

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Mode</b>                             | Choose <b>Main Mode</b> if both IPsec peers use static IP addresses. Choose <b>Aggressive Mode</b> if one of the IPsec peers uses dynamic IP addresses.                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Force UDP Encapsulation</b>          | For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Pre-shared Key</b>                   | 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.                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Remote Certificate (pem encoded)</b> | Available only when <b>X.509 Certificate</b> is chosen as the <b>Authentication</b> method, this field allows you to paste a valid X.509 certificate.                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Local ID</b>                         | In <b>Main Mode</b> , this field can be left blank. In <b>Aggressive Mode</b> , if <b>Remote Gateway IP Address</b> is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.                                                                                                                                                                                                                                                                                                        |
| <b>Remote ID</b>                        | In <b>Main Mode</b> , this field can be left blank. In <b>Aggressive Mode</b> , if <b>Remote Gateway IP Address</b> is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.                                                                                                                                                                                                                                                                                                        |
| <b>Phase 1 (IKE) Proposal</b>           | In <b>Main Mode</b> , this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In <b>Aggressive Mode</b> , only one selection is permitted.                                                                                                                                                                                                                                                                                                                    |
| <b>Phase 1 DH Group</b>                 | 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.<br><b>Group 2: 1024-bit</b> is the default value.<br><b>Group 5: 1536-bit</b> is the alternative option.                                                                                                                                                                                                                                |
| <b>Phase 1 SA Lifetime</b>              | This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at <b>3600</b> seconds.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Phase 2 (ESP) Proposal</b>           | In <b>Main Mode</b> , 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 <b>Aggressive Mode</b> , only one selection is permitted.                                                                                                                                                                                                                                                                                                                 |
| <b>Phase 2 PFS Group</b>                | 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.<br><b>None</b> - 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.<br><b>Group 2: 1024-bit</b> Diffie-Hellman group. The larger the group number, the higher the security.<br><b>Group 5: 1536-bit</b> 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.

| WAN Connection Priority |               |
|-------------------------|---------------|
| Priority                | WAN Selection |
| 1                       | WAN 1         |
| 2                       | -----         |

### WAN Connection Priority

**WAN Connection** Select the appropriate WAN connection from the drop-down menu.

### IPsec Settings

#### DPD Interval

Time interval between Dead Peer Detection (DPD) messages (R\_U\_THERE in IKEv1 or INFORMATIONAL in IKEv2) that check if the peer is still active when no other traffic is present.

Default: 10 seconds (2–30 seconds)

#### DPD Attempts

Total number of DPD messages sent before the peer is considered unreachable.

Default: 3 times (2-10 times)

## 11 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 SpeedFusion VPN.

To configure a GRE Tunnel, navigate to **Advanced > GRE Tunnel**.

| GRE Tunnel Profiles    | Remote Networks |
|------------------------|-----------------|
| No GRE profile defined |                 |
| New Profile            |                 |

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**
✕

| <b>Name</b>                              | <input style="width: 90%;" type="text"/>                                                                                                                                                                                                                                                                                                                                                |         |             |                                          |                                                                                                          |                                                             |  |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------------|------------------------------------------|----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|--|
| <b>Active</b>                            | <input checked="" type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                     |         |             |                                          |                                                                                                          |                                                             |  |
| <b>Remote GRE IP Address</b>             | <input style="width: 90%;" type="text"/>                                                                                                                                                                                                                                                                                                                                                |         |             |                                          |                                                                                                          |                                                             |  |
| <b>Tunnel Local IP Address</b>           | <input style="width: 90%;" type="text"/>                                                                                                                                                                                                                                                                                                                                                |         |             |                                          |                                                                                                          |                                                             |  |
| <b>Tunnel Remote IP Address</b>          | <input style="width: 90%;" type="text"/>                                                                                                                                                                                                                                                                                                                                                |         |             |                                          |                                                                                                          |                                                             |  |
| <b>Tunnel Subnet Mask</b>                | <input checked="" type="radio"/> Auto<br><input type="radio"/> <input style="width: 100px;" type="text" value="255.255.255.0 (/24"/>                                                                                                                                                                                                                                                    |         |             |                                          |                                                                                                          |                                                             |  |
| <b>Connection</b>                        | WAN <span style="float: right;">▼</span>                                                                                                                                                                                                                                                                                                                                                |         |             |                                          |                                                                                                          |                                                             |  |
| <b>Remote Networks</b>                   | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Network</th> <th style="width: 50%;">Subnet Mask</th> </tr> </thead> <tbody> <tr> <td><input style="width: 90%;" type="text"/></td> <td> <input style="width: 90%;" type="text" value="255.255.255.0 (/24"/> <span style="float: right;">▼</span> </td> </tr> </tbody> </table> | Network | Subnet Mask | <input style="width: 90%;" type="text"/> | <input style="width: 90%;" type="text" value="255.255.255.0 (/24"/> <span style="float: right;">▼</span> | <div style="text-align: right; padding-right: 5px;">+</div> |  |
| Network                                  | Subnet Mask                                                                                                                                                                                                                                                                                                                                                                             |         |             |                                          |                                                                                                          |                                                             |  |
| <input style="width: 90%;" type="text"/> | <input style="width: 90%;" type="text" value="255.255.255.0 (/24"/> <span style="float: right;">▼</span>                                                                                                                                                                                                                                                                                |         |             |                                          |                                                                                                          |                                                             |  |

Save

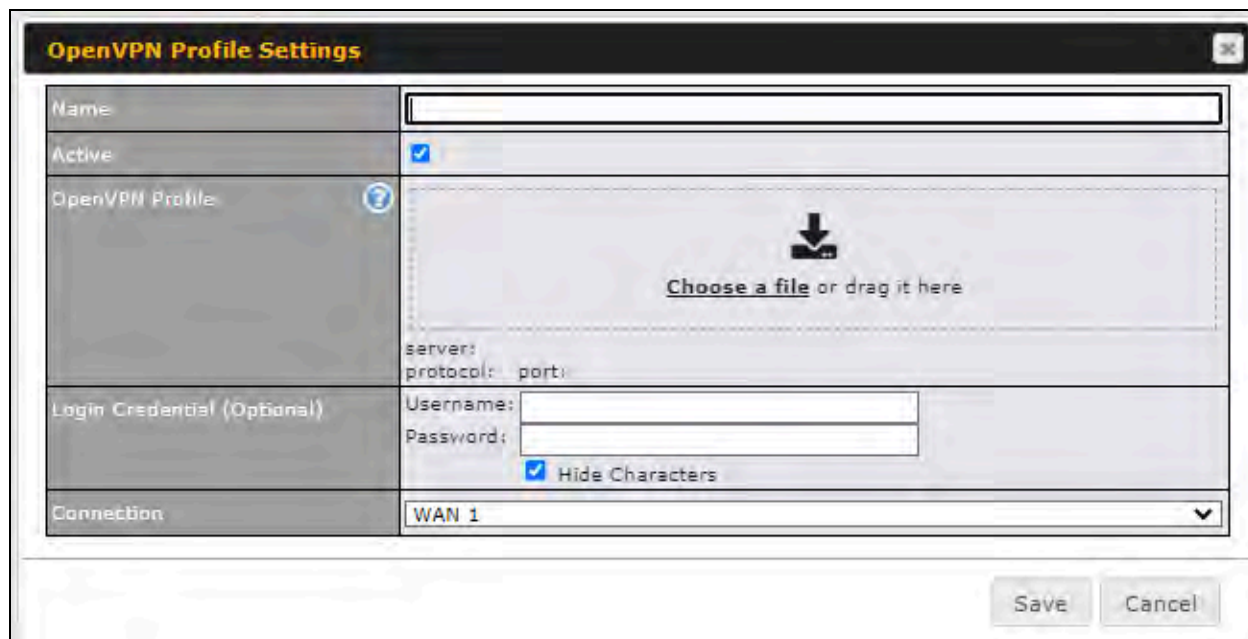
Cancel

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

## 12 OpenVPN

OpenVPN is a site to site VPN mode that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

To configure a OpenVPN, navigate to **Advanced > OpenVPN** and click the **New Profile**.



| OpenVPN Profile Settings           |                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                        | This field is for specifying a name to represent this OpenVPN profile.                                                                  |
| <b>Active</b>                      | When this box is checked, this OpenVPN connection profile will be enabled. Otherwise, it will be disabled.                              |
| <b>OpenVPN Profile</b>             | Upload the OpenVPN configuration (.ovpn) file from your service provider.                                                               |
| <b>Login Credential (Optional)</b> | This option is an optional for you to enter the username and password to login for the OpenVPN connection if the profile need to login. |
| <b>Connection</b>                  | Select the appropriate WAN connection from the drop-down menu.                                                                          |

## 13 Outbound Policy

Peplink routers can flexibly manage and load balance outbound traffic among WAN connections.

