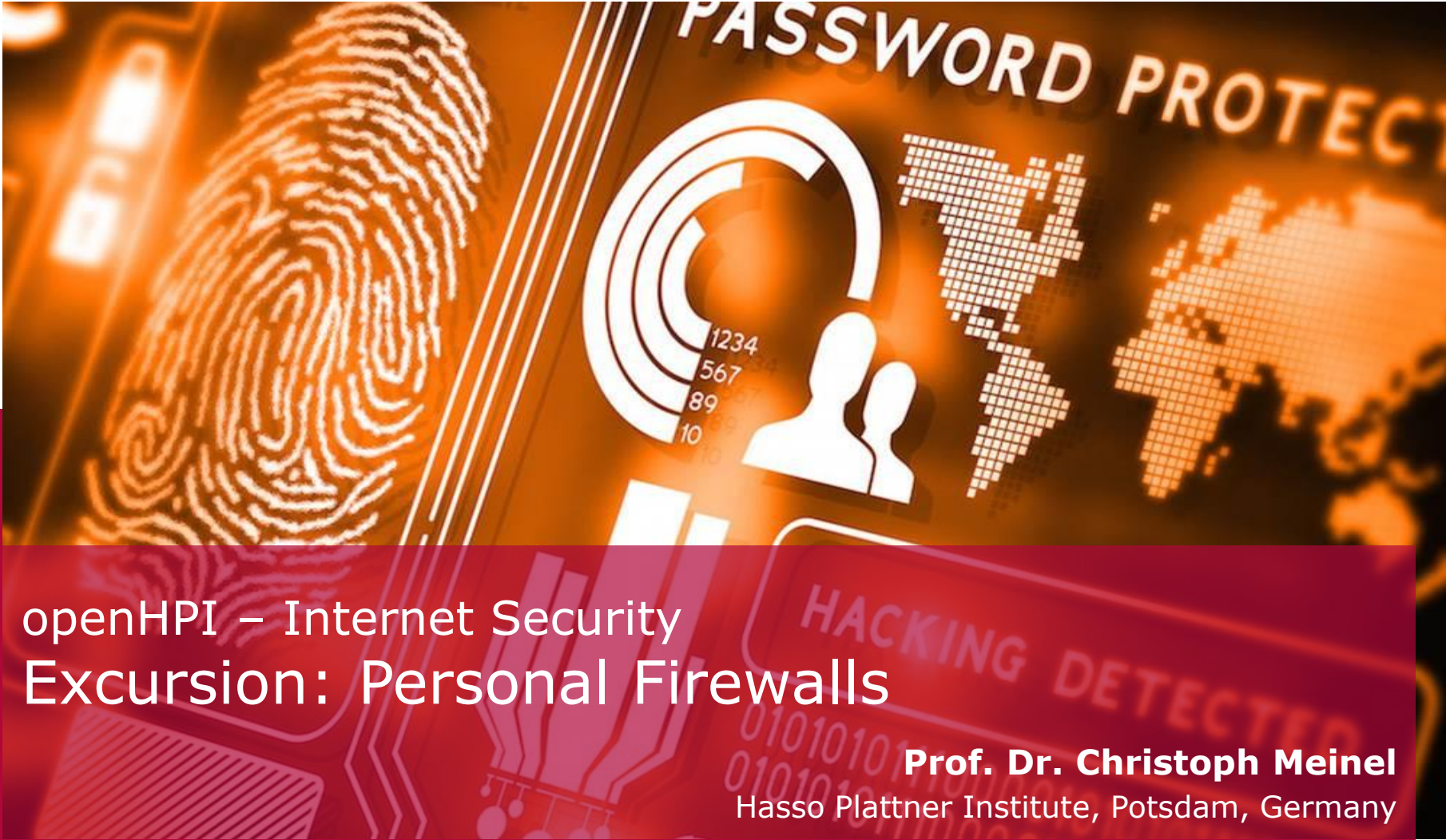


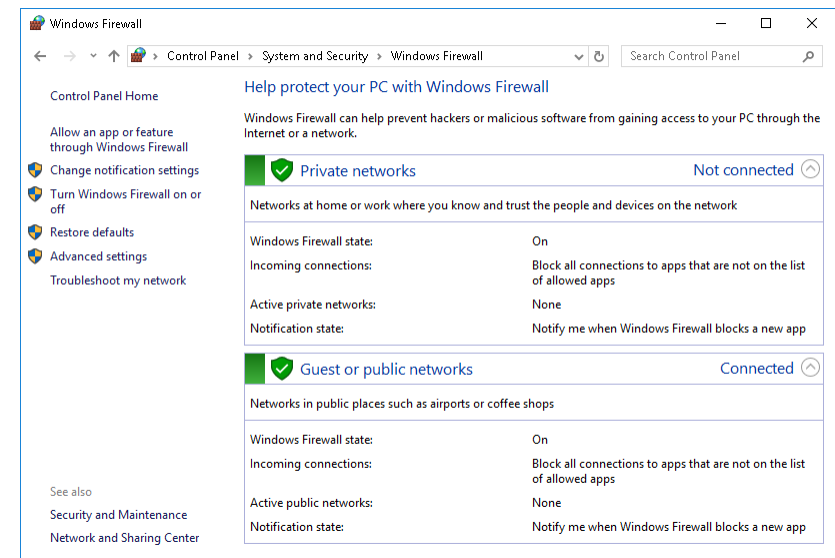


openHPI – Internet Security Excursion: Personal Firewalls

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

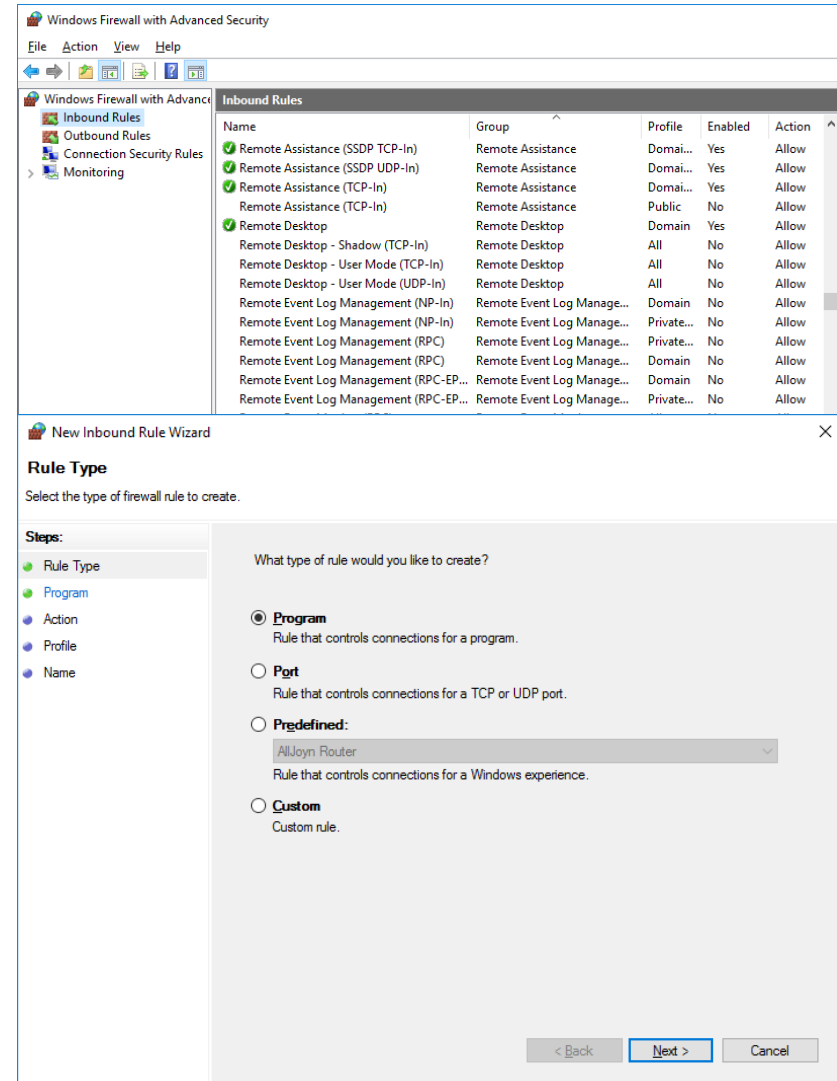
Windows Firewall (1/2)

- **Windows firewall** has been a standard component since Windows XP and Windows Server 2003
- Microsoft developed Windows firewall after disaster of "Blaster" and "Sasser" worm attacks and consequent criticism of the protection of Windows systems
- Has **network profiles** with different restrictions:
 - **Private networks**
 - Home or workplace networks
 - File and printer sharing, network recognition ...
 - **Guest or public networks**
 - Strong restrictions, incoming connections mostly not allowed



Windows Firewall (2/2)

- Active rules can be viewed, changed, and turned off
- Introduction of new rules:
 - program-based
 - port-based
 - predefined
 - user defined



Establishing a Rule to Block a Particular Program (1/4)

Navigate to

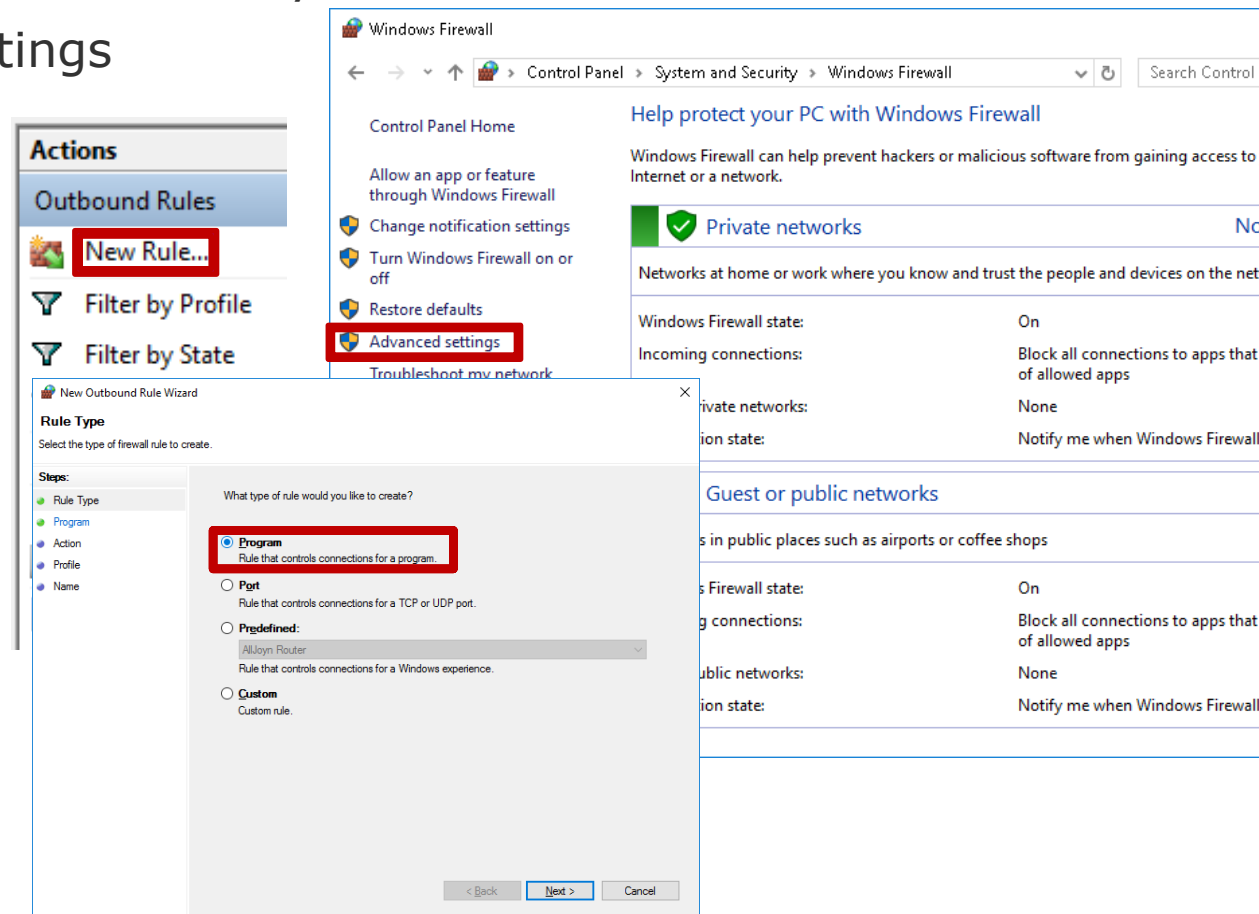
Control Panel → System and Security → Windows Firewall

- Call up Advanced settings

- Create new rule:

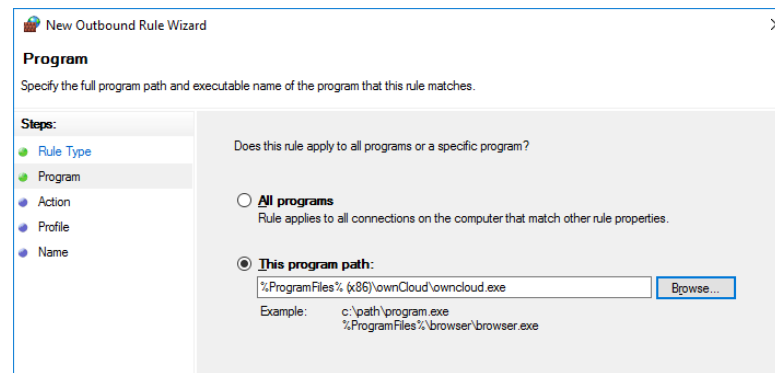
- ☐ program-based
- ☐ port-based
- ☐ predefined
- ☐ user defined

- We have chosen **program-based** for our example

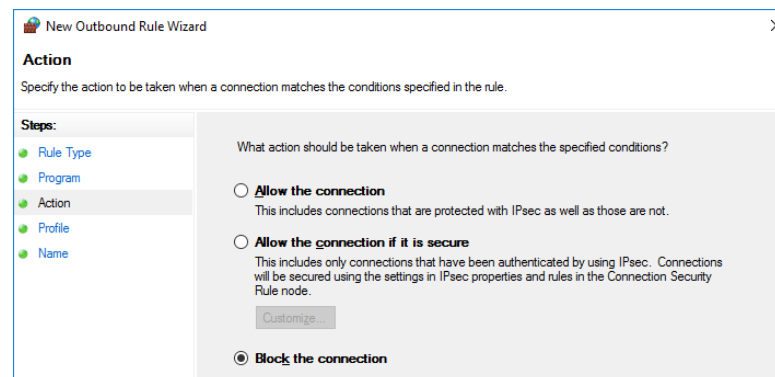


Establishing a Rule to Block a Particular Program (2/4)

- Select the respective program
 - Selection along the installation path, e.g. ownCloud

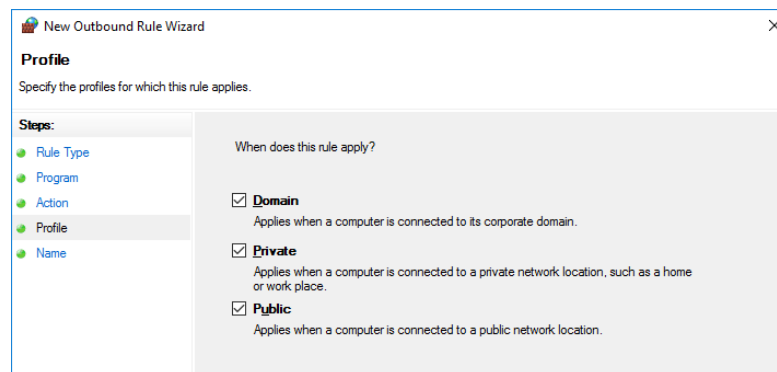


- Select the action to be performed, e.g. "Block the connection"

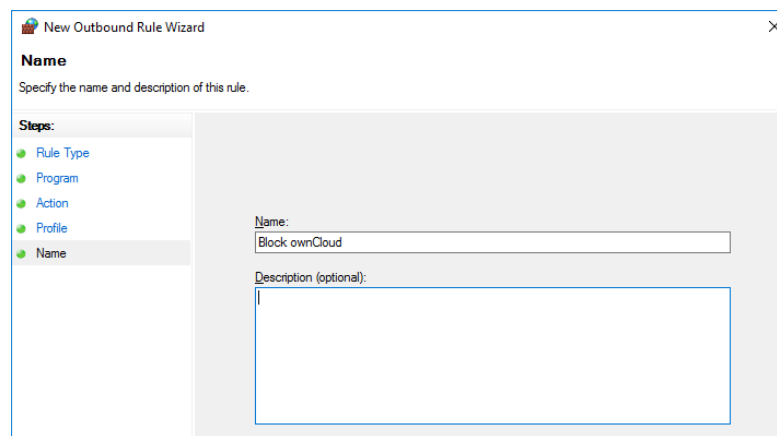


Establishing a Rule to Block a Particular Program (3/4)

- Select the types of networks to which the rule is to be applied

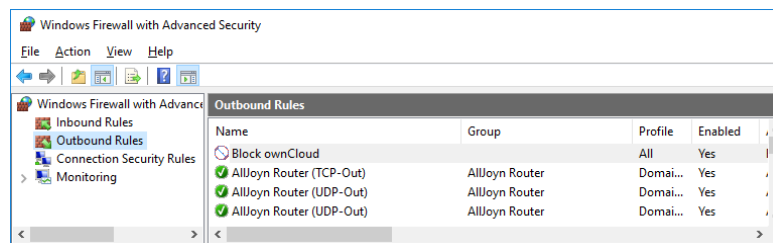


- Finally, name of the rule and optional description specified



Establishing a Rule to Block a Particular Program (4/4)

- Rule is now active and prohibits outgoing connections of the ownCloud application



- ownCloud application can no longer connect to the server

