New Feature Overview

AN-310-RT-4L2W Firmware v 1.1.64

araknis NETWORKS

Introduction

The purpose of this document is to explain changes made in Phase 2 firmware for AN-310 routers.

> **Note –** Backup configurations from previous firmware versions are not compatible with Phase 2 firmware.

Contents

200804-0942

WAN Ports on the 310

Full document can be found **here.**

WAN 2 is Now Enabled

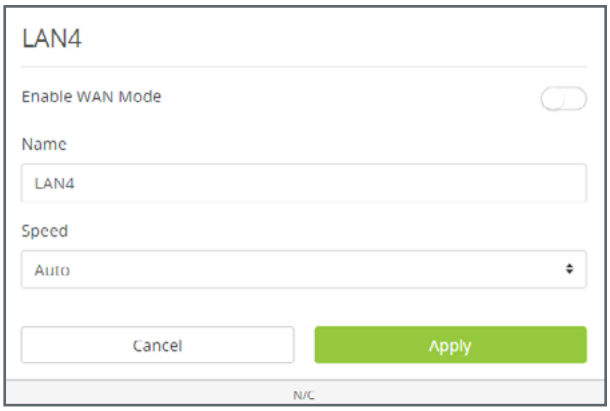
For previous router buyers please remove the sticker.

> **Note –** Rules such as Port Forwarding, ACL, Rate Limiting, and Route-Binding are configured separately for each WAN interface.

LAN 4 Can Now be Used as WAN 3

To do so, go to the LAN settings and click on LAN4. Use the toggle to Enable WAN Mode. This will remove LAN4 from your LAN settings page and show WAN3 on your WAN Settings page.

To change WAN3 back to LAN4, click on WAN3, in the WAN Settings, and use the toggle to Enable LAN Mode.



Load Balancing Across all WAN Ports

The AN-310 router uses session based packet routing and does not aggregate the total bandwidth multiple WAN ports. For example:

An example of a session would be a speed-test or video call from a single device.

When running a speed-test on multiple devices (eg. laptop, cellular, etc.), you are running multiple sessions.

The 310-router effectively load balances across sessions, choosing a singular WAN for any given session.

What is Bandwidth Control?

This feature allows you to manage WAN interface bandwidth for network clients based on IP address. Use this feature to limit the total bandwidth use, for specified clients.

Bandwidth Control is implemented by creating rules for upstream or downstream traffic limits to one or more IP addresses. Rules may be “stacked” in order to further segment bandwidth use based on the needs of each client’s applications.

Basic Example

You have a client with a guest network, but they do not want guests using all their bandwidth downloading movies or games. Bandwidth control can be used to limit the amount of bandwidth the guest network can use.

> **Note –** See page 7 for an additional setup example including menu configuration.

Using Bandwidth Control

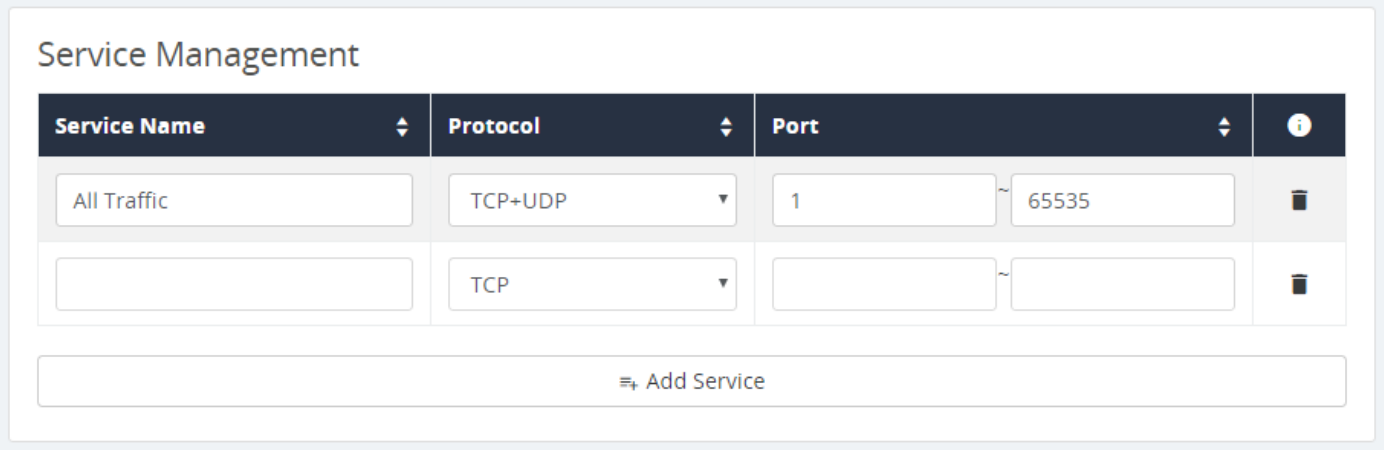
Path – Advanced > Bandwidth Control

> **Caution –** Bandwidth Control should only be used by networking professionals. Configuring this feature incorrectly will cause network performance and reliability issues.

Bandwidth Control Menu Overview

Service Management

Entries in the Service Management table are used when creating new rules in the Bandwidth Control Settings menu at the bottom of the page. Entries may be deleted or modified and new rules can be added.