### Important Note

Outbound policy is applied only when more than one WAN connection is active.

The settings for managing and load balancing outbound traffic are located at **Advanced > Outbound Policy**.



| Service                                     | Algorithm                | Source | Destination | Protocol / Port |   |
|---------------------------------------------|--------------------------|--------|-------------|-----------------|---|
| SpeedFusion VPN / OSPF / BGP / RIPv2 Routes |                          |        |             |                 |   |
| HTTPS Persistence                           | Persistence (Src) (Auto) | Any    | Any         | TCP 443         | X |
| Default                                     | (Auto)                   |        |             |                 |   |

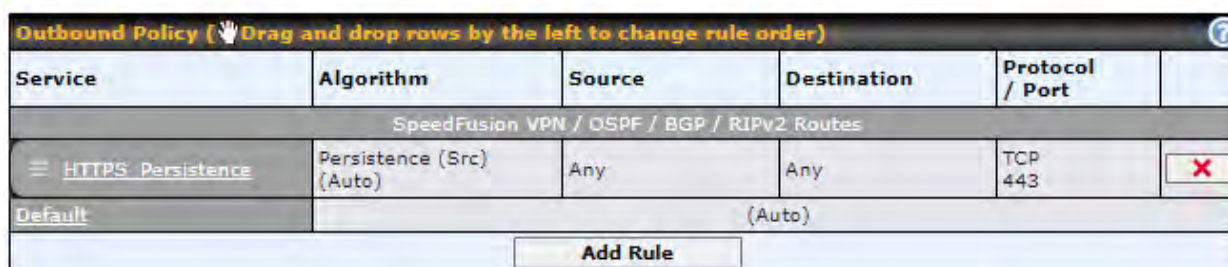
Add Rule

Expert Mode

Enabled

### 13.1 Adding Rules for Outbound Policy

The menu underneath enables you to define Outbound policy rules:



| Service                                     | Algorithm                | Source | Destination | Protocol / Port |   |
|---------------------------------------------|--------------------------|--------|-------------|-----------------|---|
| SpeedFusion VPN / OSPF / BGP / RIPv2 Routes |                          |        |             |                 |   |
| HTTPS Persistence                           | Persistence (Src) (Auto) | Any    | Any         | TCP 443         | X |
| Default                                     | (Auto)                   |        |             |                 |   |

Add Rule

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.

?

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

Drop the Traffic

Use Any Available Connections

Save

Cancel

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                      | <input style="width: 90%;" type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                             |  |
| Enable                            | <input checked="" type="checkbox"/> Always on ▾                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                             |  |
| Source                            | Any ▾                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                             |  |
| Destination                       | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> IP Network ▾ <input style="width: 150px;" type="text"/> </div> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Mask: 255.255.255.0 (/24) ▾ |  |
| Protocol                          | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> Any ▾ ← :: Protocol Selection :: ▾ </div> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                             |  |
| Algorithm                         | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> Weighted Balance ▾ </div> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                             |  |
| Load Distribution Weight          | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> <div style="margin-bottom: 5px;">WAN 1 <span style="float: right;">10</span></div> <div style="margin-bottom: 5px;">WAN 2 <span style="float: right;">10</span></div> <div style="margin-bottom: 5px;">WAN 3 <span style="float: right;">10</span></div> <div style="margin-bottom: 5px;">WAN 4 <span style="float: right;">10</span></div> <div style="margin-bottom: 5px;">WAN 5 <span style="float: right;">10</span></div> <div style="margin-bottom: 5px;">Mobile Internet <span style="float: right;">10</span></div> </div> </div> |                             |  |
| When No Connections are Available | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> Drop the Traffic ▾ </div> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                             |  |

## 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 Peplink router based on the other parameters of the rule. When **Enable** is unchecked, the rule does not take effect: the Peplink 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 specifies the source IP address(es) and port number(s) to be matched for the firewall rule. Any, IP Address, IP Network, MAC Address, Client Type (for Outbound and Internal Firewall only), and Client's Associated SSID can be specified as the Source setting, as indicated in the following screenshots:

|                          |                                                                                                                                                                                               |  |  |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
| Source                   | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> Any ▾ </div> </div>                    |  |  |
| Destination              | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> Any ▾ </div> </div>                    |  |  |
| Protocol                 | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> IP Address </div> </div>               |  |  |
| Algorithm                | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> IP Network </div> </div>               |  |  |
| Connection Type          | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> MAC Address </div> </div>              |  |  |
| Load Distribution Weight | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> Client Type </div> </div>              |  |  |
|                          | <div style="display: flex; align-items: center;"> <span style="color: blue; font-size: 1.2em; margin-right: 5px;">?</span> <div style="flex-grow: 1;"> Client's Associated SSID </div> </div> |  |  |

When you select Client Type as the Source, a drop-down list will appear for you to choose

the different types of client devices.

In addition, a single port, or a range of ports, can be specified for the **Source** settings.

This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. Any, IP Address, IP Network, Domain Name, SpeedFusion Connect, and SpeedFusion VPN Profile can be specified as the **Destination** setting, as indicated in the following screenshots:

## Destination

In addition, a single port or a range of ports can be specified for the settings.

## 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Algorithm</b>                                 | <p>This setting specifies the behavior of the Peplink router for the custom rule. One of the following values can be selected (Note that some Peplink routers provide only some of these options):</p> <ul style="list-style-type: none"> <li>• Weighted Balance</li> <li>• Persistence</li> <li>• Enforced</li> <li>• Priority</li> <li>• Overflow</li> <li>• Least Used</li> <li>• Lowest Latency</li> <li>• Fastest Response Time</li> </ul> <p>For a full explanation of each Algorithm, please see the following article:<br/> <a href="https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithms-work/8059">https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithms-work/8059</a></p> |
| <b>Load Distribution Weight</b>                  | This is to define the outbound traffic weight ratio for each WAN connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>When No connections are available</b>         | <p>This field allows you to configure the default action when all the selected Connections are not available.</p> <p><b>Drop the Traffic</b> - Traffic will be discarded.</p> <p><b>Use Any Available Connections</b> - Traffic will be routed to any available Connection, even it is not selected in the list.</p> <p><b>Fall-through to Next Rule</b> - Traffic will continue to match the next Outbound Policy rule just like this rule is inactive.</p>                                                                                                                                                                                                                                                                          |
| <b>Terminate Sessions on Connection Recovery</b> | <p>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 <b>Priority</b> 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.</p>                                                                                                                                  |

### 13.1.1 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 ? | <div>WAN 1 10</div> <div>WAN 2 10</div> <div>Wi-Fi WAN 10</div> <div>Cellular 1 10</div> <div>Cellular 2 10</div> <div>USB 10</div> |

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
- Orbit WAN 1: 10
- Orbit WAN 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 Orbit WAN 1 is 16.7% = (10 / 60) x 100%.

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

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

### 13.1.2 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.

Peplink 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 Peplink router may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Peplink 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         |  <input checked="" type="radio"/> By Source <input type="radio"/> By Destination                                                                  |
| Load Distribution        |  <input type="radio"/> Auto <input checked="" type="radio"/> Custom                                                                               |
| Load Distribution Weight |  <div> <div>WAN 1 10</div> <div>WAN 2 10</div> <div>Wi-Fi WAN 10</div> <div>Cellular 1 10</div> <div>Cellular 2 10</div> <div>USB 10</div> </div> |

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

|                        |                                                                                                                                                                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>By Source:</b>      | 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.                               |
| <b>By Destination:</b> | 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.

### 13.1.3 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 | ? | <div> <div>WAN: WAN 1</div> <div> <div>WAN: WAN 1</div> <div>WAN: WAN 2</div> <div>WAN: Wi-Fi WAN</div> <div>WAN: Cellular 1</div> <div>WAN: Cellular 2</div> <div>WAN: USB</div> <div>VPN: Connection 1</div> </div> </div> |
|                     |   | <div>Save</div> <div>Cancel</div>                                                                                                                                                                                            |

Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection. Starting from Firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection.

