



AXXESSMARINE



PEPWAVE MAX BR1 Pro LTEA

AXXESS MARINE

support@axxess-marine.com

Phone: +1 954 354 2077

www.axxess-marine.com



SUMMARY

Pepwave MAX BR1 Pro LTEA	3
Network Settings	3
Grouped Networks	5
Outbound Policy	5
Access Rules	7
Content Blocking	8
Bandwidth Control	9
Usage Reports	10

PEPWAVE MAX BR1 PRO LTEA

To access the Pepwave MAX BR1 PRO LTEA dashboard, type the Gateway on your browser and fill user/password to access the Peplink's main page. (Example: 192.168.50.1).

The screenshot displays the Pepwave MAX BR1 PRO LTEA dashboard with the following sections:

- WAN Connection Status:**
 - Priority 1 (Highest): Connected to LTE-A R A. Status: Connected. Details button.
 - Priority 2: Drag desired (Priority 2) connections here.
 - Disabled:
 - WAN: Disabled. Details button.
 - Wi-Fi WAN: Disabled. Details button.
- LAN Interface:** Router IP Address: 192.168.50.1
- Wi-Fi AP:** ON. Details button.
- Map:** Shows the location of the device in the Caribbean region, with coordinates 52.685108° N 5.948605° E. Labeled islands include Puerto Rico, British Virgin Islands, United States Virgin Islands, Anguilla, Sint Maarten, Saint-Barthélemy, Saba, Saint Kitts and Nevis, Antigua and Barbuda, and Montserrat.
- Device Information:**
 - Model: Pepwave MAX BR1 Pro
 - Firmware: 8.1.0 build 4941
 - Uptime: 9 days 5 hours 52 minutes
 - CPU Load: 12%
 - Throughput: ↓ 19.0 kbps ↑ 50.0 kbps

Network Settings

In this session, you can create and manage your Virtual LANs to define some settings and controls within your network.

Go to your Pepwave's webpage, click on **Network**, **Network Settings** and you can see your Virtual LANs.

PEPWAVE Dashboard SpeedFusion Cloud **Network** Advanced AP System Status Apply Changes

LAN

- Network Settings
- Port Settings
- Captive Portal

WAN

This configuration is being managed by [InControl](#).

LAN	VLAN	Network	
Untagged LAN	None	192.168.50.1/24	
Management VLAN	1	10.0.1.1/24	✖

New LAN

Static Route Settings

Static Route	Destination Network	Subnet Mask	Gateway	
		255.255.255.0 (/24)		+

DNS Proxy Settings

Enable	<input checked="" type="checkbox"/>						
DNS Caching	<input type="checkbox"/>						
Include Google Public DNS Servers	<input type="checkbox"/>						
Local DNS Records	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>+</td> </tr> </tbody> </table>	Host Name	IP Address				+
Host Name	IP Address						
		+					

Save

PEPWAVE Dashboard SpeedFusion Cloud **Network** Advanced AP System Status Apply Changes

LAN

- Network Settings
- Port Settings
- Captive Portal

WAN

LAN

IP Settings

IP Address	192.168.50.1	255.255.255.0 (/24)
------------	--------------	---------------------

Network Settings

Name	
Inter-VLAN routing	<input checked="" type="checkbox"/>

Drop-In Mode Settings

Enable	<input type="checkbox"/>
--------	--------------------------

DHCP Server

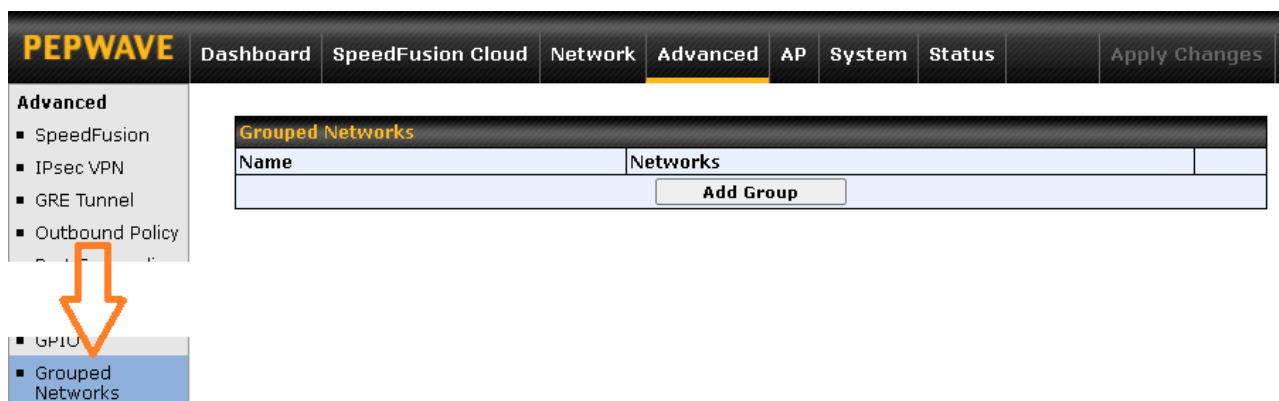
DHCP Server	<input checked="" type="checkbox"/> Enable								
DHCP Server Logging	<input type="checkbox"/>								
IP Range	192.168.50.10 - 192.168.50.250 255.255.255.0 (/24)								
Lease Time	1 Days 0 Hours 0 Mins								
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically								
BOOTP	<input type="checkbox"/>								
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2">No Extended DHCP Option</td> </tr> <tr> <td colspan="2">Add</td> </tr> </tbody> </table>	Option	Value	No Extended DHCP Option		Add			
Option	Value								
No Extended DHCP Option									
Add									
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>00:00:00:00:00:00</td> <td></td> <td>+</td> </tr> </tbody> </table>	Name	MAC Address	Static IP			00:00:00:00:00:00		+
Name	MAC Address	Static IP							
	00:00:00:00:00:00		+						

Save Cancel

All changes must be **saved** and **applied**.

Grouped Networks

In this session you can Add, Set and Edit your network groups to improve your management inside the internet in your Yacht. To do this, go to **Advanced**, scroll down and click on **Grouped Networks**, choose a name and the IP addresses that will participate in that group.

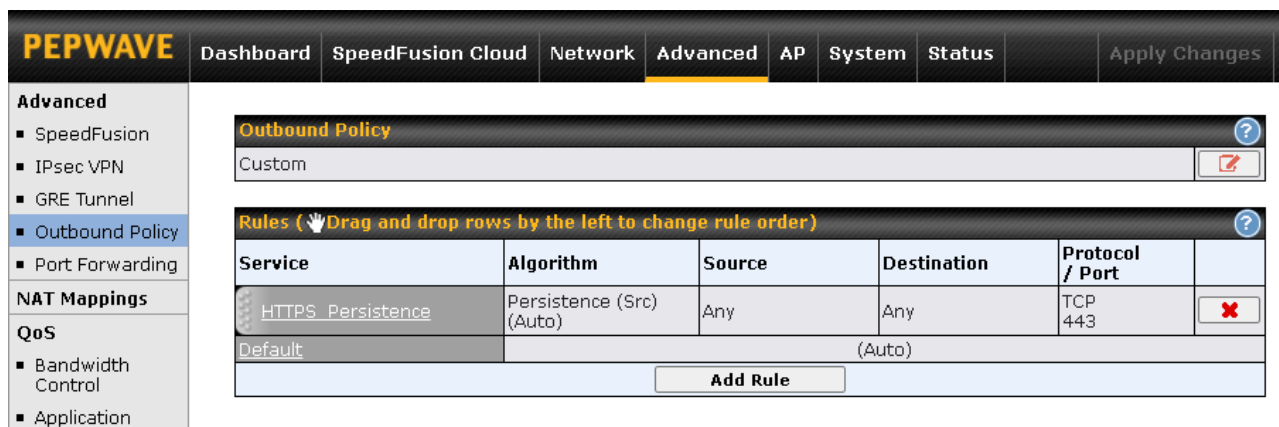


The screenshot shows the PEPWAVE web interface. The top navigation bar includes 'Dashboard', 'SpeedFusion Cloud', 'Network', 'Advanced' (highlighted), 'AP', 'System', 'Status', and 'Apply Changes'. The left sidebar shows the 'Advanced' menu with options: SpeedFusion, IPsec VPN, GRE Tunnel, Outbound Policy, and 'Grouped Networks' (highlighted with a blue background and an orange arrow pointing to it). The main content area is titled 'Grouped Networks' and contains a table with a header 'Name' and a value 'Networks'. Below the table is an 'Add Group' button.

All changes must be **saved** and **applied**.

Outbound Policy

You can define customized rules to manage the outbound traffic behavior. The rule Default will be applied to traffic that does not match with any higher precedence rules.

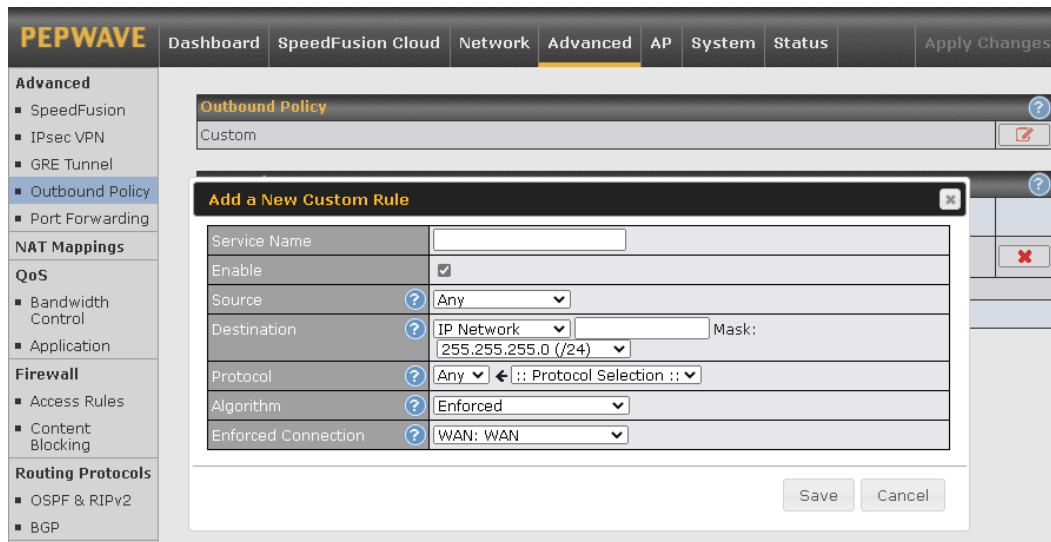


The screenshot shows the PEPWAVE web interface. The top navigation bar includes 'Dashboard', 'SpeedFusion Cloud', 'Network', 'Advanced' (highlighted), 'AP', 'System', 'Status', and 'Apply Changes'. The left sidebar shows the 'Advanced' menu with options: SpeedFusion, IPsec VPN, GRE Tunnel, 'Outbound Policy' (highlighted with a blue background), Port Forwarding, NAT Mappings, and QoS. The main content area is titled 'Outbound Policy' and shows a 'Custom' policy. Below it is a table of rules with the following columns: Service, Algorithm, Source, Destination, and Protocol / Port. The table contains one rule named 'HTTPS_Persistence' and a 'Default' rule. An 'Add Rule' button is visible at the bottom.

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

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 or the existent rule to make changes.



This field allows you to choose the WAN selection algorithm.

Weighted Balance - Traffic will be proportionally distributed among available WAN connections according to the specified load distribution weight;

Persistence - Traffic coming from the same machine will be persistently routed through the same WAN connection;

Enforced - Traffic will be routed through the specified connection regardless of the connection's health status;

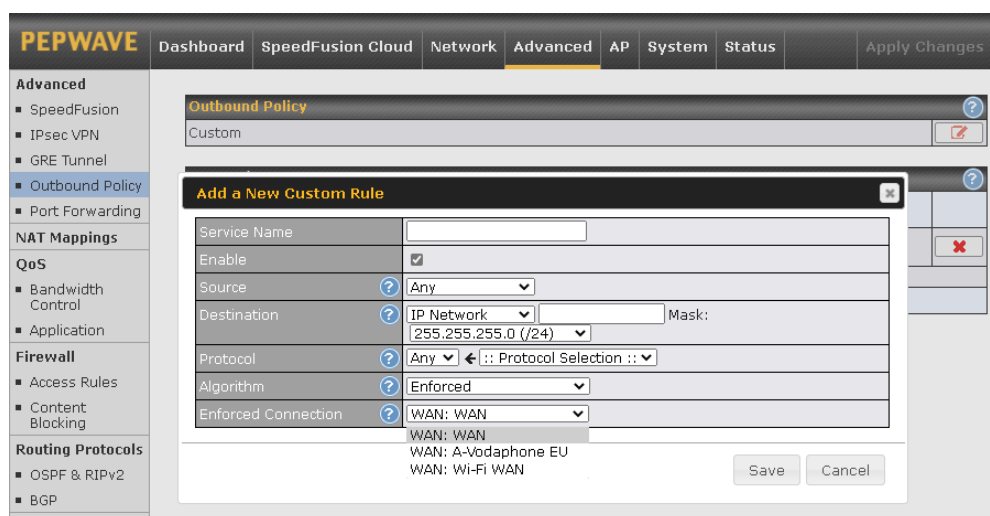
Priority - Traffic will be routed through the healthy connection that has the highest priority;

Overflow - Traffic 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;

Least Used - Traffic will be routed through the healthy WAN connection that is selected in the field Connection and has the most available downlink bandwidth;

Lowest Latency - Latency checking packets will be periodically sent to all selected healthy connections. Latency will then be determined by the response time of the second and third hops. New traffic will then be routed to a healthy connection with the lowest average latency during that detection period;

Fastest Response Time - Traffic will be duplicated and sent to all selected healthy connections. The connection with the earliest response will be used to send all further traffic from the session for the fastest possible response time. If there are any slower responses received from other connection afterwards, they will be discarded. As a result, this algorithm selects the most responsive connection on a per session basis.



This setting mean all the users in Grouped Network XYZ will be **enforced** to use the WAN.

This forces this network to use VSAT connections (for example).

Access Rules

You can create rules to deny an internet group or a specifically person. To do this, go to **Advanced, Access Rules, Internal Network Firewall Rules** and click on **Add Rule**.

The screenshot shows the PEPWAVE Advanced configuration interface. The left sidebar contains a navigation menu with the following items: Advanced (SpeedFusion, IPsec VPN, GRE Tunnel, Outbound Policy, Port Forwarding), NAT Mappings, QoS (Bandwidth Control, Application), Firewall (Access Rules, Content Blocking), Routing Protocols (OSPF & RIPv2, BGP), Remote User Access, and Misc. Settings (High Availability). The main content area displays several rule configuration sections:

- Outbound Firewall Rules:** A table with columns: Rule (Default), Protocol (Any), Source (Any), Destination (Any), Action (checked), and a status icon. An "Add Rule" button is below.
- Inbound Firewall Rules:** A table with columns: Rule (Default), Protocol (Any), WAN (Any), Source (Any), Destination (Any), Action (checked), and a status icon. An "Add Rule" button is below.
- Internal Network Firewall Rules:** A table with columns: Rule (Default), Protocol (Any), Source (Any), Destination (Any), Action (checked), and a status icon. An "Add Rule" button is below.
- Intrusion Detection and DoS Prevention:** A section with a "Disabled" status and a refresh icon.
- Local Service Firewall Rules:** A table with columns: Rule (Default), Service (Any), WAN (Any), Source (Any), Action (checked), and a status icon. An "Add Rule" button is below.

The screenshot shows the "Edit a Firewall Rule" dialog box. The "New Firewall Rule" section contains the following configuration:

- Rule Name:** Block Users to Ship
- Enable:**
- Protocol:** Any (with a help icon and a dropdown menu)
- Source:** Grouped Network (dropdown) and User WIFI Networks (dropdown)
- Destination:** Network (dropdown), IP: (input field), Mask: 255.255.255.0 (/24) (dropdown)
- Action:** Allow Deny
- Event Logging:** Enable


A blue arrow points to the "Event Logging" checkbox. At the bottom right, there are "Save" and "Cancel" buttons.

This rule example means when its allowed, all users tagged with **User WIFI Networks** into the **Grouped Networks** will be unable to use internet.

Content 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.

You can block Audio/Video Streaming, Pornography, Database, Email, File Sharing and others applications into the Pepwave. To do this, click on **Advanced, Content Blocking**, mark the applications and categories, mark or unmark the exempted users and/or groups.

To Block a specifically website, you should click on **Customized Domains**, fill with the domain. Examples: **facebook.* youtube.*** and click on .

All changes must be **saved** and **applied**.

Example: How to block **Netflix** to **Crew Network**:

Go to **Advanced, Content Blocking** and in the session **Customized Domains**, type:

nflximg.*

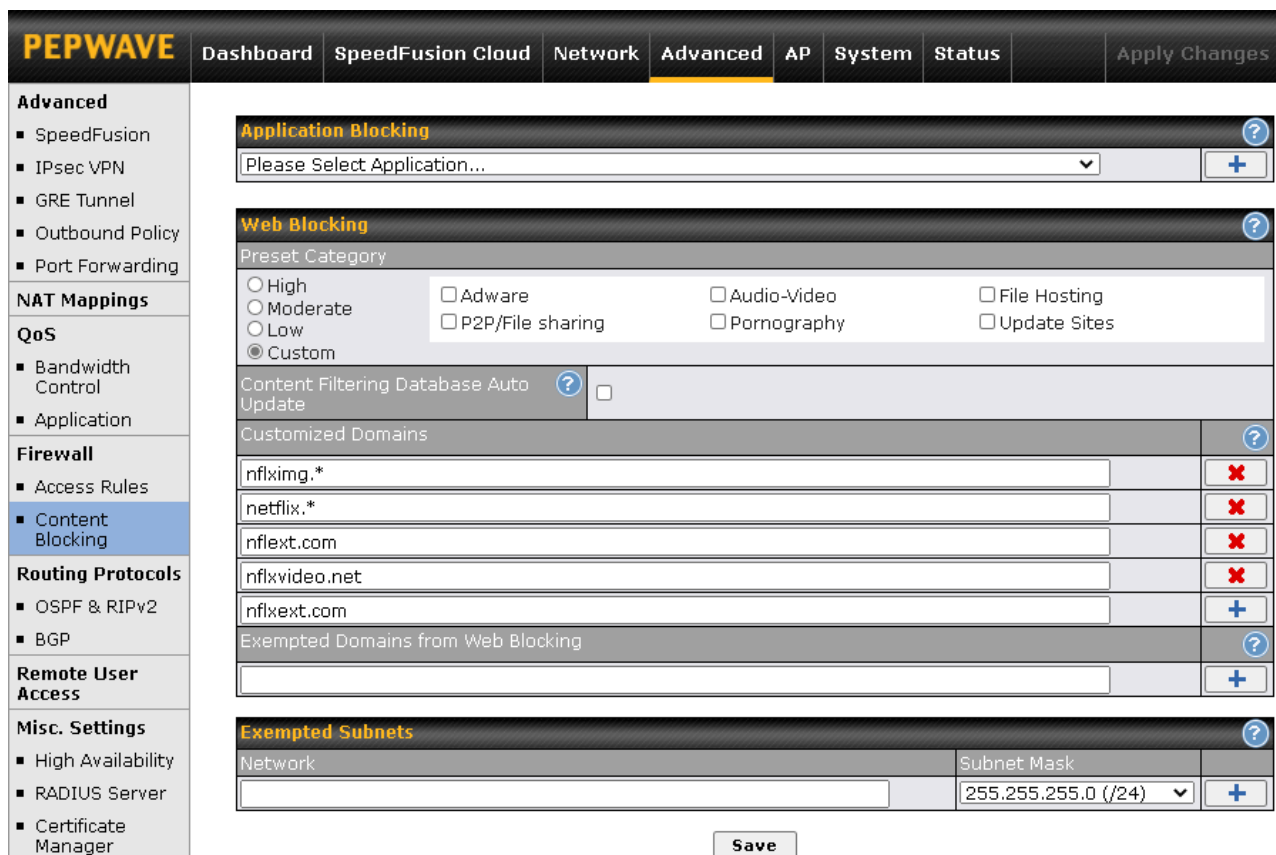
netflix.*

nflxext.com

nflxvideo.net

nflxext.com

When available, mark **Manager** and **Guest** as **Exempted User Groups**, **Save** and click on **Apply Changes**.



