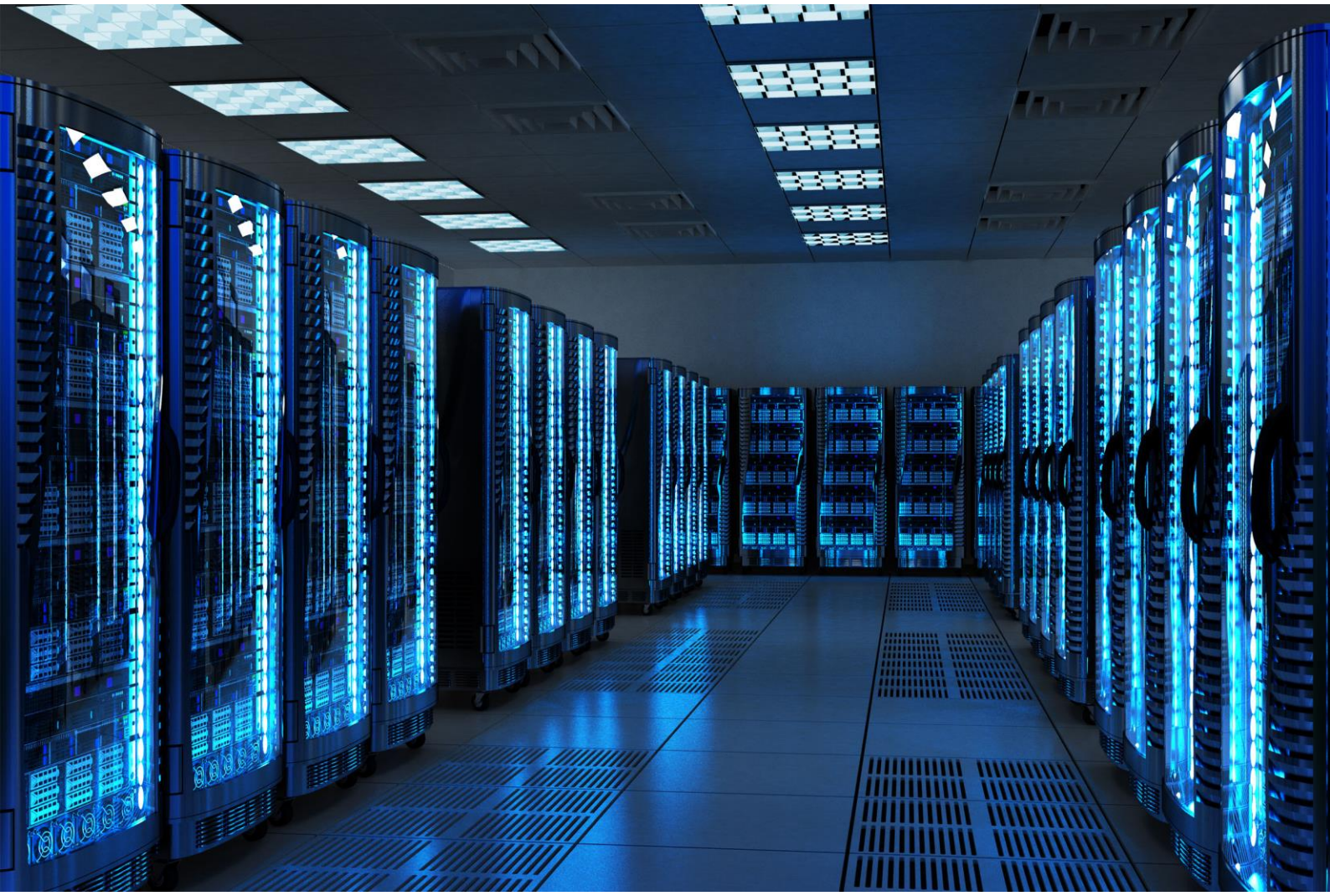
portnox™



INTEGRATION GUIDE

# How to Configure PPTP/SSTP server 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**
      - **Accounting port**
      - **Shared Secret** - this is the RADIUS client shared secret

1) 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.

