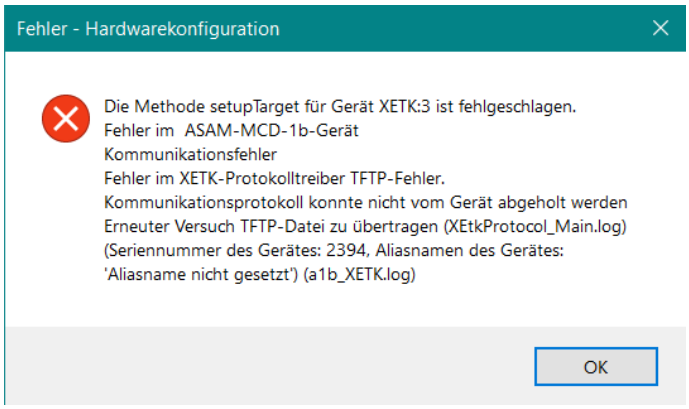
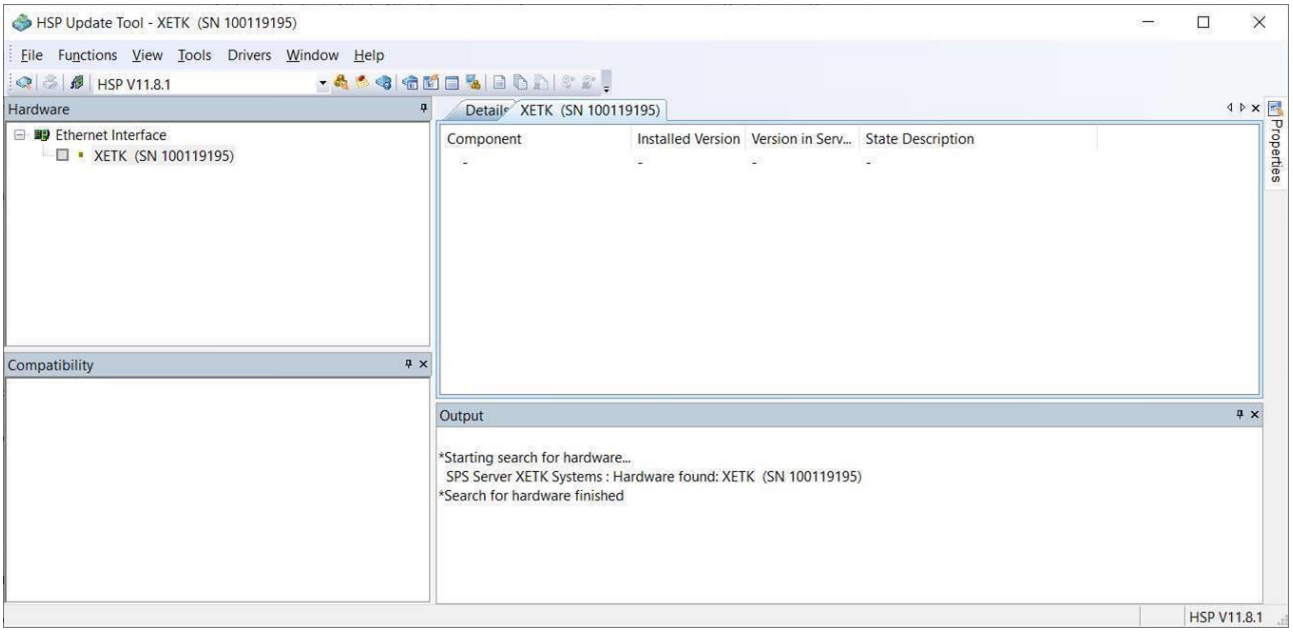
DRIVING EMBEDDED EXCELLENCE