Parameters –

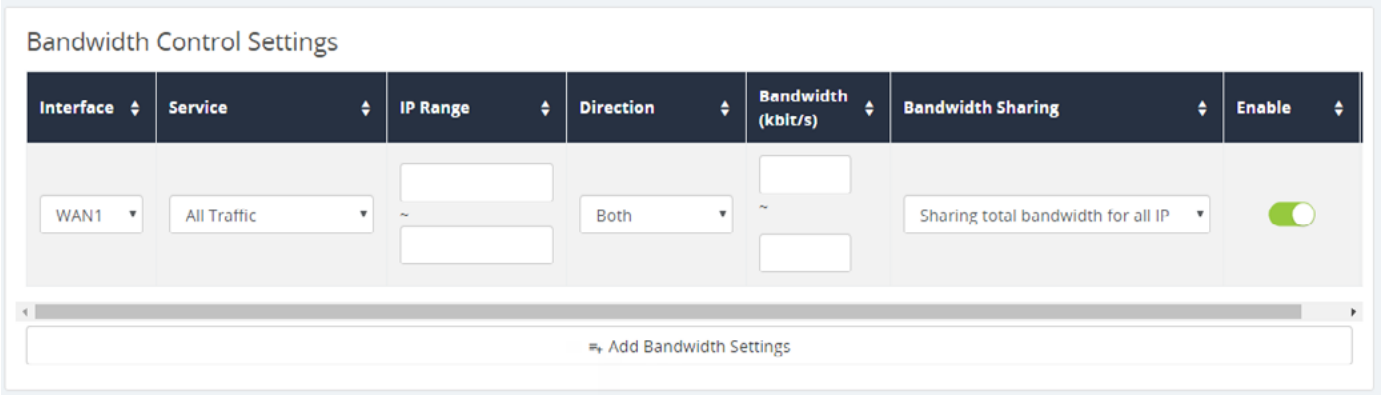
- **Service Name –** Description for the ports in the rule.
- **Protocol –** Select the protocol(s) for the ports. Options: TCP, UDP, TCP+UDP
- **Port –** Enter the port or port range for the rule. Enter the same port number in both fields to specify a single port.
- **Delete –** Click to delete a rule.
- **Add Service –** Click to add a new rule entry.

You must click **Apply** at the bottom right of the page to save changes.

> **Note –** Changes in the Bandwidth Control Services table are shared with the ACL Services table.

Bandwidth Control Settings

This menu is used to configure the total bandwidth being limited among specific clients.



Note – Bandwidth Control does not guarantee any minimum amount of bandwidth.

- **Bandwidth Control Settings**
  - **Interface –** Select the WAN interface the rule will affect.
  - **Service –** Select a service from the drop down. Use the All Traffic setting unless you want to regulate bandwidth for a specific program or service using a forwarded port.
  - **IP Range –** Set the range of IP addresses that will be affected by the rule. Enter the same address in both fields to create a rule for a single IP address.
  - **Direction –** Select whether the rule affects upstream or downstream traffic.
  - **Bandwidth (kbits/s) –** Enter the minimum and maximum bandwidth allowance for the rule.
  - **Bandwidth Sharing –** Select ***Sharing total bandwidth for all IP*** to split the specified bandwidth among the clients, or ***Assign for each IP*** to allow the full specified bandwidth for each IP.
  - **Enable –** Select whether the rule is in effect or not.
  - **Trashcan –** Delete a rule.
  - **Add Bandwidth Settings –** Click to add a new rule entry.

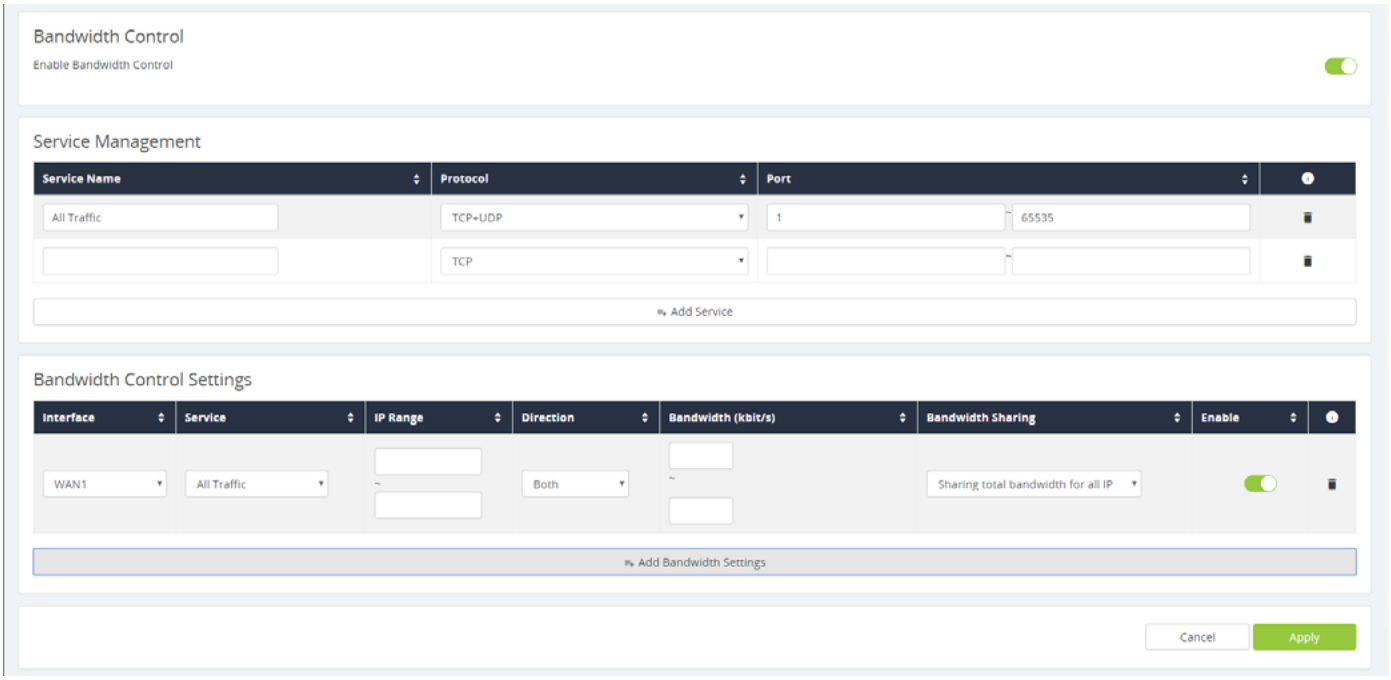
You must click **Apply** at the bottom right of the page to save changes.

Bandwidth Control Setup Instructions

Before You Begin

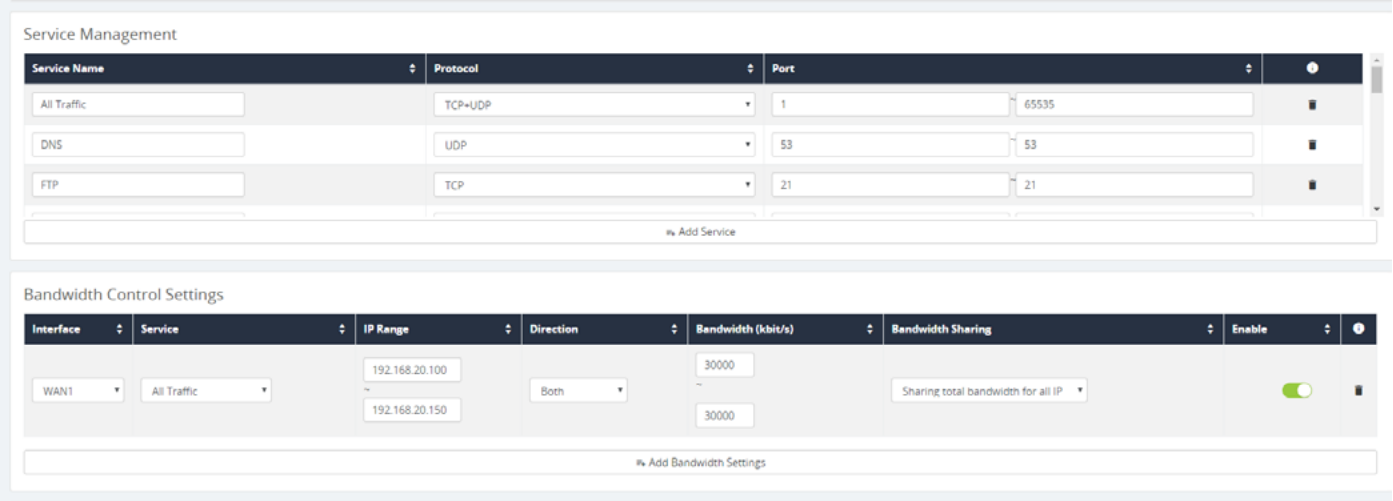
- Calculate the bandwidth requirements for all Bandwidth Control rules and make sure that remaining bandwidth is sufficient for unregulated clients.
- We recommend reserving no more than 80% of the available bandwidth from the ISP in the rules you create. This guarantees that bandwidth will remain available for unspecified IPs.

Configuration Instructions



1. Log into the router interface and navigate to the Bandwidth Control menu: Advanced > Bandwidth Control.
2. Insert the maximum bandwidth values into the appropriate Interface Bandwidth Setting fields (second menu on the page). In this example, only the WAN1 interface is being used.
3. Click the **Add** button under the Bandwidth Control Settings menu. A new entry line will appear for adding bandwidth management rules.
4. Create rules to regulate the bandwidth as needed.
5. After all of the rules have been created, click the **Apply** button to save the new configuration.
6. See the next page for additional information about the example shown above.

Menu Configuration Example



The above example shows the IP range of a Guest Network. We do not want guests using all of our bandwidth downloading movies or games.

- Enter the IP Range of the Guest Network under IP Range.
- Direction has been set to Both.
- Bandwidth has been set to 30,000kbits. Enough for a few guests to stream content, and browse the Internet.

IPSec Differences Between AN-300 and AN-310 Routers

Differences in Securing the IPSec Payload Between AN-300 and AN-310 Routers

AN-300 Router

The legacy AN-300 router uses two methods for securing the IP data transmitted through the tunnel.

7. **AH (Authentication Header) Protocol:** This method is only used to provide authentication services to ensure data integrity of the payload, while traversing the tunnel.
8. **AH + ESP (Authentication Header + Encapsulating Security Payload) Protocol:** This method is used to independently provide authentication services via AH protocol and confidentiality services via ESP protocol

    Note - the protocols are used separately in this method. AH singularly provides authentication and ESP singularly provides confidentiality.

AN-310 Router

The AN-310 router also uses two methods for securing the IP data transmitted through the tunnel.

1. **AH (Authentication Header) Protocol:** Same as the AN-300 router, the AH protocol is used for authentication purposes.
2. **ESP (Encapsulating Security Payload):** This method provides both authentication *and* confidentiality services.

