ibm.com

e-business

Symantec Enterprise Firewall for the IBM eServer iSeries running Linux

LP03

ITSO iSeries Technical Forum

Yessong Johng

Redbooks

International Technical Support Organization

Disclaimer

Information is provided "AS IS" without warranty of any kind. Mention or reference to non-IBM products is for informational purposes only and does not constitute an endorsement of such products by IBM.

This presentation contains IBM plans and directions. Such plans are subject to change without notice.

This presentation is for pre-GA product of Symantec Enterprise Firewall for iSeries running Linux V7.0.3. The actual implementation of the product can be different from what are covered here.

Objectives

Learn SEF for iSeries of its:

- Features and terminology
- Installation
- Basic setup
- Configuration
- Administration

SEF for iSeries is used for **Symantec Enterprise Firewall for iSeries running Linux** throughout this presentation.

Symantec Overview

Why SEF for iSeries?

Manageability

- Consolidating SEF to run on iSeries Linux
  - ✓ Reduces the number of machines to administer and eases manageability

Reliability

- iSeries provides an extremely reliable hardware platform for the firewall
  - ✓ iSeries has hardware redundancy
    - ► multiple power supplies
    - ► uses RAID to protect data on disk drives

Backup and Recovery

- Combined backup and recovery features
  - ✓ SEF for iSeries uses NWSD storage space for storage
    - ► This storage space is saved when the iSeries is saved providing a complete backup of your firewall
  - ✓ SEF for iSeries also has its own backup and recovery functionality that backs up the firewall configuration

Why SEF for iSeries? (cont.)

Performance

- iSeries LPAR provides dynamic resource allocation

Cost

- Consolidating SEF onto iSeries Linux
  - ✓ Eliminates the extra cost involved of purchasing additional hardware and software licenses

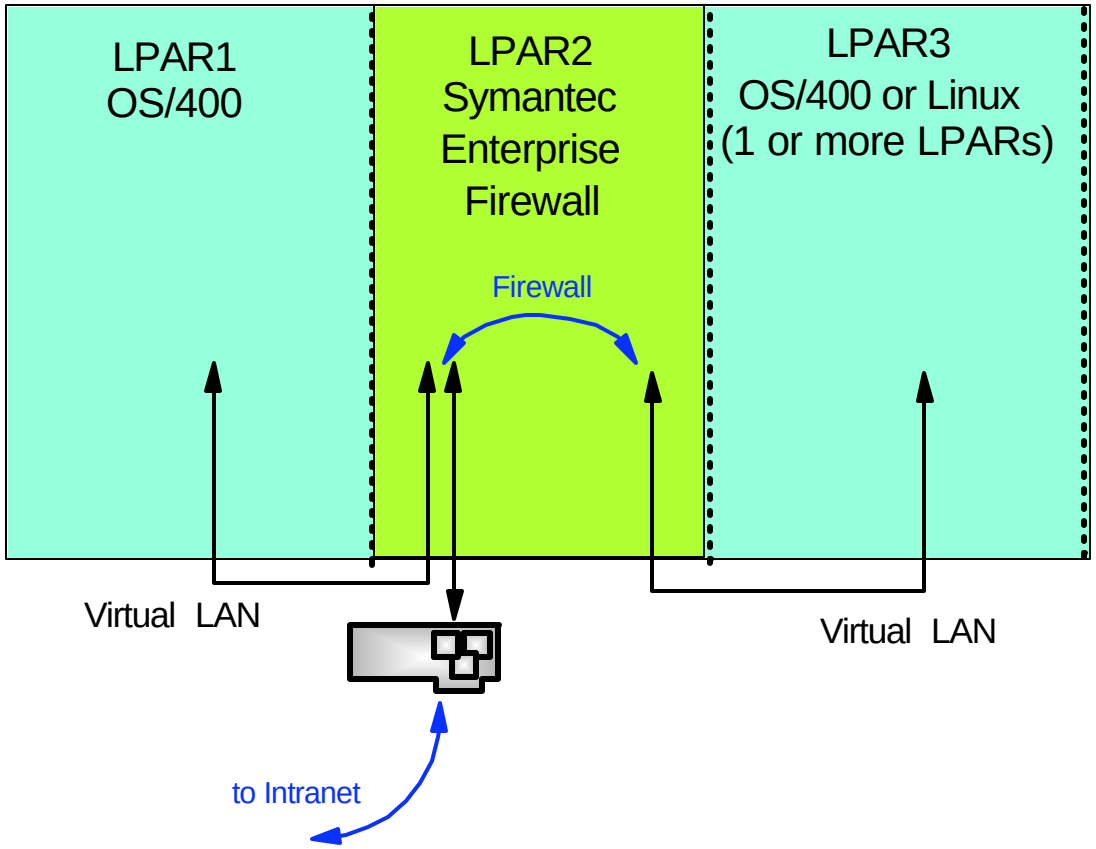
High Speed Communication

- iSeries provides virtual LAN communication between partitions
  - ✓ Allowing extremely high speed communication SEF and other partitions including OS/400 partitions

SEF for iSeries running Linux: Topologies

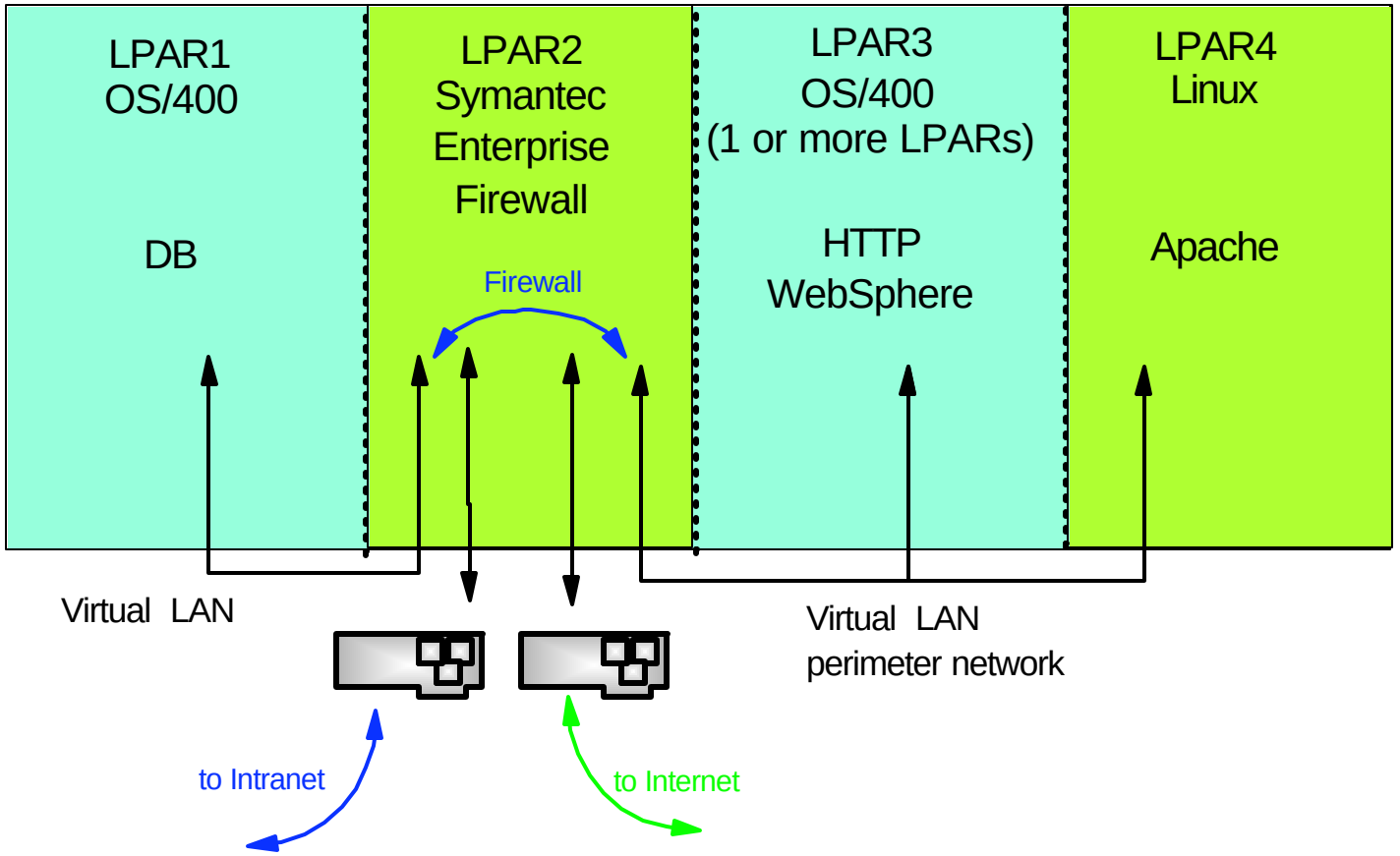
Topology 1

Symantec Enterprise Firewall with an Intranet



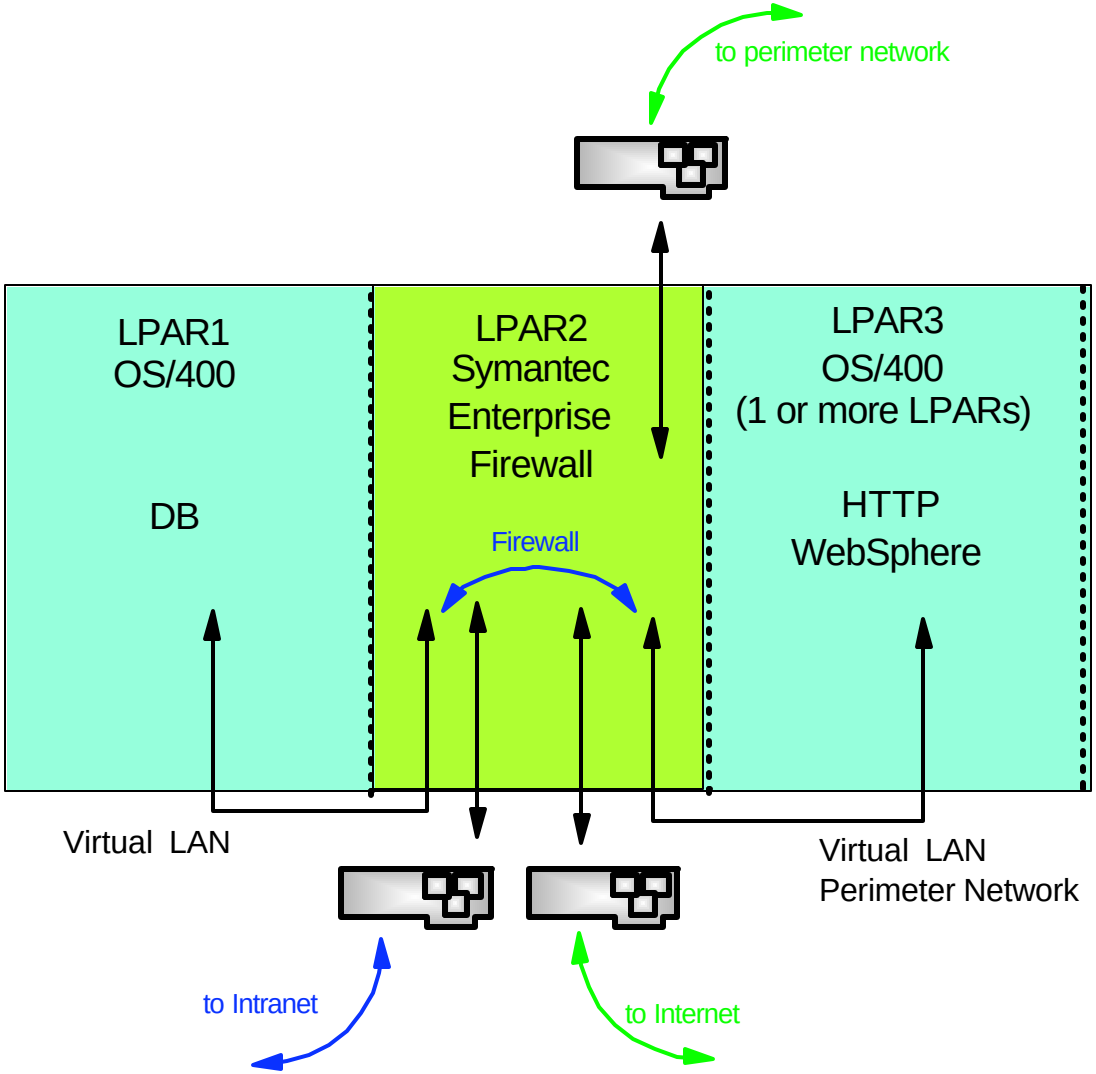
Topology 2

SEF with an Intranet and a virtual LAN perimeter network



Topology 3

SEF with an Intranet and with a perimeter network



SEF for iSeries running Linux: Features and Terminology

SEF for iSeries Features

SEF for iSeries is a comprehensive hybrid firewall

- That is designed to provide secure and fast communications
- Employing all three firewall types with features include:
  - ✓ Stateful packet inspection
  - ✓ Full application inspection with many built in application proxies and a generic service proxy called the Generic Service Passer (GSP)
  - ✓ Built in DNS server
  - ✓ Network address translation and address hiding
  - ✓ Supports user authentication with S/Key, SecurID, RADIUS, Defender, TACACS+, and OOBA
  - ✓ Protection from denial of service (DoS) attacks

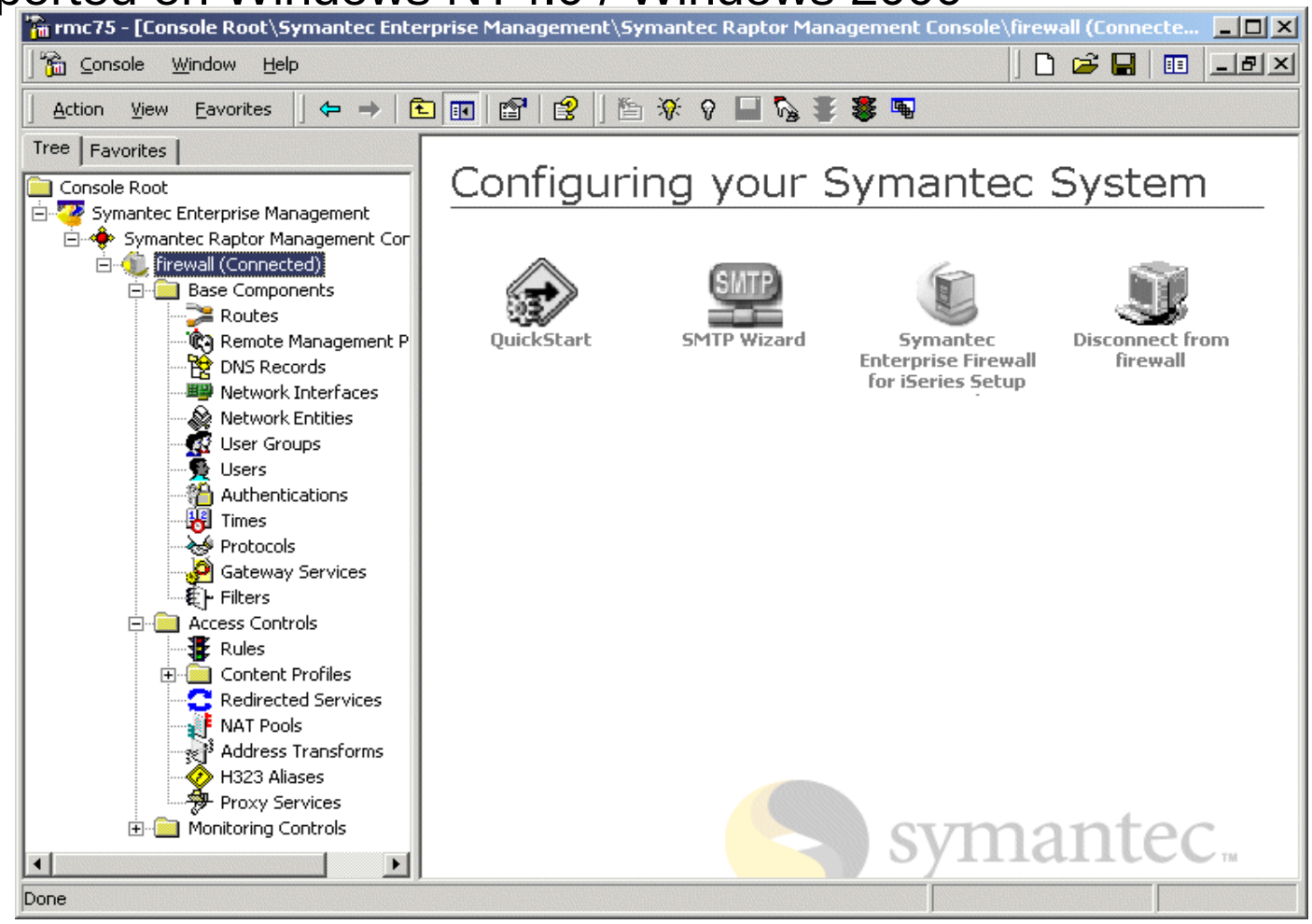
SEF for iSeries Features (cont.)

- Detailed logging facilities such as session duration, full URLs, user names and authentication methods
- Notification based on user defined events
- Diagnostic tools
- Web content filtering available with purchase of a license
- GUI configuration and easy to use setup wizards
- Remote management with the Symantec Raptor Management Console (SRMC)
- Easy installation from CD
- Hardened Linux operating system
- Supports 10/100MB iSeries ethernet adapters (2838 and 2849) and iSeries virtual LAN

SRMC

Symantec Raptor Management Console (SRMC)

- The graphical user interface to configure SEF
- Supported on Windows NT4.0 / Windows 2000



Features and Terminology

Network Entities

- The objects composing your network
  - ✓ Host
  - ✓ Subnet
  - ✓ Domain
  - ✓ Group: An entity combined hosts or subnets into one network entity

Protocols

- The protocols the requested services use
  - ✓ SEF provided protocols: HTTP*, TELNET*, ...
  - ✓ User defined protocols:
    - ► Base protocol: IP, TCP, UDP, or ICMP
    - ► Source and Destination port range: in the case of base protocol TCP
    - ► Protocol number: in the case of IP
    - ► Message type: in the case of ICMP

Features and Terminology

Filters

- Provide packet filtering
  - ✓ Allow/Deny protocol (service)
    - From Network entity A
    - To Network entity B
- Applied to inbound or outbound traffic on an interface
- Only one filter can be applied to a direction for an interface
- No application level checks are performed
- No user authentication is possible

Features and Terminology

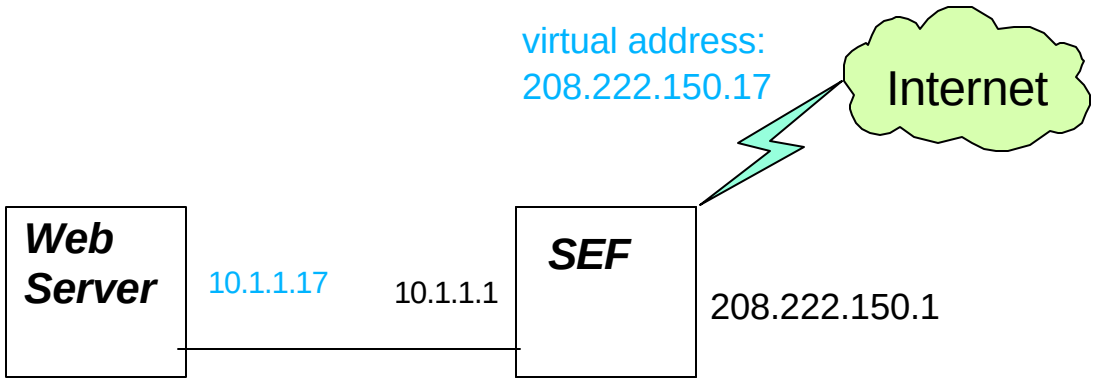
Rules

- Provide full application level checks with stateful inspection
  - ✓ Allow/Deny protocol (service) between Network entities
    - ➤ Coming in / out Network interfaces
    - ➤ Allows user authentication
    - ➤ Time restraints
- Application level checks on all packets
- More secure than filters
- Easier to configure