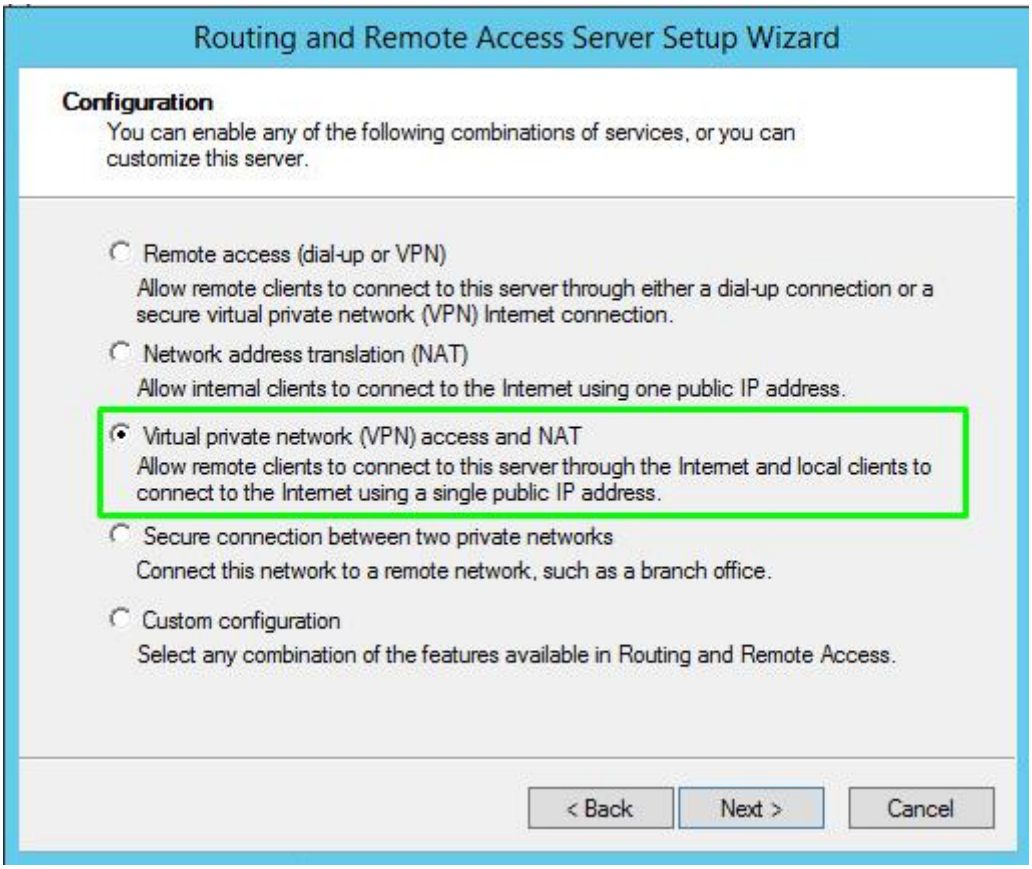
# Configuring Microsoft Routing and Remote Access on Windows Server

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 Server Management Console.

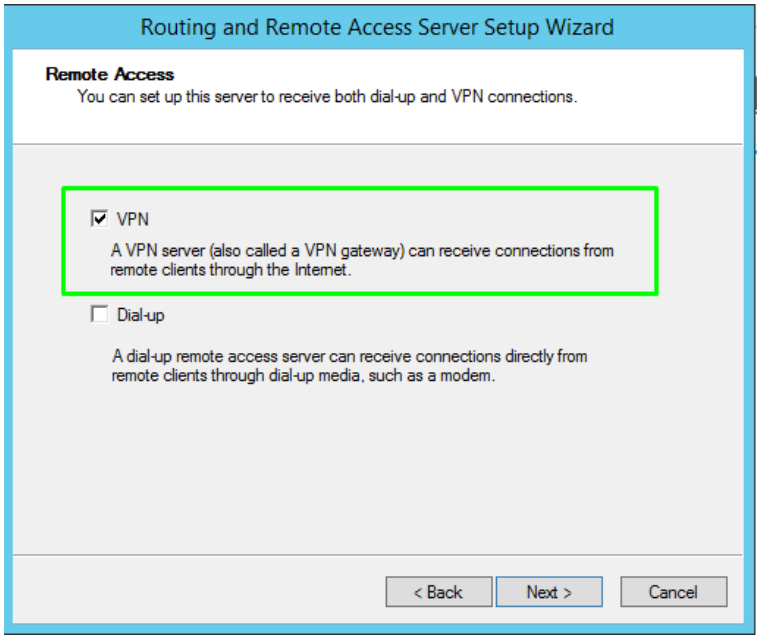
## Step 1 - Creating a new Routing Server

