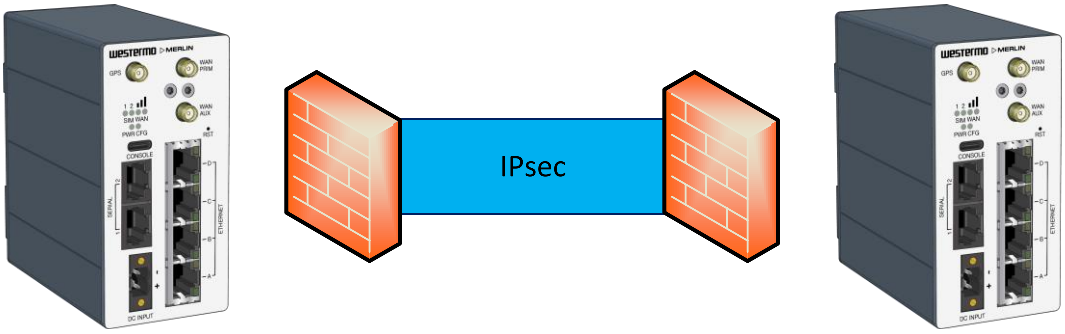
APPLICATION NOTE: AN-027-WUK

# Merlin Firewall Rules

Including IPSec, Traffic and Port Forwarding rules



## Overview

This application note shows how to configure the main Firewall functions within a Westermo Merlin 4407 router. However, it is applicable to all routers in the Merlin range.

Firmware version used: SXL-25.04.16.000

## Assumptions

This application note shows the Merlin-4407 router and assumes the router has a factory default configuration.

This application note can be applied to the other routers in the Merlin range.

## Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to support.uk@westermo.com

Requests for new Application Notes and Quick Notes can be sent to the same address.

# Introduction

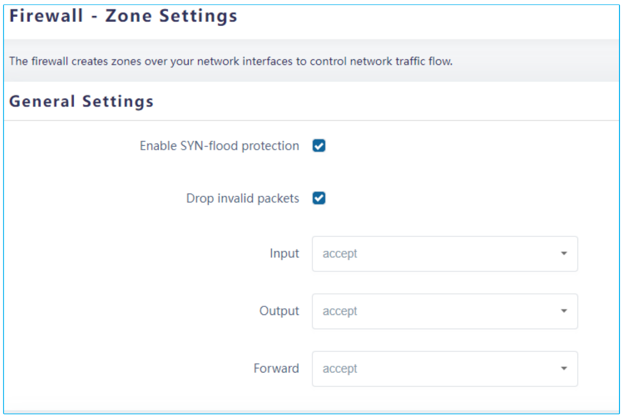
Merlin routers have a powerful firewall which allows for simple configuration through the web management or most application requirements or at a low level iptables for users who prefer more advanced command line setups.

This application note will show the typical steps required for firewall configuration through the web management for typical IPSec VPN use and user access.

A knowledge of IPSec VPN configuration is required and the setup is common for all Merlin and Virtual Access brand routers available from Westermo.

# General and Zones

The firewall has a default settings to catch any packets which fall outside the other zone settings or rules. The defaults is set to accept to aid a users initial configuration but should all be set to drop along with the users requirements for allowed and blocked traffic.



**Firewall - Zone Settings**

The firewall creates zones over your network interfaces to control network traffic flow.

**General Settings**

Enable SYN-flood protection ☑

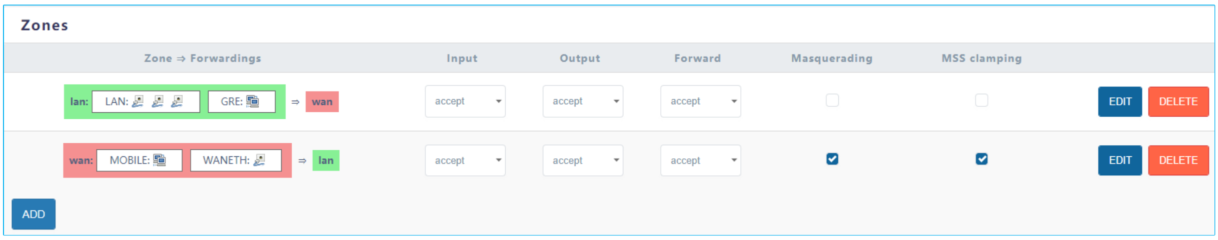
Drop invalid packets ☑

Input: accept

Output: accept

Forward: accept

Zones allow for grouping of interfaces under a set of firewall settings. By default there are zones for LAN and WAN so there is a clear separation between trusted and untrusted zones. Additional zones can be added for example a LAN for an end user and LAN2 for contractor access with additional restrictions



