FIREWALLS & NETWORK SECURITY with Intrusion Detection and VPNs, 2nd ed.

Chapter 7

Working with Proxy Servers & Application-Level Firewalls

Learning Objectives

- Discuss proxy servers and how they work
- Identify the goals that your organization can achieve using a proxy server
- Make recommendations from among proxy server configurations
- Choose a proxy server and work with the SOCKS protocol
- Evaluate the most popular proxy-based firewall products
- Explain how to deploy and use reverse proxy
- Determine when a proxy server isn’t the correct choice

Overview of Proxy Servers

- Scan and act on the data portion of an IP packet
- Act primarily on behalf of internal hosts—receiving, rebuilding, and forwarding outbound requests
- Go by many names
  - Proxy services
  - Application-level gateways
  - Application proxies

How Proxy Servers Work

- Function as a software go-between, forwarding data between internal and external hosts
- Focus on the port each service uses
  - Screen all traffic into and out of each port
  - Decide whether to block or allow traffic based on rules
- Add time to communications, but in return, they:
  - Conceal clients
  - Translate network addresses
  - Filter content

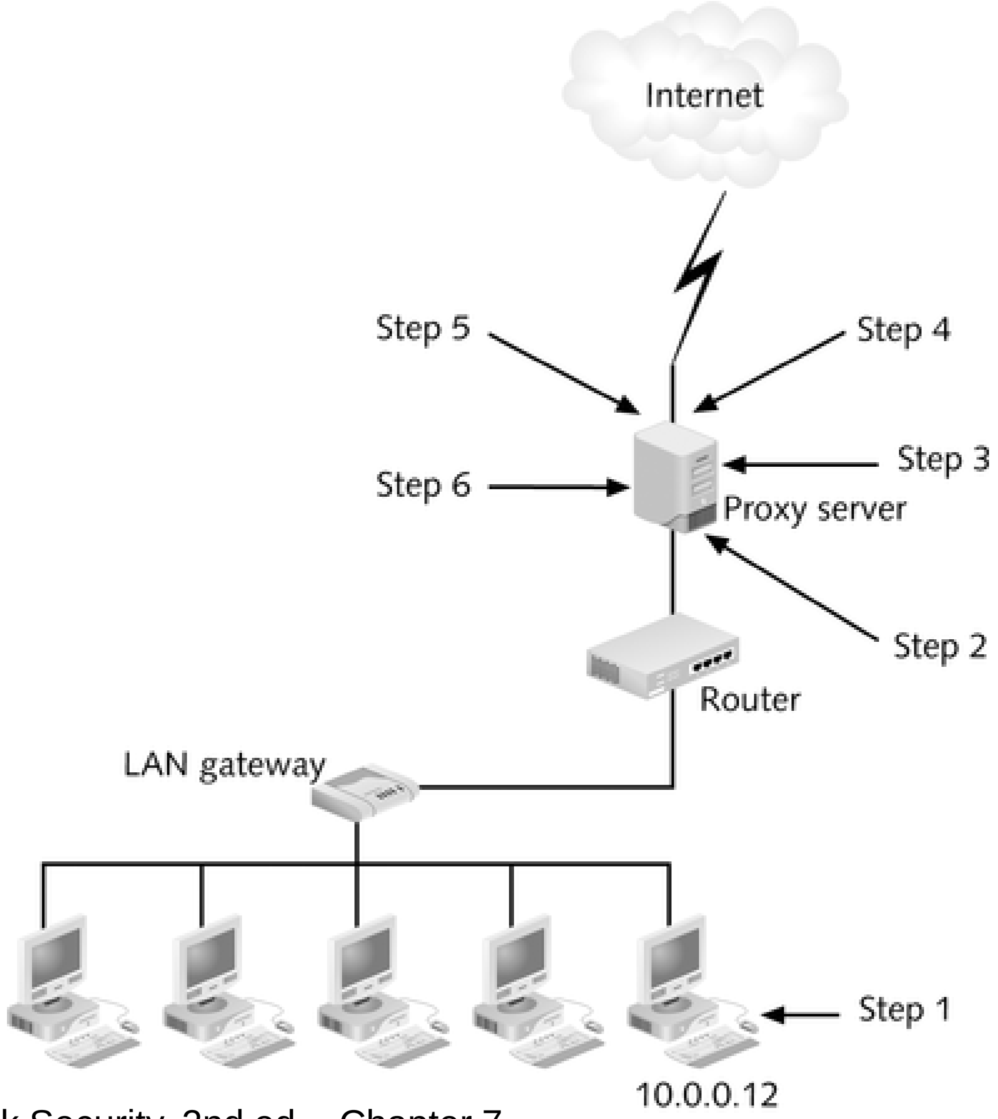
Steps Involved in a Proxy Transaction

1. Internal host makes request to access a Web site
2. Request goes to proxy server, which examines header and data of the packet against rule base
3. Proxy server recreates packet in its entirety with a different source IP address

Steps Involved in a Proxy Transaction (continued)

4. Proxy server sends packet to destination; packet appears to come from proxy server
5. Returned packet is sent to proxy server, which inspects it again and compares it against its rule base
6. Proxy server rebuilds returned packet and sends it to originating computer; packet appears to come from external host

Steps Involved in a Proxy Transaction (continued)



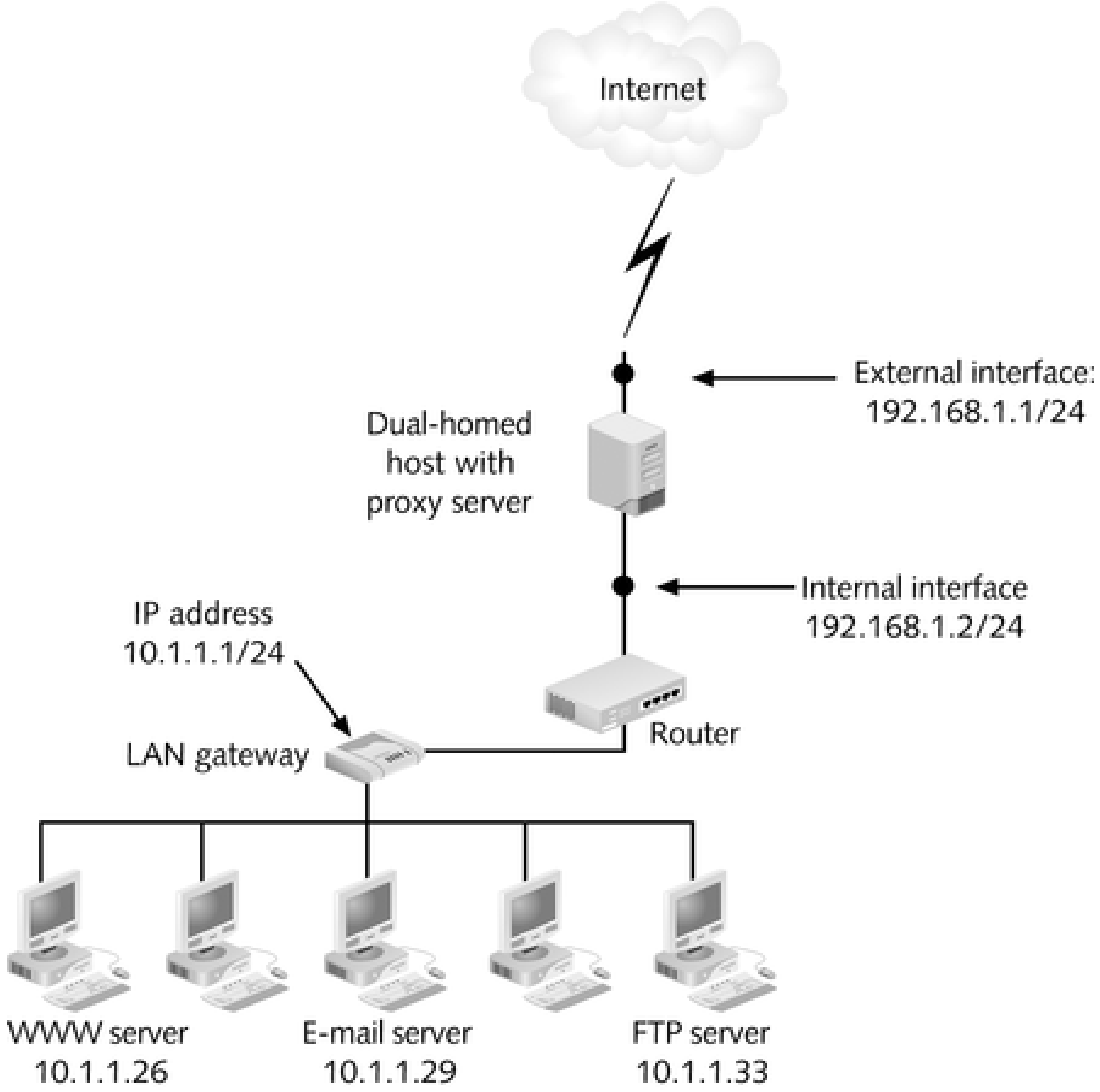
How Proxy Servers Differ from Packet Filters