Navigate to **Server Manager > Tools > Routing and Remote Access**
In Routing and Remote Access interface, right click on Routing and Remote Access > Add Server > Select "This Computer" > Right Click the new instance > Configure the Routing and Remote Access Server

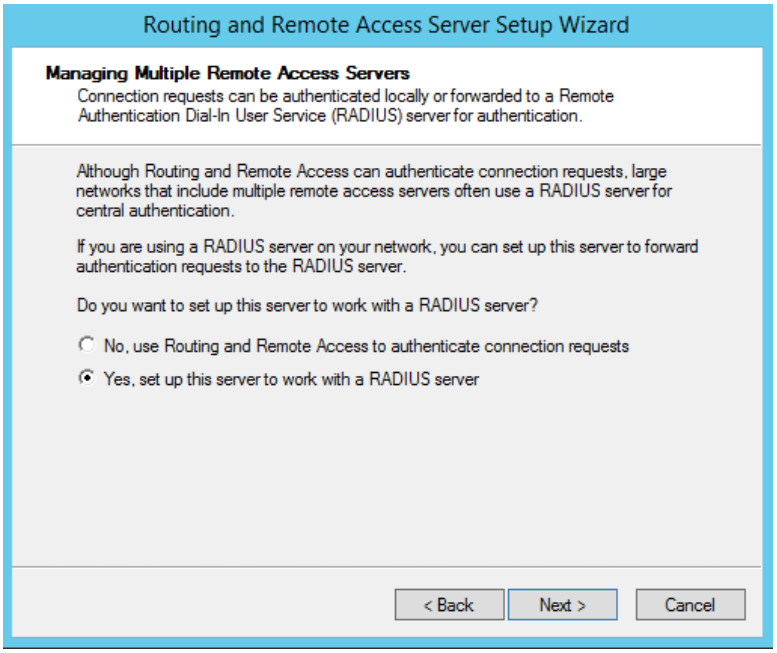
Next >



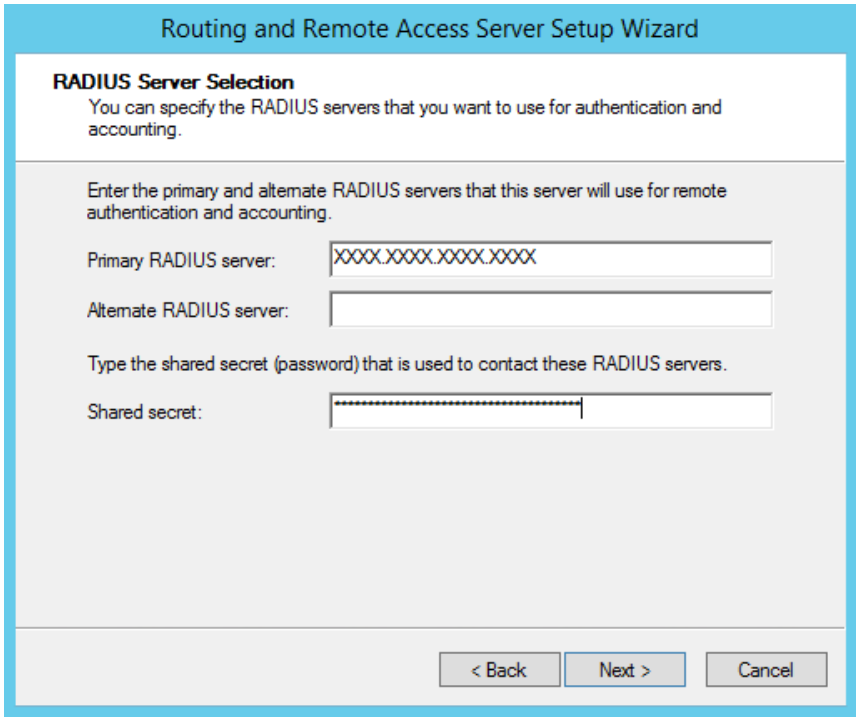
Next >




Next > (VPN Property) > Next > (VPN Property) > Next > (VPN Property)



In the RADIUS Server Selection, specify the CLEAR RADIUS IP and Shared Secret which you've noted Preliminary Actions, step 2(b):