### 13.1.4 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.

| Algorithm                                 | ?          | Priority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                  |            |          |  |                 |  |                 |  |          |  |                   |  |                |  |                |  |                    |  |                 |  |
|-------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|------------|----------|--|-----------------|--|-----------------|--|----------|--|-------------------|--|----------------|--|----------------|--|--------------------|--|-----------------|--|
| Priority Order                            | ?          | <table border="1"> <thead> <tr> <th>Highest Priority</th> <th>Not In Use</th> </tr> </thead> <tbody> <tr><td>WAN: WAN</td><td></td></tr> <tr><td>WAN: Cellular 1</td><td></td></tr> <tr><td>WAN: Cellular 2</td><td></td></tr> <tr><td>WAN: USB</td><td></td></tr> <tr><td>WAN: LAN 1 as WAN</td><td></td></tr> <tr><td>WAN: GRE WAN 1</td><td></td></tr> <tr><td>WAN: GRE WAN 2</td><td></td></tr> <tr><td>WAN: OpenVPN WAN 1</td><td></td></tr> <tr><td>Lowest Priority</td><td></td></tr> </tbody> </table> | 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 |  |
| 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 | ?          | <input type="checkbox"/> Enable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                  |            |          |  |                 |  |                 |  |          |  |                   |  |                |  |                |  |                    |  |                 |  |

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

#### Tip

Configure multiple distribution rules to accommodate different kinds of services.

### 13.1.5 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 | ? | <div> <div>Highest Priority</div> <div> <div>WAN: WAN 1</div> <div>WAN: WAN 2</div> <div>WAN: Wi-Fi WAN</div> <div>WAN: Cellular 1</div> <div>WAN: Cellular 2</div> <div>WAN: USB</div> </div> <div>Lowest Priority</div> </div> |

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.

### 13.1.6 Algorithm: Least Used

Add a New Custom Rule

|                                   |                                                                              |                  |                            |
|-----------------------------------|------------------------------------------------------------------------------|------------------|----------------------------|
| Service Name                      |                                                                              |                  |                            |
| Enable                            | <input checked="" type="checkbox"/>                                          |                  |                            |
| Source                            | ?                                                                            | Any              |                            |
| Destination                       | ?                                                                            | IP Network       | Mask: 255.255.255.0 (/24)  |
| Protocol                          | ?                                                                            | Any              | ← :: Protocol Selection :: |
| Algorithm                         | ?                                                                            | Least Used       |                            |
| Least Used Mode                   | <input checked="" type="radio"/> By Downlink <input type="radio"/> By Uplink |                  |                            |
| Connection                        | <input type="checkbox"/> WAN<br><input type="checkbox"/> VLAN WAN 1          |                  |                            |
| When No Connections are Available | ?                                                                            | Drop the Traffic |                            |

Save
Cancel

By default, traffic matching this rule will be routed through the healthy WAN connection that is selected in the '**Connection**' and has the most available download bandwidth. You can change it to 'By Uplink' to choose the connection that has the most available upload bandwidth.

The available download/upload bandwidth of a WAN connection is calculated from the total download/upload bandwidth specified on the WAN settings page and the current download/upload usage. The available bandwidth and WAN selection are determined every time an IP session is established.

### 13.1.7 Algorithm: Lowest Latency

|            |                                                                                                                                                                                                                                                                                                   |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Algorithm  | <div> <div>?</div> <div>Lowest Latency ▼</div> </div> <div>Note: Use of Lowest Latency will incur additional network usage.</div>                                                                                                                                                                 |
| Connection | <div> <input checked="" type="checkbox"/> WAN 1         <input checked="" type="checkbox"/> WAN 2         <input checked="" type="checkbox"/> Wi-Fi WAN         <input type="checkbox"/> Cellular 1         <input type="checkbox"/> Cellular 2         <input type="checkbox"/> USB       </div> |

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.

### 13.1.8 Expert Mode

**Expert Mode** is available on some Peplink 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.

Help

Close

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 of PepVPN traffic, [turn on Expert Mode](#).

## 14 Port Forwarding

Peplink routers can act as a firewall that blocks, by default, all inbound access from the Internet. By using port forwarding, Internet users can access servers behind the Peplink router. Inbound port forwarding rules can be defined at **Advanced > Port Forwarding**.

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

To define a new service, click **Add Service**.

Port Forwarding

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable                                                      | <input checked="" type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                     |
| Service Name                                                | <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                    |
| Protocol                                                    | TCP <input type="button" value="←"/> :: Protocol Selection :: <input type="button" value="v"/>                                                                                                                                                                                                                                                                                                          |
| Port                                                        | Any Port <input type="button" value="v"/>                                                                                                                                                                                                                                                                                                                                                               |
| Inbound IP Address(es)<br>(Require at least one IP address) | <div> <div>Connection / IP Address(es)</div> <div> <input type="button" value="All"/> <input type="button" value="Clear"/> </div> </div> <div> <input type="checkbox"/> WAN           <input type="checkbox"/> Cellular           <input type="checkbox"/> Wi-Fi WAN on 2.4 GHz           <input type="checkbox"/> Wi-Fi WAN on 5 GHz           <input type="checkbox"/> SpeedFusion VPN         </div> |
| Server IP Address                                           | <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                    |

| Port Forwarding Settings |                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable</b>            | This setting specifies whether the inbound service takes effect. When <b>Enable</b> is checked, the inbound service takes effect: traffic is matched and actions are taken by the Peplink router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Peplink router disregards the other parameters of the rule. |
| <b>Service Name</b>      | This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.                                                                                                                                                                                                                           |

## Protocol

The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Peplink router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single 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 remain manually modifiable.

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



**Any Port:** all traffic that is received by the Peplink router via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.

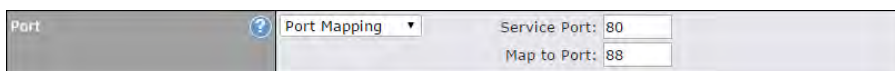


**Single Port:** traffic that is received by the Peplink router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.

## Port



**Port Range:** traffic that is received by the Peplink router 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, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.



**Port Mapping:** traffic that is received by Peplink router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting.

For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, 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 |
| <p><b>Range Mapping:</b> traffic that is received by the Peplink router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the <b>Servers</b> setting.</p> |                                                                                                                |                        |                       |
| <b>Inbound IP Address(es)</b>                                                                                                                                                                                                | This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed. |                        |                       |
| <b>Server IP Address</b>                                                                                                                                                                                                     | This setting specifies the LAN IP address of the server that handles the requests for the service.             |                        |                       |

## 14.1 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                                | <input type="checkbox"/> Enable |
| NAT-PMP                             | <input type="checkbox"/> Enable |
| <input type="button" value="Save"/> |                                 |

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

## 15 NAT Mappings

NAT mappings allow IP address mapping of all inbound and outbound NAT'd traffic to and from an internal client IP address. Settings to configure NAT mappings are located at **Advanced > NAT Mappings**.

| LAN Clients  | Inbound Mappings                   | Outbound Mappings     |                                                                                     |
|--------------|------------------------------------|-----------------------|-------------------------------------------------------------------------------------|
| 192.168.1.23 | (WAN 1):10.88.3.158 (Interface IP) | Use Interface IP only |  |
| Add NAT Rule |                                    |                       |                                                                                     |

To add a rule for NAT mappings, click **Add NAT Rule**.