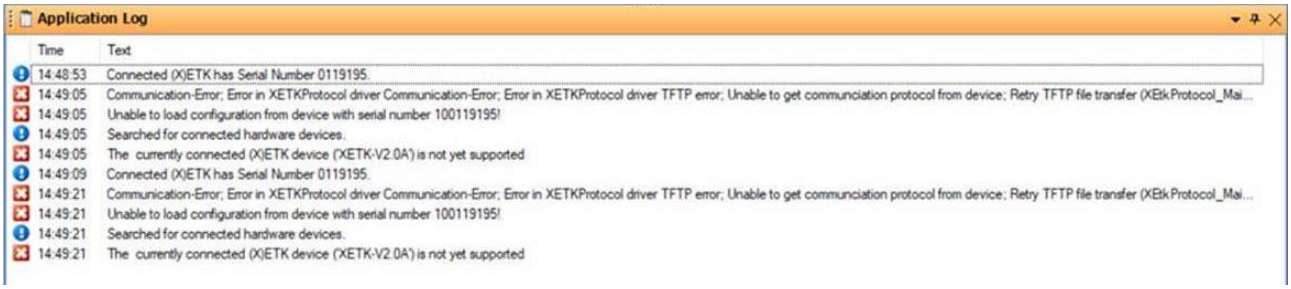
Question:

Why am I getting the TFTP error message in INCA and in XCT tool or why can I not see the firmware version from my (F/X)ETK in HSP Update Tool?

I want to update my firmware of my (F/X)ETK using the HSP Update Tool, to initialize my (F/X)ETK in INCA or to download the configuration of my (F/X)ETK using the XCT tool. This is unfortunately not possible due to the following error message:







Answer:

The connection is always initiated by PC to the (F/X)ETK. The (F/X)ETK sends data only if a connection is already established. The XCP connections use the service TCP or UDP and use for that always the port 1802. Changes to the configuration or the firmware will be read so the TFTP protocol will be used.

To use the TFTP protocol the ports 69 and 19000 to 19007 must be released in the firewall for the protocol type UDP. The port 69 of (F/X)ETK waits for the build up of first communication. For all responses to the (F/X)ETK the ports in the range of 19000 to 19007 will be used.

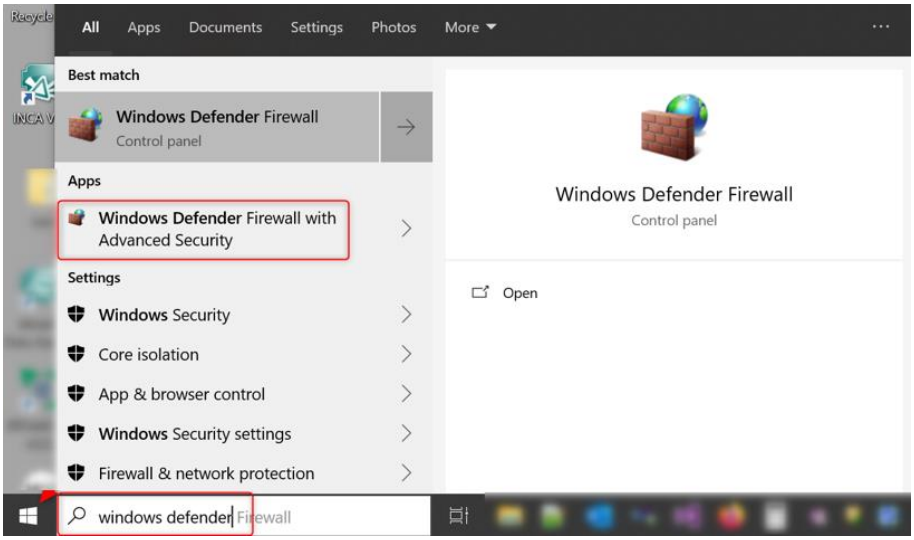
Service	Type	PC source port number	XETK dest. port number	Remarks / Description
ETAS IP Management	UDP	18001	18001	Not needed for Fixed IP and DHCP managed devices
XCP	TCP, UDP	1024..65535	1802	MC: INCA uses TCP. 3rd party tools may also use UDP
				RP: Bypass normally uses UDP, but in special cases could use TCP
TFTP connect	UDP	1024..65535	69	
TFTP transfer	UDP	1024..65535	19000..19007	PC uses the same random port that was used for TCP connect

The easiest way is to completely deactivate the firewall. If that not possible an exception must be created for the used ports or the programs in the firewall settings.

