Network and Host Enumeration

Phases of the Intrusion Kill Chain

Research, identification, and selection of targets

Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems

The weapon installs a backdoor on a target's system allowing persistent access

Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.

The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

nmap

- **`nmap`** --> Network Mapper is a free and open source utility for network discovery and security auditing

- Useful for tasks such as network inventory, monitoring hosts

nmap

- **nmap** uses raw IP packets in novel ways to determine what
  - Hosts are available on the network
  - Services those hosts are offering (ports/applications/versions)
  - Operating systems the hosts are running
  - Type of firewall and packet filters are in use
  - **nmap** runs on all major computer operating systems

nmap

- Network enumeration: `nmap -PR -sn <network>`
- Host reconnaissance: `nmap -sT <host>`

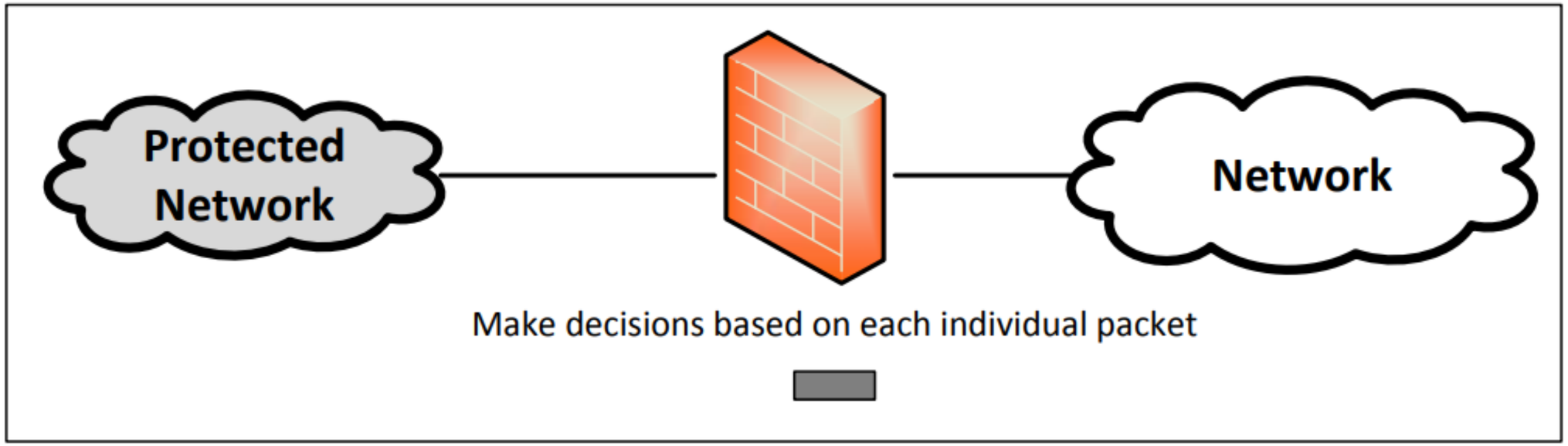
Firewall

Concept

- Direction
  - Ingress
  - Egress

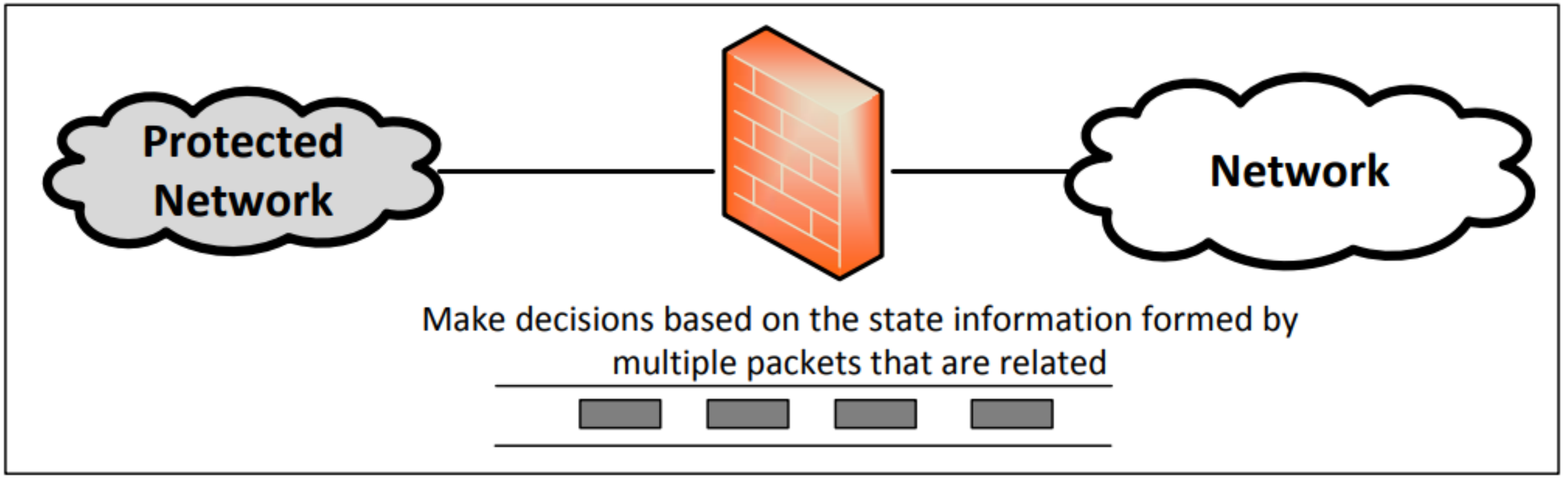
- Types
  - Packet Filter
  - Stateful Firewall
  - Application/Proxy Firewall

Packet Filter



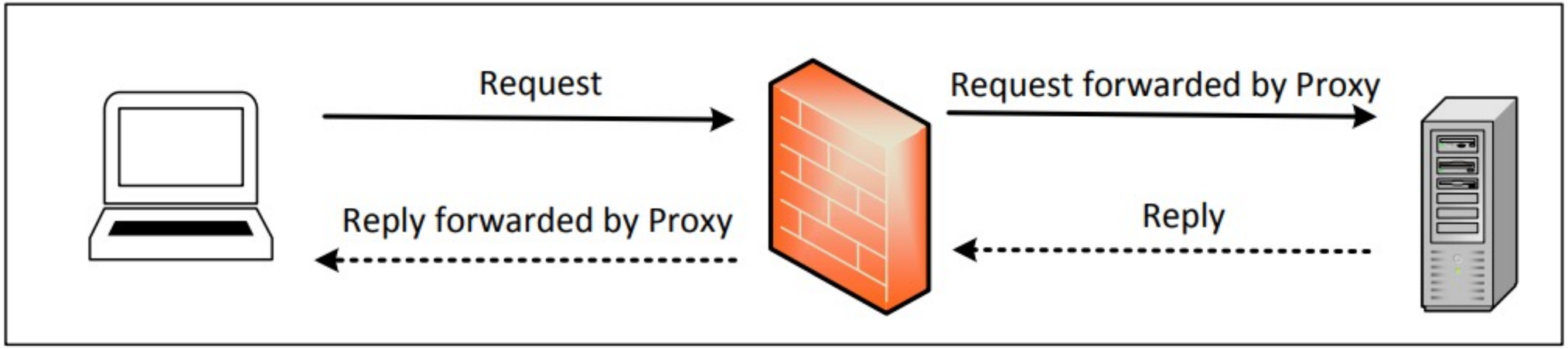
(A) Packet Filter Firewall

Stateful Firewall



(B) Stateful Firewall

Application/Proxy Firewall



(C) Application/Proxy Firewall