Weidmüller

Industrial Ethernet Training

Configuration of network groups for domain names in the firewall with Weidmueller security routers

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 only allowed network traffic passes through. This application note demonstrates the use of network groups in the firewall to allow access to certain domains in the network.

Configuration of network groups for domain names in the firewall with Weidmueller security routers

Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	IE-Training Kit-01	2874670000	1.1.2 (Build 125086)
2			
3			

IE-Training Kit Content

No.	Component name	Article No.	Hardware / Firmware version
1	IE-SR-4TX	2751270000	1.6.4
2	IE-SW-AL08M-8TX	2682280000	1.11
3	IE-SW-AL05M-5TX	2682250000	1.16
4	IE-CS-MBGW-2TX-1COM	2682600000	3.14

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

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*” for applying default IP address configuration

Note: *The mentioned Prerequisites 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 following Application and implement it by yourself.*

3 Why do I need a firewall using network groups?

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. These security rules only allow the configuration of allowed IP addresses, meaning that domain names, like “*weidmueller.com*” for example, are not accessible in the router’s local network. Accessing certain web sites via an HMI, configuring a network time protocol (NTP) server in the devices using a static domain instead of a dynamic IP, or having a device’s data stream going to a specific domain is only possible when configuring the firewall with the respective network group.

4 How does the 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 contain various information like the source and destination address and all the payload data to be 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.

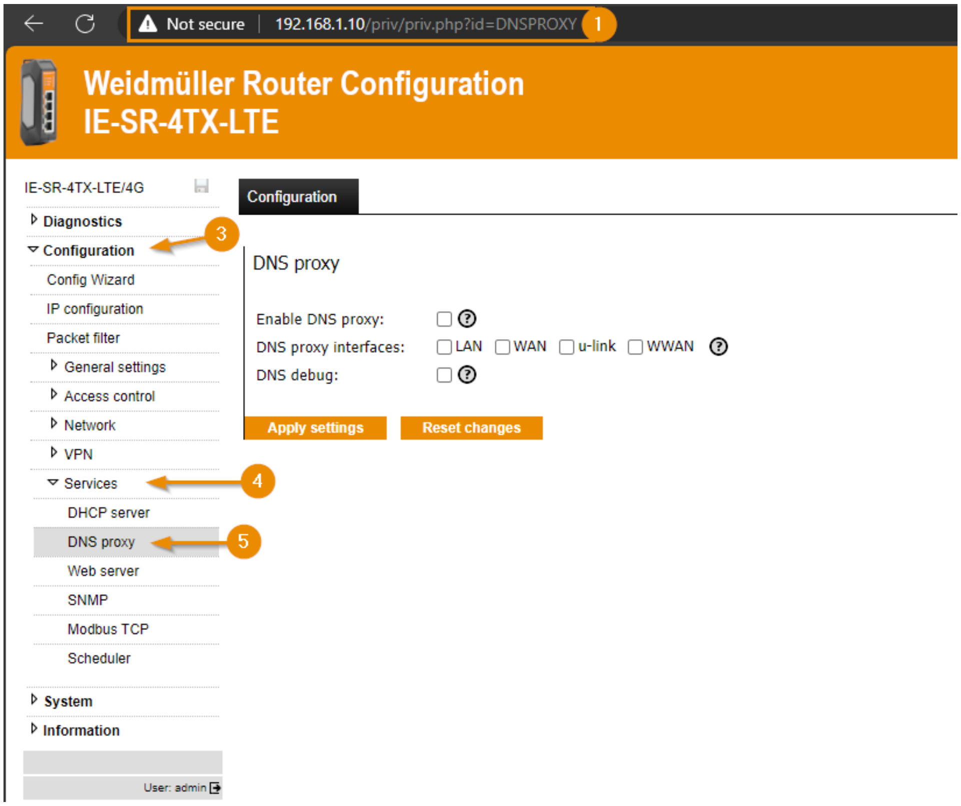
In case a packet, and more importantly, its content, does not comply with the set of rules we defined, it is denied further network access. The mentioned network can be the company's corporate network or the network in the production hall. Therefore, these measurements are taken to protect valuable data 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 and outgoing traffic of this network, except network from our known machines and the configured domains in the network groups. This is the most secure option in an industrial network environment against a possible cyber-attack.

5 Configuring DNS Proxy

An important setting for this feature is the DNS Proxy. It makes the router act as DNS server and will forward the DNS request (e.g., “*weidmueller.com”)* to the configured DNS servers. We must enable this feature since we want to access domain names in the network using the network group feature.

1. Log in to the router’s web interface and go to “*Configuration*”, then “*Services*” and click on “*DNS Proxy*”.



DNS proxy

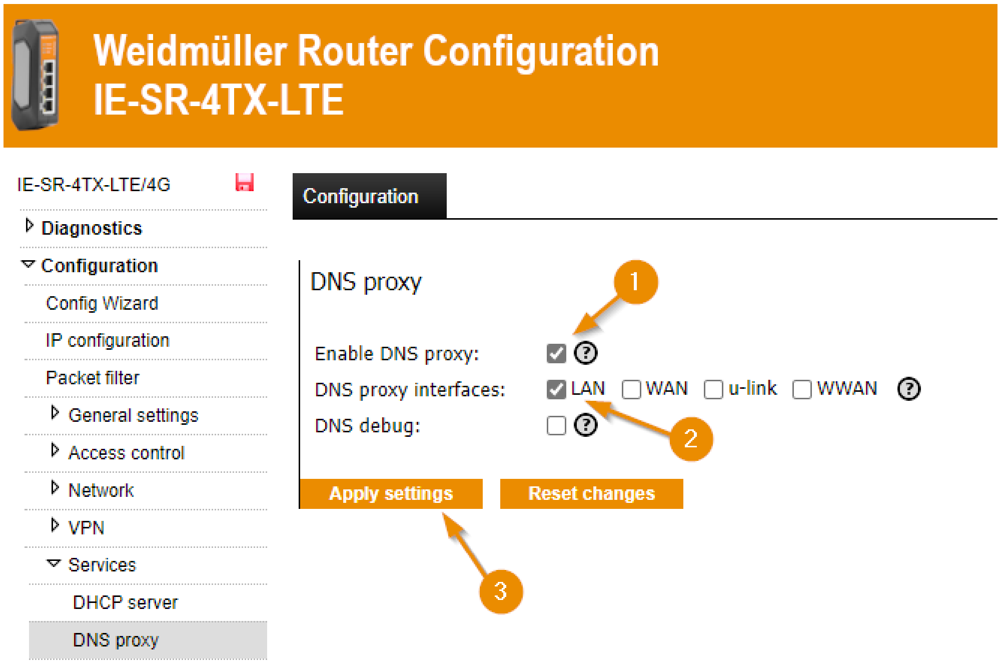
Enable DNS proxy: □ ?