- Are used together in a firewall to provide multiple layers of security
- Both work at the Application layer, but they inspect different parts of IP packets and act on them in different ways

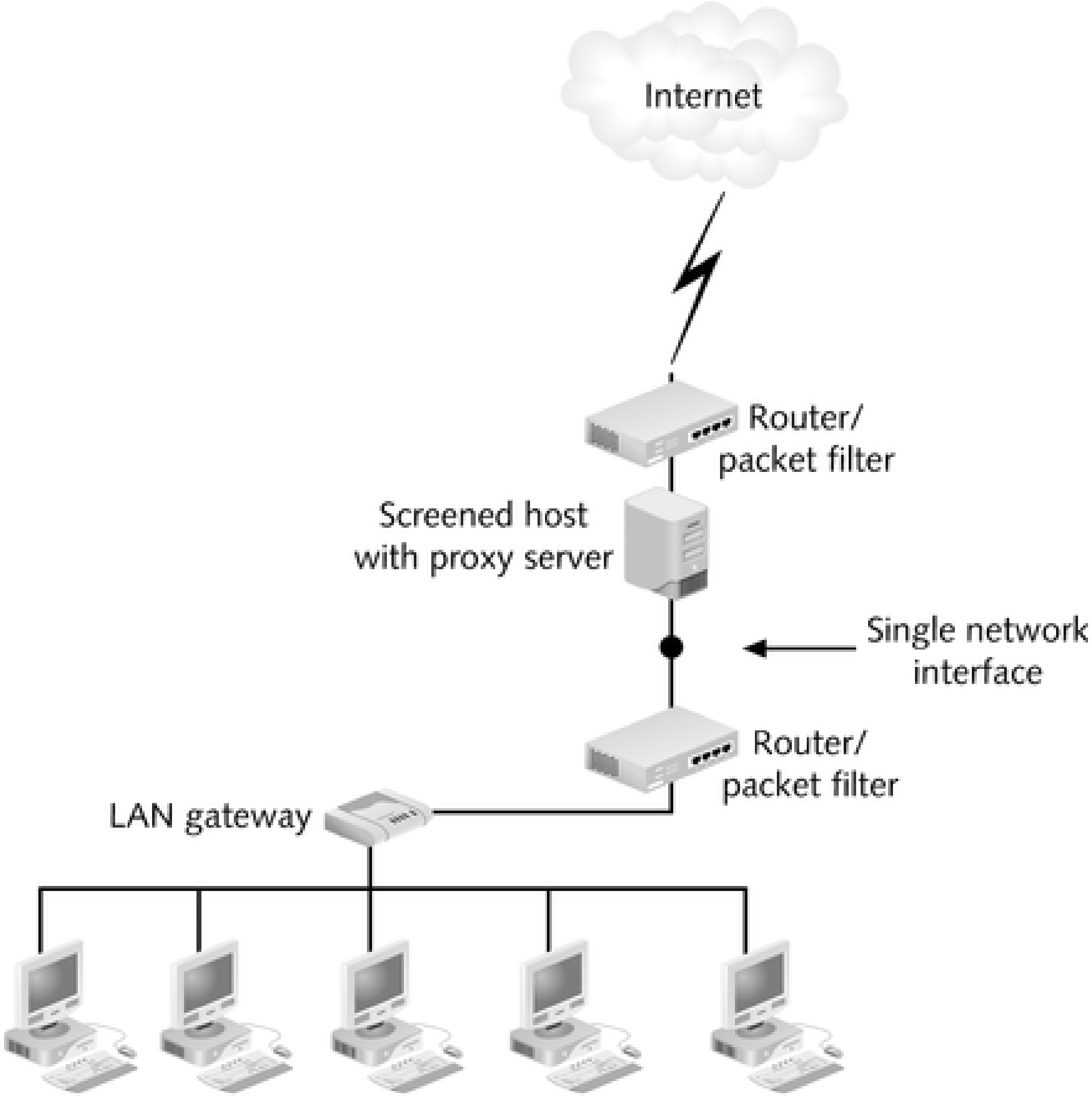
How Proxy Servers Differ from Packet Filters (continued)

- Scan entire data portion of IP packets and create more detailed log file listings
- Rebuild packet with new source IP information (shields internal users from outside users)
- Server on the Internet and an internal host are never directly connected to one another
- More critical to network communications

