

AS400 VPN Technologies and Solutions

Frank V. Paxhia
paxhia@us.ibm.com

© Copyright IBM Corporation, 1999. All Rights Reserved.

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.

(C) Copyright IBM Corporation 1999. All rights reserved



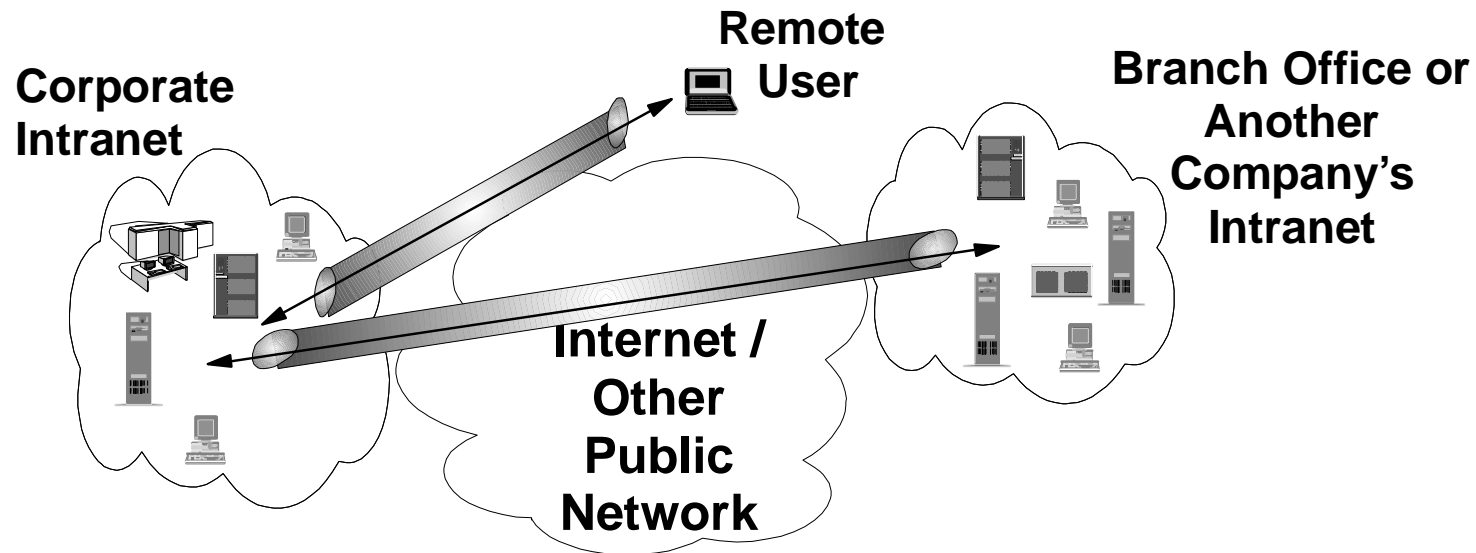
Agenda

- **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

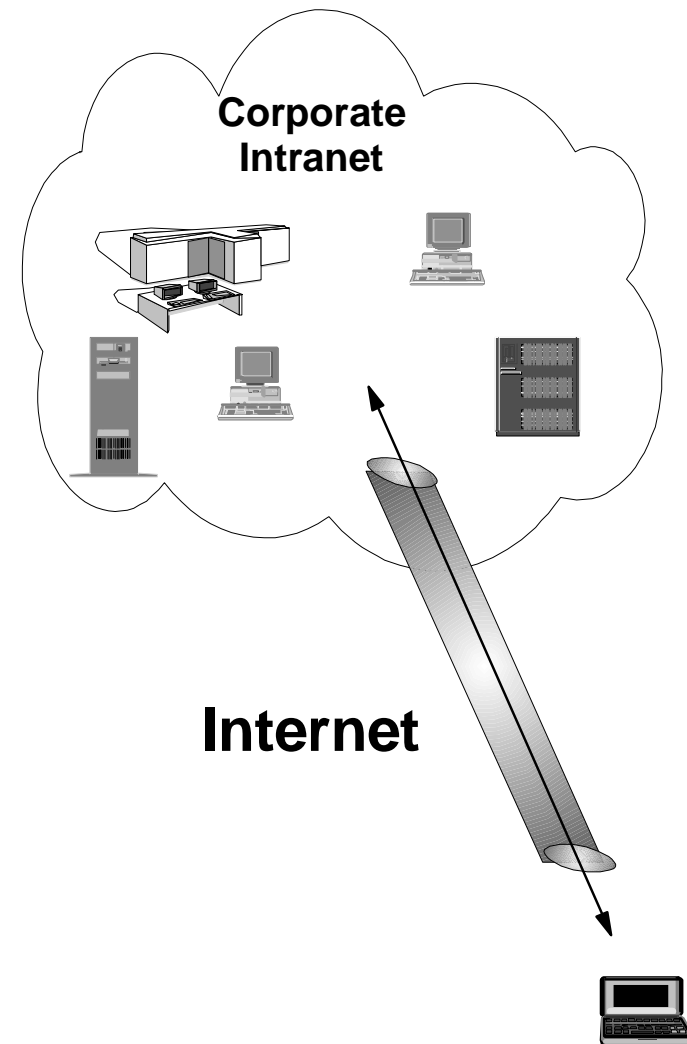


VPN Motivators

- **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!**

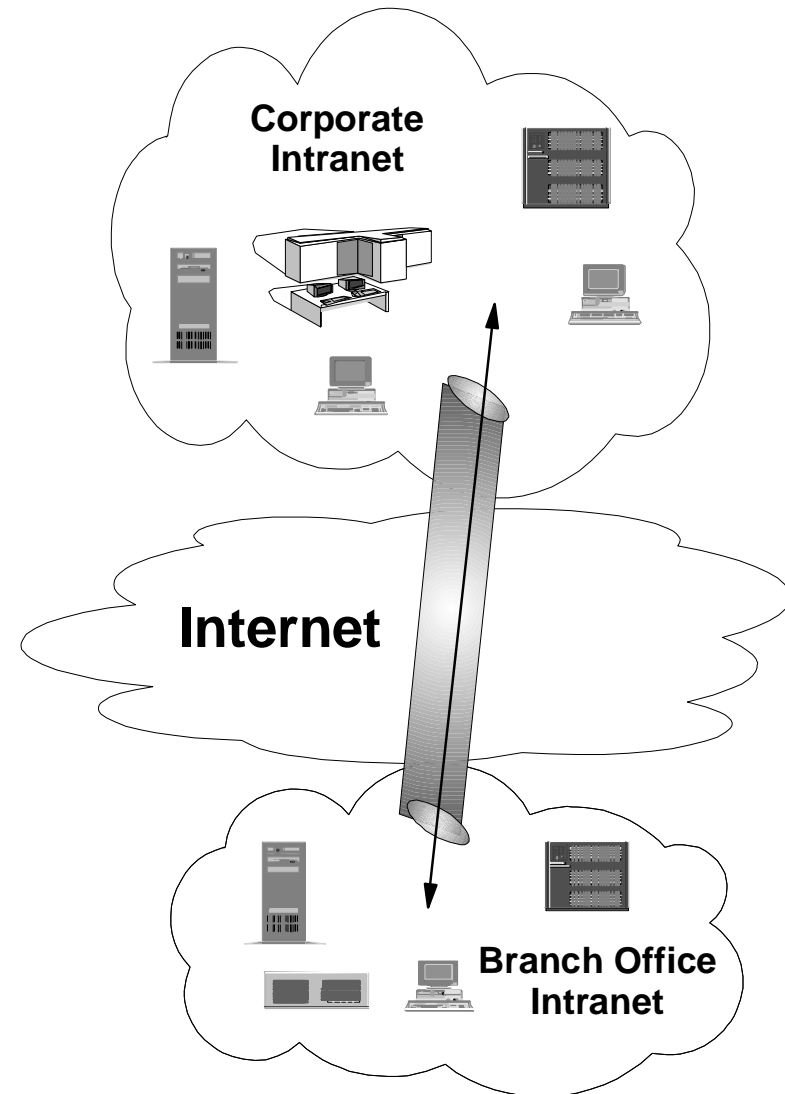
Mobile user VPN

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



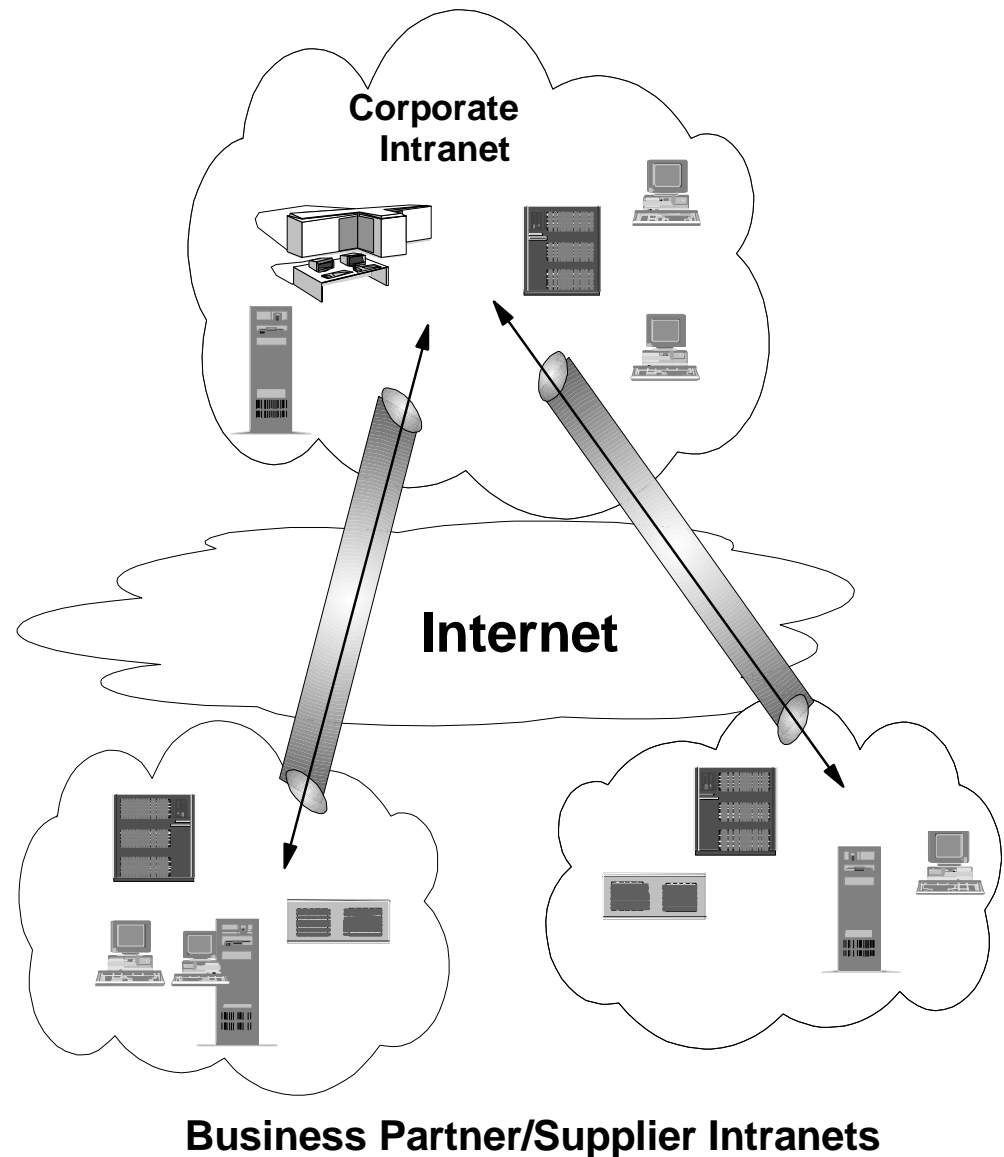
Branch Office VPN

- 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)