NAT Mappings

LAN Client

IP Address

IP Address

Inbound Mappings

Connection / Inbound IP Address(es)

☐ WAN
☐ Cellular
☐ Wi-Fi WAN on 2.4 GHz
☐ Wi-Fi WAN on 5 GHz
☐ SpeedFusion VPN

Outbound Mappings

Connection / Outbound IP Address

WAN

192.168.52.152 (Interface IP)

Cellular

Interface IP

Wi-Fi WAN on 2.4 GHz

Interface IP

Wi-Fi WAN on 5 GHz

Interface IP

Save

Cancel

| NAT Mapping Settings |                                                                                                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LAN Client</b>    | NAT mapping rules can be defined for a single LAN <b>IP Address</b> , an <b>IP Range</b> , or an <b>IP Network</b> .                                                                                                                                                  |
| <b>IP Address</b>    | 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 <b>IP Address</b> is selected.            |
| <b>IP Range</b>      | 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 <b>IP Range</b> is selected. |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP Network</b>        | 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 <b>IP Network</b> is selected.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Inbound Mappings</b>  | <p>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 <b>IP Address</b> is selected in the <b>LAN Client(s)</b> field.</p> <p><b>Note that:</b> inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode. Also note that each WAN IP address can be associated to one NAT mapping only.</p>                                                                                                             |
| <b>Outbound Mappings</b> | <p>This setting specifies the WAN IP addresses that 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).</p> <p><b>Note that:</b> 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 <b>Outbound Policy</b> section. Also note that WAN connections in drop-in mode or IP forwarding mode are not shown here.</p> |

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

#### Important Note

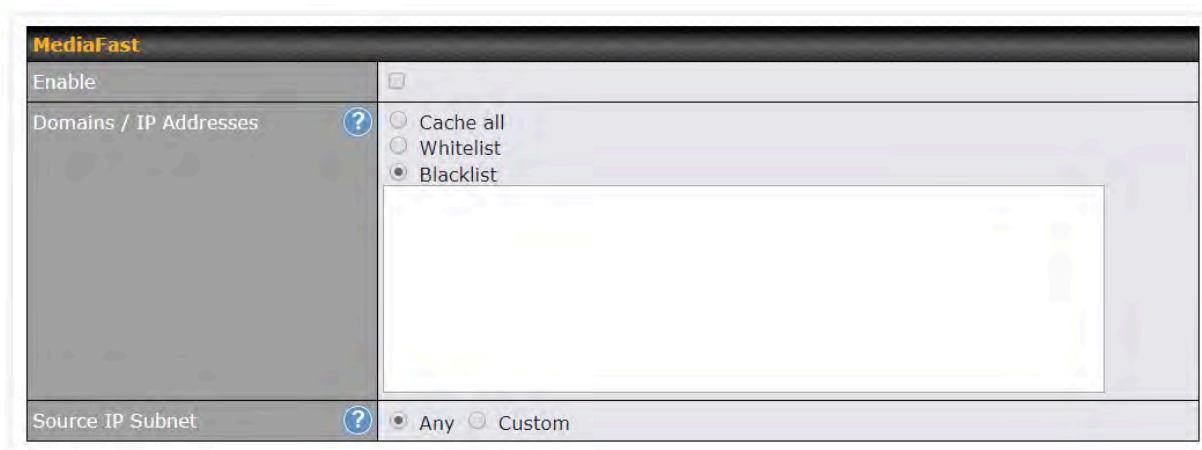
Inbound firewall rules override the **Inbound Mappings** settings.

## 16 Media Fast

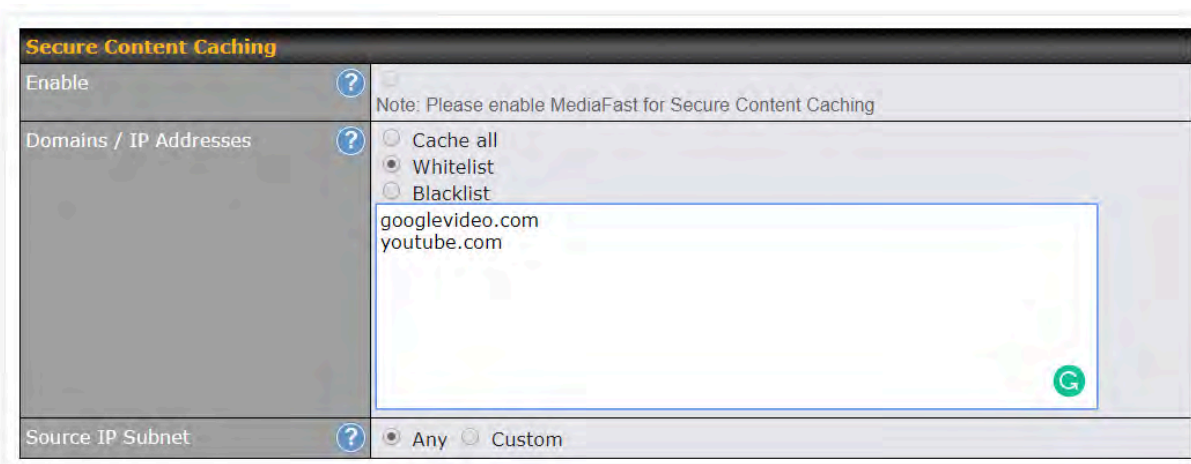
MediaFast settings can be configured from the **Advanced** menu.

### 16.1 Setting Up MediaFast Content Caching

To access MediaFast content caching settings, select **Advanced > Cache Control**

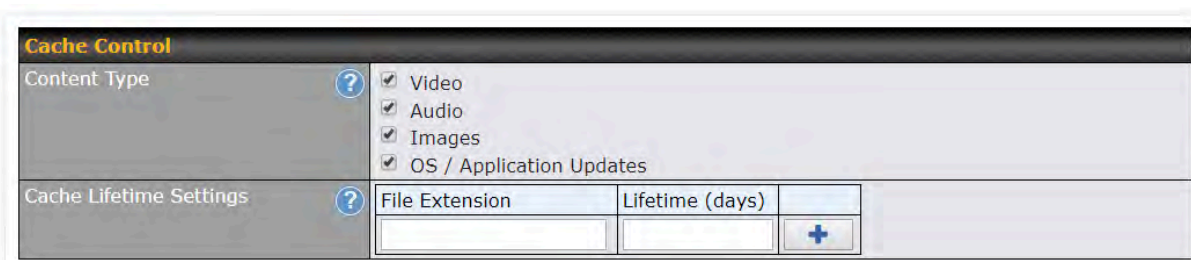


| MediaFast                     |                                                                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------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



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

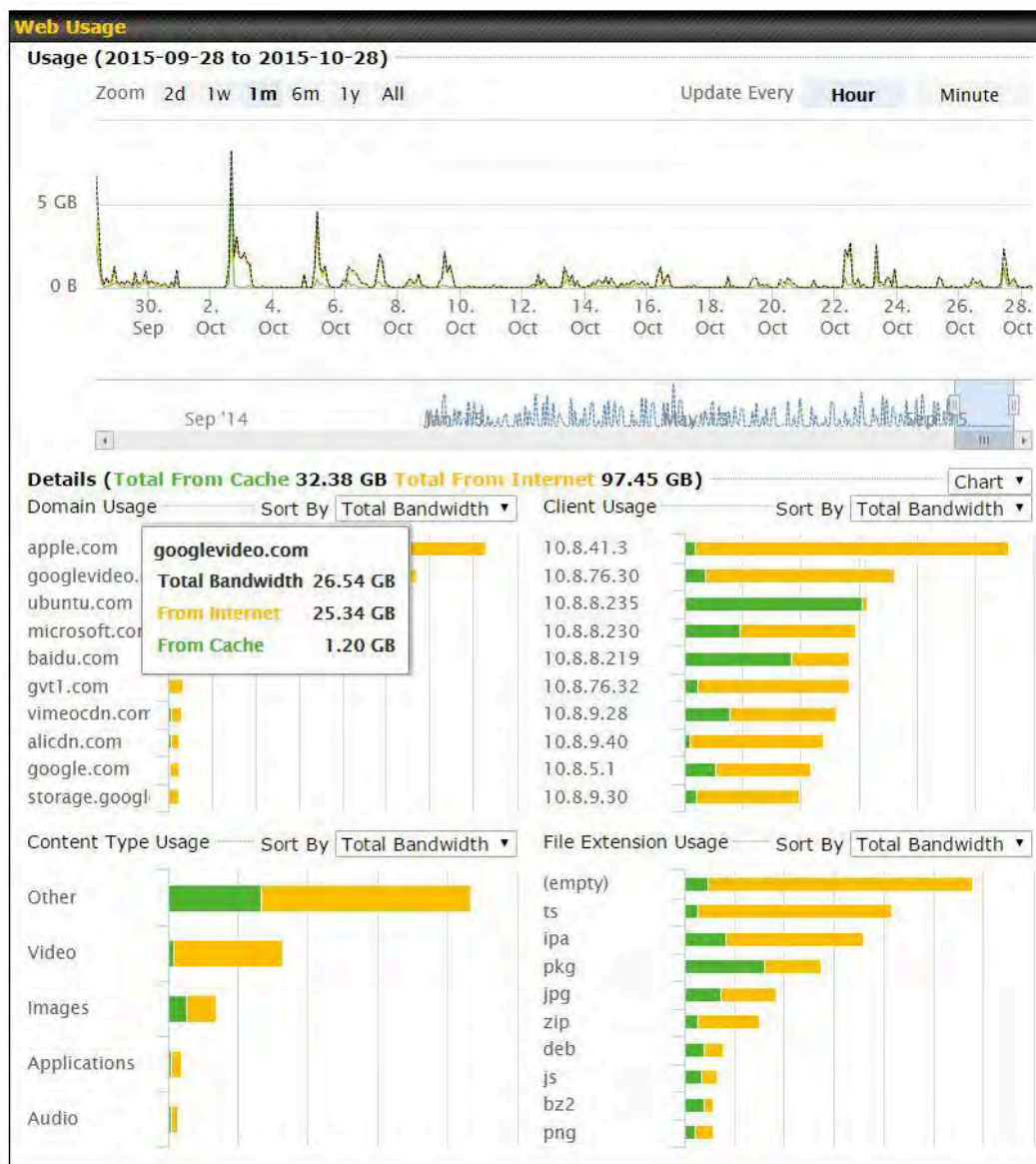
\*See <https://forum.peplink.com/t/certificate-installation-for-mediafast-https-caching/>



| Cache Control                  |                                                                                                                                                                                                |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Content Type</b>            | Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.                                                                          |
| <b>Cache Lifetime Settings</b> | 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. |

## 16.2 Viewing MediaFast Statistics

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



## 16.3 Prefetch Schedule

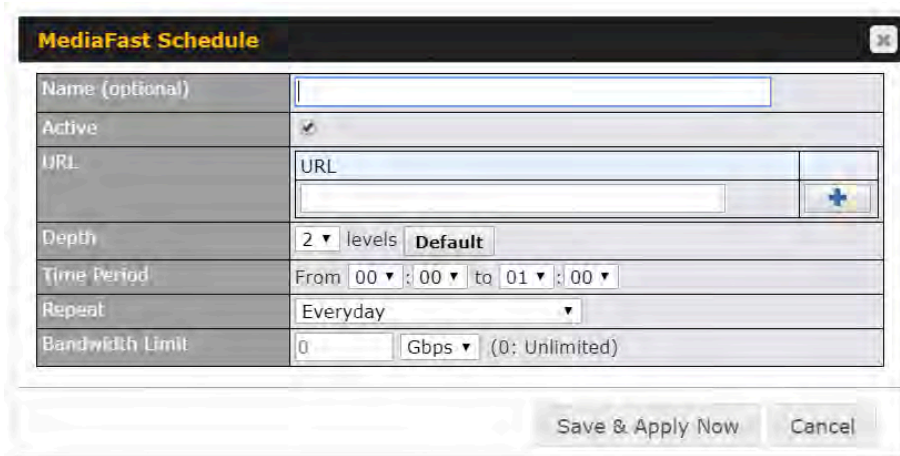
Content prefetching allows you to download content on a schedule that you define, which can help to preserve network bandwidth during busy times and keep costs down. To access MediaFast content prefetching settings, select **Advanced > Prefetch Schedule**.

| 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      |    |
| <a href="#">New Schedule</a>                                     |             |               |               |               |                                                                                     |               |                                                                                                                                                                                                                                                             |
| Tools                                                            |             |               |               |               |                                                                                     |               |                                                                                                                                                                                                                                                             |
| <a href="#">Clear Web Cache</a> <a href="#">Clear Statistics</a> |             |               |               |               |                                                                                     |               |                                                                                                                                                                                                                                                             |

| Prefetch Schedule Settings         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                        | This field displays the name given to the scheduled download.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Status</b>                      | Check the status of your scheduled download here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Next Run Time/Last Run Time</b> | These fields display the date and time of the next and most recent occurrences of the scheduled download.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Last Duration</b>               | 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.                                                                                                                                                                                                                                     |
| <b>Result</b>                      | This field indicates whether downloads are in progress (  ) or complete (  ).                                                                                                                                                                                                                                                                                            |
| <b>Last Download</b>               | 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.                                                                                                                                |
| <b>Actions</b>                     | <p>To begin a scheduled download immediately, click .</p> <p>To cancel a scheduled download, click .</p> <p>To edit a scheduled download, click .</p> <p>To delete a scheduled download, click .</p> |

Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:

### New Schedule



The dialog box titled "MediaFast Schedule" contains the following fields and controls:

- Name (optional):** A text input field.
- Active:** A checkbox that is checked.
- URL:** A text input field containing "URL" and a button with a plus sign.
- Depth:** A dropdown menu set to "2" and a button labeled "Default".
- Time Period:** A range selector showing "From 00 : 00 to 01 : 00".
- Repeat:** A dropdown menu set to "Everyday".
- Bandwidth Limit:** A text input field containing "0" and a dropdown menu set to "Gbps", with "(0: Unlimited)" in parentheses.

At the bottom right, there are two buttons: "Save & Apply Now" and "Cancel".

Simply provide the requested information to create your schedule.

### Clear Web Cache

To clear all cached content, click this button. Note that this action cannot be undone.

### Clear Statistics

To clear all prefetch and status page statistics, click this button.

## 17 Edge Computing

ContentHub allows you to deliver webpages and applications to users connected to the SSID using the local storage on your router, like the Max HD2/HD4 with Mediafast, which can store up to 8GB of media. Users will be able to access news, articles, videos, and access your web app without the need for internet access.

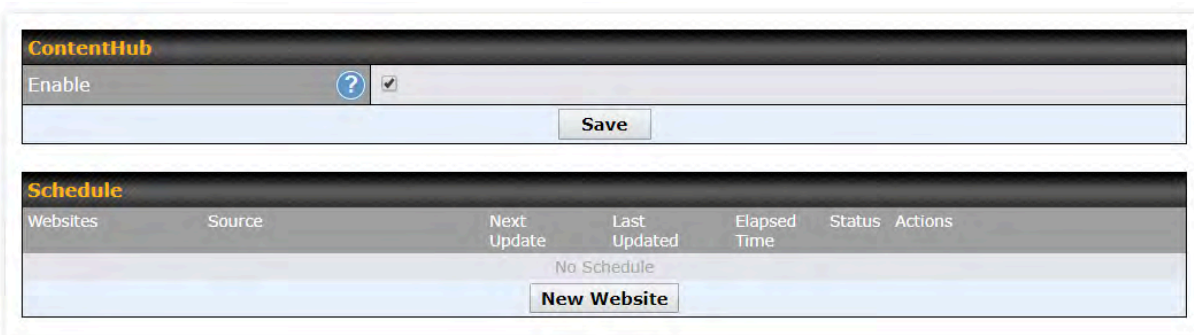
The ContentHub can be used to provide infotainment to connected users on transport.

### 17.1 Configuring the ContentHub

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 **Advanced > ContentHub** and check the **Enable** box.



| ContentHub                   |        |                                     |              |              |        |         |
|------------------------------|--------|-------------------------------------|--------------|--------------|--------|---------|
| Enable                       |        | <input checked="" type="checkbox"/> |              |              |        |         |
| <button>Save</button>        |        |                                     |              |              |        |         |
| Schedule                     |        |                                     |              |              |        |         |
| Websites                     | Source | Next Update                         | Last Updated | Elapsed Time | Status | Actions |
| No Schedule                  |        |                                     |              |              |        |         |
| <button>New Website</button> |        |                                     |              |              |        |         |

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.

