Understanding and Using the Firewall with SCALANCE S

SCALANCE S

https://support.industry.siemens.com/cs/ww/en/view/22376747

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 Introduction

1.1 Overview

Initial position

Cybersecurity is the topic that all companies have to deal with today. With "Defense in Depth" as an overarching protection concept, Siemens provides answers in the form of a depth-based defense based on the recommendations of IEC 62443 in industrial automation.

Network security

Part of Siemens' Industrial Security concept is network security to protect plant networks from unauthorized access. The safety-related segmentation of the plant network into individual protected automation cells minimizes risk and increases safety. The cells are divided, and the devices assigned according to communication and protection requirements.

With Security Integrated products from Siemens, automation networks, automation systems and industrial communication can be secured with firewalls and VPNs.

Cell protection with firewall

In order to protect the automation network from unauthorized access, the use of a firewall is an adequate solution. All Security Integrated products have an IP-based stateful packet inspection firewall integrated.

With the SCALANCE S industrial security appliance (S615 and SC-600) and the SCALANCE M industrial routers, the IP-based stateful packet inspection firewall can be configured user-specifically.

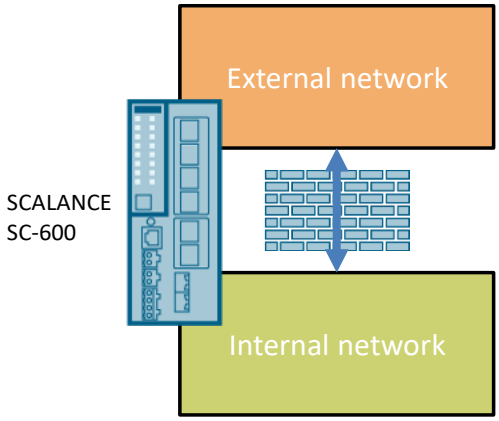
The SCALANCE SC-600 industrial security appliance also supports the bridge firewall to protect flat networks.

Applicative implementation

This application example shows you how to use the firewall with the SCALANCE S industrial security appliance. You will learn the difference between the different firewall variants (IP-based, MAC-based, user-specific) and how to configure the different firewall variants.

The application example is explained using the following configuration:

Figure 1-1



An external (insecure) network and an internal network are connected to a SCALANCE SC-600 device. The internal network is to be protected against unauthorized access by the integrated firewall in the SCALANCE S.

Note

This application example uses the Industrial Security Appliance SCALANCE SC-600, since this module supports all variants of the firewall.

You can also use SCALANCE S615 and SCALANCE M for the IP-based and user-specific variants.

1.2 Principle of operation

1.2.1 Firewall in general

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a set of defined security rules.

The data packets are checked against packet filter rules that specify the following:

- The permitted protocols
- The addresses of the allowed sources
  - IP-based firewall: IP address and ports
  - MAC based firewall MAC address
- The addresses of the permitted destinations
  - IP-based firewall: IP address and ports
  - MAC based firewall MAC address

If a data packet meets the specified parameters, it may pass through the firewall. In addition, the procedure for handling data packets that are not allowed to pass through the firewall is defined.

Simple packet filtering techniques require two packet filtering rules for the firewall per connection:

- A rule for query direction from source to destination.
- A second rule for the response direction from destination to source.

1.2.2 Firewall for Security Integrated products

Overview

All Security Integrated products have an integrated firewall. Security Integrated products include:

- The Industrial Security Appliances SCALANCE S. These are the device types:
  - SCALANCE S615
  - SC-600
- SCALANCE M Industrial Router
- Security communication processors for SIMATIC

Among the Security Integrated products there are the following firewall variants:

- IP-based Stateful Packet Inspection Firewall
- User-specific firewall
- MAC based firewall

The following table shows which firewall variant the individual Security Integrated products support:

Table 1-1

	SCALANCE S615/ SCALANCE M	SCALANCE SC-600	SIMATIC CP
IP-based	Yes	Yes	Yes
User-specific	Yes	Yes	No
MAC-based	No	Yes	No

IP-based stateful packet inspection firewall

The IP-based stateful packet inspection firewall is supported by all Security Integrated products.

Stateful Packet Inspection (SPI) is a feature of an IP-based firewall and extends the approach of a simple packet filtering technique by checking additional connection information.

It maintains a dynamic table in which information about the status of the individual connections is entered. This dynamic table allows you to block all vulnerable ports initially and open the port only when needed for a valid connection. The ports are always opened only from the protected network to the unprotected network. Data packets that do not belong to a connection stored in the status table are automatically discarded.

The IP filter rules of this firewall are direction dependent: A connection can only be established from the source to the destination, unless there is an explicit entry for the return direction.
If a connection is established, only the data packets belonging to this connection are transmitted bidirectionally. All unsolicited access that is not from the local network is reliably blocked.

With the SCALANCE S industrial security appliances and the SCALANCE M industrial routers, you can combine the IP filter rules into IP rule sets.

Note With a stateful packet inspection firewall, you only need to set a packet filtering rule for the request direction from source to destination. The response packets in the opposite direction are automatically allowed and forwarded.

User-specific firewall

The user-specific firewall is supported by the SCALANCE S industrial security appliances (S615 and SC-600) and the SCALANCE M industrial routers.

The basis of the user-specific firewall is an IP-based stateful packet inspection firewall. The user-specific firewall allows the IP rulesets of the stateful packet inspection firewall to be assigned to one or more users. If the user's login was successful, the IP ruleset intended for this user is activated.

After logging in, a timer is started. After the time has elapsed, the user is automatically logged out of the device.

MAC based firewall

The MAC-based firewall is supported by the SCALANCE SC-600 industrial security appliances. SCALANCE SC-600 can be operated in bridge mode. Since the protected and unprotected network is located in a subnet, MAC-based protocols (Layer 2) can pass through the SCALANCE SC-600.

The MAC-based firewall is a simple packet filter at Layer 2 level. It requires two packet filter rules per connection:

- A rule for the query direction from the source to the target
- A second rule for the response direction from destination to source.

Note

With a MAC-based firewall you always need two packet filter rules:

- For the request direction from the source to the destination
- For the response direction from destination to source

1.2.3 Firewall configuration options

When configuring the firewall in SCALANCE S and SCALANCE M, you have the following options:

- Use predefined packet filter rules
- Manually define your own packet filter rules

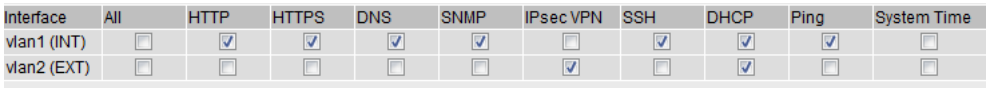
Predefined packet filter rules

With the pre-defined packet filter rules in SCALANCE, you can enable or disable common services for the firewall without much configuration effort. You can set which services of the device should be accessible from which interface or subnet. Different services are available depending on the SCALANCE device.

With all SCALANCE S and SCALANCE M you can use predefined IP services, e.g. http, https, DNS, SNMP, Telnet, IPsec. Which services are available depends on the device.

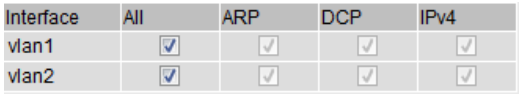
The following screenshot is taken from SCALANCE SC636-2C:

Figure 1-2



In SCALANCE SC-600 you will also find predefined MAC services, e.g. ARP, DCP and IPv4.

Figure 1-3



Note Some IP services are created automatically when SCALANCE is configured, e.g. during connection configuration (SINEMA RC, IPsec).

Note When you create manual packet filter rules, they have a higher priority than the predefined and automatically created packet filter rules.

Defining manual packet filter rules

You can also manually set packet filtering rules for the firewall and set rule parameters individually.

The manually created packet filter rules take precedence over the predefined and automatically created packet filter rules.

You can manually define IP rules for all SCALANCE S and SCALANCE M. You can set the following parameters for each IP rule:

- The choice of how to proceed with incoming IP packets:
  - "Accept" The data packets are allowed
  - "Reject": The data packets are rejected
  - "Drop": The data packets are discarded
- The communication direction of the IP rule
- The IP address or IP range of the source:
  - Single IP address, e.g. 192.168.100.1
  - IP range, e.g. 192.168.100.10 - 192.168.100.20
  - Enter "0.0.0.0/0" for all IP addresses.
  - Target (Range)
- The IP address or IP range of the destination:
  - Single IP address, e.g. 192.168.100.1
  - IP range, e.g. 192.168.100.10 - 192.168.100.20
  - Enter "0.0.0.0/0" for all IP addresses.
- The service or protocol name valid for this rule.
- Choosing whether to log the rule's compliance
- The order of the rule
- The assignment to an IP ruleset

The following screenshot is taken from the SCALANCE SC636-2C:

Figure 1-4

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service
☐	IPv4	Drop	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.2	HTTP
☐	IPv4	Drop	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.2	Syslog

In addition to the IP rules, you can also define MAC rules manually with SCALANCE SC-600. You can set the following parameters for each MAC rule:

- The selection of how to proceed with incoming MAC packets:
  - "Accept" The data packets are allowed
  - "Drop": The data packets are discarded
- The communication direction of the MAC rule
- The source MAC address of the MAC packets
- The destination MAC address of the MAC packets
- The service valid for this rule.
- Choosing whether to log the rule's compliance
- The order of the rule
- Bandwidth (kbit/s)

1.2.4 How the firewall functions

If you create manual packet filter rules, you define in a firewall rule set which data traffic is allowed through a firewall and which is forbidden. The rules in the set of rules have a sequential number.

When packets hit the firewall, the packet filter rules are checked for each packet in the series, and the first applicable packet filter rule is applied. The sequence of the packet filter rules is therefore relevant.

If no packet filter rule applies to the data packet, then the data packet is discarded and must not pass the firewall.

1.3 Components used

SCALANCE S

This application example uses the Industrial Security Appliance SCALANCE SC-600 (here: SCALANCE SC636-2C), since these modules support all variants of the firewall.

