S7-Firewall quick start guide

TRAEGER.DE
INDUSTRY COMPONENTS

Documentation for die Version 1.19

Introduction

S7 firewall is a scalable “PLC firewall”, which not only filters IP / MAC addresses, but also allows access to arbitrary data areas of the PLC to be restricted / defined. / S7-firewall detects the installation direction automatically. Only configured connections are allowed.

Hardware

Standard hardware

In the standard version, S7 firewall is equipped with a WAN port and 4 LAN ports as a switch.

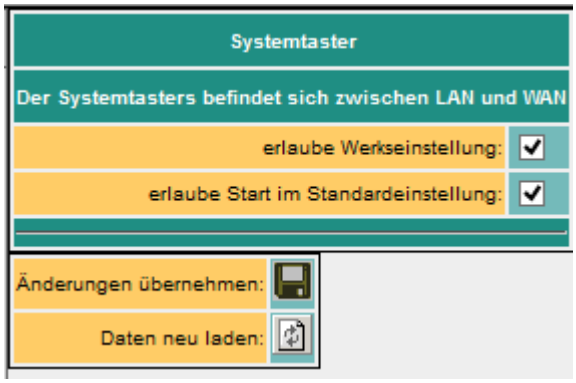
Operating modes	S7-Firewall
Services	DHCP Client/Server
	NTP Client/Server
Connections	1x WAN
	4x LAN-Port as Switch

Configuration

The network settings, etc. can be parameterized in the configuration. The input forms are usually self-explanatory. However, we are happy to accept suggestions from users to make the operation even easier.
In the delivery state, the following IP addresses are set:
192.168.1.57
192.168.2.1
You have the following options to access S7 firewall via WEB browser.
On the PC, assign an IP address from the corresponding network segment (for example, 192.168.1.100 or 192.168.2.100) and connect the PC to LAN or WAN via Ethernet. In the browser, type http: //192.168.1.57, or http: //192.168.2.1.
Or you make your PC to obtain IP address automatically and connect it to the LAN port of the S7 firewall. S7 firewall automatically assigns an IP address to the PC. In the browser you can address the device with: http: // S7 firewall.

System button, Reset system

Under the item System button, you have two options which are allowed when the button is pressed, at least one option must be selected:



allow factory settings	☑	The device can be set to the delivery condition

Allow start by default	☑	The device is set to the already stored basic settings

Attention!
Use one of the 4 switch ports to configure it because it may happen that the WAN port is no longer accessible
Do not leave the unit in operation. Disconnect the device from the production network and perform the reset in an autarkic environment. The configuration computer and the device should While not connected to the company network

No worries we do not take any work rest.
The button hides between WAN and LAN ports (small hole). Only the **activated** options are available.

Proceed as follows:

- E.g. Office clamps
- Make the device de-energized!
- Insert the clasp in the hole
- turn back on
- When the four LED's go out and only the power LED is on, hold down the button with the office clip until all four LEDs flash fast
- Release the button
- Now appears a sort of selection. When the button is pressed in the desired state, the desired action is performed
    - Basic setting
        - LED S3 (bottom right) flashes
            - The device boots in the basic setting (network / IP addresses of the delivery state are used). Now you can make the desired changes to the network settings. However, these settings are not activated until the device is restarted.
    - Factory setting
        - LED Power **and** S3 flash
            - All settings are deleted

Configuration of the device

Parameter	possible setting	Routing direction / purpose
device name	at will	
language	deutsch	Sets the language of the operating level. Possibly. After changing your WebBrowser, reload the page.
	englisch	
Standard Gateway	fix (as specified) from WAN over DHCP from WAN over PPPoE from LAN over DHCP from Modem over PPP	
1. DNS		
2. DNS		
Routing Mode	Office	LAN → Routinginterface
	Machine	Routinginterface → LAN
Routinginterface	WAN/IP	IP-Routing over WAN
	Modem	IP-Routing over Modem
	WAN/PPPOE	IP-Routing over PPPoE on WAN-Port
	WAN/OVPN	Routing over OVPN on WAN-Port
	WAN/Bridge	Ethernet-Routing on WAN-Port

