Industrial Ethernet Training 12

Configuring the firewall on a Weidmueller security router

Abstract:

The Firewall is the main security feature of your network. It allows you to filter packets over your router on Layer 2 and 3 (OSI model) meaning that unauthorized or potentially dangerous traffic cannot enter the network and cause any harm to it. This application note shows a configuration for a router with activated packet filtering for a specific use case and explains the general functionality of the packet filtering firewall of the Weidmueller security router.

Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	IE-Training Kit-01	2881730000	1.1.2 (Build 125086)
2			
3			

IE-Training Kit Content

No.	Component name	Article No.	Hardware / Firmware version
1	IE-SR-4TX	2751270000	1.4.7
2	IE-SW-AL08M-8TX	2682280000	1.08
3	IE-SW-AL05M-5TX	2682250000	1.14
4	IE-CS-MBGW-2TX-1COM	2682600000	3.11

Software reference

No.	Software name	Article No.	Software version
1			
2			
3			

File reference

No.	Name	Description	Version
1			
2			

Contact
Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
www.weidmueller.com

For any further support please contact your local sales representative:
https://www.weidmueller.com/countries

Content

1 Warning and Disclaimer

Warning
Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer
This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

Note
The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

Security notes
In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

2 Prerequisites for doing

You need to have the following hardware and documentation

- Via Ethernet connected Industrial Ethernet Training Kit
- Application Note Industrial Ethernet Training 01 “Setting up default configuration of IE Training Kit” to apply a default IP address configuration
- Application Note Industrial Ethernet Training 02 “Example application of the Serial Converter and TCP/RTU Gateway”
- Application Note Industrial Ethernet Training 10 “Routing”

Note: *The mentioned Application Notes (except Industrial Ethernet Training 01) are only mandatory for performing the exact use case we are exemplifying in this Application Note. These are optional, if you only want to understand the functionality of the firewall of the Weidmueller security router and implement it by yourself.*

3 Why do I need a Firewall?

A firewall is a digital security system that checks all incoming and outgoing traffic on a network according to a defined set of rules. Hence, a firewall blocks unauthorized traffic and only allows communications that are deemed safe, using a set of security rules that we are going to set up. This enhances the company's IT security and can, for example prevent disturbances in production line.

4 How does a Firewall work?

A firewall works by filtering incoming and outgoing traffic from a network. The Internet Protocol (IP) sends data in so called “*Packets*”, which have various information attached to them like the source and destination address and of course all the data send within this packet. A Packet filtering firewall, which is used by our Industrial Security Router can filter network traffic. It filters the content based on a set of rules, that can be individually defined by the user.

In case a packet, and more importantly its content, does not comply with the set of rules we defined, it is denied further network access. The mentioned network can be the company’s corporate network or the network in the production hall. Therefore, these measurements are taken to protect valuable data against cyberattacks like a distributed denial of service (DDoS). A so-called DDoS attack tries to overwhelm the network with an immense amount of traffic to break its infrastructure, which is not possible if the incoming traffic is analyzed and blocked in-time.

Since we are in an industrial environment and know our production machines and their data, we work with the firewall in the opposite direction. We block all incoming traffic to this network, except network from our known machines. This is the most secure option in our industrial network environment against any possible cyber-attack.

5 Packet filter firewall

As mentioned before, we are going to demonstrate the functionality of a packet filter firewall on the router. To showcase a proper configuration and how it works in general, we are going to reject for test purposes all incoming data except from the sensor and the Training Kit devices. Moreover, we connect the computer to the WAN port of the router. This means that we need to change the computer's IP address to the same network as the WAN port in order to connect to the device(*10.10.10.x*).

1. First, connect to the router's web interface by typing "*10.10.10.10*" into the URL field of your browser and then log in with your credentials. Navigate in the menu tree to "*Configuration*" and click on "*Packet filter*". Once in the menu, we have to delete the default setting called "*Allow_L3*" because this accepts any incoming traffic as of now. To do this, click on the trash can on the right side and then on the button "*delete*". After deleting the ruleset, click on "*Apply settings*" at the bottom to apply the new firewall rules.