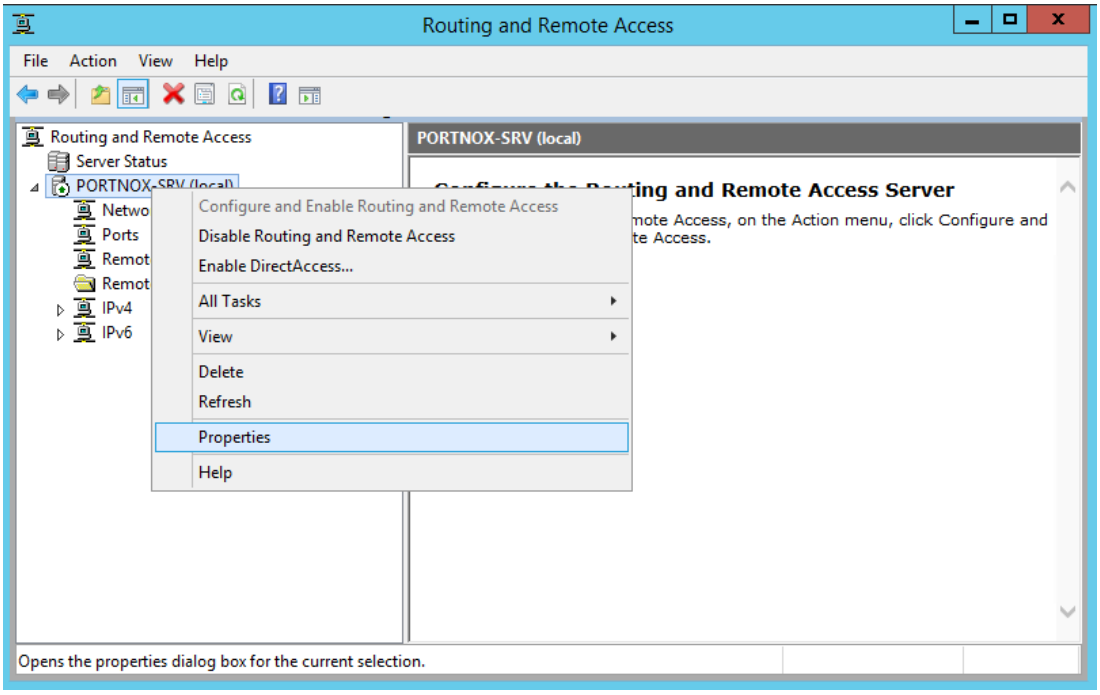


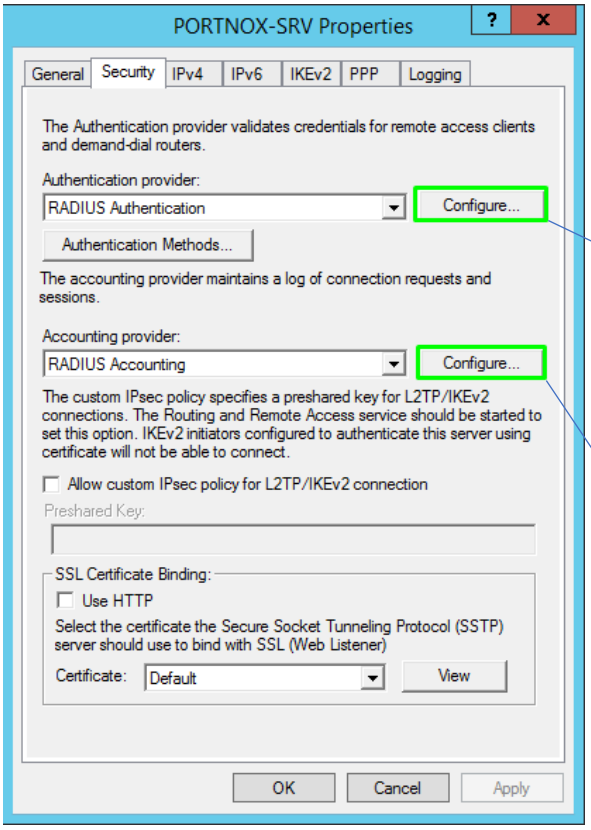

Next > Finish

## Step 2 – Fine tuning of the RADIUS parameters

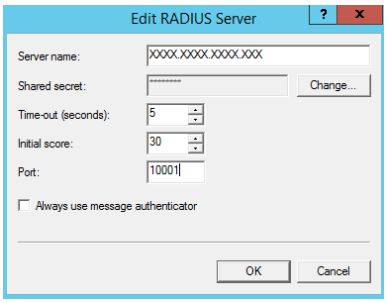
In **Routing and Remote Access** Configuration menu

