AN-310-4L2W ROUTER: ACL SETUP

USE CASES

Common ACL (Access Command List) uses are:

- Blocking undesired port use.
- Allowing the use of a printer across VLANs while restricting access to everything else.
- Restricting access to a specific website.

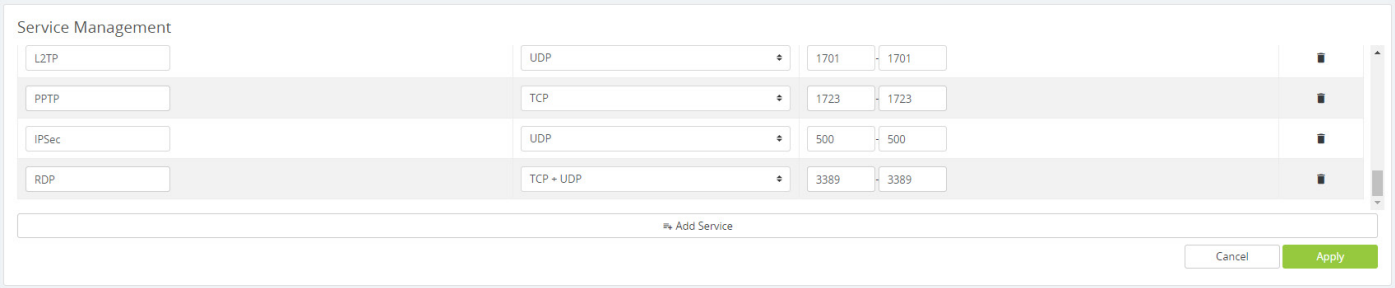
Path - Advanced > ACLs

BLOCKING UNDESIRED PORT USE

In this example we'll be blocking RDP (Remote Desktop)

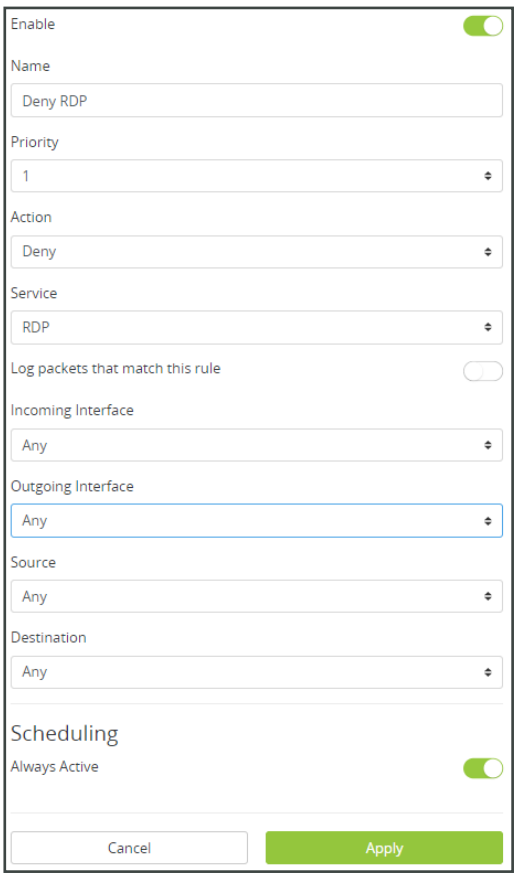
Service Management Setup

1. Click **Add Service** and enter a **Service Name**. RDP, for example.
2. Select **TCP + UDP**, connection-full (TCP) or connection-less service (UDP) from the **Protocol** drop-down.
3. Enter the **Port** range you'd like to block (RDP uses only port 3389) and click **Apply**.



Access Control List Settings

1. Click **Add ACL**.
2. **Enable** the ACL and give it an easily identifiable **Name**.
3. Select **Deny** from the **Action** drop-down.
4. From the **Service** drop-down, select **RDP**. This is the service we added to the Service Management table.
5. Set the **Incoming Interface** (receiving) and **Outgoing Interface** (transmitting) to **Any**. This includes all LAN and WAN ports.
6. Select **Any from the Source** (originating device) and **Destination** (receiving device) drop-downs.
7. Keep **Scheduling** at **Always Active** and click **Apply**.



CONTACTING TECH SUPPORT

Phone: 866.838.5052 704.909.5229
Email: TechSupport@SnapAV.com