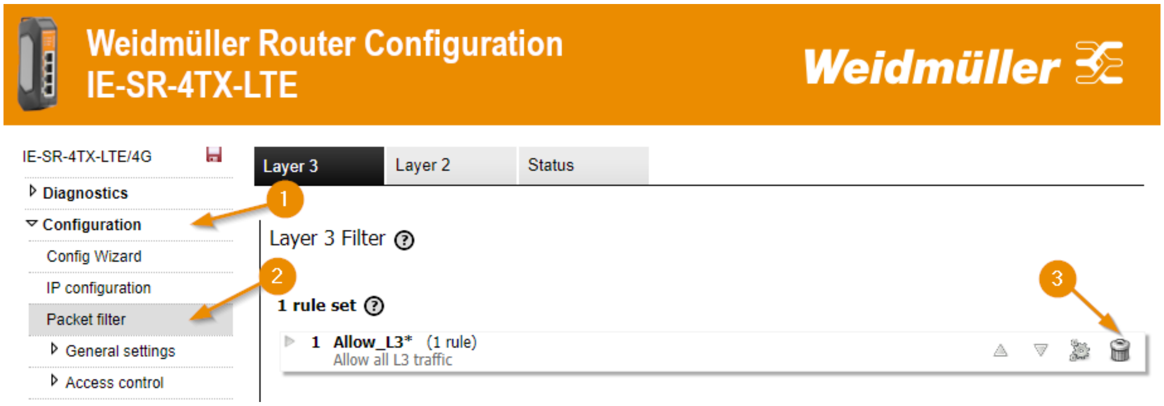
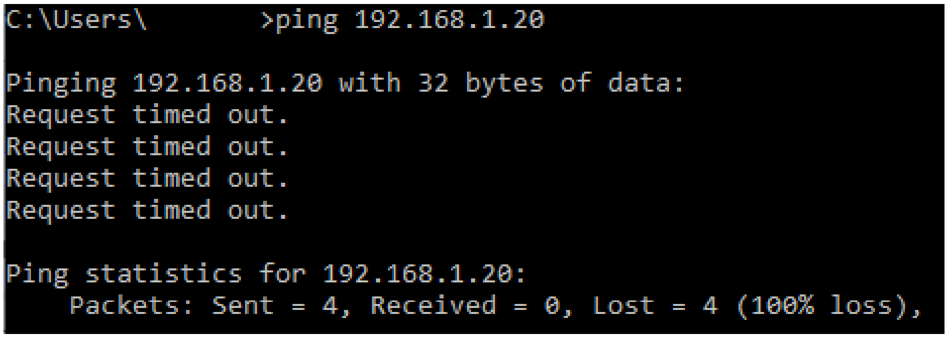


Figure 1: Deleting allow all ruleset

2. After applying the settings, any traffic coming from outside the "*10.10.10.x*" network is discarded. Therefore, we can no longer connect to the devices on the Training Kit since they are using the "*192.168.1.x*" network. We can check this by trying to ping the 8-port switch on the Training Kit in the Command Prompt. The request times out and we cannot ping it.