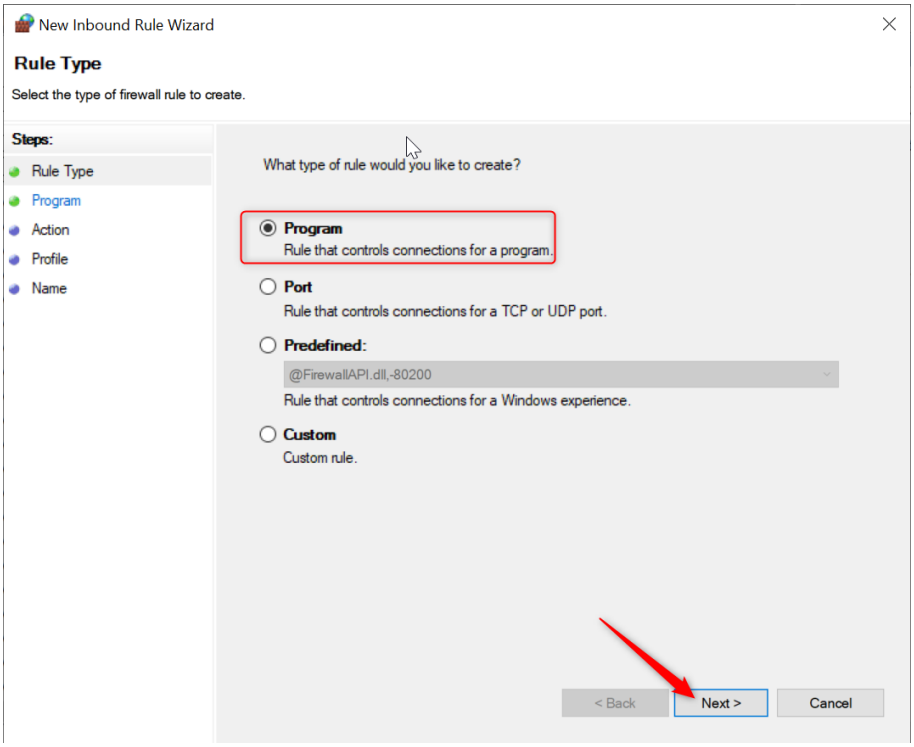
In *Windows 10* this can be done over the ***Windows Defender Firewall***. For other tools the own IT must be requested.

Create an exception for a program:

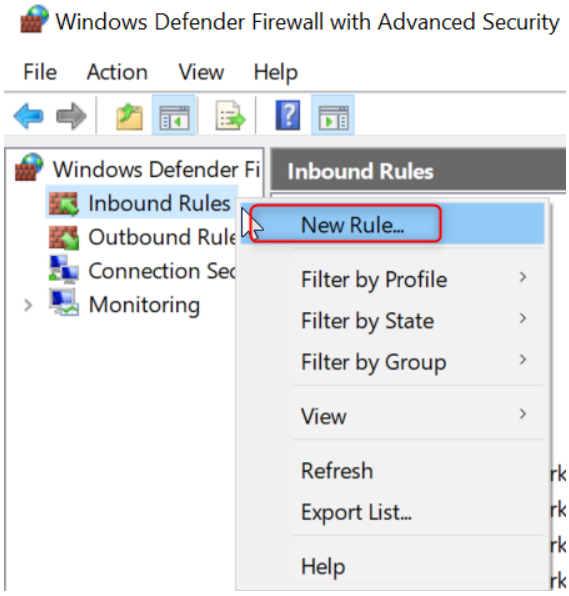
1. Start the *Windows Defender Firewall* with Advanced Security over the Windows Start icon and the input of the words **Windows Defender**.