DNS proxy interfaces: □ LAN □ WAN □ u-link □ WWAN ?

DNS debug: □ ?

Figure 1: DNS Proxy settings

2. First, check the "*DNS Proxy*" setting. This enables the forwarding of DNS requests from the router's network. Moreover, select the corresponding interfaces where you want to allow DNS requests. Since everything is connected to the router's LAN port, we only want to allow DNS requests on the LAN interface. This also minimizes the risk of unauthorized requests on other interfaces. Click on "*Apply settings*".



DNS proxy

Enable DNS proxy: ☑ ?

DNS proxy interfaces: ☑ LAN □ WAN □ u-link □ WWAN ?

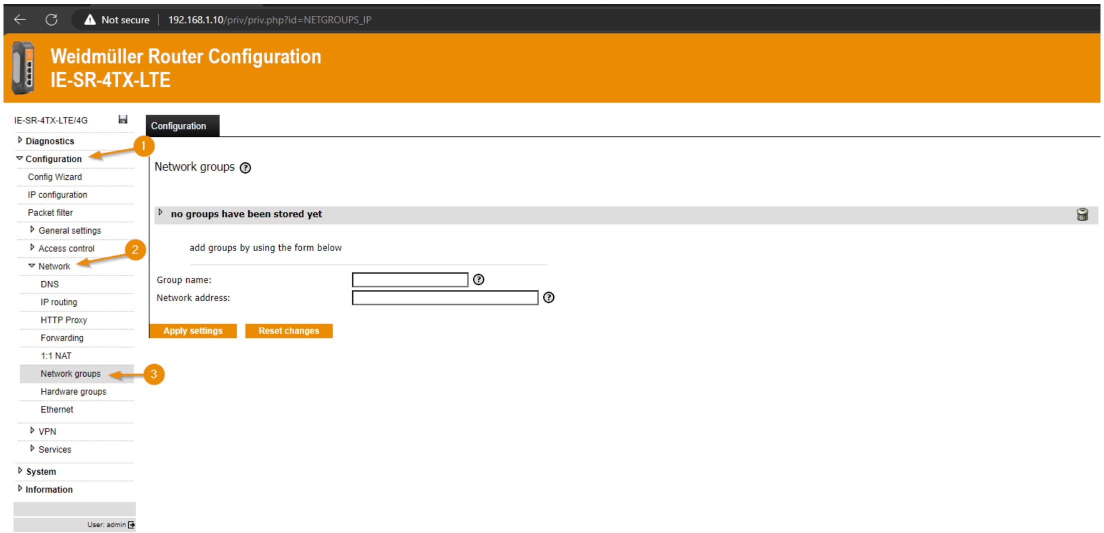
DNS debug: □ ?

Figure 2: Configuring DNS Proxy

6 Configuring Network Groups

To allow certain DNS requests inside the local area network, we must create a new network group and put the respective domain names in this group. We can then use this group in the packet filtering rules.

1. After logging in to the router's web interface, navigate to "*Configuration"*, click on "*Network*" and go to "*Network groups*".



Network groups

no groups have been stored yet

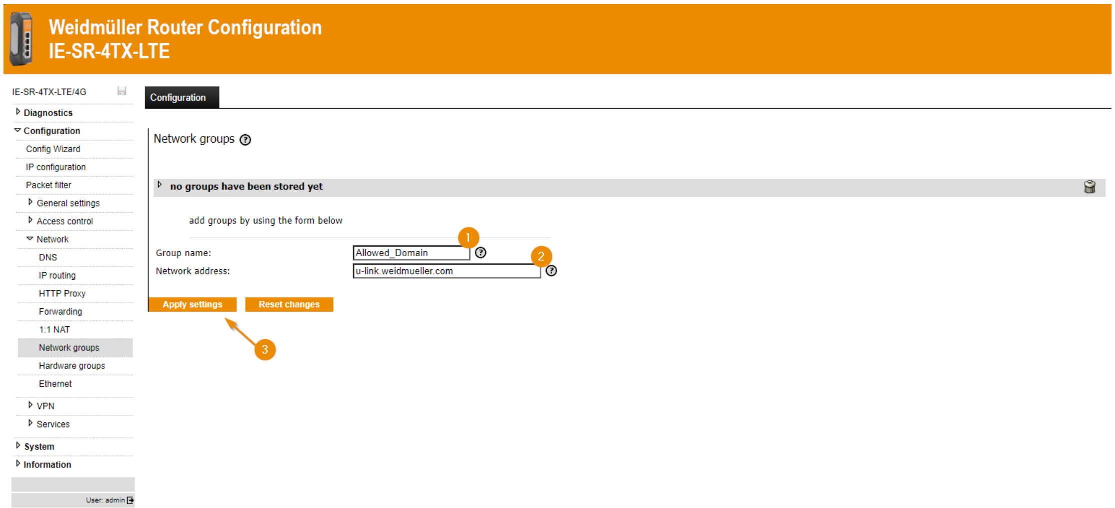
add groups by using the form below

Group name:

Network address:

Figure 3: Network groups settings

2. Create a new network group by typing in a group name and the corresponding domain you want to have in this network group and then click on "*Apply setting*". We chose "*Allowed_Domain*" as group name and put "*u-link.weidmueller.com*" as a network address. More entries can be entered in the next step.