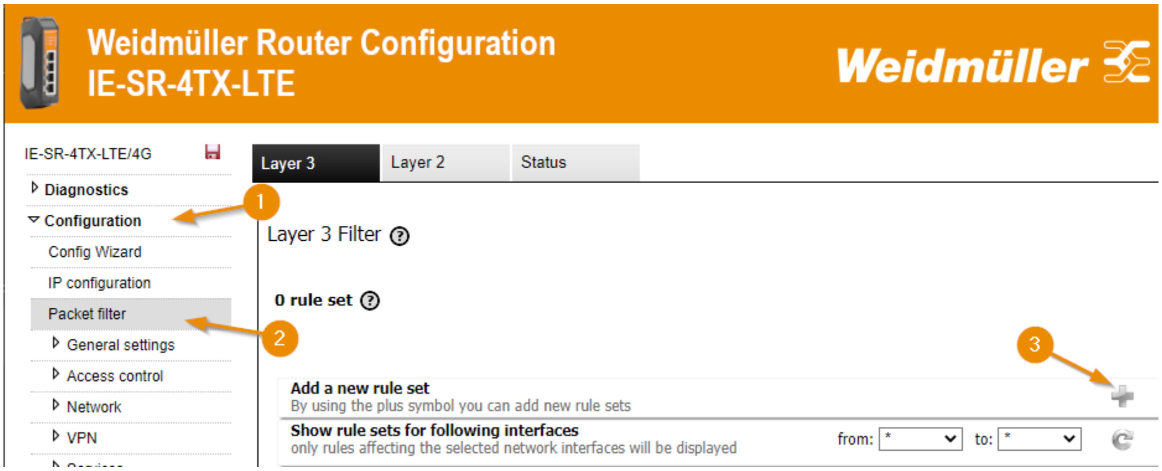
```
C:\Users\       >ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 2: Pinging switch outside of WAN network

3. To connect back to the "*192.168.1.x*" network, we must configure new rule sets that allow incoming traffic from our known devices from that network. This is also done in the menu "*Packet filter*" under "*Configuration*". Click on the grey "+" on the right-hand side and a new window opens up where we can create a new rule set.



Layer 3 Filter

0 rule set

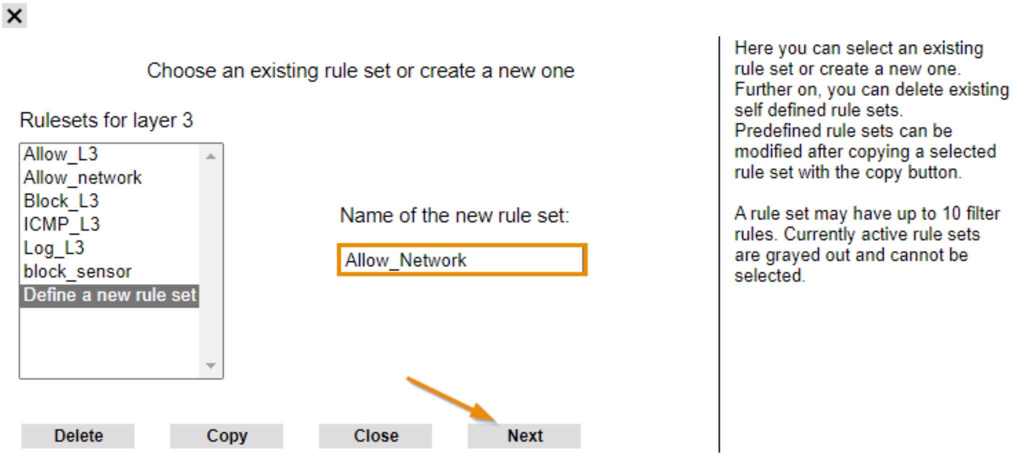
Add a new rule set
By using the plus symbol you can add new rule sets

Show rule sets for following interfaces
only rules affecting the selected network interfaces will be displayed

from: * to: *

Figure 3: Creating new rule set

4. Now, a pop-up window opens, where we can choose an existing rule set or create a new one. As already mentioned, we want to permit the networks to communicate with each other. Therefore, select "*Define a new rule set*" and enter a name with 15 or less characters. We will call it "*Allow_Network*" to know what this rule is supposed to do and then press "*Next*".



Choose an existing rule set or create a new one

Rulesets for layer 3

- Allow_L3
- Allow_network
- Block_L3
- ICMP_L3
- Log_L3
- block_sensor
- Define a new rule set

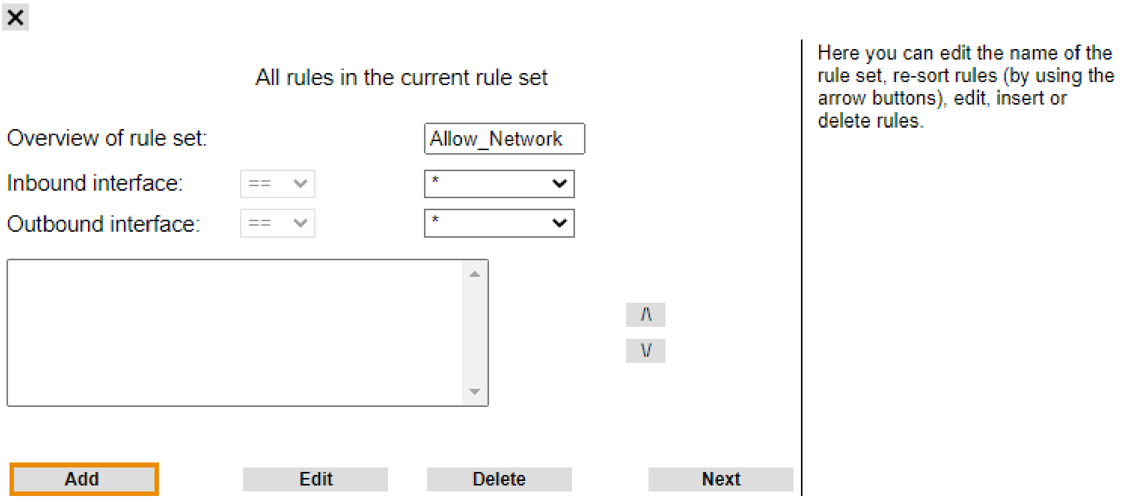
Name of the new rule set: Allow_Network

Here you can select an existing rule set or create a new one. Further on, you can delete existing self defined rule sets. Predefined rule sets can be modified after copying a selected rule set with the copy button.

A rule set may have up to 10 filter rules. Currently active rule sets are grayed out and cannot be selected.

Figure 4: Naming new rule set

5. The next settings require a configuration of the inbound and outbound interface that will be filtered. We have several options in the drop-down menu of what network interfaces should be scanned, for example the LAN or WAN interface. Selecting the "*" option means, that all interfaces are scanned by this rule set, which is the most secure option. Press "*Add*" to insert a new rule for this rule set.