Proxy Using a Dual-Homed Host



Proxy Using a Screened Host



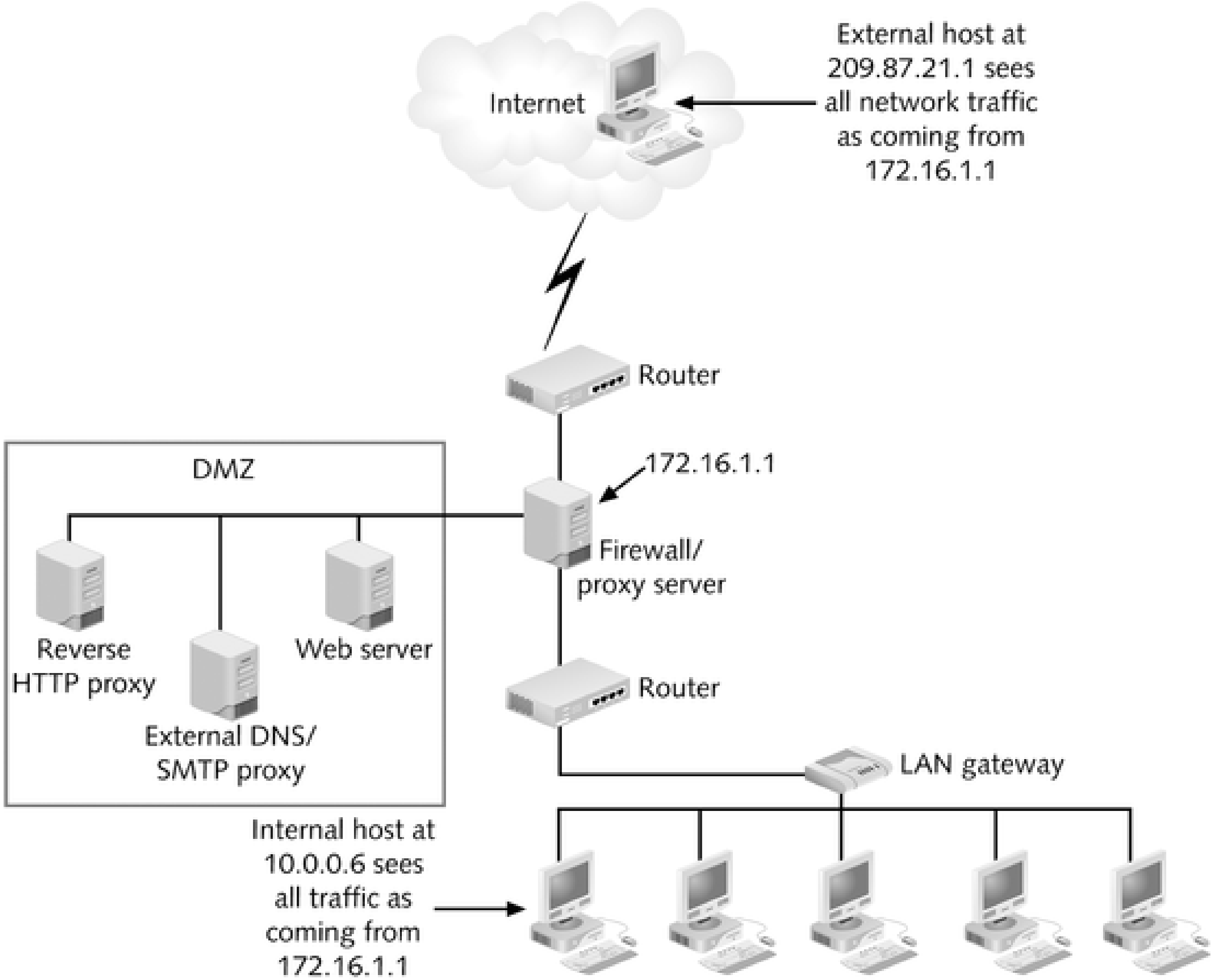
Goals of Proxy Servers

- Conceal internal clients
- Block URLs
- Block and filter content
- Protect e-mail proxy
- Improve performance
- Ensure security
- Provide user authentication
- Redirect URLs

Concealing Internal Clients

- Network appears as a single machine
- If external users cannot detect hosts on your internal network, they cannot initiate an attack against these hosts
- Proxy server receives requests as though it were the destination server and then completely regenerates a new request, which is sent to its destination

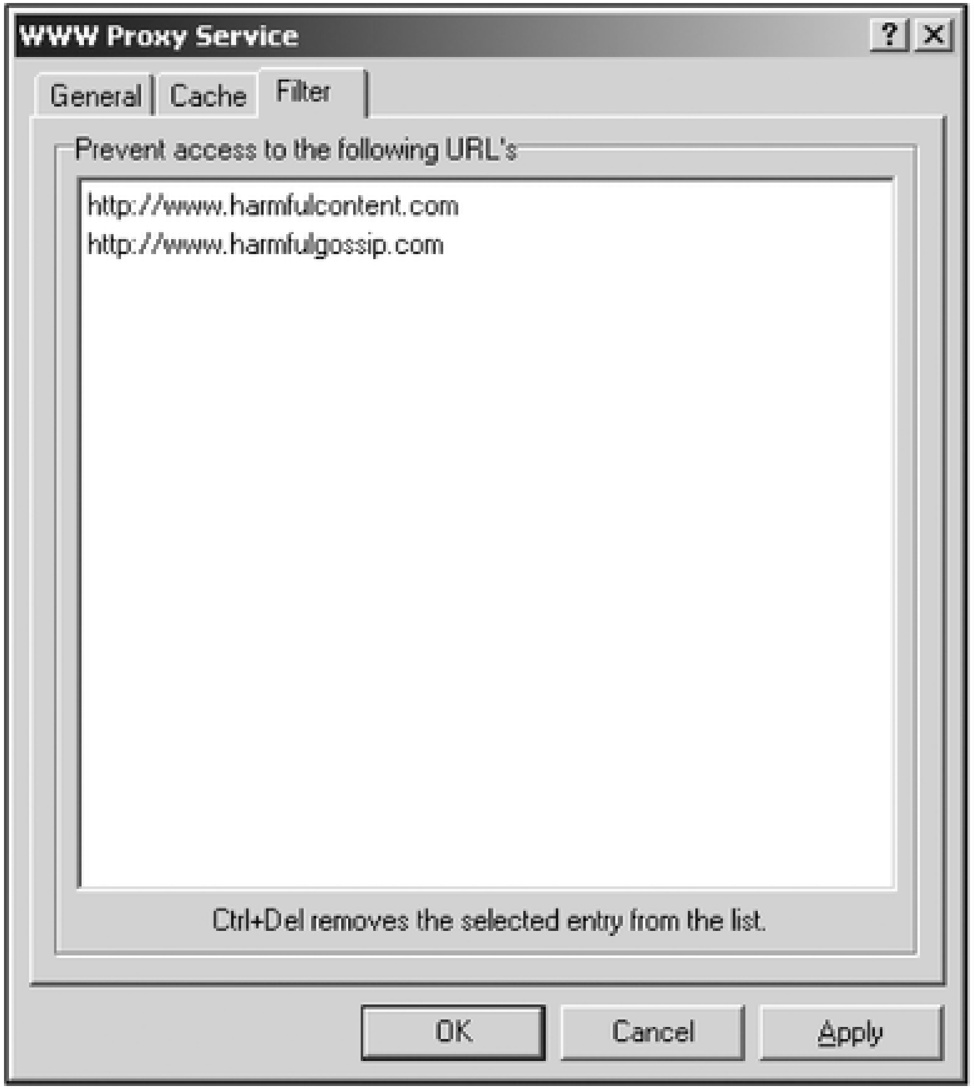
Concealing Internal Clients (continued)



Blocking URLs

- An attempt to keep employees from visiting unsuitable Web sites
- An unreliable practice; users can use the IP address that corresponds to the URL

Blocking URLs (continued)



Prevent access to the following URL's

http://www.harmfulcontent.com
http://www.harmfulgossip.com

Ctrl+Del removes the selected entry from the list.