Network groups

no groups have been stored yet

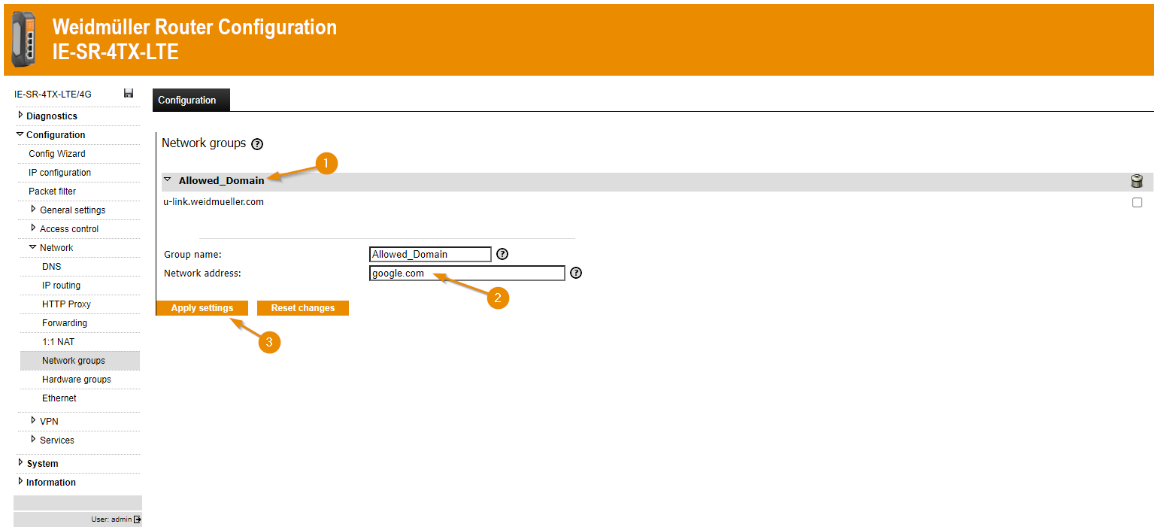
add groups by using the form below

Group name: Allowed_Domain

Network address: u-link.weidmueller.com

Figure 4: Creating network group

3. After applying the settings, we can see the group being listed at the top with every network address in it. To add more entries, simply click once on the group name or type in the group name where you want to put the network address in. In this example, the group name is “*Allowed_Domain”* and we want to add “*google.com*” as a network address to this group. Click on “*Apply settings*”.



Allowed_Domain

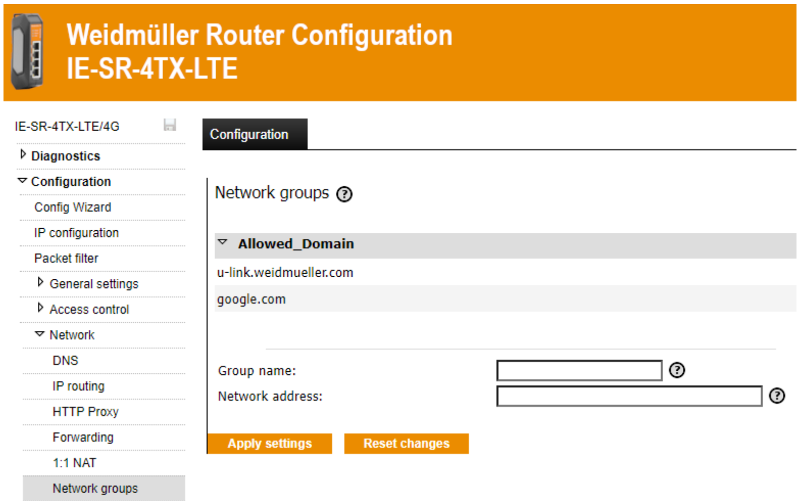
u-link.weidmueller.com

Group name: Allowed_Domain

Network address: google.com

Figure 5: Adding more entries to network group

4. The network group now consists of two network addresses. Next, we will use this group in the packet filter to allow these websites in the LAN.



Allowed_Domain

u-link.weidmueller.com

google.com

Group name:

Network address:

Figure 6: Checking network group

7 Configuring the firewall

As of now, any device and any IP address can be accessed through router since the firewall has an "*Allow all traffic*" rule active per default. We are going to change that and configure that only the domains in the network groups are accessible.

1. Navigate in the menu tree to "*Configuration*" and click on "*Packet filter*". Once in the menu, we must 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.

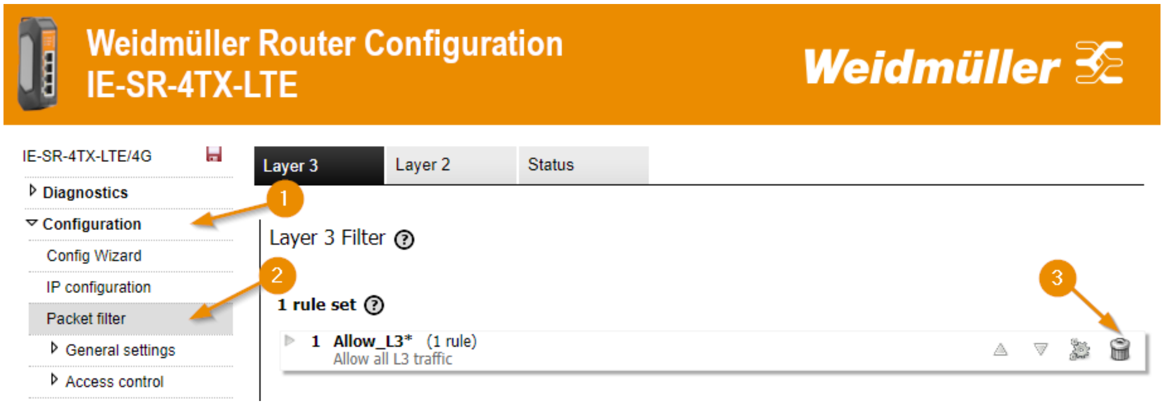
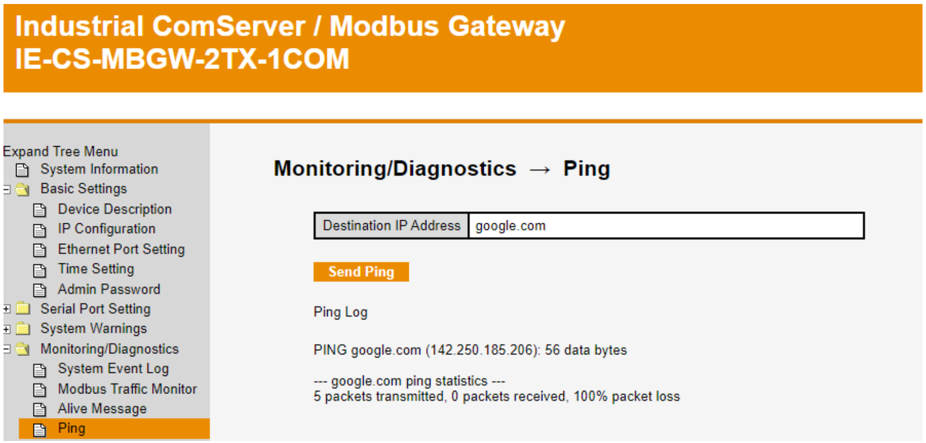


Figure 7: Deleting allow all rule set

2. After applying, we can see that the router does not forward any DNS requests. We can test that by simply trying to connect to a certain domain, like "*google.com*", using a device that is connected to the router's network. Trying to ping the "*google.com*" domain using the Modbus Gateway results in a timeout and a 100% packet loss.