Features and Terminology

Network address translation

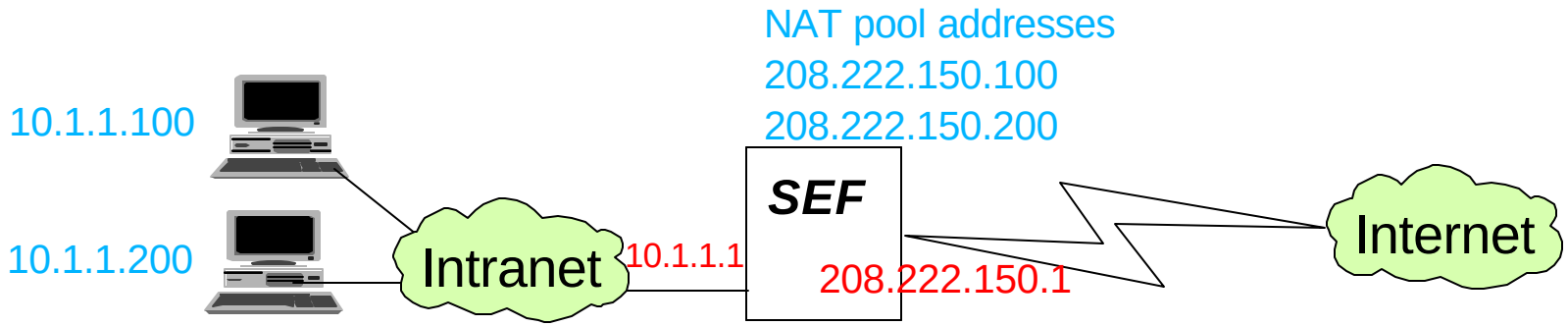
- **Redirect services**
  - ✓ Used to change the destination IP address of incoming packets
  - ✓ Allow a server with a private (non-routable) IP address to be publicly accessible
    - ➤ Example: Redirect HTTP from 208.222.150.17 to 10.1.1.17



Features and Terminology

Network address translation

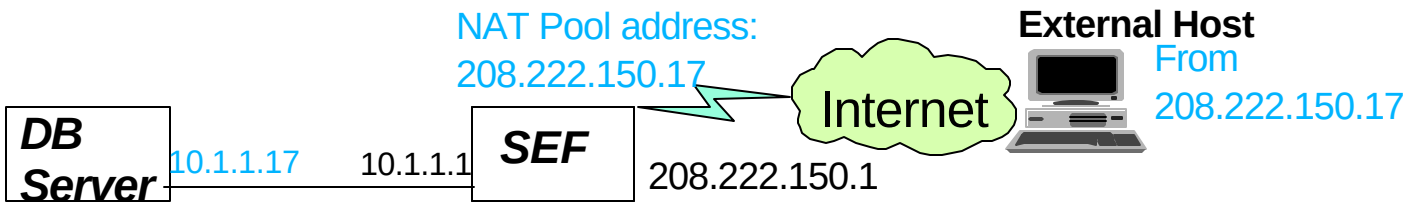
- **NAT Pools**
  - ✓ Sets of IP address
  - ✓ SEF can use address transforms to replace client IP addresses with IP addresses from a NAT pool
  - ✓ Used to hide private IP addresses from the Internet
  - ✓ Two types of NAT pools:
    - ➤ Dynamic
    - ➤ Static: one-to-one



Features and Terminology

Network address translation

- **Address Transforms**
  - ✓ Used to change the source IP address of outgoing packets
  - ✓ Has three options:
    - ➢ Use SEF address (default behavior)
    - ➢ Use original client address
    - ➢ Use an IP address from a NAT pool



Features and Terminology

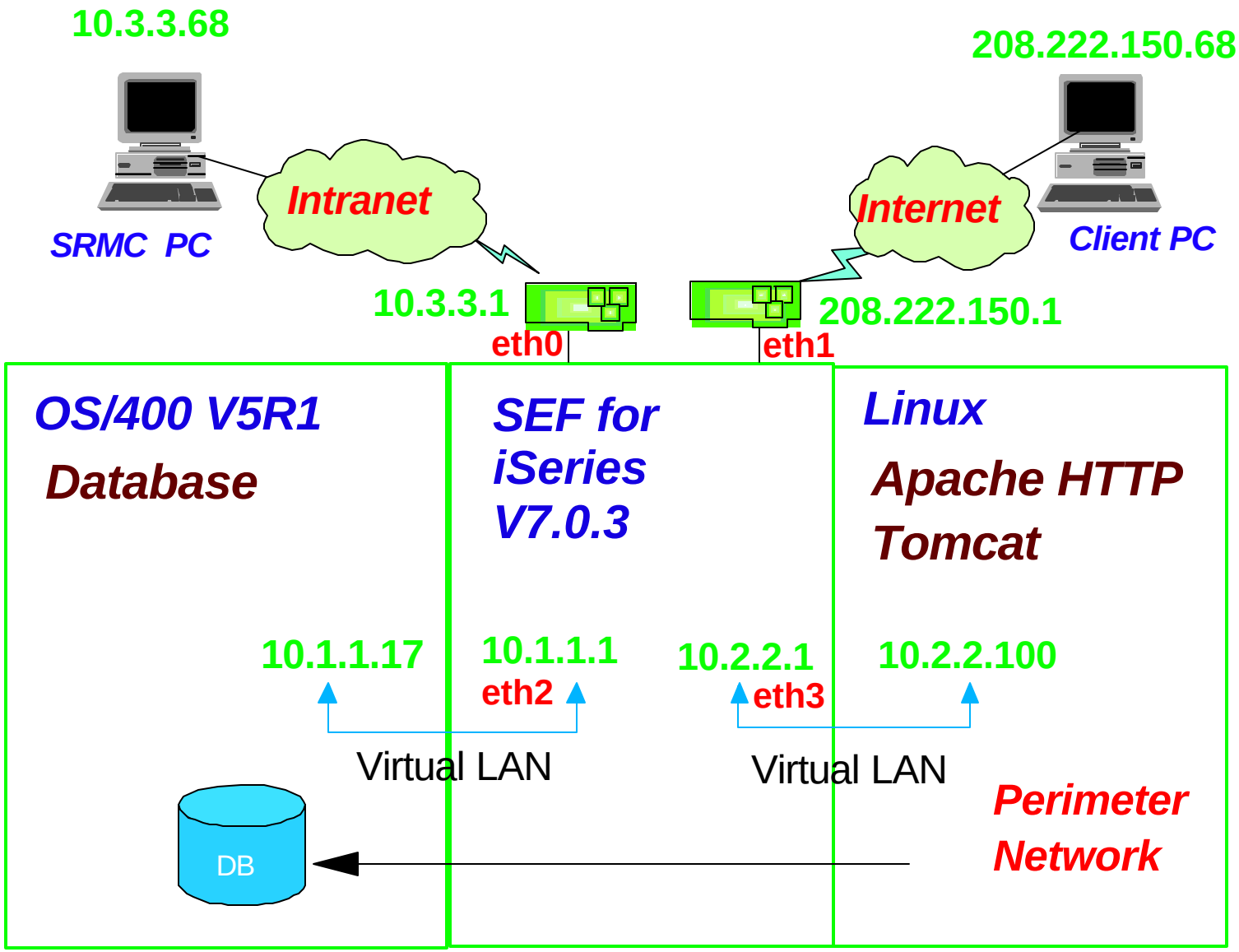
Application proxies for many common services such as:

- FTP
- HTTP
- TELNET
- SMTP
- DNS
- NTP
- NNTP
- Ping
- CIFS
- GSPD
- NBDGRAM
- RTSP
- SQLNet
- H.32

Configure from the SRMC

SEF for iSeries:
Planning and Installation

Configuration Example: Big Picture



System Preparation

System Requirement:

- iSeries 270 one-way or two-way systems
- OS/400 V5R1 installed
- Apply the latest CUM
  - ✓ Confirm the latest Linux related PTFs are applied. All Linux related PTFs can be found at this website:
    - **http://www-912.ibm.com/supporthome.nsf/document/17403848**

System Preparation

System Prerequisites:

- Create a guest partition of LPAR
  - ✓ Assign direct IOA resource(s) as needed
    - ➢ SEF supports 10/100MB iSeries ethernet adapters (2838 and 2849) only
- Create a NWSD object for SEF firewall
  - ✓ IPL source : *STMF
  - ✓ IPL stream file: '/qopt/sef-v703/ppc/iseries/vmlinux'
  - ✓ IPL parameters: ' ks=file:/tmp/ks.cfg'
- Create a NWSSTG object for SEF firewall

NWSD and NWSSTG

Create Network Server Desc (CRTNWSD)

Network server description . . . . :	FIREWALL
Option . . . . . :	*BASIC
Resource name . . . . . :	*NONE
Resource type-model . . . . . :	
Network server type . . . . . :	*GUEST
Online at IPL . . . . . :	*YES
Vary on wait . . . . . :	*NOWAIT
Partition . . . . . :	FIREWALL
Code page . . . . . :	437
Server message queue . . . . . :	*JOBLOG
Library . . . . . :	
Synchronize date and time . . . . :	*NO
IPL source . . . . . :	*STMF
IPL stream file . . . . . :	'/qopt/sef-v703/ppc/iseries/vmlinux'
IPL parameters . . . . . :	'ks=file:/tmp/ks.cfg'
Text . . . . . :	*BLANK

NWSD and NWSSTG

Create NWS Storage Space (CRTNWSSTG)

Network server storage space . . :	FIREWALL
Network server description . . . :	FIREWALL
Drive . . . . . :	1
Size in megabytes . . . . . :	10000
Format . . . . . :	*OPEN
Format complete . . . . . :	No
Auxiliary storage pool . . . . . :	1
Text . . . . . :	Storage space for SEF firewall

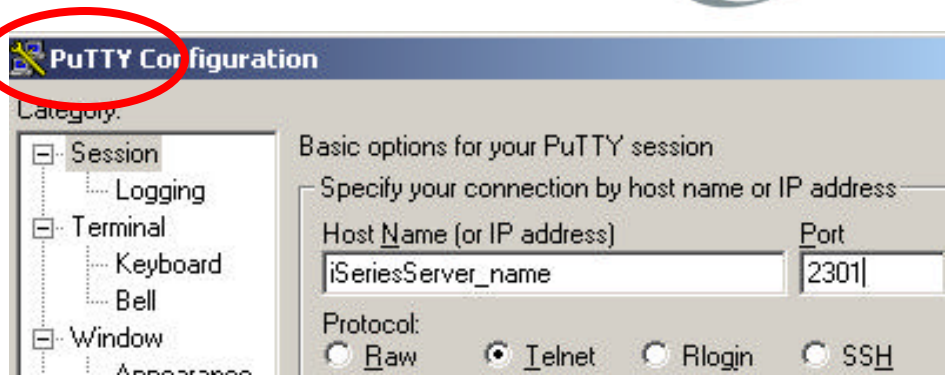
Install SEF for iSeries

Place CD in CD-ROM

1. Place SEF installation CD in the CD-ROM device of iSeries

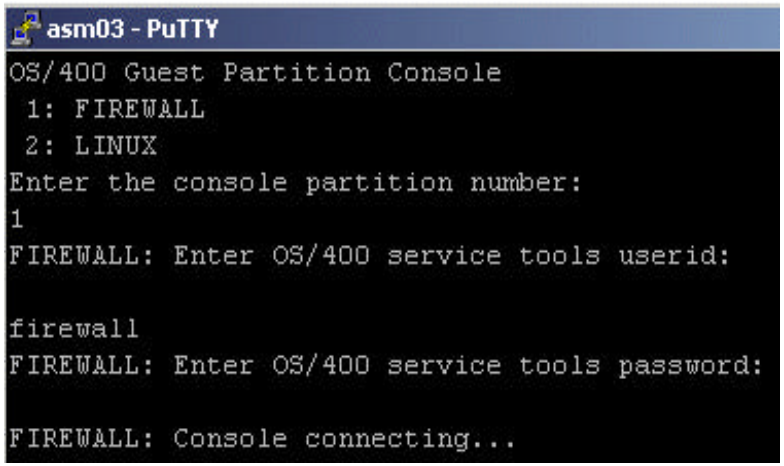
Start Telnet session

2. Start Telnet session from a PC to port 2301 of any iSeries interface.
   - 2a. Select Firewall partition
   - 2b. Type DST userID and press Enter
   - 2c. Type DST password and press Press Enter



Vary on NWSD

3. Vary on the NWSD object from a green screen
   - 3a. Type WRKCFGSTS *NWS command
   - 3b. Take Opt1 (Vary on)



SEF install and setup wizard

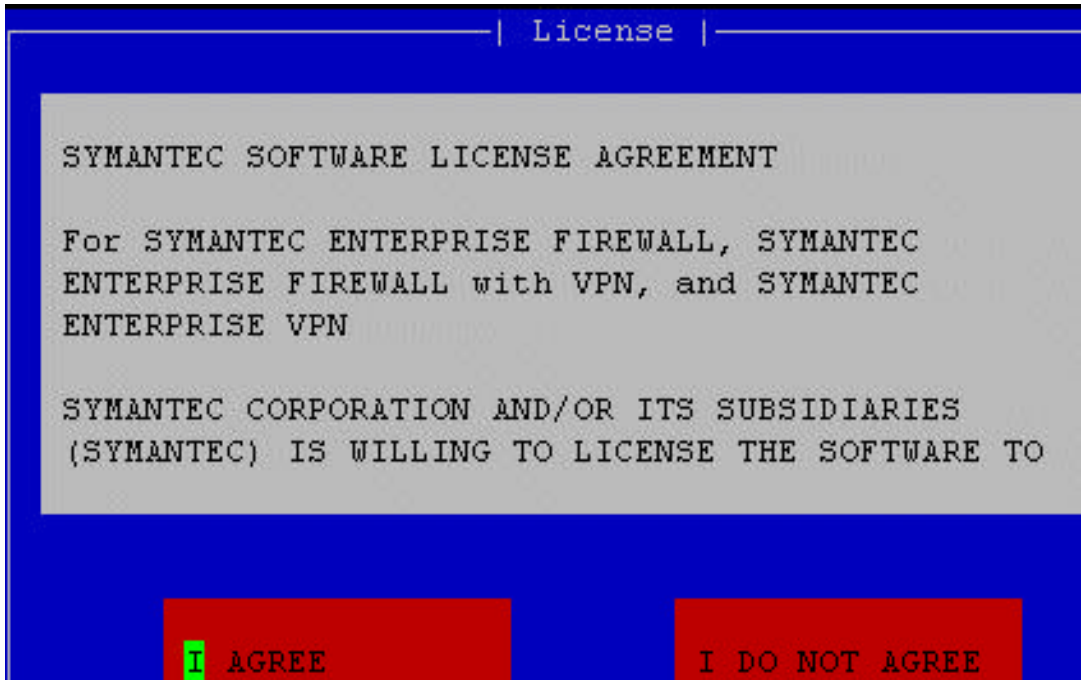
4. Setup wizard starts now. Follow the instructions.
   - Configure network interface: IPaddress / Subnet mask
   - Define the IP address and password for an SRMC client
   - Reboot

Change NWSD

5.Change NWSD
   - 5a. Vary off the NWSD using Option 2 (Vary off) from WRKCFGSTS *NWS
   - 5b. Change NWSD parameter as follows:
     - IPL source: *NWSSTG / IPL stream file: *NONE / IPL parameters: *NONE

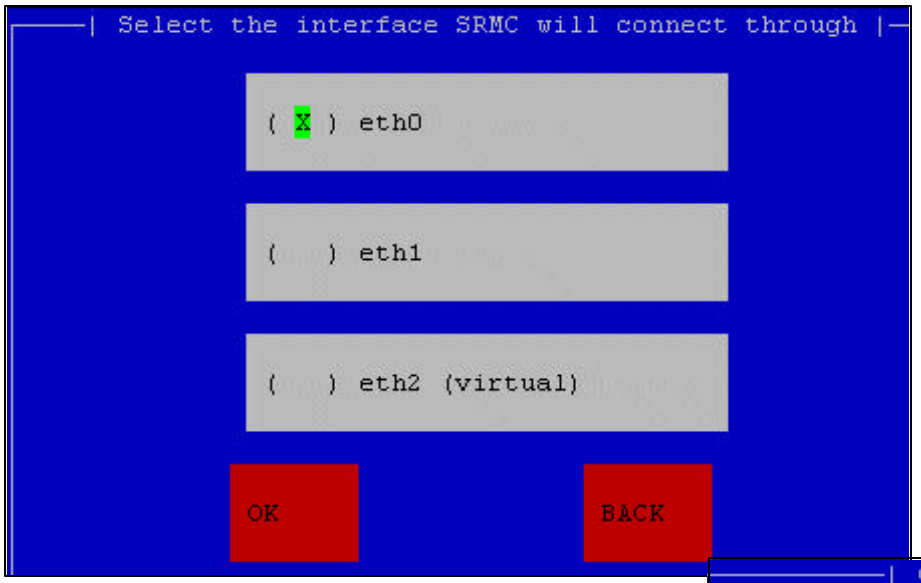
Step 1: Symantec SW License Agreement

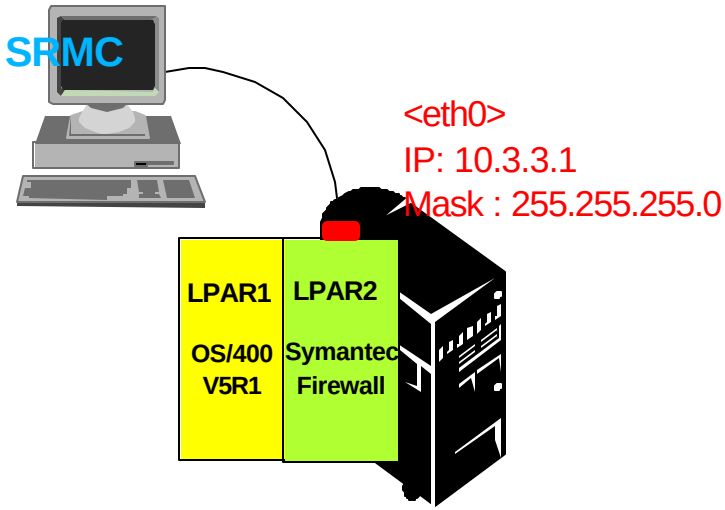
Varying on Firewall NWSD (Step 3 on previous chart) will automatically take you to this screen.



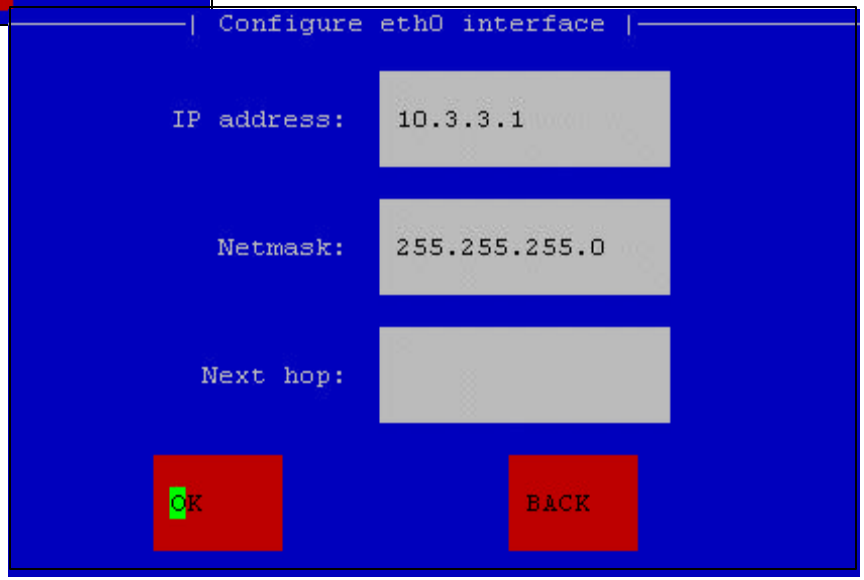
Read the license and choose your option. If you select I Agree, installation proceeds.

Step 2: Config Firewall Network Interface



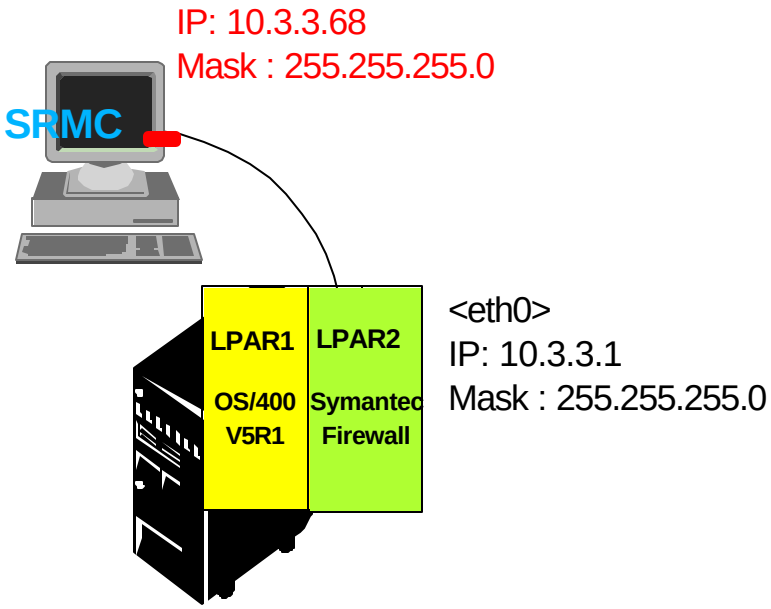


2a. Choose the interface the SRMC connects to.