You can also use the SCALANCE S615 and SCALANCE M for the IP-based and user-specific variants.

Test Components

To test the function of the firewall, in this example a SCALANCE X and a S7-1500 CPU are used as test components. You can also use any other network device.

PG

To configure SCALANCE S, you need a PG or PC with the following software:

- Internet browser
- TIA Portal (for commissioning the CPU and optionally for configuring the security components)
- Primary Setup Tool

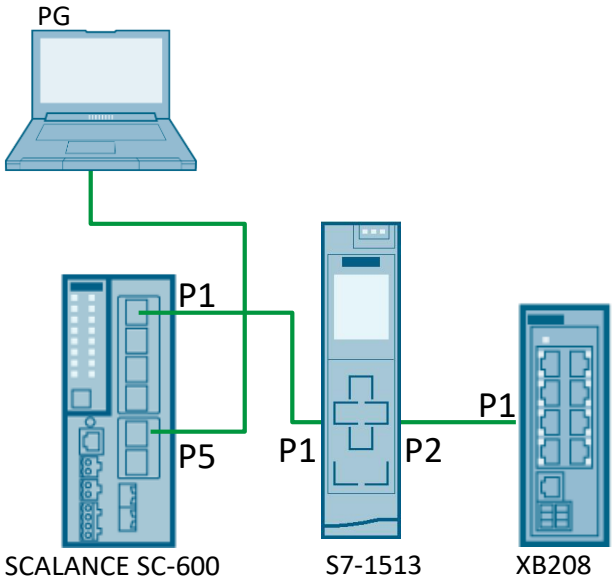
2 Engineering

2.1 Hardware setup

Setup

The hardware layout of this application example is defined as follows:

Figure 2-1



Note To configure the modules, the PG is first connected to a free port of SCALANCE XB208.

2.2 Configuration

2.2.1 Overview

Project planning possibilities

You can configure all SCALANCE S and SCALANCE M in the following ways:

- Web Based Management
- Command Line Interface (serial)

In this example, Web Based Management is used.

IP addresses

The following tables list the IP addresses used in this example. The subnet mask is always 255.255.255.0.

For the variants

- IP-based Firewall (section 2.2.4)
- User defined Firewall (section 2.2.5)

the following address settings apply:

Table 2-1

Device	Module	Router
SCALANCE SC636-2C Port 5: EXT	10.0.0.1	
SCALANCE SC636-2C Port 1: INT	192.168.1.1	
SCALANCE XB208	192.168.1.2	192.168.1.1
CPU S7-1513	192.168.1.3	192.168.1.1
Programming device	192.168.1.10 10.0.0.10	- 10.0.0.1

Note To configure the modules, the PG requires the IP address 192.168.1.10.
You can add additional IP addresses in the advanced TCP/IP settings of the network card configuration.
After completion of section 2.2 the PG may only have the IP address 10.0.0.10.

For the variant with the MAC-based firewall (section 2.2.6) the following address setting applies:

Table 2-2

Device	Module
SCALANCE SC636-2C WAN-Port 5: EXT	10.0.0.1
SCALANCE SC636-2C LAN-Port 1: INT	192.168.1.1
SCALANCE XB208	10.0.0.2
CPU S7-1513	10.0.0.3
PG	192.168.1.10 10.0.0.10

Note

To configure SCALANCE SC636-2C the PG needs the IP address 192.168.1.10.
To load the CPU the PG needs the IP address 10.0.0.10.

You can add additional IP addresses in the advanced TCP/IP settings of the network card configuration.
After completion of section 2.2 the PG may only have the IP address 10.0.0.10.

Test scenarios

The following table gives an overview of the test scenarios:

Table 2-3

Scenario	Firewall variant	Test	Target device
1.	IP-based firewall	• Allow secure protocols: - HTTPS (Port 443) - SSH (Port 22) • Prevent all other protocols	SCALANCE XB208
2.		• STEP 7 Allow remote programming (Port 102) • Allow Web Server Access (Port 443) • Prevent all other protocols	CPU S7-1513
3.	User-specific firewall	• "RemoteServiceAdmin" User: - Allow Web Server Access (Port 443) • User "RemoteIT": - Allow Ping only	SCALANCE XB208
4.		• "RemoteServiceAdmin" User: - Allow Web Server Access (Port 443) - Allow remote programming (port 102) • User "RemoteIT": - Allow Ping only	CPU S7-1513
5.		• "RemoteServiceAdmin" User: - Read and Write Authorization • User "RemoteIT": - Only login to the firewall	SCALANCE SC
6.	MAC based firewall	• Allow DCP protocol • Prohibit Web Server Access	SCALANCE XB208
7.		• Prohibit DCP protocol • Allow web server access	CPU S7-1513

2.2.2 Preparing the environment

Factory setting

To ensure that no existing configurations are stored in the SCALANCE, reset the assemblies to factory defaults.

Initial IP address assignment

At delivery, the SCALANCE devices have no IP address. The initial assignment of an IP address for the device cannot be done with Web Based Management because this configuration tool already requires an IP address. The following options are available for assigning an IP address to an unconfigured device:

- TIA Portal
- Primary Setup Tool
- CLI (serial)

Assign the IP address and the router IP address to the SCALANCE XB208 device according to Table 2-1 or Table 2-2.

Assign the IP address for VLAN 1 "192.168.1.1" to the SCALANCE S device.

TIA Portal project

Create a TIA Portal project with your used S7-1500 CPU. Configure the interface of the CPU according to Table 2-1 or Table 2-2. Activate the web server of the CPU and create a new user. Load the controller.

Web Based Management

If you configure SCALANCE via Web Based Management, then open Web Based Management via the address "https://192.168.1.1" and log in.

When you log in for the first time or after setting to factory default, the login data is set as follows:

- Name: "admin"
- Password: "admin"

When you log in for the first time or after setting to factory defaults, you will be prompted to change the password.

Note In Web Based Management, you save each setting using the "Set Values".

2.2.3 Prepare SCALANCE SC636-2C

Create IP subnet

SCALANCE SC636-2C has six ports that are factory set as follows:

- Port 1 to port 4: VLAN 1 "vlan1 (INT)"
  For access from the local area network (LAN) to the device.
- Port 5 and port 6: VLAN 2 "vlan2 (EXT)"
  For access from the external network (WAN) to the device.

Note To configure the modules, the PG is first connected to a free port of SCALANCE XB208.

The VLANs are in different IP subnets. You have already assigned the IP address for VLAN 1 by the initial IP address assignment in section 2.2.2

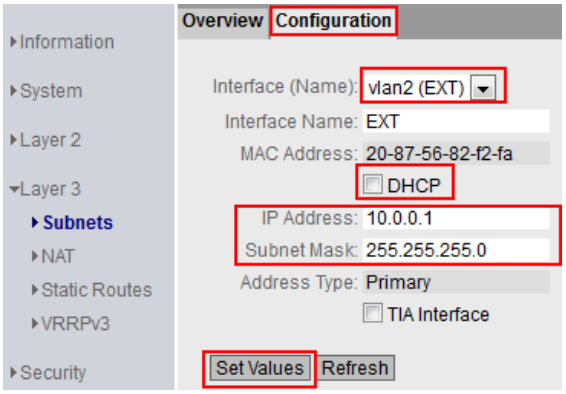
Proceed as follows to configure the IP subnet for VLAN 2:

1. Open the Web Based Management of SCALANCE SC636-2C via the IP address "192.168.1.1".

2. Click on "Layer 3 > Subnets" in the navigation pane and on the "Configuration" tab in the content pane.

3. Select "vlan2 (EXT)" from the drop-down list under "Interface (Name)". Disable the option "DHCP".
   Enter the IP address "10.0.0.1" and the subnet mask "255.255.255.0" in the input fields provided.
   To apply the settings, click on "Set Values".

   Figure 2-2



Result
The IP subnets are created in SCALANCE SC and are displayed in the "Overview" tab.

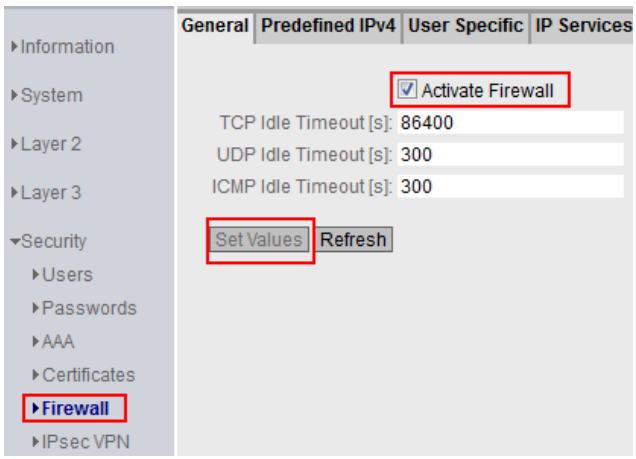
Figure 2-3

Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask
	vlan1	yes	INT	20-87-56-82-f2-fa	192.168.1.1	255.255.255.0
☐	vlan2	-	EXT	20-87-56-82-f2-fa	10.0.0.1	255.255.255.0

Activating the firewall

This example focuses on the use of the firewall. The firewall is activated by default. Check in the navigation under "Security > Firewall" in the tab "General" whether the firewall is activated and activate the firewall if necessary.
To apply the settings, click on "Set Values".

Figure 2-4



2.2.4 IP-based firewall

Description

The IP-based stateful packet inspection firewall is supported by all Security Integrated products. When configuring the firewall in SCALANCE S and SCALANCE M, you have the following options:

- Use predefined packet filter rules
- Manually define your own packet filter rules

Note In this example, the IP rules are created manually.

Overview

The following scenarios are provided for the IP-based firewall:

Table 2-4

Test	Target device
• Allow only secure protocols: - HTTPS (Port 443) - SSH (Port 22) • Prevent all other protocols	SCALANCE XB208
• STEP 7 Allow remote programming (Port 102) • Allow Web Server Access (Port 443) • Prevent all other protocols	CPU S7-1513

Note To configure the modules, the PG is first connected to a free port of SCALANCE XB208.