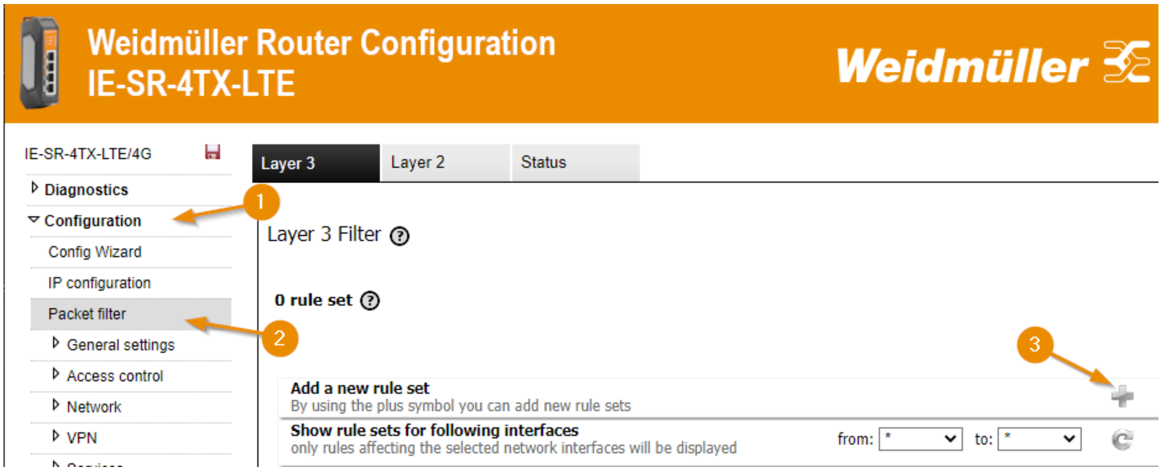
Destination IP Address: google.com

```
PING google.com (142.250.185.206): 56 data bytes

--- google.com ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

Figure 8: Pinging domain before configuration

3. Add a new rule set by clicking on the grey “+” icon on the right-hand side of the packet filter menu.

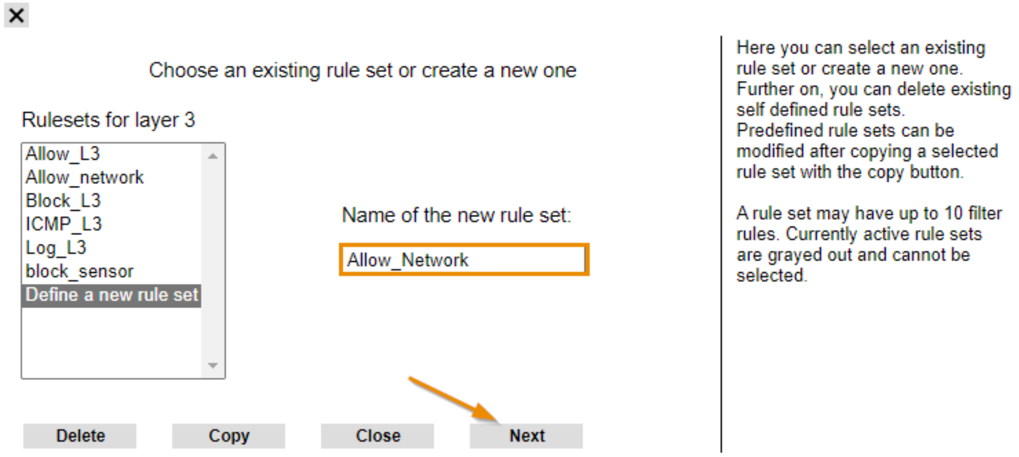


Add a new rule set
By using the plus symbol you can add new rule sets

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

Figure 9: Configuring new rule set

4. A pop-up window opens where we can either use a pre-defined rule set or define a new rule set. Click on “*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*”.



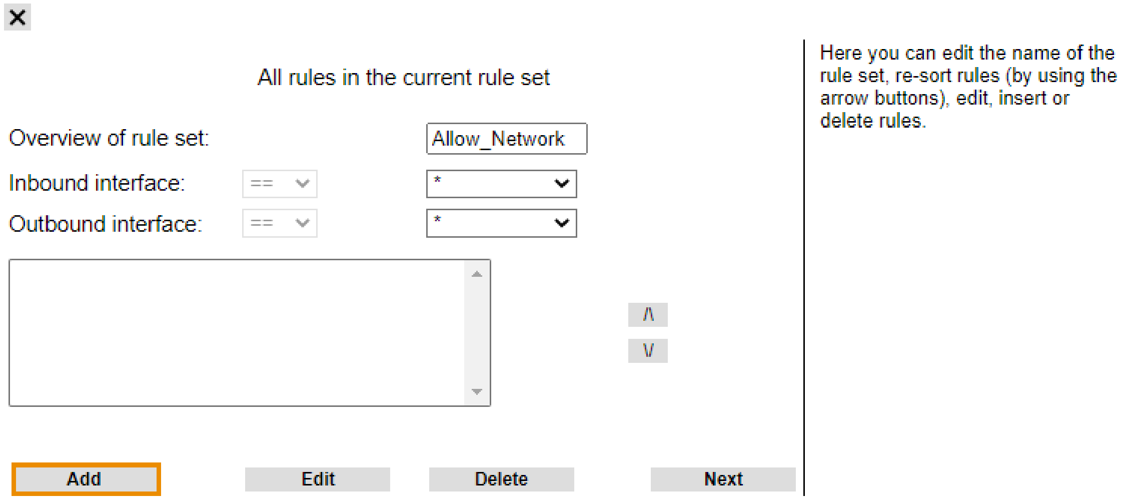
Name of the new rule set: Allow_Network

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 10: 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

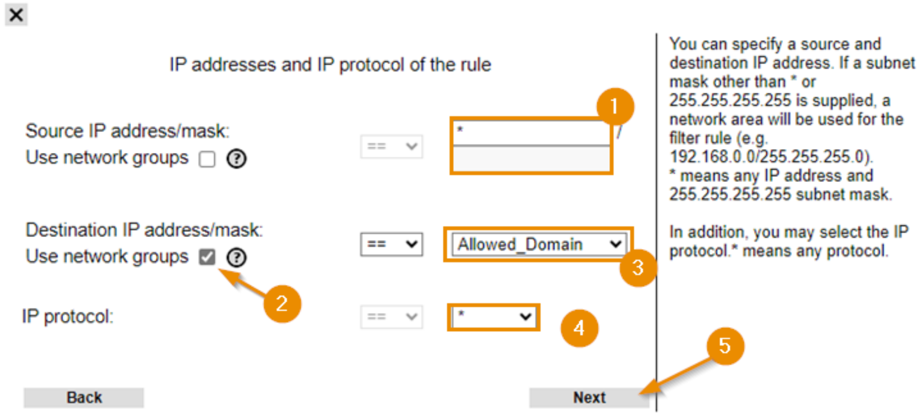
Inbound interface: == *

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 11: Defining interfaces