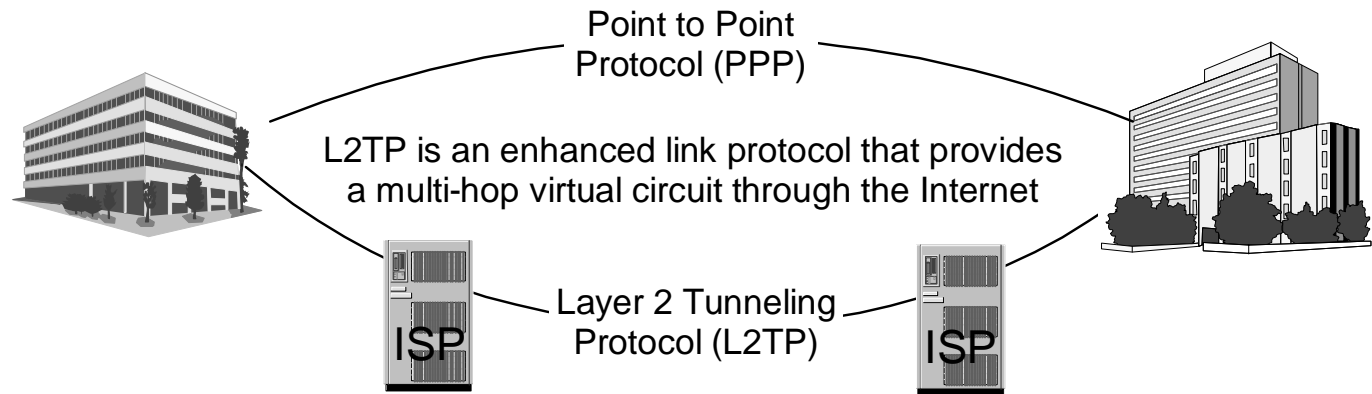
VPN Technologies



The Core VPN Standards Based Protocols

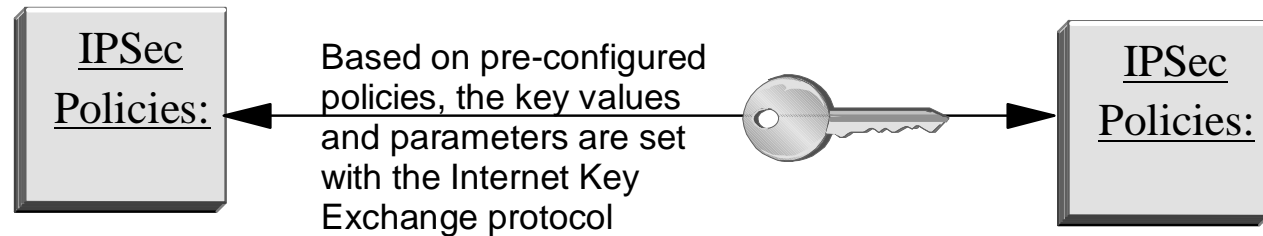
1. L2TP

open the link that creates the circuit



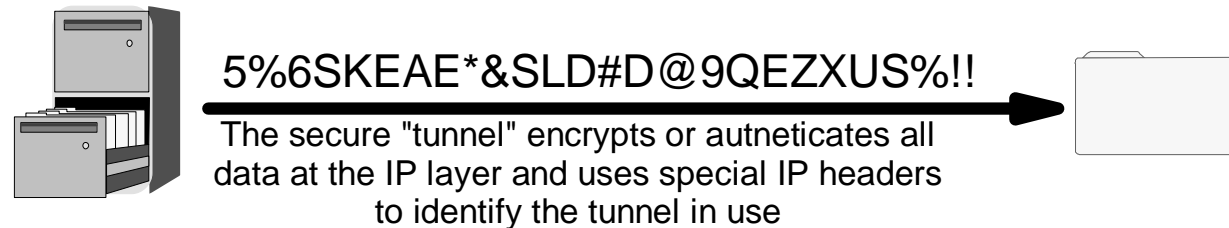
2. IKE

negotiates the encryption keys and policies

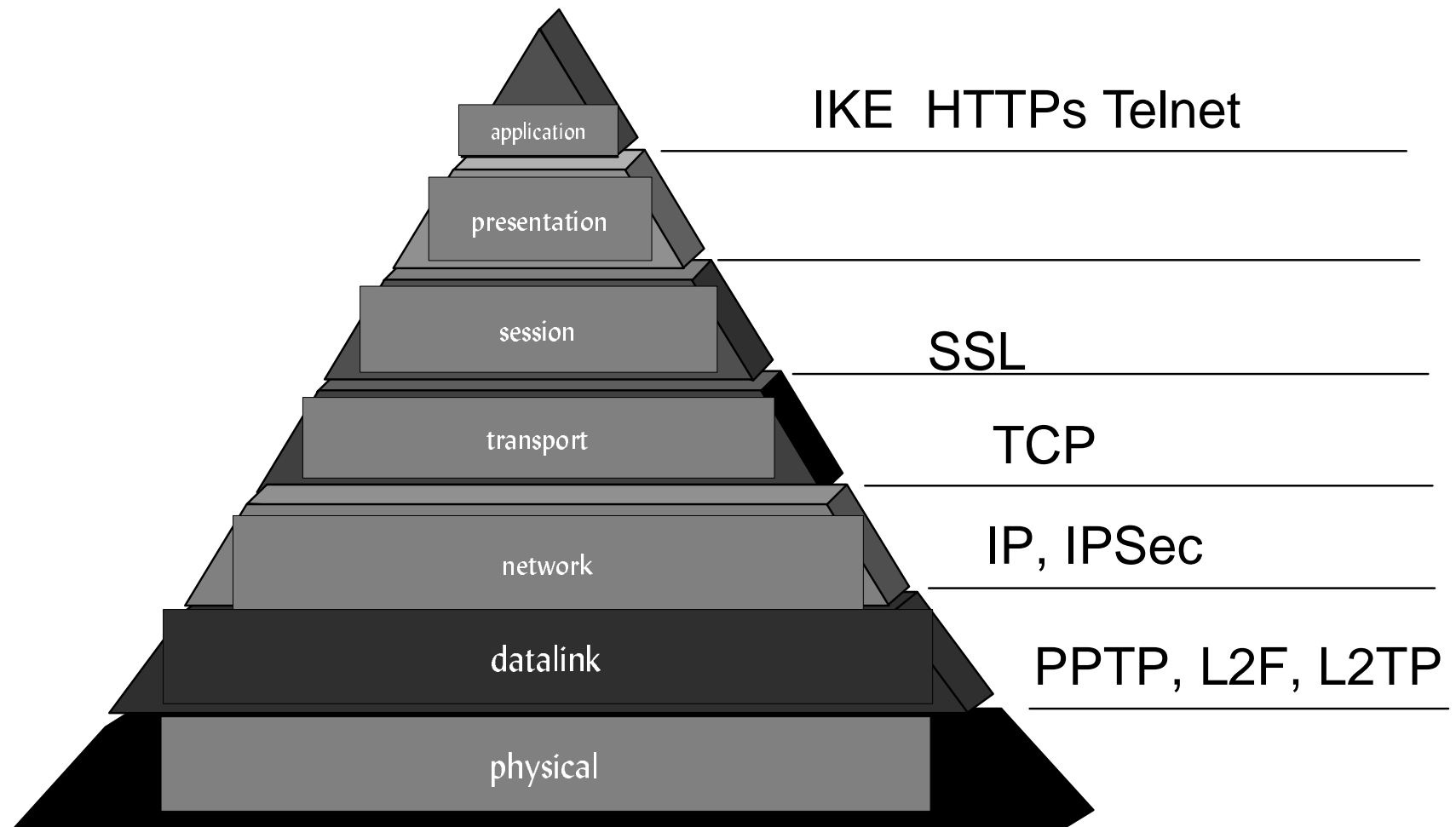


3. IPSec

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**

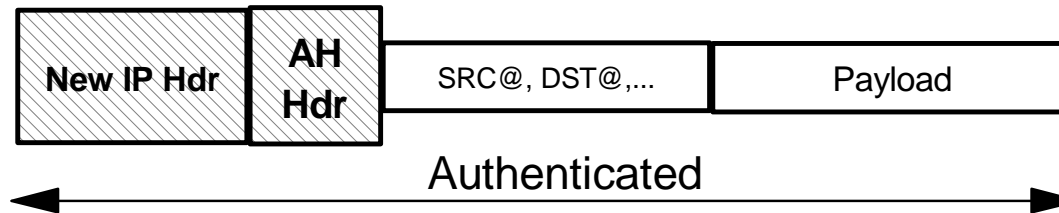
AH Coverage

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

