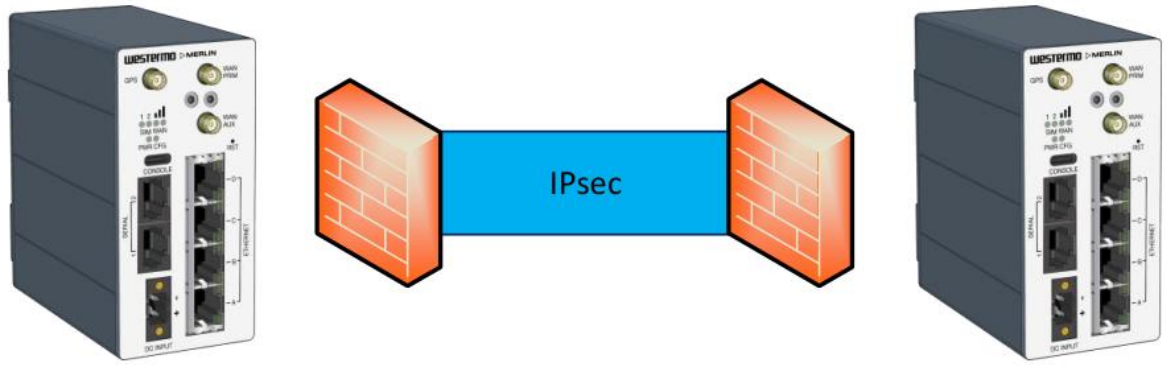
Merlin Firewall Rules

Including IPSec, Traffic and Port Forwarding rules



Hardware Models	Merlin Series (example: Merlin 4407)
Revision	1.1 (Rev. 00)
Date	13 November 2026
Firmware version	SXL-25.04.16.000
Brief description	Firewall configuration: IPsec, traffic rules and port forwarding

Contents

1 Overview 3
2 Introduction 3
3 Firewall Configuration Example 5
4 Firewall Status 7
5 Forwarding Rules 8
6 Port Forwarding 9
7 Using Firewall Logs for Intrusion Detection 9
8 Deep Packet Inspection (DPI) 10
9 Revision history 11

1 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.

1.1 Firmware information

Firmware version used: SXL-25.04.16.000

1.2 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.

1.3 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.

2 Introduction

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

This application note shows 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.

2.1 General and Zones

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

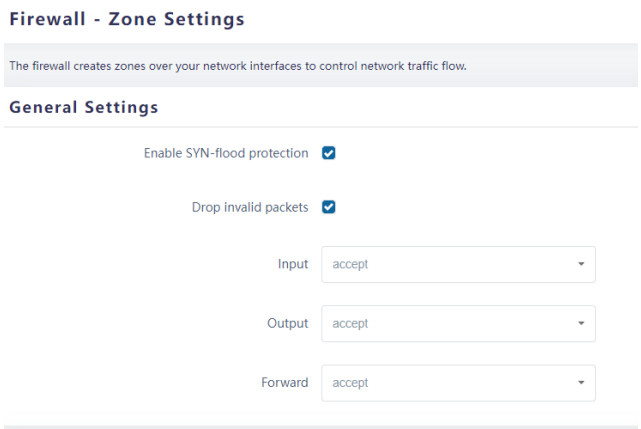


Figure 1: Firewall - Zone Settings / General Settings

Zones allow for grouping 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.

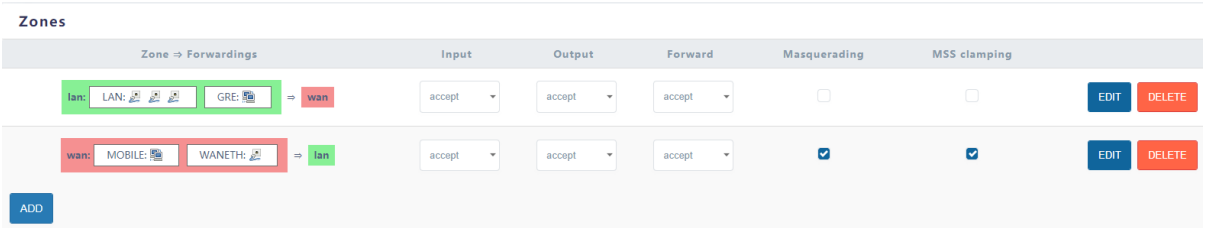


Figure 2: LAN and WAN firewall zones

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

2.2 Adding an Interface to a Zone

An interface can be added to an existing zone or a new zone can be 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, then under the **Firewall** tab.

