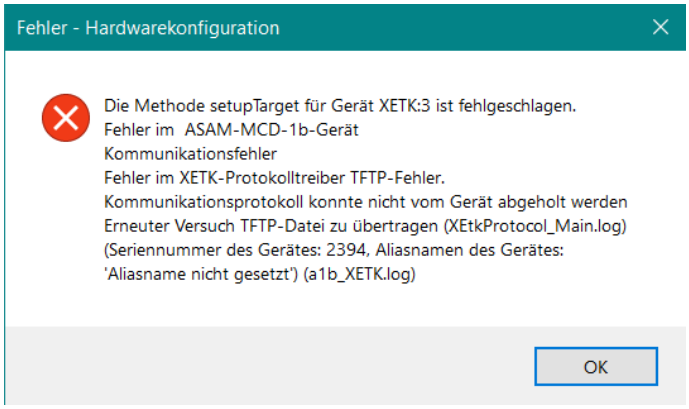
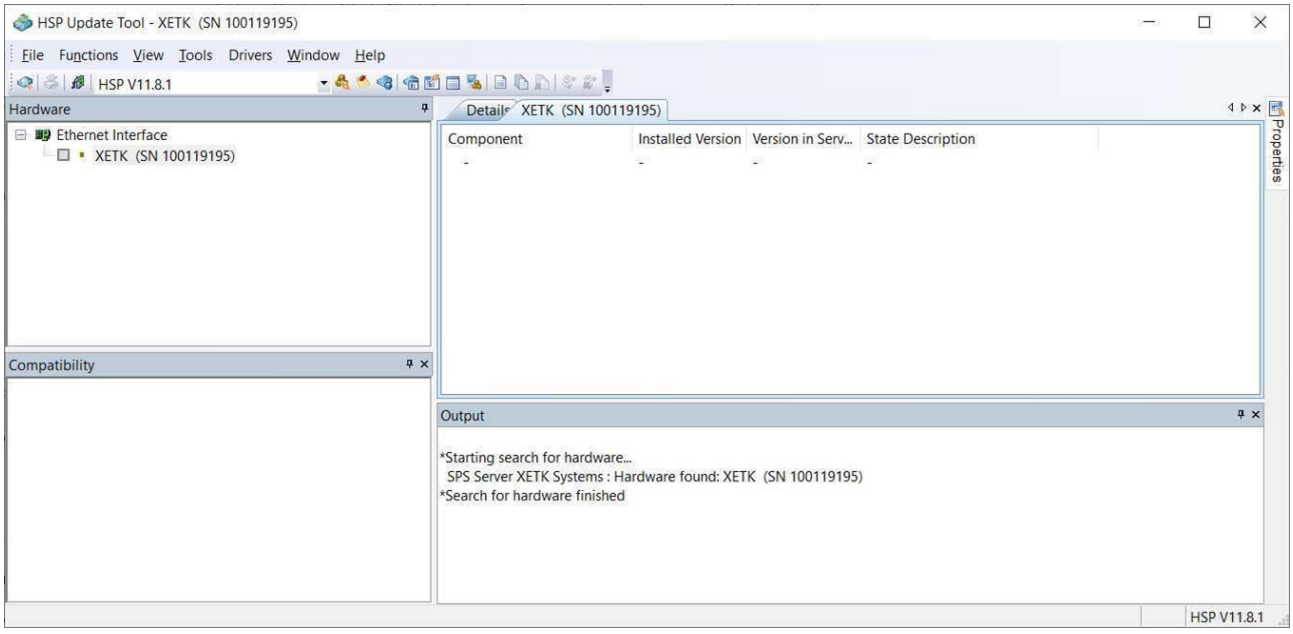
DRIVING EMBEDDED EXCELLENCE

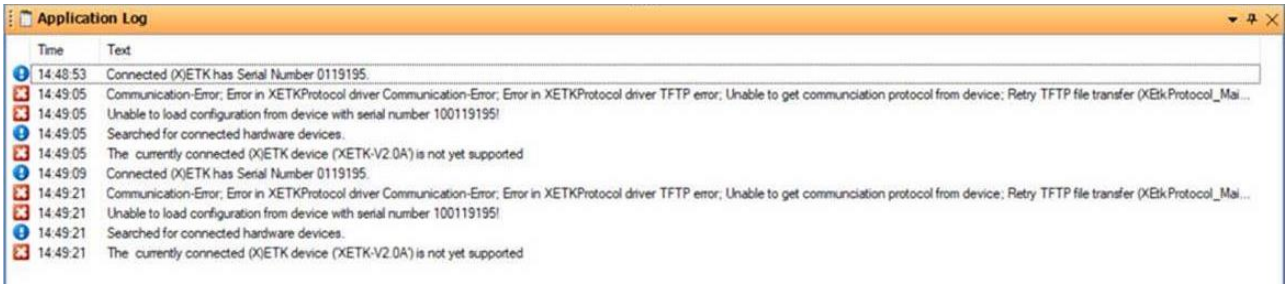
Frage:

Warum bekomme ich in INCA und im XCT Tool die TFTP Fehlermeldung oder wieso sehe ich im HSP Update Tool nicht die Firmware Version meines (F/X)ETK's?

Ich möchte meine Firmware meines (F/X)ETK's im HSP Update Tool aktualisieren, in INCA mein (F/X)ETK initialisieren oder im XCT Tool die Konfiguration meines (F/X)ETK's herunterladen. Dies ist leider aufgrund folgender Fehlermeldungen nicht möglich:







Antwort:

Eine Verbindung zum (F/X)ETK wird immer vom PC aufgebaut. Der (F/X)ETK sendet nur Daten, wenn eine Verbindung schon aufgebaut wurde. Die XCP Verbindungen verwenden den Dienst TCP oder UDP und nutzen dafür immer den Port 1802. Ändert sich nun die Konfiguration oder die Firmware soll ausgelesen werden, so wird das TFTP Protokoll verwendet.

Um das TFTP Protokoll verwenden zu können, sind die Ports 69 und 19000 bis 19007 für das TFTP Protokoll auf UDP Basis in der Firewall freizuschalten.
Der Port 69 des (F/X)ETK dient zum erstmaligen Kommunikationsaufbau. Für alle Antworten verwendet der (F/X)ETK die Ports im Bereich zwischen 19000 und 19007.

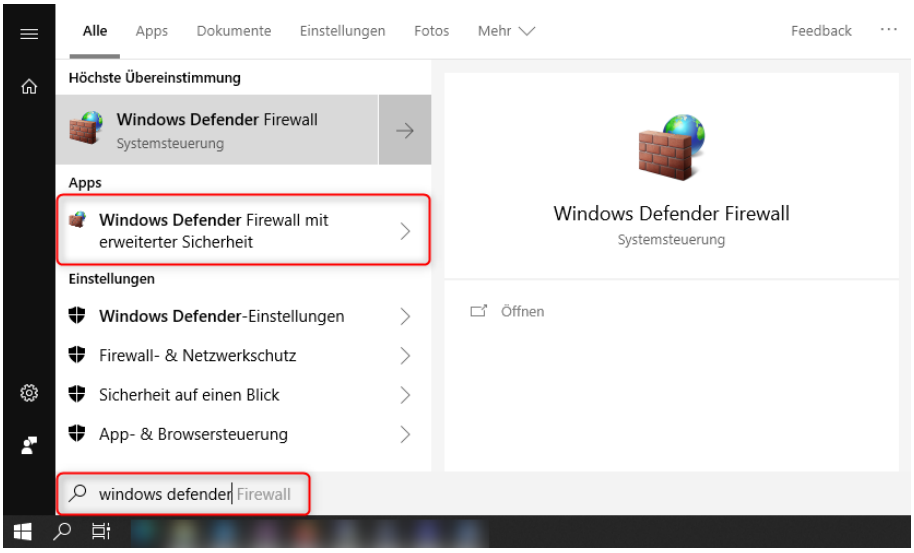
Service	Type	PC source port number	XETK dest. port number	Remarks / Description
ETAS IP Management	UDP	18001	18001	Not needed for Fixed IP and DHCP managed devices
XCP	TCP, UDP	1024..65535	1802	MC: INCA uses TCP. 3rd party tools may also use UDP
				RP: Bypass normally uses UDP, but in special cases 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

Der einfachste Weg ist die Firewall komplett zu deaktivieren. Ist dies nicht möglich, müssen die verwendeten Ports oder die Programme eine Ausnahme in den Firewalleinstellungen erhalten.

