

**TECHNOLOGIECAMPUS GENT** 



# Siemens Scalance S623



#### **Overview**

- Basic Configuration
- Standard mode Firewall
- Advanced Firewall
- Password Management
- Advanced Password Management
- VPN with PreShared Key
- VPN with Certificates
- Gateway-to-Gateway VPN
- VPN with User Authentication

# **Technology Overview**

- User Authentication
  - On-device
  - Connection with RADIUS server
- VPN
  - IPsec end-to-end



#### **Necessary Software**

- Siemens Security Configuration Tool
- Siemens SOFTNET Security Client
- Siemens Automation License Manager
- (Optional) Siemens Primary Setup Tool



In this example we set the IP addresses of all 3 interfaces on the Scalance 623

This will demonstrate configuration steps that will be reused in every following example





1. Setting up the network

- Connecting the external interface of the Scalance to the PC
- Scalance interfaces
  - External network

Red marking = unprotected network area

Internal network

Green marking = network protected by Scalance

• DMZ port

Yellow marking = unprotected or protected network



2. Making	<b>IP</b> settings	for the PC
-----------	--------------------	------------

PC	IP address	Subnet mask
PC	192.168.10.2	255.255.255.0

Open Control Panel

#### "Start" > "Control Panel"

Control Panel

• Open "Network and Sharing Center"

Adjust your computer's settings				View by:	Small icons 🔻
Y Action Center	🎨 Administrative Tools	🔜 AutoPlay	妻 Backup and Restore		
🛃 Color Management	Communication Settings	Credential Manager	💣 Date and Time		
🛷 Default Programs	🔊 Dell Audio	🚺 Dell Command   Power Manager	Dell Command   Update		
Dell Touchpad	🔩 Desktop Gadgets	🛃 Device Manager	and Printers		
💐 Display	🚱 Ease of Access Center	Flash Player (32-bit)	🕼 Folder Options		
🗼 Fonts	Free Fall Data Protection	周 Getting Started	🤣 HomeGroup		
lndexing Options	闥 Intel(R) HD Graphics	Intel® PROSet/Wireless Tools	發 Intel® Rapid Storage Technology		
🎨 Internet Options	🔬 Java	🗢 Keyboard	Location and Other Sensors	_	
Mail (Microsoft Outlook 2013) (32-bit)	📕 Memory Card Parameter Assignmen	I Mouse	💐 Network and Sharing Center		
Real Icons	😹 NVIDIA Control Panel	🍇 Parental Controls	Performance Information and Tools		
💐 Personalization	Phone and Modem	Power Options	Programs and Features		
📽 Recovery	🔗 Region and Language	lt RemoteApp and Desktop Connections	Set PG/PC Interface (32-bit)		
Sound	Speech Recognition	🖲 Sync Center	ika System		
📃 Taskbar and Start Menu	🖪 Troubleshooting	& User Accounts	💐 Windows Anytime Upgrade		
🧵 Windows CardSpace	🍓 Windows Defender	💣 Windows Firewall	🐌 Windows Mobility Center		
🕙 Windows Update					

	2. N	2. Making IP settings for the PC		
	PC	IP address	Subnet mask	
	PC	192.168.10.2	255.255.255.0	
Select "Change adapter settings"			Control Panel Home	
			Manage wireless networks	
			Change adapter settings	
			Change advanced sharing settings	

Open the Local Area Connection Properties

Doubleclick "Local Area Connection", then click

"Properties"



Local Area Connection Network cable unplugged Intel(R) Ethernet Connection I218-...

2. Making IP settings for the PC

PC	IP address	Subnet mask
PC	192.168.10.2	255.255.255.0

- Click the "Properties" button
- Select "Use the following IP"
- Enter the values from the table in the relevant boxes
- Close the dialogs with "Ok" and close Control Panel

Local Area Connection Properties		
Networking Sharing		
Connect using:		
Intel(R) Ethernet Connection I218-LM		
<u><u>C</u>or</u>	Internet Protocol Version 4 (TCP/IPv	/4) Properties
This connection uses the following items:	General	
Pier File and Printer Sharing for Microsoft Networks     SMATIC Industrial Ethernet (ISO)     A PROFINET IO RT-Protocol V2.0     A Internet Protocol Version 6 (TCP/IPv6)	You can get IP settings assigned auto supports this capability. Otherwise, y administrator for the appropriate IP s	omatically if your network iou need to ask your network settings.
✓ Internet Protocol Version 4 (TCP/IPv4) ✓ Link-l aver Topology Discovery Manner I/O Driver	Obtain an IP address automatic	ally
<ul> <li>Link-Layer Topology Discovery Responder</li> </ul>	Ouse the following IP address:	
•	IP address:	192.168.10.2
Install Uninstall Pror	Subnet mask:	255.255.255.0
Description	Default gateway:	
I ransmission Control Protocol/Internet Protocol. The deta area network protocol that provides communication acros diverse interconnected networks.	Obtain DNS server address auto	omatically
	Use the following DNS server as	ddresses
Close	Preferred DNS server:	· · ·
Close	Alternate DNS server:	· · ·
	Validate settings upon exit	Advanced
		OK Cancel

3. Creating a project and security module

- Start the Security Configuration Tool
- Select the "Project" > "New..." menu command
- Create a new user This user is assigned the "administrator" role

🛐 New administr	ator	X
User name:	[]	
Password:		Very weak
Repeat password:		
	OK Cancel	Help

**KU LEUV** 

• Confirm with "OK"

3. Creating a project and security module

- In the "Product type", "Module" and "Firmware release" areas, select the following options
  - Product type: Scalance S
  - Module: S623
  - Firmware release: V4

Selection of a module	or software configuration			X
SCALANCE S     SOFTNET configura     (SOFTNET Security     NCP VPN client, VP1	tion Client, SCALANCE M87x/MI Ndevice)	D74x.		
Module				
© \$602		S623		
© \$612		S627-2M		
© \$613				
V3			1.	
Configuration				
Name of the module:	Module1			
MAC address:	00-1B-1B-BB-99-DE			
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0	
Interface routing externa	al/internal: Routing mode	•		
internation realing enterna				

3. Creating a project and security module

 In the "Configuration" area, enter the MAC address The MAC address is printed on the front of the SCALANCE
 If selection of a module or software configuration



Product type			
SCALANCE S			1111
SOFTNET configure (SOFTNET Security NCP VPN client, VPI	tion Client, SCALANCE M87x/M V device)	D74x.	
Module			
S602		S623	
S612		S627-2M	
© \$613			
Firmware release			
V4			
○ V3			
Configuration			
Name of the module:	Module1		
MAC address:	00-1B-1B-BB-99-DE		
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0
Interface routing externa	al/internal: Routing mode	•	



3. Creating a project and security module

- In the "Configuration" area, enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- From the drop-down list, select the "Routing Mode"
- Enter the internal IP address (192.168.9.1) and the internal subnet mask (255.255.255.0)
- Confirm with "OK"

Selection of a modul	e or software configuration			×
Product type SCALANCE S SOFTNET configur	ation	074.		ĺ
NCP VPN client, VP	N device)	D74X.		l
Module				Ľ.
© S602		S623		
S612		S627-2M		1
© S613				Ł
Firmware release				Ł
V4				1
○ V3				
Configuration				
Name of the module:	Module1			
MAC address:	00-1B-1B-BB-99-DE			
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0	
Interface routing extern	al/internal: Routing mode	•		
IP address (int.):	192,168,9,1	Subnet mask (int.):	255 255 255 0	

3. Creating a project and security module

- Select the security module created and select the "Edit" > "Properties" menu command, "Interfaces" tab
- Select the "Activate Interface" check box in the "DMZ port (X3)" area
- Enter the IP address (192.168.8.1) and the subnet mask (255.255.255.0) for the DMZ interface
- Confirm with "OK"

DMZ port (X3)		
IP assignment:	Static address	
IP address:	192.168.8.1	
Subnet mask:	255.255.255.0	
MAC address:	00-1B-1B-BB-99-E0	
Comment:		

4. Downloading the configuration to the security module

- Select the "Project" > "Save" menu command
- Select the security module in the content area
- Select the "Transfer" > "To module(s)..." menu command

B Download cont	iguration data to security module
Module name:	Module I
Address:	192.168.10.1
MAC address:	00-1B-1B-BB-99-DE
	✓ Log on as current user
Transfer type	
Modified files	only O All files
	Start     Cancel     Details >>     Close     Help

KUI

Start the download with the "Start" button

4. Downloading the configuration to the security module

- If the download was completed successfully, the Scalance is restarted automatically and the configuration activated
- The Scalance is now in productive operation
- Configurations can be download via all interfaces
- The configured IP addresses can be modified