Typically this would be done on creation of a new interface, for example a new local management **LAN** or a GRE tunnel interface, using the **Firewall** tab as for an existing interface. An existing zone can be selected, or a new zone created using the text entry box for a new, unique zone name (i.e. not **LAN** or **WAN**).

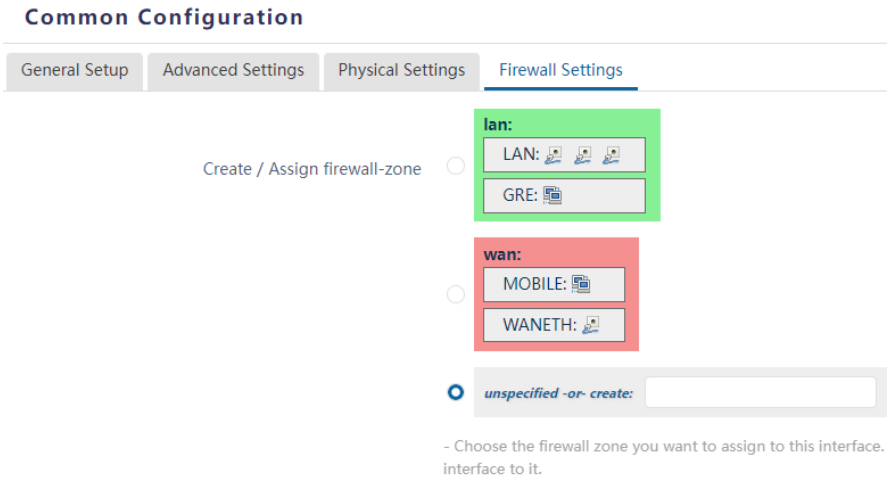


Figure 3: Assigning an interface to an existing or new firewall zone

3 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, specific firewall rules must be created.

3.1 Block incoming traffic

From the main menu go to **Security** and select **Firewall**. Scroll down to the bottom of the page to the **Zones** section and select drop from the **Input** and **Forward** drop-down boxes on the **WAN: MOBILE** interface (leave **Output** as accept). Click **Save & Apply** to activate the setting.