Creating IP services

You can use the IP service definitions to define packet filtering rules for the firewall that are applied to specific services. You assign a name and assign the service parameters to it.

In this example, the following IP services are set up:

Table 2-5

IP service	Destination port	Protocol
HTTPS	443	TCP
SSH	22	TCP
STEP7	102	TCP

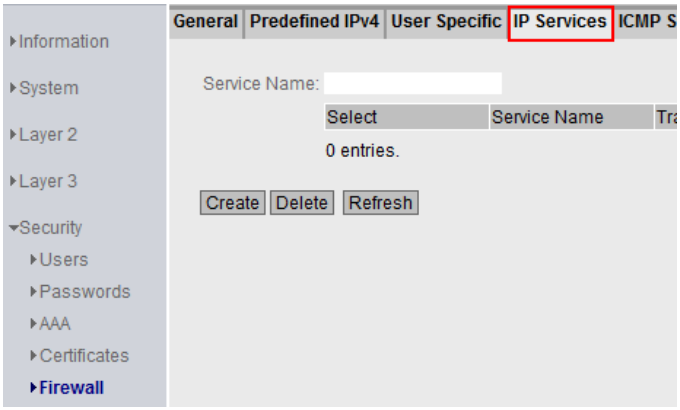
Note You always define the destination port. The source port is usually unknown and cannot be restricted.

To determine the services, proceed as follows:

1. Open the Web Based Management of SCALANCE SC636-2C via the IP address "192.168.1.1".

2. Navigate to the "Security > Firewall" menu and here to the "IP Services" tab.

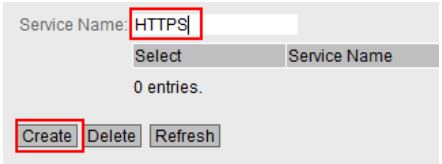
   Figure 2-5



3. In the entry field "Service Name" you define a unique name for the IP service. Enter the name "HTTPS" for this example.

   To generate a new table row, click the Create button.

   Figure 2-6



4. Change the new table row. Use the screenshot as a guide.
   To confirm your settings, click on the "Set Values" button.

   Figure 2-7

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
☐	HTTPS	TCP	*	443

5. Repeat step 2 and step 3 for each IP service required in this example (see Table 2-5) so that all IP services are created in the table.

   Figure 2-8

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
☐	SSH	TCP	*	22
☐	HTTPS	TCP	*	443
☐	STEP7	TCP	*	102

Result

You have created the IP services required for this example and assigned unique names. Use this name when configuring the IP rules.

Defining the IP rules

If you create your own IP rules, these IP rules have priority:

- over the predefined IP packet filter rules (Predefined IPv4) and
- over the IP packet filter rules, which are automatically created based on a connection configuration (SINEMA RC).

In order for the PG with the IP address "10.0.0.10" to communicate internally from external to internal only to a limited extent, you must define the IP rules.

Note With a stateful packet inspection firewall, you only need to set a firewall rule for the request direction from source to destination. The second rule is added implicitly.

The following IP rules are provided for this example:

Table 2-6

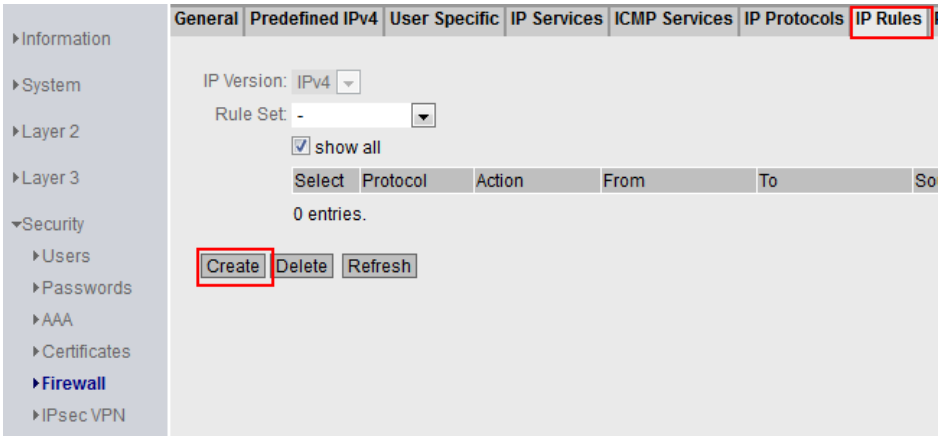
Action	Direction	Source	Goal	IP service
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.2 (XB208)	HTTPS
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.2 (XB208)	SSH
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.3 (CPU)	HTTPS
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.3 (CPU)	STEP7

Note If a packet hits the firewall that is neither HTTPS, SSH, or STEP7, then there is no match with any of the packet filtering rules for the firewall. The data packet is discarded.

To create your own IP rules, proceed as follows:

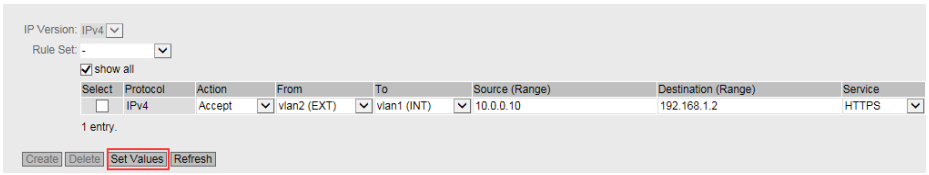
1. Navigate to the "Security > Firewall" menu and here to the "IP Rules" tab. To generate a new table row, click the Create button.

   Figure 2-9



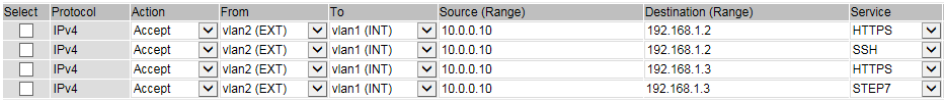
2. Change the line. Use the screenshot as a guide. To confirm your settings, click on the "Set Values" button.

   Figure 2-10



3. Repeat step 2 and step 3 for each IP rule required in this example (see Table 2-6) so that all IP rules are entered in the table.

   Figure 2-11



Result

You have created IP rules manually. With these IP rules, the PG with the IP address "10.0.0.10" can communicate with the internal network to a limited extent.

2.2.5 User-specific firewall

Description

The user-specific firewall is supported by the SCALANCE S industrial security appliances (S615 and SC-600) and the SCALANCE M industrial routers. The user-specific firewall allows the IP rulesets of the stateful packet inspection firewall to be assigned to one or more users.

If the user's login was successful, the firewall ruleset intended for this user is activated. After logging in, a timer is started. After the time has elapsed, the user is automatically logged out of the device.

User access

The access for the user to the Web Based Management of SCALANCE and the logon to the firewall is controlled by the following objects:

- Role
  - Admin: Read and write rights in Web Based Management from SCALANCE.
  - User: Read-only rights in Web Based Management from SCALANCE.
  - Self-defined roles.
- Remote access: Three settings are available for remote access:
  - "Only" The user can only log on to the firewall, but not to the Web Based Management of SCALANCE.
  - "None" The user can only access the Web Based Management of SCALANCE.
  - "Additional" The user can log on to the firewall and additionally access the Web Based Management of SCALANCE.
- Rule set with packet filter rules of the firewall.

Overview

The following scenarios are provided for the user-specific firewall:

Table 2-7

Test	Target device
• "RemoteServiceAdmin" User: - Allow Web Server Access (Port 443) • User "RemoteIT": - Allow Ping only	SCALANCE XB208
• "RemoteServiceAdmin" User: - Allow Web Server Access (Port 443) - Allow remote programming (port 102) • User "RemoteIT": - Allow Ping only	CPU S7-1513
• "RemoteServiceAdmin" User: - Read and Write Authorization - Login to the firewall • User "RemoteIT": - Login to the firewall	SCALANCE SC

Note To configure the modules, the PG is first connected to a free port of SCALANCE XB208.

Creating users

The following users are used for the user-specific firewall in this application example:

- "RemoteServiceAdmin" User: The user gets the predefined role "admin" and the remote access setting "additional".
  With this combination, the user receives the right for remote access and read and write access to the Web Based Management of SCALANCE.
- User "RemoteIT": The user gets the predefined role "user" and the remote access setting "only".
  With this combination, the user is only granted remote access rights, i.e. he has no rights other than logon to the user-specific firewall.

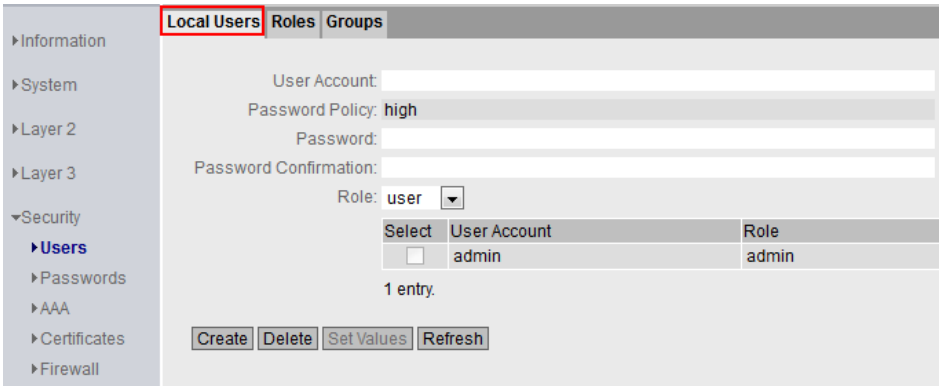
Note To be able to create a new user, the logged in user must have the role "admin".