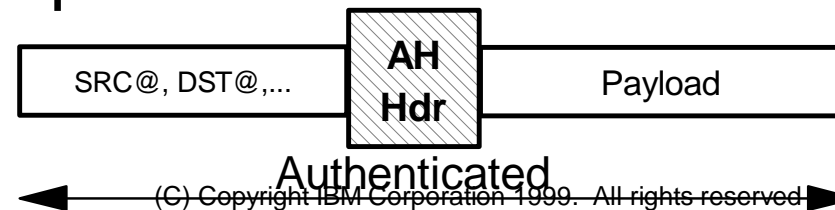
Original Datagram



AH-Tunnel:



AH-Transport:



ESP Coverage

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

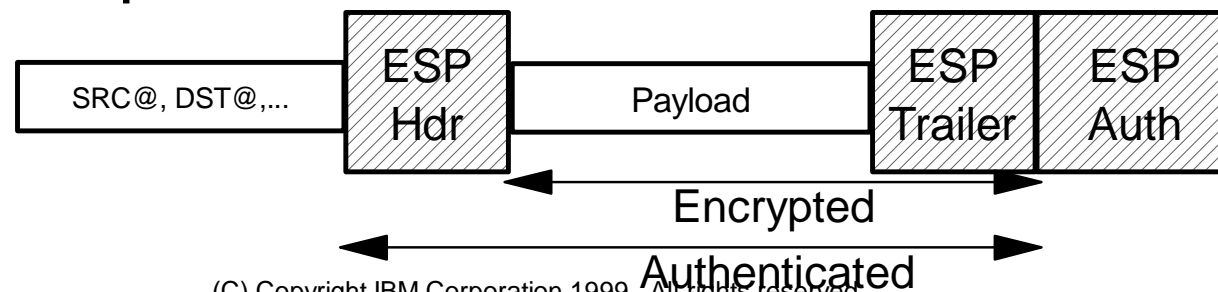


Original Datagram

ESP-Tunnel:

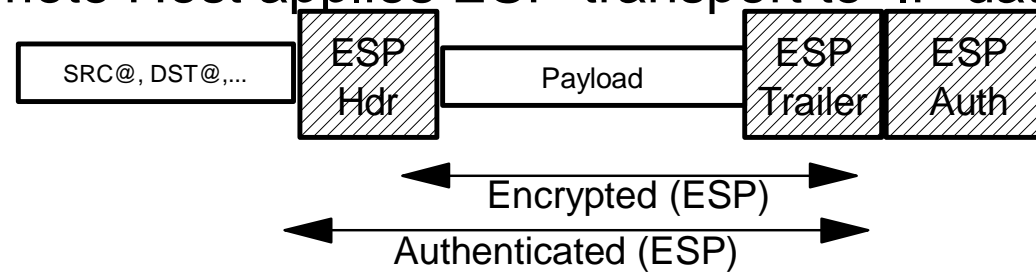


ESP-Transport:

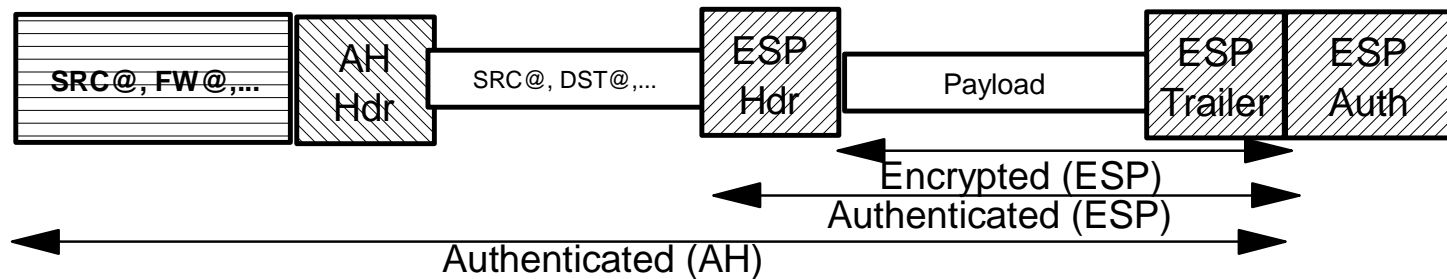


AH and ESP Combine

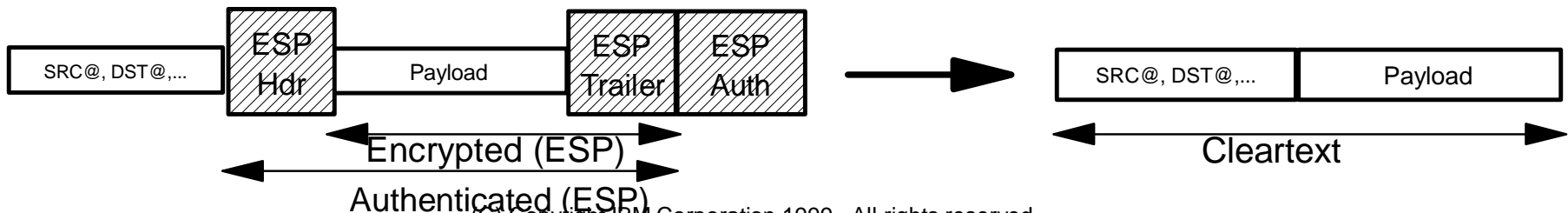
- First, Remote Host applies ESP-transport to IP datagram:



- 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**

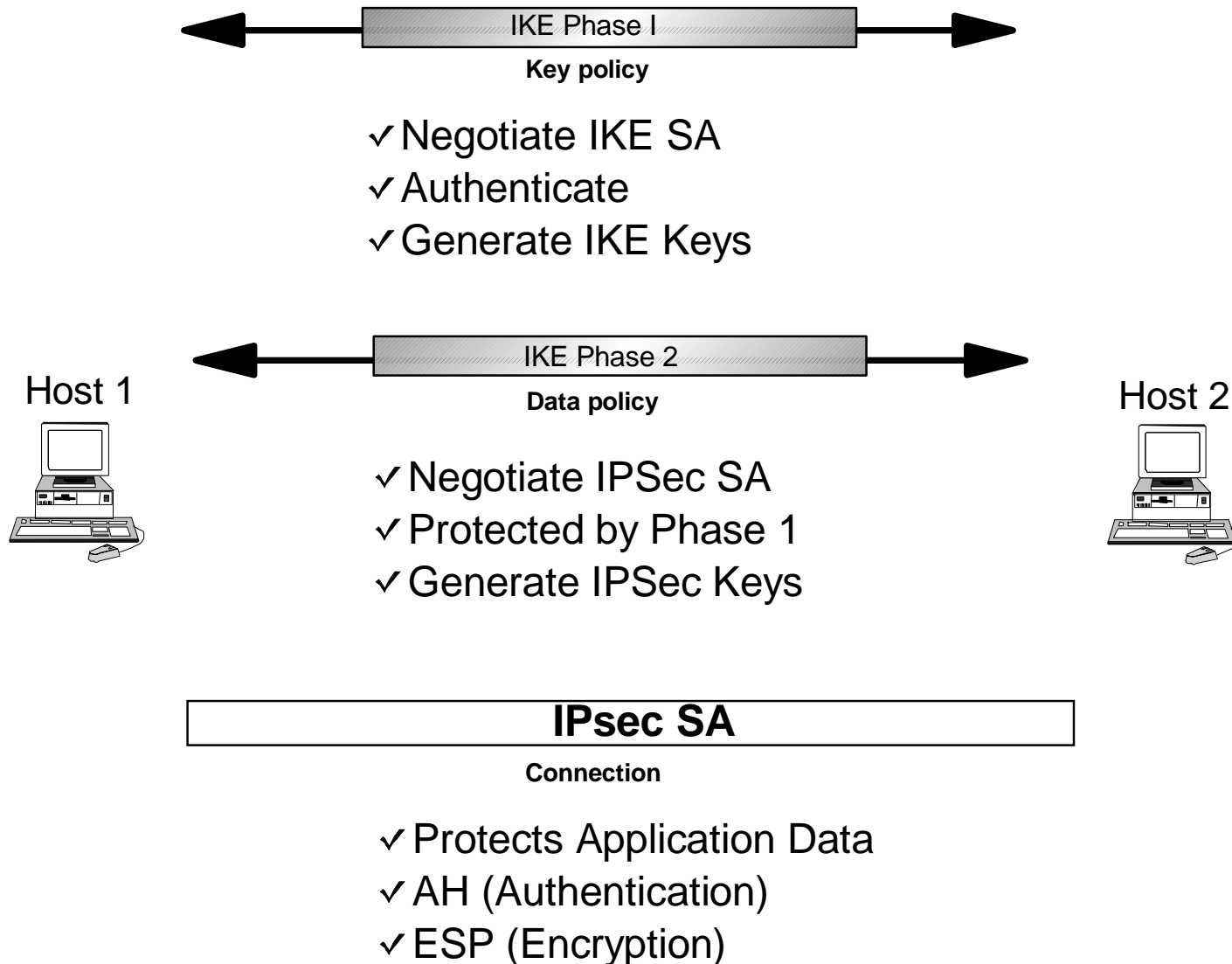
Internet Key Exchange (IKE)

- **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



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 Technologies

■ Firewall for AS/400

- Manual Tunnels
- IBM Tunnels for dynamic key exchange
- Configured using web browser

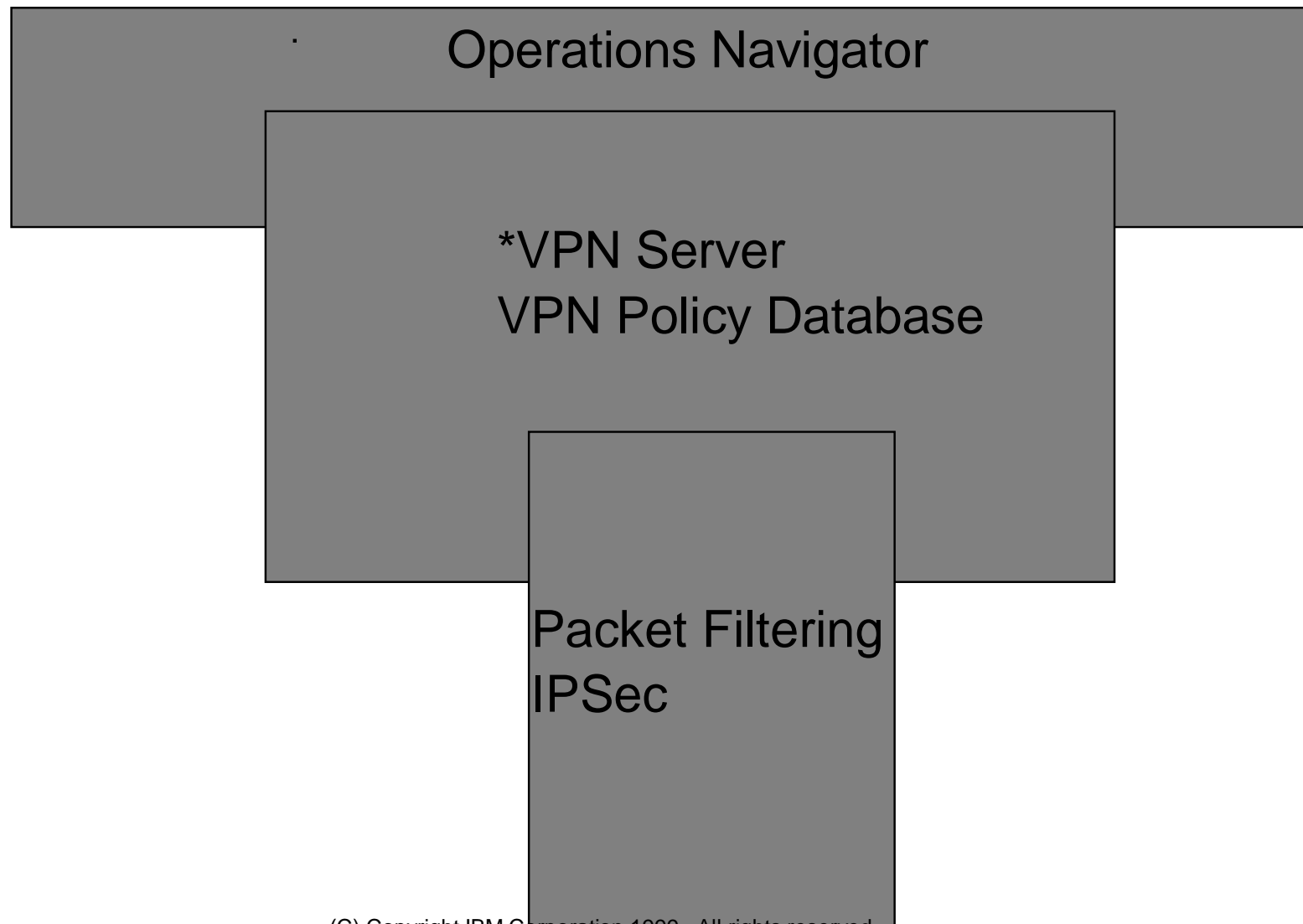
■ Native IP Filtering and NAT

- 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 Dynamic 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, ENDTCPSPVR
 - 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 traffic to flow between systems
- L2TP uses UDP well known port 1701

AS/400 Native VPN - Configuration

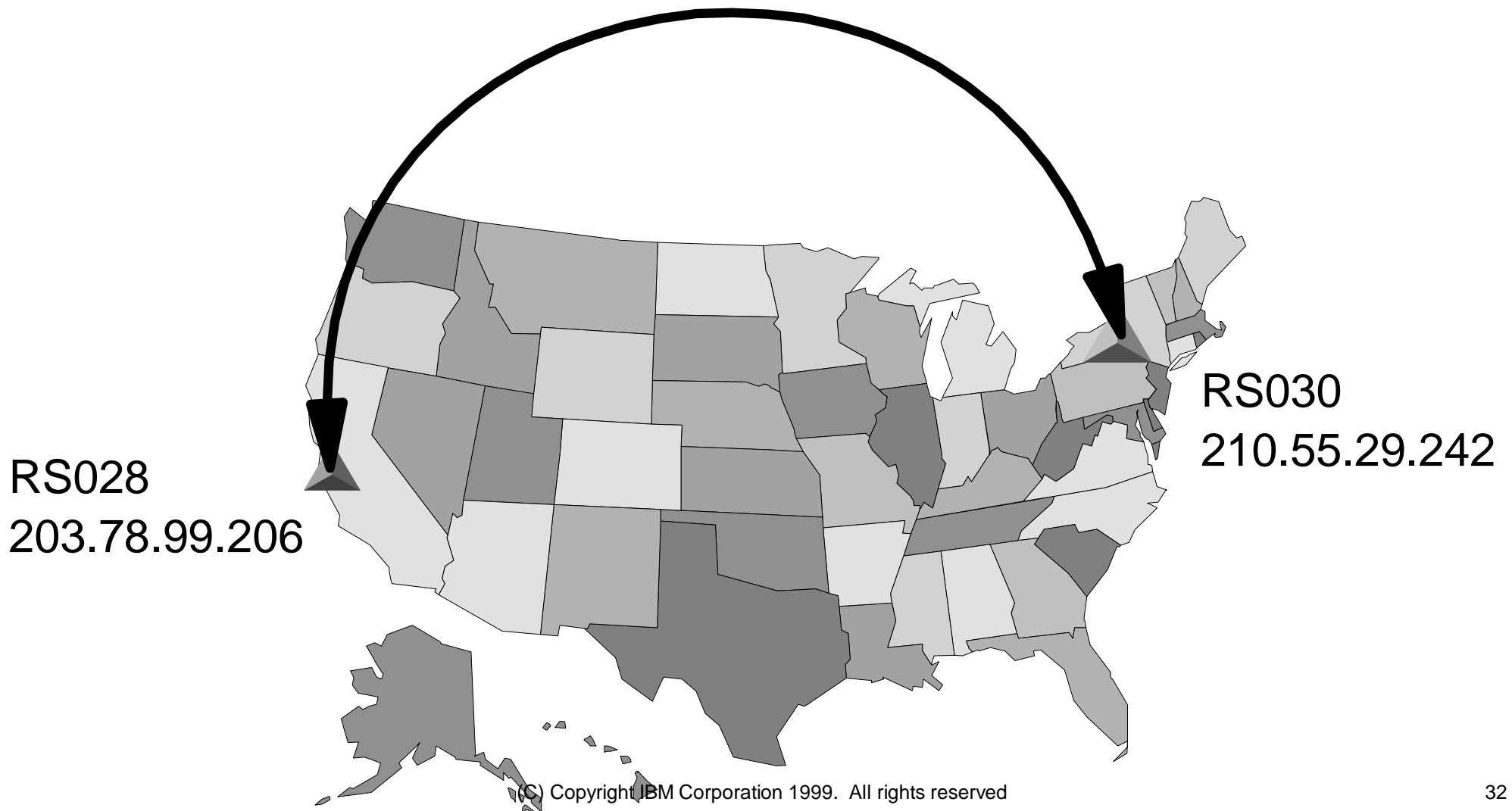
- **Documented in the Information Center**
- **Plan your VPN security policy**
 - Endpoints (host or gateway)
 - Data protection (AH, ESP or both)
 - Key management (manual or dynamic)
- **Use Operations Navigator to configure**
 - VPN Policy
 - IP Packet Security Filtering Rules

