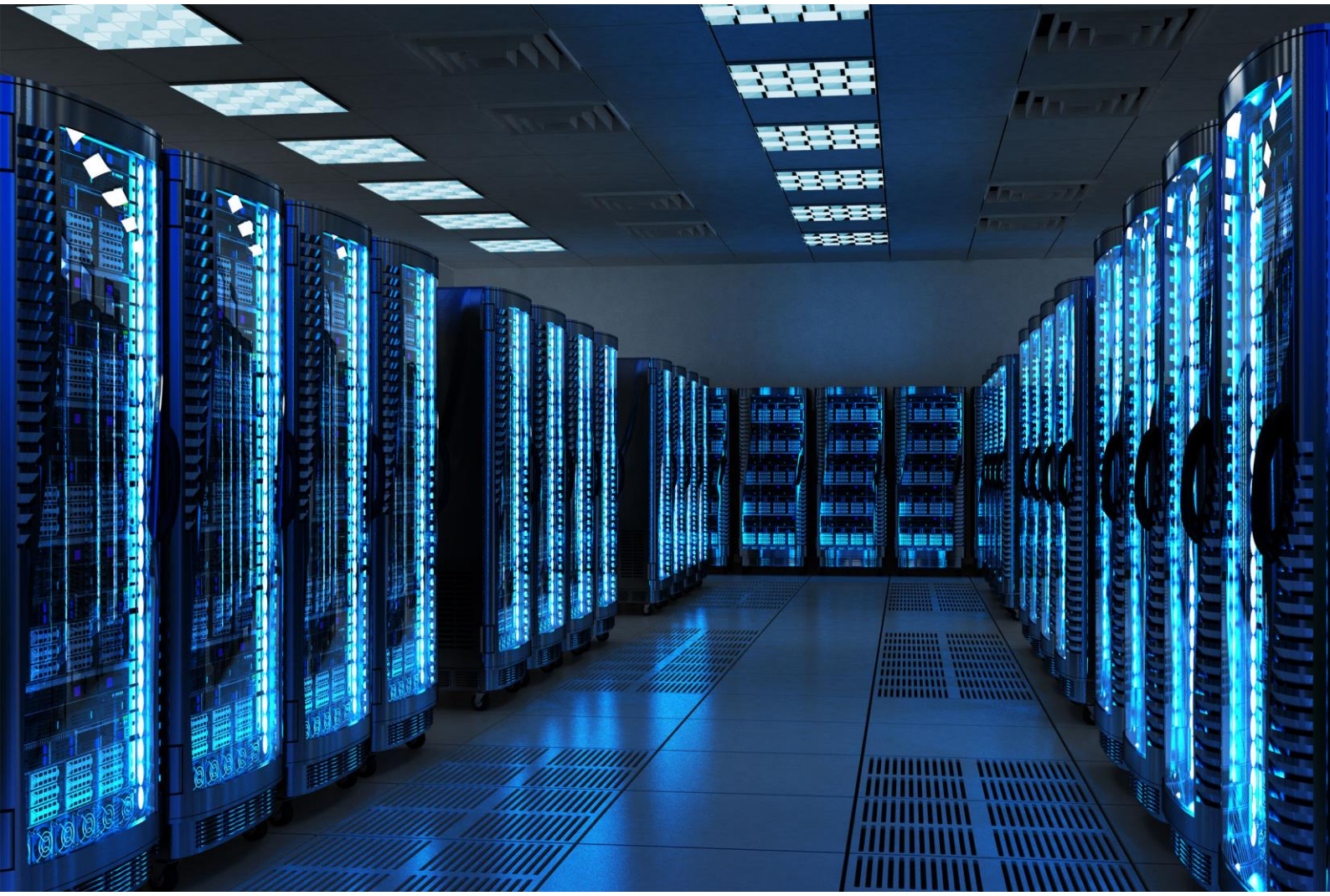
portnox™



INTEGRATION GUIDE

How to Configure Juniper Switch to Secure your Wired Network with Portnox CLEAR

Introduction

This document guides you step by step how to configure your Juniper wired switch environment using Portnox CLEAR to ensure secure and trusted user access.

Enabling CLEAR RADIUS Service

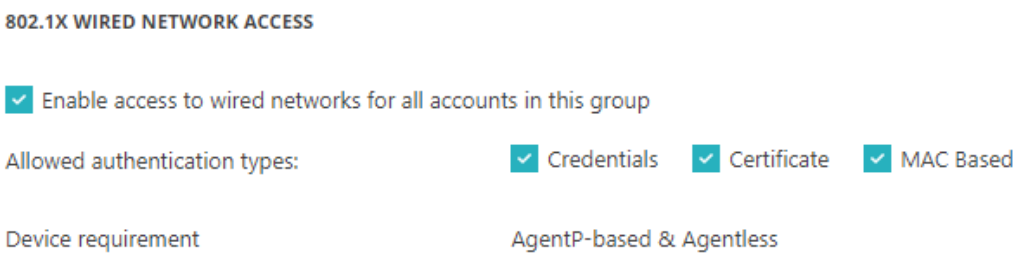
The first step is to enable the CLEAR RADIUS service:

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 the WatchGuard switch:
      - **Cloud RADIUS IP** - this is the IP address of the CLEAR RADIUS server
      - **Authentication port**
      - **Accounting port** - needed for the RADIUS accounting server
      - **Shared Secret** - this is the RADIUS client shared secret

Allow Access to Wired Networks in CLEAR

The second step is to allow, in the CLEAR portal, access to wired networks you will be securing.

1) Navigate in the portal to **Groups**.
2) Edit the default “Default” group or create a new security group.
3) Whether you are creating or editing a group, in **Group Settings** check the **Enable wired access using 802.1x authentication for devices in this group** check box:



Configuring the Juniper Wired Switch

In the final step, we configure the Juniper wired switch to be secured and protected based on CLEAR RADIUS authentication.

For 802.1X, In the Juniper CLI:

1) Configure a Radius server.

   Enter the following CLEAR RADIUS server details, which you noted in Enabling CLEAR RADIUS Service, step (2)b:

   - In **radius-server**, enter the Cloud RADIUS IP.
   - In **port**, enter the Authentication port number.
   - In **accounting-port**, enter the Accounting port number.
   - In **secret**, enter the Shared Secret.
   - In **source address**, enter the switch IP address.

```
ex3200>edit
ex3200# edit access radius-server <radius-server-address>
ex3200# set port 1002 accounting-port 1003 secret XXXXXXXXXXXX source-address <switch-ip>
ex3200# set access profile juniper-access-profile radius authentication-server <radius-server-address>
ex3200# no-mac-table-binding
ex3200# commit
ex3200# exit
```

2) Enable 802.1X on the port/s.

```
ex3200# edit protocols
ex3200# set dot1x authenticator interface ge-0/0/8 mac-radius
ex3200# set dot1x authenticator interface ge-0/0/8 supplicant multiple
ex3200# commit
ex3200# exit
```

Configuration Example:

```
protocols {
   dot1x {
      authenticator {
         authentication-profile-name <ProfileName>;
         no-mac-table-binding;
         interface {
            ge-0/0/8.0 {
               mac-radius;
            }
            ge-0/0/12.0 {
               supplicant multiple;
            }
         }
      }
   }
}
access {
   radius-server {
      <RadiusIP> {
         port <RadiusPort>;
         accounting-port <AccuntingPort>;
         secret "<SharedSecret>"; ## SECRET-DATA
         source-address <SwitchIP>;
      }
   }
   profile <ProfileName>{
      authentication-order radius;
      radius {
         authentication-server <RadiusIP>;
      }
   }
}
```