Session 37CO

TCP/IP Intrusion Detection 101

Mike Williams

(mdw@us.ibm.com)

This publication may refer to products that are not currently available in your country.
IBM makes no commitment to make available any products referred to herein.

Agenda

- TCP/IP Intrusion Detection basics
  - Why worry and what you should worry about
- Classifying TCP/IP Intrusions
  - What do they look like
  - How can they be detected
- What is available on the AS/400 to help?
- Reference Information
- Q & A

TCP/IP Intrusion Detection Basics

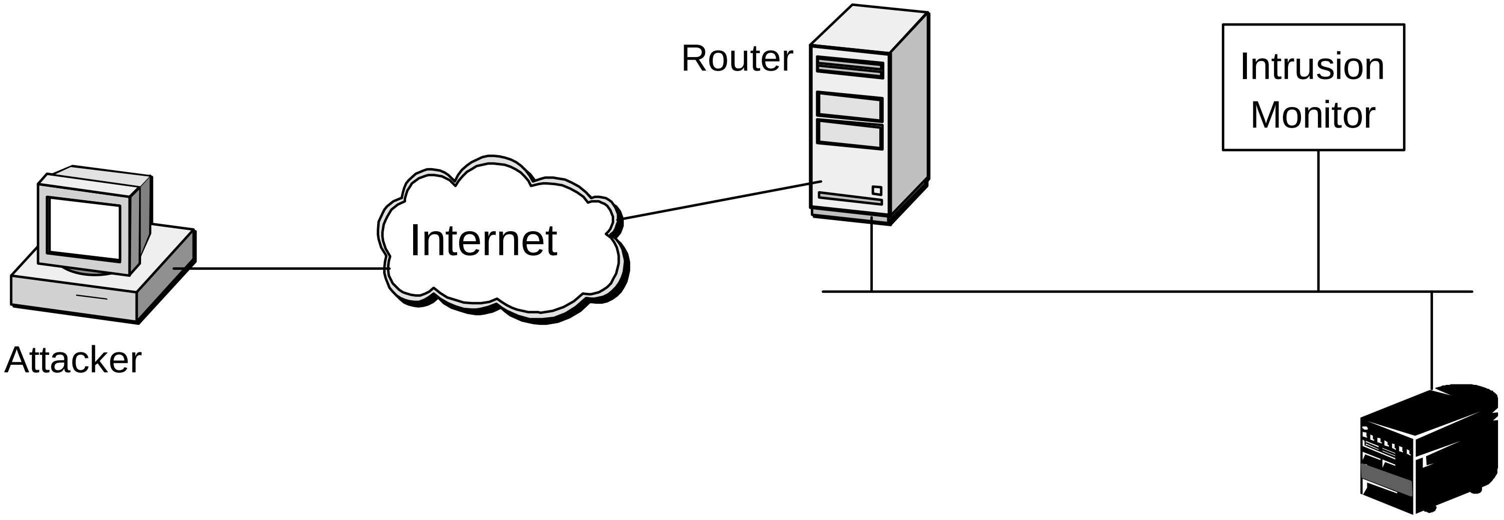
Why detect network intrusion attempts?

- "Over the past year there has been a rise in attempts by cyber thieves to break into corporate systems where much of the valuable business data is stored"

  According to, "Corporate America’s Security Intelligence Risk," an upcoming WarRoom research report

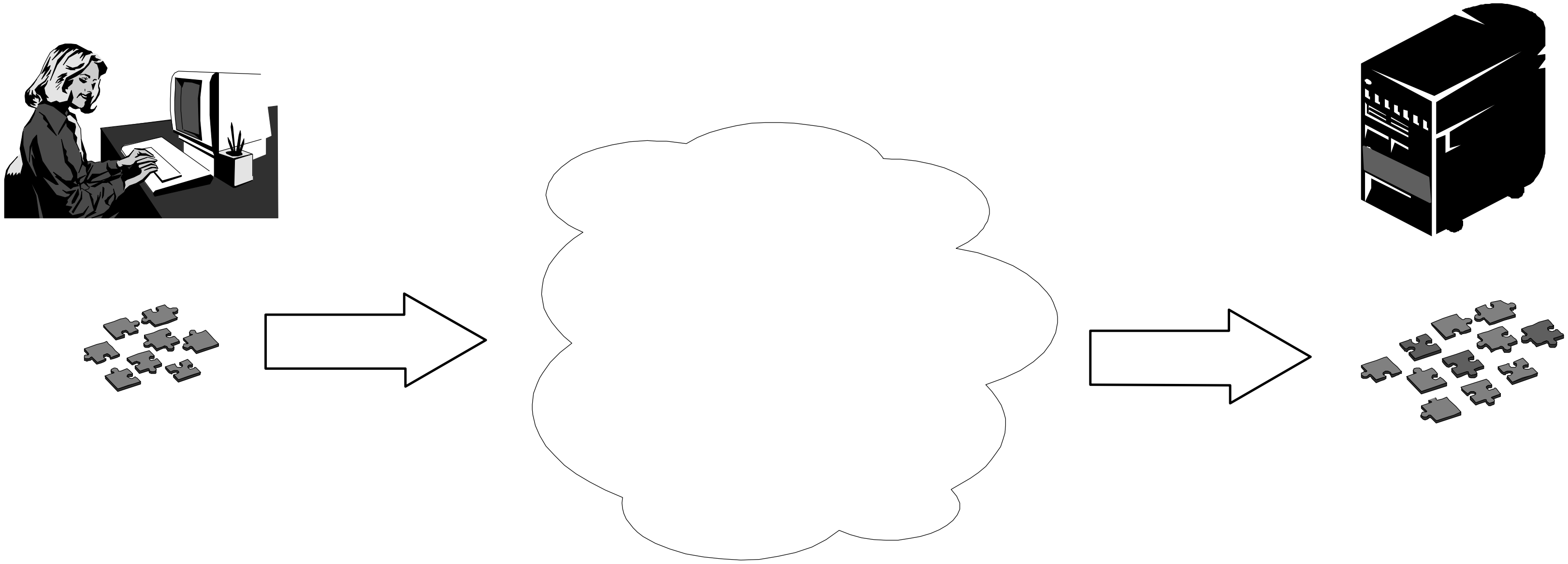
- Intrusion detection should be a key part of your overall network architecture and network security policy.
  - Without a *network security policy*, none of this matters.
- Intrusion detection is not good enough by itself and should be used with a combination of firewalls, authentication, and encryption.