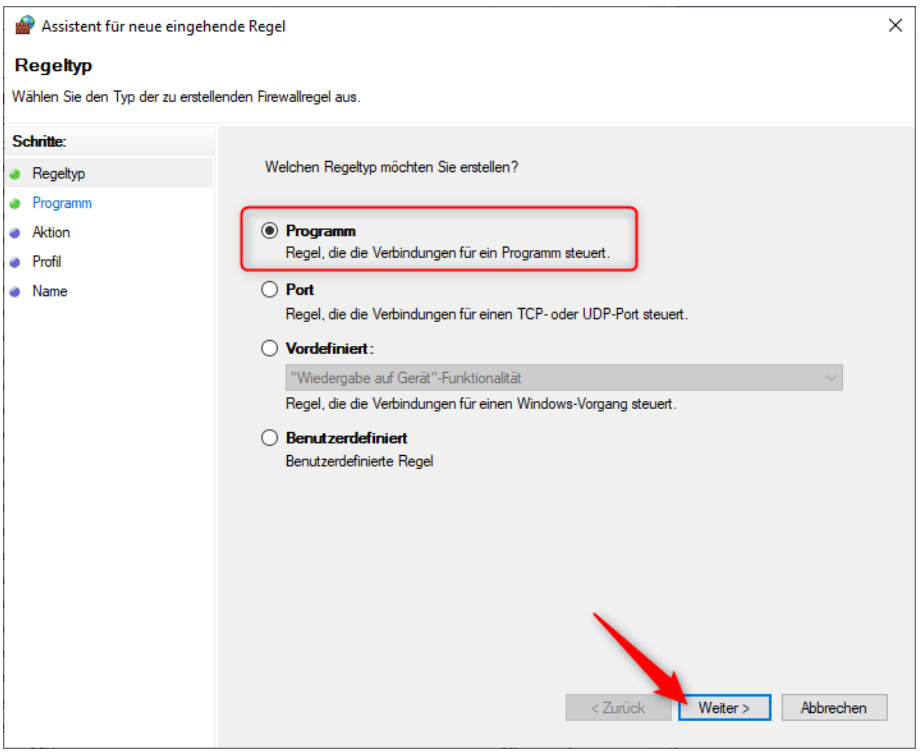
In *Windows 10* wird dies über die ***Windows Defender Firewall*** wie folgt durchgeführt. Für andere Programme bitte Ihre eigene IT einbeziehen.

Ausnahme für ein Programm:

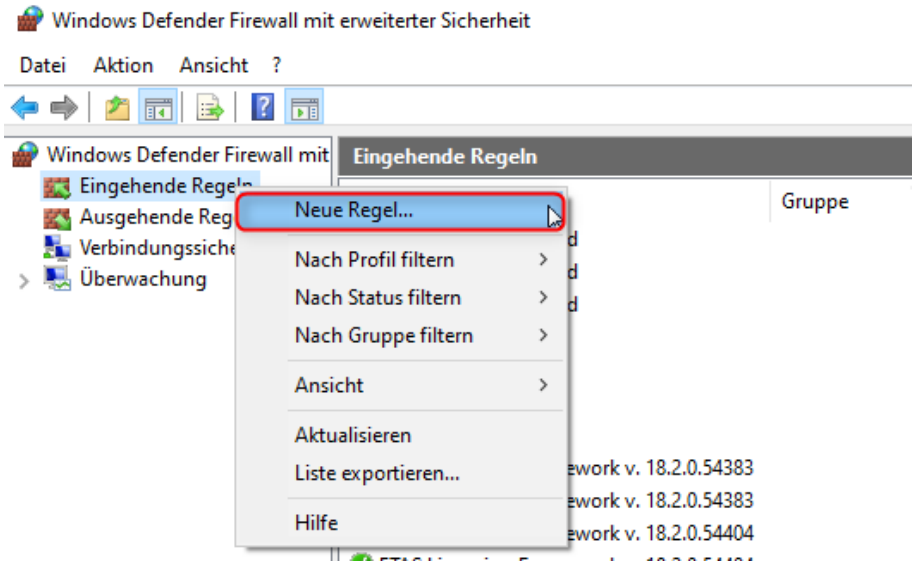
1. Starten der *Windows Defender Firewall* mit erweiterter Sicherheit über Windows Startlogo und Eingabe des Wortes **Windows Defender**.