In this example, the firewall will be configured to allow IP traffic to only be initiated by the internal network





1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface

2. Making IP settings for the PCs								
PC	IP address	Subnet mask						
PC1	192.168.10.2	255.255.255.0						
PC2	192.168.10.3	255.255.255.0						

• Set the IP addresses of the PCs as in the table above



3. Creating a project and security module

- Create a new project
- In the "Configuration" area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)

Belection of a module or software configuration		× )
Product type SCALANCE S SOFTNET configuration (SOFTNET Security Client, SCALANCE M87x/MD NCP VPN client, VPN device)	174x.	
Module S602 S612 S613	● S623 ● S627-2M	
Firmware release ● V4 ○ V3		
Configuration Name of the module: Module1 MAC address: 00-1B-1B-BB-99-DE		
IP address (ext.): 192.168.10.1 Interface routing external/internal: Bridge mode	Subnet mask (ext.):	255 255 255 0
IP address (int.):	Subnet mask (int.):	

KU

• Confirm with "OK"

4. Configuring the firewall

- Select the security module in the content area
- Select the "Edit" > "Properties..." menu command
- Select the "Firewall" tab in the displayed dialog
- Activate the settings shown in the picture Result: IP traffic is only initiated from the internal network
- Logging is selected to record data traffic
- Close with OK
- Save the project

Module properties - Module1									
terfaces Firewall Internet connection F	Routing Time synchroniz	ation VPN SNM	IP RADIUS						
Predefined firewall rules									
General Enable firewall Tunnel communication only									
Services									
	Internal => External	Extern => Intern	Internal => DMZ	DMZ => Intern					
Allow IP communication									
Allow S7 protocol									
Allow FTP/FTPS (explicit mode) Allow HTTP									
Allow HTTPS									
Allow DNS									
Allow SMTP									
Allow NTP									
Allow DHCP									
	nternal => External	External => Interna							
Allow MAC level communication									
Allow ISO communication									
Allow SiCLOCK									
Allow DCP									
IP log settings			MAC log settings						
Log tunneled packets			Log tunnele	d packets					
Log blocked incoming packets			Log blocked	l incoming packets					
Log blocked outgoing packets			Log blocked	l outgoing packets					

5. Downloading the configuration to the security module

• Transfer the configuration to the security module



6. Testing the firewall function (ping test/logging)

- Open the command prompt on PC2 "Start" > "All programs" >"Accessories" > "Command Prompt"
- Enter the ping command from PC2 to PC1 "ping 192.168.10.2"

```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=3ms TTL=64
Reply from 192.168.10.2: bytes=32 time=3ms TTL=64
Reply from 192.168.10.2: bytes=32 time=4ms TTL=64
Ping statistics for 192.168.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 4ms, Average = 3ms
C:\>
```

**KU LEUVEN** 

All packets reach PC1

6. Testing the firewall function (ping test/logging)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC2 "ping 192.168.10.3"

```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.10.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>■
```

**KU LEUVEN** 

All packets are blocked at Scalance

6. Testing the firewall function (ping test/logging)

- In the SCT change to online mode by selecting the menu option "View" > "Online"
   View Options Help
- Select "Edit" > "View Diagnostics"
- Select the "Packet filter log" tab

View		Options	Help		
	Ac	lvanced mo	Ctrl+E		
~	Sh	ow Details	window	Ctrl+Alt+D	
$\bigcirc$	Of	fline	Ctrl+Shift+D		
٢	Or	nline	Ctrl+D		
	Up	odate	F5		

**KU LEUV** 

6. Testing the firewall function (ping test/logging)

- Click the "Start reading" button
- Acknowledge with "OK"
- Log entries are read and displayed here

tatus   Date	and time of d	av Interface s	ettings   Dynami	ic DNS   System log	Audit log P	acket filter log	ARP tab	ole   Loga	ed in users Communications status
lo.	Date	Time of	Source	Destination	Protocol	Interface	Action	Directi	Additional information
* 1461	8/26/2015	1:44:06 PM	192 168 10 2	192,168,10,3	ICMP	Ext	Dropp	In	ICMP: Type = 8. Code = 0. Reason: Mat
* 1462	8/26/2015	1:44:11 PM	192,168,10,2	192,168,10,3	ICMP	Ext	Dropp	In	ICMP: Type = 8, Code = 0, Reason: Mat
× 1463	8/26/2015	1:44:16 PM	192.168.10.2	192.168.10.3	ICMP	Ext	Dropp	In	ICMP: Type = 8, Code = 0, Reason: Ma
* 1464	8/26/2015	1:44:21 PM	192.168.10.2	192.168.10.3	ICMP	Ext	Dropp	In	ICMP: Type = 8, Code = 0, Reason: Ma
				111					
Delete d	splay		Buffer settings:	Ring buffer			Open		Stop reading Stop logging



In this example, the firewall is configured to allow IP traffic from PC2 to PC1. The packets are forwarded to the outside with an IP address translated to the IP address of the security module and a dynamically assigned port number. Only replies to these packets can enter the internal network



1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface

#### 2. Making IP settings for the PCs

PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.9.2	255.255.255.0	192.168.9.1

• Set the IP addresses of the PCs as in the table above



#### 3. Creating a project and security module

- Create a new project
- In the "Configuration" area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the "Routing mode"
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with "OK"

Selection of a module	or software configuration		×					
Product type SCALANCE S SOFTNET configura (SOFTNET Security NCP VPN client, VPN	tion Client, SCALANCE M87x/ME V device)	)74x.						
Module								
© S602		<ul> <li>S623</li> <li>CC27 2M</li> </ul>						
© \$612		S627-2M						
Firmware release								
V4								
○ V3								
Configuration								
Name of the module:	Module1							
MAC address:	00-1B-1B-BB-99-DE							
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0					
Interface routing externa	al/internal: Routing mode	▼						
IP address (int.):	192.168.9.1	Subnet mask (int.):	255.255.255.0					

#### 4. Configuring the firewall

- Change the configuration view to advance mode with the menu command "View" > "Advanced Mode"
- Select the module in the content area

View		Options	Help		
	Ac	dvanced mo	Ctrl+E		
~	Sh	ow Details	/ Ctrl+Alt+D		
۲	Of	fline		Ctrl+Shift+D	
$\bigcirc$	Or	nline		Ctrl+D	

KUL

- Select the "Edit" > "Properties..." menu command
- Go to the "NAT/NAPT" tab

#### 4. Configuring the firewall

- Select the "Activate NAT" checkbox
- Click the "Add" button in the "NAT" input area
- Configure the NAT rule with the following parameters
  - Action: "Source NAT"
  - From: "Internal"
  - To: "External"
  - Source IP address: "\*"
  - Source translation: "192.168.10.1
- Confirm with "Apply"

Iodule properties -	Module1		NATAIADT T		< 1.000 DU0		100 01	211.10	
aces   Firewall   Inte	rnet connection	DNS   Rout	ing NAT/NAPT Tin	ne synchronization   Log	settings   VPN   DHC	P-Server   SNMP   Proxy	ARP   RA	DIUS	
rface information									
emal (X1): 192.168.1	). 1, Internal (X2): 1	192.168.9.1,	DMZ port (X3): disable	d					
т									
Activate NAT									
ction	From	То	Source IP addre	Source translation	Destination IP a	Destination translat	No.	Comment	
ource-NAT	Internal	External	*	192.168.10.1			NAT_1		

KUL

4. Configuring the firewall

- Select the "Firewall" tab
- Expand the firewall rule created by SCT with the following
   Destination IP address: 192.168.10.2
- Select the "Logging" check box

Í	Ð	Module	e properti	es - Module	e1			-	-	×			
1	In	terfaces	Firewall	Internet con	nection DNS	Routing	NAT/NAF	PT   Tir	me synchro	onization	Log settin	gs VPN	DHCP-Ser
IP rules [1] MAC rules (inactive) [0] Default rules for IP services													
		Action	From	То	Source IP addr	e D	estination I	P a	Servi	Bandwi	dth (M	Loggi	No.
		Allow	Internal	External		19	92.168.10.2	2	(all)			$\checkmark$	NAT_1

**KU LEUVEN** 

Confirm with "OK"
5. Downloading the configuration to the security module

• Transfer the configuration to the security module



6. Testing the firewall function (ping test/logging)

**KU LEUVEN** 

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC1 "ping 192.168.10.2"

C:\Windows\system32\cmd.exe

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data: Reply from 192.168.10.2: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.10.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>

All packets reach PC1

6. Testing the firewall function (ping test/logging)

- Change to online mode in the SCT with the "View" > "Online" menu command
- Select the module in the content area and the menu command "Edit" > "Online diagnostics"
- Go to the "Packet filter log" tab