**Zones**

| Zone ⇒ Forwardings | Input | Output | Forward | Masquerading | MSS clamping | |
|---|---|---|---|---|---|---|
| lan: LAN: GRE: ⇒ wan | accept | accept | accept | □ | □ | EDIT DELETE |
| wan: MOBILE: WANETH: ⇒ lan | accept | accept | accept | ☑ | ☑ | EDIT DELETE |

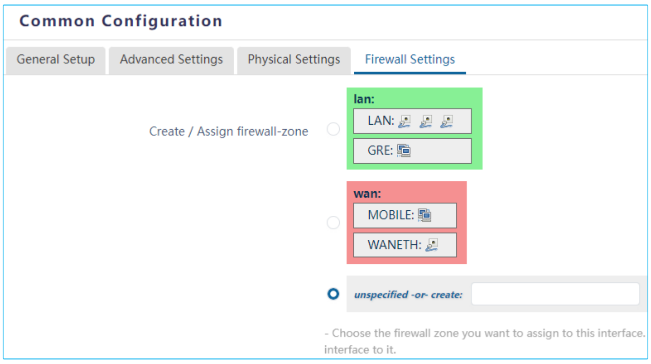
One example of grouping interfaces is in the example above where a trusted GRE tunnel has been added in the LAN zone. If a GRE interface was added to the WAN zone then the NAT/Masquerade setting would perform address translation on it.

# Adding an Interface to a Zone

An interface can be added to an existing zone or could have a new zone created for it.

To view and edit the firewall zone for an existing interface go to **Network -> Interfaces** and edit the interface either from the button at the end of the row or via the tab with the interface name and then under the Firewall tab

Typically it would be on creation of a new interface for example for a new local management LAN or for a GRE tunnel interface and then under the Firewall tab the same as for an existing interface. An existing zone can be selected or a new zone created using the text entry box for the new zone name which must be unique i.e. not LAN or WAN



Create / Assign firewall-zone

○ lan: LAN: GRE:

○ wan: MOBILE: WANETH:

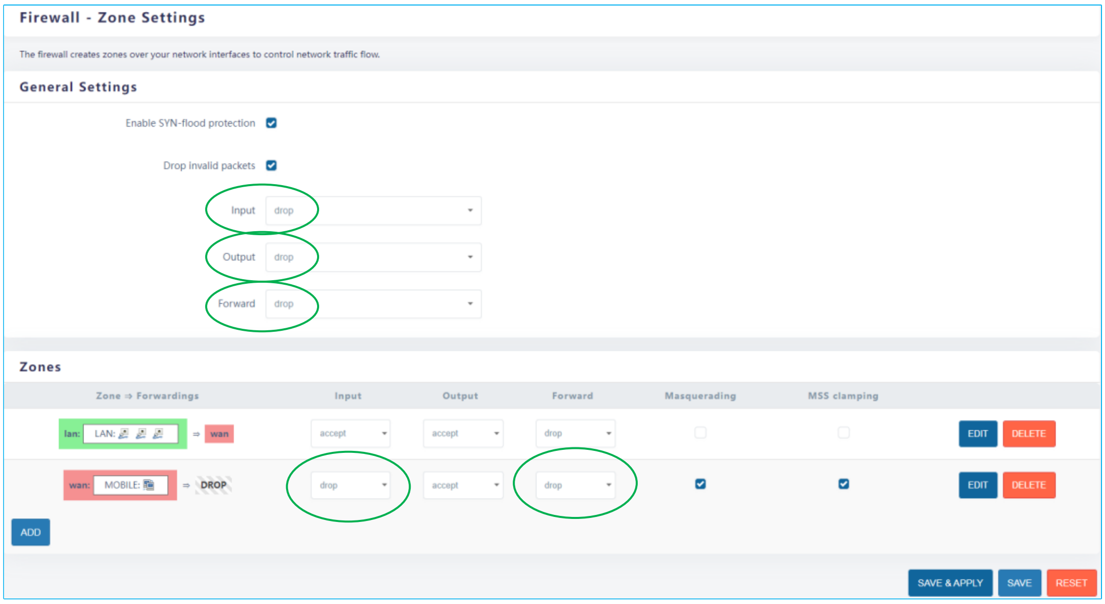
● *unspecified -or- create:*

- Choose the firewall zone you want to assign to this interface.
interface to it.

