Network Firewall

A firewall defines a logical defense parameter
and acts an access control between two networks

➡ Packet filtering based on IP addresses (TCP filtering)

- inbound traffic from the Internet trying to get into the protected network
- outbound traffic going the other way

✓ For the most part, we trust the outbound but not the inbound

Widely used in practice

Assuming the attacks comes from outside, a firewall can prevent

- Most scanning attacks
- Some spoofing attacks
- Some flooding attacks (as long as it can handle the load)
- Anomalous messages e.g smurf attack
- and others

➡ But more generally, it can restrict access to protected hosts