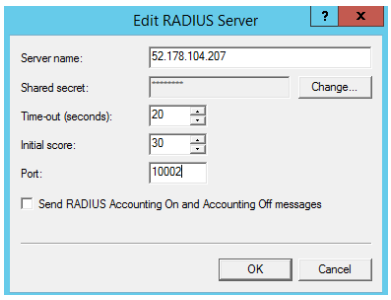
Right Click on the new Server>Properties>Security Tab



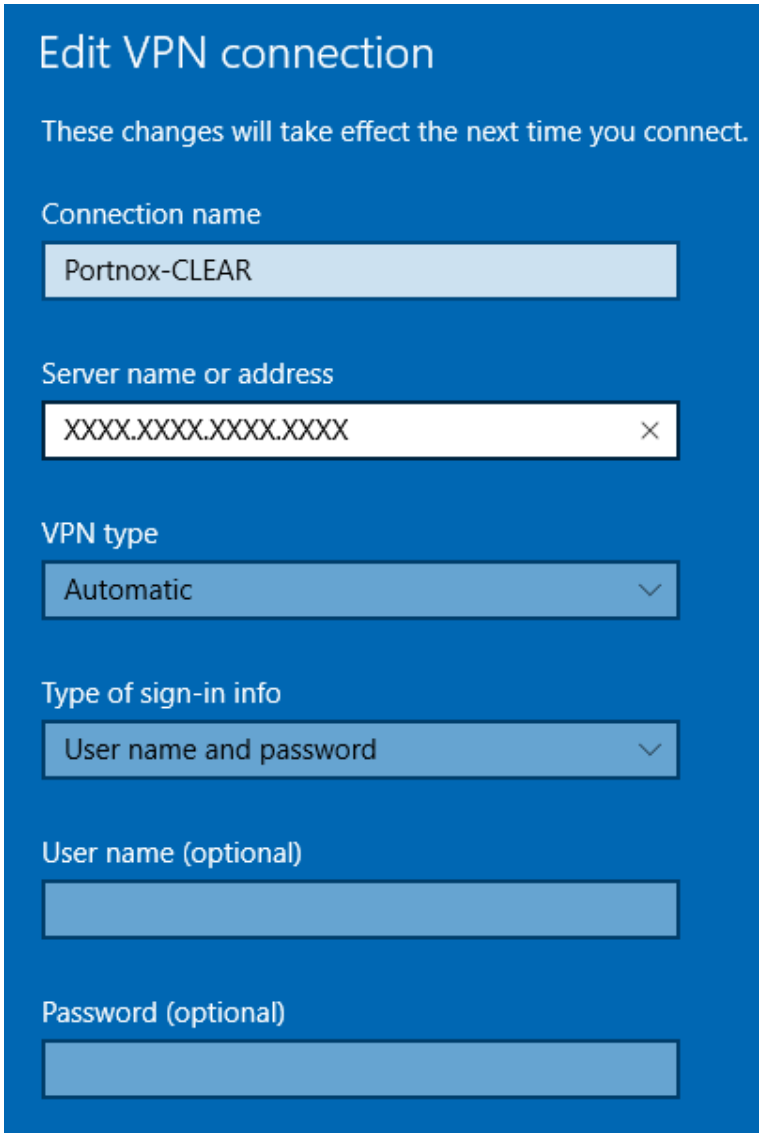

Update the RADIUS Authentication and the RADIUSU Accounting ports according to the values you've noted in Preliminary Actions, step 2(b):



# VPN Connection on Client Side

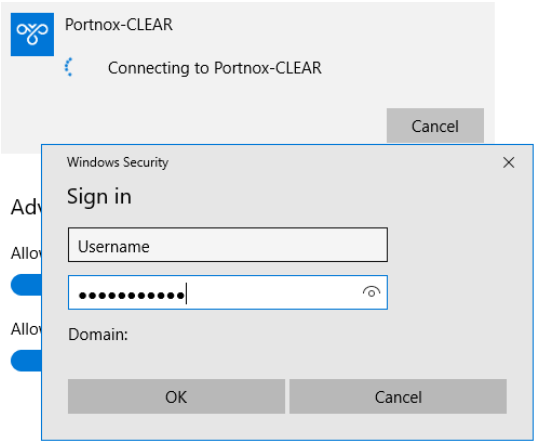
Access Network and Sharing Center > VPN > Add a VPN Connection



# 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: