



AXXESSMARINE



# PEPLINK MEDIAFAST 500

**AXXESS MARINE**

[support@axxess-marine.com](mailto:support@axxess-marine.com)

Phone: +1 954 354 2077

[www.axxess-marine.com](http://www.axxess-marine.com)



# SUMMARY

Peplink MEDIAFAST 500	3
Network Settings	3
Grouped Networks	4
Outbound Policy	5
Access Rules	7
Content Blocking	8
Bandwidth Control	9
Usage Reports	10

# PEPLINK MEDIAFAST 500

To access the Peplink MediaFast 500 dashboard, type the Gateway on your browser and fill user/password to access the Peplink's main page.

The screenshot shows the Peplink MediaFast 500 dashboard. The top navigation bar includes 'peplink', 'Dashboard', 'Network', 'AP', 'System', 'Status', and 'Apply Changes'. The main content area is divided into several sections:

- WAN 1 - 4G SIM1:** IP Address: [Details...], Status: ● Connected, Disconnect
- WAN 2 - 4G SIM2:** IP Address: [Details...], Status: ● Connected, Disconnect
- WAN 3 - VSAT Data:** IP Address: [Details...], Status: ● Connected, Disconnect
- WAN 4 - GSM Data:** IP Address: (none), Status: ● No Cable Detected
- LAN Interface:** Router IP Address: [Input field]
- Device Information:**
  - Model: Peplink MediaFast 500
  - Firmware: 8.0.2 build 2721
  - Uptime: 10 days 11 hours 20 minutes
  - CPU Load: █ 15%
  - Fan Speed: 7458 rpm
  - Temperature: 49.0 °C / 120.2 °F
  - Throughput: ↓ 168.0 kbps ↑ 466.0 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.

The screenshot shows the Peplink MediaFast 500 Network Settings page. The top navigation bar includes 'peplink', 'Dashboard', 'Network', 'AP', 'System', 'Status', and 'Apply Changes'. The left sidebar contains a menu with the following items:

- WAN
- LAN
  - Network Settings
  - Port Settings
- VPN
  - SpeedFusion
  - IPsec VPN
  - GRE Tunnel
- Outbound Policy
- Inbound Access
  - Servers
  - Services
  - DNS Settings
- NAT Mappings

The main content area displays the following settings:

Connection Name	Method	Routing Mode	Type
1. WAN 1 - 4G SIM1	DHCP	NAT	Always-on
2. WAN 2 - 4G SIM2	DHCP	NAT	Always-on
3. WAN 3 - VSAT Data	DHCP	NAT	Always-on
4. WAN 4 - GSM Data	DHCP	NAT	Always-on
5. WAN 5 - Not Used	PPPoE	NAT	Always-on
6. Mobile Internet - Not Used	PPP	-	Backup (Priority 2)

Below the table, there are two sections:

- IPv6:** Disabled [Edit]
- WAN Quality Monitoring:** Auto [Help] [Edit]

The screenshot displays the LAN configuration page in the Peplink interface. The left sidebar shows a navigation menu with categories like WAN, LAN, VPN, Outbound Policy, Inbound Access, NAT Mappings, MediaFast, ContentHub, Docker, MDM Settings, and Captive Portal. The LAN section is expanded, showing sub-items like Network Settings, Port Settings, SpeedFusion, IPsec VPN, GRE Tunnel, Servers, Services, DNS Settings, Cache Settings, Prefetch Schedule, and ContentHub. The main content area is titled 'LAN' and contains several sections: 'IP Settings' with an IP address field set to 255.255.255.0 (/24); 'Network Settings' with fields for Name, VLAN ID, and a checked 'Inter-VLAN routing' checkbox; 'DHCP Server' with an unchecked 'Enable' checkbox, 'DHCP Server Logging' unchecked, 'IP Range' set to 255.255.255.0 (/24), 'Lease Time' set to 1 Day, 0 Hours, 0 Mins, 'DNS Servers' checked, 'WINS Servers' unchecked, and 'BOOTP' unchecked. Below this is an 'Extended DHCP Option' table with columns for 'Option' and 'Value', which is currently empty, with an 'Add' button at the bottom.

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 **Network**, scroll down and click on **Grouped Networks**, choose a name and the IP addresses that will participate in that group.

