AS/400e

AS400 VPN Technologies and Solutions

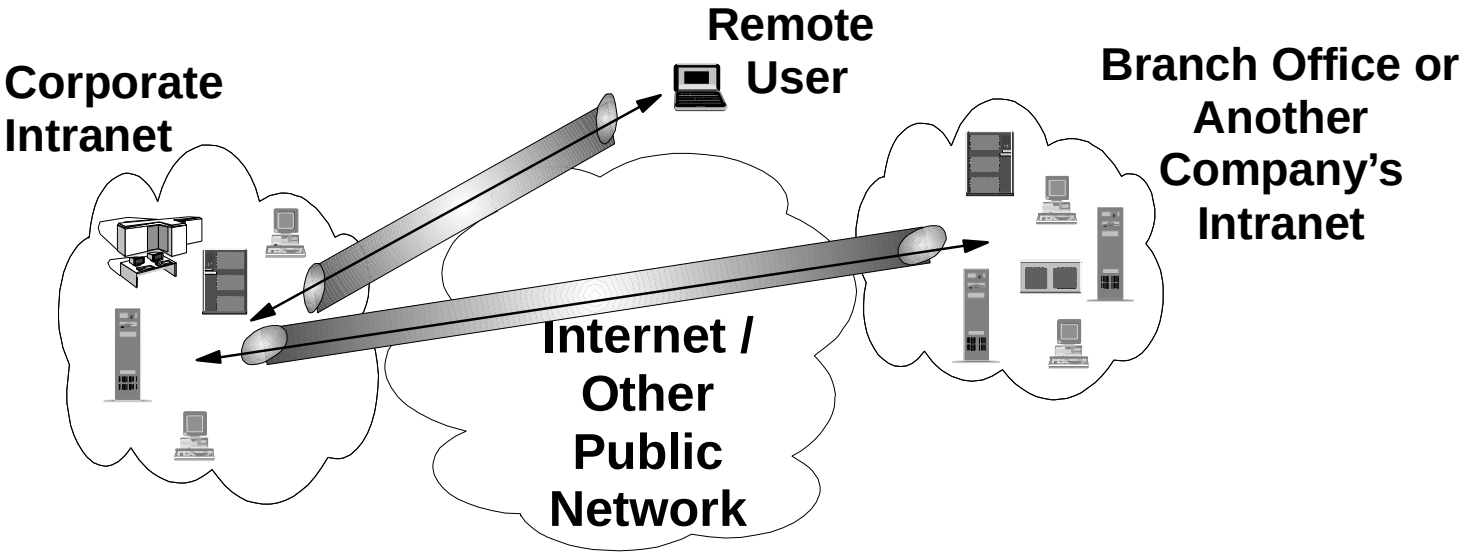
Frank V. Paxhia
paxhia@us.ibm.com

Agenda

- What is a VPN?
- Why would I want a VPN?
- What are some of the technologies that make a VPN possible?
- AS/400 VPN solutions
- What is new in V4R4
- An Example Configuration
- Q&A

What is a VPN?

What is a VPN?



- A VPN (Virtual Private Network) is an extension of an enterprise's private intranet, across a public network (such as the Internet), creating a secure connection
  - *encrypt the user's data*
  - *validate the user's data*
  - *authenticate the source of the data*
  - *establish & maintain cryptographic secrets*

Desirable VPN Characteristics

- **Secure**
  - **private (encrypted)**
  - **challenged (authenticated)**
  - **safe (integrity)**
- **Interoperable**
- **Centrally Managed**
- **Distributed, Deployable**
- **Applicable (applications can use it)**
- **Apple Pie (easy to use, competitive, integrated, intuitive)**

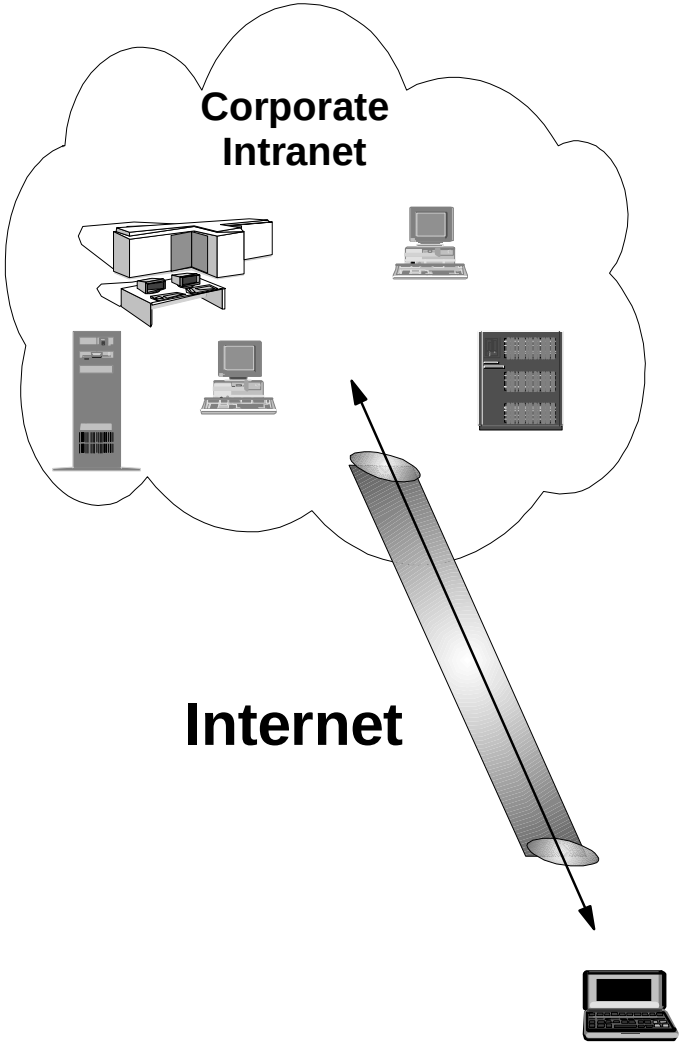
Motivations for building VPNs

VPN Motivators

- Bottom line, profit margins
  - using low cost public nets for business
- ebiz - VPNs might be required to play
- Business dynamics (aquisitions, geographical separation, mobile users)
- Security is key!

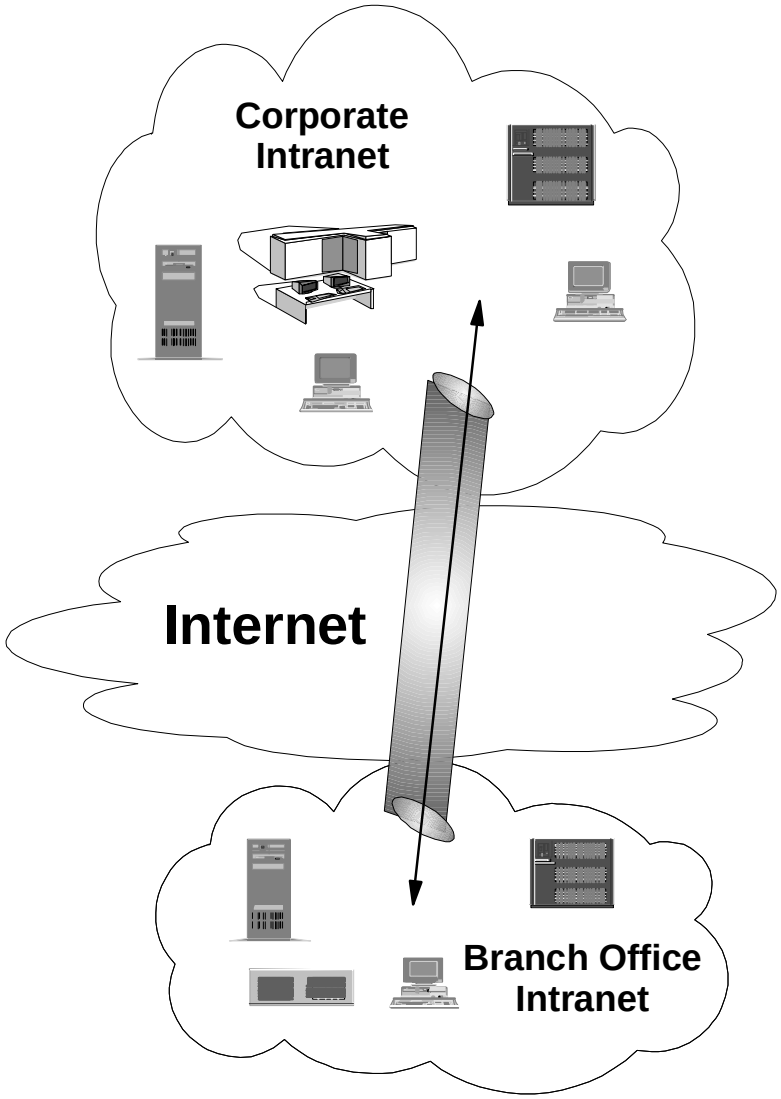
Mobile user VPN

- Allow access to corporate data , anywhere, anytime
- Reduce long distance charges, use local point of presence
- Utilize public networks (via ISPs)



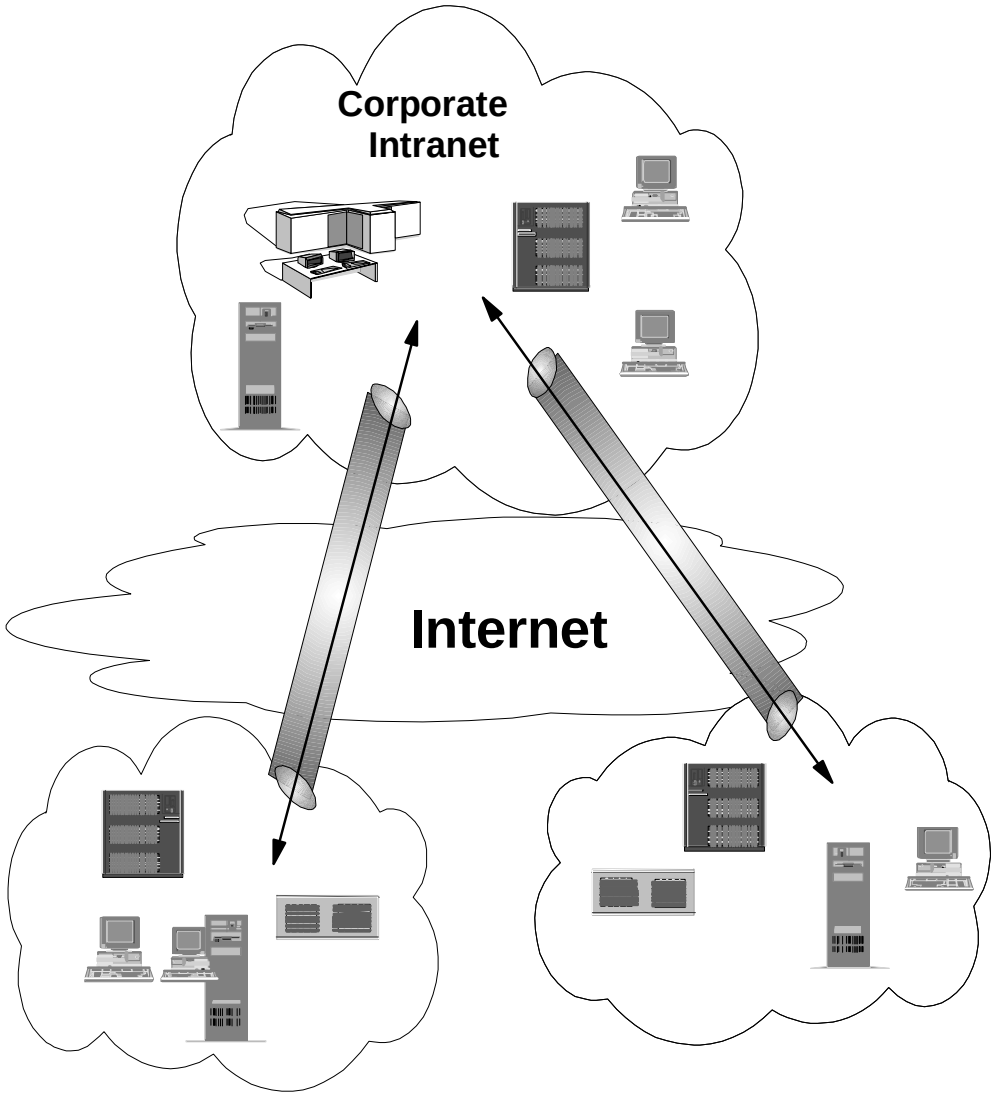
Branch Office VPN

- Give BO access to HQ Intranet
- Eliminate leased line costs, can have single connection provide access to Internet and HQ services
- Utilize public networks (via ISPs)



ExtraNet (ValueNet) VPN

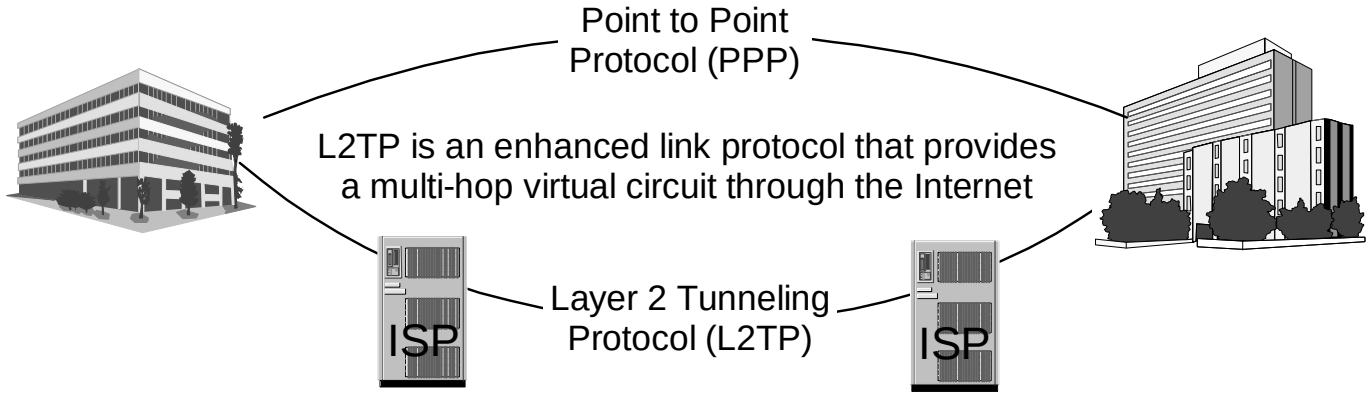
- Constructs co-operative, competitive businesses
- Improves communications, business processes
- Utilize public networks (via ISPs)



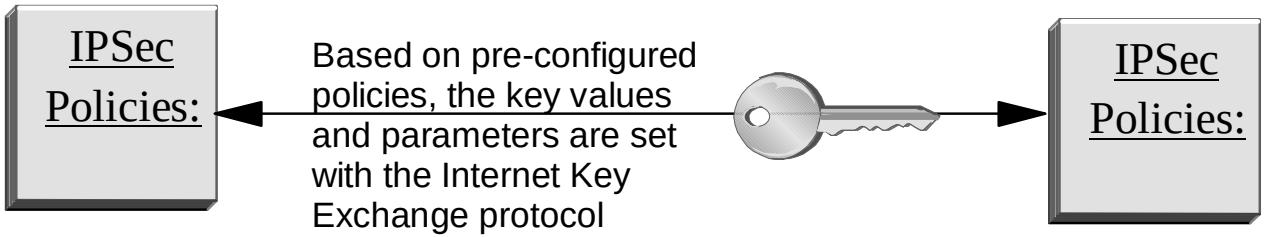
VPN Technologies

The Core VPN Standards Based Protocols

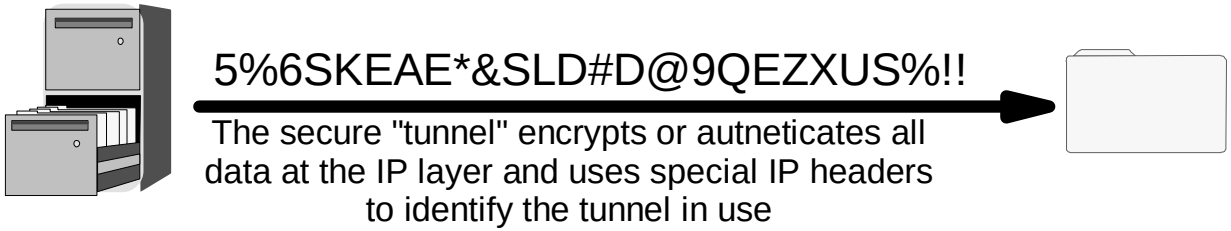
1. L2TP
open the link that creates the circuit



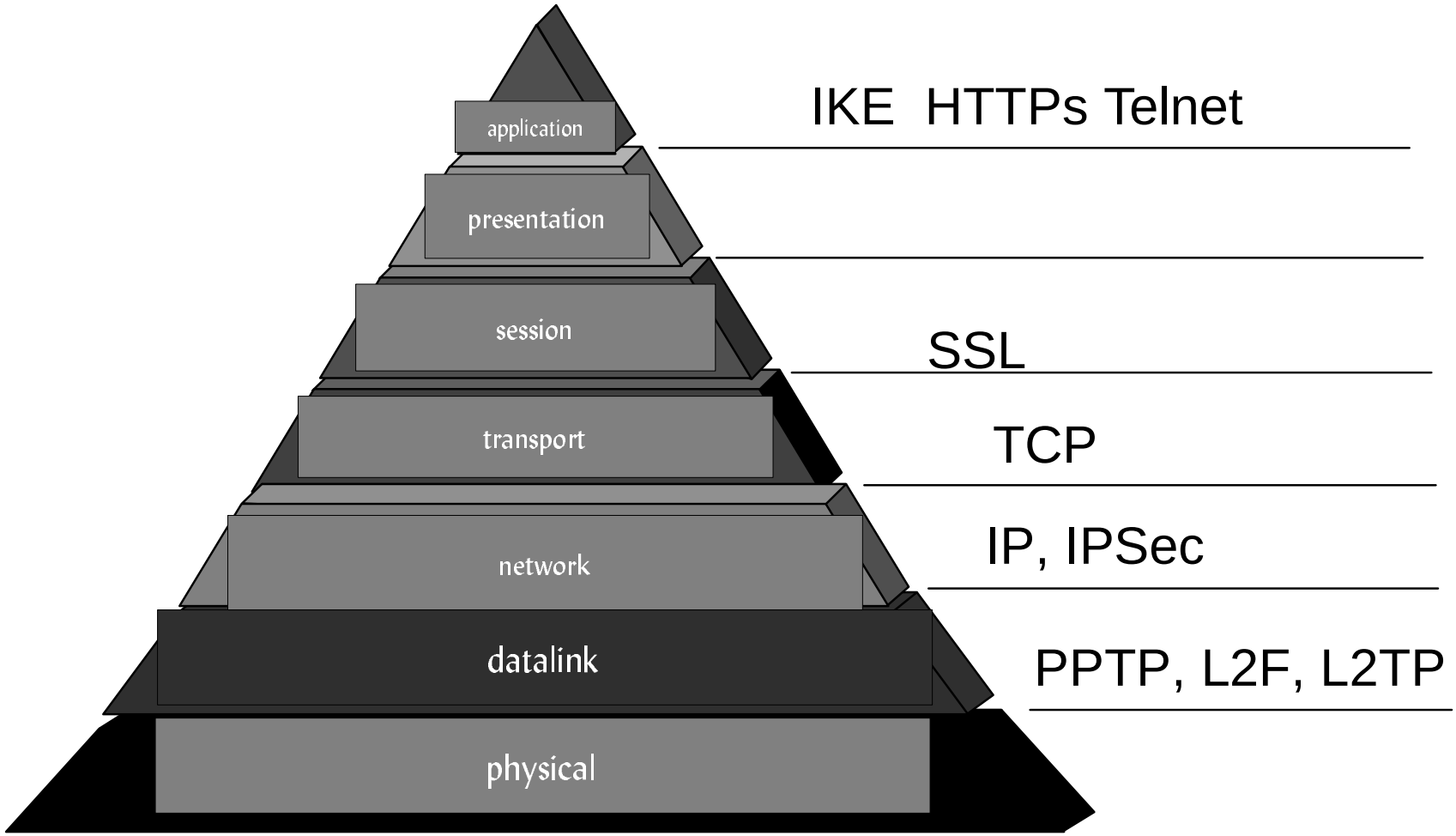
2. IKE
negotiates the encryption keys and policies



3. IPSec
transfer the data encrypted or authenticated at the IP layer



Where do all of these technologies fit?



IPSec

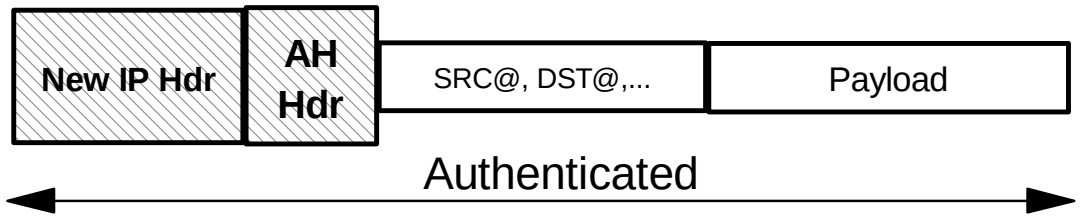
- **Mandatory for IPV6**
- **Optional for IPV4**
  - Bridge pattern for V4 ==> V6
- **Authentication Header (AH)**
- **Encapsulating Security Protocol (ESP)**
- **AH and ESP Combined**
- **Tunnel and Transport**

AH Coverage

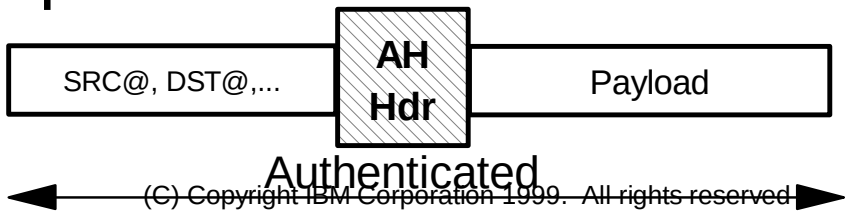
- Two modes: "Tunnel" and "Transport"
- Datagram content is "cleartext"
- AH provides data integrity and data origin authentication

Original Datagram

AH-Tunnel:



AH-Transport:

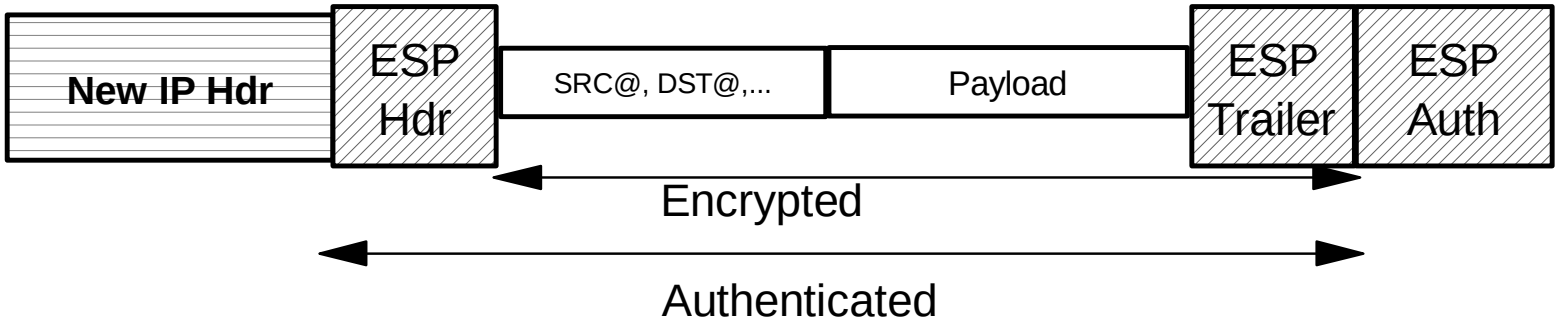


ESP Coverage

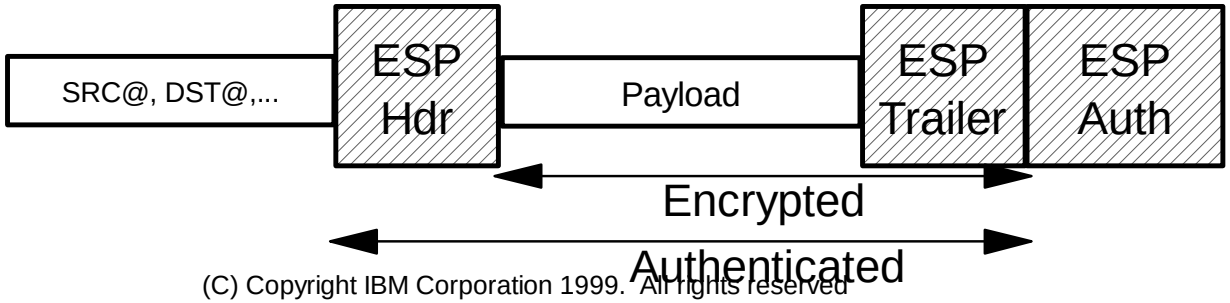
- Two modes: "Tunnel" and "Transport"
- Just IP payload or whole IP datagram can be encrypted

Original Datagram

ESP-Tunnel:

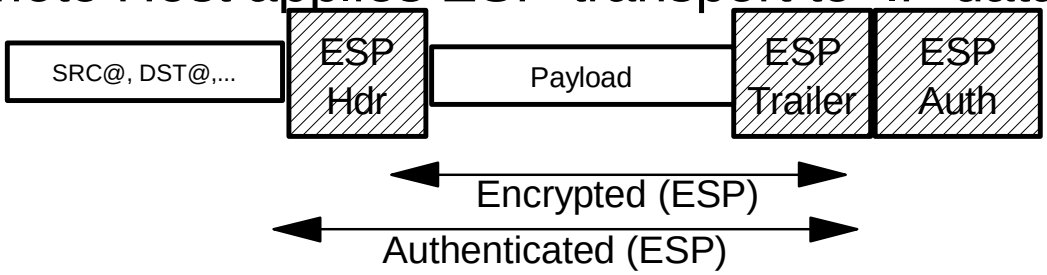


ESP-Transport:

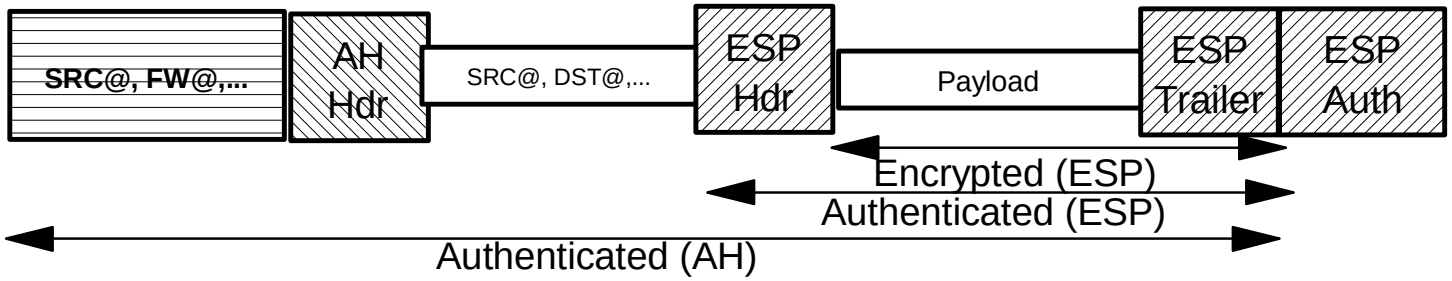


AH and ESP Combine

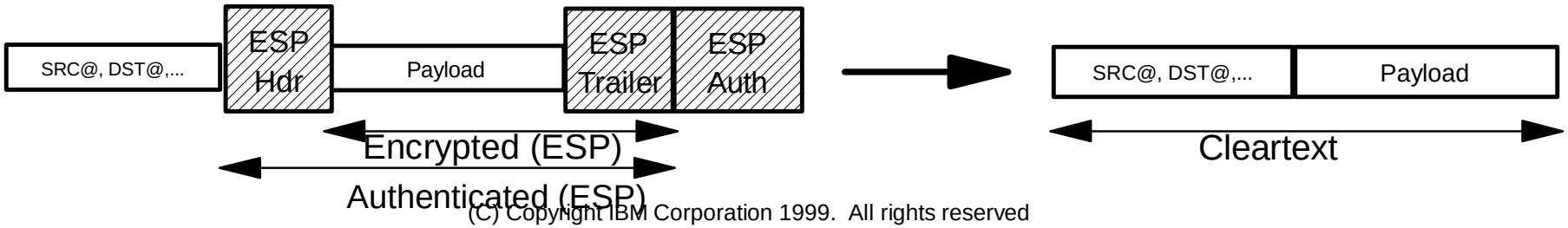
- First, Remote Host applies ESP-transport to IP datagram:



- Next, Remote Host applies AH-tunnel :



- Firewall authenticates, removes AH-overhead, forwards ESP-tunneled datagram to Destination, which authenticates and decrypts the payload:



Key Management

- **Security Association (SA) requires that shared keys are known to all participating parties**
  - Requires manual key entry or out-of-band key distribution
  - Keys can become lost, compromised or expire
  - Manual techniques do not scale
- **Key Management Protocol is the process of securely establishing SAs in a dynamic network environment**
- **Requirements**
  - Independent of specific cryptographic algorithms
  - Provide authentication of key management entities
  - Able to establish SA over "unsecured" transport
- **Internet Key Exchange (IKE) is the Key Management Protocol for IPsec**

Internet Key Exchange (IKE)

- **IKE is the practical intersection of several larger, more generalized protocols**
  - ISAKMP - Internet Security Association and Key Management
  - IPSec DOI - IP Security Domain of Interpretation
  - Oakley - Oakley Key Determination Protocol
- **Security Associations (SA) - all the information needed to specify the appropriate IPSec processing**
  - Algorithms (encryption, authentication)
  - Key lengths and lifetimes
  - Peer identities (who is your partner)
  - Modes (tunnel or transport)
- **Key generation and strong authentication procedures using digital certificates**

IKE's 2 Phase Approach

IKE Phase I

Key policy

- ✓ Negotiate IKE SA
- ✓ Authenticate
- ✓ Generate IKE Keys

IKE Phase 2

Data policy

Host 1

Host 2

- ✓ Negotiate IPSec SA
- ✓ Protected by Phase 1
- ✓ Generate IPSec Keys

IPsec SA

Connection

- ✓ Protects Application Data
- ✓ AH (Authentication)
- ✓ ESP (Encryption)

Other VPN Related Technologies

- **Network Address Translation**
- **Packet Filtering**
- **Layer 2 Tunnels (L2TP, L2F, PPTP)**
- **Application Gateways**
  - protect individual application payloads (e.g., SSL, S-MIME), but network headers are exposed!
- **Cryptography**
- **Certificate Management for Public Key Cryptography**
- **VPN Policy**

AS/400 VPN Solutions

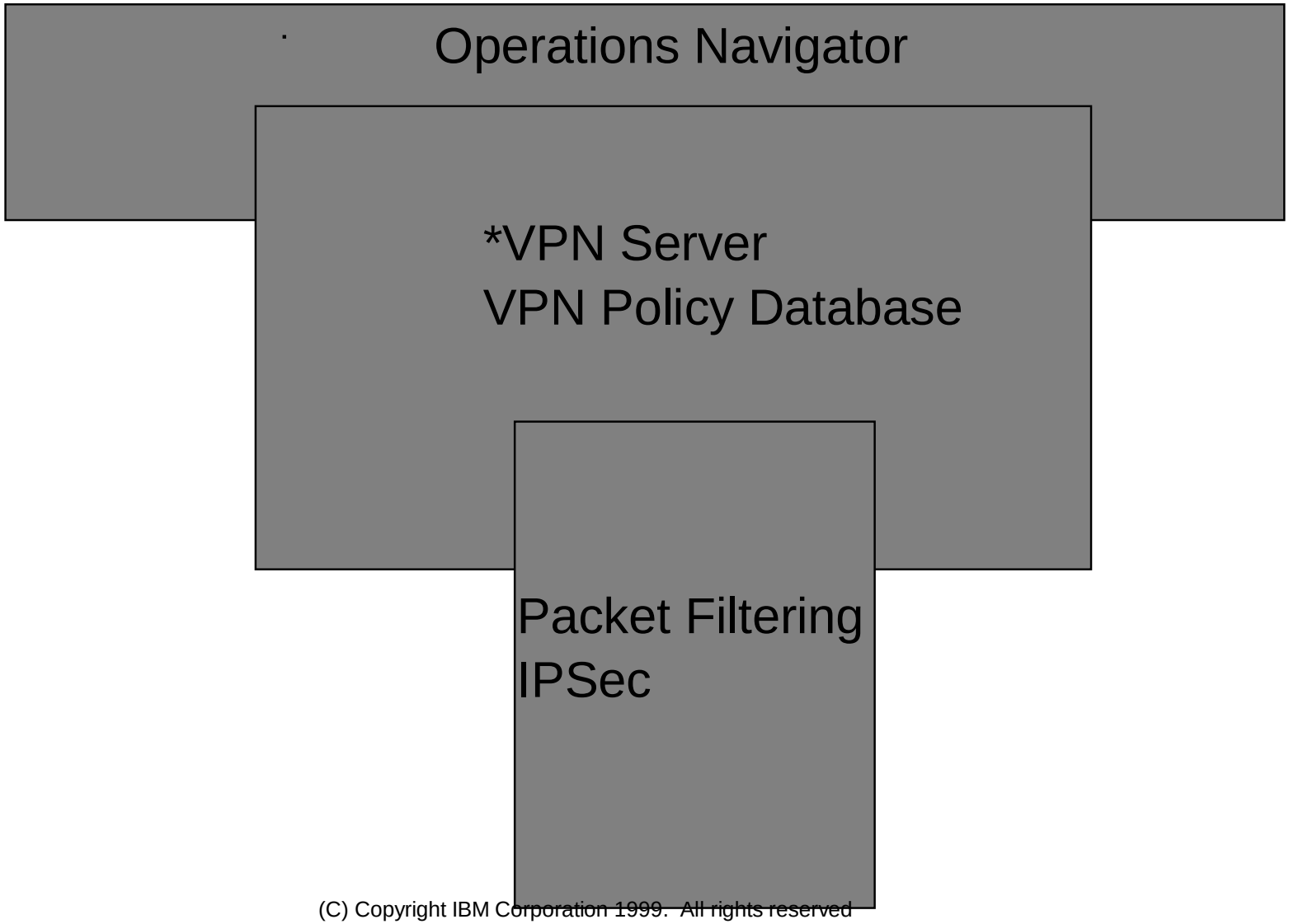
V4R3 VPN Solutions and Techologies

- **Firewall for AS/400**
  - Manual Tunnels
  - IBM Tunnels for dynamic key exchange
  - Configured using web browser
- **Native IP Filtering and NAT**
  - Built within AS/400 native TCP/IP stack
  - Configured using Operations Navigator

New in V4R4 - Native VPNs

- **Included in V4R4 OS/400 5769-SS1**
- **Manual Connections based on latest IPSec RFCs**
  - Cryptographic keys are pre-defined
- **Dynamic Connections based on latest IPSec RFCs**
  - Cryptographic keys are negotiated
  - IKE protocol for dynamic key exchange
- **Support for Dyamic IP**
  - PPP dial up
- **Support for Remote Users using L2TP (Layer 2 Tunneling Protocol)**

AS/400 Native VPN components



AS/400 Native VPN - Op Navigator

- **Included with Client Access Express**
  - Need to install the Operations Navigator Components
- **Selected via the IPSecurity option in the Network folder**
  - VPN Configuration and Management
  - IP Packet Security (Filtering and NAT) Configuration
- **Includes VPN Connection Wizard**

AS/400 Native VPN - *VPN Server

- ***VPN Server (OS/400)**
  - Connection Manager (QTOVMAN job)
  - Key Manager/IKE server (QTOKVPNIKE job)
  - Supported by:
    - STRTCPSVR, ENDTCPSVR
    - TRCTCPAPP
  - No Configuration commands
  - Requires AC2 or AC3 cryptographic enabler

AS/400 Native VPN - VPN Policy DB

- **Configured using Operations Navigator**
- **Contains all VPN configuration details**
  - Crypto Keys for manual connections
  - Key Manager (IKE) Negotiation Policies
- **Stored on the AS/400 in QUSRSYS**
  - Need to include in your backup/recovery plan

AS/400 Native VPN - Packet Security

- **Packet Filtering and IPSec**
  - Packet Filtering enhanced to include another action-keyword "IPSEC"
  - You must have a filter rule with an action of "IPSEC" to invoke IPSec within the TCP/IP stack.
  - The rule must specify a connection group name
- **Packet Filtering and IKE**
  - Will need to allow IKE traffic to flow between systems
  - IKE uses UDP well known port 500
- **Packet Filtering and L2TP**
  - May need to allow L2TP traffice to flow between systems
  - L2TP uses UDP well known port 1701

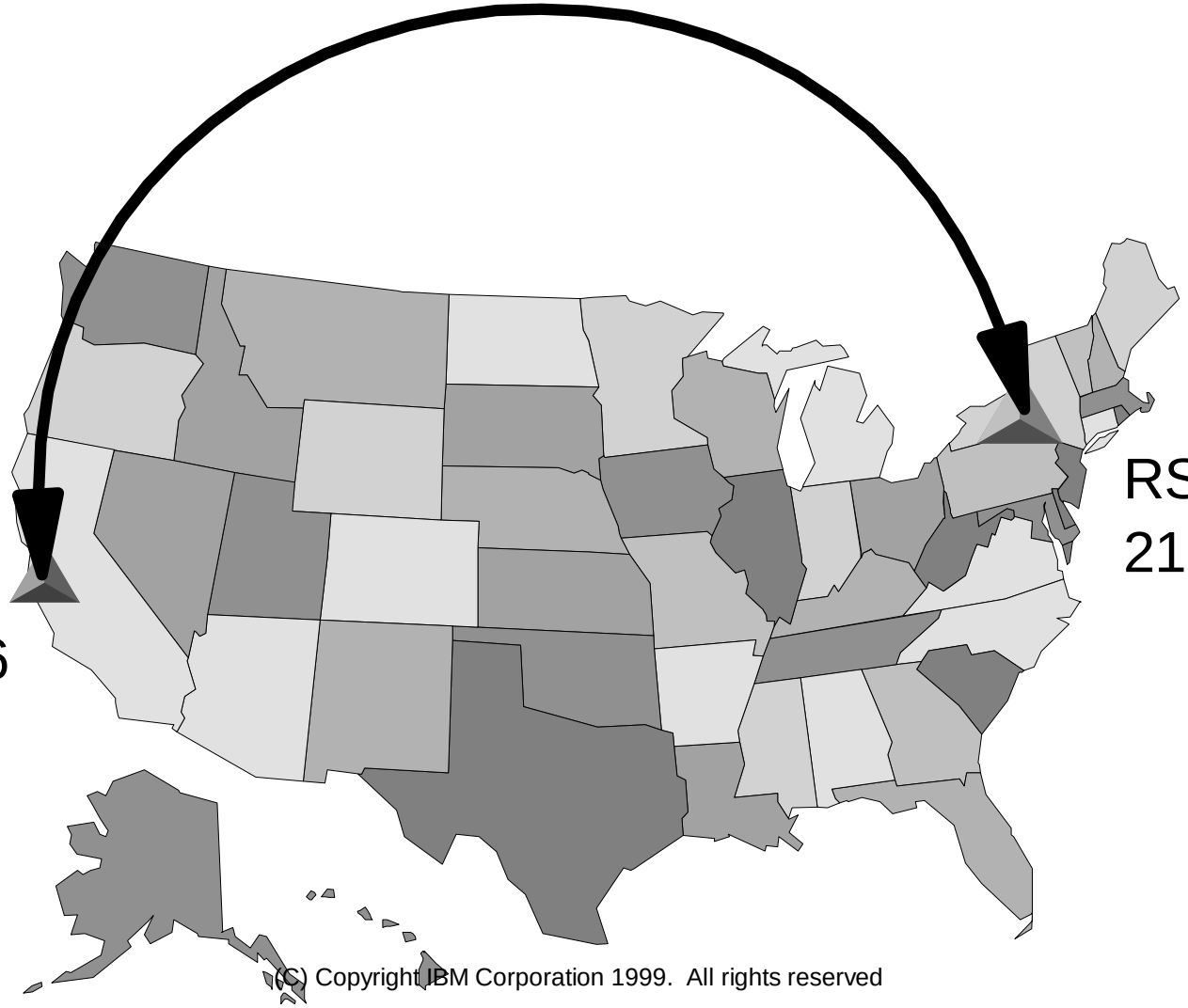
AS/400 Native VPN - Configuration

- **Documented in the Information Center**
- **Plan your VPN security policy**
  - Endpoints (host or gateway)
  - Data protection (AH, ESP or both)
  - Key management (manual or dynamic)
- **Use Operations Navigator to configure**
  - VPN Policy
  - IP Packet Security Filtering Rules

An Example Configuration....

Monday morning, in San Francisco

You need to create a VPN between the Moscone Center and your home office in New York



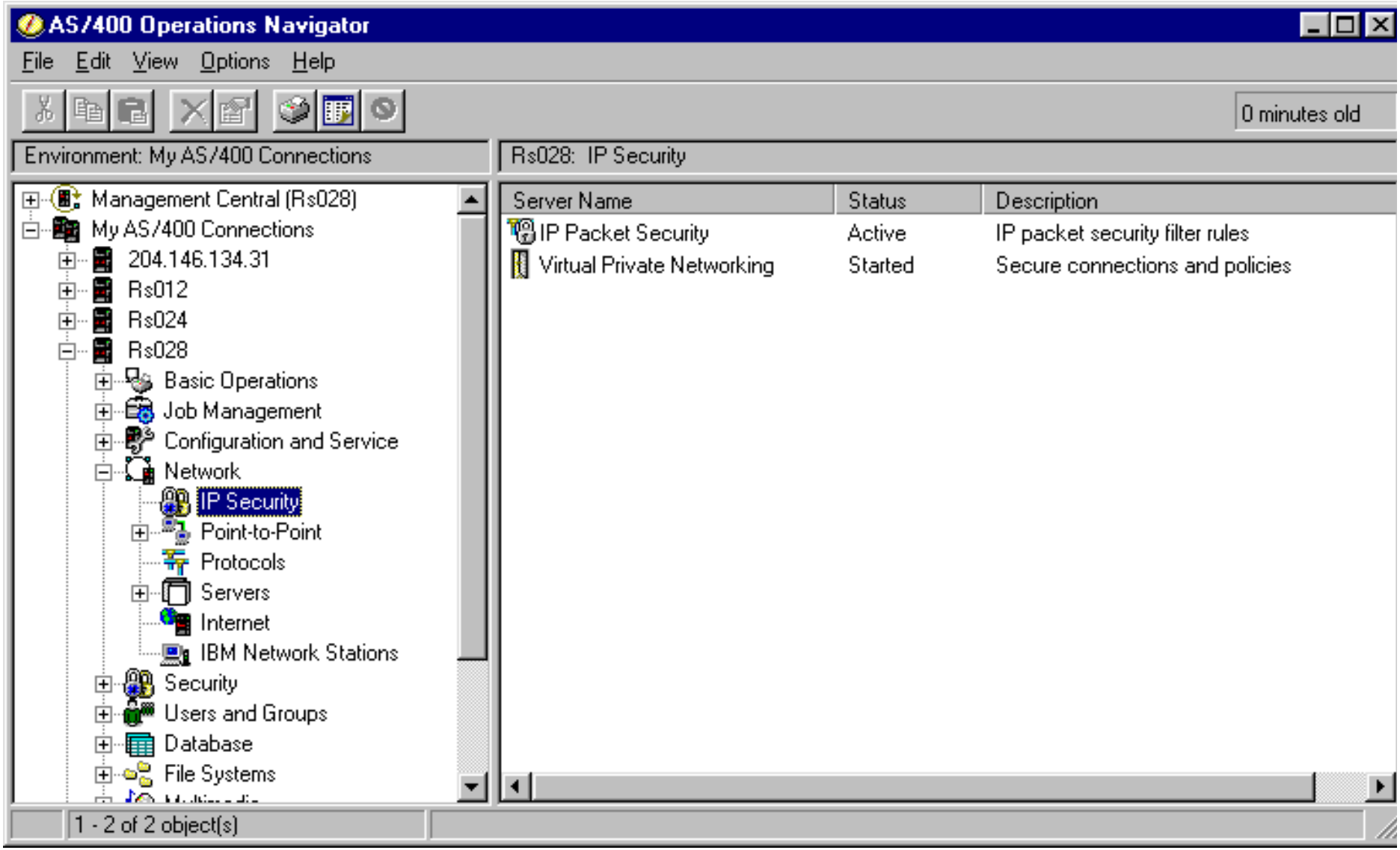
Planning Considerations

- Network Security Policy is a Must!
- Manual or Dynamic?
- Host to Host, Gateway to Gateway, etc?
- What level of Key Security?
- What level of Data Security?
- Identify the endpoints (i.e. IP Addresses)

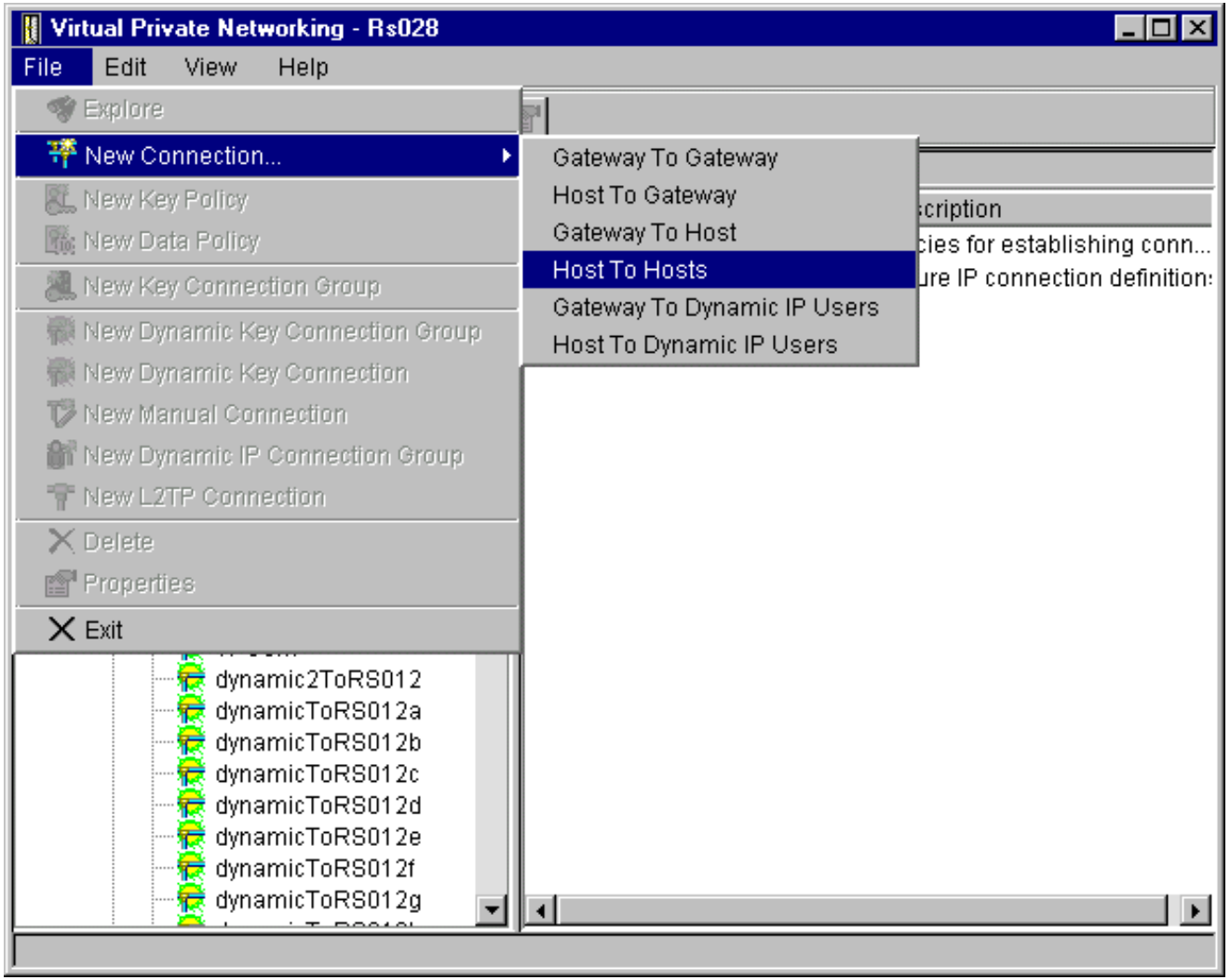
Configuration Steps and Operation

- **Verify IP connectivity between systems**
- **Configure San Francisco VPN Policy**
  - Configure Dynamic Key Connection using the Wizard
- **Configure San Francisco IP Filtering**
  - Configure PERMIT rule(s) for IKE traffic
  - Configure rule defining IPSEC action
- **Configure New York VPN Policy**
- **Configure New York IP Filtering**
- **Start the Connection**
- **View the Active Connections**

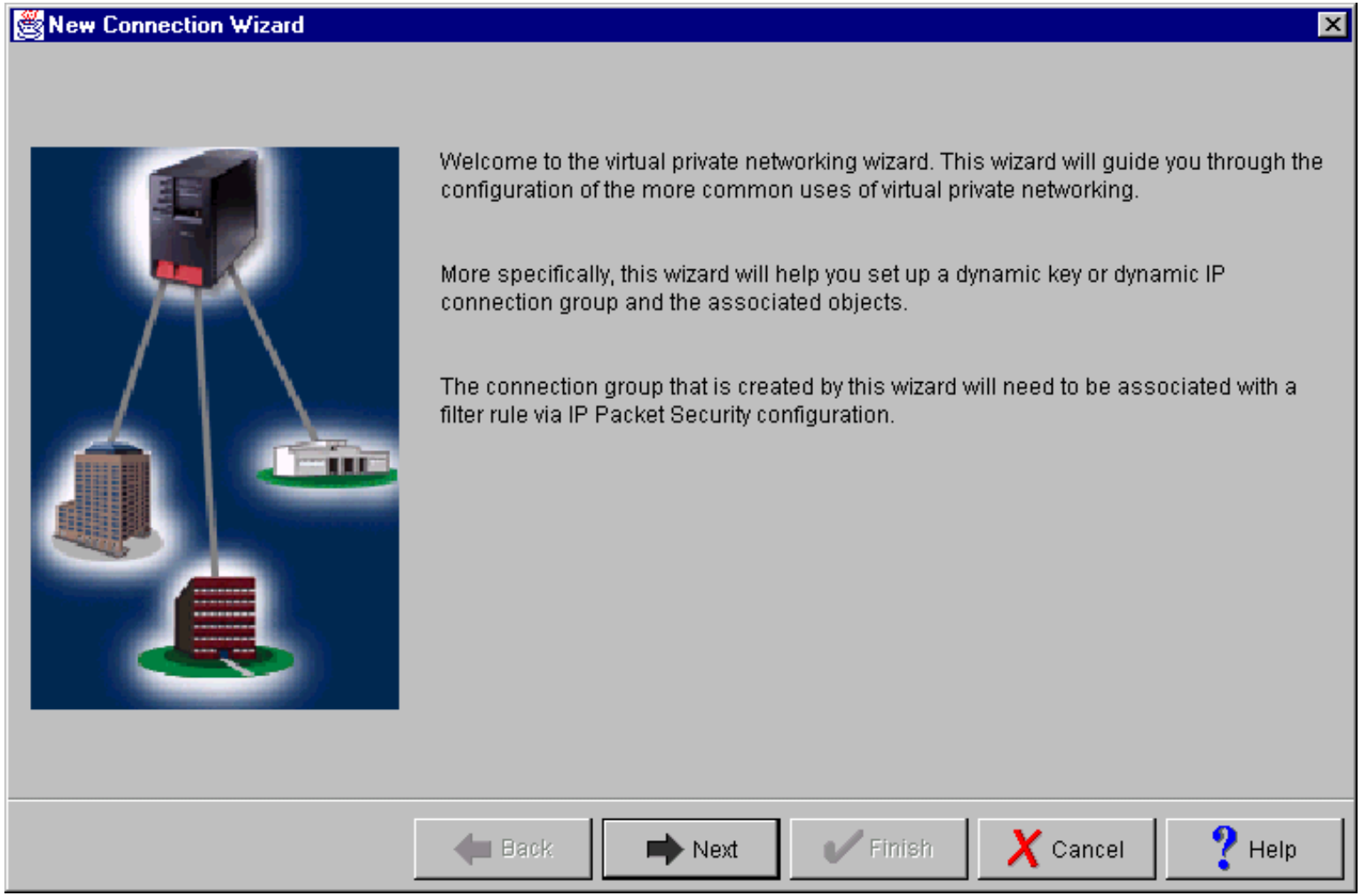
Operations Navigator IP Security



Op Nav Virtual Private Networking

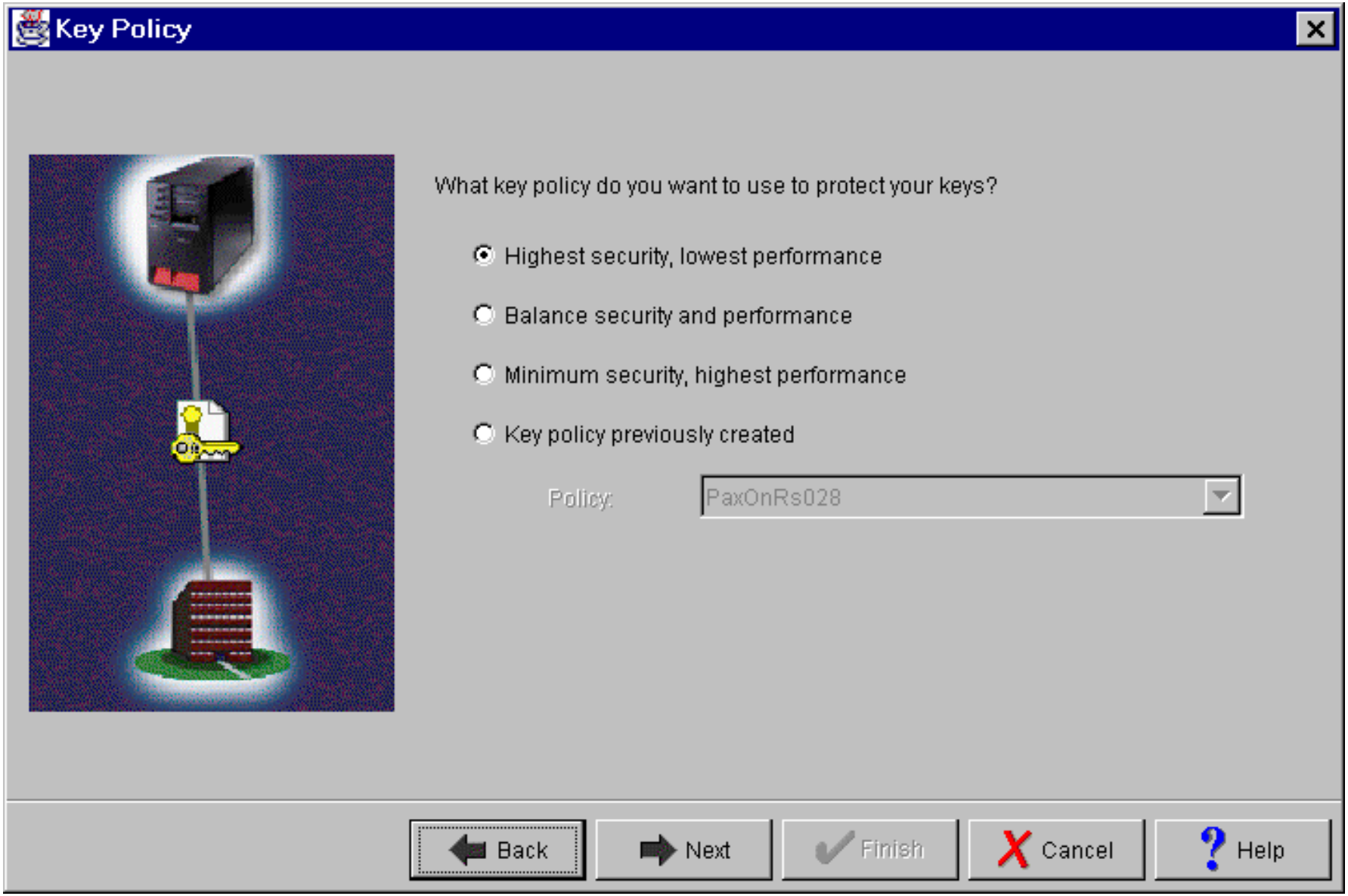


The New Connection Wizard

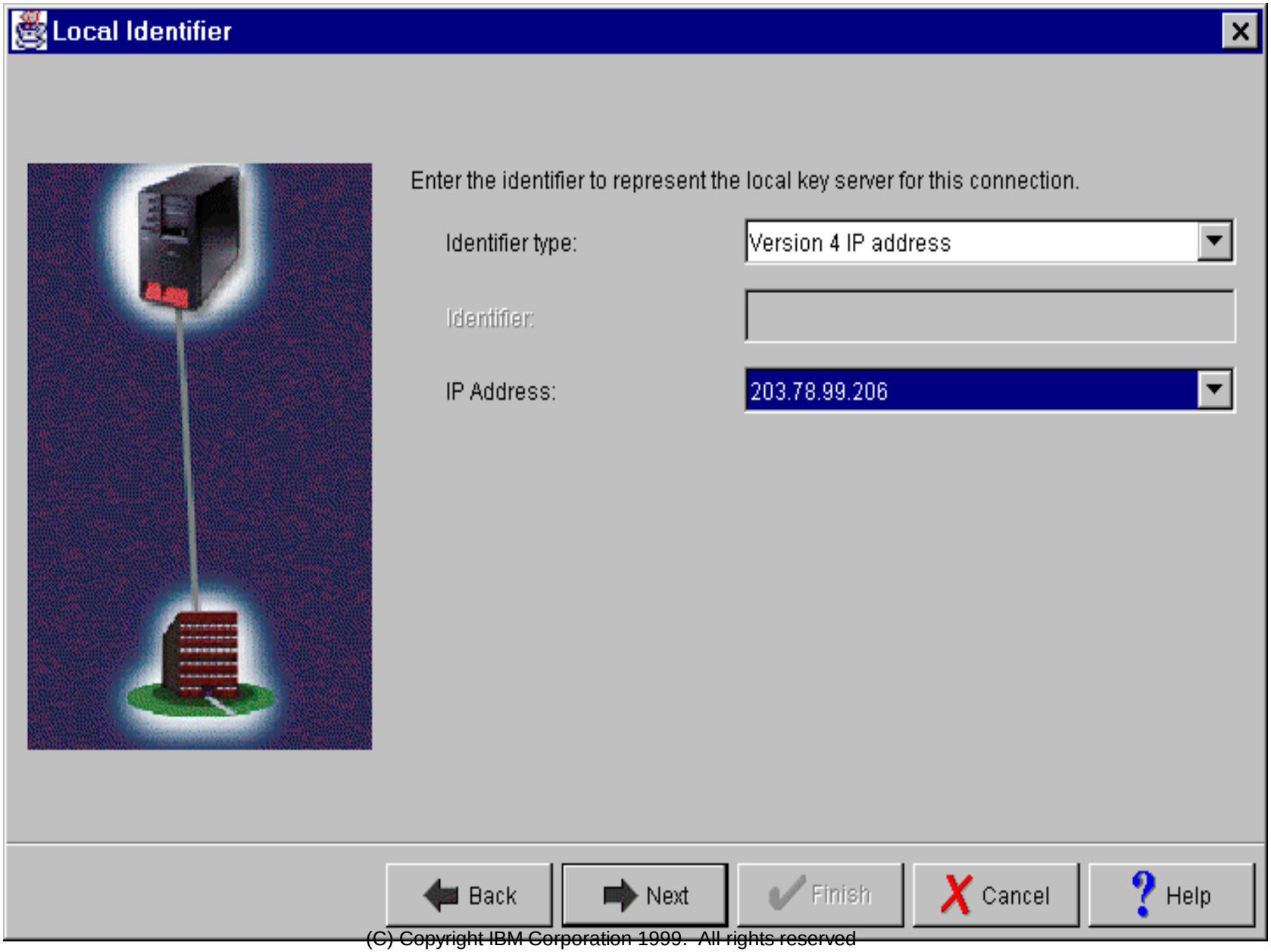


Naming the Connection

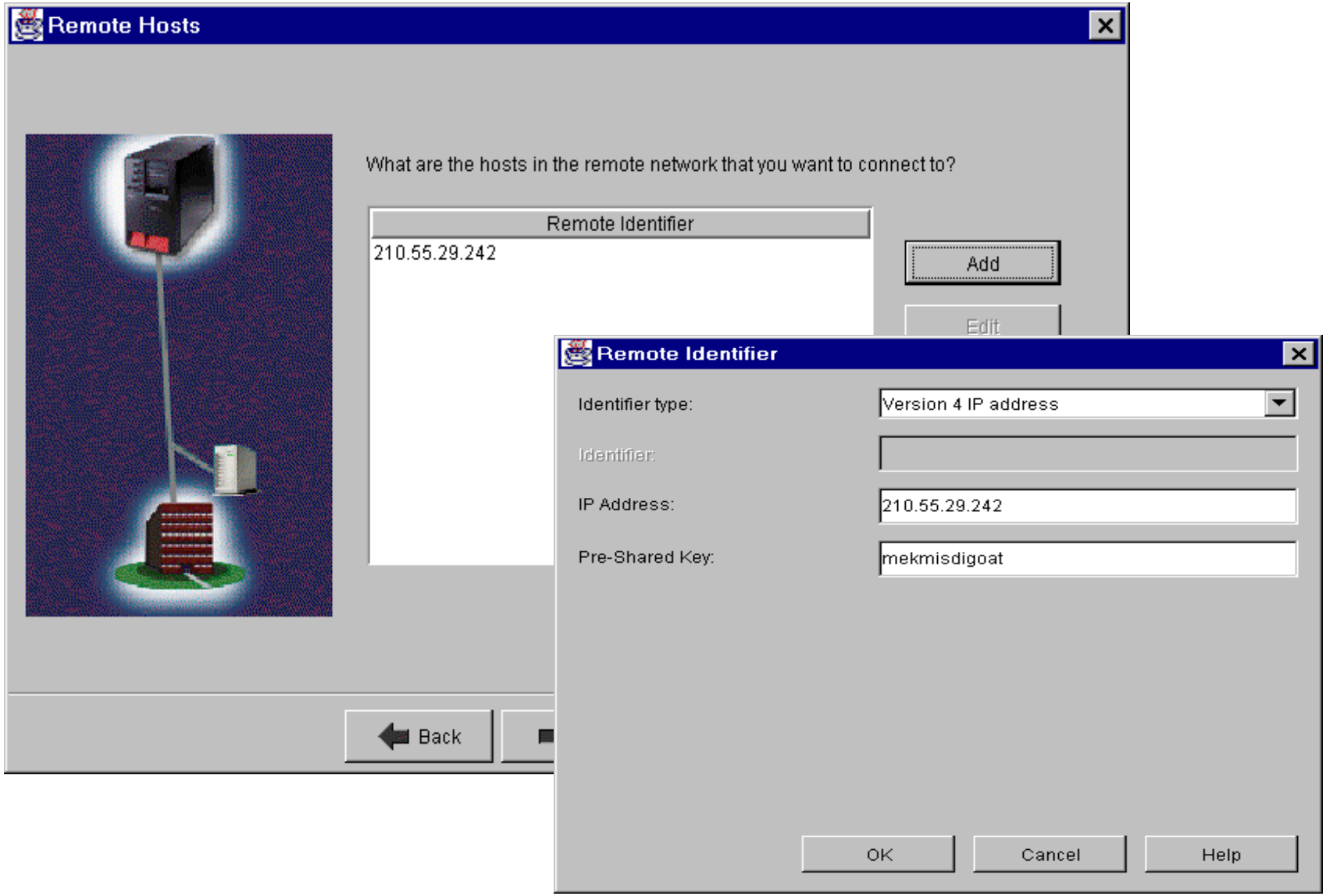
Choosing Key Policy for IKE



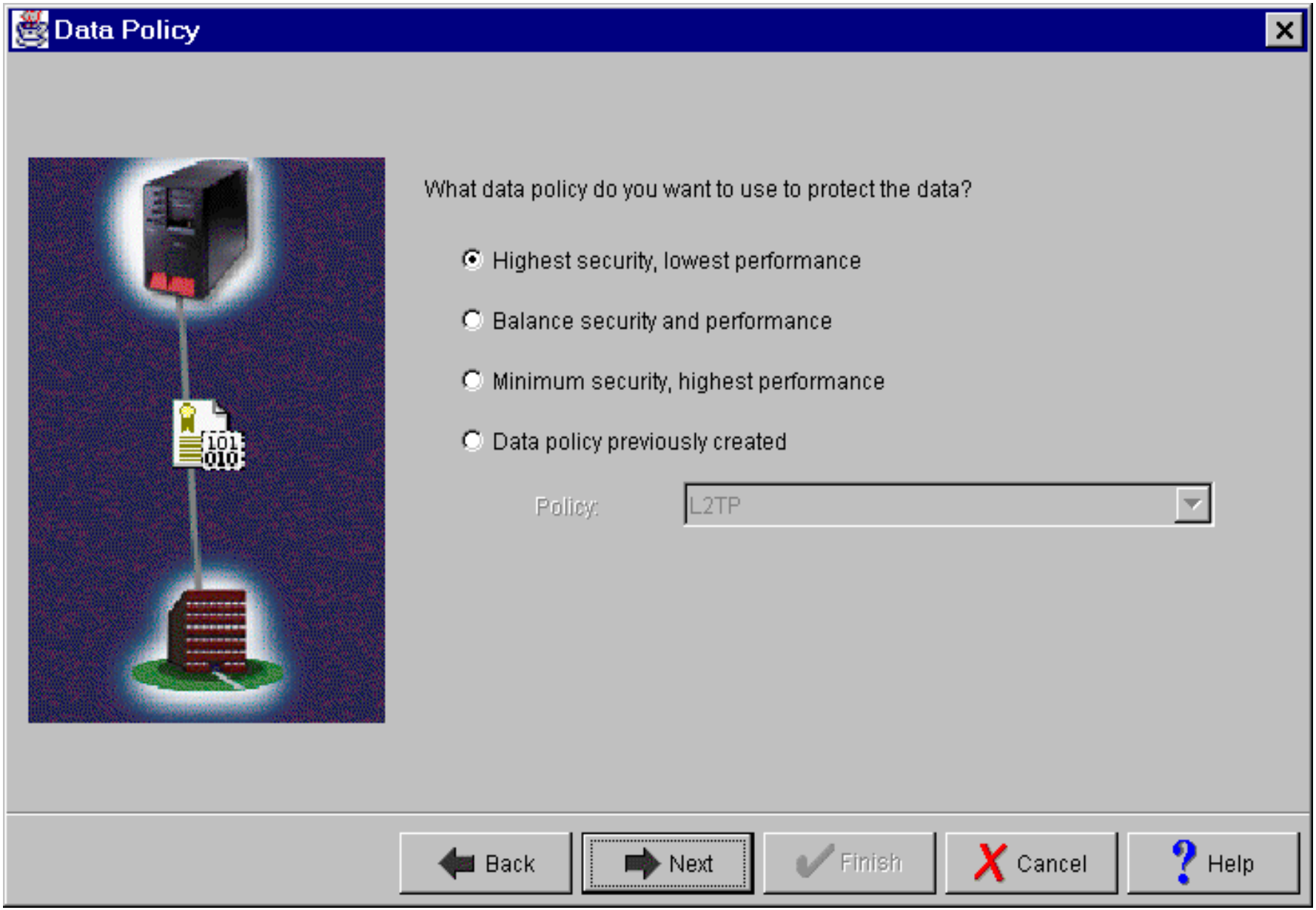
Identifying the local systems



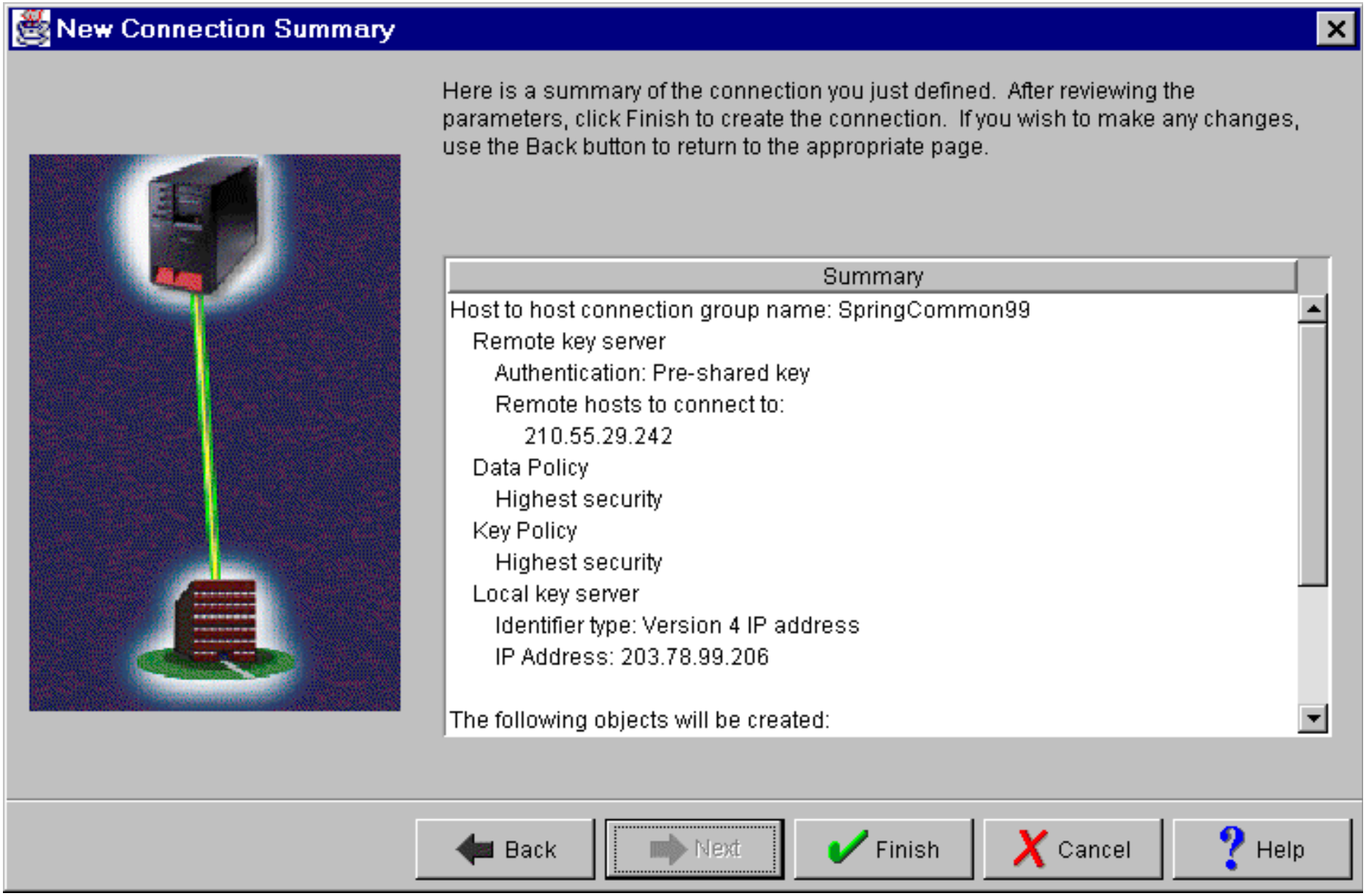
Identifying the remote system(s)



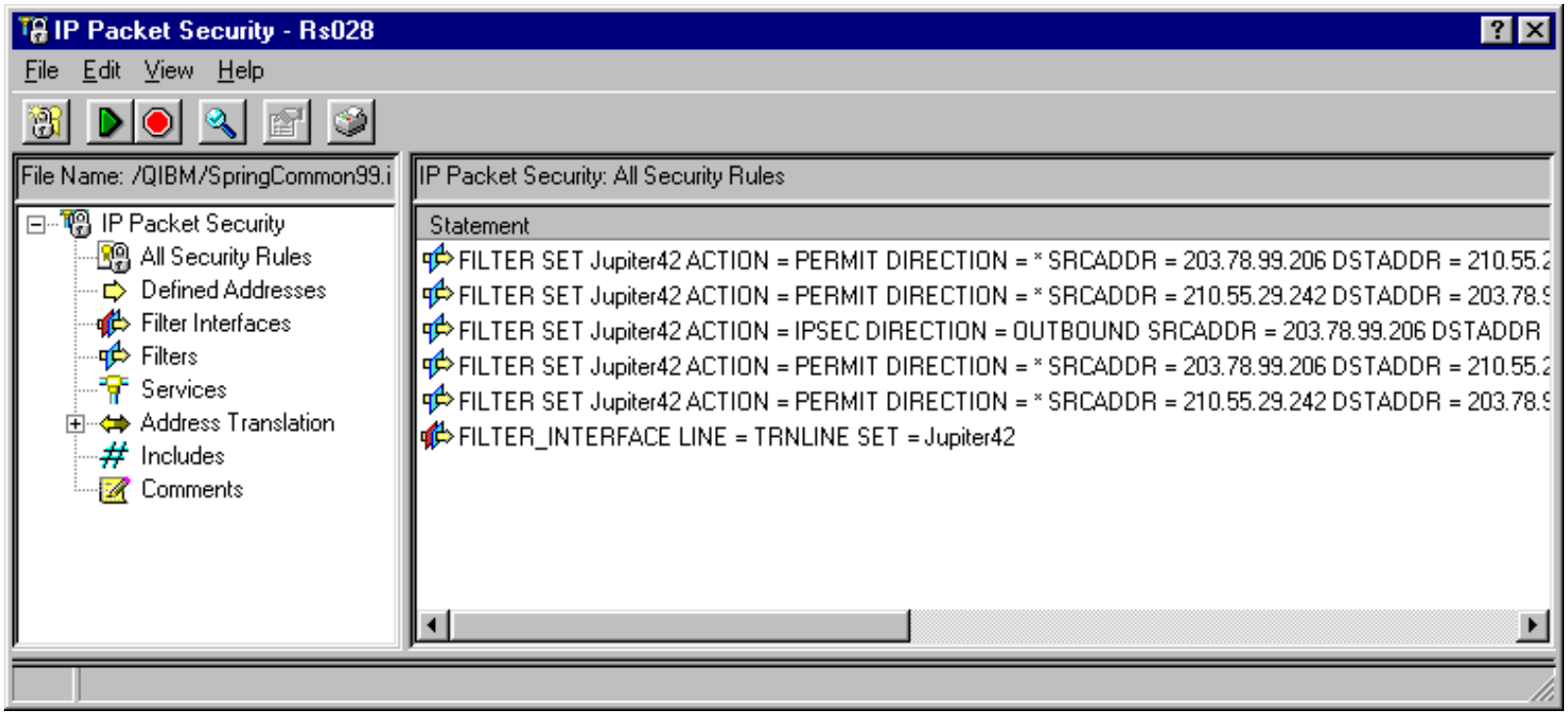
Choosing Data Policy for IPSec



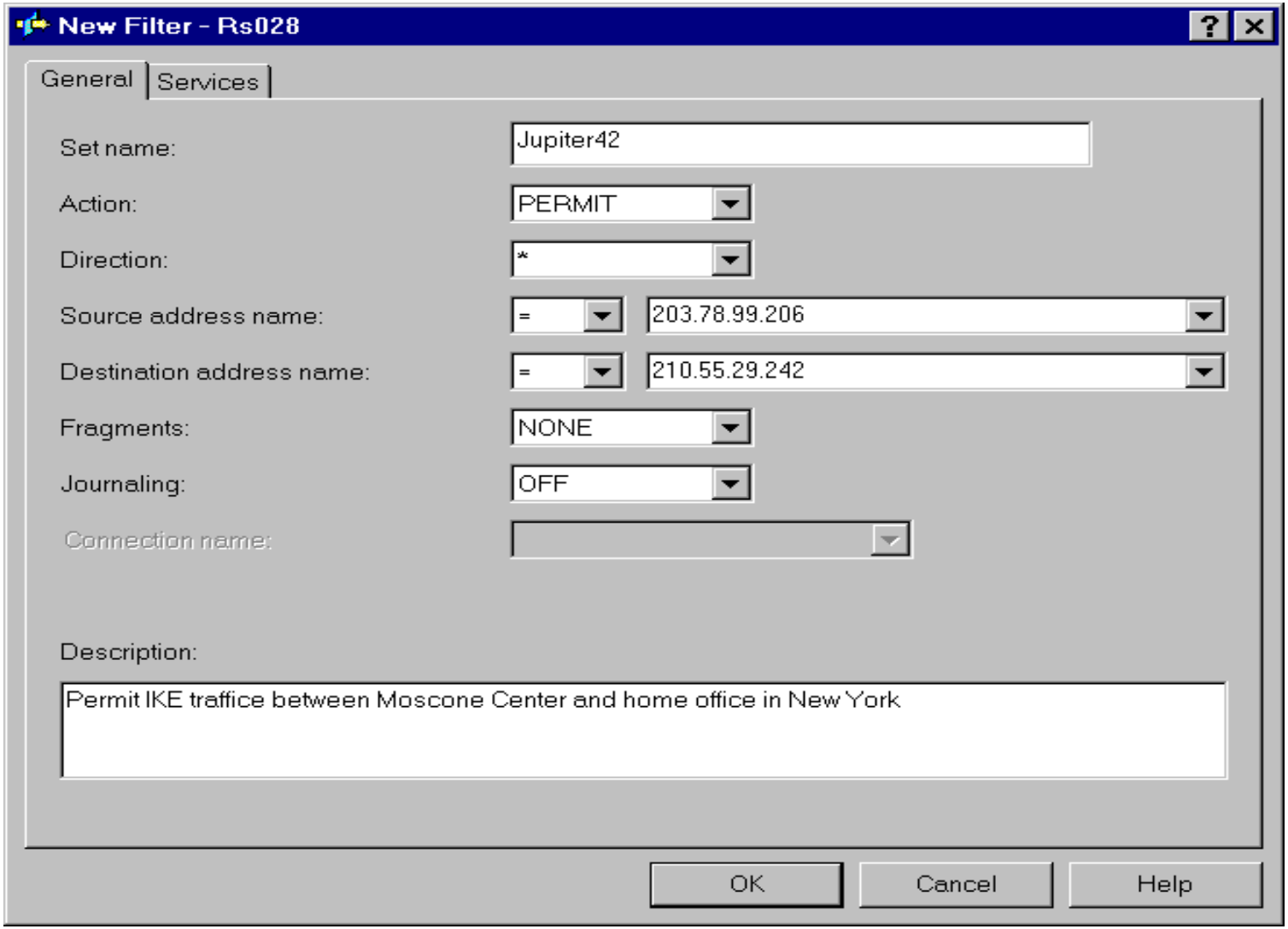
Verify the results of the Wizard



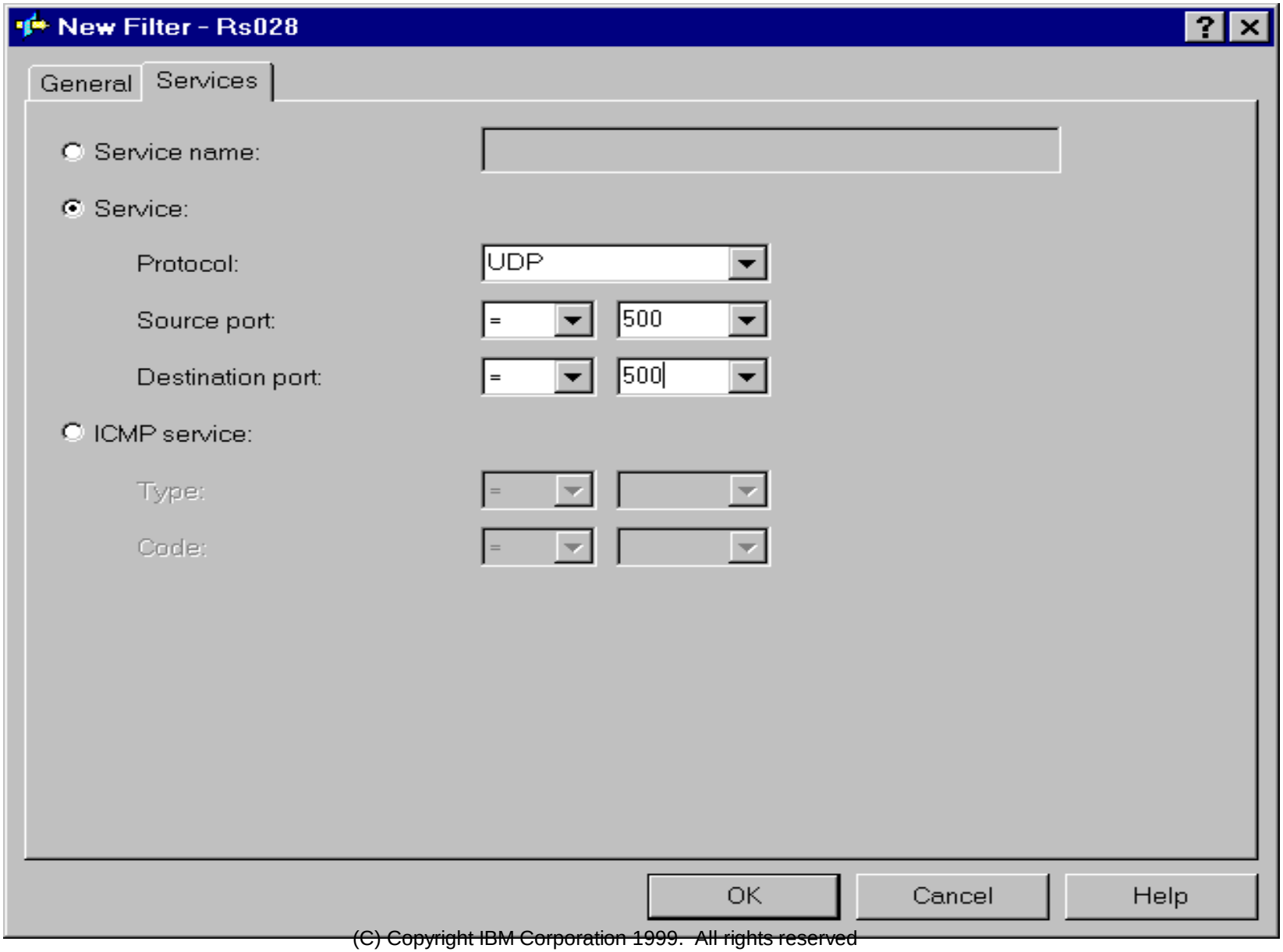
Define the IP Filtering Rules



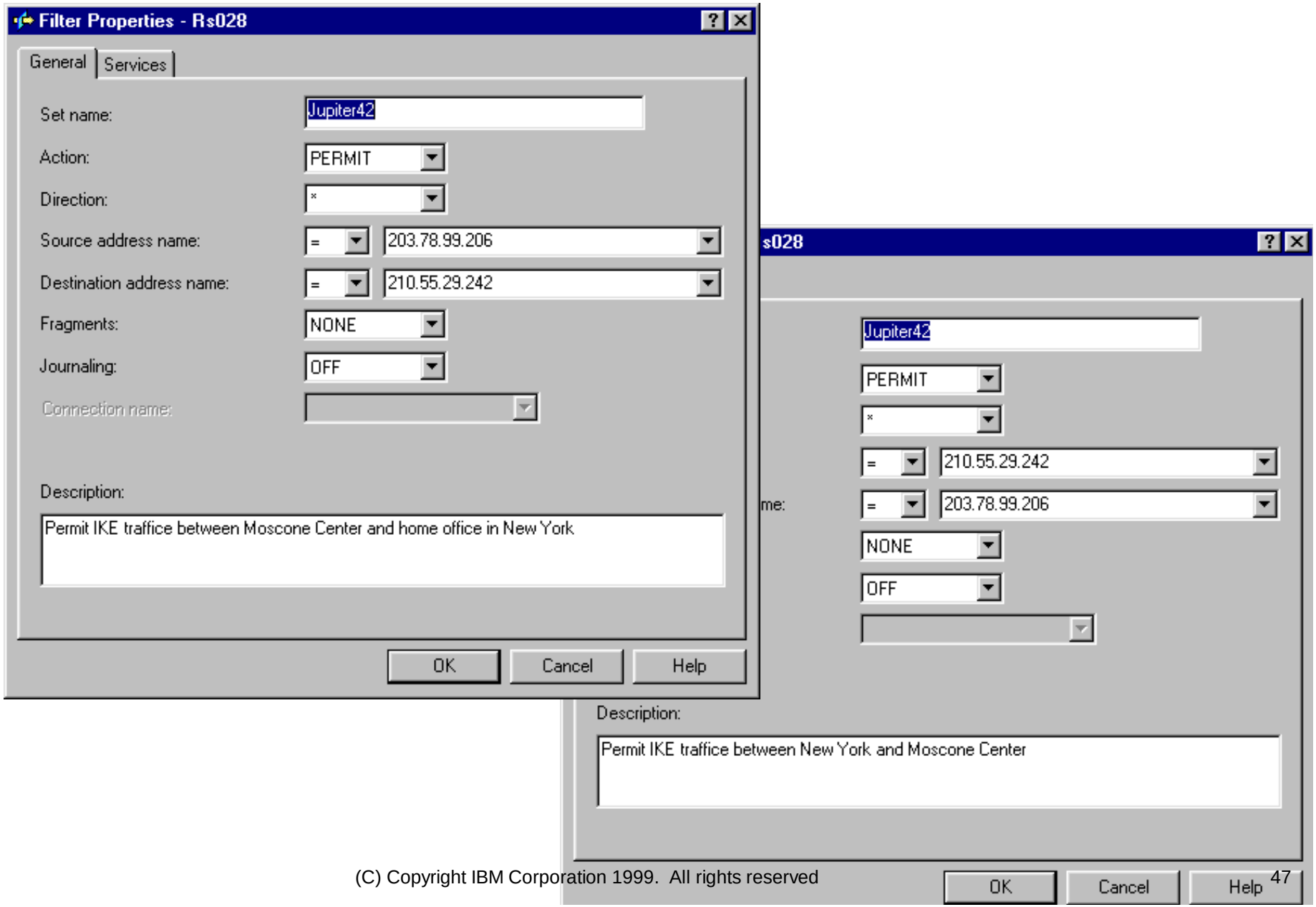
Create a rule to PERMIT IKE



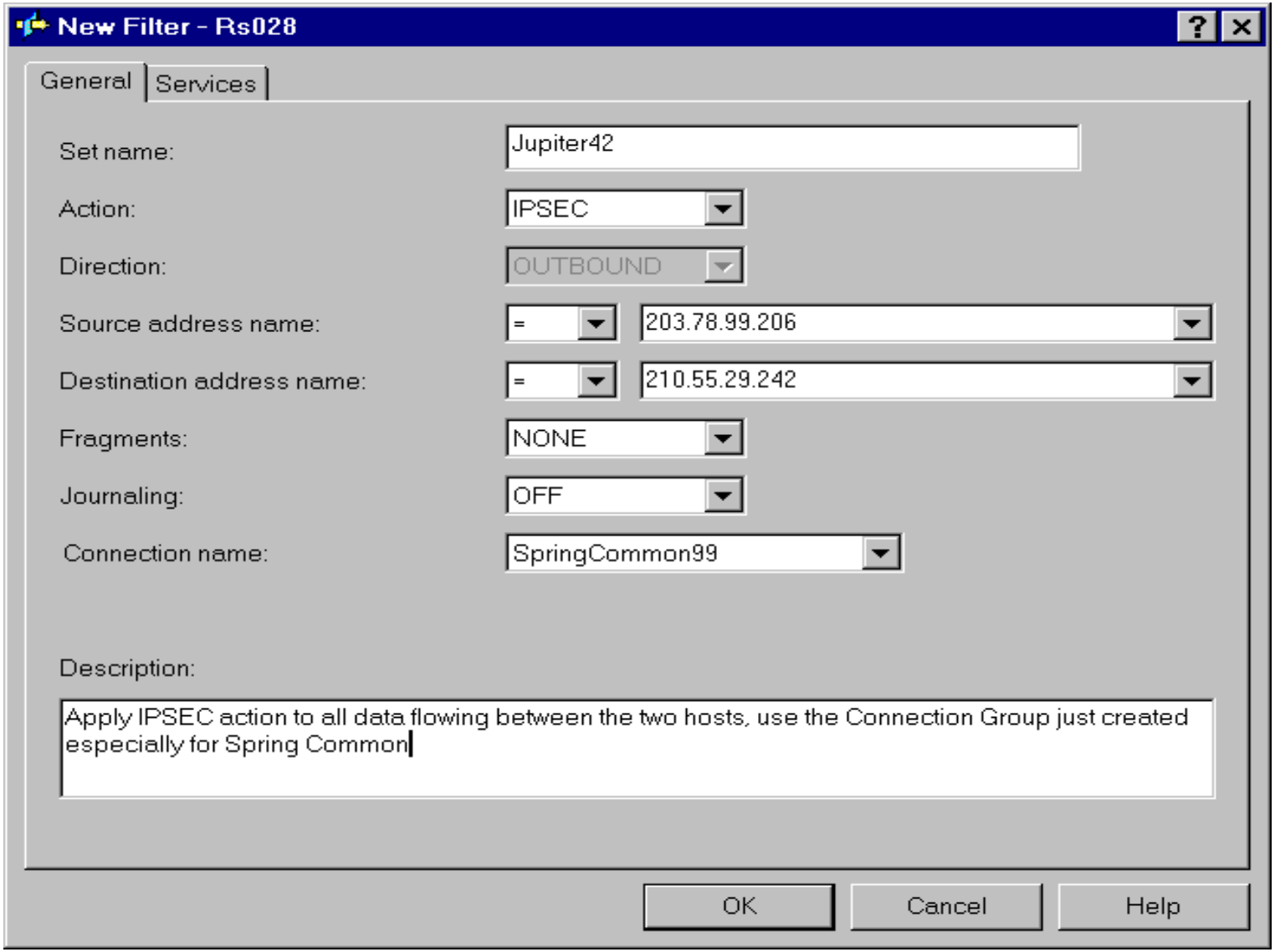
IKE uses UDP well known port 500



IKE must flow both directions...

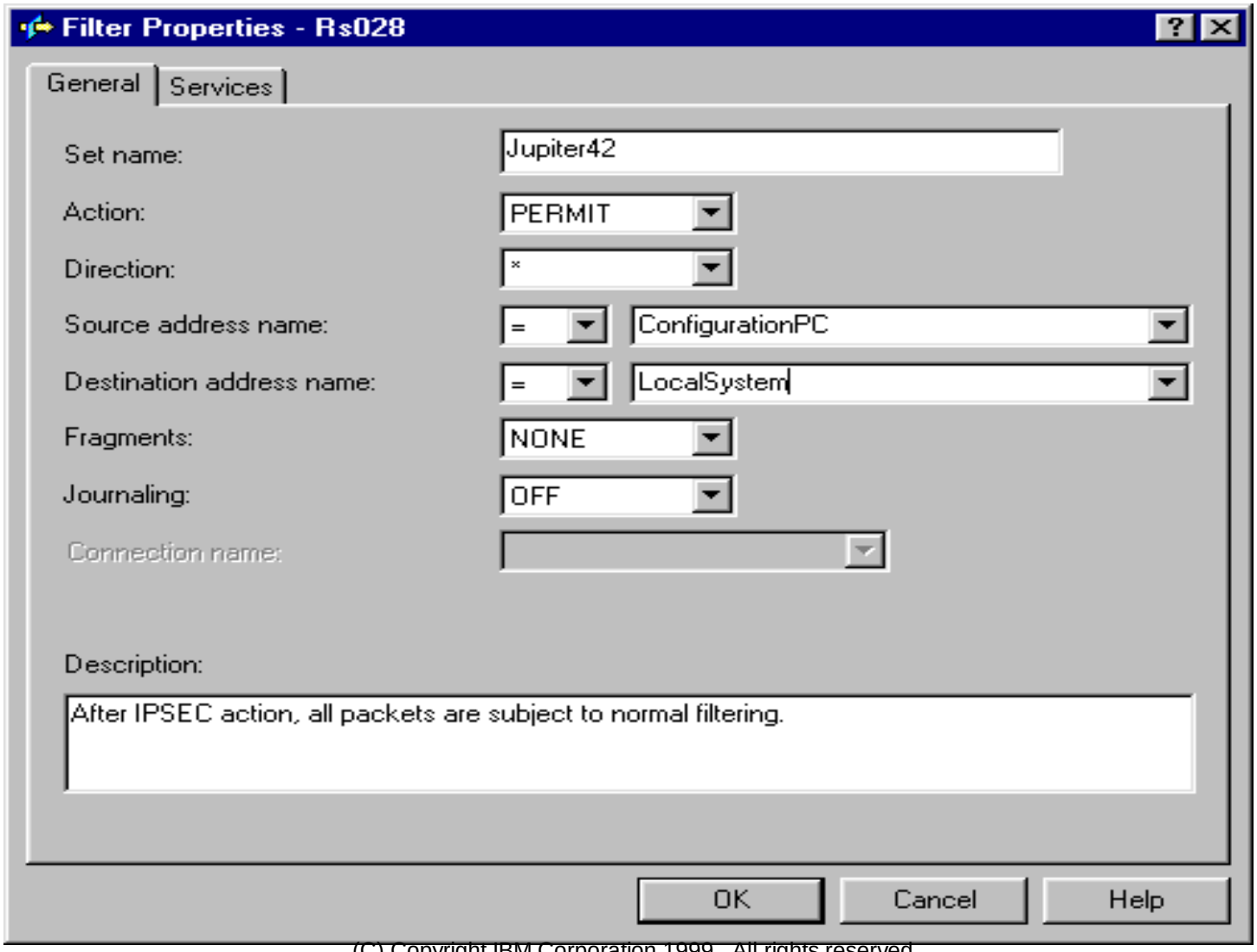


Create a rule to IPSEC

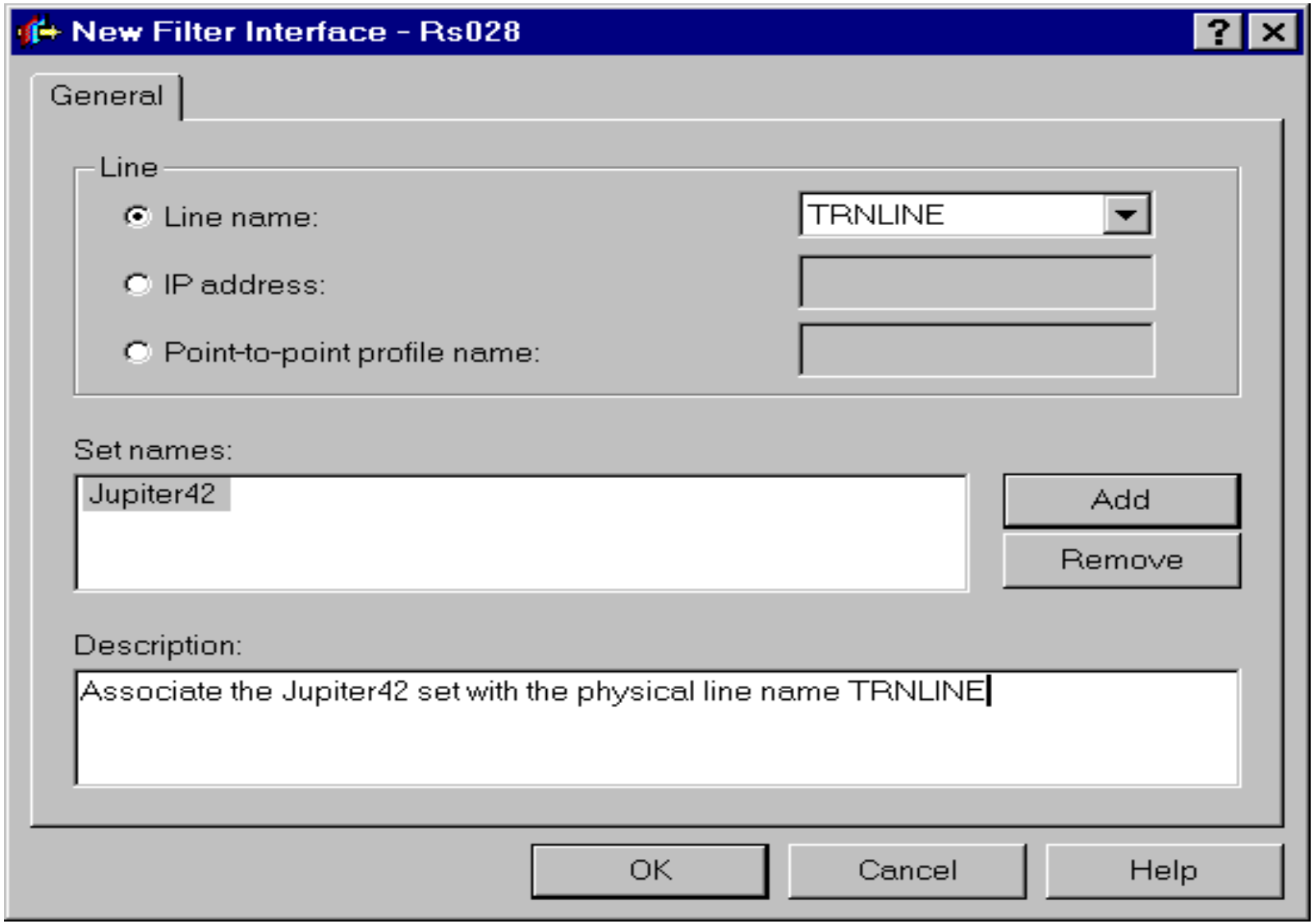


PERMIT other traffic

- **Default IP Filtering action is DENY everything...**

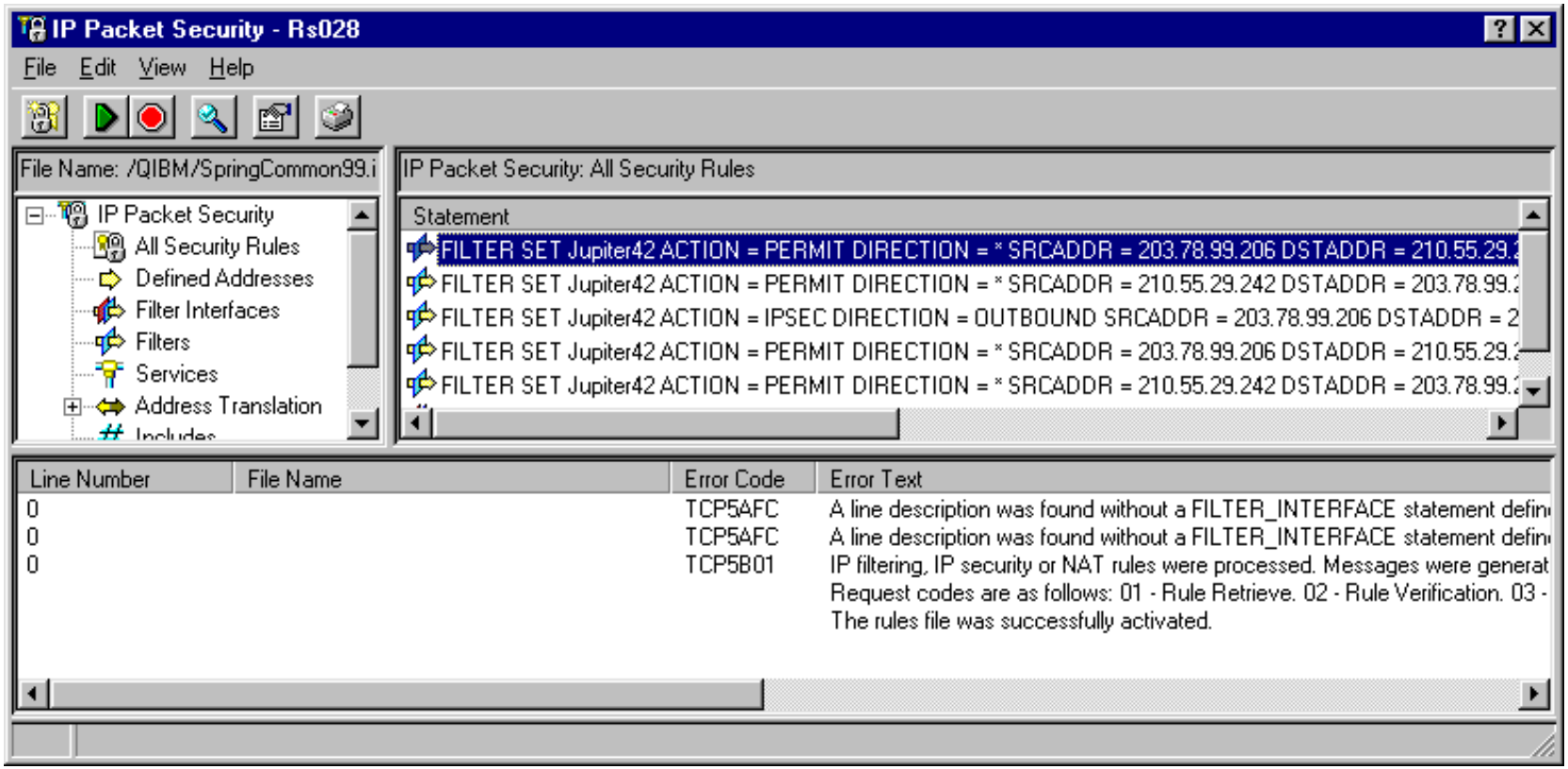


Associate rules with a line



Load the filter rules

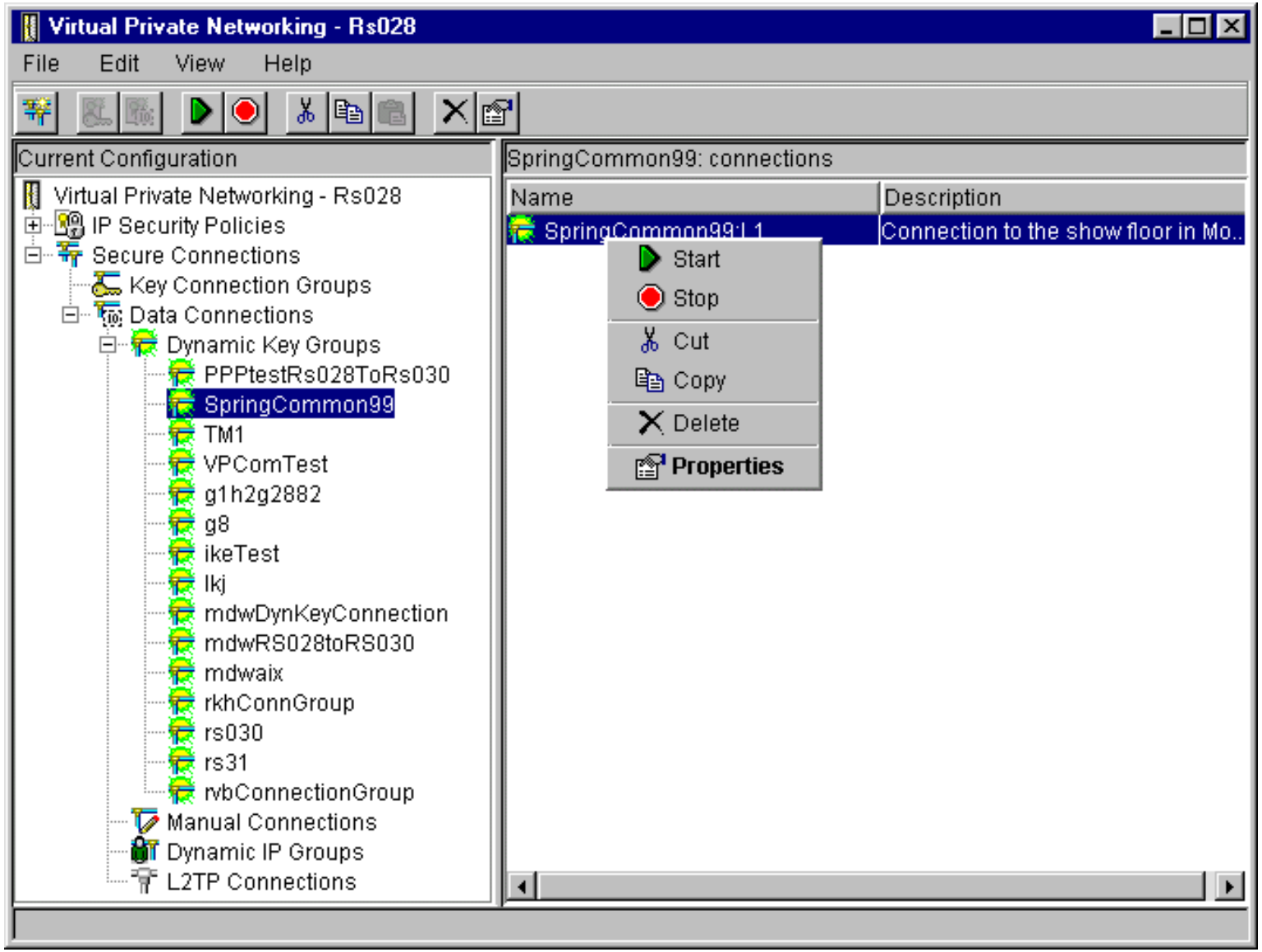
- **Rules will be verified before they are loaded**



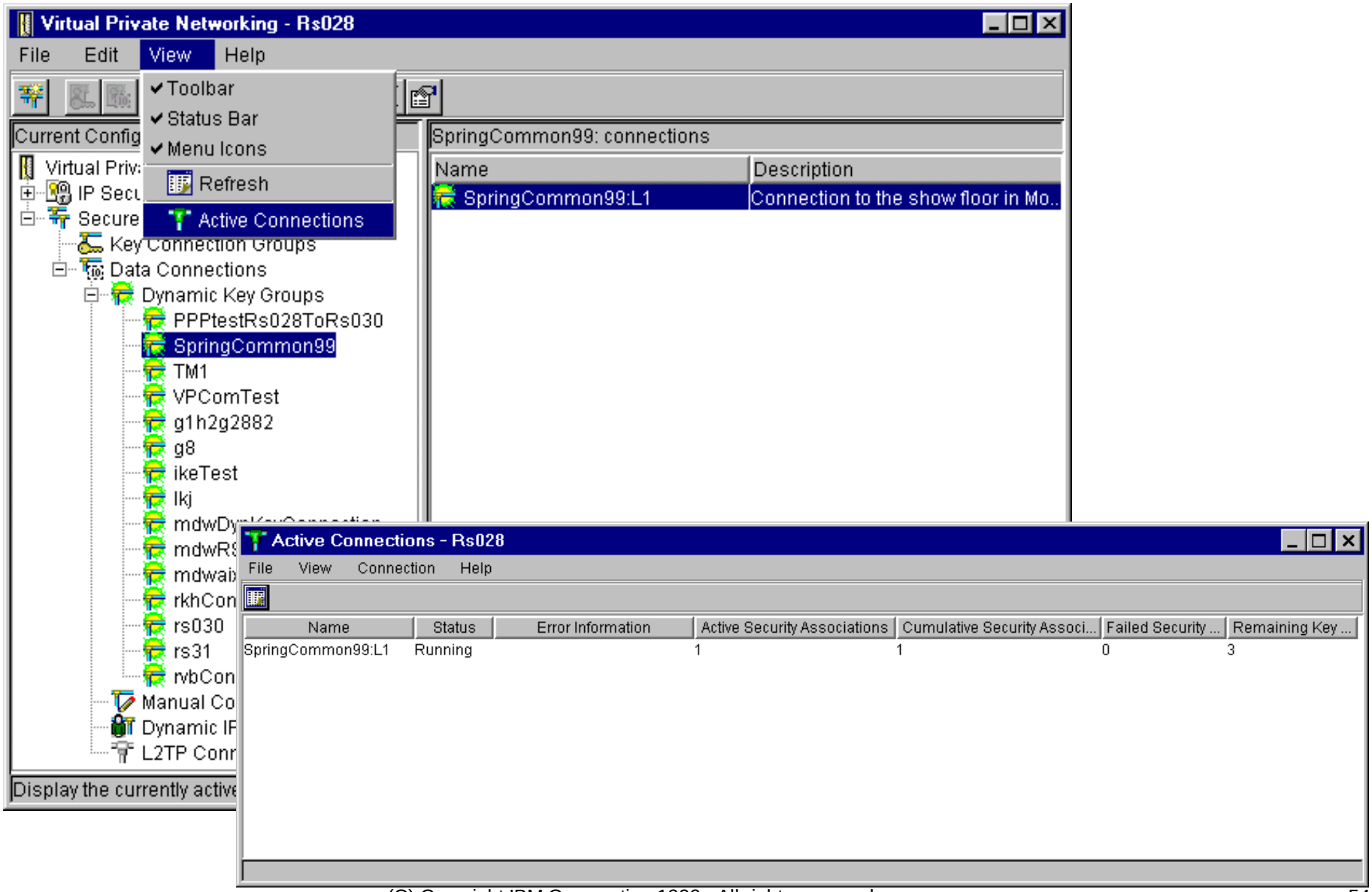
Off to New York!!!

- **We've completed the configuration in San Francisco**
- **Now we have to configure the other end of the VPN Connection in New York**
  - Create the VPN Policy Using the Wizard
  - Create the IP Filter rule for IKE and IPSec
  - Load the IP Filter Rules

Now Start the connection in San Francisco



The Active Connection Monitor....



In Summary..

- **Virtual Private Networking is a technology that is real today!**
- **New in V4R4, the AS/400 provides a complete native VPN solution based on:**
  - L2TP
  - IKE
  - IPSec
- **Your Network Security Policy is key.**

Trademarks

AS/400, IBM, and OS/400 are trademarks of the IBM Corporation in the United States or other countries or both.

Other company, product, and service names may be trademarks or service marks of others.