Packet Filtering

Objectives

- Describe packets and packet filtering
- Explain the approaches to packet filtering
- Recommend specific filtering rules

Introduction

- Packets: discrete blocks of data; basic unit of data handled by a network
- Packet filter: hardware or software designed to block or allow transmission of packets based on criteria such as port, IP address, protocol
- To control movement of traffic through the network perimeter, know how packets are structured and what goes into packet headers

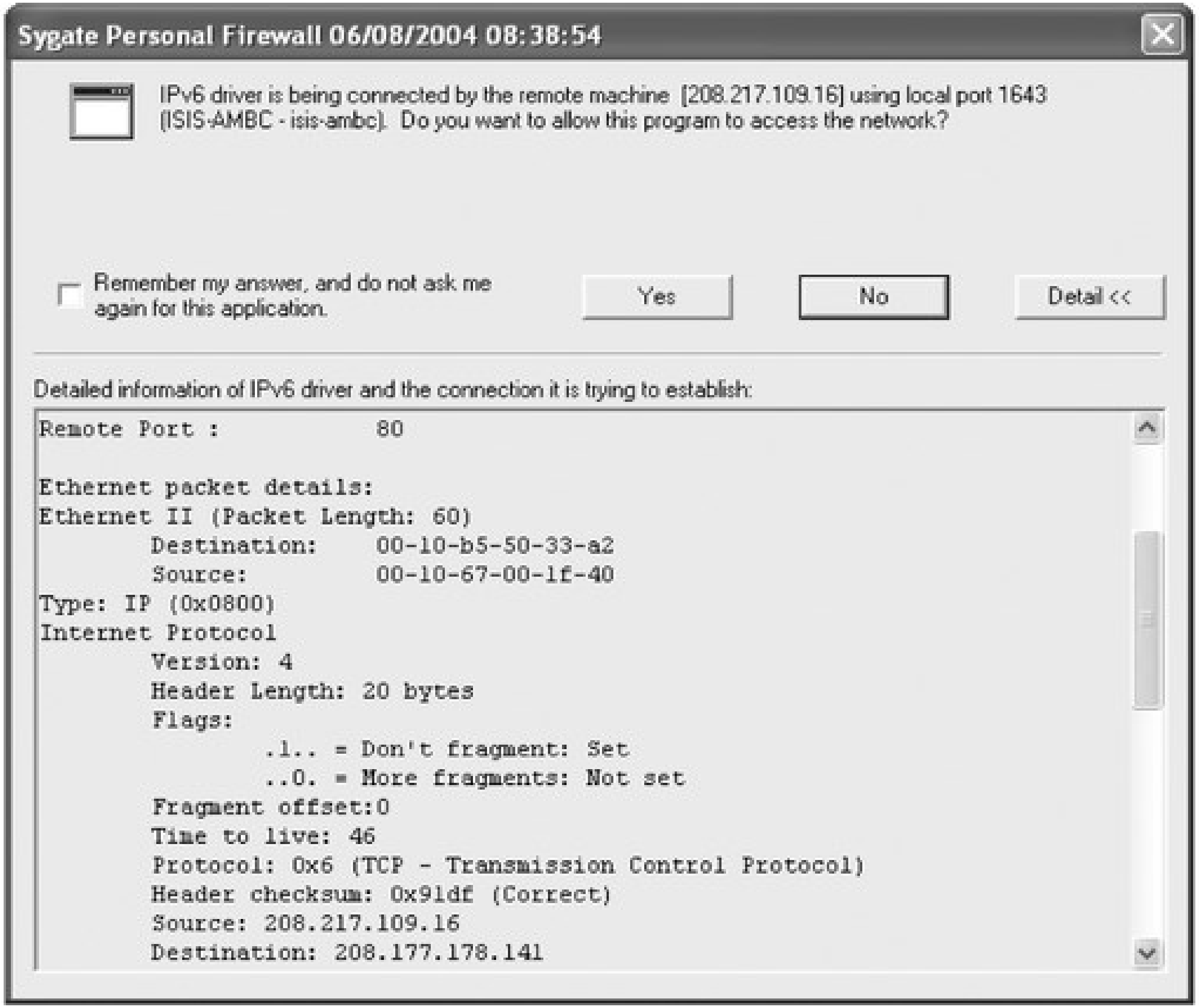
Understanding Packets and Packet Filtering

- Packet filter inspects packet headers before sending packets on to specific locations within the network
- A variety of hardware devices and software programs perform packet filtering:
  - Routers: probably most common packet filters
  - Operating systems: some have built-in utilities to filter packets on TCP/IP stack of the server software
  - Software firewalls: most enterprise-level programs and personal firewalls filter packets

Anatomy of a Packet

- Header
  - Contains IP source and destination addresses
  - Not visible to end users
- Data
  - Contains the information that it is intending to send (e.g., body of an e-mail message)
  - Visible to the recipient

Anatomy of a Packet (continued)



Sygate Personal Firewall 06/08/2004 08:38:54

IPv6 driver is being connected by the remote machine [208.217.109.16] using local port 1643 (ISIS-AMBC - isis-ambc). Do you want to allow this program to access the network?