# Firewall Configuration Example

By default, the router's firewall for the WAN interface is set to OFF (accept) which allows all external traffic to the router. To block any unwanted traffic on the external interface it is necessary to turn it on (Drop) which will then block ALL traffic.  To allow only the desired traffic you will need to create specific firewall rules.

**Block incoming traffic**
From the main menu go to **Security** and then select **Firewall**. Scroll down to the bottom of the page to the **Zones** section and select **drop** from the drop-down boxes for the **Input** and **Forward** settings on the WAN: MOBILE interface (leave the Output setting as accept). Click on the **Save & Apply** button to activate the setting (see image below for desired setting).



**Firewall - Zone Settings**

The firewall creates zones over your network interfaces to control network traffic flow.

**General Settings**

Enable SYN-flood protection ☑

Drop invalid packets ☑

Input: drop

Output: drop

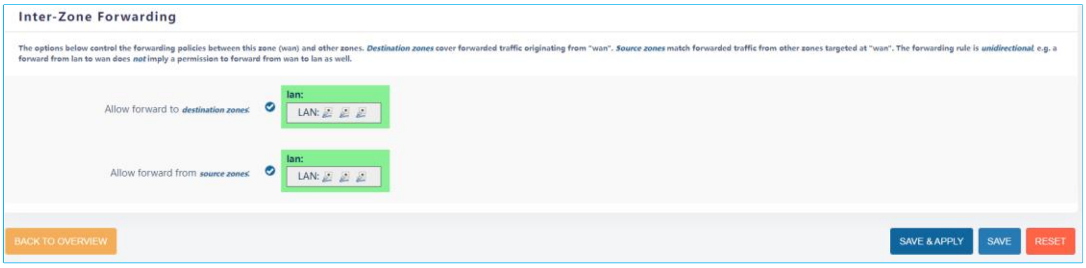
Forward: drop

**Zones**

| Zone ⇒ Forwardings | Input | Output | Forward | Masquerading | MSS clamping | |
|---|---|---|---|---|---|---|
| lan: LAN: ⇒ wan | accept | accept | drop | ☐ | ☐ | EDIT DELETE |
| wan: MOBILE: ⇒ DROP | drop | accept | drop | ☑ | ☑ | EDIT DELETE |

By setting the WAN to drop Forwarded traffic it will block ALL traffic from passing to the LAN, which will include any traffic being sent through any type of VPN. To specifically allow this type of traffic to reach the LAN a bi-directional ruleset is required in the WAN zone.

To do this click on the **Edit** button for the WAN zone and scroll down to the **Inter-zone Forwarding** section. Enable the **Allow forward to destination zones** rule, which should mean both rules are now enabled (see image below). Click on **Save & Apply** button.



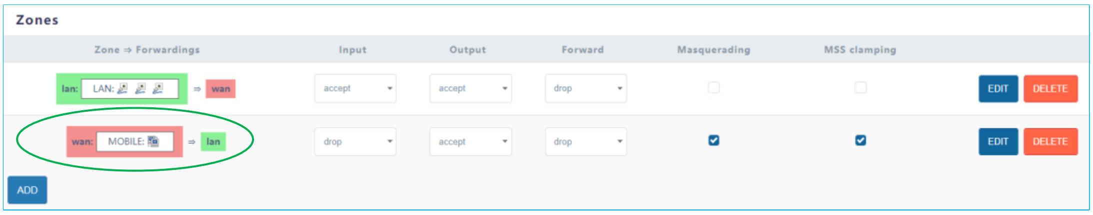
**Inter-Zone Forwarding**

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic originating from "wan". *Source zones* match forwarded traffic from other zones targeted at "wan". The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*: ☑ lan: LAN:

Allow forward from *source zones*: ☑ lan: LAN:

The WAN zone should now show that it can forward to the LAN:



Zones

| Zone ⇒ Forwardings | Input | Output | Forward | Masquerading | MSS clamping | |
|---|---|---|---|---|---|---|
| lan: LAN: ⇒ wan | accept | accept | drop | □ | □ | EDIT DELETE |
| wan: MOBILE: ⇒ lan | drop | accept | drop | ☑ | ☑ | EDIT DELETE |