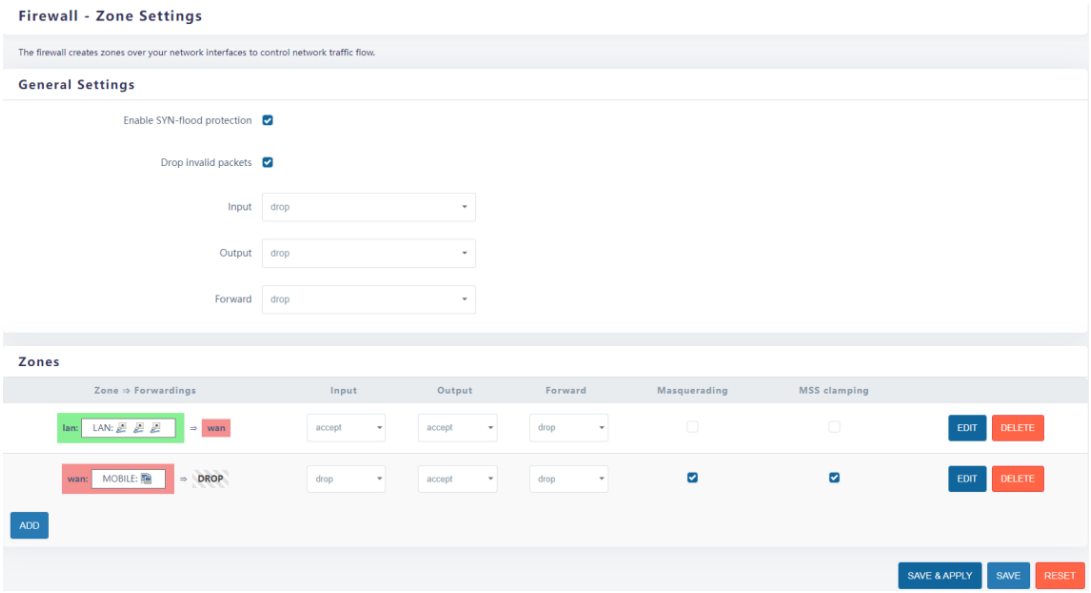


Figure 4: Setting WAN input and forward policies to drop

By setting the WAN to drop forwarded traffic, all traffic from passing to the LAN will be blocked, including any traffic 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.

Click **Edit** for the WAN zone and scroll down to **Inter-zone Forwarding**. Enable **Allow forward to destination zones**, which should mean both rules are now enabled. Click **Save & Apply**.



Figure 5: Inter-zone Forwarding options

3.2 Allowing Specific Traffic Inbound

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

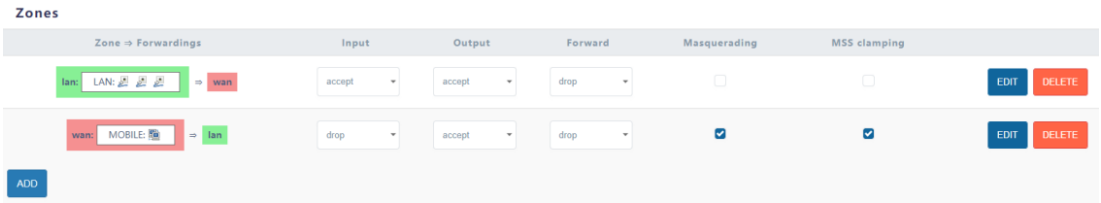


Figure 6: WAN zone forwarding to LAN

To allow the desired traffic, 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 (text reference) **Protocol:** Other… **External port:** (leave blank)

Click **Add** to display the new rule page with the remaining configurable fields. For this example, set the protocol field to **ICMP**. All other default settings are suitable to allow incoming pings. Click **Save & Apply** to create the rule.

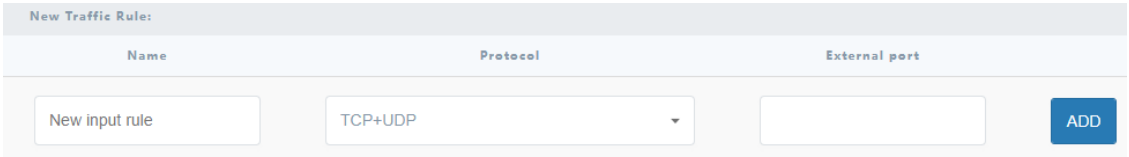


Figure 7: New input rule

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

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

To configure a different protocol from those in the drop-down list, enter a label (e.g. **Esp_Traffic**), click **Add**, then select **-custom-** from the **Protocol** list and change it to the required protocol (e.g. 50 for ESP). Click **Save & Apply**.



Figure 8: Custom ESP protocol (50)

These rules can be further refined to restrict IPSec connections to known IP addresses. When creating the rules, fill in the **source address** field with the static IP address of the connecting device.

When complete, the rule set should look like the example below:

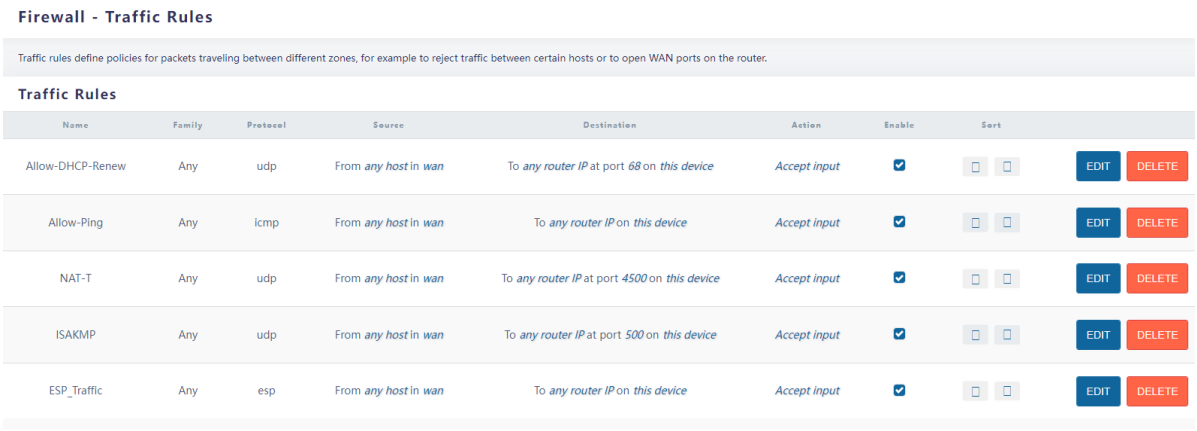


Figure 9: Completed inbound traffic rules

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

4 Firewall Status

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

It is possible to reset the packet hit counters and also restart the firewall, which can help with fault finding more complex rules to ensure the correct rule is being matched and the packet is not being resolved by another. Rules can be re-ordered in the configuration screen.

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

5 Forwarding Rules

5.1 Allowing Specific Traffic Outbound

The WAN firewall settings are currently set to allow all outbound traffic, which may not be desirable. In certain cases, outbound traffic may need to be restricted to prevent web browsing. Leave the **Zones Outbound** setting set to **accept** and create rules to deny certain traffic.

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

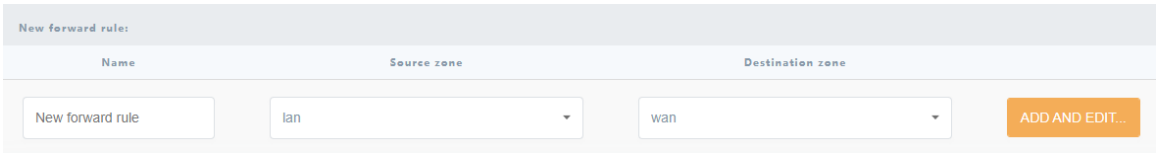


Figure 10: New forward rule

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

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

Click **Add and edit**. On the rule page, set **Protocol** to **TCP**, destination port to **443** and **Action** to **drop**. Click **Save & Apply**.

An identical rule can also be created to block port 80, used for unsecured websites (HTTP). If the connected device is a Windows machine, it may try to reach Internet hosts for updating or other purposes.

To block this traffic, create a rule to block DNS UDP port 53, which will stop the device from resolving hostnames.

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

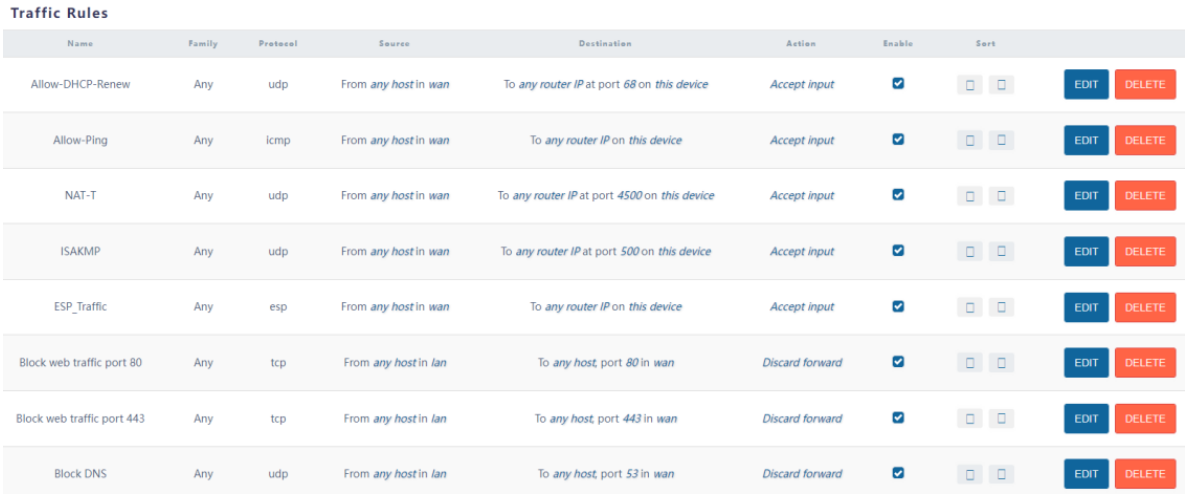


Figure 11: Outbound TCP/80, TCP/443 and UDP/53 restrictions

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.