The screenshot shows the 'Grouped Networks' configuration page in the Peplink interface. The left sidebar is similar to the previous screenshot, but with 'Service Passthrough' and 'Grouped Networks' highlighted. An orange arrow points from 'Grouped Networks' to the main content area. The main content area is titled 'Grouped Networks' and contains a table with two columns: 'Name' and 'Networks'. The table lists five network groups: 'All Networks', 'AV', 'User WIFI Networks', 'Crew & Officer', and 'owner and guest'. Each group has a red 'X' icon in the 'Networks' column. 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 'Outbound Policy' configuration page in the peplink interface. The page is titled 'Outbound Policy' and shows a table of rules. The table has columns for Service, Algorithm, Source, Destination, and Protocol / Port. The 'Default' rule is highlighted, and an 'Add Rule' button is visible at the bottom.

Service	Algorithm	Source	Destination	Protocol / Port	
			Any	Any	✖
			Any	Any	✖
			Any	Any	✖
			Any	Any	✖
			Any	Any	✖
			IP Network	Any	✖
			Any	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.

The screenshot shows the 'Outbound Policy' configuration page in the peplink interface. The 'Edit Custom Rule' dialog box is open, showing fields for Service Name, Enable, Source, Destination, Protocol, Algorithm, and Enforced Connection. The 'Enforced Connection' field is highlighted, and the 'Save' and 'Cancel' buttons are visible.

Service	Algorithm	Source	Destination	Protocol / Port	
All Networks	Enforced WAN: WAN 3 - VS...	Grouped Network All Networks	Any	Any	✖
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default			(Auto)		

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.

The screenshot displays the Peplink management interface. The left sidebar shows navigation options: WAN, LAN (Network Settings, Port Settings), VPN (SpeedFusion, IPsec VPN, GRE Tunnel), **Outbound Policy**, Inbound Access (Servers, Services, DNS Settings), NAT Mappings, MediaFast (Cache Settings, Prefetch Schedule), ContentHub, Docker, MDM Settings, Captive Portal, and QoS. The main area shows the 'Outbound Policy' configuration with a dropdown set to 'Custom'. An 'Edit Custom Rule' dialog is open, showing the following fields:

- Service Name: [Empty]
- Enable:
- Source: Grouped Network [XYZ]
- Destination: Any
- Protocol: Any
- Algorithm: Enforced
- Enforced Connection: WAN: WAN 3 - VSAT Data

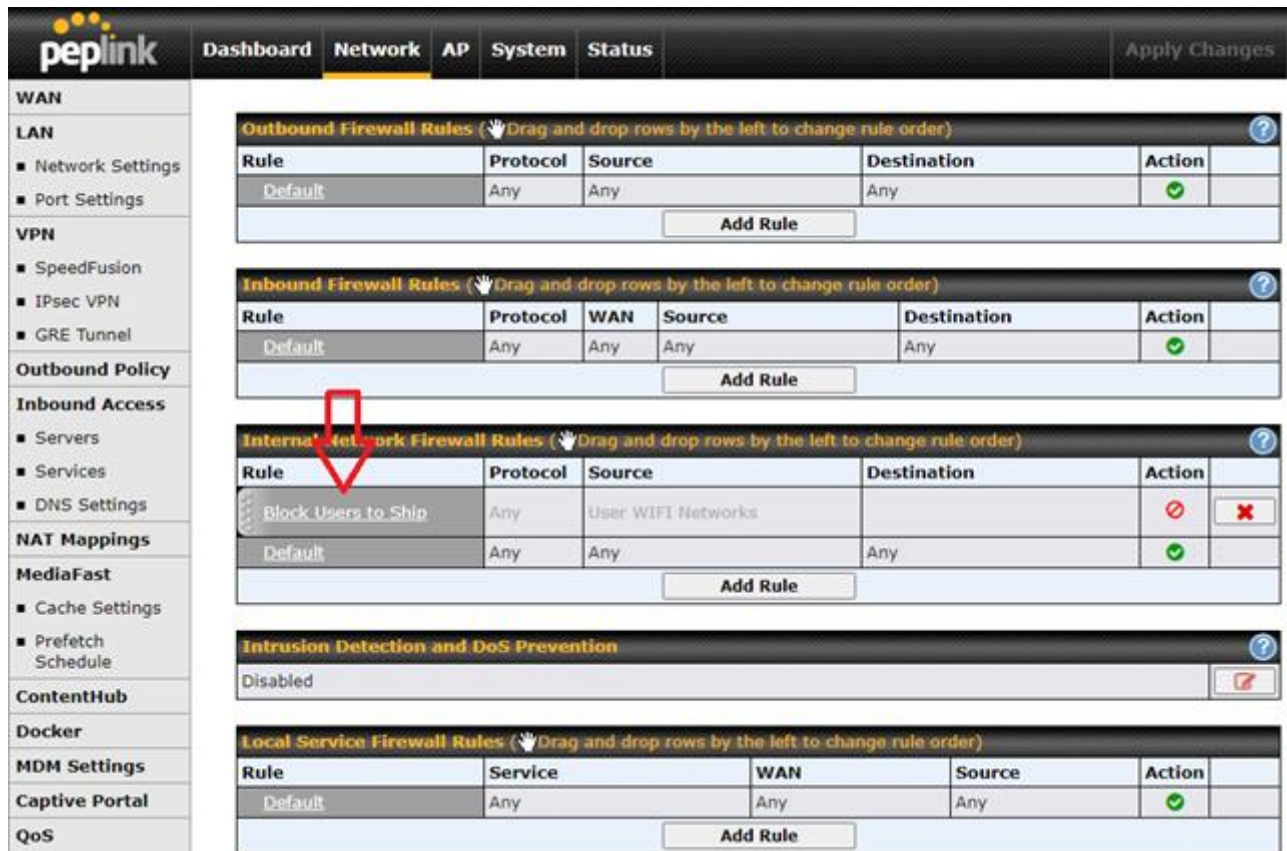
The dialog also includes 'Save' and 'Cancel' buttons. In the background, a table of existing rules is visible:

Service Name	Source	Destination	Protocol	Algorithm	Enforced Connection	Action
All Networks	WAN: WAN 3 - VSAT Data	All Networks	Any	Any	Any	✗
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	Any	✗
Default	(Auto)	(Auto)	(Auto)	(Auto)	(Auto)	

This setting means all the users in Grouped Network XYZ will be **enforced** to use the WAN 3. This forces Crew/Officer networks to use VSAT connections (for example).

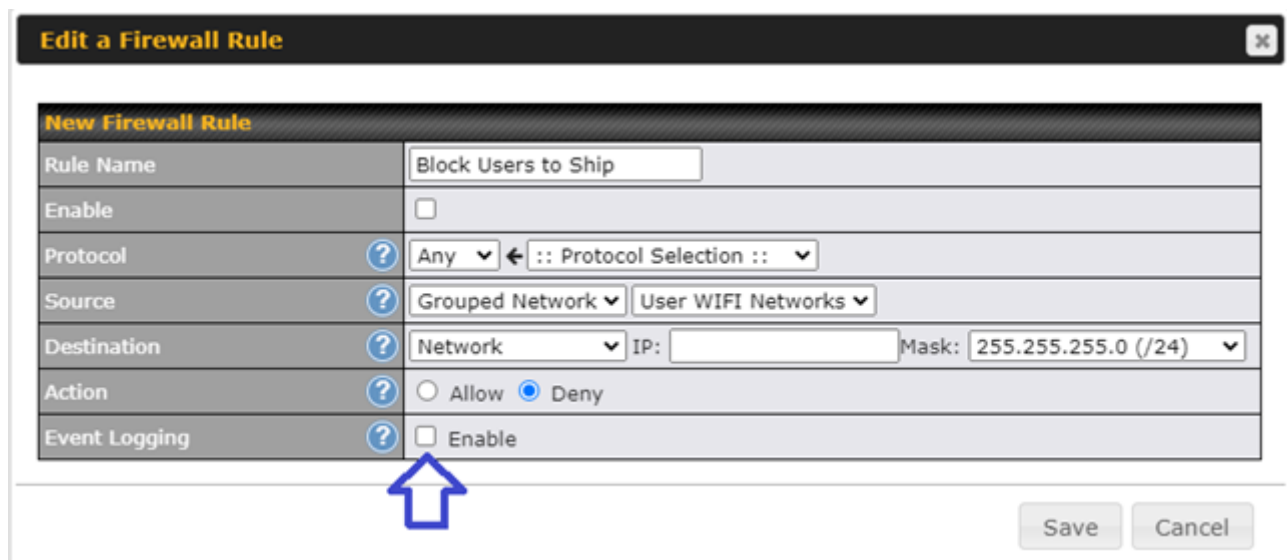
## Access Rules

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



The screenshot shows the PepiLink dashboard with the 'Network' tab selected. The 'Internal Network Firewall Rules' section is expanded, showing a table of rules. A red arrow points to the 'Block Users to Ship' rule.

Rule	Protocol	Source	Destination	Action
Default	Any	Any	Any	✓
Block Users to Ship	Any	User WIFI Networks		✗
Default	Any	Any	Any	✓



The 'Edit a Firewall Rule' dialog box is shown. The 'Event Logging' checkbox is highlighted with a blue arrow.

