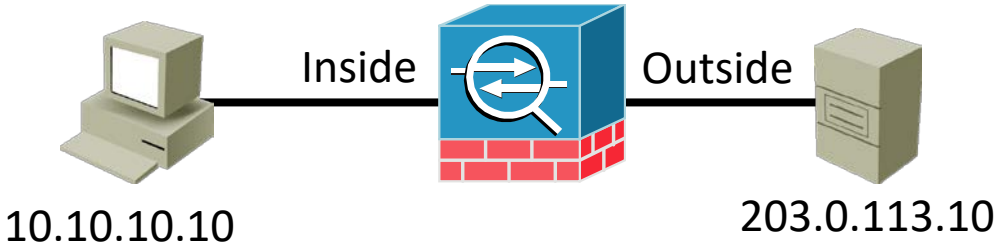
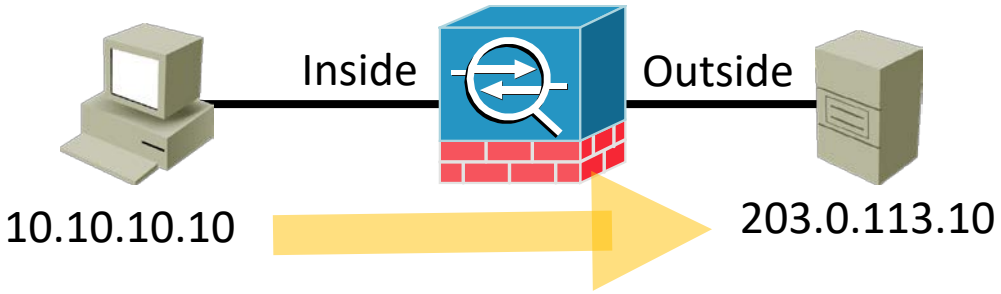
# How Stateful Firewalls Work

- Firewalls secure traffic passing through them by either permitting or denying it
- Stateful firewalls maintain a connection table which tracks the two-way 'state' of traffic passing through the firewall
- Return traffic is permitted by default
- Firewall rules example:
  - Deny all traffic from outside to inside
  - Permit outbound web traffic from 10.10.10.0/24

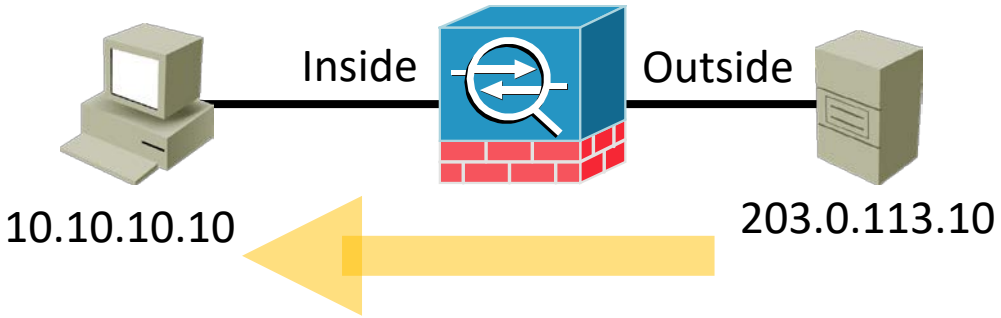


# How Stateful Firewalls Work



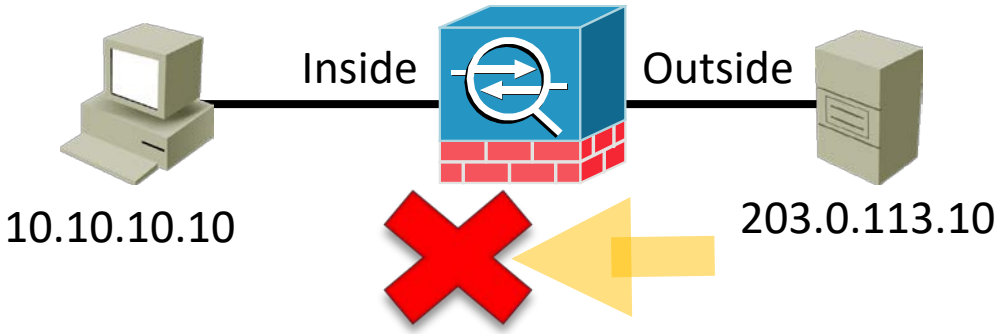

- Traffic is allowed by ‘Permit outbound web traffic from 10.10.10.0/24’ rule
- Connection table: 10.10.10.10:49160 > 203.0.113.10:80

# How Stateful Firewalls Work




- Traffic from 203.0.113.10:80 > 10.10.10.10:49160 is permitted because it is valid return traffic for a connection in the connection table
- This overrides the ‘Deny all traffic from outside to inside’ rule

# How Stateful Firewalls Work




- In this example the connection has not been initiated from the host on the inside
- Traffic from 203.0.113.10:80 > 10.10.10.10:49160 is dropped according to the ‘deny all traffic from outside to inside’ rule

# Next Generation Firewalls

- Next Generation Firewalls move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and user based security
- Deep packet inspection analyses packets up to layer 7 of the OSI stack
- Different permissions can be applied to different users
- The Cisco ASA with FirePower is a Next Generation Firewall

# How Packet Filters Work

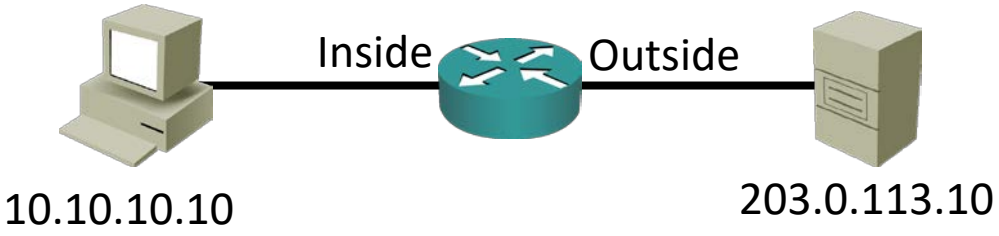
- An Access Control List security policy is a packet filter
- Packet filters do not maintain a connection table
- They affect traffic in one direction only and do not track the state of two way connections going through the router

# How Packet Filters Work

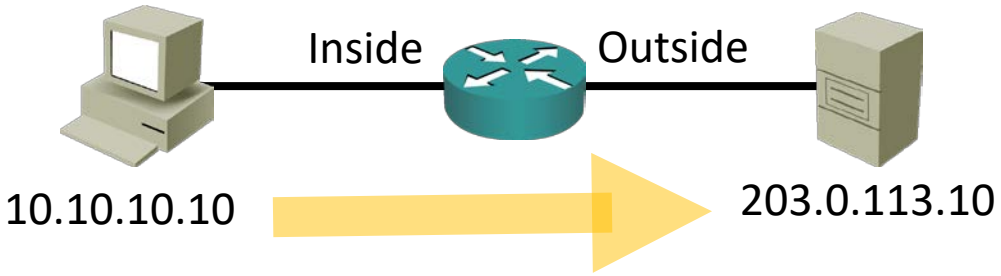
- If you have an ACL applied on the way out only, the return traffic will be allowed because all traffic is allowed when an ACL is not applied
- If you have ACLs applied in both directions, you will need explicit entries to allow both the outbound and the return traffic

# How Packet Filters Work

- Access Control List example:
  - Inbound ACL on outside interface: Deny all traffic
  - Inbound ACL on inside interface: Permit web traffic from 10.10.10.0/24

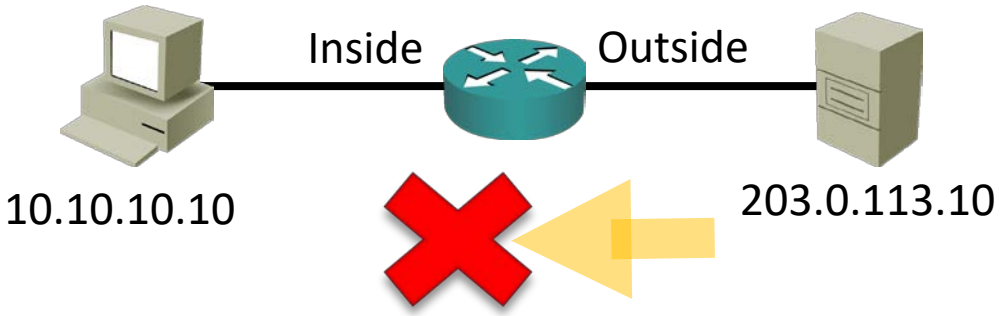


# How Packet Filters Work



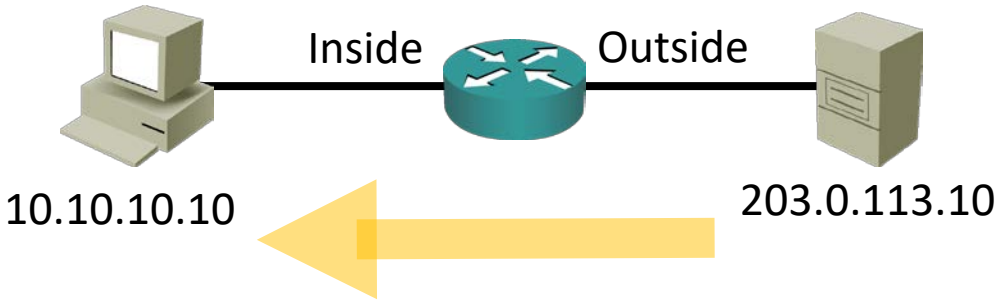

- Inbound ACL on inside interface: Permit web traffic from 10.10.10.0/24 allows traffic out to the web server
- The connection is not tracked in a connection table

# How Packet Filters Work




- Traffic from 203.0.113.10:80 > 10.10.10.10:49160 is dropped because of Inbound ACL on outside interface: Deny all traffic

# How Packet Filters Work




- To allow the return traffic you need to remove the ‘deny all traffic from outside to inside’ ACL on the outside interface
- Or add ‘permit tcp any eq 80 10.10.10.0 0.0.0.255 range 49152 65535’
- Neither is a secure option for a router connected to the Internet

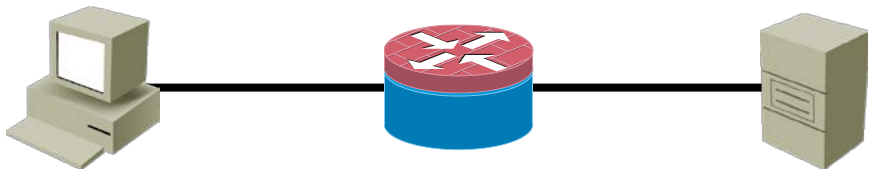
# The ‘Established’ Keyword

```
R1(config)#access-list 100 permit tcp any eq 80
10.10.10.0 0.0.0.255 established
```

- The Established keyword in an ACL only checks for the ‘Ack’ flag in return traffic
- This does not make the router a stateful firewall and it still does not keep a connection table!

# IOS Firewall

- You can configure a router as a stateful firewall with the IOS Firewall feature set
- This uses different commands than ACLs



# Internal and External Threats

- ACL packet filters on routers can add to an overall defence in depth strategy
- Standard practice is to use firewalls on major security boundaries, and augment this with internal ACLs
- Purely external threats are primarily covered with strong firewall and IPS protection on the network perimeter.
- Sensitive hosts should also have firewall and IPS protection from internal hosts

# Example Firewall and IPS Topology