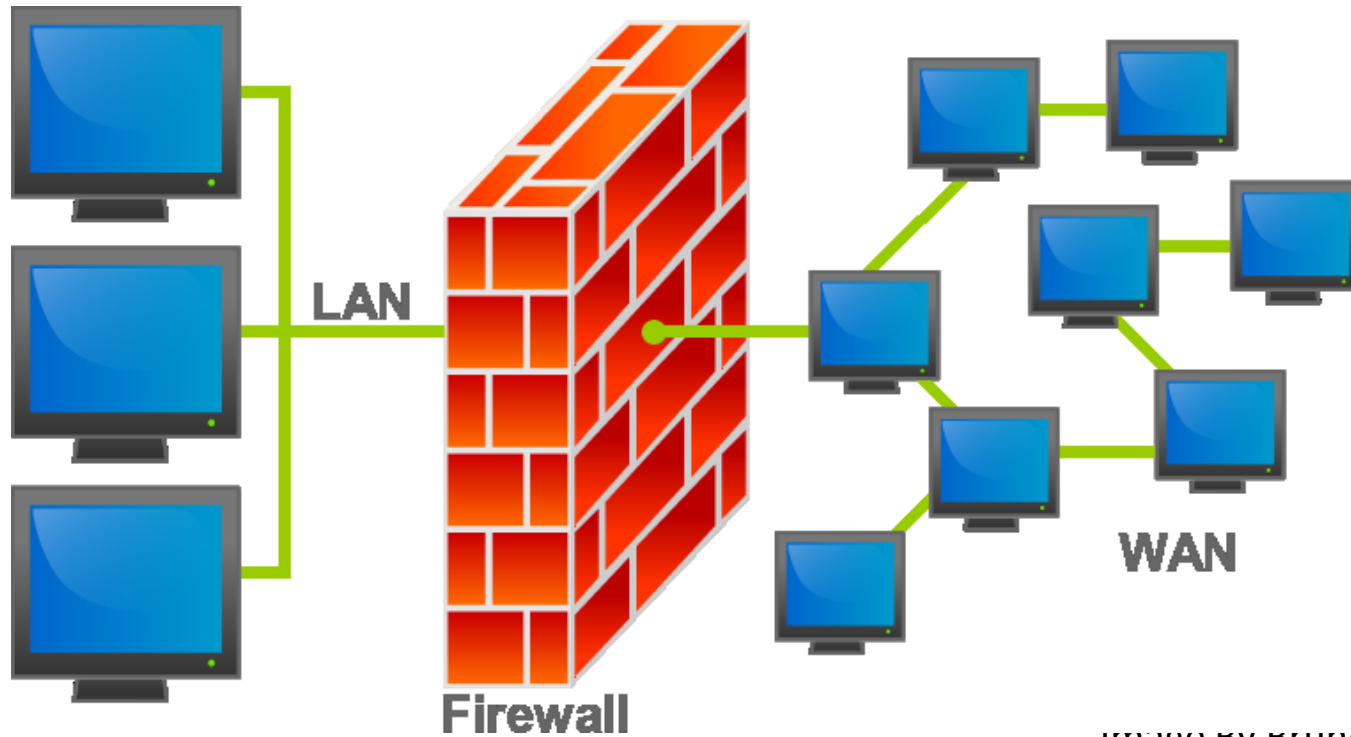


Firewalls

Defining Firewalls

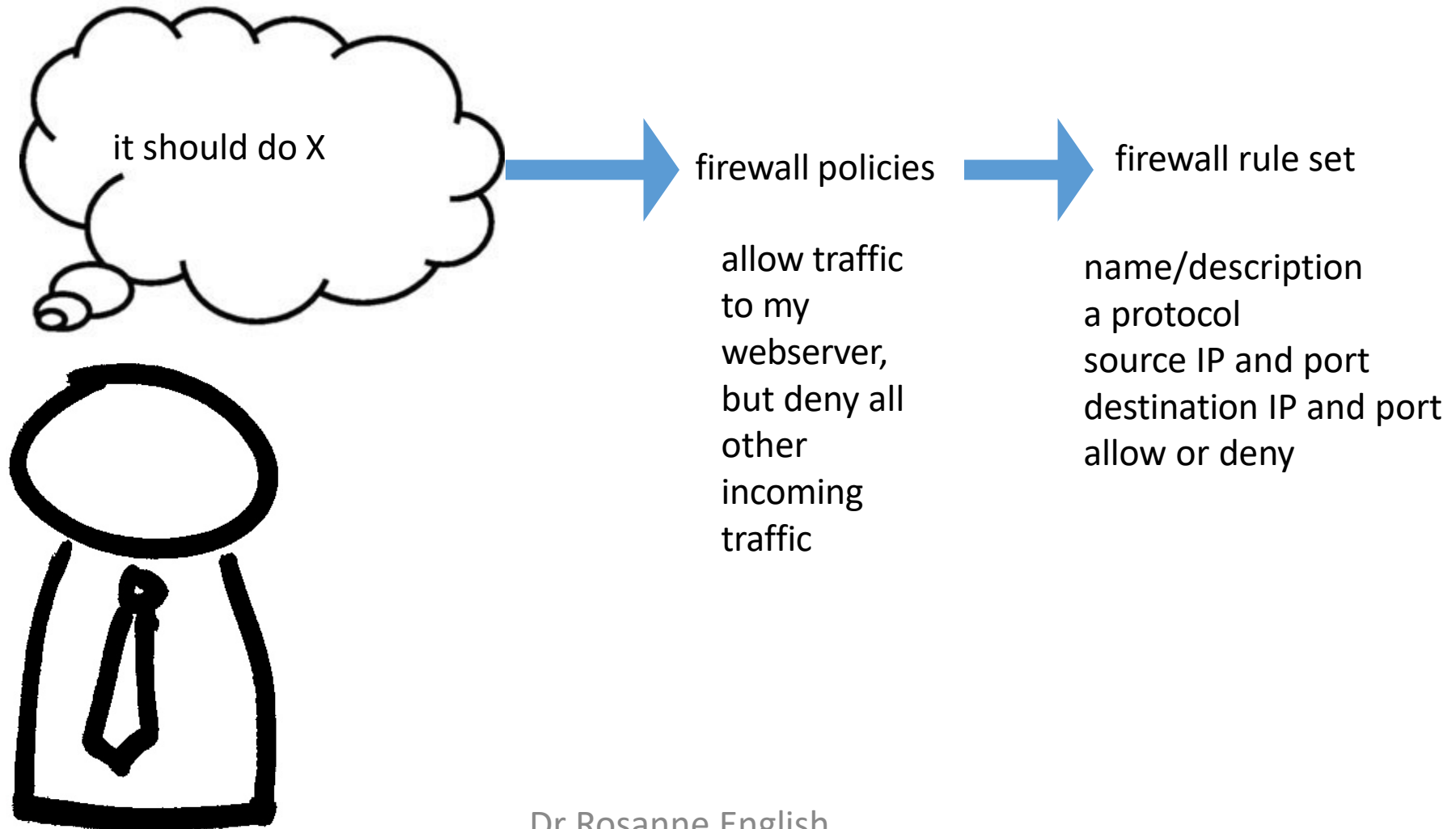
- Aim to protect your network and devices connected to it
- Any security system protecting the boundary of an internal network
- Typically uses packet filters and/or proxies



Packet Filtering





- Can be based on
 - Source address e.g. packets from internet with internal IP
 - Destination address e.g. only allow packets to bastion host
 - Protocol e.g. Telnet, SSH etc. ports
- Custom rules – inbound/outbound
- Accepted | Denied | Dropped

Firewall policies and rule sets process



Firewall policies and rule sets

Only looks for requests from port 80 to port 80, but we could have HTTP requests from any port between 1024-65535

Outbound Firewall Rules (Drag and drop rows to change rule order) ?					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
<u>Bad Rule</u>	TCP	Any 80	24.180.49.139 80	Deny	 
<u>Good Rule</u>	TCP	Any Any	24.180.49.139 80	Deny	 
<u>Default</u>	Any	Any	Any	Allow	
<div>Add Rule</div>					

Dr Rosanne English

Rules Image from used under fair use [Properly configuring your firewall rules image](#)

Good or bad rules?

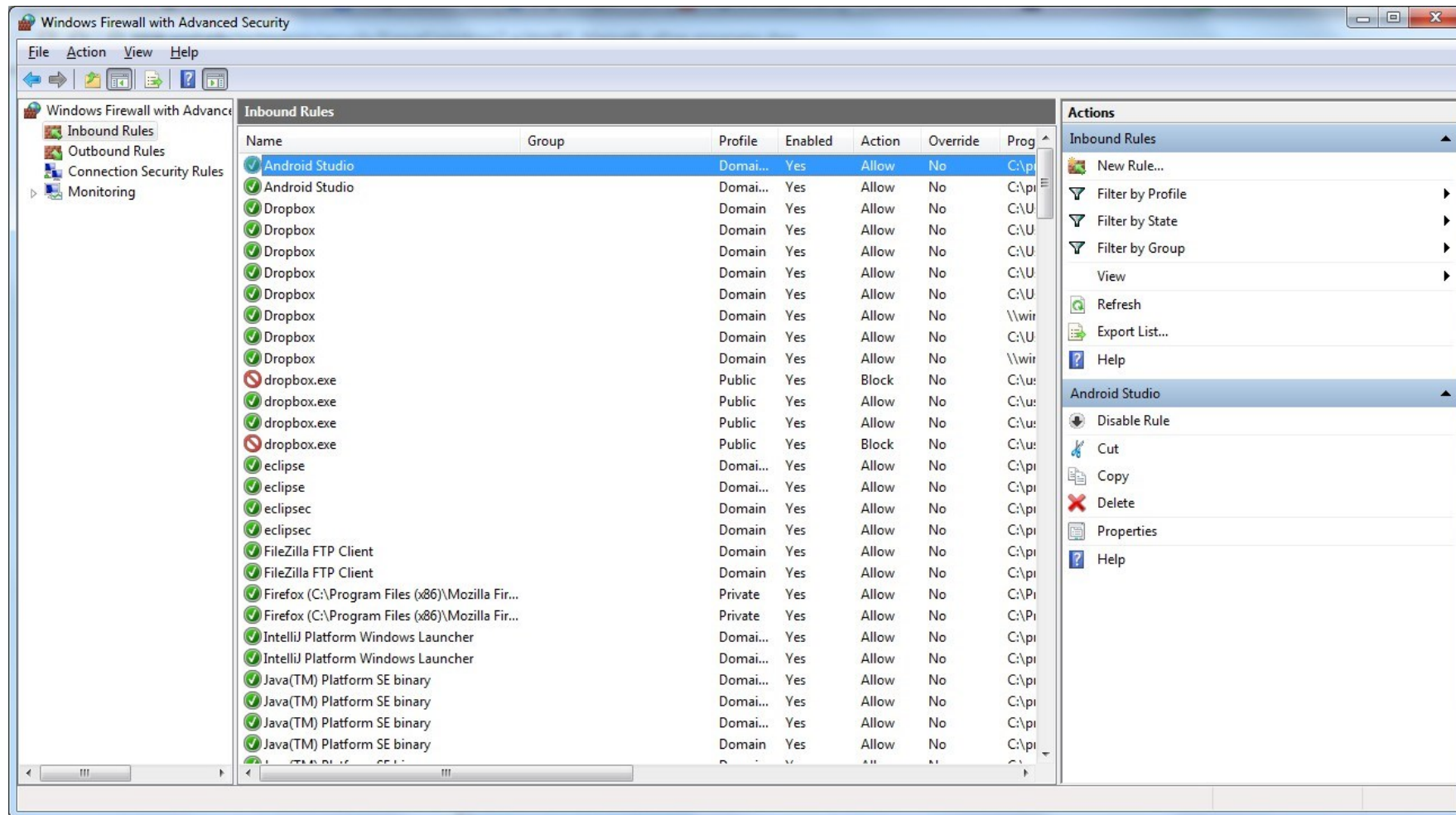
- Conflating policies
- Default rule



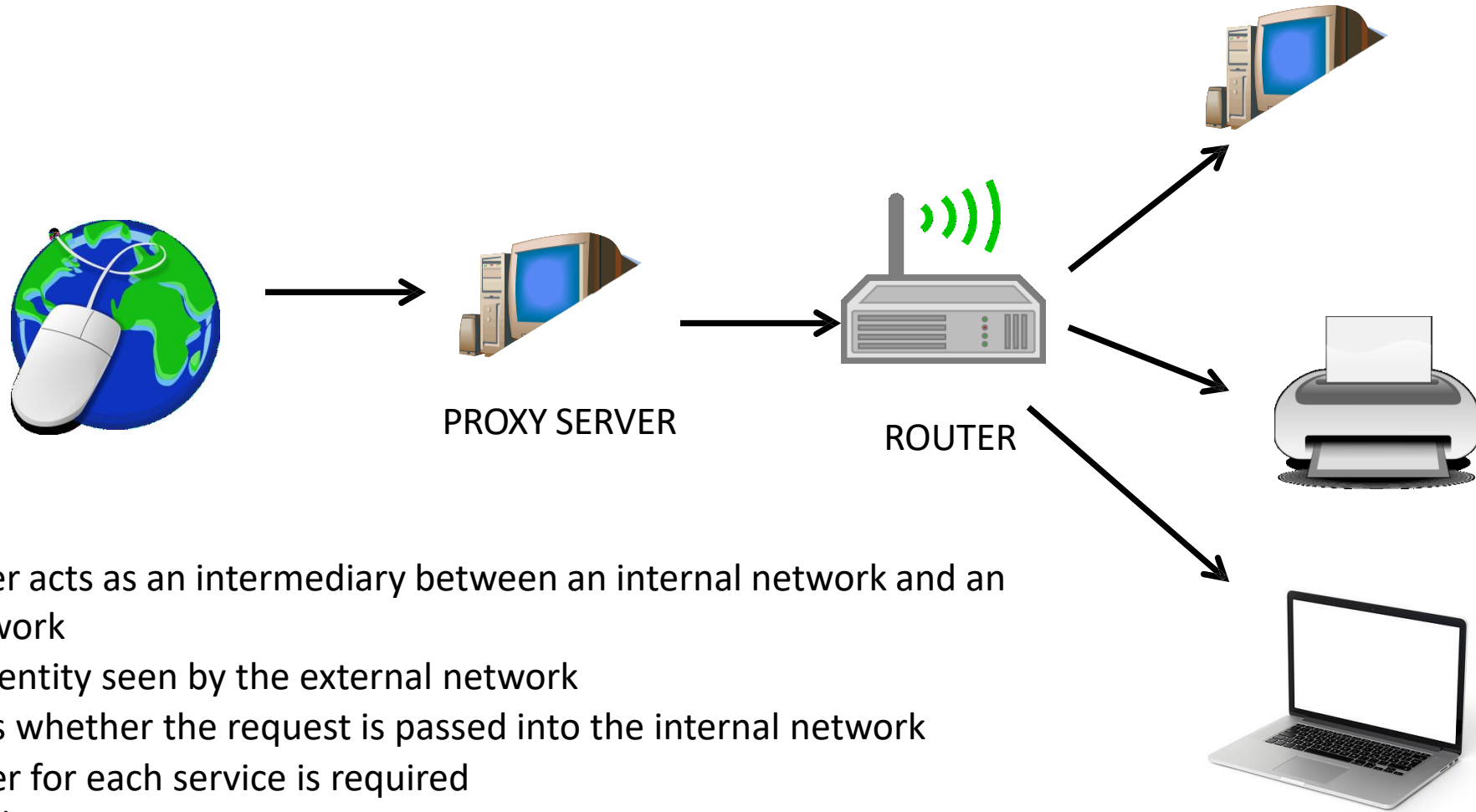
Common Policies

- Deny everything which hasn't been specifically allowed (white listed)
- Allow everything not specifically denied (black listed)

Windows Firewall



Proxies



A proxy server acts as an intermediary between an internal network and an external network

It is the only entity seen by the external network

It determines whether the request is passed into the internal network

A proxy server for each service is required
outside world

Proxy Firewall Operations

- Host IP address hiding
- Header destruction
- Protocol enforcement