

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

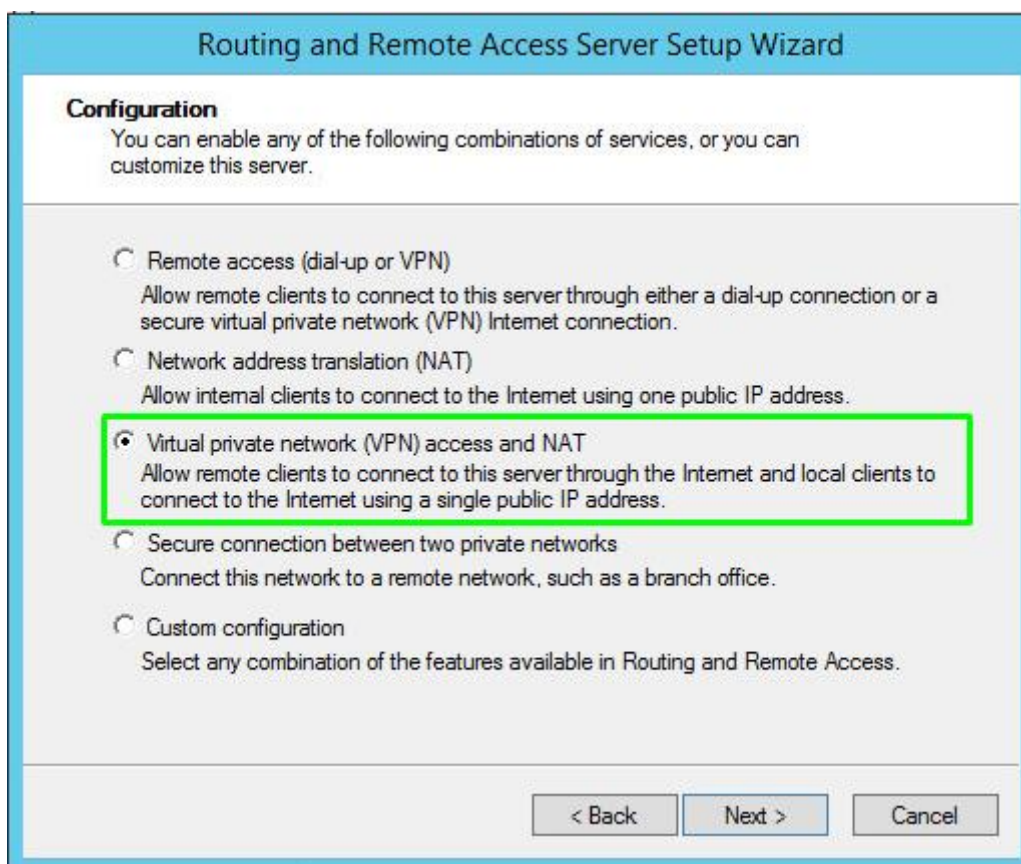
In the following steps, we configure the VPN authentication to be secured and protected based on RADIUS authentication. The following steps should be performed in the Server Management Console.

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 >



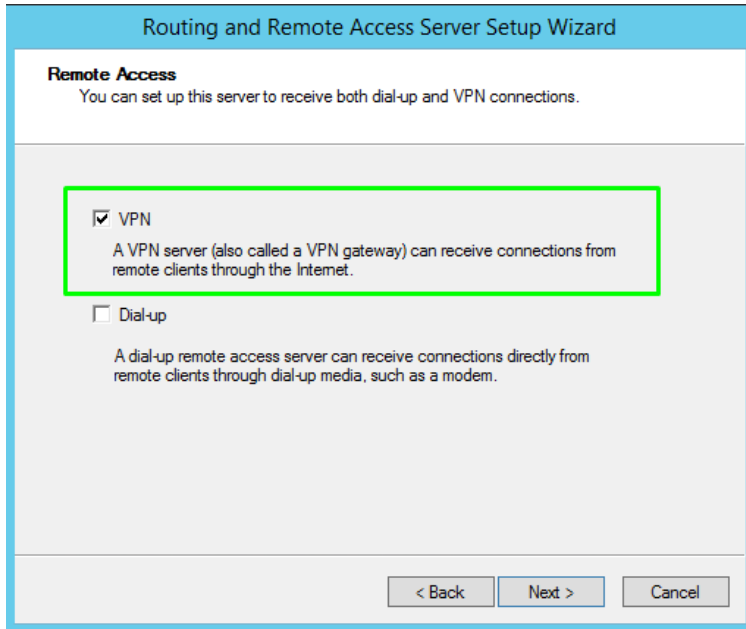
The screenshot shows the "Routing and Remote Access Server Setup Wizard" window. The title bar reads "Routing and Remote Access Server Setup Wizard". The main area is titled "Configuration" and contains the following text: "You can enable any of the following combinations of services, or you can customize this server." Below this text are five radio button options, each with a description. The third option, "Virtual private network (VPN) access and NAT", is selected and highlighted with a green rectangular box. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