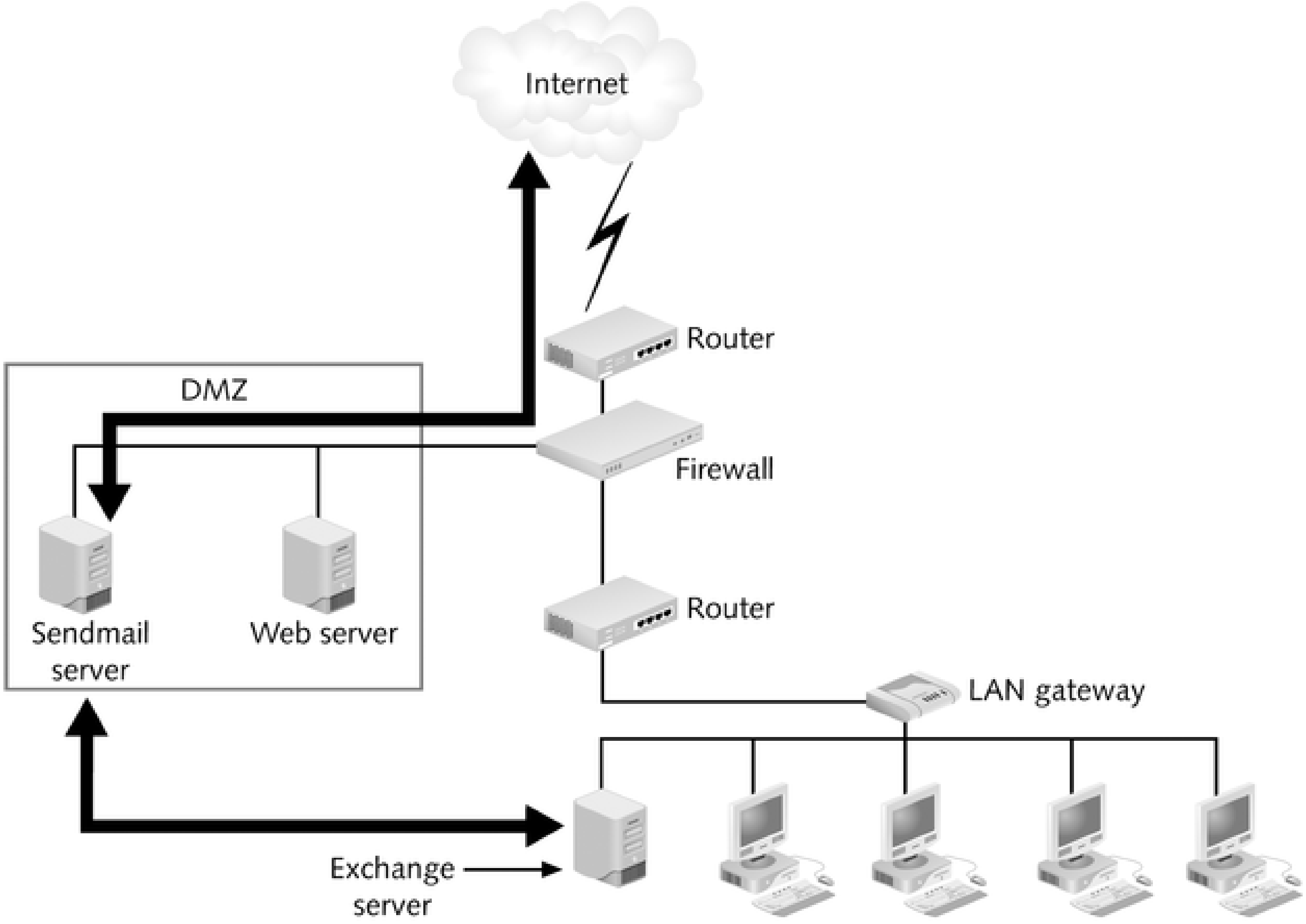
Blocking and Filtering Content

- Can block and strip out Java applets or ActiveX controls
- Can delete executable files attached to e-mail messages
- Can filter out content based on rules that contain a variety of parameters (e.g., time, IP address, port number)

E-Mail Proxy Protection

- External e-mail users never interact directly with internal hosts

E-Mail Proxy Protection (continued)



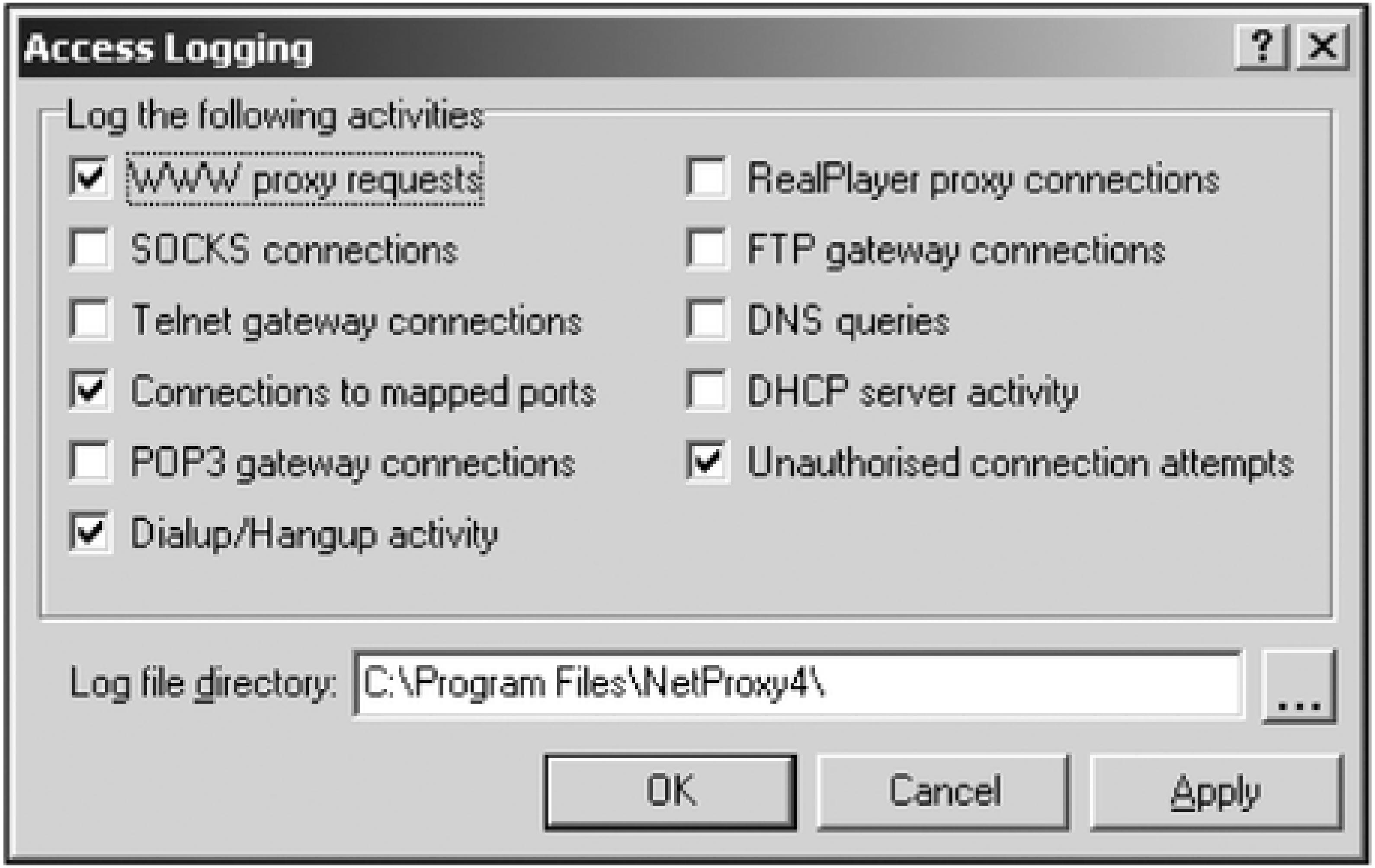
Improving Performance

- Speed up access to documents that have been requested repeatedly

Ensuring Security with Log Files

- Log file
  - Text file set up to store information about access to networked resources
  - Can ensure effectiveness of firewall
    - Detect intrusions
    - Uncover weaknesses
    - Provide documentation