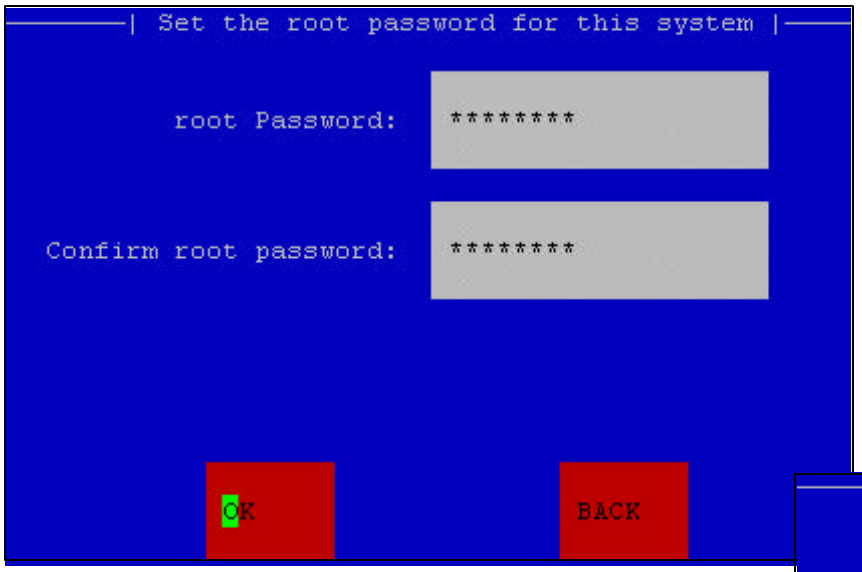
2b. Enter IP address and subnet mask of that interface.

Step 3: Config SRMC Network Interface

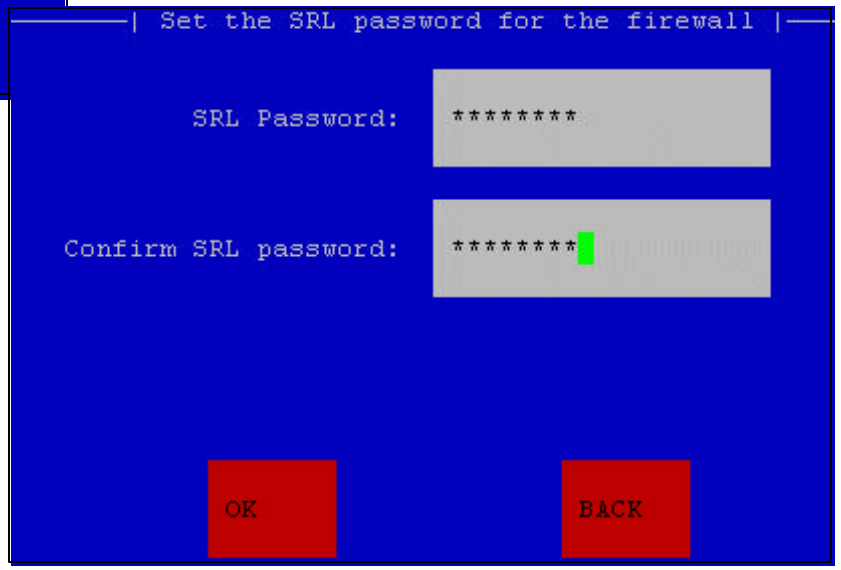


Enter IP address and password of the SRMC client.

Step 4: Set Password

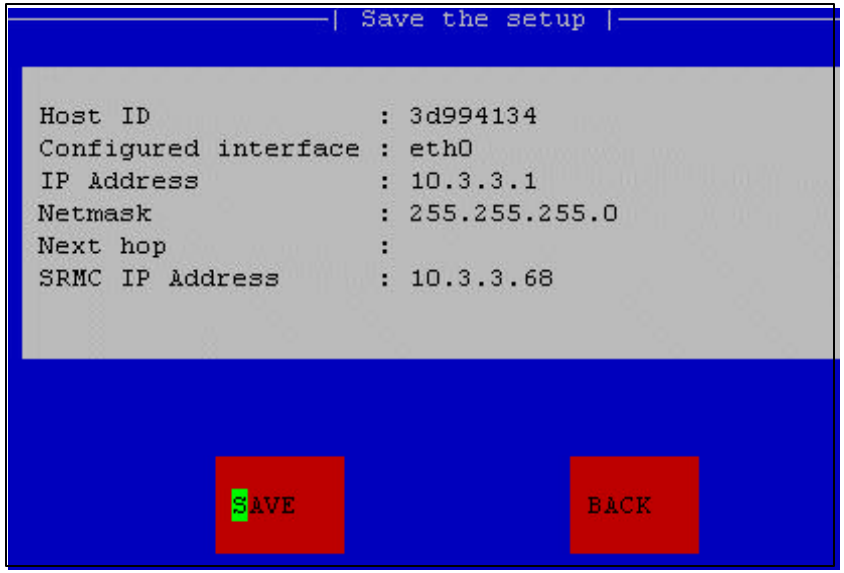


4a.Set the root password for Linux (RedHat).



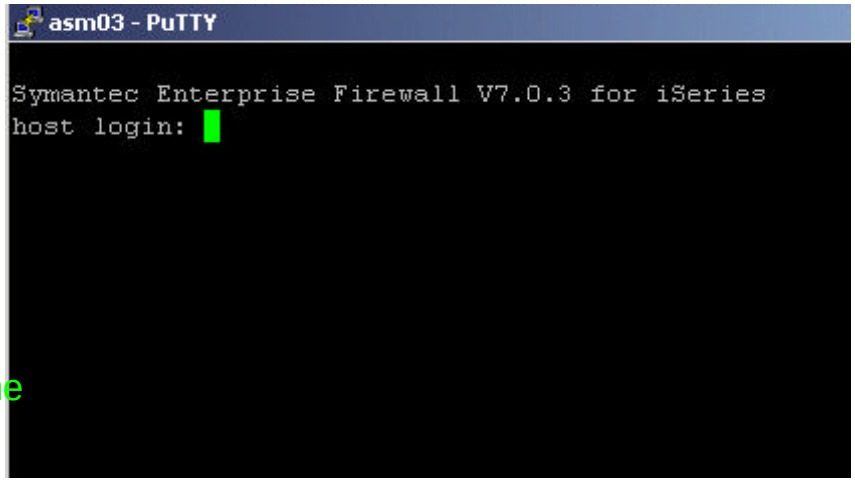
4b.Set the SRL password.

Step 5: Save Configuration



5a.Confirm setup information, and save it.

5b. The login screen appears after rebooting.



You should not login!

- You should connect the SRMC to move on to next step, which is configuring the firewall.

Post-Installation Step

Change the NWSD object from the green screen

- Change the NWSD to boot from disk (NWSSTG) rather than CD-ROM after the installation
- Steps:
  - ✓ Vary off the NWSD
  - ✓ Change the NWSD
    - IPL source : *NWSSTG
    - IPL steam file : *NONE
    - IPL parameters : *NONE
  - ✓ Vary on the NWSD

Change Network Server Desc (CHGNWSD)

Network server description . . . . :	FIREWALL
Option . . . . . :	*BASIC
Resource name . . . . . :	*NONE
Resource type-model . . . . . :	
Network server type . . . . . :	*GUEST
Online at IPL . . . . . :	*YES
Vary on wait . . . . . :	*NOWAIT
Partition . . . . . :	FIREWALL
Code page . . . . . :	437
Server message queue . . . . . :	*JOBLOG
Library . . . . . :	
Synchronize date and time . . . . :	*NO
IPL source . . . . . :	*NWSSTG
IPL stream file . . . . . :	*NONE
IPL parameters . . . . . :	*NONE
Text . . . . . :	*BLANK

SRMC:
Installation and Configuration

SRMC Setup

Requirement:

- Windows2000/NT with the latest Service Packs
- Static IP address for a SRMC console

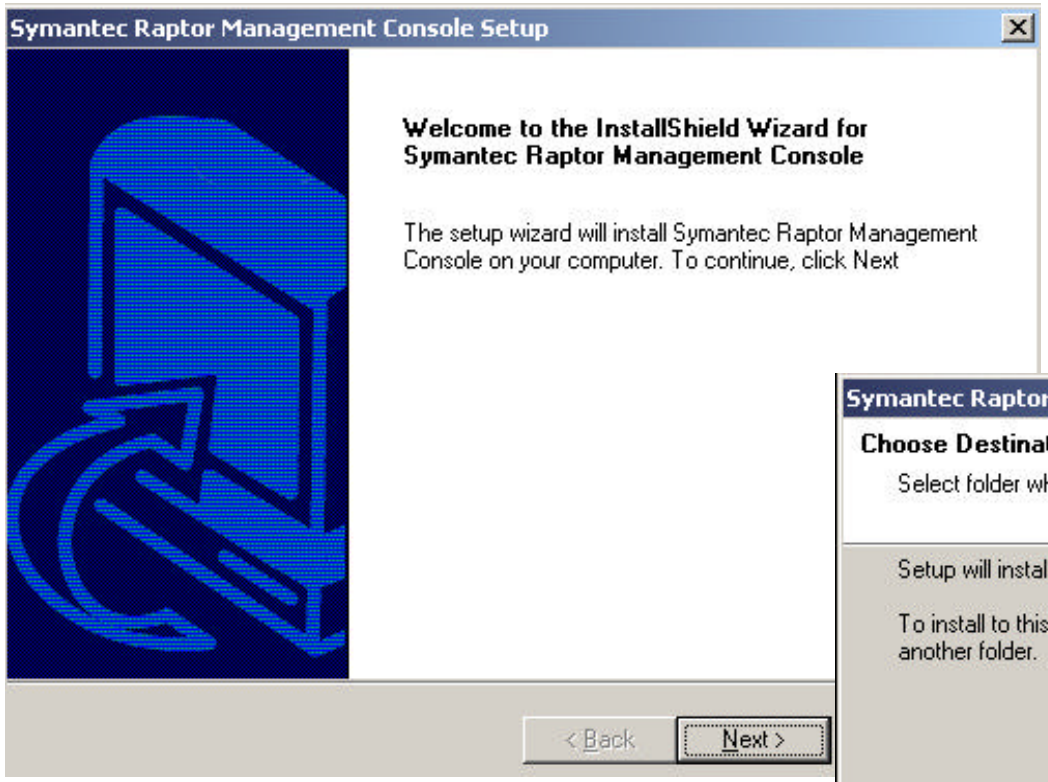
Installation

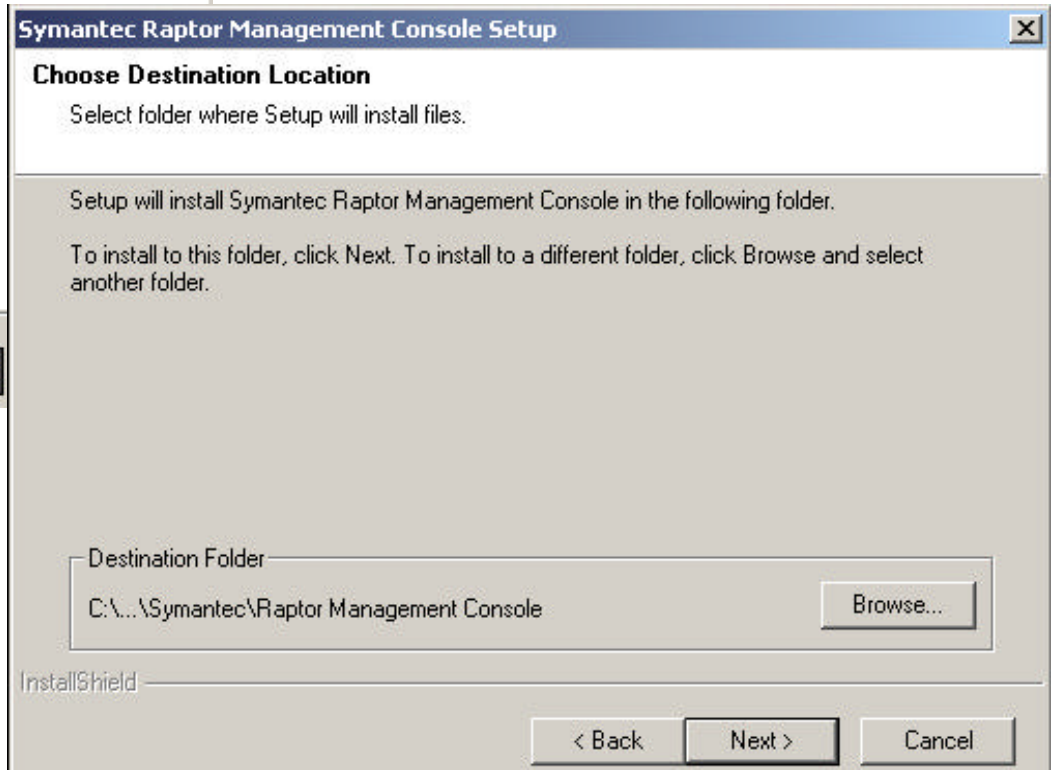
- Start the installation wizard by double clicking <ClientSoftware\SymantecRMC\Setup.exe> on the SEF installation CD
- Follow the installation wizard
- Start the SRMC by double clicking the icon on the desktop

★ To uninstall the SRMC, do the following:
- Start -> Programs -> Symantec Raptor Management Console -> Uninstall Raptor Management Console

or
- Start -> Settings -> Control Panel -> Add/Remove Programs

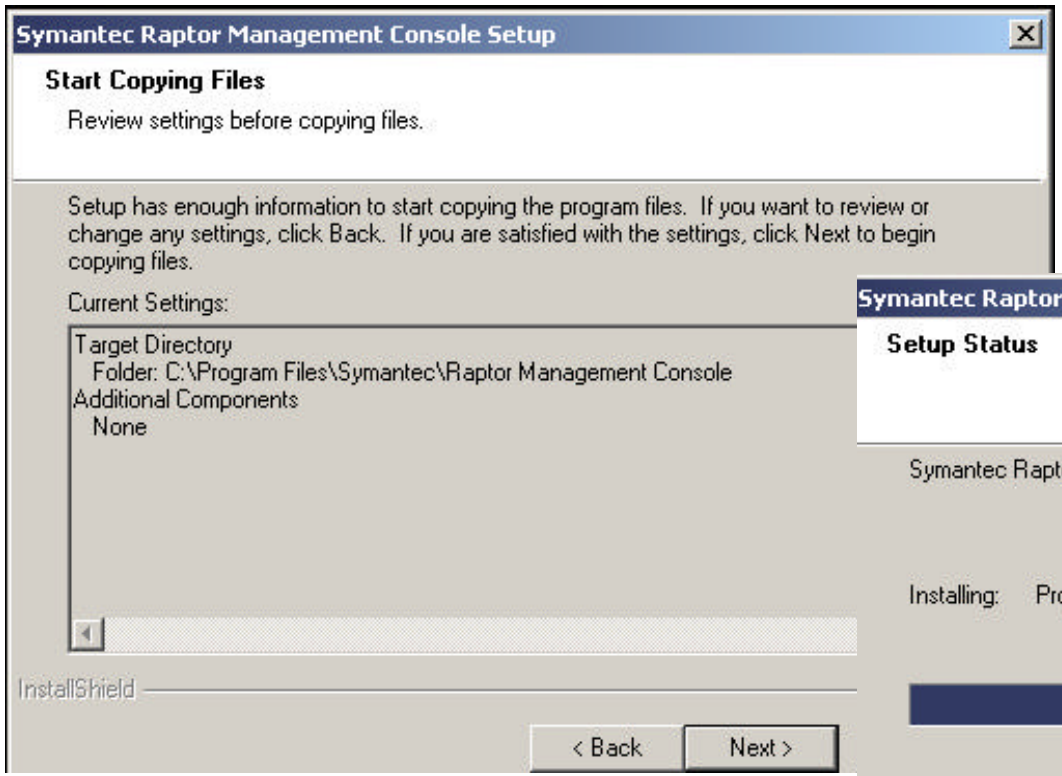
Installing SRMC on PC

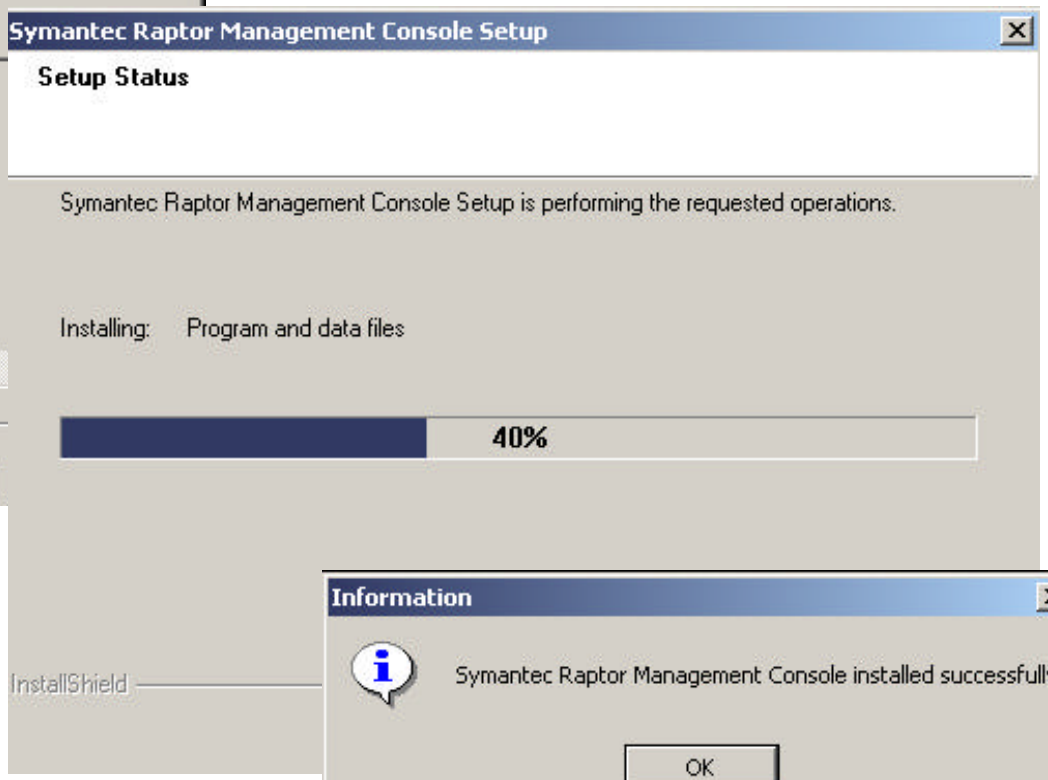




Select the folder for the SRMC installation.

Installing SRMC on PC (cont.)





When the installation ends successfully, the icon appears on your desktop. You can start the SRMC by double clicking this icon.