ID cannot be done alone....



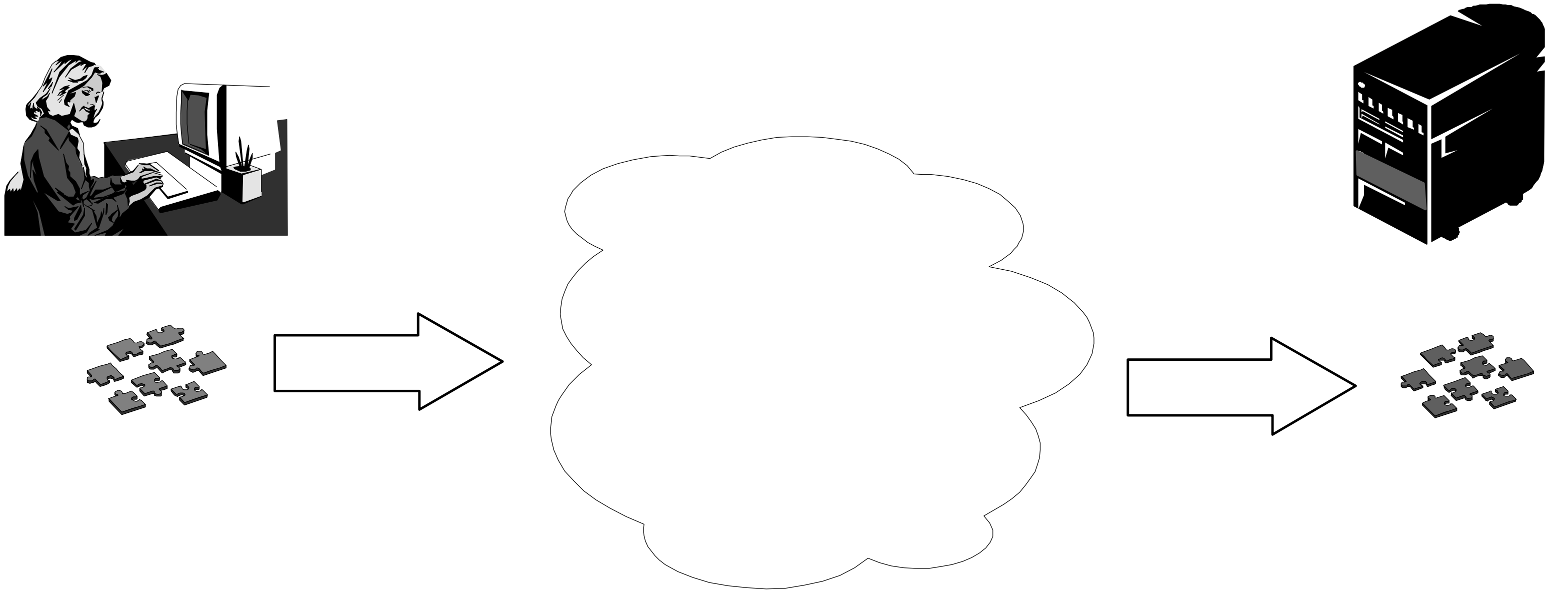
- Even some of the most basic configurations may require more than what any single system can do alone.
  - The Intrusion Detection Monitor System monitors traffic on the network.
  - However, the systems on the network need to also properly prepare and handle instrusion attempts

Invasion Intrusion Attempts



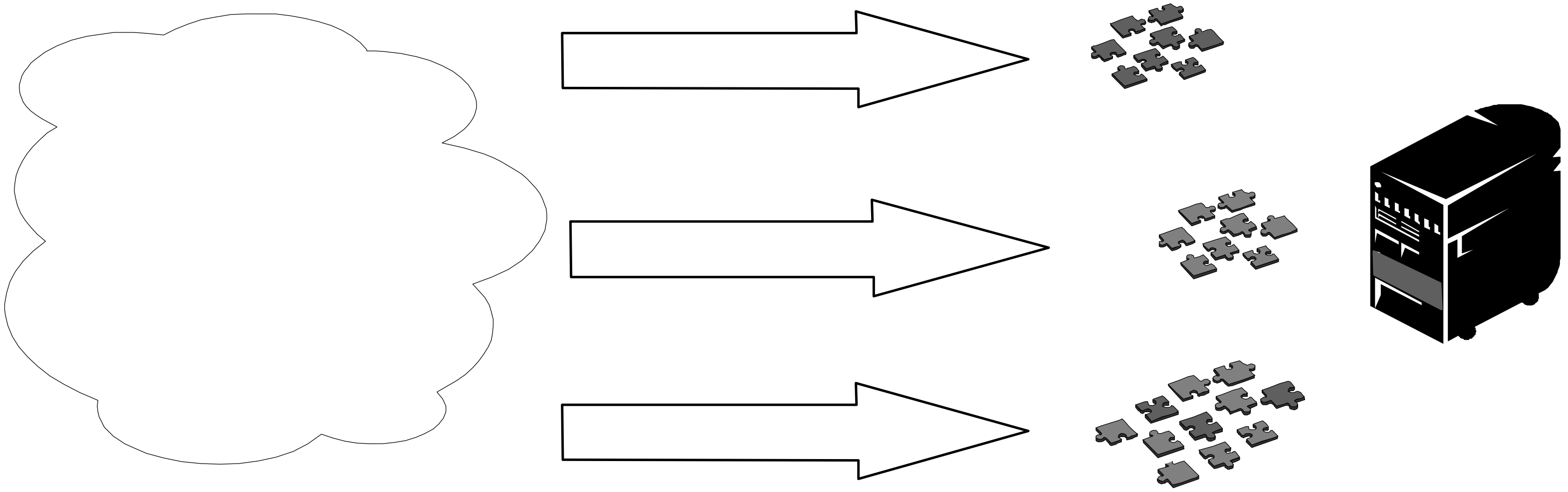
- Data is *added* to legitimate TCP/IP traffic
- Defeats the ability to perform pattern matching ("signature analysis") on known types of attacks

Evasion Intrusion Attempts



- Legitimate TCP/IP traffic is *replaced*
- Defeats the ability to perform pattern matching ("signature analysis") on known types of attacks

Denial of Service Attacks



- System is bombarded with requests and data
- Or with data that is able to break the receiving system

What makes Intrusions possible?