PEPWAVE Dashboard SpeedFusion Cloud Network **Advanced** AP System Status Apply Changes

Advanced

- SpeedFusion
- IPsec VPN
- GRE Tunnel
- Outbound Policy
- Port Forwarding

NAT Mappings

QoS

- Bandwidth Control
- Application

Firewall

- Access Rules
- Content Blocking**

Routing Protocols


- OSPF & RIPv2
- BGP

Remote User Access

Misc. Settings

- High Availability
- RADIUS Server
- Certificate Manager

Application Blocking

Please Select Application... 

Web Blocking


Preset Category


High Adware Audio-Video File Hosting






Moderate P2P/File sharing Pornography Update Sites


Low


Custom


Content Filtering Database Auto Update 


Customized Domains 

nflximg.*	
netflix.*	
nflxext.com	
nflxvideo.net	
nflxext.com	

Exempted Domains from Web Blocking 

	
--	---

Exempted Subnets 

Network	Subnet Mask
	255.255.255.0 (/24) 

Save

Bandwidth Control

Using the Peplink you can define how much minimum bandwidth will be reserved to each user when a WAN connection is in full load **or/and** you can define a maximum download speed will be reserved for each WAN connection.

To do this, go to **Advanced, Bandwidth Control**, mark **Enable** and set the Download and Upload for your users. Example:

Individual Bandwidth Limit	
Enable	<input checked="" type="checkbox"/>
User Bandwidth Limit	Download: <input type="text" value="1"/> Mbps Upload: <input type="text" value="500"/> kbps (0: unlimited)
<input type="button" value="Save"/>	

These settings mean all the Users will be limited to use 1Mbps (Download) and 500kbps (Upload).