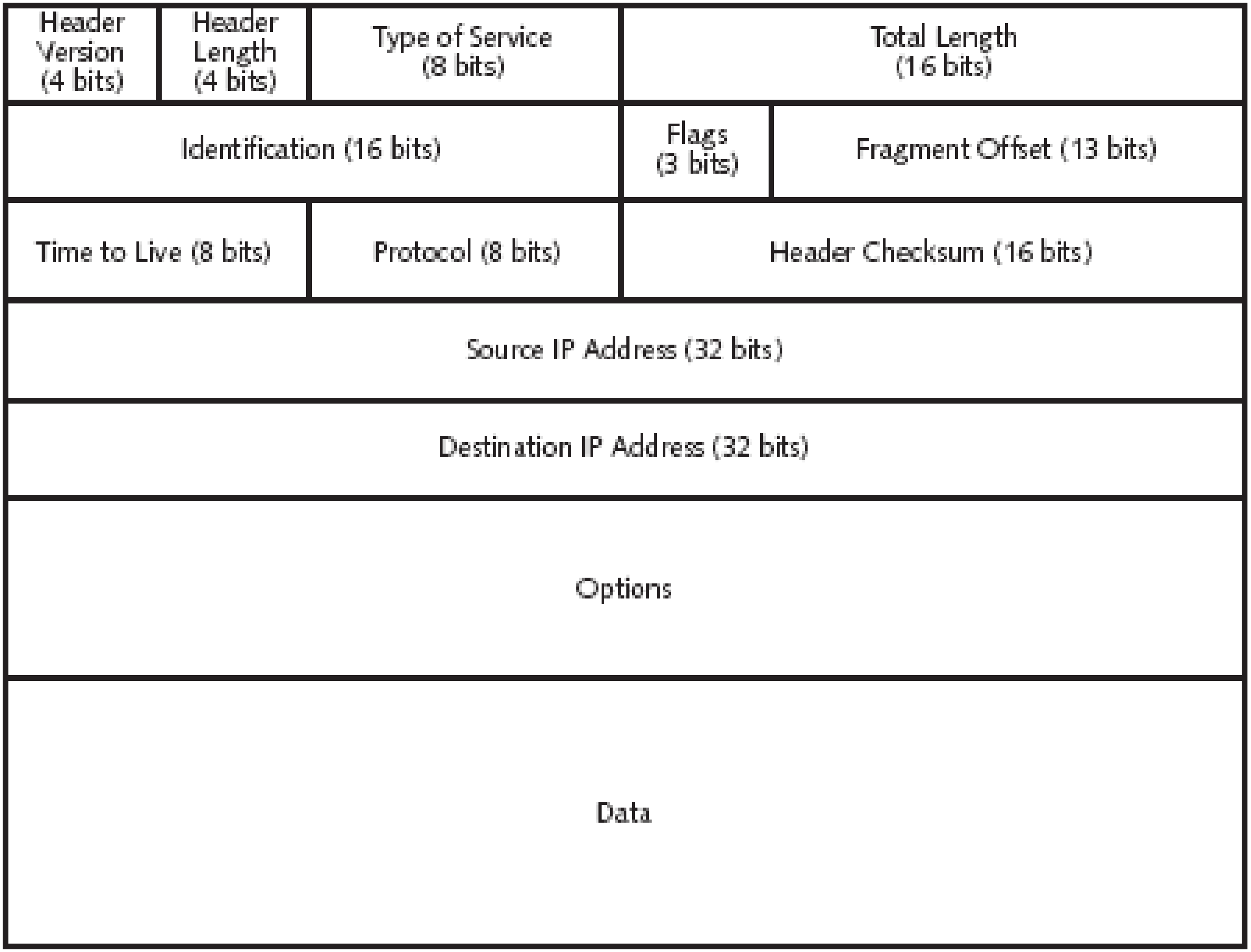
□ Remember my answer, and do not ask me again for this application.

Detailed information of IPv6 driver and the connection it is trying to establish:

```
Remote Port :           80

Ethernet packet details:
Ethernet II (Packet Length: 60)
        Destination:    00-10-b5-50-33-a2
        Source:         00-10-67-00-1f-40
Type: IP (0x0800)
Internet Protocol
        Version: 4
        Header Length: 20 bytes
        Flags:
                .1.. = Don't fragment: Set
                ..0. = More fragments: Not set
        Fragment offset:0
        Time to live: 46
        Protocol: 0x6 (TCP - Transmission Control Protocol)
        Header checksum: 0x91df (Correct)
        Source: 208.217.109.16
        Destination: 208.177.178.141
```

Anatomy of a Packet (continued)



Header Version (4 bits)
Header Length (4 bits)
Type of Service (8 bits)
Total Length (16 bits)

Identification (16 bits)
Flags (3 bits)
Fragment Offset (13 bits)

Time to Live (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)

Source IP Address (32 bits)

Destination IP Address (32 bits)

Options

Data

Packet-Filtering Rules

- Packet filtering: procedure by which packet headers are inspected by a router or firewall to make a decision on whether to let the packet pass
- Header information is evaluated and compared to rules that have been set up (Allow or Deny)
- Packet filters examine only the header of the packet (application proxies examine data in the packet)

Packet-Filtering Rules (continued)

- Drop all inbound connections; allow only outbound connections on Ports 80 (HTTP), 25 (SMTP), and 21 (FTP)
- Eliminate packets bound for ports that should not be available to the Internet (e.g., NetBIOS)
- Filter out ICMP redirect or echo (ping) messages (may indicate hackers are attempting to locate open ports or host IP addresses)
- Drop packets that use IP header source routing feature

Packet-Filtering Rules (continued)

- Set up an access list that includes all computers in the local network by name or IP address so communications can flow between them
  - Allow all traffic between “trusted” hosts
  - Set up rules yourself

Packet-Filtering Methods

- Stateless packet filtering
- Stateful packet filtering

Stateless Packet Filtering

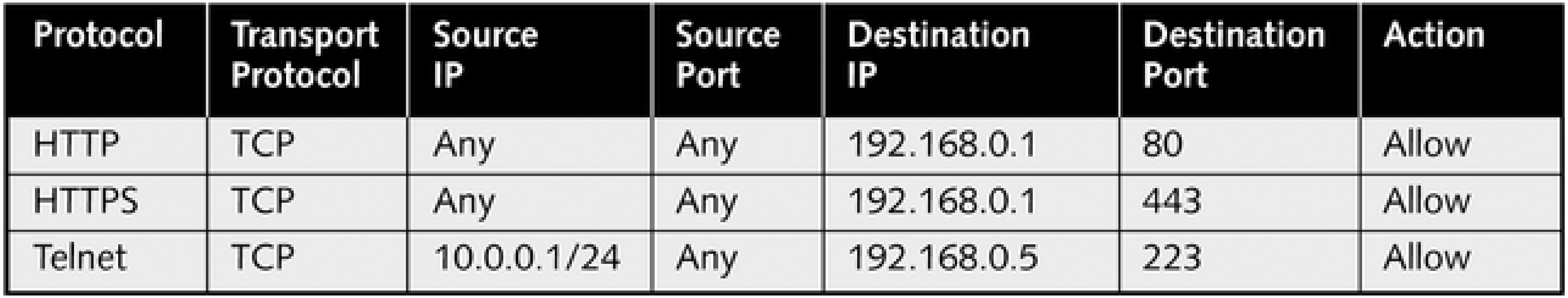
- Determines whether to block or allow packets—based on several criteria—without regard to whether a connection has been established
- Also called static packet filtering
- Useful for completely blocking traffic from a subnet or other network

