How to Configure a Meraki Access Switch to Secure Your Wired Network

LEGAL NOTICE:

Copyright © 2017 Access Layers US, Inc. (Portnox)

All rights reserved. Proprietary and confidential material.

Introduction

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

Enabling CLEAR RADIUS Service

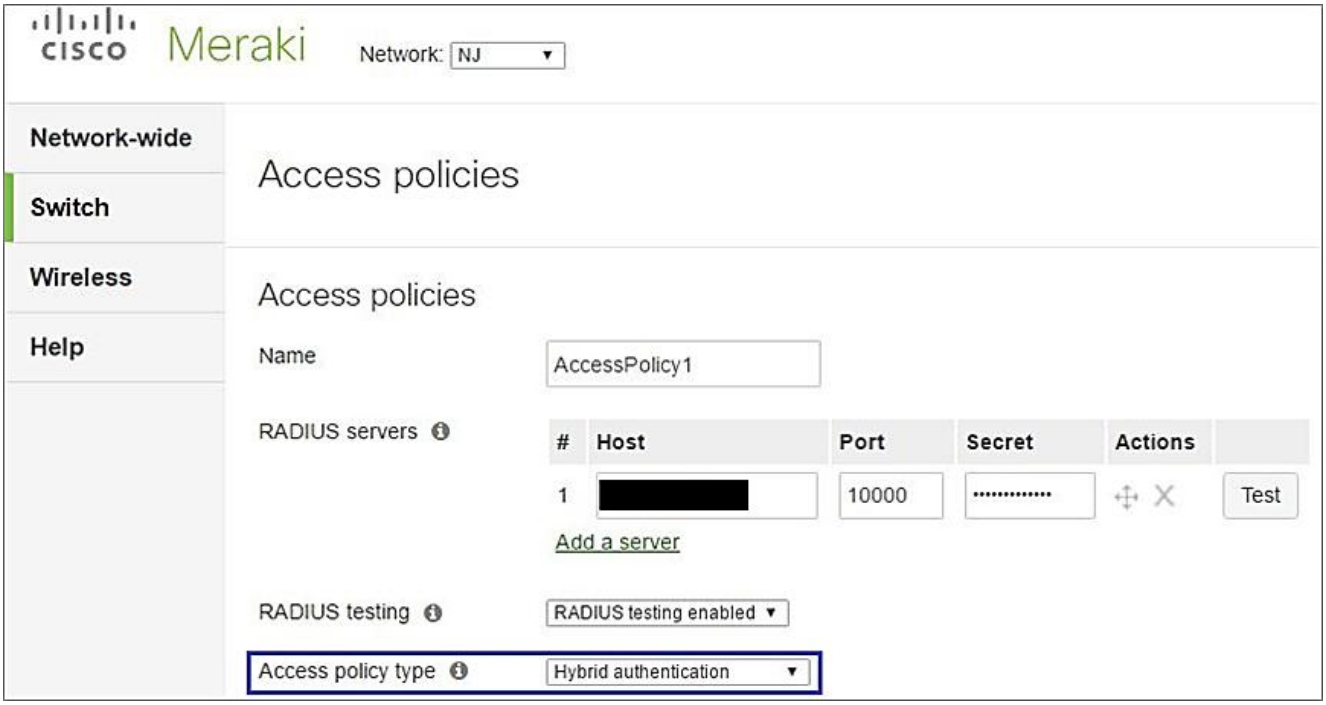
Before configuring the Meraki switch:

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 Meraki switch:
        - **Cloud RADIUS IP** - this is the IP address of the CLEAR RADIUS server
        - **Authentication port**
        - **Shared Secret** – this is the RADIUS client shared secret

Configuring the Meraki Switch

In the following steps, we configure the Meraki switch to be secured and protected based on CLEAR RADIUS authentication.