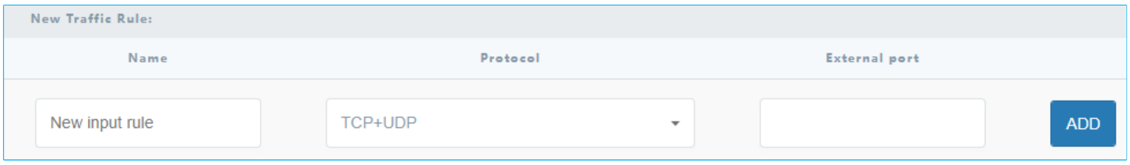
### Allowing Specific Traffic Inbound

To allow the desired traffic you then create specific rules in the **Traffic Rules** section of the firewall. For inbound traffic rules go to the '**Open ports on router**' section and create a rule.

For example, to create a rule that allows inbound pings to the WAN IP address:

*Name*: Allow-Ping (This a text reference)   *Protocol*: Other…   *External port*: (leave blank)

Then click on **Add** and it should bring up the page for the new rule and show all the other fields that are configurable. For this particular rule Example set the protocol field to 'ICMP'. All other default settings are suitable to allow incoming pings, so click on **Save & Apply** to create.



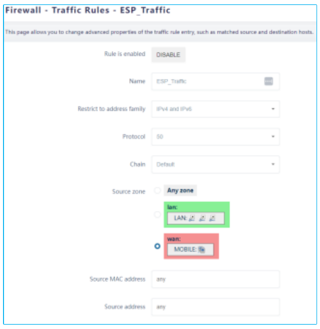
New Traffic Rule:

| Name | Protocol | External port | |
|---|---|---|---|
| New input rule | TCP+UDP | | ADD |

Now complete this process for all other traffic that is to be allowed into the router. In the case of IPSec VPN traffic, you need to create three separate rules:

- NAT-T UDP protocol port 4500
- IKE UDP protocol port 500
- ESP protocol 50

To configure a different protocol from those listed in the pulldown list just enter a label e.g. Esp_Traffic and then click the Add button and the extra setup for the rule with be shown. Select -custom- from the Protocol list and then edit it to the protocol required e.g. 50 for ESP then Save and Apply.



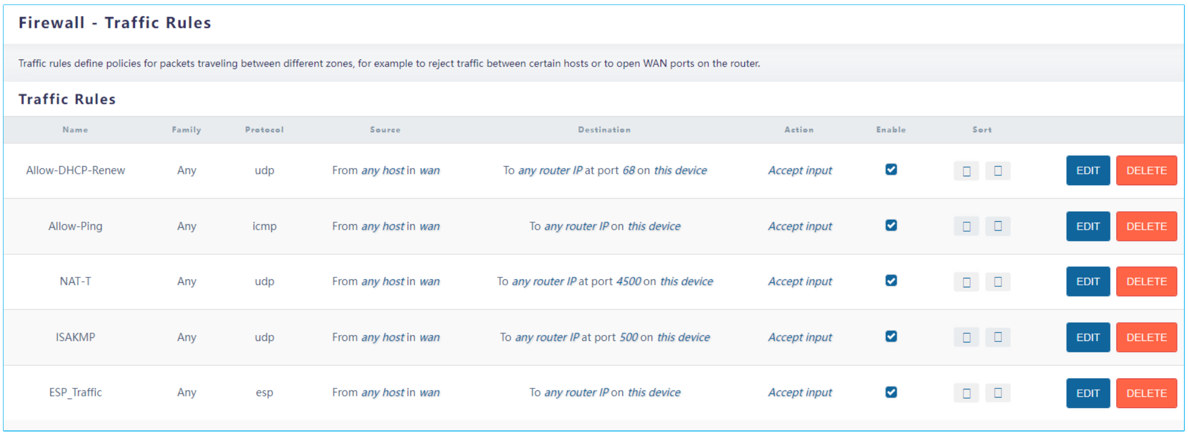
Firewall - Traffic Rules - ESP_Traffic

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

| | |
|---|---|
| Rule is enabled | DISABLE |
| Name | ESP_Traffic |
| Restrict to address family | IPv4 and IPv6 |
| Protocol | 50 |
| Chain | Default |
| Source zone | ○ Any zone<br>○ lan: LAN:<br>● wan: MOBILE: |
| Source MAC address | any |
| Source address | any |

You can further refine these rules if you want to restrict the IPSec connections from known IP addresses. When creating the rules just fill in the 'source address' field of the rule with the static IP address of the connecting device.