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

The screenshot displays the AS/400 Operations Navigator interface. The window title is "AS/400 Operations Navigator". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for Cut, Copy, Paste, Delete, Refresh, and Stop. The status bar indicates "0 minutes old".

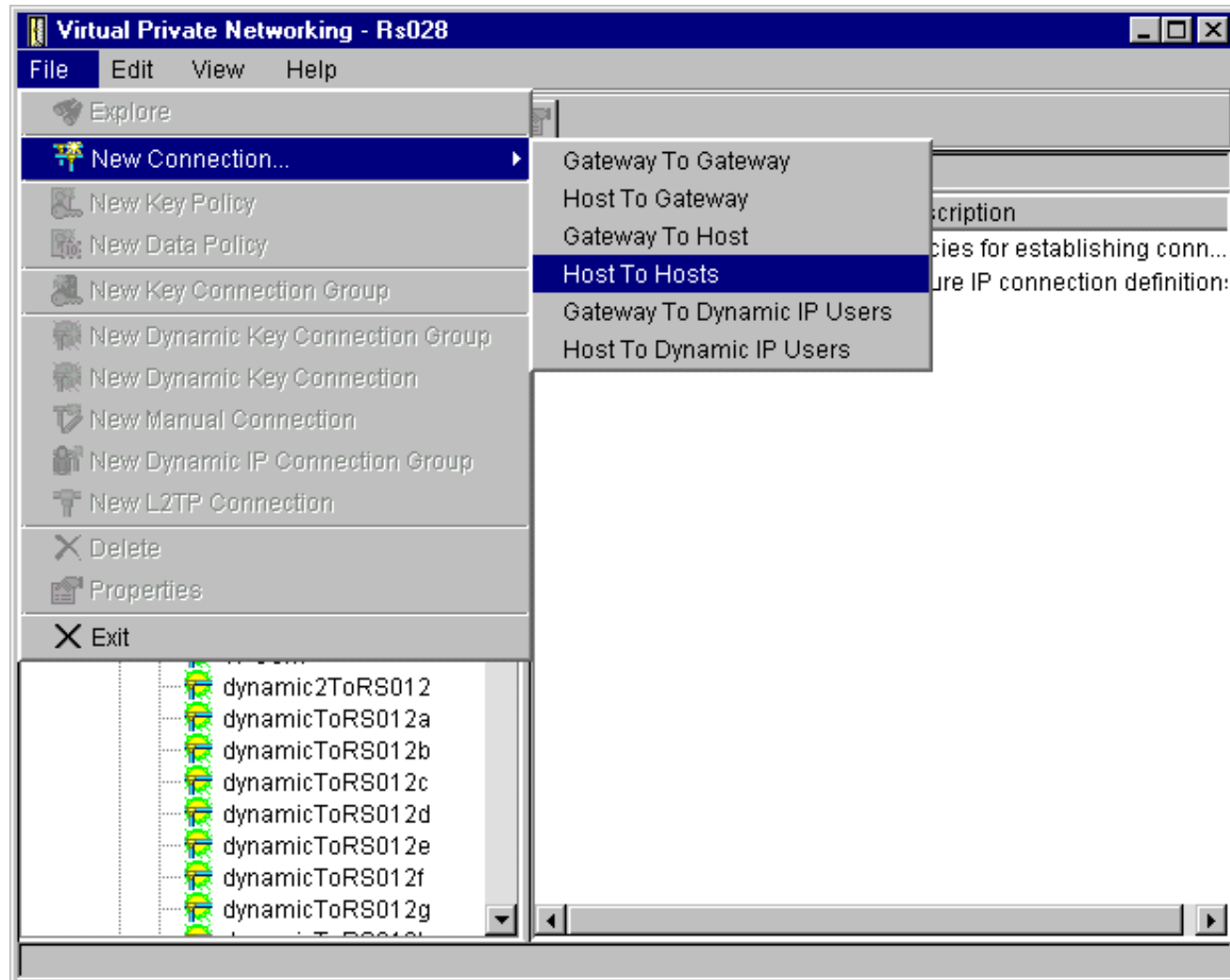
The interface is divided into two main panes:

- Left Pane (Environment):** Shows a tree view of the system configuration. The selected path is "My AS/400 Connections" > "Rs028" > "Network" > "IP Security".
- Right Pane (Rs028: IP Security):** Displays a table of IP Security objects.

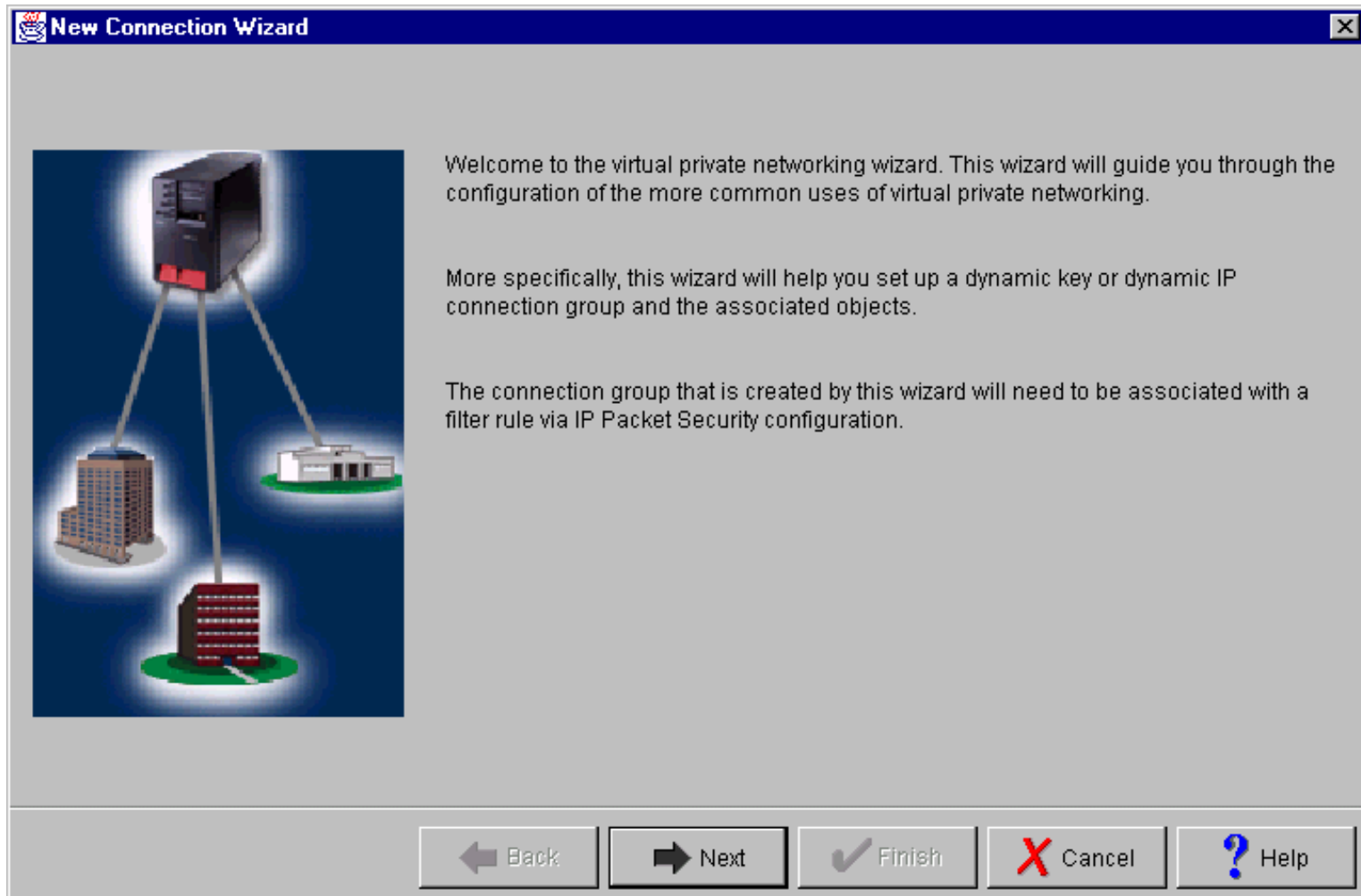
Server Name	Status	Description
IP Packet Security	Active	IP packet security filter rules
Virtual Private Networking	Started	Secure connections and policies

The status bar at the bottom indicates "1 - 2 of 2 object(s)".