6 Port Forwarding

Port forwarding can be useful to reach resources behind the Merlin router, such as a server's web page. A WAN-side device can direct its traffic to the router's 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 a 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 that device. Click **Add**, then **Save & Apply** when all port forwarding rules are complete.

In this example, port **8080** is used on the Merlin. Traffic reaching the router's WAN IP address on port **8080** is forwarded to the server on the LAN at **192.168.100.205** using the standard HTTP port **80**.

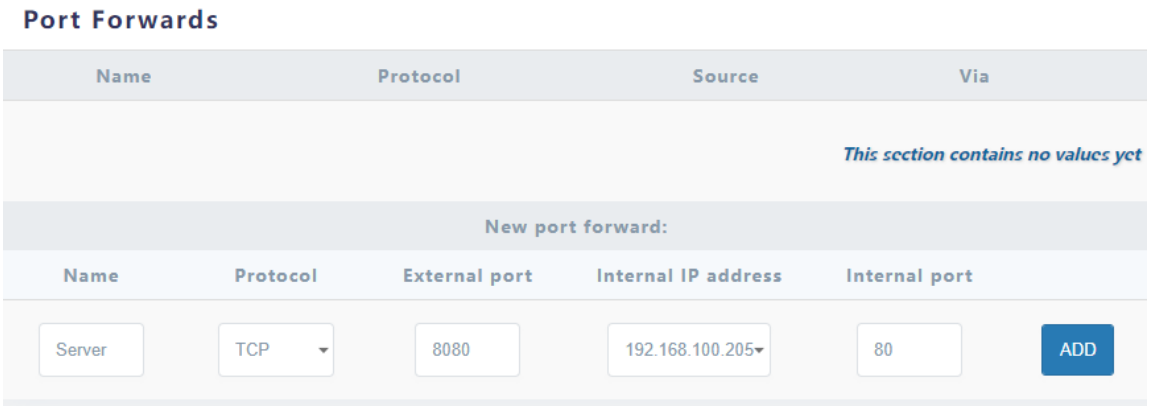


Figure 12: Forwarding WAN TCP/8080 to 192.168.100.205 TCP/80

7 Using Firewall Logs for Intrusion Detection

The Merlin firewall can be used to aid in intrusion detection by monitoring and logging dropped or rejected network traffic. These logs can help identify suspicious connection attempts, unauthorized access attempts, and potential network scanning activities.

To enable logging, navigate to **Security** → **Firewall** → **Zone** → **Advanced** and enable **"Raise events for dropped/rejected traffic in this zone"**.

Once enabled, firewall events will be recorded in the **System Log** for monitoring and troubleshooting.

Additionally, automated delivery of firewall events to a remote monitoring system or SIEM can be configured using the **Event System**, enabling centralized security monitoring and analysis.