Basic Setup of the Firewall

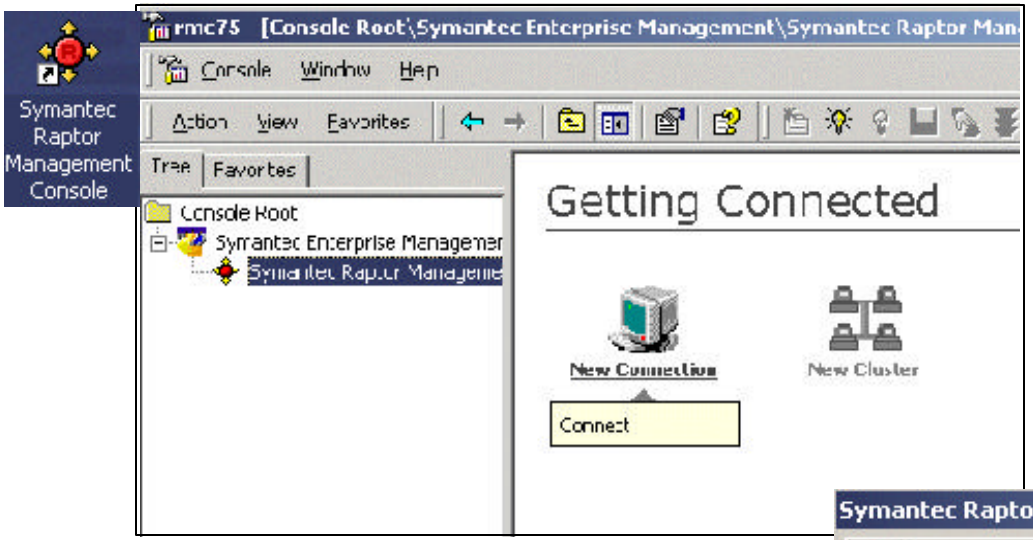
Connect the SRMC to the Firewall

- Already configured while installing SEF:
  - ✓ Firewall network interface (10.3.3.1)
  - ✓ SRMC network interface (10.3.3.68) and password
- Sign on to the Firewall
  - ✓ Use the SRMC password configured during installation

Launch the SEF Basic Setup Wizard

- Set the firewall name and domain name
- Configure all network interfaces
- Set the system time and date

Create Connection to Firewall



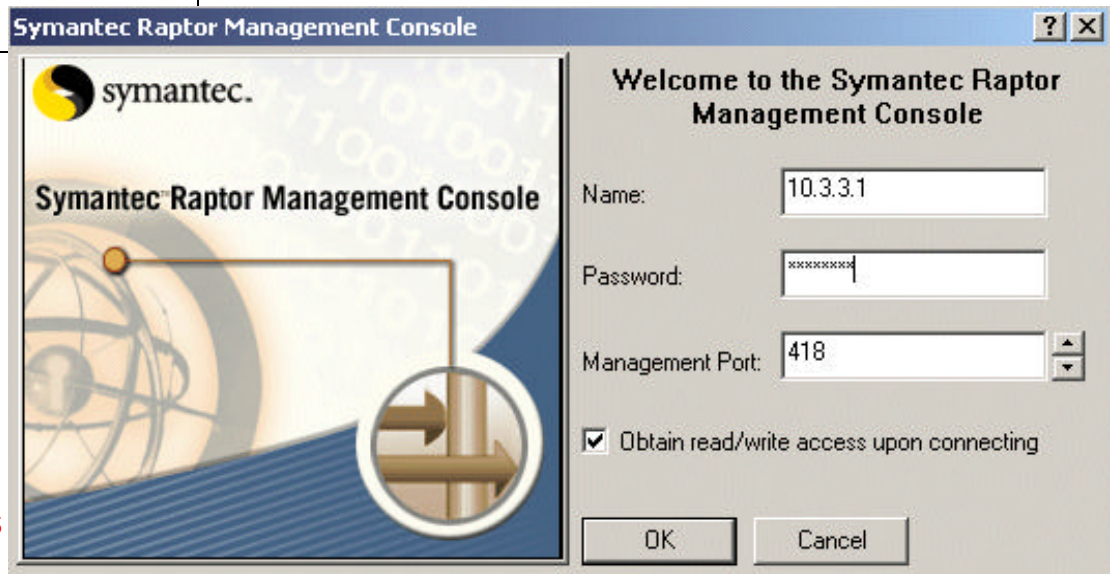
1. Start the SRMC by double clicking the icon on the desktop or select:

   Start =>Programs

   => Symantec Raptor Management Console

   => Raptor Management Console

2. Click New Connection.



3. Sign on to the firewall.

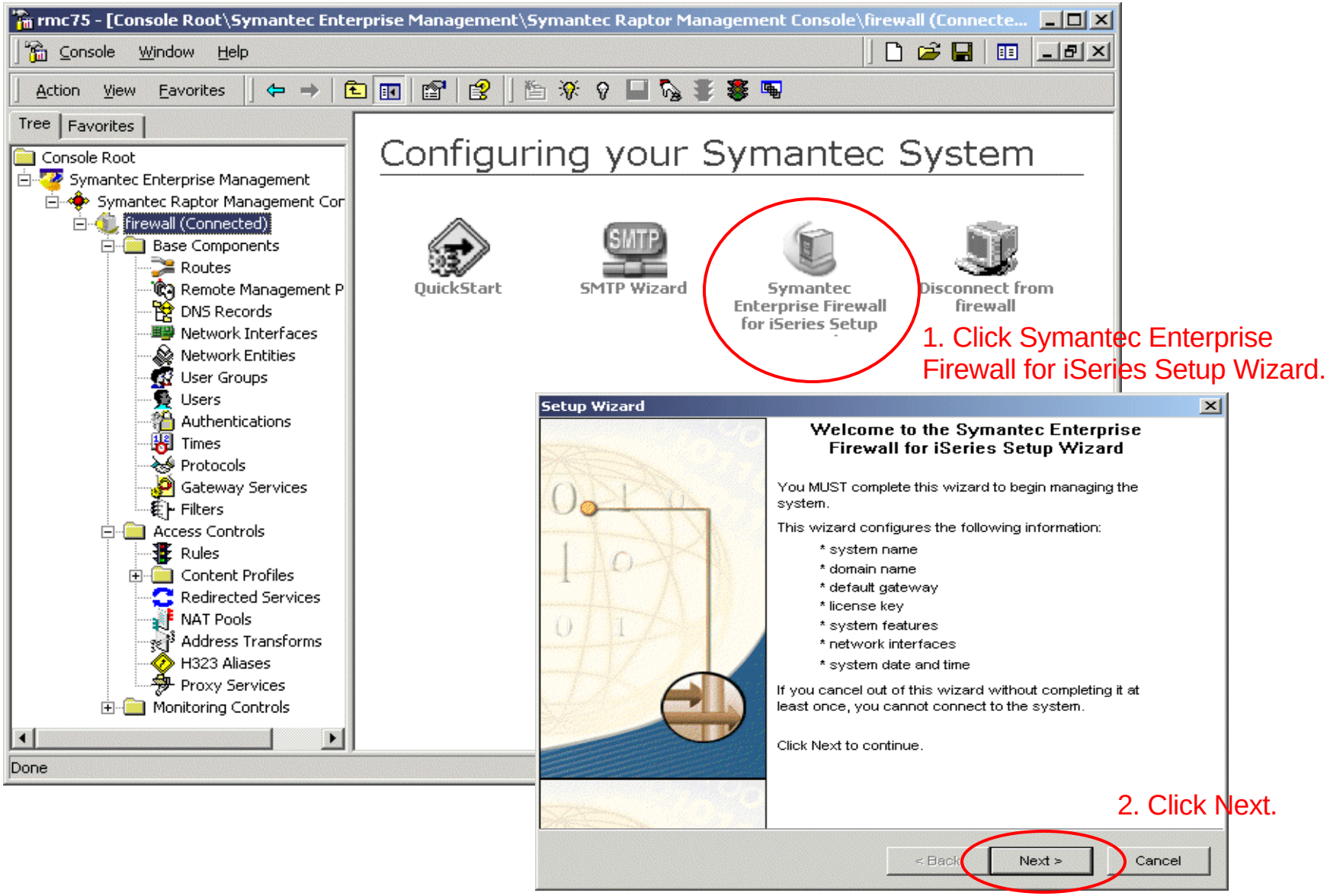
Name: name or IP address of the firewall

Password: Which you already set at the installation (SRMC password)

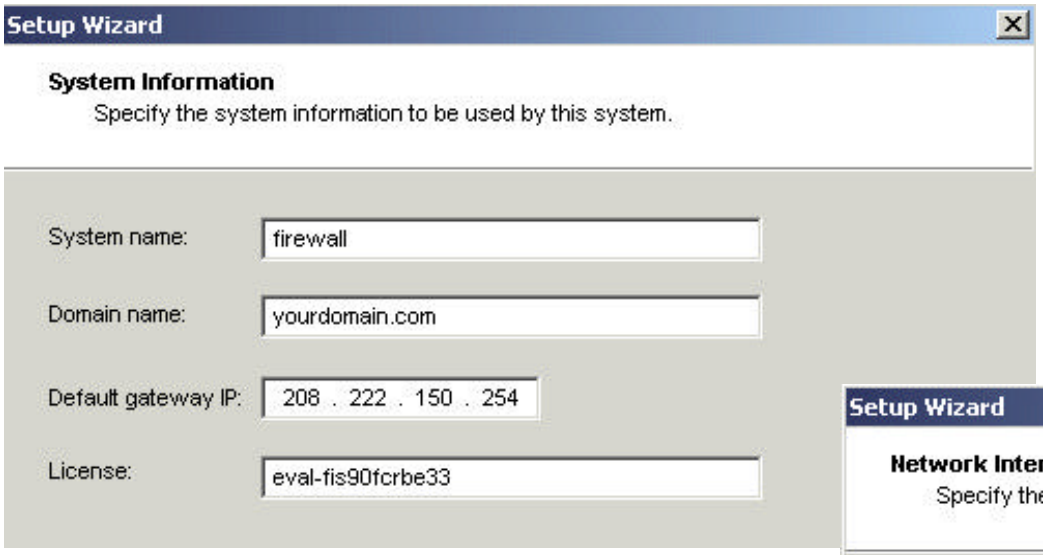
Port: 418

Check the box for Obtain read/write access upon connecting.

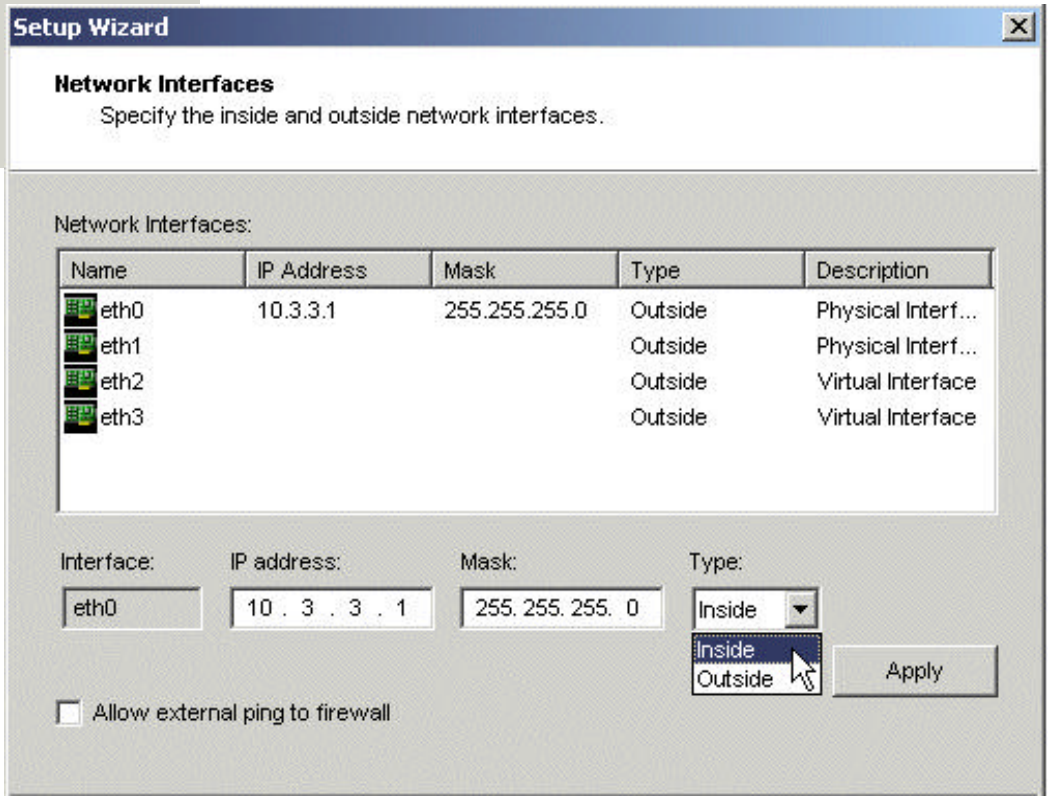
Launch SEF Basic Setup Wizard



SEF Basic Setup Wizard

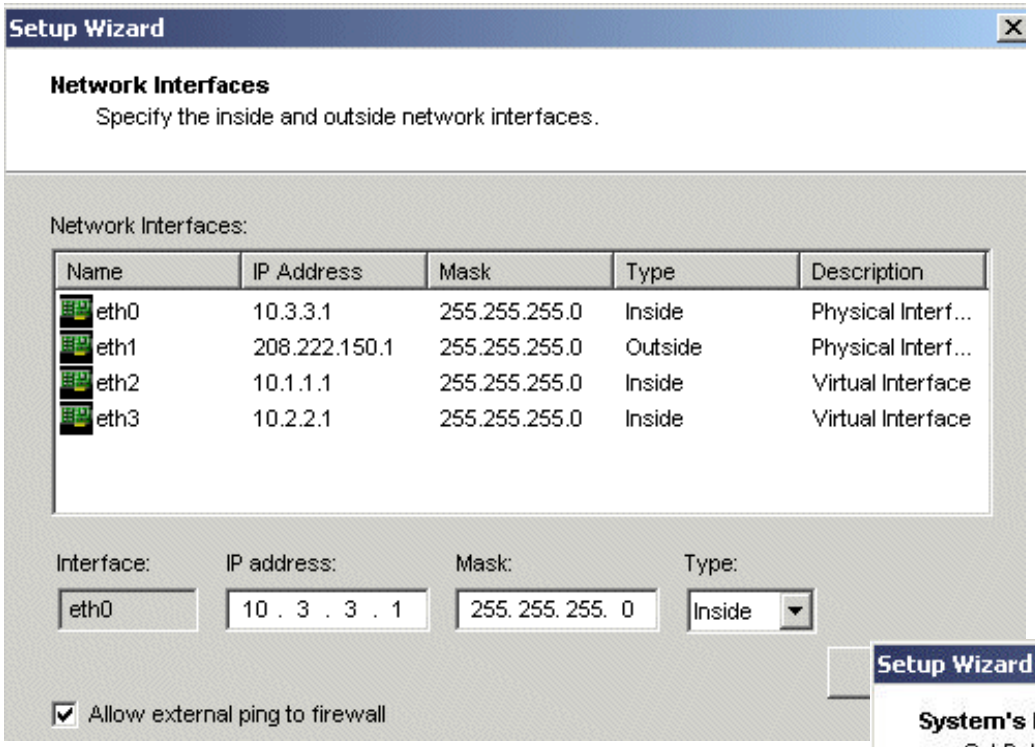


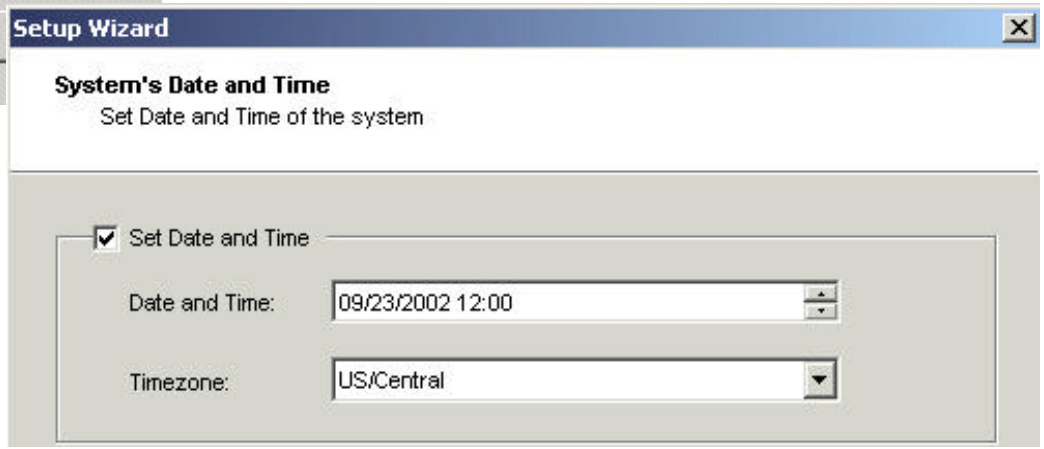
3. Type the system information.



4. Configure Network Interfaces.

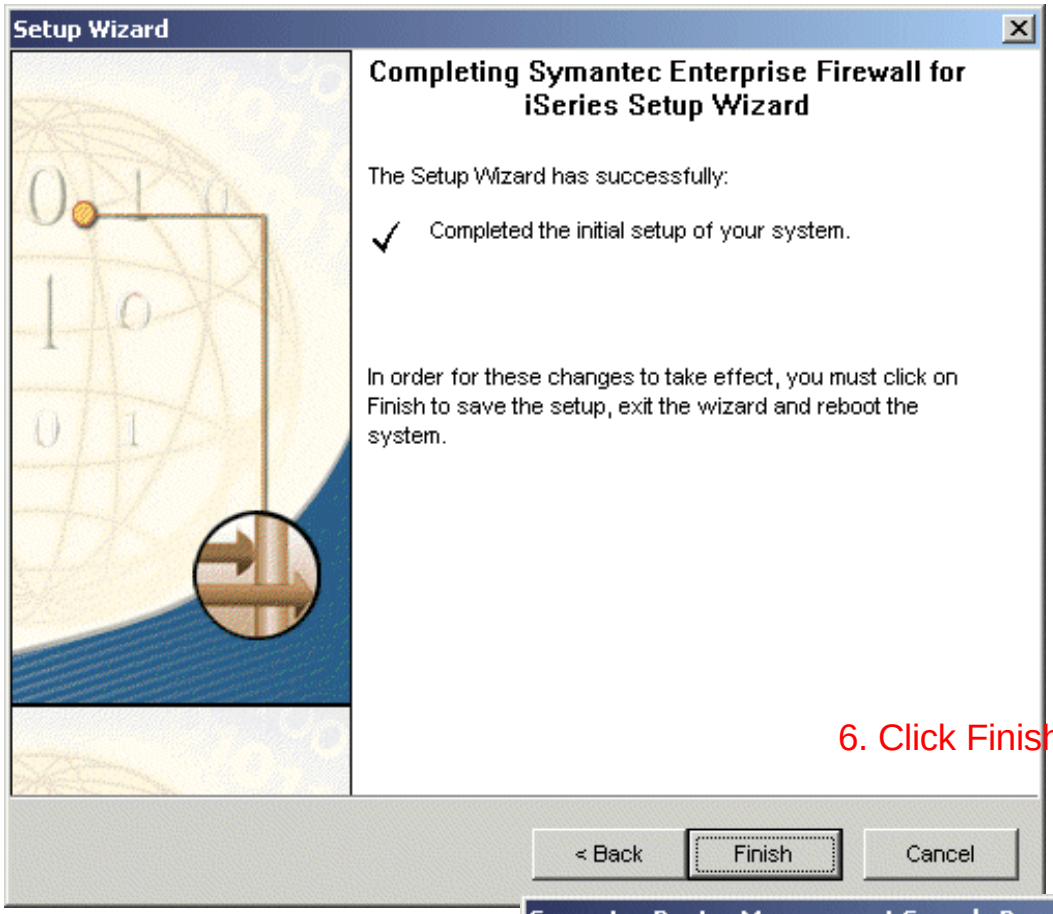
SEF Basic Setup Wizard





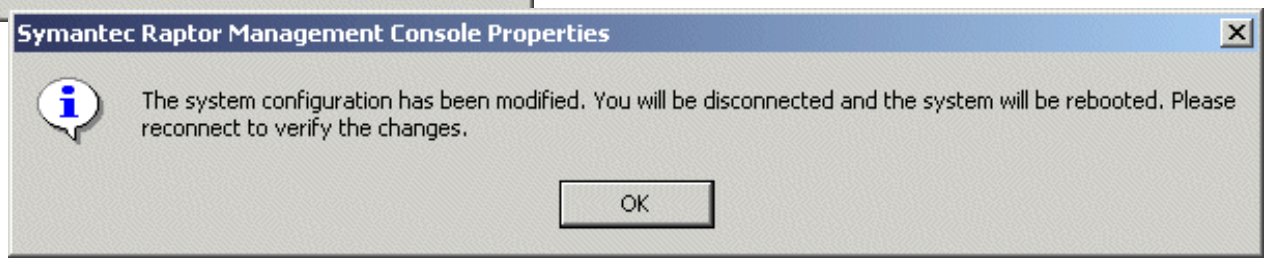
5. Set system's date and time

SEF Basic Setup Wizard

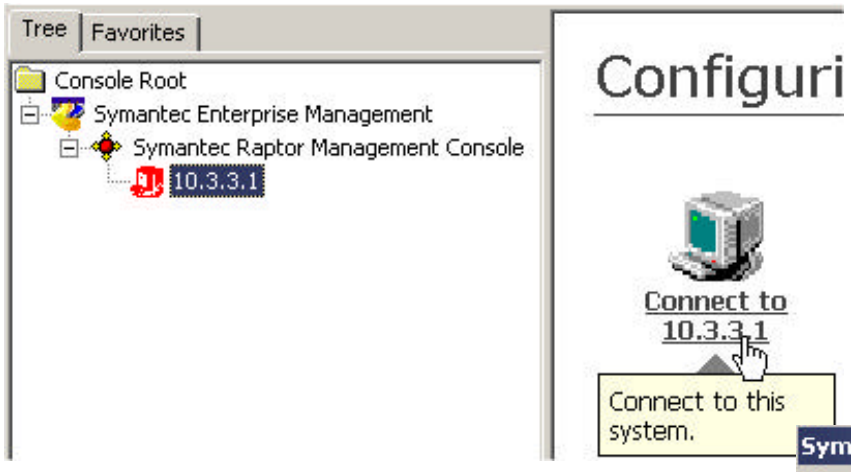


6. Click Finish.

7. The SEF reboots automatically.

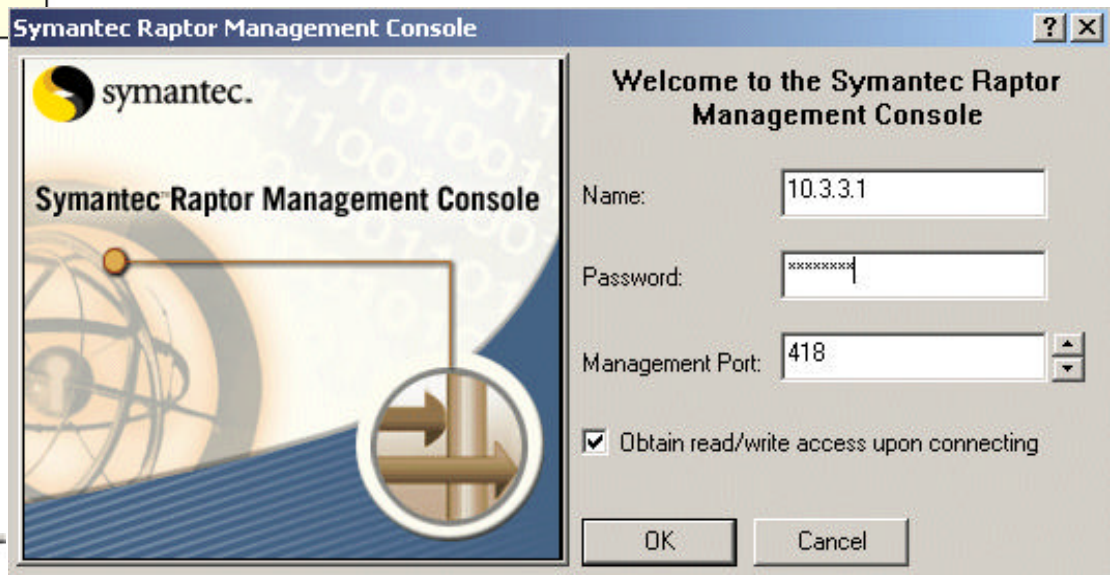


Connect to SEF



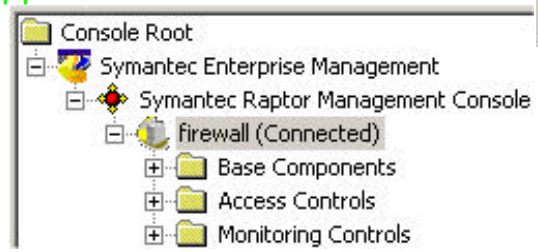
The Connection appears.