Network settings

Parameter	mögliche Einstellung	Zweck
Nr.	automatisch	fortlaufende Nummer
Name	frei vom Benutzer einzugeben	Name der Station
aktiv	ja (x)	Verbindungen mit dieser Station werden von der Firewall verarbeitet
	nein ()	Verbindungen mit dieser Station werden nicht verarbeitet, d.h sie werden geblockt
IP-Adresse	IP-Adresse der SPS-Station	Identifikation des Absenders Eingabe unbedingt notwendig

Parameter	**Possible setting**	**Purpose**
Standard Gateway	fix (as defined), over DHCP	
1. DNS		
2. DNS		
1-3. IP address with Netmask	IP address / Netmask	Netmask 0.0.0.0 automatically calculates netmask, depending on A, B, C-B network. e.g. 192.168.0.x → 255.255.255.0 10.x.x.x → 255.0.0.0 When using fixed IP addresses, at least the 1st IP address must be configured. Otherwise the device starts with the factory setting
DHCP	no	Do not use DHCP The remaining DHCP parameters are not used
	Client	The network interface is called a DHCP client and obtains the IP address automatically from a DHCP server. The remaining DHCP parameters are not used
	Server	The network interface operates a DHCP server. The remaining DHCP parameters must be parameterized.
Start-IP	Start-IP-Address	Start IP address when operating as a DHCP server
End-IP	End-IP-Address	End IP address when operating as a DHCP server
Subnet	Subnetaddress	Address of the subnet for assigning the IP addresses as a DHCP server
Domain	Free	Name of the domain when used as a DHCP server
Router-IP	IP-Address	Is the IP address, which is passed as a DHCP server as a gateway during operation

The WAN / LAN port has shared IP addresses

Up to 3 different IP addresses and subnets can be configured. The port can also be operated as a DHCP server or client. The necessary data for the IP assignment is entered here. For the operation as DHCP / server fixed assignments MAC-IP address can be fixed. (See “DHCP fixed addresses). It also determines which services are available at the port (Web Config), Ping, SSH (for developers only)

DHCP Fixed MAC / IP address assignment

If the built-in DHCP server (on the WAN or LAN) is operated, it can be useful to allocate the same IP address to the IP addresses. Here you can specify which MAC address receives which IP address.

Web-User

Here is the form for the input of the WEB-Interface users. Per user, different authorizations can be assigned. In principle, only one user can make changes with “SU”. U1 - U5 is only allowed to operate the interface. In the S7 firewall expansion modules, “U1” - “U5” have more precisely specified operating rights.

S7-Firewall-settings

The PLC firewall connections result from the combination of HMI / PG station and PLC station

S7-Firewall operation

Modi	Description
off	no active Firewall
S7-Firewall Router	WAN port and LAN ports have separate IP networks. All functions and purchased options of the TeleR <4> / sup> can be used
S7-Firewall Classic	WAN port and LAN ports are an IP network. Only IP address ranges entered in the **WAN** page are handled. for example IP WAN 192.168.2.15 IP LAN: 192.168.3.3 If a device with the IP 192.168.3.6 is connected, this is not treated until a 192.168.3.xxx address is entered in the WAN

Enter the HMI / PG stations

		Nr.	Name	aktiv	IP-Adr-Bereich	MAC-Adresse	Verbindungskanal	lokaler TSAP	entfernter TSAP
		1	A		192.168.0.1-192.168.0.255	00:00:00:00:00:00	S7 over TSAP	\x04\x01	\x04\x01
		2	OP		192.168.0.1-192.168.0.255	00:00:00:00:00:00	OP/HMI		
		3	TSAP 02 00	x	192.168.0.1-192.168.0.255	00:00:00:00:00:00	RFC 1006 with TSAP	%02%00	%02%00
		4		x	0.0.0.0	00:00:00:00:00:00	OP/HMI		

Parameter	Possible setting	Purpose
Nr.	Automatic	consecutive number
Name	Free from the user	station name
active	yes (x)	Connections to this station are handled by the firewall
	no ()	Connections to this station are not processed, i.e. they are blocked
IP-Address	IP address of the HMI / PG device	Identification of the sender Input is essential
MAC-Address	MAC address of the HMI / PG device	Identifies the HMI / PG additionally via the MAC address. 00: 00: 00: 00: 00: 00 means that the MAC address is not checked. If the value is not equal to 0, the MAC address of the station must match the input