6. Testing the firewall function (ping test/logging)

- Click "Start reading..."
- Confirm the dialog with "OK"

Online vi	iew [Module1]	l							
Status Dat	te and time of d	av Interface s	ettings Dynamic DI	NS System log A	Audit log F	Packet filter log	ARP tab	le Loga	ed in users Communications status IP blacklist
No.	Date	Time of	Source	Destination	Protocol	Interface	Action	Directi	Additional information
-2-88	8/28/2015	9:25:34 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
289	8/28/2015	9:25:35 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
-22-90	8/28/2015	9:25:35 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
-2-91	8/28/2015	9:25:36 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
292	8/28/2015	9:25:45 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	ln.	Prot ID = 0x2
-2-93	8/28/2015	9:25:45 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
294	8/28/2015	9:25:45 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	ln.	Prot ID = 0x2
-2-95	8/28/2015	9:25:45 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
-22.96	8/28/2015	9:25:45 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
297	8/28/2015	9:25:47 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
-2-98	8/28/2015	9:25:47 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	ln	Prot ID = 0x2
299	8/28/2015	9:25:47 AM	192 168 9 2	224 0 0 22	IGMP	Int	Passed	In	Prot ID = 0x2
2 100	8/28/2015	9:25:49 AM	192 168 9 2	192 168 10 2	ICMP	Fxt	Passed	Out	ICMP <sup>-</sup> Type = 8 Code = 0 Reason <sup>-</sup> Match Rule num
2 101	8/28/2015	9:25:49 AM	192,168,10,2	192,168,9,2	ICMP	Ext	Passed	In	ICMP: Type = 0. Code = 0. Reason: Match. Rule num
2 102	8/28/2015	9:25:50 AM	192 168 10 1	192 168 10 2	ICMP	Ext	Passed	Out	ICMP: Type = 8 Code = 0 Reason: Match Rule num
2 103	8/28/2015	9:25:50 AM	192 168 10 2	192 168 9 2	ICMP	Ext	Passed	In	ICMP: Type = 0 Code = 0 Reason: Match, Pale num
-2 104	8/28/2015	9:25:51 AM	192 168 10 1	192 168 10 2	ICMP	Ext	Passed	Out	ICMP: Type = 8 Code = 0 Reason: Match Rule num
×2 105	8/28/2015	9:25:51 AM	192 168 10 2	192 168 9 2	ICMP	Ext	Passed	In	ICMP: Type = 0 Code = 0 Reason: Match Bule num
× 106	8/28/2015	9:25:52 AM	192 168 10 1	192 168 10 2	ICMP	Ext	Passed	Out	ICMP: Type = 8 Code = 0 Reason: Match Rule num
2 107	8/28/2015	9:25:52 AM	192 168 10 2	192 168 9 2	ICMP	Ext	Passed	In	ICMP: Type = 0 Code = 0 Reason: Match, Pale num
•				III					4
Delete	display		Buffer settings:	Ring buffer				Open	Starting reading Stop logging
ady									Close Help

#### **KU LEUVEN**



In this example, only a specific user is allowed to access PC2 in the internal network from PC1 in the external network. For other users, access is blocked

**KU LEUVEN** 



1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface

#### 2. Making IP settings for the PCs

PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.9.2	255.255.255.0	192.168.9.1

**KU LEUVEN** 

• Set the IP addresses of the PCs as in the table above

#### 3. Creating a project and security module

- Create a new project
- In the "Configuration" area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the "Routing mode"
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with "OK"

Selection of a module	e or software configuration		X
Product type SCALANCE S SOFTNET configure (SOFTNET Security NCP VPN client, VPI	stion Client, SCALANCE M87x/ME N device)	)74x.	
Module			
S602		S623	
© S612		S627-2M	
© \$613			
Firmware release			
V4			
© V3			
Configuration			
Name of the module:	Module1		
MAC address:	00-1B-1B-BB-99-DE		
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0
Interface routing extern	al/internal: Routing mode	•	
IP address (int.):	192.168.9.1	Subnet mask (int.):	255.255.255.0

**KU LEUVEN** 

4. Creating remote access users

- Select the "Options" > "User management..." menu command
- Click the "Add..." button in the "User" tab
- Create a new user with the settings in the figure
- Confirm with "OK"

Create new user								
User data								
User name:	Remote							
Authentication method:	Password							
Password:	Very weak							
Repeat password:								
Comment:								
Settings for user-specific IP rule sets Maximum time of the session: 30 🚔 Minutes								
Role Assigned role: remote access								
	OK Cancel Help							

5. Setting and assigning a user-specific IP rule set

- Change the configuration to advanced mode via "View" > "Advanced Mode"
- Select the "User-specific IP rule sets" object in the navigation panel
- Select the "Add rule set..." entry in the shortcut menu



5. Setting and assigning a user-specific IP rule set

• Enter a rule in the dialog as shown below

		Name:	User-spec. IP rul	le set1							
	D	escription:	Description Use	r-spec. IP rule set1							
les N	AT NAP	т									
ction	From	То	Source IP ad	Destination I	Servi	Bandwidth (M	Loggi	No.	Comment		
llow	External	Internal		192.168.9.2	(all)		~	U_1.1			
					Add	rule D	elete rule	:	÷ +	IP services	
		Ava	ilable users and role	es:				Assig	ned users and role	s:	
		ad ad	min (User) ministrator (Role)					Ren	note (User)		
		ad dia	ministrator(radius) gnostics (Role)	(Role)							
		rad	lius (Role) note access (Role	)			Assign				
		sta	ndard (Role)				Remove				

- From the "Available users and roles" list, select the "Remote (user)" entry and click the "Assign" button
- Confirm with "OK"

5. Setting and assigning a user-specific IP rule set

- Select the security module in the navigation panel and drag it to the newly created user-specific IP rule set
- The assignment can be checked by opening the module properties and selecting the "Firewall" tab



#### 5. Setting and assigning a user-specific IP rule set

ces i es [1]	MAC rule	Internet con es (inactive)	101 Default rules for	uting   NA I/NAP I   Tir r IP services	me synchro	onization   Log settin	gs   VPN	DHCP-S	Server   SNMP   Proxy ARP   RAUIUS
on	From	То	Source IP addre	. Destination IP a	Servi	Bandwidth (M	Loggi	No.	Comment
-spe	c. IP rule	set1 (Assi	gned users: Remo	te; assigned roles:)					
			Add rule	Delete rule	•	↓ IPs	ervices		Expand rule sets Collapse rule sets Add rule sets

EUVEN

5. Setting and assigning a user-specific IP rule set

• "Expand rule set" shows the user-specific rule in detail

ıles (1	] MAC rule	es (inactive	) [0] Default rules for	IP services	ine synch	Tomzauon   Log setu	iiga vi iv	Dirici a		
tion	From	То	Source IP addre	Destination IP a	Servi	Bandwidth (M	Loggi	No.	Comment	
ow	External	Internal		192.168.9.2	(all)	······	1	U_1.1		
					•					
			Add rule	Delete rule	7	IP s	services		Expand rule sets Add rule sets	
										-11

6. Downloading the configuration to the security module

• Transfer the configuration to the security module



7. Logging in on the Web page

 In the Web browser of PC1, enter the address "https://192.168.10.1"

SIEMENS		English 💌 <u>Go</u>
	SCALANCE S	-
	Welcome to the SCALANCE S user-specific firewall	
	Please log on:	
	Name	
	Log in	



7. Logging in on the Web page

• If the web page does not show the login fields, try changing the language in the upper right corner

SIEMENS		English 💌 Go
	SCALANCE S	2



7. Logging in on the Web page

 Enter the user name "Remote" and corresponding password and click the "Log in" button

SIEMENS	English 💌 Go
	SCALANCE S
	Welcome to the SCALANCE S user-specific firewall
	Please log on:
	Name Remote
	Log in



7. Logging in on the Web page

• The defined IP rule set is enabled for the "Remote" user.