To create a new user, proceed as follows:

1. Open the Web Based Management of SCALANCE SC636-2C via the IP address "192.168.1.1".

2. Navigate to the "Security > Users" menu and here to the "Local Users" tab.

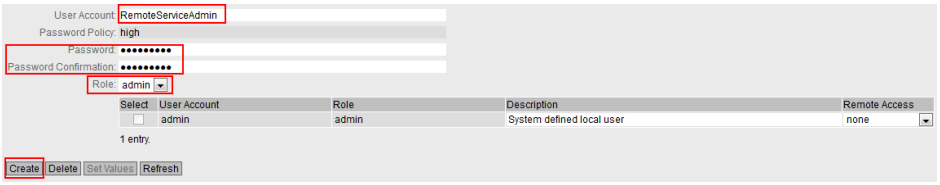
Figure 2-12



3. Create a new user:
   - In the "User Account" field, enter the name of the user. The name must be unique and between 1 and 250 characters long.
     Use the name "RemoteServiceAdmin" for this example.
   - Enter the password for the user in the "Password" input field. To confirm the password, re-enter the password in the "Password Confirmation" input field.
   - In the "Role" drop-down list, select the role of the user. In this example, the RemoteServiceAdmin user has the predefined "admin" role.

   To add the user to the table, click the Create button.

   Figure 2-13



4. The new user is added to the table.

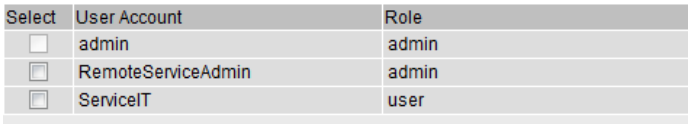
   Figure 2-14

Select	User Account	Role
☐	admin	admin
☐	RemoteServiceAdmin	admin

5. To set up another user, repeat step 2.
   Use the name "RemoteIT" and give the user the predefined role "user".

6. The new user is added to the table.

   Figure 2-15

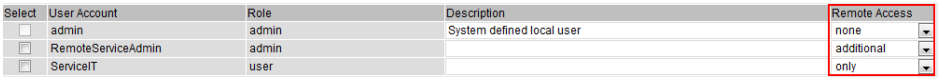


Select	User Account	Role
	admin	admin
	RemoteServiceAdmin	admin
	ServiceIT	user

7. In the "Remote Access" column of the table, you can assign users the right for remote access. The default setting is that users are not granted remote access.
   The following authorizations are available via the selection list:
   - "only": Remote access only, i.e. no rights other than logon for the custom firewall.
   - "none": No remote access. The user is logged on with the rights of the linked role.
   - "additional": Remote access and rights assigned to the user.

   Assign the authorizations provided to the users in this example. Use the screenshot as a guide.
   To confirm your settings, click on the "Set Values" button.

   Figure 2-16



Select	User Account	Role	Description	Remote Access
	admin	admin	System defined local user	none
	RemoteServiceAdmin	admin		additional
	ServiceIT	user		only

Note You can only use the users with remote access "only" or "additional" for the custom firewall.

Result
You have set up the RemoteServiceAdmin and RemoteIT users and granted them remote access privileges.

Creating IP services

You can use the IP service definitions to define packet filtering rules for the firewall that are applied to specific services. You assign a name and assign the service parameters to it.
In this example, the following IP services are set up:

Table 2-8

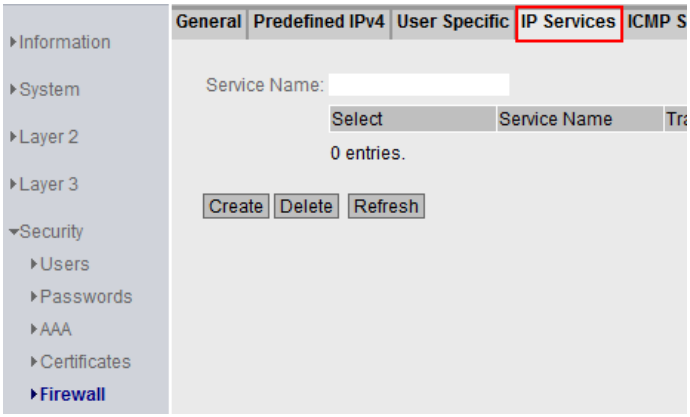
IP service	Destination port	Protocol
HTTPS	443	TCP
STEP7	102	TCP

Note You always define the destination port. The source port is usually unknown and cannot be restricted.

To determine the services, proceed as follows:

1. Navigate to the "Security > Firewall" menu and here to the "IP Services" tab.

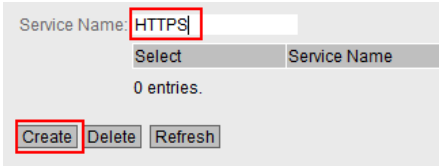
   Figure 2-17



2. In the entry field "Service Name" you define a unique name for the IP service. Enter the name "HTTPS" for this example.

   To generate a new table row, click the Create button.

   Figure 2-18



3. Change the new table row. Use the screenshot as a guide.
   To confirm your settings, click on the "Set Values" button.

   Figure 2-19

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
☐	HTTPS	TCP	*	443

4. Repeat step 2 and step 3 for each IP service required in this example (see Table 2-8) so that all IP services are created in the table.

   Figure 2-20

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
☐	HTTPS	TCP	*	443
☐	STEP7	TCP	*	102

Result
You have created the IP services required for this example and assigned unique names. When configuring the IP rules, simply use that name.

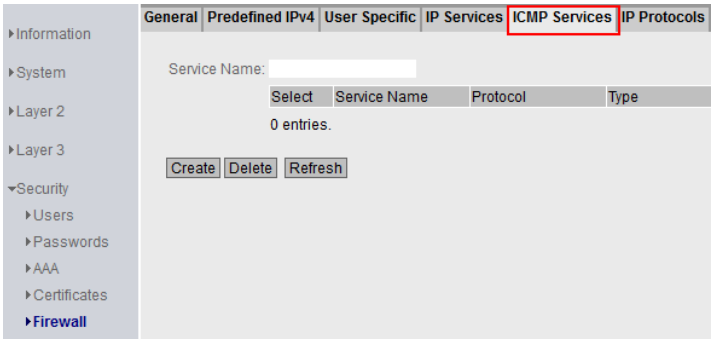
Creating IP services

You can use the ICMP service definitions to define packet filtering rules for the firewall that are applied to ICMP commands.

To determine the services, proceed as follows:

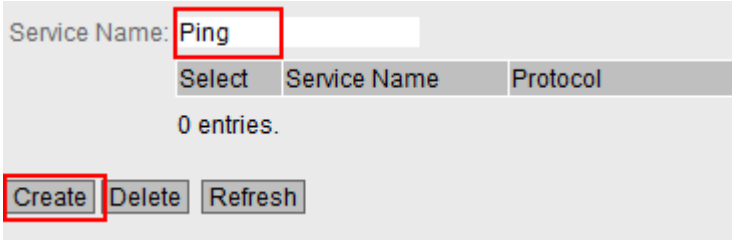
1. Navigate to the "Security > Firewall" menu and here to the "ICMP Services" tab.

   Figure 2-21



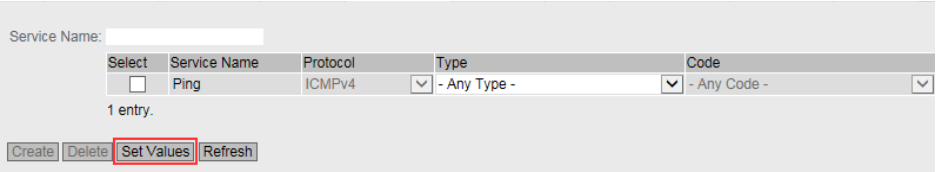
2. In the entry field "Service Name" you define a unique name for the ICMP service. Enter the name "Ping" for this example.

   To generate a new table row, click the Create button.
   Figure 2-22



3. A new table row appears. You do not need to make any further changes in the table line.
   To confirm your settings, click on the "Set Values" button.

   Figure 2-23



Define rule sets

With a rule set, the packet filter rules for the firewall can be combined and assigned to one or more users. If the user's login was successful, the firewall ruleset intended for this user is activated.

In this example, the following rule sets are set up:

Table 2-9

Rule set	Meaning
RemoteService	This rule set contains the packet filter rules for the firewall for the RemoteServiceAdmin user.
IT	The packet filter rules for the firewall for the user "RemoteIT" are summarized under this rule set.

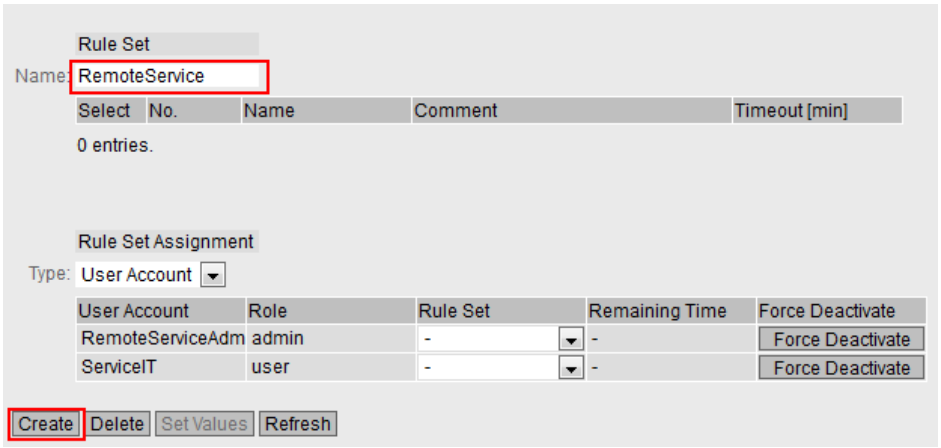
To create new rule records, proceed as follows:

1. Navigate to the "Security > Firewall" menu and here to the "User Specific" tab. Page is made up of the sections
   - "Rule set" and
   - "Rule set Assignment".