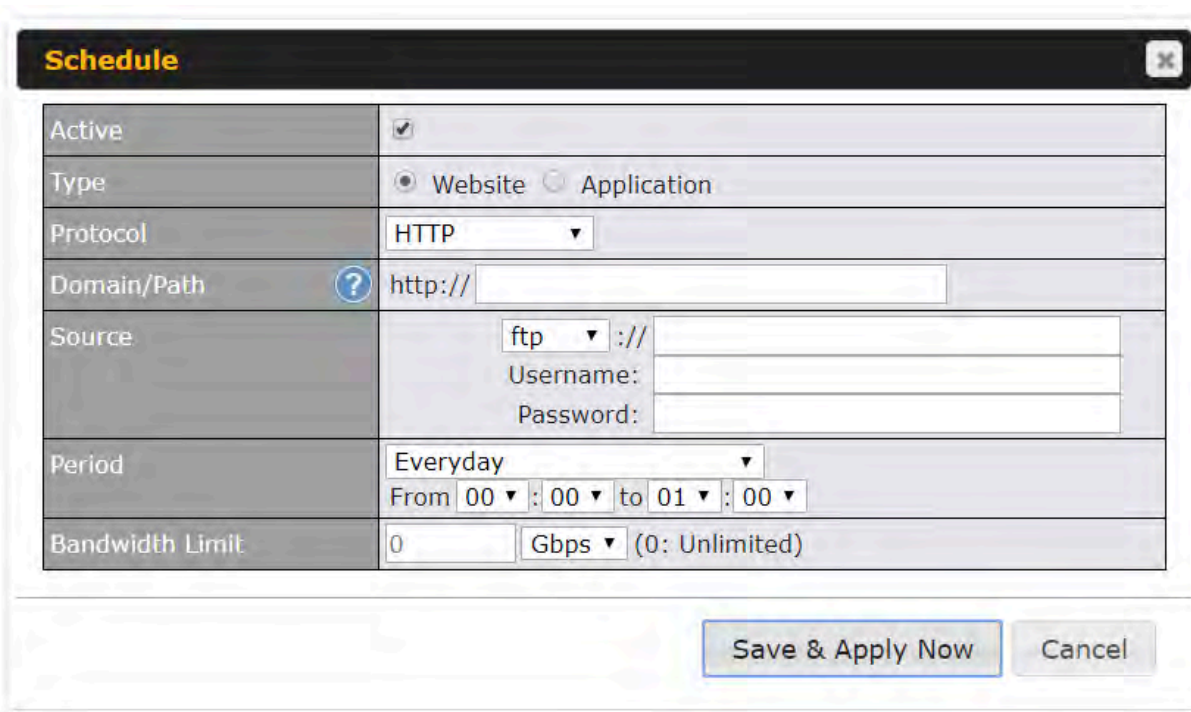
### 17.2 Configure a website for ContentHub

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.

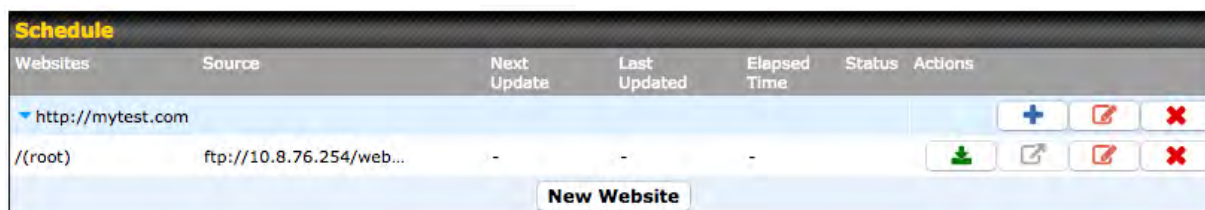
The content should be uploaded to an FTP server before you sync it with ContentHub.

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



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

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

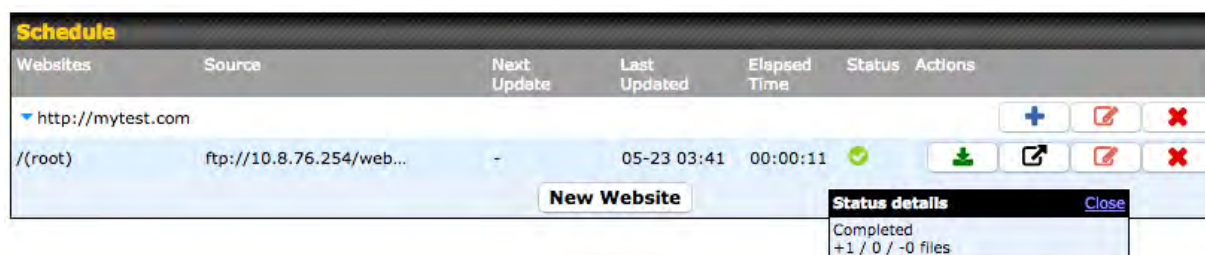


| Websites            | Source                   | Next Update | Last Updated | Elapsed Time | Status | Actions                                                                                                                                                                                                                                                                                                                                         |
|---------------------|--------------------------|-------------|--------------|--------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ▼ http://mytest.com |                          |             |              |              |        |                                                                                        |
| /(root)             | ftp://10.8.76.254/web... | -           | -            | -            |        |     |

**New Website**

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:



| 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     |  |     |

**New Website**

**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>).

## 17.3 Configure an application for 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:

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

**System**

- Admin Security
- Firmware
- Time
- Schedule
- Email Notification
- Event Log
- SNMP
- InControl
- Configuration
- Feature Add-ons
- Reboot

**Tools**

- Ping
- Traceroute
- Wake-on-LAN
- WAN Analysis
- Storage Manager
- Package Manager**

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

**Package List** Update All

|                                                                                                  |  |
|--------------------------------------------------------------------------------------------------|--|
| <b>Node.js</b><br>Version: 6.9.2 (17178)<br>Size: 8.92 MB<br>Date: Fri Feb 24 07:45:28 UTC 2017  |  |
| <b>Python</b><br>Version: 2.7.12 (17178)<br>Size: 20.29 MB<br>Date: Fri Feb 24 07:45:28 UTC 2017 |  |
| <b>Ruby</b><br>Version: 2.3.3 (17178)<br>Size: 31.44 MB<br>Date: Fri Feb 24 07:45:32 UTC 2017    |  |

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

**Schedule** ✕

|                 |                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------|
| Active          | <input checked="" type="checkbox"/>                                                              |
| Type            | <input type="radio"/> Website <input checked="" type="radio"/> Application                       |
| Protocol        | HTTP                                                                                             |
| Domain          | http://                                                                                          |
| Method          | <input checked="" type="radio"/> Sync <input type="radio"/> File Upload                          |
| Source          | ftp <input type="text"/> ://<br>Username: <input type="text"/><br>Password: <input type="text"/> |
| Period          | Everyday<br>From 00:00 to 01:00                                                                  |
| Bandwidth Limit | 0 Gbps (0: Unlimited)                                                                            |

Save & Apply Now Cancel

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.

## 18 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 routers with MediaFast, such as the MAX HD2 and the MAX HD4.

Due to the nature of Docker and its unlimited variables, this feature is supported by Peplink 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 Peplink 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>

## 19 QoS

### 19.1 User Groups

Other than the three default user groups, you can add more user groups by entering the group name into the column and clicking the '+' button. The user group limit is up to 10.

| User Group |   |
|------------|---|
| Name       |   |
| Manager    | X |
| Staff      | X |
| Guest      | X |
| Group#4    | X |
| Group#5    | X |
| Group#6    | X |
| Group#7    | X |
| Group#8    | X |
| Group#9    | X |
| Group#10   | X |
|            | + |

Save

### 19.2 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         |
| <input checked="" type="checkbox"/> | 50%           | 30%           | 20%           |
| WAN 1                               | 500.0M/500.0M | 300.0M/300.0M | 200.0M/200.0M |
| WAN 2                               | 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                     | <input checked="" type="checkbox"/> |           |  |           |                |
| User Bandwidth Limit       |                                     | Download  |  | Upload    |                |
|                            | Manager                             | Unlimited |  | Unlimited |                |
|                            | Staff                               | 0 Mbps    |  | 0 Mbps    | (0: Unlimited) |
|                            | Guest                               | 0 Mbps    |  | 0 Mbps    | (0: Unlimited) |

## 19.3 Application Queue

This section is to define the QoS Application Queue. You can set guaranteed bandwidth for a queue and assign it to applications.

| QoS Application Queue        |  |
|------------------------------|--|
| No Application Queue Defined |  |
| <a href="#">Add</a>          |  |

Click the Add button to create the QoS Application Queue.