SIEMENS	3	English 💌 <u>Go</u>
	SCALANCE S	-
	Welcome, <i>Remot</i> e	
	You have logged in successfully from address 192.168.10.2	
	Your session expires in 29 Minutes 49 Seconds	
	Extend timeout	
	Log out	



8. Testing the firewall function (ping test)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC2 "ping 192.168.9.2"

```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.9.2
Pinging 192.168.9.2 with 32 bytes of data:
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Ping statistics for 192.168.9.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>=
```

**KU LEUVEN** 

• All packets reach PC2



In this example, a RADIUS server is set up to manage user accounts. Only users that can authenticate to the RADIUS server can access the internal network from the external network

**KU LEUVEN** 



1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface
- Connect the Linux PC that will be used as RADIUS server to the DMZ interface



2. Making	<b>IP</b> settings	for the PCs
-----------	--------------------	-------------

PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.9.2	255.255.255.0	192.168.9.1
RADIUS	192.168.8.2	255.255.255.0	192.168.8.1

- Set the IP addresses of the PCs as in the table above
- The IP address of the Linux PC is preset to the correct value



#### 3. Creating a project and security module

- Create a new project
- In the "Configuration" area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the "Routing mode"
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with "OK"

3 Selection of a module or software configuration					
Product type SCALANCE S SOFTNET configuration (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)					
Module					
S602		S623			
© S612		S627-2M			
© \$613					
Firmware release	Firmware release				
V4					
© V3					
Configuration					
Name of the module:	Module1				
MAC address:	00-1B-1B-BB-99-DE				
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0		
Interface routing externa	l/internal: Routing mode	•			
IP address (int.):	192.168.9.1	Subnet mask (int.):	255.255.255.0		

**KU LEUVEN** 

3. Creating a project and security module

- Select the security module created and select the "Edit" > "Properties" menu command, "Interfaces" tab
- Select the "Activate Interface" check box in the "DMZ port (X3)" area
- Enter the IP address (192.168.8.1) and the subnet mask (255.255.255.0) for the DMZ interface
- Confirm with "OK"

DMZ port (X3) Activate interface		
IP assignment:	Static address	
IP address:	192.168.8.1	
Subnet mask:	255.255.255.0	
MAC address:	00-1B-1B-BB-99-E0	
Comment:		

4. Setting up the RADIUS server

- On the Linux PC open the Web browser and go to "http://freeradius.org/download.html"
- Download version 3.0.9 of the RADIUS server
   Downloads

3.0.x Series - Stable

Version 3.0.9: tar.gz (PGP Signature) Version 3.0.9: tar.bz2 (PGP Signature)

 Open the Terminal Open the Dash and type "terminal"



4. Setting up the RADIUS server

- Go to the "Downloads" map ("cd Downloads")
   vincent@vincent-VirtualBox:~\$ cd Downloads
   vincent@vincent-VirtualBox:~/Downloads\$
- Unpack the RADIUS server ("tar zxvf freeradius-server-3.0.9.tar.gz")
- Enter the newly made map ("cd freeradius-server-3.0.9")

4. Setting up the RADIUS server

- Install the server with the following commands "./configure"
  - "make"
  - "sudo make install"

vincent@vincent-VirtualBox:~/Downloads/freeradius-server-3.0.9\$ sudo make instal

[sudo] password for vincent:

The password is **TBD** 

**KU LEUVEN** 

4. Setting up the RADIUS server

- The next step is to configure the clients of the server
- Open the file explorer with "gksudo nautilus"
   Enter the sudo password in the following prompt
   Enter your password to perform administrative tasks
   The application 'nautilus' lets you modify essential parts of your system.
- Using Nautilus browse to "Computer"
   "usr" > "local" > "etc" > "raddb"



Password:

Cancel

OK

4. Setting up the RADIUS server

- Open "clients.conf" and add a new client as in the image #Scalance client for demo client Scalance { ipaddr = 192.168.8.1 secret = SiemensSecret
- Save and close the window
- Open "users" and add the following users

radius Cleartext-Password := "password"
radius2 Cleartext-Password := "password2"

Save and close the window



4. Setting up the RADIUS server

- With the server installed and configured, run "sudo radiusd
  - -X" to start the server in debug mode

Refusing to start with libssl version OpenSSL 1.0.1f 6 Jan 2014 0x1000106f (1.0. 1f release) (in range 1.0.1 dev - 1.0.1f release) Security advisory CVE-2014-0160 (Heartbleed) For more information see http://heartbleed.com Once you have verified libssl has been correctly patched, set security.allow\_vul nerable\_openssl = 'CVE-2014-0160'

- If this error shows up, check the OpenSSL version with "openssl version –a" This command should show the following date:
  - 'built on: Thu Jun 11'

vincent@vincent-VirtualBox:~\$ openssl version -a OpenSSL 1.0.1f 6 Jan 2014 built on: Thu Jun 11 15:28:12 UTC 2015



4. Setting up the RADIUS server

- If this date is not shown update the library with the following command "sudo apt-get update"
   "sudo apt-get upgrade"
- If OpenSSL is correctly updated, open "radius.conf" and change the "allow\_vulnerable\_openssl" parameter to yes

allow\_vulnerable\_openssl = no allow\_vulnerable\_openssl = yes

KU L

- Save and close the window
- Try starting the server again with "sudo radiusd -X"

5. Configuring the firewall

- Enter "Advanced mode" in the Security Configuration Tool
- Use the menu command "Options" > "User Management"
- Create a new user with the following settings
- Confirm with "OK"

🖁 Edit users	X		
User data			
User name:	radius		
Authentication method:	RADIUS		
Password:			
Repeat password:			
Comment:			
Settings for user-specific IP rule sets Maximum time of the session: 30 💭 Minutes			
Role			
Assigned role:	radius 🔻		
	OK Cancel Help		



5. Configuring the firewall

- Select the "User-specific IP rule sets" in the navigation window
- Select the "Add rule set..." option in the shortcut menu



**KU LEUVEN**
5. Configuring the firewall

• Enter a rule in the dialog as shown below

3	Firewall us	er-specific	IP rule se	tUser-spec. IP ru	le set1							
			Name:	User-spec. IP rul	e set1							
		D	escription:	Description Use	r-spec. IP rule set1							
	IP rules N	AT NAP	г									
	Action	From	То	Source IP ad	Destination I	Servi	Bandwidth (M	Loggi	No.	Comment		
	Allow	External	Internal		192.168.9.2	(all)		$\checkmark$	U_1.1			
	-											
						Add	rule De	elete rule	1	t t	IP services	



5. Configuring the firewall

 From the "Available users and roles" list, select the "radius (user)" entry and click the "Assign" button, then select the "radius (role)" entry and click "Assign"

Available users and roles:	1	Assigned users and roles:
admin (User) administrator (Role) administrator(radius) (Role) diagnostics (Role) remote access (Role) standard (Role)	Assign Remove	radius (Role) radius (User)

KUL

Confirm with "OK"

5. Configuring the firewall

- Select the security module in the navigation panel and drag it to the newly created user-specific IP rule set
- The assignment can be checked by opening the module properties and selecting the "Firewall" tab



### 6. Linking the RADIUS server and security module

- Select the menu option "Options" > "Configuration of the RADIUS server..."
- Click the "Add…" button in the dialog

Name	IP address / FQDN	Port ID	Comment

Op	otions	Help					
	IP services						
	MAC services						
	Netw	ork adapter					
	Language						
	Log files						
Symbo		olic names					
	Confi	guration of the NTP server					
	Confi	guration of the RADIUS server					
	Consi	stency checks					
User management		management					
	Certif	ïcate manager					

**KU LEUVEN** 

6. Linking the RADIUS server and security module

- Define the server with the following values
  - IP address/FQDN: 192.186.8.2
  - Shared secret: SiemensSecret
  - Repeat shared secret: SiemensSecret
- Confirm with "OK"

Definition of a RADIU	S server					
Name:	RADIUS server					
IP address / FQDN:	192.168.8.2					
Port:	1812					
Shared secret:	•••••		]			
Repeat shared secret:	•••••		]			
Authentication method:	PAP					
Comment:						
				Caraal	lala 🗌	
		0	ĸ	Cancel	тегр	
						1

6. Linking the RADIUS server and security module

 Open the SCALANCE S module properties and go to the "RADIUS" tab



- Check the "Enable RADIUS authentication" box
- Click the "Add" button This adds the newly configured RADIUS server

DADU

RADIUS	ADIUS server							
No.	Name	IP address	Comment					
1	RADIUS server	192.168.8.2						



6. Linking the RADIUS server and security module

 In the "RADIUS setting" area, check the "Allow RADIUS authentication of non-configured users" box

RADIUS settings					
RADIUS timeout:	1	Seconds			
RADIUS retries:	5				
Allow RADIUS authentication of non-configured users					
Filter ID is required for authentication					

Confirm with "OK"



7. Downloading the configuration to the security module

• Transfer the configuration to the SCALANCE S module



8. Logging in on the Web page

 In the Web browser of PC1, enter the address "https://192.168.10.1"

SIEMENS		English 💌 Go
	SCALANCE S	-
	Welcome to the SCALANCE S user-specific firewall	
	Please log on:	
	Name	



8. Logging in on the Web page

• If the web page does not show the login fields, try changing the language in the upper right corner

5



8. Logging in on the Web page

• Enter the user name "radius" and corresponding password and click the "Log in" button

SIEMENS		sh 💌 <u>Go</u>
	SCALANCE S	5
	Welcome to the SCALANCE S user-specific firewall	
	Please log on:	
	Name radius Password	
	Log in	



8. Logging in on the Web page

• The defined IP rule set is enabled for the "radius" user.