New Firewall Rule	
Rule Name	Block Users to Ship
Enable	<input type="checkbox"/>
Protocol	Any
Source	Grouped Network   User WIFI Networks
Destination	Network   IP:   Mask: 255.255.255.0 (/24)
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

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 **Network, 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 10.0.8.1 **Network, Content Blocking** and in the session **Customized Domains**, type:

nflximg.\*

netflix.\*

nflex.com

nflxvideo.net

nflxext.com

Mark **Manager** and **Guest** as **Exempted User Groups**, **Save** and click on **Apply Changes**.

The screenshot shows the Pepwave web interface with the following sections:

- Navigation:** Dashboard, Network (selected), AP, System, Status, Apply Changes.
- Left Sidebar:** WAN, LAN (Network Settings, Port Settings), VPN (SpeedFusion, IPsec VPN, GRE Tunnel), Outbound Policy, Inbound Access (Servers, Services, DNS Settings), NAT Mappings, MediaFast (Cache Settings, Prefetch Schedule), ContentHub, Docker, MDM Settings, Captive Portal, QoS (User Groups, Bandwidth Control, Application), Firewall (Access Rules, Content Blocking), Routing Protocols.
- Application Blocking:** Please Select Application... (dropdown), + button.
- Web Blocking:**
  - Preset Category: High, Moderate, Low, Custom (selected).
  - Checked items: Adware, P2P/File sharing, Malware, Social Networking, Pornography, Proxy/Anonymizer.
  - Other items: Aggressive, Drugs, Gambling, Audio-Video, File Hosting, Games, Update Sites, Violence, Contraband, Weapons.
  - Content Filtering Database Auto Update:
- Customized Domains:**

Domain	Action
nflximg.*	✖
netflix.*	✖
nflex.com	✖
nflxvideo.net	✖
nflxext.com	+
- Exempted Domains from Web Blocking:** (empty field), + button.
- Exempted User Groups:**

User Group	Exempt
Manager	<input checked="" type="checkbox"/>
Staff	<input type="checkbox"/>
Guest	<input type="checkbox"/>
- Exempted Subnets:**

Network	Subnet Mask	Action
	255.255.255.0 (/24)	+
- URL Logging:** (empty field)



## Bandwidth Control

Using the Peplink you can define how much minimum bandwidth will be reserved to each user group 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 Guest/Crew (owner no limit).

To do this, you need to know your VLANs and IP Addresses and go to **Network, User Groups, Add** and in **Grouped by** mark **Subnet** and fill the IP Address from Owner/Crew/Guest and mark as **Manager/Staff/Guest** respectively. Example:

The screenshot shows the Peplink web interface with the 'Add / Edit User Group' dialog box open. The 'Grouped by' dropdown is set to 'Subnet' and the 'Group' dropdown is set to 'Manager'. The IP address field is empty and the mask is set to '255.255.255.0 (/24)'. There are 'Save', 'Cancel', and 'Add' buttons.

These settings mean the IP addresses 0.0.0.0/24 will follow the bandwidth rules as **Manager** (Normally Owner - no limit by default).

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

The screenshot shows the Peplink web interface with the 'Group Bandwidth Reservation' and 'Individual Bandwidth Limit' settings. The 'Group Bandwidth Reservation' checkbox is unchecked. The 'Individual Bandwidth Limit' checkbox is checked. The 'User Bandwidth Limit' table shows settings for Manager, Staff, and Guest.