Configuration
You can enable any of the following combinations of services, or you can customize this server.

- Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
- Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
- Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
- Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
- Custom configuration
Select any combination of the features available in Routing and Remote Access.

< Back Next > Cancel

Next >



Routing and Remote Access Server Setup Wizard

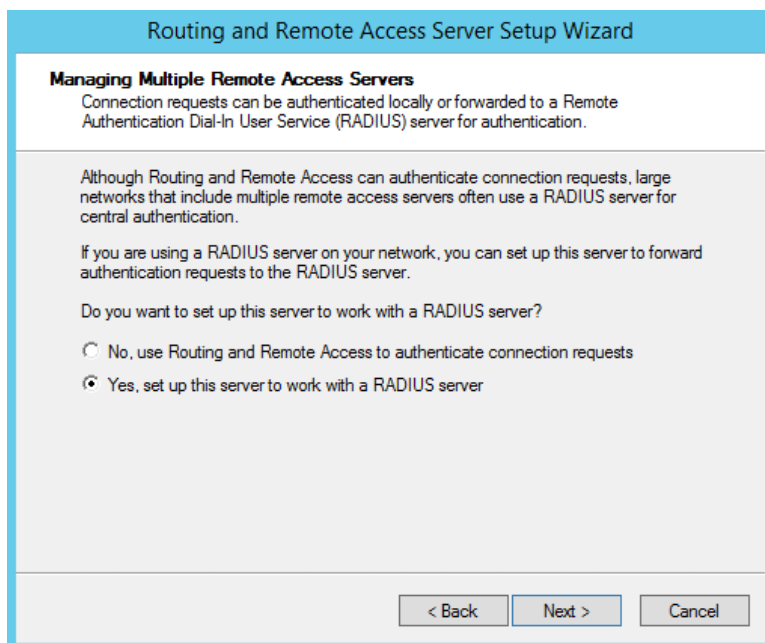
Remote Access
You can set up this server to receive both dial-up and VPN connections.

VPN
A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.

Dial-up
A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.

< Back Next > Cancel

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



Routing and Remote Access Server Setup Wizard

Managing Multiple Remote Access Servers
Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.

Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

Do you want to set up this server to work with a RADIUS server?

No, use Routing and Remote Access to authenticate connection requests

Yes, set up this server to work with a RADIUS server

< Back Next > Cancel

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

Routing and Remote Access Server Setup Wizard

RADIUS Server Selection
You can specify the RADIUS servers that you want to use for authentication and accounting.

Enter the primary and alternate RADIUS servers that this server will use for remote authentication and accounting.

Primary RADIUS server:

Alternate RADIUS server:

Type the shared secret (password) that is used to contact these RADIUS servers.

Shared secret:

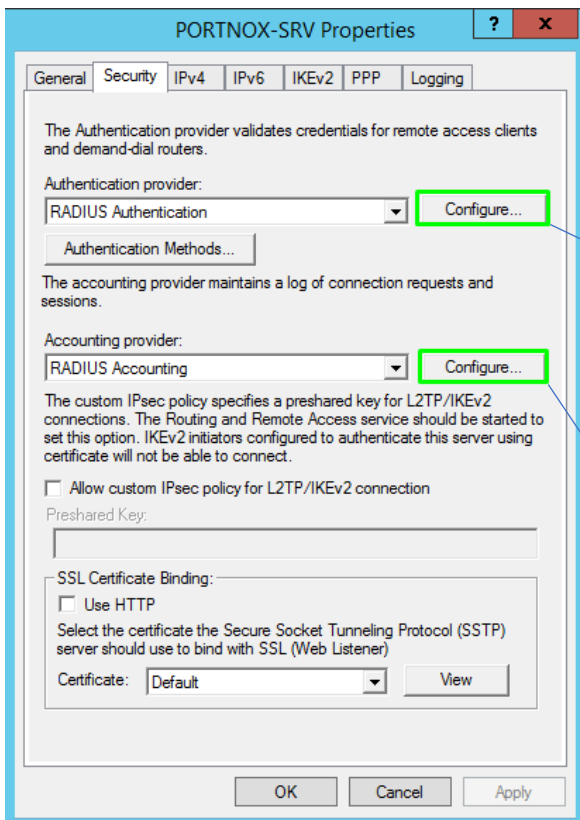
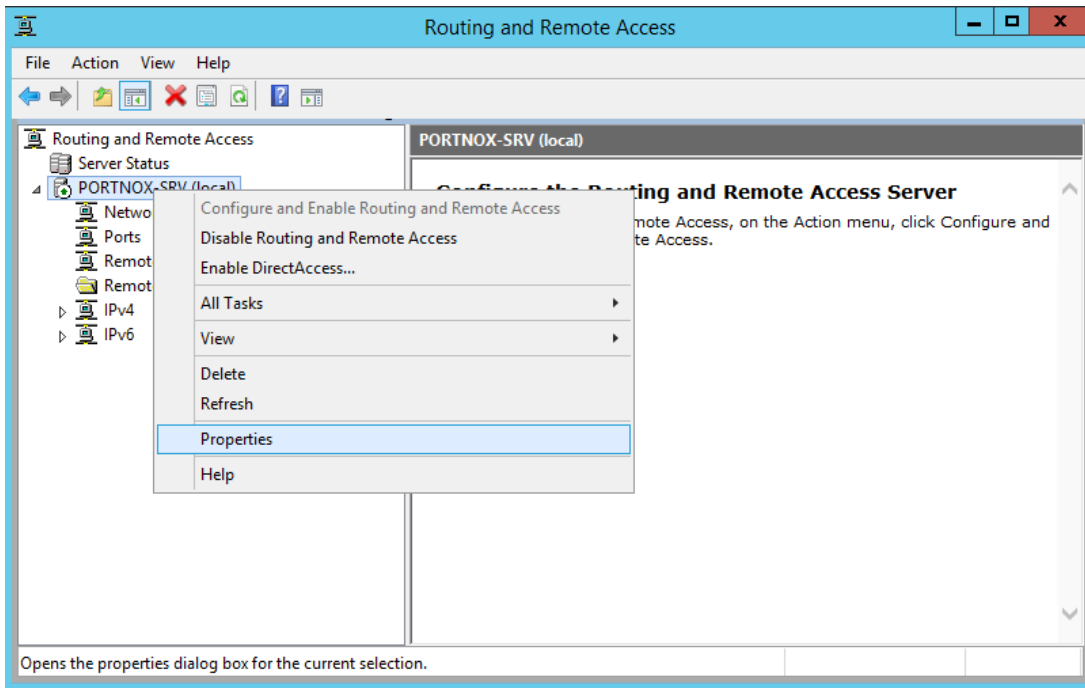
< Back Next > Cancel

Next > Finish

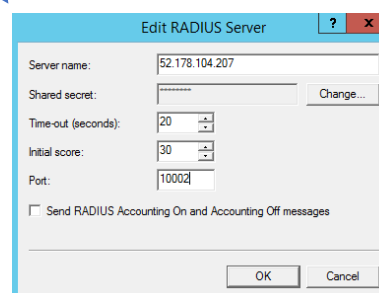
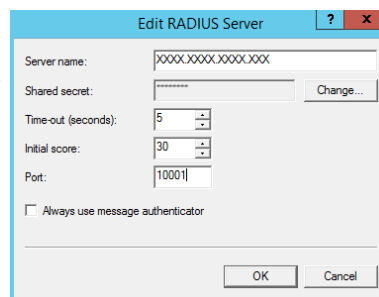
Step 2 – Fine tuning of the RADIUS parameters