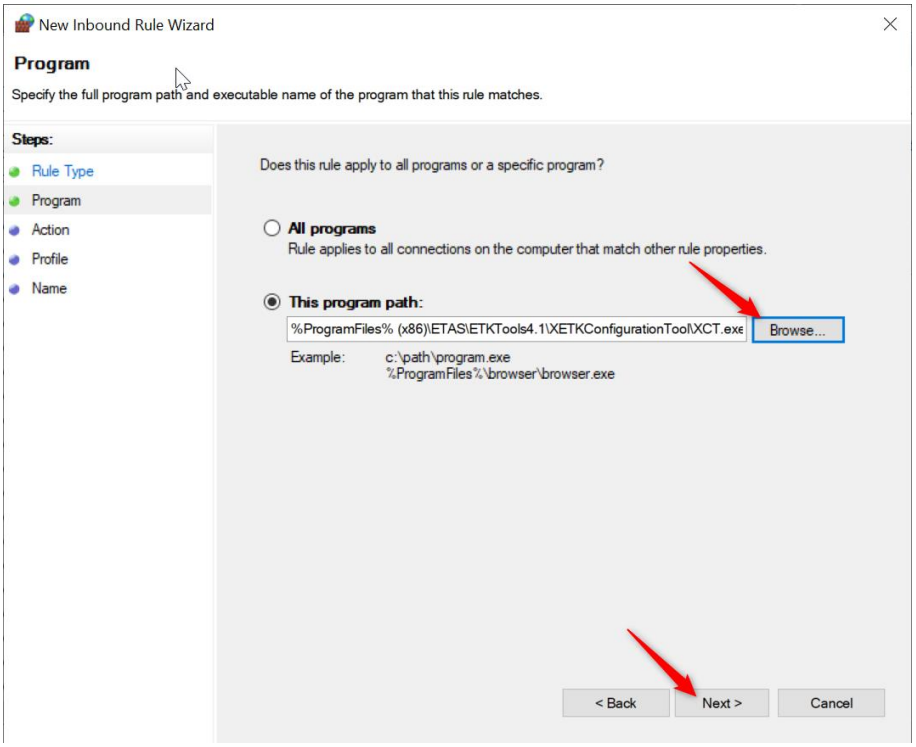
2. Right click on **Inbound Rules** and select **New Rule...** .



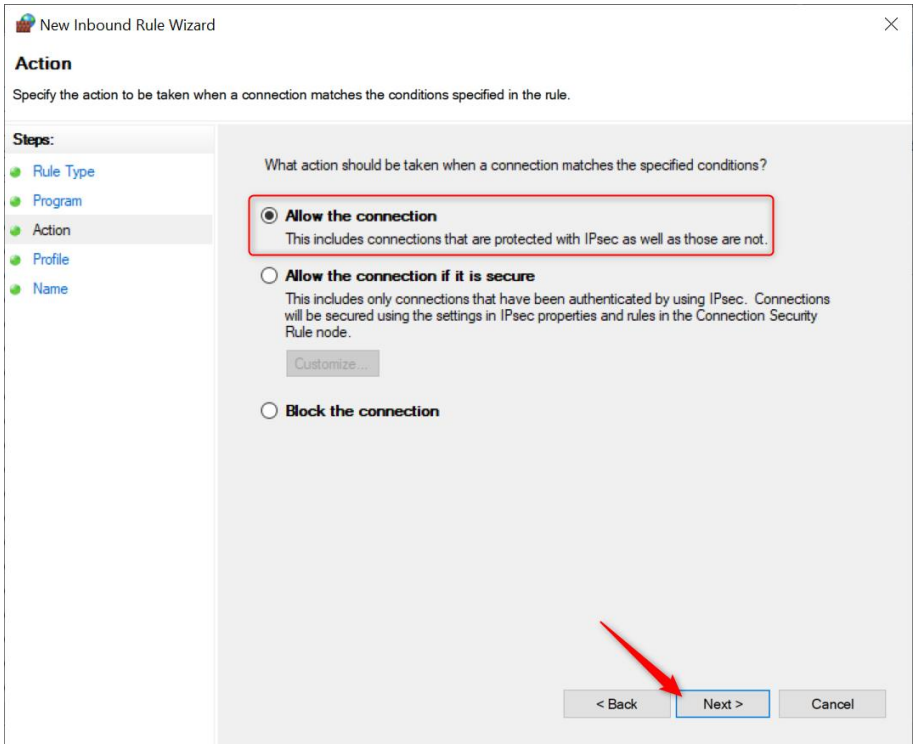
3. Select **Program** as rule and click on **Next**.