SIEMENS		English 💌 <u>G</u> i	2
	SCALANCE S		
	Welcome, radius You have logged in successfully from address 192.168.10.2 Your session expires in 30 Minutes Extend timeout Log out		



8. Logging in on the Web page

- Now click the "Log out" button
- Enter the user name "radius2" and corresponding password and click the "Log in" button

ENS	English
SCALANCE S	
Welcome to the SCALANCE S user-specific firewall	
Please log on:	
Name radius2	
Password	
Log in	

8. Logging in on the Web page

• The defined IP rule set for the "radius" role is enabled

→ Users that are not defined on the module can log in

SIEMENS	English 🔽 Ga
	SCALANCE S
	Use Section S

9. Testing the firewall function (ping test)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC2 "ping 192.168.9.2"

```
C:\Windows\system32\cmd.exe
C:\>ping 192.168.9.2
Pinging 192.168.9.2 with 32 bytes of data:
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Reply from 192.168.9.2: bytes=32 time=2ms TTL=63
Ping statistics for 192.168.9.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>=
```

**KU LEUVEN** 

• All packets reach PC2



In this example, a VPN tunnel is configured between a security module and the SOFTNET Security Client With this configuration, IP traffic is possible only over the established VPN tunnel connection between the two authorized partners



1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the switch to the external network interface
- Connect the PC with the Security Configuration Tool (PC1) and the PC with the SOFTNET Security Client (PC2) to the switch
- Connect PC3 to the internal network interface



### 2. Making IP settings for the PCs

PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.10.3	255.255.255.0	192.168.10.1
PC3	192.168.9.2	255.255.255.0	192.168.9.1

• Set the IP addresses of the PCs as in the table above



#### 3. Creating a project and security module

- Create a new project
- In the "Configuration" area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the "Routing mode"
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with "OK"

Selection of a module or software configuration					
Product type SCALANCE S SOFTNET configure (SOFTNET Security NCP VPN client, VP	ation Client, SCALANCE M87x/MI N device)	074x.			
Module S602 S612 S613		● S623 ● S627-2M			
Firmware release V4 V3			1.		
Configuration Name of the module: MAC address:	Module1 00-1B-1B-BB-99-DE				
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0		
IP address (int.):	192.168.9.1	Subnet mask (int.):	255.255.255.0		

**KU LEUVEN** 

3. Creating a project and security module

- Use the "Insert" > "Module" menu command with the following parameters
  - Product type: SOFTNET configuration
  - Module: SOFTNET Security Client
  - Firmware release: V4
- Confirm with "OK"

Product type  SCALANCE S			
SOFTNET configur (SOFTNET Security NCP VPN client, VP	ation / Client, SCALANCE M87 N device)	x/MD74x,	
Odule	Client	VPN device	
SCALANCE M87x/N	1D74x	<u> </u>	
NCP VPN client for	Android		
Firmware release		@ 2005	
○ V3		0 2003	I
2008			Children .
Configuration			
Name of the module:	Module?		
MAC address:	00-1B-1B-00-00-00		
IP address (ext.):	192.168.10.2	Subnet mask (ext.):	255.255.255.0
Interface routing extern	al/internal:	•	
10 11 6 13		Cubrat mark (int )	

4. Configuring a VPN group

- Select "VPN groups" in the navigation
- Select the "Insert" > "Group" menu command
- In the navigation panel, click the "All modules" entry
- Drag the Scalance S Module to the VPN group "Group1" in the navigation panel The module is now assigned to the VPN group The color of the key symbol changes to blue



4. Configuring a VPN group

 Drag the SOFTNET Security Client module to the VPN group "Group1" in the navigation panel The module is now assigned to the VPN group The color of the key symbol changes to blue



**KU LEUV** 

Activate "Advanced Mode"

4. Configuring a VPN group

- Select the VPN group "Group1" in the Navigation windows and select the menu command "Edit" > "Properties"
- Select the "Preshared key" option in the "Authentication method" area

VPN group properties - Group1				
Authentication method				
Preshared key	Certifica	te		
Key: M5aZ6dImUOz5B4J9	Name:	PEA46-G9A54		
New	Date issued:	9/1/2015 1:05 PM		
			New Display	

KUL

Confirm with "OK"

5. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the project
- Use the menu command "Transfer" > "To all modules..."

Module name	Project status	Downloading status	
Module2 (SSC)	ОК	Loaded	
Module1 (SCALANCE S)	ОК	Loaded	
Log on as current user			Select all
Show only modified modules			Deselect all
Current module:			
Transfer type			
Transfer type Modified files only	All files		

**KU LEUVEN** 

Start the download with the "Start" button

5. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the configuration file "projectname.Module2.dat" in your project folder
- Confirm the popup with "OK"



6. Setting up a tunnel with the SOFTNET Security Client

• Open the SOFTNET Security Client on PC2

SOFTNET Security Client						
File Options Help						
Communication options						
Load Configuration	Tunnel Overview	Enable				
Minimize	Exit	Help About				

**KU LEUVEN** 

- Select "Load Configuration" and browse to where "projectname.Module2.dat" has been saved
- Open the configuration with the "Open" button

6. Setting up a tunnel with the SOFTNET Security Client

 Loading a new configuration will delete any previous configurations

SOFTNET Security Client - Configuration Data Already Exists	X
Configuration data already exist for the SOFTNET Security Client. Should the stored configuration data be	
deleted	
C kept and merged with the new one, whereas modules with identical IP addresses shall	lbe
imported and replaced	
◯ not imported	
Next	Cancel

 When the dialog above pops up, select "deleted" and confirm with "Next"

**KU LEUV** 

6. Setting up a tunnel with the SOFTNET Security Client

 The VPN tunnel can now be opened by clicking the "Enable" button

SOFTNET Security Client		
File Options Help		
Communication options		
Load Configuration	Tunnel Overview	Enable
Minimize	Exit	Help About



6. Setting up a tunnel with the SOFTNET Security Client

"Tunnel Overview" shows the status of the tunnel

unnel l	List:				
Stat	Name	Member IP / Subnet	Tunnel Endpoint IP	Tunnel over	
•	"Module1" Subset of "Medule1"	SCALANCE S623	192.168.10.1	192.168.10.2	
			102.100.10.1		
				enable active learning	Delete
ogging Det 27 Det 27 Det 27 Det 27	g Console: 2 2015 - 09:30:48] [QuickMode] 2 2015 - 09:30:49] [QuickMode] 2 2015 - 09:30:52] [QuickMode] 2 2015 - 09:30:52] [QuickMode]	Deleted Security Association From 1 Deleted Security Association From 1 Added Security Association From 19 Added Security Association From 19	92.168.10.2 To 192.168.10.1/3 92.168.10.2 To 192.168.90/24 12.168.10.2 To 192.168.90/24 2.168.10.2 To 192.168.10.1/32	32 4 2	

**KU LEUVEN** 

The green circle shows that the tunnel has been established

6. Setting up a tunnel with the SOFTNET Security Client

- If the tunnel does not get set up, check whether the Windows Firewall has been enabled
- Open the <u>"Control</u> Panel" > "Windows Firewall"

Control Panel Home	Help protect your computer with Windows Firewall			
Allow a program or feature through Windows Firewall	Windows Firewall can help prevent hackers or n through the Internet or a network.	nalicious software from gaining access to your computer		
😌 Change notification settings	How does a firewall help protect my computer?	2		
Turn Windows Firewall on or off	What are network locations?			
😽 Restore defaults	🛛 🥑 Home or work (private) netw	vorks Connected 🔿		
Advanced settings Troubleshoot my network	Networks at home or work where you know an	d trust the people and devices on the network		
nouslessioot my network	Windows Firewall state:	On		
	Incoming connections:	Block all connections to programs that are not on the list of allowed programs		
	Active home or work (private) networks:	🕪 hubkaho.be		
	Notification state:	Notify me when Windows Firewall blocks a new program		
	Public networks	Not Connected 💌		

 If the firewall is not enabled, click "Turn Windows Firewall on or off" and enable it

**KU LEUVEN** 

6. Setting up a tunnel with the SOFTNET Security Client

 In the Logging Console, the sequence of executed connection attempts is displayed



• The SCALANCE S module and the SOFTNET Security Client have established a communication tunnel

**KU LEU** 

7. Test the tunnel function

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC3 "ping 192.168.9.2"

C:\Vindows\system32\cmd.exe C:\>ping 192.168.9.2 Pinging 192.168.9.2 with 32 bytes of data: Reply from 192.168.9.2: bytes=32 time=4ms TTL=63 Ping statistics for 192.168.9.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 3ms, Maximum = 4ms, Average = 3ms C:\>