- The peculiarities of communication protocols.

- At the transport layer, TCP can transmit any amount of data
  - "Sequencing" allows the data to be spread accross several unordered packets
  - "Reassembly" is performed by the end system

- At the network layer, IP is may use "fragmentation" to allow for trasmission between systems.

Classifying TCP/IP Intrusions

What you need to watch for.....

- Systems areas to monitor for intrusion detection:
  - System Probing
  - Abnormal system utilization
  - Blatant access attempts
  - Abnormal deletions ("Covering their tracks")
  - Installing backdoors
  - Activation of services
  - Server exploitation

System Probing

- Areas to monitor for System Probing intrusion attempts
  - Connection attempts to inactive servers
  - Packets with source routing
    - These packets should not be forwarded
  - Packets denied due to packet filtering rules
    - Journaling can be enabled for native packet filtering
  - TCP/IP connections left in an unusual state
    - Connection in FIN-WAIT state for minutes
    - Netstat can help analyze this
  - Excessive PINGs and other ICMP traffic

Abnormal System Utilization

- Areas to monitor for Abnormal System Utilization
  - Abnormal or excessive CPU usage
  - Abnormal or excessive I/O usage
    - Bandwidth used
  - Disk usage
  - Use of services outside of normal working times
    - TELNET at 3:00 AM
  - CPU, I/O, and Disk can be monitored via performance monitoring on the AS/400

Blatant access attempts

- Areas to monitor for Blatant access attempts
  - Authentication failures (SSL and IPSec)
  - Authorization failures to objects
  - SSL key operation failure
  - Digital signature verification failure
  - Authentication and authorization failures are audited in the AS/400 Audit Journal

Abnormal deletions

- Areas to monitor for abnormal deletions
  - Audit log deletion
  - Deleting QSYSOPR, QSYSMSG, or QHST messages
  - Deleting problem log entries
  - Changing audit status
  - Stopping monitor program
  - Changes and deletions to objects can be monitored in the AS/400 Audit Journal

Installing backdoors

- **Areas to monitor for installation of backdoors**
  - **New objects installed on the system**
  - **Changes in (can be monitored via auditing):**
    - **System value**
    - **User profile**
    - **Validation list**
    - **Object authority**
    - **Work management (job descriptions, subsystem, etc.)**
    - **Job scheduler**
    - **Programs or service programs**
    - **Files**
    - **Communication configurations (Lines, interfaces, etc)**
    - **PTF installation/removal**

Activation of services

- Areas to monitor for abnormal activation of services
  - Job started
  - Subsystem started
  - Communication lines varied on/off
  - Servers being started
    - TCP/IP servers
    - Client Access servers
  - Starting and stopping job, servers, and communication lines can all be monitored using the AS/400 Audit Journal

Server exploitation

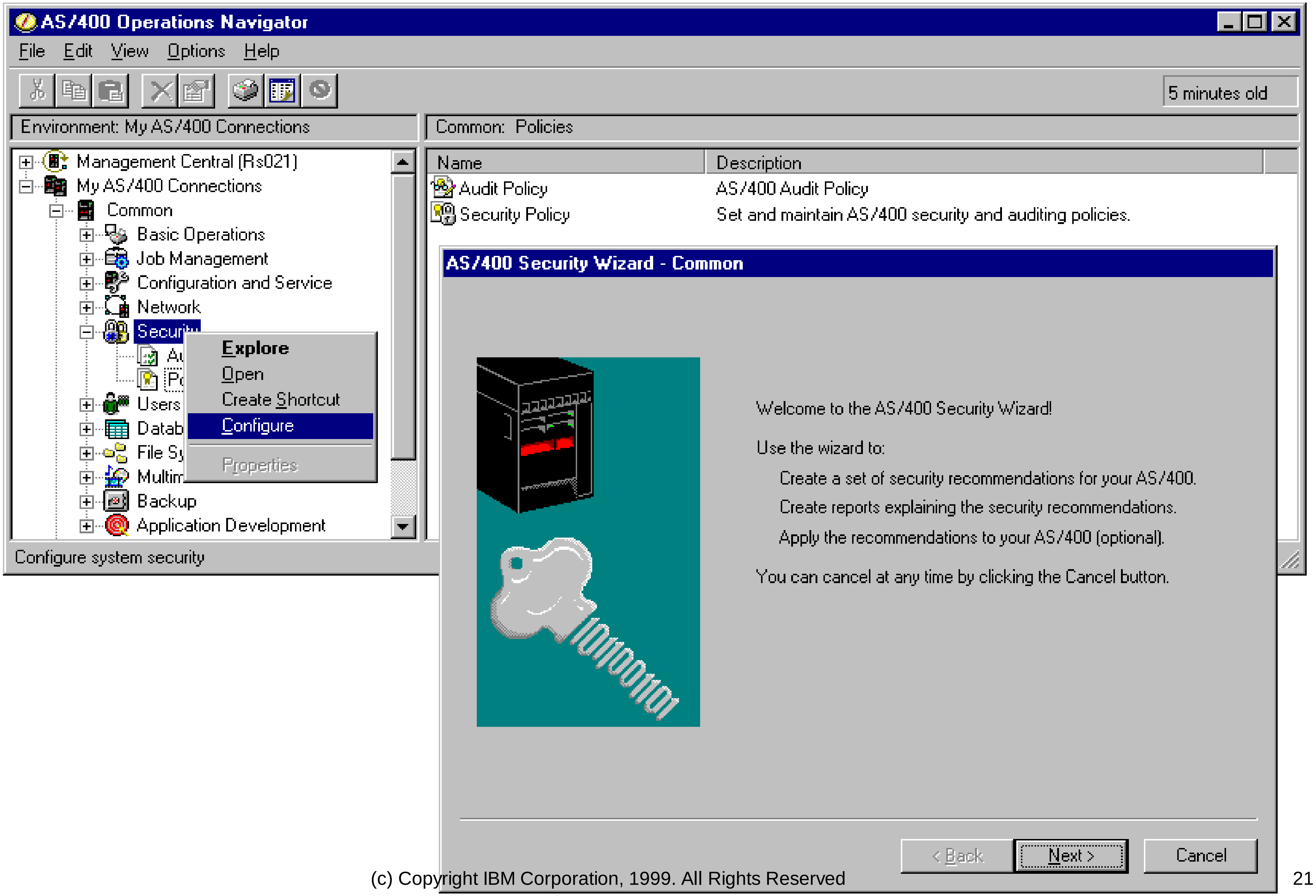
- Items to monitor for server exploitation
  - Pattern matching ("signature analysis") and thresholds
  - General monitoring items:
    - Malformed requests
    - Authentication failures
    - Invalid request methods
    - Trend deviation
  - Servers:
    - HTTP (invalid URLs, DoS triggers, cgi-bin program failures)
    - FTP (invalid path)
    - SMTP (spamming, mail volume for a specific user)
    - DNS (zone transfers, reverse queries for site mapping)
    - TELNET
    - Domino

What is available on the AS/400 to help

How the AS/400 can help today!