When complete your rule set should look like the list below:



**Firewall - Traffic Rules**

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

**Traffic Rules**

| Name | Family | Protocol | Source | Destination | Action | Enable | Sort | |
|---|---|---|---|---|---|---|---|---|
| Allow-DHCP-Renew | Any | udp | From *any host* in *wan* | To *any router IP* at port *68* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| Allow-Ping | Any | icmp | From *any host* in *wan* | To *any router IP* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| NAT-T | Any | udp | From *any host* in *wan* | To *any router IP* at port *4500* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| ISAKMP | Any | udp | From *any host* in *wan* | To *any router IP* at port *500* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| ESP_Traffic | Any | esp | From *any host* in *wan* | To *any router IP* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |

It is recommended to leave the ICMP (ping) rule enabled for testing and commissioning, and when the system has been fully tested you can disable the ICMP rule using the tick box.

# Firewall Status

A status page can be found under **Status -> Firewall** where packets counts can be seen against the low level firewall rule hits.

It is possible to reset the packet hit counters and to also restart the firewall which can be helpful when fault finding more complex rules to ensure the correct rule is being matched and the packet is not being resolved by another. In that case it is possible to re-order rules in the configuration screen.

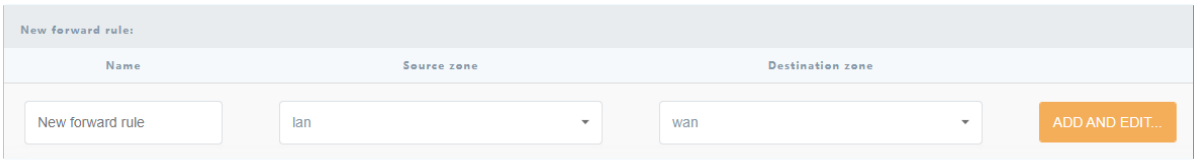
Input rules are traffic to the router, Output rules are from the router and forwarding rules are between zones/interfaces.

# Forwarding Rules

### Allowing Specific Traffic Outbound

The WAN firewall settings are currently set to allow all outbound traffic, which may not be desirable. In certain cases, you may want to restrict outbound traffic to prevent it being used for web browsing. Leave the Zones **Outbound** setting set to **accept** and create some rules to **deny** certain traffic.

For outbound traffic rules go to the '**New forward rule**' section and create a rule.



New forward rule:

| Name | Source zone | Destination zone | |
|---|---|---|---|
| New forward rule | lan | wan | ADD AND EDIT... |

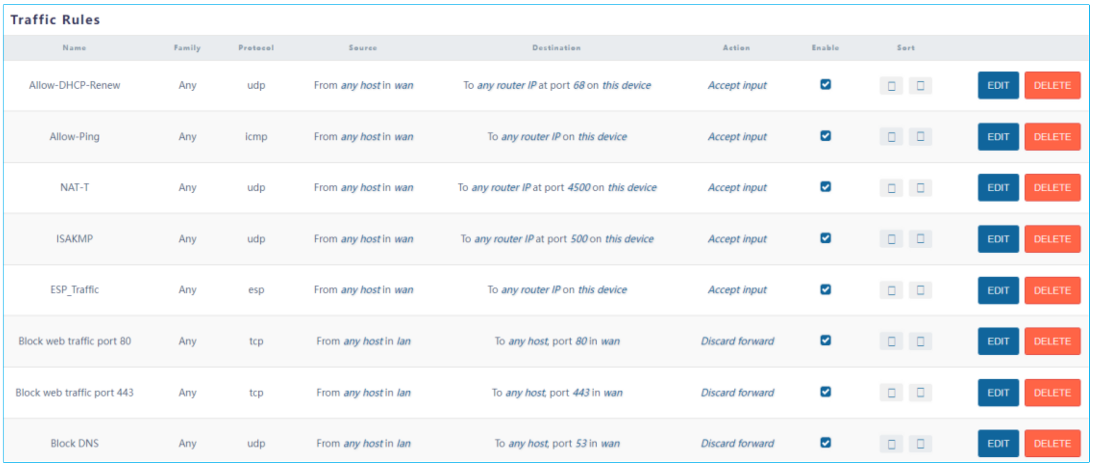
For example, to create a rule that denies outbound traffic to secure websites (https):

*Name*: Block web traffic (This a text reference) *Source zone*: lan *Destination zone*: wan

Then click on **Add and edit** and this will bring the rule page for editing. Set the **protocol** to **TCP**, the destination port to **443** and the **Action** to **drop**. Now click on the **Save & Apply** button.