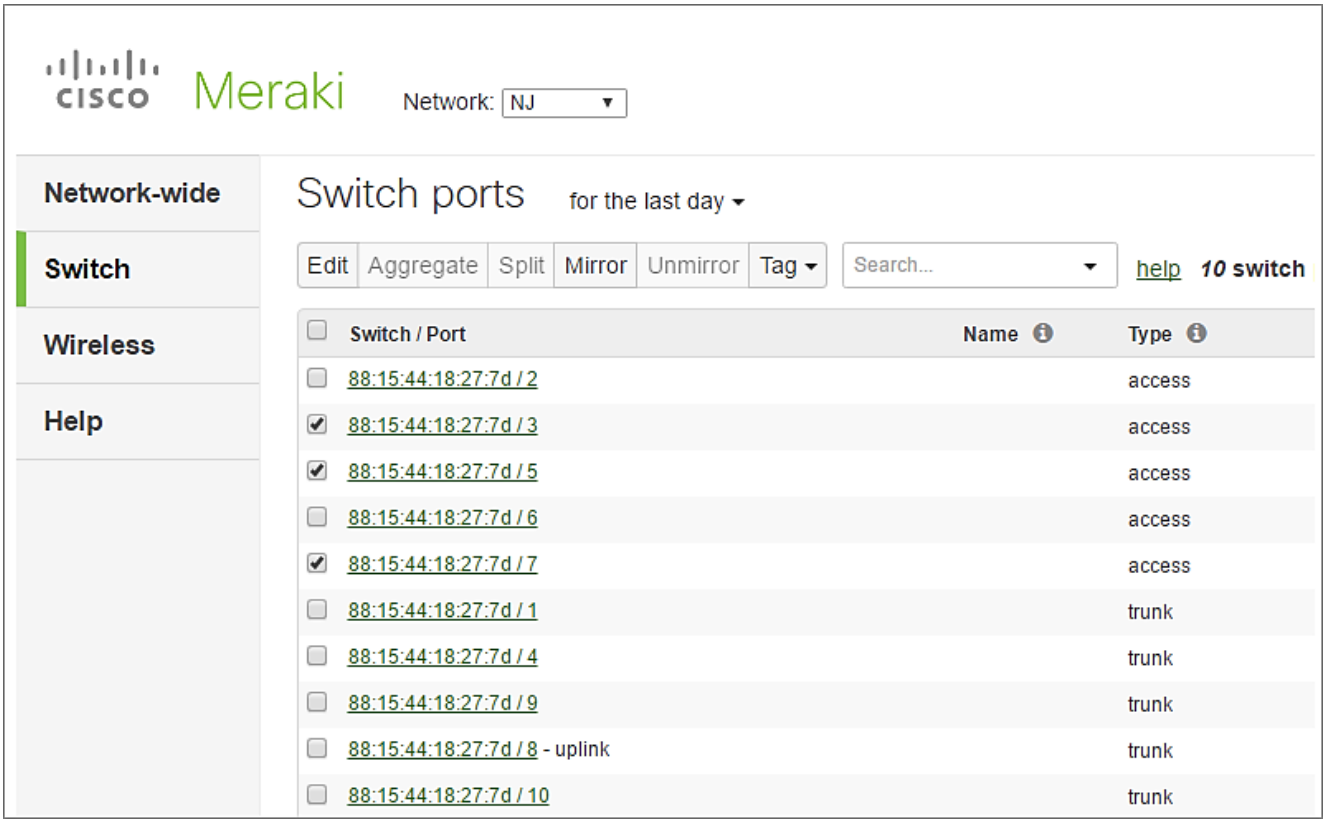
1) In the Meraki portal, navigate to **Switch** > **Configure** > **Access policies** and click **Add an access policy**.
2) In the Access Policies window:
   a. Specify a **Name** for the policy.
   b. Enter the following CLEAR RADIUS server details, which you noted in [Enabling CLEAR RADIUS Service](), step 2b:
      - In **Host**, enter the Cloud RADIUS IP.
      - In **Port**, enter the Authentication port.
      - In **Secret**, enter the Shared Secret.
   c. Specify the **Access policy type**: 802.1x, MAC authentication bypass, or Hybrid authentication.



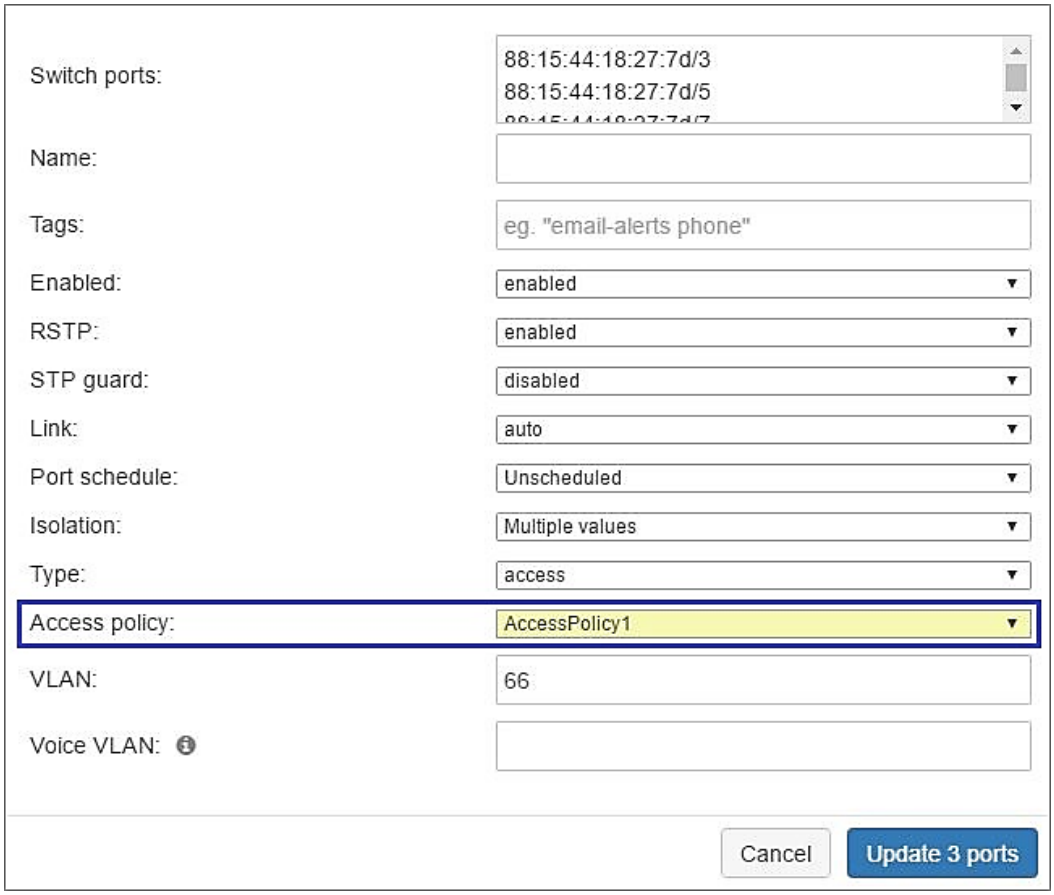
   d. Click **Save Changes**.

3) In the Meraki portal, navigate to **Switch** > **Monitor** > **Switch ports**.

4) In the Switch Ports window, select the **Switch ports** to which you want to apply the policy, and click **Edit**.



5) In the edit window, select the relevant **Access policy** and click **Update**.



<u>Note</u>: You can create multiple access policies and assign different access policies to different ports.