All rules in the current rule set

Overview of rule set: Allow_Network

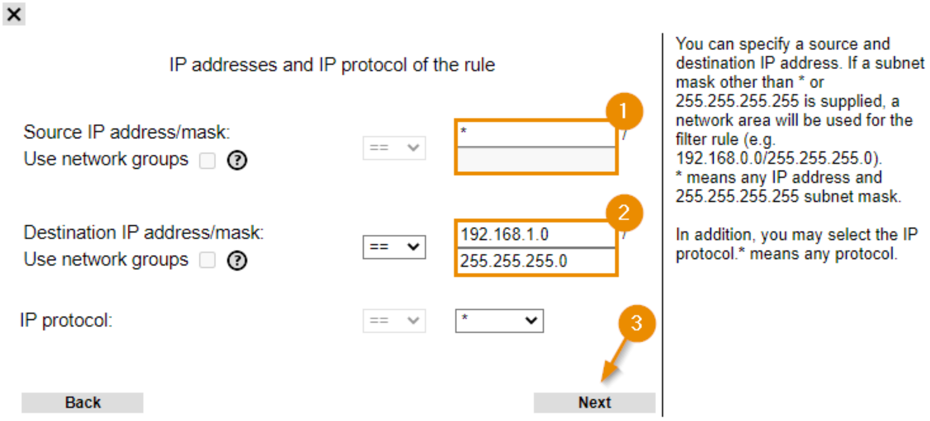
Inbound interface: == *

Outbound interface: == *

Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

Figure 5: Adding new rule set

6. To add a new rule, we must enter a source IP address from which the packets should be scanned. We type "*" into the "*Source IP address/mask*" field, defining that all incoming traffic from any IP address is scanned. The destination, in this case, the network whose incoming traffic should be scanned, is the IP "*192.168.1.0*". Thus, enter "*192.168.1.0*" as the IP and "*255.255.255.0*" as the subnet mask in the "*Destination IP address/mask*" field. The 0 at the end defines that we mean any device in this network, which is also declared within the subnet mask by having a 0 in the last position. This is important to do because a subnet mask of "*255.255.255.255*" means that we exclusively scan the IP "*192.168.1.0*" and not the whole "*192.168.1.x*" network. After that, click on "*Next*".



IP addresses and IP protocol of the rule

Source IP address/mask: == *
Use network groups □

Destination IP address/mask: == 192.168.1.0 / 255.255.255.0
Use network groups □

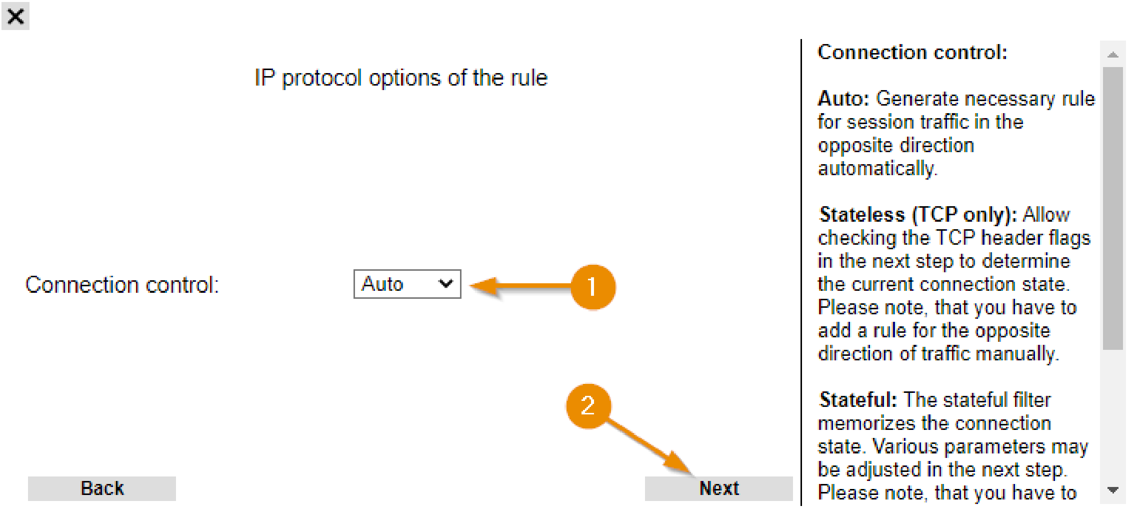
IP protocol: == *

You can specify a source and destination IP address. If a subnet mask other than * or 255.255.255.255 is supplied, a network area will be used for the filter rule (e.g. 192.168.0.0/255.255.255.0).
* means any IP address and 255.255.255.255 subnet mask.

In addition, you may select the IP protocol.* means any protocol.

Figure 6: IP addresses of the rule

7. Afterwards, select a connection control. Opting for “*Auto*” means, that the necessary traffic rules to scan the packets are generated automatically, whereas the other options like “*Stateless*” or “*Manual*” require a further configuration of the traffic connection and various parameters. We can simply select “*Auto*” in the drop-down to automatically generate the necessary rules and press “*Next*”.



IP protocol options of the rule

Connection control: Auto

Connection control:

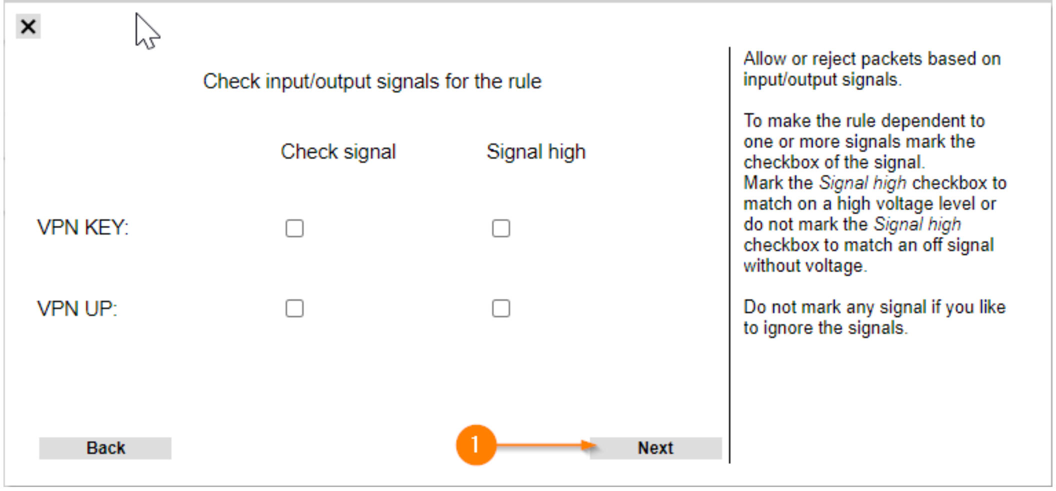
Auto: Generate necessary rule for session traffic in the opposite direction automatically.

Stateless (TCP only): Allow checking the TCP header flags in the next step to determine the current connection state. Please note, that you have to add a rule for the opposite direction of traffic manually.

Stateful: The stateful filter memorizes the connection state. Various parameters may be adjusted in the next step. Please note, that you have to

Figure 7: Connection control of rule set

8. In the next step we are asked to select the input/output signals for the rule. These rules include the “*VPN KEY*” and “*VPN UP*” option. “*VPN KEY*” is a setting that is usually activated by a VPN key which works via an analog switch. This setting allows or rejects the connection via VPN. “*VPN UP*” checks whether someone is connected via VPN or not. We are going to leave these settings on default (unmarked) since they do not matter for the incoming traffic from the network.



Check input/output signals for the rule

	Check signal	Signal high
VPN KEY:	□	□
VPN UP:	□	□

Allow or reject packets based on input/output signals.

To make the rule dependent to one or more signals mark the checkbox of the signal.
Mark the *Signal high* checkbox to match on a high voltage level or do not mark the *Signal high* checkbox to match an off signal without voltage.

Do not mark any signal if you like to ignore the signals.

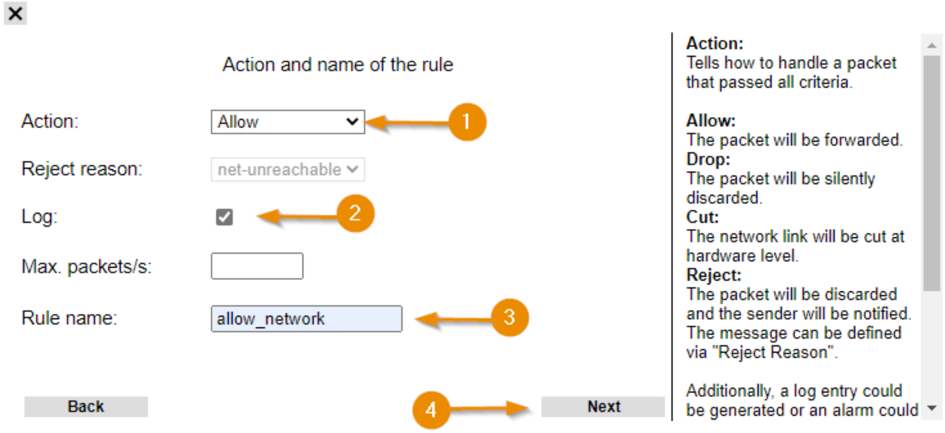
Figure 8: VPN settings of rule set

9. Lastly, we define the action the firewall takes when it detects a packet that fits the configuration we have implemented so far. Logically, we want to allow the packet. In this case, we can choose “Allow” in the drop-down menu “*Action*”.

   If we want to reject any packets, we could use one of the following options:

   - *Drop: The packet gets discarded without further notification*
   - *Cut: The network connection will be cut on hardware level when a malicious packet is detected*
   - *Reject: The packet gets discarded, and sender is notified about rejection*