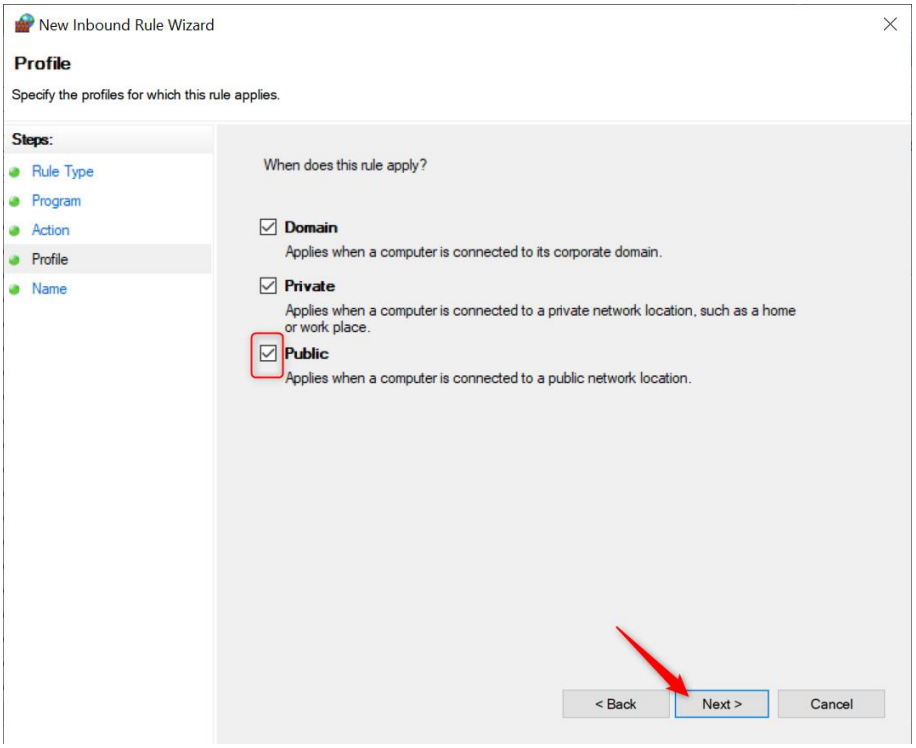
4. Then go to **This program path:** and click on **Browse**… and f.e. link the *XCT.exe* file under *C:\Program Files (x86)\ETAS\ETKTools4.1\XETKConfigurationTool* and confirm with **Next**.



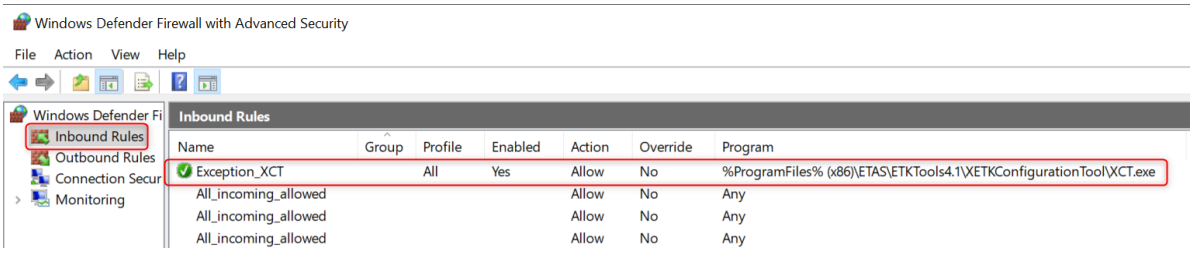
5. In the new windows select **Allow the connection** and confirm with **Next**.



6. The rule shall be applied at least for **Public**.



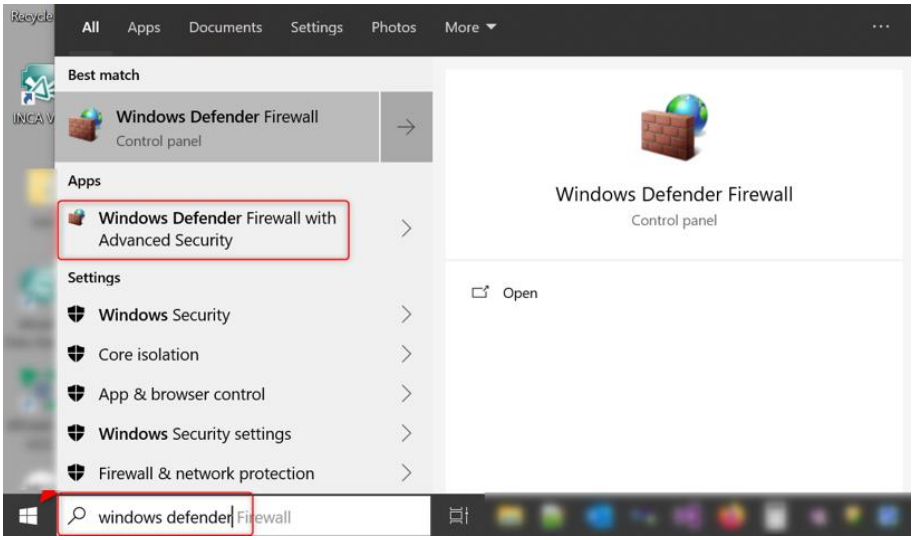
7. Finally an own name for the rule can be forgiven and will be definitely created with the button **Finish**.