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. For the allowed destination address, click on the "*Use network groups*" checkbox and select the respective group in the drop-down menu. This means that packets with the destination "*google.com*" can go through. Keep the "*" to have any protocol in the "*IP Protocol*" option. Click on "*Next*".



IP addresses and IP protocol of the rule

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

Destination IP address/mask: == Allowed_Domain
Use network groups ☑

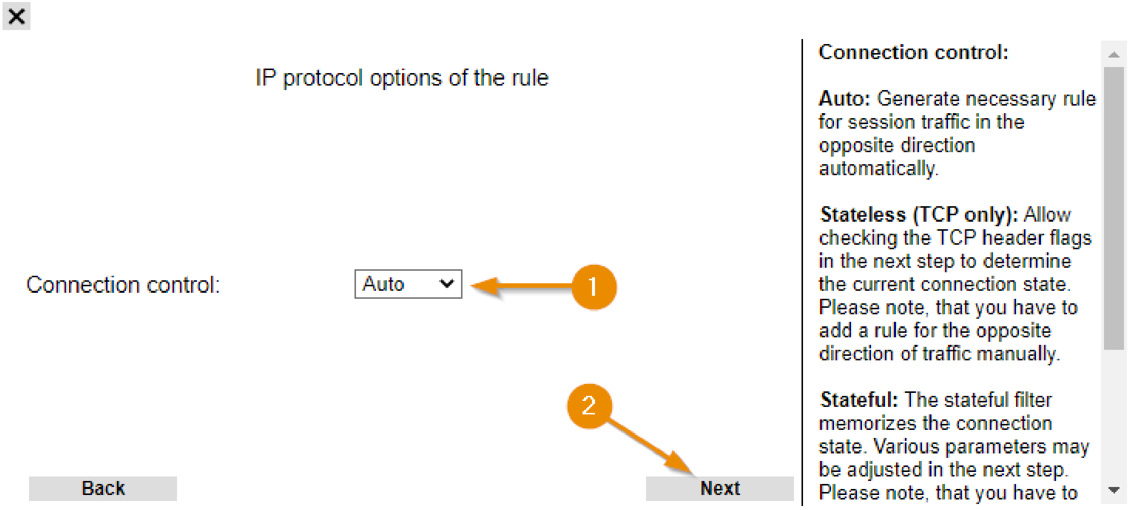
IP protocol: == *

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 12: IP addresses and protocol 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:

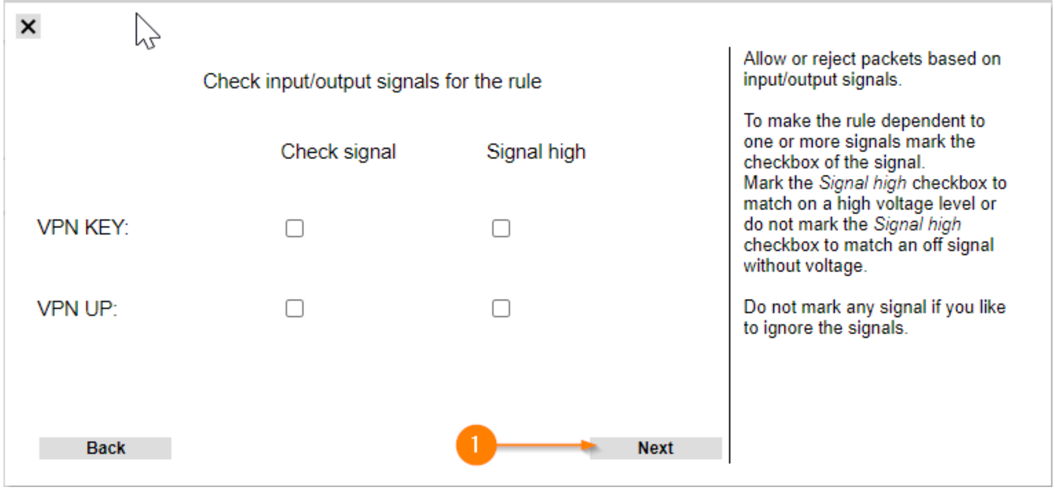
Auto: Generate necessary rule for session traffic in the opposite direction automatically.

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 13: Connection control of rule set

8. Next, 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.

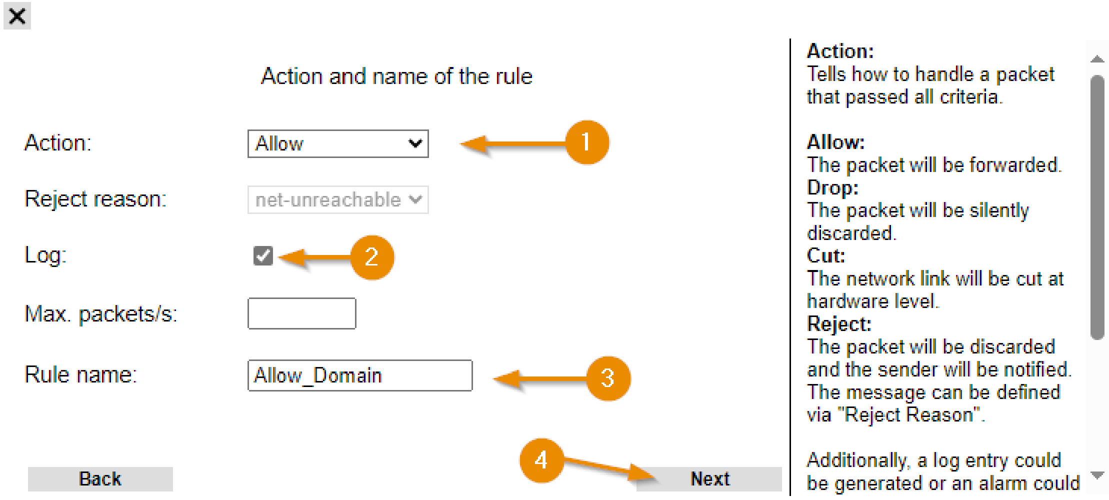