   Moreover, we check the “*Log*” checkbox. It is useful to follow and track all the incoming traffic that got blocked or approved by the firewall. Also, we do not want to define a maximum number of packets per second so leave this box empty. We name the action “*allow_network*” in order to be able to identify the exact purpose of this ruleset for further usage and click “*Next*” afterwards.



Action and name of the rule

Action: Allow
Reject reason: net-unreachable
Log: ☑
Max. packets/s:
Rule name: allow_network

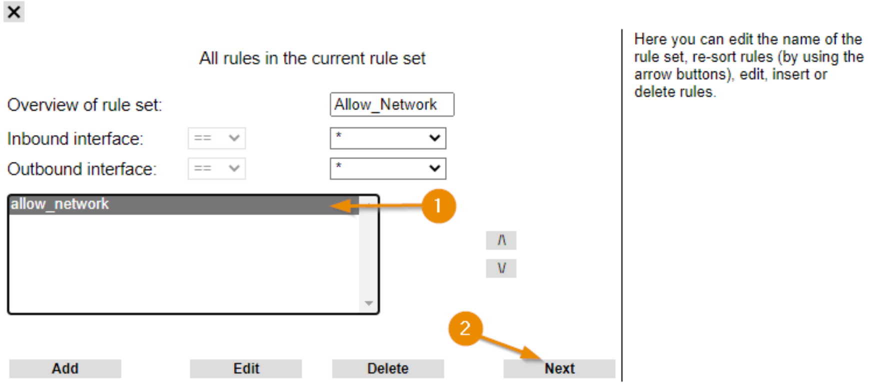
Action:
Tells how to handle a packet that passed all criteria.

Allow:
The packet will be forwarded.
Drop:
The packet will be silently discarded.
Cut:
The network link will be cut at hardware level.
Reject:
The packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".

Additionally, a log entry could be generated or an alarm could

Figure 9: Action and name of rule set

10. We are now back in the menu of step 4. Since we have configured our own ruleset, we can add it by marking it and then pressing “*Next*”.



All rules in the current rule set

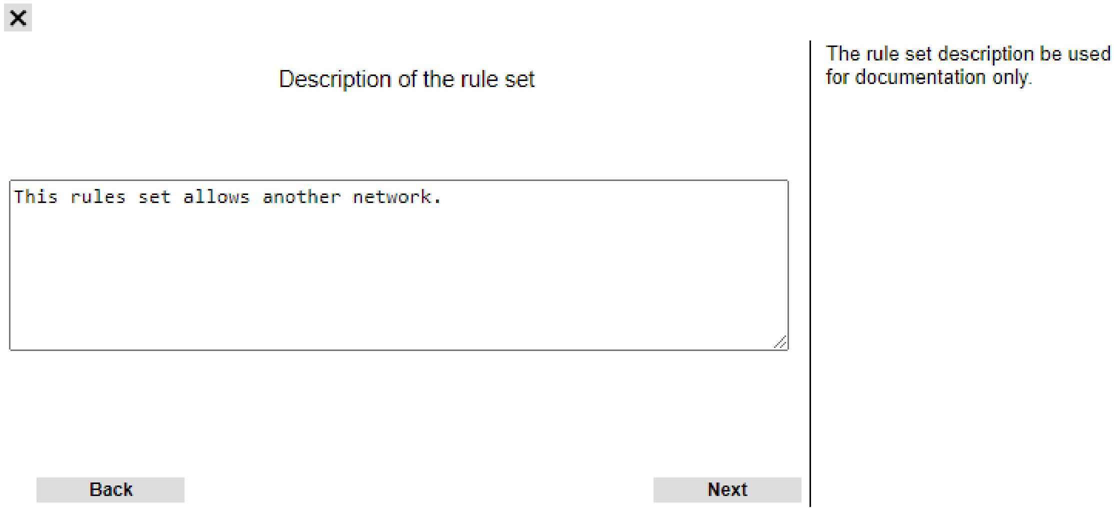
Overview of rule set: Allow_Network
Inbound interface: == *
Outbound interface: == *

allow_network

Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

Figure 10: Adding rule to rule set

11. We are now asked to add a description to the rule set, which is only used for documentation purposes and does not affect the rule itself.



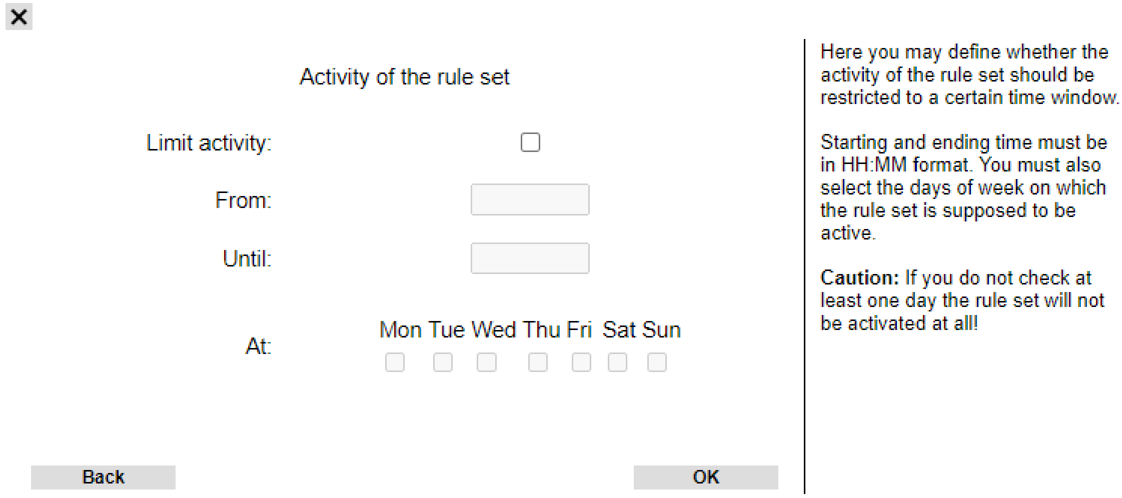
Description of the rule set

This rules set allows another network.

The rule set description be used for documentation only.

Figure 11: Documentation of rule set

12. We can also limit the activity of this rule set by choosing different days and time settings. We want the firewall to be active all the time, hence we do not check the "*Limit activity*" box and press "*OK*".



Activity of the rule set

Limit activity: □

From:

Until:

At: Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun □

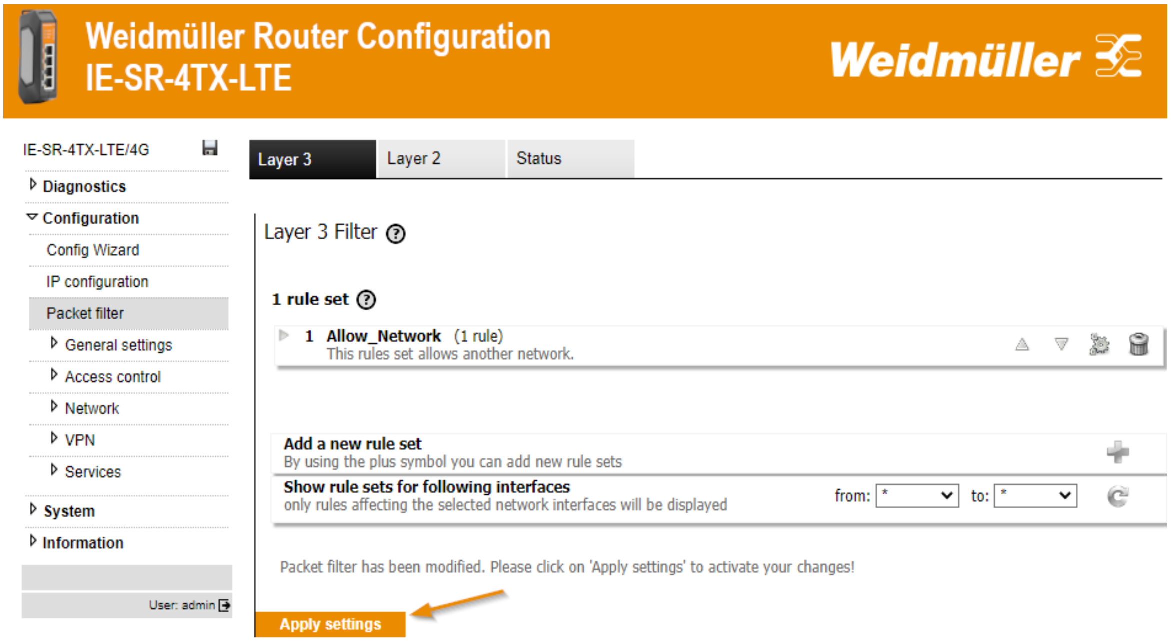
Here you may define whether the activity of the rule set should be restricted to a certain time window.