**KU LEUVEN** 

All packets reach PC3 through the tunnel

7. Test the tunnel function

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC3 "ping 192.168.9.2"



 The packets cannot reach PC3 since there is no tunnel communication between these two devices

**KU LEUVEN** 

# **VPN with Certificates**



**KU LEUVEN** 

In this example, a VPN tunnel is configured between a security module and the SOFTNET Security Client The endpoints authenticate using certificates

# **VPN with Certificates**


1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the switch to the external network interface
- Connect the PC with the Security Configuration Tool (PC1) and the PC with the SOFTNET Security Client (PC2) to the switch
- Connect PC3 to the internal network interface



#### 2. Making IP settings for the PCs

PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.10.3	255.255.255.0	192.168.10.1
PC3	192.168.9.2	255.255.255.0	192.168.9.1

• Set the IP addresses of the PCs as in the table above



#### 3. Creating a project and security module

- Create a new project
- In the "Configuration" area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the "Routing mode"
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with "OK"

Selection of a module	or software configuration		×
Product type SCALANCE S SOFTNET configura (SOFTNET Security NCP VPN client, VPN	tion Client, SCALANCE M87x/ME I device)	)74x.	
Module S602 S612 S613		● S623 ● S627-2M	
Firmware release V4 V3			
Configuration Name of the module: MAC address:	Module1 00-1B-1B-BB-99-DE		
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0
Interface routing externa	I/internal: Routing mode	▼ Subnet mask (int.):	255 255 255.0

3. Creating a project and security module

- Use the "Insert" > "Module" menu command with the following parameters
  - Product type: SOFTNET configuration
  - Module: SOFTNET Security Client
  - Firmware release: V4
- Confirm with "OK"

SCALANCE S			
SOFTNET configur (SOFTNET Security NCP VPN client, VP	ation / Client, SCALANCE M87 N device)	x/MD74x,	
Module SOFTNET Security SCALANCE M87x/N NCP VPN client for /	Client ID74x Android	VPN device	
Firmware release ● V4 ● V3 ● 2008		© 2005	
Configuration			
Name of the module:	Module?		
MAC address:	00-1B-1B-00-00-00		
IP address (ext.):	192.168.10.2	Subnet mask (ext.):	255.255.255.0
Interface routing extern	al/internal:	•	



- Select "VPN groups" in the navigation
- Select the "Insert" > "Group" menu command
- In the navigation panel, click the "All modules" entry
- Drag the Scalance S Module to the VPN group "Group1" in the navigation panel The module is now assigned to the VPN group The color of the key symbol changes to blue



#### 4. Configuring a VPN group

 Drag the SOFTNET Security Client module to the VPN group "Group1" in the navigation panel The module is now assigned to the VPN group The color of the key symbol changes to blue



**KU LEUVEN** 

Activate "Advanced Mode"

4. Configuring a VPN group

- Select the VPN group "Group1" in the Navigation windows and select the menu command "Edit" > "Properties"
- Select the "Certificate" option in the "Authentication method" area

🛐 VPN	group properties - Gro	up1				
Authen	tication method					
© Pr	eshared key		Oertifica	te		
Key:	cQ35ZIpbWIW5KxHt		Name:	PEA46-G9A54		
		New	Date issued:	9/2/2015 11:09 AM		
					New Display	

**KU LEUV** 

Confirm with "OK"

5. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the project
- Use the menu command "Transfer" > "To all modules..."

👔 Download configuration data	to security modules		
Module name	Downloading status		
Module2 (SSC)	ОК	Loaded	
Module1 (SCALANCE S)	ок	Loaded	
			Coloria all
Log on as current user			Select all
Show only modified modules			Deselect all
Current module:			
Transfer type			
Modified files only	All files		
Start	Cancel	Details >>	Close Help

**KU LEUVEN** 

Start the download with the "Start" button

5. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the configuration file "projectname.Module2.dat" in your project folder
- Assign a password to the certificate
- Confirm the popup with "OK"



6. Setting up a tunnel with the SOFTNET Security Client

• Open the SOFTNET Security Client on PC2

SOFTNET Security Client			
File Options Help			
Communication options			
Load Configuration	Tunnel Overview	Enable	
Minimize	Exit	Help About	

- Select "Load Configuration" and browse to where "projectname.Module2.dat" has been saved
- Open the configuration with the "Open" button

6. Setting up a tunnel with the SOFTNET Security Client

 Loading a new configuration will delete any previous configurations

SOFTNET Security Client - Configuration Data Already Exists	X
Configuration data already exist for the SOFTNET Security Client. Should the stored configuration data be	
deleted	
kept and merged with the new one, whereas modules with identical IP addresses shall	be
imported and replaced	
○ not imported	
Next	Cancel

 When the dialog above pops up, select "deleted" and confirm with "Next"

6. Setting up a tunnel with the SOFTNET Security Client

 The VPN tunnel can now be opened by clicking the "Enable" button

SOFTNET Security Client		
File Options Help		
Communication options —		
Load Configuration	Tunnel Overview	Enable
Minimize	Exit	elp About

**KU LEUVEN** 

• Enter the certificate password in the dialog

6. Setting up a tunnel with the SOFTNET Security Client

"Tunnel Overview" shows the status of the tunnel

unnell	ist				
Stat	Name	Member IP / Subnet	Tunnel Endonint IP	Tunnel over	
	"Module1" Subnet of: "Module1"	SCALANCE S623 192.168.9.0/255.255.255.0	192.168.10.1 192.168.10.1	192.168.10.2 192.168.10.2	
			Г	enable active learning	Delete
ogging Det 27 Det 27 Det 27 Det 27	g Console: 2 (2015 - 09 30-46) [OuickMode] 2 (215 - 09 30-49) [OuickMode] 2 (215 - 09 30-52) [OuickMode] 2 (215 - 09 30 52) [OuickMode] 2 (215 - 09 30 52) [OuickMode]	Deleted Security Association From 1 Deleted Security Association From 1 Added Security Association From 15 Added Security Association From 15	92.168.10.2 To 192.168.10.1/ 92.168.10.2 To 192.168.90/24 2.168.10.2 To 192.168.90/24 2.168.10.2 To 192.168.90/24 2.168.10.2 To 192.168.10.1/32	32 4 2	
					Þ
					Clear

**KU LEUVEN** 

 The green circle shows that the tunnel has been established

6. Setting up a tunnel with the SOFTNET Security Client

- If the tunnel does not get set up, check whether the Windows Firewall has been enabled
- Open the <u>"Control</u> Panel" > "Windows Firewall"

Control Panel Home	Help protect your computer with Windows Firewall				
Allow a program or feature through Windows Firewall	Windows Firewall can help prevent hackers or n through the Internet or a network.	nalicious software from gaining access to your computer			
😽 Change notification settings	How does a firewall help protect my computer?	2			
Turn Windows Firewall on or off	What are network locations?				
😽 Restore defaults	Home or work (private) netw	vorks Connected 🔿			
Advanced settings Troubleshoot my network	Networks at home or work where you know an	d trust the people and devices on the network			
	Windows Firewall state:	On			
	Incoming connections:	Block all connections to programs that are not on the list of allowed programs			
	Active home or work (private) networks:	🕪 hubkaho.be			
	Notification state:	Notify me when Windows Firewall blocks a new program			
	Public networks	Not Connected 😒			

 If the firewall is not enabled, click "Turn Windows Firewall on or off" and enable it

6. Setting up a tunnel with the SOFTNET Security Client

 In the Logging Console, the sequence of executed connection attempts is displayed



• The SCALANCE S module and the SOFTNET Security Client have established a communication tunnel

**KU LEU** 

7. Test the tunnel function

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC3 "ping 192.168.9.2"

C:\Vindows\system32\cmd.exe C:\>ping 192.168.9.2 Pinging 192.168.9.2 with 32 bytes of data: Reply from 192.168.9.2: bytes=32 time=4ms TTL=63 Ping statistics for 192.168.9.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 3ms, Maximum = 4ms, Average = 3ms C:\>

**KU LEUVEN** 

All packets reach PC3 through the tunnel

7. Test the tunnel function

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC3 "ping 192.168.9.2"



 The packets cannot reach PC3 since there is no tunnel communication between these two devices



In this example, a VPN tunnel is set up between two security modules

**KU LEUVEN** 

With this configuration, IP traffic is possible only over the established tunnel connections with authorized partners



**KU LEUV** 

1. Setting up the network

- Connect the PC with the Security Configuration Tool (PC1) to the switch
- Connect both SCALANCE S modules to the switch through their external interface
- Connect PC2 and PC3 to the internal interface of a SCALANCE S module