In **Routing and Remote Access** Configuration menu

Right Click on the new Server>Properties>Security Tab

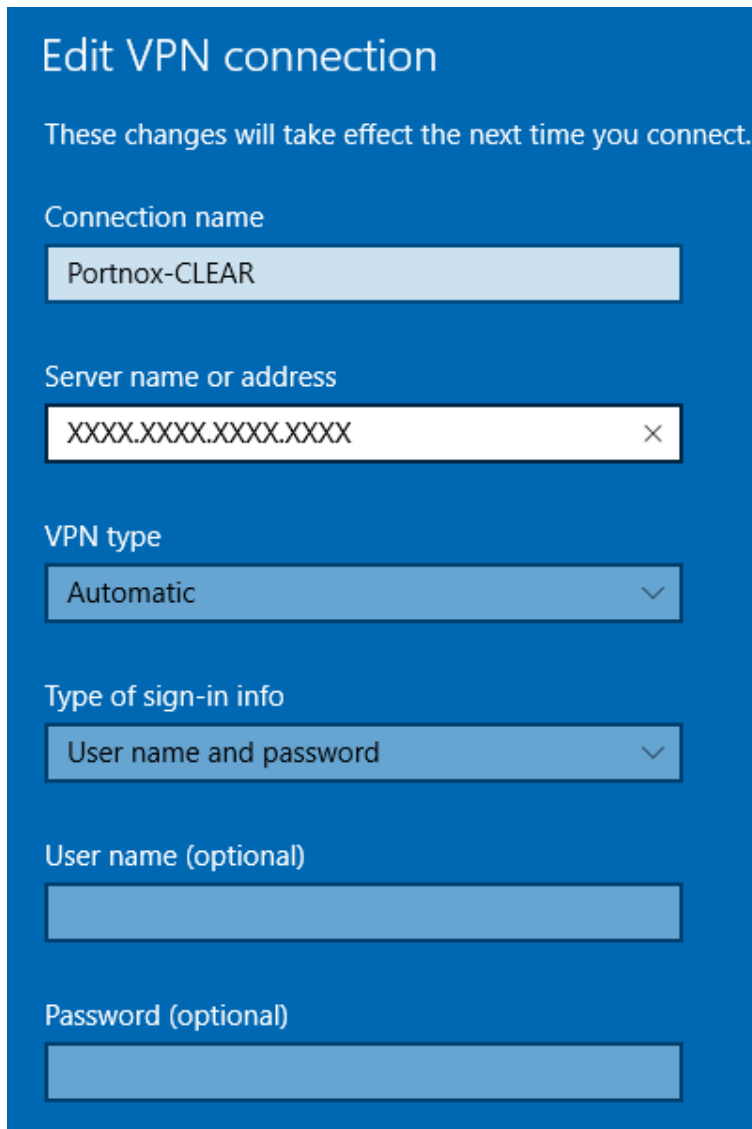


Update the RADIUS Authentication and the RADIUSU Accounting ports according to the values you've noted in Preliminary Actions, step 2(b):



VPN Connection on Client Side

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



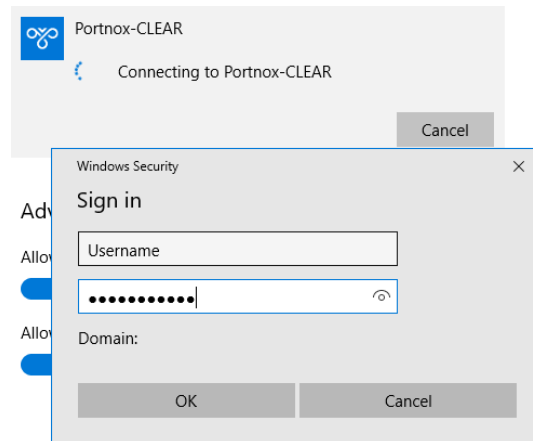
The screenshot shows the 'Edit VPN connection' window in Windows. The title bar is blue with the text 'Edit VPN connection'. Below the title bar, there is a message: 'These changes will take effect the next time you connect.' The form contains several fields:

- Connection name:** A text box containing 'Portnox-CLEAR'.
- Server name or address:** A text box containing 'XXXX.XXXX.XXXX.XXXX' with a clear button (X) on the right.
- VPN type:** A dropdown menu with 'Automatic' selected and a downward arrow.
- Type of sign-in info:** A dropdown menu with 'User name and password' selected and a downward arrow.
- User name (optional):** An empty text box.
- Password (optional):** An empty text box.

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:

