Balance

User Manual

Peplink Products:
20X Pro

Peplink Balance Firmware 8.2.0
March 2022

Table of Contents

Introduction and Scope

Peplink Balance routers provide link aggregation and load balancing across multiple WAN connections. We develop products and technologies that can help you build SD-WAN networks with unbreakable connection resilience, unmatched deployment flexibility, and intuitive ease of use.

Our product and technology focus has always been on WAN virtualization and the intelligent use of multiple WAN links at the same time to increase reliability and bandwidth whilst reducing costs.
We have two key WAN virtualization technologies, Intelligent load balancing for Internet access and SpeedFusion VPN Bonding for secure branch to branch connectivity.

The Peplink MediaFast series are a range of routers capable of content caching.
Designed with education and entertainment in mind, MediaFast downloads and accelerates video, iTunes iOS updates, app downloads, and other content for uninterrupted learning and fun anytime.
The MediaFast can prefetch content during off-peak hours, saving connectivity costs and reducing network burden during busy times.

This manual applies to the following Peplink Balance products:

- Peplink Balance 20X Pro

The manual covers setting up your Peplink Balance or MediaFast and provides a collection of case studies detailing the advanced features of the Peplink Balance.

1 Glossary

The following terms, acronyms, and abbreviations are frequently used in this manual:

Term	Definition
3G	3rd generation standards for wireless communications (e.g., HSDPA)
4G	4th generation standards for wireless communications (e.g., LTE)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EVDO	Evolution-Data Optimized
FQDN	Fully Qualified Domain Name
HSDPA	High-Speed Downlink Packet Access
HTTP	Hyper-Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol

LAN	Local Area Network
MAC Address	Media Access Control Address
MTU	Maximum Transmission Unit
MSS	Maximum Segment Size
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network
210+	Refers to Peplink Balance 210/310/380/580/710/1350/2500
380+	Refers to Peplink Balance 380/580/710/1350/2500

2 Product Features

Peplink Balance Series products enable all LAN users to share broadband Internet connections and provide advanced features to enhance Internet access. The following is a list of supported features:

WAN

- Multiple public IP support (DHCP, PPPoE, static IP address)
- Static IP support for PPPoE
- 10/100/1000Mbps Ethernet connection in full/half duplex
- Built-in HSPA and EVDO cellular modems
- USB mobile connection **(only one USB modem can be connected at a time)**
- Drop-in mode on selectable WAN port with MAC address passthrough **n**etwork address translation (NAT) / port address translation (PAT)

- Inbound and outbound NAT mapping
- Multiple static IP addresses per WAN connection
- MAC address clone
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS (supported service providers: changeip.com, dyndns.org, no-ip.org,tzo.com, and DNS-O-Matic)
- Ping, DNS lookup, and HTTP-based health check
- WAN throughput and consistency diagnosis
- WAN to WAN speed test
- USB Ethernet Adapter support

LAN

- DHCP server on LAN
- Extended DHCP option support
- Static routing rules
- Local DNS proxy server
- 802.1q VLANs
- Port-based VLANs
- Virtual Network Mapping

VPN

- Secure SpeedFusion^{TM}
- SpeedFusion performance analyzer
- X.509 certificate support
- Bandwidth bonding and failover among selected WAN connections
- Ability to route traffic to a remote VPN peer
- Optional pre-shared key setting
- Layer 2 bridging
- Layer 2 Peer Isolation
- SpeedFusion^{TM} throughput, ping, and traceroute tests
- Built-in L2TP / PPTP / OpenVPN VPN server
- Authenticate L2TP / PPTP clients using RADIUS and LDAP servers
- Multi-Site PepVPN Profile
- IPsec VPN for network-to-network connections
- L2TP / PPTP and IPsec passthrough
- Simultaneous L2 & L3 VPN tunnel between the same pair of devices

Inbound Traffic Management

- TCP/UDP traffic redirection to dedicated LAN server(s)
- Inbound link load balancing by means of DNS

Outbound Policy

- Link load distribution per TCP/UDP service
- Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms
- Time-based scheduling

AP Controller

- Configure and manage Pepwave AP devices
- Review the status of connected AP

QoS

- Quality of service for different applications and custom protocols
- User group classification for different service levels
- Bandwidth usage control and monitoring on group- and user-level
- Application prioritization for custom protocols and DSL optimization

Firewall

- Outbound (LAN to WAN) firewall rules
- Inbound (WAN to LAN) firewall rules per WAN connection
- Intrusion detection and prevention
- Specification of NAT mappings
- Web blocking
- Application blocking
- Time-based scheduling
- Outbound firewall rules can be defined by destination domain name

Captive Portal

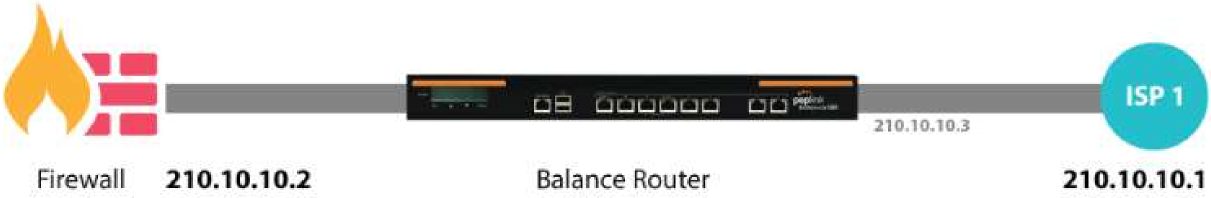
- Social Wi-Fi Hotspot Support
- Splash screen of open networks, login page for secure networks
- Customizable built-in captive portal
- Supports linking to outside page for captive portal

Other Supported Features

- Easy-to-use web administration interface
- HTTP and HTTPS support for web administration interface
- Configurable web administration port and administrator password
- Read-only user for web admin
- Shared-IP drop-in mode
- Authentication and accounting by RADIUS server for web admin
- Firmware upgrades, configuration backups, ping, and traceroute via web administration interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Remote reporting to Peplink Balance reporting server
- Hardware high availability via VRRP, with automatic configuration synchronization
- Real-time, hourly, daily and monthly bandwidth usage reports and charts
- Hardware backup via LAN bypass
- Built-in WINS server
- Time server synchronization
- SNMP
- Email notification
- Syslog
- SIP passthrough
- PPTP packet passthrough
- Active sessions
- Active client list
- WINS client list
- UPnP / NAT-PMP
- Event log is persistent across reboots
- IPv6 support
- Support for USB tethering on Android phones

3 Advanced Feature Summary

3.1 Drop-in Mode and LAN Bypass: Transparent Deployment

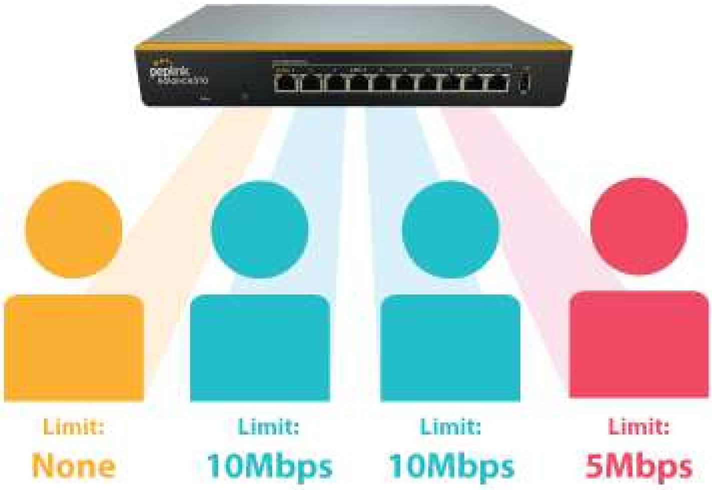


As your organization grows, it may require more bandwidth, but modifying your network can be tedious. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. For any reason your Peplink router looses power, the **LAN Bypass** will safely and automatically bypass the Peplink router to resume your original network connection.

3.2 QoS: Clearer VoIP

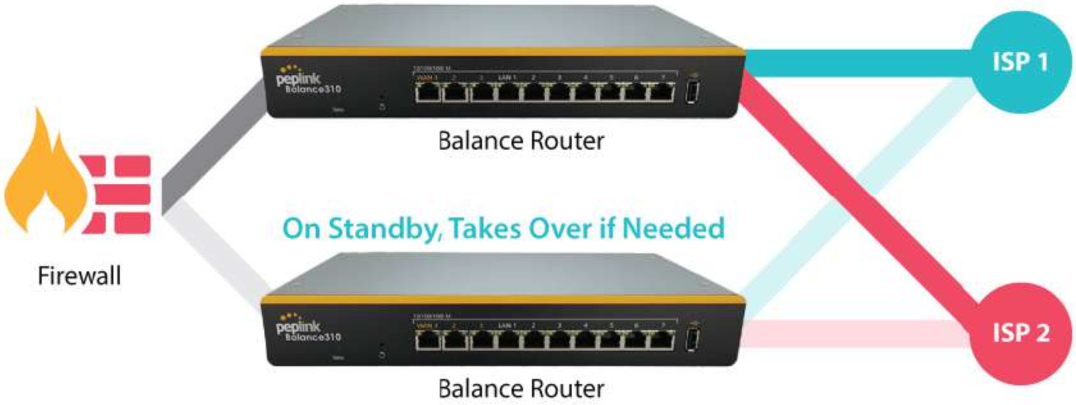
VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP traffic and assign it the highest priority, giving you crystal-clear calls.

3.3 Per-User Bandwidth Control



With per-user bandwidth control, you can define bandwidth control policies for up to 3 groups of users to prevent network congestion. Define groups by IP address and subnet, and set bandwidth limits for every user in the group.

3.4 High Availability via VRRP



When your organization has a corporate requirement demanding the highest availability with no single point of failure, you can deploy two Peplink routers in High Availability mode. With High Availability mode, the second device will take over when needed.

3.5 USB Modem and Android Tethering

For increased WAN diversity, plug in a USB LTE modem as backup. Peplink routers are compatible with over 200 modem types. You can also tether to smartphones running Android 4.1.X and above.

By default, the USB port is "USB Modem" mode. If you need to use it to connect to USB Ethernet Adapter, you need to change it to "USB Ethernet" mode,
https://forum.peplink.com/t/can-i-use-ethernet-adapters-on-the-usb-wan/8327

3.6 Built-In Remote User VPN Support

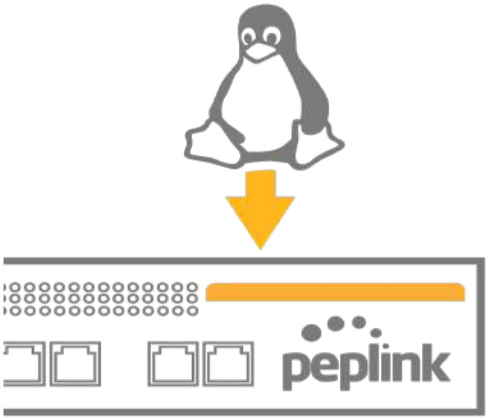
Use OpenVPN or L2TP with IPsec to safely and conveniently connect remote clients to your private network. L2TP with IPsec is supported by most devices, but legacy devices can also connect using PPTP.

Click here for the full instructions on setting up L2TP with IPsec.
Click here for the full instructions on setting up OpenVPN connections

3.7 LACP NIC Bonding

Use 802.3ad to combine multiple LAN connections into a virtual LAN connection. This virtual connection has higher throughput and redundancy in case any single link fails.

3.8 KVM Virtualization



KVM is a virtualisation module that allows administrators using our routers to host a large range of virtual machines. KVM is now supported by some of the MediaFast / ContentHub routers.

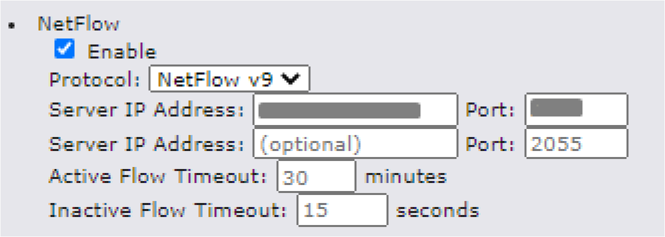
Click here for the full instructions on how to set up KVM
Click here for the full instructions on how to set up KVM with USB Storage

3.9 DPI Engine

The DPI report written in the updated KB article will show further information on InControl2 through breaking down application categories into subcategories.
https://forum.peplink.com/t/updated-ic2-deep-packet-inspection-dpi-reports-and-everything-you-need-to-know-about-it/29658

3.10 NetFlow

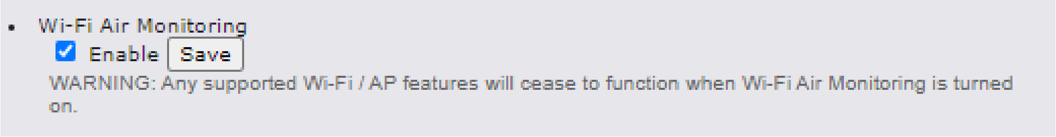
NetFlow protocol is used to track network traffic. Tracking information from NetFlow can be sent to the NetFlow collector, which analyzes data and generates reports for review.
Note: To enable this feature, go to https://<Device's IP>/cgi-bin/MANGA/support.cgi



- NetFlow
  - ☑ Enable
  - Protocol: NetFlow v9
  - Server IP Address: [redacted] Port: [redacted]
  - Server IP Address: (optional) Port: 2055
  - Active Flow Timeout: 30 minutes
  - Inactive Flow Timeout: 15 seconds

3.11 Wi-Fi Air Monitoring

Peplink routers support Wi-Fi "Air Monitoring Mode" which is used to troubleshoot remotely and proactively monitor Wi-Fi and WAN performance. After enabling Wi-Fi Air Monitoring, reports can be viewed under **InControl 2** > **Reports** > **AirProbe Reports**.
Note: To enable this feature, go to https://<Device's IP>/cgi-bin/MANGA/support.cgi



- Wi-Fi Air Monitoring
  - ☑ Enable Save
  - WARNING: Any supported Wi-Fi / AP features will cease to function when Wi-Fi Air Monitoring is turned on.

3.12 SP Default Configuration

The SP Default Configuration feature written in the updated KB article allows for the provisioning of custom made settings (a.k.a. InControl2 configuration) via the Ethernet LAN port and is ideal for those wanting to do a bulk deployment of many Peplink devices.
Note: If you would like to use this feature, please contact your purchase point (Eg.VAD).

3.13 SpeedFusion Cloud Relay

Cloud Service Providers often restrict access to certain applications. With SFC Relay, you can route traffic before going out to the Internet, allowing access to previously restricted applications experienced with the public SpeedFusion Cloud nodes. Available as an add-on for your home router or as an upgradable license to your Peplink router, SFC Relay is sure to impress you and any peers you give access to.
https://forum.peplink.com/t/configure-speedfusion-cloud-relay-server-and-client/6215ca9b017e48e0f3ff2479/

3.14 DNS over HTTPS (DoH)

DoH provides the benefits of communicating DNS information over a secure HTTPS connection in an encrypted manner. The protocol offers increased privacy and confidentiality by preventing data interception and man-in-the-middle attacks.

4 Package Contents

The contents of Peplink Balance product packages are as follows:

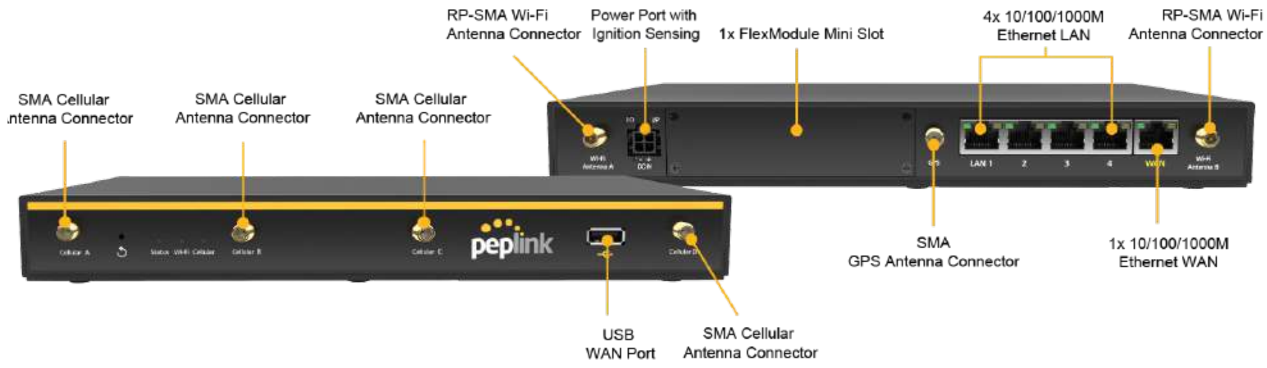
4.1 Peplink Balance 20X Pro

- Peplink Balance 20X Pro
- 2x LTE Antenna, 1x GPS Antenna, 2x Wi-Fi Antenna
- Power adapter
- Information slip

5 Peplink Balance Overview

5.1 Peplink Balance 20X Pro

5.1.1 Panel Appearance


RP-SMA Wi-Fi Antenna Connector
Power Port with Ignition Sensing
1x FlexModule Mini Slot
4x 10/100/1000M Ethernet LAN
RP-SMA Wi-Fi Antenna Connector
SMA Cellular ntenna Connector
SMA Cellular Antenna Connector
SMA Cellular Antenna Connector
SMA GPS Antenna Connector
1x 10/100/1000M Ethernet WAN
USB WAN Port
SMA Cellular Antenna Connector

5.1.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

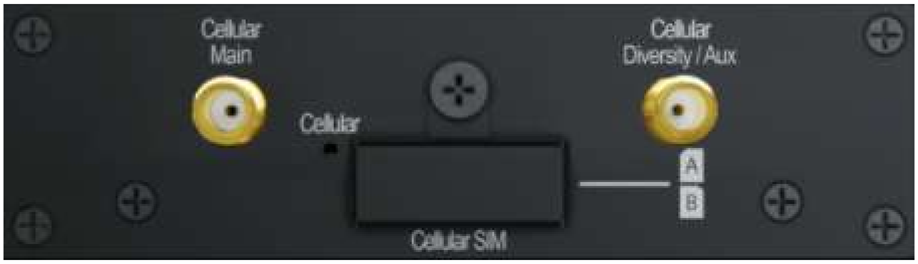
Power and Status Indicators	
Status	OFF – Upgrading firmware
	Red – Booting up or busy
	Blinking red – Boot up error
	Green – Ready

LAN and WAN Ports	
Green LED	ON – 1000 Mbps OFF – 10 / 100 Mbps or port is not connected
Orange LED	Blinking – Data is transferring
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

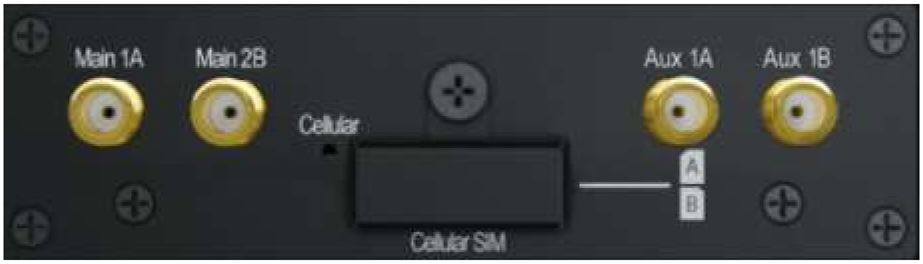
Wi-Fi AP Indicators		
Wi-Fi AP	OFF	Disabled
	ON	Enabled

USB Port	
USB Ports	For connecting a 4G/3G USB modem

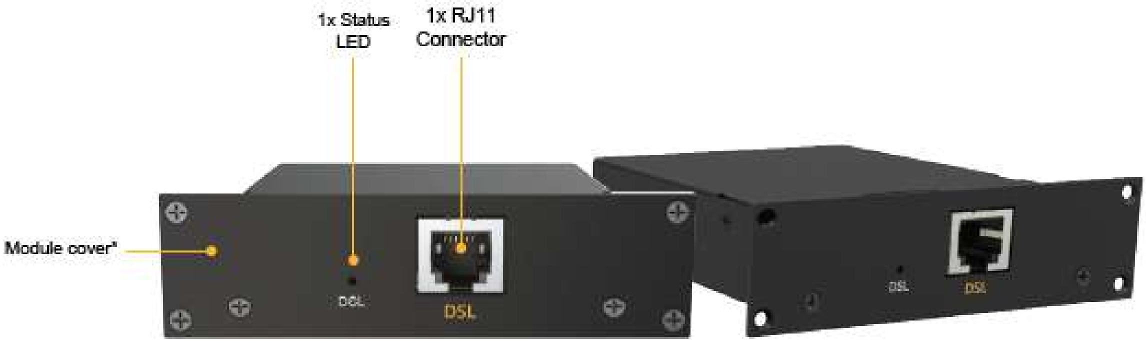
5.1.3 Flex Module Mini



1x LTE-A Module	
Interface	1x Embedded LTE-A Cellular Modems with Redundant SIM Slots
Antenna Connectors	2x SMA Cellular Antenna Connectors
Downlink / Uplink Datarate	300Mbps/50Mbps (CAT-6) 600Mbps/150Mbps (CAT-12)
Power Consumption	10W
Weight	0.83 pounds | 375 grams



1xLTE-A Module	
Interface	1x Embedded LTE-A Cellular Modems with Redundant SIM Slots
Antenna Connectors	4x SMA Cellular Antenna Connectors
Downlink / Uplink Datarate	1.2 Gbps/150 Mbps (CAT-18)
Power Consumption	10W
Weight	0.83 pounds | 375 grams



1x VDSL Module	
Interface	1x RJ11 Connector, 1x Status LED
Power Consumption	9W
Weight	0.44 pounds | 200 grams

6 LCD Display Menu

> HA State: Master/Slave				
	> LAN IP			
	> VIP			
> System Status				
	> System			
		> Firmware ver.		(shows firmware version)
		> Serial number		(shows serial number)
		> System time		(shows current time)
		> System uptime		(shows system uptime since last reboot)
		> CPU load		(shows current CPU loading, 0-100%)
		> LAN		
			> Status	(shows LAN port physical status)
			> IP address	(shows LAN IP address)
			> Subnet mask	(shows LAN subnet mask)
	> Link status			(shows Connected/Disconnected, IP address list)
		> WAN1		
		> WAN2		
		> WAN3*		
	> VPN status			(shows Connected/Disconnected)
		>*VPN Profile 1*		
		>*VPN Profile 2*		
		>*…*		
		>*VPN Profile n*		
	> Link usage			
		> Throughput in		(shows transfer rate in Kbps)
			> WAN1	
			> WAN2	
			> WAN3*	
		> Throughput out		(shows transfer rate in Kbps)
			> WAN1	
			> WAN2	
			> WAN3*	
	> Data Transfered			(shows volume transferred since last reboot in MB)
		> WAN1		
		> WAN2		
		> WAN3*		
> Maintenance				
	> Reboot > Reboot? (Yes/No)			(to reboot the unit)
	> Factory default		> Factory default? (Yes/No)	(to restore factory defaults)
> LAN config				
	> Port speed			(shows port speed: Auto, 10baseT-FD, 10baseT-HD, 100baseTx-FD, 100baseTx-HD, 1000baseTx-FD)
		> LAN		
		> WAN1		
		> WAN2		
		> WAN3*		

*Layout continues as such for all available WAN ports

7 Installation

The following section details connecting the Peplink Balance to your network:

7.1 Preparation

Before installing your Peplink Balance, please prepare the following:

- At least one Internet/WAN access account
- For each network connection, one 10/100BaseT UTP cable with RJ45 connector, one 1000BaseT Cat5E UTP cable for the Gigabit port, or one USB modem for the USB WAN port
- A computer with the TCP/IP network protocol and a web browser installed— Supported browsers include Microsoft Internet Explorer 11 or above, Mozilla Firefox 24 or above, Apple Safari 7 or above, and Google Chrome 18 or above.

7.2 Constructing the Network

At the high level, construct the network according to the following steps:

1. With an Ethernet cable, connect a computer to one of the LAN ports on the Peplink Balance. For Peplink Balance models that support multiple connections, repeat with different cables connect up to 4 computers.
2. With another Ethernet cable, connect the WAN/broadband modem to one of the WAN ports on the Peplink Balance. Repeat using different cables to connect from two to 13 WAN/broadband connections or connect a USB modem to the USB WAN port.
3. Connect the provided power adapter or cord to the power connector on the Peplink Balance, and then plug the power adapter into a power outlet.

8 Basic Configuration

8.1 Connecting to the Web Admin Interface

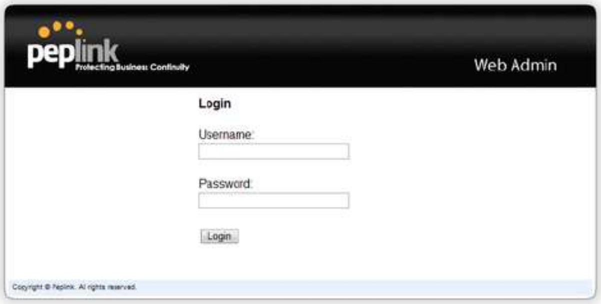
Start a web browser on a computer that is connected with the Peplink Balance through the LAN.

To connect to the web admin of the Peplink Balance, enter the following LAN IP address in the address field of the web browser:

https://192.168.1.1

(This is the default LAN IP address of the Peplink Balance.) Enter the following to access the web admin interface.

Username: admin
Password: admin



Login

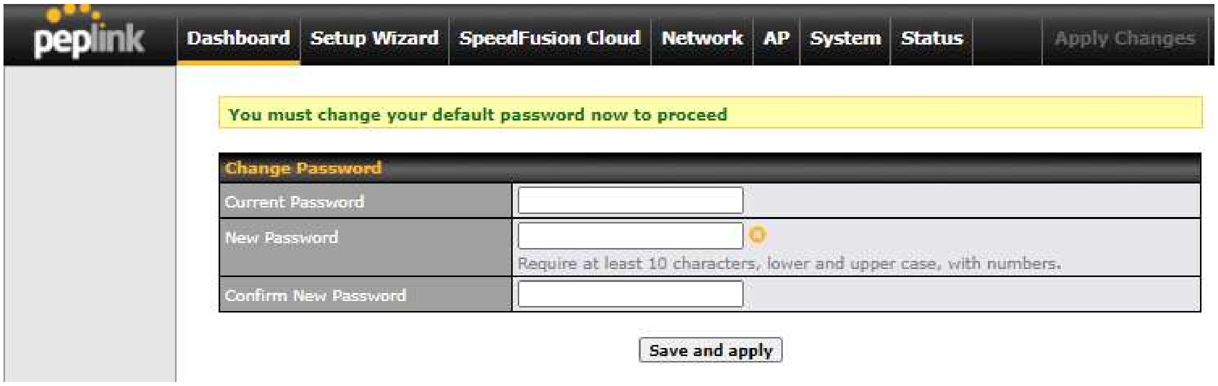
Username:

Password:

Copyright © Peplink. All rights reserved.

(This is the default admin user login of the Peplink Balance.)
You must change the default password on the first successful logon.
Password requirements are: A minimum of 10 lower AND upper case characters, including at least 1 number.

When HTTP is selected, the URL will be redirected to HTTPS by default.



You must change your default password now to proceed

Change Password	
Current Password	
New Password	Require at least 10 characters, lower and upper case, with numbers.
Confirm New Password	

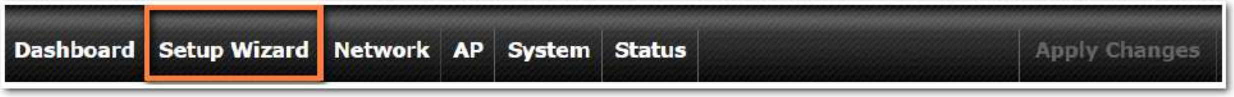
After successful login, the **Dashboard** of the web admin interface will be displayed.

Important Note
The **Save** button causes the changes to be saved. Configuration changes (e.g., WAN, LAN, admin settings, etc.) take effect after clicking the **Apply Changes** button on each page's top-right corner.

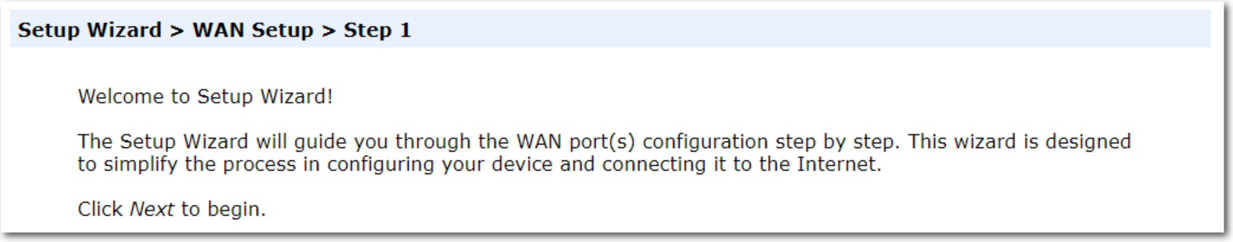
8.2 Configuration with the Setup Wizard

The Setup Wizard simplifies the task of configuring WAN connection(s) by guiding the configuration process step-by-step.

To begin, click **Setup Wizard** after connecting to the web admin interface.



Click **Next >>** to begin.



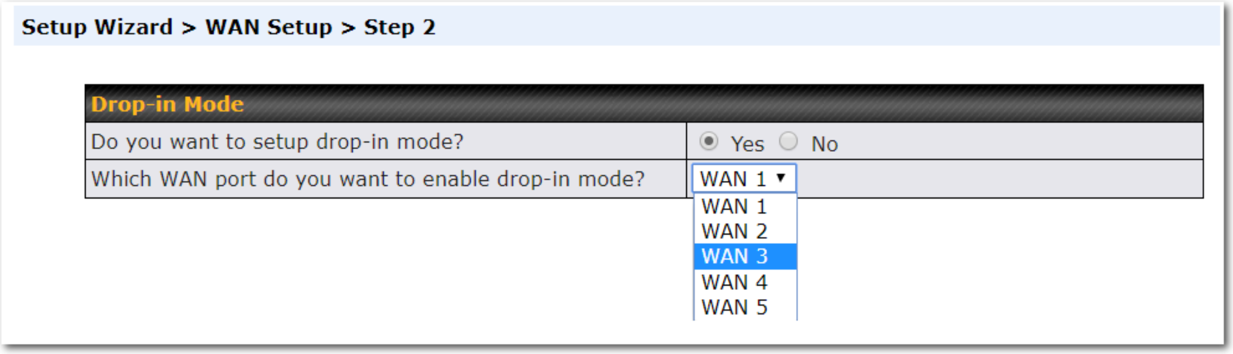
Setup Wizard > WAN Setup > Step 1

Welcome to Setup Wizard!

The Setup Wizard will guide you through the WAN port(s) configuration step by step. This wizard is designed to simplify the process in configuring your device and connecting it to the Internet.

Click *Next* to begin.

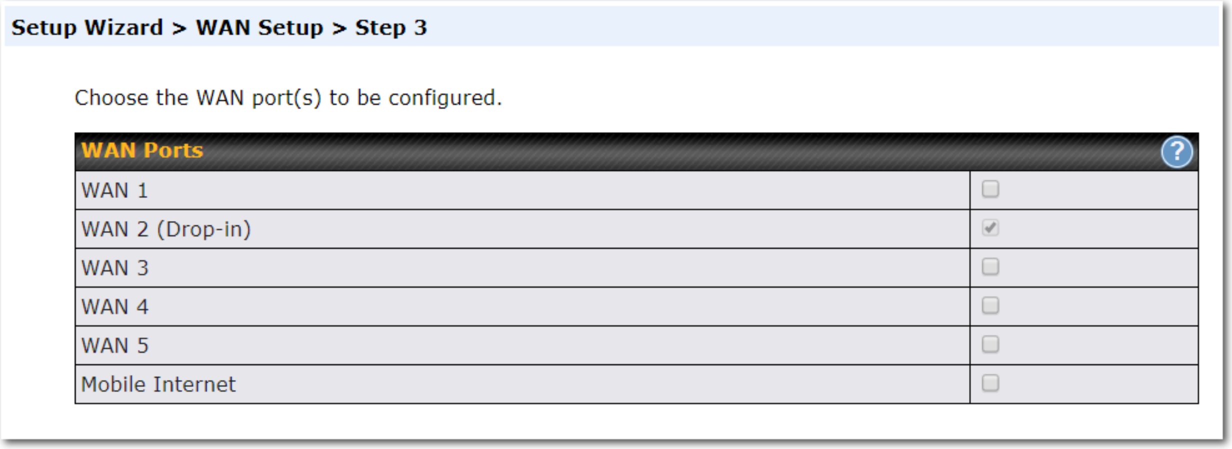
Select **Yes** if you want to set up drop-in mode using the Setup Wizard.



Setup Wizard > WAN Setup > Step 2

Drop-in Mode	
Do you want to setup drop-in mode?	● Yes ○ No
Which WAN port do you want to enable drop-in mode?	WAN 1 ▾

Click on the appropriate checkbox(es) to select the WAN connection(s) to be configured. If you have chosen to configure drop-in mode using the Setup Wizard, the WAN port to be configured in drop-in mode will be checked by default.

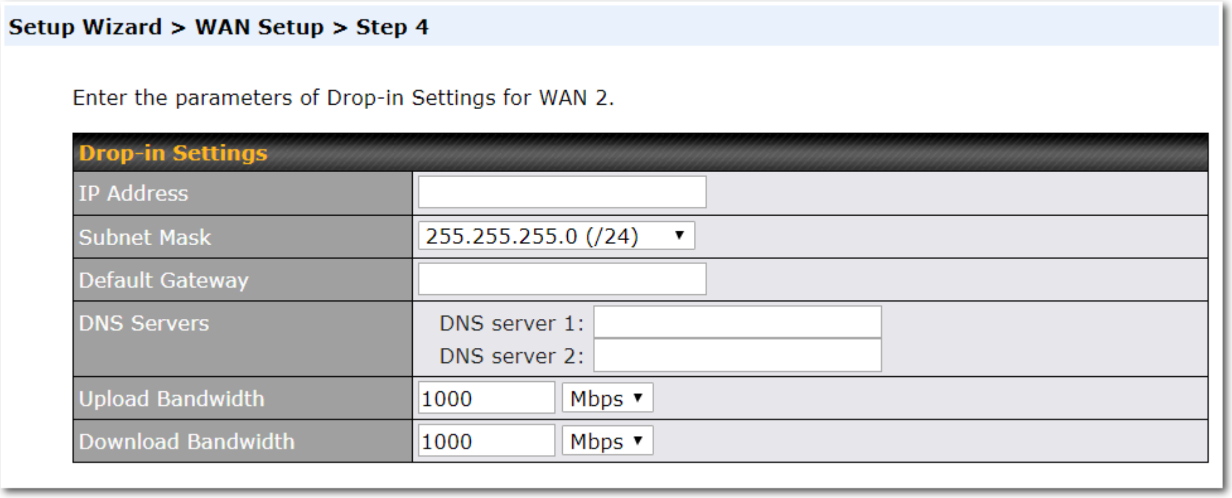


Setup Wizard > WAN Setup > Step 3

Choose the WAN port(s) to be configured.

WAN Ports	
WAN 1	□
WAN 2 (Drop-in)	☑
WAN 3	□
WAN 4	□
WAN 5	□
Mobile Internet	□

If drop-in mode is going to be configured, the setup wizard will move on to **Drop-in Settings**.

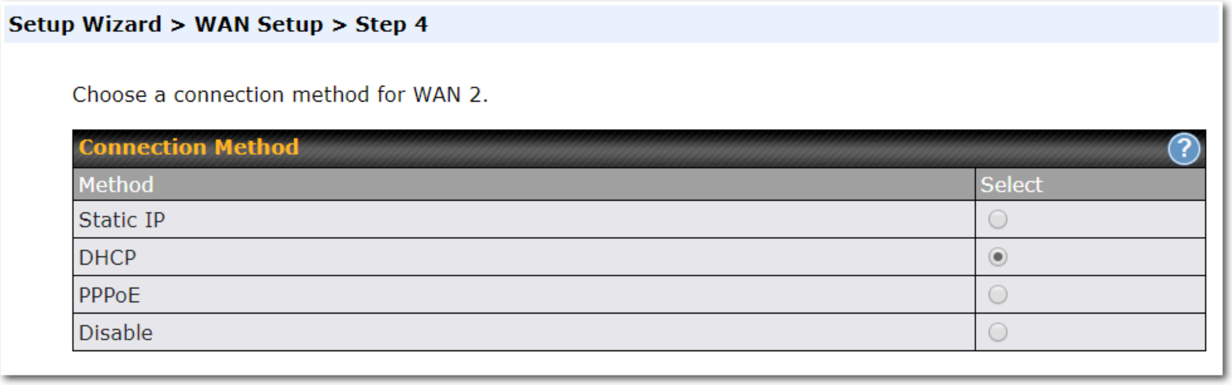


Setup Wizard > WAN Setup > Step 4

Enter the parameters of Drop-in Settings for WAN 2.

Drop-in Settings	
IP Address	
Subnet Mask	255.255.255.0 (/24) ▼
Default Gateway	
DNS Servers	DNS server 1: DNS server 2:
Upload Bandwidth	1000 Mbps ▼
Download Bandwidth	1000 Mbps ▼

If you are not using drop-in mode, select the connection method for the WAN connection(s) from the following screen:



Setup Wizard > WAN Setup > Step 4

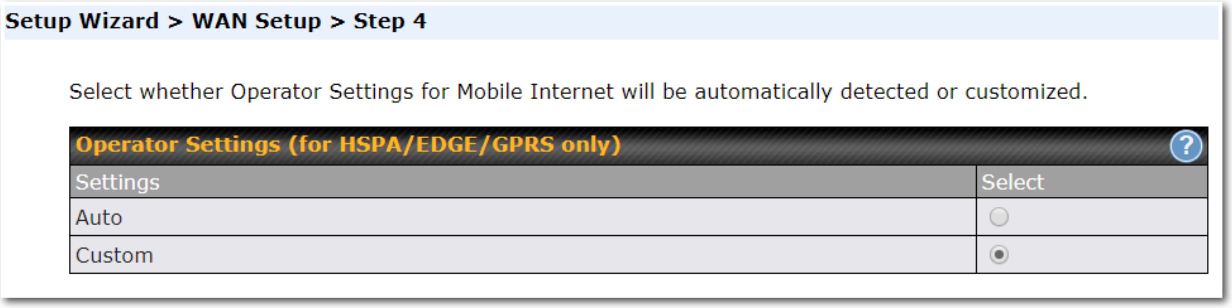
Choose a connection method for WAN 2.

Connection Method

Method	Select
Static IP	○
DHCP	●
PPPoE	○
Disable	○

Depending on the selection of connection type, further configuration may be needed. For example, PPPoE and static IP require additional settings for the selected WAN port. Please refer to **Section 13, Configuring the WAN Interface(s)** for details on setting up DHCP, static IP, and PPPoE.

If **Mobile Internet Connection** is checked, the setup wizard will move on to **Operator Settings**.



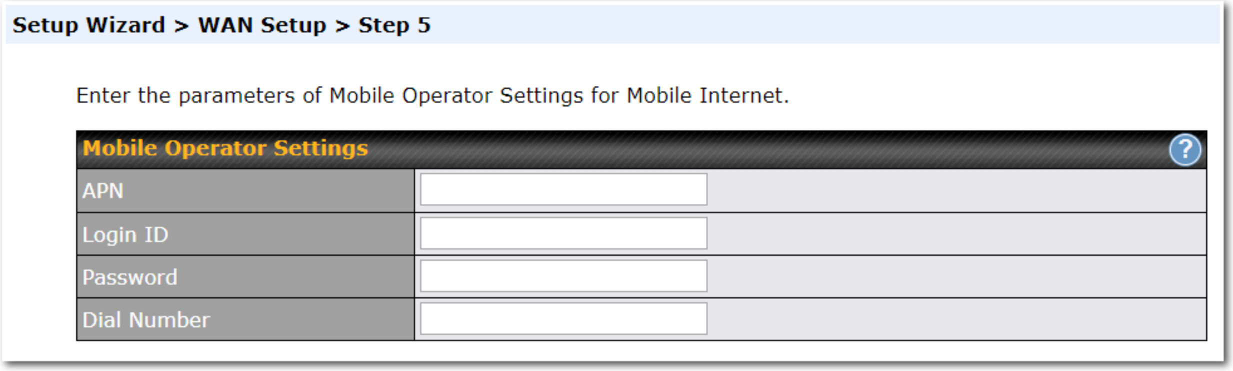
Setup Wizard > WAN Setup > Step 4

Select whether Operator Settings for Mobile Internet will be automatically detected or customized.

Operator Settings (for HSPA/EDGE/GPRS only)

Settings	Select
Auto	○
Custom	●

If **Custom Mobile Operator Settings** is selected, APN parameters are required. Some service providers may charge a fee for connecting to a different APN. Please consult your service provider for the correct settings.

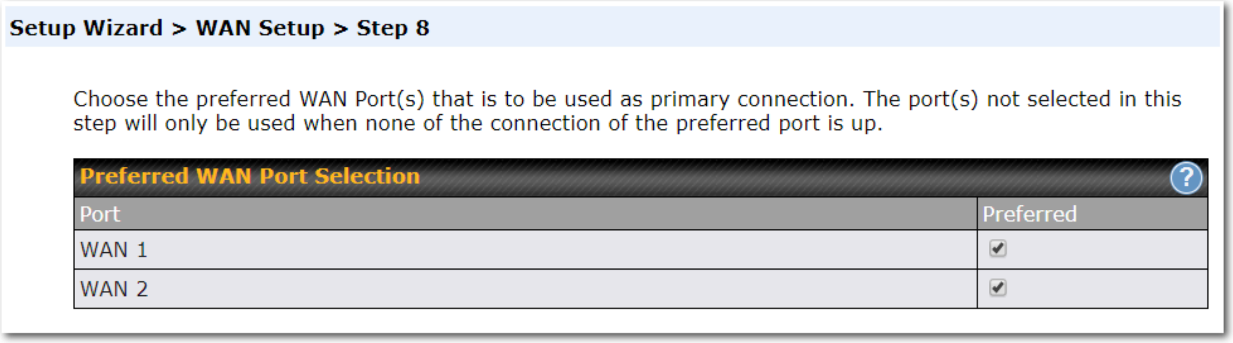


Setup Wizard > WAN Setup > Step 5

Enter the parameters of Mobile Operator Settings for Mobile Internet.

Mobile Operator Settings	
APN	
Login ID	
Password	
Dial Number	

Click on the appropriate check box(es) to select the preferred WAN connection(s). Connection(s) not selected in this step will be used as a backup only. Click **Next >>** to continue.



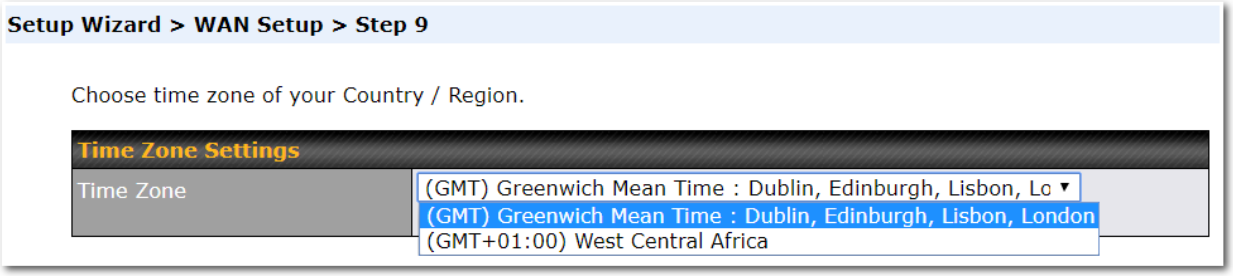
Setup Wizard > WAN Setup > Step 8

Choose the preferred WAN Port(s) that is to be used as primary connection. The port(s) not selected in this step will only be used when none of the connection of the preferred port is up.

Preferred WAN Port Selection

Port	Preferred
WAN 1	☑
WAN 2	☑

Choose the time zone of your country/region. Check the box **Show all** to display all time zone options.



Setup Wizard > WAN Setup > Step 9

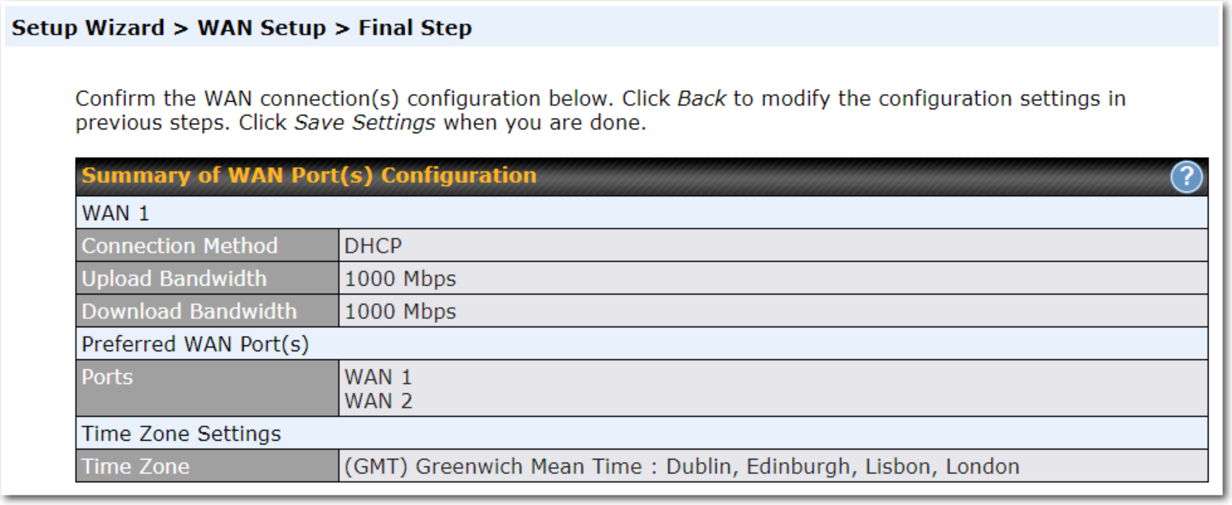
Choose time zone of your Country / Region.

Time Zone Settings

Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lo ▾

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
(GMT+01:00) West Central Africa

Check in the following screen to make sure all settings have been configured correctly, and then click "**Save Settings"** to confirm.



Setup Wizard > WAN Setup > Final Step

Confirm the WAN connection(s) configuration below. Click *Back* to modify the configuration settings in previous steps. Click *Save Settings* when you are done.

Summary of WAN Port(s) Configuration	
WAN 1	
Connection Method	DHCP
Upload Bandwidth	1000 Mbps
Download Bandwidth	1000 Mbps
Preferred WAN Port(s)	
Ports	WAN 1 WAN 2
Time Zone Settings	
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

After finishing the last step in the setup wizard, click **Apply Changes** on the page header to allow the configuration changes to take effect.

9 SpeedFusion Cloud

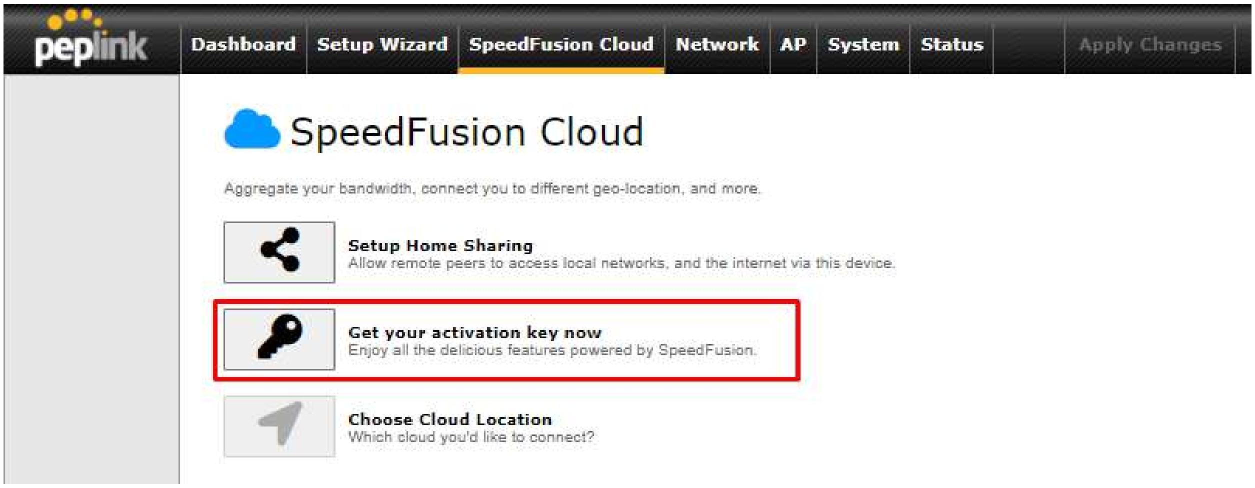
With Peplink products, your device is able to connect to SpeedFusion Cloud without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.*

Hosted by peplink
SpeedFusion
Cloud
peplink

*SpeedFusion Cloud is supported in firmware version 8.1.0 and above. SpeedFusion Cloud is a subscription basis. SpeedFusion Cloud license can be purchased at https://store.peplink.com/ **> Cloud Solutions > SpeedFusion Cloud Service**.

9.1 Activate SpeedFusion Cloud Service

You are entitled to a 30-day free period with 100GB of SpeedFusion usage upon activation of the SpeedFusion Cloud service. This offer is limited to once per device. To get your activation key please visit SpeedFusion Cloud.



SpeedFusion Cloud

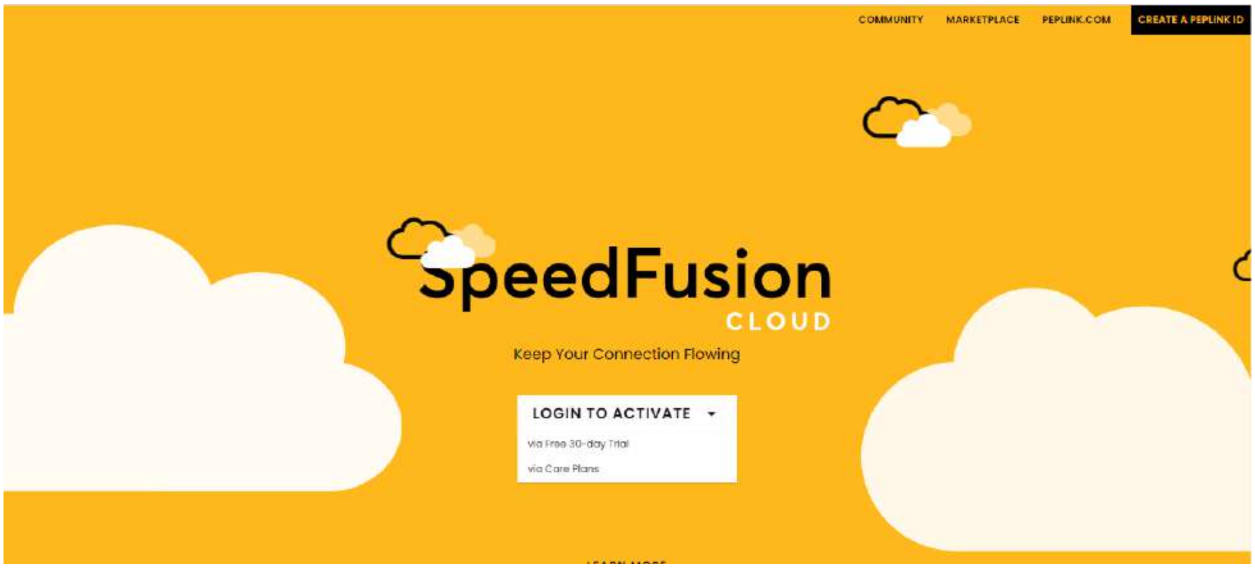
Aggregate your bandwidth, connect you to different geo-location, and more.

Setup Home Sharing
Allow remote peers to access local networks, and the internet via this device.

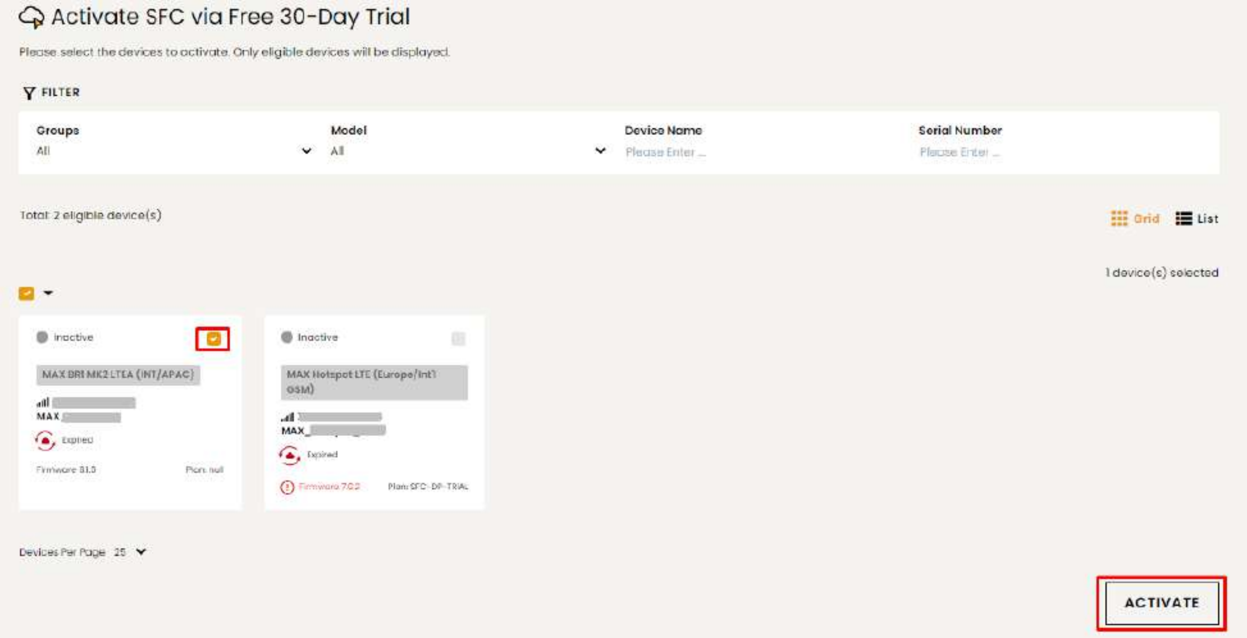
Get your activation key now
Enjoy all the delicious features powered by SpeedFusion.

Choose Cloud Location
Which cloud you'd like to connect?

Go to activate.speedfusion.com and select the type of SpeedFusion Cloud service, “Via Free 30-days Trial” or “Via Care Plans”, that you would like to activate. Next, register or login to your account.



Select the devices that you wish to activate SpeedFusion Cloud on and click **ACTIVATE**.



Activate SFC via Free 30-Day Trial

Please select the devices to activate. Only eligible devices will be displayed.

FILTER

Groups	Model	Device Name	Serial Number
All	All	Please Enter ...	Please Enter ...

Total: 2 eligible device(s)

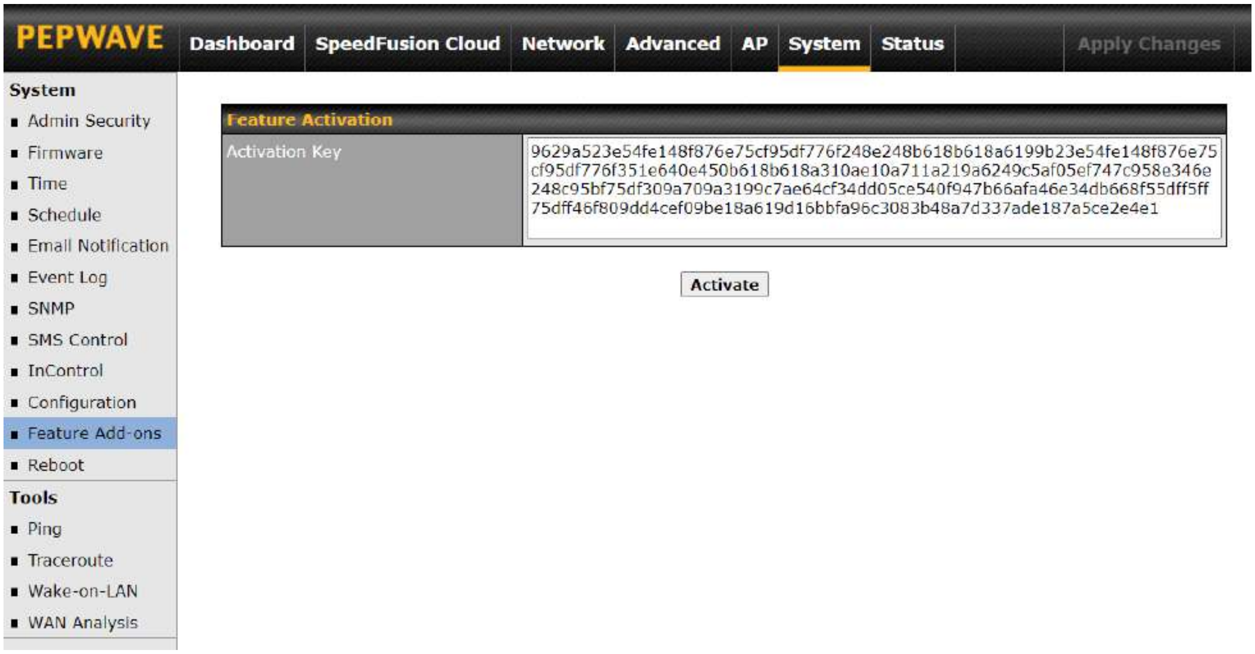
1 device(s) selected

☑ Inactive
MAX BR1 MK2 LTEA (INT/APAC)
[redacted]
MAX [redacted]
Expired
Firmware 8.1.3 Plan: null

☐ Inactive
MAX Hotspot LTE (Europe/Int'l GSM)
[redacted]
MAX_[redacted]
Expired
Firmware 7.0.2 Plan: SFC-DP-TRIAL

Devices Per Page 25

From **System > Features Add-ons**, paste the license key into the window and click on **Activate** once you have received the license key.

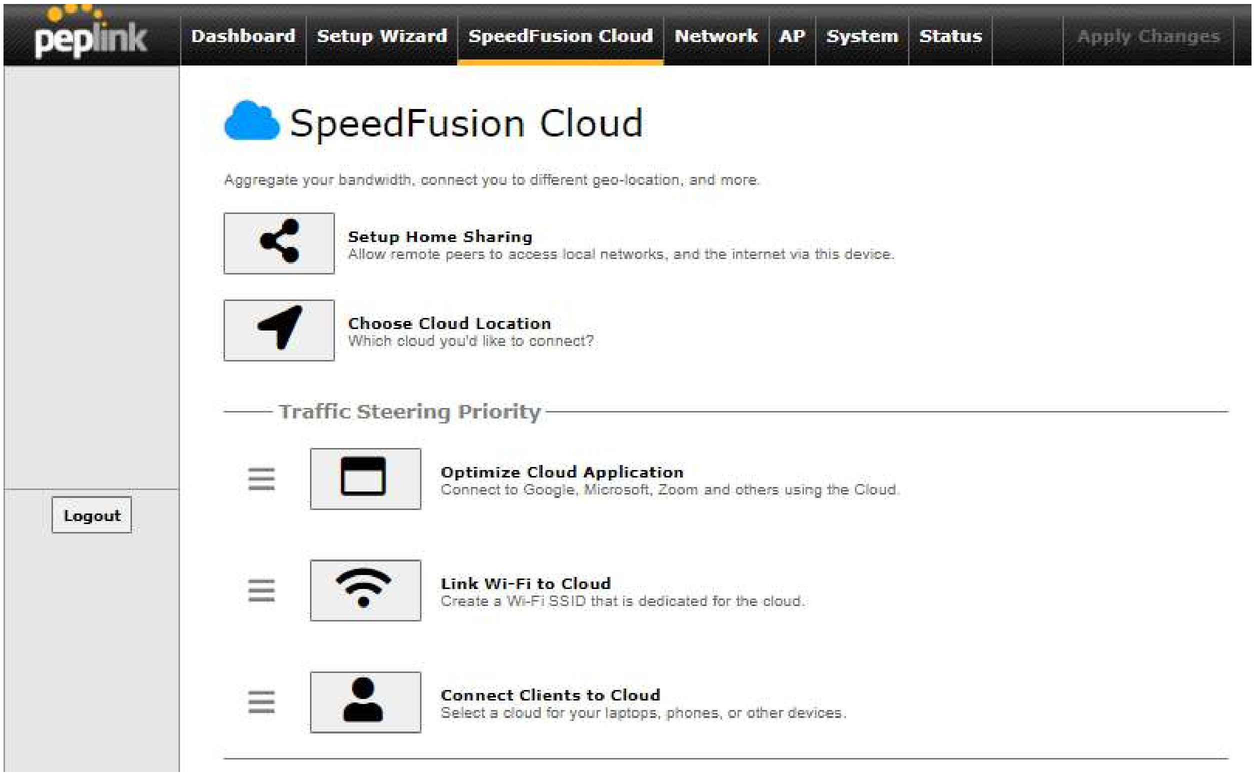


Activation Key

```
9629a523e54fe148f876e75cf95df776f248e248b618b618a6199b23e54fe148f876e75
cf95df776f351e640e450b618b618a310ae10a711a219a6249c5af05ef747c958e346e
248c95bf75df309a709a3199c7ae64cf34dd05ce540f947b66afa46e34db668f55dff5ff
75dff46f809dd4cef09be18a619d16bbfa96c3083b48a7d337ade187a5ce2e4e1
```

9.2 Enable SpeedFusion Cloud

Access the Web Admin of the device you want to create as the SFC Relay Server, navigating to the “SpeedFusion Cloud” tab.



SpeedFusion Cloud

Aggregate your bandwidth, connect you to different geo-location, and more.

Setup Home Sharing
Allow remote peers to access local networks, and the internet via this device.

Choose Cloud Location
Which cloud you'd like to connect?

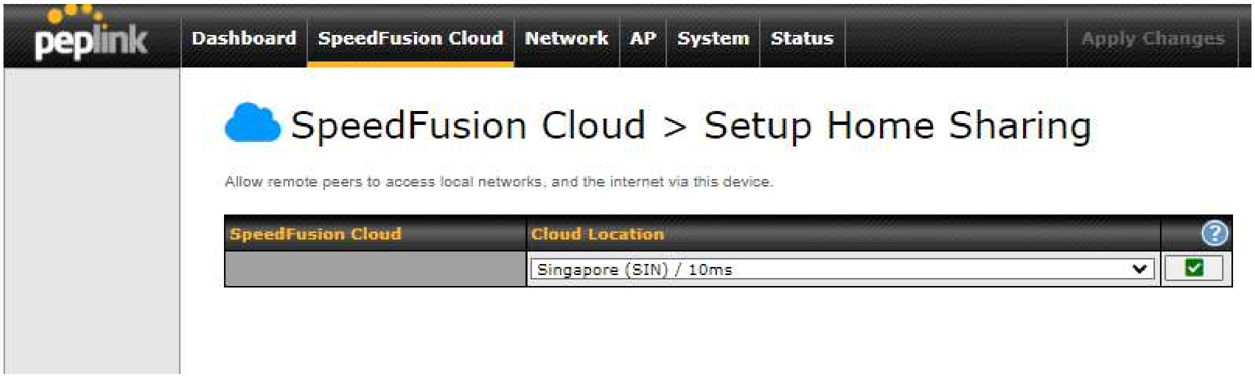
Traffic Steering Priority

Optimize Cloud Application
Connect to Google, Microsoft, Zoom and others using the Cloud.

Link Wi-Fi to Cloud
Create a Wi-Fi SSID that is dedicated for the cloud.

Connect Clients to Cloud
Select a cloud for your laptops, phones, or other devices.

To setup a SpeedFusion Cloud Relay Server, select "**Setup Home Sharing**" > Choose the **Cloud Location** you wish to connect to > Click on the **green tick button** to confirm the change.

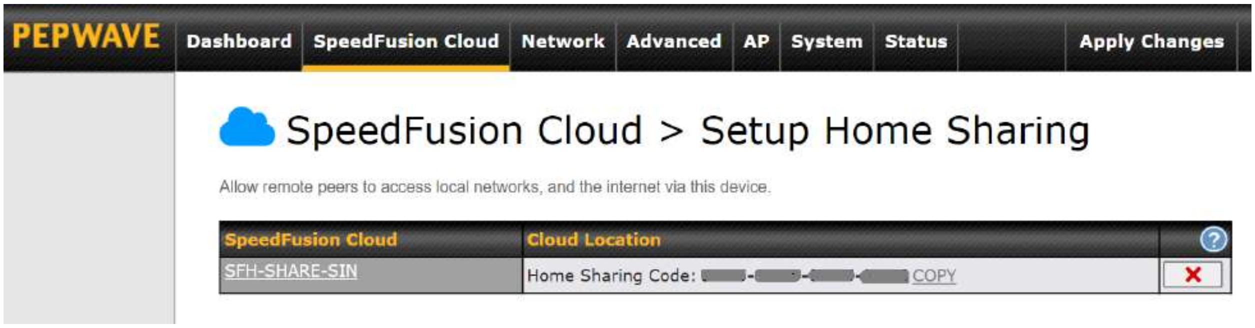


SpeedFusion Cloud > Setup Home Sharing

Allow remote peers to access local networks, and the internet via this device.

SpeedFusion Cloud	Cloud Location	?
	Singapore (SIN) / 10ms	☑

The Home Sharing Code will be generated and other peers can use this code to establish a SpeedFusion Cloud connection that will forward the traffic to this device, allowing them to access local networks and the Internet via your WAN connection.

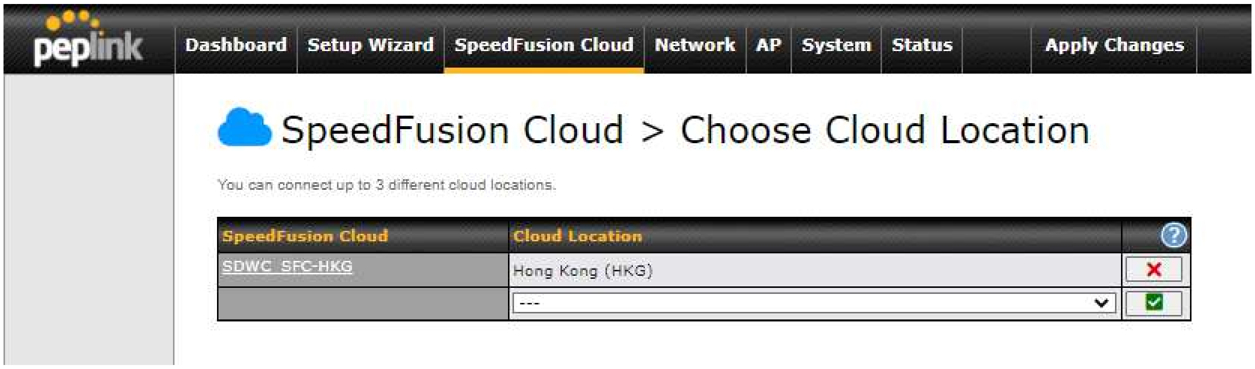


SpeedFusion Cloud > Setup Home Sharing

Allow remote peers to access local networks, and the internet via this device.

SpeedFusion Cloud	Cloud Location	?
SFH-SHARE-SIN	Home Sharing Code: [redacted] COPY	✗

To connect to SpeedFusion Cloud, you can select a Cloud Location of your choice, or simply **Automatic**, then the device will establish a connection to the nearest cloud server.

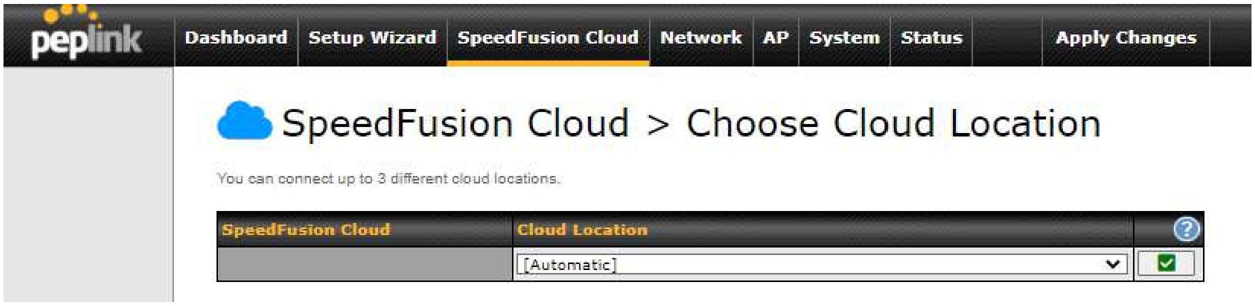


SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	?
SDWC_SFC-HKG	Hong Kong (HKG)	✗
	---	✓

Choose **Automatic > Click on the green tick button** to confirm the change.

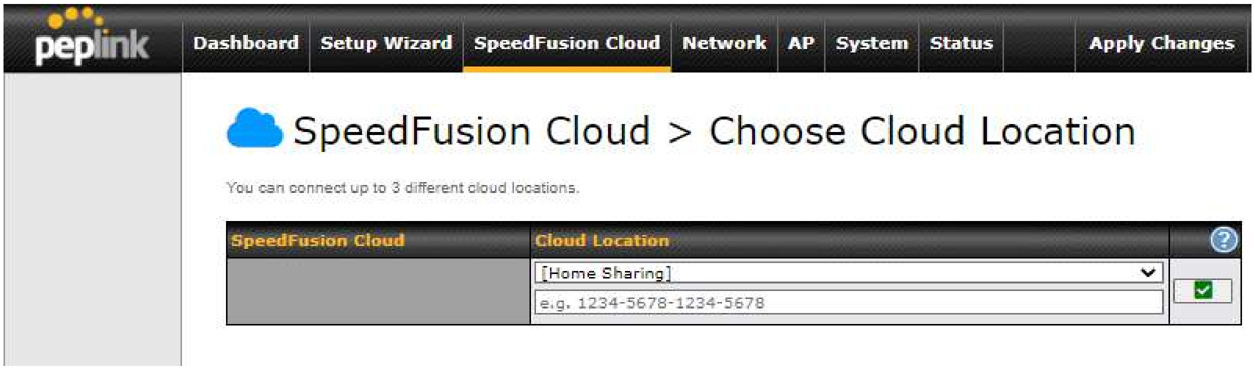


SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	?
	[Automatic]	✓

Or you may select **Home Sharing** and use your **Home Sharing Code** to create a profile if you have set up a SpeedFusion Cloud Relay Client on another device.

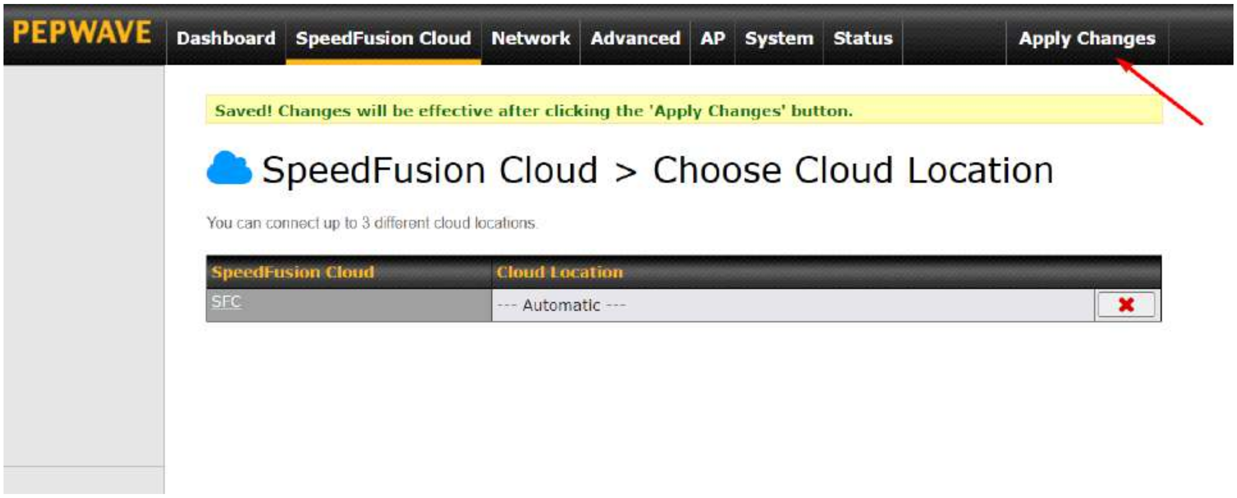


SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	?
	[Home Sharing] e.g. 1234-5678-1234-5678	☑

Click on **Apply Changes** to save the change.

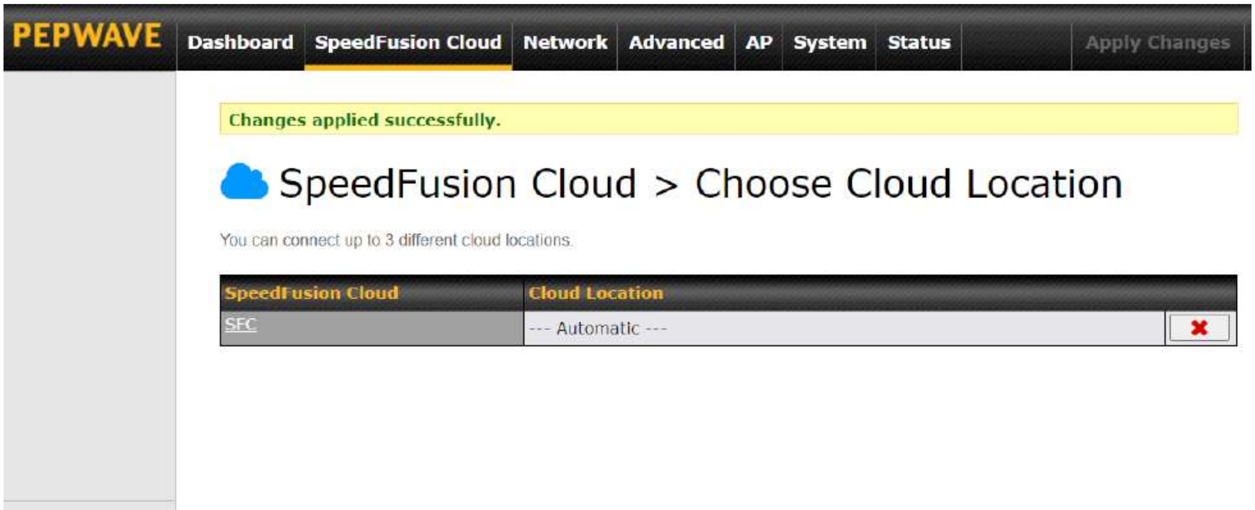


Saved! Changes will be effective after clicking the 'Apply Changes' button.

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	
SFC	--- Automatic ---	✖



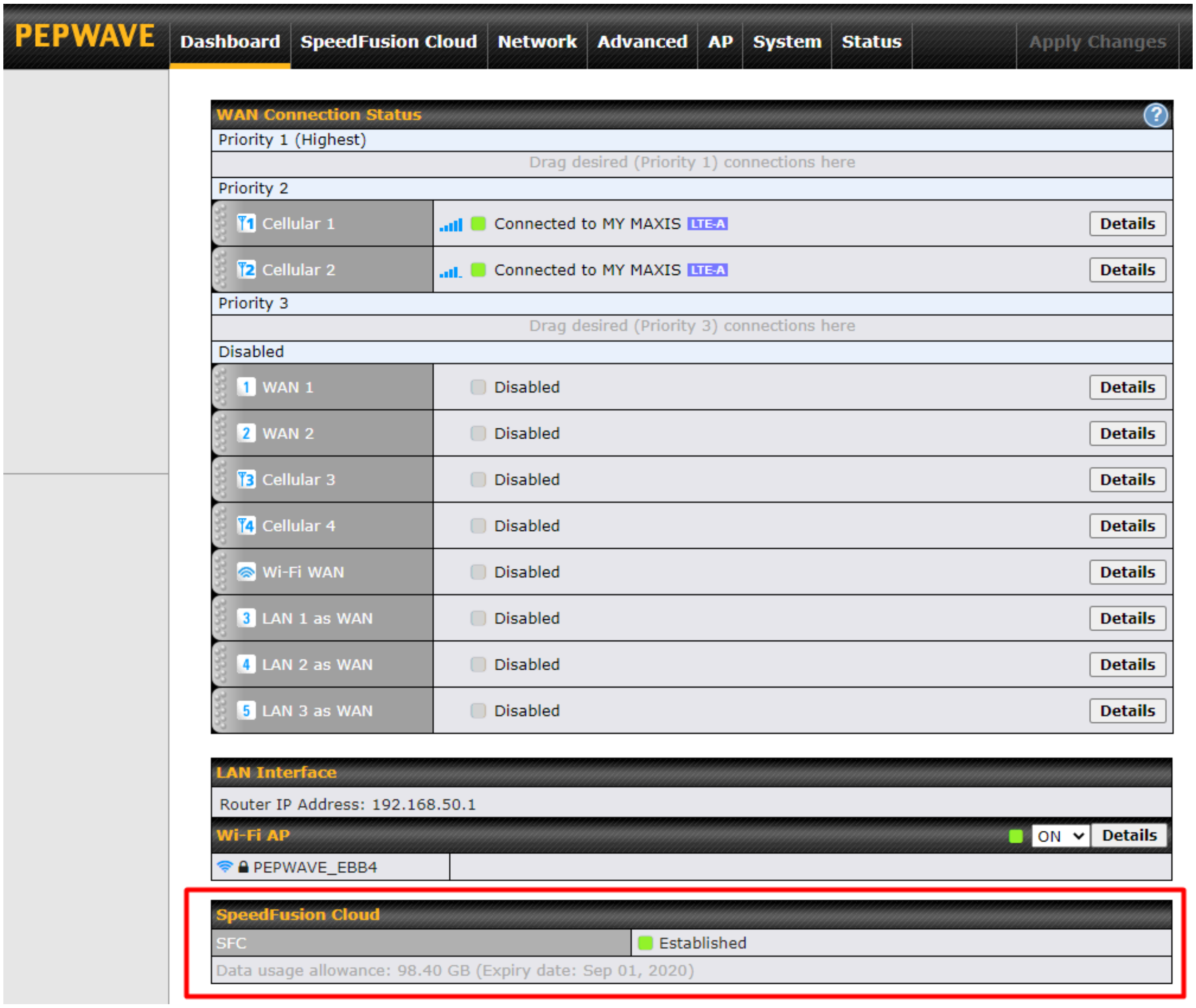
Changes applied successfully.

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	
SFC	--- Automatic ---	✖

By default, the router will build a SpeedFusion tunnel to the SpeedFusion Cloud



WAN Connection Status

Priority 1 (Highest)		
	Drag desired (Priority 1) connections here	
Priority 2		
Cellular 1	🟩 Connected to MY MAXIS LTE-A	Details
Cellular 2	🟩 Connected to MY MAXIS LTE-A	Details
Priority 3		
	Drag desired (Priority 3) connections here	
Disabled		
WAN 1	Disabled	Details
WAN 2	Disabled	Details
Cellular 3	Disabled	Details
Cellular 4	Disabled	Details
Wi-Fi WAN	Disabled	Details
LAN 1 as WAN	Disabled	Details
LAN 2 as WAN	Disabled	Details
LAN 3 as WAN	Disabled	Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP 🟩 ON Details

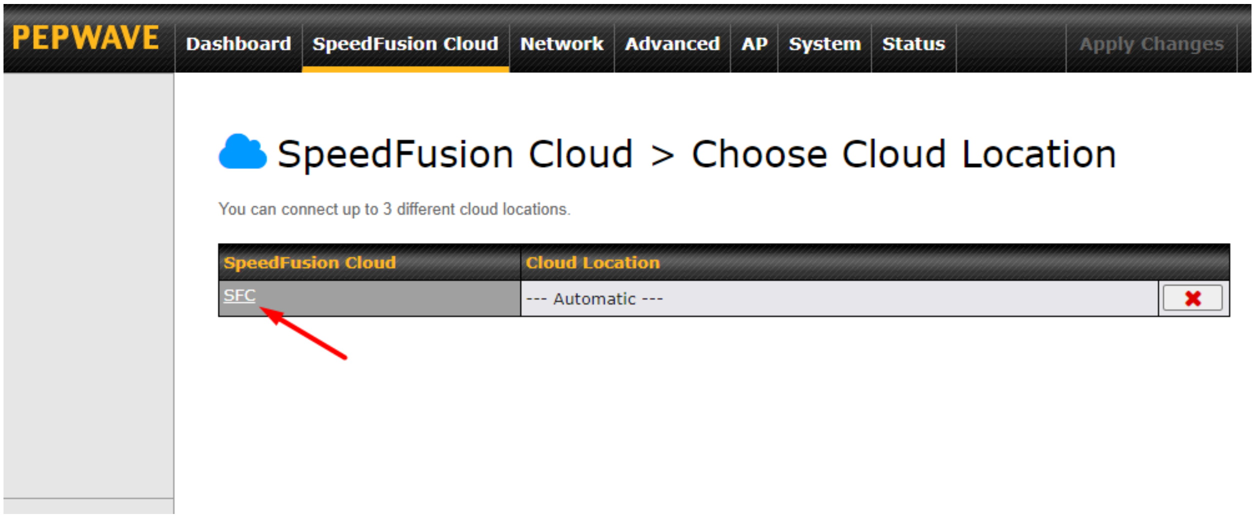
PEPWAVE_EBB4

SpeedFusion Cloud

SFC 🟩 Established

Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)

If you are running a latency sensitive service like video streaming or VOIP, a WAN Smoothing sub-tunnel can be created. Navigate to **Speedfusion Cloud > Choose a cloud location > SFC**.

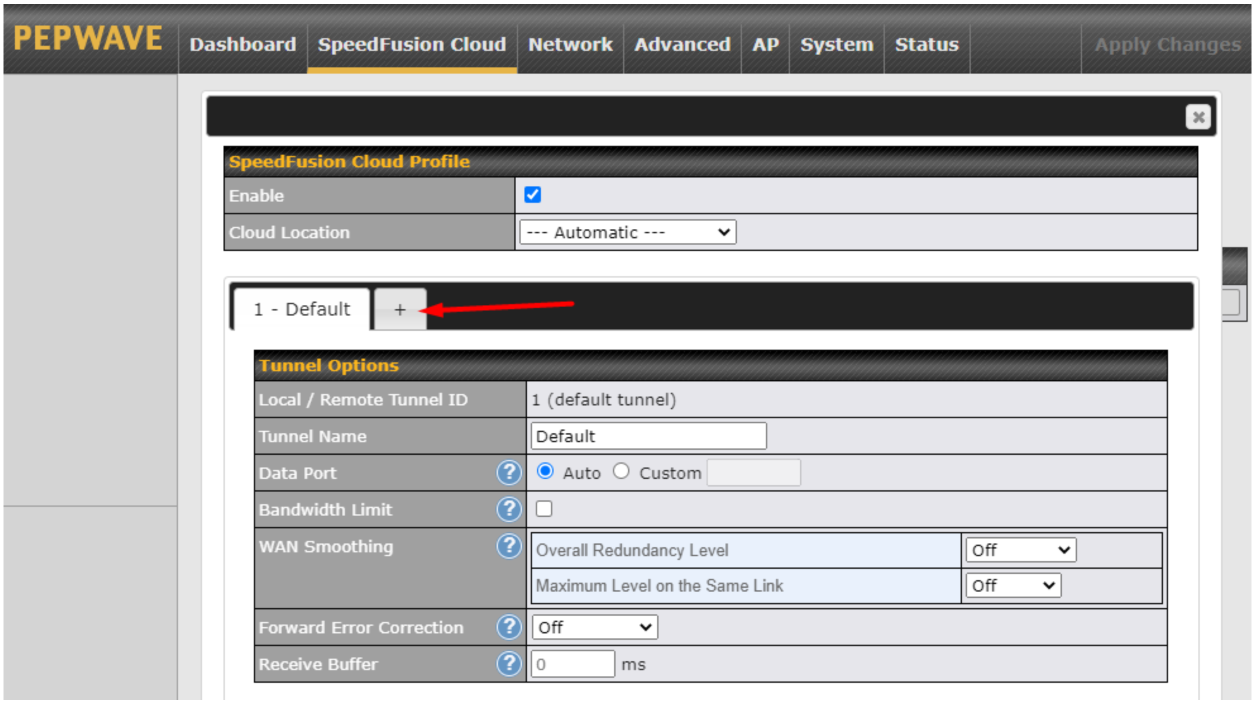


SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location	
SFC	--- Automatic ---	✖

A Speedfusion tunnel configuration window will pop out. Click on the **+** sign to create the WAN Smoothing sub-tunnel.

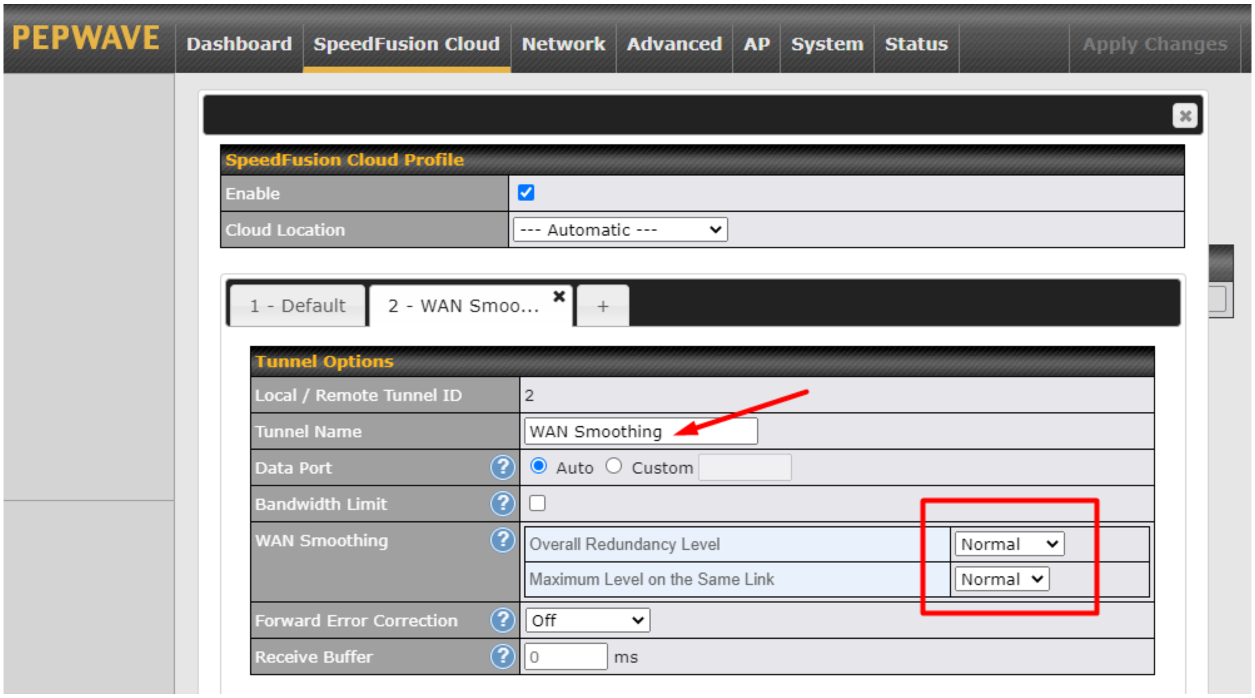


SpeedFusion Cloud Profile

Enable	☑
Cloud Location	--- Automatic ---

Tunnel Options

Local / Remote Tunnel ID	1 (default tunnel)
Tunnel Name	Default
Data Port	● Auto ○ Custom
Bandwidth Limit	□
WAN Smoothing	Overall Redundancy Level: Off Maximum Level on the Same Link: Off
Forward Error Correction	Off
Receive Buffer	0 ms



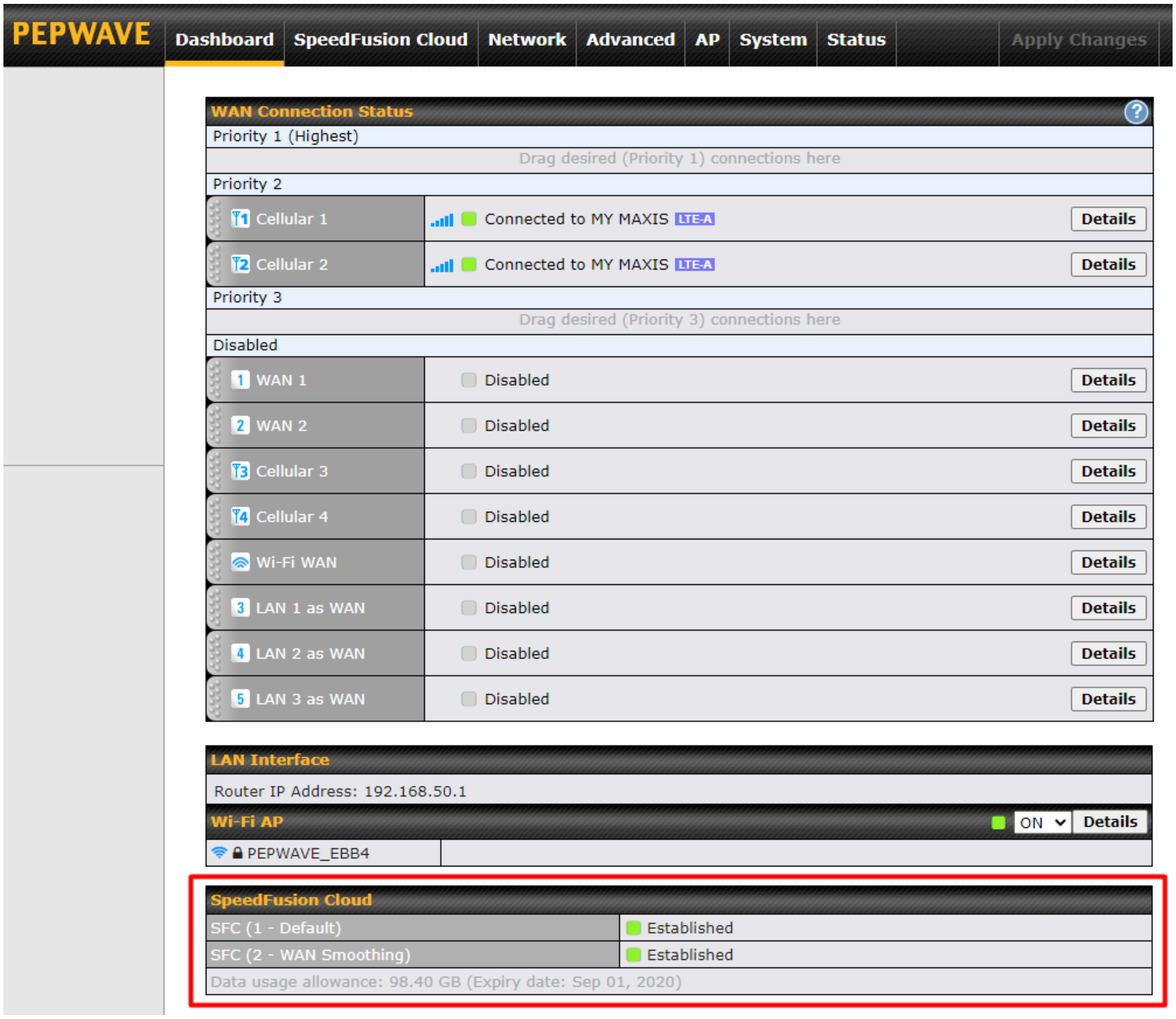
SpeedFusion Cloud Profile

Enable	☑
Cloud Location	--- Automatic ---

Tunnel Options

Local / Remote Tunnel ID	2
Tunnel Name	WAN Smoothing
Data Port	● Auto ○ Custom
Bandwidth Limit	□
WAN Smoothing	Overall Redundancy Level: Normal Maximum Level on the Same Link: Normal
Forward Error Correction	Off
Receive Buffer	0 ms

Click on **Save** and **Apply Changes** to save the configuration. Now, the router has 2 Speedfusion tunnels to the Speedfusion Cloud.



WAN Connection Status

Priority 1 (Highest)	
Drag desired (Priority 1) connections here	
Priority 2	
Cellular 1	Connected to MY MAXIS LTE-A — Details
Cellular 2	Connected to MY MAXIS LTE-A — Details
Priority 3	
Drag desired (Priority 3) connections here	
Disabled	
WAN 1	Disabled — Details
WAN 2	Disabled — Details
Cellular 3	Disabled — Details
Cellular 4	Disabled — Details
Wi-Fi WAN	Disabled — Details
LAN 1 as WAN	Disabled — Details
LAN 2 as WAN	Disabled — Details
LAN 3 as WAN	Disabled — Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP ON Details

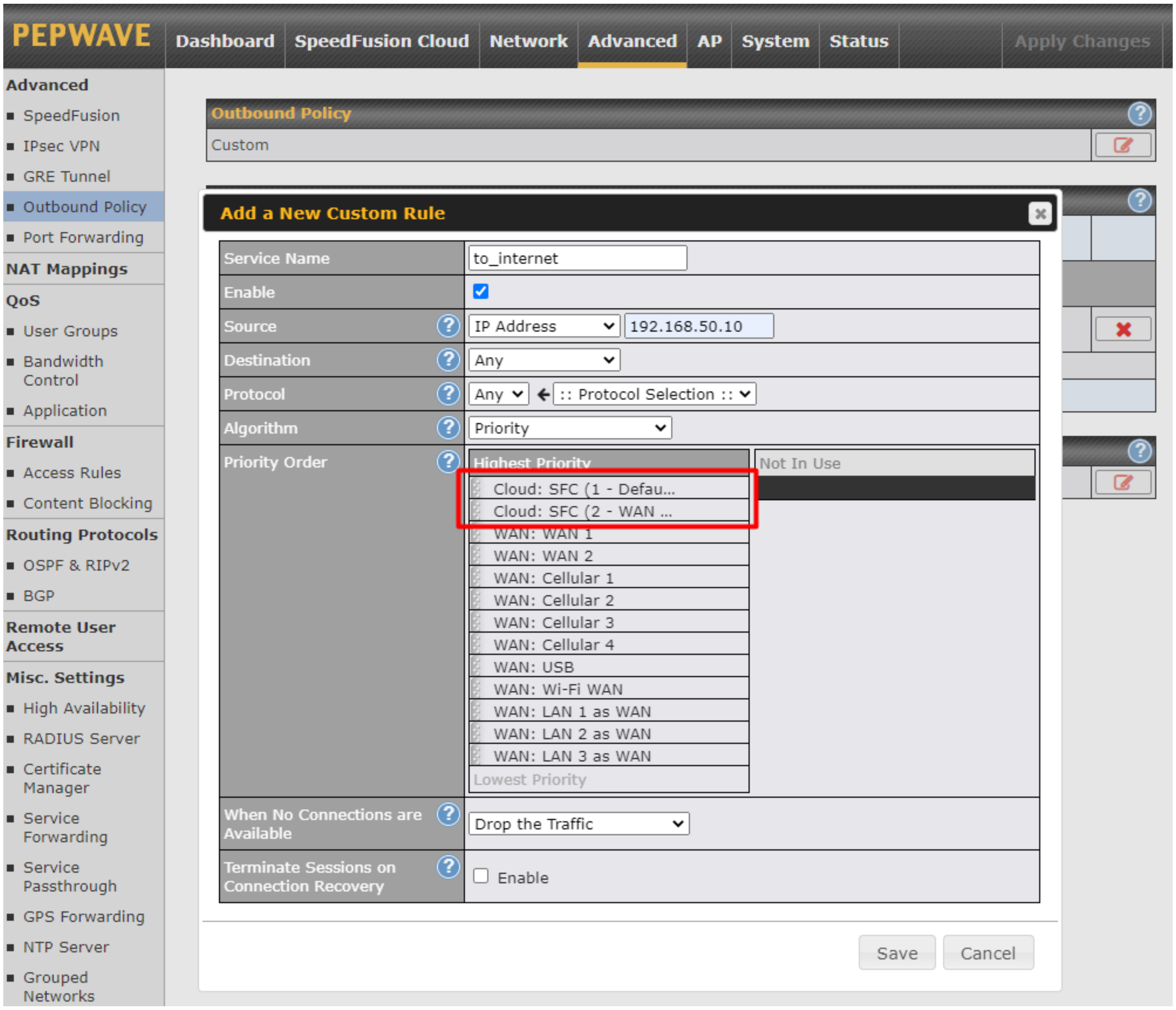
PEPWAVE_EBB4

SpeedFusion Cloud

SFC (1 - Default)	🟩 Established
SFC (2 - WAN Smoothing)	🟩 Established

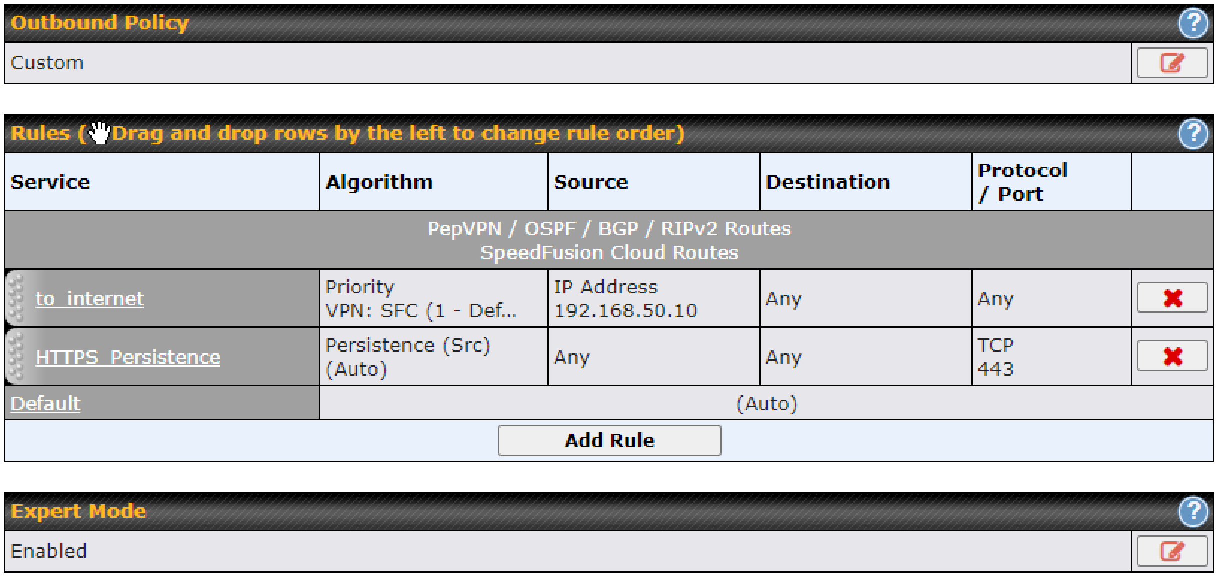
Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)

Create an outbound policy to steer the internet traffic to go into Speedfusion Cloud. Please go to **Advanced > Outbound Policy**, click on **Add Rule** to create a new outbound policy.



Add a New Custom Rule

Service Name	to_internet
Enable	☑
Source	IP Address 192.168.50.10
Destination	Any
Protocol	Any ← :: Protocol Selection ::
Algorithm	Priority
Priority Order	Highest Priority Cloud: SFC (1 - Defau... Cloud: SFC (2 - WAN ... WAN: WAN 1 WAN: WAN 2 WAN: Cellular 1 WAN: Cellular 2 WAN: Cellular 3 WAN: Cellular 4 WAN: USB WAN: Wi-Fi WAN WAN: LAN 1 as WAN WAN: LAN 2 as WAN WAN: LAN 3 as WAN Lowest Priority Not In Use
When No Connections are Available	Drop the Traffic
Terminate Sessions on Connection Recovery	□ Enable



Outbound Policy

Custom

Rules (Drag and drop rows by the left to change rule order)

Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN / OSPF / BGP / RIPv2 Routes SpeedFusion Cloud Routes					
to_internet	Priority VPN: SFC (1 - Def...	IP Address 192.168.50.10	Any	Any	✖
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				

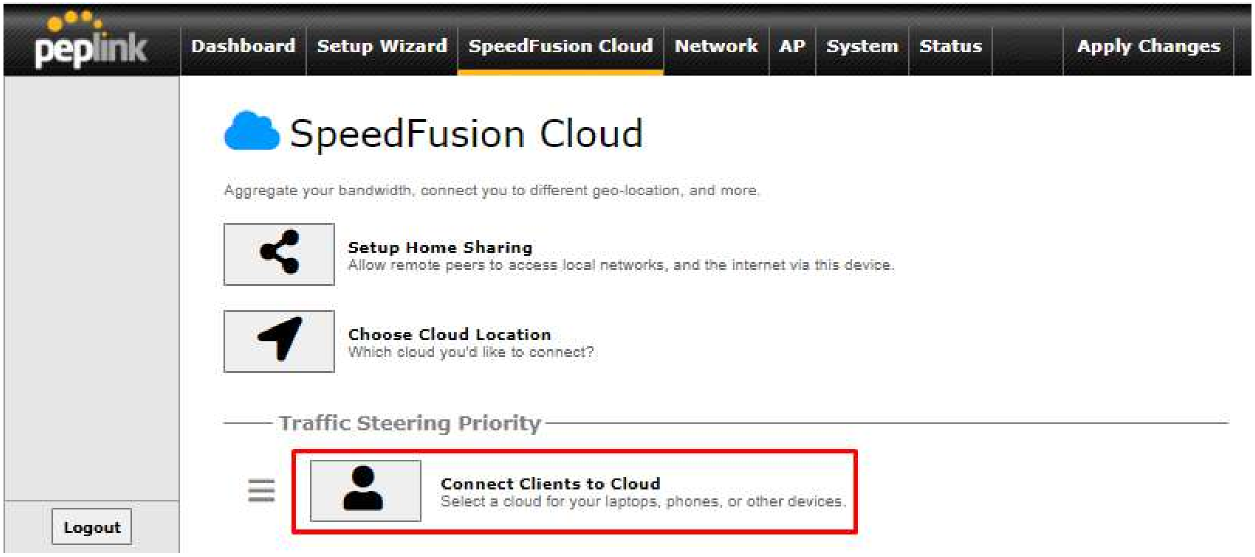
Add Rule

Expert Mode

Enabled

9.3 Connect Clients to Cloud

SpeedFusion Cloud provides a convenient way to route the LAN client to the cloud. From **SpeedFusion Cloud > Connect Clients to Cloud**.



SpeedFusion Cloud

Aggregate your bandwidth, connect you to different geo-location, and more.

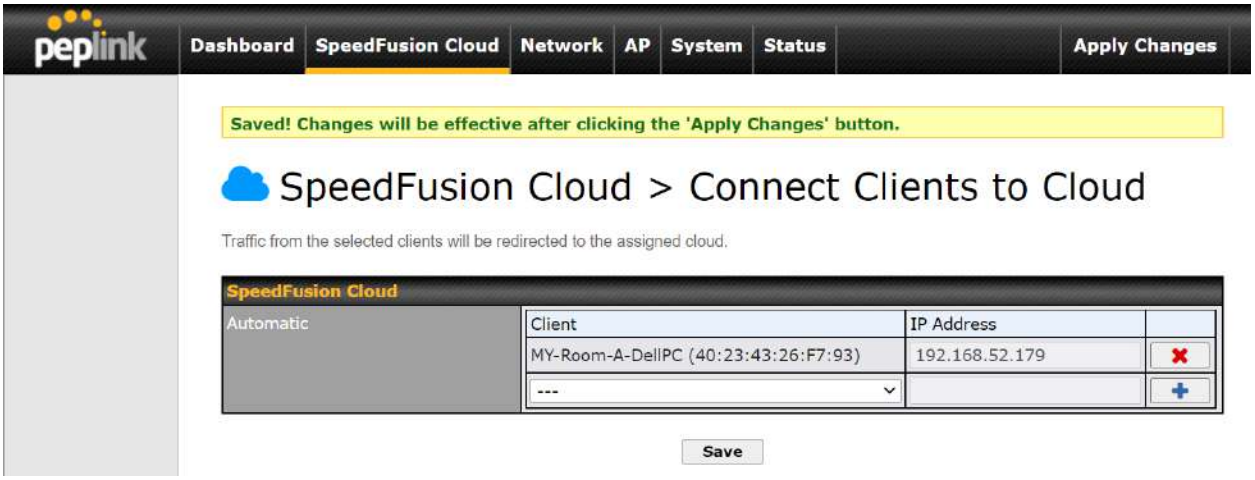
Setup Home Sharing
Allow remote peers to access local networks, and the internet via this device.

Choose Cloud Location
Which cloud you'd like to connect?

Traffic Steering Priority

Connect Clients to Cloud
Select a cloud for your laptops, phones, or other devices.

Choose a client from the drop down list > Click + > Save > Apply Changes.



Saved! Changes will be effective after clicking the 'Apply Changes' button.

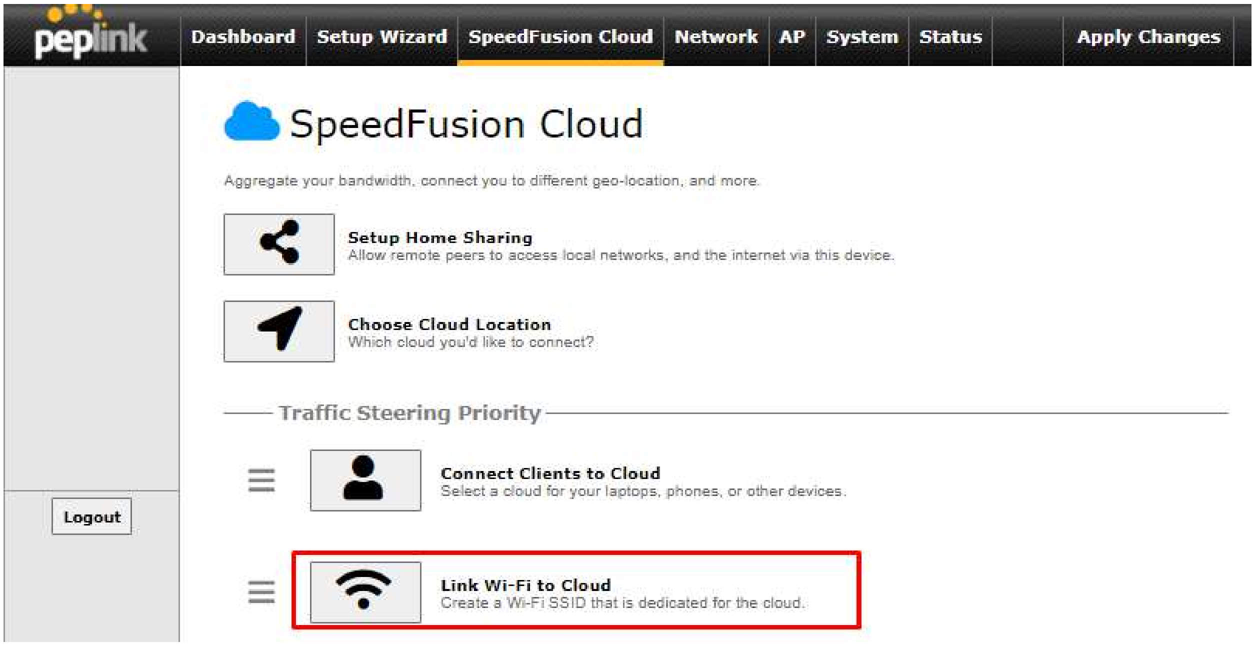
SpeedFusion Cloud > Connect Clients to Cloud

Traffic from the selected clients will be redirected to the assigned cloud.

SpeedFusion Cloud	Client	IP Address	
Automatic	MY-Room-A-DellPC (40:23:43:26:F7:93)	192.168.52.179	✖
	---		+

9.4 Link Wi-Fi to Cloud

SpeedFusion Cloud provides a convenient way to route the Wi-Fi client to the cloud from **SpeedFusion Cloud > Link Wi-Fi to Cloud**. **This option is available for Balance 20X Pro, Balance 30 Pro, and Balance One**.



SpeedFusion Cloud

Aggregate your bandwidth, connect you to different geo-location, and more.

Setup Home Sharing
Allow remote peers to access local networks, and the internet via this device.

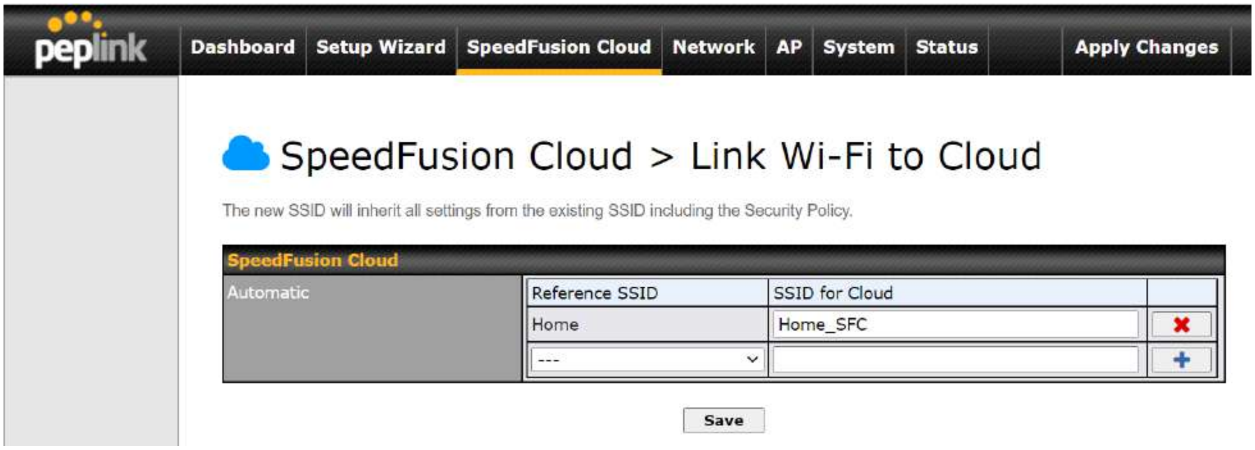
Choose Cloud Location
Which cloud you'd like to connect?

Traffic Steering Priority

Connect Clients to Cloud
Select a cloud for your laptops, phones, or other devices.

Link Wi-Fi to Cloud
Create a Wi-Fi SSID that is dedicated for the cloud.

Create a new SSID for SpeedFusion Cloud. The new SSID will inherit all settings from one of the existing SSIDs including the Security Policy. Then click **Save** follow by **Apply Changes**.

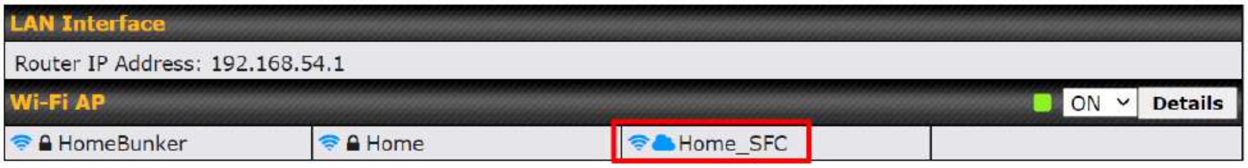


SpeedFusion Cloud > Link Wi-Fi to Cloud

The new SSID will inherit all settings from the existing SSID including the Security Policy.

SpeedFusion Cloud			
Automatic	Reference SSID	SSID for Cloud	
	Home	Home_SFC	✖
	---		+

SpeedFusion Cloud SSID will be shown on **Dashboard**.



LAN Interface

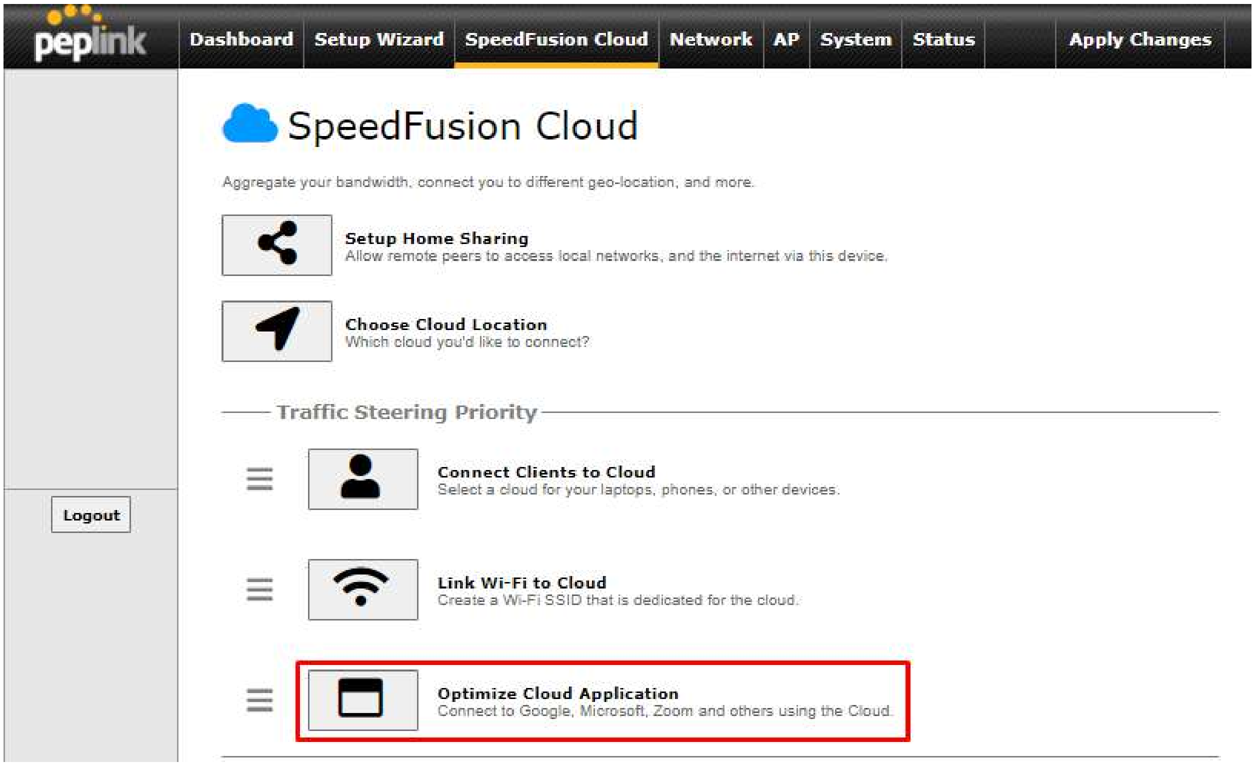
Router IP Address: 192.168.54.1

Wi-Fi AP

HomeBunker	Home	Home_SFC	

9.5 Optimize Cloud Application

Optimize Cloud Application allows you to route Internet traffic through SpeedFusion Cloud based on the application. Go to **SpeedFusion Cloud > Optimize Cloud Application**.



SpeedFusion Cloud

Aggregate your bandwidth, connect you to different geo-location, and more.

Setup Home Sharing
Allow remote peers to access local networks, and the internet via this device.

Choose Cloud Location
Which cloud you'd like to connect?

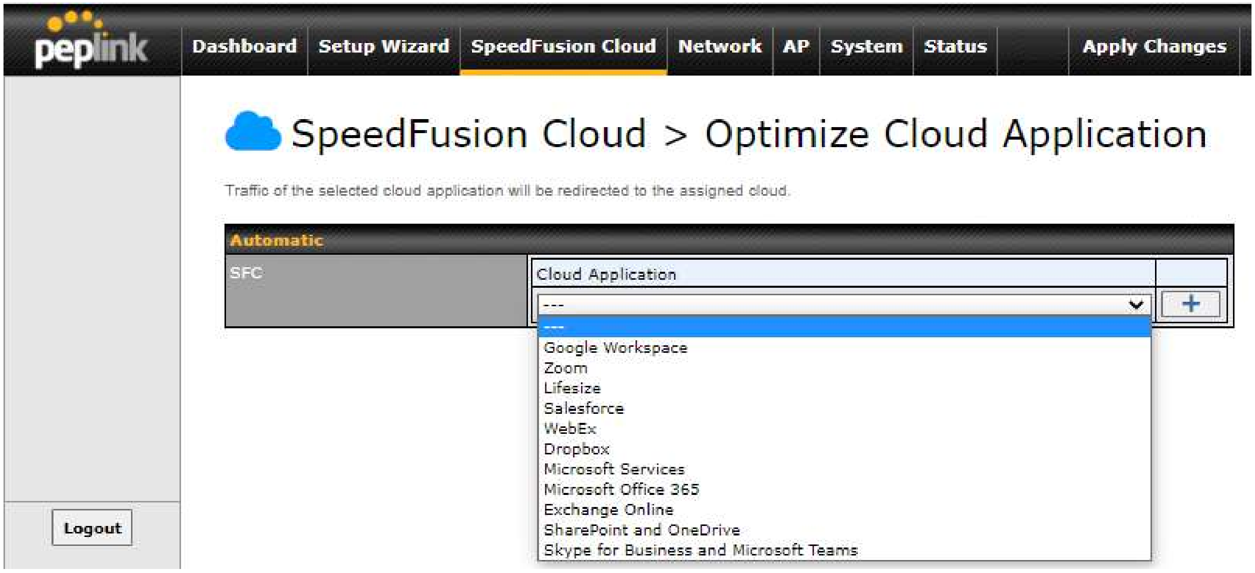
Traffic Steering Priority

Connect Clients to Cloud
Select a cloud for your laptops, phones, or other devices.

Link Wi-Fi to Cloud
Create a Wi-Fi SSID that is dedicated for the cloud.

Optimize Cloud Application
Connect to Google, Microsoft, Zoom and others using the Cloud.

Select a Cloud application to route through SpeedFusion Cloud from the drop down list **>** Click **+** **>** Save > Apply Changes. Click the ✖ to remove a selected Cloud application from routing through SpeedFusion Cloud.



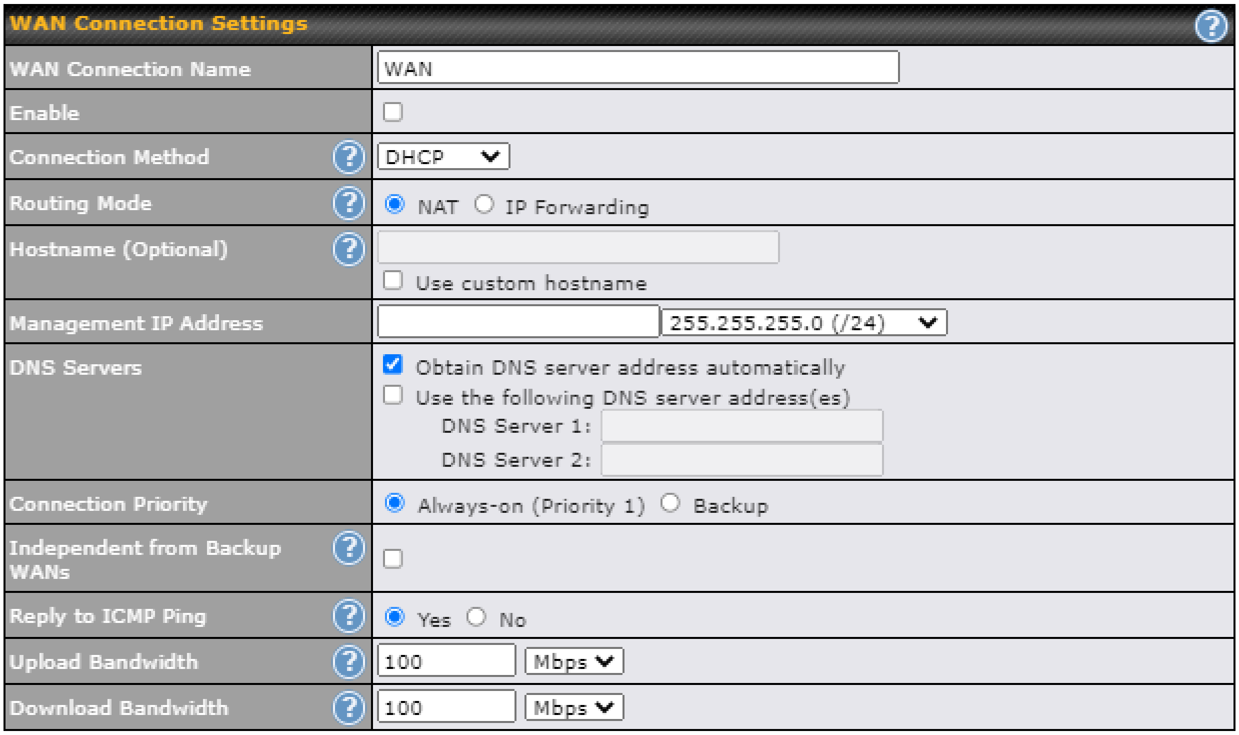
SpeedFusion Cloud > Optimize Cloud Application

Traffic of the selected cloud application will be redirected to the assigned cloud.

10 Network Tab

10.1 WAN

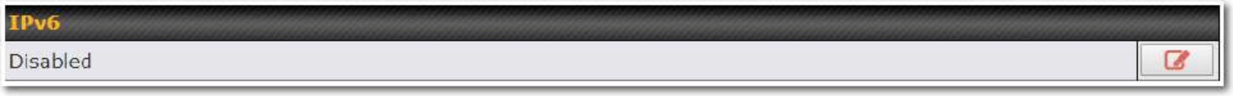
From **Network > WAN,** choose a WAN connection by clicking it.



WAN Connection Settings	
WAN Connection Name	WAN
Enable	□
Connection Method	DHCP
Routing Mode	● NAT ○ IP Forwarding
Hostname (Optional)	□ Use custom hostname
Management IP Address	255.255.255.0 (/24)
DNS Servers	☑ Obtain DNS server address automatically □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Connection Priority	● Always-on (Priority 1) ○ Backup
Independent from Backup WANs	□
Reply to ICMP Ping	● Yes ○ No
Upload Bandwidth	100 Mbps
Download Bandwidth	100 Mbps

IPv6

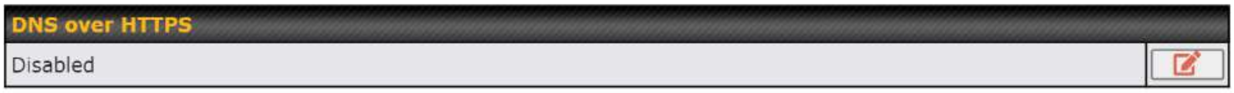
You can also enable IPv6 support in this section.



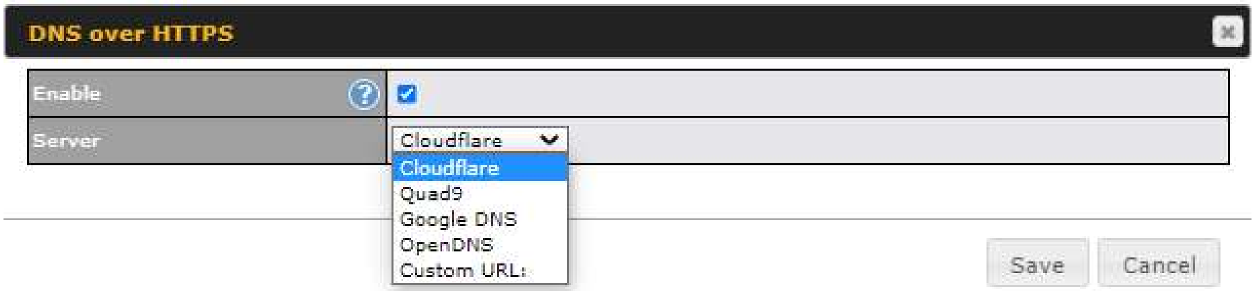
IPv6
Disabled

DNS over HTTPS (DoH)

You can enable the DoH support in this section.



DNS over HTTPS
Disabled



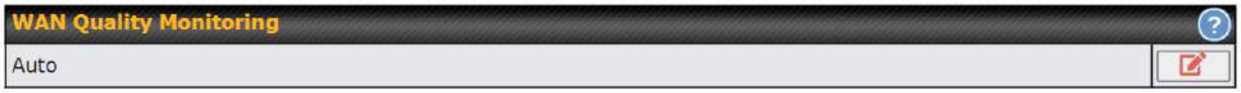
DNS over HTTPS

Enable	☑
Server	Cloudflare

DNS over HTTPS	
Enable	When this option is enabled, the DNS proxy server will use HTTPS connections to forward DNS requests to the DoH resolver; it will not fallback to traditional UDP DNS options.
Server	The options to configure DoH with a predefined server are: ● Cloudflare - The DNS server IP addresses for **Cloudflare** will be using 1.1.1.1, which is unfiltered. ● Quad9 - The DNS server IP addresses for **Quad9** will be using 9.9.9.9 and 142.112.112.112, which is malware blocking and DNSSEC. ● Google DNS - The DNS server IP addresses for **Google DNS** will be using 8.8.8.8 and 8.8.4.4, which is RFC8484 standard. ● OpenDNS - The DNS server IP addresses for **OpenDNS** will be using 208.67.222.222 and 208.67.220.220, which is standard DNS. ● Custom URL - You may select **Custom URL:**, and enter the **resolver URL** and **IP address**.

WAN Quality Monitoring

This settings advice how WAN Quality information is being gathered.



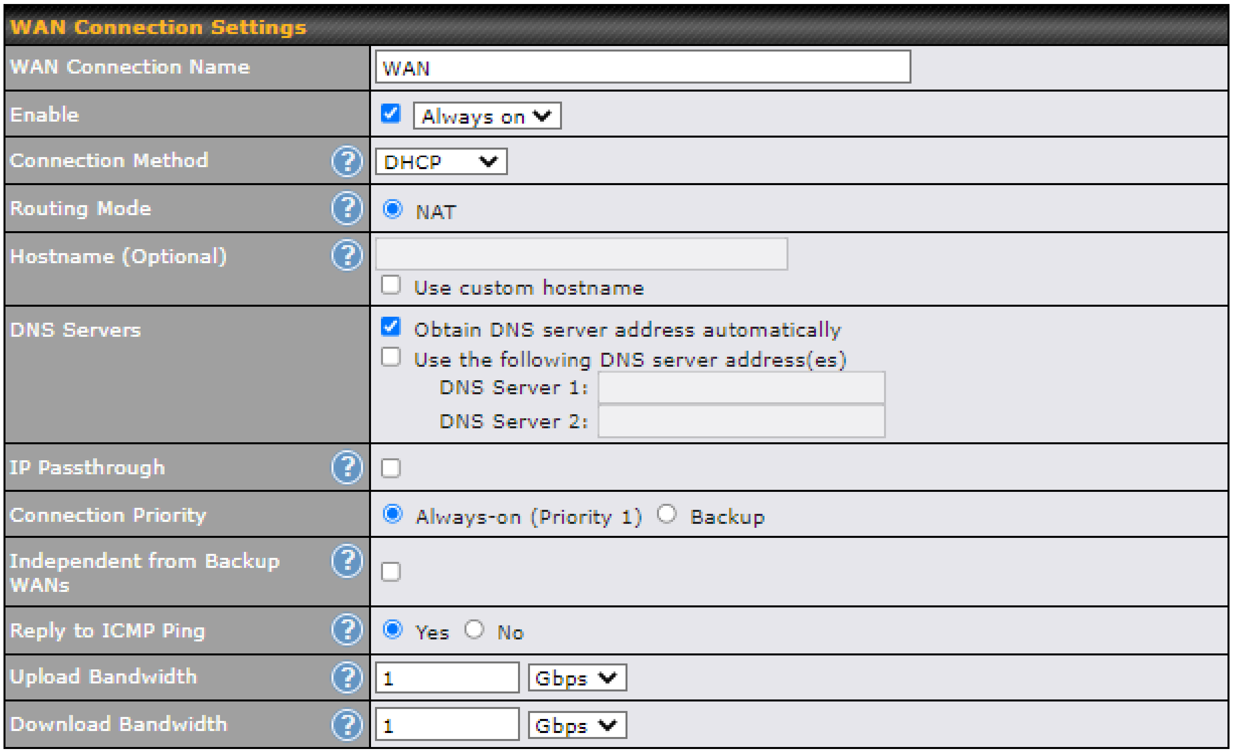
WAN Quality Monitoring

Auto

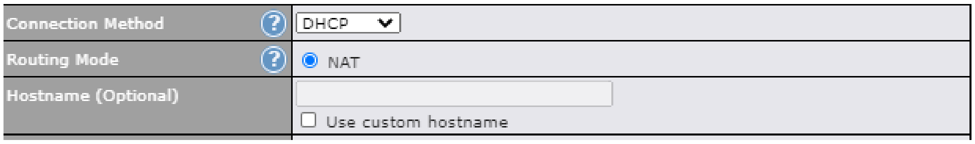
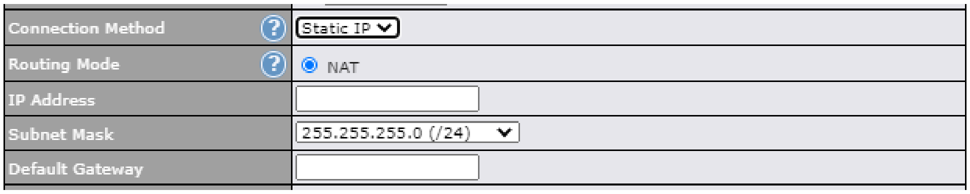
By default, WAN Quality will always be observed and gathered automatically. With customized choice of WAN connections, the device will always observe WAN Quality of those selected WAN connections. Other WAN connections may stop observing WAN Quality information if it is not necessary for the underlying features.

WAN Connection Settings (Ethernet)

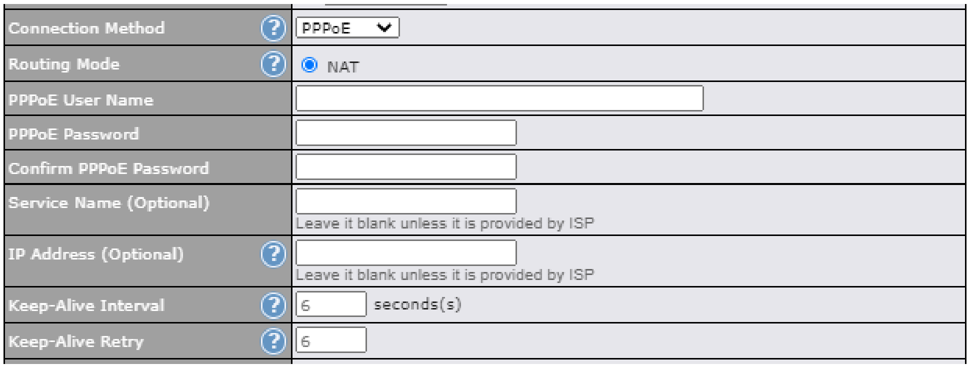
Clicking an Ethernet WAN connection will result in the following screen:



WAN Connection Settings	
WAN Connection Name	WAN
Enable	☑ Always on
Connection Method	DHCP
Routing Mode	● NAT
Hostname (Optional)	 □ Use custom hostname
DNS Servers	☑ Obtain DNS server address automatically □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough	□
Connection Priority	● Always-on (Priority 1) ○ Backup
Independent from Backup WANs	□
Reply to ICMP Ping	● Yes ○ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

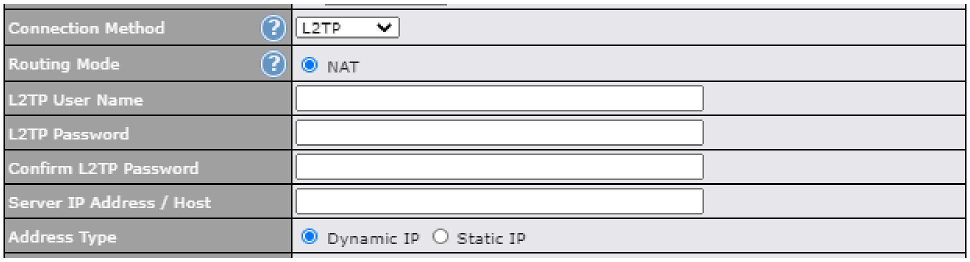
WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Enable	This setting enables the WAN connection. If schedules have been defined, you will be able to select a schedule to apply to the connection.
Connection Method	There are five possible connection methods for Ethernet WAN: • **DHCP**  Connection Method: DHCP Routing Mode: ● NAT Hostname (Optional): □ Use custom hostname • **Static IP**  Connection Method: Static IP Routing Mode: ● NAT IP Address: Subnet Mask: 255.255.255.0 (/24) Default Gateway:

- **PPPoE**



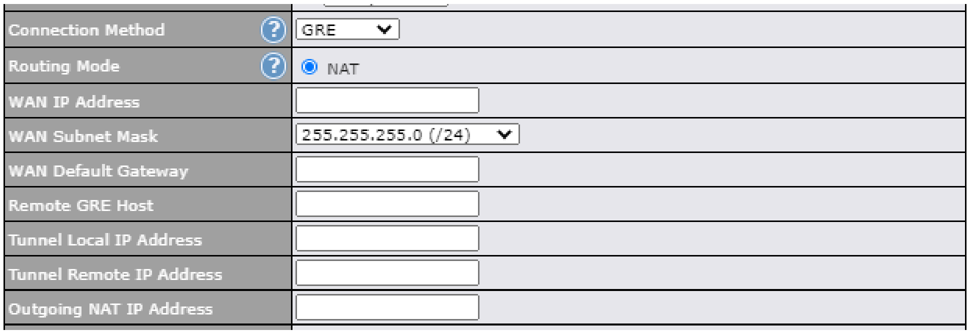
Connection Method	PPPoE
Routing Mode	● NAT
PPPoE User Name	
PPPoE Password	
Confirm PPPoE Password	
Service Name (Optional)	Leave it blank unless it is provided by ISP
IP Address (Optional)	Leave it blank unless it is provided by ISP
Keep-Alive Interval	6 seconds(s)
Keep-Alive Retry	6

- **L2TP**



Connection Method	L2TP
Routing Mode	● NAT
L2TP User Name	
L2TP Password	
Confirm L2TP Password	
Server IP Address / Host	
Address Type	● Dynamic IP ○ Static IP

- **GRE**



Connection Method	GRE
Routing Mode	● NAT
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24)
WAN Default Gateway	
Remote GRE Host	
Tunnel Local IP Address	
Tunnel Remote IP Address	
Outgoing NAT IP Address	

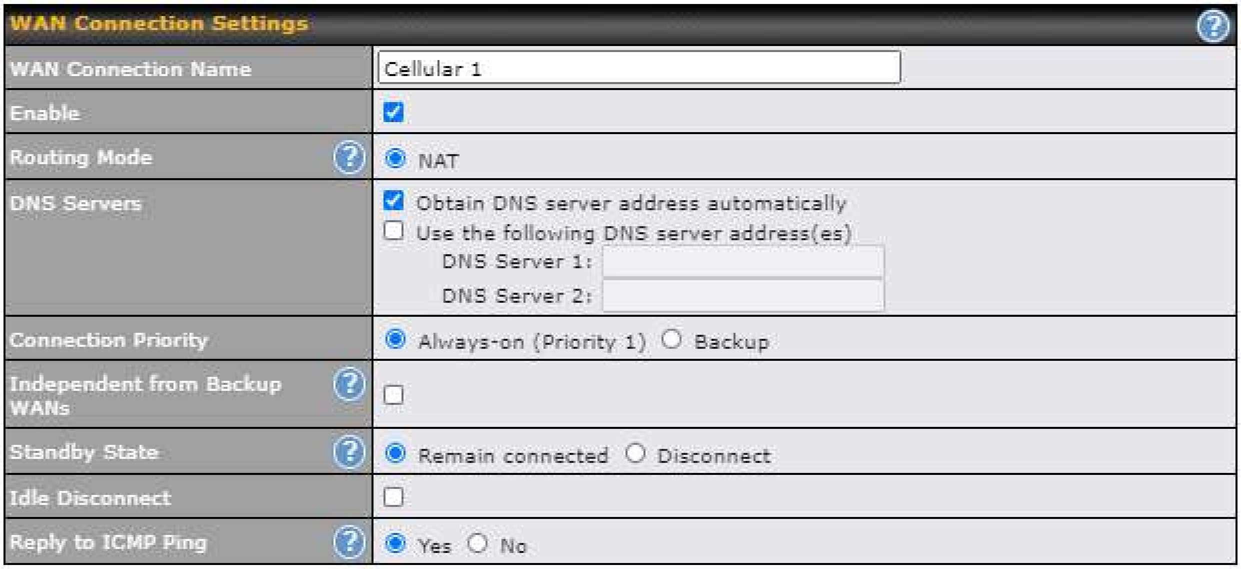
The connection method and details are determined by, and can be obtained from the ISP. See the following sections for details on each connection method. DNS server settings can be configured in the corresponding menu for each connection method.

Routing Mode	This field shows that **NAT** (network address translation) will be applied to the traffic routed over this WAN connection. **IP Forwarding** is available when you click the link in the help ? icon.
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with a hostname, you can safely bypass this option.

Management IP Address	**Management IP Address** is available for configuration when you click the link in the help ? icon via the Hostname. This option allows you to configure the management IP address for the DHCP WAN connection.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.
Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If **Always-on** is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If **Backup** is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Reply to ICMP PING	If the checkbox is **unticked**, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: **ticked** (Yes)
Upload Bandwidth	This field refers to the maximum upload speed. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.
Download Bandwidth	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.

WAN Connection Settings (Cellular)

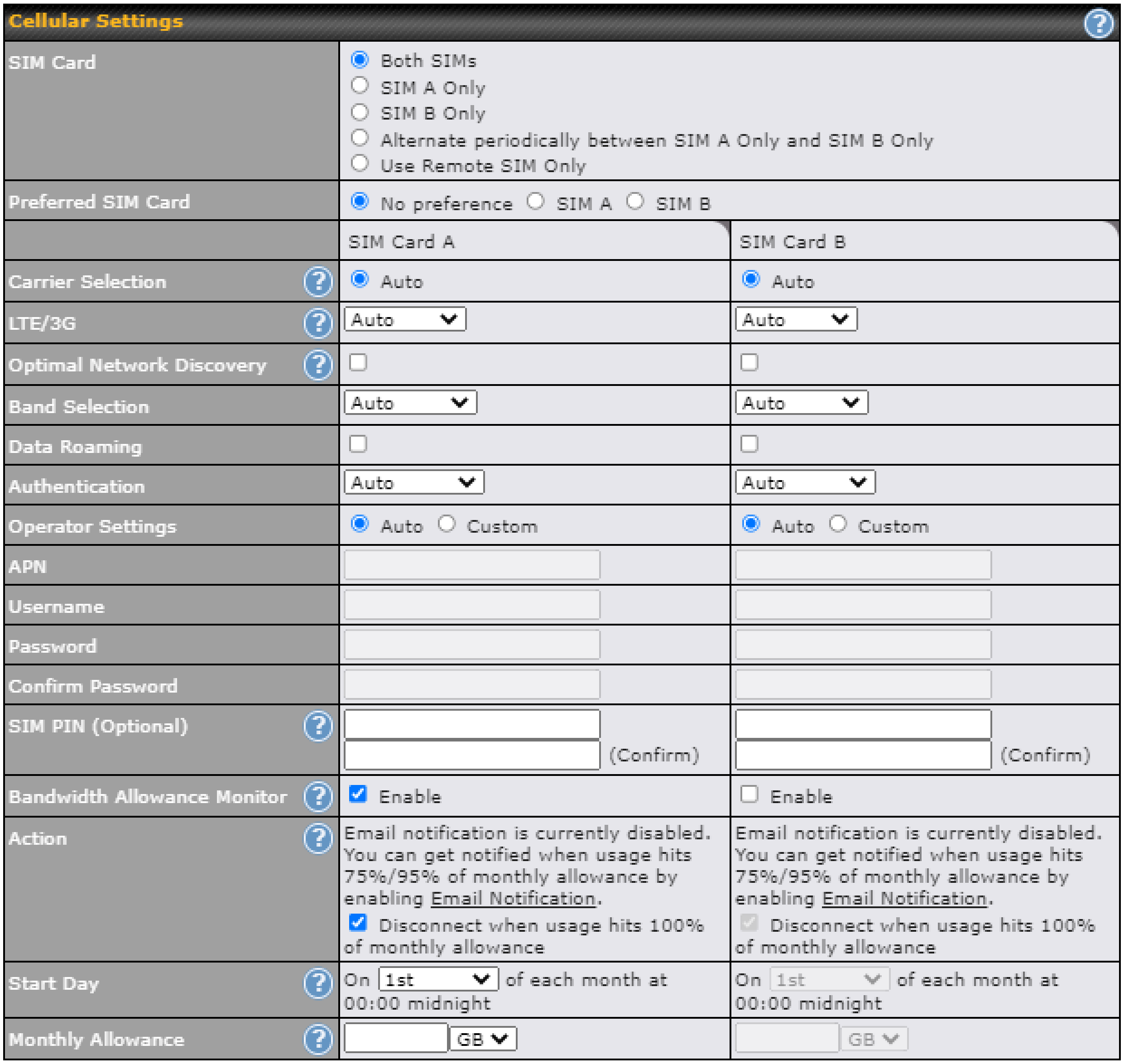
Clicking an Ethernet WAN connection will result in the following screens:



WAN Connection Settings	
WAN Connection Name	Cellular 1
Enable	☑
Routing Mode	● NAT
DNS Servers	☑ Obtain DNS server address automatically □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Connection Priority	● Always-on (Priority 1) ○ Backup
Independent from Backup WANs	□
Standby State	● Remain connected ○ Disconnect
Idle Disconnect	□
Reply to ICMP Ping	● Yes ○ No

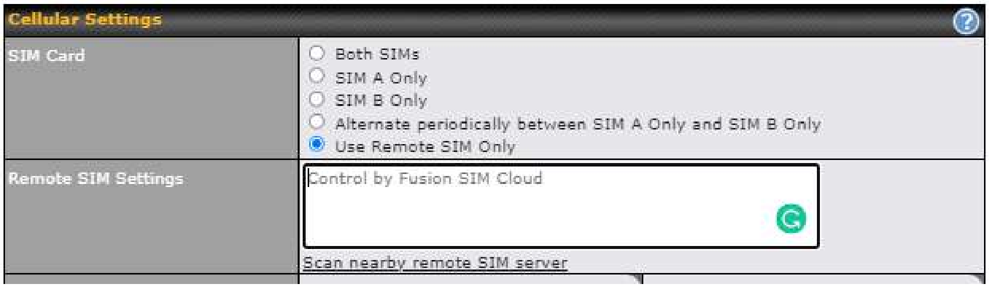
WAN Connection Settings	
WAN Connection Name	Indicate a name you wish to give this WAN connection
Enable	Click the checkbox to toggle the on and off state of this connection.
Routing Mode	This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding. In the case if you need to choose IP Forwarding for your scenario. Click the ? button to enable IP Forwarding.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.
Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If **Always-on** is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If **Backup** is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.

Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Idle Disconnect	If this is checked, the connection will disconnect when idle after the configured Time value. This option is disabled by default.
Reply to ICMP PING	If the checkbox is **unticked**, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: **ticked** (Yes)



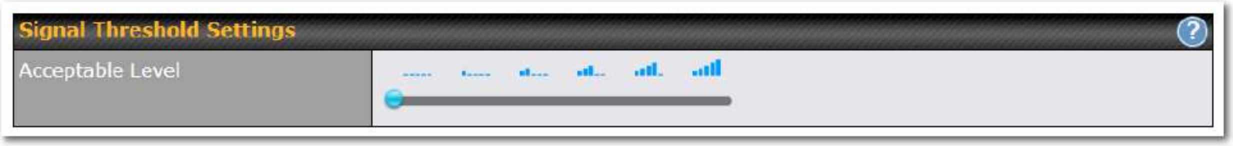
Cellular Settings

SIM Card	● Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ○ Use Remote SIM Only	
Preferred SIM Card	● No preference ○ SIM A ○ SIM B	
	SIM Card A	SIM Card B
Carrier Selection	● Auto	● Auto
LTE/3G	Auto	Auto
Optimal Network Discovery	□	□
Band Selection	Auto	Auto
Data Roaming	□	□
Authentication	Auto	Auto
Operator Settings	● Auto ○ Custom	● Auto ○ Custom
APN		
Username		
Password		
Confirm Password		
SIM PIN (Optional)	(Confirm)	(Confirm)
Bandwidth Allowance Monitor	☑ Enable	□ Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st of each month at 00:00 midnight	On 1st of each month at 00:00 midnight
Monthly Allowance	GB	GB

Cellular Settings	
SIM Card	Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards. For routers that support the SIM Injector, you may select the "Use Remote SIM Only" to provision a SIM from a SIM Injector. Further details on the SIM Injector found is available here: https://www.peplink.com/products/sim-injector/.
Preferred SIM Card	If "**Both SIMs**" were selected on the above field, then you can designate the priority of the SIM card slots here.
Remote SIM Settings	If "**Use Remote SIM Only**" is selected in the SIM card section, the **Remote SIM Settings** will be shown.  Cellular Settings SIM Card ○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ● Use Remote SIM Only Remote SIM Settings Control by Fusion SIM Cloud Scan nearby remote SIM server You may need to enable the remote SIM Host settings in the Remote SIM management, see the **section 13.14.7** or **Appendix C** for more details on FusionSIM. After that, click on "**Scan nearby remote SIM server**" to show the serial number(s) of the connected SIM Injector(s). If you want to select a specific SIM, in the Cellular Settings, type "**:**" and then the number of the SIM slot, eg.1111-2222-3333:7.
LTE/3G	This drop-down menu allows restricting cellular to particular band. Click the ? button to enable the selection of specific bands.
Optimal Network Discovery	Cellular WAsN by default will only handover from 3G to LTE network when there is no active data traffic, enable this option will make it run the handover procedures after fallback to 3G for a defined effective period, even this may interrupt the connectivity for a short while.
Band Selection	When set to **Auto,** band selection allows for automatically connecting to available, supported bands (frequencies) . When set to Manual, you can manually select the bands (frequencies) the SIM will connect to.
Data Roaming	This checkbox enables data roaming on this particular SIM card. When data roaming is enabled this option allows you to select in which countries the SIM has a data connection. The option is configured by using MMC (country) codes.Please check your service provider's data roaming policy before proceeding.
Authentication	Choose from **PAP Only** or **CHAP Only** to use those authentication methods exclusively. Select **Auto** to automatically choose an authentication method.
Operator Settings	This setting allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connections, you may select **Custom** to enter your carrier's **APN**, **Login**, **Password**, and

	Dial Number settings manually. The correct values can be obtained from your carrier. The default and recommended setting is **Auto**.
APN / Login / Password / SIM PIN	When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
Bandwidth Allowance Monitor	Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Signal Threshold Settings


Signal Threshold Settings

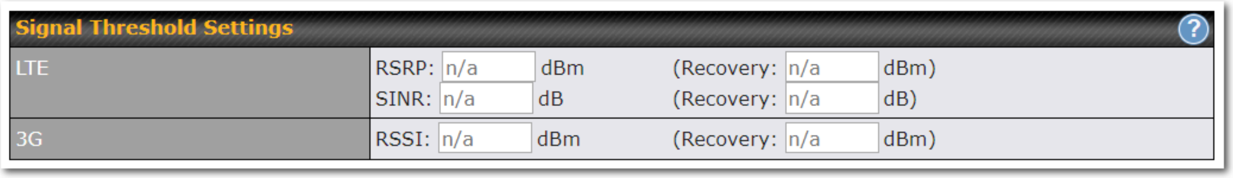
Acceptable Level

If signal threshold is defined, this connection will be treated as down when a weaker than threshold signal is determined.

The following values are used by the threshold scale:

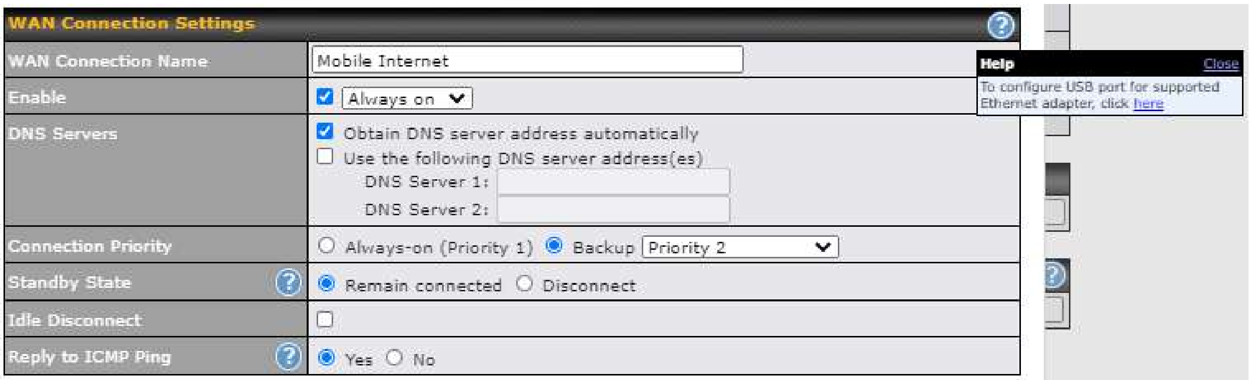
	0 bars	1 bar	2 bars	3 bars	4 bars	5 bars
LTE / RSSRP	-140	-128	-121	-114	-108	-98
3G / RSSI	-120	-100	-95	-90	-85	-75

To define the threshold manually using specific signal strength values, please click on the question Mark and the following field will be visible.


Signal Threshold Settings

LTE	RSRP: n/a dBm (Recovery: n/a dBm) SINR: n/a dB (Recovery: n/a dB)
3G	RSSI: n/a dBm (Recovery: n/a dBm)

WAN Connection Settings (USB)



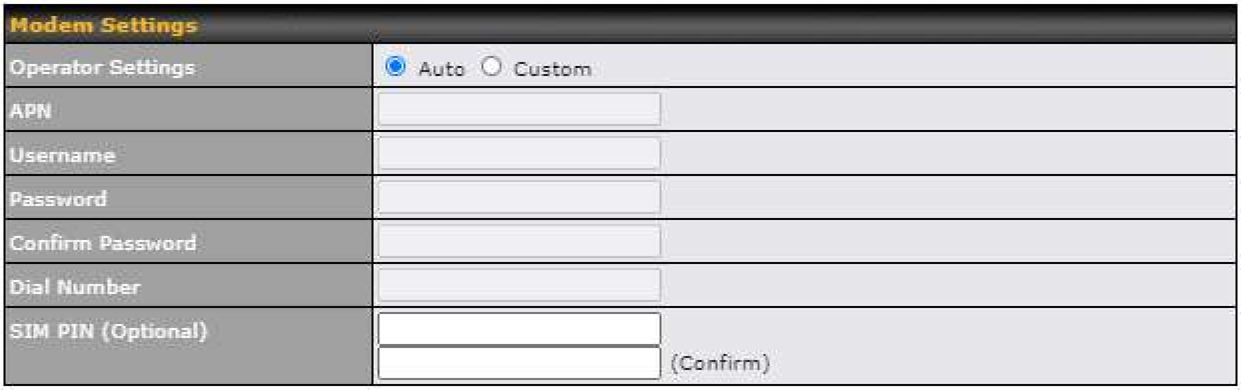
WAN Connection Settings	
WAN Connection Name	Mobile Internet
Enable	☑ Always on
DNS Servers	☑ Obtain DNS server address automatically □ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Connection Priority	○ Always-on (Priority 1) ● Backup Priority 2
Standby State	● Remain connected ○ Disconnect
Idle Disconnect	□
Reply to ICMP Ping	● Yes ○ No

Help Close

To configure USB port for supported Ethernet adapter, click here

WAN Connection Settings	
WAN Connection Name	Indicate a name you wish to give this WAN connection
Enable	This setting enables the WAN connection. If schedules have been defined, you will be able to select a schedule to apply to the connection.
DNS Server	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.
Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If **Always-on** is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If **Backup** is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
Standby State	This option allows you to choose whether to remain the connection connected or disconnect it when this WAN connection is no longer in the highest priority and has entered the standby state.
Idle Disconnect	If this is checked, the connection will disconnect when idle after the configured Time value. This option is disabled by default.
Reply to ICMP Ping	If the checkbox is **unticked**, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: **ticked** (Yes)

By default, the USB port is “USB Modem” mode. If you need to use it to connect to USB Ethernet Adapter, you need to change it to “USB Ethernet” mode, by enabling the hidden feature ?. Once this feature is enabled, the interface will behave as normal Ethernet WAN. The options that are the same as the ethernet WAN connection configuration are shown in the Ethernet WAN section.

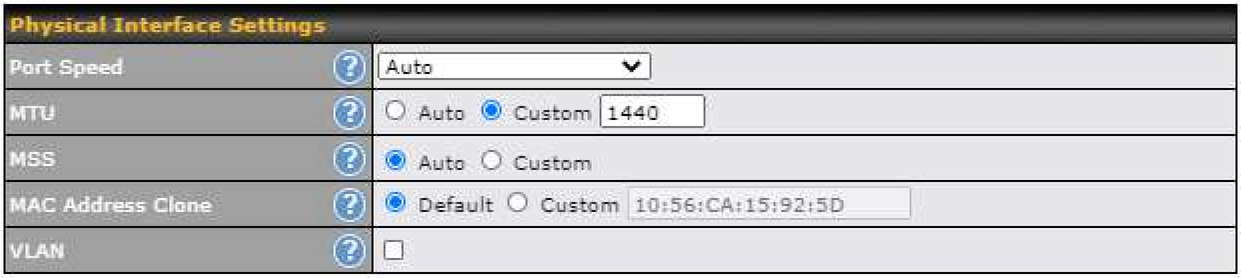


Modem Settings	
Operator Settings	● Auto ○ Custom
APN	
Username	
Password	
Confirm Password	
Dial Number	
SIM PIN (Optional)	(Confirm)

ModemSettings	
Operator Settings	This setting allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connections, you may select **Custom** to enter your carrier’s **APN**, **Login**, **Password**, and **Dial Number** settings manually. The correct values can be obtained from your carrier. The default and recommended setting is **Auto**.
APN / Login / Password / SIM PIN	When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP.

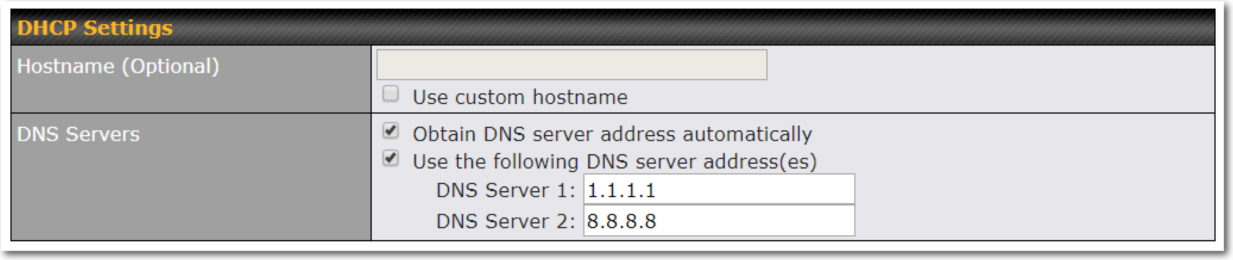
WAN Connection Settings (Common)

The remaining WAN-related settings are common to both Ethernet and cellular WAN



Physical Interface Settings	
Port Speed ?	Auto
MTU ?	○ Auto ● Custom 1440
MSS ?	● Auto ○ Custom
MAC Address Clone ?	● Default ○ Custom 10:56:CA:15:92:5D
VLAN ?	□

Physical Interface Settings	
Speed	This is the port speed of the WAN connection. It should be set to the same speed as the connected device in case of any port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device or not. Advertise Speed is selected by default. You can choose not to advertise the port speed if the port has difficulty in negotiating with the peer device. Default: Auto
MTU	This field is for specifying the Maximum Transmission Unit value of the WAN connection. An excessive MTU value can cause file downloads stall shortly after connected. You may consult your ISP for the connection's MTU value. Default value is 1440.
MSS	This field is for specifying the Maximum Segment Size of the WAN connection. When Auto is selected, MSS will be depended on the MTU value. When Custom is selected, you may enter a value for MSS. This value will be announced to remote TCP servers for maximum data that it can receive during the establishment of TCP connections. Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections. Normally, MSS equals to MTU minus 40. You are recommended to reduce the MSS only if changing of the MTU value cannot effectively inform some remote servers to size down data size. Default: Auto
MAC Address Clone	Some service providers (e.g. cable network) identify the client's MAC address and require client to always use the same MAC address to connect to the network. If it is the case, you may change the WAN interface's MAC address to the client PC's one by entering the PC's MAC address to this field. If you are not sure, click the Default button to restore to the default value.
VLAN	Check the box to assign a VLAN to the interface.



DHCP Settings	
Hostname (Optional)	□ Use custom hostname
DNS Servers	☑ Obtain DNS server address automatically ☑ Use the following DNS server address(es) DNS Server 1: 1.1.1.1 DNS Server 2: 8.8.8.8

DHCP Settings	
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with a hostname, you can safely bypass this option.

DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

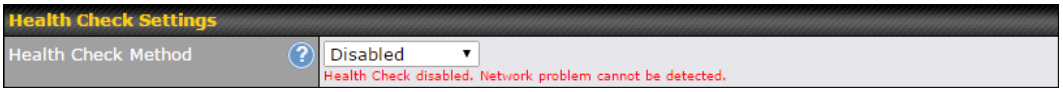
Health Check Settings

To ensure traffic is routed to healthy WAN connections only, the Peplink Balance can periodically check the health of each WAN connection.
Health Check settings for each WAN connection can be independently configured via **Network > Interfaces > WAN > *Connection name* > Health Check Settings.**

Enable Health Check by selecting PING, DNS Lookup, or HTTP from the Health Check Method drop-down menu.

Health Check Settings	
Method	This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

Health Check Disabled

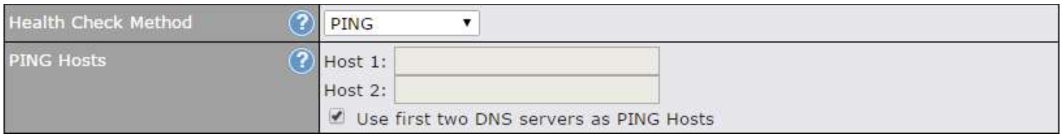


Health Check Settings

Health Check Method	Disabled ▾ Health Check disabled. Network problem cannot be detected.

When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

Health Check Method: PING

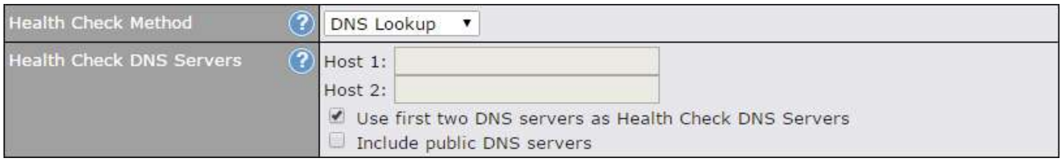


Health Check Method	PING ▾
PING Hosts	Host 1: Host 2: ☑ Use first two DNS servers as PING Hosts

ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

PING Hosts	This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup



Health Check Method	DNS Lookup ▾
Health Check DNS Servers	Host 1: Host 2: ☑ Use first two DNS servers as Health Check DNS Servers □ Include public DNS servers

DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

Health Check DNS Servers

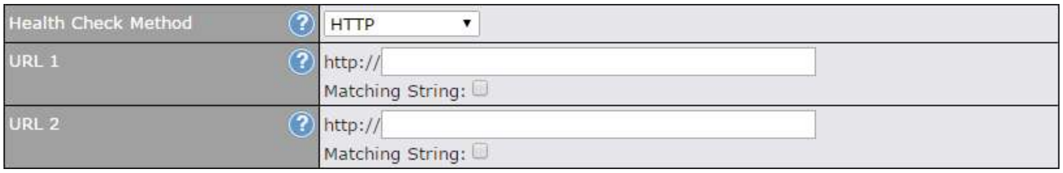
This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS Lookup.

If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.

If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP



Health Check Method	HTTP ▾
URL 1	http:// Matching String: □
URL 2	http:// Matching String: □

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1

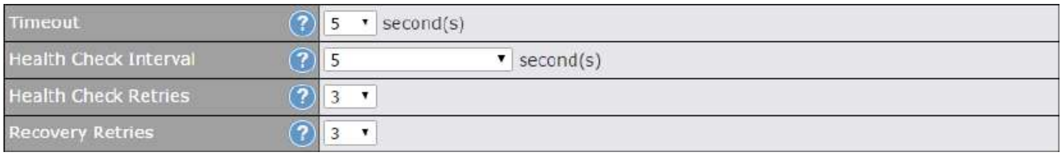
The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

If **URL2** is also provided, a health check will pass if either one of the tests passed.

Other Health Check Settings



Timeout	5 second(s)
Health Check Interval	5 second(s)
Health Check Retries	3
Recovery Retries	3

Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**.
Health Check Retries	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink Balance will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.
Recovery Retries	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Peplink Balance treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

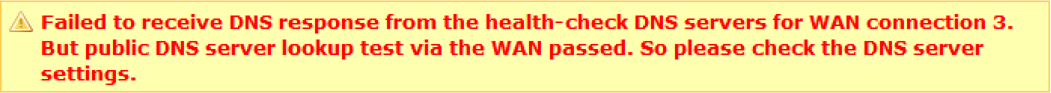
Note

If a WAN connection goes down, all of the WAN connections not set with a **Connection Type** of **Always-on** will also be brought up until any one of higher priority WAN connections is up and found to be healthy. This design could increase overall network availability.

For example, if WAN1, WAN2, and WAN3 have connection types of **Always-on**, **Backup Priority Group 1**, and **Backup Priority Group 2**, respectively, when WAN1 goes down, WAN2 and WAN3 will try to connect. If WAN3 is connected first, WAN2 will still be kept connecting. If WAN2 is connected, WAN3 will disconnect or stop connecting.

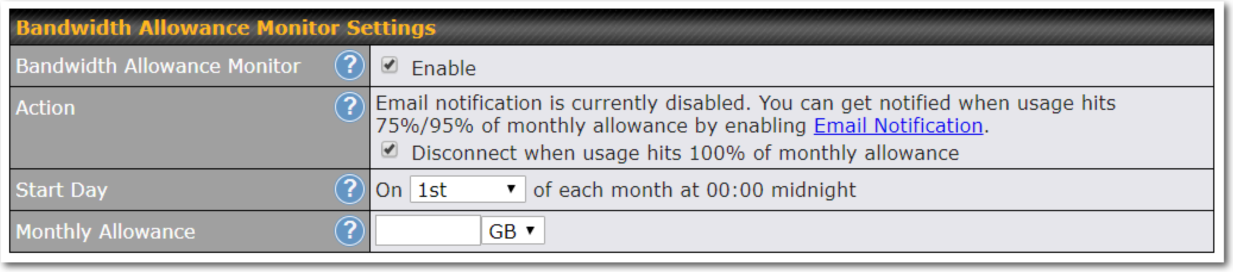
Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and checks fail, the Balance will automatically perform DNS lookups on some public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:



⚠ **Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.**

Bandwidth Allowance Monitor Settings

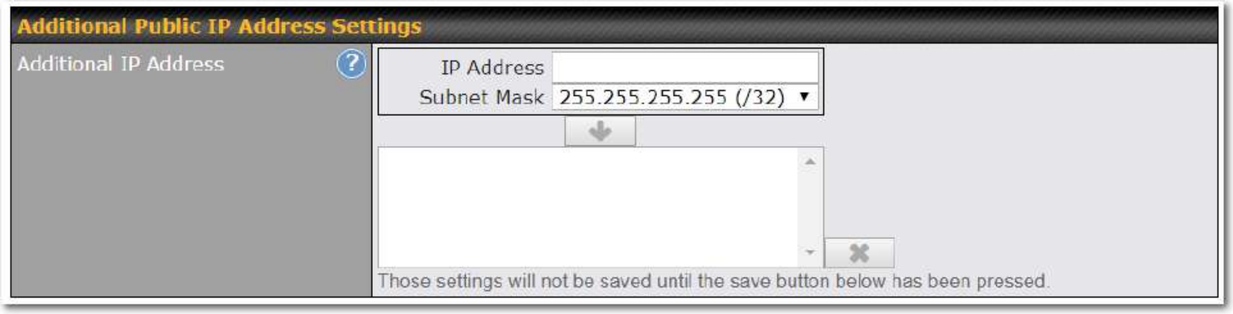


Bandwidth Allowance Monitor Settings	
Bandwidth Allowance Monitor	☑ Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st ▾ of each month at 00:00 midnight
Monthly Allowance	GB ▾

Bandwidth Allowance Monitor	
Action	If **Email Notification** is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Disclaimer
Due to different network protocol overheads and conversions, the amount of data reported by this Peplink device is not representative of actual billable data usage as metered by your network provider. Peplink disclaims any obligation or responsibility for any events arising from the use of the numbers shown here.

Additional Public IP Settings



Additional Public IP Address Settings	
Additional IP Address	IP Address Subnet Mask 255.255.255.255 (/32) ▾ Those settings will not be saved until the save button below has been pressed.

Additional Public IP Settings	
IP Address List	**IP Address List** represents the list of fixed Internet IP addresses assigned by the ISP in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the **Down Arrow** button to populate IP address entries to the **IP Address List**.

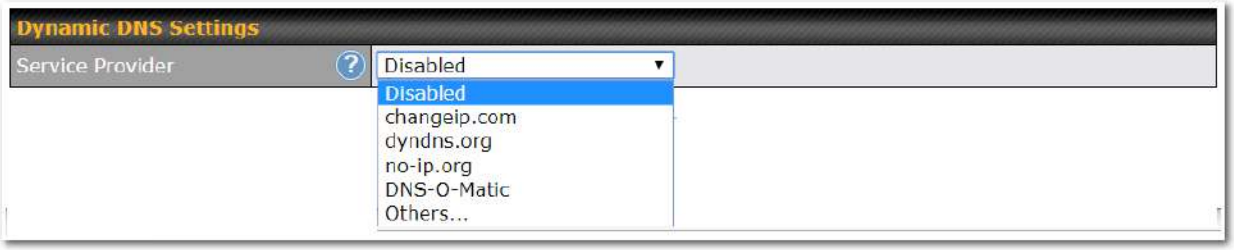
Dynamic DNS Settings

Peplink Balance routers allow registering domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a hostname. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address externally even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

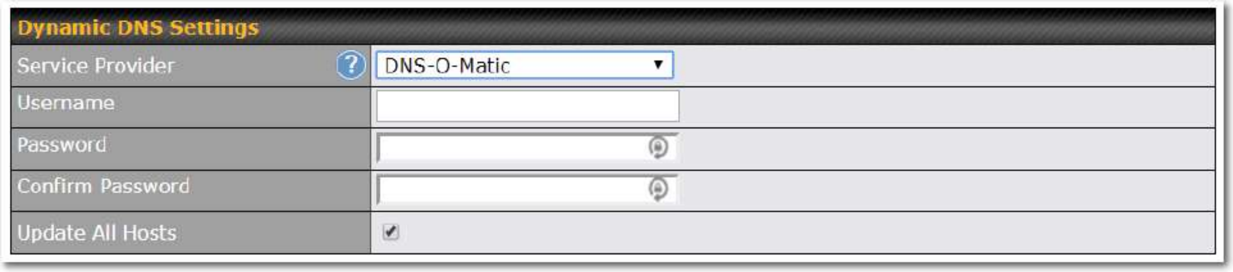
Either upon a change in IP addresses or every 23 days without link reconnection, the Peplink Balance will connect to the dynamic DNS service provider to update the provider’s IP address records.

The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via **Network>Interfaces>WAN>*Connection name*>Dynamic DNS Settings**.


Dynamic DNS Settings

Service Provider: Disabled

If your desired provider is not listed, you may check with **DNS-O-Matic**. This service supports updating 30 other dynamic DNS service providers. (Note: Peplink is not affiliated with DNS-O-Matic.)



Dynamic DNS Settings	
Service Provider	DNS-O-Matic ▾
Username	
Password	
Confirm Password	
Update All Hosts	☑

Dynamic DNS Settings	
Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are: ● changeip.com ● dyndns.org ● no-ip.org ● tzo.com ● DNS-O-Matic ● Others… support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API. Select **Disabled** to disable this feature.
User ID / User / Email	This setting specifies the registered user name for the dynamic DNS service.
Password / Pass / TZO Key	This setting specifies the password for the dynamic DNS service.
Update All Hosts	Check this box to automatically update all hosts.
Hosts / IDs	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

Important Note

In order to use dynamic DNS services, appropriate hostname registration(s), as well as a valid account with a supported dynamic DNS service provider, are required.

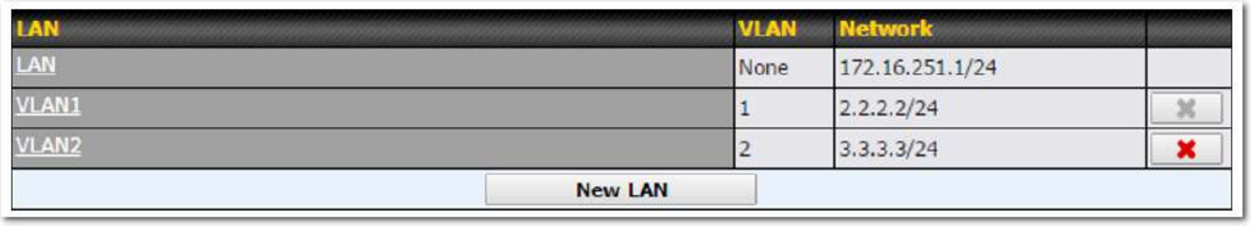
A dynamic DNS update is performed whenever a WAN's IP address is changed, such as when an IP is changed after a DHCP IP refresh or reconnection.

Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record has not been not updated for a long time. Therefore, the Peplink Balance performs an update every 23 days, even if a WAN's IP address did not change.

10.2 LAN

10.2.1 Network Settings

LAN interface settings are located at **Network>LAN>Network Settings**. Navigating to that page will show the following dashboard:

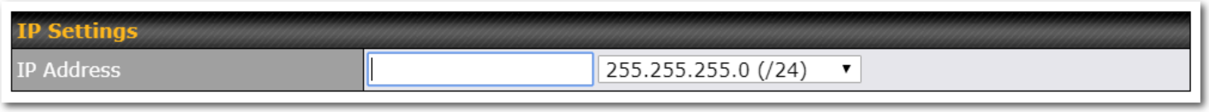


LAN	VLAN	Network	
LAN	None	172.16.251.1/24	
VLAN1	1	2.2.2.2/24	✖
VLAN2	2	3.3.3.3/24	✖

This represents the LAN interfaces that are active on your router (including VLAN). A grey “X” means that the VLAN is used in other settings and cannot be deleted. You can find which settings are using the VLAN by hovering over the grey “X”.

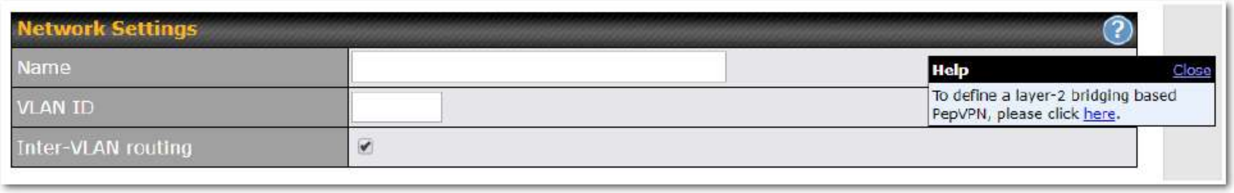
Alternatively, a red “X” means that there are no settings using the VLAN. You can delete that VLAN by clicking the red “X”

Clicking on any of the existing LAN interfaces (or creating a new one) will show the following :



IP Settings	
IP Address	255.255.255.0 (/24) ▾

IP Settings	
IP Address	The IP address and subnet mask of the Pepwave router on the LAN.

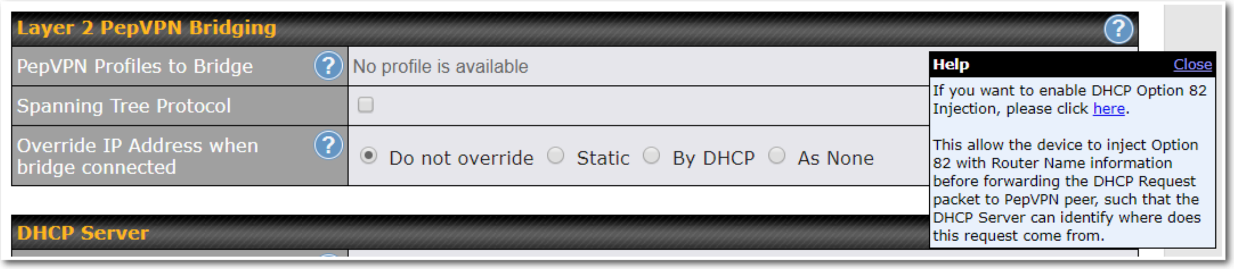


Network Settings	
Name	
VLAN ID	
Inter-VLAN routing	☑

Help Close
To define a layer-2 bridging based PepVPN, please click here.

Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a number for your VLAN.
Inter-VLAN	Check this box to enable routing between virtual LANs.

routing



Layer 2 PepVPN Bridging

PepVPN Profiles to Bridge	No profile is available
Spanning Tree Protocol	□
Override IP Address when bridge connected	● Do not override ○ Static ○ By DHCP ○ As None

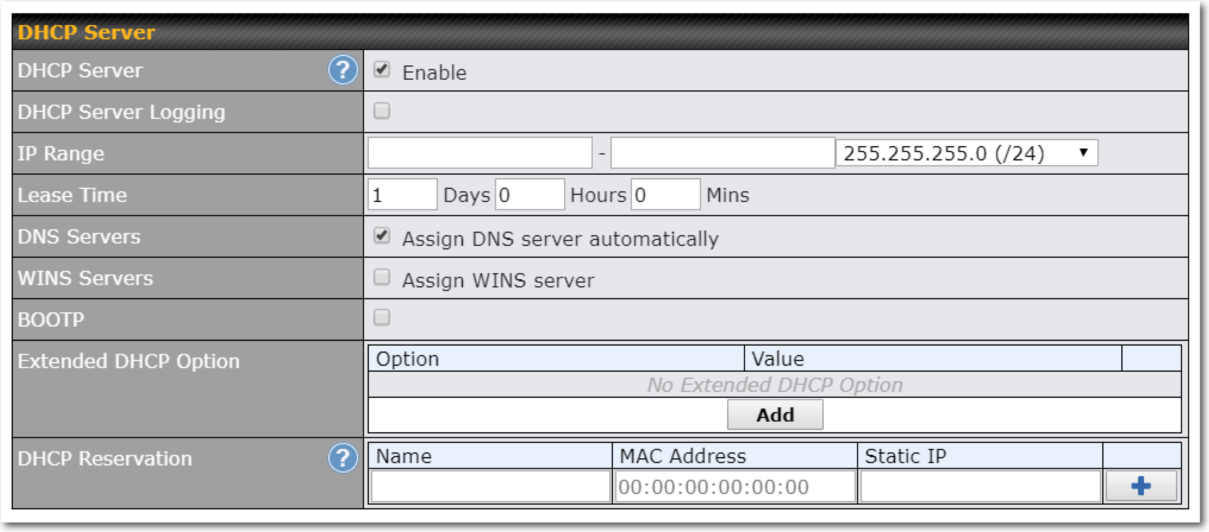
DHCP Server

Help Close

If you want to enable DHCP Option 82 Injection, please click here.

This allow the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to PepVPN peer, such that the DHCP Server can identify where does this request come from.

Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Remote Network Isolation	Enable this option if you want to block network traffic between the remote networks, this will not affect the connectivity between them and this local LAN.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
Override IP Address when bridge connected	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up. If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.
DHCP Option 82	Click on the question Mark if you want to enable DHCP Option 82. This allows the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to a PepVPN peer, such that the DHCP Server can identify where the request originates from.

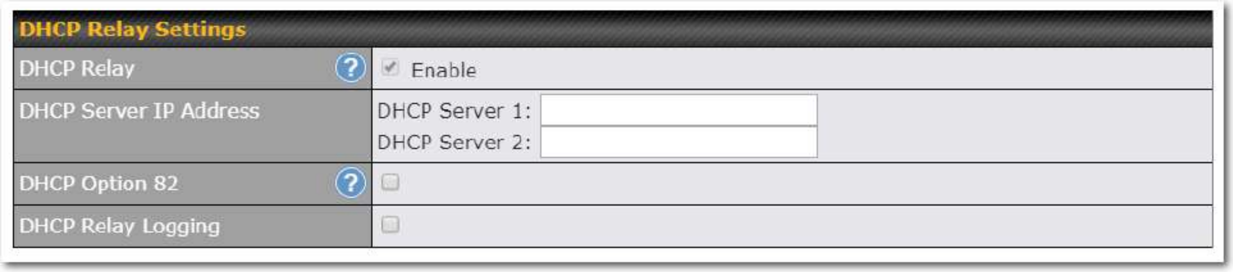


DHCP Server

DHCP Server	☑ Enable
DHCP Server Logging	□
IP Range	- 255.255.255.0 (/24)
Lease Time	1 Days 0 Hours 0 Mins
DNS Servers	☑ Assign DNS server automatically
WINS Servers	□ Assign WINS server
BOOTP	□
Extended DHCP Option	Option / Value *No Extended DHCP Option* Add
DHCP Reservation	Name / MAC Address / Static IP 00:00:00:00:00:00 +

DHCP Server Settings	
DHCP Server	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.
DHCP Server Logging	Enable logging of DHCP events in the eventlog by selecting the checkbox.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Servers	This option allows you to optionally specify a Windows Internet Name Service (WINS) server. You may choose to use the **built-in WINS server** or **external WINS servers**. When this unit is connected using SpeedFusion^{TM}, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP **WINS Server** setting. Afterward, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.

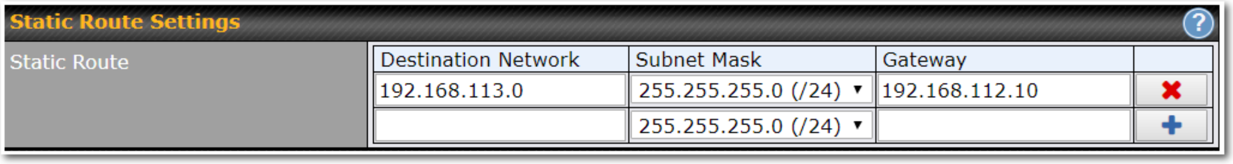
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press + to create a new record. Press ✖ to remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3.**



DHCP Relay Settings	
DHCP Relay	☑ Enable
DHCP Server IP Address	DHCP Server 1: DHCP Server 2:
DHCP Option 82	□
DHCP Relay Logging	□

DHCP Relay Settings	
DHCP Relay	Enter the address of the DHCP server here. DHCP requests will be relayed to it.
DHCP Server IP Address	DHCP requests from the LAN are relayed to the entered DHCP server. For active-passive DHCP server configurations, enter active and passive DHCP server IPs into the **DHCP Server 1** and **DHCP Server 2** fields.
DHCP Option 82	This feature includes device information as relay agent for the attached client when forwarding DHCP requests from a DHCP client to a DHCP server. Device MAC address and network name are embedded to circuit ID and Remote ID in option 82.
DHCP Relay Logging	Check this box to log DHCP relay activity.

10.2.2 Network Settings (Common Settings)

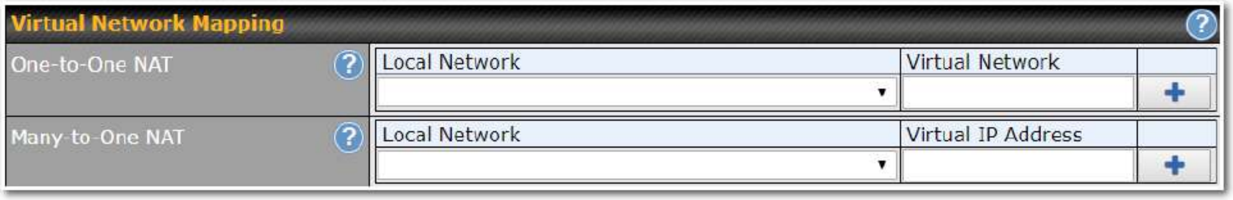


Static Route Settings

Static Route	Destination Network	Subnet Mask	Gateway	
	192.168.113.0	255.255.255.0 (/24) ▾	192.168.112.10	✖
		255.255.255.0 (/24) ▾		+

Static Route Settings	
Static Route	This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in *w.x.y.z* format. The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnet. Click + to create a new route. Click ✖ to remove a route. Entries in this list will allow traffic to route to a different subnet that is connected to the LAN interface. Any traffic destined for a network/mask pair will be directed to the corresponding gateway instead of routed through WANs.

[A] - Advanced feature, please click the ? button on the top right hand corner of the Static Route session to activate and configure Virtual Network Mapping to resolve network address conflict with remote peers.



Virtual Network Mapping

	Local Network	Virtual Network	
One-to-One NAT ?	▾		+

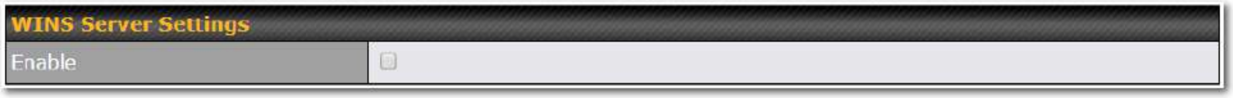
	Local Network	Virtual IP Address	
Many-to-One NAT ?	▾		+

In case of a network address conflict with remote peers (i.e. PepVPN / IPsec VPN / IP Forwarding WAN are considered as remote connections), you can define Virtual Network Mapping to resolve it.

Note: OSPF & RIPv2 settings should be updated as well to avoid advertising conflicted networks.

For further details on virtual network mapping watch this video: https://youtu.be/C1FMdZCn3Z8

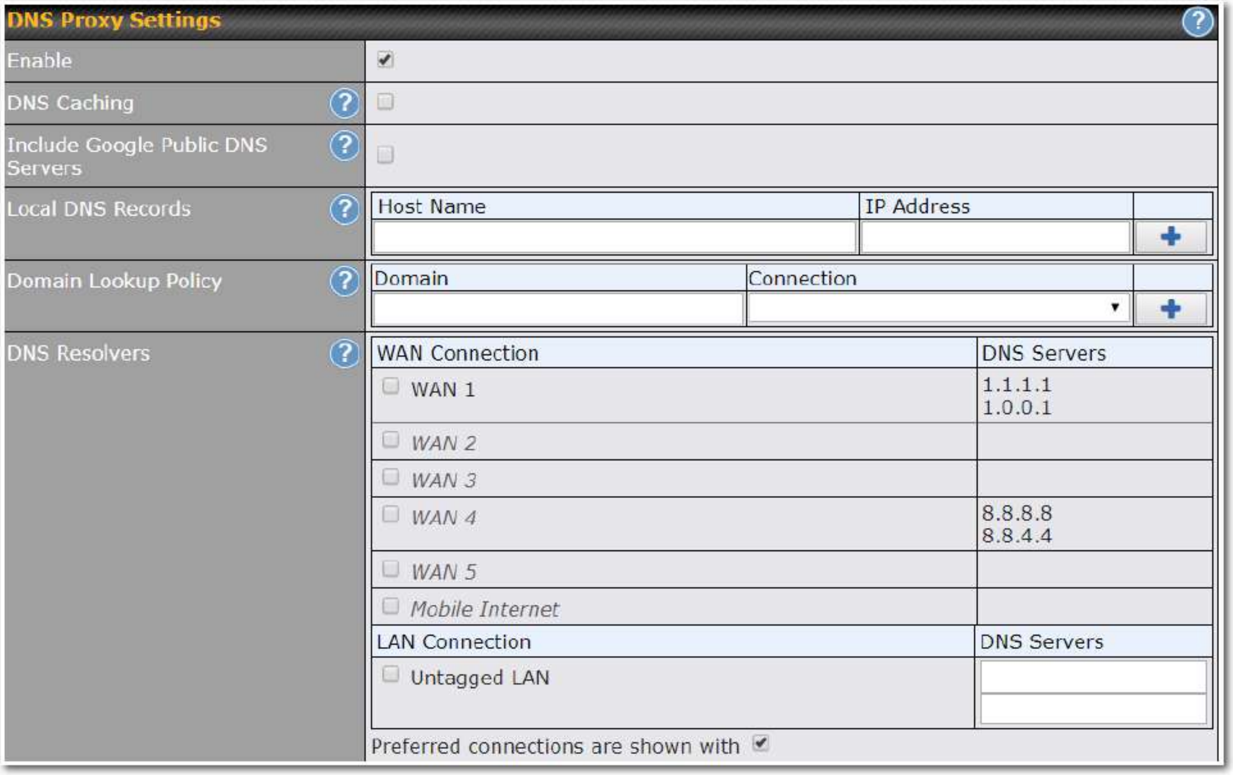
Virtual Network Mapping	
One-to-One NAT	Every IP Address in the Local Network has a corresponding unique Virtual IP Address for NAT. Traffic originating from the Local Network to remote connections will be SNAT'ed and behave like coming from the defined Virtual Network. While traffic initiated by remote peers to the Virtual Network will be DNAT'ed accordingly.
Many-to-One NAT	The subnet range defined in Local Network will be mapped to a single Virtual IP Address for NAT. Traffic can only be initiated from local to remote, and these traffic will be NAT'ed and behaves like coming from the same Virtual IP Address.



WINS Server Settings	
Enable	□

WINS Server Settings	
Enable	Check the box to enable the WINS Server. A list of WINS clients will be displayed at **Status>WINS Clients**.

Enter any needed DNS proxy settings. Once all settings have been entered, click **Save** to store your changes.



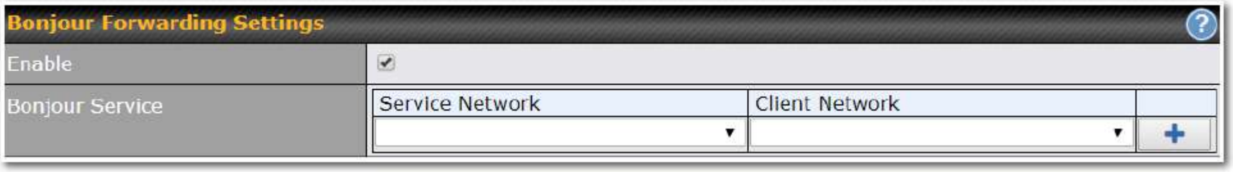
DNS Proxy Settings	
Enable	☑
DNS Caching	□
Include Google Public DNS Servers	□
Local DNS Records	Host Name | IP Address | +
Domain Lookup Policy	Domain | Connection | +
DNS Resolvers	WAN Connection | DNS Servers □ WAN 1 | 1.1.1.1 1.0.0.1 □ WAN 2 □ WAN 3 □ WAN 4 | 8.8.8.8 8.8.4.4 □ WAN 5 □ Mobile Internet LAN Connection | DNS Servers □ Untagged LAN Preferred connections are shown with ☑

DNS Proxy Settings	
Enable	To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**. A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion^{TM} peers. Requests are forwarded to the **DNS servers/resolvers** defined for each WAN connection.
DNS Caching	This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can improve DNS response time by storing all received DNS results for faster DNS lookup. However, it cannot return the most updated result for frequently updated DNS records. By default, **DNS Caching** is disabled.

Include Google Public DNS Servers	When this option is enabled, the DNS proxy server will forward DNS requests to Google's public DNS servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.
Local DNS Records	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Peplink Balance, the corresponding IP address will be returned. To display the option to set TTL manually, click ?. Click + to create a new record. Click ✖ to remove a record.
Domain Lookup Policy	DNS proxy will look up the domain names defined here using only the specified connections.
DNS Resolvers[A]	Check the box to enable the WINS server. A list of WINS clients will be displayed at **Network>LAN>DNS Proxy Settings>DNS Resolvers**. This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es). Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

[A] - Advanced feature, please click the ? button on the top right-hand corner to activate.

Finally, if needed, configure your Bonjour forwarding settings. Once all settings have been entered, click **Save** to store your changes.



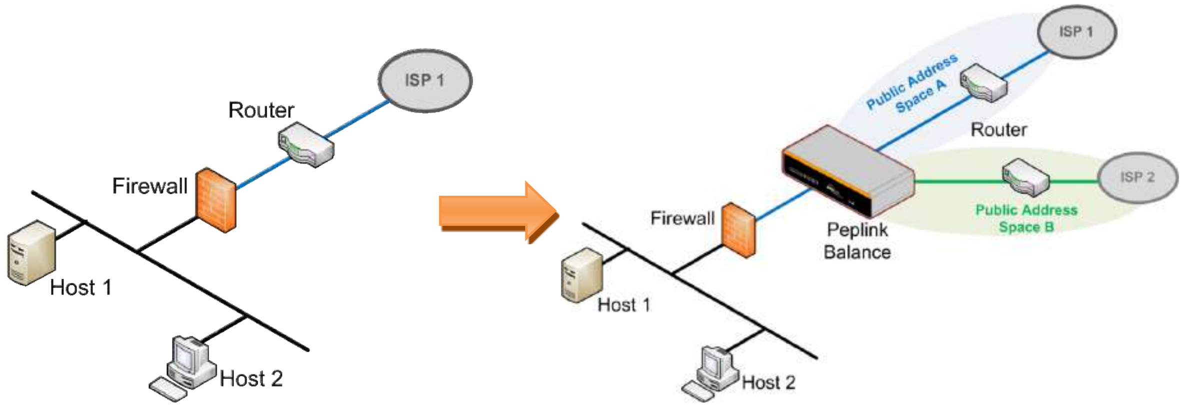
Bonjour Forwarding Settings			
Enable	☑		
Bonjour Service	Service Network	Client Network	
	▾	▾	+

Bonjour Forwarding Settings	
Enable	Check this box to turn on Bonjour forwarding.
Bonjour Service	Choose **Service** and **Client** networks from the drop-down menus, and then click + to add the networks. To delete an existing Bonjour listing, click ✖. Bonjour Forwarding is supported on All Balance models, MAX 700, HD2, HD4

Drop-In Mode

Drop-in mode (or transparent bridging mode) eases the installation of the Peplink Balance on a live network between the firewall and router, such that changes to the settings of existing equipment are not required.

The following diagram illustrates drop-in mode setup:

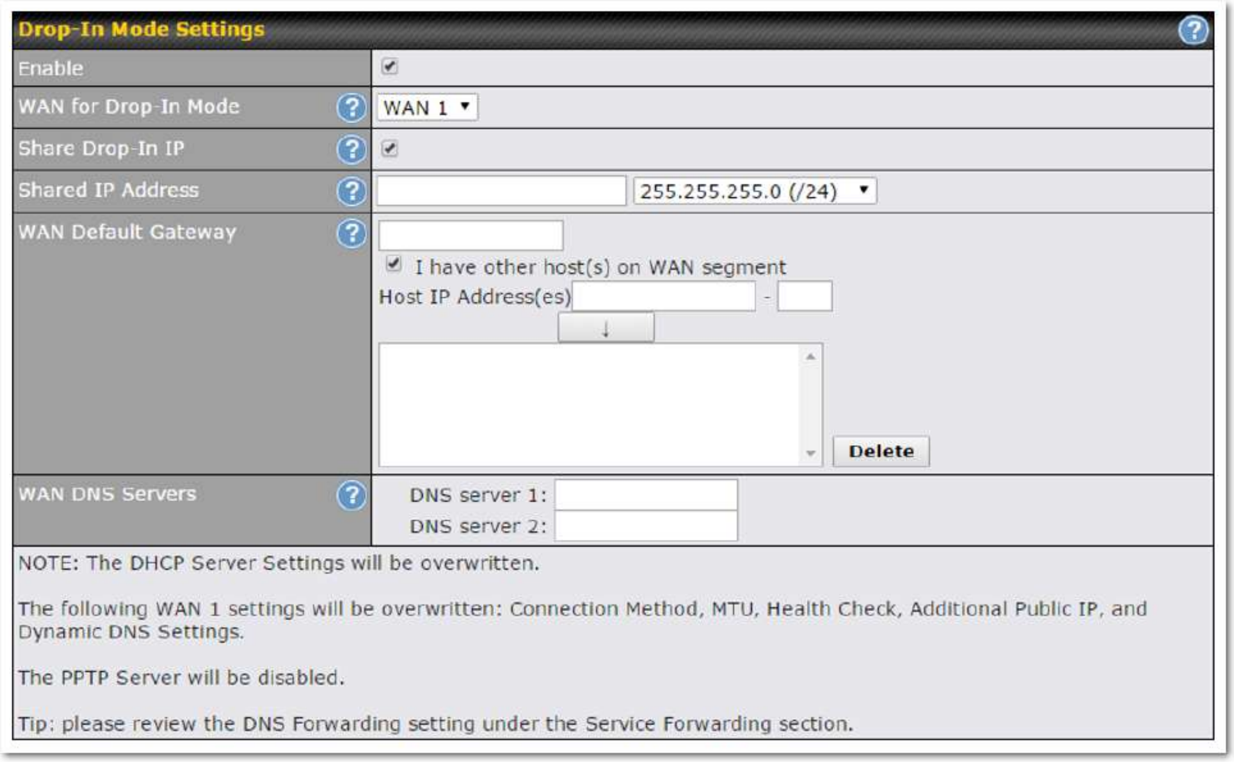


Enable drop-in mode using the Setup Wizard. After enabling this feature and selecting the WAN for drop-in mode, various settings, including the WAN's connection method and IP address, will be automatically updated.

When drop-in mode is enabled, the LAN and the WAN for drop-in mode ports will be bridged. Traffic between the LAN hosts and WAN router will be forwarded between the devices. In this case, the hosts on both sides will not notice any IP or MAC address changes.

After successfully setting up the Peplink Balance as part of the network using drop-in mode, it will, depending on model, support one or more WAN connections. Some MediaFast units also support multiple WAN connections after activating drop-in mode, though a SpeedFusion license may be required to activate more than one WAN port.

Please note the Drop-In Mode is mutually exclusive with VLAN.



Drop-In Mode Settings	
Enable	☑
WAN for Drop-In Mode	WAN 1 ▾
Share Drop-In IP	☑
Shared IP Address	255.255.255.0 (/24) ▾
WAN Default Gateway	☑ I have other host(s) on WAN segment Host IP Address(es) -
WAN DNS Servers	DNS server 1: DNS server 2:

NOTE: The DHCP Server Settings will be overwritten.

The following WAN 1 settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.

The PPTP Server will be disabled.

Tip: please review the DNS Forwarding setting under the Service Forwarding section.

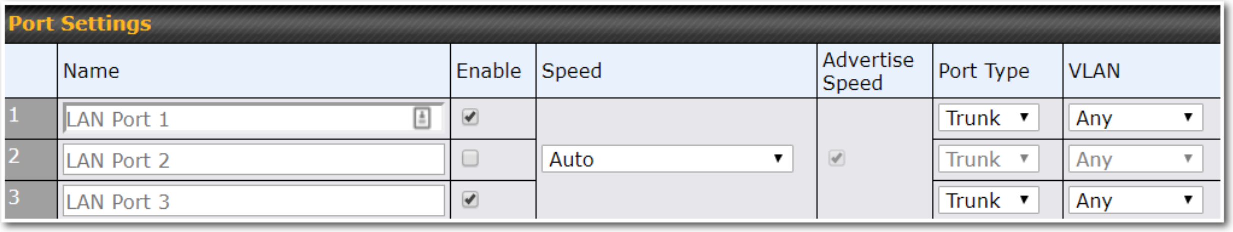
Drop-in Mode Settings	
Enable	Drop-in mode eases the installation of the Peplink Balance on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature. Please refer to **Section 12, Drop-in Mode** for details.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If **WAN 1 with LAN Bypass** is selected, the high availability feature will be disabled automatically.
Shared Drop-In IP^A	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Balance will listen for this IP address when WAN hosts access services provided by the Balance (web admin access from the WAN, DNS server requests, etc.). To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The Balance will listen for this IP address when LAN hosts access services provided by the Balance (web admin access from the WAN, DNS proxy, etc.).
Shared IP Address^A	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)
WAN Default	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the ? button next to "WAN Default Gateway" and check

Gateway	the I **have other host(s) on WAN segment** box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

[A] - Advanced feature, please click the ? button on the top right-hand corner to activate.

10.2.3 Port Settings

To configure port settings, navigate to **Network > Port Settings**



Port Settings

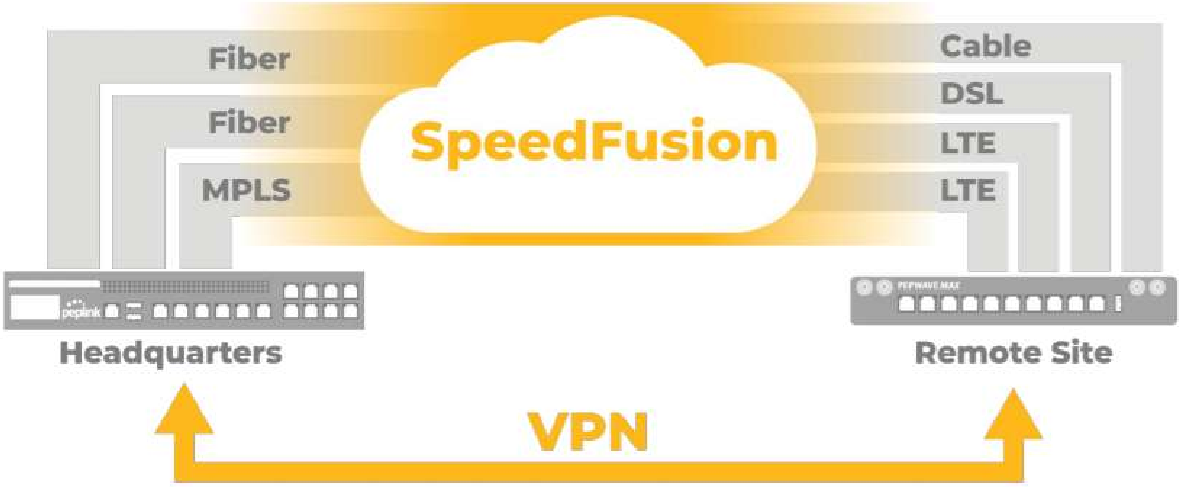
	Name	Enable	Speed	Advertise Speed	Port Type	VLAN
1	LAN Port 1	☑	Auto ▾	☑	Trunk ▾	Any ▾
2	LAN Port 2	□			Trunk ▾	Any ▾
3	LAN Port 3	☑			Trunk ▾	Any ▾

This section allows you to:

- Enable or disable specific LAN ports
- Configure the negotiation speed of the LAN ports
- Configure the port type (Trunk or Access)
- Assign a VLAN to a LAN port (in Access mode)

10.3 VPN

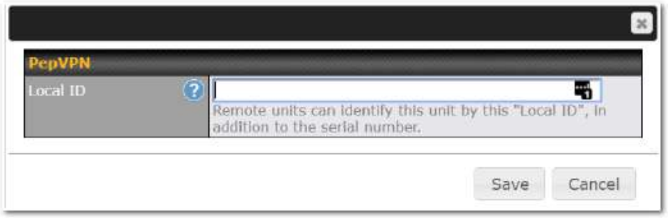
10.3.1 SpeedFusion



Peplink Balance SpeedFusion^{TM} Bandwidth Bonding is our patented technology that enables our SD-WAN routers to bond multiple Internet connections to increase site-to-site bandwidth and reliability. SpeedFusion securely connects one or more branch offices to your company's main headquarters or to other branches. The data, voice, and video communications between these locations are kept confidential across the public Internet.

The SpeedFusion^{TM} of the Peplink Balance is specifically designed for multi-WAN environments. With SpeedFusion, in case of failures and network congestion at one or more WANs, other WANs can be used to continue carrying the network traffic. Peplink Balance routers can bond all WAN connections' bandwidth for routing SpeedFusion^{TM} traffic. Unless all the WAN connections of one site are down, the Peplink Balance can keep the VPN up and running.
Bandwidth bonding is enabled by default.

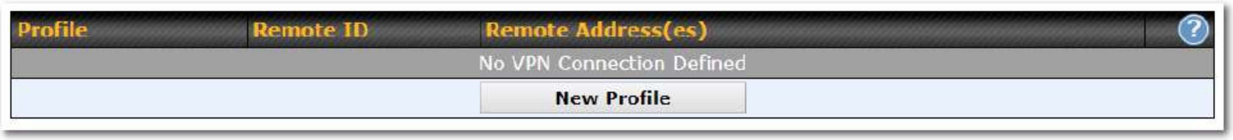
To begin, navigate to **Network > VPN > SpeedFusion** and enter a Local ID and click save.



PepVPN

Local ID	Remote units can identify this unit by this "Local ID", in addition to the serial number.

This device will be identified by other SpeedFusion Peers by this local ID. The following menus will appear:

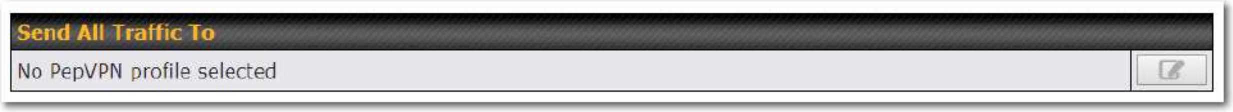


Profile	Remote ID	Remote Address(es)
No VPN Connection Defined		
New Profile		

SpeedFusion Profiles

This table displays all defined profiles. Click the **New Profile** button to create a new profile for making a VPN connection to a remote unit via available WAN connections. Each pair of VPN connection requires its own profile.

The local LAN subnet and subnets behind the LAN (defined under Static Route on the LAN Settings page) will be advertised to the VPN. All VPN members will be able to route to local subnets.

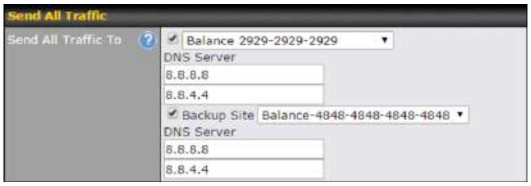


Send All Traffic To

No PepVPN profile selected

Send All Traffic To

This feature allows you to redirect all traffic to a specified PepVPN connection. Click the ✎ button to select your connection and the following menu will appear:



Send All Traffic

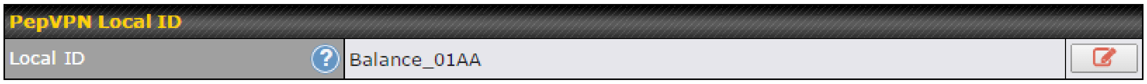
Send All Traffic To: ☑ Balance 2929-2929-2929 ▾

DNS Server: 8.8.8.8, 8.8.4.4

☑ Backup Site: Balance-4848-4848-4848-4848 ▾

DNS Server: 8.8.8.8, 8.8.4.4

You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over should the main PepVPN connection fail.

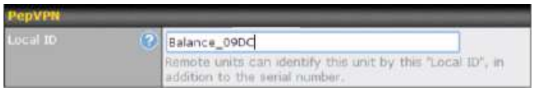


PepVPN Local ID

Local ID: Balance_01AA

PepVPN Local ID

This feature allows you to change the local ID of a PepVPN connection. Click the ✎ button to select your connection and the following menu will appear:

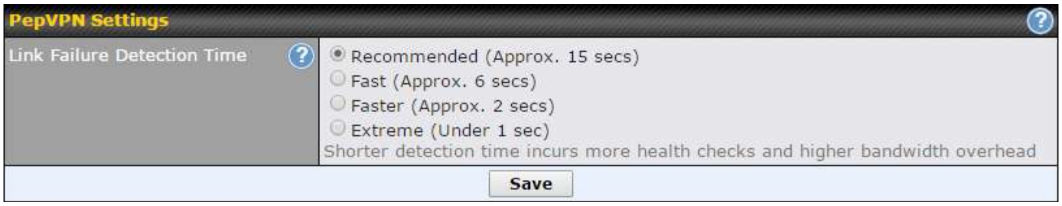


PepVPN

Local ID: Balance_09DC

Remote units can identify this unit by this "Local ID", in addition to the serial number.

After updating the local ID, click **Save** to store your changes.



PepVPN Settings

Link Failure Detection Time

● Recommended (Approx. 15 secs)
○ Fast (Approx. 6 secs)
○ Faster (Approx. 2 secs)
○ Extreme (Under 1 sec)

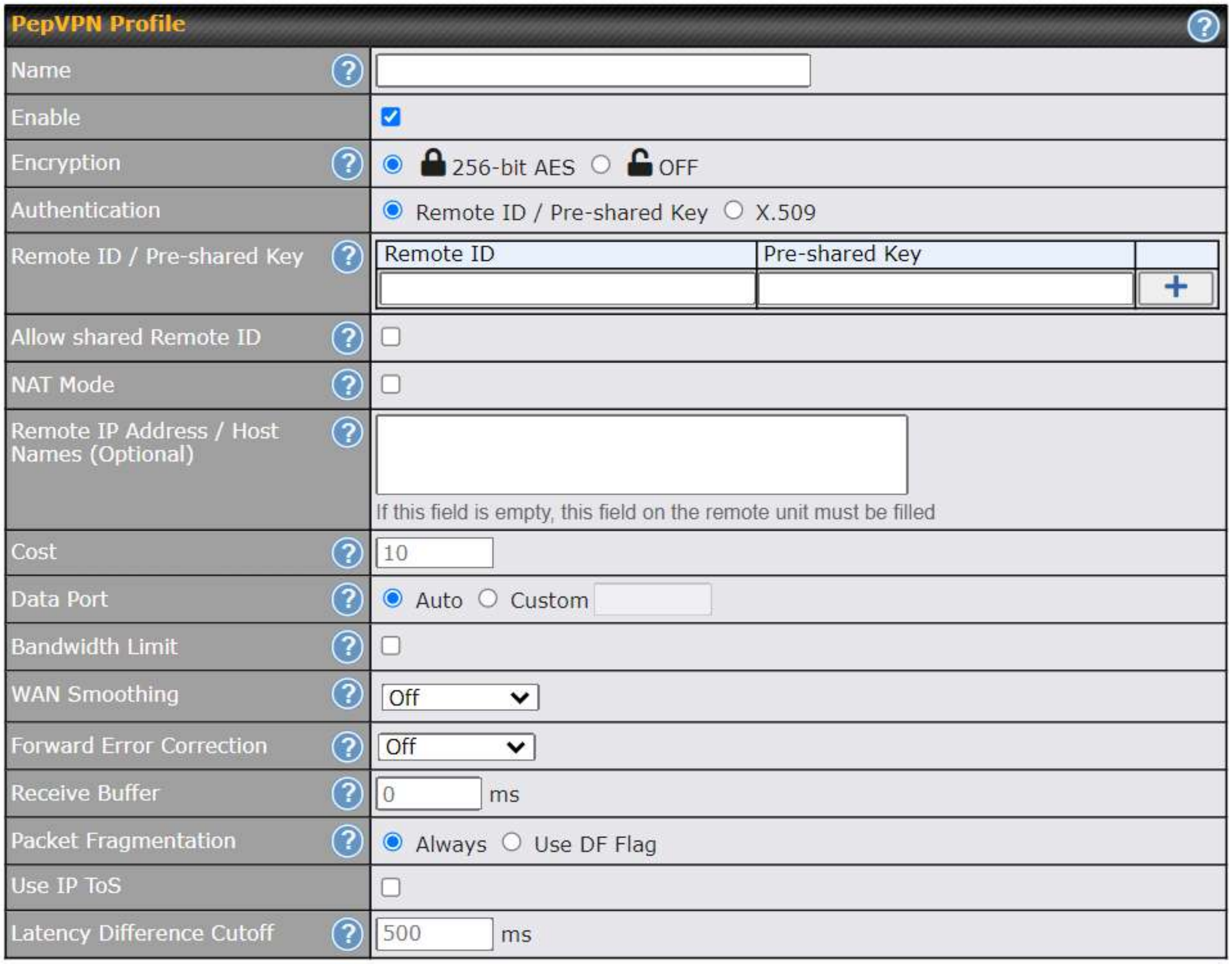
Shorter detection time incurs more health checks and higher bandwidth overhead

Link Failure Detection	
Link Failure Detection Time	The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed. When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds. When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds. When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds. When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

Important Note
Peplink proprietary SpeedFusion^{TM} uses TCP port 32015 and UDP port 4500 for establishing VPN connections. If you have a firewall in front of your Peplink Balance devices, you will need to add firewall rules for these ports and protocols to allow inbound and outbound traffic to pass through the firewall.

SpeedFusion: Profile Configuration

Click the **New Profile** button, or click one of the existing profiles, and the following menus will appear:



PepVPN Profile	
Name	
Enable	☑
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key ○ X.509
Remote ID / Pre-shared Key	Remote ID / Pre-shared Key / +
Allow shared Remote ID	□
NAT Mode	□
Remote IP Address / Host Names (Optional)	If this field is empty, this field on the remote unit must be filled
Cost	10
Data Port	● Auto ○ Custom
Bandwidth Limit	□
WAN Smoothing	Off
Forward Error Correction	Off
Receive Buffer	0 ms
Packet Fragmentation	● Always ○ Use DF Flag
Use IP ToS	□
Latency Difference Cutoff	500 ms

A list of defined SpeedFusion connection profiles and a **Link Failure Detection Time** option will be shown. Click the **New Profile** button to create a new VPN connection profile for making a VPN connection to a remote Peplink Balance via the available WAN connections. Each profile is for making a VPN connection with one remote Peplink Balance.

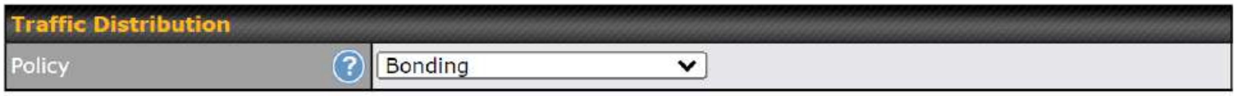
PepVPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ( ). Click the ? icon next to the **PepVPN Profile** title bar to use the IP ToS field of your data packet on PepVPN WAN traffic.

Enable	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with **256-bit AES**. If **Off** is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from **By Remote ID Only**, **Preshared Key**, or **X.509** to specify the method the Peplink Balance will use to authenticate peers. When selecting **By Remote ID Only**, be sure to enter a unique peer ID number in the **Remote ID** field.
Remote ID / Pre-shared Key	This optional field becomes available when **Remote ID / Pre-shared Key** is selected as the Peplink Balance's VPN **Authentication** method, as explained above. **Pre-shared Key** defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored. Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the ? icon next to the "Remote ID / Preshared Key" setting.
Remote ID/Remote Certificate	These optional fields become available when **X.509** is selected as the Peplink Balance's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the **Show Details** link below the field.
Allow Shared Remote ID	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When **NAT Mode** is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	If **NAT Mode** is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted. This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established. Click the ? icon to customize the handshake port of the remote Host (TCP)
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10
Data Port	This field is used to specify a UDP port number for transporting outgoing VPN data. If **Default** is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If **Custom** is selected, enter an outgoing port number from 1 to 65535.

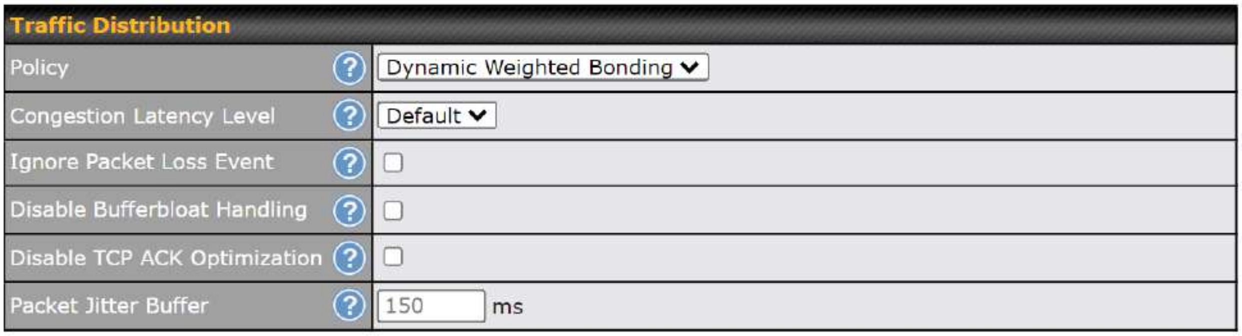
	Click the ? icon to configure data stream using TCP protocol [EXPERIMENTAL]. In the case TCP protocol is used, the exposed TCP session option can be authorised to work with TCP accelerated WAN link.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
WAN Smoothing	While using PepVPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the WAN's available bandwidth. Off - Disable WAN Smoothing. Normal - The total bandwidth consumption will be at most 2x of the original data traffic. Medium - The total bandwidth consumption will be at most 3x of the original data traffic. High - The total bandwidth consumption depends on the number of connected active tunnels.
Forward Error Correction	Forward Error Correction (FEC) can help to recover packet loss by using extra bandwidth to send redundant data packets. Higher FEC level will recover packets on a higher loss rate link. The expected overhead of Low is 13.3% and High is 26.7%. Require peer using PepVPN version 8.0.0 and above.
Receive Buffer	Receive Buffer can help to reduce out-of-order packets and jitter, but will introduce extra latency to the tunnel. Default is 0 ms, which disables the buffer, and maximum buffer size is 2000 ms.
Packet Fragmentation	If the packet size is larger than the tunnel's MTU, it will be fragmented inside the tunnel in order to pass through. Select Always to fragment any packets that are too large to send, or Use DF Flag to only fragment packets with Don't Fragment bit cleared. This can be useful if your application does Path MTU Discovery, usually sending large packets with DF bit set, if allowing them to go through by fragmentation, the MTU will not be detected correctly.
Use IP ToS[A]	If Use IP ToS is enabled, the ToS value of the data packets will be copied to the PepVPN header during encapsulation.
Latency Difference Cutoff[A]	Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used)

[A] - Advanced feature, please click the ? button on the top right-hand corner to activate.

To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>*LAN Profile Name***

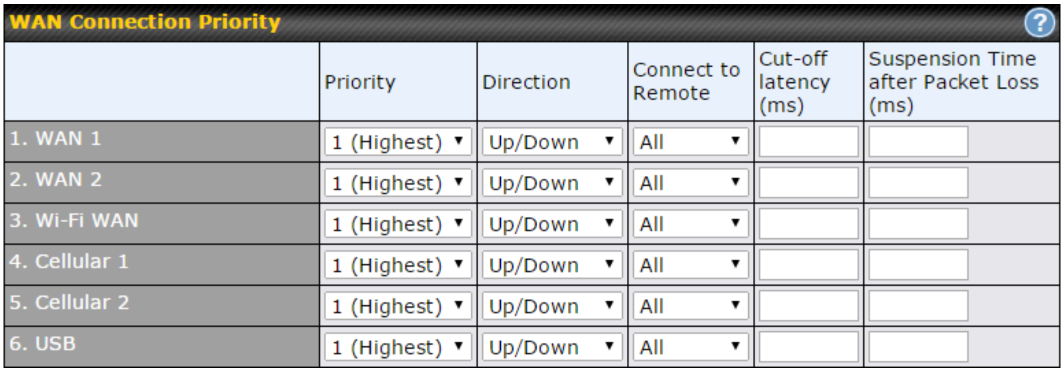


Traffic Distribution	
Policy	Bonding



Traffic Distribution	
Policy	Dynamic Weighted Bonding
Congestion Latency Level	Default
Ignore Packet Loss Event	□
Disable Bufferbloat Handling	□
Disable TCP ACK Optimization	□
Packet Jitter Buffer	150 ms

Traffic Distribution	
Policy	This option allows you to select the desired out-bound traffic distribution policy: ● Bonding - Aggregate multiple WAN-to-WAN links into a single higher throughput tunnel. ● Dynamic Weighted Bonding - Aggregates WAN-to-WAN links with similar latencies. By default, Bonding is selected as a traffic distribution policy.
Congestion Latency Level	For most WANs, especially on cellular networks, the latency will increase when the link becomes more congested. Setting the **Congestion Latency Level** to **Low** will treat the link as congested more aggressively. Setting it to **High** will allow the latency to increase more before treating it as congested.
Ignore Packet Loss Event	By default, when there is packet loss, it is considered as a congestion event. If this is not the case, select this option to ignore the packet loss event.
Disable Bufferbloat Handling	Bufferbloat is a phenomenon on the WAN side when it is congested. The latency can become very high due to buffering on the uplink. By default, the Dynamic Weighted Bonding policy will try its best to mitigate bufferbloat by reducing TCP throughput when the WAN is congested. However, as a side effect, the tunnel might not achieve maximum bandwidth. Selecting this option will **disable** the bufferbloat handling mentioned above.
Disable TCP ACK Optimization	By default, TCP ACK will be forwarded to remote peers as fast as possible. This will consume more bandwidth, but may help to improve TCP performance as well. Selecting this option will **disable** the TCP ACK optimization mentioned above.
Packet Jitter Buffer	The default jitter buffer is 150ms, and can be modified from 0ms to 500ms. The jitter buffer may increase the tunnel latency. If you want to keep the latency as low as possible, you can set it to 0ms to disable the buffer. **Note**: If the Receive Buffer is set, the Packet Jitter Buffer will be automatically disabled.



WAN Connection Priority ?

	Priority	Direction	Connect to Remote	Cut-off latency (ms)	Suspension Time after Packet Loss (ms)
1. WAN 1	1 (Highest) ▾	Up/Down ▾	All ▾		
2. WAN 2	1 (Highest) ▾	Up/Down ▾	All ▾		
3. Wi-Fi WAN	1 (Highest) ▾	Up/Down ▾	All ▾		
4. Cellular 1	1 (Highest) ▾	Up/Down ▾	All ▾		
5. Cellular 2	1 (Highest) ▾	Up/Down ▾	All ▾		
6. USB	1 (Highest) ▾	Up/Down ▾	All ▾		

WAN Connection Priority	
WAN Connection Priority	If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be used. To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the ? button.

Peplink also published a whitepaper about Speedfusion which can be downloaded from the following url:
http://download.peplink.com/resources/whitepaper-speedfusion-and-best-practices-2019.pdf

10.3.2 IPsec VPN

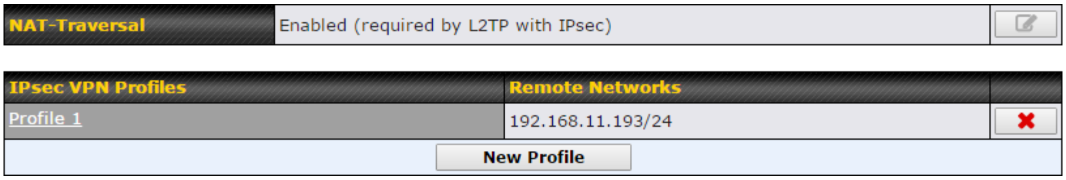
Peplink Balance IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between these locations are kept safe and confidential across the public Internet.

All Peplink products can make multiple IPsec VPN connections with Peplink routers, as well as Cisco and Juniper routers.

Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN with a selection of encryption standards, such as 3DES, AES-128, and AES-256.

To configure, navigate to **Network > VPN >IPsec VPN**.



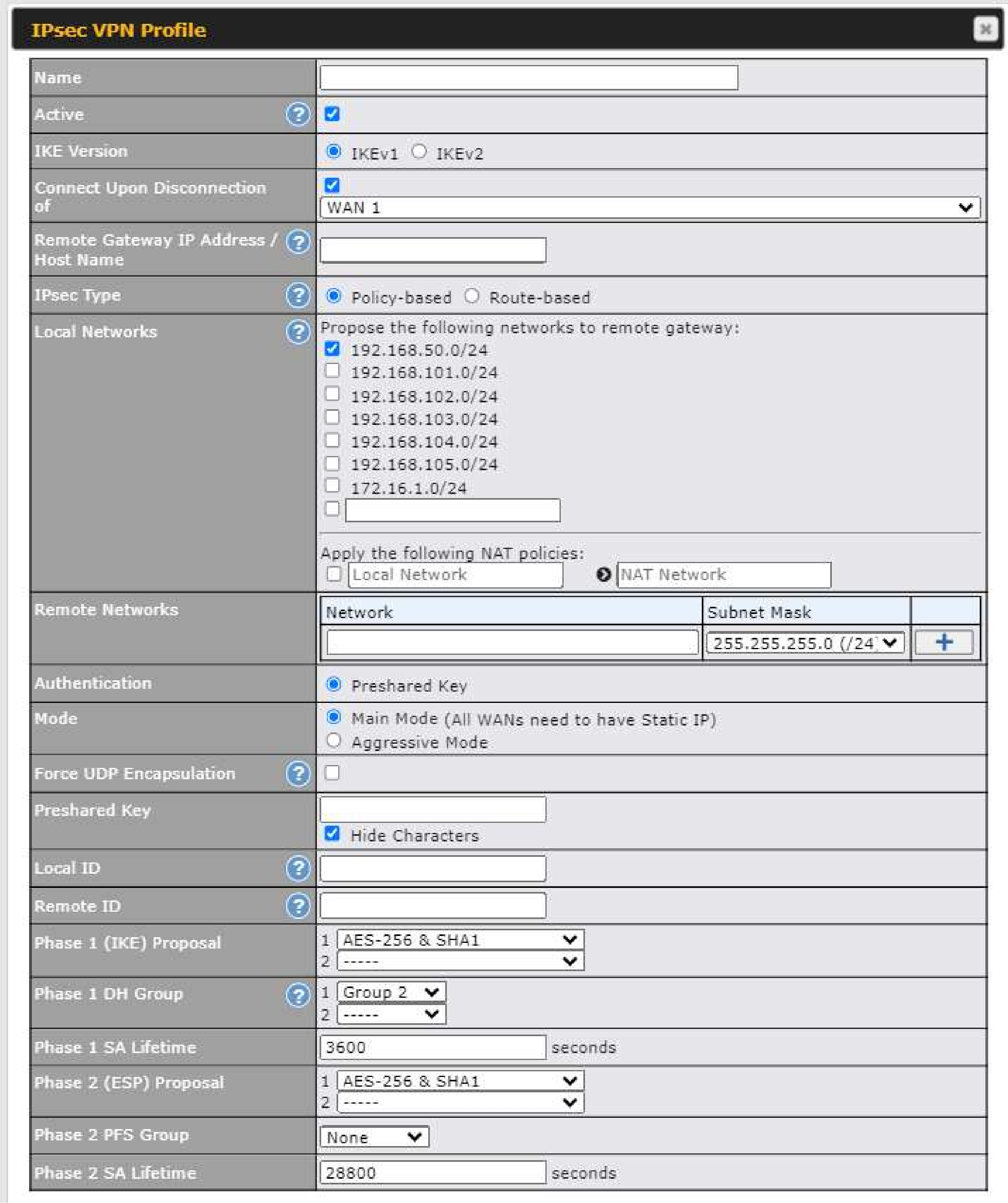
NAT-Traversal	Enabled (required by L2TP with IPsec)	

IPsec VPN Profiles	Remote Networks	
Profile 1	192.168.11.193/24	✖

A **NAT-Traversal** option and list of defined **IPsec VPN** profiles will be shown.

NAT-Traversal should be enabled if your system is behind a NAT router.

Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Peplink Balance, Cisco, or Juniper Routers via available WAN connections. To edit any of the profiles, click on its associated connection name in the leftmost column.



IPsec VPN Profile

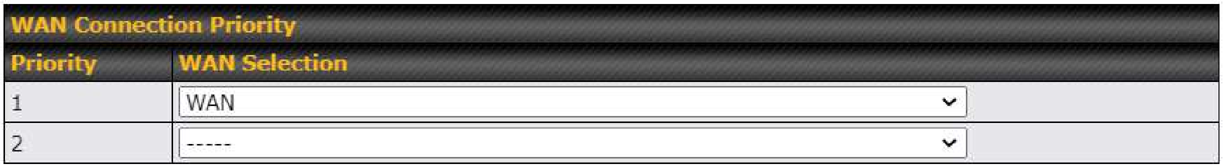
Name	
Active	☑
IKE Version	● IKEv1 ○ IKEv2
Connect Upon Disconnection of	☑ WAN 1
Remote Gateway IP Address / Host Name	
IPsec Type	● Policy-based ○ Route-based
Local Networks	Propose the following networks to remote gateway: ☑ 192.168.50.0/24 ☐ 192.168.101.0/24 ☐ 192.168.102.0/24 ☐ 192.168.103.0/24 ☐ 192.168.104.0/24 ☐ 192.168.105.0/24 ☐ 172.16.1.0/24 ☐ Apply the following NAT policies: ☐ Local Network ➜ NAT Network
Remote Networks	Network | Subnet Mask 255.255.255.0 (/24 +
Authentication	● Preshared Key
Mode	● Main Mode (All WANs need to have Static IP) ○ Aggressive Mode
Force UDP Encapsulation	☐
Preshared Key	☑ Hide Characters
Local ID	
Remote ID	
Phase 1 (IKE) Proposal	1 AES-256 & SHA1 2 -----
Phase 1 DH Group	1 Group 2 2 -----
Phase 1 SA Lifetime	3600 seconds
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 2 -----
Phase 2 PFS Group	None
Phase 2 SA Lifetime	28800 seconds

IPsec VPN Settings	
Name	This field is for specifying a local name to represent this connection profile.
Active	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
IKE Version	Two versions of the IKE standards are available: ● IKEv1 ● IKEv2
Connect Upon Disconnection of	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected. To activate this function, click the ? button next to the “Active” option.
Remote Gateway IP Address / Host Name	Enter the remote peer’s public IP address. For **Aggressive Mode**, this is optional.
IPsec Type	Policy-based - (default) All the matched traffic as defined in Local Networks and Remote Networks will be routed to this IPsec connection, this cannot be overridden by other routing methods. Route-based - Outbound Policy rule is required to route traffic to this tunnel and comes with more flexibility to control how to route traffic compared to Policy-based. If you want to modify the traffic selector instead of using the default (0.0.0.0/0). **Note**: This option is only available for the following models: ● Balance: 30 LTE/Pro, One/Two, 210/310 HW4 or above, 305/380 or above ● MediaFast ● X series
Local Networks	Enter the local LAN subnets here. If you have defined static routes, they will be shown here. Using NAT, you can map a specific local network / IP address to another, and the packets received by remote gateway will appear to be coming from the mapped network / IP address. This allows you to establish IPsec connection to a remote site that has one or more subnets overlapped with local site. Two types of NAT policies can be defined: **One-to-One NAT policy**: if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 > 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too. **Many-to-One NAT policy**: if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 > 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate a

	connection to the local clients.
Remote Networks	Enter the LAN and subnets that are located at the remote site here.
Authentication	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the **Preshared Key** and **X.509 Certificate** methods of authentication.
Mode	Choose **Main Mode** if both IPsec peers use static IP addresses. Choose **Aggressive Mode** if one of the IPsec peers uses dynamic IP addresses.
Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Remote Certificate (pem encoded)	Available only when **X.509 Certificate** is chosen as the **Authentication** method, this field allows you to paste a valid X.509 certificate.
Local ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Remote ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Phase 1 (IKE) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In **Aggressive Mode**, only one selection is permitted.
Phase 1 DH Group	This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. **Group 2**: **1024-bit** is the default value. **Group 5**: **1536-bit** is the alternative option.
Phase 1 SA Lifetime	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at **3600** seconds.
Phase 2 (ESP) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In **Aggressive Mode**, only one selection is permitted.
Phase 2 PFS Group	Perfect forward secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key. **None** - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. **Group 2**: 1024-bit Diffie-Hellman group. The larger the group number, the higher the security.

	Group 5: **1536-bit** is the third option.
Phase 2 SA Lifetime	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds.

IPsec VPN on the Peplink Balance is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for his multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen problems (e.g.,unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover



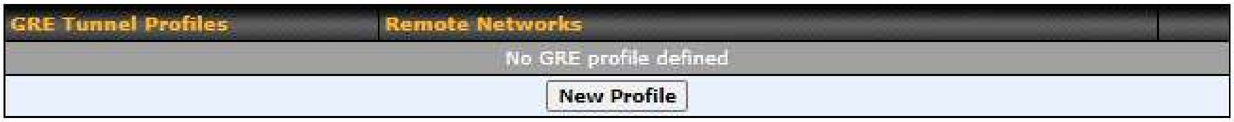
WAN Connection Priority

Priority	WAN Selection
1	WAN
2	-----

IPsec Status shows the current connection status of each connection profile and is displayed at **Status > IPsec VPN***.*

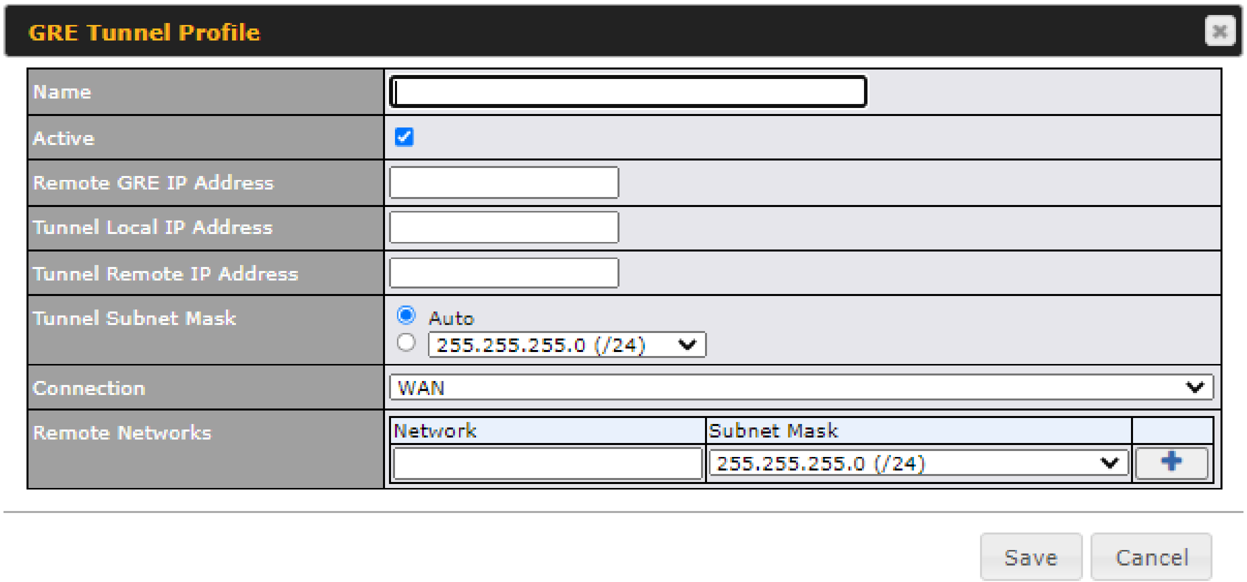
10.3.3 GRE Tunnel

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. A GRE tunnel is similar to IPSec or PepVPN.
To configure a GRE Tunnel, navigate to **Network > VPN > GRE Tunnel**.



GRE Tunnel Profiles	Remote Networks	
No GRE profile defined		

Click the **New Profile** button to create new GRE tunnel profiles that establish tunnel connections to remote tunnel endpoints via available WAN connections. To edit the profiles, click on its associated connection name in the leftmost column.



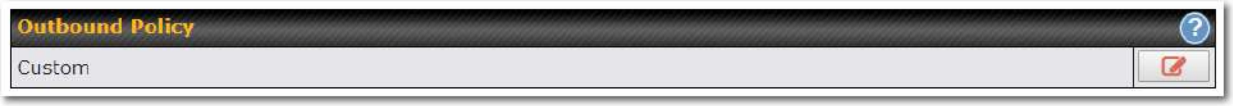
GRE Tunnel Profile

Name	
Active	☑
Remote GRE IP Address	
Tunnel Local IP Address	
Tunnel Remote IP Address	
Tunnel Subnet Mask	● Auto ○ 255.255.255.0 (/24)
Connection	WAN
Remote Networks	Network: Subnet Mask: 255.255.255.0 (/24)

GRE Tunnel Profile Settings	
Name	This field is for specifying a name to represent this GRE Tunnel connection profile.
Active	When this box is checked, this GRE Tunnel connection profile will be enabled. Otherwise, it will be disabled.
Remote GRE IP Address	This field is for entering the remote GRE's IP address
Tunnel Local IP Address	This field is for specifying the tunnel source IP address.
Tunnel Remote IP Address	This field is for specifying the tunnel destination IP address
Tunnel Subnet Mask	This field is to select the subnet mask that is to be used for the GRE tunnel.
Connection	Select the appropriate WAN connection from the drop-down menu.
Remote Networks	Input the LAN and subnets that are located at the remote site here.

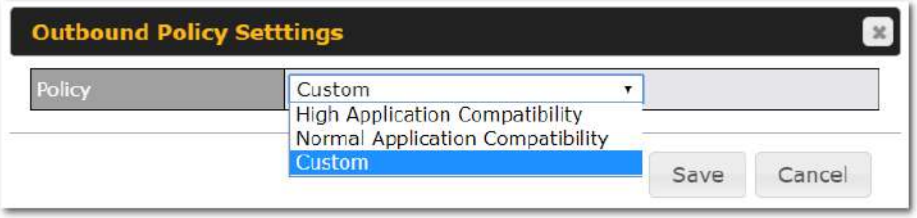
10.4 Outbound Policy

Outbound policies for managing and load balancing outbound traffic are located at **Network>Outbound Policy**. Click the button beside the **Outbound Policy** box:



Outbound Policy

Policy: Custom



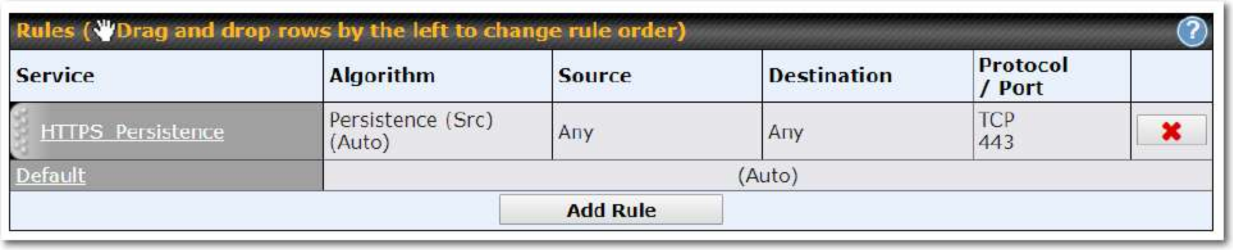
Outbound Policy Setttings

Policy: Custom
- High Application Compatibility
- Normal Application Compatibility
- Custom

A selection menu will appear, giving you the choice between three different Outbound Policy Settings:

Outbound Policy Settings	
High Application Compatibility	Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the highest application compatibility.
Normal Application Compatibility	Outbound traffic from a source LAN device to the same destination Internet IP address will be routed through the same WAN connection persistently, regardless of protocol. This option provides high compatibility to most applications, and users still benefit from WAN link load balancing when multiple Internet servers are accessed.
Custom	Outbound traffic behavior can be managed by defining rules in a custom rule table. A default rule can be defined for connections that cannot be matched with any of the rules.

The menu underneath enables you to define Outbound policy rules:

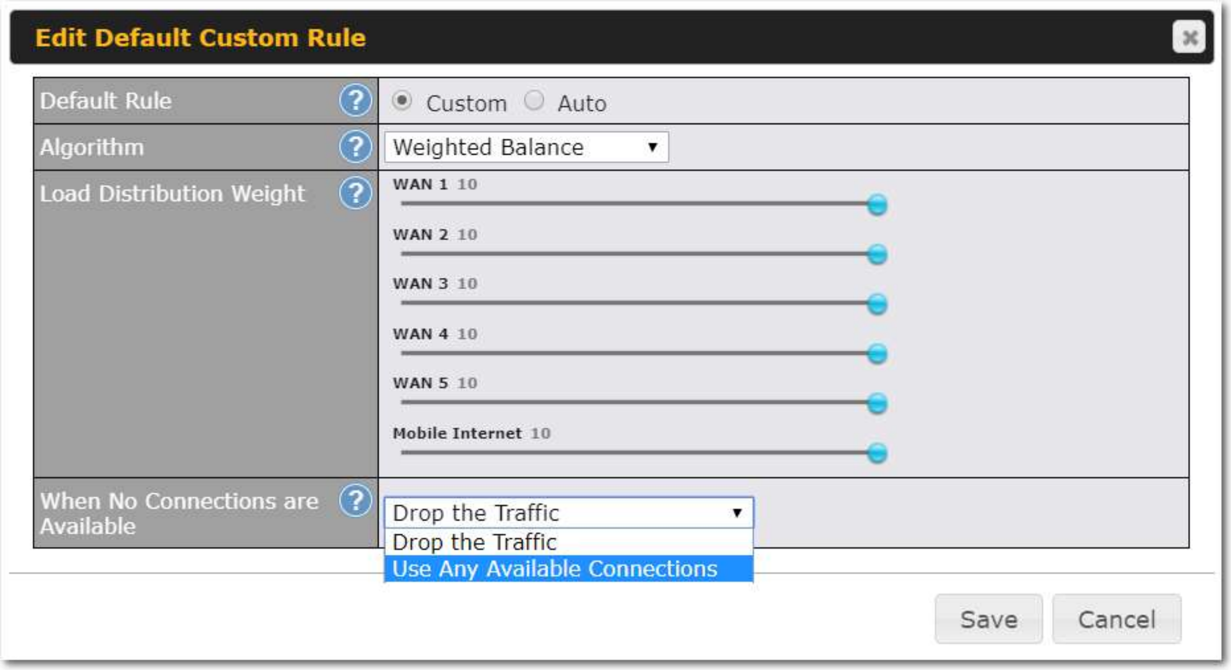


Rules (Drag and drop rows by the left to change rule order)

Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				

The bottom-most rule is **Default**. Edit this rule to change the device's default manner of controlling outbound traffic for all connections that do not match any of the rules above it. Under the **Service** heading, click **Default** to change these settings.

To rearrange the priority of outbound rules, drag and drop them into the desired sequence.

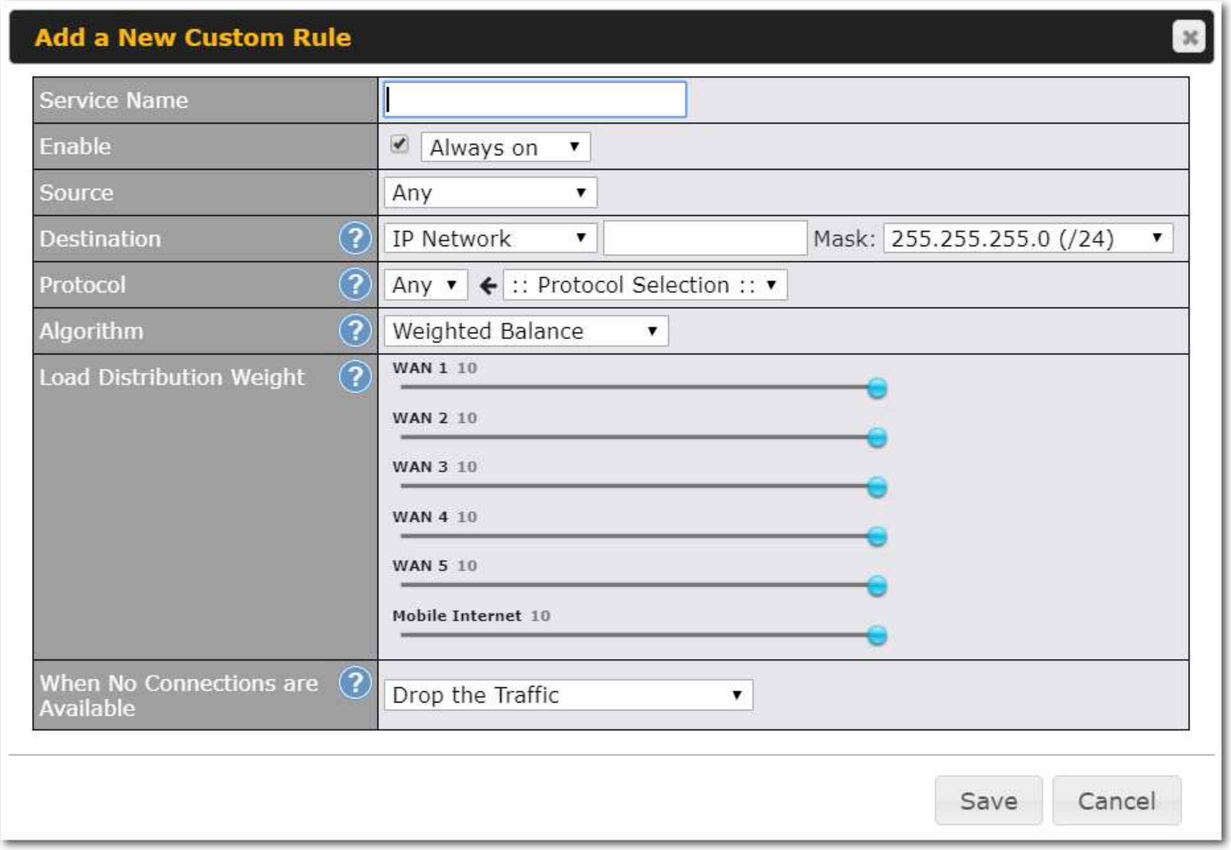


Edit Default Custom Rule

Default Rule	● Custom ○ Auto
Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic

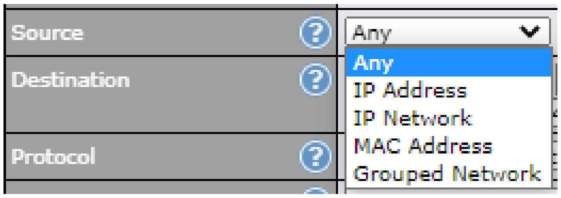
By default, **Auto** is selected as the **Default Rule**. You can select **Custom** to change the algorithm to be used. Please refer to the upcoming sections for the details on the available algorithms.

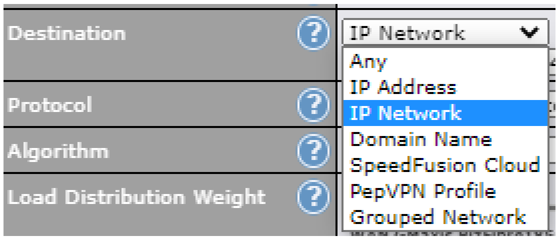
To create a custom rule, click **Add Rule** at the bottom of the table.



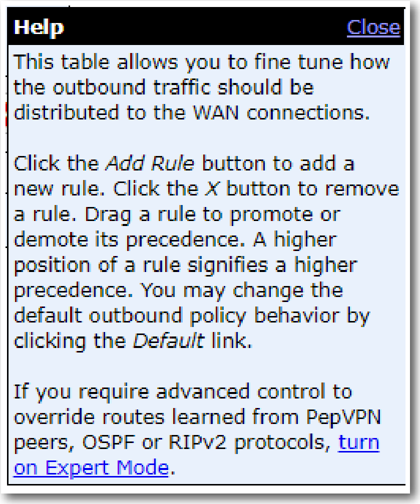
Add a New Custom Rule

Service Name	
Enable	☑ Always on
Source	Any
Destination	IP Network Mask: 255.255.255.0 (/24)
Protocol	Any ← :: Protocol Selection ::
Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic

New Custom Rule Settings	
Service Name	This setting specifies the name of the outbound traffic rule.
Enable	This setting specifies whether the outbound traffic rule takes effect. When **Enable** is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When **Enable** is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule. Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.
Source	This setting specifies the source IP address, IP network, MAC address or Grouped network for traffic that matches the rule.  Source: Any Source Destination Protocol Any IP Address IP Network MAC Address Grouped Network
Destination	This setting specifies the destination IP address, IP network, Domain name, SpeedFusion Cloud, PepVPN Profile or Grouped network for traffic that matches the rule.

	 Destination Protocol Algorithm Load Distribution Weight IP Network Any IP Address IP Network Domain Name SpeedFusion Cloud PepVPN Profile Grouped Network If **Domain Name** is chosen and a domain name, such as *foobar.com*, is entered, any outgoing accesses to *foobar.com* and **.foobar.com* will match this criterion. You may enter a wildcard (.*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter *foobar.*,* for example, *www.foobar.com*, *www.foobar.co.jp*, or *foobar.co.uk* will also match. Placing wildcards in any other position is not supported. NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, access to any one of the server names will also match this rule.
Protocol and Port	This setting specifies the IP protocol and port of traffic that matches this rule. Via a drop-down menu, the following protocols can be specified: ● Any ● TCP ● UDP ● IP ● DSCP Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.
Algorithm	This setting specifies the behavior of the Pepwave router for the custom rule. One of the following values can be selected (note that some Pepwave routers provide only some of these options): ● Weighted Balance ● Persistence ● Enforced ● Priority ● Overflow ● Least Used ● Lowest Latency ● Fastest Response Time For a full explanation of each Algorithm, please see the following article: https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithmns-work/8059
Load Distribution Weight	This is to define the outbound traffic weight ratio for each WAN connection.

When No connections are available	This field allows you to configure the default action when all the selected Connections are not available. **Drop the Traffic** - Traffic will be discarded. **Use Any Available Connections** - Traffic will be routed to any available Connection, even it is not selected in the list. **Fall-through to Next Rule** - Traffic will continue to match next Outbound Policy rule just like this rule is inactive.
Terminate Sessions on Link Recovery	This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the **Priority** algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.



This table allows you to fine tune how the outbound traffic should be distributed to the WAN connections.

Click the *Add Rule* button to add a new rule. Click the *X* button to remove a rule. Drag a rule to promote or demote its precedence. A higher position of a rule signifies a higher precedence. You may change the default outbound policy behavior by clicking the *Default* link.

If you require advanced control to override routes learned from PepVPN peers, OSPF or RIPv2 protocols, turn on Expert Mode.

Expert Mode is available on some Pepwave routers for use by advanced users. To enable the feature, click on the help icon and click **turn on Expert Mode**.

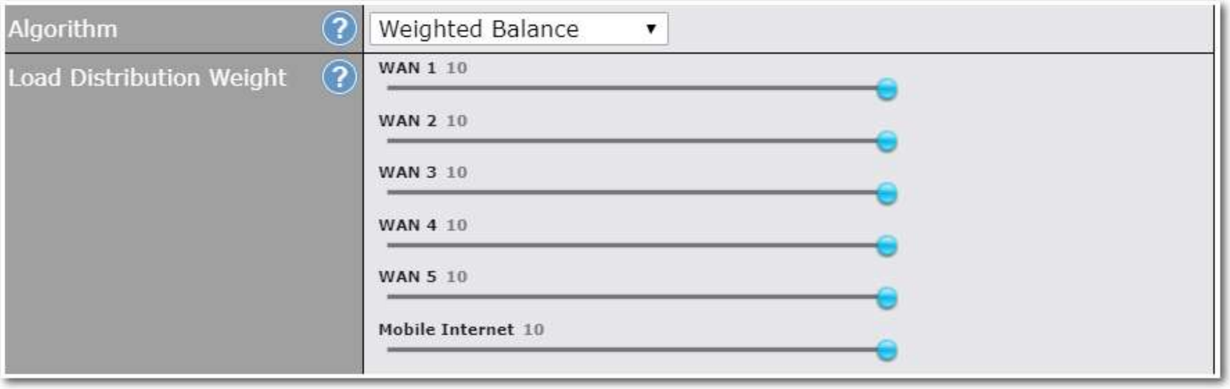
In Expert Mode, a new special rule, **SpeedFusion™ Routes**, is displayed in the **Custom Rules** table. This rule represents all SpeedFusion™ routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. This position means that traffic for remote VPN subnets will be routed to the corresponding VPN peer. You can create custom **Priority** or **Enforced** rules and move them

above the bar to override the SpeedFusion™ routes.

Upon disabling Expert Mode, all rules above the bar will be removed.

Algorithm: Weighted Balance

This setting specifies the ratio of WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Weighted Balance**.



Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10

The amount of matching traffic that is distributed to a WAN connection is proportional to the weight of the WAN connection relative to the total weight. Use the sliders to change each WAN's weight.

For example, with the following weight settings:

- Ethernet WAN1: 10
- Ethernet WAN2: 10
- Wi-Fi WAN: 10
- Cellular 1: 10
- Cellular 2: 10
- USB: 10

Total weight is 60 = (10 +10 + 10 + 10 + 10 + 10).

Matching traffic distributed to Ethernet WAN1 is 16.7% = (10 / 60 x 100%.

Matching traffic distributed to Ethernet WAN2 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Wi-Fi WAN is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Cellular 1 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Cellular 2 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to USB is 16.7% = (10 / 60) x 100%.

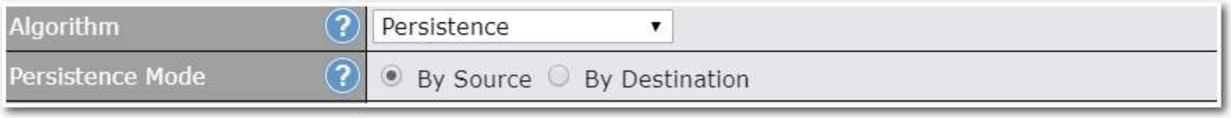
Algorithm: Persistence

The configuration of persistent services is the solution to the few situations where link load distribution for Internet services is undesirable. For example, for security reasons, many e-banking and other secure websites terminate the session when the client computer's Internet IP address changes mid-session.

In general, different Internet IP addresses represent different computers. The security concern is that an IP address change during a session may be the result of an unauthorized intrusion attempt. Therefore, to prevent damages from the potential intrusion, the session is terminated upon the detection of an IP address change.

Pepwave routers can be configured to distribute data traffic across multiple WAN connections. Also, the Internet IP depends on the WAN connections over which communication actually takes place. As a result, a LAN client computer behind the Pepwave router may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Pepwave router with three WAN connections may communicate on the Internet using three different IP addresses.

With the persistence feature, rules can be configured to enable client computers to persistently utilize the same WAN connections for e-banking and other secure websites. As a result, a client computer will communicate using one IP address, eliminating the issues mentioned above.



Algorithm	Persistence ▾
Persistence Mode	● By Source ○ By Destination

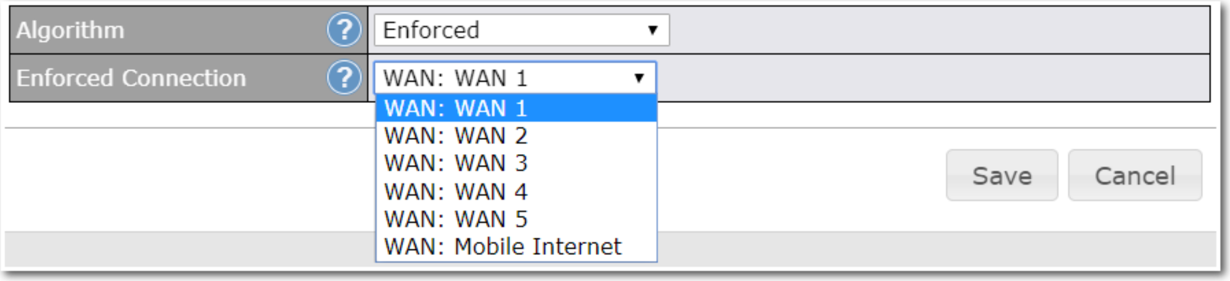
There are two persistent modes: **By Source** and **By Destination**.

By Source:	The same WAN connection will be used for traffic matching the rule and originating from the same machine, regardless of its destination. This option will provide the highest level of application compatibility.
By Destination:	The same WAN connection will be used for traffic matching the rule, originating from the same machine, and going to the same destination. This option can better distribute loads to WAN connections when there are only a few client machines.

The default mode is **By Source**. When there are multiple client requests, they can be distributed (persistently) to WAN connections with a weight. If you choose **Auto** in **Load Distribution**, the weights will be automatically adjusted according to each WAN's **Downstream Bandwidth** which is specified in the WAN settings page). If you choose **Custom**, you can customize the weight of each WAN manually by using the sliders.

Algorithm: Enforced

This setting specifies the WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Enforced**.

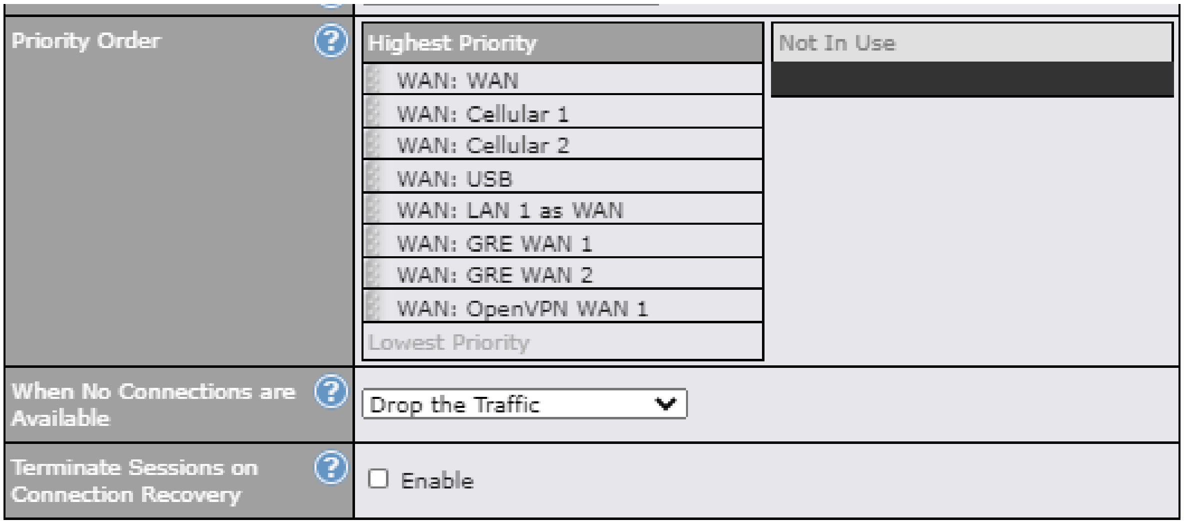


Algorithm	Enforced
Enforced Connection	WAN: WAN 1

Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection. Outbound traffic can also be enforced to go through a specified SpeedFusion^{TM} connection.

Algorithm: Priority

This setting specifies the priority of the WAN connections used to route the specified network service. The highest priority WAN connection available will always be used for routing the specified type of traffic. A lower priority WAN connection will be used only when all higher priority connections have become unavailable.



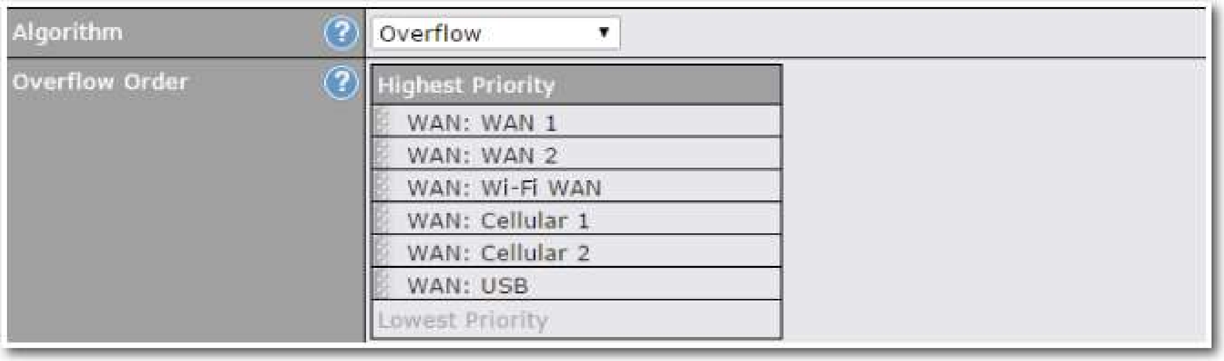
Priority Order	Highest Priority	Not In Use
	WAN: WAN	
	WAN: Cellular 1	
	WAN: Cellular 2	
	WAN: USB	
	WAN: LAN 1 as WAN	
	WAN: GRE WAN 1	
	WAN: GRE WAN 2	
	WAN: OpenVPN WAN 1	
	Lowest Priority	
When No Connections are Available	Drop the Traffic	
Terminate Sessions on Connection Recovery	☐ Enable	

Starting from Firmware 5.2, outbound traffic can be prioritized to go through SpeedFusion^{TM} connection(s). By default, VPN connections are not included in the priority list.

Tip
Configure multiple distribution rules to accommodate different kinds of services.

Algorithm: Overflow

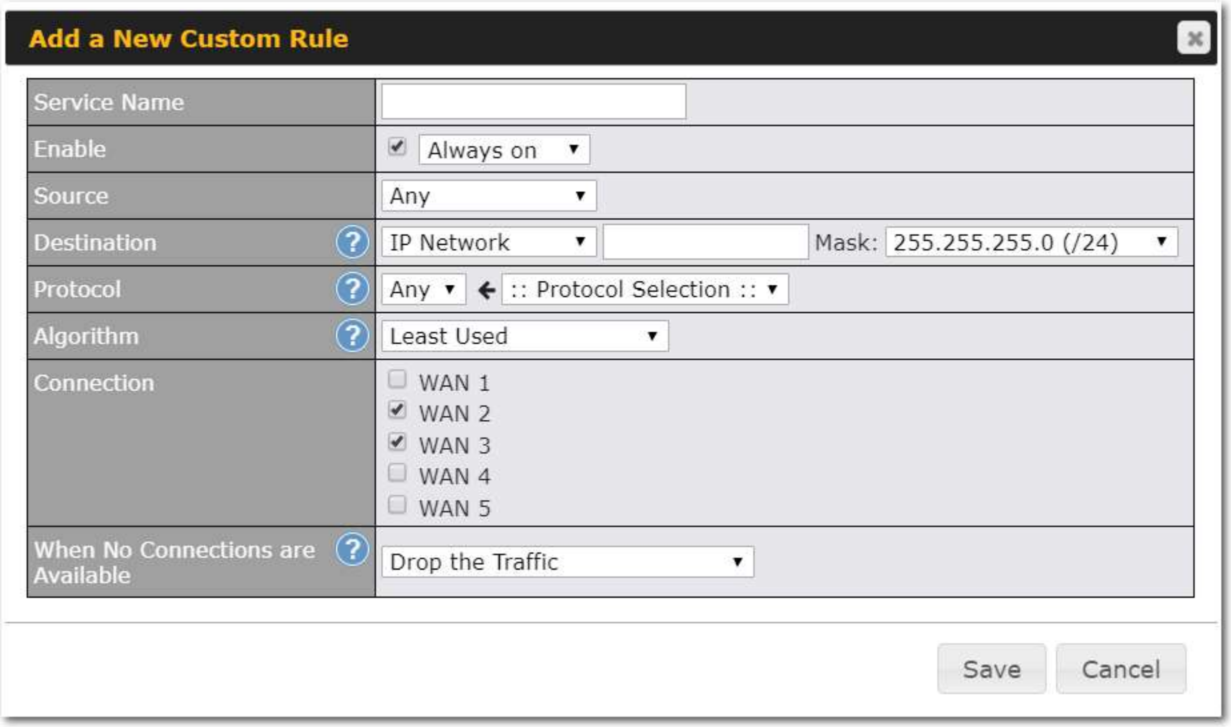
The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.



Algorithm	Overflow
Overflow Order	Highest Priority WAN: WAN 1 WAN: WAN 2 WAN: Wi-Fi WAN WAN: Cellular 1 WAN: Cellular 2 WAN: USB Lowest Priority

Drag and drop to specify the order of WAN connections to be used for routing traffic. Only the highest priority healthy connection that is not in full load will be used.

Algorithm: Least Used

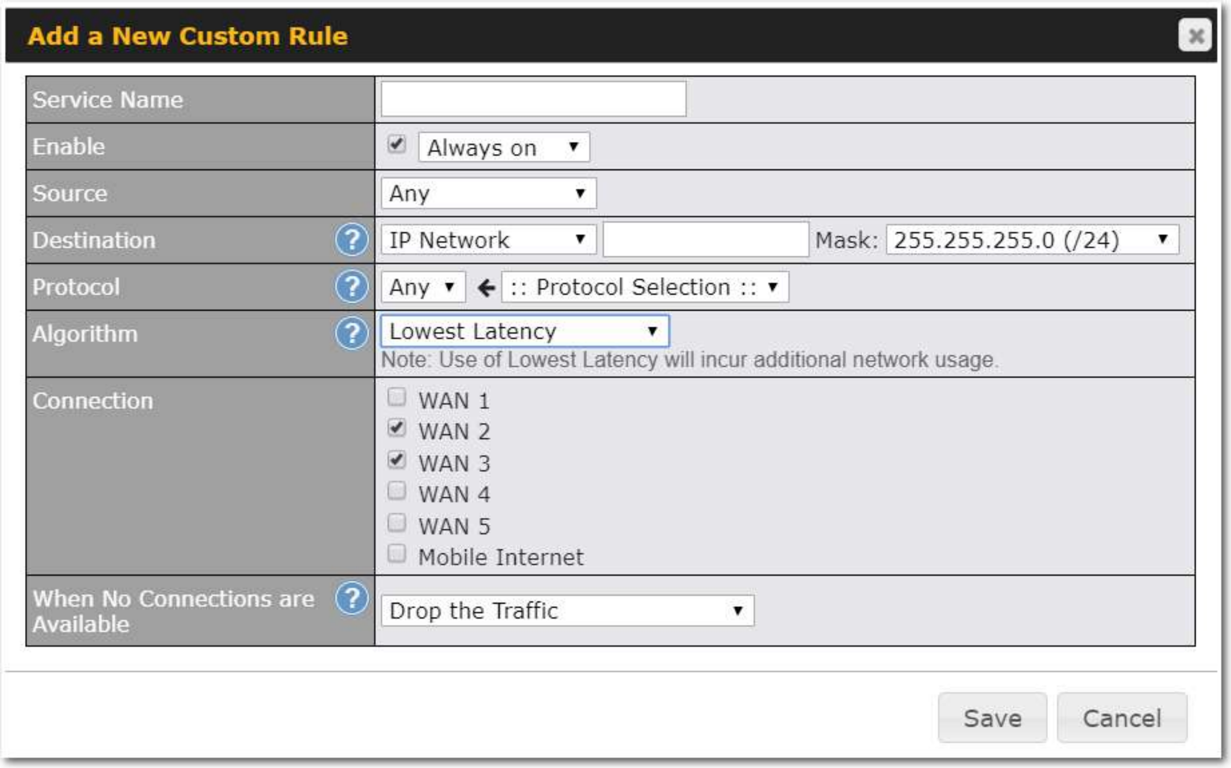


Add a New Custom Rule

Service Name	
Enable	☑ Always on
Source	Any
Destination	IP Network Mask: 255.255.255.0 (/24)
Protocol	Any ← :: Protocol Selection ::
Algorithm	Least Used
Connection	□ WAN 1 ☑ WAN 2 ☑ WAN 3 □ WAN 4 □ WAN 5
When No Connections are Available	Drop the Traffic

The traffic matching this rule will be routed through the healthy WAN connection that is selected in **Connection** and has the most available download bandwidth. The available download bandwidth of a WAN connection is calculated from the total download bandwidth specified on the WAN settings page and the current download usage. The available bandwidth and WAN selection is determined every time an IP session is made.

Algorithm: Lowest Latency



Add a New Custom Rule

Service Name	
Enable	☑ Always on
Source	Any
Destination	IP Network; Mask: 255.255.255.0 (/24)
Protocol	Any ← :: Protocol Selection ::
Algorithm	Lowest Latency Note: Use of Lowest Latency will incur additional network usage.
Connection	□ WAN 1 ☑ WAN 2 ☑ WAN 3 □ WAN 4 □ WAN 5 □ Mobile Internet
When No Connections are Available	Drop the Traffic

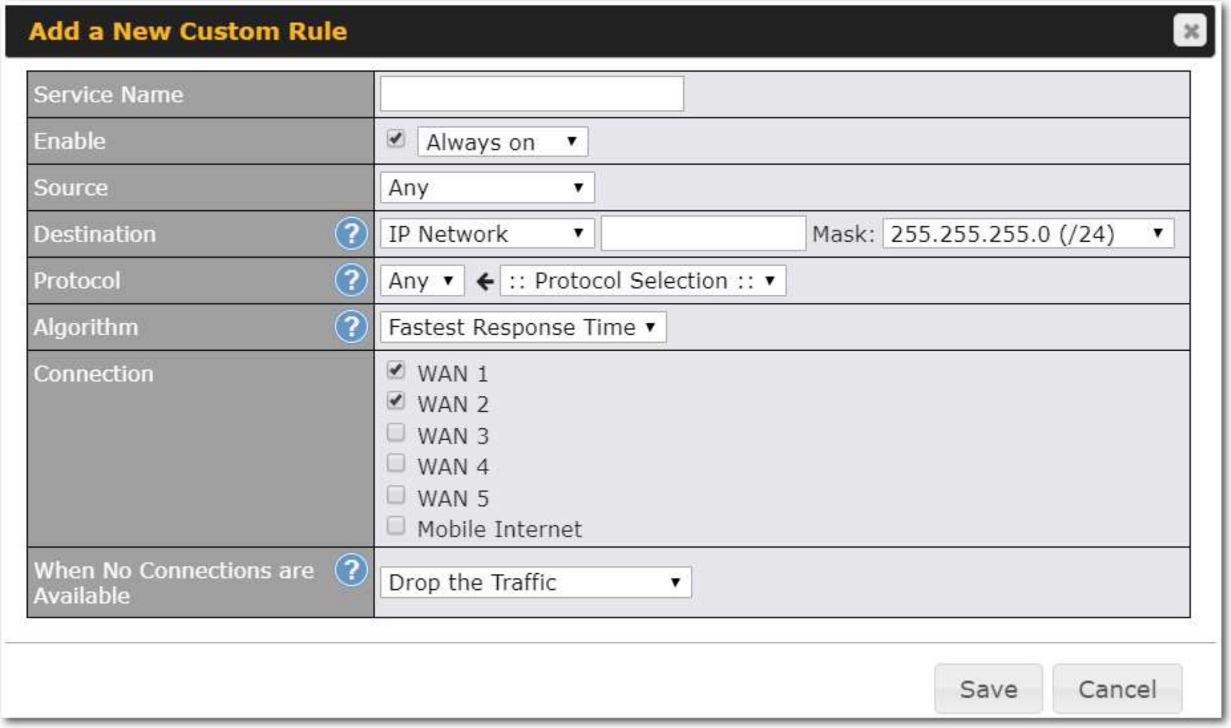
The traffic matching this rule will be routed through the healthy WAN connection that is selected in **Connection** and has the lowest latency. Latency checking packets are issued periodically to a nearby router of each WAN connection to determine its latency value. The latency of a WAN is the packet round trip time of the WAN connection. Additional network usage may be incurred as a result.

Tip

The roundtrip time of a 6M down/640k uplink can be higher than that of a 2M down/2M up link because the overall round trip time is lengthened by its slower upload bandwidth, despite its higher downlink speed. Therefore, this algorithm is good for two scenarios:

- All WAN connections are symmetric; or
- A latency sensitive application must be routed through the lowest latency WAN, regardless of the WAN's available bandwidth.

Algorithm : Fastest Response Time



Add a New Custom Rule

Service Name	
Enable	☑ Always on ▾
Source	Any ▾
Destination	IP Network ▾ Mask: 255.255.255.0 (/24) ▾
Protocol	Any ▾ ← :: Protocol Selection :: ▾
Algorithm	Fastest Response Time ▾
Connection	☑ WAN 1 ☑ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5 □ Mobile Internet
When No Connections are Available	Drop the Traffic ▾

The Fastest response Time algorithm works as follows:

When a network session is created, the first outgoing packet of that particular session is duplicated to all the available WANs.

When the first response is received from a remote server, any further traffic for this session will be routed over that particular WAN connection for the fastest possible response time.

If any slower responses are received on other connections afterwards, they will be discarded.

10.5 Inbound Access

Inbound access is also known as inbound port address translation. On a NAT WAN connection, all inbound traffic to the server behind the Peplink unit requires inbound access rules.

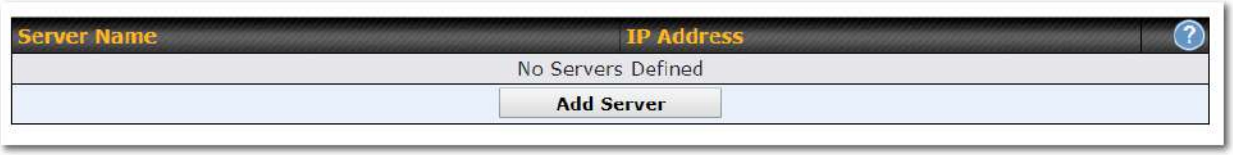
By the custom definition of servers and services for inbound access, Internet users can access the servers behind Peplink Balance. Advanced configurations allow inbound access to be distributed among multiple servers on the LAN.

Important Note
Inbound access applies only to WAN connections that operate in NAT mode. For WAN connections that operate in drop-in mode or IP forwarding, inbound traffic is forwarded to the LAN by default.

10.5.1 Servers

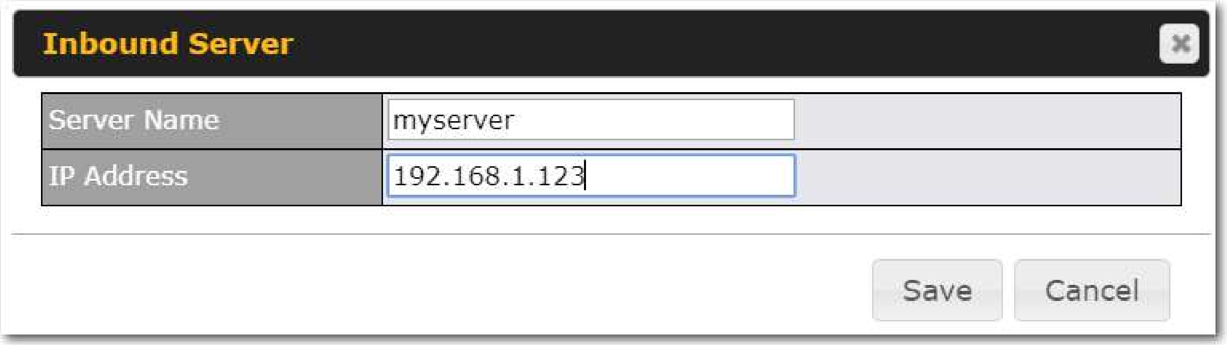
The settings to configure servers on the LAN are located at **Network>Inbound Access>Servers**.

Inbound connections from the Internet will be forwarded to the specified Inbound IP address(es) based on the protocol and port number. When more than one server is defined, requests will be distributed to the servers in the weight ratio specified for each server.



Server Name	IP Address
No Servers Defined	

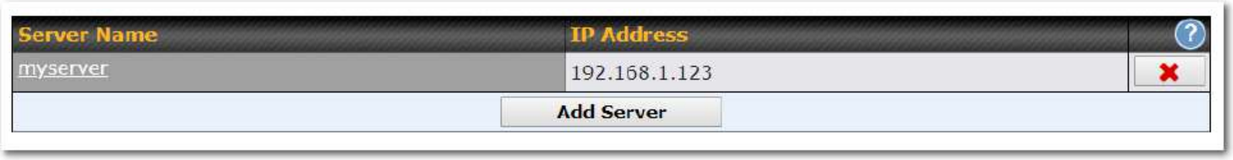
To define a new server, click **Add Server**, which displays the following screen:



Inbound Server

Server Name	myserver
IP Address	192.168.1.123

Enter a valid server name and its corresponding LAN IP address. Upon clicking **Save** after entering required information, the following screen appears.

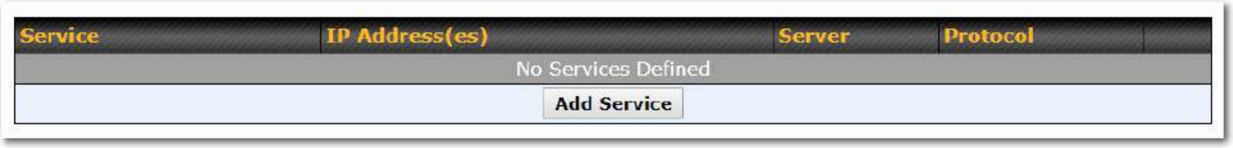


Server Name	IP Address	
myserver	192.168.1.123	✖
Add Server		

To define additional servers, click **Add Server** and repeat the above steps.

10.5.2 Services

Services are defined at **Network>Inbound Access>Services**.

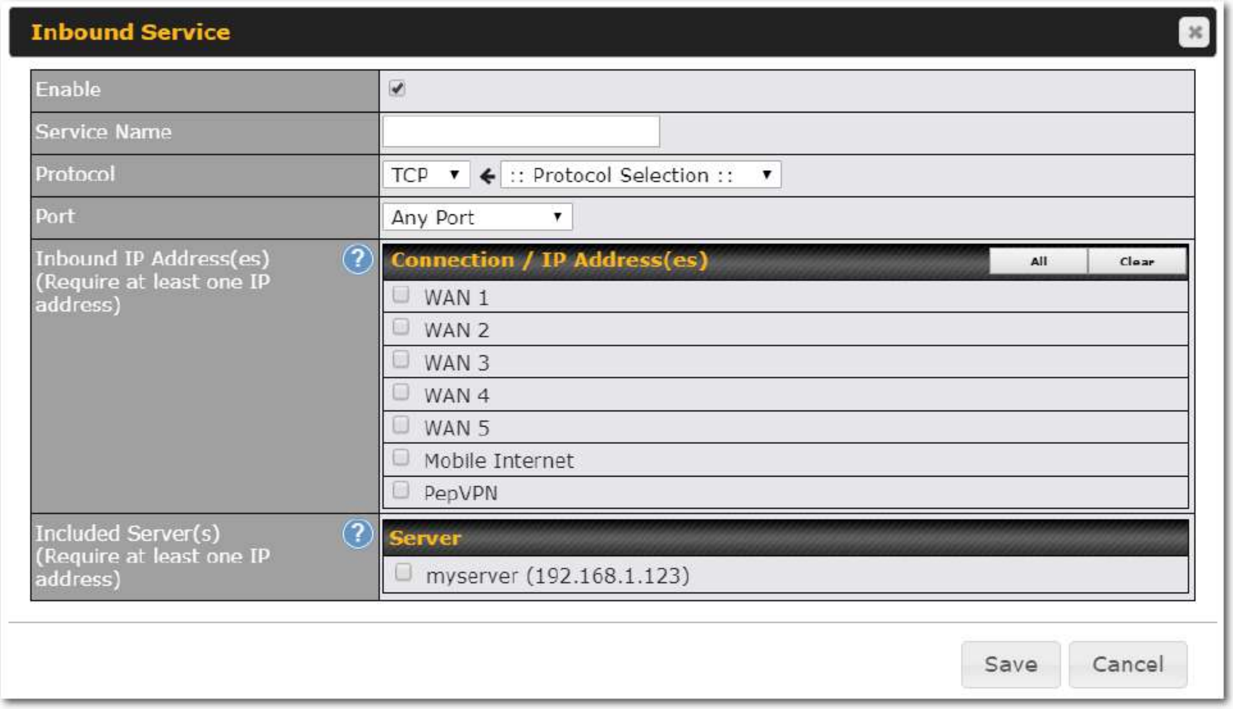


Service	IP Address(es)	Server	Protocol
No Services Defined			
Add Service			

Tip

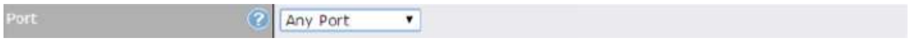
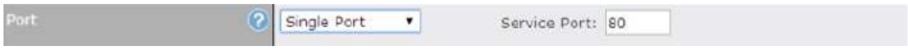
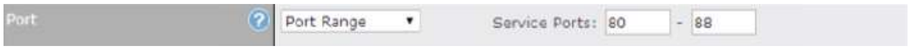
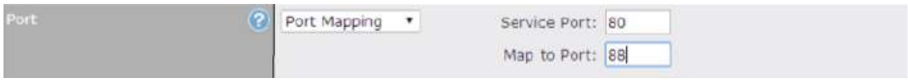
At least one server must be defined before services can be added.

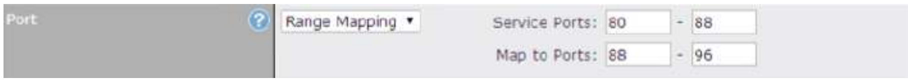
To define a new service, click the **Add Service** button, upon which the following menu appears:



Inbound Service

Enable	☑
Service Name	
Protocol	TCP ▾ ← :: Protocol Selection :: ▾
Port	Any Port ▾
Inbound IP Address(es) (Require at least one IP address)	**Connection / IP Address(es)** All Clear □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ WAN 5 □ Mobile Internet □ PepVPN
Included Server(s) (Require at least one IP address)	**Server** □ myserver (192.168.1.123)

Services Settings	
Enable	This setting specifies whether the inbound service rule takes effect. When **Yes** is selected, the inbound service rule takes effect. If the inbound traffic matches the specified IP protocol and port, action will be taken by the Peplink Balance based on the other parameters of the rule. When **No** is selected, the inbound service rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Only alphanumeric and the underscore "_" characters are valid.
IP Protocol	The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Inbound traffic that matches the specified **IP Protocol** and **Port**(s) will be forwarded to the LAN hosts specified by the **Servers** setting. Upon choosing a protocol, the **Protocol Selection Tool** drop-down menu can be used to automatically the port information of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and the port number will remain manually modifiable.
Port	The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners: **Any Port**, **Single Port**, **Port Range**, **Port Map**, and **Range Mapping**  Port: Any Port **Any Port**: all traffic that is received by the Peplink Balance via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, if I**P Protocol** is set to **TCP** and **Port** is set to **Any Port**, then all TCP traffic will be forwarded to the configured servers.  Port: Single Port Service Port: 80 **Single Port**: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, if I**P Protocol** is set to **TCP**, **Port** is set to **Single Port,** and **Service Port** is set to 80, then TCP traffic received on Port 80 will be forwarded to the configured servers via port 80.  Port: Port Range Service Ports: 80 - 88 **Port Range**: traffic that is received by the Peplink Balance via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, if **IP Protocol** is set to **TCP**, **Port** is set to **Port Range,** and **Service Port** set to 80-88, then TCP traffic received on ports 80 through 88 will be forwarded to the configured servers via the respective ports.  Port: Port Mapping Service Port: 80 Map to Port: 88 **Port Mapping**: traffic that is received by the Peplink Balance via the specified protocol at the specified port is forwarded via a different port to the servers specified by the Servers setting. For example, if **IP Protocol** is set to **TCP**, **Port** is set to **Port Mapping**, **Service Port** is set to 80, and **Map to Port** is set to 88, then TCP traffic on port 80 is forwarded to the configured servers via port 88. (Please see below for details on the **Servers** setting.)

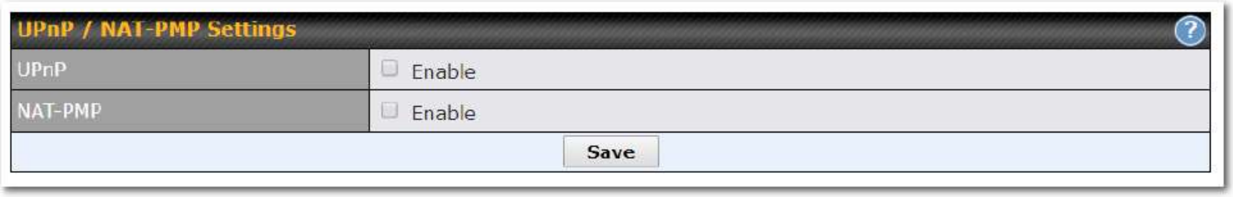
	 Port Range Mapping ▾ Service Ports: 80 - 88 Map to Ports: 88 - 96 **Range Mapping**: traffic that is received by Peplink Balance via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.
Inbound IP Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.
Included Server(s)	This setting specifies the LAN servers that handle requests for the service, and the relative weight values. The amount of traffic that is distributed to a server is proportional to the weight value assigned to the server relative to the total weight. Example: With the following weight settings on a Peplink Balance: ● demo_server_1: 10 ● demo_server_2: 5 The total weight is 15 = (10 + 5) Matching traffic distributed to demo_server_1:67% = (10 / 15) x 100% Matching traffic distributed to demo_server_2:33% = (5 / 15) x 100%

UPnP / NAT-PMP Settings

UPnP and NAT-PMP are network protocols which allow a computer connected to the LAN port to automatically configure the router to allow parties on the WAN port to connect to itself. That way, the process of inbound port forwarding becomes automated.

When a computer creates a rule using these protocols, the specified TCP/UDP port of all WAN connections' default IP address will be forwarded.

Check the corresponding box(es) to enable UPnP and/or NAT-PMP. Enable these features only if you trust the computers connected to the LAN ports.



UPnP / NAT-PMP Settings

UPnP	□ Enable
NAT-PMP	□ Enable

When the options are enabled, a table listing all the forwarded ports under these two protocols can be found at **Network > Services > UPnP / NAT-PMP**.

10.5.3 DNS Settings

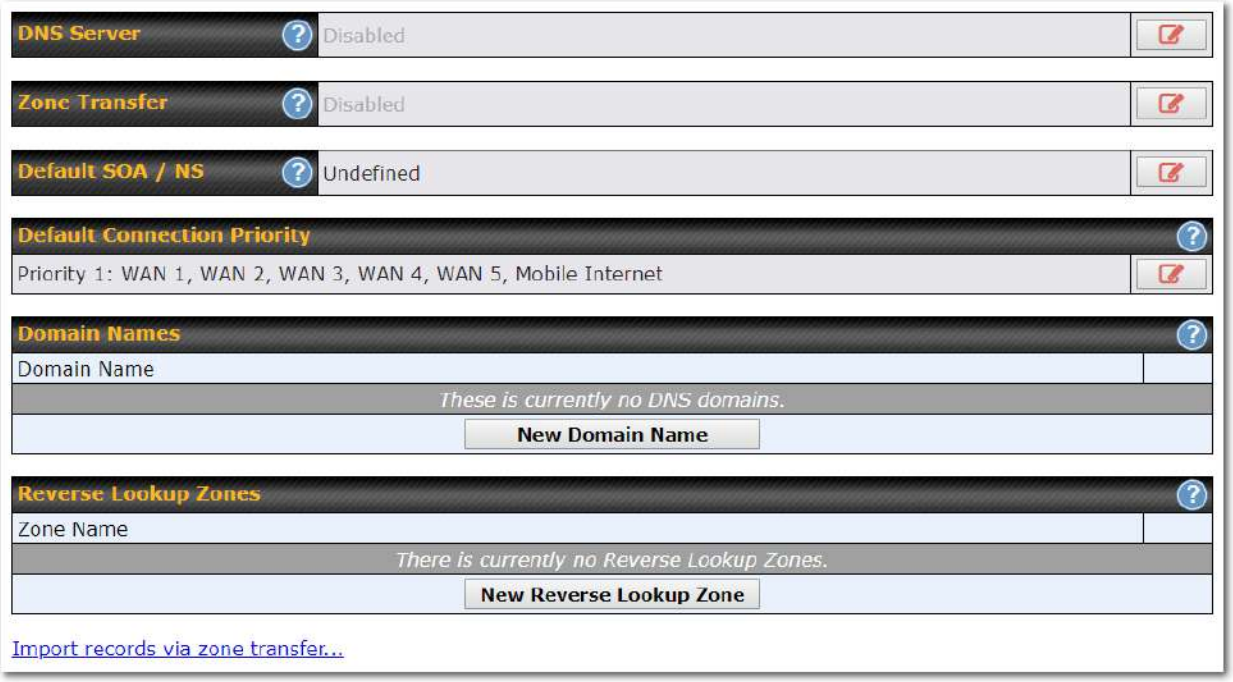
The built-in DNS server functionality of the Peplink Balance facilitates inbound load balancing. With this functionality, NS/SOA DNS records for a domain name can be delegated to the Internet IP address(es) of the Peplink Balance. Upon receiving a DNS query, the Peplink Balance can return (as an "A" record) the IP address for the domain name on the most appropriate healthy WAN connection. It can also act as a generic DNS server for hosting "A", "CNAME", "MX", "TXT" and "NS" records.

The settings for defining the DNS records to be hosted by the Peplink Balance are located at **Network > Inbound Access > DNS Settings**.

Note: DNS names may only contain alphanumeric characters (A-Z and 0-9), hyphens (-), and periods (.). The period is only allowed when it is used to delimit the components of domain style names.

For more information, see the following websites:

- rfc952
- rfc1123



DNS Server: Disabled

Zone Transfer: Disabled

Default SOA / NS: Undefined

Default Connection Priority

Priority 1: WAN 1, WAN 2, WAN 3, WAN 4, WAN 5, Mobile Internet

Domain Names

Domain Name

These is currently no DNS domains.

New Domain Name

Reverse Lookup Zones

Zone Name

There is currently no Reverse Lookup Zones.

New Reverse Lookup Zone

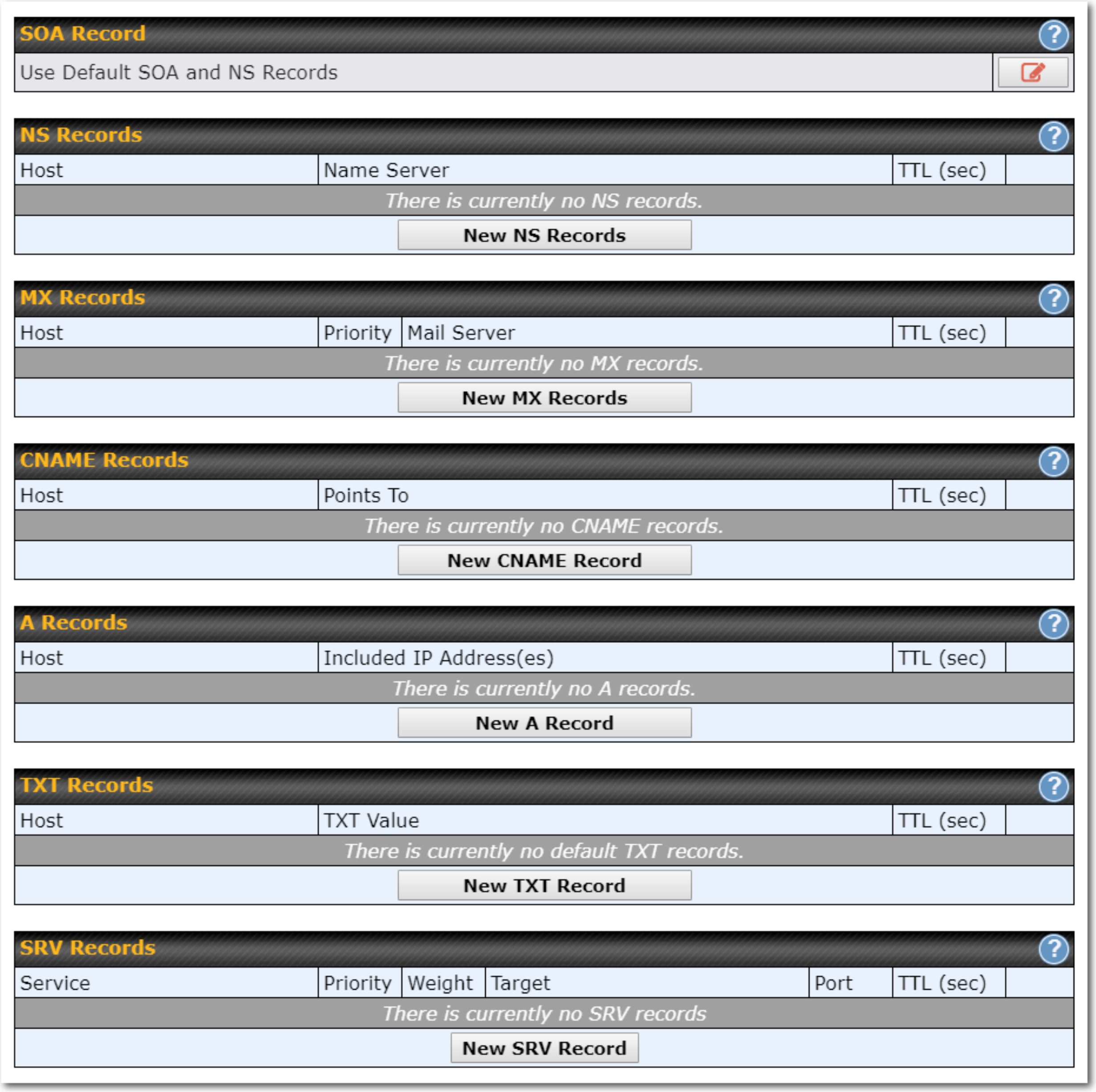
Import records via zone transfer...

	DNS Settings
DNS Servers	This setting specifies the WAN IP addresses on which the DNS server of the Peplink Balance should listen. If no addresses are selected, the inbound link load balancing feature will be disabled and the Peplink Balance will not respond to DNS requests.

	To specify and/or modify the IP addresses on which the DNS server should listen, click the button that corresponds to **DNS Server**, and a selection screen will be displayed: To specify the Internet IP addresses on which the DNS server should listen, select the desired WAN connection then select the desired associated IP addresses. (Multiple items in the list can be selected by holding CTRL and clicking on the items.) Click **Save** to save the settings when configuration is complete.
Zone Transfer	This setting specifies the IP address(es) of the secondary DNS server(s)authorized to retrieve zone records from the DNS server of the Peplink Balance. The zone transfer server of the Peplink Balance listens on TCP port 53. The Peplink Balance serves both the clients that are accessing from the specified IP addresses, and the clients that are accessing its LAN interface.
Routing Control by Subnet Database	When this function is enabled, the system will check to see if an incoming DNS client is within any WAN's ISP subnet. Only the matched WAN(s)'s IP addresses will be returned. Note that this feature is available only when a subnet database has been defined.
Default SOA / NS	Click the button to define a default SOA / NS record for all domain names. When defining a default SOA record, **Name Server IP Address** is optional. If left blank, the Address (A) record for the same server should be defined manually in each domain. For defining default NS records, the host *[domain]* indicates that this record is for the domain name itself without a sub-domain prefix. To add a secondary NS server, just create a second NS record with the **Host** field left empty. When the entered name server is a fully qualified domain name (FQDN), the **IP Address** field will be disabled.
Default Connection Priority	**Default Connection Priority** defines the default priority group of each WAN connection in resolving A records. It applies to Address (A) records which have the **Connection Priority** set to **Default**. Please refer to **Section 17.3.9** for details. The WAN connection(s) with the highest priority (smallest number) will be chosen. Those with lower priorities will not be chosen in resolving A records unless the higher priority ones become unavailable. To specify the primary and backup connections, click the button that corresponds to **Default Connection Priority**. A selection screen will appear. Each WAN connection is associated with a priority number. Click **Save** to save the settings when configuration is complete.
Domain name	This section shows a list of domain names to be hosted by the Peplink Balance. Each domain can have its “NS”, “MX” and “TXT” records, and its sub-domains’ “A” and “CNAME” records. Add a new record by clicking the **New Domain Name** button. Click on a domain name to edit. Press the red X to remove a domain name.

New Domain Name

Upon clicking the New Domain Name button, and the following screen will appear:



SOA Record

Use Default SOA and NS Records	

NS Records

Host	Name Server	TTL (sec)	
There is currently no NS records.			
New NS Records			

MX Records

Host	Priority	Mail Server	TTL (sec)	
There is currently no MX records.				
New MX Records				

CNAME Records

Host	Points To	TTL (sec)	
There is currently no CNAME records.			
New CNAME Record			

A Records

Host	Included IP Address(es)	TTL (sec)	
There is currently no A records.			
New A Record			

TXT Records

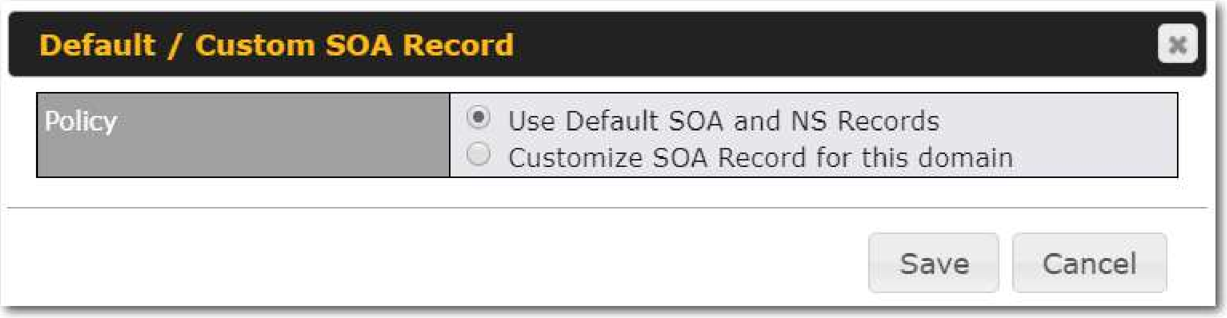
Host	TXT Value	TTL (sec)	
There is currently no default TXT records.			
New TXT Record			

SRV Records

Service	Priority	Weight	Target	Port	TTL (sec)	
There is currently no SRV records						
New SRV Record						

This page is for defining the domain's SOA, NS, MX, CNAME, A, TXT, and SRV records. Seven tables are presented in this page for defining the five types of records.

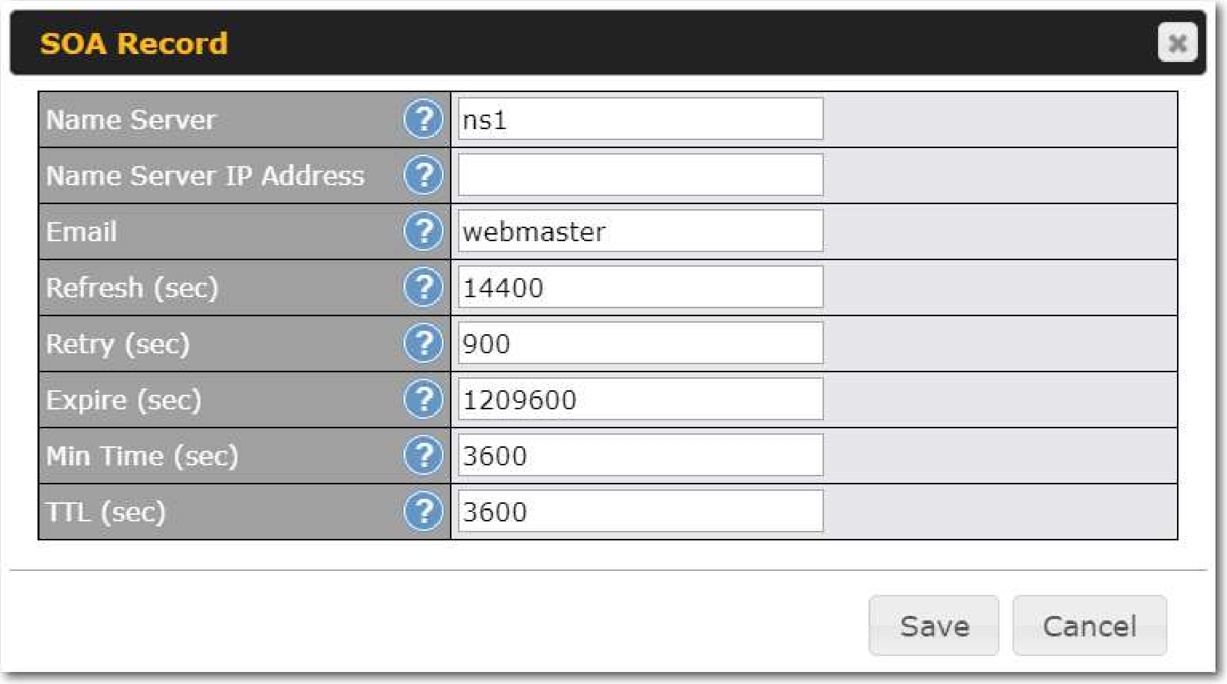
SOA Records



Default / Custom SOA Record

Policy	● Use Default SOA and NS Records ○ Customize SOA Record for this domain

Click on the ✎ icon to choose whether to use the pre-defined default SOA record and NS records. If the option **Use Default SOA and NS Records** is selected, any changes made in the default SOA/NS records will be applied to this domain automatically. Otherwise, select the option **Customize SOA Record** for this domain to customize this domain's SOA and NS records.



SOA Record

Name Server	ns1
Name Server IP Address	
Email	webmaster
Refresh (sec)	14400
Retry (sec)	900
Expire (sec)	1209600
Min Time (sec)	3600
TTL (sec)	3600

This table displays the current SOA record. When the option **Customize SOA Record for this domain** is selected, you can click the link **Click here to define SOA record** to create or click on the **Name Server** field to edit the SOA record.

In the SOA record, you have to fill out the fields **Name Server**, **Name Server IP Address**, **Email**, **Refresh**, **Retry**, **Expire**, **Min Time**, and **TTL**.

Default values are set for SOA and NS records,

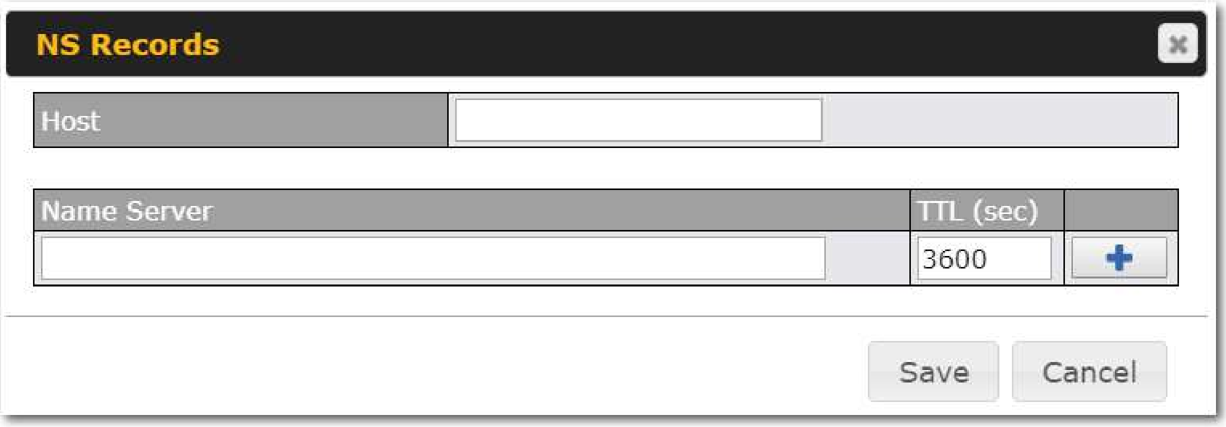
- **Name Server IP Address:** This is the IP address of the authoritative name server. An entry in this field is optional. If the Balance is the authoritative name server of the domain, this field's value should be the WAN connection's name server IP address that is registered in the DNS registrar. If this field is entered, a corresponding A record for the name server will be created automatically. If it is left blank, the A record for the name server must be created manually.

- **E-mail**: Defines the e-mail address of the person responsible for this zone. Note: format should be *mailbox-name.domain.com*, e.g., *hostmaster.example.com*.
- **Refresh**: Indicates the length of time (in seconds) when the slave will try to refresh the zone from the master.
- **Retry**: Defines the duration (in seconds) between retries if the slave (secondary) fails to contact the master and the refresh (above) has expired.
- **Expire**: Indicates the time (in seconds) when the zone data is no longer authoritative. This option applies to slave DNS servers only.
- **Min Time**: Is the negative caching time which defines the time (in seconds) after an error record is cached.
- **TTL (Time-to-Live)**: Defines the duration (in seconds) that the record may be cached.

NS Records

The **NS Records** table shows the NS servers and TTL that correspond to the domain. The NS record of the name server defined in the SOA record is automatically added here.

To add a new NS record, click the **New NS Records** button in the **NS Records** box. Then the table will expand to look like the following:



NS Records

Host	

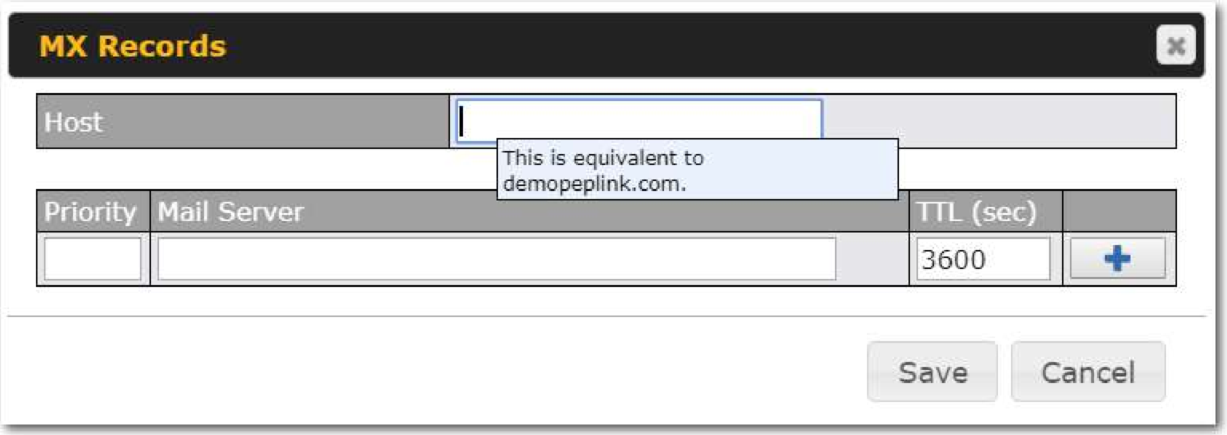
Name Server	TTL (sec)	
	3600	+

When creating an NS record for the domain itself (not a sub-domain), the **Host** field should be left blank.

Enter a name server host name and its IP address into the corresponding boxes. The host name can be a non-FQDN (fully qualified domain name). Please be sure that a corresponding A record is created. Click the + button on the right to finish and to add other name servers. Click the **Save** button to save your changes.

MX Records

The **MX Record** table shows the domain's MX records. To add a new MX record, click the **New MX Records** button in the **MX Records** box. Then the table will expand to look like the following:



Host	

This is equivalent to demopeplink.com.

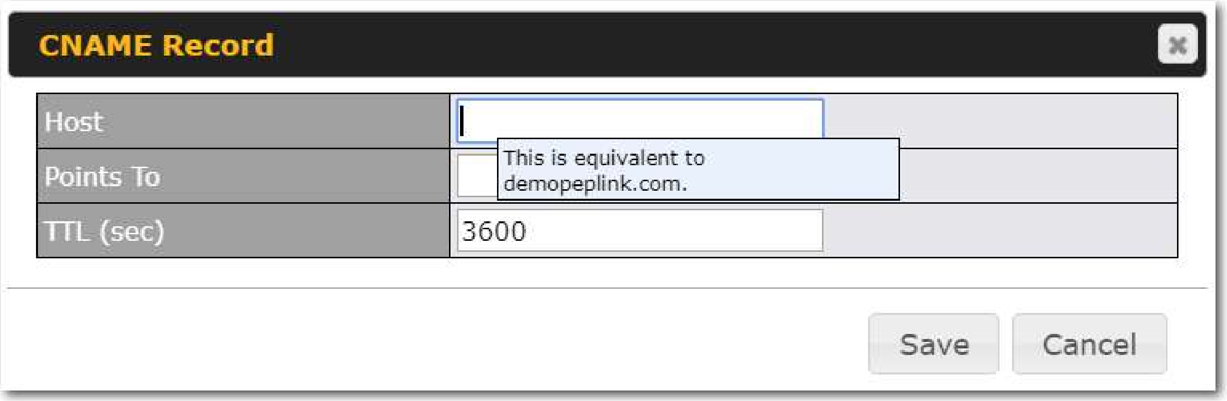
Priority	Mail Server	TTL (sec)	
		3600	+

When creating an MX record for the domain itself (not a sub-domain), the **Host** field should be left blank.

For each record, **Priority** *and* **Mail Server** name must be entered. **Priority** typically ranges from 10 to 100. Smaller numbers have a higher priority. After finishing adding MX records, click the **Save** button.

CNAME Records

The **CNAME Record** table shows the domain's CNAME records. To add a new CNAME record, click the **New CNAME Records** button in the **CNAME Record** box. Then the table will expand to look like the following:



Host	
Points To	
TTL (sec)	3600

This is equivalent to demopeplink.com.

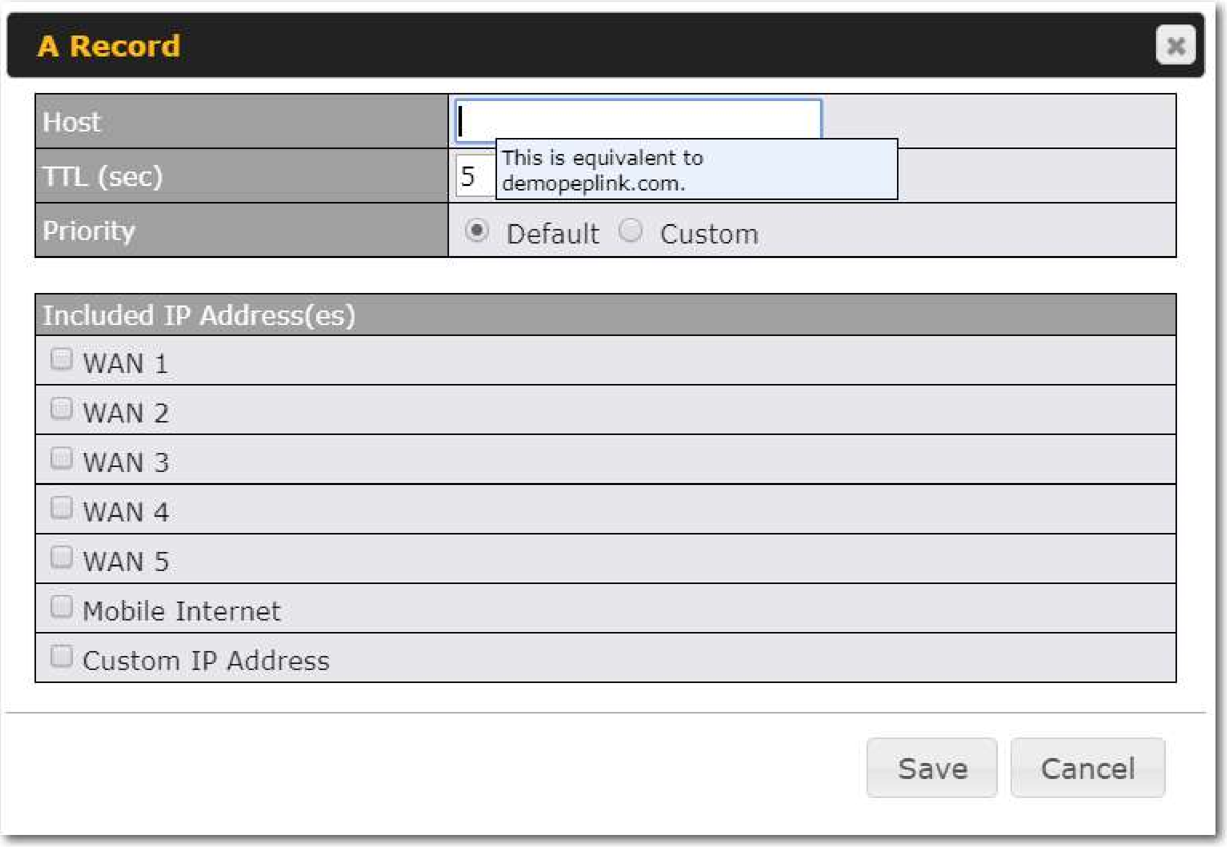
When creating a CNAME record for the domain itself (not a sub-domain), the **Host** field should be left blank.

The wildcard character "*"is supported in the **Host** field. The reference of ".*domain.name*" will be returned for every name ending with ".*domain.name*" except names that have their own records.

The **TTL** field tells the time to live of the record in external DNS caches.

A Records

This table shows the A records of the domain name. To add an A record, click the **New A Record** button. The following screen will appear:



A Record

Host	
TTL (sec)	5
Priority	● Default ○ Custom

This is equivalent to demopeplink.com.

Included IP Address(es)
□ WAN 1
□ WAN 2
□ WAN 3
□ WAN 4
□ WAN 5
□ Mobile Internet
□ Custom IP Address

A record may be automatically added for the SOA records with a name server IP address provided.

A Record	
Host Name	This field specifies the A record of this sub-domain to be served by the Peplink Balance. The wildcard character "*" is supported. The IP addresses of "*.*domain.name*" will be returned for every name ending with *".domain.name"* except names that have their own records.
TTL	This setting specifies the time to live of this record in external DNS caches. In order to reflect any dynamic changes on the IP addresses in case of link failure and recovery, this value should be set to a smaller value, e.g., 5 secs, 60 secs, etc.
Priority	This option specifies the priority of different connections. Select the **Default** option to apply the **Default Connection Priority** (refer to the table

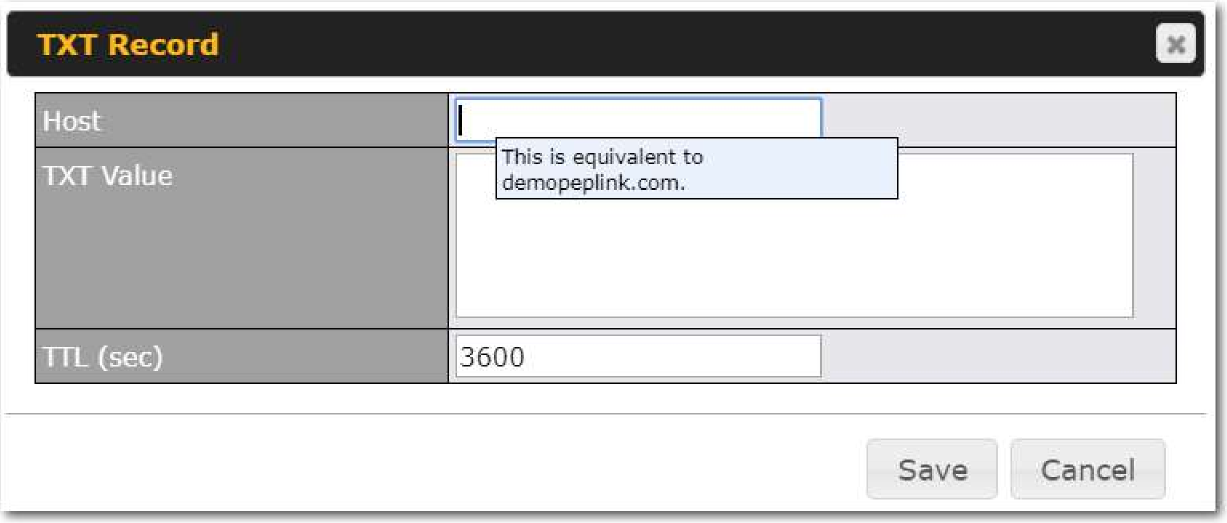
	shown on the main DNS settings page) to an A record. To customize priorities, choose the **Custom** option and a priority selection table will be shown at the bottom.
Included IP Address(es)	This setting specifies lists of WAN-specific Internet IP addresses that are candidates to be returned when the Peplink Balance responds to DNS queries for the domain name specified by **Host Name**. The IP addresses listed in each box as **default** are the Internet IP addresses associated with each of the WAN connections. Static IP addresses that are not associated with any WAN can be entered into the **Custom IP** list. A PTR record is also created for each custom IP. For WAN connections that operate under drop-in mode, there may be other routable IP addresses in addition to the default IP address. Therefore, the Peplink Balance allows custom Internet IP addresses to be added manually via filling the text box on the right-hand side and clicking the ⊞ button. Only the checked IP addresses in the lists are candidates to be returned when responding to a DNS query. If a WAN connection is down, the corresponding set of IP addresses will not be returned. However, the IP addresses in the **Custom IP Address** field will always be returned. If the **Connection Priority** field is set to **Custom**, you can also specify the usage priority of each WAN connection. Only selected IP address(es) of available connection(s) with the highest priority, and custom IP addresses will be returned. By default, **Connection Priority** is set to **Default**.

PTR Records

PTR records are created along with A records pointing to custom IPs. For example, if you created an A record *www.mydomain.com* pointing to *11.22.33.44*, then a PTR record *44.33.22.11.in-addr.arpa* pointing to *www.mydomain.com* will also be created. When there are multiple host names pointing to the same IP address, only one PTR record for the IP address will be created. In order for PTR records to function, you also need to create NS records. For example, if the IP address range *11.22.33.0* to *11.22.33.255* is delegated to the DNS server on the Peplink Balance, you will also have to create a domain *33.22.11.in-addr.arpa* and have its NS records pointing to your DNS server's (the Peplink Balance's) public IP addresses. With the above records created, the PTR record creation is complete.

TXT Records

This table shows the TXT record of the domain name.



TXT Record

Host	
TXT Value	
TTL (sec)	3600

This is equivalent to demopeplink.com.

To add a new TXT record, click the **New TXT Record** button in the **TXT Records** box. Click the **Edit** button to edit the record. The time-to-live value and the TXT record's value can be entered. Click the **Save** button to finish.

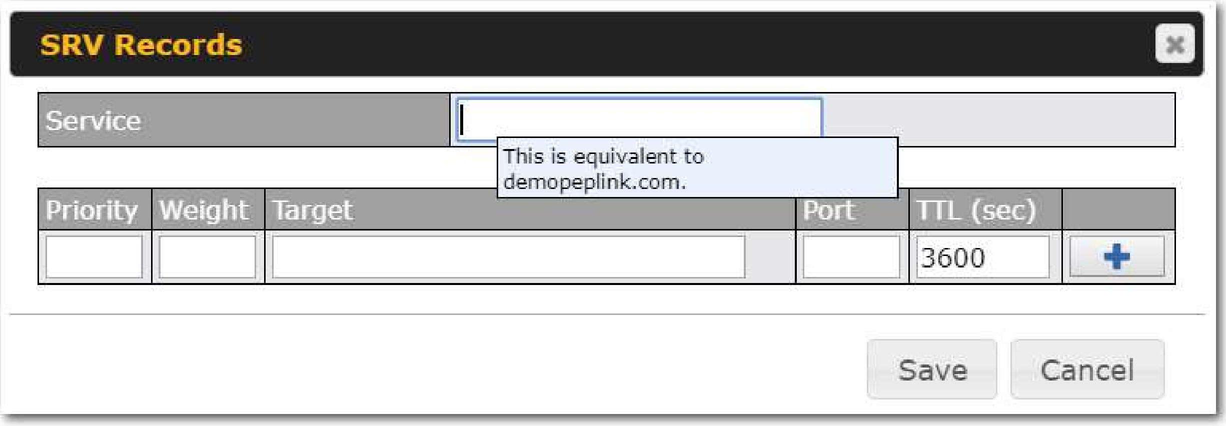
When creating a TXT record for the domain itself (not a sub-domain), the **Host** field should be left blank.

The maximum size of the TXT Value is 255 bytes.

After editing the five types of records, you can leave the page by simply going to another section of the web admin interface.

SRV Records

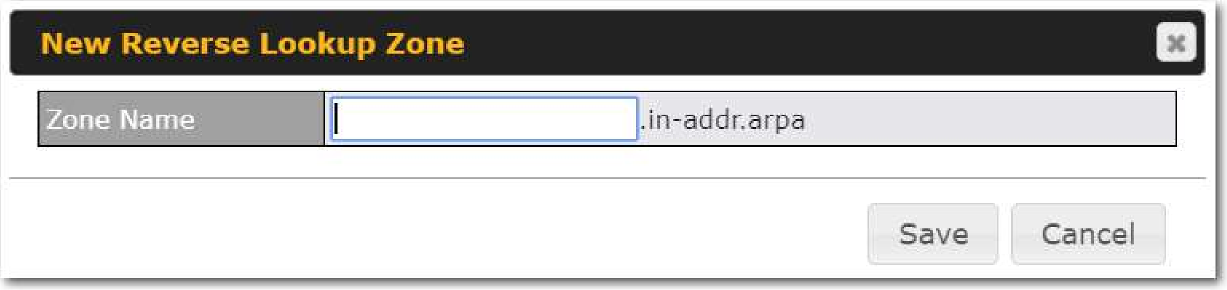
To add a new SRV record, click the **New SRV Record** button in the **SRV Records** box.



- **Service:** The symbolic name of the desired service.
- **Priority**: Indicates the priority of the target; the smaller the value, the higher the priority.
- **Weight**: A relative weight for records with the same priority.
- **Target**: The canonical hostname of the machine providing the service.
- **Port**: Enter the TCP or UDP port number on which the service is to be found.

Reverse Lookup Zones

Reverse lookup zones can be configured in **Network>Inbound Access>DNS Settings**.



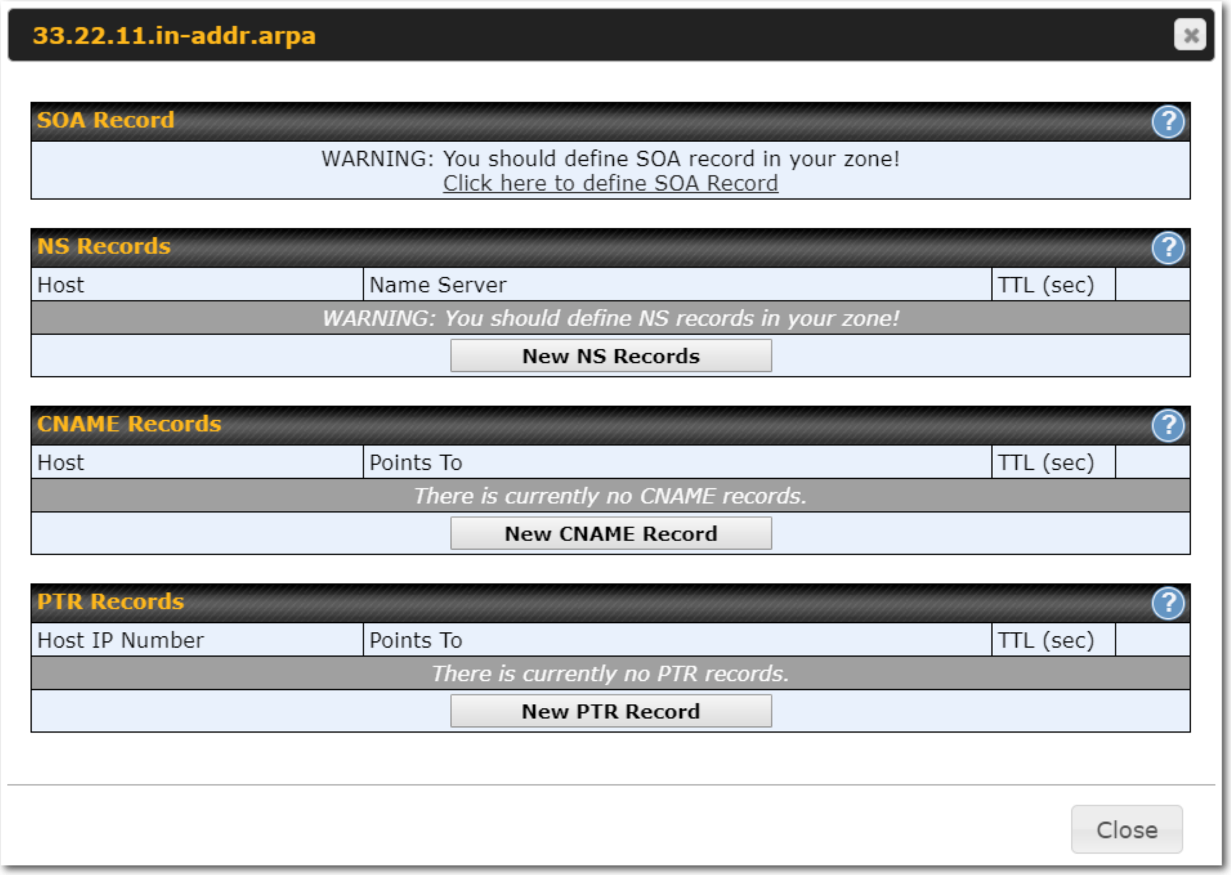
Reverse lookup refers to performing a DNS query to find one or more DNS names associated with a given IP address.

The DNS stores IP addresses in the form of specially formatted names as pointer (PTR) records using special domains/zones. The zone is *in-addr.arpa*.

To enable DNS clients to perform a reverse lookup for a host, perform two steps:

- Create a reverse lookup zone that corresponds to the subnet network address of the host.
  In the reverse lookup zone, add a pointer (PTR) resource record that maps the host IP address to the host name.
- Click the **New Reverse Lookup Zone** button and enter a reverse lookup zone name. If

you are delegated the subnet *11.22.33.0/24*, the **Zone Name** should be *33.22.11.in-arpa.add*r. PTR records for *11.22.33.1, 11.22.33.2, ... 11.22.33.254* should be defined in this zone where the host IP numbers are *1, 2, ... 254*, respectively.



33.22.11.in-addr.arpa

SOA Record

WARNING: You should define SOA record in your zone!
Click here to define SOA Record

NS Records

Host	Name Server	TTL (sec)	

WARNING: You should define NS records in your zone!

CNAME Records

Host	Points To	TTL (sec)	

There is currently no CNAME records.

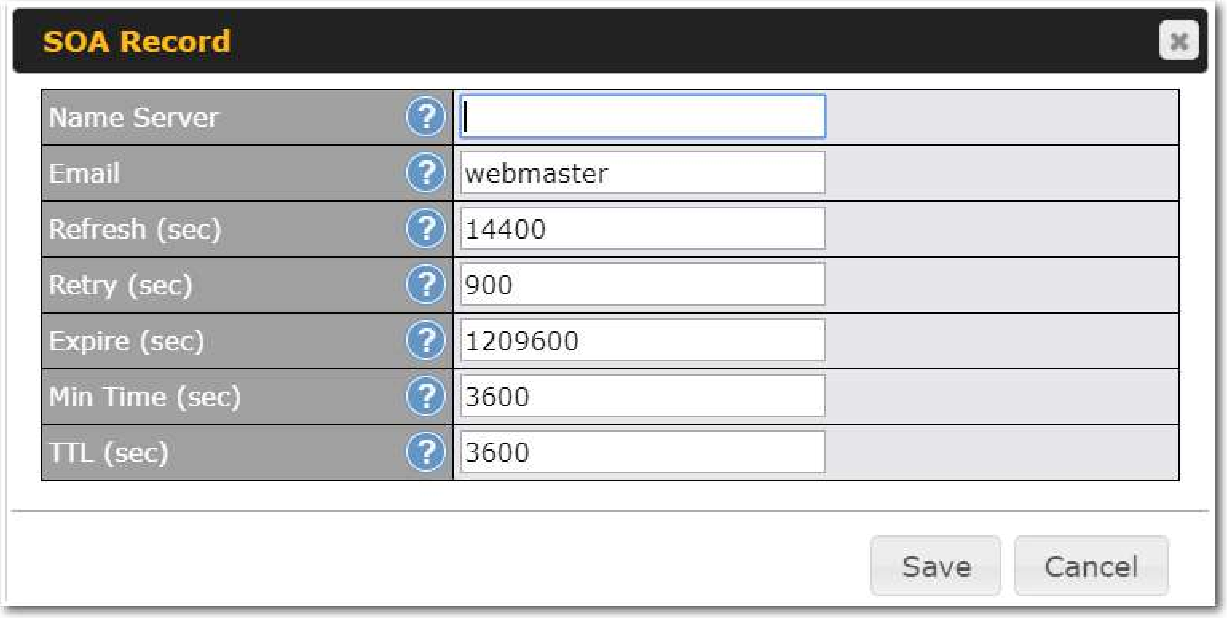
PTR Records

Host IP Number	Points To	TTL (sec)	

There is currently no PTR records.

SOA Record

You can click the link **Click here to define SOA record** to create or click on the **Name Server** field to edit the SOA record.



SOA Record

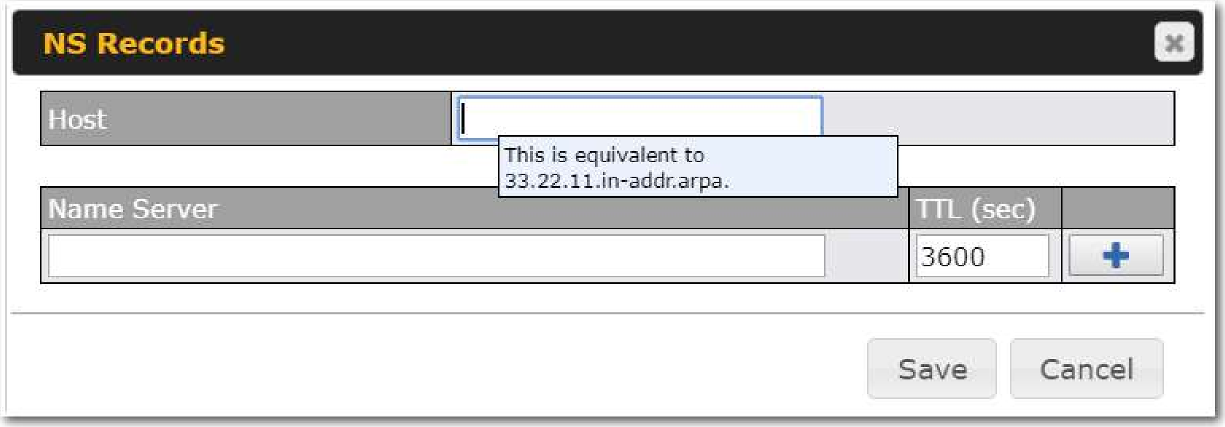
Name Server	
Email	webmaster
Refresh (sec)	14400
Retry (sec)	900
Expire (sec)	1209600
Min Time (sec)	3600
TTL (sec)	3600

Name Server: Enter the NS record's FQDN server name here.

For example:
"ns1.mydomain.com" (equivalent to "www.1stdomain.com.")
"ns2.mydomain.com."

Email, Refresh, Retry, Expire, Min Time, and TTL are entered in the same way as in the forward zone. Please refer to **Section 17.3.5** for details.

NS Records



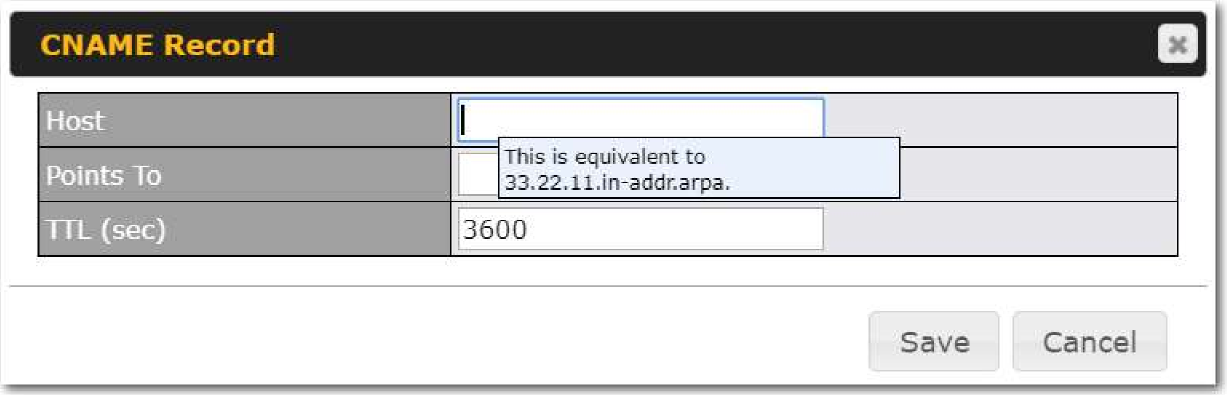
This is equivalent to 33.22.11.in-addr.arpa.

TTL (sec): 3600

The NS record of the name server defined in the SOA record is automatically added here. To create a new NS record, click the **New NS Records** button.

When creating an NS record for the *reverse lookup zone* itself (not a sub-domain or dedicated zone), the **Host** field should be left blank. **Name Server** must be a FQDN.

CNAME Records



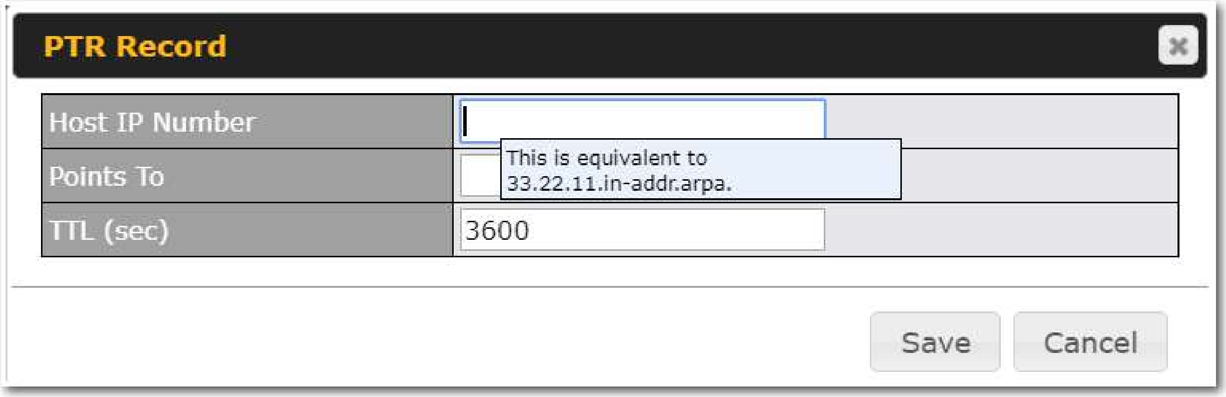
This is equivalent to 33.22.11.in-addr.arpa.

TTL (sec): 3600

To create a new CNAME record, click the **New CNAME Record** button.

CNAME records are typically used for defining classless reverse lookup zones. Subnetted reverse lookup zones are further described in RFC 2317, "Classless IN-ADDR.ARPA delegation."

PTR Records



PTR Record

Host IP Number	
Points To	
TTL (sec)	3600

This is equivalent to 33.22.11.in-addr.arpa.

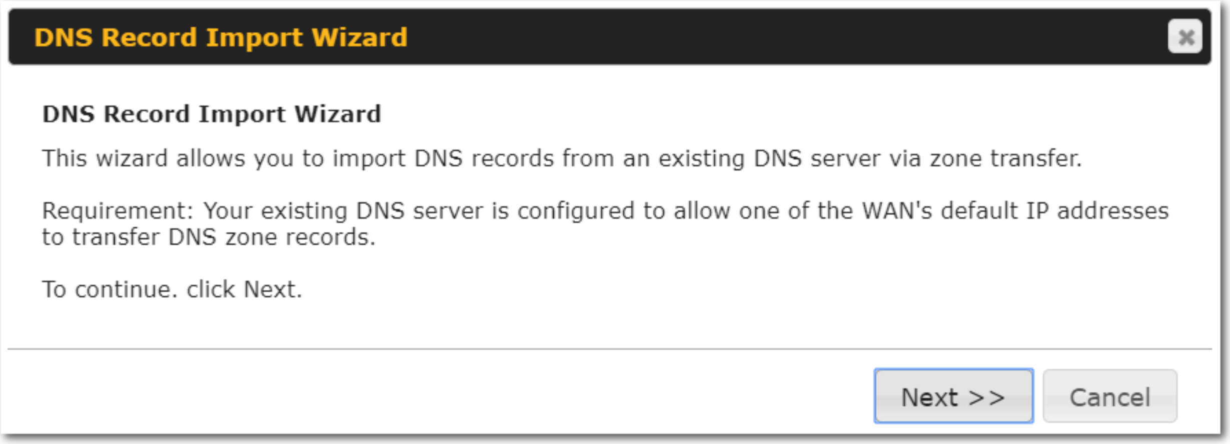
To create a new PTR record, click the **New PTR Record** button.

For **Host IP Number** field, enter the last integer in the IP address of a PTR record. For example. for the IP address *11.22.33.44*, where the reverse lookup zone is *33.22.11.in-arpa.addr*, the **Host IP Number** should be *44*.

The **Points To** field defines the host name which the PTR record should be pointed to. It must be a FQDN.

DNS Record Import Wizard

At the bottom of the DNS settings page, the link **Import records via zone transfer…**is used to import DNS record using an import wizard.



DNS Record Import Wizard

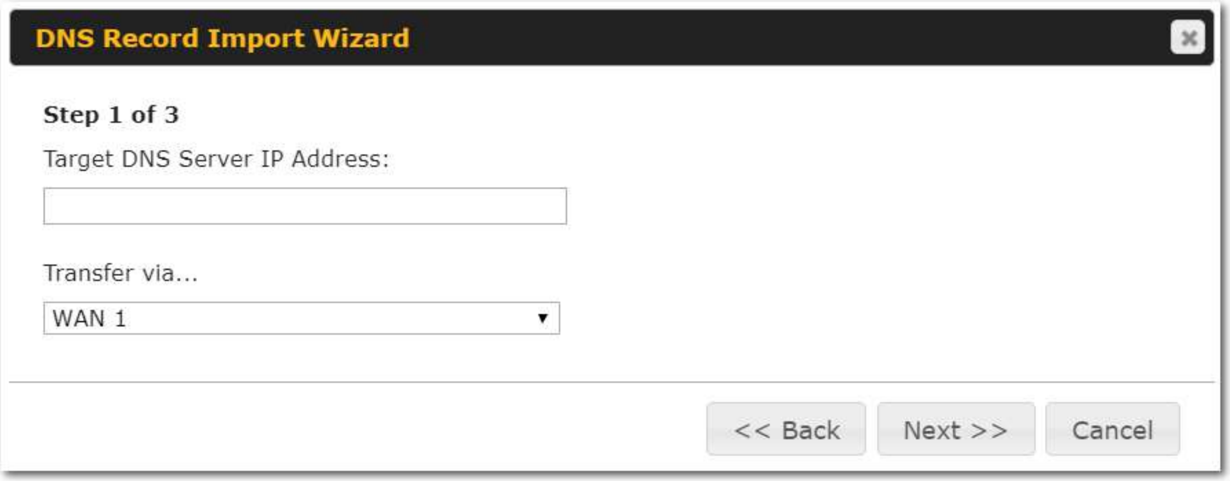
DNS Record Import Wizard

This wizard allows you to import DNS records from an existing DNS server via zone transfer.

Requirement: Your existing DNS server is configured to allow one of the WAN's default IP addresses to transfer DNS zone records.

To continue. click Next.

- Select **Next >>** to continue.



DNS Record Import Wizard

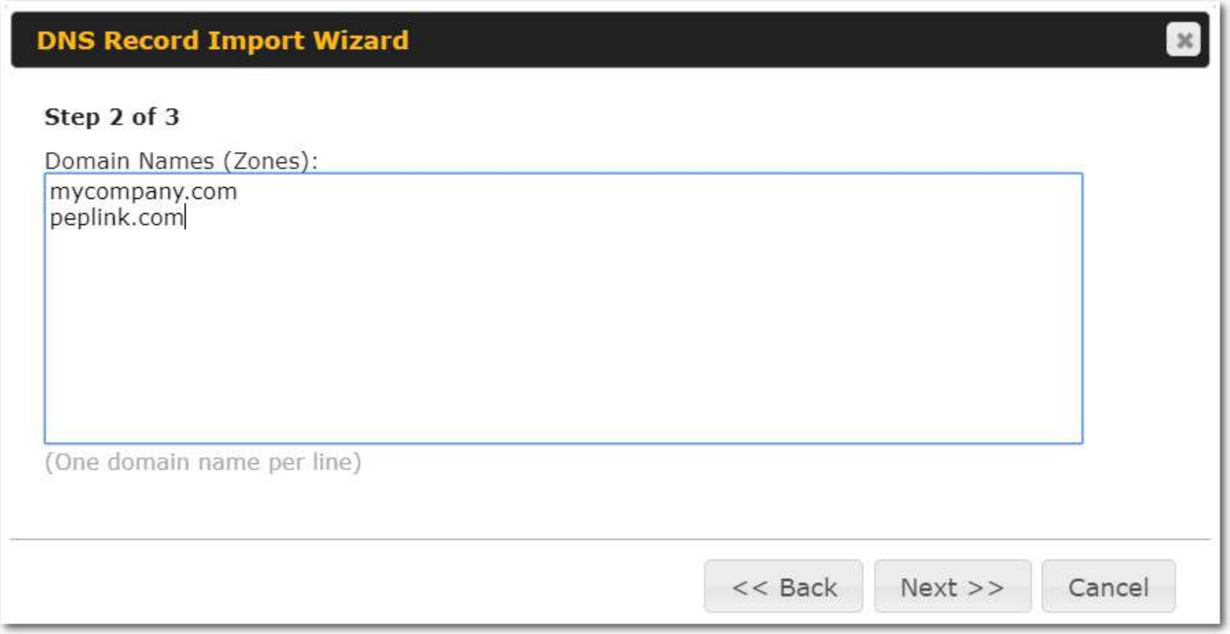
Step 1 of 3

Target DNS Server IP Address:

Transfer via...

WAN 1

- In the **Target DNS Server IP Address** field, enter the IP address of the DNS server.
- In the **Transfer via...**field, choose the connection which you would like to transfer through.
- Select **Next >>** to continue.



DNS Record Import Wizard

Step 2 of 3

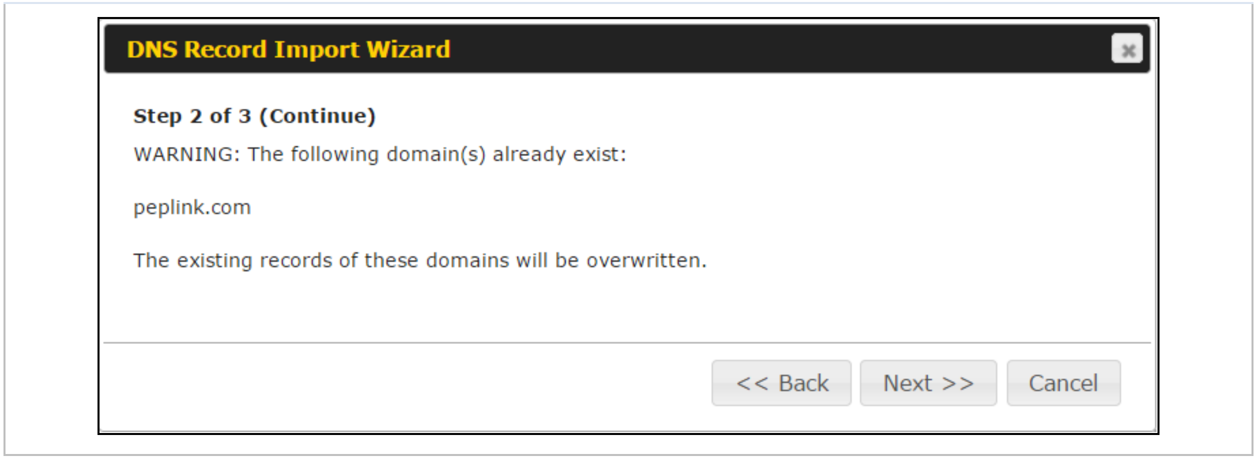
Domain Names (Zones):

mycompany.com
peplink.com

(One domain name per line)

- In the blank space, enter the **Domain Names (Zones)** which you would like to assign the IP address entered in the previous step. Enter one domain name per line.
- Select **Next >>** to continue.

Important Note
If you have entered domain(s) which already exist in your settings, a warning message will appear. Select **Next >>** to overwrite the existing record or **<< Back** to go back to the previous step.



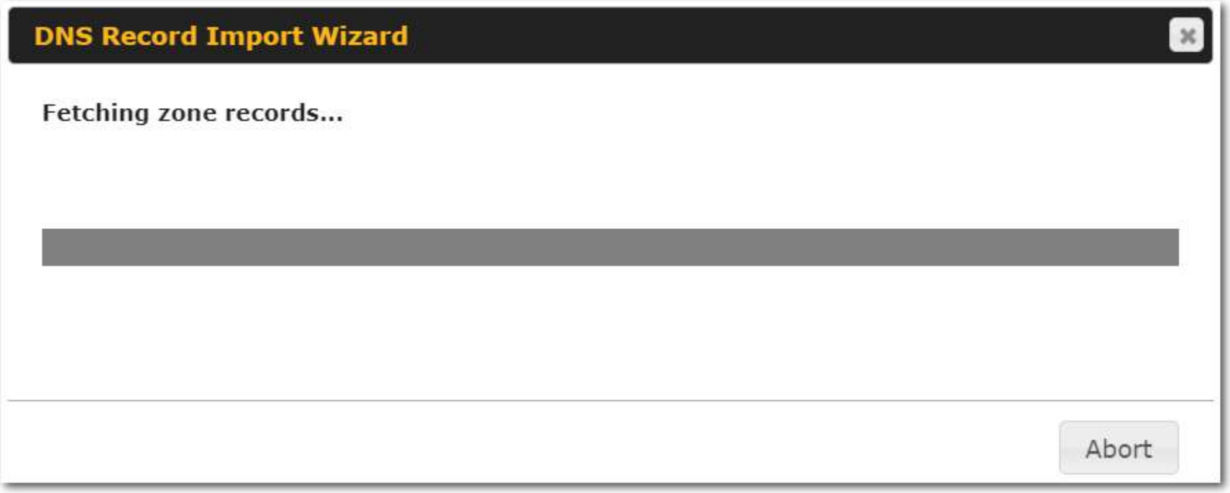
DNS Record Import Wizard

Step 2 of 3 (Continue)

WARNING: The following domain(s) already exist:

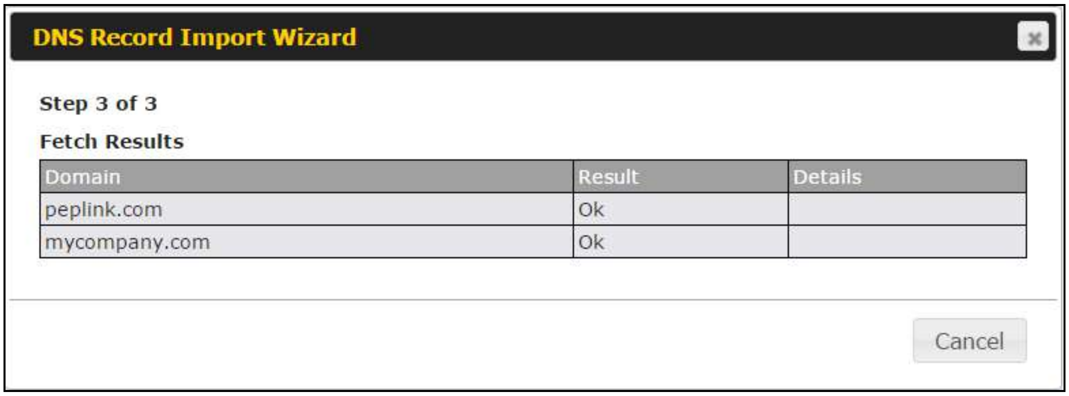
peplink.com

The existing records of these domains will be overwritten.



DNS Record Import Wizard

Fetching zone records...



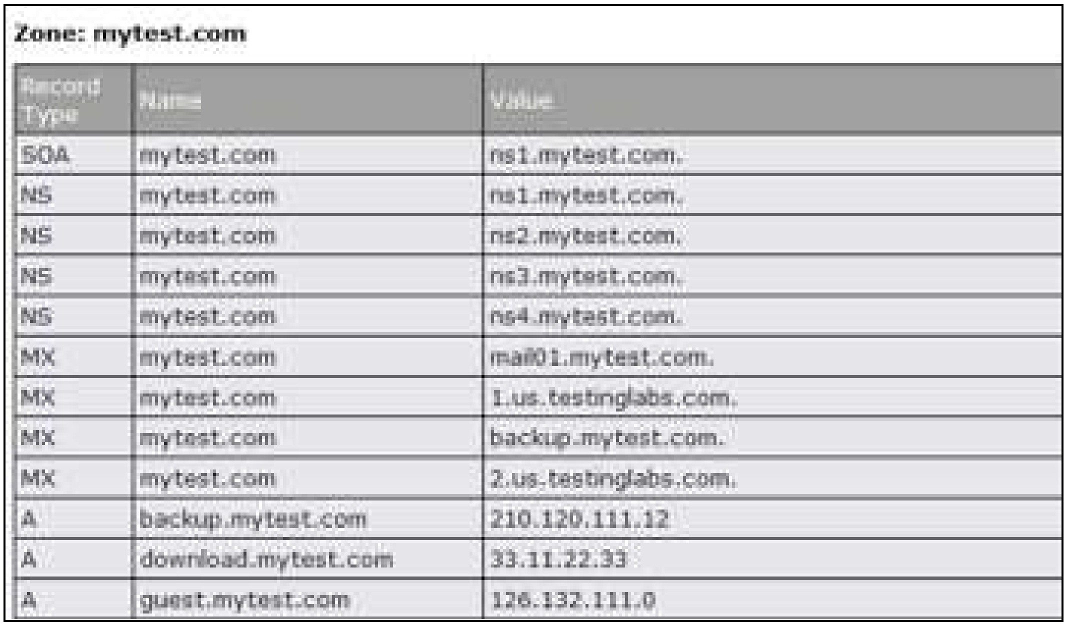
DNS Record Import Wizard

Step 3 of 3

Fetch Results

Domain	Result	Details
peplink.com	Ok	
mycompany.com	Ok	

After the zone records process have been fetched, the fetch results would be shown as above. You can view import details by clicking the corresponding hyperlink on the right-hand side.



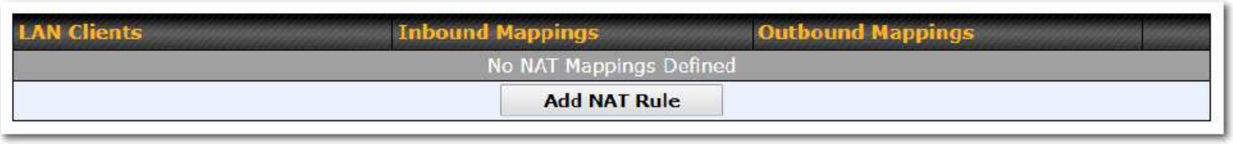
Zone: mytest.com

Record Type	Name	Value
SOA	mytest.com	ns1.mytest.com.
NS	mytest.com	ns1.mytest.com.
NS	mytest.com	ns2.mytest.com.
NS	mytest.com	ns3.mytest.com.
NS	mytest.com	ns4.mytest.com.
MX	mytest.com	mail01.mytest.com.
MX	mytest.com	1.us.testinglabs.com.
MX	mytest.com	backup.mytest.com.
MX	mytest.com	2.us.testinglabs.com.
A	backup.mytest.com	210.120.111.12
A	download.mytest.com	33.11.22.33
A	guest.mytest.com	126.132.111.0

10.6 NAT Mappings

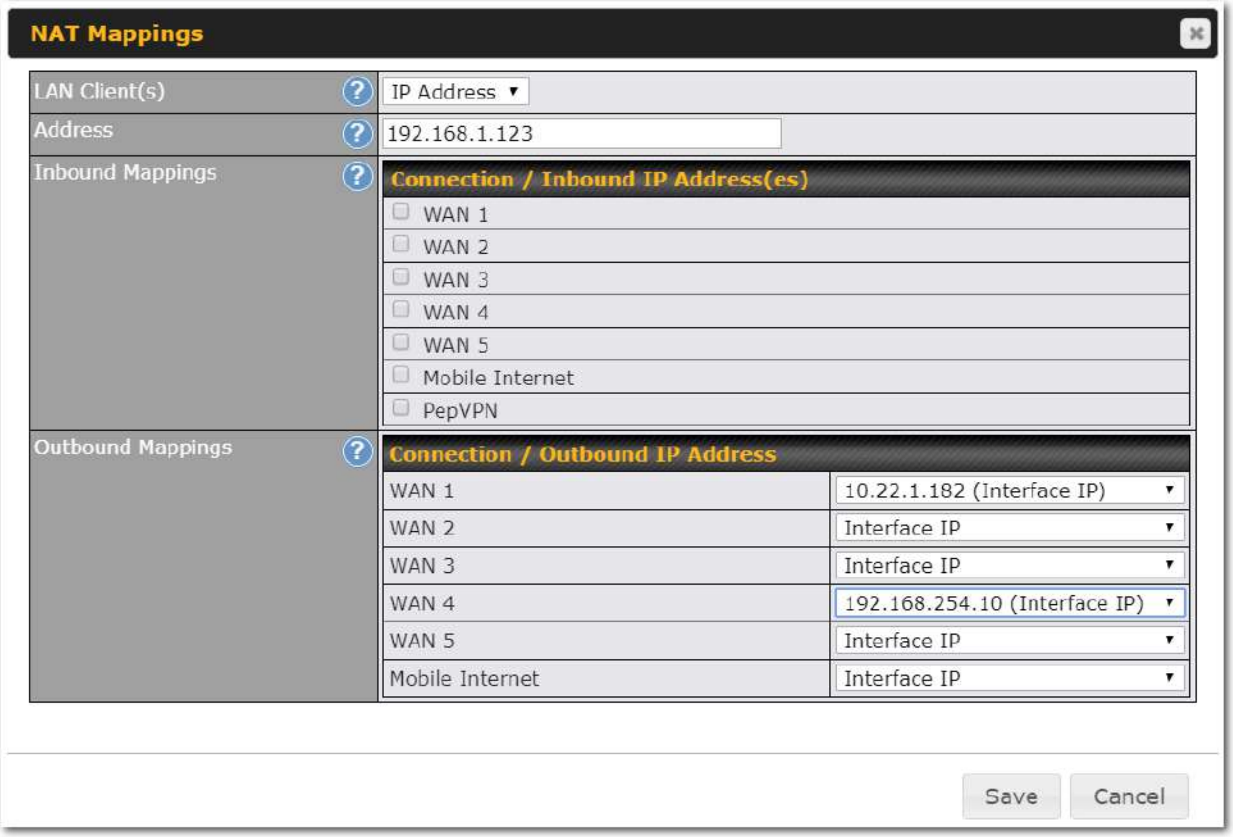
The Peplink Balance allows the IP address mapping of all inbound and outbound NATed traffic to and from an internal client IP address.

NAT mappings can be configured at **Network>NAT Mappings**.



LAN Clients	Inbound Mappings	Outbound Mappings
No NAT Mappings Defined		

To add a rule for NAT mappings, click **Add NAT Rule** and the following screen will be displayed:



NAT Mappings

LAN Client(s)	IP Address
Address	192.168.1.123

Inbound Mappings

Connection / Inbound IP Address(es)
□ WAN 1
□ WAN 2
□ WAN 3
□ WAN 4
□ WAN 5
□ Mobile Internet
□ PepVPN

Outbound Mappings

Connection / Outbound IP Address	
WAN 1	10.22.1.182 (Interface IP)
WAN 2	Interface IP
WAN 3	Interface IP
WAN 4	192.168.254.10 (Interface IP)
WAN 5	Interface IP
Mobile Internet	Interface IP

NAT Mapping Settings	
LAN Client(s)	NAT Mapping rules can be defined for a single LAN **IP Address**, an **IP Range**, or an **IP Network**.

Address	This refers to the LAN host’s private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when **IP Address** is selected.
Range	The IP range is a contiguous group of private IP addresses used by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when **IP Range** is selected.
Network	The IP network refers to all private IP addresses and ranges managed by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when **IP Network** is selected.
Inbound Mappings	This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when **IP Address** is selected in the **LAN Client(s)** field. Note 1: Inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode. Note 2: Each WAN IP address can be associated to one NAT mapping only.
Outbound Mappings	This setting specifies the WAN IP addresses should be used when an IP connection is made from a LAN host to the Internet. Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility). Note 1: If you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the **Outbound Policy** section. Note 2: WAN connections in drop-in mode or IP forwarding mode are not shown here.

Click **Save** to save the settings when configuration has been completed.

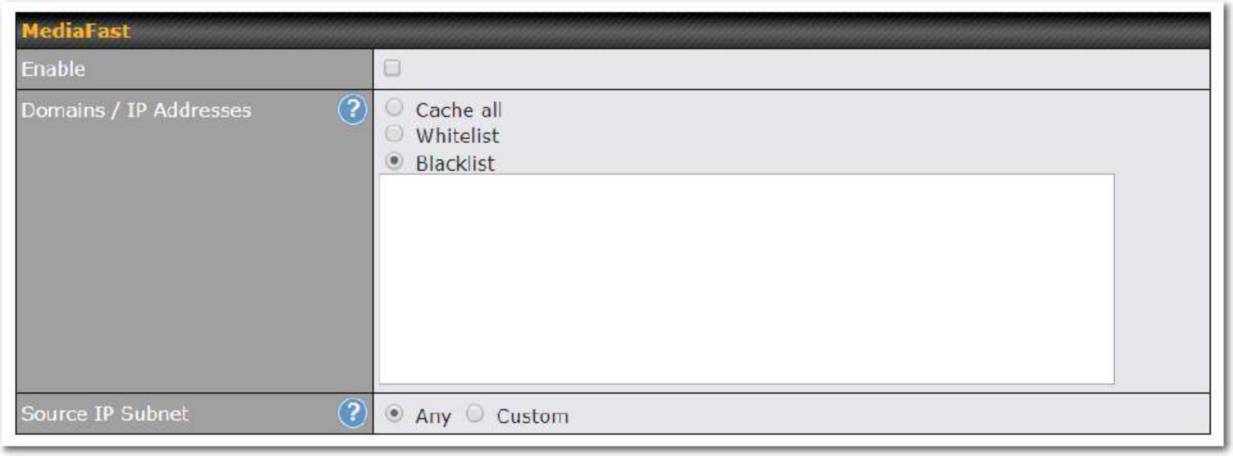
Important Note
Inbound firewall rules override inbound mapping settings.

10.7 MediaFast

MediaFast settings can be configured by navigating to **Network > MediaFast**.

Setting Up MediaFast Content Caching

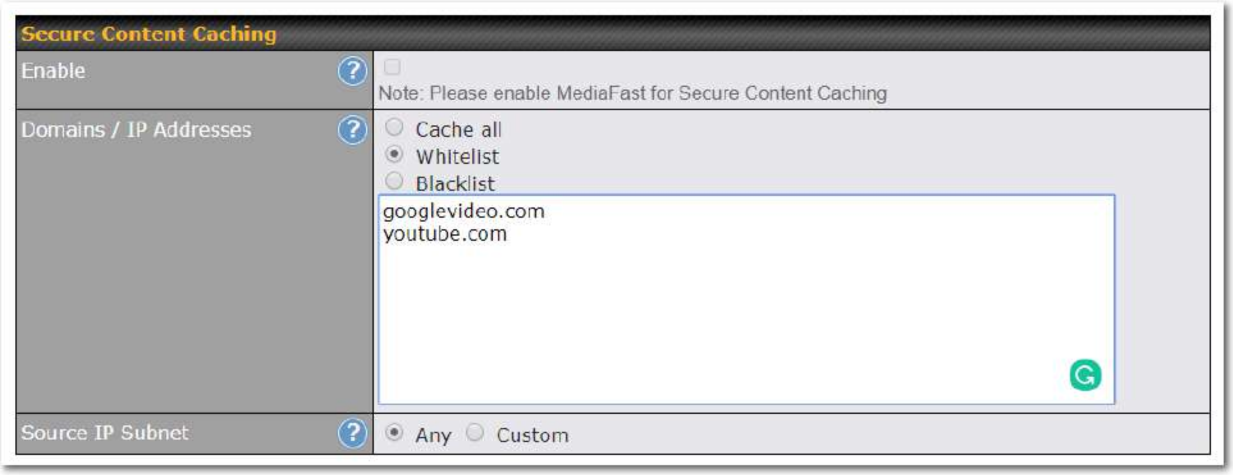
To access MediaFast content caching settings, select **Network > MediaFast**.



MediaFast

Enable	□
Domains / IP Addresses	○ Cache all ○ Whitelist ● Blacklist
Source IP Subnet	● Any ○ Custom

MediaFast	
Enable	Click the checkbox to enable MediaFast content caching.
Domains / IP Addresses	Choose to **Cache on all domains**, or enter domain names and then choose either **Whitelist** (cache the specified domains only) or **Blacklist** (do not cache the specified domains).
Source IP Subnet	This setting allows caching to be enabled on custom subnets only. If "Any" is selected, then caching will apply to all subnets.

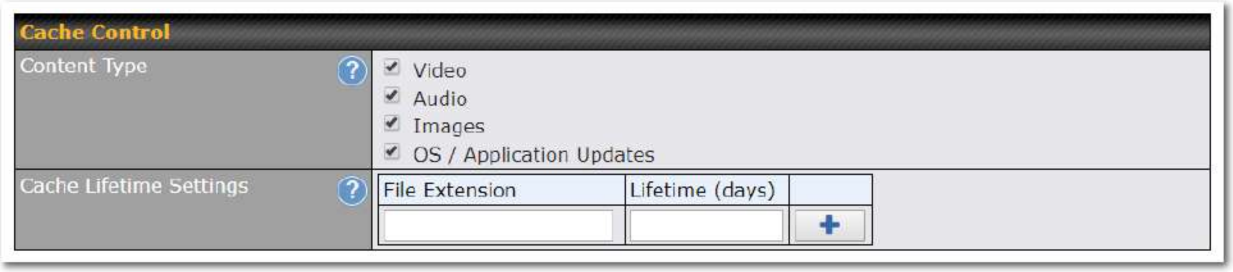


Secure Content Caching

Enable	□ Note: Please enable MediaFast for Secure Content Caching
Domains / IP Addresses	○ Cache all ● Whitelist ○ Blacklist googlevideo.com youtube.com
Source IP Subnet	● Any ○ Custom

The **Secure Content Caching** menu operates identically to the **MediaFast** menu, except it is for secure content cachting accessible through https://.
In order for Mediafast devices to cache and deliver HTTPS content, every client needs to have the necessary certificates installed*.

*See https://forum.peplink.com/t/certificate-installation-for-mediafast-https-caching/



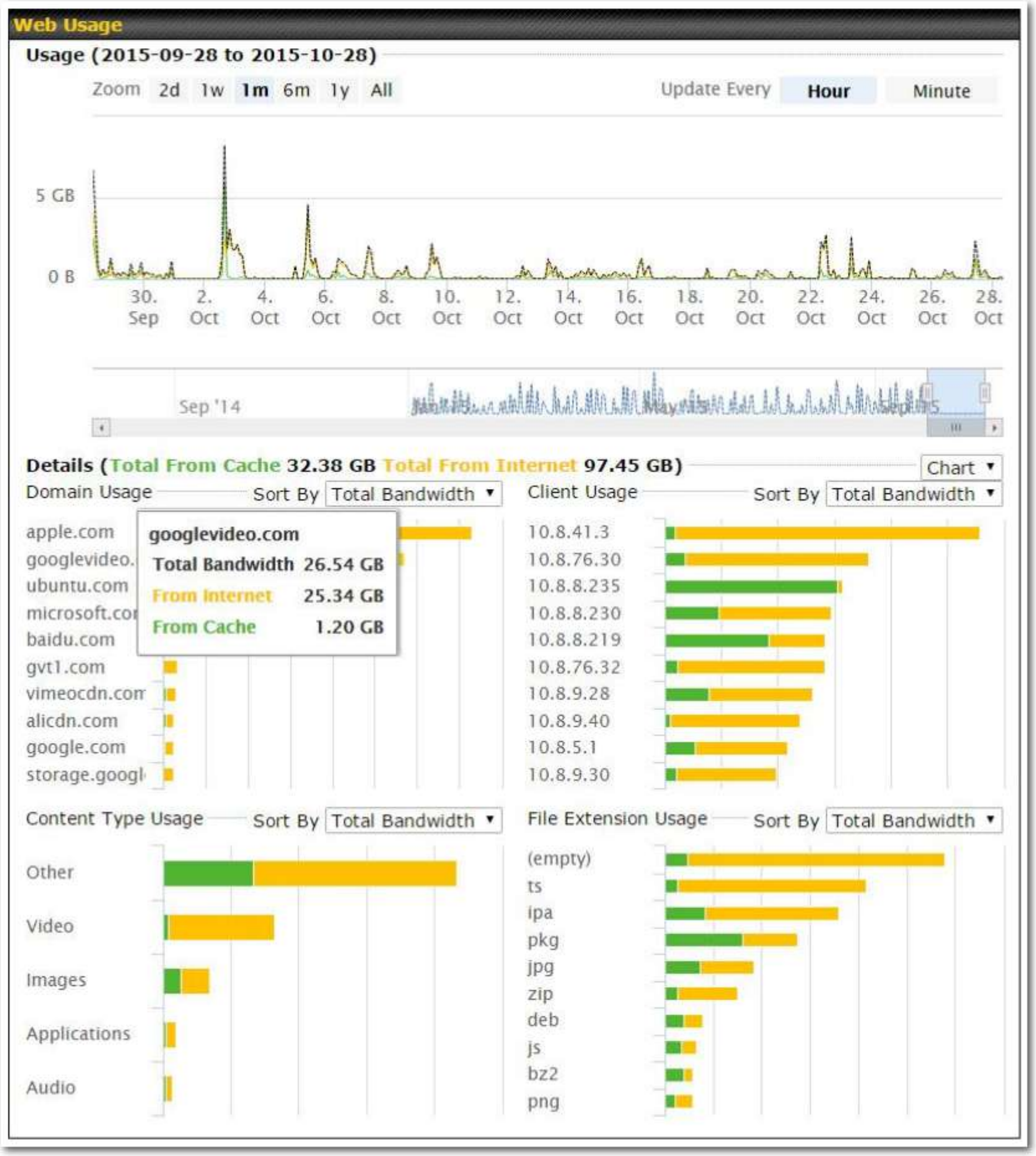
Cache Control

Content Type	☑ Video ☑ Audio ☑ Images ☑ OS / Application Updates
Cache Lifetime Settings	File Extension | Lifetime (days) | +

Cache Control	
Content Type	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
Cache Lifetime Settings	Enter a file extension, such as JPG or DOC. Then enter a lifetime in days to specify how long files with that extension will be cached. Add or delete entries using the controls on the right.

Viewing MediaFast Statistics

To get details on storage and bandwidth usage, select **Status>MediaFast**.



Web Usage

Usage (2015-09-28 to 2015-10-28)

Zoom 2d 1w **1m** 6m 1y All

Update Every **Hour** Minute

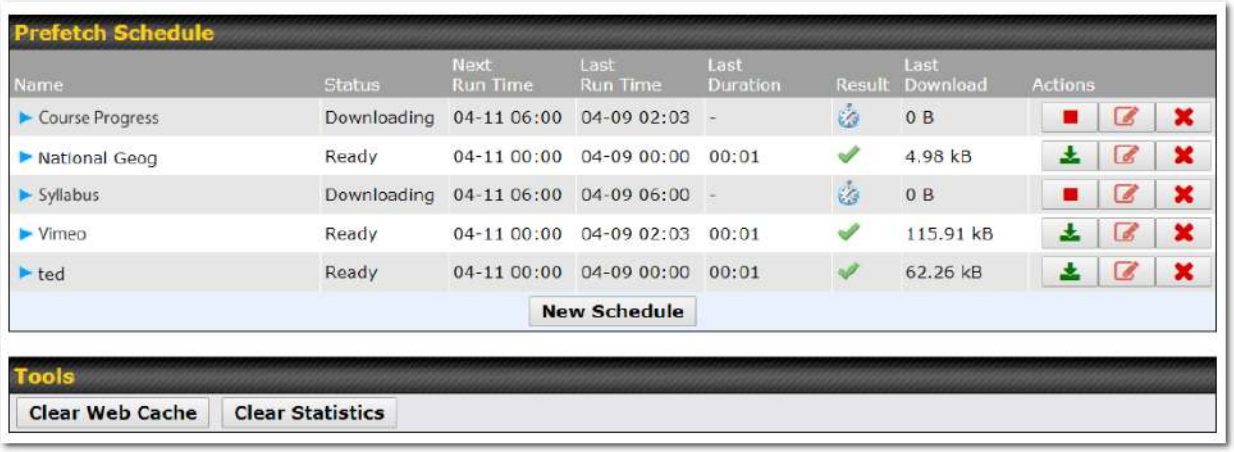
Details (Total From Cache 32.38 GB Total From Internet 97.45 GB)

googlevideo.com

Total Bandwidth	26.54 GB
From Internet	25.34 GB
From Cache	1.20 GB

Prefetch Schedule

Content prefetching allows you to download content on a schedule that you define, which can help to preserve network bandwidth during busy times and keep costs down. To access MediaFast content prefetching settings, select **Network > MediaFast > Prefetch Schedule**.

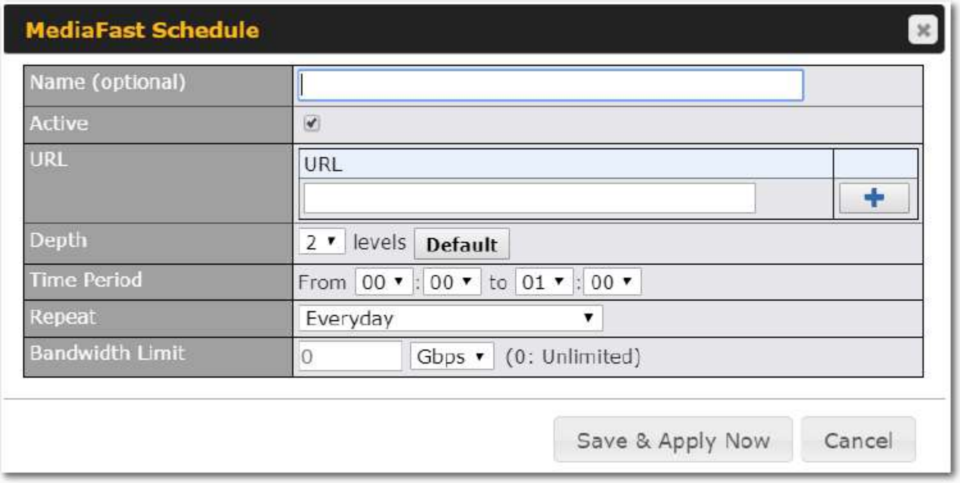


Prefetch Schedule

Name	Status	Next Run Time	Last Run Time	Last Duration	Result	Last Download	Actions
▶ Course Progress	Downloading	04-11 06:00	04-09 02:03	-	⏱	0 B	■ ✎ ✖
▶ National Geog	Ready	04-11 00:00	04-09 00:00	00:01	✓	4.98 kB	⬇ ✎ ✖
▶ Syllabus	Downloading	04-11 06:00	04-09 06:00	-	⏱	0 B	■ ✎ ✖
▶ Vimeo	Ready	04-11 00:00	04-09 02:03	00:01	✓	115.91 kB	⬇ ✎ ✖
▶ ted	Ready	04-11 00:00	04-09 00:00	00:01	✓	62.26 kB	⬇ ✎ ✖

Tools

Prefetch Schedule Settings	
Name	This field displays the name given to the scheduled download.
Status	Check the status of your scheduled download here.
Next Run Time/Last Run Time	These fields display the date and time of the next and most recent occurrences of the scheduled download.
Last Duration	Check this field to ensure that the most recent download took as long as expected to complete. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time.
Result	This field indicates whether downloads are in progress (⏱) or complete (✓).
Last Download	Check this field to ensure that the most recent download file size is within the expected range. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time. This field is also useful for quickly seeing which downloads are consuming the most storage space.
Actions	To begin a scheduled download immediately, click ⬇. To cancel a scheduled download, click ■. To edit a scheduled download, click ✎. To delete a scheduled download, click ✖.
New Schedule	Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:

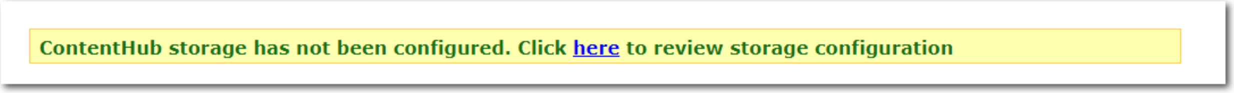
	 MediaFast Schedule Name (optional) Active ☑ URL Depth 2 levels Default Time Period From 00 : 00 to 01 : 00 Repeat Everyday Bandwidth Limit 0 Gbps (0: Unlimited) Save & Apply Now Cancel Simply provide the requested information to create your schedule.
Clear Web Cache	Click to clear all cached content. Note that this action cannot be undone.
Clear Statistics	Click to clear all prefetch and status page statistics.

10.8 ContentHub

ContentHub allows you to deliver webpages and applications to users connected to the SSID using the local storage on your router. Users will be able to access news, articles, videos, and access your web app without the need for internet access.

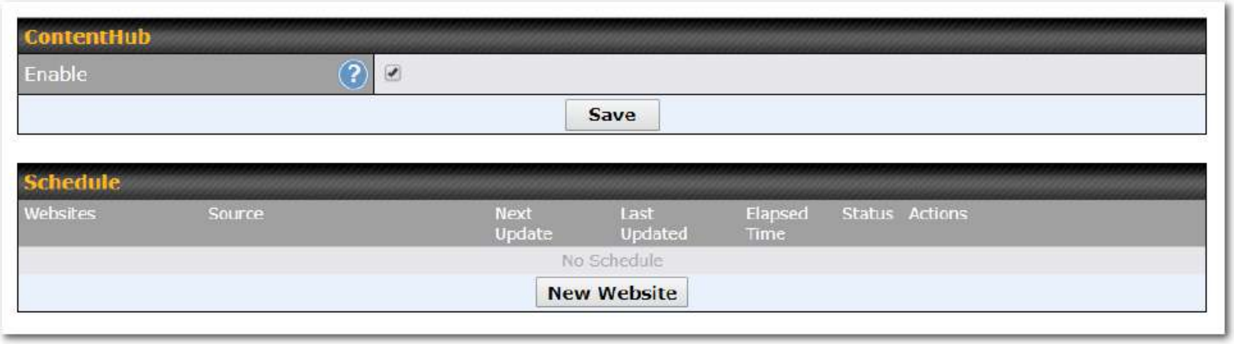
The ContentHub can be used to provide infotainment to connected users on transport.

ContentHub storage needs to be configured before content can be uploaded to the ContentHub. Click on the link on the information panel to configure storage.



ContentHub storage has not been configured. Click here to review storage configuration

To access ContentHub, navigate to **Network > ContentHub** and check the **Enable** box.:



ContentHub

Enable ?	☑

Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
No Schedule						

On an external server, configure content (a website or application) that will be synced to the ContentHub. For example, an html5 website.

To configure a website or application as content, follow the steps below.

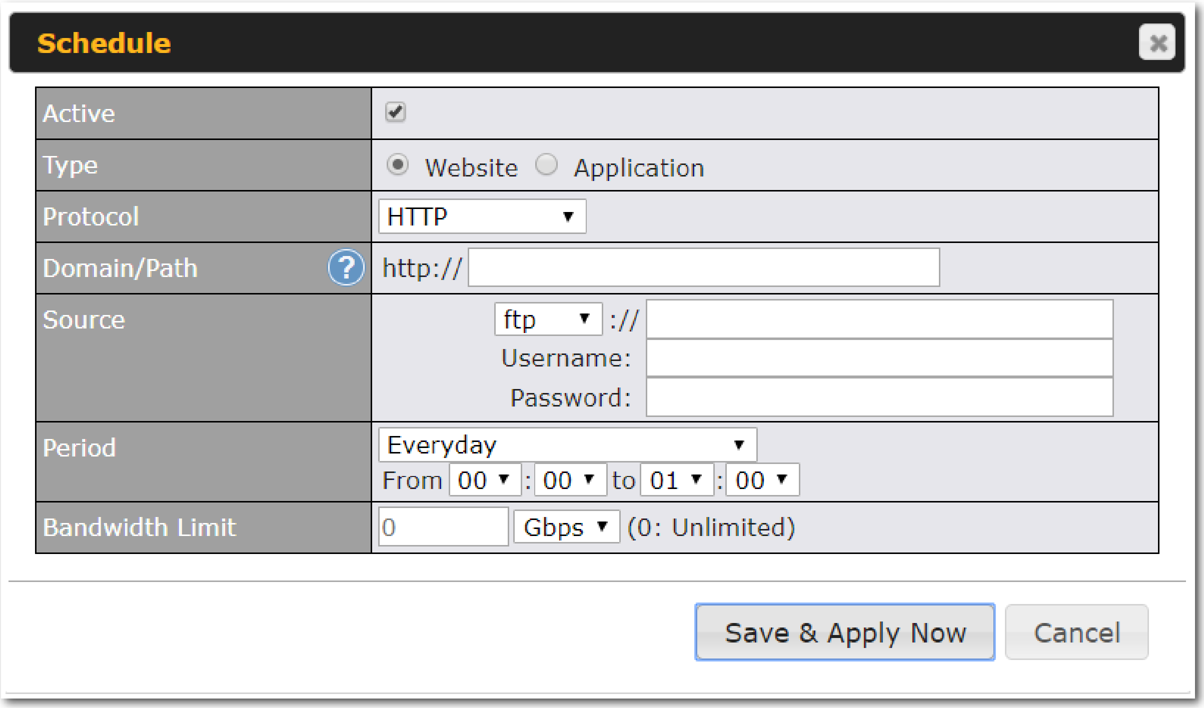
Configure a website for the ContentHub

This option allows you to sync a website to the Peplink router. This website will then be published with the specified domain from the router itself and makes the content available to the client via the HTTP/HTTPS protocol.

Only FTP sync is supported for this type of ContentHub content.

The content should be uploaded to an FTP server before you sync it with ContentHub.

Click **New Website** and a window with the following configuration options will appear:

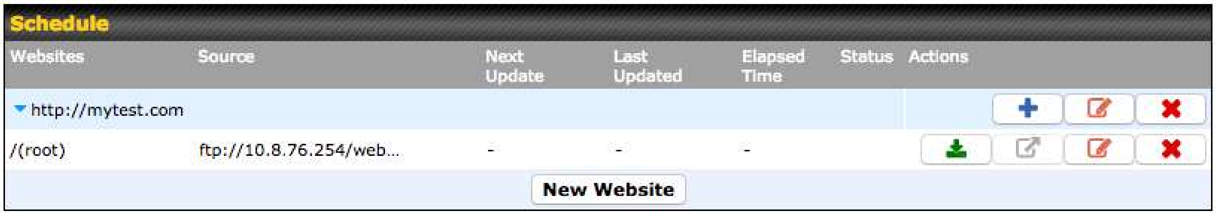


Schedule

Active	☑
Type	● Website ○ Application
Protocol	HTTP ▾
Domain/Path	http://
Source	ftp ▾ :// Username: Password:
Period	Everyday ▾ From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾
Bandwidth Limit	0 Gbps ▾ (0: Unlimited)

Schedule	
Active	Checking the box toggles the activation of the content.
Type	Select the type of content: Website or Application.
Protocol	Configure the protocol to be used: HTTP, HTTPS or both.
Domain/Path	Enter the URL for the ContenHub to use as the domain name for client access (such as http://mytest.com).
Method	Only applicable for **Application** type content. Choose between sync or file upload.
Source	Enter the details of the server that the content will be downloaded from. Enter credentials under **Username** and **Password**.
Period	This field determines how often the router will search for updates to the source content.
Bandwidth Limit	Set a bandwidth limit for clients.

Click “**Save & Apply Now**” to activate the changes. A screenshot of the display after configuration is shown below:

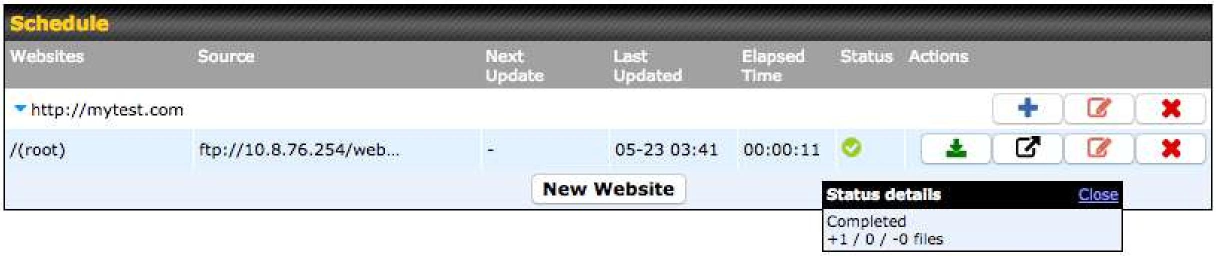


Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▾ http://mytest.com						✚ ✎ ✖
/(root)	ftp://10.8.76.254/web...	-	-	-		⬇ ↗ ✎ ✖

The content will be synced regularly according to the time set in the **Period** that was configured earlier.

If you want to activate the sync manually, you can click the “ ⬇ ” icon. The “Status” column will display the sync progress. When the sync is completed, a summary will be displayed, as shown in the screenshot below:



Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▾ http://mytest.com						✚ ✎ ✖
/(root)	ftp://10.8.76.254/web...	-	05-23 03:41	00:00:11	✓	⬇ ↗ ✎ ✖

Status details Close

Completed
+1 / 0 / -0 files

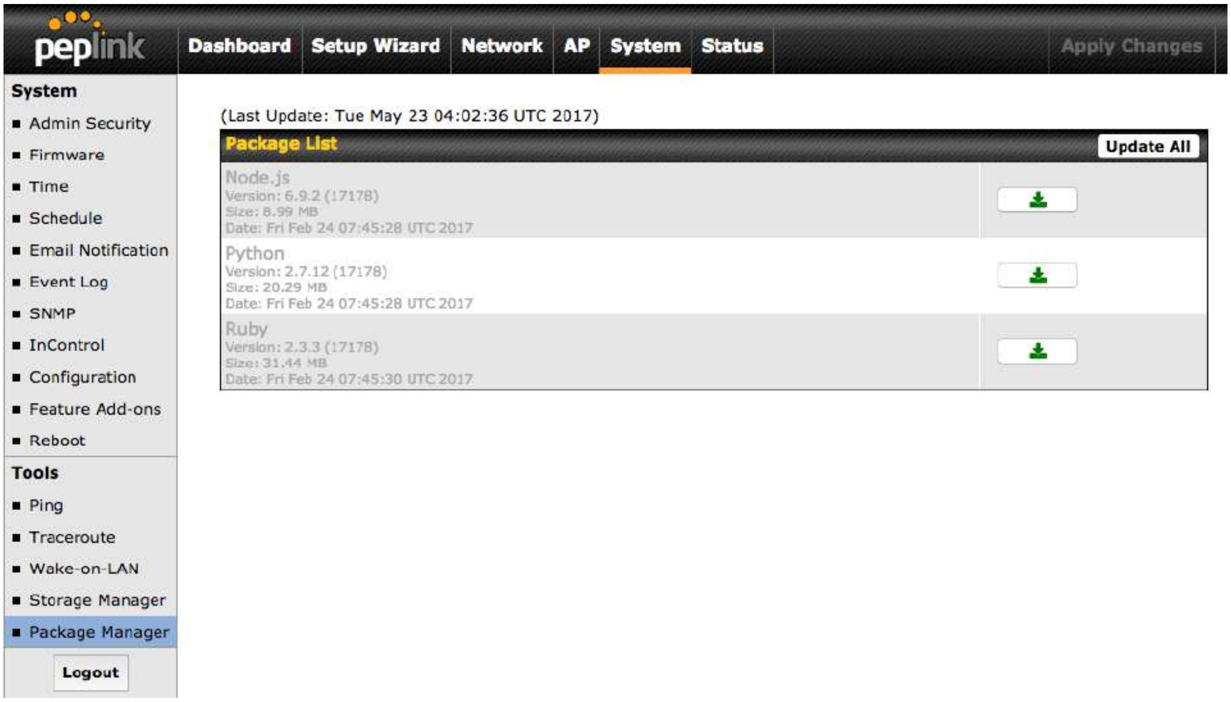
To access the content, open a browser in the MFA’s client and enter the domain details that were configured earlier (such as http://mytest.com).

Configure an application for the ContentHub

MediaFast routers allow you to configure and publish any application from the router itself by using one of the supported frameworks below:

- Python (version 2.7.12)
- Ruby (version 2.3.3)
- Node.js (version 6.9.2)

Install the desired framework under “Package Manager” as shown below:

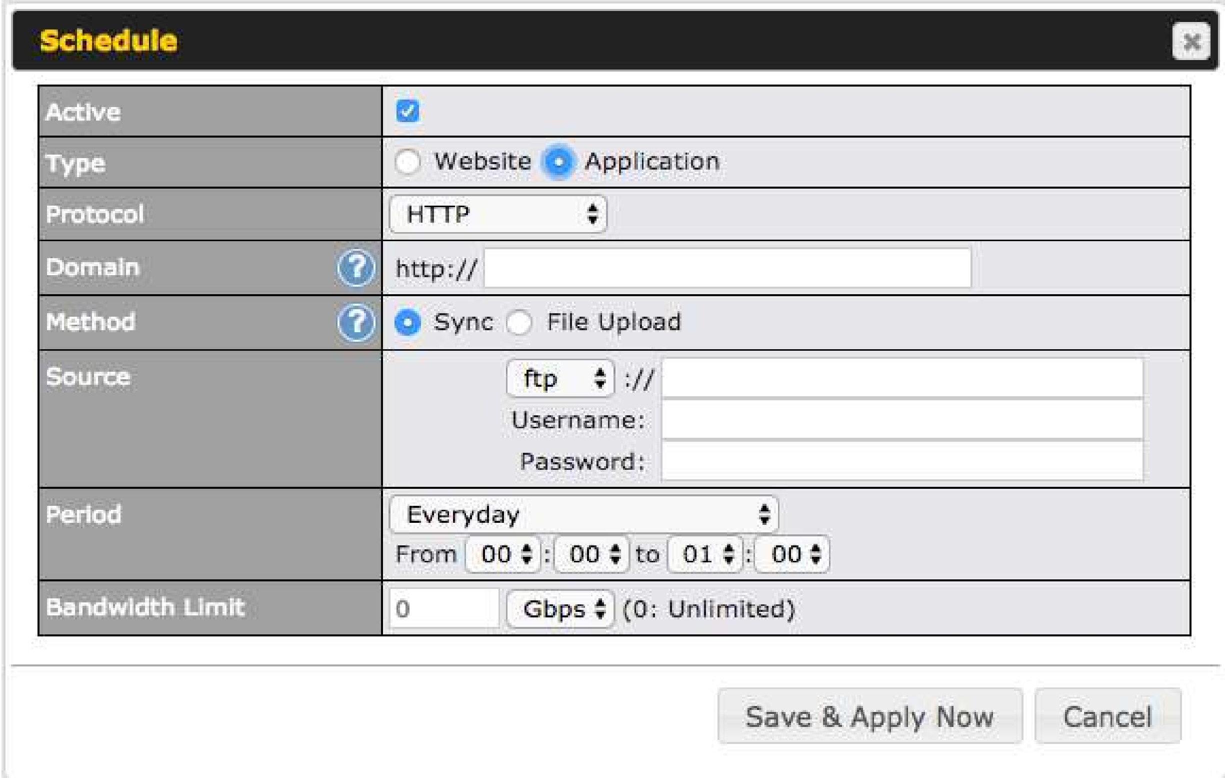


(Last Update: Tue May 23 04:02:36 UTC 2017)

Package List

Node.js Version: 6.9.2 (17178) Size: 8.99 MB Date: Fri Feb 24 07:45:28 UTC 2017
Python Version: 2.7.12 (17178) Size: 20.29 MB Date: Fri Feb 24 07:45:28 UTC 2017
Ruby Version: 2.3.3 (17178) Size: 31.44 MB Date: Fri Feb 24 07:45:30 UTC 2017

After installing the framework, change the ”Type” to “Application” and configure the website.



Schedule

Active	☑
Type	○ Website ● Application
Protocol	HTTP
Domain	http://
Method	● Sync ○ File Upload
Source	ftp :// Username: Password:
Period	Everyday From 00 : 00 to 01 : 00
Bandwidth Limit	0 Gbps (0: Unlimited)

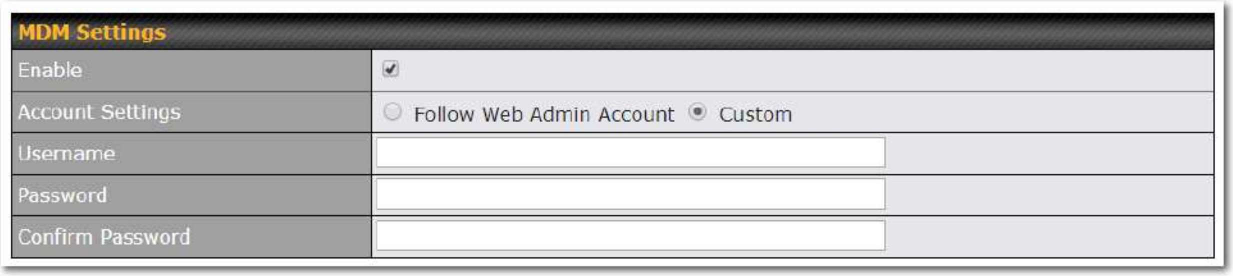
The setting is the same as the Website type (refer to the description in the section above).

Application type content need to be packed as explained below:

1. Implement two bash script files, start.sh and stop.sh in the root folder, to start and stop your application. The MediaFast router will only execute start.sh and stop.sh when the corresponding website is enabled and disabled respectively.
2. Compress the application files and the bash script to .tar.gz format.
3. Upload this tar file to the router.

MDM Settings

In addition to performing content caching, MediaFast-enabled routers can also serve as an MDM, administrating to client devices. To access MDM Settings, navigate to **Network > MDM Settings**:



MDM Settings	
Enable	☑
Account Settings	○ Follow Web Admin Account ● Custom
Username	
Password	
Confirm Password	

MDM Settings	
Enable	Click this checkbox to enable MDM on your router.
Account Settings	Click **Follow Web Admin Account** to allow client devices to use the built-in administrator account when performing MDM. Set **Custom** to specify a username and password your router will use to log into your client devices.

Please refer to the knowledgebase for information about enrolling client devices to MDM: https://forum.peplink.com/t/how-to-enroll-a-device-to-the-mdm-server/8454

Docker

MediaFast enabled routers can host Docker containers when running Firmware 7.1 or later.
Docker is an open platform for developing, shipping, and running applications.
From Firmware version 7.1.0 and upwards, it is possible to install and run Docker Containers on your Peplink Mediafast 500 or 750 router.

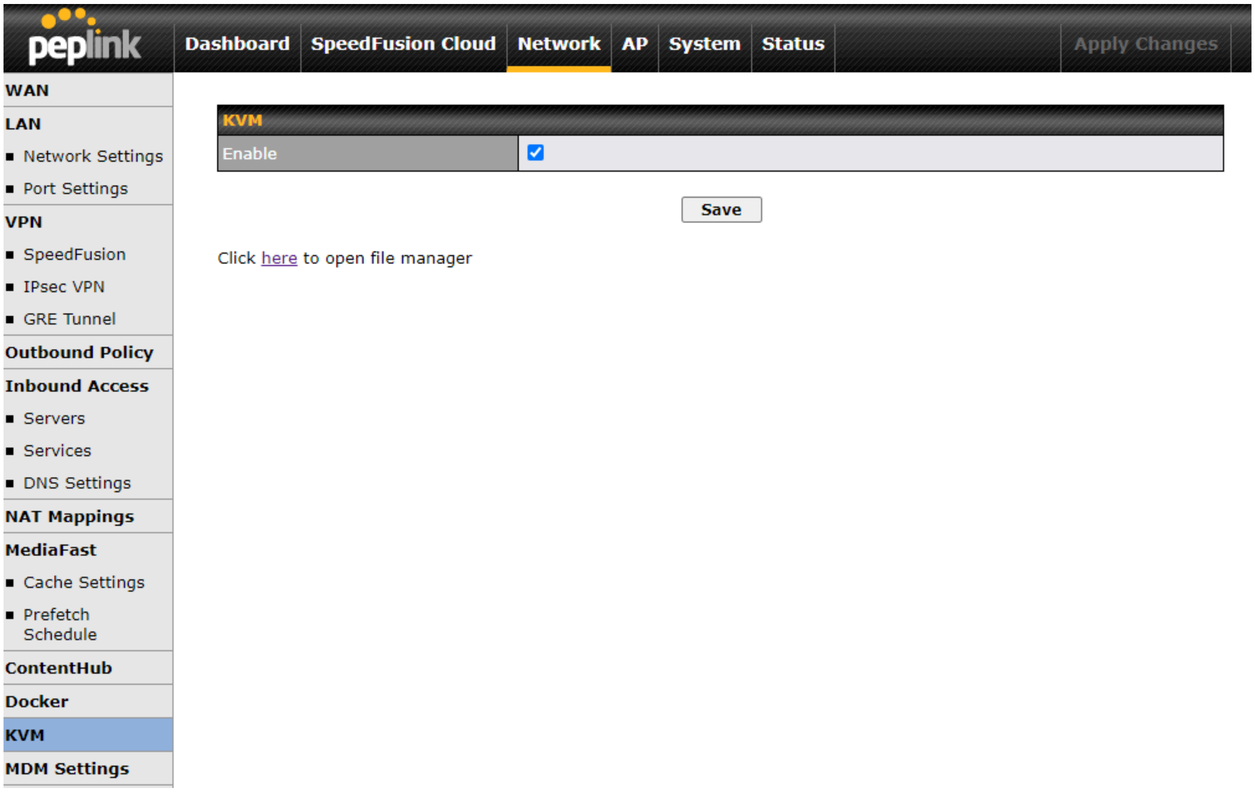
Due to the nature of Docker and its unlimited variables, this feature is supported by Pepwave up to the point of creating a running Docker Container.
Information about Docker can be found on the Docker Documentation site:
https://docs.docker.com/ 2

This will allow you to run a file sharing platform (ownCloud), a web server (WordPress, Joomla!) , a learning platform (Moodle), or a visualisation tool for viewing large scale data (Kibana).
When creating a new Docker Container, the Pepwave router will search through the Docker Hub repository. https://hub.docker.com/explore/ 7

For detailed configuration instructions, refer to our knowledge base:
https://forum.peplink.com/t/how-to-run-a-docker-application-on-a-peplink-mediafast-router/16021

KVM

MediaFast enabled routers now support KVM. Users will have to download and install Virtual Machine Manager to manage the KVM virtual machines. Through this, users are able to virtualise a Linux environment.



KVM	
Enable	☑

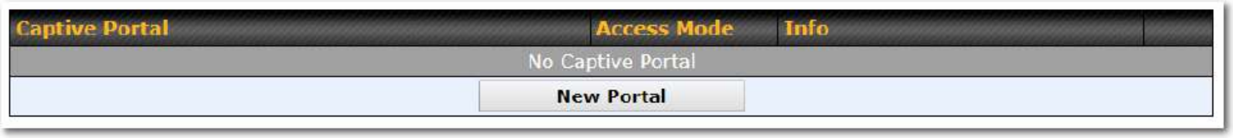
Click here to open file manager

For detailed configuration instructions, refer to our knowledge base articles:

1. How to install a Virtual Machine on Peplink/Pepwave - MediaFast/ContentHub Routers

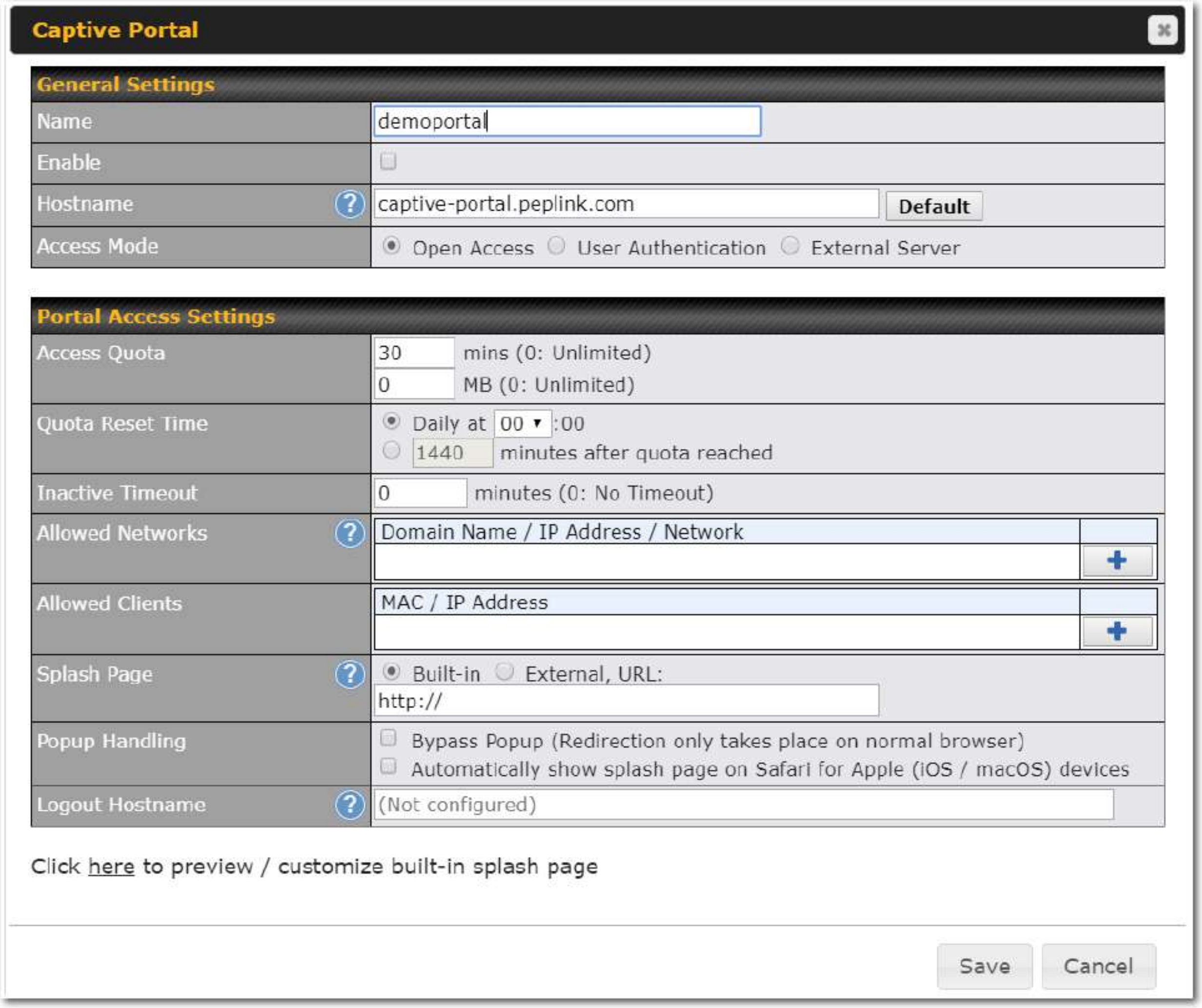
2. How to Install Virtual Machine with USB storage on Peplink/Pepwave - MediaFast/ContentHub Routers

10.9 Captive Portal



Captive Portal	Access Mode	Info
No Captive Portal		

The captive portal serves as a gateway that clients have to pass if they wish to access the Internet using your router. To configure, navigate to **Network > Captive Portal**.



Captive Portal

General Settings

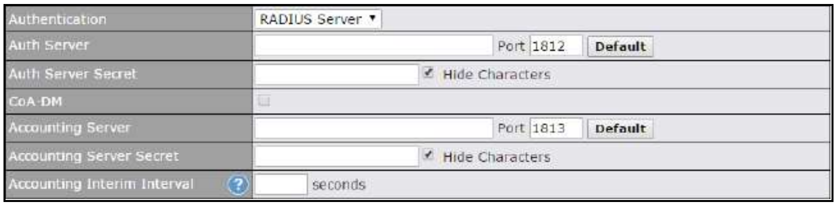
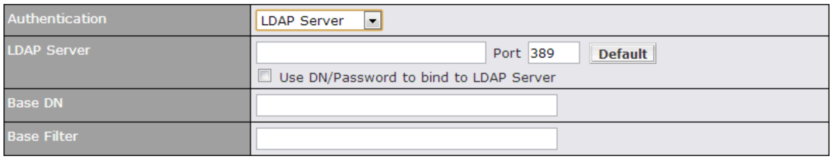
Name	demoportal
Enable	□
Hostname	captive-portal.peplink.com [Default]
Access Mode	● Open Access ○ User Authentication ○ External Server

Portal Access Settings

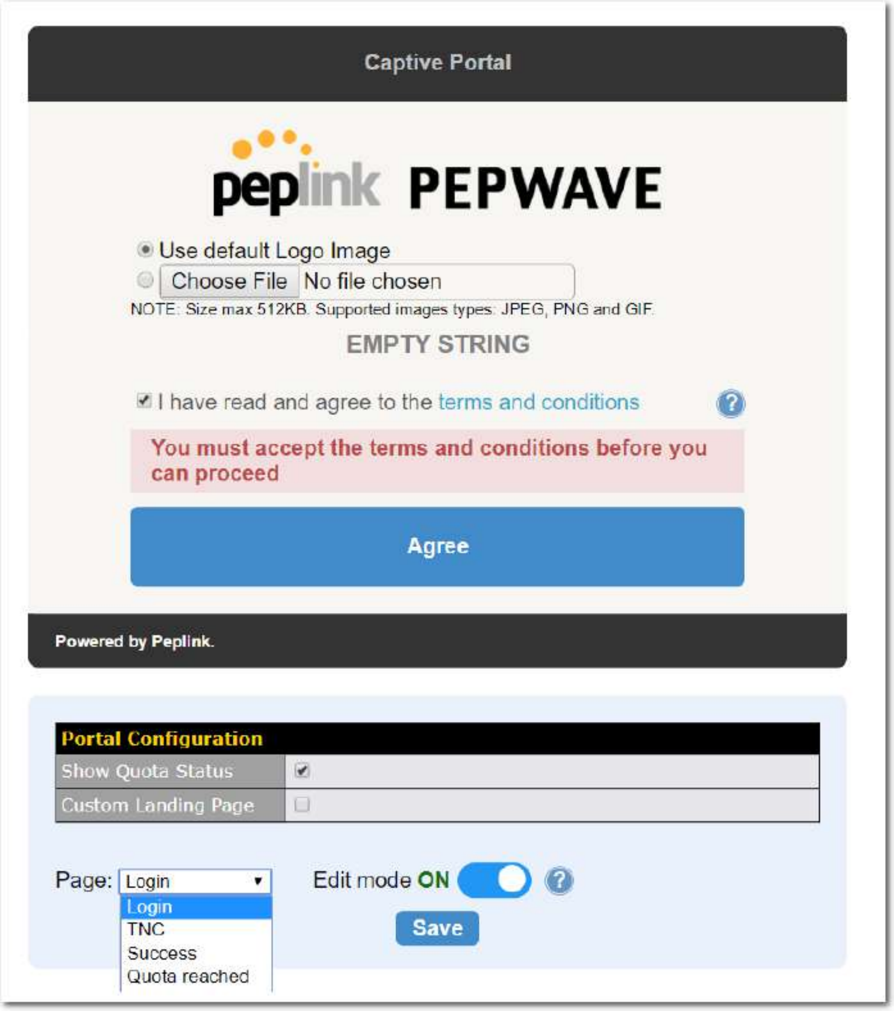
Access Quota	30 mins (0: Unlimited) 0 MB (0: Unlimited)
Quota Reset Time	● Daily at 00 :00 ○ 1440 minutes after quota reached
Inactive Timeout	0 minutes (0: No Timeout)
Allowed Networks	Domain Name / IP Address / Network
Allowed Clients	MAC / IP Address
Splash Page	● Built-in ○ External, URL: http://
Popup Handling	□ Bypass Popup (Redirection only takes place on normal browser) □ Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostname	(Not configured)

Click here to preview / customize built-in splash page

Captive Portal Settings	
Enable	Check **Enable** and then, optionally, select the LANs/VLANs that will use the captive portal.

Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click **Default**.
Access Mode	Click **Open Access** to allow clients to freely access your router. Click **User Authentication** to force your clients to authenticate before accessing your router. Select **External Server** to use the Captive Portal with a HotSpot system. As described in the following knowledgebase article: https://forum.peplink.com/t/using-hotspotsystem-wi-fi-on-pepwave-max-routers/
RADIUS Server	This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:  Authentication: RADIUS Server ▾ Auth Server: Port 1812 Default Auth Server Secret: ☑ Hide Characters CoA-DM: □ Accounting Server: Port 1813 Default Accounting Server Secret: ☑ Hide Characters Accounting Interim Interval ?: seconds Fill in the necessary information to complete your connection to the server and enable authentication.
LDAP Server	This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:  Authentication: LDAP Server ▾ LDAP Server: Port 389 Default □ Use DN/Password to bind to LDAP Server Base DN: Base Filter: Fill in the necessary information to complete your connection to the server and enable authentication.
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.
Inactive Timeout	Clients will get disconnected when the inactive the configured time is reached. Default 0: no timeout
Allowed Networks	To whitelist a network, enter the domain name / IP address here and click + . To delete an existing network from the list of allowed networks, click the ✖ button next to the listing.

Allowed Clients	To whitelist a client, enter the MAC address / IP address here and click + . To delete an existing client from the list of allowed clients, click the ✖ button next to the listing.
Splash Page	Here, you can choose between using the Balance's built-in captive portal and redirecting clients to a URL you define.
Popup Handling	Configurable options for popup handling: - Bypass Popup (Redirection only takes place on normal browser) - Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostname	A hostname that can be used to logout captive portal when being accessed on browser.
Customize splash page	Click on the provided link in the Captive portal profile to customize the splash page. A new browser tab is opened with a WYSIWYG editor of the splash page o edit the content, click on the corresponding element after switching Edit Mode to ON.



Captive Portal

peplink PEPWAVE

● Use default Logo Image

○ Choose File No file chosen

NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.

EMPTY STRING

☑ I have read and agree to the terms and conditions ?

You must accept the terms and conditions before you can proceed

Agree

Powered by Peplink.

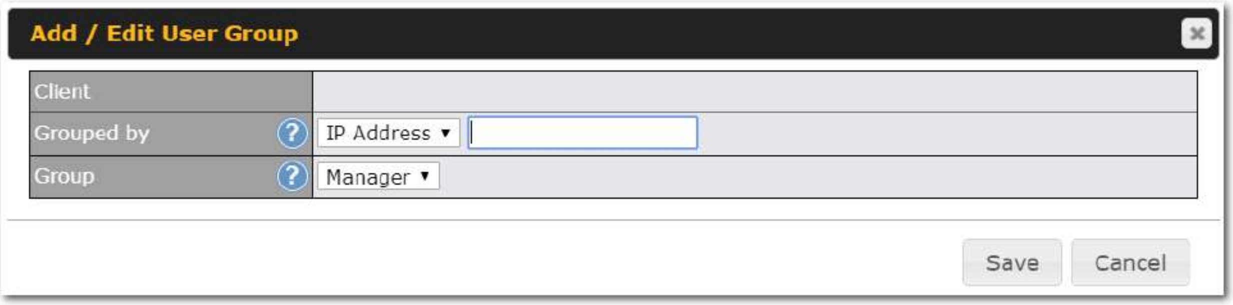
Portal Configuration	
Show Quota Status	☑
Custom Landing Page	□

Page: Login ▾ Edit mode ON ?

10.10 QoS

10.10.1 User Groups

LAN and PPTP clients can be categorized into three user groups - **Manager, Staff, and Guest**. This menu allows you to define rules and assign client IP addresses or subnets to a user group. You can apply different bandwidth and traffic prioritization policies on each user group in the **Bandwidth Control** and **Application** sections.
The table is automatically sorted, and the table order signifies the rules' precedence. The smaller and more specific subnets are put towards the top of the table and have higher precedence; larger and less specific subnets are placed towards the bottom.
Click the **Add** button to define clients and their user group. Click the ✖ button to remove the defined rule.
Two default rules are predefined and put at the bottom. They are **All DHCP reservation clients** and **Everyone**, and they cannot be removed. The **All DHCP reservation client represents** the LAN clients defined in the DHCP Reservation table on the LAN settings page. **Everyone** represents all clients that are not defined in any rule above. Click on a rule to change its group.



Add / Edit User Group

Client	
Grouped by	IP Address ▾
Group	Manager ▾

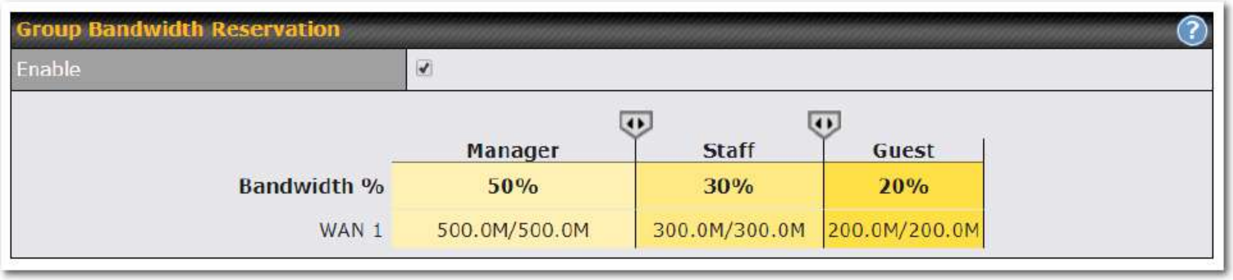
Add / Edit User Group	
Subnet / IP Address	From the drop-down menu, choose whether you are going to define the client(s) by an **IP Address** or a **Subnet**. If **IP Address** is selected, enter a name defined in DHCP reservation table or a LAN client's IP address. If **Subnet** is selected, enter a subnet address and specify its subnet mask.
Group	This field is to define which **User Group** the specified subnet / IP address belongs to.

Once users have been assigned to a user group, their internet traffic will be restricted by rules defined for that particular group. Please refer to the following two sections for details.

10.10.2 Bandwidth Control

This section is to define how much minimum bandwidth will be reserved to each user group when a WAN connection is **in full load**. When this feature is enabled, a slider with two indicators will be shown. You can move the indicators to adjust each group's weighting. The lower part of the table shows the corresponding reserved download and uploads bandwidth value of each connection.

By default, **50%** of bandwidth has been reserved for Manager, **30%** for Staff, and **20%** for Guest.

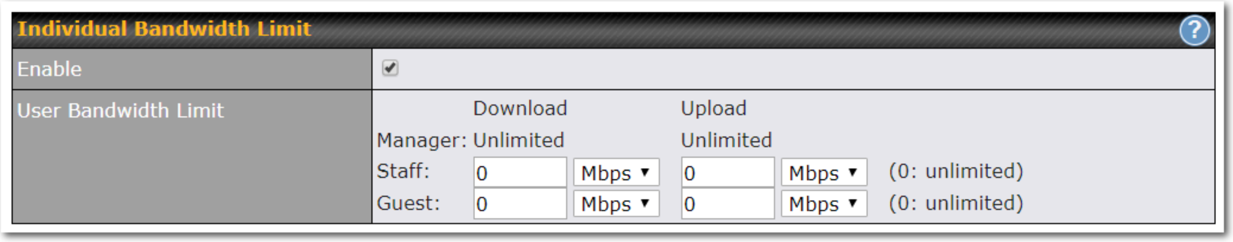


Group Bandwidth Reservation

Enable ☑

	Manager	Staff	Guest
Bandwidth %	50%	30%	20%
WAN 1	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M

You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Managers. By default, download and upload bandwidth limits are set to unlimited (set as **0)**.



Individual Bandwidth Limit

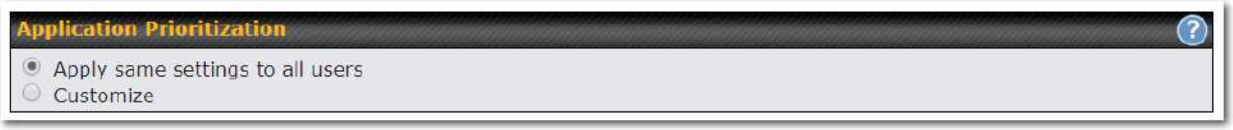
Enable ☑

User Bandwidth Limit

	Download		Upload		
Manager:	Unlimited		Unlimited		
Staff:	0	Mbps ▾	0	Mbps ▾	(0: unlimited)
Guest:	0	Mbps ▾	0	Mbps ▾	(0: unlimited)

10.10.3 Application

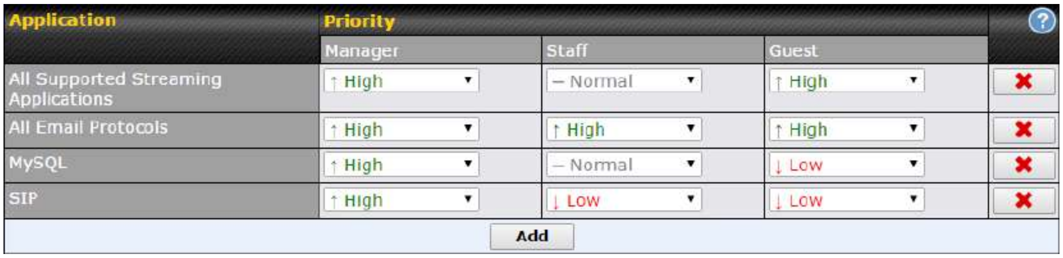
You can choose whether to apply the same prioritization settings to all user groups or customize the settings for each group.



Application Prioritization

● Apply same settings to all users
○ Customize

Three priority levels can be set for application prioritization: ↑**High**,— **Normal**, and↓**Low**. The Peplink Balance can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference of supported applications is placed at the top of the table. Custom applications are at the bottom.

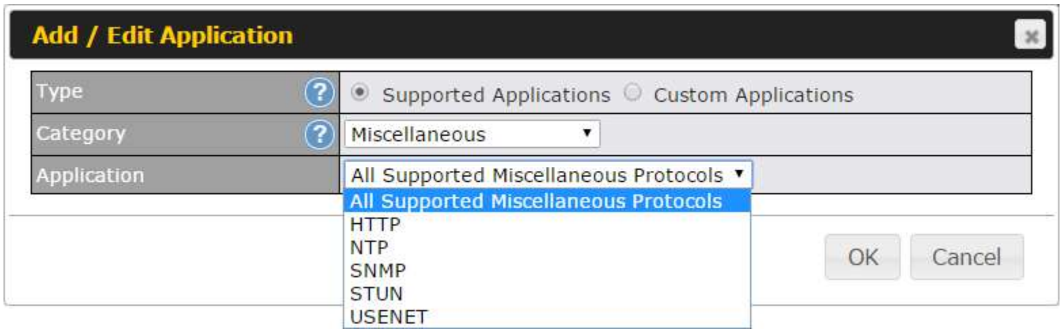


Application	Priority			
	Manager	Staff	Guest	
All Supported Streaming Applications	↑ High	– Normal	↑ High	✖
All Email Protocols	↑ High	↑ High	↑ High	✖
MySQL	↑ High	– Normal	↓ Low	✖
SIP	↑ High	↓ Low	↓ Low	✖

Prioritization for Custom Application

Click the **Add** button to define a custom application. Click the button ✖ in the **Action** column to delete the custom application in the corresponding row.

When **Supported Applications** is selected, the Peplink Balance will inspect network traffic and prioritize the selected applications. Alternatively, you can select **Custom Applications** and define the application by providing the protocol, scope, port number, and DSCP value.



Add / Edit Application

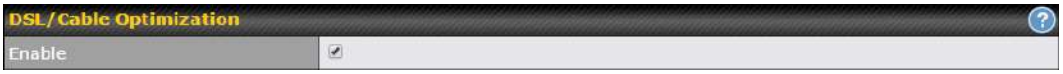
Type	● Supported Applications ○ Custom Applications
Category	Miscellaneous
Application	All Supported Miscellaneous Protocols

Category and **Application** availability will be different across different Peplink Balance models.

DSL/Cable Optimization

DSL/cable-based WAN connections have lower upload bandwidth and higher download bandwidth.

When a DSL/cable circuit's uplink is congested, the download bandwidth will be affected. Users will not be able to download data at full speed until the uplink becomes less congested. **DSL/Cable Optimization** can relieve such an issue. When it is enabled, the download speed will become less affected by the upload traffic. By default, this feature is enabled.



DSL/Cable Optimization	
Enable	☑

10.11 Firewall

A firewall is a mechanism that selectively filters data traffic between the WAN side (the Internet) and the LAN side of the network. It can protect the local network from potential hacker attacks, access to offensive websites, and/or other inappropriate uses.

The firewall functionality of Peplink Balance supports the selective filtering of data traffic in both directions:

Outbound (LAN to WAN)
Inbound (WAN to LAN)
Internal Network (VLAN to VLAN)

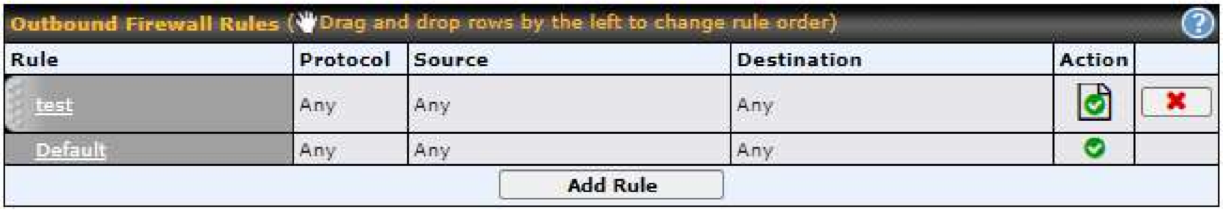
The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

With SpeedFusion^{TM} enabled, the firewall rules also apply to VPN tunneled traffic. The Firewall function can be found at **Network>Firewall**

10.11.1 Access Rules

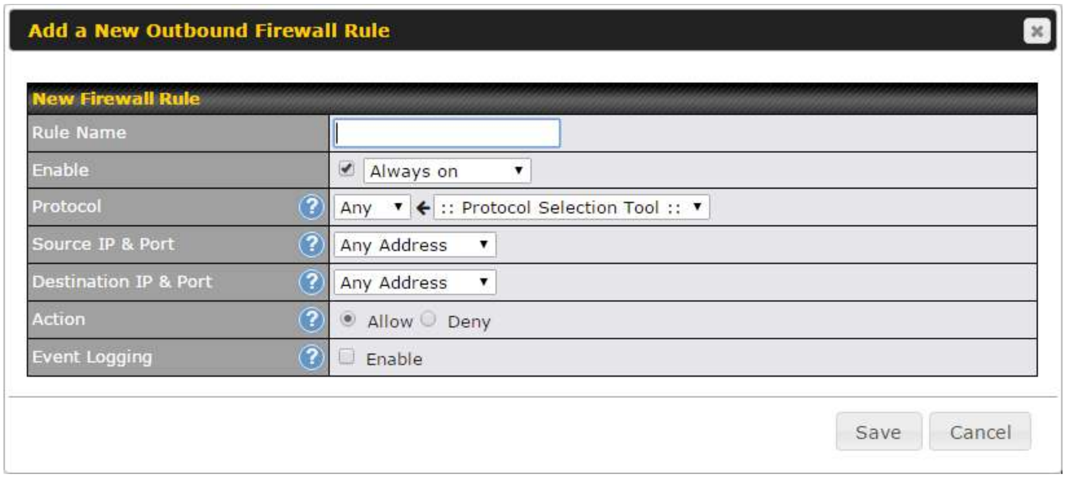
The outbound firewall settings are located at **Network>Firewall>Access Rules**.



Outbound Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any	✓	✗
Default	Any	Any	Any	✓	

Click **Add Rule** to display the following screen:

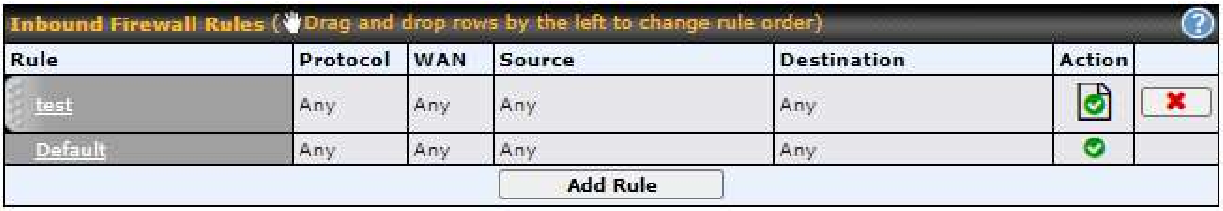


Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☑ Always on
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	● Allow ○ Deny
Event Logging	□ Enable

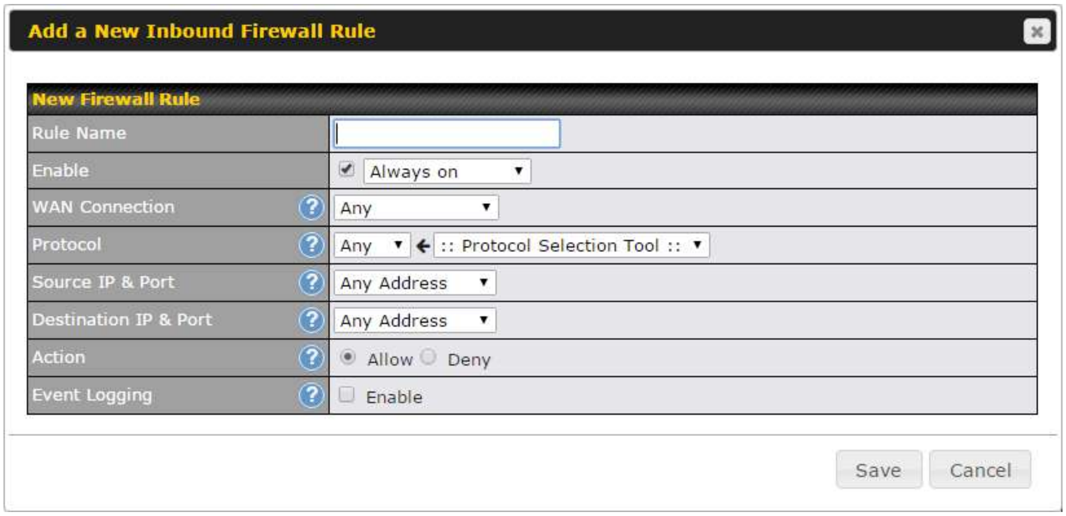
The inbound firewall settings are located at **Network>Firewall>Access Rules**.



Inbound Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Protocol	WAN	Source	Destination	Action	
test	Any	Any	Any	Any	✓	✖
Default	Any	Any	Any	Any	✓	

Click **Add Rule** to display the following window:

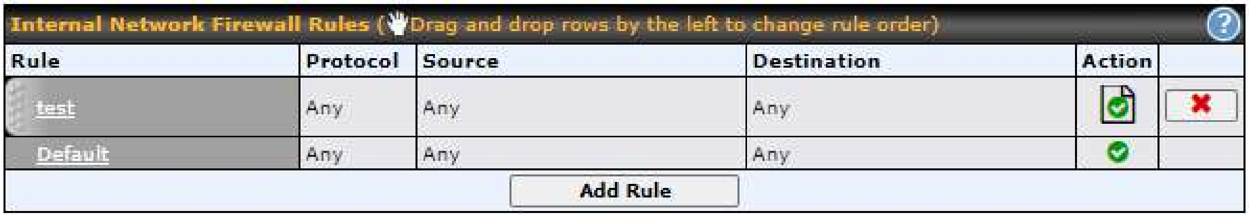


Add a New Inbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☑ Always on
WAN Connection	Any
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	● Allow ○ Deny
Event Logging	□ Enable

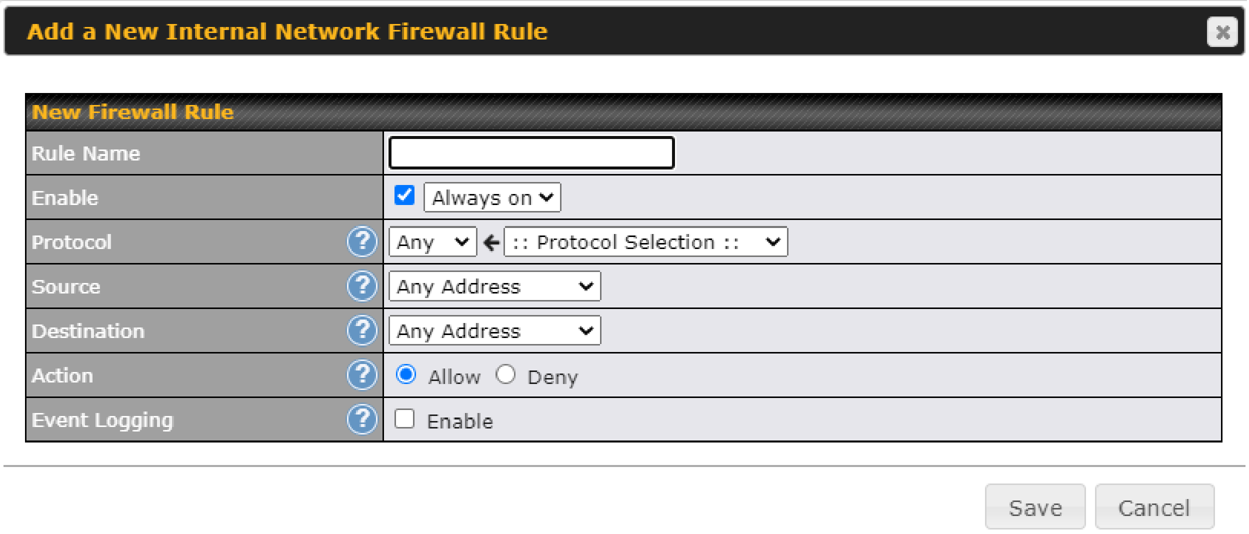
The Internal Network firewall settings are located at **Network>Firewall>Access Rules**.



Internal Network Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any	✓	✖
Default	Any	Any	Any	✓	

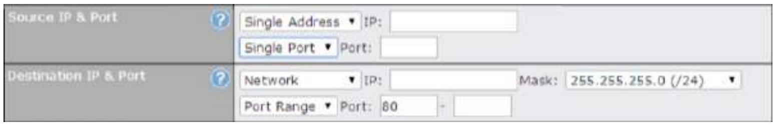
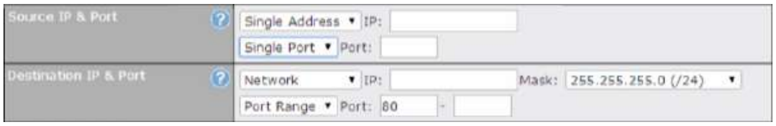
Click **Add Rule** to display the following window:



Add a New Internal Network Firewall Rule

New Firewall Rule	
Rule Name	
Enable	☑ Always on
Protocol	Any ← :: Protocol Selection ::
Source	Any Address
Destination	Any Address
Action	● Allow ○ Deny
Event Logging	☐ Enable

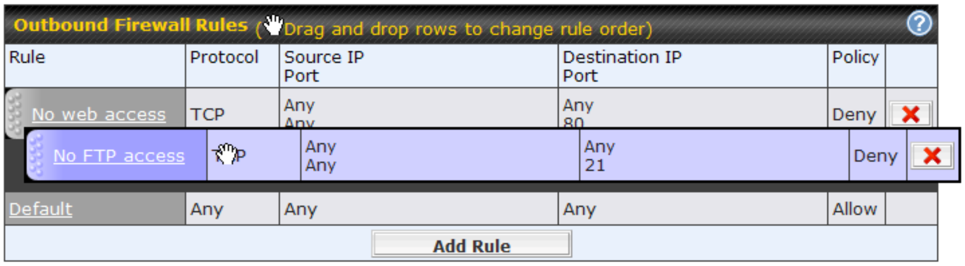
Inbound / Outbound / Internal Network Firewall Settings	
Rule Name	This setting specifies a name for the firewall rule.
Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by Peplink Balance based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule. Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: ● **Any** ● **TCP** ● **UDP** ● **ICMP** ● **DSCP** ● **IP** Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.
Source and	This specifies the source IP address(es) and port number(s) to be matched for the firewall

Port	rule. A single address, or a network, can be specified as the **Source IP & Port** setting, as indicated with the following screenshots:  Source IP & Port: Single Address ▾ IP: Single Port ▾ Port: Destination IP & Port: Network ▾ IP: Mask: 255.255.255.0 (/24) ▾ Port Range ▾ Port: 80 - In addition, a single port, or a range of ports, can be specified for the **Source** settings.
Destination and Port	This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Destination IP & Port** setting, as indicated with the following screenshots:  Source IP & Port: Single Address ▾ IP: Single Port ▾ Port: Destination IP & Port: Network ▾ IP: Mask: 255.255.255.0 (/24) ▾ Port Range ▾ Port: 80 - In addition, a single port, or a range of ports, can be specified for the settings.
Action	This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following: ● Source IP & port ● Destination IP & port With the value of **Allow** for the **Action** setting, the matching traffic passes through the router (to be routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the router (and is discarded).
Event Logging	This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows: Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80 ● **CONN:** The connection where the log entry refers to ● **SRC:** Source IP address ● **DST:** Destination IP address ● **LEN:** Packet length ● **PROTO:** Protocol ● **SPT:** Source port ● **DPT:** Destination port

Click **Save** to store your changes. To create an additional firewall rule, click **Add Rule** and repeat the above steps.

To change a rule's priority, simply drag and drop the rule:

- Hold the left mouse button on the rule.
- Move it to the desired position.
- Drop it by releasing the mouse button.



Outbound Firewall Rules (Drag and drop rows to change rule order)

Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No web access	TCP	Any Any	Any 80	Deny	✖
No FTP access	P	Any Any	Any 21	Deny	✖
Default	Any	Any	Any	Allow	

To remove a rule, click the ✖ button.

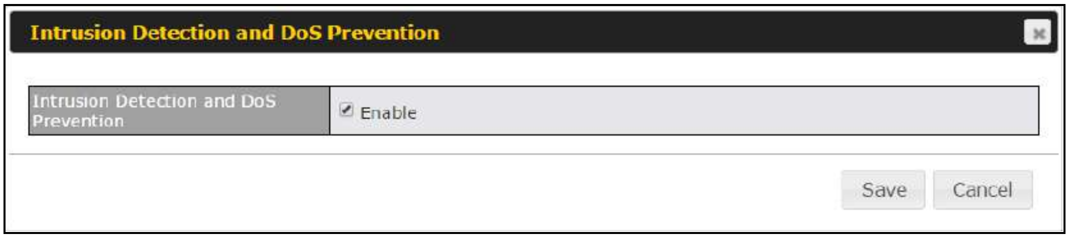
Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the **Default** rule will be applied.

The **Default** rule is **Allow** for Outbound, Inbound and Internal Network access.

Tip

If the default inbound rule is set to **Allow** for NAT-enabled WANs, no inbound Allow firewall rules will be required for inbound port forwarding and inbound NAT mapping rules. However, if the default inbound rule is set as **Deny**, a corresponding Allow firewall rule will be required.

Intrusion Detection and DoS Prevention



Intrusion Detection and DoS Prevention

Intrusion Detection and DoS Prevention	☑ Enable

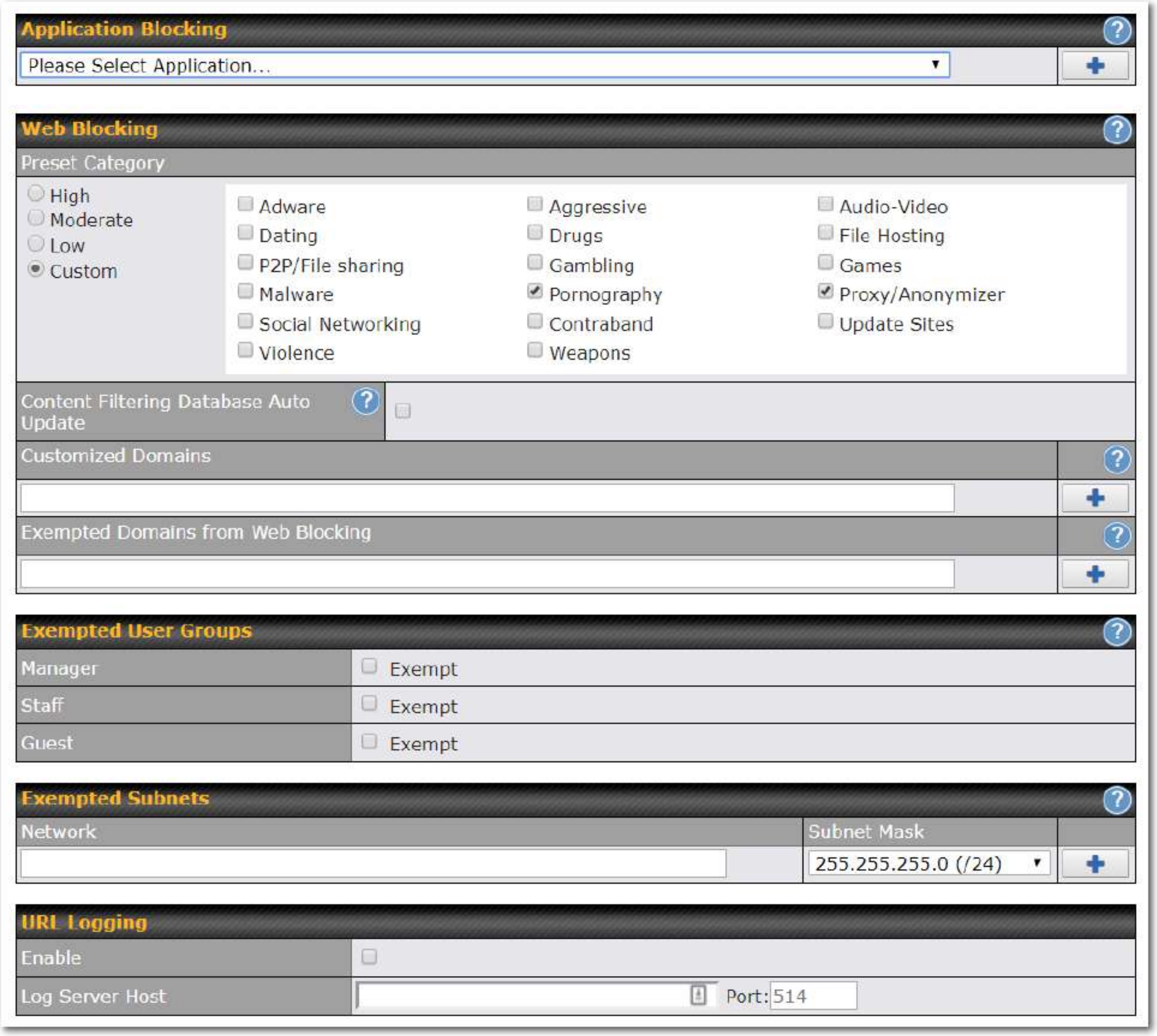
The Balance can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click ✎, check the **Enable** check box for the **Intrusion Detection and DoS Prevention**, and press the **Save** button.

When this feature is enabled, the Balance will detect and prevent the following kinds of intrusions and denial-of-service attacks.

- Port scan
    - NMAP FIN/URG/PSH
    - Xmas tree
    - Another Xmas tree
    - Null scan
    - SYN/RST
    - SYN/FIN

- SYN flood prevention
- Ping flood attack prevention

10.11.2 Content Blocking



Application Blocking

Please Select Application... ▾ +

Web Blocking

Preset Category

○ High
○ Moderate
○ Low
● Custom

□ Adware	□ Aggressive	□ Audio-Video
□ Dating	□ Drugs	□ File Hosting
□ P2P/File sharing	□ Gambling	□ Games
□ Malware	☑ Pornography	☑ Proxy/Anonymizer
□ Social Networking	□ Contraband	□ Update Sites
□ Violence	□ Weapons	

Content Filtering Database Auto Update □

Customized Domains +

Exempted Domains from Web Blocking +

Exempted User Groups

Manager	□ Exempt
Staff	□ Exempt
Guest	□ Exempt

Exempted Subnets

Network	Subnet Mask	
	255.255.255.0 (/24) ▾	+

URL Logging

Enable	□
Log Server Host	Port: 514

Application Blocking

Choose applications to be blocked from LAN/PPTP/PepVPN peer clients' access, except for those on the Exempted User Groups or Exempted Subnets defined below.

Web Blocking

Defines website domain names to be blocked from LAN/PPTP/PepVPN peer clients' access except for those on the Exempted User Groups or Exempted Subnets defined below.

If "foobar.com" is entered, any web site with a host name ending in foobar.com will be blocked, e.g. www.foobar.com, foobar.com, etc. However, "myfoobar.com" will not be blocked.

You may enter the wild card ".*" at the end of a domain name to block any web site with a host name having the domain name in the middle. If you enter "foobar.*", then "www.foobar.com", "www.foobar.co.jp", or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The device will inspect and look for blocked domain names on all HTTP and HTTPS traffic.

Customized Domains

Enter an appropriate website address, and the Peplink Balance will block and disallow LAN/PPTP/SpeedFusion^{TM} peer clients to access these websites. Exceptions can be added using the instructions in **Sections 21.2.1.4** and **21.2.1.5.**

You may enter the wild card ".*" at the end of a domain name to block any web site with a host name having the domain name in the middle. For example, If you enter "foobar.*," then "www.foobar.com," "www.foobar.co.jp," or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The Peplink Balance will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

Exempted User Groups

Check and select pre-defined user group(s) who can be exempted from the access blocking rules. User groups can be defined at **QoS>User Groups** section. Please refer to **Section 20.1** for details.

Exempted Subnets

With the subnet defined in the field, clients on the particular subnet(s) can be exempted from the access blocking rules.

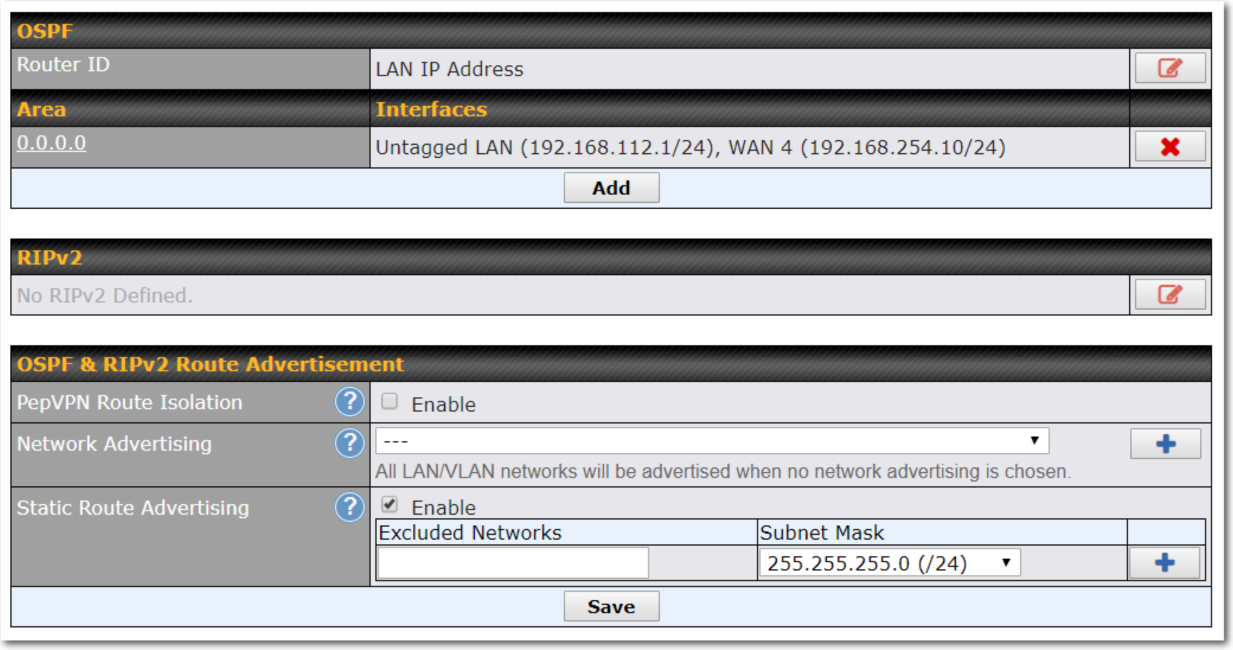
URL Logging

Click **enable**, and then enter the ip address and port (if applicable) where your remote syslog server is located.

10.12 Routing Protocols

10.12.1 OSPF & RIPv2

The Peplink Balance supports OSPF and RIPv2 dynamic routing protocols. Click the **Network** tab from the top bar, and then click the **Routing Protocols > OSPF & RIPv2** item on the sidebar to reach the following menu:

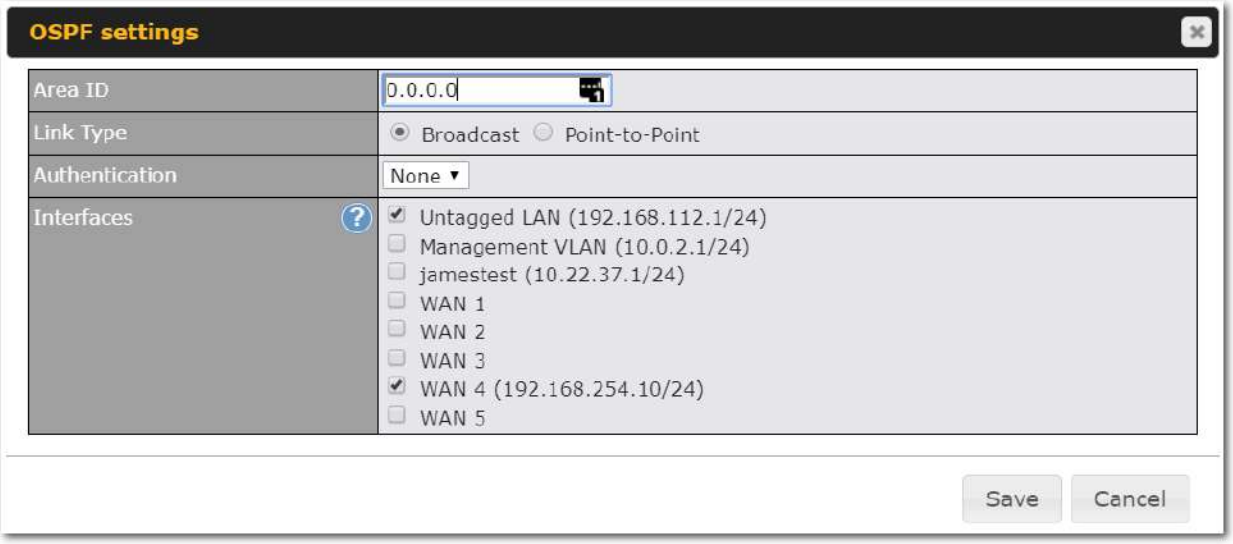


OSPF		
Router ID	LAN IP Address	
Area	**Interfaces**	
0.0.0.0	Untagged LAN (192.168.112.1/24), WAN 4 (192.168.254.10/24)	✖
	Add	

RIPv2
No RIPv2 Defined.

OSPF & RIPv2 Route Advertisement	
PepVPN Route Isolation ?	☐ Enable
Network Advertising ?	--- ▾ + All LAN/VLAN networks will be advertised when no network advertising is chosen.
Static Route Advertising ?	☑ Enable Excluded Networks / Subnet Mask 255.255.255.0 (/24) ▾ +
	Save

OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the WAN IP address. If you want to specify your own ID, enter it into the **Custom** field.
Area	This is an overview of the OSPF areas that you have defined. Clicking on the name under Area allows you to configure the connection. To define a new area, click Add. To delete an existing area, click on the ✖ .

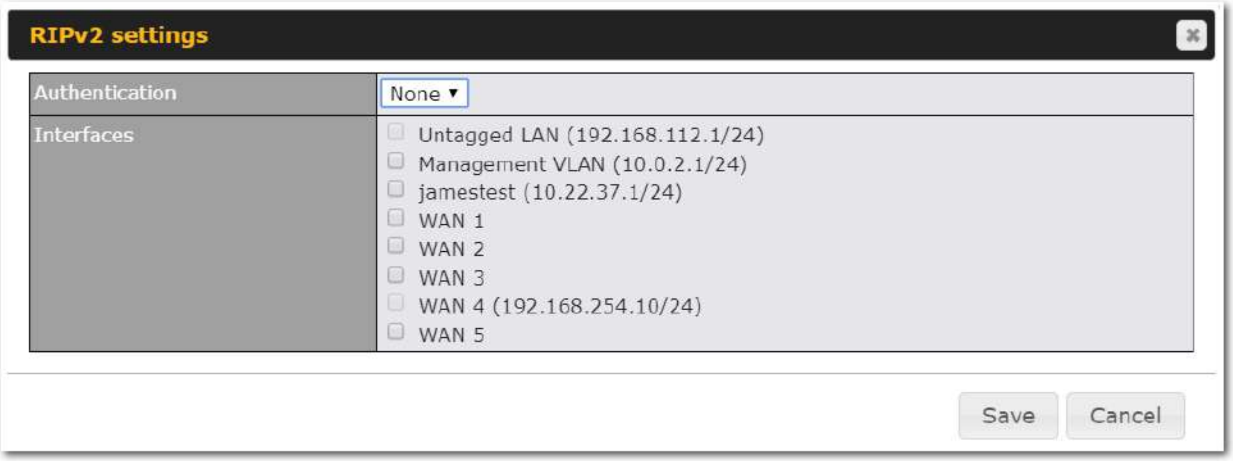


OSPF settings

Area ID	0.0.0.0
Link Type	● Broadcast ○ Point-to-Point
Authentication	None ▾
Interfaces	☑ Untagged LAN (192.168.112.1/24) □ Management VLAN (10.0.2.1/24) □ jamestest (10.22.37.1/24) □ WAN 1 □ WAN 2 □ WAN 3 ☑ WAN 4 (192.168.254.10/24) □ WAN 5

OSPF Settings	
Area ID	Assign a name to be applied to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore them.
Link Type	Choose the type of network that this area will use.
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are **MD5** and **Text**. Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver OSPF packets.

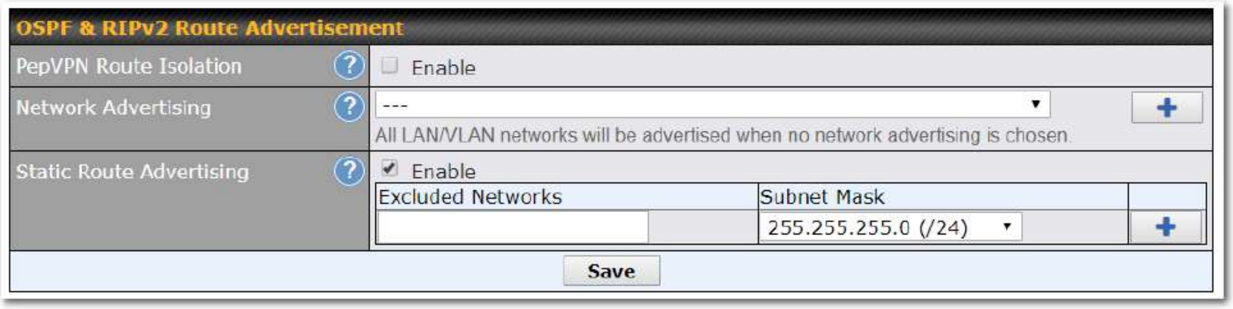
To access RIPv2 settings, click on .



RIPv2 settings

Authentication	None ▾
Interfaces	□ Untagged LAN (192.168.112.1/24) □ Management VLAN (10.0.2.1/24) □ jamestest (10.22.37.1/24) □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 (192.168.254.10/24) □ WAN 5

RIPv2 Settings	
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are **MD5** and **Text**. Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver RIPv2 packets.



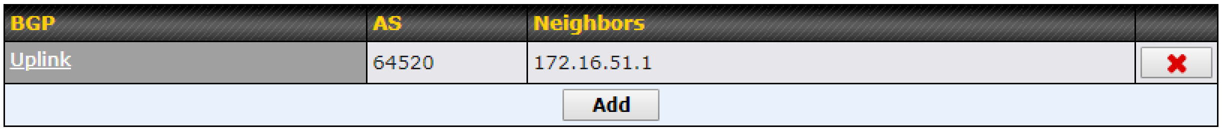
OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation	□ Enable
Network Advertising	--- ▾ All LAN/VLAN networks will be advertised when no network advertising is chosen
Static Route Advertising	☑ Enable Excluded Networks / Subnet Mask: 255.255.255.0 (/24) ▾

OSPF & RIPv2 Route Advertisement	
PepVPN Route Isolation	Isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption..
Network Advertising	Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.
Static Route Advertising	Enabling OSPF & RIPv2 Route Advertising allows it to advertise LAN static routes over OSPF & RIPv2. Static routes on the Excluded Networks table will not be advertised.

10.12.2 BGP

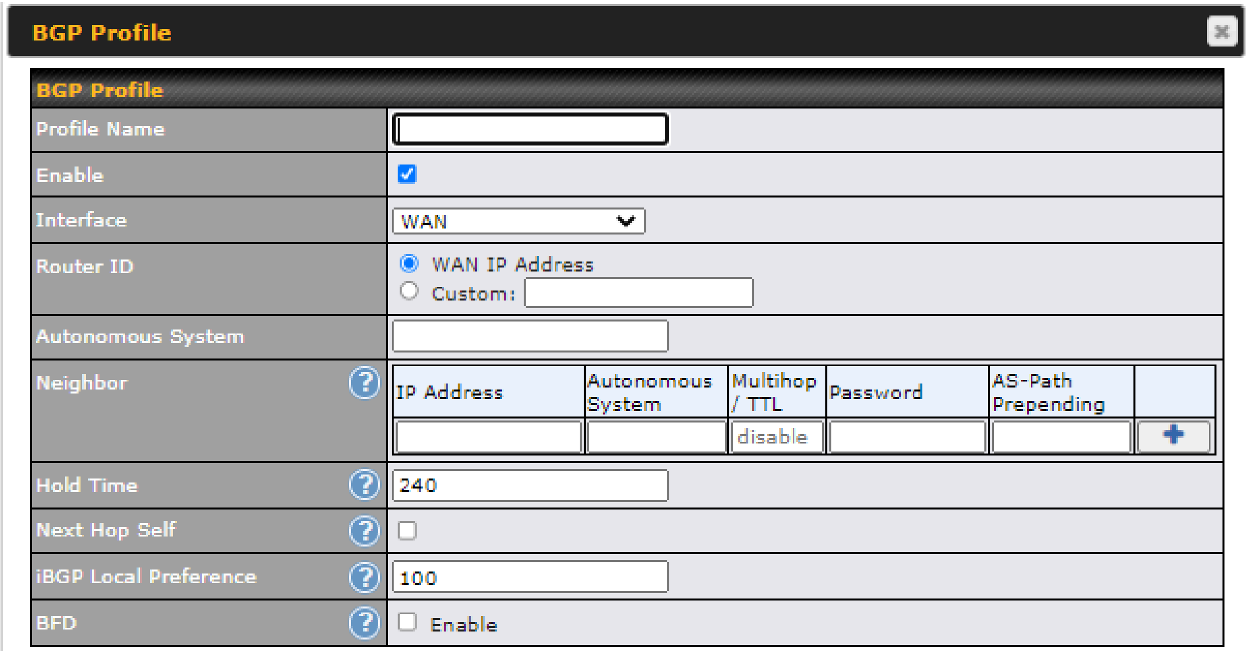
Click the **Network** tab along the top bar, and then click the **BGP** item on the sidebar to configure BGP.



BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	✖

Add

Click the "x" to delete a BGP profile.
Click "**Add**" to create a new BGP profile.

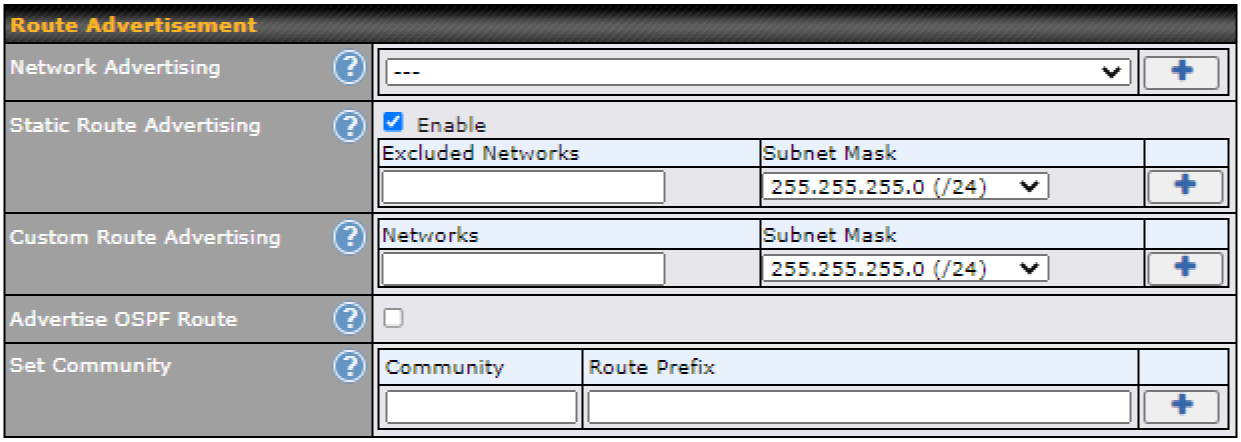


BGP Profile

BGP Profile	
Profile Name	
Enable	☑
Interface	WAN
Router ID	● WAN IP Address ○ Custom:
Autonomous System	
Neighbor ?	IP Address / Autonomous System / Multihop / TTL / Password / AS-Path Prepending disable
Hold Time ?	240
Next Hop Self ?	□
iBGP Local Preference ?	100
BFD ?	□ Enable

BGP	
Name	This field specifies the name that represents this profile.
Enable	When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled.
Interface	The interface in which the BGP neighbor is located.
Autonomous System	The Autonomous System Number (ASN) assigned to this profile.
Neighbor	BGP Neighbors and their details.
IP address	The IP address of the Neighbor.
Autonomous	The Neighbor's ASN.

System	
Multihop/TTL	This field determines the Time-to-live (TTL) of BGP packets. Leave this field blank if the BGP neighbor is directly connected, otherwise you must specify a TTL value. This option should be used if the configured Neighbor's IP address does not match the selected Interface's network subnets. The TTL value must be between 2 to 255.
Password	(Optional) Assign a password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this Neighbor. Values must be ASN and separated by commas. For example: inputting "64530,64531" will prepend "64530, 64531" to received routes.
Hold Time	Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240
Next Hop Self	Enable this option to advertise your own source address as the next hop when propagating routes.
iBGP Local Preference	This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively. Default: 100
BFD	Enable this option to add Bidirectional Forwarding Detection for path failure. All directly connected Neighbors that use the same physical interface share the same BFD settings. All mulithop Neighbors share the same multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled.

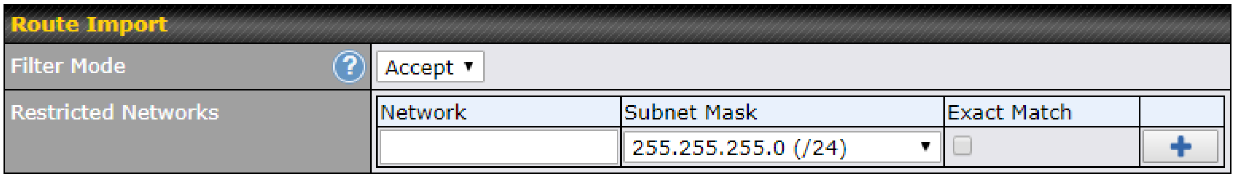


Route Advertisement

Network Advertising	---
Static Route Advertising	☑ Enable Excluded Networks: (blank) Subnet Mask: 255.255.255.0 (/24)
Custom Route Advertising	Networks: (blank) Subnet Mask: 255.255.255.0 (/24)
Advertise OSPF Route	□
Set Community	Community / Route Prefix

Route Advertisement	
Network Advertising	Select the Networks that will be advertised to the BGP Neighbor.
Static Route Advertising	Enable this option to advertise static LAN routes. Static routes that match the Excluded Networks table will not be advertised.

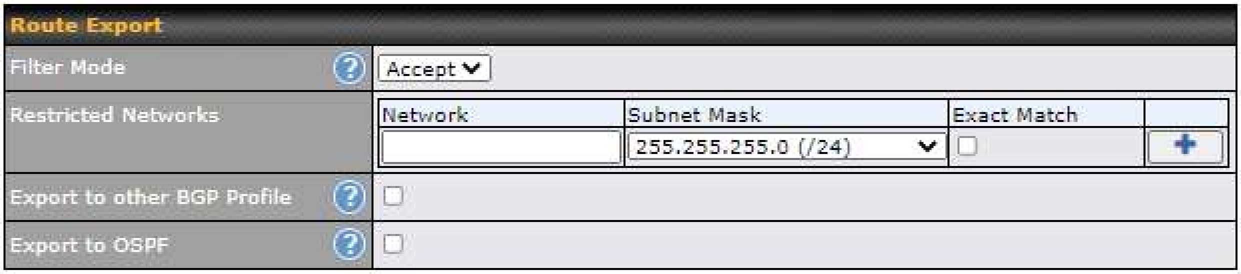
Custom Route Advertising	Additional routes to be advertised to the BGP Neighbor.
Advertise OSPF Route	When this box is checked, every learnt OSPF route will be advertised.
Set Community	Assign a prefix to a Community Community: Two numbers in new-format. e.g. 65000:21344 Well-known communities: no-export 65535:65281 no-advertise 65535:65282 no-export-subconfed 65535:65283 no-peer 65535:65284 Route Prefix: Comma separated networks. e.g. 172.168.1.0/24,192.168.1.0/28



Route Import

Filter Mode	Accept ▾
Restricted Networks	Network: (empty) · Subnet Mask: 255.255.255.0 (/24) ▾ · Exact Match: □ · +

Route Import Settings	
Filter Mode	This field allows for the selection of the filter mode for route import. **None**: All BGP routes will be accepted. **Accept**: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected. **Reject**: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.
Restricted Networks	This field specifies the network(s) in the “route import” entry. **Exact Match:** When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.



Route Export

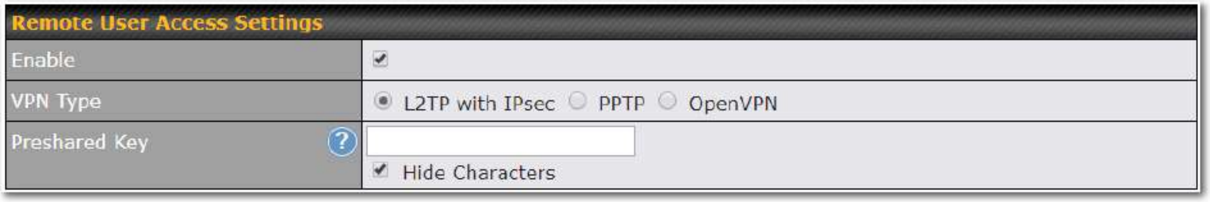
Filter Mode	Accept
Restricted Networks	Network: Subnet Mask: 255.255.255.0 (/24) Exact Match: □
Export to other BGP Profile	□
Export to OSPF	□

Filter Mode	This field allows for the selection of the filter mode for route export. **None**: All BGP routes will be accepted. **Accept**: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected. **Reject**: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.
Restricted Networks	This field specifies the network(s) in the “route export” entry. **Exact Match:** When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.
Export to other BGP Profile	When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.
Export to OSPF	When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.

10.13 Remote User Access

A remote-access VPN connection allows an individual user to connect to a private business network from a remote location using a laptop or desktop computer connected to the Internet. Networks routed by a Peplink router can be remotely accessed via OpenVPN, L2TP with IPsec or PPTP. To configure this feature, navigate to **Network > Remote User Access** and choose the required VPN type.

10.13.1 L2TP with IPsec

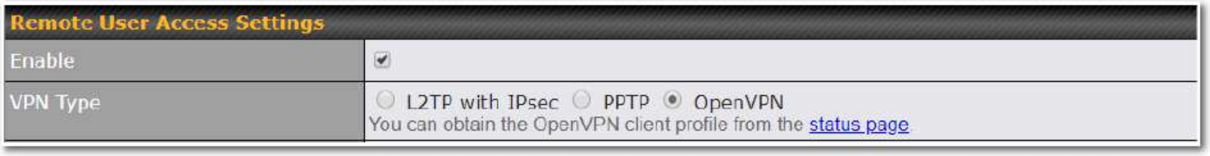


Remote User Access Settings	
Enable	☑
VPN Type	● L2TP with IPsec ○ PPTP ○ OpenVPN
Preshared Key	☑ Hide Characters

L2TP with IPsec Remote User Access Settings	
Pre-shared Key	Enter your pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
Listen On	This setting is for specifying the WAN IP addresses that allow remote user access.
Disable Weak Ciphers	Click the ? button to show and enable this option. When checked, weak ciphers such as 3DES will be disabled.

Continue to configure the authentication method.

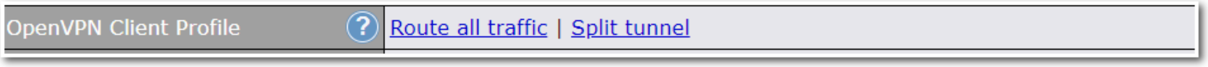
10.13.2 OpenVPN



Remote User Access Settings	
Enable	☑
VPN Type	○ L2TP with IPsec ○ PPTP ● OpenVPN You can obtain the OpenVPN client profile from the status page

Select OpenVPN and continue to configure the authentication method.

The OpenVPN Client profile can be downloaded from the **Status > device** page after the configuration has been saved.



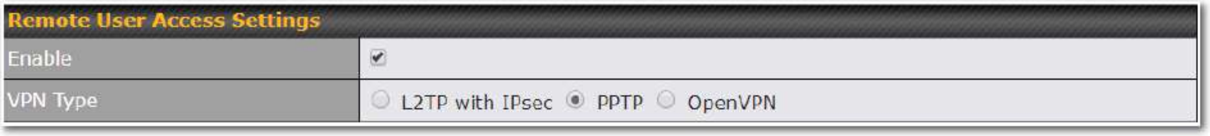
OpenVPN Client Profile	Route all traffic | Split tunnel

You have a choice between 2 different OpenVPN Client profiles:

Option 1: "Route all traffic" profile
Using this profile, VPN clients will send all the traffic through the OpenVPN tunnel

Option 2: "Split tunnel" profile
Using this profile, VPN clients will ONLY send those traffic designated to the untagged LAN and VLAN segment through the OpenVPN tunnel.

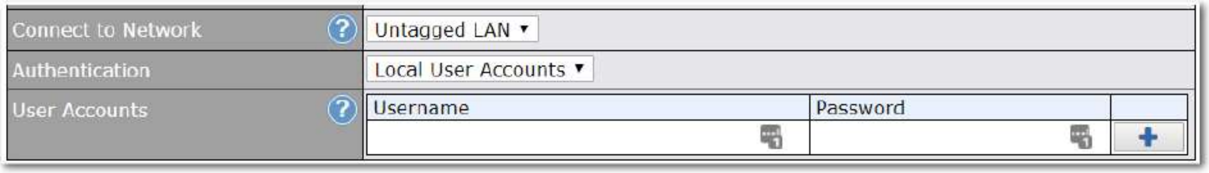
10.13.3 PPTP



Remote User Access Settings	
Enable	☑
VPN Type	○ L2TP with IPsec ● PPTP ○ OpenVPN

No additional configuration required.
The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private networks. PPTP has many well known security issues
Continue to configure authentication methods.

10.13.4 Authentication Methods



Connect to Network ?	Untagged LAN ▾
Authentication	Local User Accounts ▾
User Accounts ?	Username | Password | +

Authentication Method	
Connect to Network	Select the VLAN network for remote users to enable remote user access on.
Authentication	Determine the method of authenticating remote users

User accounts:

This setting allows you to define the Remote User Accounts.
Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password.

Note:

The username must contain lowercase letters, numerics, underscore(_), dash(-), at sign(@), and period(.) only.