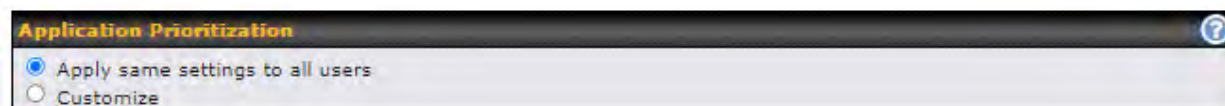
| Add Queue                                   |                                                                                                                          |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Name                                        | <input type="text"/>                                                                                                     |
| Bandwidth                                   | <input type="checkbox"/> Upload <input type="text"/> Mbps<br><input type="checkbox"/> Download <input type="text"/> Mbps |
| Borrow Spare Bandwidth                      | <input type="checkbox"/>                                                                                                 |
| <a href="#">Save</a> <a href="#">Cancel</a> |                                                                                                                          |

| Add Queue                     |                                                                                                                                                                         |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                   | This setting specifies a name for the QoS Application Queue.                                                                                                            |
| <b>Bandwidth</b>              | Bandwidth to be reserved (for each WAN connection) for this queue. When WAN is congested, this bandwidth will remain available for applications assigned to this queue. |
| <b>Borrow Spare Bandwidth</b> | Enable this option if you want this queue to utilize WAN's unused bandwidth.                                                                                            |

## 19.4 Application

### 19.4.1 Application Prioritization

On many Peplink routers, 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

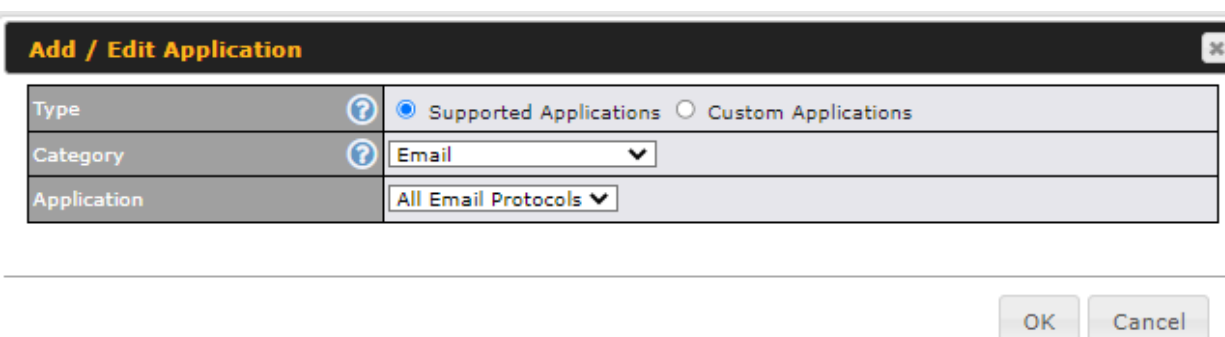
Three application priority levels can be set: **↑ High**, **— Normal**, and **↓ Low**. Peplink routers can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference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

| Application                          | Manager | Staff  | Guest  |   |
|--------------------------------------|---------|--------|--------|---|
| All Supported Streaming Applications | ↑ High  | ↑ High | ↑ High | ✖ |
| All Database Applications            | ↑ High  | ↑ High | ↑ High | ✖ |
| Add                                  |         |        |        |   |

### 19.4.2 Prioritization for Custom Applications

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 router 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: Email

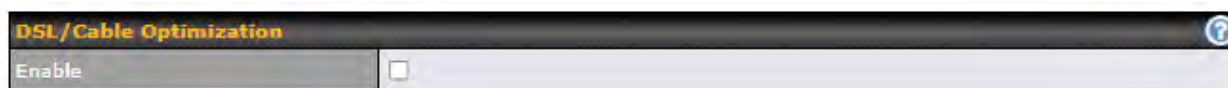
Application: All Email Protocols

OK Cancel

### 19.4.3 DSL/Cable Optimization

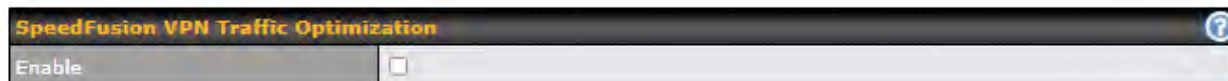
DSL/cable-based WAN connections have lower upload bandwidth and higher

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 disabled.



#### 19.4.4 SpeedFusion VPN Traffic Optimization

To enable this option to allow SpeedFusion VPN traffic has highest priority when WAN is congested.



## 20 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 routers supports the selective filtering of data traffic in both directions:

- 
- 
- Outbound (LAN to WAN)
- Inbound (WAN to LAN)
- Internal Network (VLAN to VLAN)
- Local Service

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

With SpeedFusion™ enabled, the firewall rules also apply to VPN tunneled traffic.

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

| Rule    | Protocol | Source | Destination | Action |  |
|---------|----------|--------|-------------|--------|--|
| Default | Any      | Any    | Any         | ✓      |  |

Add Rule

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

| Rule    | Protocol | WAN | Source | Destination | Action |  |
|---------|----------|-----|--------|-------------|--------|--|
| Default | Any      | Any | Any    | Any         | ✓      |  |

Add Rule

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

| Rule    | Protocol | Source | Destination | Action |  |
|---------|----------|--------|-------------|--------|--|
| Default | Any      | Any    | Any         | ✓      |  |

Add Rule

**Intrusion Detection and DoS Prevention**

Disabled

**Local Service Firewall Rules** ( Drag and drop rows by the left to change rule order)

| Rule    | Service | WAN | Source | Action |  |
|---------|---------|-----|--------|--------|--|
| Default | Any     | Any | Any    | ✓      |  |

Add Rule

## 20.1 Access Rules

### Outbound Firewall Rules

The outbound firewall settings are located at **Advanced > 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         | ✓      |   |

Add Rule

To enable or disable the Outbound Firewall to manage device local network traffic, click on the help icon and click [here](#), the screen will show below.

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

| Rule                                                                     | Protocol | Source | Destination | Action |   |
|--------------------------------------------------------------------------|----------|--------|-------------|--------|---|
| ⚠ Device local network traffic is now managed by Outbound Firewall Rules |          |        |             |        |   |
| ☰ test                                                                   | Any      |        |             | 🚫      | ✖ |
| ☰ test1                                                                  | Any      |        |             | 🚫      | ✖ |
| Default                                                                  | Any      | Any    | Any         | ✅      |   |
| Add Rule                                                                 |          |        |             |        |   |

## Note

To utilize the Outbound Firewall Rule to block the Peplink device from contacting InControl 2. may refer to the link below:

<https://forum.peplink.com/t/faq-prevent-device-reaching-incontrol-2./63f48fd466df34ab475f55/>

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

### Add a New Outbound Firewall Rule

#### New Firewall Rule

|                       |                                                                   |
|-----------------------|-------------------------------------------------------------------|
| Rule Name             |                                                                   |
| Enable                | <input checked="" type="checkbox"/> Always on                     |
| Protocol              | Any :: Protocol Selection Tool ::                                 |
| Source IP & Port      | Any Address                                                       |
| Destination IP & Port | Any Address                                                       |
| Action                | <input checked="" type="radio"/> Allow <input type="radio"/> Deny |
| Event Logging         | <input type="checkbox"/> Enable                                   |

Save Cancel

## Inbound Firewall Rules

Inbound firewall settings are located at **Advanced > 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         | ✔      |   |
| Add Rule                                                                      |          |     |        |             |        |   |

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

Add a New Inbound Firewall Rule

### New Firewall Rule

|                       |                                                                   |
|-----------------------|-------------------------------------------------------------------|
| Rule Name             |                                                                   |
| Enable                | <input checked="" type="checkbox"/>                               |
| WAN Connection        | Any                                                               |
| Protocol              | Any <small>Protocol Selection Tool</small>                        |
| Source IP & Port      | Any Address                                                       |
| Destination IP & Port | Any Address                                                       |
| Action                | <input checked="" type="radio"/> Allow <input type="radio"/> Deny |
| Event Logging         | <input type="checkbox"/> Enable                                   |

Save
Cancel

## Internal Network Firewall Rules

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

| Rule     | Protocol | Source | Destination | Action                              |                                     |
|----------|----------|--------|-------------|-------------------------------------|-------------------------------------|
| test     | Any      | Any    | Any         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Default  | Any      | Any    | Any         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Add Rule |          |        |             |                                     |                                     |

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

Add a New Internal Network Firewall Rule

### New Firewall Rule

|               |                                                                   |
|---------------|-------------------------------------------------------------------|
| Rule Name     |                                                                   |
| Enable        | <input checked="" type="checkbox"/> Always on                     |
| Protocol      | Any <small>Protocol Selection</small>                             |
| Source        | Any Address                                                       |
| Destination   | Any Address                                                       |
| Action        | <input checked="" type="radio"/> Allow <input type="radio"/> Deny |
| Event Logging | <input type="checkbox"/> Enable                                   |