- World Class System Security
  - System Security Wizard
  - AS/400 Object Security
- General IP Security features
  - IP Packet Filtering and NAT
  - Port Restrictions
- System wide Auditing and Journaling
- Server specific protection
  - HTTP
  - Mail
  - DNS
  - Telnet
  - FTP
  - RouteD

Setting up system security



Welcome to the AS/400 Security Wizard!

Use the wizard to:

Create a set of security recommendations for your AS/400.

Create reports explaining the security recommendations.

Apply the recommendations to your AS/400 (optional).

You can cancel at any time by clicking the Cancel button.

The AS/400 Security Wizard

- Asks high level systems questions, for example..
  - Does your AS/400 use TCP/IP to communicate with other systems in the network?
  - Is your AS/400 directly connected to the Internet or a network that is connected to the Internet?
  - Do you want audit security-related actions on your AS/400?
- Produces a Summary of the Security Recommendations
- Allows Recommendations to be applied

General TCP/IP Security Tips

- Only start TCP/IP servers that are needed
- Consider using non-routable IP addresses
- Prevent applications from using well-known ports
- Turn *IP Source Routing* off
- Allow *IP Datagram Forwarding* only when needed
- Don’t leave PPP or SLIP lines waiting in answer state

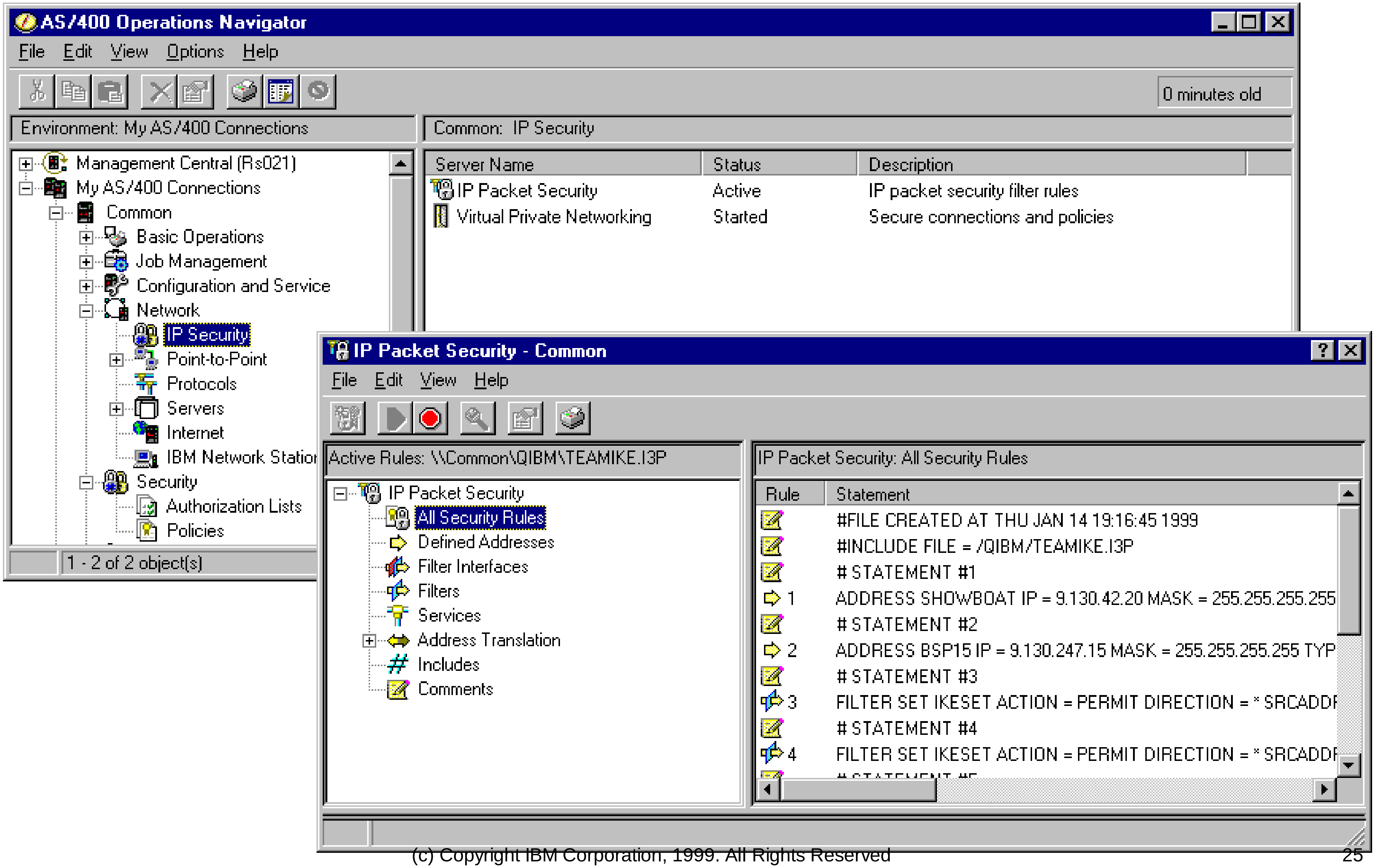
Native AS/400 Packet Security

- Introduced in V4R3

- IP Packet Filtering can be used to PERMIT or DENY based on the packet characteristics
  - Source and Destination IP Address
  - Source and Destination IP Port
  - Packet Direction
  - Packet Fragments

- IP Network Address Translation (NAT)
  - Can be used to hide private network behind a single public IP Interface (address)