Ensuring Security with Log Files (continued)



Access Logging

Log the following activities

☑ WWW proxy requests

□ SOCKS connections

□ Telnet gateway connections

☑ Connections to mapped ports

□ POP3 gateway connections

☑ Dialup/Hangup activity

□ RealPlayer proxy connections

□ FTP gateway connections

□ DNS queries

□ DHCP server activity

☑ Unauthorised connection attempts

Log file directory: C:\Program Files\NetProxy4\

Providing User Authentication

- Enhances security
- Most proxy servers can prompt users for username and password

Redirecting URLs

- Proxy can be configured to recognize two types of content and perform URL redirection to send them to other locations
  - Files or directories requested by the client
  - Host name with which the client wants to communicate (most popular)

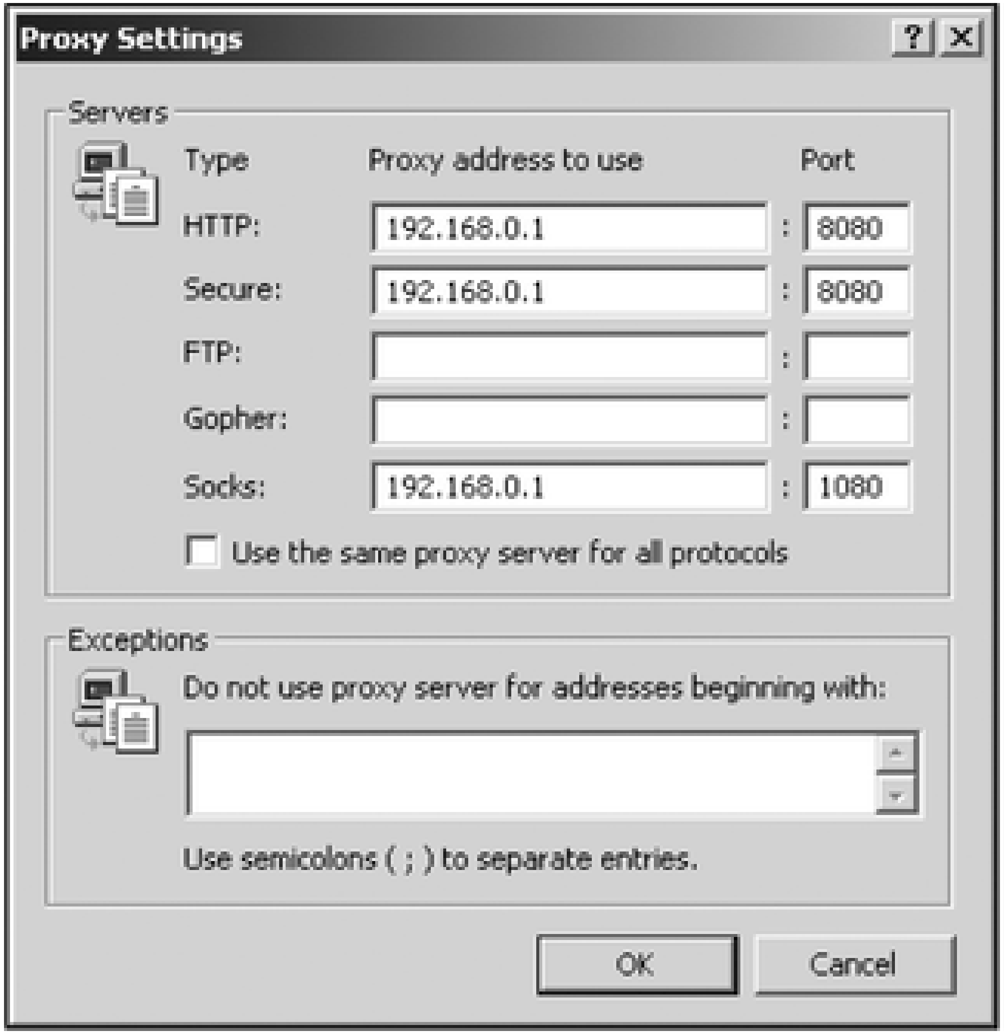
Proxy Server Configuration Considerations

- Scalability issues
- Need to configure each piece of client software that will use the proxy server
- Need to have a separate proxy service available for each network protocol
- Need to create packet-filter rules
- Security vulnerabilities
  - Single point of failure
  - Buffer overflow

Providing for Scalability

- Add multiple proxy servers to the same network connection

Working with Client Configurations



Servers

Type	Proxy address to use		Port
HTTP:	192.168.0.1	:	8080
Secure:	192.168.0.1	:	8080
FTP:		:	
Gopher:		:	
Socks:	192.168.0.1	:	1080

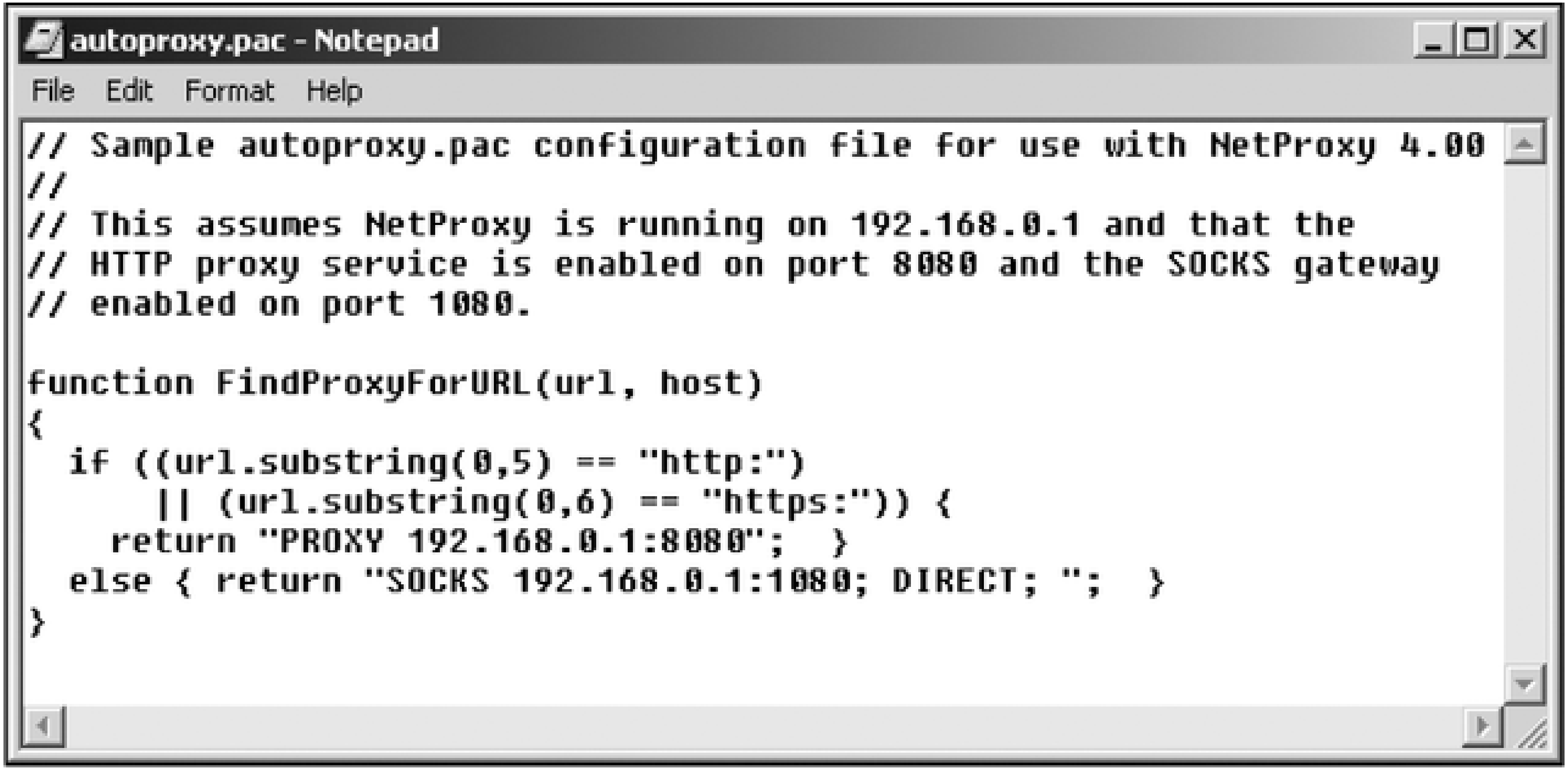
□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