Figure 14: VPN settings of rule set

9. Lastly, we define the action the firewall takes when it detects a packet that fits the rule set 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_Domain*” 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_Domain

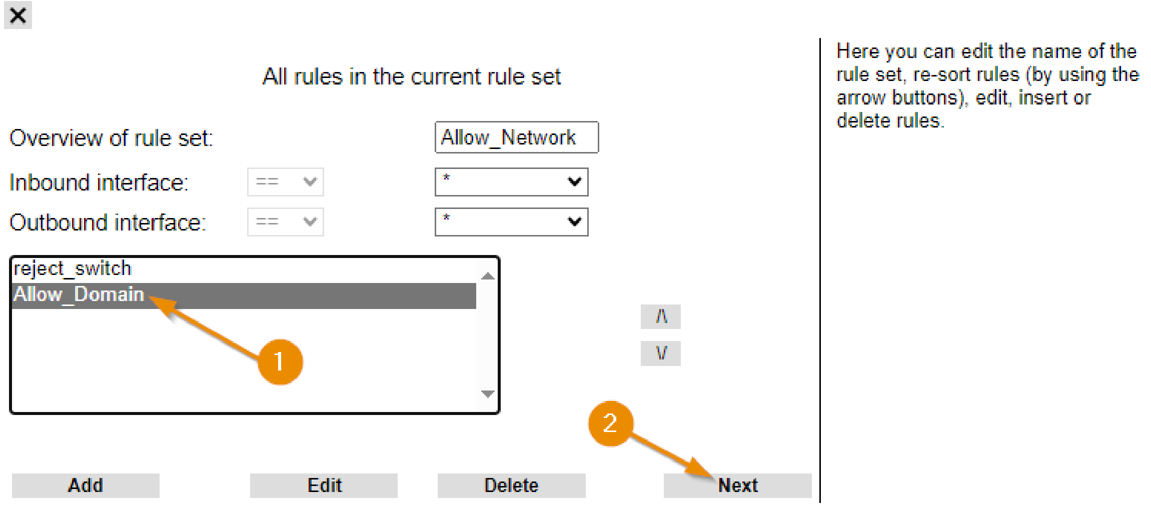
Action:
Tells how to handle a packet that passed all criteria.

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 15: Action and name of rule

10. We are now back in the menu of step 5. Since we have configured our own ruleset, we can select it by marking it and then pressing “*Next*”.



All rules in the current rule set

Overview of rule set: Allow_Network

Inbound interface: == *

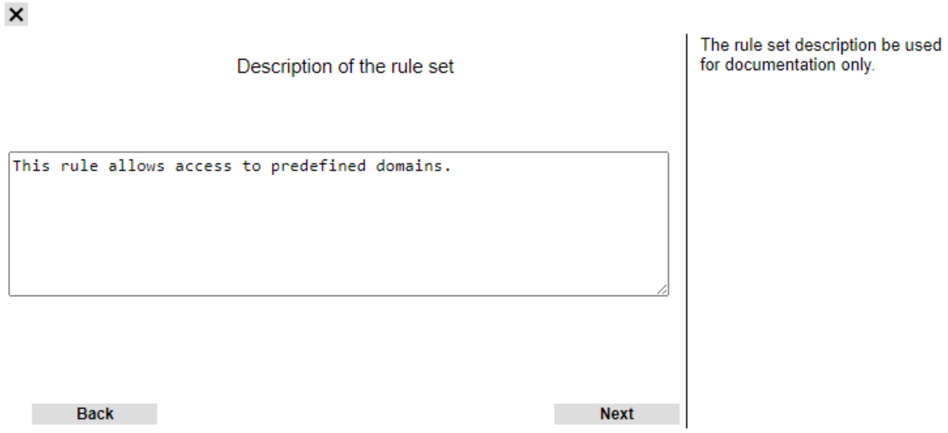
Outbound interface: == *

reject_switch
Allow_Domain

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

Figure 16: Selecting configured rule set

11. Next, give the rule a description for documentation purposes to know the function of it.



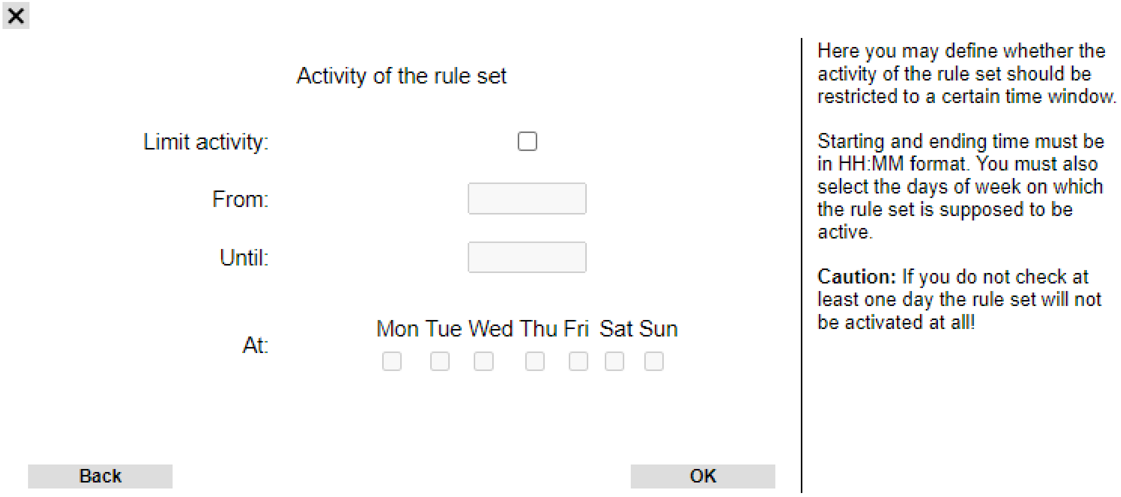
Description of the rule set