2. Making IP settings for the PCs

PC	IP address	Subnet mask
PC1	192.168.10.2	255.255.0.0
PC2	192.168.10.3	255.255.0.0
PC3	192.168.10.4	255.255.0.0

• Set the IP addresses of the PCs as in the table above



3. Creating a project and security module

- Create a new project
- In the "Configuration" area enter the MAC address
- Enter the external IP address (192.168.10.201) and the external subnet mask (255.255.0.0)
- Confirm with "OK"

Selection of a module	or software configuration			X
Product type SCALANCE S SOFTNET configural (SOFTNET Security NCP VPN client, VPN	tion Client, SCALANCE M87x/ME I device)	074x.		
Module				
S602		S623		
S612		S627-2M	1	
© S613				
Firmware release				
V4				
○ V3			44 12 12 14 14 14 14 14 14 14 14 14 14 14 14 14	
Configuration				
Name of the module:	Module1			
MAC address:	00-1B-1B-BB-99-DE			
IP address (ext.):	192.168.10.201	Subnet mask (ext.):	255.255.0.0	
Interface routing externa	l/internal: Bridge mode	-		
IP address (int.):		Subnet mask (int.):		

3. Creating a project and security module

- Select the menu command "Insert" > "Module"
- Select the same options as for the previous module but with the following address parameters
  - MAC address: MAC address of the module
  - IP address (ext): 192.186.10.202
  - Subnet mask (ext): 255.255.0.0
- Confirm with "OK"

#### 4. Configuring a VPN group

- Select "VPN groups" in the navigation
- Select the "Insert" > "Group" menu command
- In the navigation panel, click the "All modules" entry
- Drag the SCALANCE S Module to the VPN group "Group1" in the navigation panel The module is now assigned to the VPN group The color of the key symbol changes to blue



4. Configuring a VPN group

 Drag the second SCALANCE S module to the VPN group "Group1" in the navigation panel The module is now assigned to the VPN group The color of the key symbol changes to blue





5. Downloading the configuration to the security module

- Save the project
- Use the menu command "Transfer" > "To all modules..."

🛐 Download configuration data to	security modules			X
Module name Module1 (SCALANCE S) Module2 (SCALANCE S)	Project status Modified Modified	Downloading status Not loaded Not loaded		
Log on as current user     Show only modified modules     Current module:			Select all Deselect all	
Transfer type Modified files only Start Skip	Cancel	Details >>	Close Help	

**KU LEUV** 

Start the download with the "Start" button

6. Testing the tunnel function (ping test)

- Open the command prompt on PC2
- Enter the ping command from PC2 to PC3 "ping 192.168.10.4"

C:\Windows\system32\cmd.exe C:\Users\Uincent>ping 192.168.10.4 Pinging 192.168.10.4 with 32 bytes of data: Reply from 192.168.10.4: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.10.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\Users\Uincent>\_

**KU LEUVEN** 

All packets reach PC3 through the tunnel

6. Testing the tunnel function (ping test)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC3 "ping 192.168.10.4"

C:\Windows\system32\cmd.exe
C:\Users\Uincent>ping 192.168.10.4
Pinging 192.168.10.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.10.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Uincent>

 The packets cannot reach PC3 since there is no tunnel communication between these two devices



In this example, a VPN tunnel is established between a PC and a security module using the SOFTNET Security Client The firewall is configured so that the access from PC1 in the external network to PC2 in the internal network is possible for a specific user only, who needs to log in at the RADIUS server



1. Setting up the network

- Reset the Scalance to factory settings by pressing the Reset button and holding it down for at least 5 seconds
- Connect the PC with the Security Configuration Tool (PC1) to the external network interface
- Connect PC2 to the internal network interface
- Connect the Linux PC that will be used as RADIUS server to the DMZ interface



#### 2. Making IP settings for the PCs

PC	IP address	Subnet mask	Default Gateway
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.9.2	255.255.255.0	192.168.9.1
RADIUS	192.168.8.2	255.255.255.0	192.168.8.1

- Set the IP addresses of the PCs as in the table above
- The IP address of the Linux PC is preset to the correct value



3. Creating a project and security module

- Create a new project
- In the "Configuration" area enter the MAC address
- Enter the external IP address (192.168.10.1) and the external subnet mask (255.255.255.0)
- Select the "Routing mode"
- Enter the internal IP address (192.168.9.1) and subnet mask (255.255.255.0)
- Confirm with "OK"

Selection of a module	or software configuration		×
Product type SCALANCE S SOFTNET configural (SOFTNET Security NCP VPN client, VPN	ion Client, SCALANCE M87x/ME I device)	)74x.	
Module S602 S612 S613		<ul> <li>● S623</li> <li>● S627-2M</li> </ul>	
Firmware release			
Configuration			
Name of the module:	Module1		
MAC address:	00-1B-1B-BB-99-DE		
IP address (ext.):	192.168.10.1	Subnet mask (ext.):	255.255.255.0
Interface routing externa	l/internal: Routing mode	-	
IP address (int.):	192.168.9.1	Subnet mask (int.):	255.255.255.0

3. Creating a project and security module

- Select the security module created and select the "Edit" > "Properties" menu command, "Interfaces" tab
- Select the "Activate Interface" check box in the "DMZ port (X3)" area
- Enter the IP address (192.168.8.1) and the subnet mask (255.255.255.0) for the DMZ interface
- Confirm with "OK"

DMZ port (X3) Activate interface		
IP assignment:	Static address	
IP address:	192.168.8.1	
Subnet mask:	255.255.255.0	
MAC address:	00-1B-1B-BB-99-E0	
Comment:		

3. Creating a project and security module

- Use the "Insert" > "Module" menu command with the following parameters
  - Product type: SOFTNET configuration
  - Module: SOFTNET Security Client
  - Firmware release: V4
- Confirm with "OK"

SCALANCE S			
SOFTNET configur (SOFTNET Security NCP VPN client, VP	ation / Client, SCALANCE M87 N device)	x/MD74x.	
Module	_		
SOFTNET Security	Client	VPN device	
SCALANCE M87x/N	1D74x Android		Distance in the second s
Firmware release V4 V3 2008		© 2005	
Configuration			
Name of the module:	Module?		
MAC address:	00-1B-1B-00-00-00		
IP address (ext.):	192.168.10.2	Subnet mask (ext.):	255.255.255.0
Interface routing extern	al/internal:	•	
12 00 0 0			

4. Configuring a RADIUS server

• We'll use the previously configured RADIUS server for this example
5. Configuring the firewall

- Select "VPN groups" in the navigation
- Select the "Insert" > "Group" menu command
- In the navigation panel, click the "All modules" entry
- Drag the SCALANCE S Module to the VPN group "Group1" in the navigation panel The module is now assigned to the VPN group The color of the key symbol changes to blue



5. Configuring the firewall

 Drag the SOFTNET Security Client module to the VPN group "Group1" in the navigation panel The module is now assigned to the VPN group The color of the key symbol changes to blue



**KU LEUV** 

Activate "Advanced Mode"

5. Configuring the firewall

- Use the menu command "Options" > "User Management"
- Create a new user with the following settings
- Confirm with "OK"

ያ Edit users	X
User data	
User name:	radius
Authentication method:	RADIUS
Password:	
Repeat password:	
Comment:	
Settings for user-speci Maximum time of the ses	fic IP rule sets sion: 30 🚔 Minutes
Role	
Assigned role:	radius 💌
	OK Cancel Help

5. Configuring the firewall

- Select the "User-specific IP rule sets" in the navigation window
- Select the "Add rule set..." option in the shortcut menu



5. Configuring the firewall

• Enter a rule in the dialog as shown below

	or opecin		tobol opean ia									
		Name:	User-spec. IP rul	e set1								
	C	escription:	Description Use	r-spec. IP rule set1								
es NA	AT NAP	Т										 
ction	From	То	Source IP ad	Destination I	Servi	Bandwidth (M	Loggi	No.	Comment			
llow	Tunnel	Internal		192.168.9.2	(all)		$\checkmark$	U_1.1				
					Add	rule De	elete rule		<b>•</b>	IP service	S	



5. Configuring the firewall

 From the "Available users and roles" list, select the "radius (user)" entry and click the "Assign" button, then select the "radius (role)" entry and click "Assign"

Available users and roles:	Assigned users and roles:
admin (User) administrator (Role) administrator(radius) (Role) diagnostics (Role) remote access (Role) standard (Role)	Assign Remove

Confirm with "OK"

5. Configuring the firewall

- Select the security module in the navigation panel and drag it to the newly created user-specific IP rule set
- The assignment can be checked by opening the module properties and selecting the "Firewall" tab