1. Click the created connection.



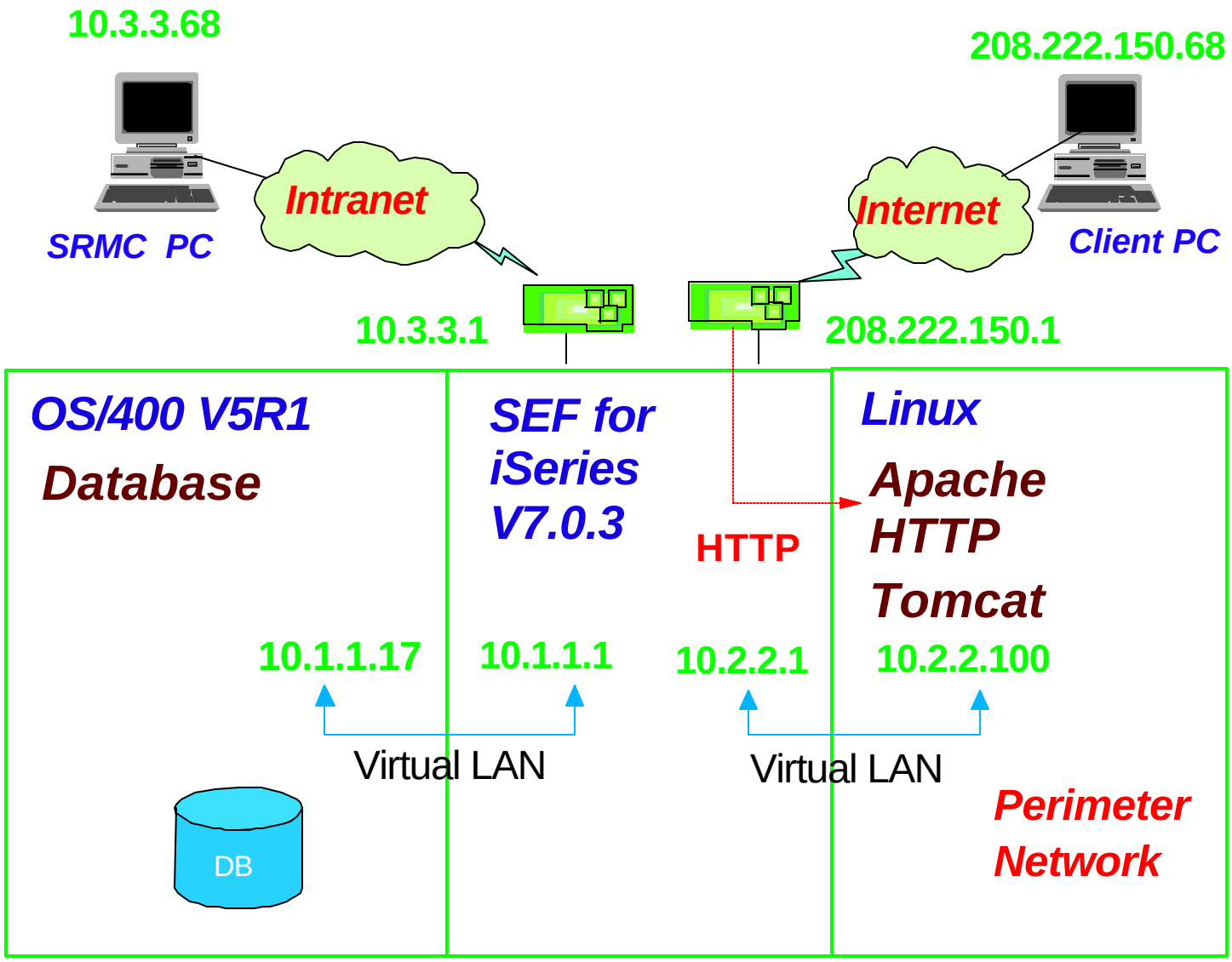
2. Enter the following :
   - SEF system name or IP address
   - The password defined in SEF installation
   - Port number : 418

3. The SEF system accepts the connection, the folders appear on the SRMC screen.

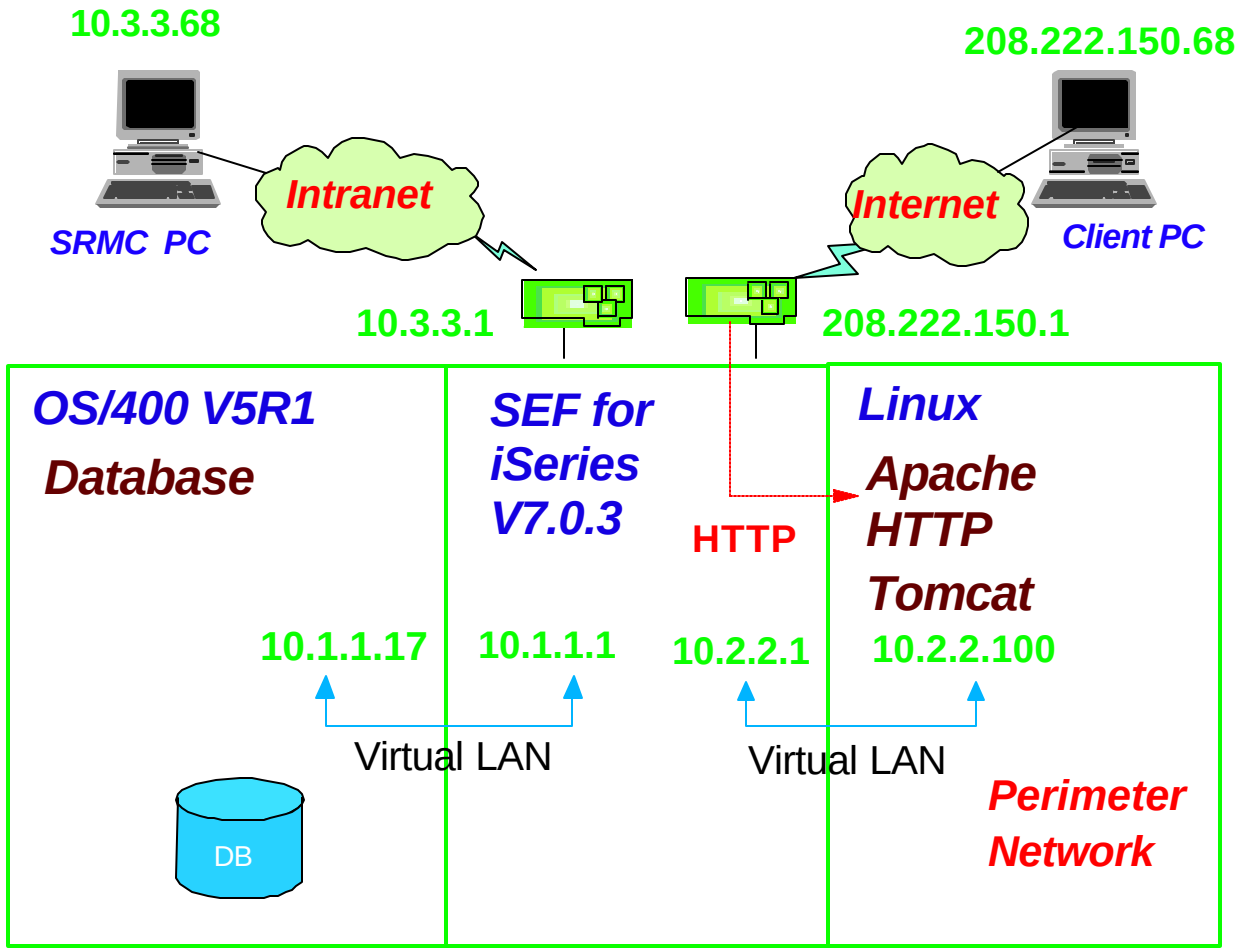


SEF for iSeries:
Configuration Examples

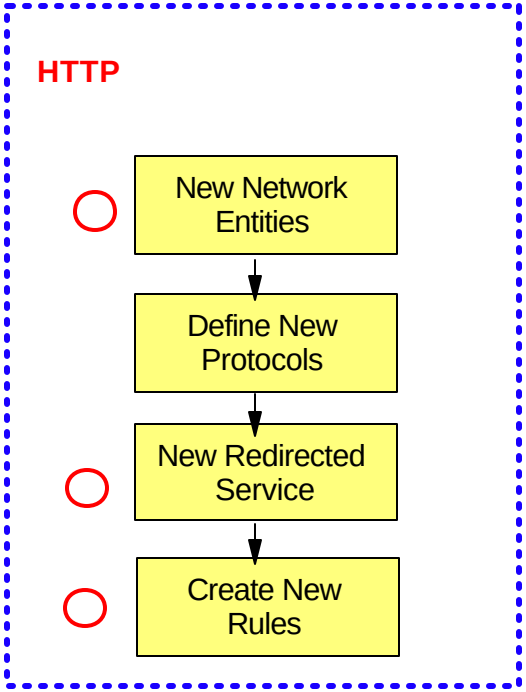
Configuration Example 1: HTTP



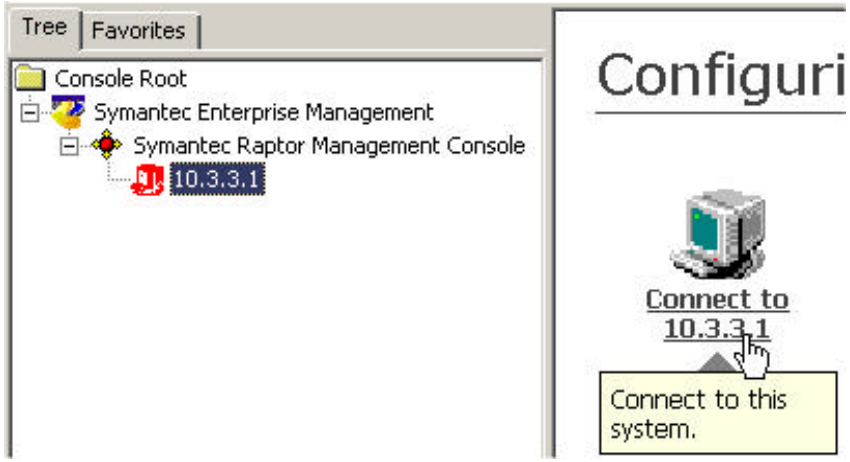
Configuration Example 1: HTTP

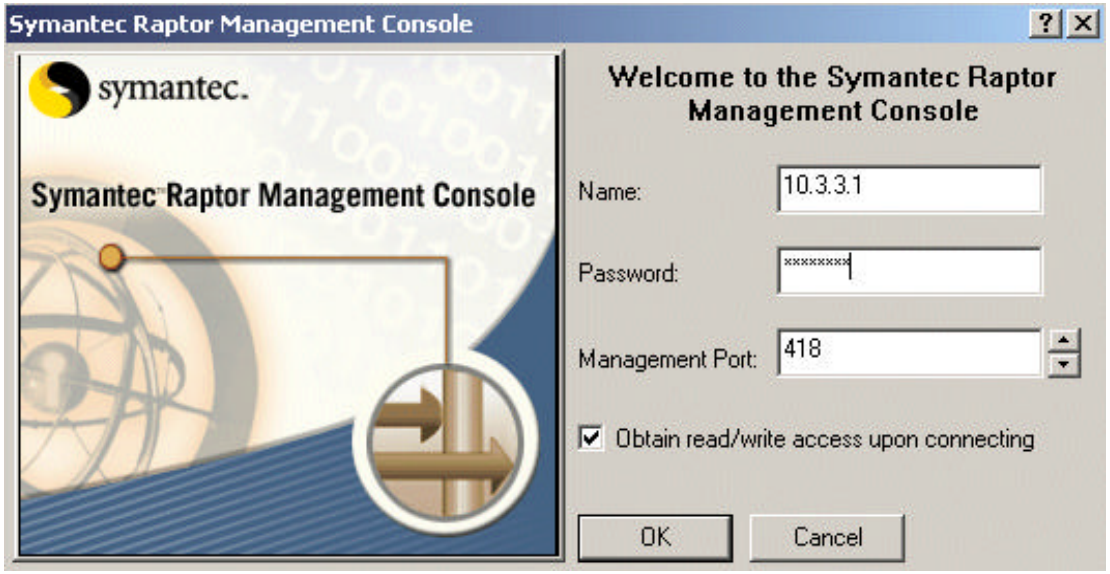


Steps:

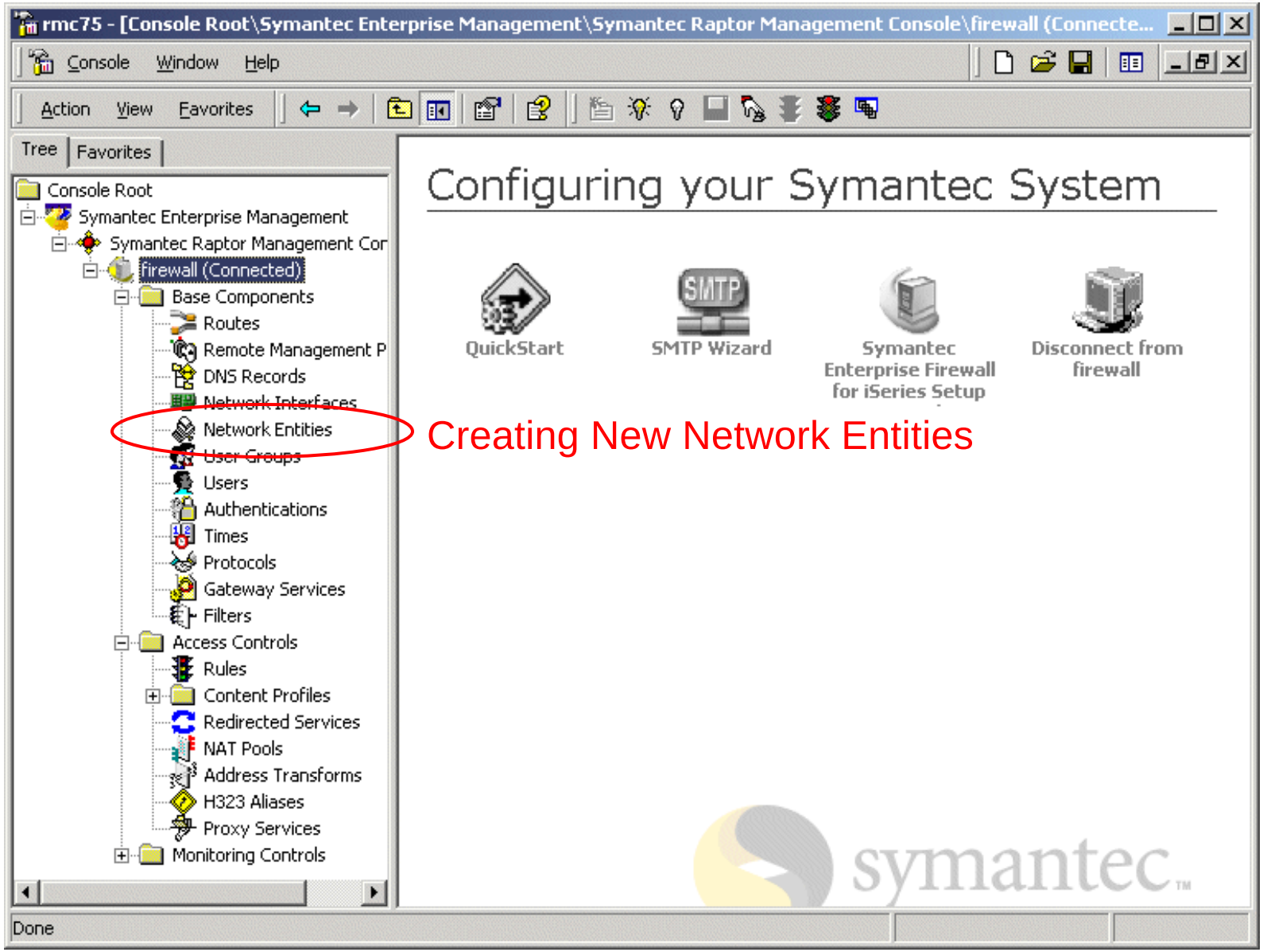


First, Starting SRMC





Starting SRMC...continued

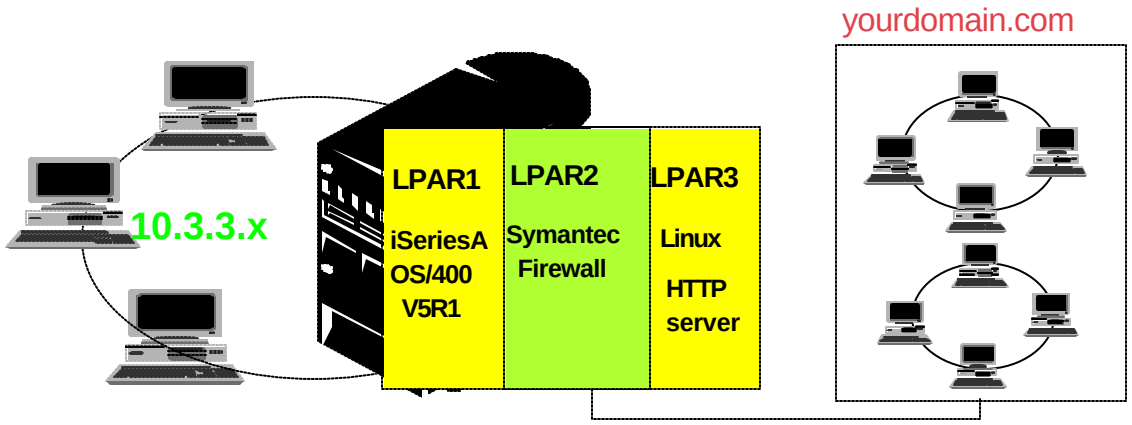


Step 1: Creating New Network Entity

Network Entities

- Objects used when configuring rules
- Defines the computers that pass data through the SEF system