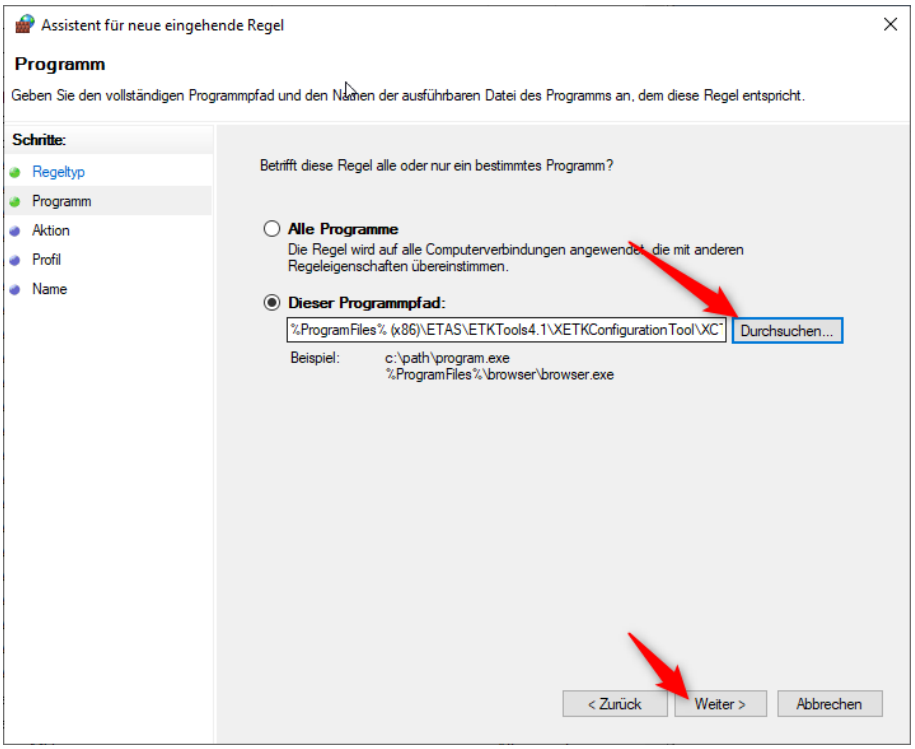
2. Rechtsklick auf **Eingehende Regeln** und im Kontextmenü **Neue Regel...** wählen.



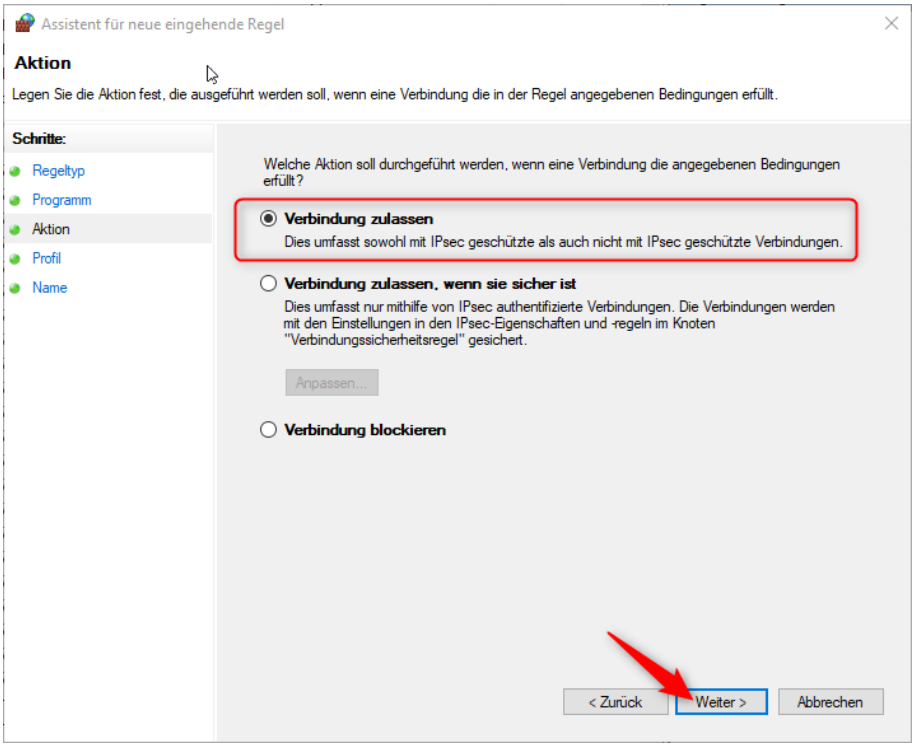
3. **Programm** als Regeltyp selektieren und auf **Weiter** klicken.



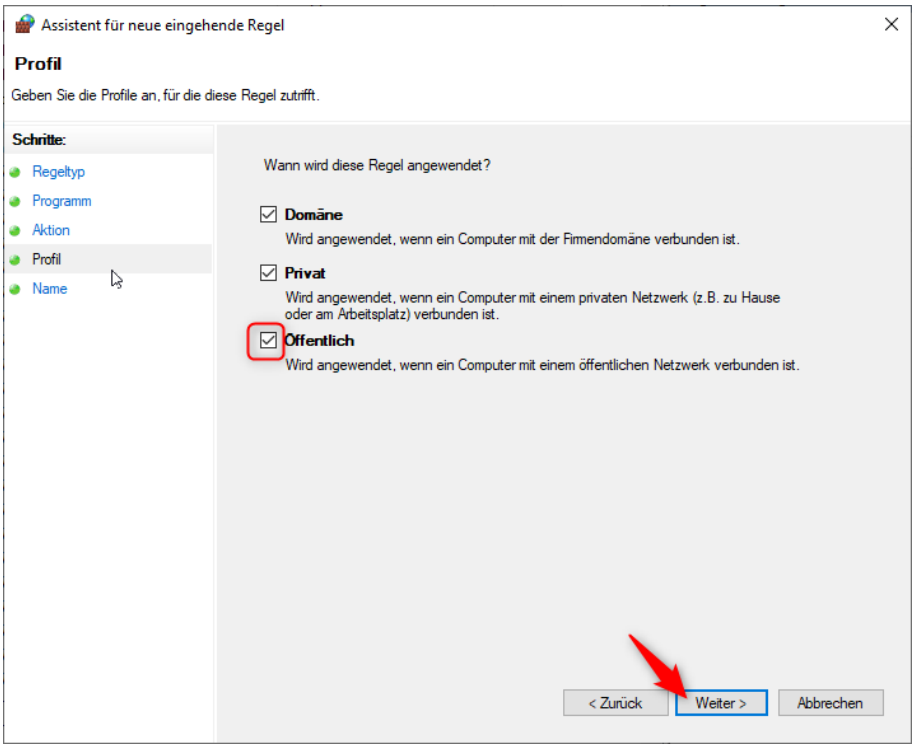
4. Unter **Dieser Programmpfad:** auf **Dursuchen…** klicken und z.B. die XCT.exe Datei unter *C:|Program Files (x86)|ETAS|ETKTools4.1|XETKConfigurationTool* verlinken und mit **Weiter** bestätigen.



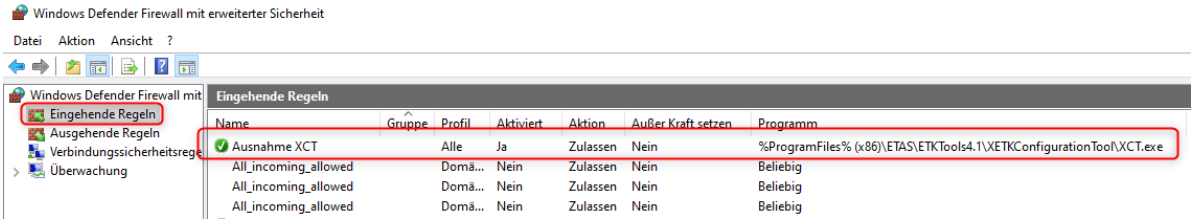
5. Im neuen Fenster die Auswahl auf **Verbindung zulassen** belassen und mit **Weiter** bestätigen.



6. Die Regel sollte mindestens für den Bereich **Öffentlich** gesetzt bleiben.



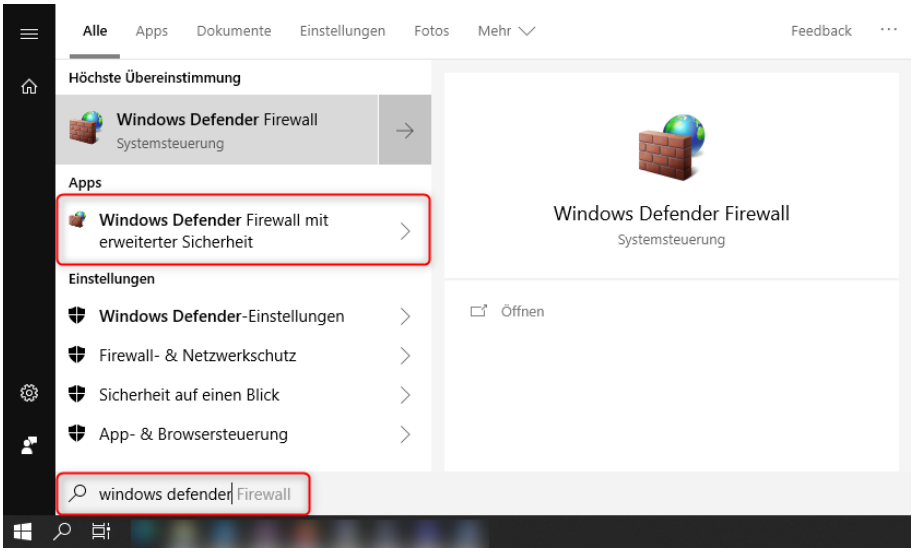
7. Abschließend vergeben Sie der Regel noch einen eigenen Namen und erstellen diese endgültig über den Button **Fertig stellen**.



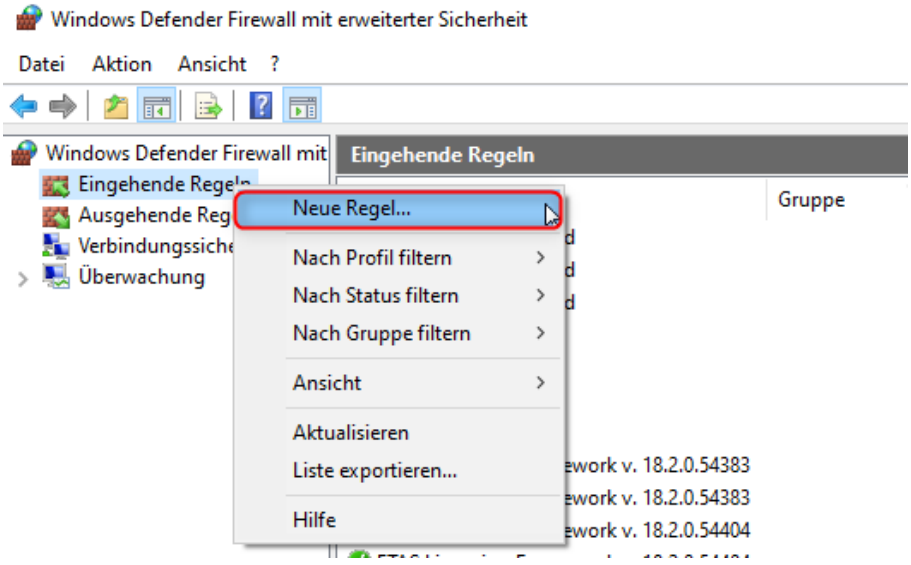
Zum Schluss können Sie das gleiche noch für die **Ausgehende Regeln** erstellen.

Ausnahme für den Protokolltyp UDP:

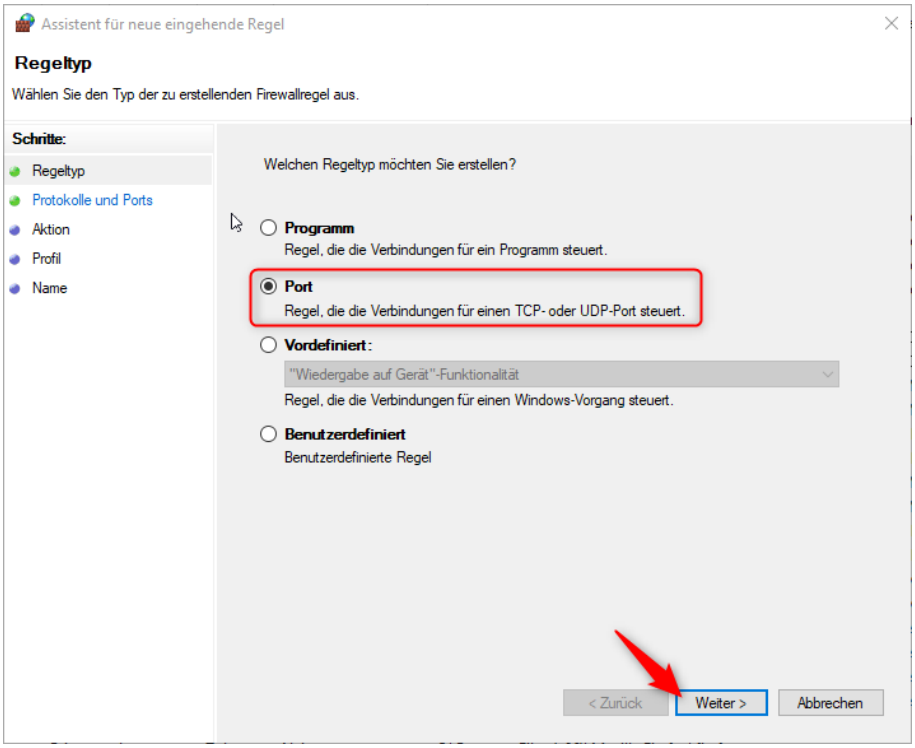
1. Starten der *Windows Defender Firewall* mit erweiterter Sicherheit über das Window Startlogo und Eingabe des Wortes **Windows Defender**.



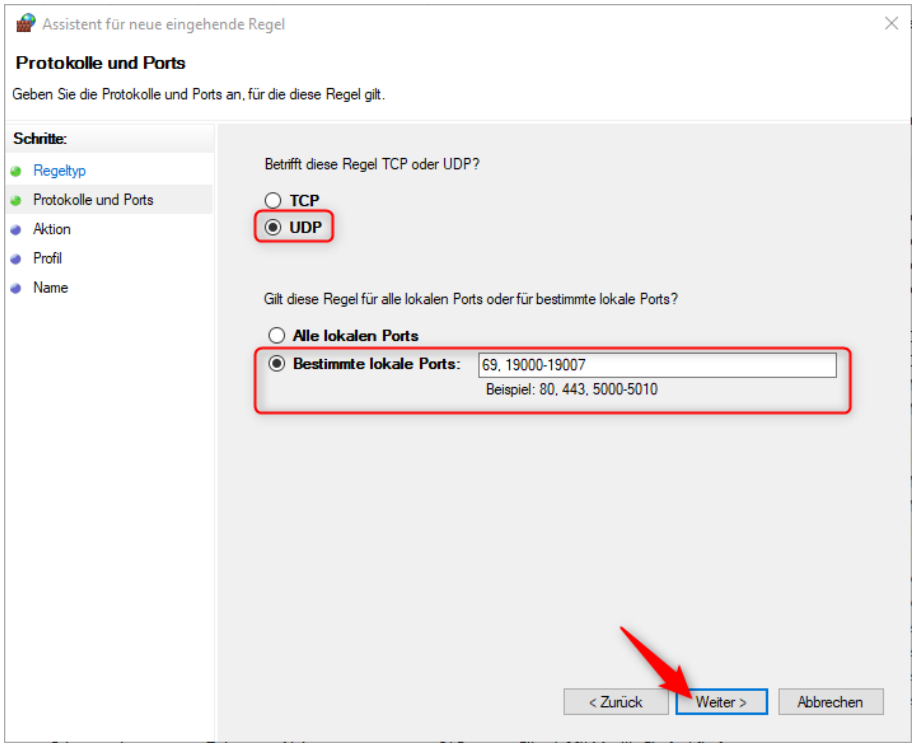
2. Rechtsklick auf **Eingehende Regeln** und im Kontextmenü **Neue Regel...** wählen



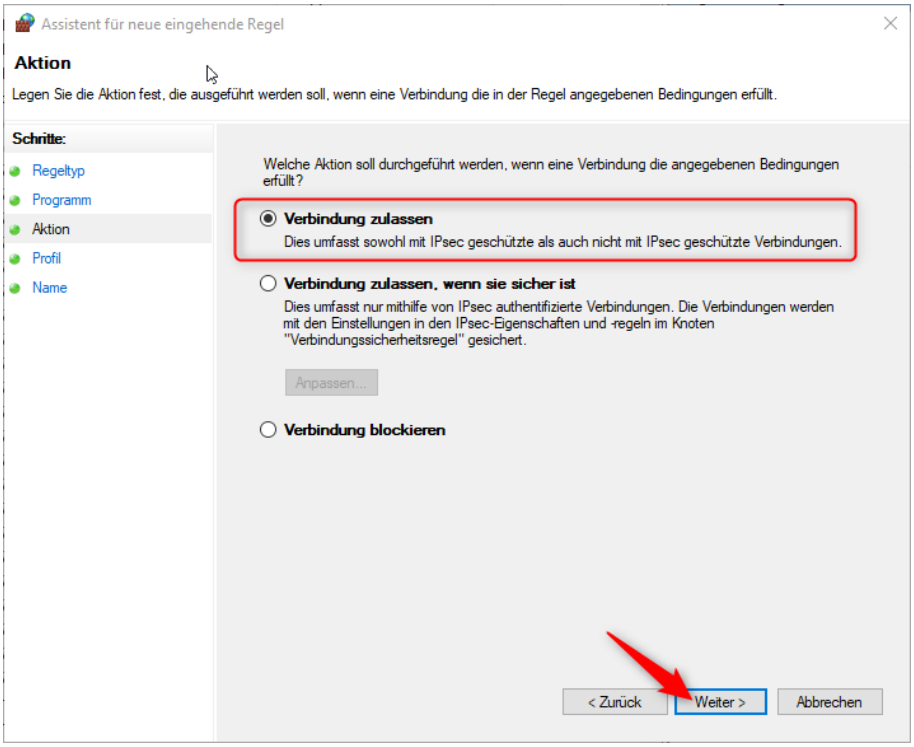
3. **Port** als Regeltyp selektieren und auf **Weiter** klicken.



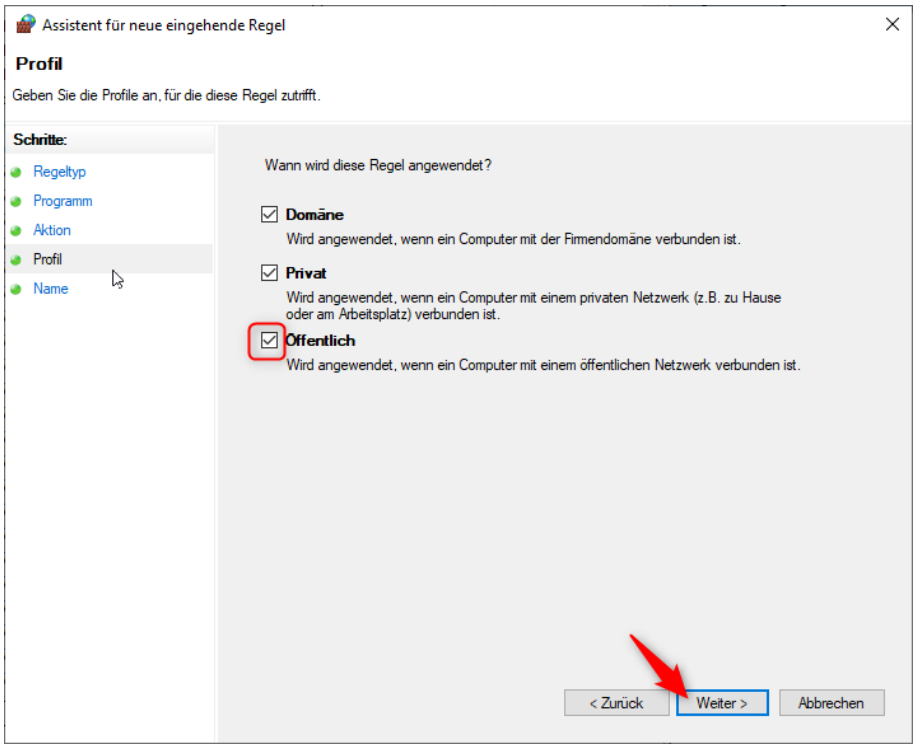
4. Hier wählen Sie **UDP** als Porttyp und geben bei **Bestimmte lokale Ports:** 69, 19000-19007 ein. Damit werden der Port 69 und die Ports von 19000 bis 19007 freigegeben.



5. Im neuen Fenster die Auswahl auf **Verbindung zulassen** lassen und mit **Weiter** bestätigen.



6. Die Regel sollte mindestens für den Bereich **Öffentlich** gesetzt bleiben.



7. Abschließend vergeben Sie der Regel noch einen eigenen Namen und erstellen diese endgültig über den Button **Fertig stellen**.

Zum Schluss können Sie das gleiche noch für **Ausgehende Regeln** erstellen.
Hier für die Ports 1024 bis 65535.

Weitere Informationen:

Es können ebenso die Programme INCA.exe, XCT.exe und FWUT.exe (HSP Update Tool) in der Firewall als Ausnahme hinzugefügt werden.

Sie haben dennoch eine Frage?

Für weitere Fragen stehen wir Ihnen gern zur Verfügung.
Unsere Hotline-Nummer finden Sie unter http://www.etas.com/de/hotlines.php