Starting and ending time must be in HH:MM format. You must also select the days of week on which the rule set is supposed to be active.

Caution: If you do not check at least one day the rule set will not be activated at all!

Figure 12: Option of limiting the rule set

13. To activate the newly created ruleset click the “*Apply settings*” button on the bottom left corner.



Weidmüller Router Configuration
IE-SR-4TX-LTE

Layer 3 Filter ?

1 rule set ?

1 Allow_Network (1 rule)
This rules set allows another network.

Add a new rule set
By using the plus symbol you can add new rule sets

Show rule sets for following interfaces
only rules affecting the selected network interfaces will be displayed
from: * to: *

Packet filter has been modified. Please click on 'Apply settings' to activate your changes!

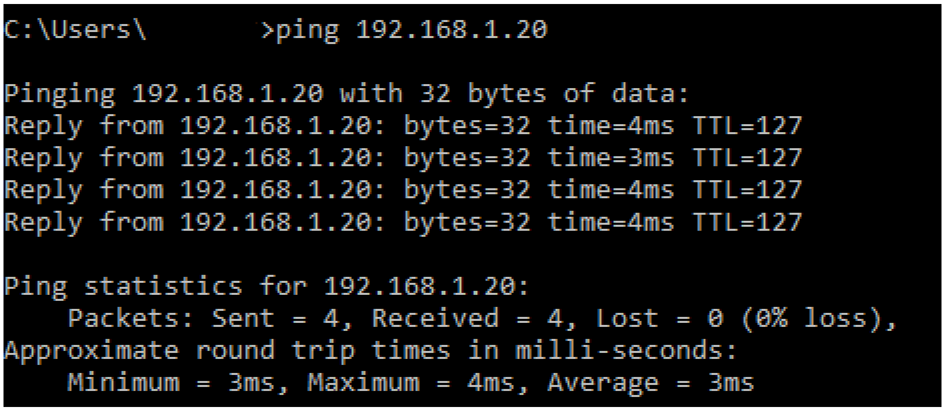
Figure 13: Applying the rule set

After this, navigate to “*System*” and then “*Save*” to save this configuration in case of a power interruption of the router.

6 Results

After implementing all the steps, we can successfully reach the “*192.168.1.x*” network and further defend the main network (*10.10.10.x*) from potential threats from outside. Configuring the firewall with this method ensures maximum security since any unknown network trying to enter is immediately discarded by the firewall.
To check if the firewall works properly, we can ping any of the devices on the Training Kit that are connected via LAN. We can further check if the sensor on the Training Kit still transmits the data as intended.

1. We can once again ping one of the devices on the Training Kit. We will ping the 8-port switch with the IP “*192.168.1.20*” with the Command Prompt as we did in the beginning.
   As we can see, we can successfully reach the switch meaning that the firewall successfully recognized and approved the device from the known network.



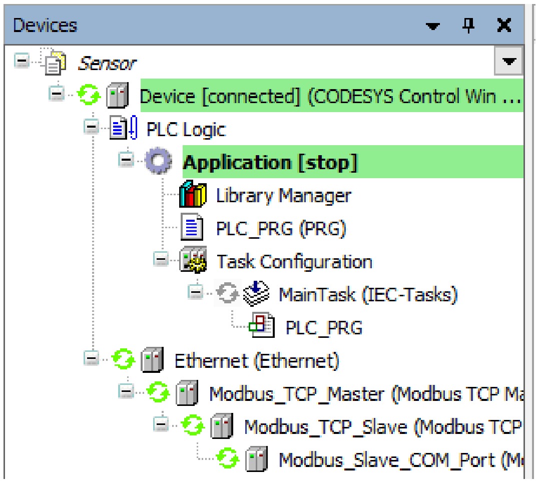
```
C:\Users\       >ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time=4ms TTL=127
Reply from 192.168.1.20: bytes=32 time=3ms TTL=127
Reply from 192.168.1.20: bytes=32 time=4ms TTL=127
Reply from 192.168.1.20: bytes=32 time=4ms TTL=127

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Figure 14: Pinging the switch

2. To further check the functionality of the firewall, we can test if any machine data sent via Modbus still gets transmitted properly by testing the CODESYS Application used in Application Note 02 Serial Converter Modbus RTU. (Note that you would need to renew the Ethernet interface since we are using WAN instead of LAN as described in the Application Note 02).
   First, with the green icons and colors we can tell that every device is running properly and that a connection is successfully established.

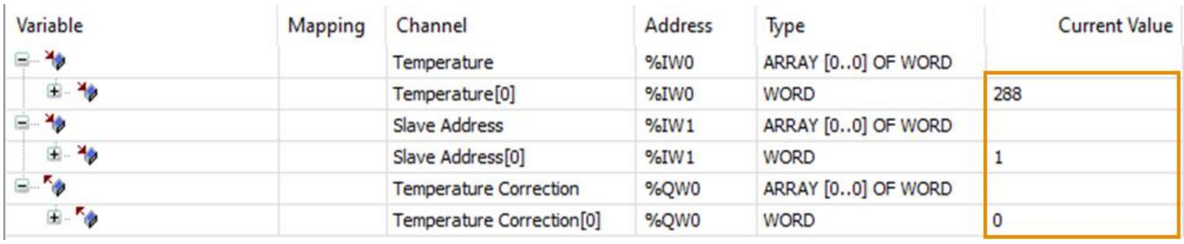


Devices

- Sensor
  - Device [connected] (CODESYS Control Win ...
    - PLC Logic
      - Application [stop]
        - Library Manager
        - PLC_PRG (PRG)
        - Task Configuration
          - MainTask (IEC-Tasks)
            - PLC_PRG
    - Ethernet (Ethernet)
      - Modbus_TCP_Master (Modbus TCP Ma
        - Modbus_TCP_Slave (Modbus TCP
          - Modbus_Slave_COM_Port (M

Figure 15: Devices connected properly

Furthermore, the data from the sensor is being received and shown in the table, as depicted below.



Variable	Mapping	Channel	Address	Type	Current Value
		Temperature	%IW0	ARRAY [0..0] OF WORD	
		Temperature[0]	%IW0	WORD	288
		Slave Address	%IW1	ARRAY [0..0] OF WORD	
		Slave Address[0]	%IW1	WORD	1
		Temperature Correction	%QW0	ARRAY [0..0] OF WORD	
		Temperature Correction[0]	%QW0	WORD	0

Figure 16: Reading current Modbus values

7 List of figures