Chapter 8

PIX Firewall

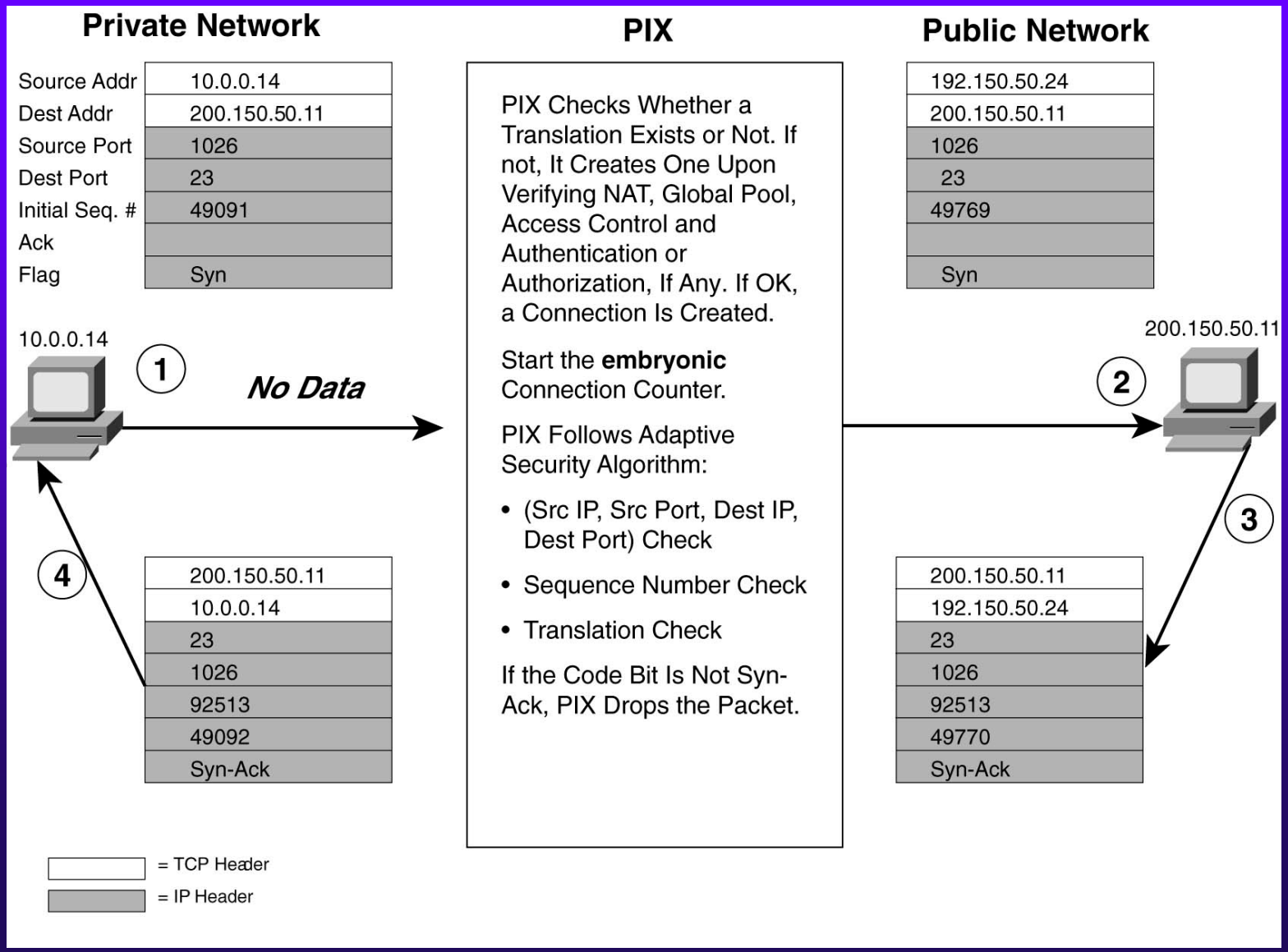
Adaptive Security Algorithm (ASA)

- Used by Cisco PIX Firewall
- Keeps track of connections originating from the protected inside network to the outside public network so that return traffic with connection is allowed
- All other traffic from the outside public network is blocked by firewall

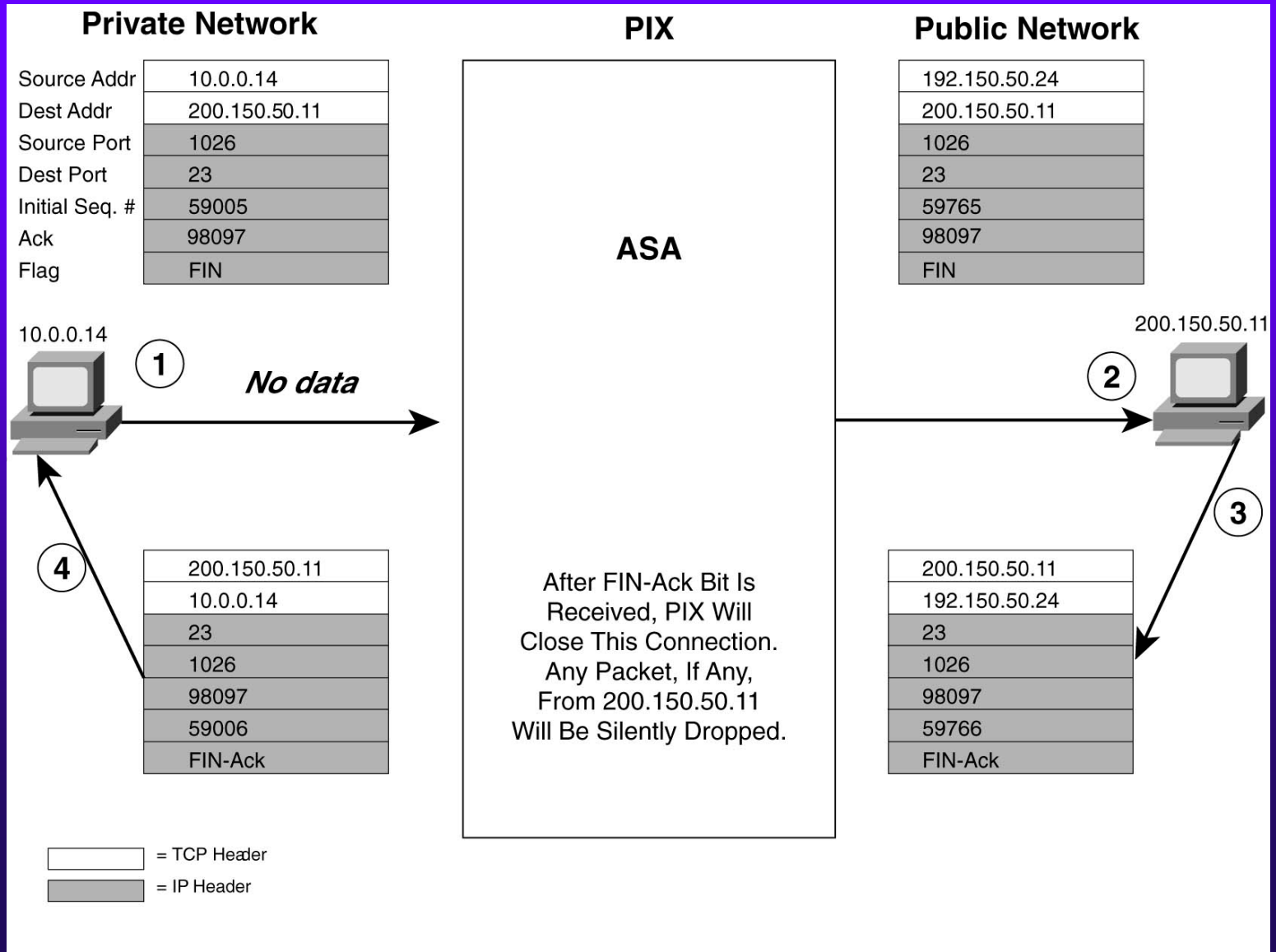
Adaptive Security Algorithm (ASA)

- Used by Cisco PIX Firewall
- Keeps track of connections originating from the protected inside network to the outside public network so that return traffic with connection is allowed
- All other traffic from the outside public network is blocked by firewall

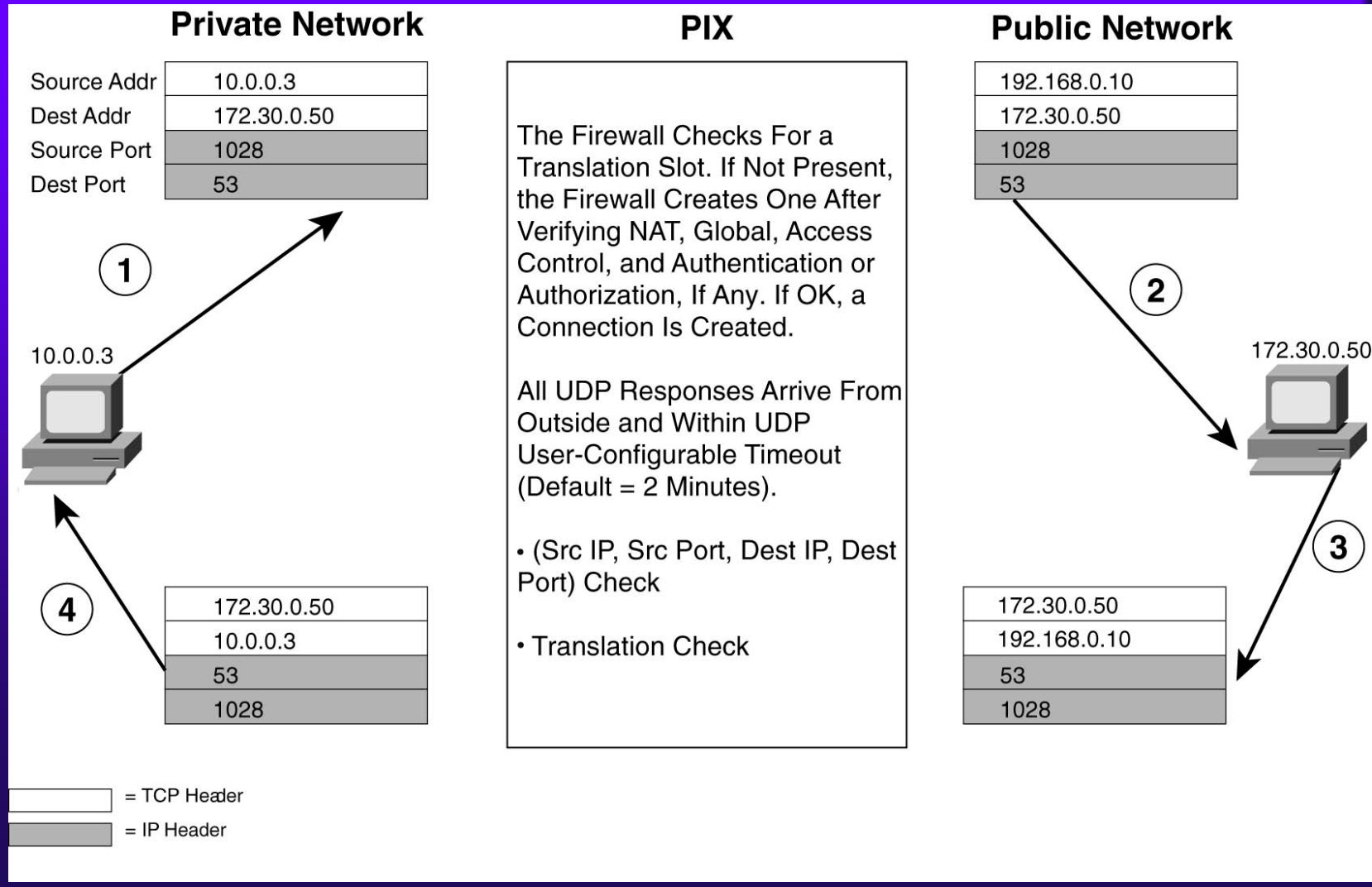
TCP Connection Setup



TCP Connection Teardown



UDP Transmission



Default PIX Firewall Rules

- Packets cannot traverse the PIX Firewall without a translation, connection, and state
- Outbound connections (originating from higher security interface and destined to lower security interface) are allowed except those specifically denied by ACLs
- Inbound connections are blocked except those specifically permitted
- All ICMP packets are denied unless explicitly permitted

PIX Interface Security Levels

- Each interface is assigned a security level from 0 to 100
  - Security level 100 usually assigned to interface connected to the inside private network
  - Security level 0 usually assigned to outside public interface
- By default, traffic can flow from a higher security level to a lower security level provided that a NAT (xlate) is built for the source IP address
- connections from lower security interface to a higher security interface must be explicitly permitted via ACL or conduit

Network Address Translation

- NAT must be set up in order to pass traffic between any two interfaces
- PIX can also support PAT
- Dynamic NAT versus Static NAT

Other Features of PIX

- Can act a an inline IDS
- Can provide stateful failover to a redundant PIX
- Application awareness implement via “fixup” commands

PIX Configuration

- See Cisco PIX Firewall and VPN configuration guide

Access Control Lists

- Used to permit connection originating from a less secure interface (eg. Outside) to a more secure interface (eg. Inside)
- Used in conjunction with static NAT traslation