You may also want to create an identical rule to block port 80, which is for unsecure websites (http). If the connected device is a Windows machine it may attempt to reach hosts on the internet for updating or other purposes. To block this traffic you can set up a rule to block DNS UDP port 53, which will stop it from resolving hostnames.

Once all three outbound rules are configured the rule set will look like this:



Traffic Rules

| Name | Family | Protocol | Source | Destination | Action | Enable | Sort | |
|---|---|---|---|---|---|---|---|---|
| Allow-DHCP-Renew | Any | udp | From *any host* in *wan* | To *any router IP* at port *68* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| Allow-Ping | Any | icmp | From *any host* in *wan* | To *any router IP* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| NAT-T | Any | udp | From *any host* in *wan* | To *any router IP* at port *4500* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| ISAKMP | Any | udp | From *any host* in *wan* | To *any router IP* at port *500* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| ESP_Traffic | Any | esp | From *any host* in *wan* | To *any router IP* on *this device* | *Accept input* | ☑ | □ □ | EDIT DELETE |
| Block web traffic port 80 | Any | tcp | From *any host* in *lan* | To *any host*, port *80* in *wan* | *Discard forward* | ☑ | □ □ | EDIT DELETE |
| Block web traffic port 443 | Any | tcp | From *any host* in *lan* | To *any host*, port *443* in *wan* | *Discard forward* | ☑ | □ □ | EDIT DELETE |
| Block DNS | Any | udp | From *any host* in *lan* | To *any host*, port *53* in *wan* | *Discard forward* | ☑ | □ □ | EDIT DELETE |

Note that the Allow-DHCP-Renew and Allow-Ping are default rules and can be edited, disabled or removed as required for the particular use case

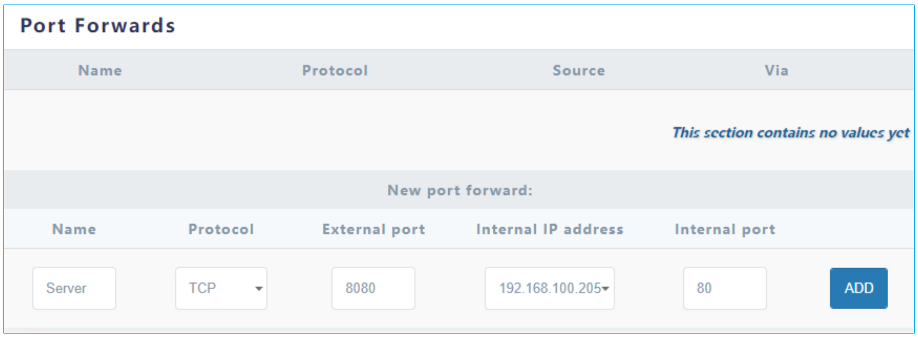
# Port Forwarding

Port forwarding can be useful to reach resources behind the Merlin router such as a servers web page. A WAN side device can direct its traffic towards the routers IP address and a defined port which will then be forwarded to a port on the device on the LAN.

In this example a PC on the WAN side needs to connect to the website using HTTP port 80 on a server on the LAN side of the router.

In **Security->Firewall**, select the Port Forwards tab and enter a name for the Port Forward rule, the protocol, Source port (the WAN port on the router), the IP address of the LAN side device and the internal port to use on the LAN side device then click Add and the Save and Apply when all Port Forward rules are complete.

In this example, to reach the Server the port 8080 is used on the Merlin and any traffic coming to the routers WAN IP directed at port 8080 will be forwarded to the Server on LAN side with IP 192.168.100.205 using the standard HTTP port 80.



Port Forwards

| Name | Protocol | Source | Via |
|---|---|---|---|
| | | | *This section contains no values yet* |

New port forward:

| Name | Protocol | External port | Internal IP address | Internal port | |
|---|---|---|---|---|---|
| Server | TCP | 8080 | 192.168.100.205 | 80 | ADD |

# Revision history for version 1.0

| Revision | Rev by | Revision note | Date |
|---|---|---|---|
| 00 | VC | Release version | 21/11/24 |
| 01 | | | |
| 02 | | | |
| 03 | | | |
| 04 | | | |
| 05 | | | |
| 06 | | | |
| 07 | | | |