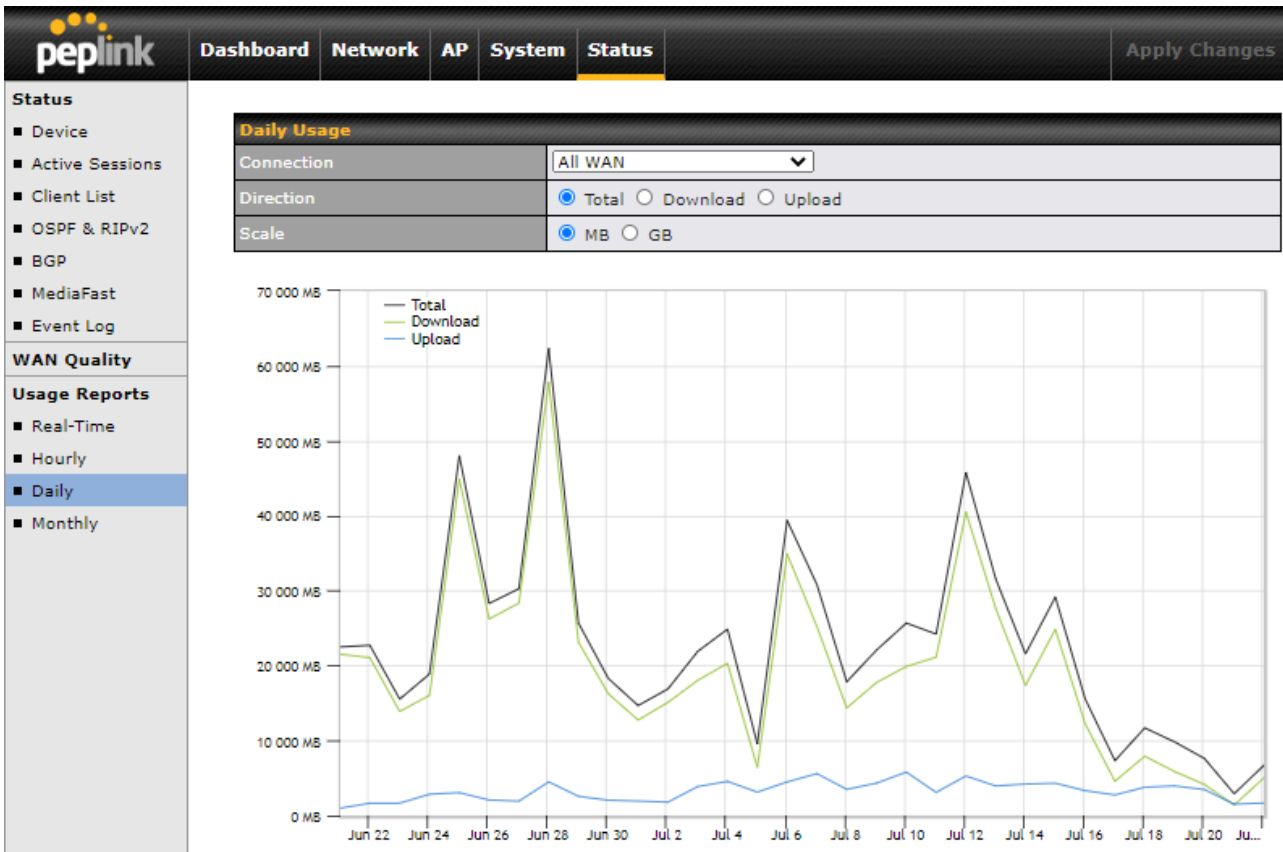
User Bandwidth Limit	Download	Upload
Manager:	Unlimited	Unlimited
Staff:	0 Mbps	0 Mbps (0: Unlimited)
Guest:	0 Mbps	0 Mbps (0: Unlimited)

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

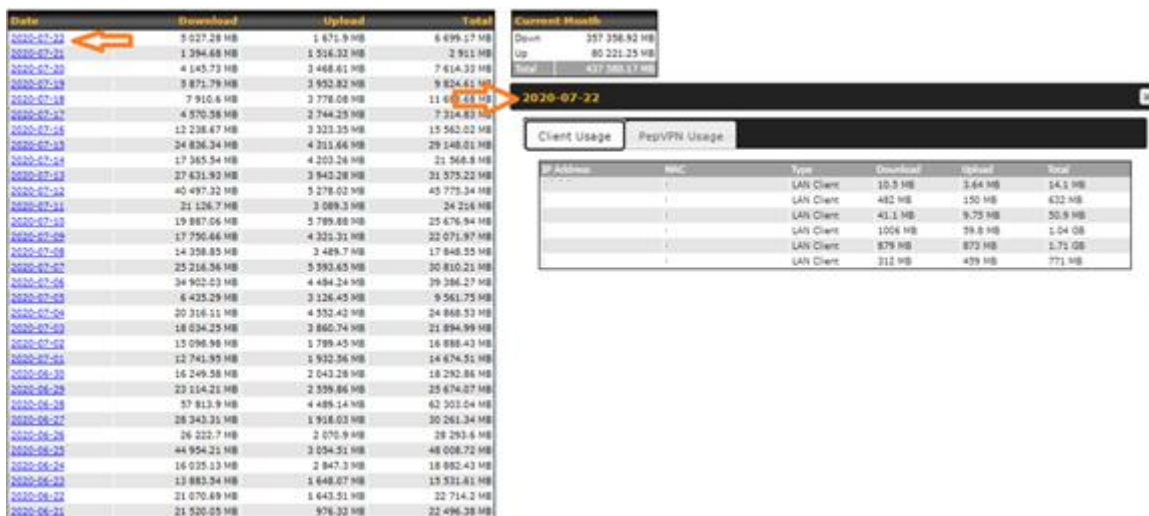
## Usage Reports

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):



*\* 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.*