Save
Cancel

| Inbound / Outbound / Internal Network Firewall Settings |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rule Name</b>                                        | This setting specifies a name for the firewall rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Enable</b>                                           | <p>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 the Peplink router based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Peplink router will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p>                                                                                    |
| <b>WAN Connection (Inbound)</b>                         | Select the WAN connection that this firewall rule should apply to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Protocol</b>                                         | <p>This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified:</p> <ul style="list-style-type: none"> <li>• Any</li> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• DSCP</li> <li>• IP</li> </ul> <p>Alternatively, the <b>Protocol Selection Tool</b> drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)</p> <p>After selecting an item from the <b>Protocol Selection Tool</b> drop-down menu, the protocol and port number remains manually modifiable.</p> |
| <b>Source IP &amp; Port</b>                             | <p>This specifies the source 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 <b>Source IP &amp; Port</b> setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the <b>Source IP &amp; Port</b> settings.</p>                                                                                                                                                     |
| <b>Destination IP &amp; Port</b>                        | <p>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 <b>Destination IP &amp; Port</b> setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the <b>Destination IP &amp; Port</b> settings.</p>                                                                                                                                      |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Action</b>        | <p>This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:</p> <ul style="list-style-type: none"> <li>• Source IP &amp; port</li> <li>• Destination IP &amp; port</li> </ul> <p>With the value of <b>Allow</b> for the <b>Action</b> setting, the matching traffic passes through the router (to be routed to the destination). If the value of the <b>Action</b> setting is set to <b>Deny</b>, the matching traffic does not pass through the router (and is discarded).</p>                                                                                                         |
| <b>Event Logging</b> | <p>This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page <b>Status&gt;Event Log</b>. A sample message is as follows:</p> <p>Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1<br/>DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80</p> <ul style="list-style-type: none"> <li>• <b>CONN</b>: The connection where the log entry refers to</li> <li>• <b>SRC</b>: Source IP address</li> <li>• <b>DST</b>: Destination IP address</li> <li>• <b>LEN</b>: Packet length</li> <li>• <b>PROTO</b>: Protocol</li> <li>• <b>SPT</b>: Source port</li> <li>• <b>DPT</b>: Destination port</li> </ul> |

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                                                     | TCP      | Any Any        | Any 21              | Deny   |  |
| Default                                                           | Any      | Any            | Any                 | Allow  |  |
| Add Rule                                                          |          |                |                     |        |  |

To remove a rule, click the button.

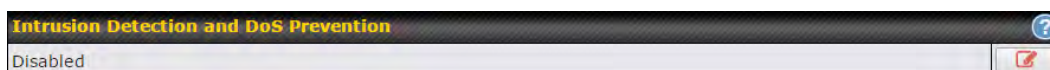
Rules are matched from top to bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match, the **Default** rule will be applied. By default,

the **Default** rule is set as **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



Peplink routers 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, and press the **Save** button.

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

- Port scan
  - o NMAP FIN/URG/PSH
  - o Xmas tree
  - o Another Xmas tree
  - o Null scan
  - o SYN/RST
  - o SYN/FIN
- SYN flood prevention
- Ping flood attack prevention

## Local Service Firewall Rules

For every WAN inbound traffic to local service, rules will be matched to take the defined action. The Local Service firewall settings are located at **Advanced > Firewall > Access Rules**.

| Local Service Firewall Rules <small>(Drag and drop rows by the left to change rule order)</small> |         |     |        |                                                                                       |  |
|---------------------------------------------------------------------------------------------------|---------|-----|--------|---------------------------------------------------------------------------------------|--|
| Rule                                                                                              | Service | WAN | Source | Action                                                                                |  |
| Default                                                                                           | Any     | Any | Any    |  |  |
| Add Rule                                                                                          |         |     |        |                                                                                       |  |

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

### Local Service Firewall Rule

|                |                                                                   |
|----------------|-------------------------------------------------------------------|
| Rule Name      | <input type="text"/>                                              |
| Enable         | <input checked="" type="checkbox"/>                               |
| Service        | <input type="text" value="Any"/>                                  |
| WAN Connection | <input type="text" value="Any"/>                                  |
| Source         | <input type="text" value="Any"/>                                  |
| Action         | <input checked="" type="radio"/> Allow <input type="radio"/> Deny |
| Event Logging  | <input type="checkbox"/>                                          |

| Local Service Firewall Settings |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rule Name</b>                | This setting specifies a name for the firewall rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Enable</b>                   | <p>This setting specifies whether the firewall rule should take effect.</p> <p>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.</p> <p>If the box is not checked, the firewall rule does not take effect. The Peplink Balance will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p>                               |
| <b>Service</b>                  | <p>This option allows you to define the supported local service to be matched.</p> <p>If Any is chosen, the firewall rule will match to all supported local services from the list.</p> <p>Via a drop-down menu, the following services can be specified:</p> <ul style="list-style-type: none"> <li>Any</li> <li>SpeedFusion / PepVPN Handshake</li> <li>SpeedFusion / PepVPN Data Port</li> <li>Web Admin Access</li> <li>DNS Server</li> <li>SNMP Server</li> <li>KVM Management Port</li> <li>KVM VNC Port</li> <li>FusionSIM Agent / Remote SIM Proxy</li> </ul> |
| <b>WAN Connection</b>           | Select the WAN connection that this firewall rule should apply to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Source</b>                   | This specifies the source IP address and IP Network to be matched for the firewall rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Action</b>                   | With the value of <b>Allow</b> for the <b>Action</b> setting, the matching traffic passes through the router (to be routed to the destination). If the value of the <b>Action</b> setting is set to <b>Deny</b> , 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

## 20.2 Content Blocking

**Application Blocking**
?

Please Select Application...
+

**Web Blocking**
?

Preset Category

☐ High
☐ Moderate
☐ Low
☒ Custom

☐ Adware
☐ P2P/File sharing
☐ Audio-Video
☐ Pornography
☐ File Hosting
☐ Update Sites

Content Filtering Database Auto Update
☐
?

Customized Domains
+
?

Exempted Domains from Web Blocking
+
?

**Exempted User Groups**
?

|         |                                 |
|---------|---------------------------------|
| Manager | <input type="checkbox"/> Exempt |
| Staff   | <input type="checkbox"/> Exempt |
| Guest   | <input type="checkbox"/> Exempt |

**Exempted Subnets**
?

| Network | Subnet Mask         |                  |
|---------|---------------------|------------------|
|         | 255.255.255.0 (/24) | + <span>?</span> |

Save

### 20.2.1 Application Blocking

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

### 20.2.2 Web Blocking

Defines website domain names to be blocked from LAN/PPTP/SpeedFusion VPN 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.

### 20.2.3 Customized Domains

Enter an appropriate website address, and the Peplink MAX will block and disallow LAN/PPTP/SpeedFusion™ peer clients to access these websites. Exceptions can be added using the instructions in Sections 20.1.3.2 and 20.1.3.3.

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

### 20.2.4 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 17.1** for details.

### 20.2.5 Exempted Subnets

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

## 21 Routing Protocols

### 21.1 OSPF & RIPv2

The Peplink supports OSPF and RIPv2 dynamic routing protocols.

Click the **Advanced** 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 | <input type="text" value="LAN IP Address"/>  |
| Area      | <div>Interfaces</div> <div>No OSPF Area Defined.</div> <div>Add</div>                                                           |

| RIPv2                                                                                                            |  |
|------------------------------------------------------------------------------------------------------------------|--|
| <div>No RIPv2 Defined.</div>  |  |

| OSPF & RIPv2 Route Advertisement |                                                                                                                                                                                                                                |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SpeedFusion VPN Route Isolation  | <input type="checkbox"/> Enable                                                                                                                                                                                                |
| Network Advertising              | <div> <input type="text" value="---"/>  </div> <div>All LAN/VLAN networks will be advertised when no network advertising is chosen.</div> |
| Static Route Advertising         | <input checked="" type="checkbox"/> Enable                                                                                                                                                                                     |
| Excluded Networks                | <div> <input type="text"/> <input type="text" value="255.255.255.0 (/24)"/>  </div>                                                       |
| <div>Save</div>                  |                                                                                                                                                                                                                                |

| 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 <b>Custom</b> 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 <b>Add</b> . To delete an existing area, click on the  . |