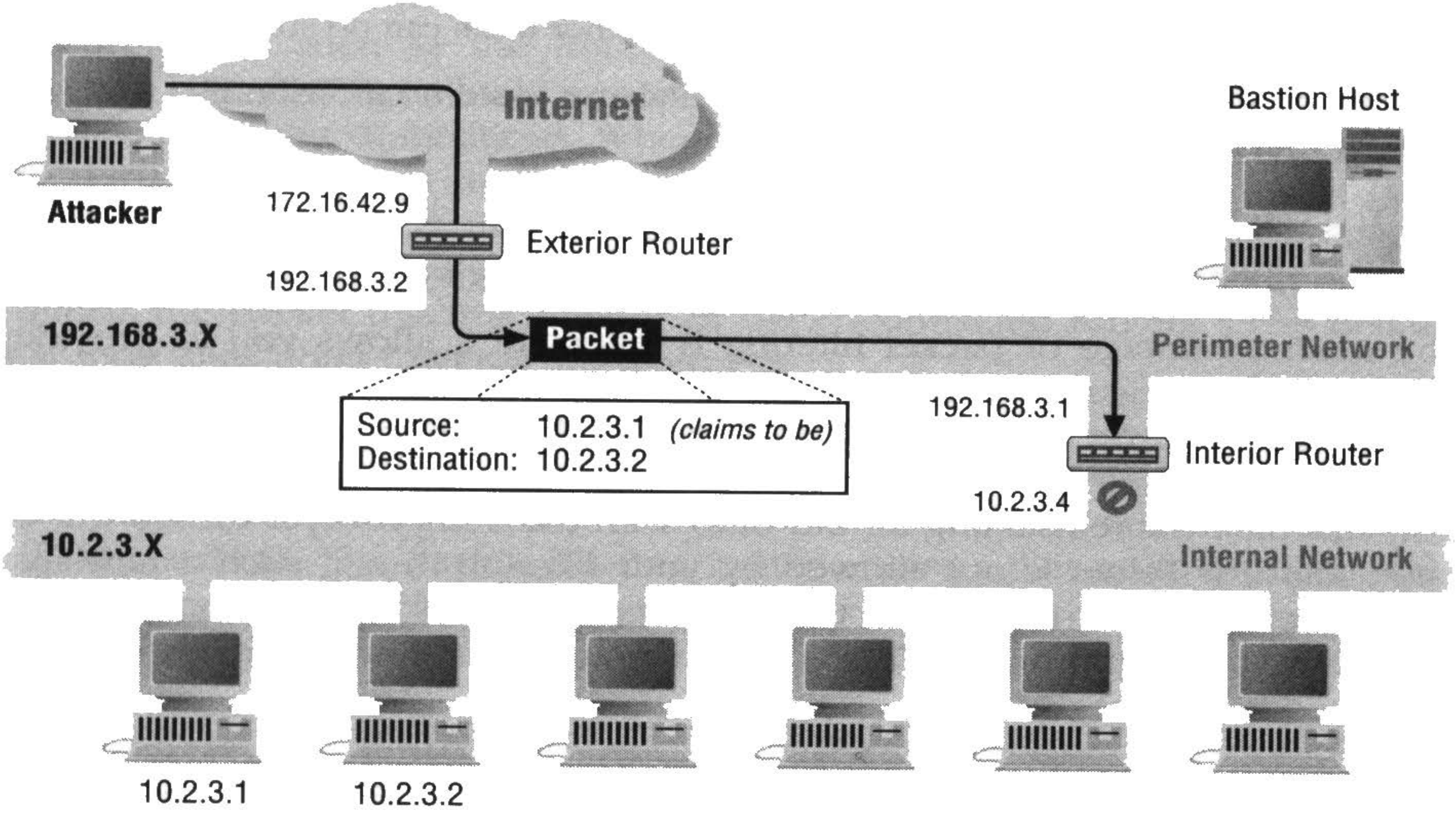
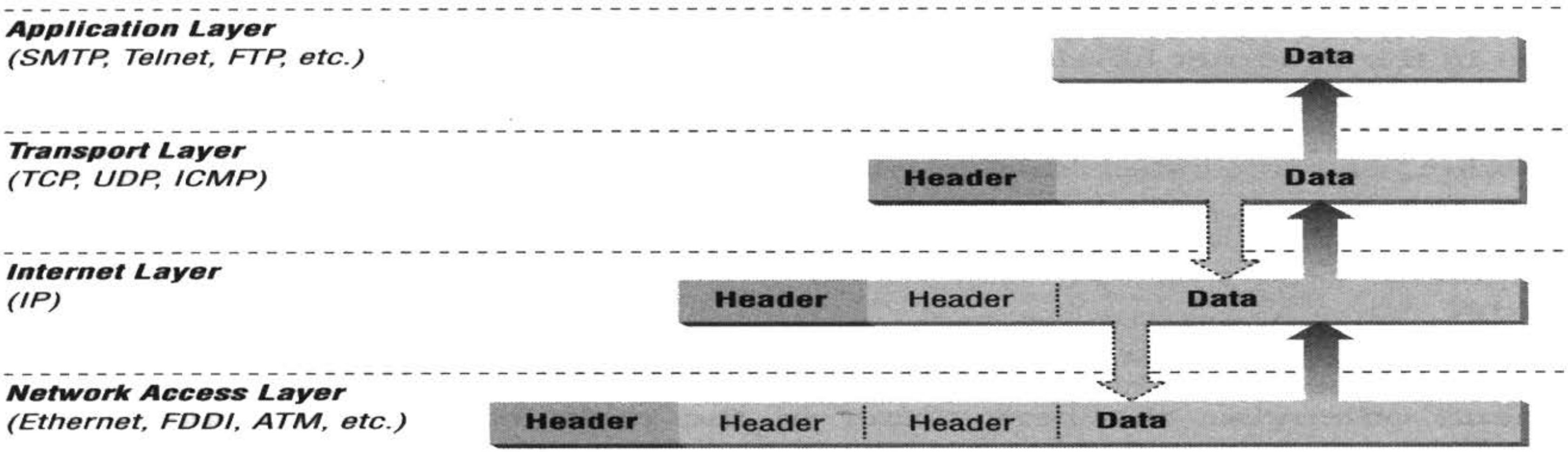
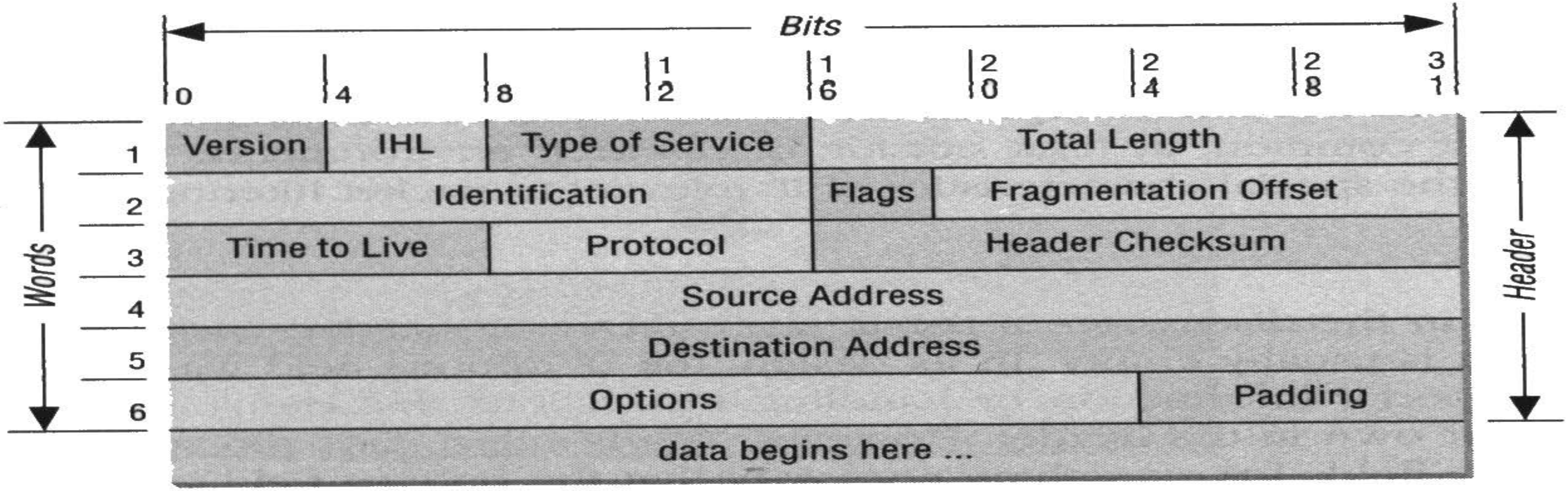
Packet Filtering

- Why?
  - Allow network-level filtering
  - Simple for routers
- Advantages:
  - One screening router can help protect an entire network
  - Does not require user knowledge or cooperation
  - Widely available in many routers
- Disadvantages:
  - Current filtering tools are not perfect
  - Some protocols are not well suited to packet filtering
  - Some policies can’t readily be enforced by normal packet filtering routers


Internet
Attacker
172.16.42.9
Exterior Router
192.168.3.2
Bastion Host
192.168.3.X
Packet
Perimeter Network
Source: 10.2.3.1 (claims to be)
Destination: 10.2.3.2
192.168.3.1
Interior Router
10.2.3.4
10.2.3.X
Internal Network
10.2.3.1
10.2.3.2





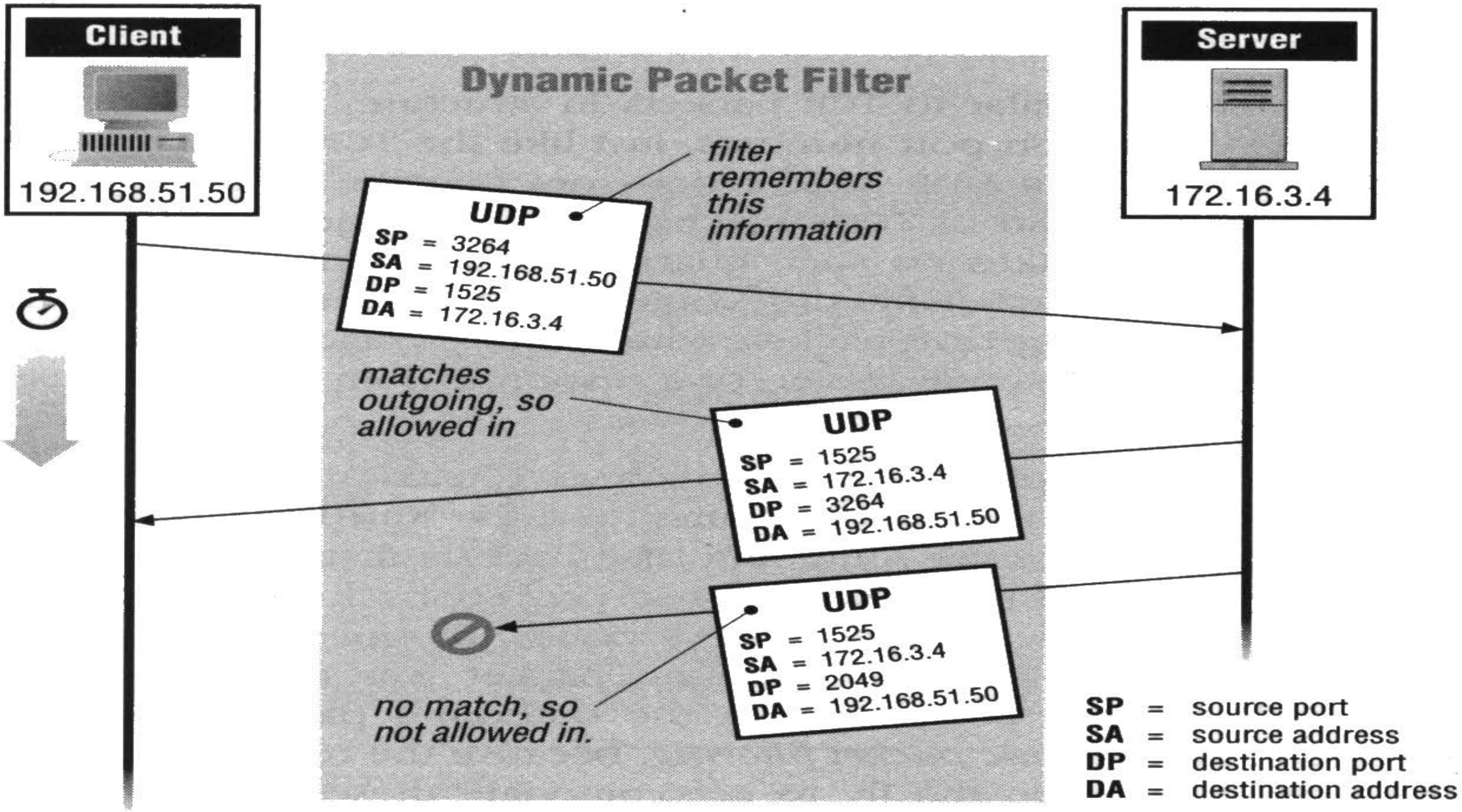
1	Version	IHL	Type of Service	Total Length	
2	Identification			Flags	Fragmentation Offset
3	Time to Live		Protocol	Header Checksum	
4	Source Address				
5	Destination Address				
6	Options				Padding
	data begins here ...				

What Does a Packet Look Like?

- IP Layer
  - IP source address
  - IP destination address
  - IP protocol type
  - IP options field
    - rarely used
    - source routing (where security problem could be)
- TCP Layer
  - TCP source port
  - TCP destination port
  - TCP flags field
    - ACK bit to indicate the first packet of a TCP connection

Security Issues on Fields

- IP
  - IP options (as describe above)
    - simply drop this field
  - IP fragmentation
    - only the first one has TCP header
    - Filter only the first one, and pass the rest
    - Security problems:
      - denial of service attack
      - figure out the existence from ICMP, so must remove ICMP for both directions.
- TCP
  - ACK bit (as described above)
- UDP
  - In order to figure out outbound services, match the last packet, called dynamic packet filtering.


Client
192.168.51.50
Server
172.16.3.4
Dynamic Packet Filter
UDP
SP = 3264
SA = 192.168.51.50
DP = 1525
DA = 172.16.3.4
filter remembers this information
matches outgoing, so allowed in
UDP
SP = 1525
SA = 172.16.3.4
DP = 3264
DA = 192.168.51.50
UDP
SP = 1525
SA = 172.16.3.4
DP = 2049
DA = 192.168.51.50
no match, so not allowed in.
SP = source port
SA = source address
DP = destination port
DA = destination address

What Does the Router Do with Packets?

Consider:

  - Pass the packet
  - Drop the packet

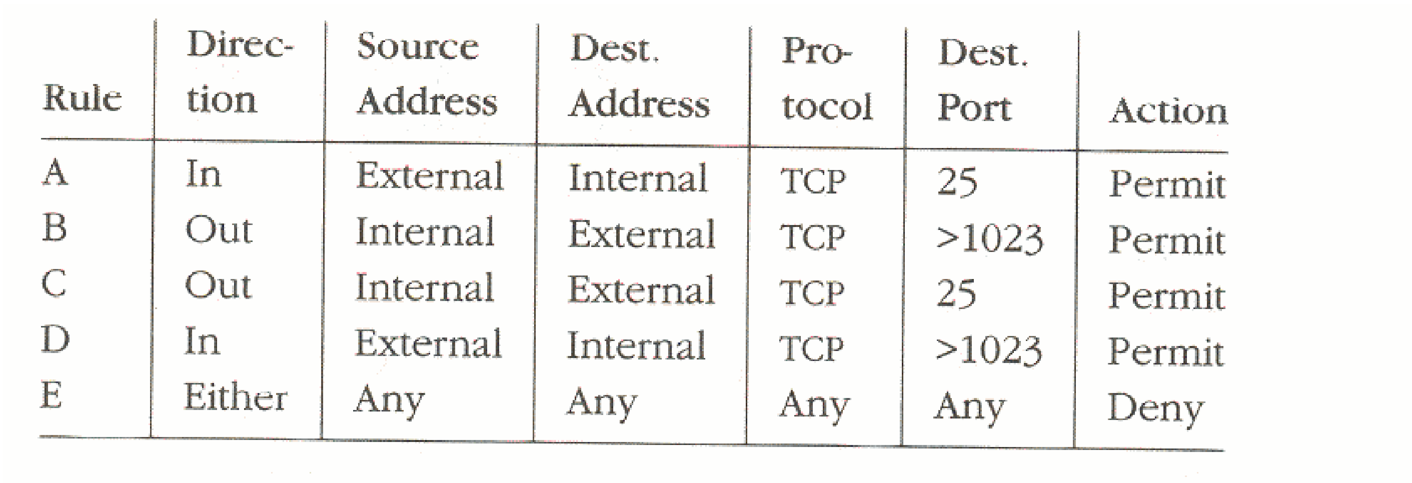
- Logging Actions
  - might log start-of-connection
  - log only specific information
- Returning ICMP Error Codes
  - Two types of ICMP Error codes
    - destination unreachable
    - destination administratively unreachable
  - Dilemma:
    - Return the first error code might kill other connections
    - Return the second error code which some new system do not support
  - Solution: Just do not generate any.

Example: Telnet

- Outbound Telnet services
  - Outbound packets
    - IP source address: internal
    - IP destination address: external
    - TCP protocol
    - destination port: 23
    - source port: >1023
    - first packet (not have ACK set)
  - Inbound packets
    - IP source address: external
    - IP destination address: internal
    - TCP protocol
    - destination port: >1023
    - source port: 23
    - all packets (have ACK set)

Case Study: SMTP

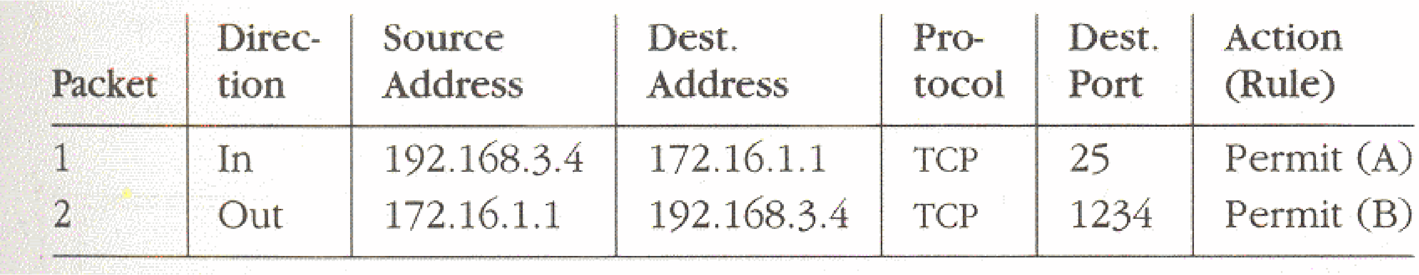
- Policy:
  - Allow inbound SMTP
  - Allow outbound SMTP
  - Allow nothing else.
- Rules



Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

  - Rules A&B: inbound SMTP connections. (incoming email)
  - Rules C&D: outbound SMTP connections (outgoing email)
  - Rule E: the default rule if all else fails.

Scenario 1



Packet	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action (Rule)
1	In	192.168.3.4	172.16.1.1	TCP	25	Permit (A)
2	Out	172.16.1.1	192.168.3.4	TCP	1234	Permit (B)

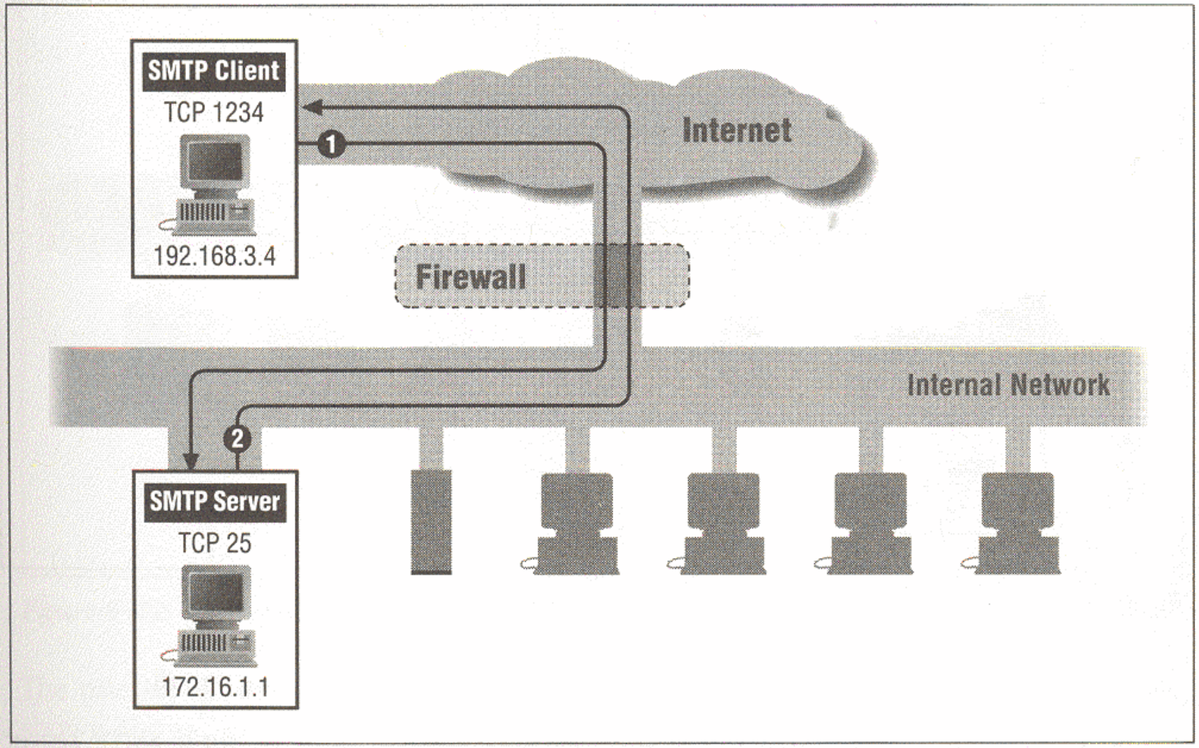
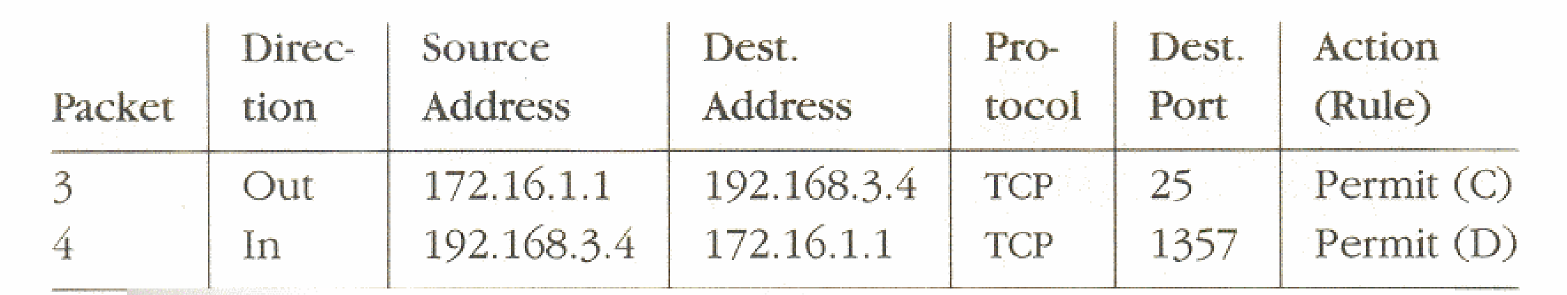


Figure 6–10: Packet filtering: inbound SMTP (sample packets 1 and 2)

Scenario 2



Packet	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action (Rule)
3	Out	172.16.1.1	192.168.3.4	TCP	25	Permit (C)
4	In	192.168.3.4	172.16.1.1	TCP	1357	Permit (D)

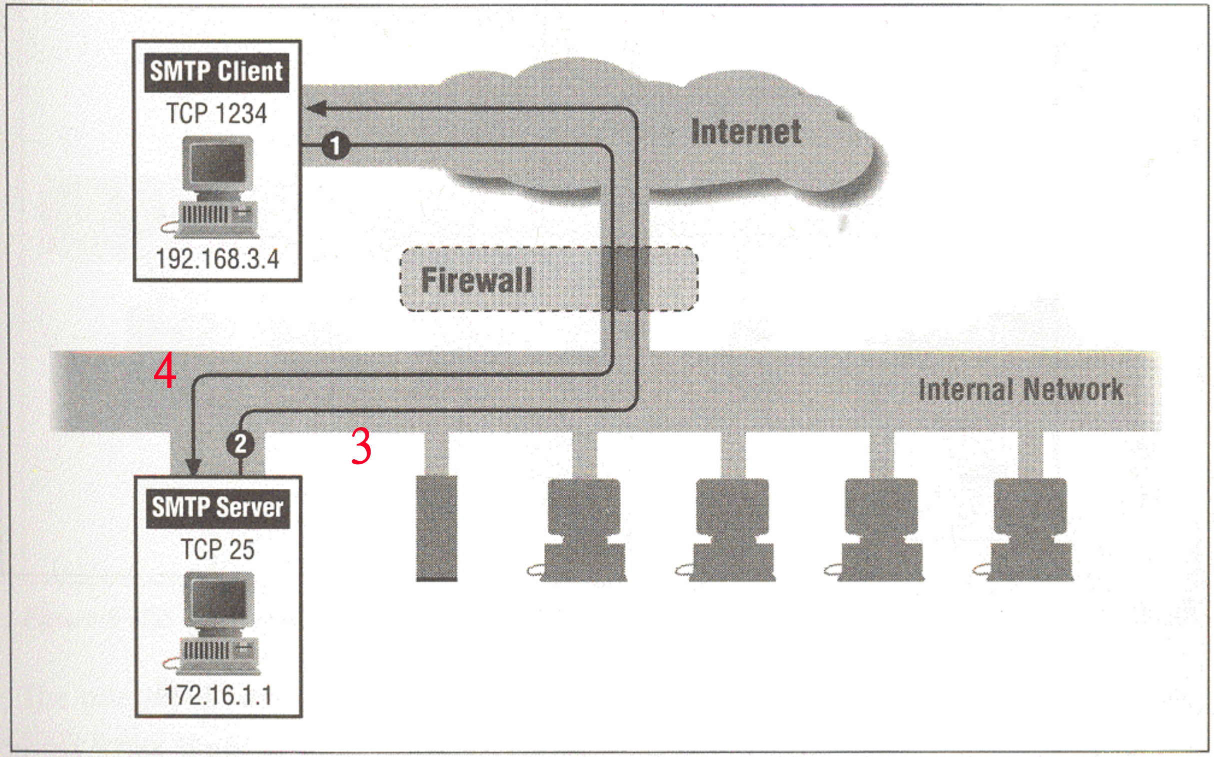
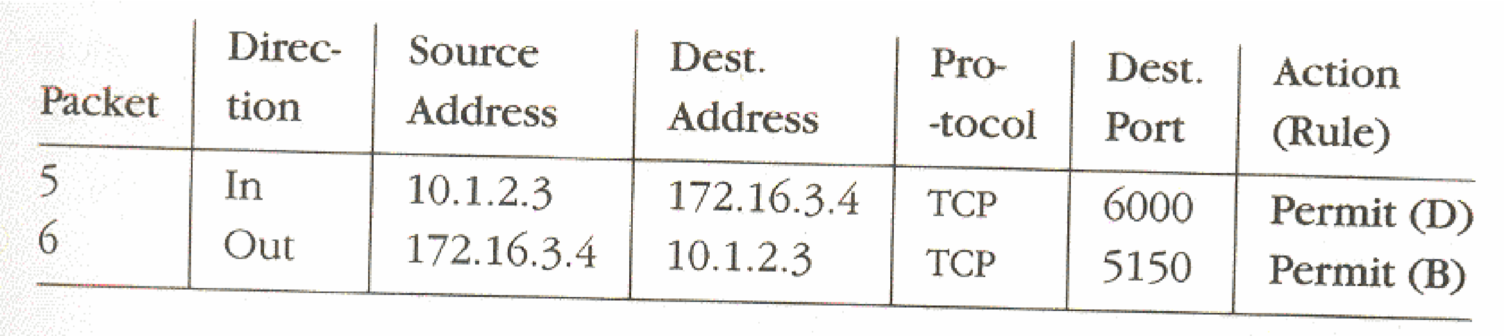


Figure 6-10: Packet filtering: inbound SMTP (sample packets 1 and 2)

Problem



Packet	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action (Rule)
5	In	10.1.2.3	172.16.3.4	TCP	6000	Permit (D)
6	Out	172.16.3.4	10.1.2.3	TCP	5150	Permit (B)

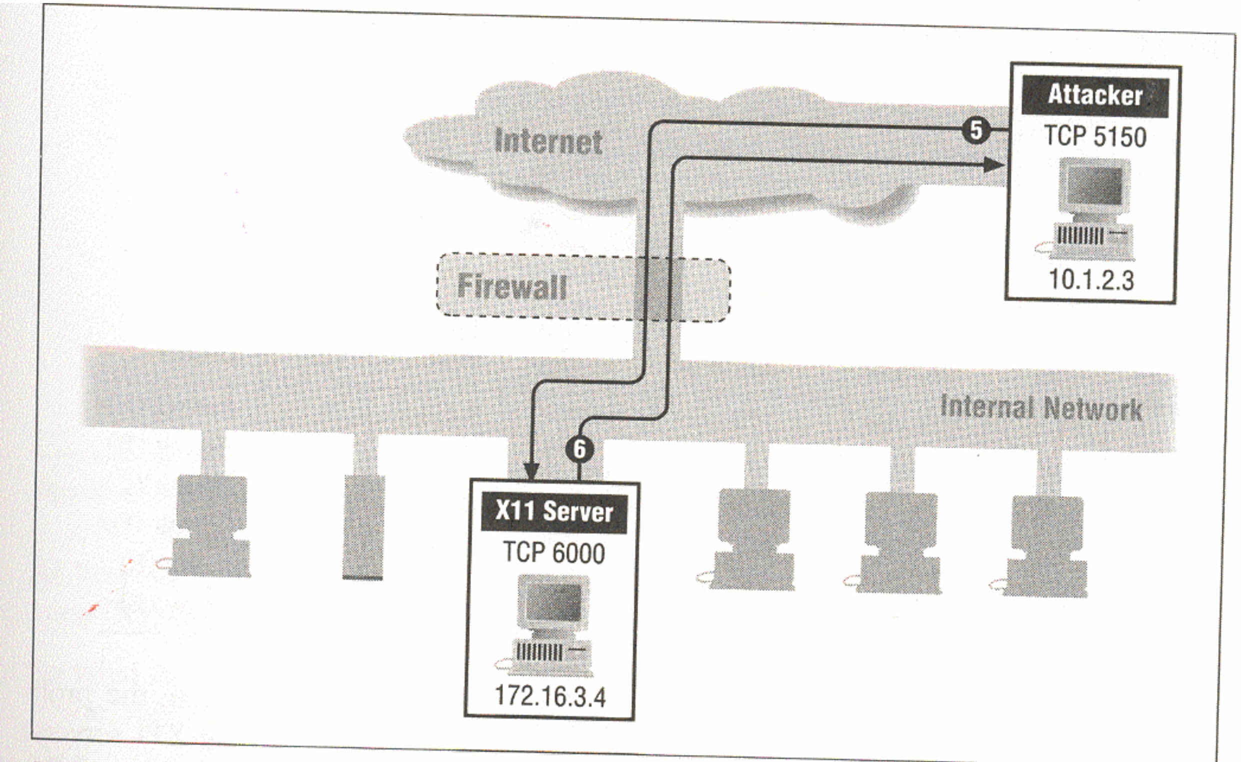
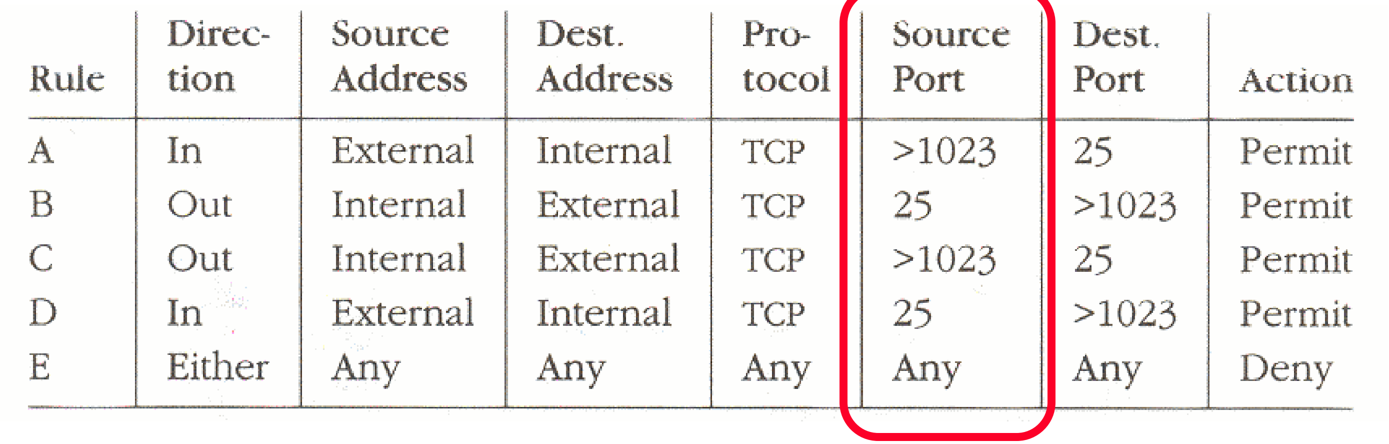


Figure 6-12: Packet filtering: inbound SMTP *(sample packets 5 and 6)*

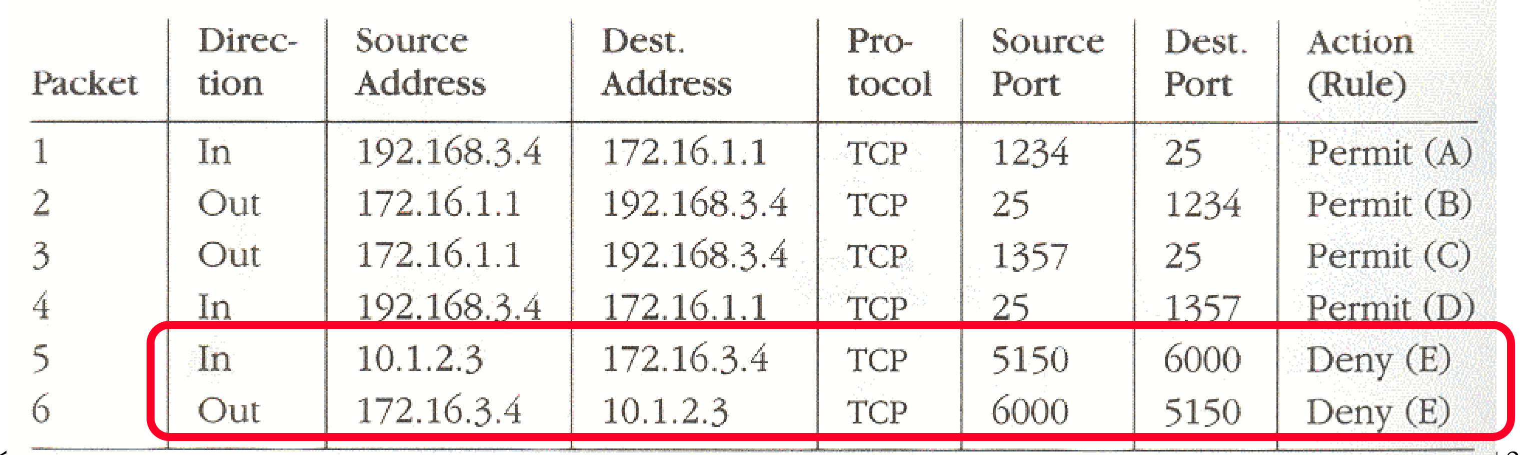
Change Rules

- Add “source port” field.



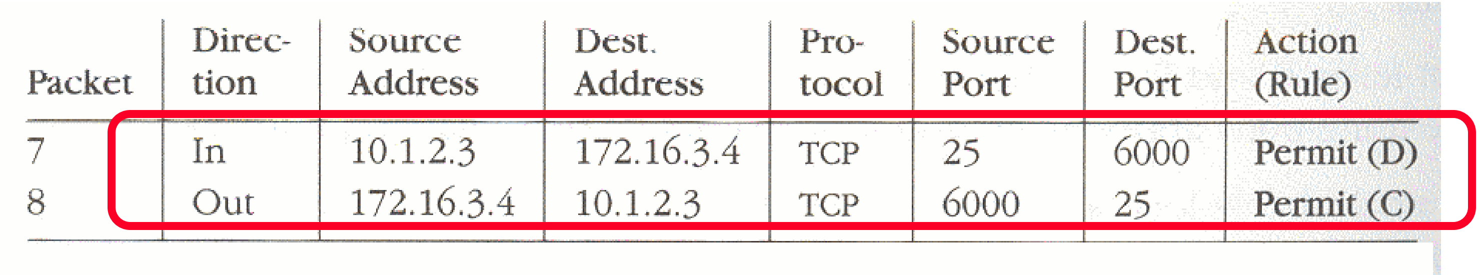
Rule	Direc-tion	Source Address	Dest. Address	Pro-tocol	Source Port	Dest. Port	Action
A	In	External	Internal	TCP	>1023	25	Permit
B	Out	Internal	External	TCP	25	>1023	Permit
C	Out	Internal	External	TCP	>1023	25	Permit
D	In	External	Internal	TCP	25	>1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

- Result:



Packet	Direc-tion	Source Address	Dest. Address	Pro-tocol	Source Port	Dest. Port	Action (Rule)
1	In	192.168.3.4	172.16.1.1	TCP	1234	25	Permit (A)
2	Out	172.16.1.1	192.168.3.4	TCP	25	1234	Permit (B)
3	Out	172.16.1.1	192.168.3.4	TCP	1357	25	Permit (C)
4	In	192.168.3.4	172.16.1.1	TCP	25	1357	Permit (D)
5	In	10.1.2.3	172.16.3.4	TCP	5150	6000	Deny (E)
6	Out	172.16.3.4	10.1.2.3	TCP	6000	5150	Deny (E)

Problem Still



Packet	Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Action (Rule)
7	In	10.1.2.3	172.16.3.4	TCP	25	6000	Permit (D)
8	Out	172.16.3.4	10.1.2.3	TCP	6000	25	Permit (C)

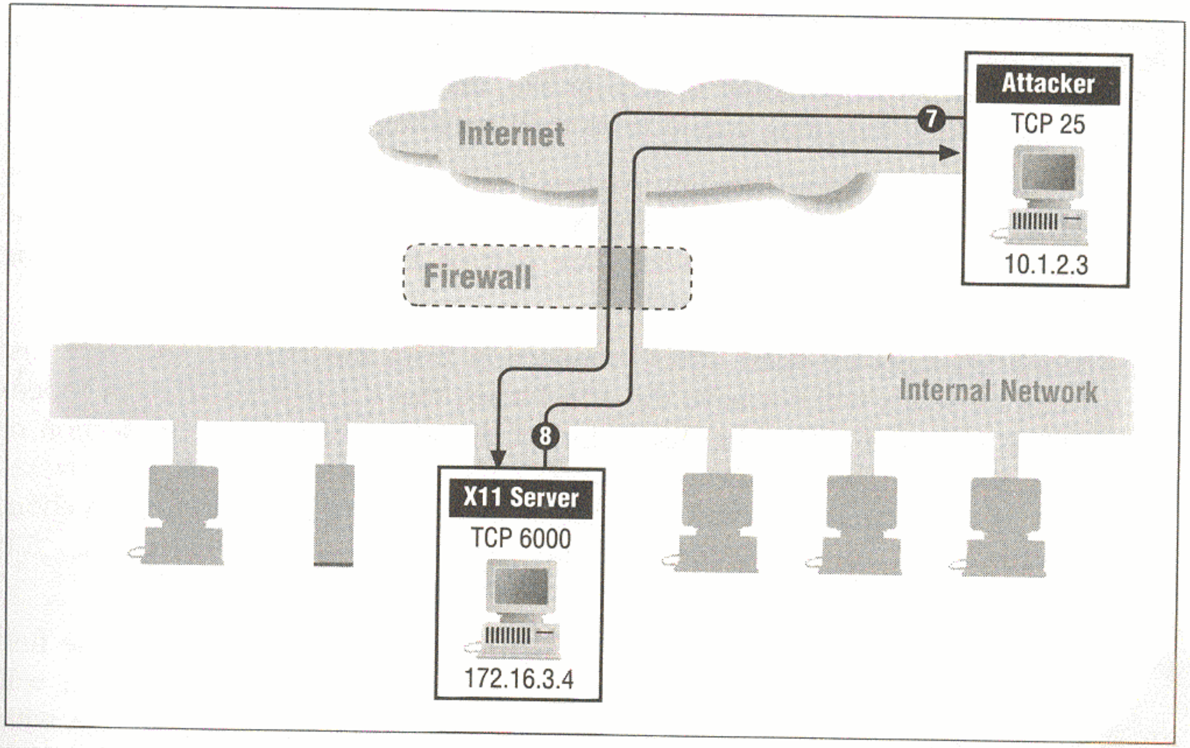
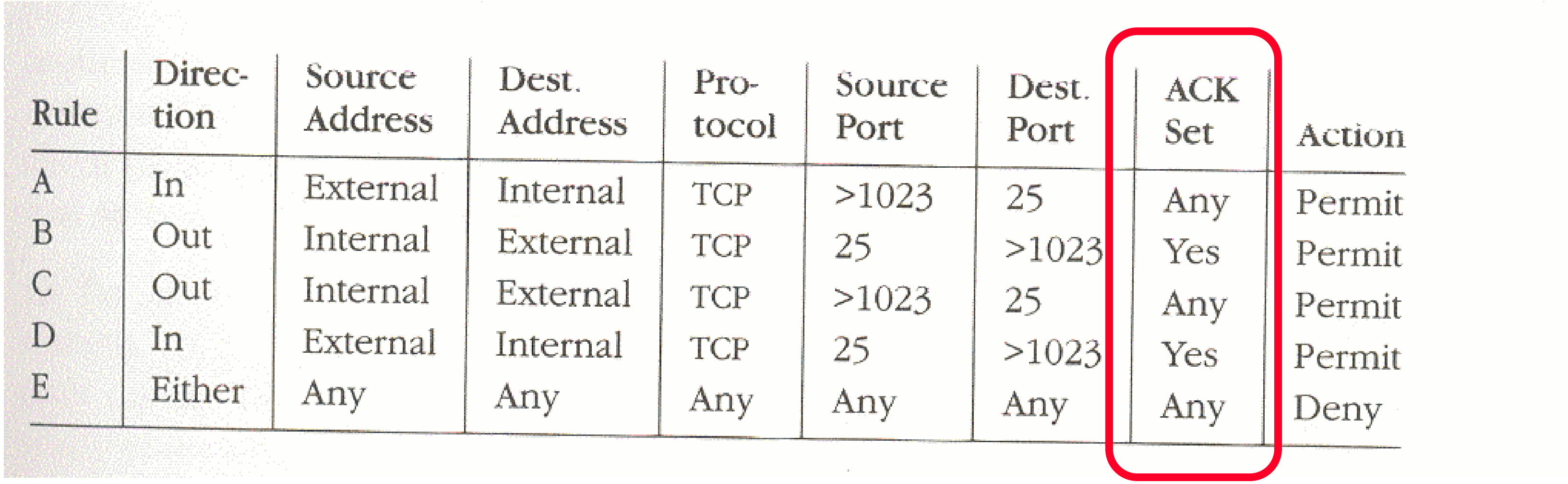


Figure 6-13: Packet filtering: inbound SMTP (sample packets 7 and 8)

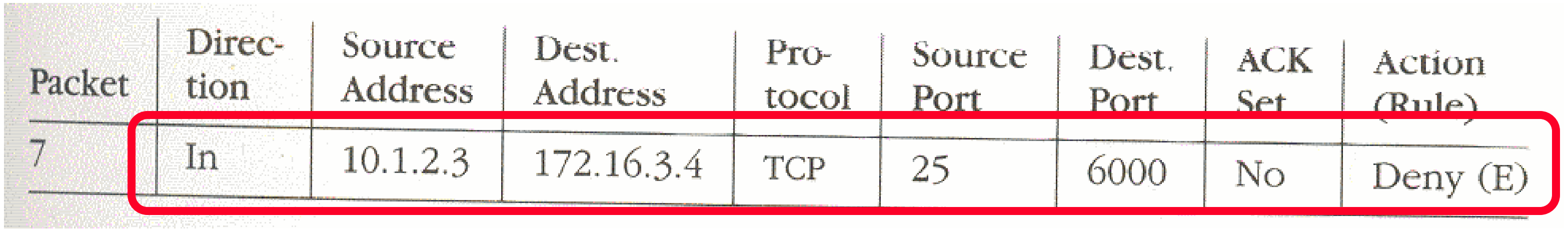
Change Rules Again

- Add the ACK bit.



Rule	Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	ACK Set	Action
A	In	External	Internal	TCP	>1023	25	Any	Permit
B	Out	Internal	External	TCP	25	>1023	Yes	Permit
C	Out	Internal	External	TCP	>1023	25	Any	Permit
D	In	External	Internal	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

- Result:



Packet	Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	ACK Set	Action (Rule)
7	In	10.1.2.3	172.16.3.4	TCP	25	6000	No	Deny (E)