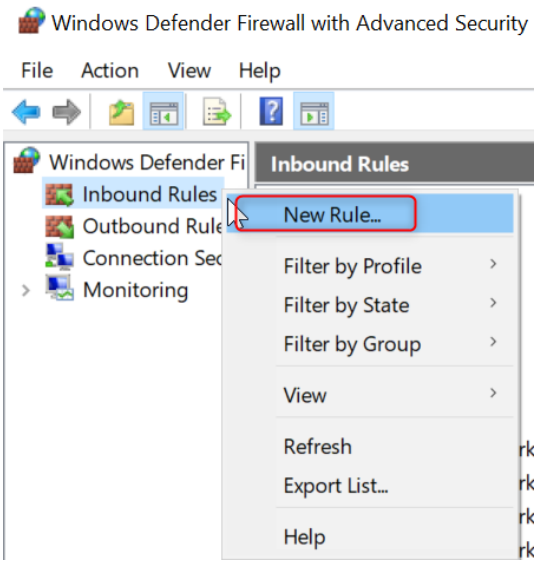
Similarly the same steps can be done for **Outbound Rules**.

Create an exception for the protocoll type UDP:

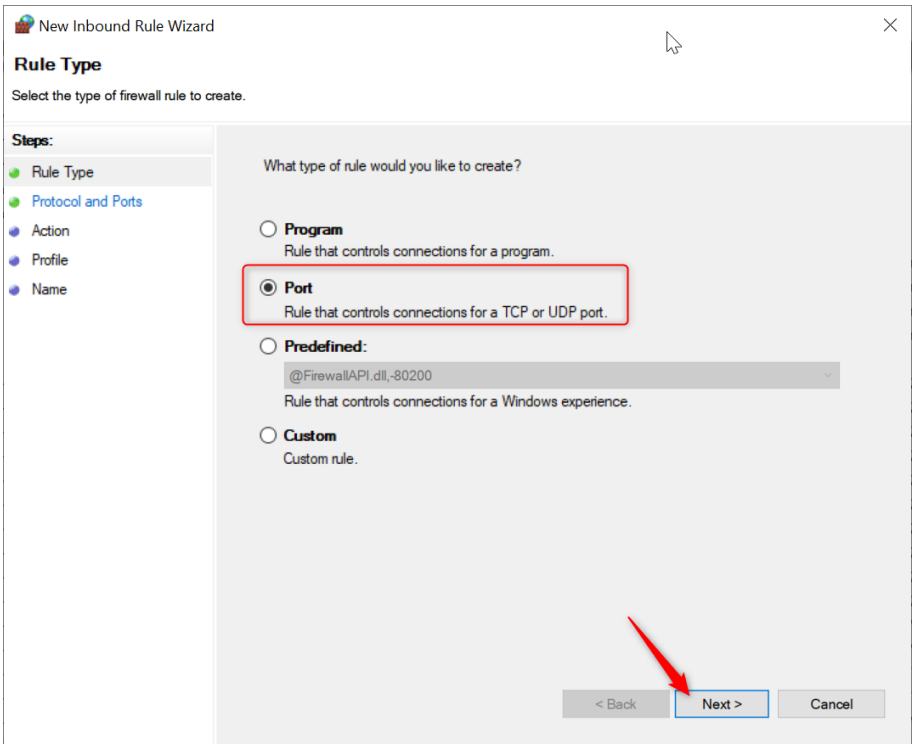
1. Start the Windows Defender Firewall with Advanced Security over the Windows Start icon and the input of the words **Windows Defender**.