Why the protocol change was made from AN-300 to AN-310 Routers

Per RFC 8221 ,created in 2017, it states that *...Encryption Must Be Authenticated. Encryption without authentication is not effective and MUST NOT be Used.*

RFC 8221 also points out that the AH+ESP method *...is NOT RECOMMENDED* as it is slow and bulky in nature. Due to the IETF recommendation, the AN-310 router's IPSec implementation has removed the **AH + ESP** method as an option.

How it affects the creation of a tunnel between AN-300 to AN-310 Routers

Due to the changes mentioned above, both the AN-300 and AN-310 routers are able to make a connection, but not all configurable options work.

The AN-300 and AN-310 routers, in regards to **AH** and **ESP**, interact in the following ways:

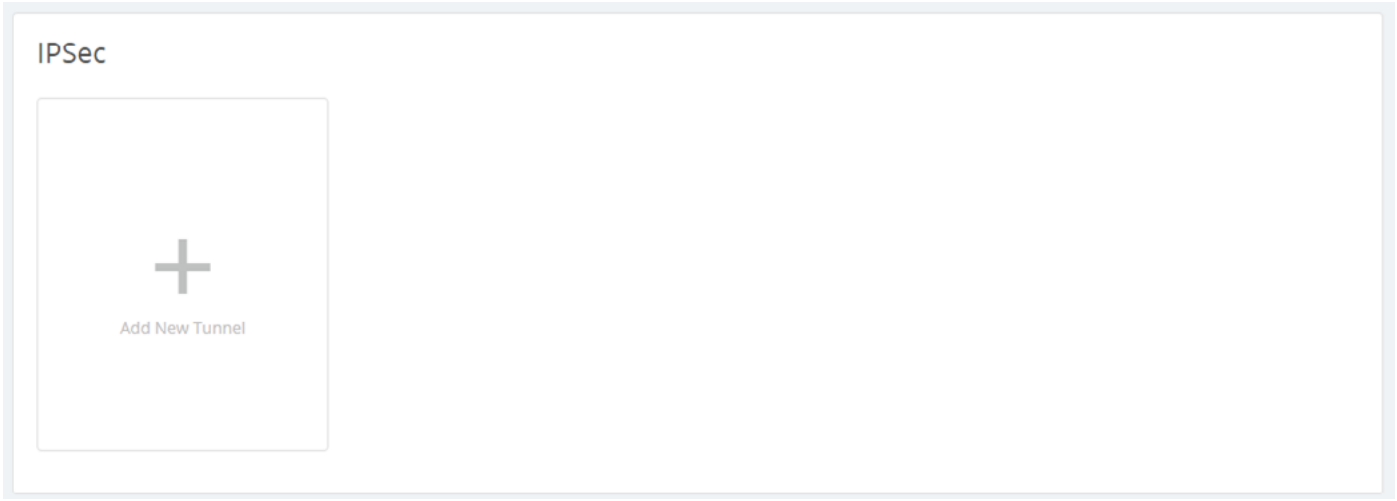
- **AH disabled on both devices:** 310 (ESP only)----300 (ESP only) ....Successful connection
- **AH enabled on both devices:** 310 (AH only)---300 (AH+ESP)....Unsuccessful connection

Using IPSec VPN (Gateway to Gateway)

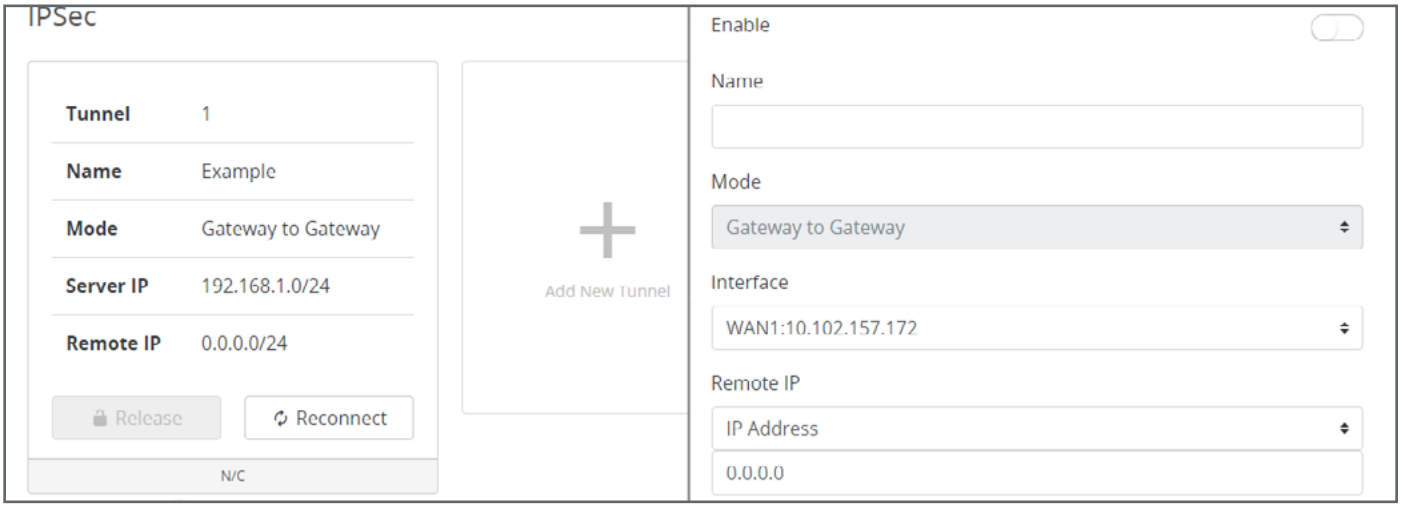
Path – Advanced > VPN > IPSec

IPSec Section of VPN Settings

Configure a VPN between two routers so that devices on each network can communicate through the VPN tunnel.

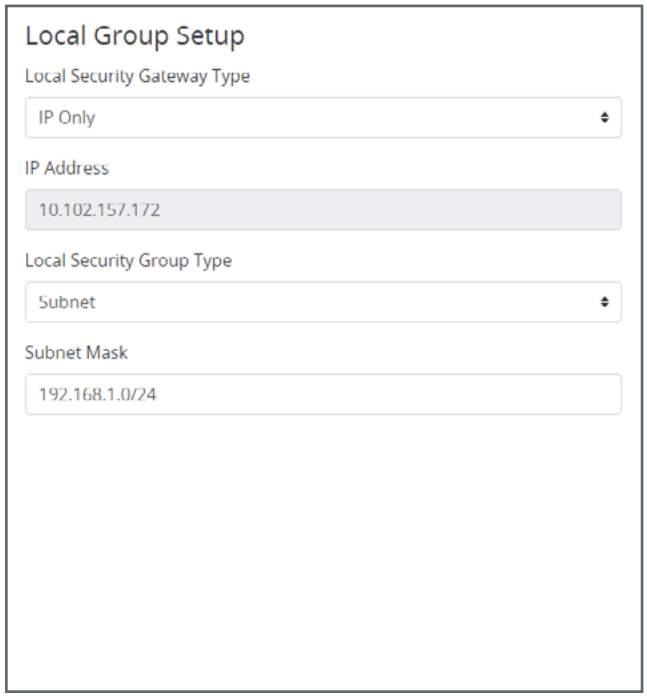


Click the **+ Add New Tunnel** button to create a new IPSec tunnel.



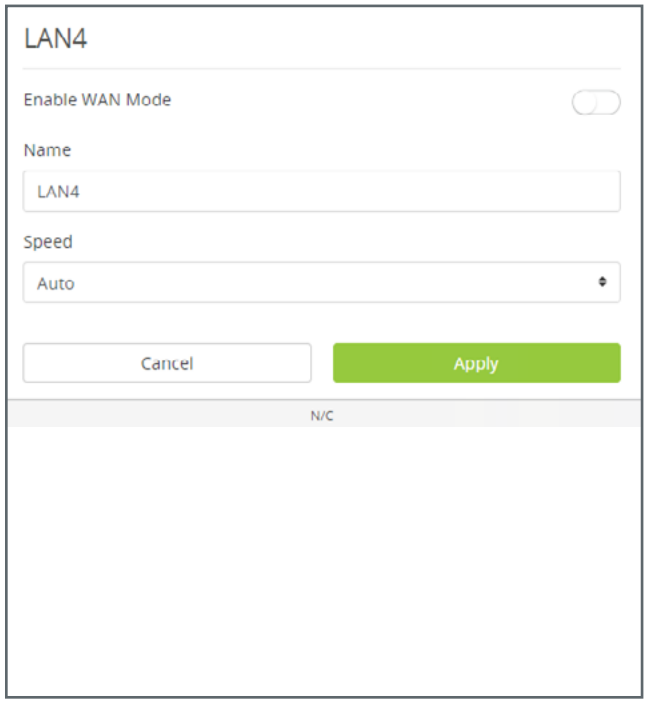
- **Tunnel No. –** Number identifying the tunnel being configured.
- **Tunnel Name –** Name for the tunnel to make it easily identifiable.
- **Interface –** Port the VPN will connect through. Options: WAN1, WAN2, and WAN3.
- **Enable –** Check the box to enable the new tunnel.
- **Mode –** Gateway to Gateway is the only option.

Local Group Setup



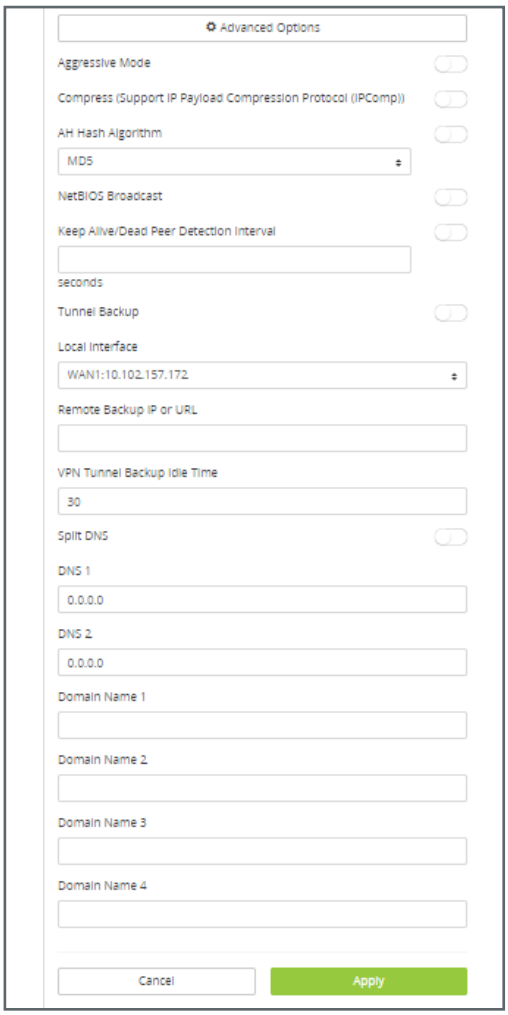
- **Local Security Gateway Type –** Options presented in the drop-down change the availabe fields.
  - IP Only.
  - IP and Domain Name.
  - IP and Email Address.
  - Dynamic IP and Domain Name.
  - Dynamic IP and Email Address.
- **IP Address –** IP address for the local group.
- **Local Security Group Type –** Options presented in the drop-down change the available fields.
  - IP Address.
  - Subnet.
  - IP Range.
- **IP Address –** IP address for the network device connecting to the local group.
- **Subnet Mask –** Subnet mask for the connection.

Remote Group Setup



- **Remote Security Gateway Type –** Options presented in the drop-down change the available fields.
  - IP Only.
  - IP and Domain Name.
  - IP and Email Address.
  - Dynamic IP and Domain Name.
  - Dynamic IP and Email Address.
- **IP Address –** IP address for the local group.
- **Remote Security Group Type –** Options presented in the drop-down change the available fields.
  - IP Address.
  - Subnet.
  - IP Range.
- **IP Address –** IP address for the network device connecting to the local group.
- **Subnet Mask –** Subnet mask for the connection.

Advanced Options



- **Aggressive Mode –** Check the box to enable Aggressive Mode.
- **Compress (Support IP Payload Compression Protocol (IPComp)) –** Check to enable Compression.
- **AH Hash Algorithm –** Check to enable AH Hash Algorithm Select the type from the drop-down.
- **NetBIOS Broadcast –** Check to enable NetBIOS Broadcast.
- **Keep Alive/Dead Peer Detection Interval (Seconds) –** Check to enable and set the Dead Peer Detection Interval.
- **Tunnel Backup –** Check to enable Tunnel Backup. Enter the following values to configure the setting:
  - Remote Backup IP Address – Enter the IP address of the backup tunnel.
  - Local Interface – Select which port to use for connecting the backup tunnel.
  - Remote Backup IP or URL – IP address or Domain to fall back to in case of disconnection.
  - VPN Tunnel Backup Idle Time (seconds) – Set the amount of time to wait before switching to the backup tunnel. (Range: 30~999)
- **Split DNS –** Check to enable Split DNS.
  - DNS1/DNS2 – Enter the Split DNS addresses.
  - Domain Name 1/2/3/4 – Enter up to four domain names.

Using OpenVPN with Dual-WAN

The OpenVPN feature has been updated to give you the option to make **TCP** or **UDP** connections.

- **UDP** offers faster speeds, lower latency, and is the preferred OpenVPN connection method. In rare occasions, UDP can be less reliable, because the protocol does not guarantee delivery of the packets.
- **TCP** offers a more stable connection, as the protocol guarantees delivery of the packets and is less likely to be blocked by firewalls. This method tends to slow transfer rates down.

> **Note –** For Dual-WAN Connections you must use TCP protocol.

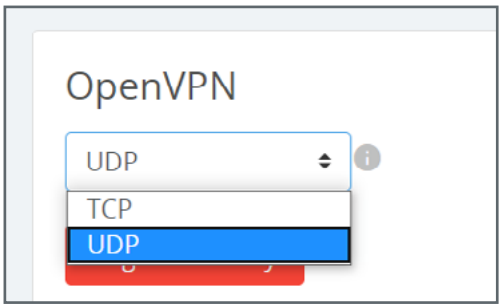
Path – Advanced > VPN > OpenVPN

As indicated by the green box, there's a new drop-down list that allows you to select UDP or TCP. OpenVPN uses UDP connections by default, so there's no need to download a new config file, or Regenerate a key if you just updated the firmware.
If you do change the **Connection Type** from the drop-down, follow the steps below.

> **Note –** At any given time, you can only use one Connection Type (TCP or UDP) with your established OpenVPN tunnels.
> Each time you export a config file it will follow the Connection Type selected from the drop-down menu.

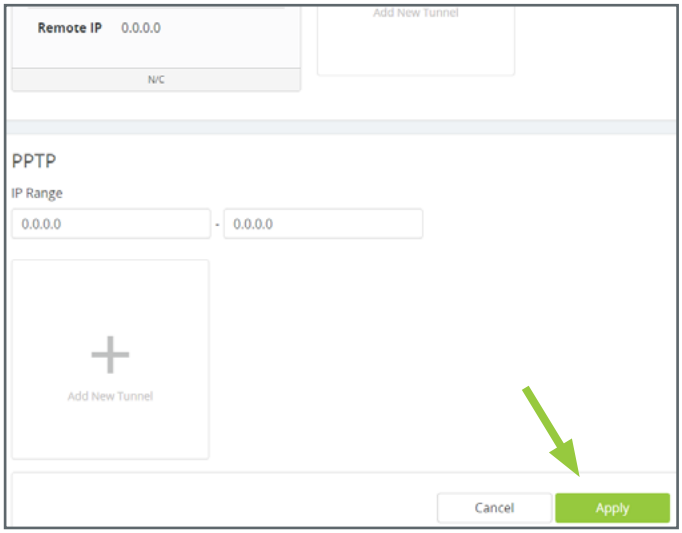
To change the Connection Type for existing OpenVPN configurations:

1. Select a **Connection Type** from the drop-down.

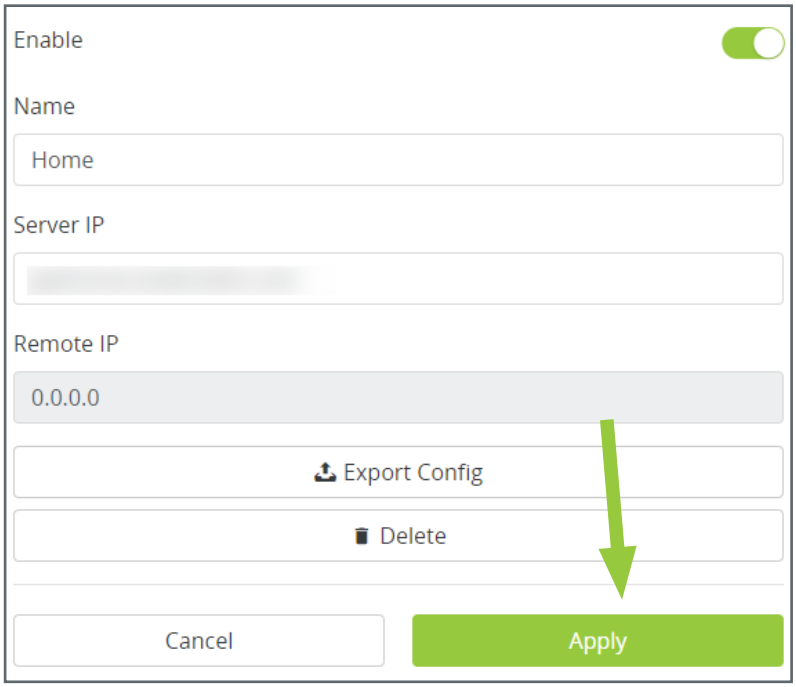


Click the info button for further information on TCP and UDP connections.

2. Scroll down the page and click the **Apply** button in the lower right corner.



3. Click your **Config** file and download the tunnel created before you switched the **Connection Type**.

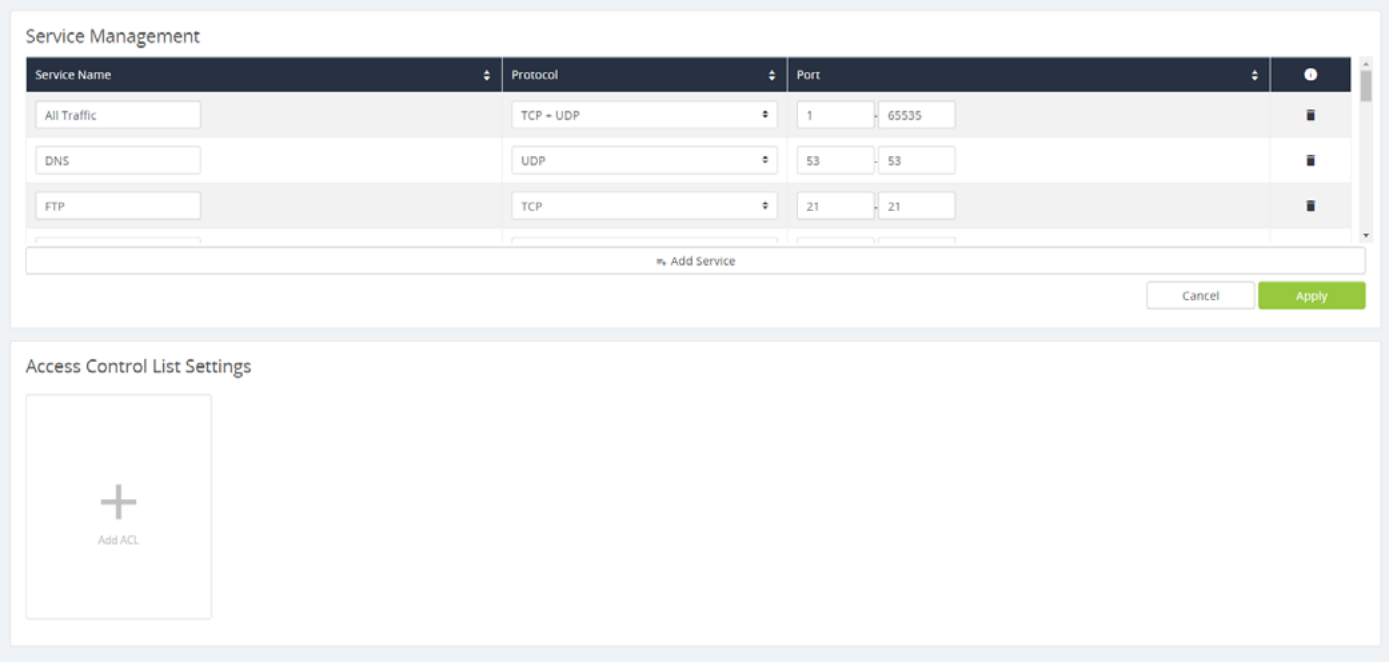


Using ACLs

Path – Advanced > ACLs

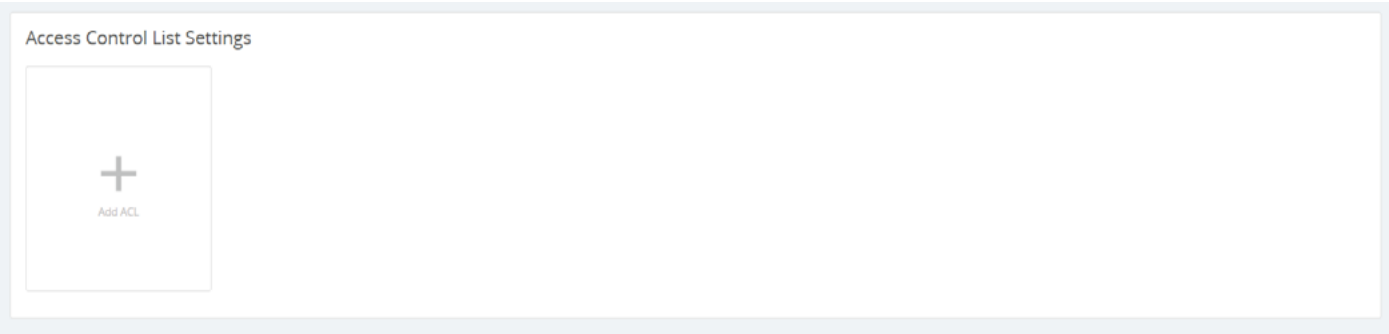
Use Access Control List entries to restrict undesired port use.

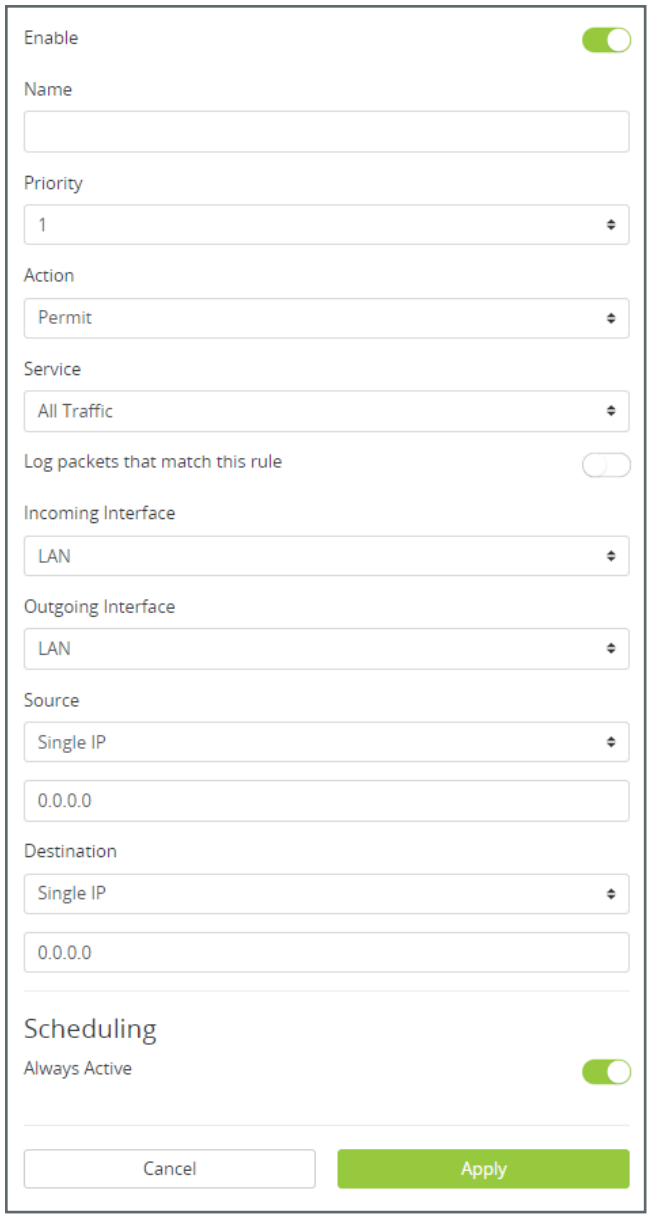
Service Management Settings



- **Service Name –** Enter a name to identify the service rule.
- **Protocol –** Set the protocol the service rule affects.
- **Port –** Set the start and end port to enforce the service rule on.
- **Trashcan –** Click the Trashcan to delete a service rule.

Access Control List Settings





- **Enable –** Check the box to enable the rule.
- **Name –** Enter a name to identify the rule.
- **Priority –** Select the priority of the rule from the drop-down. The rules are enforced in order: Priority 1 takes precedence over all other rules (2, 3, 4...).
- **Action –** Displays whether the rule is set to permit or deny traffic.
- **Service –** Describes the traffic and ports enforced by the rule.
- **Log packets that match this rule –** Enable to record activity in the system log.
- **Incoming Interface –** Select LAN or WAN port from the drop-down.
- **Outgoing Interface –** Select LAN or WAN port from the drop-down.
- **Source –** Single IP, IP Range, or MAC address.
- **Destination –** Single IP or IP Range.
- **Scheduling –** Describes when the rule is in effect.
- **Add –** Click to add a new Access Control Rule.

Adding a New Access Control Rule

1. Click Add ACL to open above window.
2. Set the desired Action, Service, and Log settings using the drop-downs.
3. Select the Incoming and Outgoing Interface, of the traffic to control, from the drop-down.
4. Enter a Source IP address, IP range, or MAC address the traffic will come from.
5. Enter a Destination IP address or range the traffic will be traveling toward.
6. Set up scheduling for when the rule will be active. If the rule needs to be active at all times, leave Time set to Always.
7. Click Apply to enable the newly created rule.