

INTEGRATION GUIDE

# How to Configure FortiGate to secure VPN access with Portnox CLEAR

## Introduction

This document guides you step by step how to configure your VPN environment using Portnox CLEAR to enable secure and trusted cloud-based RADIUS access with an optional push-to-access MFA.

## Preliminary Actions

Before configuring VPN authentication, you need to verify the following:

- 1) Verify your organization is registered on Portnox CLEAR Cloud Services: <https://clear.portnox.com/>
- 2) In the CLEAR portal, go to **Settings > Services** and expand **CLEAR RADIUS Service**. Then:
  - a. If the **Enable Cloud RADIUS** checkbox is not checked, click **Edit** and check the **Enable Cloud RADIUS** checkbox.
  - b. Note the RADIUS server details which you will need when configuring VPN access:
    - **Cloud RADIUS IP** – this is the IP address of the CLEAR RADIUS server
    - **Authentication port**
    - **Shared Secret** - this is the RADIUS client shared secret
- 3) In the CLEAR portal, go to **Settings > Groups** and create a group for VPN users, or edit an existing one. In the **group settings > VPN Access** select the following:
  - Allowed authentication type = credentials.
  - (optional) Multi-Factor Authentication = push-to-access on mobile only.  
Note, MFA on mobile devices require AgentP to be enrolled on the mobile device.
  - For implementation with AgentP, check the: validate risk score for all managed devices.

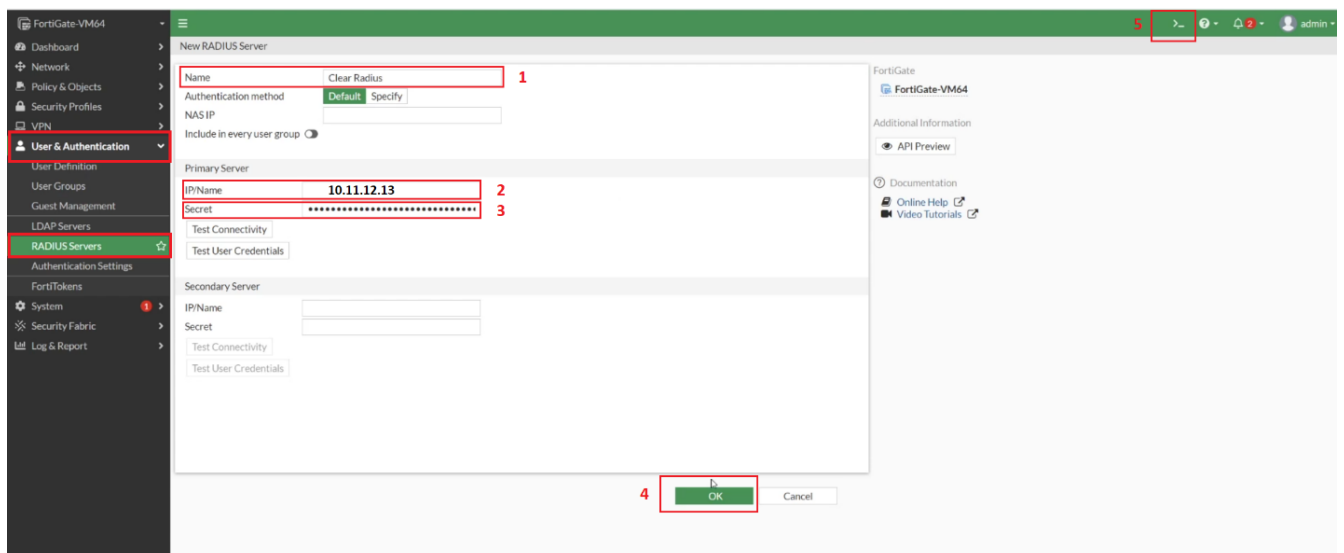
# Configuring FortiGate SSL VPN

In the following steps, we configure the VPN authentication to be secured and protected based on RADIUS authentication. The following steps should be performed in the FortiGate Web UI/CLI.

## Add a new Radius Server

Navigate to Under “User & Authentication” > RADIUS Servers, create a new RADIUS Server:

1. Enter a name.
2. Enter Primary Radius Server IP.
3. Enter Secret.
4. Click “OK”.
5. Enter the CLI.



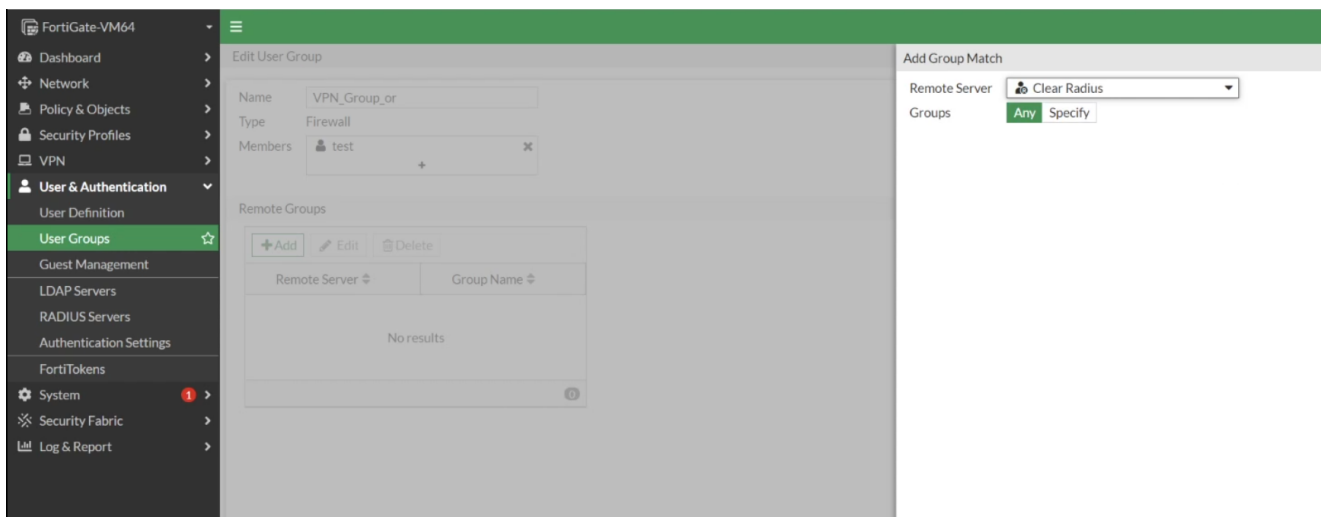
Within the CLI, change the authentication port to the relevant port used by CLEAR radius:

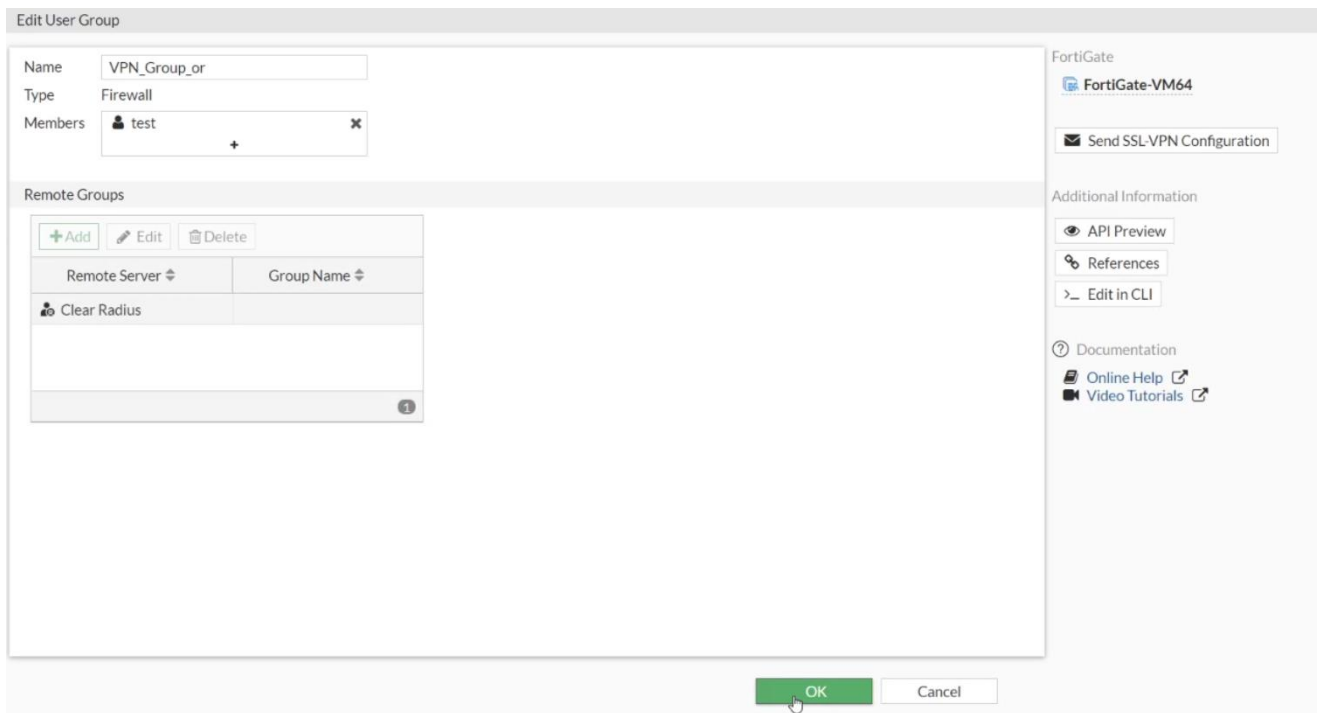
```
CLI Console (1)
FortiGate-VM64 # config system global
FortiGate-VM64 (global) # set radius-port 12345
FortiGate-VM64 (global) # end
FortiGate-VM64 # config user radius
FortiGate-VM64 (radius) # edit Clear\ Radius
FortiGate-VM64 (Clear Radius) # set auth-type auto
FortiGate-VM64 (Clear Radius) # set server 10.11.12.13
FortiGate-VM64 (Clear Radius) # set secret AABBC123456RRTT
FortiGate-VM64 (Clear Radius) # end
FortiGate-VM64 #
```