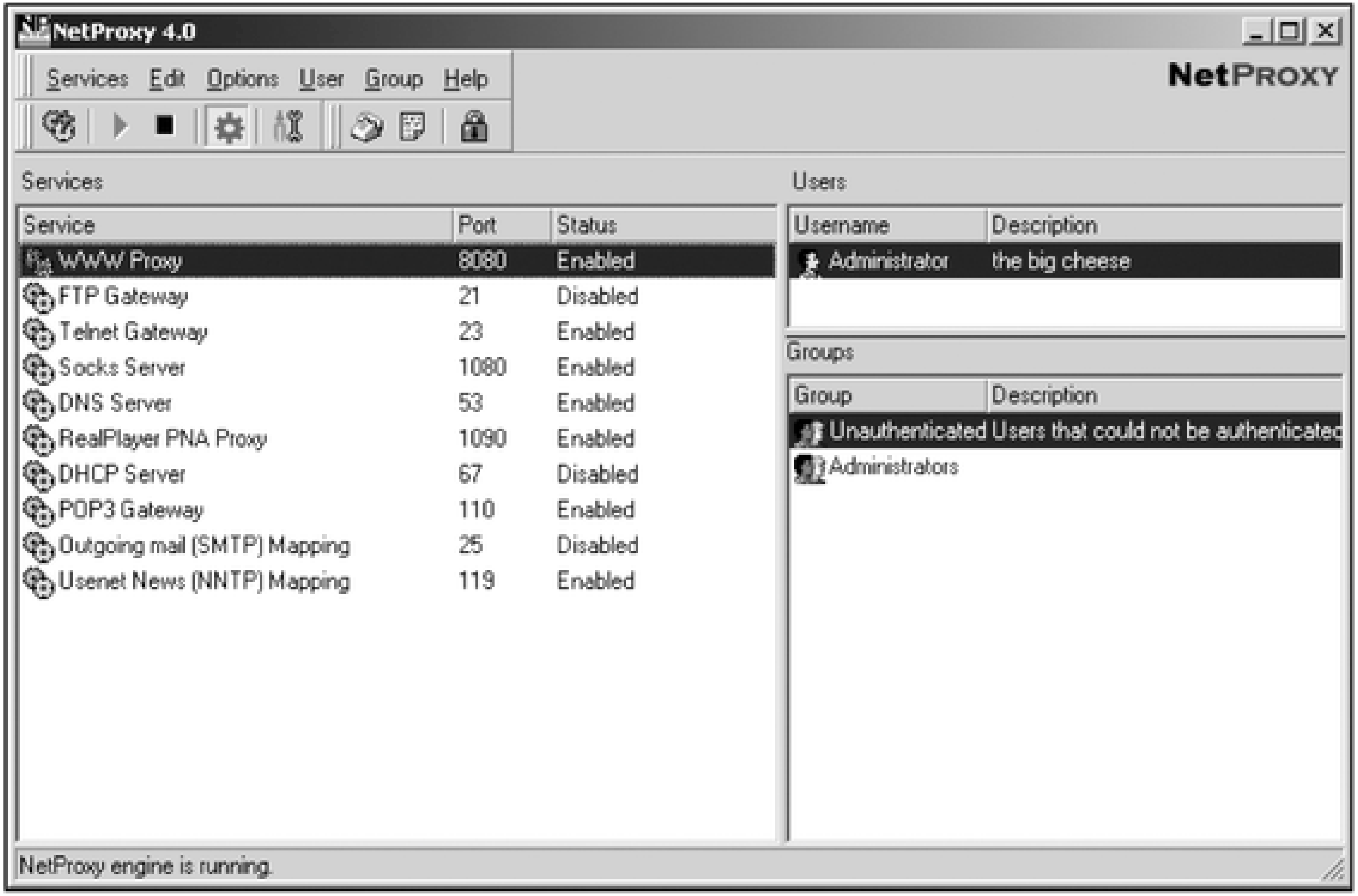
Working with Client Configurations (continued)



```
// Sample autoproxy.pac configuration file for use with NetProxy 4.00
//
// This assumes NetProxy is running on 192.168.0.1 and that the
// HTTP proxy service is enabled on port 8080 and the SOCKS gateway
// enabled on port 1080.

function FindProxyForURL(url, host)
{
  if ((url.substring(0,5) == "http:")
      || (url.substring(0,6) == "https:")) {
    return "PROXY 192.168.0.1:8080";  }
  else { return "SOCKS 192.168.0.1:1080; DIRECT; ";  }
}
```

Working with Service Configurations



Services

Service	Port	Status
WWW Proxy	8080	Enabled
FTP Gateway	21	Disabled
Telnet Gateway	23	Enabled
Socks Server	1080	Enabled
DNS Server	53	Enabled
RealPlayer PNA Proxy	1090	Enabled
DHCP Server	67	Disabled
POP3 Gateway	110	Enabled
Outgoing mail (SMTP) Mapping	25	Disabled
Usenet News (NNTP) Mapping	119	Enabled

Users

Username	Description
Administrator	the big cheese

Groups

Group	Description
Unauthenticated	Users that could not be authenticated
Administrators	

NetProxy engine is running.