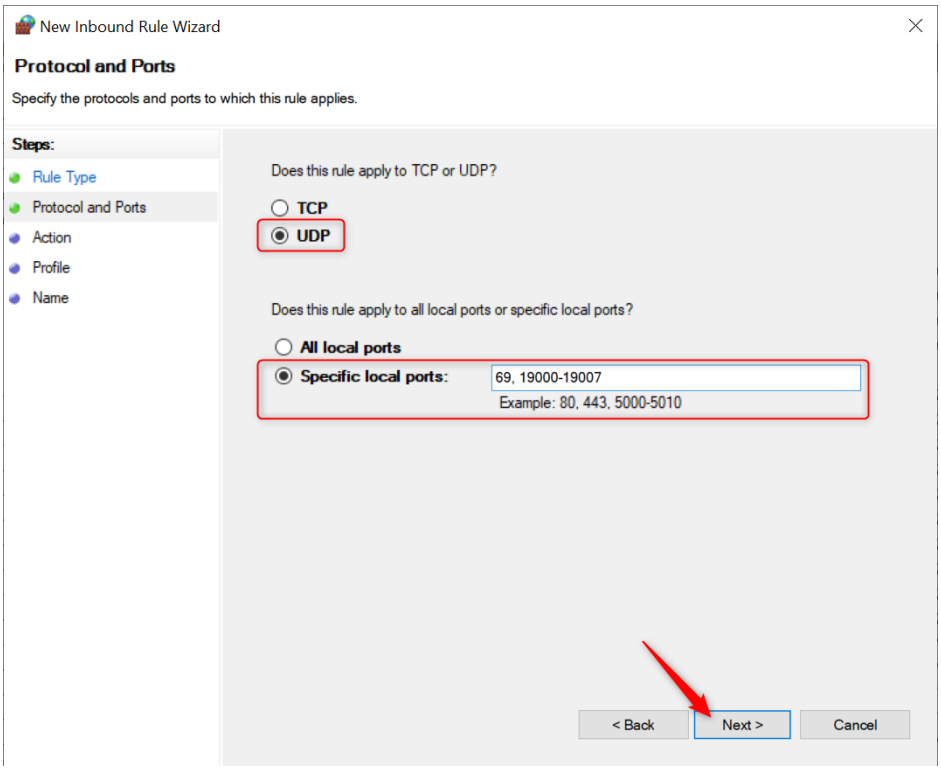
2. Right click on **Inbound Rules** and select **New Rule...** .



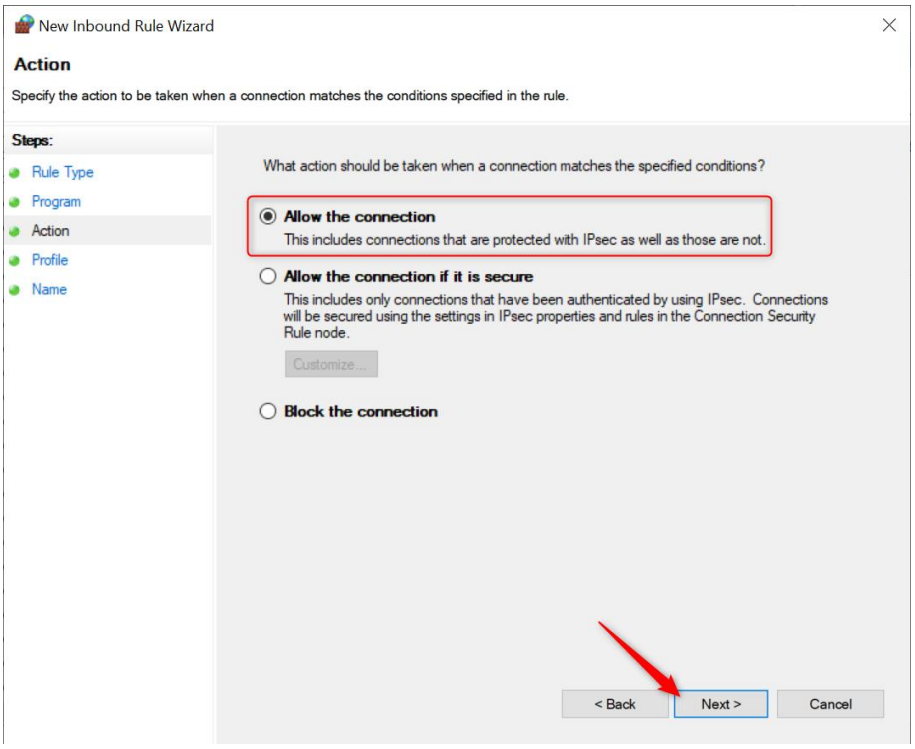
3. Select **Port** as rule and click on **Next**.