```
This rule allows access to predefined domains.
```

The rule set description be used for documentation only.

Figure 17: Description of rule set

12. The activity of this rule can also be restricted to a certain time window 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
□ □ □ □ □ □ □

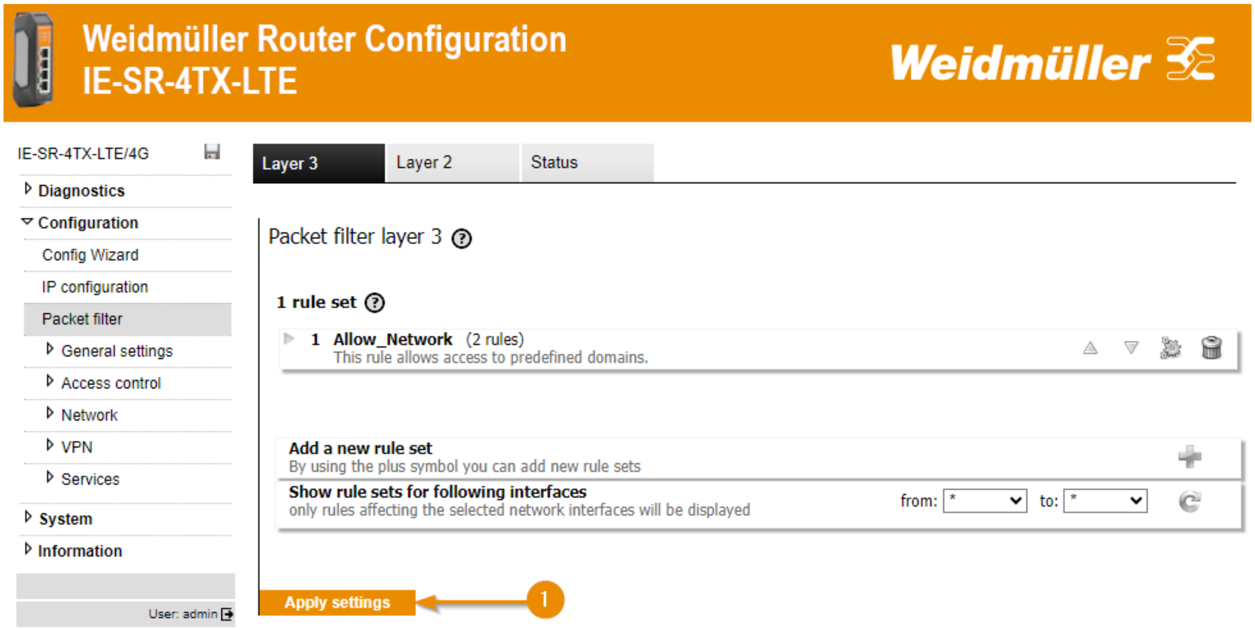
Here you may define whether the activity of the rule set should be restricted to a certain time window.

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 18: Option of limiting the rule set

13. Activate the configured rule by clicking on “*Apply settings*”.



Weidmüller Router Configuration
IE-SR-4TX-LTE

Packet filter layer 3

1 rule set

1 **Allow_Network** (2 rules)
This rule allows access to predefined domains.

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

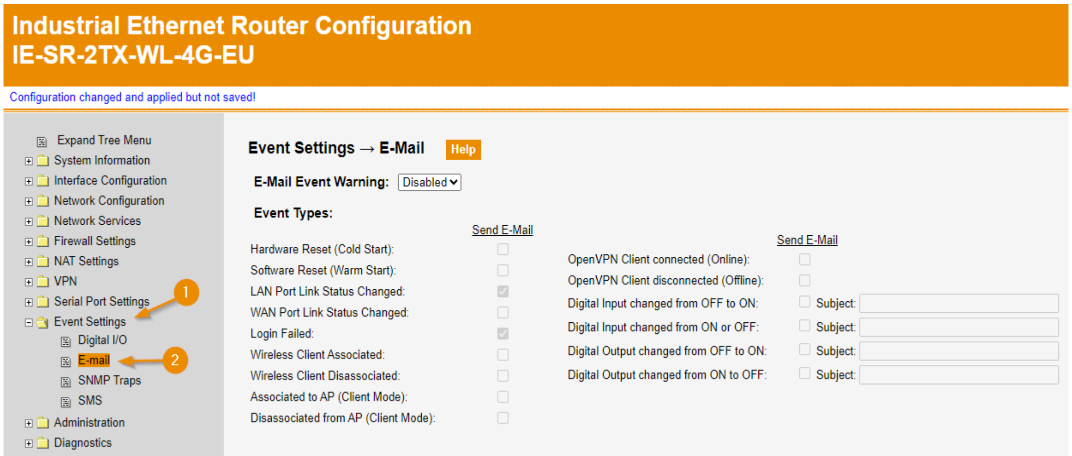
from: * to: *

Figure 19: Activating rule set

8 Using Network Groups for e-mail alerts

To use the integrated E-Mail alert (for example with the IE-SR-2TX router), e.g. when a port link status changes or a login attempt failed, the SMTP server address also needs to be added to the allowed network group (as shown already in 6).

1. Log into the device that supports E-Mail alerts, in this case the IE-SR-2TX-WL-4G router. Navigate to "*Event Settings*" and click on "*E-Mail*".



Industrial Ethernet Router Configuration
IE-SR-2TX-WL-4G-EU

Configuration changed and applied but not saved!

Event Settings → E-Mail

E-Mail Event Warning: Disabled

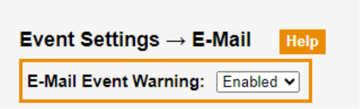
Event Types:

	Send E-Mail
Hardware Reset (Cold Start):	□
Software Reset (Warm Start):	□
LAN Port Link Status Changed:	☑
WAN Port Link Status Changed:	□
Login Failed:	☑
Wireless Client Associated:	□
Wireless Client Disassociated:	□
Associated to AP (Client Mode):	□
Disassociated from AP (Client Mode):	□

	Send E-Mail	
OpenVPN Client connected (Online):	□	
OpenVPN Client disconnected (Offline):	□	
Digital Input changed from OFF to ON:	□	Subject:
Digital Input changed from ON or OFF:	□	Subject:
Digital Output changed from OFF to ON:	□	Subject:
Digital Output changed from ON to OFF:	□	Subject:

Figure 20: E-Mail alert menu

2. First, switch the "*E-Mail Event Warning*" option to "*Enabled*" using the drop-down menu.

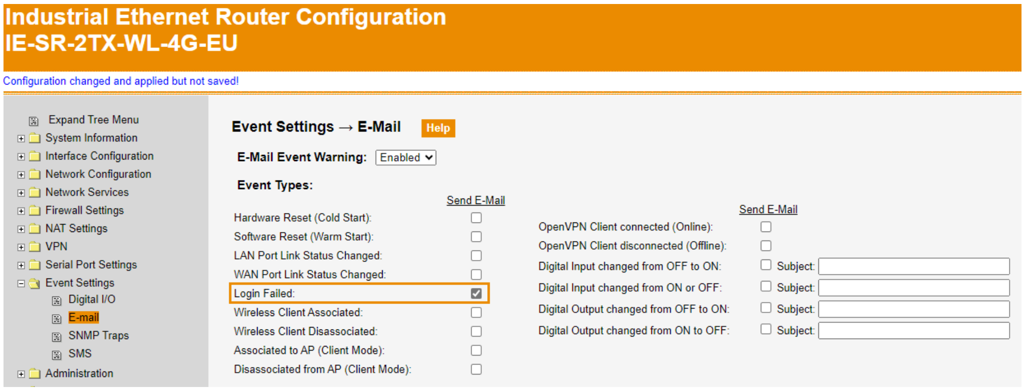


Event Settings → E-Mail

E-Mail Event Warning: Enabled

Figure 21: Enabling E-Mail alert

3. Select the corresponding Event types for which you want to get notified, for instance here a failed login attempt sends an E-Mail alert.



Industrial Ethernet Router Configuration
IE-SR-2TX-WL-4G-EU

Configuration changed and applied but not saved!

Event Settings → E-Mail

E-Mail Event Warning: Enabled

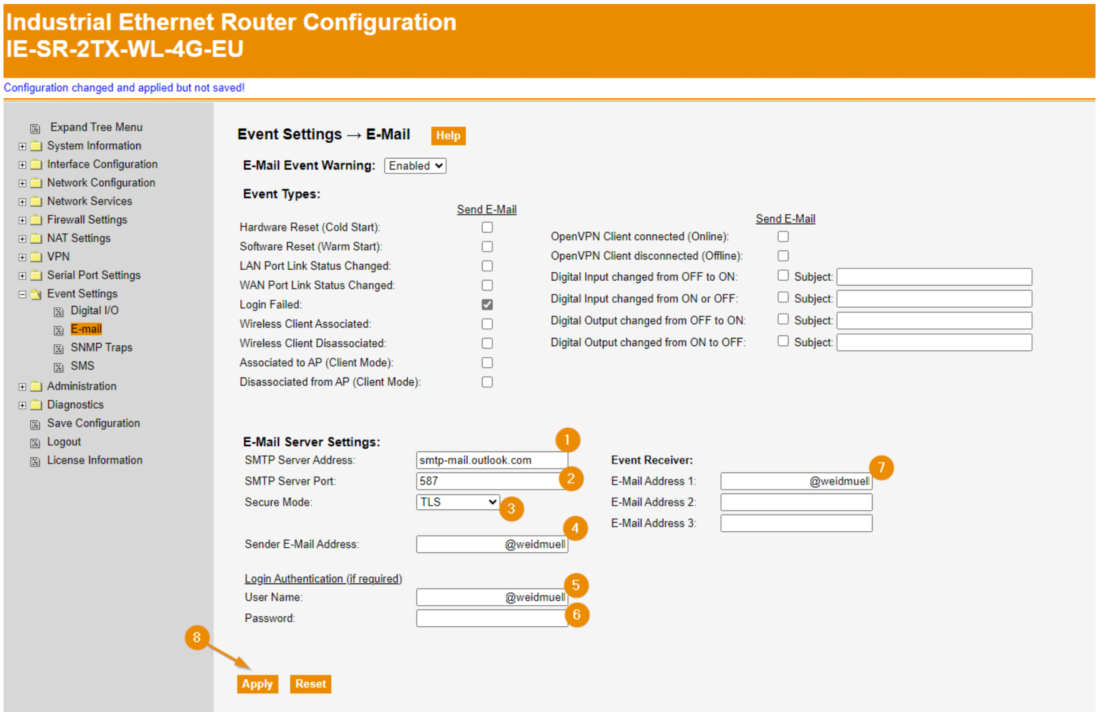
Event Types:

	Send E-Mail
Hardware Reset (Cold Start):	□
Software Reset (Warm Start):	□
LAN Port Link Status Changed:	□
WAN Port Link Status Changed:	□
Login Failed:	☑
Wireless Client Associated:	□
Wireless Client Disassociated:	□
Associated to AP (Client Mode):	□