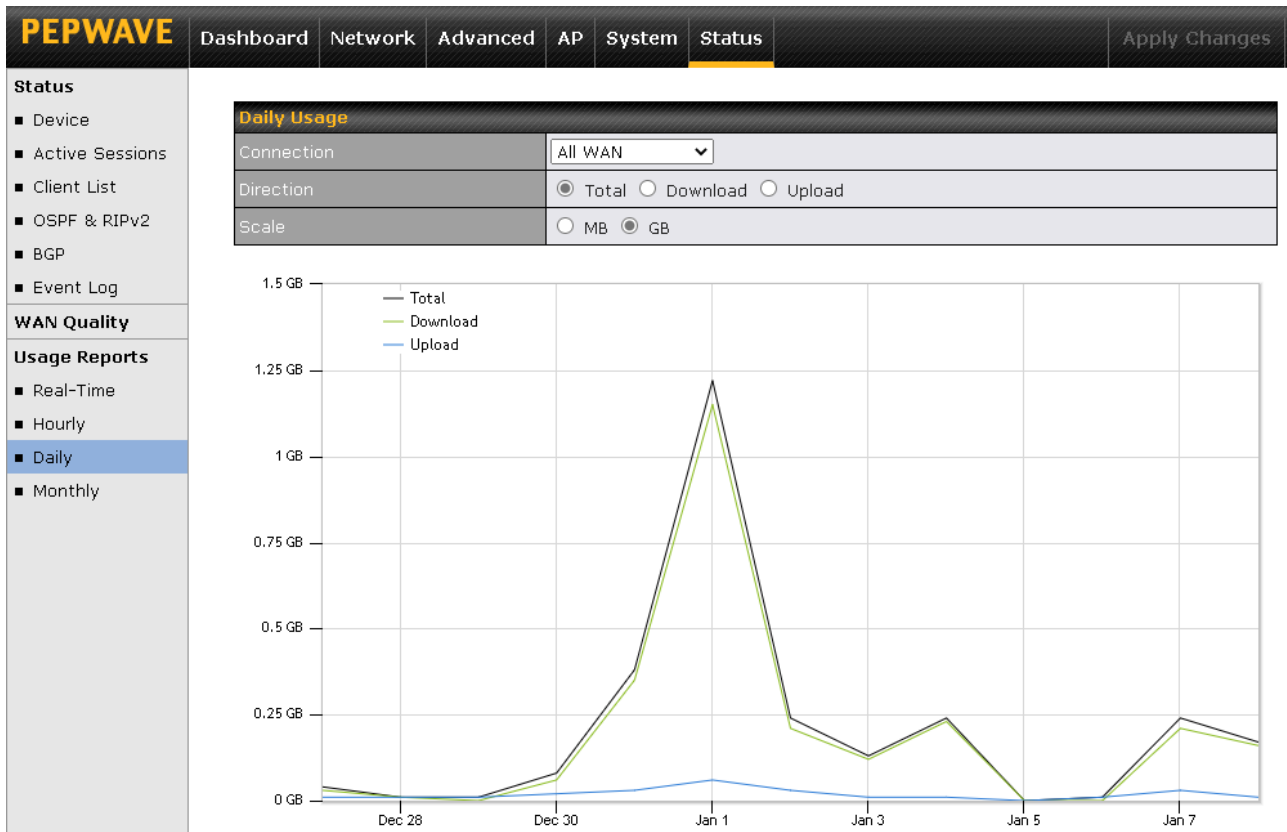
After to defining all groups, click on **Bandwidth Control** and check the best option for you and change the settings according to your needs.

All changes must be **saved** and **applied**.

Usage Reports

Your Peplink is able to show you all the internet usage in different times (Real time, Hourly, Daily and Monthly). You can see how much download each user made in these different times. To see these informations, go to **Status** and click on **Real time**, **Hourly**, **Daily** or **Monthly**.

Example: You click in **Daily** and see a usage graph:



Scrolling down and you see the usage total per day (figure below left), clicking in a day, you can see details about this day (figure below right):

Date	Download	Upload	Total
2021-01-08	0.16 GB	0.01 GB	0.17 GB
2021-01-07	0.21 GB	0.03 GB	0.24 GB
2021-01-06	0 GB	0.01 GB	0.01 GB
2021-01-05	0 GB	0 GB	0 GB
2021-01-04	0.23 GB	0.01 GB	0.24 GB
2021-01-03	0.12 GB	0.01 GB	0.13 GB
2021-01-02	0.21 GB	0.03 GB	0.24 GB
2021-01-01	1.15 GB	0.06 GB	1.22 GB
2020-12-31	0.35 GB	0.03 GB	0.38 GB
2020-12-30	0.06 GB	0.02 GB	0.08 GB
2020-12-29	0 GB	0.01 GB	0.01 GB
2020-12-28	0.01 GB	0.01 GB	0.01 GB
2020-12-27	0.03 GB	0.01 GB	0.04 GB

Current Month	
Down	2.09 GB
Up	0.16 GB
Total	2.25 GB

** If you want to make changes, we are here (Support Phone and [Portal](#)) to help if you have problems. But also if you want to change something, you can always ask us and we can do it remotely.*