### Add a new User Group:

Under “User & Authentication” > User Groups, create a new group.

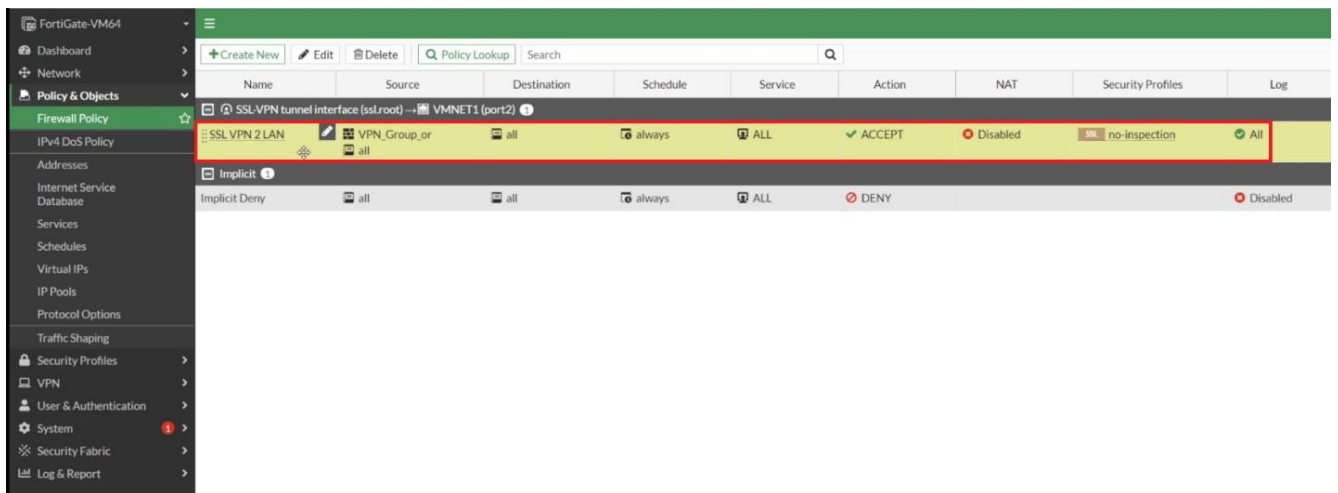
Under “Remote Groups”, add relevant “Clear Radius” server:





**Allow “Firewall Policy” access:**

Under “Policy & Objects” >> “Firewall Policy”, create a new “Rule”:



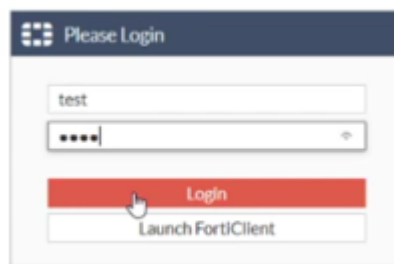
Edit that relevant rule:

Add “VPN\_Group” under “Source”.

# Instructions for Supplying VPN Credentials

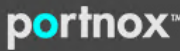
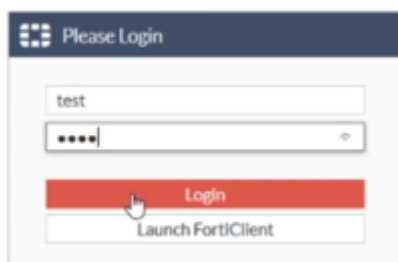
## Supplying VPN Credentials without MFA

For successful VPN authentication using Portnox CLEAR RADIUS, users are required to provide their username + password:



## Supplying VPN Credentials with push-to-access MFA

For successful VPN authentication using Portnox CLEAR RADIUS and push-to-access MFA, users are required to provide their username + password and allow the push notification on their mobile device:



**NEW SIGN IN**  
Your device attempted to access the corporate network. Please confirm.

portnox2

Aug 14, 2020 | 3:27 PM

---

**DENY** **ALLOW**