Op Nav Virtual Private Networking



The New Connection Wizard



Naming the Connection

 Connection Name X

What would you like to name this connection group?

Name:

How would you like to describe this connection group?

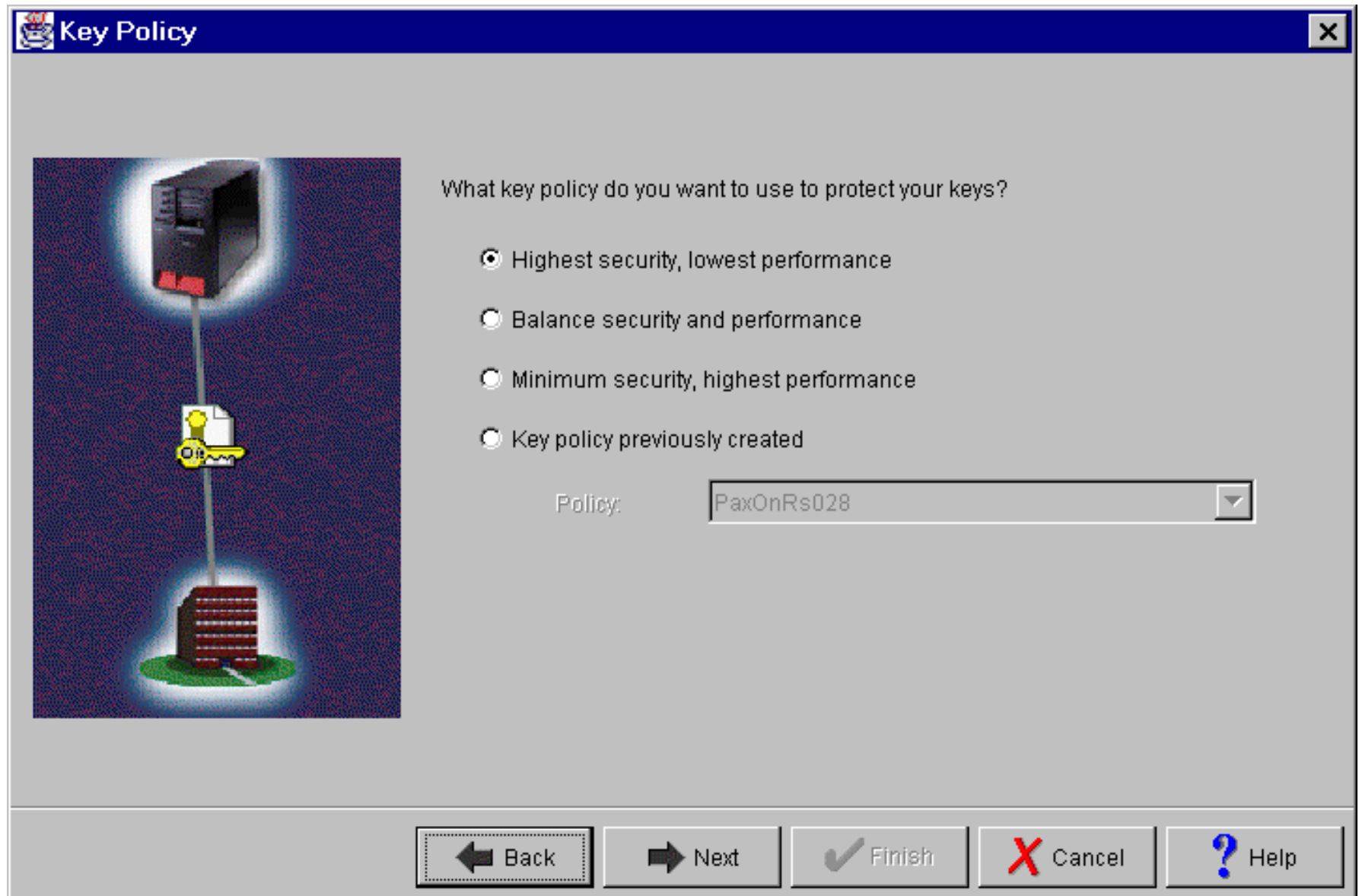
Description:



(C) Copyright IBM Corporation 1999. All rights reserved

38

Choosing Key Policy for IKE



Identifying the local systems

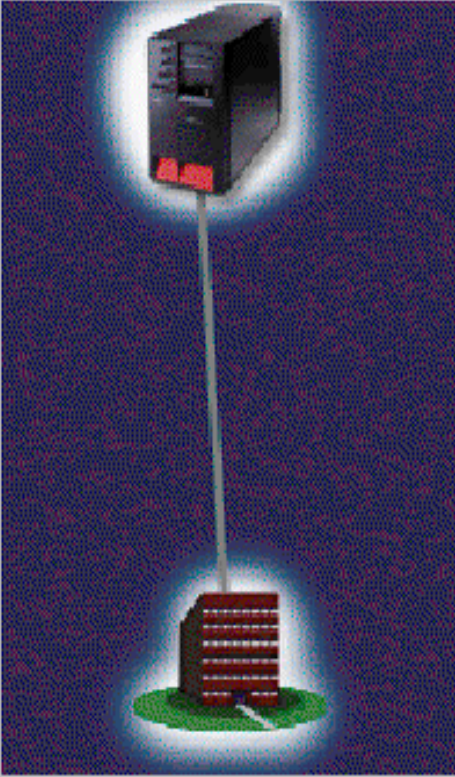
Local Identifier [X]

Enter the identifier to represent the local key server for this connection.

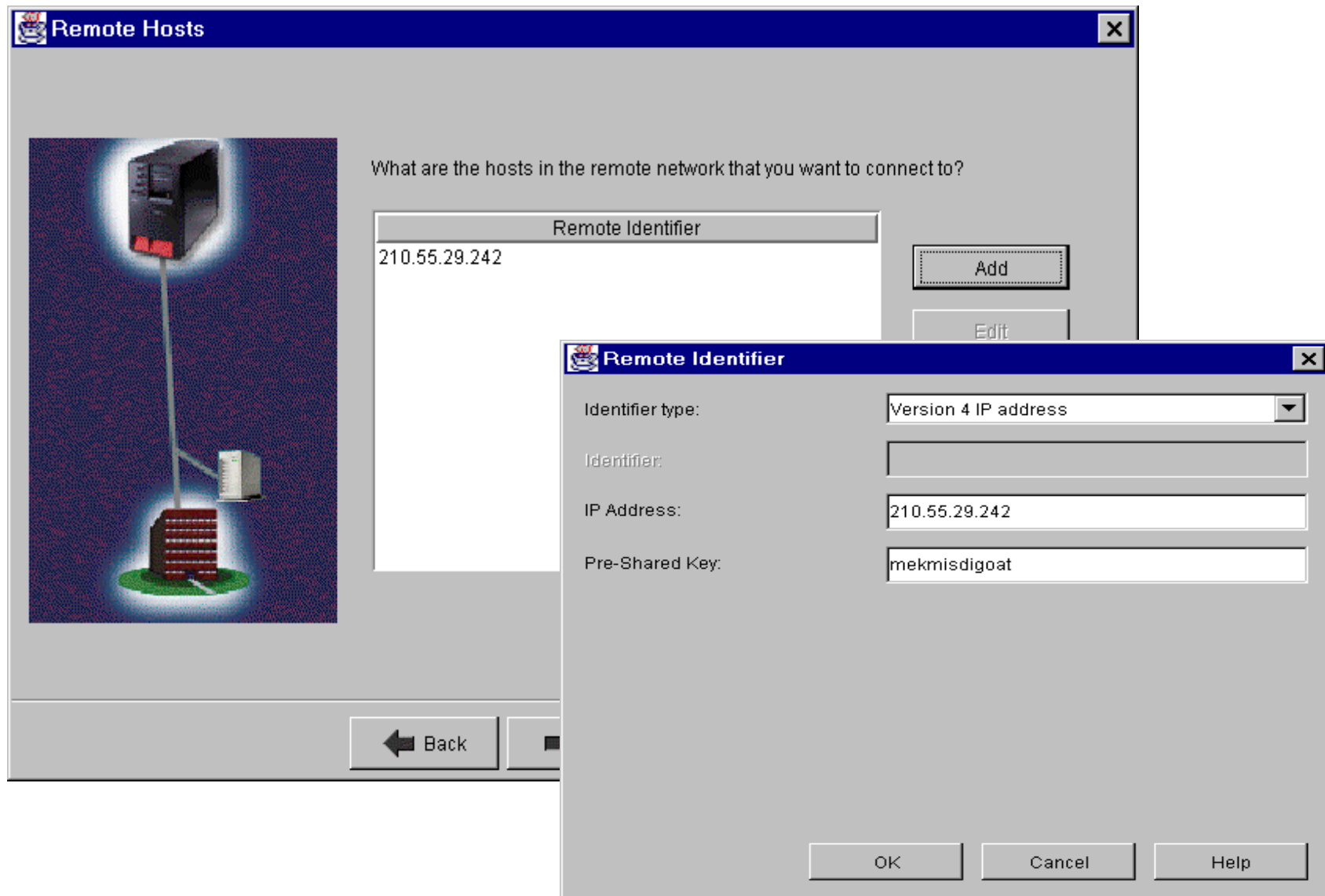
Identifier type:

Identifier:

IP Address:

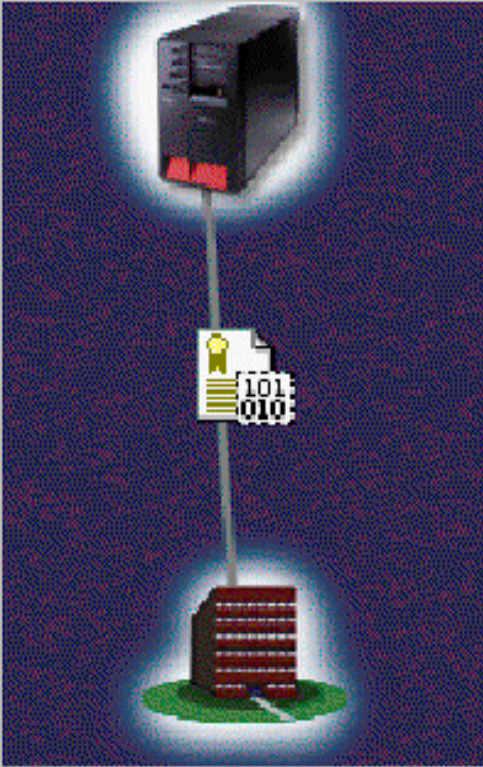


Identifying the remote system(s)



Choosing Data Policy for IPSec

Data Policy [X]



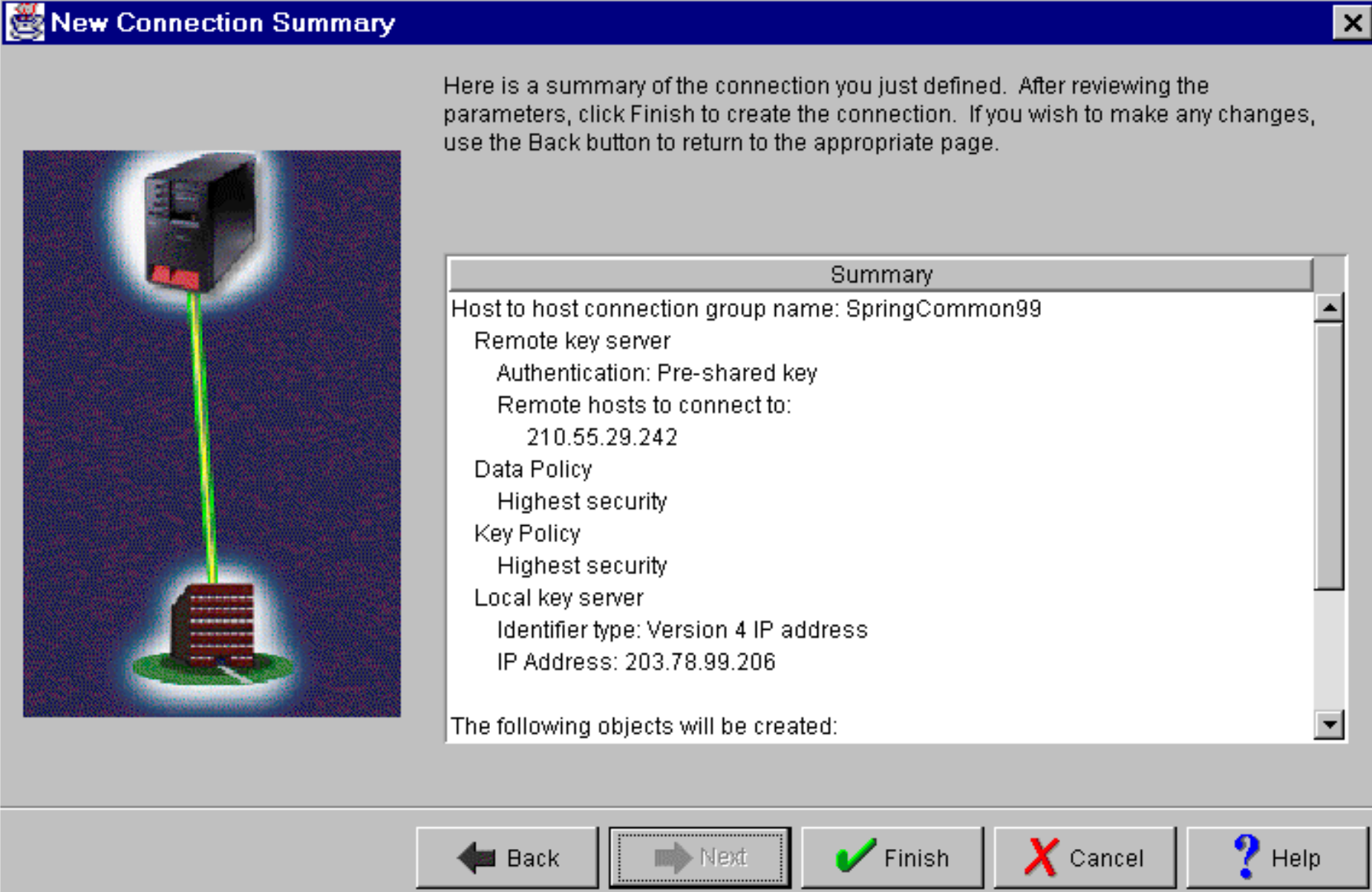
What data policy do you want to use to protect the data?

- Highest security, lowest performance
- Balance security and performance
- Minimum security, highest performance
- Data policy previously created

Policy:

← Back **→ Next** ✓ Finish ✗ Cancel ? Help

Verify the results of the Wizard



New Connection Summary

Here is a summary of the connection you just defined. After reviewing the parameters, click Finish to create the connection. If you wish to make any changes, use the Back button to return to the appropriate page.