Criteria That a Stateless Filter Can Be Configured to Use

- IP header information
- TCP or UDP port number being used
- Internet Control Message Protocol (ICMP) message type
- Fragmentation flags (e.g., ACK and SYN)

Filtering on IP Header Criteria

- Packet’s source IP address
- Destination or target IP address
- Specify a protocol for the hosts to which you want to grant access
- IP protocol ID field in the header



Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	Any	Any	192.168.0.1	80	Allow
HTTPS	TCP	Any	Any	192.168.0.1	443	Allow
Telnet	TCP	10.0.0.1/24	Any	192.168.0.5	223	Allow

Filtering by TCP or UDP Port Number

- Helps filter wide variety of information
  - SMTP and POP e-mail messages
  - NetBIOS sessions
  - DNS requests
  - Network News Transfer Protocol (NNTP) newsgroup sessions
- Commonly called port filtering or protocol filtering

Filtering by ICMP Message Type

- ICMP helps networks cope with communication problems
- No authentication method; can be used by hackers to crash computers on the network
- Firewall/packet filter must be able to determine, based on its message type, whether an ICMP packet should be allowed to pass

Filtering by Fragmentation Flags

- Security considerations
  - TCP or UDP port number is provided only at the beginning of a packet; appears only in fragments numbered 0
  - Fragments numbered 1 or higher will be passed through the filter
  - If a hacker modifies an IP header to start all fragment numbers of a packet at 1 or higher, all fragments will go through the filter

Filtering by Fragmentation Flags (continued)

- Configuration considerations
  - Configure firewall/packet filter to drop all fragmented packets
  - Have firewall reassemble fragmented packets and allow only complete packets to pass through

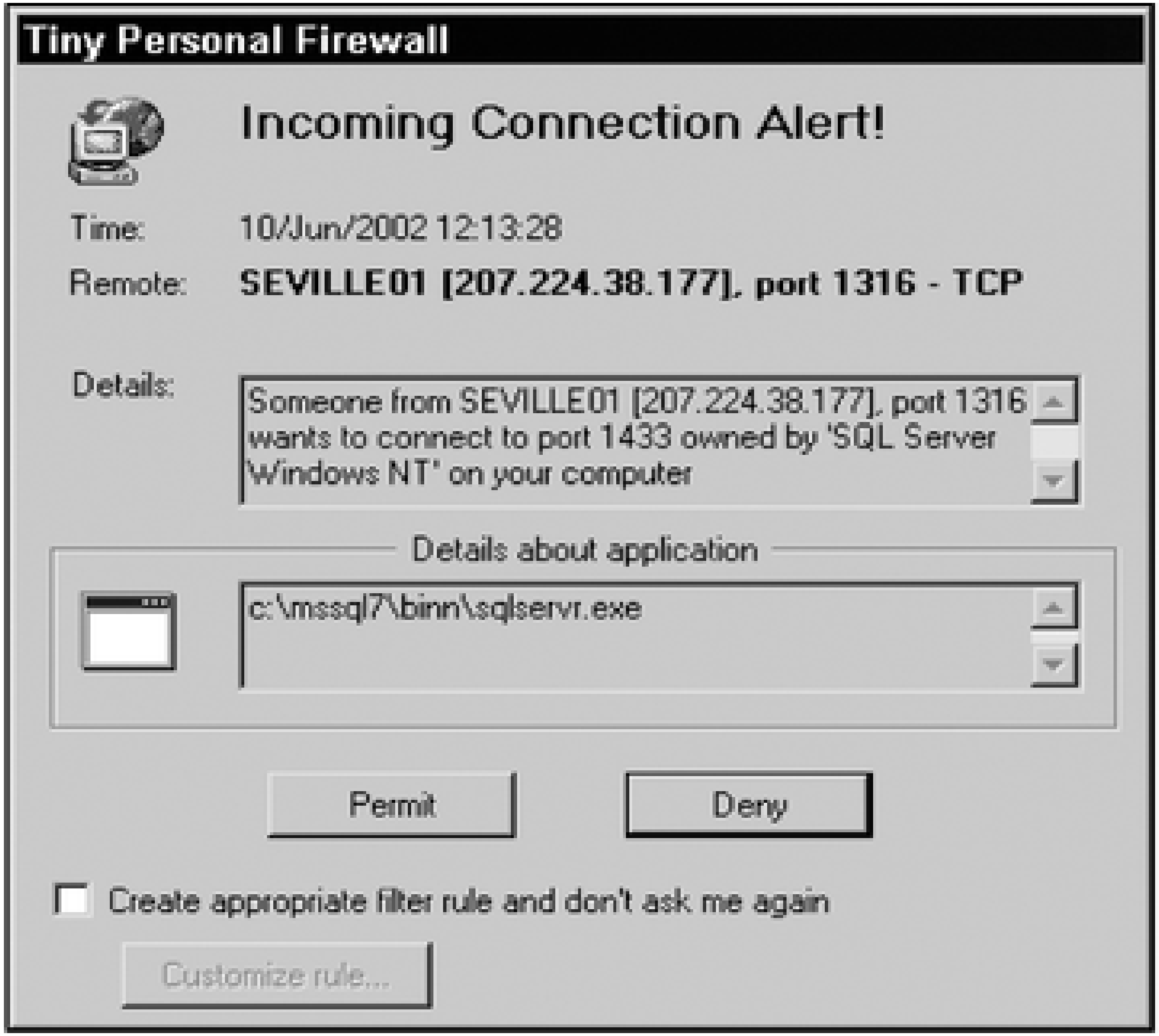
Filtering by ACK Flag

- ACK flag
  - Indicates whether a packet is requesting a connection or whether the connection has already been established
  - A hacker can insert a false ACK bit of 1 into a packet
- Configure firewall to allow packets with the ACK bit set to 1 to access only the ports you specify and only in the direction you want

Filtering Suspicious Inbound Packets

- Firewall sends alert message if a packet arrives from external network but contains an IP address from inside network
- Most firewalls let users decide whether to permit or deny the packet
  - Case-by-case basis
  - Automatically, by setting up rules

Filtering Suspicious Inbound Packets (continued)



Tiny Personal Firewall

Incoming Connection Alert!

Time: 10/Jun/2002 12:13:28

Remote: **SEVILLE01 [207.224.38.177], port 1316 - TCP**

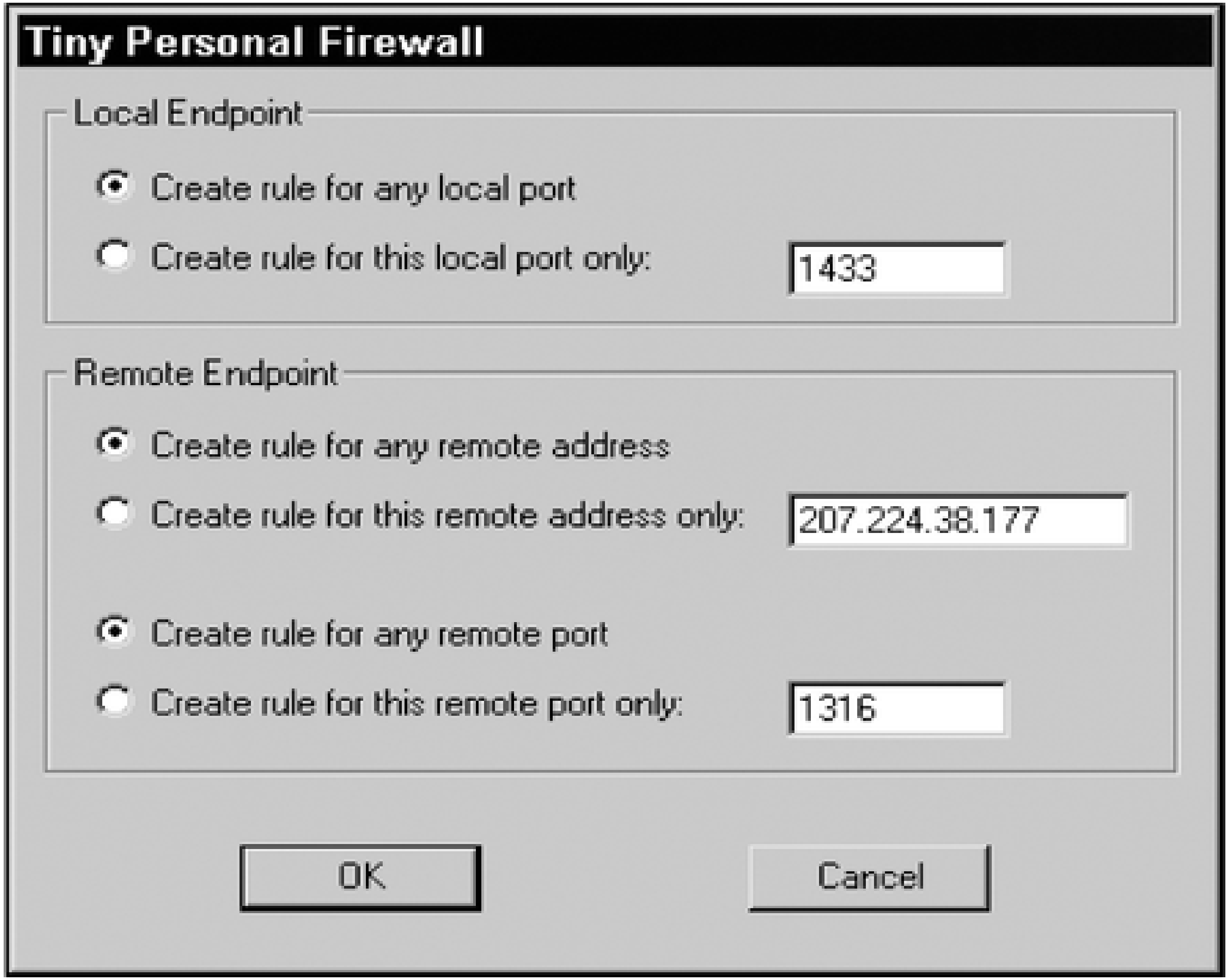
Details: Someone from SEVILLE01 [207.224.38.177], port 1316 wants to connect to port 1433 owned by 'SQL Server Windows NT' on your computer

Details about application

c:\mssql7\binn\sqlservr.exe

□ Create appropriate filter rule and don't ask me again

Filtering Suspicious Inbound Packets (continued)



Tiny Personal Firewall

Local Endpoint

● Create rule for any local port

○ Create rule for this local port only: 1433

Remote Endpoint

● Create rule for any remote address

○ Create rule for this remote address only: 207.224.38.177

● Create rule for any remote port

○ Create rule for this remote port only: 1316

Stateful Packet Filtering

- Performs packet filtering based on contents of the data part of a packet and the header
- Filter maintains a record of the state of a connection; allows only packets that result from connections that have already been established
- More sophisticated and secure
- Has a rule base and a state table

Filtering Based on Packet Content

- Stateful inspection
- Proxy gateway
- Specialty firewall

Setting Specific Packet-Filter Rules

- Rules to filter potentially harmful packets
- Rules to pass packets that you want to be passed through

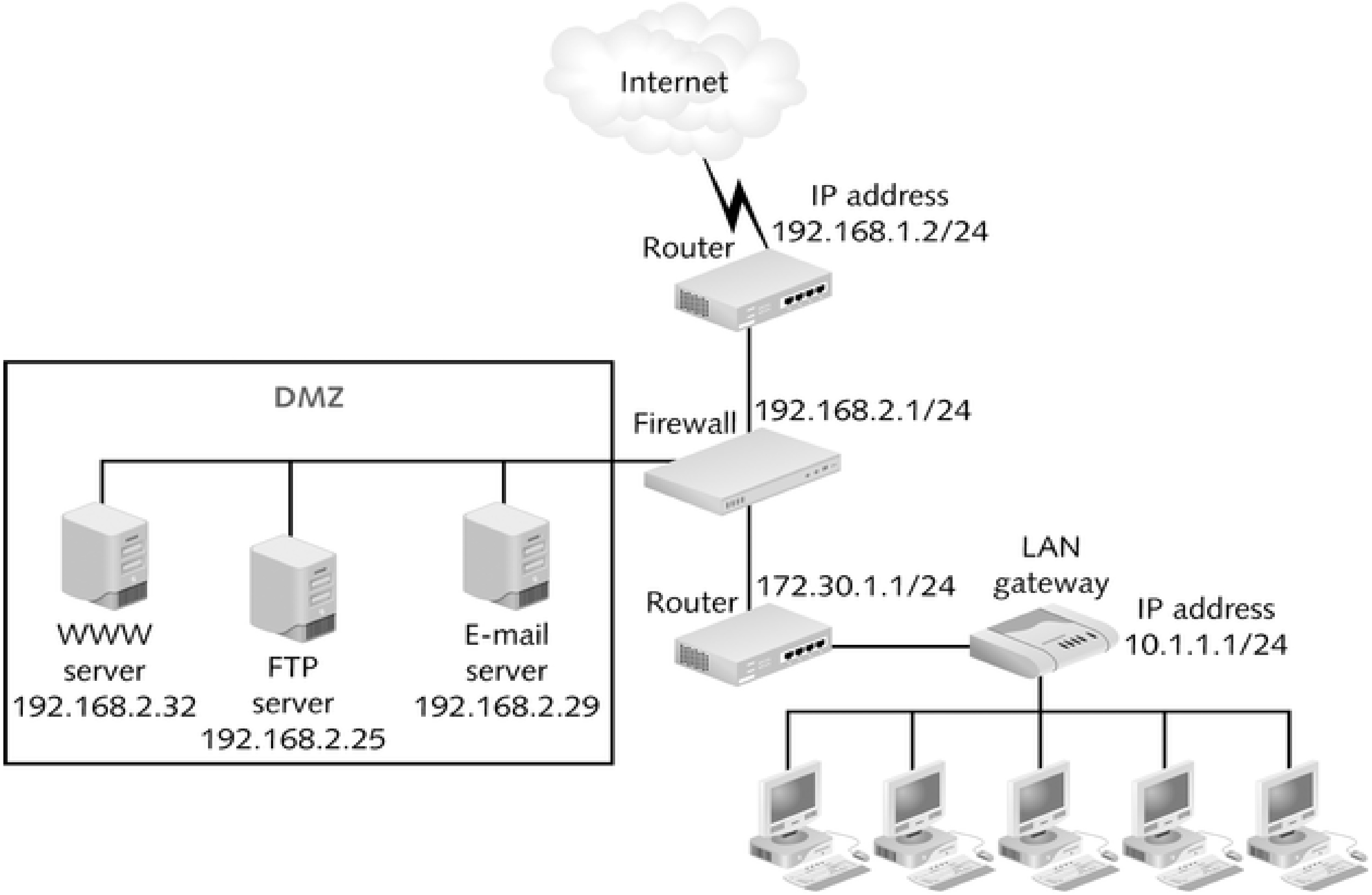
Best Practices for Firewall Rules

- All traffic from trusted network is allowed out
- Firewall device is never accessible directly from public network
- SMTP data allowed to pass through firewall but all is routed to well-configured SMTP gateway
- All ICMP data is denied
- Telnet access to all internal servers from public networks is blocked
- When Web services are offered outside firewall, implement proxy access or DMZ architecture

Rules That Cover Multiple Variations

- Must account for all possible ports that a type of communication might use or for all variations within a protocol

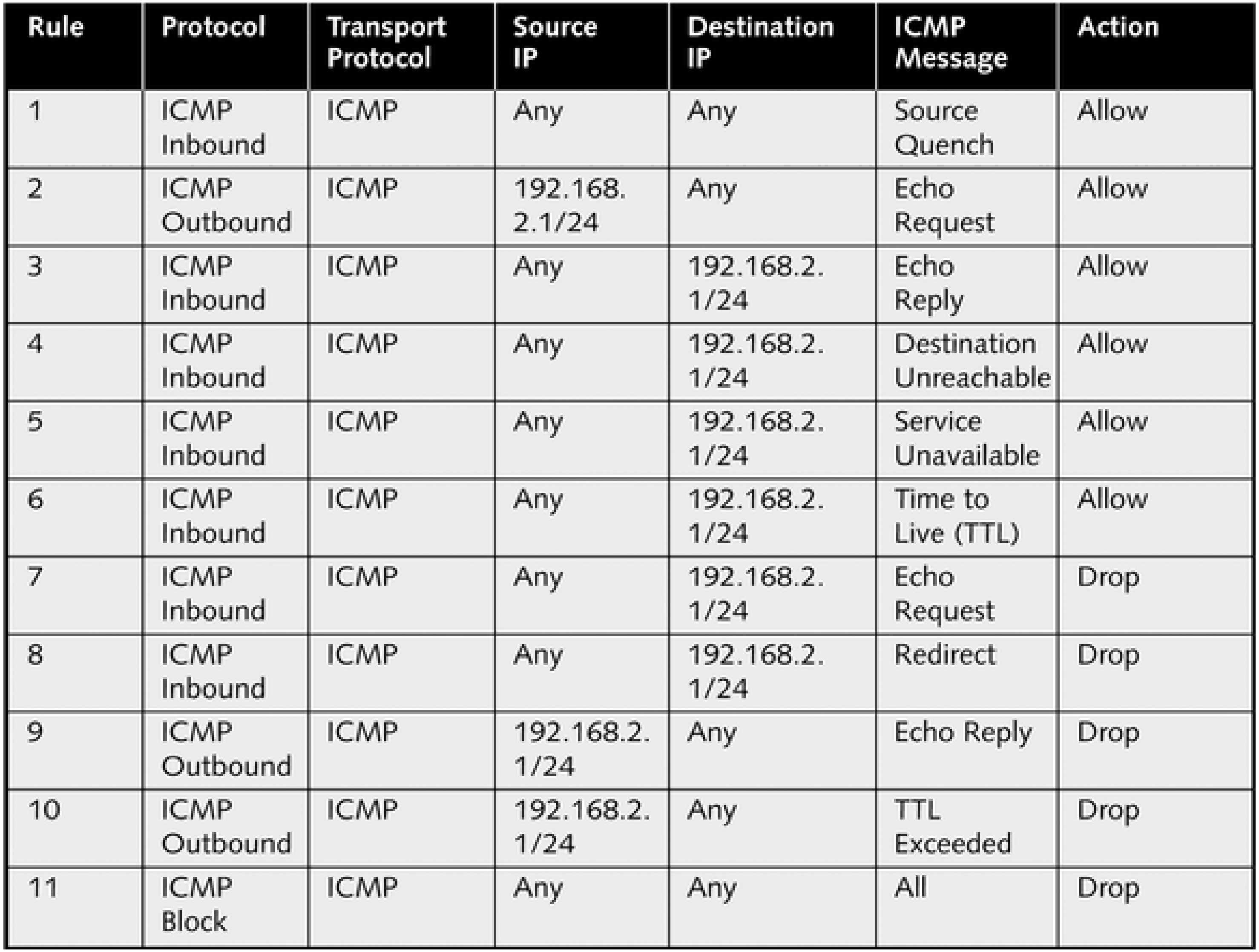
Sample Network to Be Protected by a Firewall



Rules for ICMP Packets

- ICMP lets you test network connectivity and makes you aware of communications problems
- Rules are especially important because ICMP packets can be easily forged and used to redirect other communications

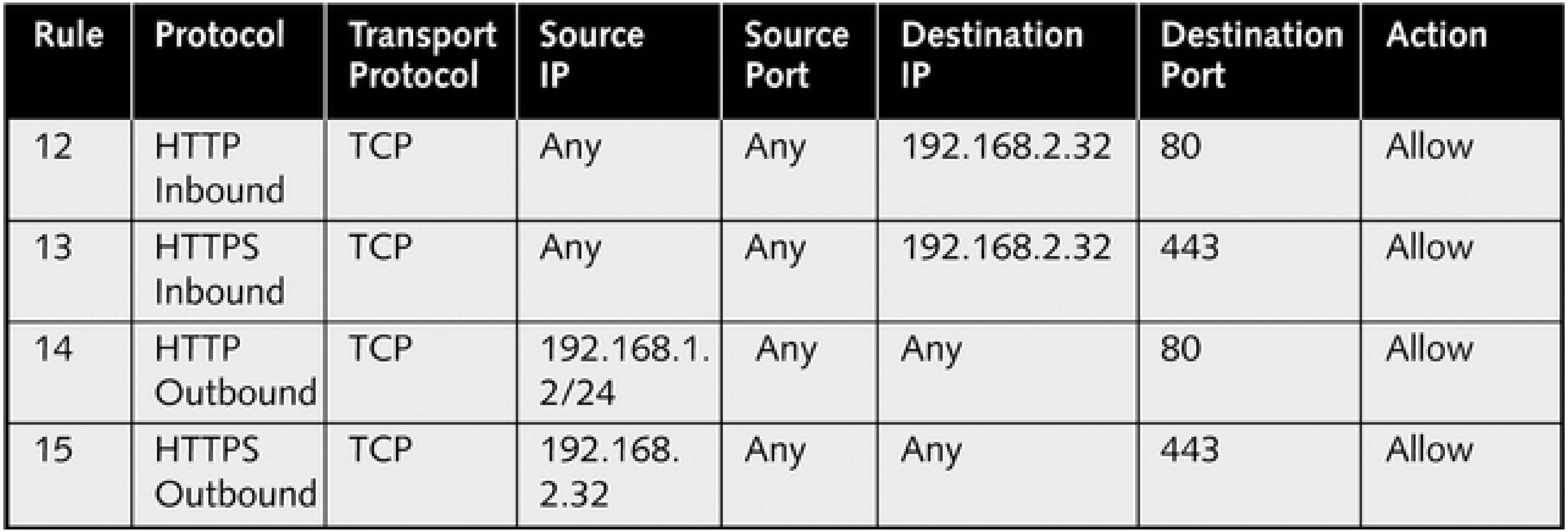
ICMP Packet-Filter Rules



Rule	Protocol	Transport Protocol	Source IP	Destination IP	ICMP Message	Action
1	ICMP Inbound	ICMP	Any	Any	Source Quench	Allow
2	ICMP Outbound	ICMP	192.168. 2.1/24	Any	Echo Request	Allow
3	ICMP Inbound	ICMP	Any	192.168.2. 1/24	Echo Reply	Allow
4	ICMP Inbound	ICMP	Any	192.168.2. 1/24	Destination Unreachable	Allow
5	ICMP Inbound	ICMP	Any	192.168.2. 1/24	Service Unavailable	Allow
6	ICMP Inbound	ICMP	Any	192.168.2. 1/24	Time to Live (TTL)	Allow
7	ICMP Inbound	ICMP	Any	192.168.2. 1/24	Echo Request	Drop
8	ICMP Inbound	ICMP	Any	192.168.2. 1/24	Redirect	Drop
9	ICMP Outbound	ICMP	192.168.2. 1/24	Any	Echo Reply	Drop
10	ICMP Outbound	ICMP	192.168.2. 1/24	Any	TTL Exceeded	Drop
11	ICMP Block	ICMP	Any	Any	All	Drop

Rules That Enable Web Access

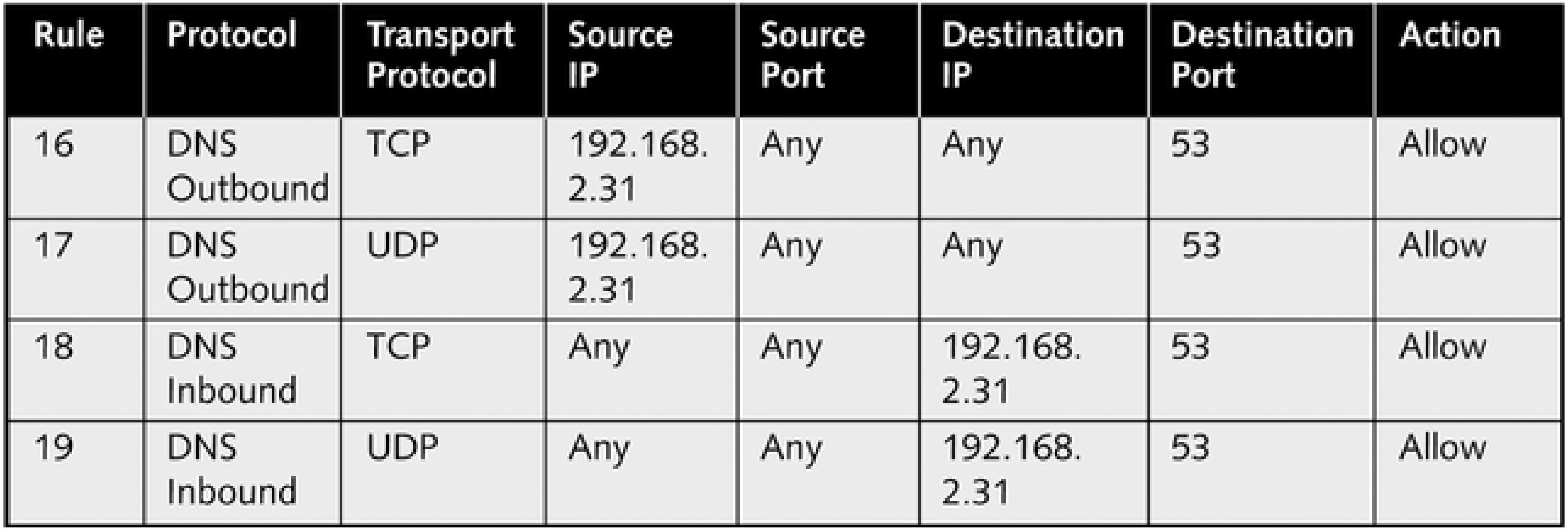
- Rules need to cover both standard HTTP traffic on TCP Port 80 as well as Secure HTTP (HTTPS) traffic on TCP Port 443



Rule	Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
12	HTTP Inbound	TCP	Any	Any	192.168.2.32	80	Allow
13	HTTPS Inbound	TCP	Any	Any	192.168.2.32	443	Allow
14	HTTP Outbound	TCP	192.168.1.2/24	Any	Any	80	Allow
15	HTTPS Outbound	TCP	192.168.2.32	Any	Any	443	Allow

Rules That Enable DNS

- Set up rules that enable external clients to access computers in your network using the same TCP and UDP ports

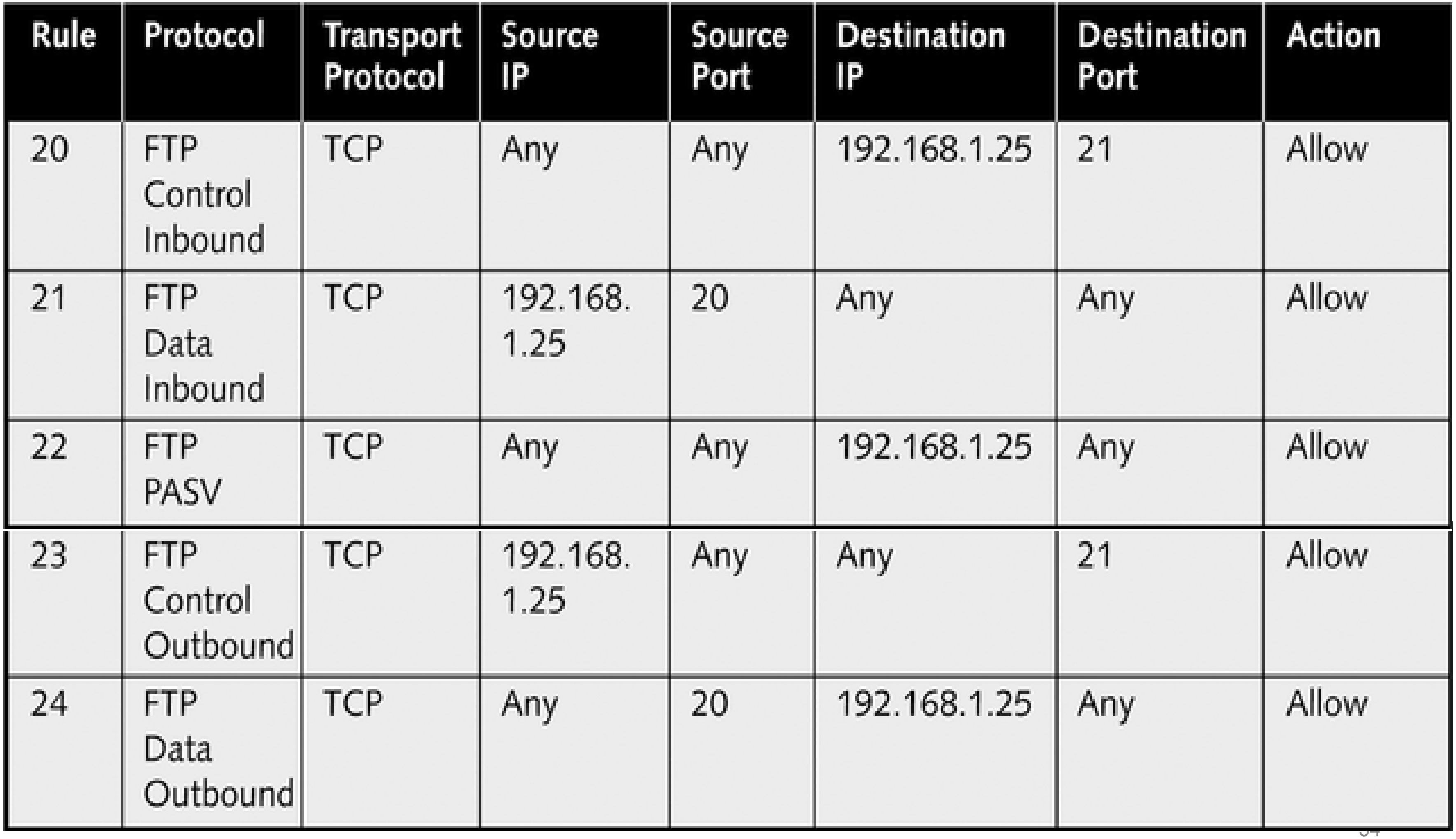


Rule	Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
16	DNS Outbound	TCP	192.168.2.31	Any	Any	53	Allow
17	DNS Outbound	UDP	192.168.2.31	Any	Any	53	Allow
18	DNS Inbound	TCP	Any	Any	192.168.2.31	53	Allow
19	DNS Inbound	UDP	Any	Any	192.168.2.31	53	Allow

Rules That Enable FTP

- Rules need to support two separate connections
  - TCP Port 21 (FTP Control port)
  - TCP 20 (FTP Data port)

Rules That Enable FTP (continued)

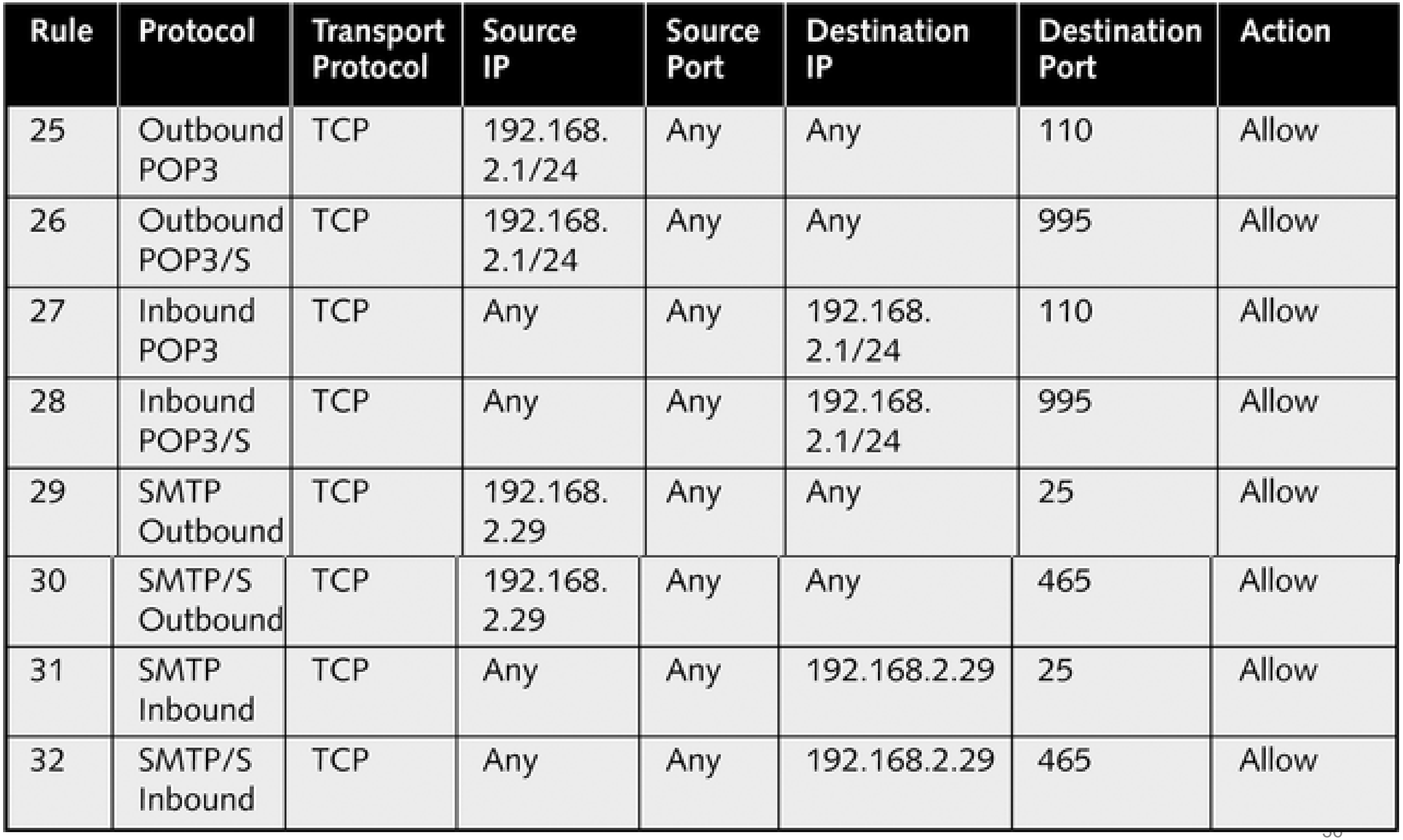


Rule	Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
20	FTP Control Inbound	TCP	Any	Any	192.168.1.25	21	Allow
21	FTP Data Inbound	TCP	192.168. 1.25	20	Any	Any	Allow
22	FTP PASV	TCP	Any	Any	192.168.1.25	Any	Allow
23	FTP Control Outbound	TCP	192.168. 1.25	Any	Any	21	Allow
24	FTP Data Outbound	TCP	Any	20	192.168.1.25	Any	Allow

Rules That Enable E-Mail

- Complicated; a variety of protocols might be used
    - For inbound mail transport
        - Post Office Protocol version 3 (POP3)
        - Internet E-mail Access Protocol version 4 (IMAP4)
    - For outbound mail transport
        - Simple Mail Transfer Protocol (SMTP)
    - For looking up e-mail addresses
        - Lightweight Directory Access Protocol (LDAP)
    - For Web-based mail service
        - HyperText Transport Protocol (HTTP)

POP3 and SMTP E-Mail Rules



Rule	Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
25	Outbound POP3	TCP	192.168.2.1/24	Any	Any	110	Allow
26	Outbound POP3/S	TCP	192.168.2.1/24	Any	Any	995	Allow
27	Inbound POP3	TCP	Any	Any	192.168.2.1/24	110	Allow
28	Inbound POP3/S	TCP	Any	Any	192.168.2.1/24	995	Allow
29	SMTP Outbound	TCP	192.168.2.29	Any	Any	25	Allow
30	SMTP/S Outbound	TCP	192.168.2.29	Any	Any	465	Allow
31	SMTP Inbound	TCP	Any	Any	192.168.2.29	25	Allow
32	SMTP/S Inbound	TCP	Any	Any	192.168.2.29	465	Allow