   Figure 2-24

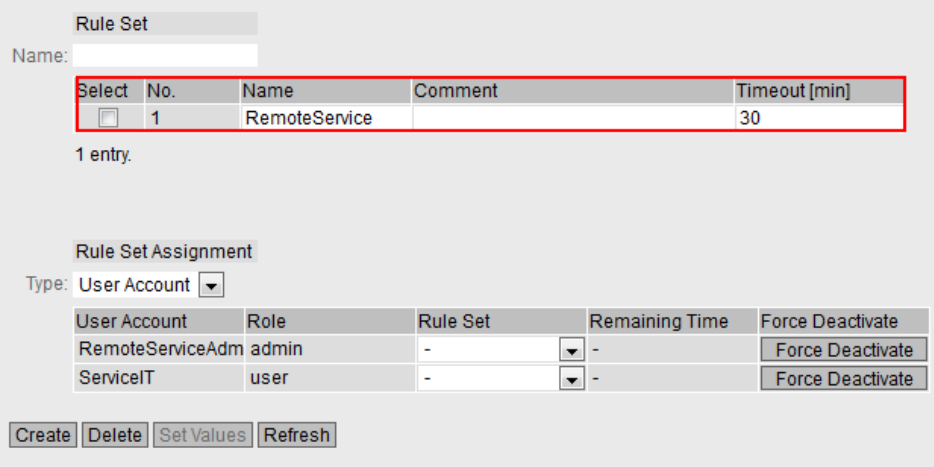
2. In the "Rule Set" section, define a unique name for the rule set in the "Name" input field. Enter the name "RemoteService" for this example.
   To generate a new table row, click the Create button.

   Figure 2-25



3. The new rule record is displayed in the table. The allowed access time is set to 30 minutes by default and can be adjusted if necessary.

   Figure 2-26



4. Repeat step 2 for the second rule set. Select the name "IT" for this example.

5. The new rule record appears in the table.

   Figure 2-27

Select	No.	Name	Comment	Timeout [min]
	1	RemoteService		30
	2	IT		30

Result

You have defined two new rule sets and can assign them to the users.

Define rule sets

In the section "Rule Set Assignment" you can assign the newly created rule sets to users or to the digital input of SCALANCE.

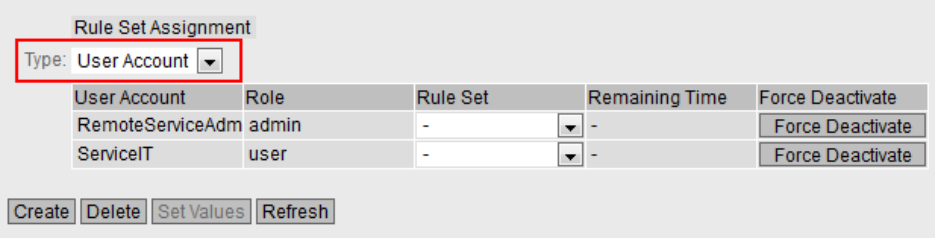
Note

Only those users are displayed in the table who have remote access "only" or "additional".

To assign a rule record to one or more users, proceed as follows:

1. In the "Type" drop-down list, select the "User Account" type.

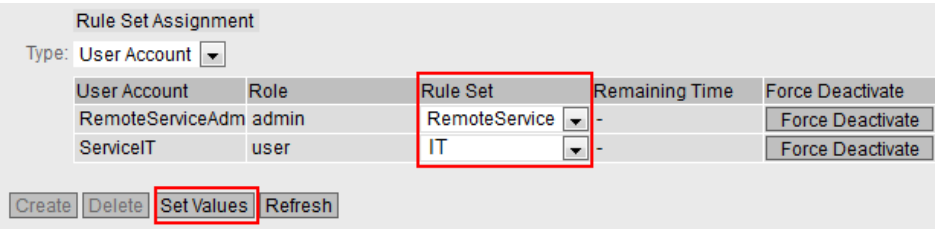
   Figure 2-28



2. In the table column "Rule Set", you define the rule set that is valid for this user. The selection list lists all the rule records that you have previously created. Change the table column. Use the screenshot as a guide.

   To confirm your settings, click on the "Set Values" button.

   Figure 2-29



Result

For this example, you have assigned one rule record per user. When the user logs on to SCALANCE, the assigned rule record is activated for him or her.

Define IP Rules and Assign to a Rule Set

You must define the IP rules and assign these IP rules to a rule set so that users can only communicate from external to internal to a limited extent.

Note With a stateful packet inspection firewall, you only need to set a firewall rule for the request direction from source to destination. The second rule is added implicitly.

The following IP rules are provided for this example:

Table 2-10

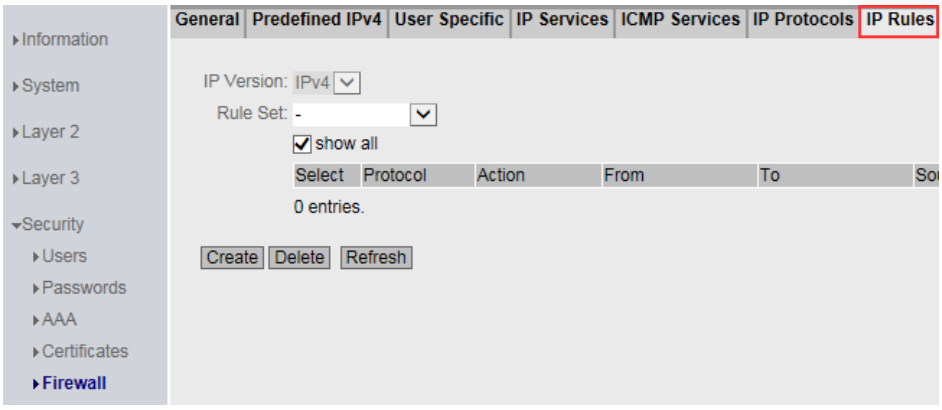
Action	Direction	Source	Goal	IP service	Rule set
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.2 (XB208)	HTTPS	RemoteService
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.3 (CPU)	HTTPS	RemoteService
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.3 (CPU)	STEP7	RemoteService
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.3 (CPU)	Ping	IT
Accept	vlan 2 -> vlan 1	10.0.0.10 (PG)	192.168.1.2 (XB208)	Ping	IT
Accept	vlan 2 -> Device	10.0.0.10 (PG)	10.0.0.1 (SCALANCE SC)	HTTPS	-

Note The last packet filter rule ("Accept vlan 2 -> Device") is required to access Web Based Management and the firewall logon of SCALANCE SC from VLAN 2.
By default, access to Web Based Management and firewall logon is only permitted via VLAN 1.

To create your own IP rules, proceed as follows:

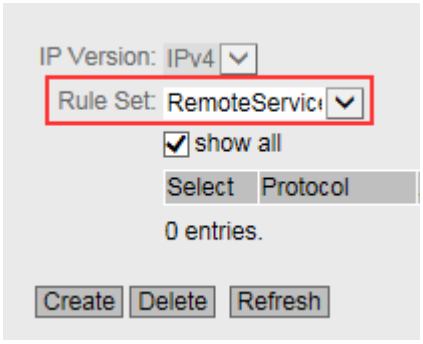
1. Navigate to the "Security > Firewall" menu and here to the "IP Rules" tab.

   Figure 2-30



2. To create the packet filter rules for the rule set "RemoteService", select the rule set "RemoteService" from the selection list under "Rule Set".

   Figure 2-31

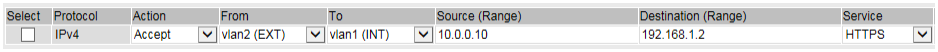


3. To generate a new table row, click the Create button.

   Figure 2-32

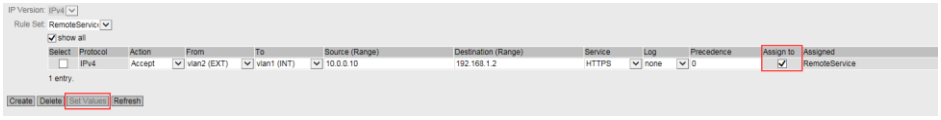
4. Change the line. Use the screenshot as a guide.

   Figure 2-33



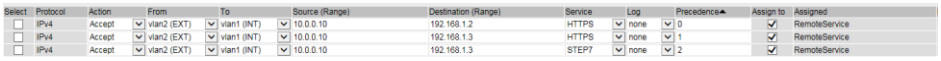
5. To assign the IP rule to the "RemoteService" rule set, activate the option box in the "Assigned to" column. The assigned rule set is displayed in the "Assigned" column.
   To confirm your settings, click on the "Set Values" button.

   Figure 2-34



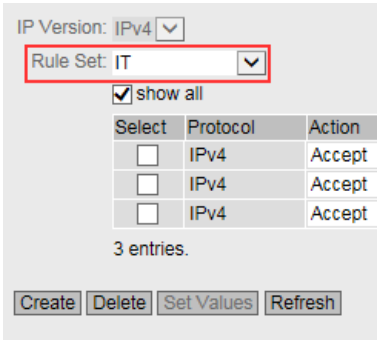
6. Repeat step 3 to step 5 for the other two IP rules for the rule set "RemoteService" (see Table 2-10) so that all IP rules are entered in the table.

   Figure 2-35



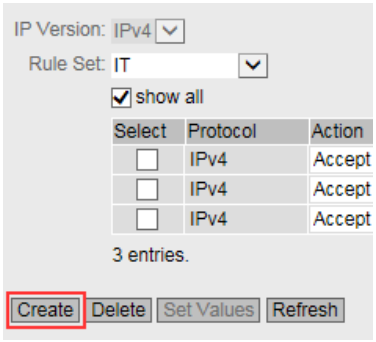
7. To create the packet filter rules for the rule set "IT", select the rule set "IT" from the selection list under "Rule Set".

   Figure 2-36



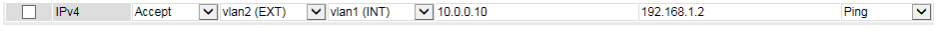
8. To generate a new table row, click the Create button.