Setting up Packet Security

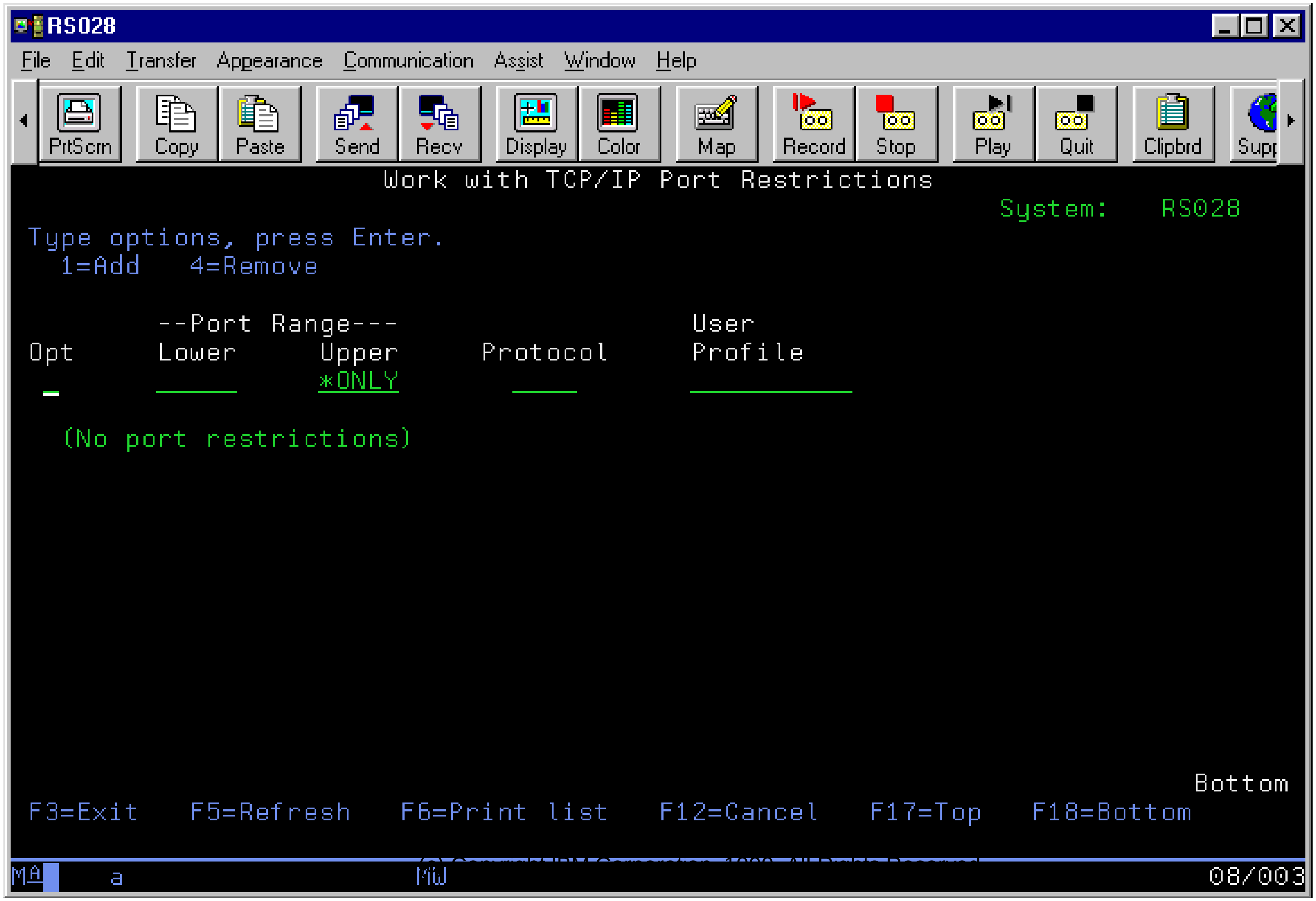


Server Name	Status	Description
IP Packet Security	Active	IP packet security filter rules
Virtual Private Networking	Started	Secure connections and policies

Rule	Statement
	#FILE CREATED AT THU JAN 14 19:16:45 1999
	#INCLUDE FILE = /QIBM/TEAMIKE.I3P
	# STATEMENT #1
1	ADDRESS SHOWBOAT IP = 9.130.42.20 MASK = 255.255.255.255
	# STATEMENT #2
2	ADDRESS BSP15 IP = 9.130.247.15 MASK = 255.255.255.255 TYP
	# STATEMENT #3
3	FILTER SET IKESET ACTION = PERMIT DIRECTION = * SRCADDI
	# STATEMENT #4
4	FILTER SET IKESET ACTION = PERMIT DIRECTION = * SRCADDI

Restricting AS/400 Ports

- Can be used to restrict what users can use what ports
- Can help prevent unauthorized use of well known ports