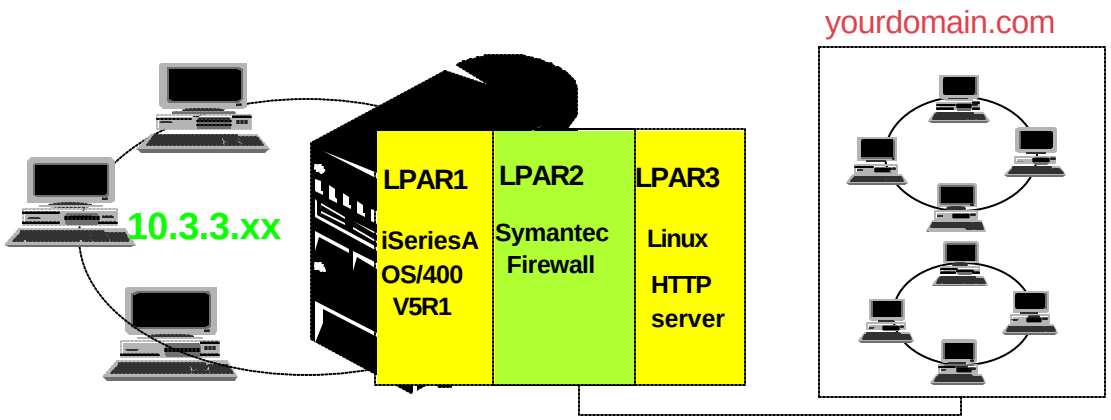
Type	*Explanation*	*Definition*
Host	A single computer	IP address; MAC address
Subnet	All computers in the same subnet address	address; subnet mask
Domain	A group of computers sharing the same domain	domain name
Group	A group you choose from hosts, subnets, domains	hosts, subnets, domains



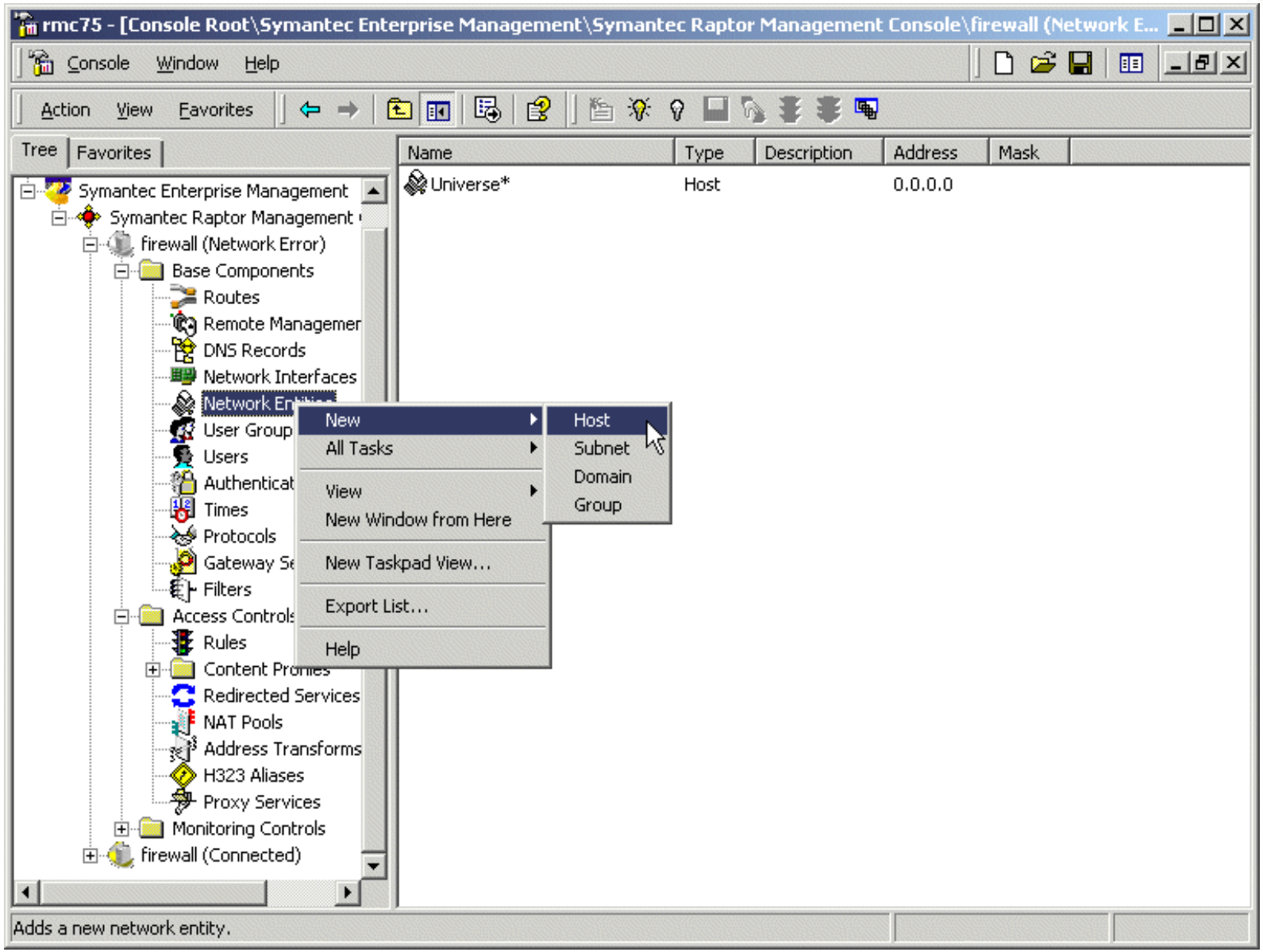
Step 1: Creating New Network Entity

Needed Network Entities for Configuration Example 1

- Host Entity: for Linux partition

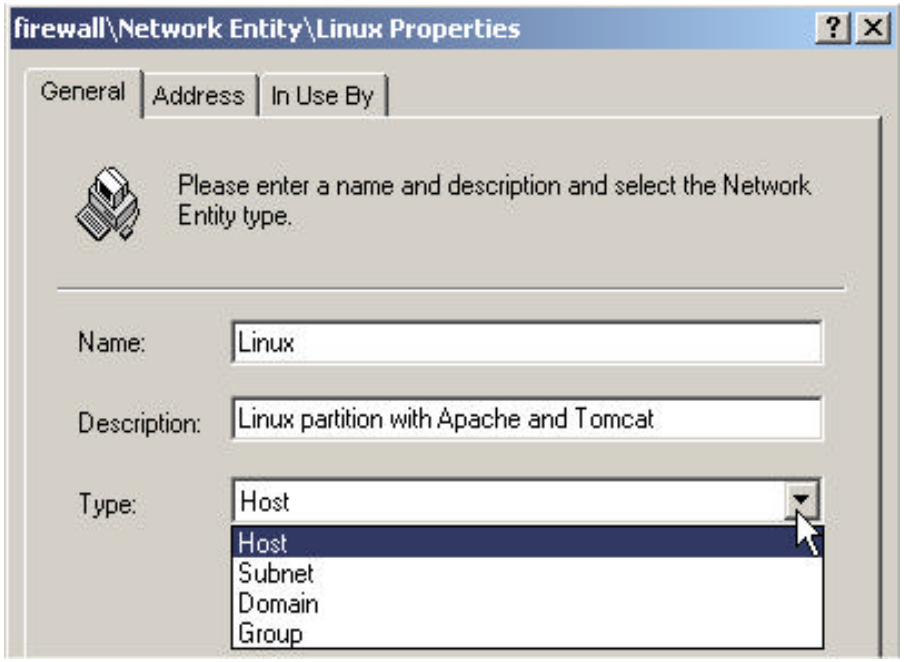


Step 1: Creating New Network Entity



Step 1: Creating New Network Entity

Creating Host type Network Entity for Linux partition

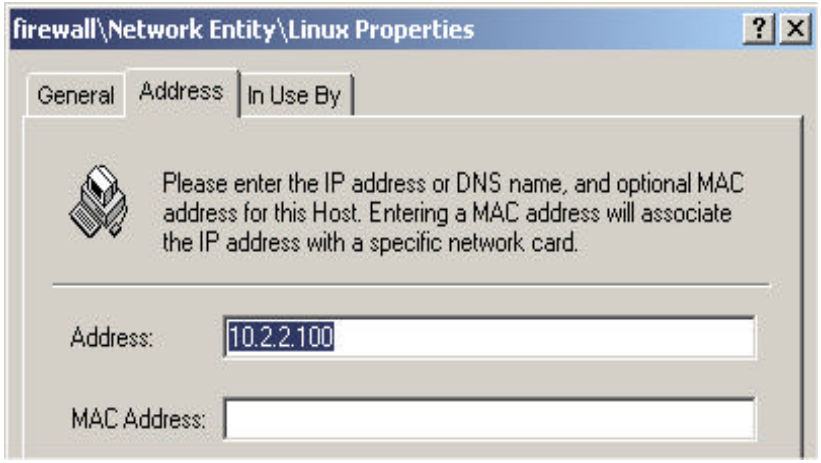


On General tab:

1a. Enter name (entity name)
1b. Select type: Host

Step 1: Creating New Network Entity

Creating Host type Network Entity for Linux partition



On Address tab:

1c. Enter IP address of Linux partition: 10.2.2.100

Step 2: Defining New Protocol

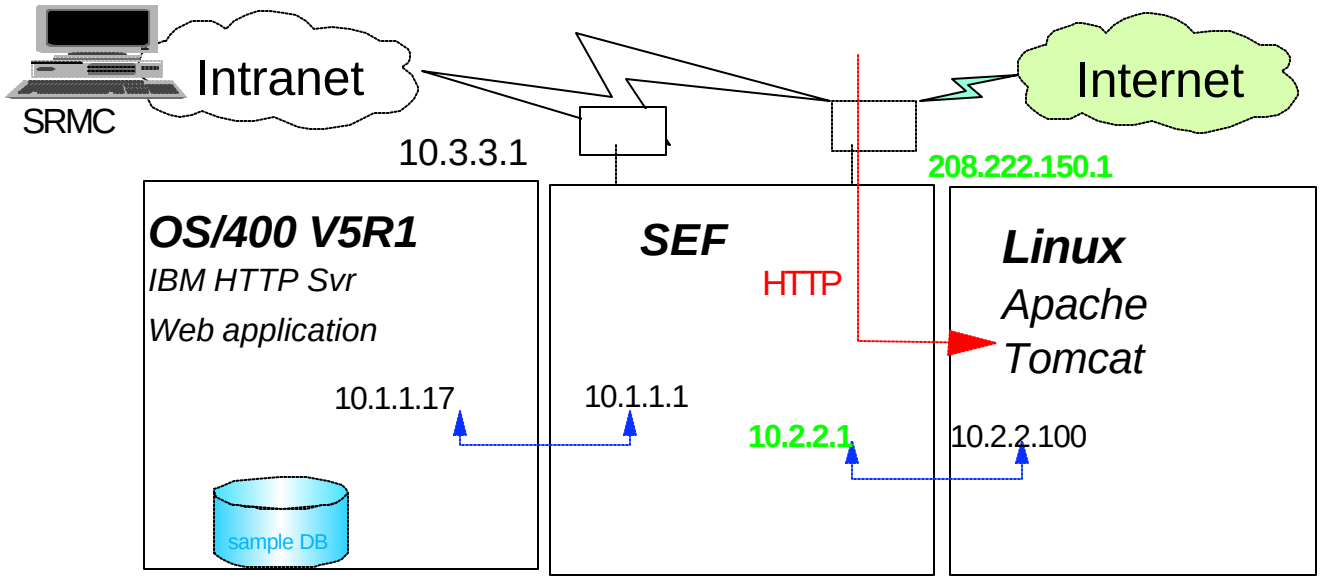
SEF for iSeries provides predefined protocol for HTTP

- You don't need to create new protocol.

Step 3: Creating Redirected Service

Redirected services

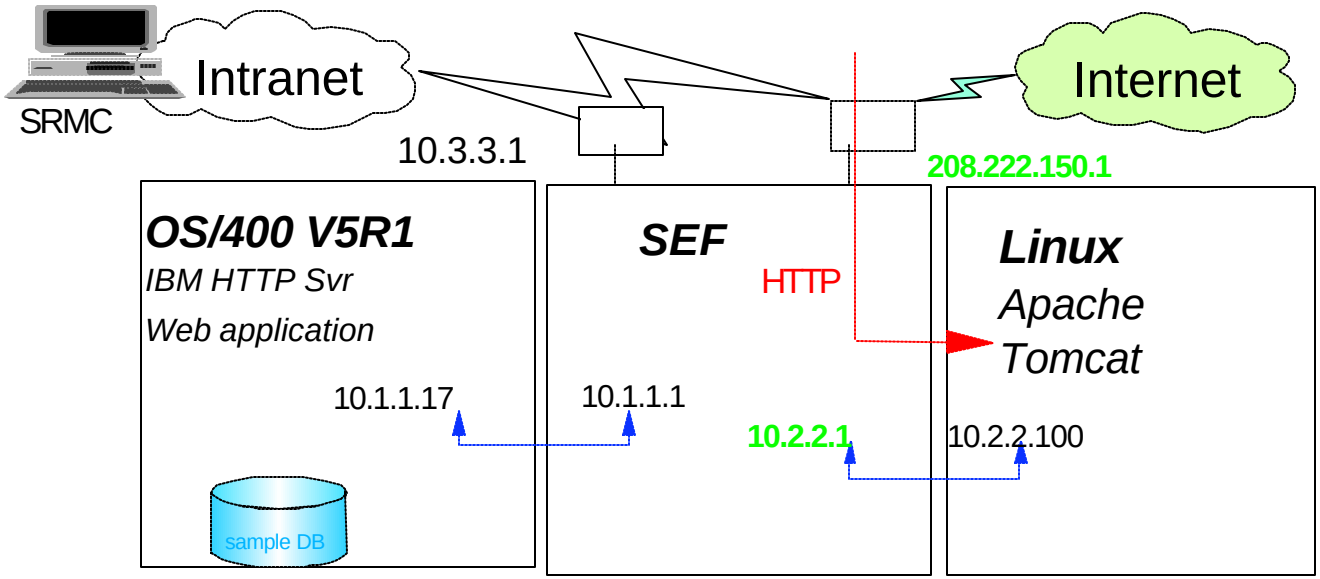
- Redirect traffic from one IP address and port to another IP address and port
- Allow a server to be publicly accessible while having a private IP address



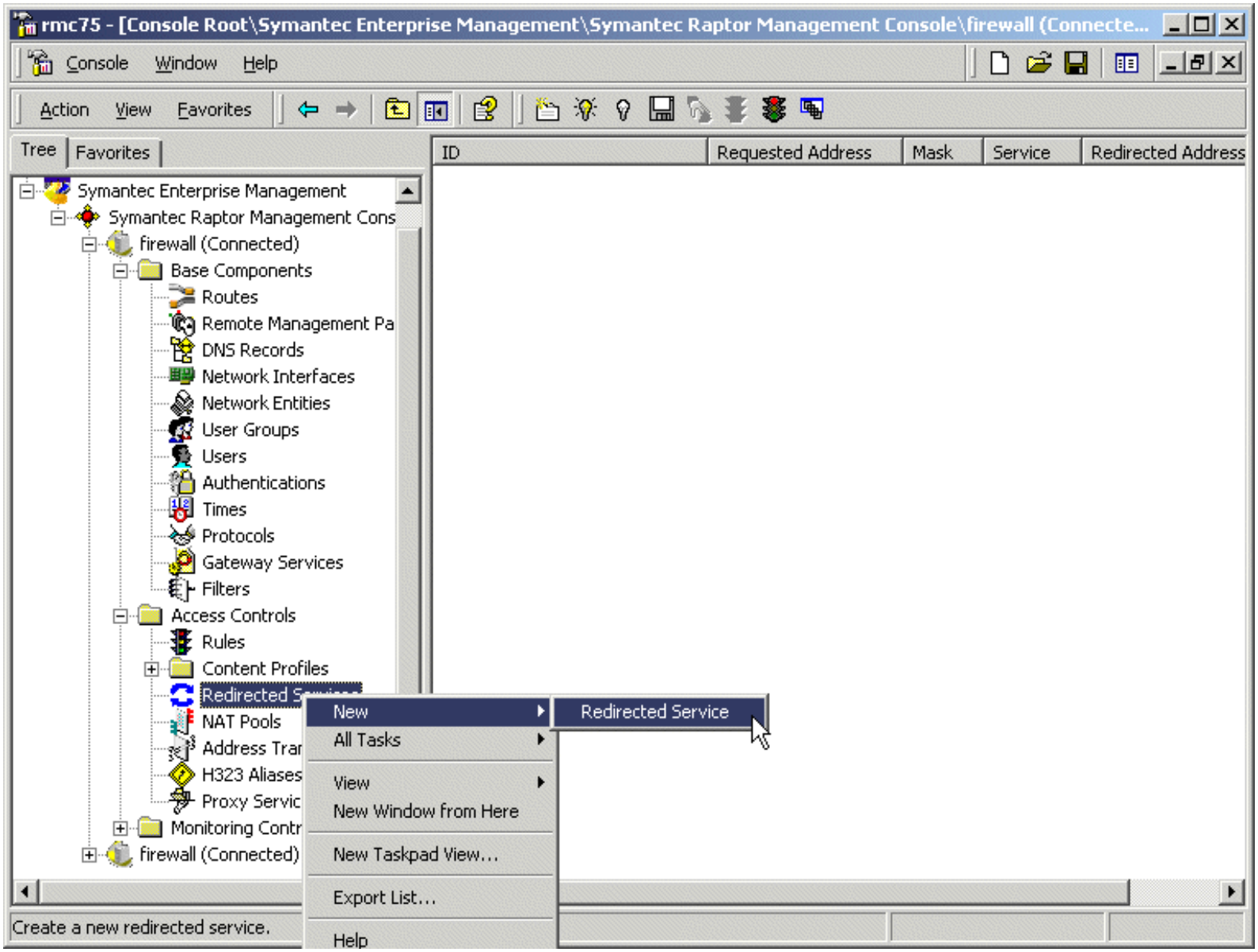
Step 3: Creating Redirected Service

Redirected services

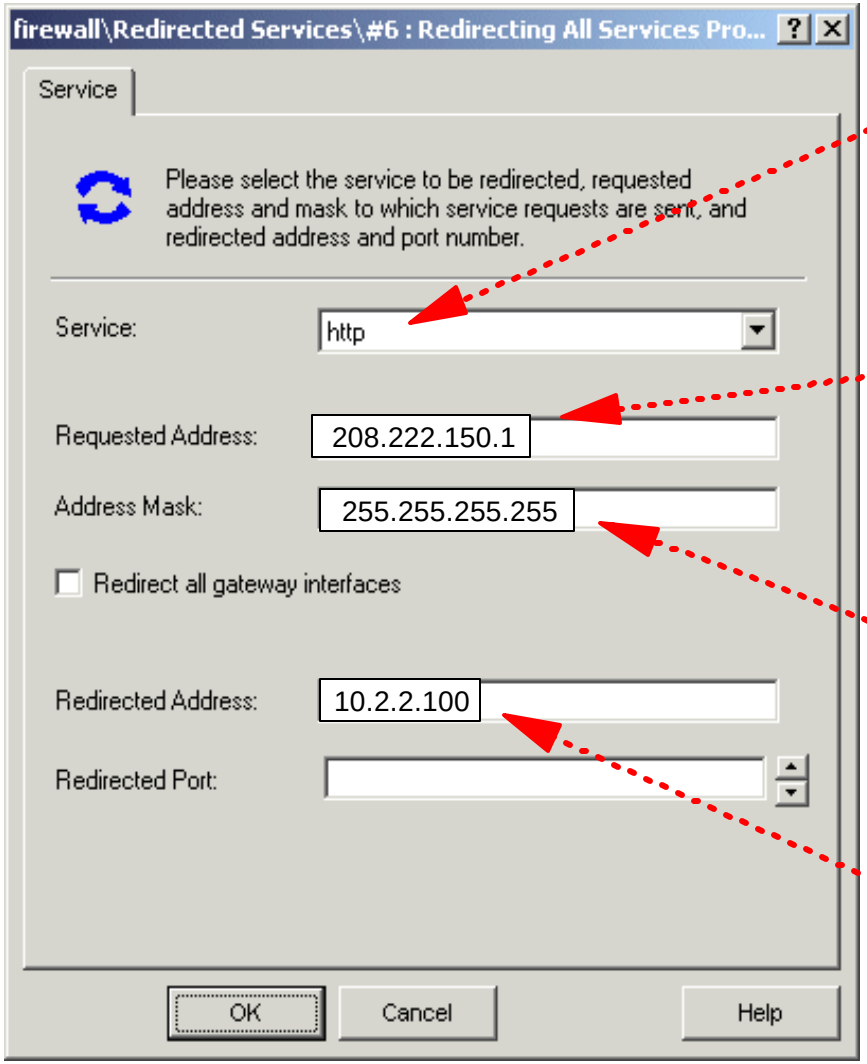
- Definition:
  - ✓ Service: HTTP
  - ✓ Requested IP address : 208.222.150.1
    - ➤ IP address used by outside users
  - ✓ Redirected IP address : 10.2.2.100
    - ➤ Real IP address of an application server



Step 3: Creating Redirected Service



Step 3: Creating Redirected Service



3a. Select http from the Service drop down selection box.