Summary

Host to host connection group name: SpringCommon99

Remote key server
Authentication: Pre-shared key

Remote hosts to connect to:
210.55.29.242

Data Policy
Highest security

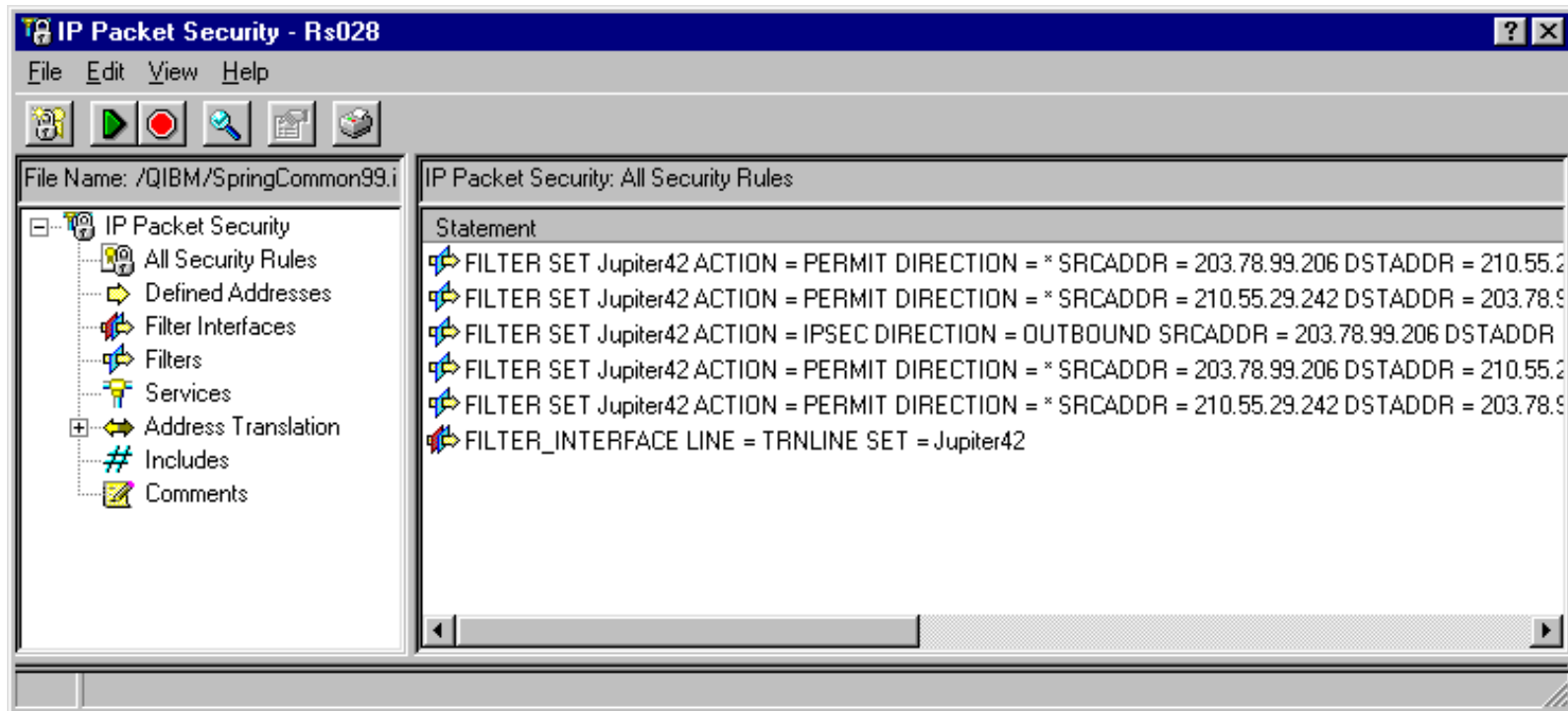
Key Policy
Highest security

Local key server
Identifier type: Version 4 IP address
IP Address: 203.78.99.206

The following objects will be created:

Back Next Finish Cancel Help

Define the IP Filtering Rules



Create a rule to PERMIT IKE

New Filter - Rs028

General | Services

Set name: Jupiter42

Action: PERMIT

Direction: *

Source address name: = 203.78.99.206

Destination address name: = 210.55.29.242

Fragments: NONE

Journaling: OFF

Connection name:

Description:
Permit IKE traffice between Moscone Center and home office in New York

OK Cancel Help

IKE uses UDP well known port 500

The screenshot shows a dialog box titled "New Filter - Rs028" with a "Services" tab selected. The "Service" radio button is selected, and the "Protocol" is set to "UDP". Both "Source port" and "Destination port" are set to "500".

General Services

Service name:

Service:

Protocol: UDP

Source port: = 500

Destination port: = 500

ICMP service:

Type: =

Code: =

OK Cancel Help

IKE must flow both directions...

Filter Properties - Rs028

General Services

Set name:

Action:

Direction:

Source address name:

Destination address name:

Fragments:

Journaling:

Connection name:

Description:

OK Cancel Help

s028

Description:

OK Cancel Help

Create a rule to IPSEC

New Filter - Rs028

General Services

Set name: Jupiter42

Action: IPSEC

Direction: OUTBOUND

Source address name: = 203.78.99.206

Destination address name: = 210.55.29.242

Fragments: NONE

Journaling: OFF

Connection name: SpringCommon99

Description:
Apply IPSEC action to all data flowing between the two hosts, use the Connection Group just created especially for Spring Common

OK Cancel Help

PERMIT other traffic

- Default IP Filtering action is DENY everything...

Filter Properties - Rs028

General Services

Set name: Jupiter42

Action: PERMIT

Direction: *

Source address name: = ConfigurationPC

Destination address name: = LocalSystem

Fragments: NONE

Journaling: OFF

Connection name:

Description:
After IPSEC action, all packets are subject to normal filtering.

OK Cancel Help

Associate rules with a line

New Filter Interface - Rs028

General

Line

Line name: TRNLINE

IP address:

Point-to-point profile name:

Set names:

Jupiter42

Add

Remove

Description:

Associate the Jupiter42 set with the physical line name TRNLINE

OK Cancel Help

Load the filter rules

- Rules will be verified before they are loaded

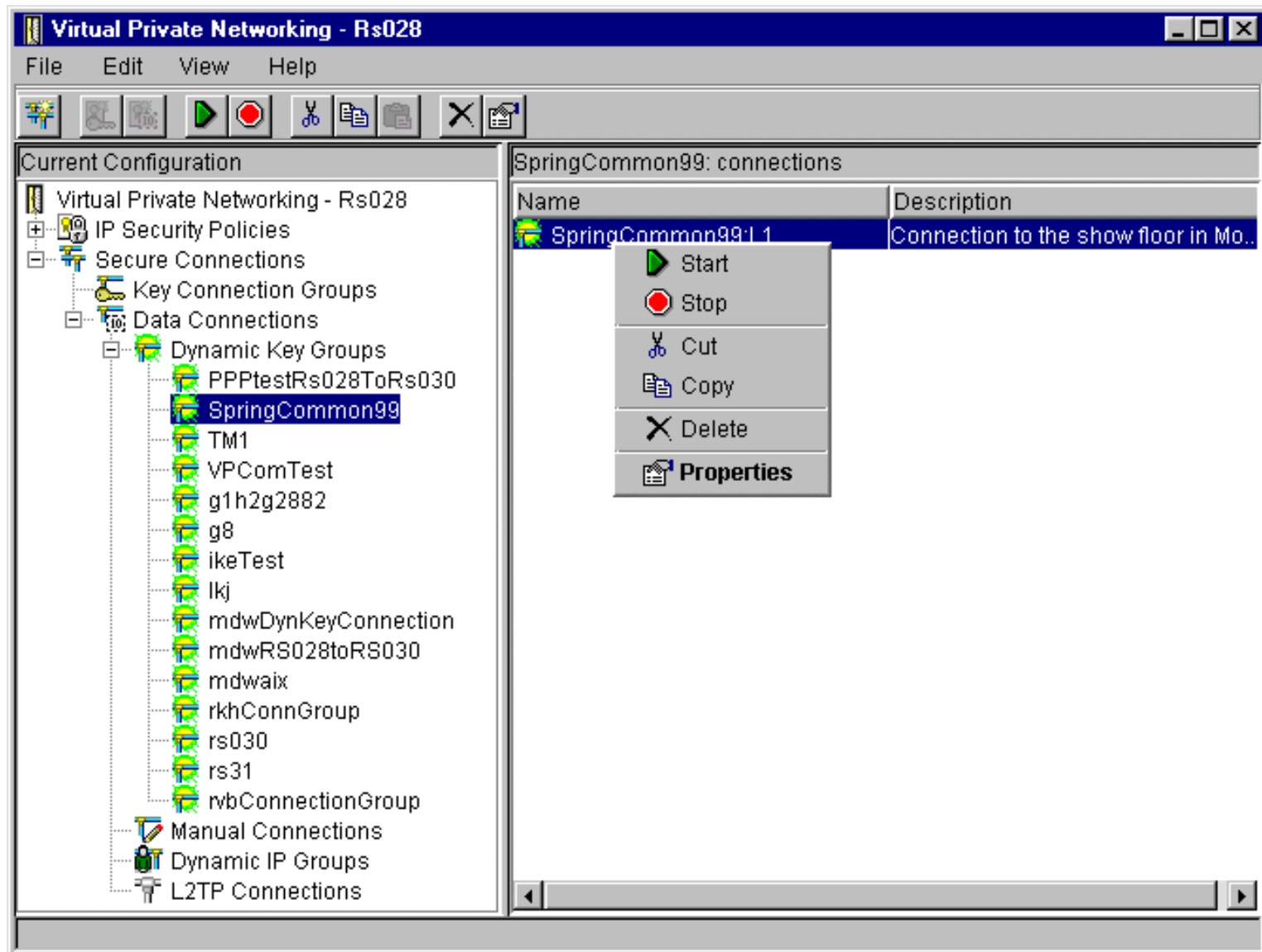
The screenshot shows the 'IP Packet Security - Rs028' window. The left pane displays a tree view with 'All Security Rules' selected. The right pane shows a list of filter rules for 'Jupiter42'. Below the rules, a table displays error messages from the log.

Line Number	File Name	Error Code	Error Text
0		TCP5AFC	A line description was found without a FILTER_INTERFACE statement defini
0		TCP5AFC	A line description was found without a FILTER_INTERFACE statement defini
0		TCP5B01	IP filtering, IP security or NAT rules were processed. Messages were generat Request codes are as follows: 01 - Rule Retrieve. 02 - Rule Verification. 03 - The rules file was successfully activated.

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....

The screenshot displays the 'Virtual Private Networking - Rs028' window. The 'View' menu is open, showing options like 'Active Connections'. The left pane shows a tree view of connection groups, with 'SpringCommon99' selected. The right pane shows a table of connections for 'SpringCommon99: connections'.

Name	Description
SpringCommon99:L1	Connection to the show floor in Mo..

Below this, the 'Active Connections - Rs028' window is open, showing a detailed table of active connections.

Name	Status	Error Information	Active Security Associations	Cumulative Security Associ...	Failed Security ...	Remaining Key ...
SpringCommon99:L1	Running		1	1	0	3

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.