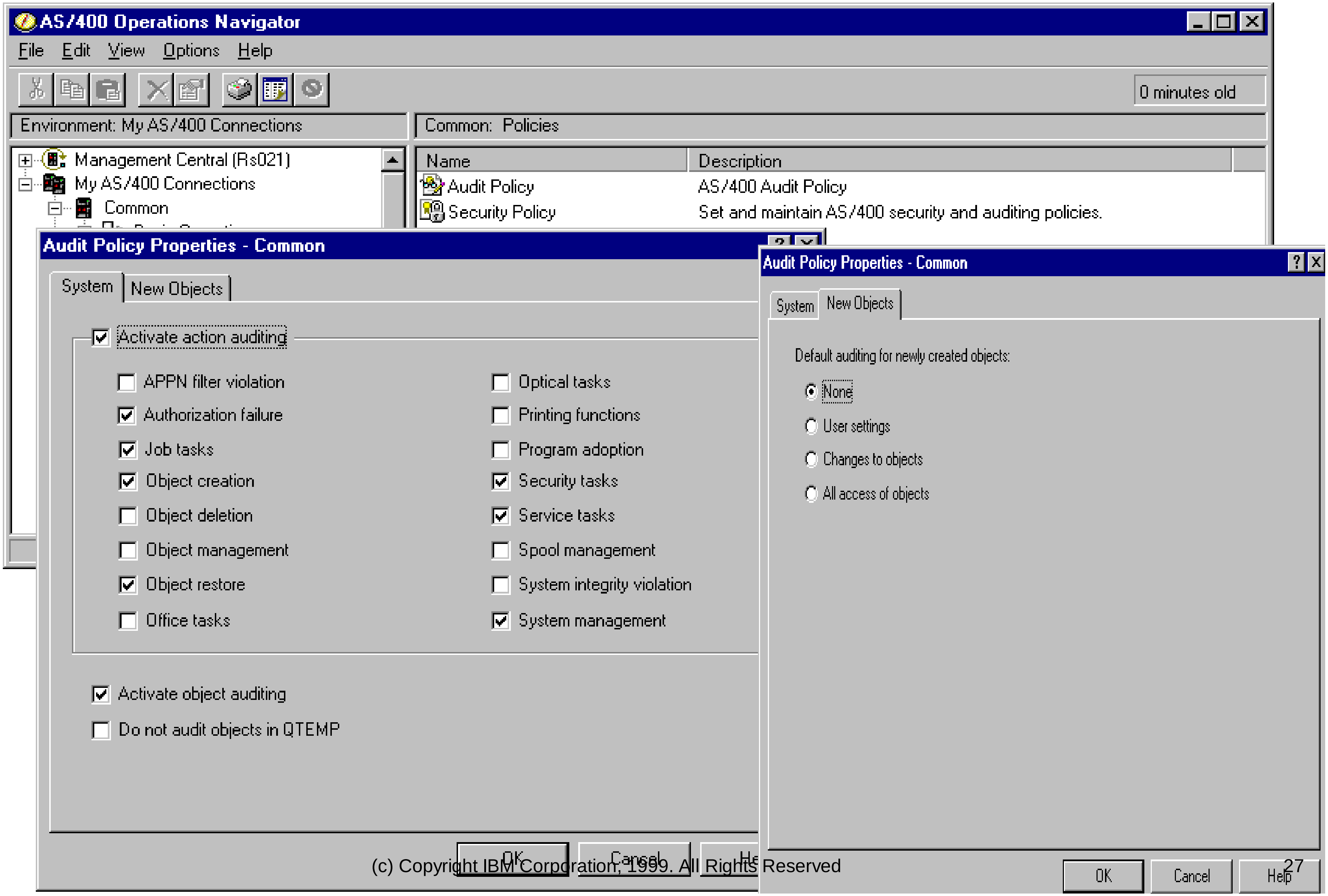
```
                         Work with TCP/IP Port Restrictions
                                                              System:    RS028
 Type options, press Enter.
   1=Add    4=Remove

         --Port Range---                            User
 Opt     Lower      Upper      Protocol           Profile
  _      _____      *ONLY        ____             __________

   (No port restrictions)

                                                                        Bottom
 F3=Exit    F5=Refresh    F6=Print list    F12=Cancel    F17=Top    F18=Bottom
```

Setting up AS/400 Auditing


AS/400 Operations Navigator
File Edit View Options Help
0 minutes old
Environment: My AS/400 Connections
Common: Policies
Management Central (Rs021)
My AS/400 Connections
Common
Name
Description
OK
Cancel
Help

Name	Description
Audit Policy	AS/400 Audit Policy
Security Policy	Set and maintain AS/400 security and auditing policies.

Audit Policy Properties - Common

System | New Objects

☑ Activate action auditing

- □ APPN filter violation
- ☑ Authorization failure
- ☑ Job tasks
- ☑ Object creation
- □ Object deletion
- □ Object management
- ☑ Object restore
- □ Office tasks
- □ Optical tasks
- □ Printing functions
- □ Program adoption
- ☑ Security tasks
- ☑ Service tasks
- □ Spool management
- □ System integrity violation
- ☑ System management

☑ Activate object auditing

□ Do not audit objects in QTEMP

Audit Policy Properties - Common

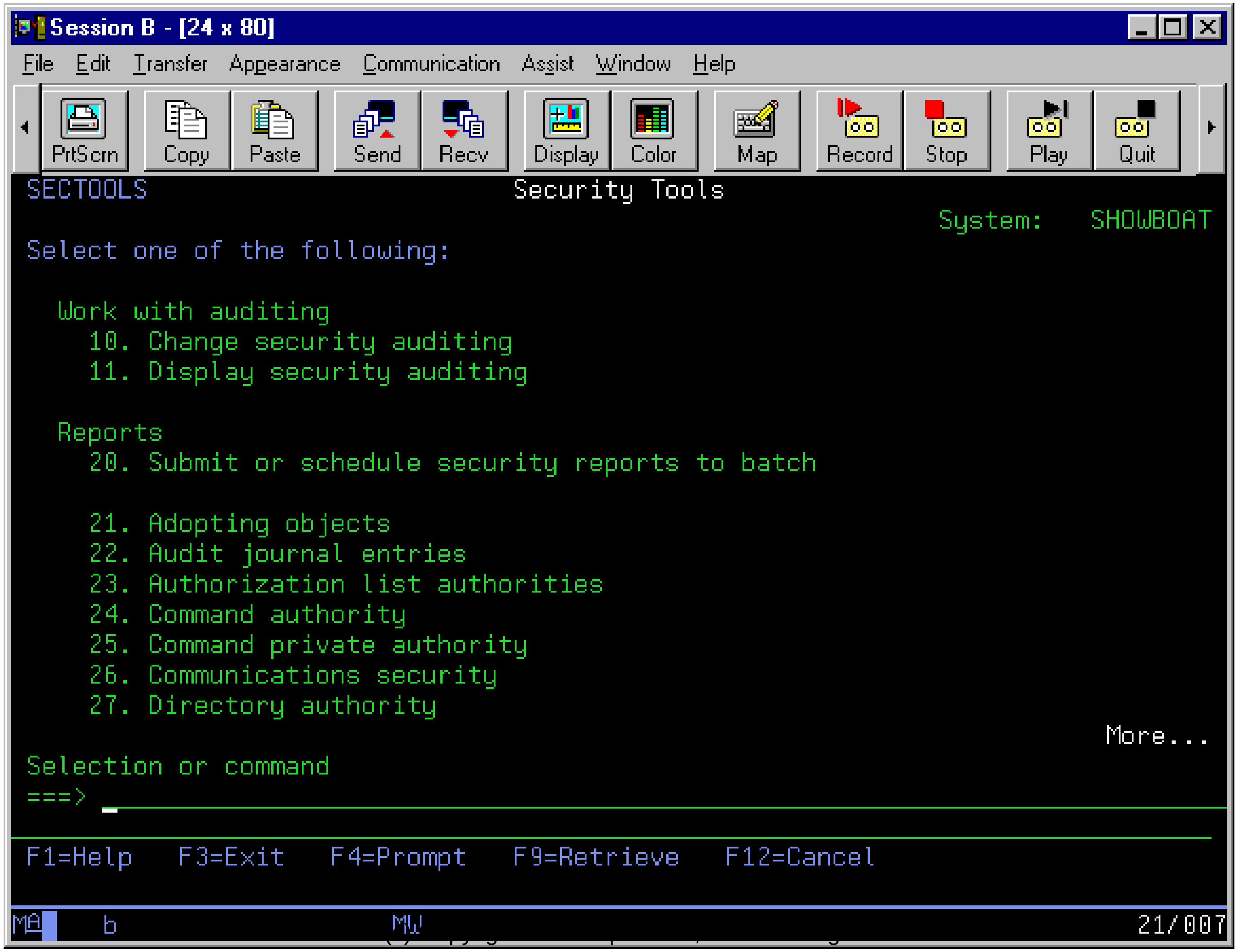
System | New Objects

Default auditing for newly created objects:

- ● None
- ○ User settings
- ○ Changes to objects
- ○ All access of objects

Working with Auditing results

- go sectools and create audit reports
- Third party tools available for analyzing auditing



```
SECTOOLS                        Security Tools
                                                        System:   SHOWBOAT
Select one of the following:

  Work with auditing
    10. Change security auditing
    11. Display security auditing

  Reports
    20. Submit or schedule security reports to batch

    21. Adopting objects
    22. Audit journal entries
    23. Authorization list authorities
    24. Command authority
    25. Command private authority
    26. Communications security
    27. Directory authority
                                                                     More...
Selection or command
===> _

F1=Help   F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel

MA    b                    MW                                         21/007
```

The Web and HTTP on the AS/400

- New Denial of Service Directives added
  - DenialOfServicePenalty
  - DenialOfServiceThreshold
  - DenialOfServiceTrusted

- Documented on the Web
  - HTTP Server for AS/400 Webmaster’s Guide
  - http://www.as400.ibm.com/http

- Available with the following PTFs
  - V4R1 SF49766
  - V4R2 SF49764
  - V4R3 SF50167

Mail on the AS/400

- SMTP the Simple Mail Transport Protocol
  - Spamming Prevention
    - Prevents unwanted connections
    - Prevents unwanted use as relay
    - Documented in the APAR cover letter
    - V4R2 - SF52864
    - V4R3 - SF53421
    - V4R4 - SF54014
- POP the Post Office Protocol
  - Excessive Mail Volume Prevention
    - Use AS/400 ASP to manage mail space
    - Set reasonable ASP thresholds

Telnet on the AS/400

- User Exit Program Available on the Web
  - http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr.htm
  - Allow and Disallow access based on IP Address or Subnet
  - Logging shows connections and denied access attempts
  - User Exits available in V4R2 with SF99033
- AS/400 System Values
  - QMAXSIGN defines number of failed attempts
  - QMAXSGNACN defines max signon action
    - Very Off Device
    - Disable User Profile
    - Very Off Device and Disable User Profile

FTP on the AS/400

- User Exists available starting in V3R2
  - Could write exits to prevent unwanted access
  - Could write exists to log access
- QMAXSIGN does not apply to FTP
- Unsuccessful sign-on attempts generate CPF2234 to be written to the QHST log

The AS/400 Domain Name System

- The AS/400 DNS supports Bind 4.9.3

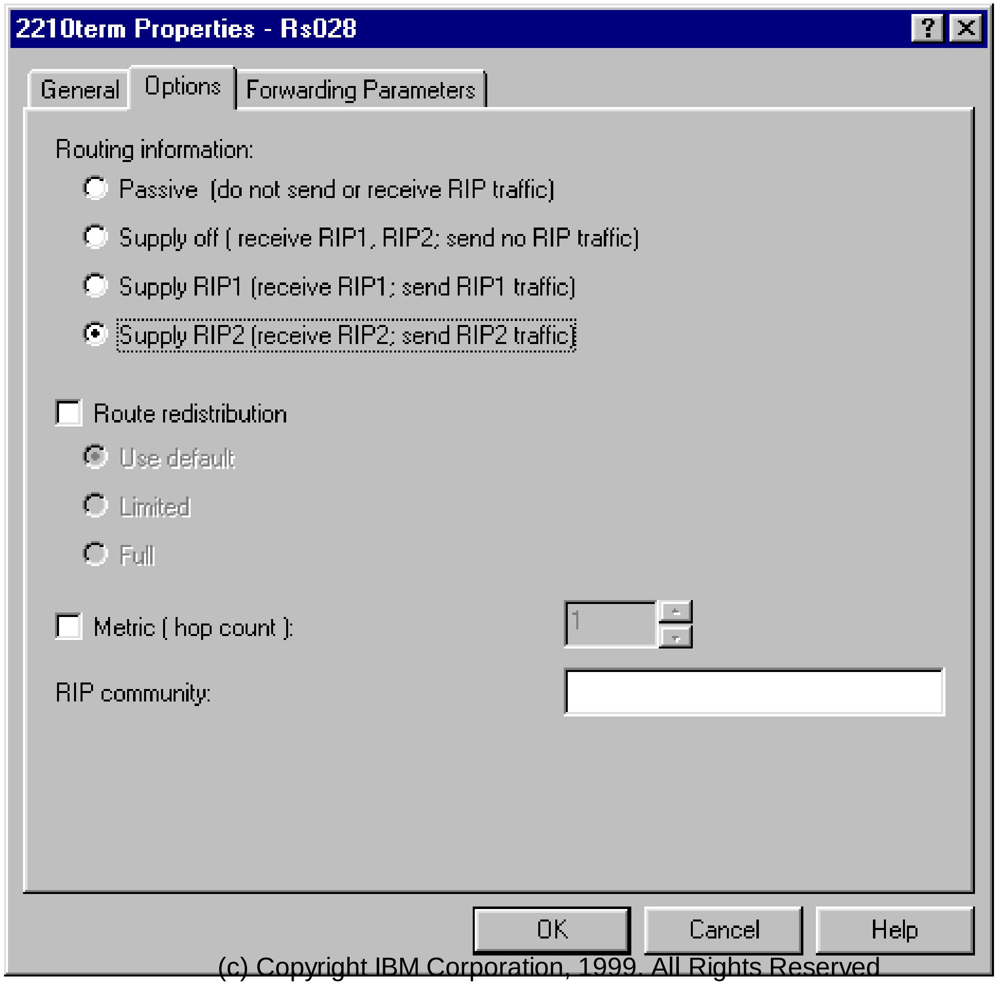
- xfernets: Restrict Zone Transfers
  - Restrict by IP Address
  - Restrict by Subnet