   Figure 2-37



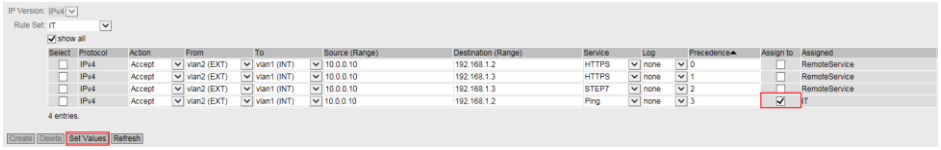
9. Change the line. Use the screenshot as a guide.

   Figure 2-38



10. To assign the IP rule to the "IT" rule set, activate the option box in the "Assign to" column. The assigned rule set is displayed in the "Assigned" column.
    To confirm your settings, click on the "Set Values" button.

    Figure 2-39



11. Repeat step 8 to step 10 for the second IP rule for the rule set "IT" (see Table 2-10) so that all IP rules are entered in the table.

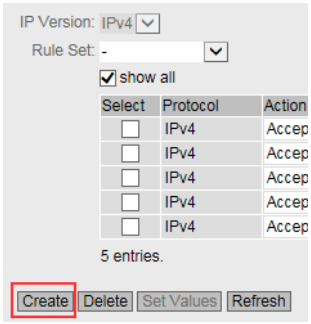
    Figure 2-40

12. To create the packet filter rule for accessing SCALANCE SC from VLAN2, do not select a rule set ("-") from the selection list under "Rule Set".

    Figure 2-41

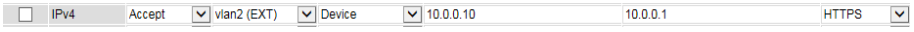
13. To generate a new table row, click the Create button.

    Figure 2-42



14. Change the line. Use the screenshot as a guide.
    To confirm your settings, click on the "Set Values" button.

    Figure 2-43



Result

You have created IP rules manually and assigned each IP rule to a rule set. When the user logs on to the firewall, the assigned rule set is activated and the IP rules it contains take effect. The user can communicate with the internal network to a limited extent.

Figure 2-44

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence▲	Assign to	Assigned
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.2	HTTPS	none	0	☐	RemoteService
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.3	HTTPS	none	1	☐	RemoteService
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.3	STEP7	none	2	☐	RemoteService
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.2	Ping	none	3	☐	IT
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.3	Ping	none	4	☐	IT

With the additional packet filter rule with "Device" as target, you can now also achieve Web Based Management and firewall logon of SCALANCE SC from VLAN 2.

Figure 2-45

	IPv4	Accept	vlan2 (EXT)	Device	10.0.0.10	10.0.0.1	HTTPS

2.2.6 MAC based firewall

Description

The MAC-based firewall is supported by all devices of the SCALANCE SC series, as these devices can work in bridge mode.

You have the following options when configuring the firewall:

- Use predefined rules
- Define your own rules manually

Note In this example, the MAC rules are created manually.

Inter-VLAN Bridge

With the "Inter-VLAN Bridge" function of SCALANCE SC, you can operate the board in bridge mode.
The Inter-VLAN Bridge feature bridges multiple VLANs to achieve a flat network.

SCALANCE SC allows you to create one bridge per device and add a maximum of six VLANs to the bridge. When configuring the "Inter-VLAN Bridge", you specify between which VLANs a bridge is to be set up and specify a VLAN as the master VLAN.
Once the "Inter-VLAN Bridge" function is activated, the bridge takes over the IP address configuration of the master VLAN. After activating the bridge, the devices of the VLANs can no longer be reached via their own IP addresses, but only via the IP address of the bridge.

In this example, the VLAN 2 is configured as master VLAN and the VLAN 1 as member VLAN.

Note If you operate the SCALANCE SC in bridge mode, the interface configured as TIA interface must be the master VLAN.

Overview

The following scenarios are provided for the MAC-based firewall:

Table 2-11

Test	Target device
• Allow DCP protocol • Prohibit Web Server Access	SCALANCE XB208
• Prohibit DCP protocol • Allow web server access	CPU S7-1513

Note To configure the modules, the PG is first connected to a free port of SCALANCE XB208.

Allow access to the WBM via VLAN 2

By default, access to Web Based Management is only permitted via VLAN 1. Since an Inter-VLAN Bridge is set up for the MAC-based firewall and the TIA interface must be changed to VLAN 2, you must also allow access to Web Based Management via VLAN 2.

You can create your own IP packet filter rule or use the predefined packet filter rules.

Note Since this section focuses on the MAC-based firewall, access to Web Based Management from VLAN 2 is enabled via the predefined packet filter rules.

To allow access to Web Based Management also via VLAN 2, proceed as follows:

1. Open the Web Based Management of SCALANCE SC636-2C via the IP address "192.168.1.1".

2. Navigate to the "Security > Firewall" menu and here to the "Predefined IPv4" tab.
   Activate the option box "HTTPS" in the line "vlan 2 (EXT)".

   Figure 2-46

3. To confirm your settings, click on the "Set Values" button.

Changing the TIA Interface

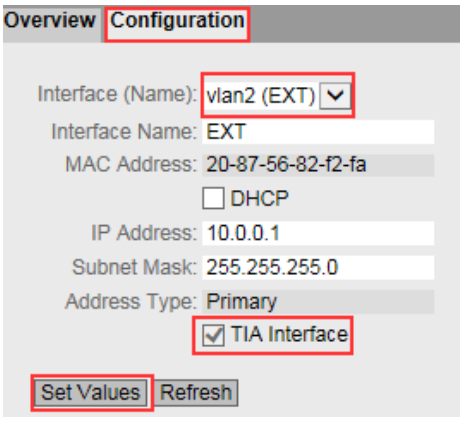
If you operate the SCALANCE SC in bridge mode, the interface configured as TIA interface must be the master VLAN. Otherwise the bridge cannot be activated. The TIA interface is by default in VLAN 1 and must therefore be changed to VLAN 2.

To change the TIA interface, proceed as follows:

1. Click on "Layer 3 > Subnets" in the navigation pane and on the "Configuration" tab in the content pane.

2. Select "vlan2 (EXT)" from the drop-down list under "Interface (Name)". Activate the "TIA Interface" option box.
   To apply the settings, click on "Set Values".

   Figure 2-47



3. Connect the PG to port 5 of the SCALANCE SC (see Figure 2-1).
   Web Based Management can now be accessed via the IP address "10.0.0.1".

Result

The TIA interface is set to VLAN 2.

Figure 2-48

Select	Interface	TIA Interface	Interface Name
☐	vlan1	-	INT
	vlan2	yes	EXT

Activating the bridge mode

With the "Inter-VLAN Bridge" function of SCALANCE SC, you can operate the board in bridge mode.
The Inter-VLAN Bridge feature bridges multiple VLANs to achieve a flat network.

In this example, the types of interfaces are defined as follows:

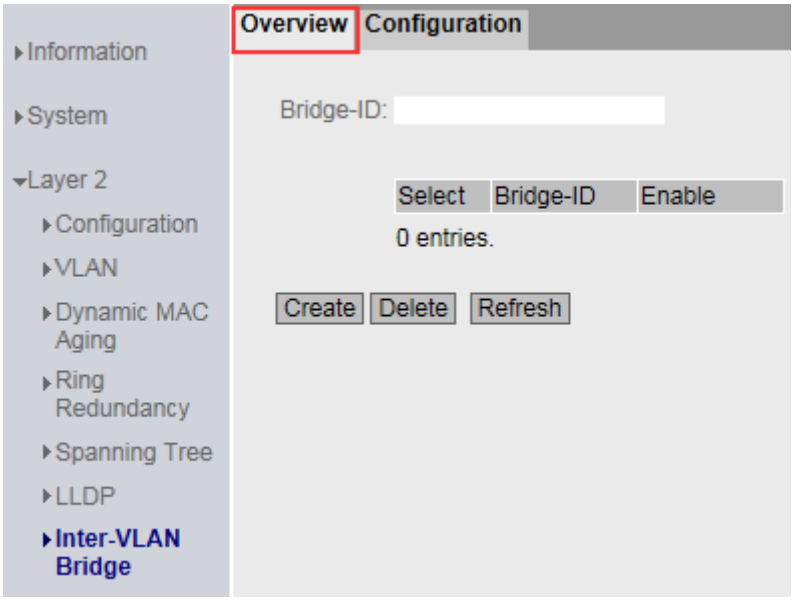
Table 2-12

Interface	Type
VLAN 2 "vlan2"	Master
VLAN 1 "vlan1"	Member

To create a new bridge, proceed as follows:

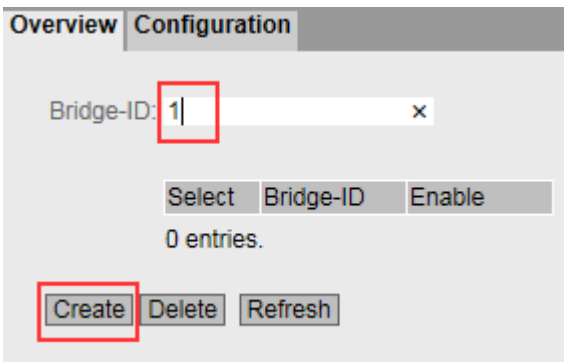
1. Navigate to the "Layer 2 > Inter-VLAN Bridge" menu and here to the "Overview" tab.

   Figure 2-49



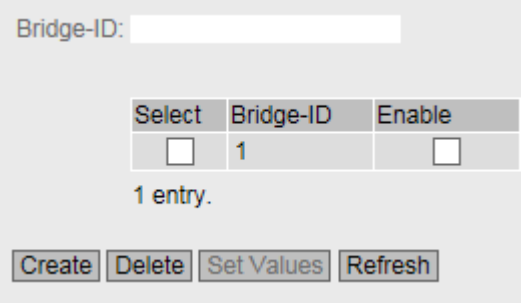
2. Enter a number between 1 and 255 as the Bridge ID in the "Bridge ID" input field. In this example the ID "1" is used.
   To generate a new table row, click the Create button.

   Figure 2-50



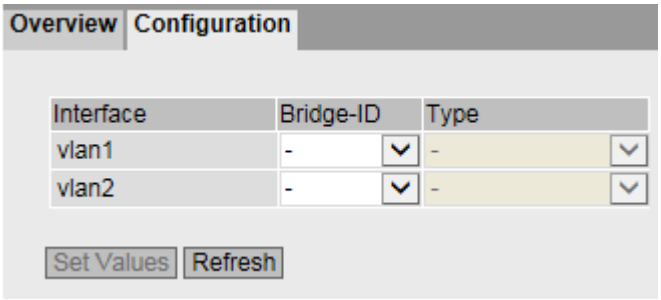
3. A new table row appears.

Figure 2-51



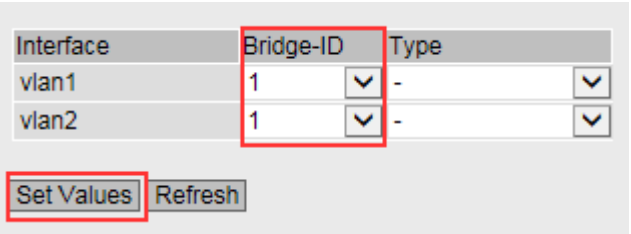
4. Switch to the "Configuration" tab. On this page you specify which VLANs a bridge is to be set up between and which VLAN is to be used as master VLAN. Only the VLANs that you defined in SCALANCE SC are displayed in the table.

Figure 2-52



5. In the Bridge ID table column, for all rows, select the bridge ID that you previously defined in step 2. In this example, the number "1" was selected as the ID.
To confirm your settings, click on the "Set Values" button.

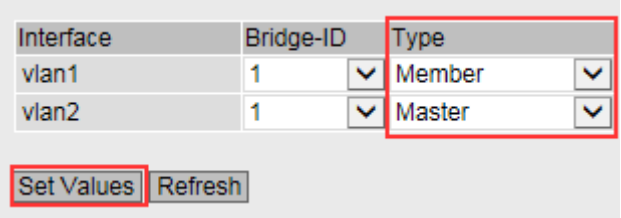
Figure 2-53



6. In this example, "vlan2" is used as master VLAN. All devices from VLAN 1 are therefore in the same network as VLAN 2. Change the type of the interfaces in the table column "Type". Use the screenshot as a guide.
   You are offered the following options:
   - Member: The IP address configuration of the VLAN is not used for the bridge.
   - Master: The IP address configuration of the VLAN is used for the bridge.

   To confirm your settings, click on the "Set Values" button.

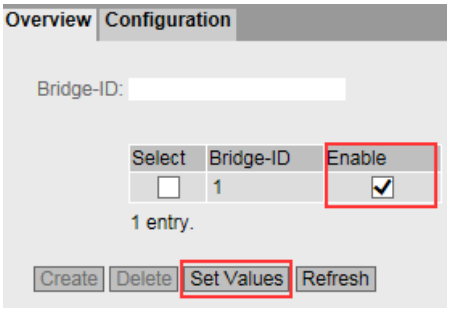
   Figure 2-54



7. Switch back to the "Overview" tab. Activate the bridge from step 2 by setting the option box in the "Enable" column.

   To confirm your settings, click on the "Set Values" button.

   Figure 2-55



Result

You have set up and activated bridge mode in SCALANCE SC. VLAN 1 and VLAN 2 are now flat networks and can also be reached at Layer 2 level.

Creating MAC services

You can use the IP service definitions to define packet filtering rules for the firewall that are applied to specific services. You assign a name and assign the service parameters to it.

In this example, the following MAC services are set up:

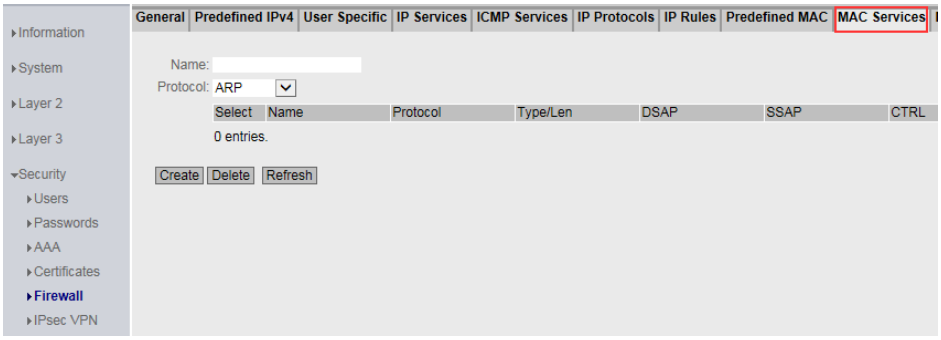
Table 2-13

Name	Protocol	Note
DCP	DCP	Used, for example, by the PST tool for node naming.
IP	IPv4	IP telegrams

To determine the services, proceed as follows:

1. Navigate to the "Security > Firewall" menu and here to the "MAC Services" tab.

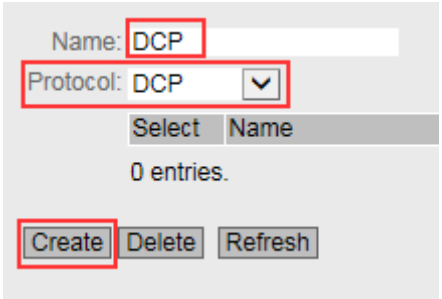
   Figure 2-56



2. In the entry field "Service Name" you define a unique name for the IP service. Enter the name "DCP" for this example and select the protocol "DCP" from the selection list under "Protocol".

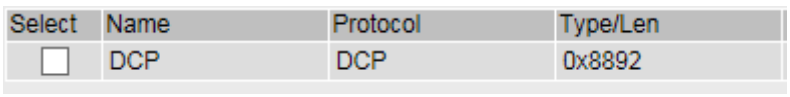
   To generate a new table row, click the Create button.

   Figure 2-57



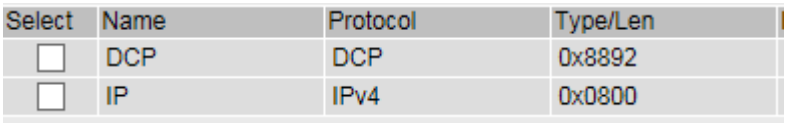
3. A new table row appears. You do not need to make any further changes in the table line.

   Figure 2-58



4. Repeat step 2 and step 3 for the second MAC service so that all services are created in the table (see Table 2-13).

Figure 2-59



Select	Name	Protocol	Type/Len
☐	DCP	DCP	0x8892
☐	IP	IPv4	0x0800

Result
You have created the MAC services required for this example and assigned unique names. Use this name for the project engineering of the MAC rules.

Define MAC rules

If you create your own MAC rules, then these MAC rules have priority over the predefined MAC packet filter rules.

In order for the PG to communicate from external to internal on Layer 2 level only to a limited extent, you must define the MAC rules.

Note

With a MAC-based firewall, you always need two packet filter rules for the firewall:

- For the request direction from the source to the destination
- For the response direction from destination to source

The following MAC rules are provided for this example:

Table 2-14

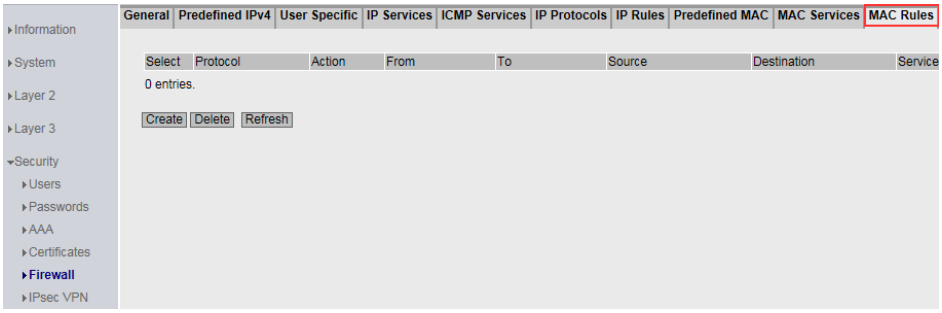
Action	Direction	Source	Goal	MAC-service	Comment
Accept	vlan 2->vlan 1	MAC address PG	---------[1]	DCP	Allows DCP request to VLAN1 from PG
Accept	vlan 1->vlan 2	MAC address XB208		DCP	Allows DCP response to VLAN2 from XB208
Drop	vlan 1->vlan 2	MAC address CPU	---------[1]	DCP	Prohibits DCP response to VLAN2 from CPU
Drop	vlan 2->vlan 1	MAC address PG	MAC address XB208	IP	Prohibits IP request to VLAN1 to XB208
Accept	vlan 2->vlan 1	MAC address PG	MAC address CPU	IP	Allows IP request to VLAN1 to CPU
Accept	vlan 1->vlan 2	MAC address CPU	MAC address PG	IP	Allows IP response to VLAN2 from CPU

[1] DCP is a multicast protocol. No specific MAC address is allowed here.

To create your own MAC rules, proceed as follows:

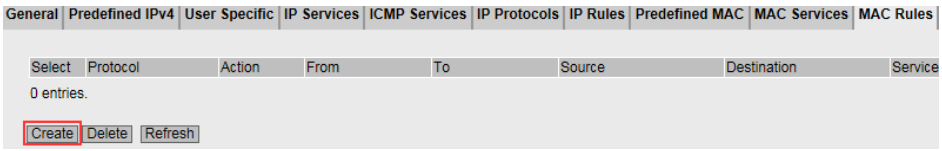
1. Navigate to the "Security > Firewall" menu and here to the "MAC Rules" tab.

Figure 2-60



2. To generate a new table row, click the Create button.

Figure 2-61



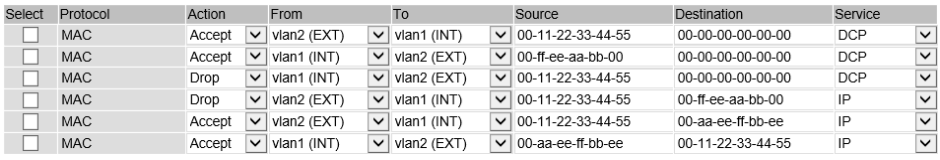
3. Change the line. Use the screenshot as a guide. Use the MAC address of your devices:
   - "Source" column: MAC address PG
   - "Destination" column: undefined MAC address

   To confirm your settings, click on the "Set Values" button.

Figure 2-62

4. Repeat step 2 and step 3 for each IP rule required in this example (see Table 2-14) so that all MAC rules are entered in the table.
   Table 2-14 shows which MAC addresses must be entered in the columns "Source" and "Destination".

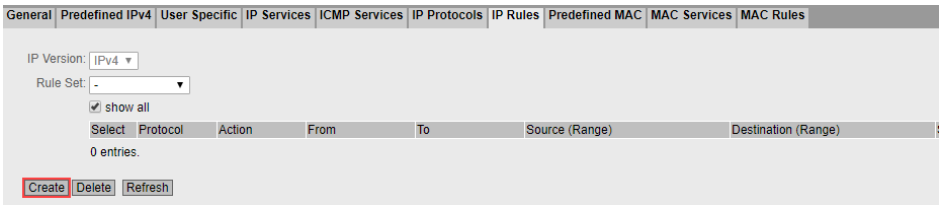
Figure 2-63



5. Create finally an IP rule that allows all IP traffic from vlan2 to vlan1.

   Navigate to "Security > Firewall" and here to the "IP Rules" tab.

Abbildung 2-64



To generate a new table row, click the Create button ("Create").

6. Change the line. Use the screenshot as a guide.
   - "From" column: vlan2(EXT)
   - "To" column: vlan1(INT)
   - "Services" column: "all"

   To confirm your settings, click on the "Set Values" button.

Abbildung 2-65

Result
You have created MAC rules manually. With these MAC rules, the PG can communicate with the internal network to a limited extent.

2.3 Operation

2.3.1 Requirement

In order to be able to test the application example, the following prerequisites are necessary:

- All participating devices are networked with each other as shown in Figure 2-1.
- The environment is prepared (See section 2.2.2).
- The web server of the CPU is accessible and a corresponding user is created.
- The PG only has the network setting:
  - IP address:10.0.0.10
  - Gateway: 10.0.0.1
- SCALANCE SC is configured (see section 2.2.3) and the firewall is configured.
  - For the "IP-based firewall" scenario, you must complete section 2.2.4
  - For the "User-specific firewall" scenario, you must complete section 2.2.5.
  - For the scenario "MAC-based firewall" you must complete section 2.2.6.

2.3.2 IP-based firewall

To test the IP-based firewall, you can run the following test scenarios on the PG:

Table 2-15

No.	Scenario	Result
1.	Open the Web Based Management of SCALANCE XB208 with the PG via the IP address "https://192.168.1.2" or the CPU via the IP address "https://192.168.1.3".	A packet filter rule exists. The data packets can pass through the firewall and Web Based Management is opened.
2.	Open the Web Based Management of SCALANCE XB208 with the PG via the IP address "http://192.168.1.2" or the CPU via the IP address "https://192.168.1.3".	A packet filter rule exists. The data packets are discarded and Web Based Management is not opened.
3.	Use the PG to establish an SSH connection to the SCALANCE XB208.	A packet filter rule exists. The data packets can pass through the firewall and an SSH connection is possible.
4.	Use the PG to establish a Telnet connection to the SCALANCE XB208.	A packet filter rule exists. The data packets are discarded.
5.	Use TIA Portal to establish an online connection to the CPU.	A packet filter rule exists. The data packets can pass through the firewall.

Change the IP address of the PG to the IP address 10.0.0.20 and repeat the test scenarios. All test scenarios are unsuccessful because only the IP address 10.0.0.10 is allowed as the source in all packet filter rules of the firewall.

2.3.3 User-specific firewall

In this example, the users "RemoteServiceAdmin" and "RemoteIT" were created for the user-specific firewall.

If the user's login was successful, the firewall ruleset intended for this user is activated. After login a timer is started. After the time has elapsed, the user is automatically logged out of the device.

To test the user-specific firewall, you can use the PG to perform various test scenarios.

"RemoteServiceAdmin" test scenarios

For the "RemoteServiceAdmin" user, the packet filter rules from the "RemoteService" rule set apply (see Table 2-10). You can test the following scenarios:

Table 2-16

No.	Scenario	Result
1.	Open the Web Based Management of SCALANCE XB208 with the PG via the IP address "https://192.168.1.2" or the CPU via the IP address "https://192.168.1.3".	A packet filter rule exists. The data packets can pass through the firewall and Web Based Management is opened.
2.	Open the Web Based Management of SCALANCE XB208 with the PG via the IP address "http://192.168.1.2" or the CPU via the IP address "https://192.168.1.3".	A packet filter rule exists. The data packets are discarded and Web Based Management is not opened.
3.	Use the PG to establish a data connection (e.g. SSH or Telnet) to the SCALANCE XB208.	A packet filter rule exists. The data packets are discarded.
4.	Set with the PG a "Ping" command on SCALANCE XB208 or the CPU.	A packet filter rule exists. The data packets are discarded.
5.	Use TIA Portal to establish an online connection to the CPU.	A packet filter rule exists. The data packets can pass through the firewall.

Test scenarios "RemoteIT"

For the user "RemoteIT", the packet filter rules from the rule set "IT" apply (see Table 2-10). You can test the following scenarios:

Table 2-17

No.	Scenario	Result
1.	Open the Web Based Management of SCALANCE XB208 with the PG via the IP address "https://192.168.1.2" or the CPU via the IP address "https://192.168.1.3".	A packet filter rule exists. The data packets are discarded and Web Based Management is not opened.
2.	Use the PG to establish a data connection (e.g. SSH or Telnet) to the SCALANCE XB208.	A packet filter rule exists. The data packets are discarded.
3.	Set with the PG a "Ping" command on SCALANCE XB208 or the CPU.	A packet filter rule exists. The data packets can pass through the firewall.
4.	Use TIA Portal to establish an online connection to the CPU.	A packet filter rule exists. The data packets are discarded.

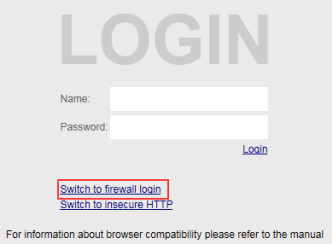
Firewall login

To log on to the SCALANCE SC firewall, proceed as follows:

1. Open the Web Based Management of SCALANCE SC via the address "https://10.0.0.1".

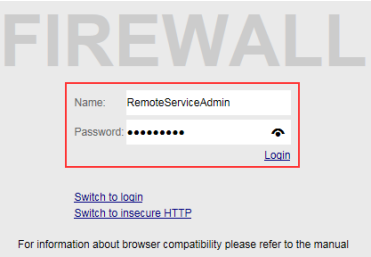
2. Click "Switch to firewall login" in the login window.

   Figure 2-66



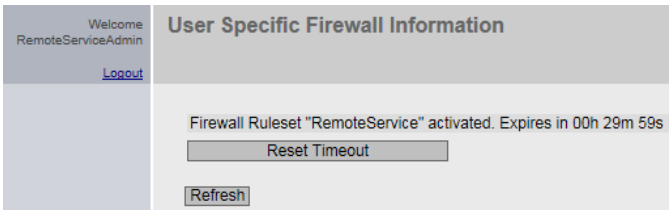
3. Log in with the user "RemoteServiceAdmin" or "RemoteIT" and the corresponding password.

   Figure 2-67



4. After successful login, the "User Specific Firewall Information" page opens. The rule set assigned to the user is activated and the timer for the permitted access time expires. In this example, the allowed access time is set to 30 minutes.

   Figure 2-68



5. Test the firewall with the proposed test scenarios.

Note During the access time, the "User specific firewall information" page must not be closed. If necessary, the user can extend the access time using the "Reset Timeout" button.

Firewall logout

To disconnect a user from the firewall, there are the following options:

- The permitted access time has expired.
- The user logs off by closing the "User specific firewall information" page.
- The device administrator deactivates the active user using the Force Deactivate button. You will find the button in the Web Based Management menu "Security > Firewall" and here in the tab "User Specific".

2.3.4 MAC based firewall

To test the MAC-based firewall, you can run the following test scenarios on the PG:

Table 2-18

No.	Scenario	Result
1.	Start a node naming tool on the PG, such as TIA Portal, Primary Setup Tool.	You only see SCALANCE XB208. There is a packet filter rule that allows the packet to the MAC address of SCALANCE XB208 to drop the packet to the MAC address of the CPU.
2.	Open the Web Based Management of SCALANCE XB208 with the PG via the IP address "http://10.0.0.2".	A packet filter rule exists. The data packets are discarded and Web Based Management is not opened.
3.	Open with the PG the Web Based Management of the CPU via the IP address "https://10.0.0.3".	A packet filter rule exists. The data packets can pass through the firewall.

Repeat the test scenarios with another PG. All test scenarios are unsuccessful because the MAC address of the PG is stored as the source in all packet filter rules.

3 Appendix

3.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:
https://support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:
www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:
www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:
https://support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:
https://support.industry.siemens.com/cs/ww/en/sc/2067

3.2 Links and literature

Table 3-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/22376747
\3\	Getting Started: Industrial Remote Communication Remote Networks - User-specific firewall https://support.industry.siemens.com/cs/ww/en/view/109764614
\4\	Project engineering manual: SIMATIC NET: Industrial Ethernet Security SCALANCE SC-600 Web Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109754815
\5\	Training: Security in Industrial Networks with SCALANCE (IK-SEC-S) https://www.sitrain-learning.siemens.com/DE/en/rw46479/Security-in-Industrial-Networks-mit-SCALANCE

3.3 Change documentation

Table 3-2

Version	Date	Modifications
V1.0	10/2014	First version
V2.0	07/2019	Complete revision
V2.1	12/2019	Correction of chapter MAC based firewall