5. Configuring the firewall

 Open the properties of the SCALANCE module and go to the "Firewall" tab

#### • Add a firewall rule as in the image

6	Module properties - Module1										
	Interfaces Firewall Internet connection DNS Routing NAT/NAPT Time synchronization Log settings VPN DHCP-Server SNMP Proxy ARP RADIUS										
	IP rules [2] MAC rules (inactive) [0] Default rules for IP services										
	Action	From	То	Source IP addre	Destination IP a	Servi	Bandwidth (M	Loggi	No.	Comment	
ш	User-spec. IP rule set1 (Assigned users: ; assigned roles:radius)										
	Drop	Tunnel	Internal			(all)		$\checkmark$	IP-R_1		

**KU LEUVEN** 

• Confirm with "OK"

#### 6. Linking the RADIUS server and security module

- Select the menu option "Options" > "Configuration of the RADIUS server..."
- Click the "Add…" button in the dialog

Name	IP address / FQDN	Port ID	Comment

Op	otions	Help					
	IP ser	vices					
	MAC services						
	Netw	ork adapter					
	Langu	Jage					
	Log f	iles					
	Symb	olic names					
	Confi	guration of the NTP server					
	Confi	guration of the RADIUS server					
	Consi	stency checks					
	User i	management					
	Certif	ïcate manager					

6. Linking the RADIUS server and security module

- Define the server with the following values
  - IP address/FQDN: 192.186.8.2
  - Shared secret: SiemensSecret
  - Repeat shared secret: SiemensSecret
- Confirm with "OK"

Definition of a RADIU	S server				×
Name:	RADILIS server				
IP address / FODN:	102 169 9 2				
Dest:	192.100.0.2				
Polt.	1812				
Shared secret:	•••••				
Repeat shared secret:	•••••				
Authentication method:	PAP				
Comment:					
		ОК	Cancel	Hel	P

6. Linking the RADIUS server and security module

 Open the SCALANCE S module properties and go to the "RADIUS" tab

3	Module	e properti	es - Module1											_	X
Int	erfaces	Firewall	Internet connection	DNS	Routing	NAT/NAPT	Time synchronization	Log settings	VPN	DHCP-Server	SNMP	Proxy ARP	RADIUS		
	Enable	RADIUS a	uthentication												

- Check the "Enable RADIUS authentication" box
- Click the "Add" button This adds the newly configured RADIUS server

RADIUS	ADIUS server							
No.	Name	IP address	Comment					
1	RADIUS server	192.168.8.2						



6. Linking the RADIUS server and security module

 In the "RADIUS setting" area, check the "Allow RADIUS authentication of non-configured users" box

RADIUS settings						
RADIUS timeout:	1	Seconds				
RADIUS retries:	5					
Allow RADIUS authentication of non-configured users						
Filter ID is required for authentication						

Confirm with "OK"



7. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the project
- Use the menu command "Transfer" > "To all modules..."

ያ Download configuration data	to security modules		
Module name	Project status	Downloading status	
Module2 (SSC)	OK	Loaded	
Module1 (SCALANCE S)	ОК	Loaded	
✓ Log on as current user			Select all
Show only modified modules			
Current module:			Deselect all
Transfer type			
Modified files only	All files		
Skip	Cancel	Details >>	Close Help

**KU LEUV** 

Start the download with the "Start" button

7. Downloading the configuration to the security module and saving the SOFTNET Security Client configuration

- Save the configuration file "projectname.Module2.dat" in your project folder
- Assign a password to the certificate
- Confirm the popup with "OK"



8. Setting up a tunnel with the SOFTNET Security Client

• Open the SOFTNET Security Client on PC2

SOFTNET Security Client		
File Options Help		
Communication options		
Load Configuration	Tunnel Overview	Enable
Minimize	Exit	Help About

- Select "Load Configuration" and browse to where "projectname.Module2.dat" has been saved
- Open the configuration with the "Open" button

8. Setting up a tunnel with the SOFTNET Security Client

 Loading a new configuration will delete any previous configurations

SOFTNET Security Client - Configuration Data Already Exists	X
Configuration data already exist for the SOFTNET Security Client. Should the stored configuration data be	
deleted	
kept and merged with the new one, whereas modules with identical IP addresses shall be	
imported and replaced	
O not imported	
Next Ca	incel

 When the dialog above pops up, select "deleted" and confirm with "Next"

**KU LEUV** 

8. Setting up a tunnel with the SOFTNET Security Client

 The VPN tunnel can now be opened by clicking the "Enable" button

SOFTNET Security Client		
File Options Help		
Communication options		
Load Configuration	Tunnel Overview	Enable
Minimize	Exit	Help About

**KU LEUVEN** 

• Enter the certificate password in the dialog

8. Setting up a tunnel with the SOFTNET Security Client

"Tunnel Overview" shows the status of the tunnel

unnel	list				
Stat	Name	Member IP / Subnet	Tunnel Endnoint IP	Tunnel over	
• <b>N</b>	"Module1" Subnet of: "Module1"	SCALANCE S623 192.168.9.0/255.255.255.0	192.168.10.1 192.168.10.1	192.168.10.2 192.168.10.2	
				enable active learning	Delete
ogging Oct 27 Oct 27 Oct 27 Oct 27	g Console: , 2015 - 09:30:48] [OuickMode] , 2015 - 09:30:49] [OuickMode] , 2015 - 09:30:52] [OuickMode] , 2015 - 09:30:52] [OuickMode]	Deleted Security Association From 1 Deleted Security Association From 1 Added Security Association From 15 Added Security Association From 15	92.168.10.2 To 192.168.10.1/; 92.168.10.2 To 192.168.9.0/24 1.68.10.2 To 192.168.9.0/24 12.168.10.2 To 192.168.10.1/32 1.68.10.2 To 192.168.10.1/32	32 4 2	
(					4
					Clear

**KU LEUVEN** 

The green circle shows that the tunnel has been established

6. Setting up a tunnel with the SOFTNET Security Client

- If the tunnel does not get set up, check whether the Windows Firewall has been enabled
- Open the <u>"Control</u> Panel" > "Windows Firewall"

Control Panel Home	Help protect your computer with Wi	indows Firewall	
Allow a program or feature through Windows Firewall	Windows Firewall can help prevent hackers or n through the Internet or a network.	nalicious software from gaining access to your computer	
😽 Change notification settings	How does a firewall help protect my computer?	2	
Turn Windows Firewall on or off	What are network locations?		
😽 Restore defaults	Home or work (private) netw	vorks Connected 🔿	
Advanced settings Troubleshoot my network	Networks at home or work where you know and trust the people and devices on the network		
	Windows Firewall state:	On	
	Incoming connections:	Block all connections to programs that are not on the list of allowed programs	
	Active home or work (private) networks:	🕪 hubkaho.be	
	Notification state:	Notify me when Windows Firewall blocks a new program	
	Public networks	Not Connected 😒	

 If the firewall is not enabled, click "Turn Windows Firewall on or off" and enable it

9. Logging in on the Web page

 In the Web browser of PC1, enter the address "https://192.168.10.1"

SIEMENS		English 💌 Go
	SCALANCE S	-
	Welcome to the SCALANCE S user-specific firewall	
	Please log on:	
	Name	



9. Logging in on the Web page

• If the web page does not show the login fields, try changing the language in the upper right corner

SIEMENS		English 🗾 <u>Go</u>
	SCALANCE S	

KUL

9. Logging in on the Web page

• Enter the user name "radius" and corresponding password and click the "Log in" button

SIEMENS	English 💙 Sa
	SCALANCE S
	Welcome to the SCALANCE S user-specific firewall
	Please log on:
	Name radius Password
	Log in



9. Logging in on the Web page

• The defined IP rule set is enabled for the "radius" user.

SIEMENS		English 💌 <u>G</u>	2
	SCALANCE S		2
	Welcome, radius You have logged in successfully from address 192.168.10.2 Your session expires in 30 Minutes Extend timeout Log out		



10. Testing the firewall function (ping test)

- Open the command prompt on PC1
- Enter the ping command from PC1 to PC2 "ping 192.168.9.2"

C:\Windows\system32\cmd.exe C:\>ping 192.168.9.2 Pinging 192.168.9.2 with 32 bytes of data: Reply from 192.168.9.2: bytes=32 time=4ms TTL=63 Reply from 192.168.9.2: bytes=32 time=3ms TTL=63 Reply from 192.168.9.2: bytes=32 time=4ms TTL=63 Reply from 192.168.9.2: bytes=32 time=4ms TTL=63 Ping statistics for 192.168.9.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 3ms, Maximum = 4ms, Average = 3ms C:\>

**KU LEUVEN** 

All packets reach PC2 through the tunnel