- secure-zone: Restrict Access to Domains
  - Restrict by IP Address
  - Restrict by Subnet

- secure-zone can also be used for reverse mapping

The AS/400 Routing Daemon ROUTED

- RIP Version 2 introduced in V4R2
- RIP v2 Uses Community Name to restrict access



2210term Properties - Rs028

Routing information:

○ Passive (do not send or receive RIP traffic)
○ Supply off (receive RIP1, RIP2; send no RIP traffic)
○ Supply RIP1 (receive RIP1; send RIP1 traffic)
● Supply RIP2 (receive RIP2; send RIP2 traffic)

☐ Route redistribution

● Use default
○ Limited
○ Full

☐ Metric (hop count): 1

RIP community:

Reference Information

- AS/400 Publications
  - AS/400 Tips and Tools for Securing Your AS/400 (SC41-5300)

- The AS/400 on the Web
  - www.as400.ibm.com
  - www.as400.ibm.com/tcpip
  - www.as400.ibm.com/tcpip/vpn
  - as400bks.rochester.ibm.com
  - redbooks.ibm.com

- Other resources on the Web
  - http://www.cs.purdue.edu/coast/ids

- Intrusion Detection Mail List
  - Send e-mail to "ids-request@uow.edu.au" with the word "help" in the message body

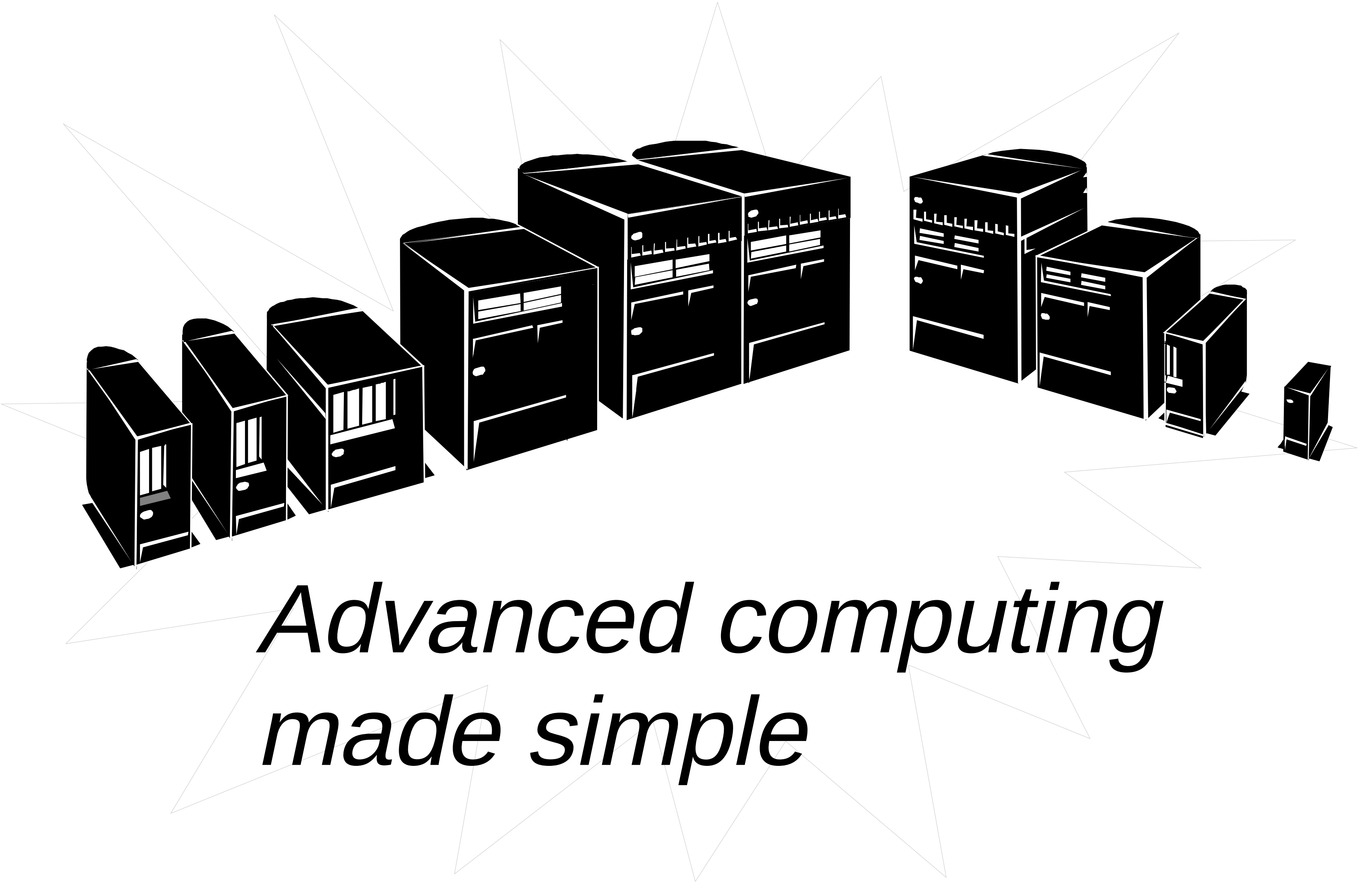
In summary.....

- A network security policy is a must!
- Instrusion detection should be an integral part of a network architecture and network security policy!
- Intrusion Detection and Monitoring requires participation from all systems in the network.
- Take a look at your AS/400 in the areas discussed and determine what changes you should make.

Notice

- This publication may refer to products that are not currently available in your country. IBM makes no commitment to make available any products referred to herein.
- Trademark and service marks:
  - AS/400, IBM, OS/400, AIX, OfficeVision, PROFS, OS/2, Facsimile Support/400 and APPN are trademarks of the IBM Corporation in the United States or other countries or both.
  - LOTUS, LOTUS Notes, cc:Mail, and cc:Mail for the Internet are trademarks of the LOTUS Development Corporation.
  - JAVA are registered trademarks of Sun Microsystems, Inc.
  - Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.
  - Other company, product and service names may be trademarks or service marks of others.

IBM AS/400e



Advanced computing made simple