Creating Filter Rules

- Allow certain hosts to bypass the proxy
- Filter out URLs
- Enable internal users to send outbound requests only at certain times
- Govern length of time a session can last

Security Vulnerabilities: Single Point of Failure

- Be sure to have other means of enabling traffic to flow with some amount of protection (e.g., packet filtering)
- Create multiple proxies that are in use simultaneously

Security Vulnerabilities: Buffer Overflow

- Occur when proxy server attempts to store more data in a buffer than the buffer can hold
- Render the program nonfunctional
- Check Web site of manufacturer for security patches

Choosing a Proxy Server

- Some are commercial products for home and small-business users
- Some are designed to protect one type of service and to serve Web pages stored in cache
- Most are part of a hybrid firewall (combining several different security technologies)
- Some are true standalone proxy servers

Types of Proxy Servers

- Transparent
- Nontransparent
- SOCKS based

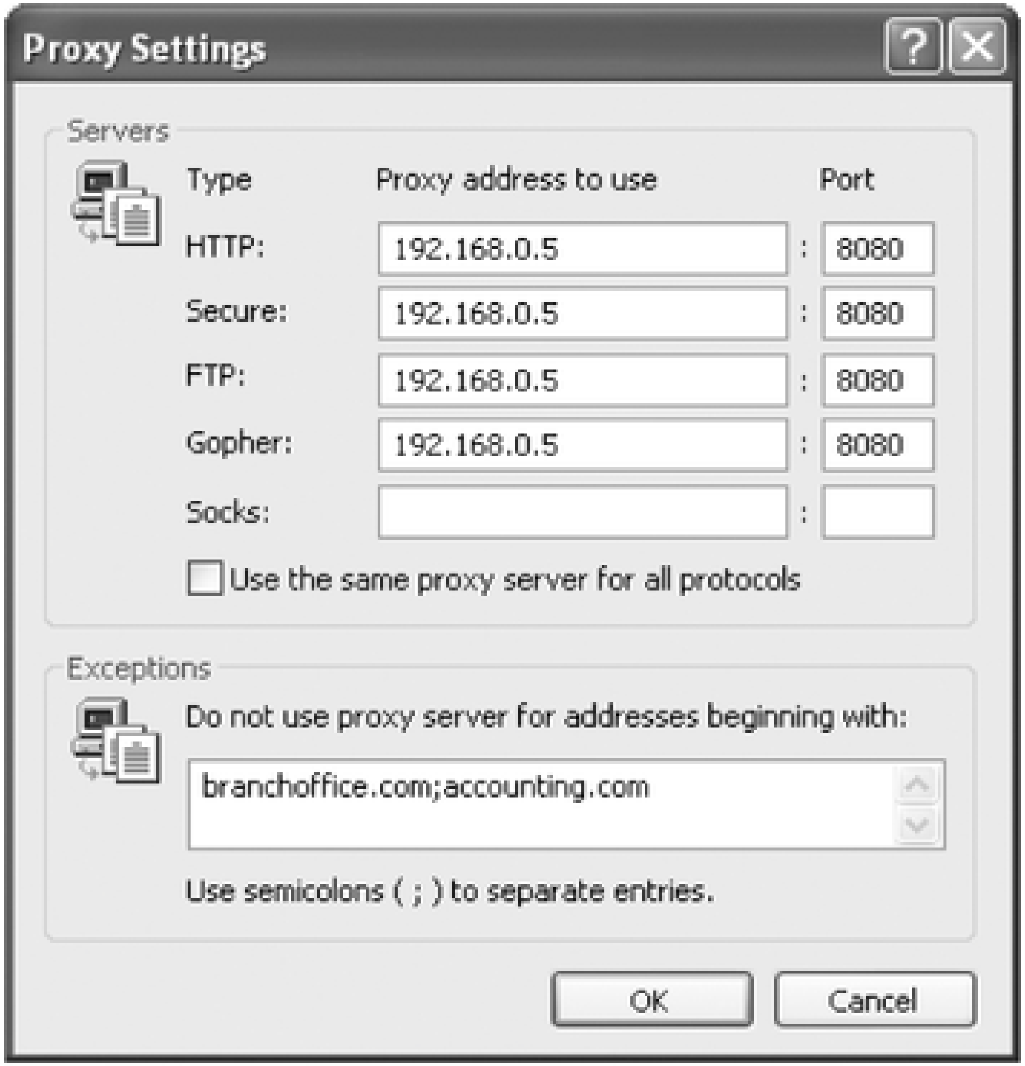
Transparent Proxies

- Can be configured to be totally invisible to end user
- Sit between two networks like a router
- Individual host does not know its traffic is being intercepted
- Client software does not have to be configured

Nontransparent Proxies

- Require client software to be configured to use the proxy server
- All target traffic is forwarded to the proxy at a single target port (typically use SOCKS protocol)
- More complicated to configure but provide greater security
- Also called explicit proxies

Nontransparent Proxies (continued)



Servers

Type	Proxy address to use	Port
HTTP:	192.168.0.5	8080
Secure:	192.168.0.5	8080
FTP:	192.168.0.5	8080
Gopher:	192.168.0.5	8080
Socks:		

□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

branchoffice.com;accounting.com

Use semicolons (;) to separate entries.

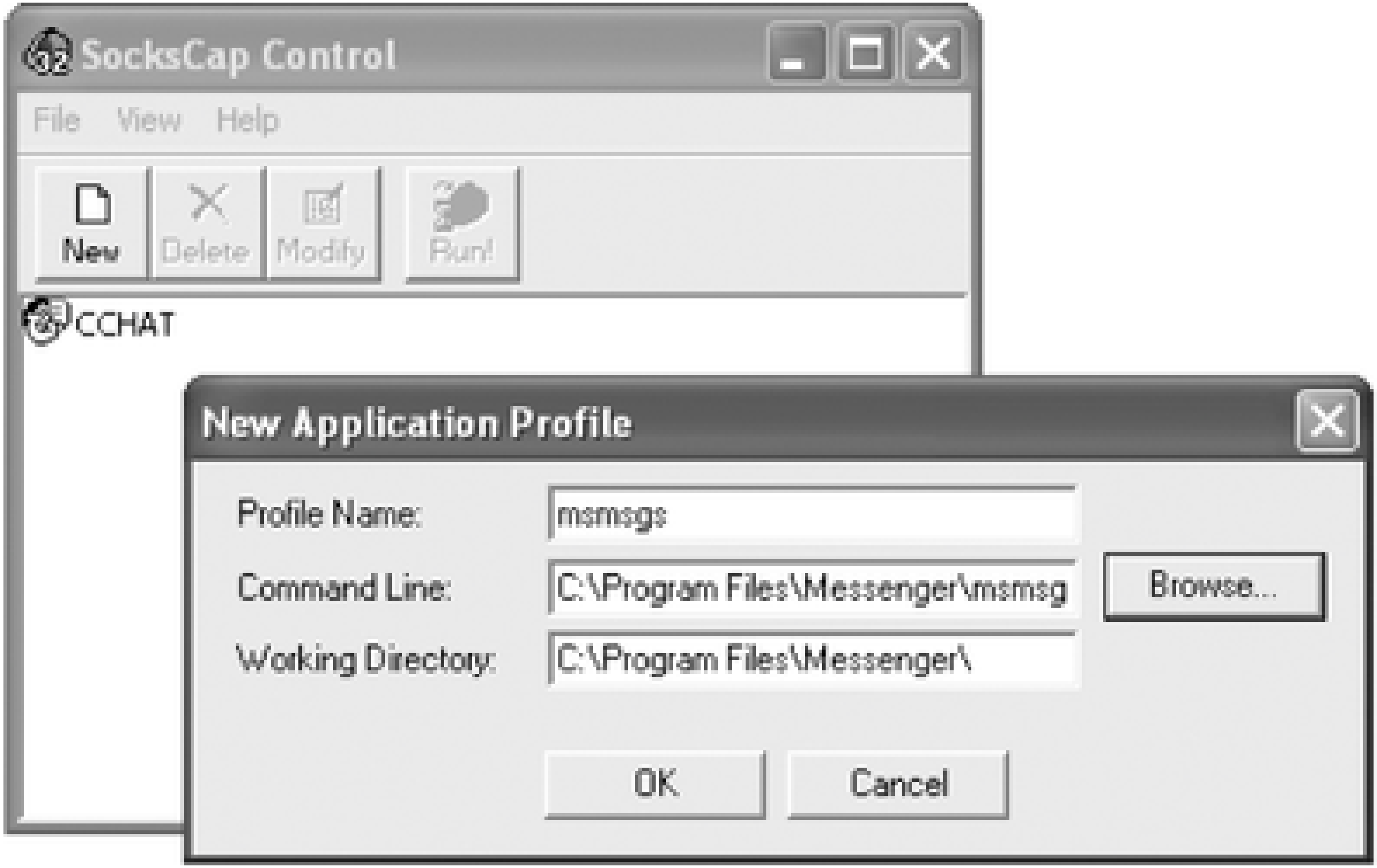
SOCKS-Based Proxies

- SOCKS protocol
  - Enables establishment of generic proxy applications
  - Flexible
  - Typically used to direct all traffic from client to the proxy using a target port of TCP/1080