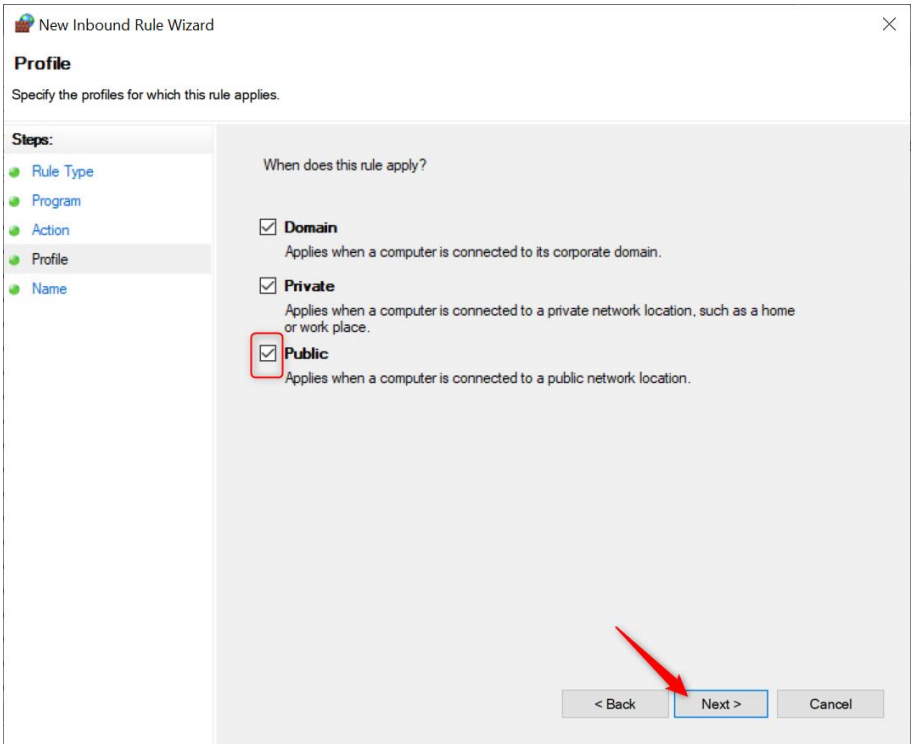
4. Here choose **UDP** as rule type and enter at **Specific local port:** 69, 19000 – 19007. With that the port 69 and the ports from 19000 to 19007 will be released.



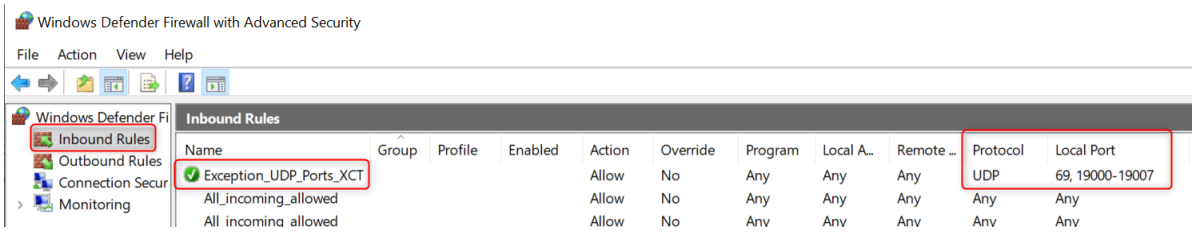
5. In the new windows select **Allow the connection** and confirm with **Next**.



6. The rule shall be applied at least for **Public**.



7. Finally an own name for the rule can be forgiven and will be definitaley created over the button **Finish**.



Similarly the same steps can be done for **Outbound Rules**. Then for the ports 1024 to 65535.

Additional information:

It can be also added in the firewall as exception the programs INCA.exe, XCT.exe and FWUT.exe (HSP Update Tool).

In case of further questions:

Please feel free to contact our Support Center, if you have further questions.
Here you can find all information: http://www.etas.com/en/hotlines.php?langS=true&