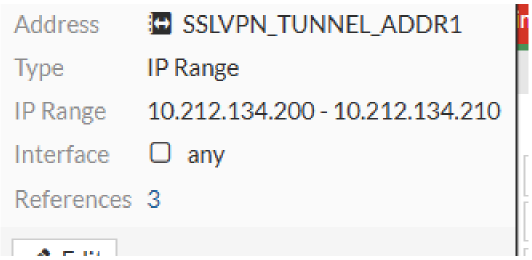
Enter your username and password.

Click Connect.

Make sure the status changes to “Connected”.

2.Verify the assigned IP address

After connecting: Check the VPN assigned IP in FortiClient



Address	SSLVPN_TUNNEL_ADDR1
Type	IP Range
IP Range	10.212.134.200 - 10.212.134.210
Interface	□ any
References	3

Confirm that it matches the SSL VPN IP Pool you configured on the FortiGate.

3.Test basic connectivity (Ping)
From your PC (while connected):
Test 3.1 — Ping the internal gateway ping
Test 3.2 — Ping a device inside the LAN

ping <LAN host IP>

Expected result: Replies = the firewall policy is allowing access.

4. Check firewall logs
On FortiGate:

Go to Log & Report → Forward Traffic

Filter by:

Source: SSL VPN user

Interface: ssl.root