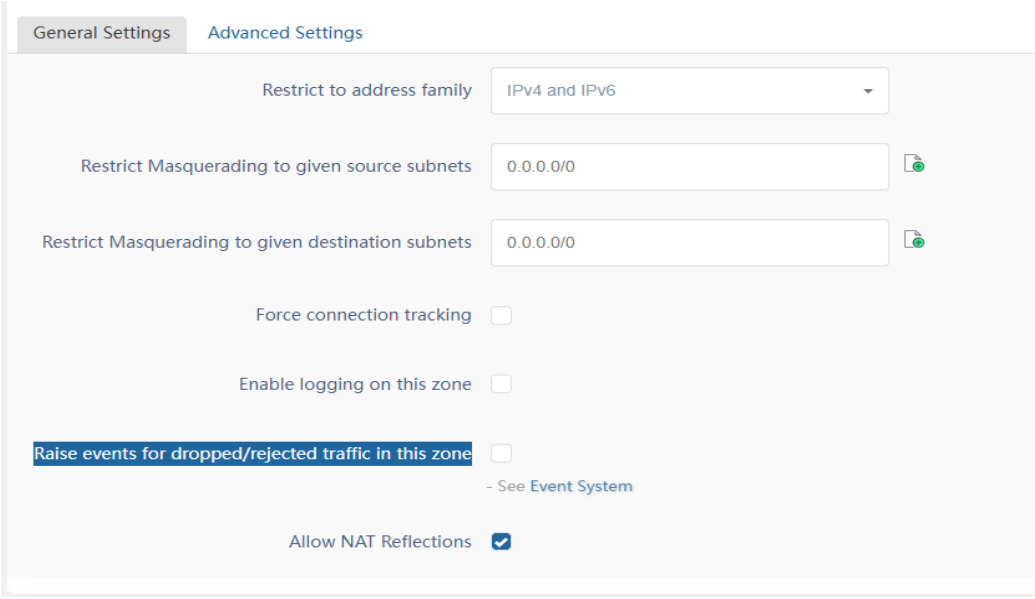


Figure 13: Firewall Logging

8 Deep Packet Inspection (DPI)

The Merlin firewall supports application-layer Deep Packet Inspection (DPI) for selected industrial SCADA protocols: **Modbus TCP, IEC 60870-5-104 (IEC104), and DNP3**.

Unlike standard firewall rules that filter traffic based on IP addresses, ports and protocols, DPI allows filtering based on fields within SCADA messages, such as function codes, register addresses and device addresses.

DPI is configured through **Security → Firewall → Traffic Rules**, using the **Extra arguments** field to specify protocol-specific matching conditions. These conditions can be combined with standard firewall rules to allow, reject or drop matching traffic.

Supported DPI Match Options

Modbus TCP (-m modbus)

The following matching options are supported:

- --id — Transaction identifier
- --prot — Protocol identifier
- --len — Message length
- --unit — Modbus Unit ID
- --fc — Modbus function code
- --reg — Register address

IEC104 (-m iec104)

The following matching options are supported:

- --typeid — ASDU Type Identifier
- --varsq — Variable Structure Qualifier
- --cot — Cause of Transmission
- --oa — Originator Address
- --casdu — Common ASDU Address

DNP3 (-m dnp3)

The following matching options are supported:

- --destination-addr or --daddr — DNP3 destination address
- --source-addr or --saddr — DNP3 source address
- --function-code or --fc — DNP3 application function code

Most options support matching individual values or ranges using the start:end syntax. DNP3 function codes additionally support comma-separated lists of values.

Examples of DPI Rules

Modbus TCP — Match Read Holding Registers (FC03) for Unit ID 7

-m modbus --unit 7 --fc 3

IEC104 — Match Single Point Information (Type ID 1) for Common ASDU Address 7

-m iec104 --typeid 1 --casdu 7

DNP3 — Match Confirm, Read and Write commands (FC 0, 1, 2) for Destination Address 1

-m dnp3 --daddr 1 --fc 0,1,2

These expressions are entered in the **Extra arguments** field of the corresponding traffic rule. The rule's action determines whether matching packets are accepted, dropped or rejected.

Note: DPI is limited to the three supported SCADA protocols

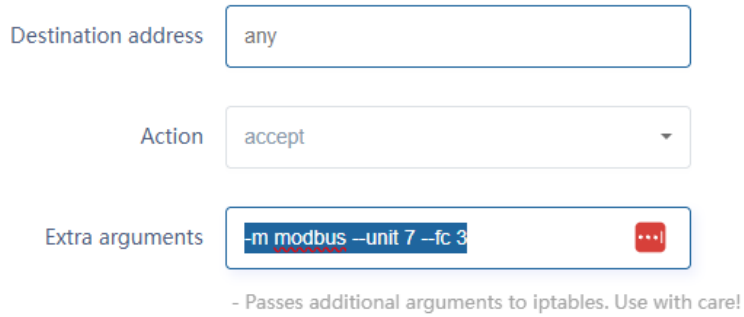


Figure 14: Deep packet inspection

9 Revision history

Revision	Rev by	Revision note	Date
00	VC	Release version	21/11/24
01	AW	Added section 7 and 8	13/11/26
02			
03			
04			
05			
06			
07			