Parameter	Possible setting	Purpose
Connection channel	Used channel of the connection	In the Simatic S7 PG and OP channels are available. This channel is used as an additional feature for identifying the sender. Both PG and OP functions are possible on each of the two channels. Operating units / WinCC etc. usually use OP channels. This channel is also recommended for HMI devices. The Siemens PG software basically uses the PG channel. Unfortunately, there is a variety of software on the market that does not have the expertise to set this channel. This can be found in the LOG file. A reasonable HMI software, or the corresponding software driver, provides for the adjustability of this channel. For example, (PG / HMI identical) from the same computer, the PG / OP channel remains to identify the sender. The PLC channel corresponds to the “other” or “other” channel in the PLC

Input the PLC stations

Parameter	Possible setting	Purpose
Nr.	automatic	consecutive number
Name	Free of the user	Name of the Station
active	yes (x)	Connections to this station are handled by the firewall
	no()	Connections to this station are not processed, i. They are blocked
IP-Address	IP address of the PLC station	Identification of the sender Entry required

Enter the S7 firewall connections

The connections are made up of the combination HMI / PG station and PLC station. Each HMI / PLC station can be used several times. If the Mac or IP address is changed, this must only be changed centrally in the HMI / PG station or PLC station. Each connection is assigned a connection rule.
If “PG full function” is selected, this connection is a full access. In the future, this access can be divided more closely (Read / write defined blocks, PLC start / stop, reset, system data (read / write)).

Parameter	Possible setting	Purpose
Nr.	automatic	consecutive number
Name	Free of the user	Connection name Also serves as a “link” to open and edit the rule script.
active	yes (x)	This connection is processed by the firewall
	no ()	This connection is not processed, i. It is blocked
Allow PG Full Function	(x)	This connection is a PG connection and can carry out all functions
	no ()	This connection is a Restricted Connection. Only accesses to the shared function and data areas, as defined in the associated rule script, are permitted.

The rule script

In the rule script, the data areas or possible accesses for the respective connection are defined. The script can be reached via the link of the name of the connection.

Syntax of the control script

first Character	Function	Rest of the line
#	The line is a comment	free Text
Double slash		
(No character, it equals operand / range)	The following section is only for reading (readonly)	Operand / Range see below
r:		
w:	The following area is only for writing (writeonly)	
rw:	The following area is readable and writable (read / write)	

In a RuleRow, a single operand, or I can enter a range.

Example for entering individual operands: (source from Siemens STEP-S7 PG software)

Allowed operand	Data type	Example(Mnemonik German)	Example (Mnemonik English)
Input I Output I Flag	BYTE	EB 1 I AB 10 I MB 10	IB 1 I QB 10 I MB 10
Input I Output I Flag	WORD	EW 1 I AW 10 I MW 10	IW 1 I QW 10 I MW 10
Input I Output I Flag	DWORD	ED 1 I AD 10 I MD 10	ID 1 I QD 10 I MD 10
Periphery (Input I Output)	BYTE	PB 0 I PEB 0 I PAB 1	PB 0 I PIB 0 I PQB 1
Periphery (Input I Output)	WORD	PW 0 I PEW 0 I PAW 1	PW 0 I PIW 0 I PQW 1
Periphery (Input I Output)	DWORD	PW 0 I PED 0 I PAD 1	PD 0 I PID 0 I PQD 1
Timer	TIMER	T 1	T 1
Counter	COUNTER	Z 1	C 1
Data block	BOOL	DB1.DBX 1.0	DB1.DBX 1.0
Data block	BYTE	DB1.DBB 1	DB1.DBB 1
Data block	WORD	DB1.DBW 1	DB1.DBW 1
Data block	DWORD	DB1.DBD 1	DB1.DBD 1

Note: The entry of “DB0 …” is not allowed due to internal use.

Example for entering ranges, with number of units:

since Flag 60, 10 Byte: MB60, 10

since DB10, Data word 2, 5 words: DB10.DW2, 5

After the comma, the number of units required (depending on the address type, BOOL, BYTE, WORD, DWORD)

Example for entering ranges from “from” to ”:“

Flag Byte 70 bis Flag Byte 200: MB 70 – MB 200

Output A 10.2 bis Output 14.7: A 10.2 – A14.7

Just after start operands with, -, specify the end operand (end address). The end address is included!

Table of Contents