SOCKS Features

- Security-related advantages
  - Functions as a circuit-level gateway
  - Encrypts data passing between client and proxy
  - Uses a single protocol both to transfer data via TCP and UDP and to authenticate users
- Disadvantage
  - Does not examine data part of a packet

SocksCap



Profile Name: msmsgs

Command Line: C:\Program Files\Messenger\msmsg

Working Directory: C:\Program Files\Messenger\

Proxy Server-Based Firewalls Compared

- Firewalls based on proxy servers:
  - T.REX
  - Squid
  - WinGate
  - Symantec Enterprise Firewall
  - Microsoft Internet Security & Acceleration Server
- Choice depends on your platform and the number of hosts and services you need to protect

T.REX Open-Source Firewall

- Free UNIX-based solution
- Handles URL blocking, encryption, and authentication
- Complex configuration; requires proficiency with proxy server configuration

Squid

- High-performance, free open-source application
- Acts as a proxy server and caches files for Web and FTP servers
- Not full-featured
  - Performs access control and filtering
  - Quickly serves files that are held in cache
- Runs on UNIX-based systems
- Popular; plug-ins available
- Economical

WinGate

- Most popular proxy server for home and small business environments
- Well-documented Windows-based program
- Offers customer support and frequent upgrades

Symantec Enterprise Firewall

- Combines proxy services with encryption, authentication, load balancing, and packet filtering
- Configured through a snap-in to the MMC
- Commercial firewall with built-in proxy servers
- More full-featured than WinGate

Microsoft Internet Security & Acceleration Server (ISA)

- Complex, full-featured
- Includes stateful packet filtering, proxy services, NAT, and intrusion detection
- Competes with high-performance firewall products

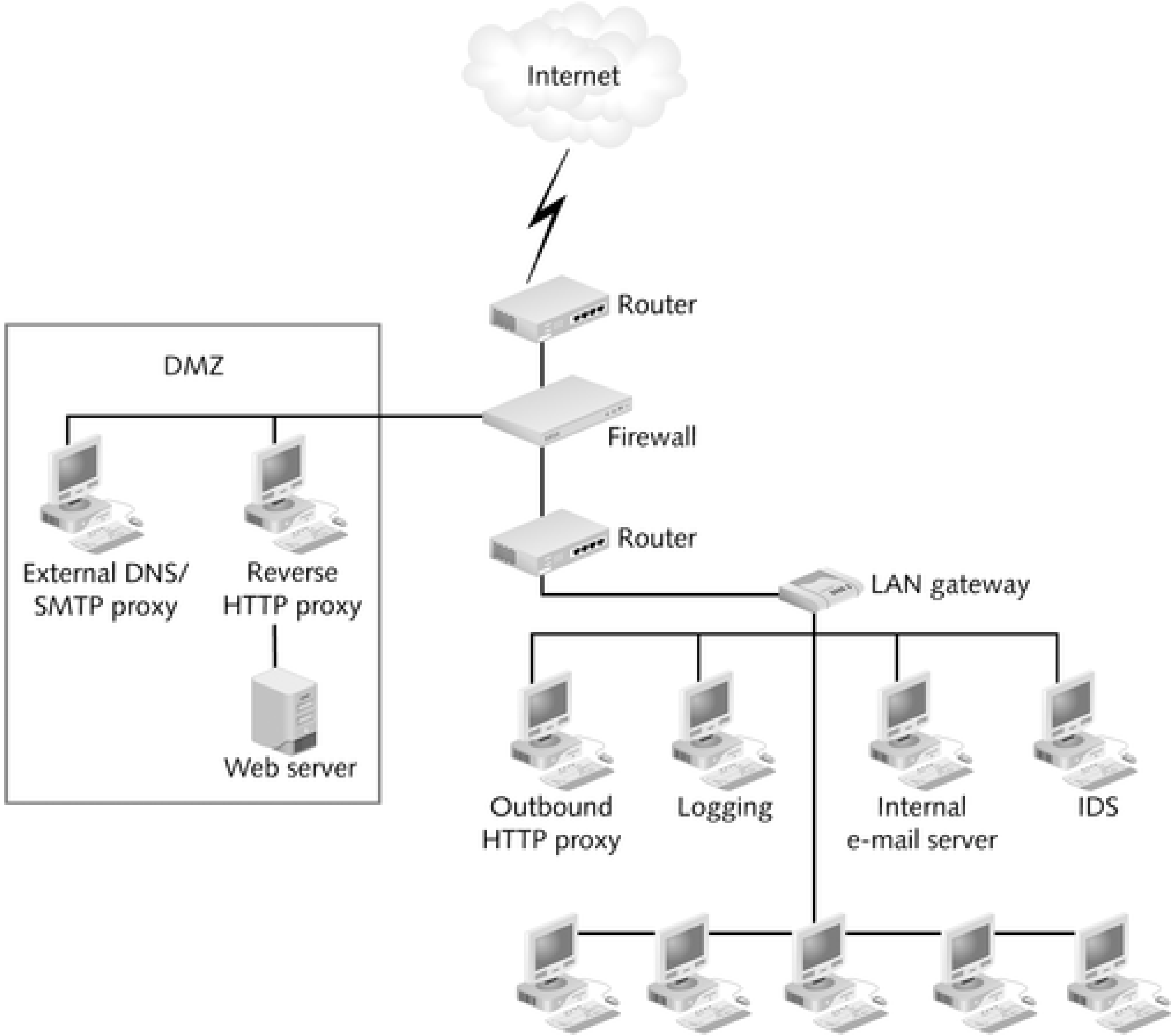
Two Editions of ISA

- Standard Edition
  - Standalone
  - Supports up to four processors
- Enterprise Edition
  - Multiserver product with centralized management
  - No limit on number of processors supported

Reverse Proxies

- Monitor inbound traffic
- Prevent direct, unmonitored access to server’s data from outside the company
- Advantages
  - Performance
  - Privacy

Reverse Proxies (continued)



When a Proxy Service Isn’t the Correct Choice

- Can slow down traffic excessively
- The need to authenticate via the proxy server can make connection impossible
- If you don’t want to use your own proxy server:
  - External users can connect to firewall directly using Secure Sockets Layer (SSL) encryption
  - Use proxy server of an ISP

Chapter Summary

- Overview of proxy servers and how they work
- Goals of proxy servers
- Vulnerabilities and other drawbacks that proxy servers bring to a security setup
- Kinds of proxy servers
- Comparison of proxy-based firewalls