Disassociated from AP (Client Mode):	□

	Send E-Mail	
OpenVPN Client connected (Online):	□	
OpenVPN Client disconnected (Offline):	□	
Digital Input changed from OFF to ON:	□	Subject:
Digital Input changed from ON or OFF:	□	Subject:
Digital Output changed from OFF to ON:	□	Subject:
Digital Output changed from ON to OFF:	□	Subject:

Figure 22: Selecting Event Types

4. Next, fill in the E-Mail server settings for the provider you are using (these can be found on the provider’s website), we used Outlook for this example.
   Also, fill in the sender’s e-mail address and the corresponding login credentials, followed by the e-mail that receives the alert. Lastly, hit “*Apply*”.
   Note that due to new security restrictions, Gmail (Google Mail) might not be available for certain accounts. This might apply to certain providers with stricter authentication requirements, too.



Event Settings → E-Mail

E-Mail Event Warning: Enabled

Event Types:

	Send E-Mail
Hardware Reset (Cold Start):	□
Software Reset (Warm Start):	□
LAN Port Link Status Changed:	□
WAN Port Link Status Changed:	□
Login Failed:	☑
Wireless Client Associated:	□
Wireless Client Disassociated:	□
Associated to AP (Client Mode):	□
Disassociated from AP (Client Mode):	□

	Send E-Mail	
OpenVPN Client connected (Online):	□	
OpenVPN Client disconnected (Offline):	□	
Digital Input changed from OFF to ON:	□	Subject:
Digital Input changed from ON or OFF:	□	Subject:
Digital Output changed from OFF to ON:	□	Subject:
Digital Output changed from ON to OFF:	□	Subject:

E-Mail Server Settings:

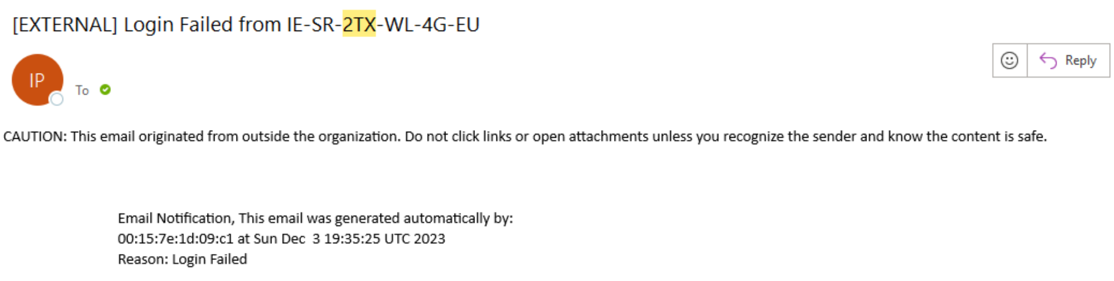
SMTP Server Address: smtp-mail.outlook.com
SMTP Server Port: 587
Secure Mode: TLS
Sender E-Mail Address: @weidmuell

Login Authentication (if required)
User Name: @weidmuell
Password:

Event Receiver:
E-Mail Address 1: @weidmuell
E-Mail Address 2:
E-Mail Address 3:

Figure 23: Configuring E-Mail Server Settings

5. Try the alerts, by triggering one of the selected event types, for example typing in a wrong password when logging in. You should receive the following e-mail alerting you about the incident (please check spam/junk folder as well).



[EXTERNAL] Login Failed from IE-SR-2TX-WL-4G-EU

CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Email Notification, This email was generated automatically by:
00:15:7e:1d:09:c1 at Sun Dec 3 19:35:25 UTC 2023
Reason: Login Failed

Figure 24: E-Mail notification

Depending on the provider, receiving this notification might take a few minutes

9 Results

After implementing and configuring the network groups in the firewall, we are now able to access certain domain name servers in the network while unauthorized domain name servers remain inaccessible in the network for maximum security. Getting notified with configured E-Mail alerts is also possible and can be used for even more security and surveillance of the devices.
We can test this by simply trying to access the domains that are listed in the configured network group e.g., google.com.