3b. Type in the public IP address in the Requested Address field.

3c. Type in the subnet mask for the requested address in Address Mask filed.

3d. Type in the real IP address where the service resides in the Redirected Address field.

Step 4: Creating Rules

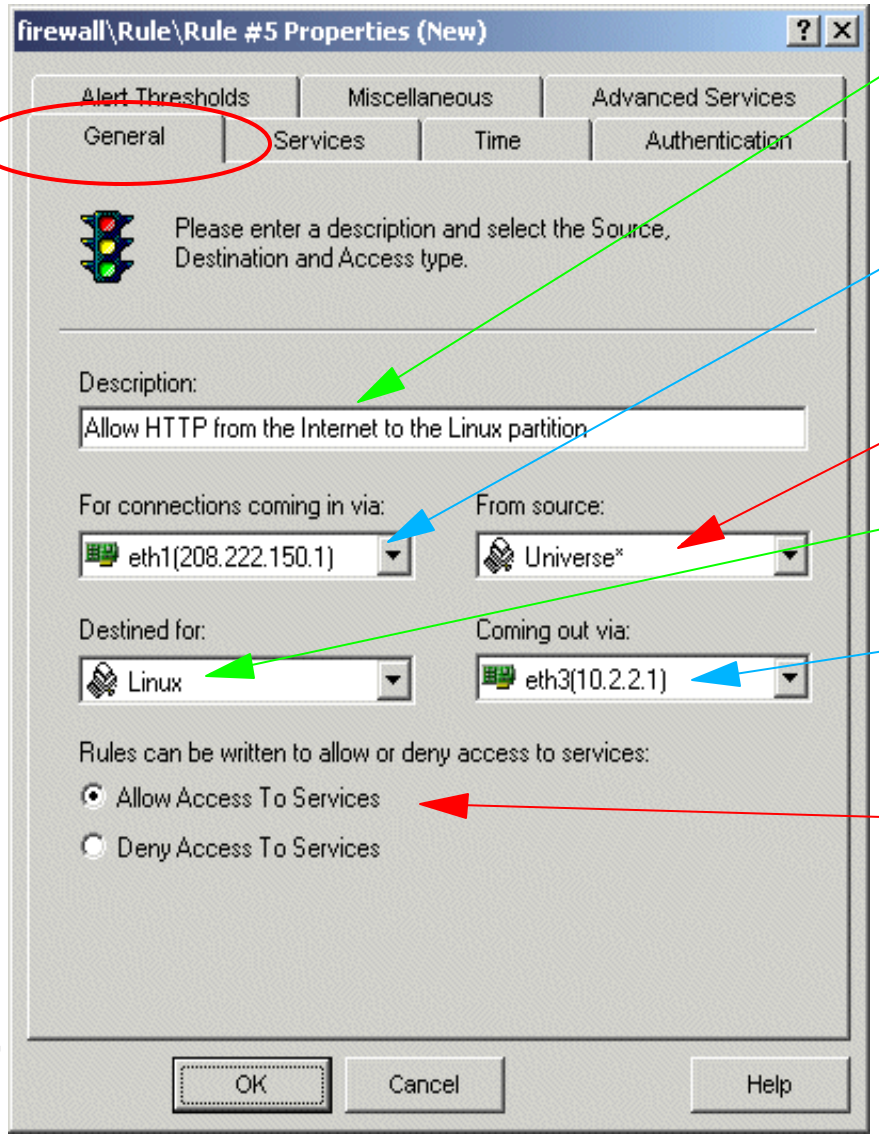
Rules

- Used to define access controls through the SEF
- Define a protocol X from entity Y to entity Z
- Rule definitions include:
  - ✓ Allow or deny
  - ✓ Source and destination entities
  - ✓ Interface packets are coming in
  - ✓ Interface packets are going out
  - ✓ Services

In case of our configuration example 1:

Allow/Deny	Interface coming in	From which entity	To which entity	Interface going out	Services
Allow	208.222.150.1	anybody	Linux	10.2.2.1	HTTP

Step 4: Creating Rules



4a. Type in a meaningful description for the rule in the Description field.

4b. Select eth1(208.222.150.1) for connections coming in field.

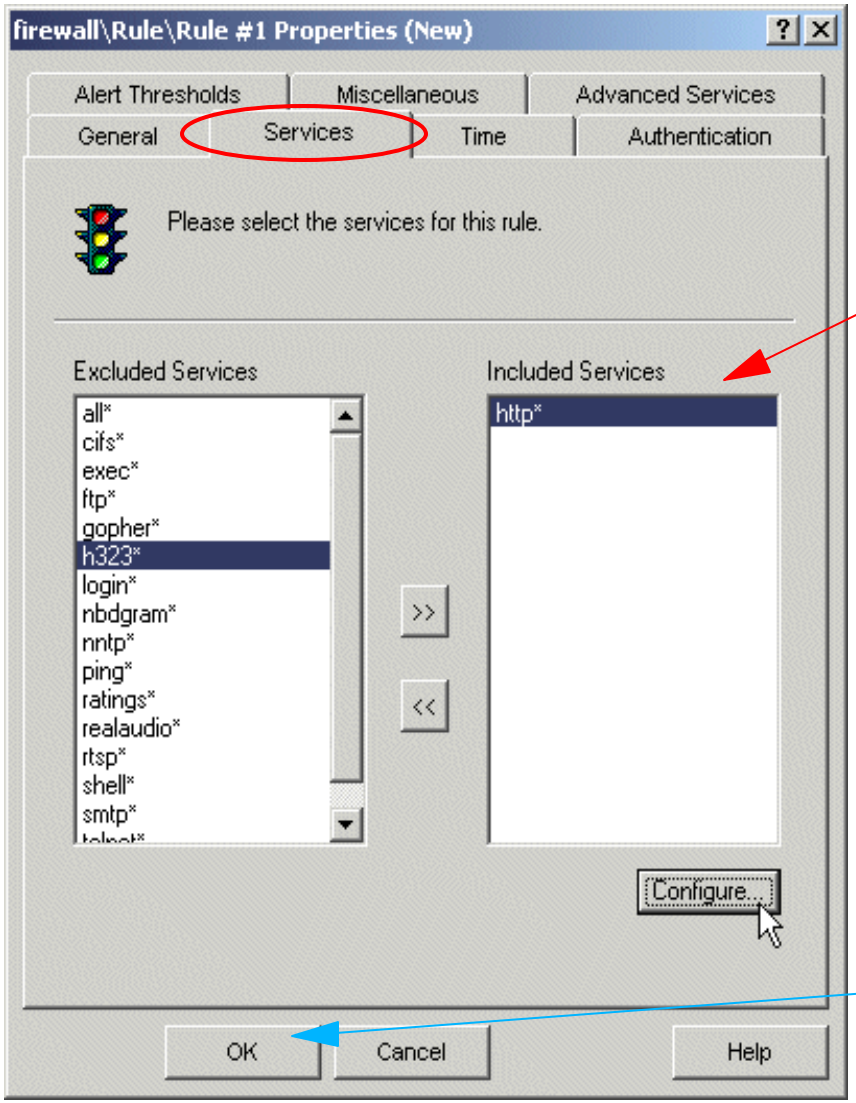
4c. Select Universe* for source field.

4d. Select Linux for Destined for field.

4e. Select eth3(10.2.2.1) for Coming out via field.

4f. Click on Allow Access to Services radio button.

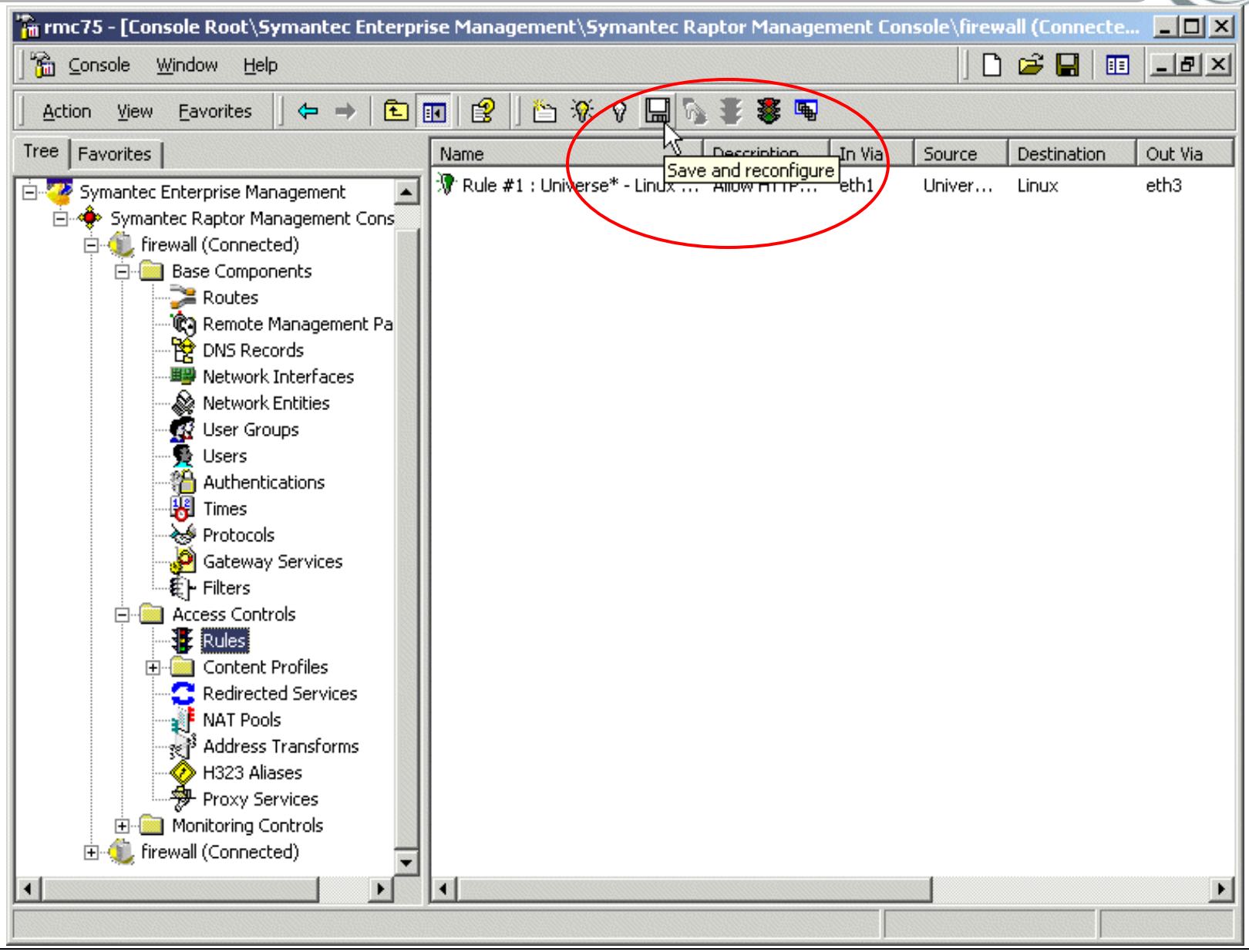
Step 4: Creating Rules



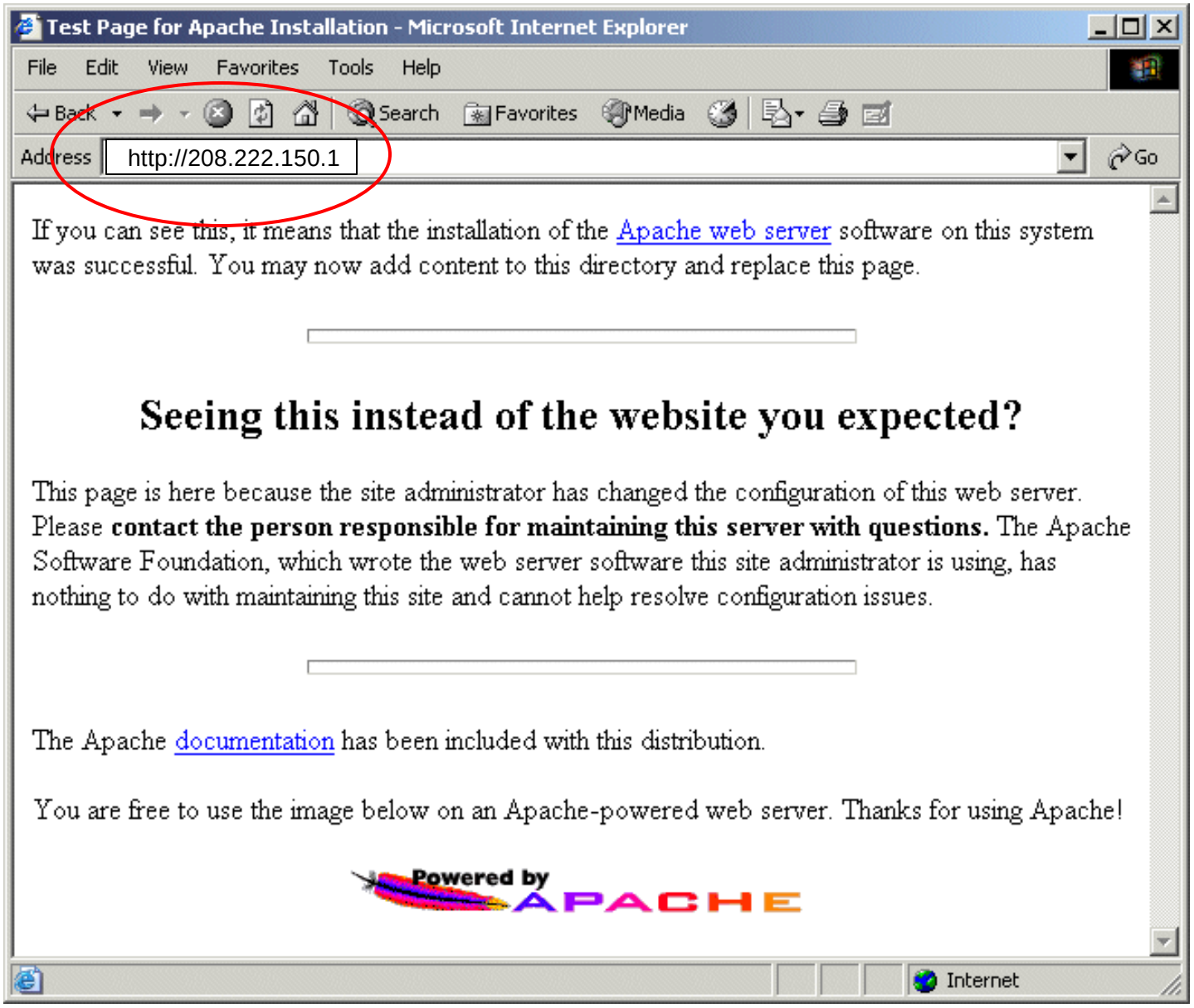
4g. On Service tab, add the http protocol to the Included Services field.

4h. Click OK to save the new rule.

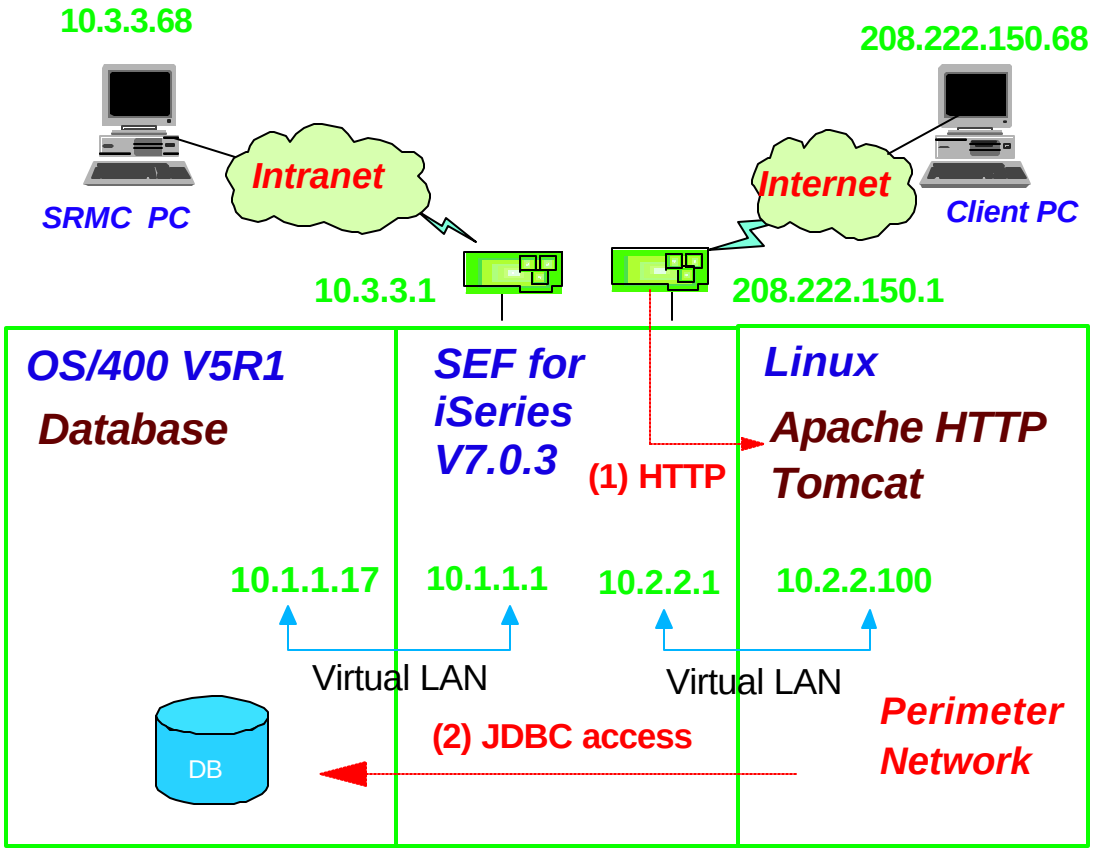
Saving Changes



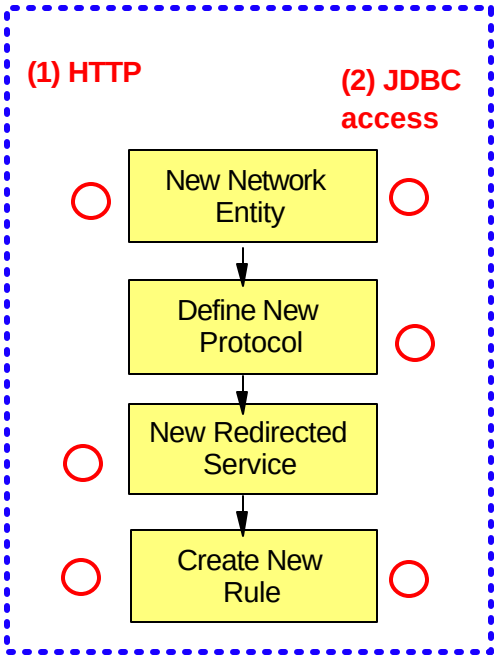
Test New Configuration Changes



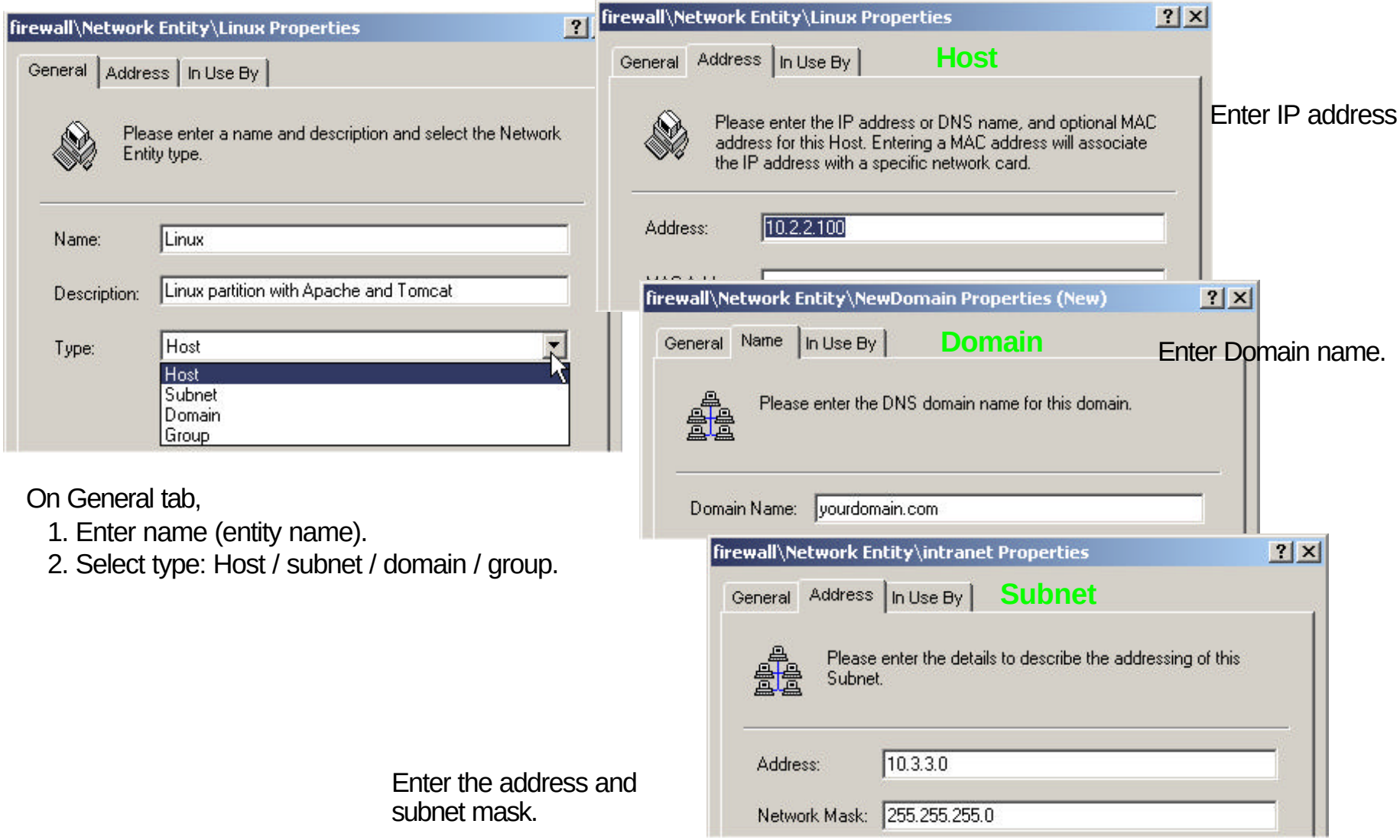
Configuration Example 2: JDBC Access



Steps:



Step 1: Creating New Network Entities

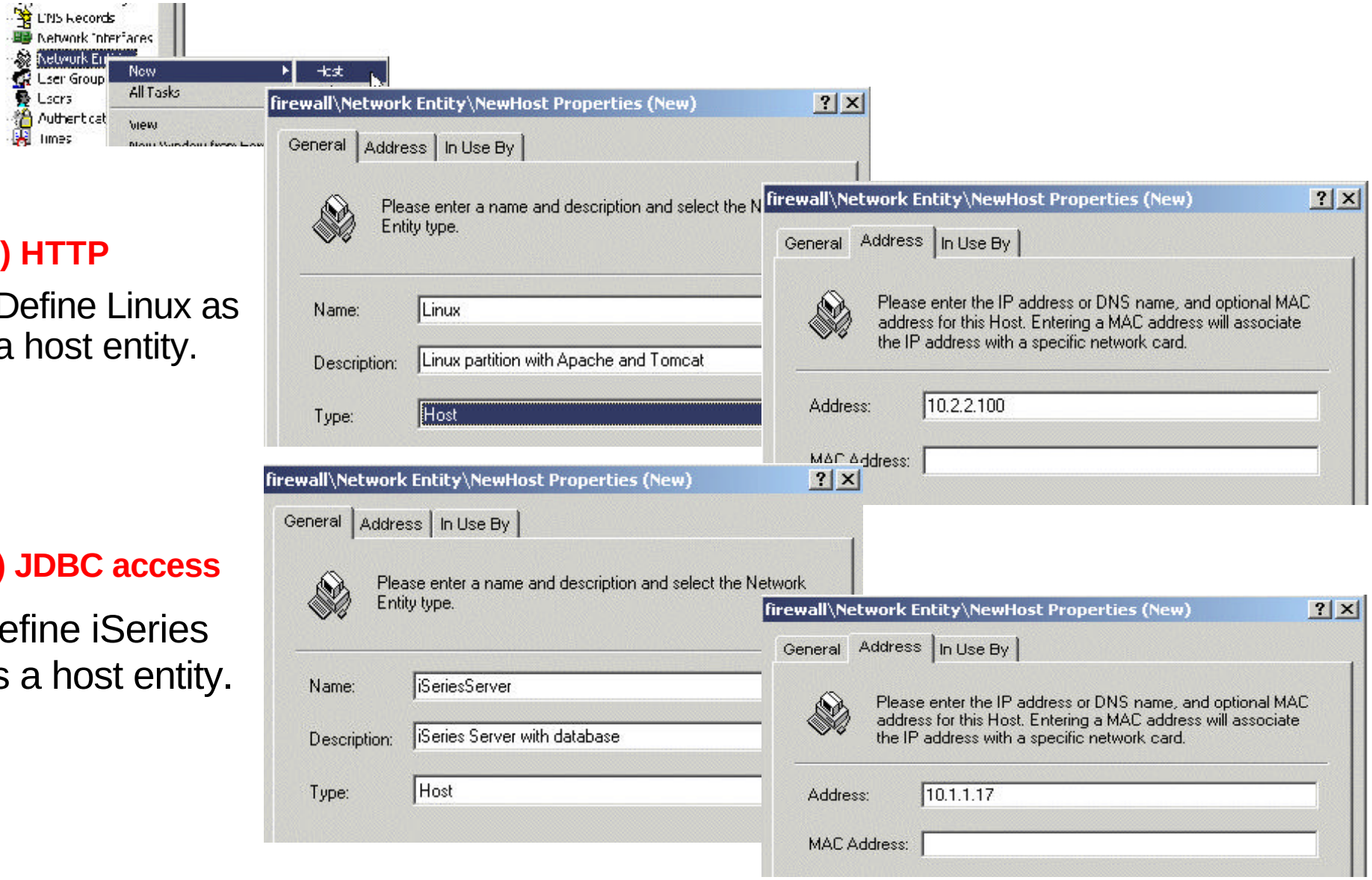


On General tab,

1. Enter name (entity name).
2. Select type: Host / subnet / domain / group.

Enter the address and subnet mask.

Step 1: Creating New Network Entities



(1) HTTP

Define Linux as a host entity.

(2) JDBC access

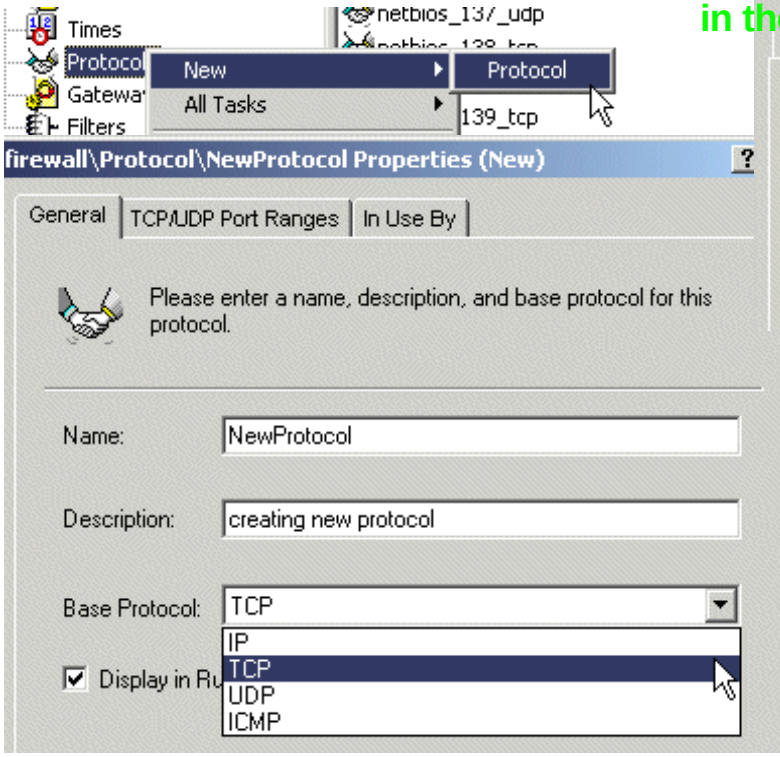
Define iSeries as a host entity.

Step 2: Defining New Protocols

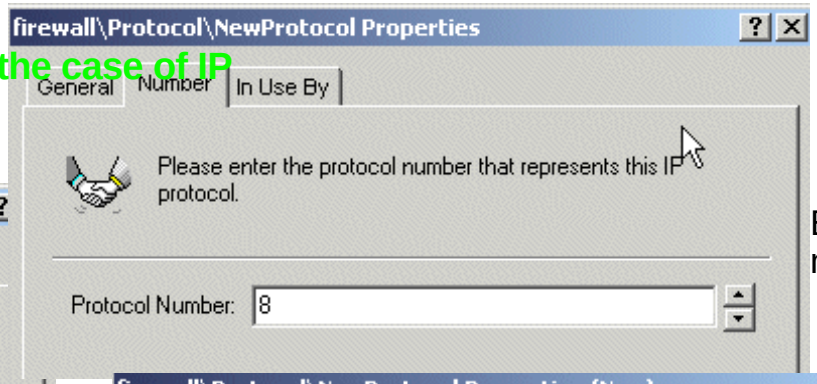
Protocols:

- Protocols are used to define types of traffic or services, such as HTTP, FTP, Telnet, etc.
- SEF has many predefined protocols
  - If SEF doesn't have protocols defined that you need, you must define them.
    - You need to know which protocols, or services, are needed in your firewall configuration.
- For example:
  - Internet <=> Linux:
    - HTTP(80)
  - Linux <=> OS/400:
    - Database(8471)
    - Signon(8476)
    - Server mapper(449)

Step 2: Defining New Protocols

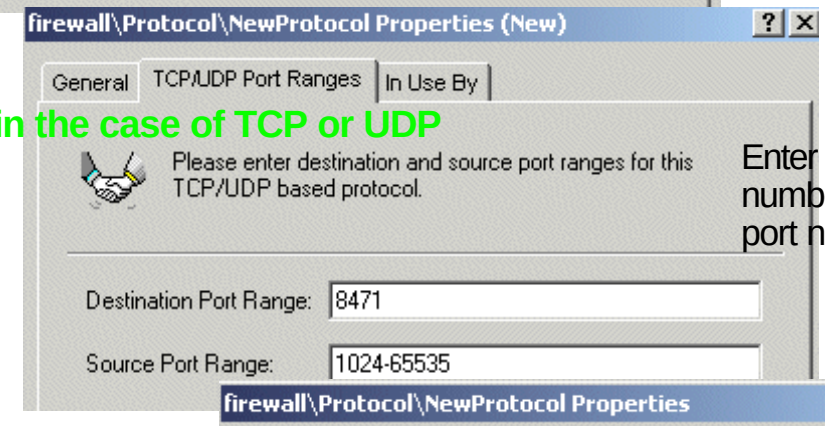


in the case of IP



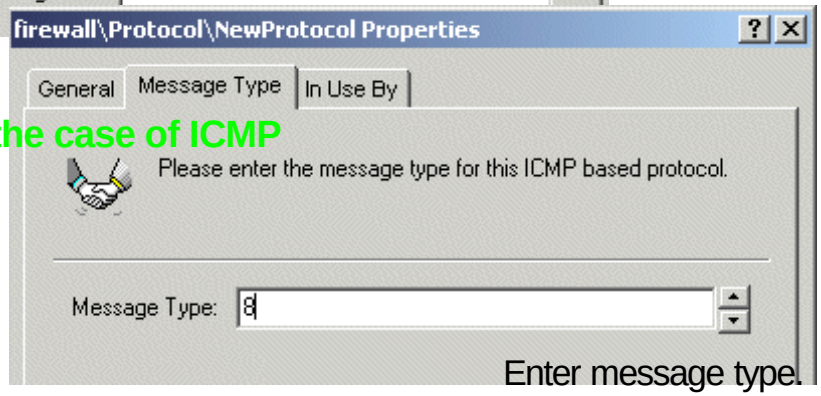
Enter protocol number.

in the case of TCP or UDP



Enter destination port number and source port number.

in the case of ICMP



Enter message type.

On General tab,

1. Enter name (protocol name).
2. Select Base Protocol: IP / TCP / UCP / ICMP.
3. Check Display in Rule Window.

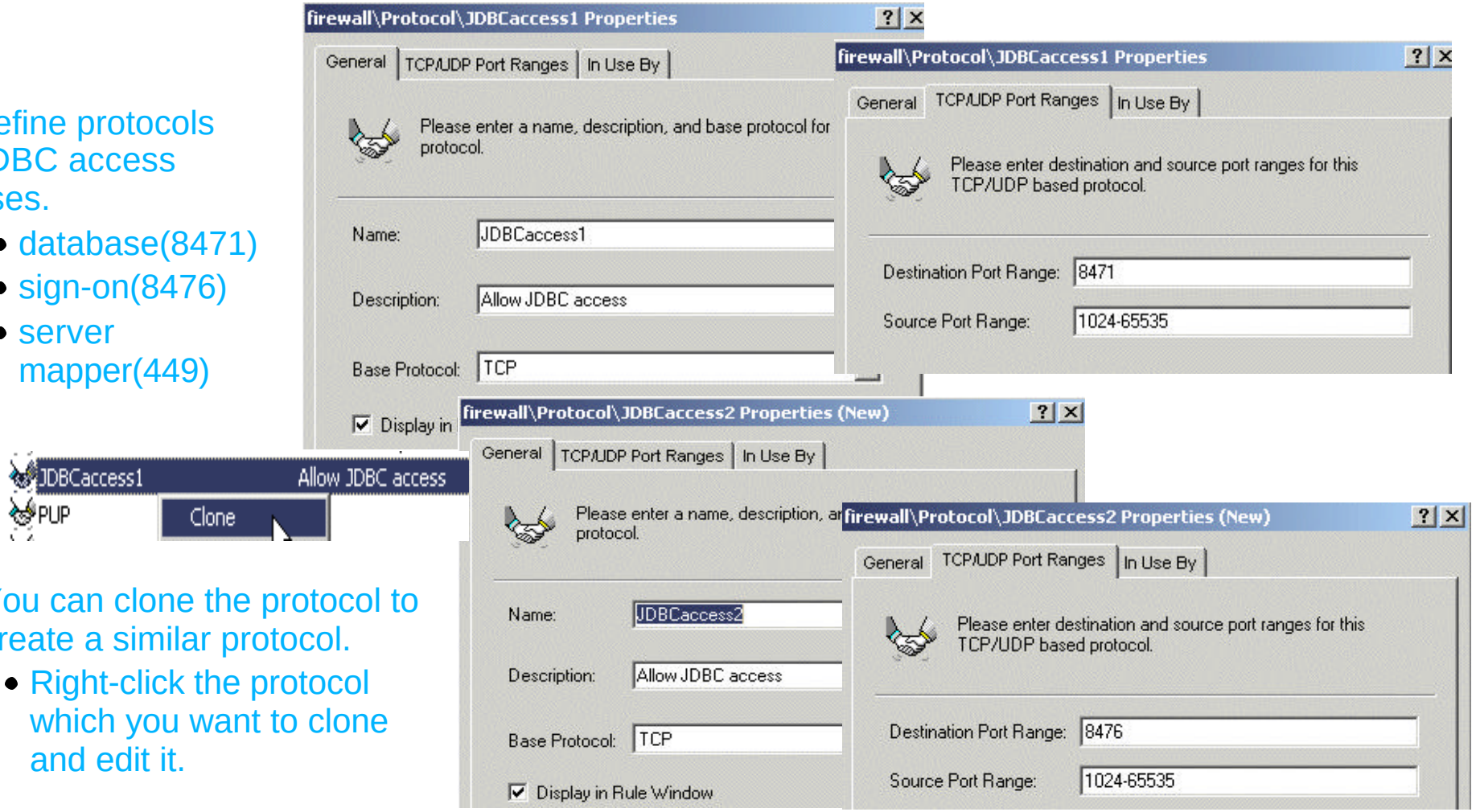
Step 2: Defining New Protocols

(1) HTTP: You don't need to configure protocol for HTTP because SEF provides it by default.

(2) JDBC access

Define protocols JDBC access uses.

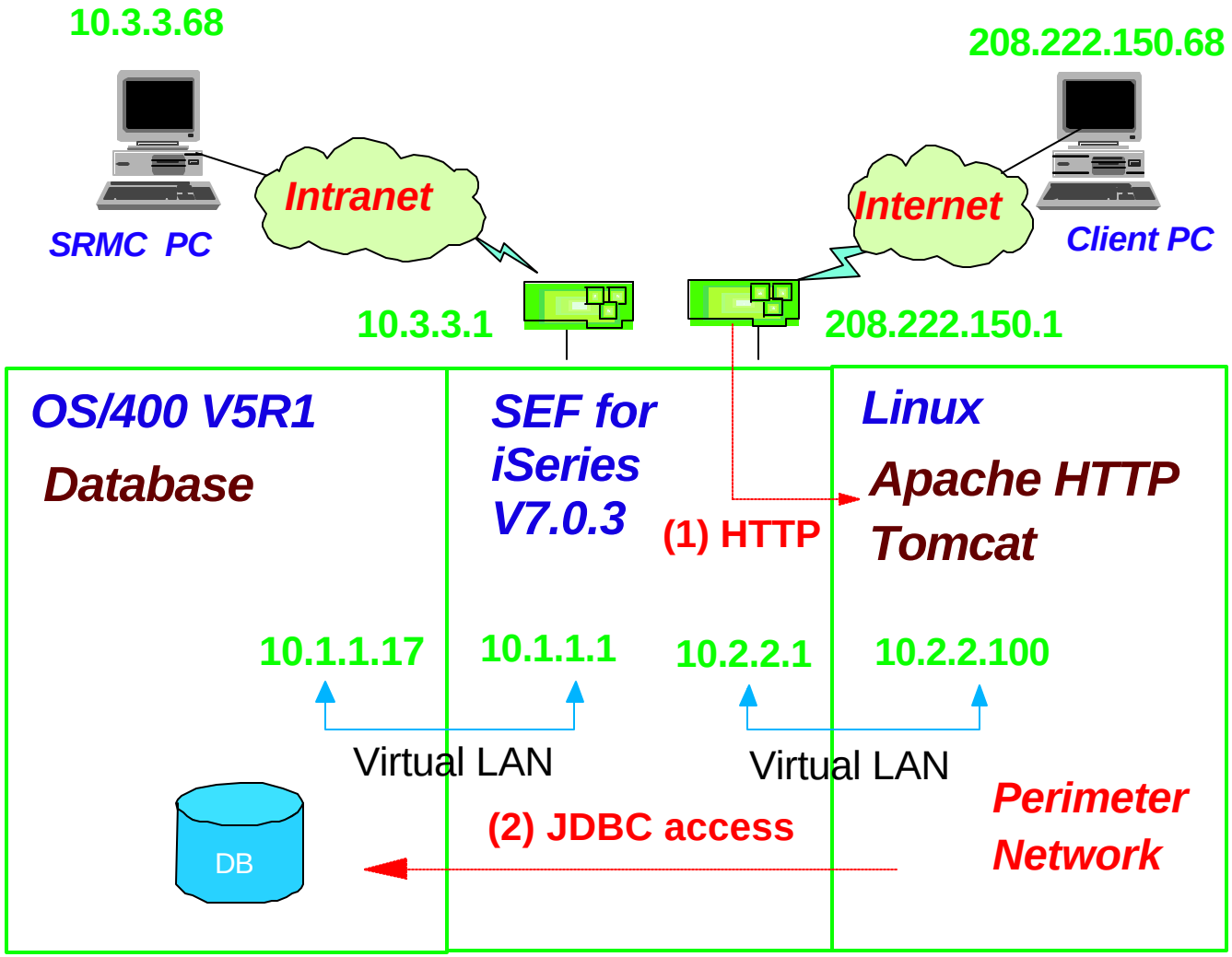
- database(8471)
- sign-on(8476)
- server mapper(449)



You can clone the protocol to create a similar protocol.

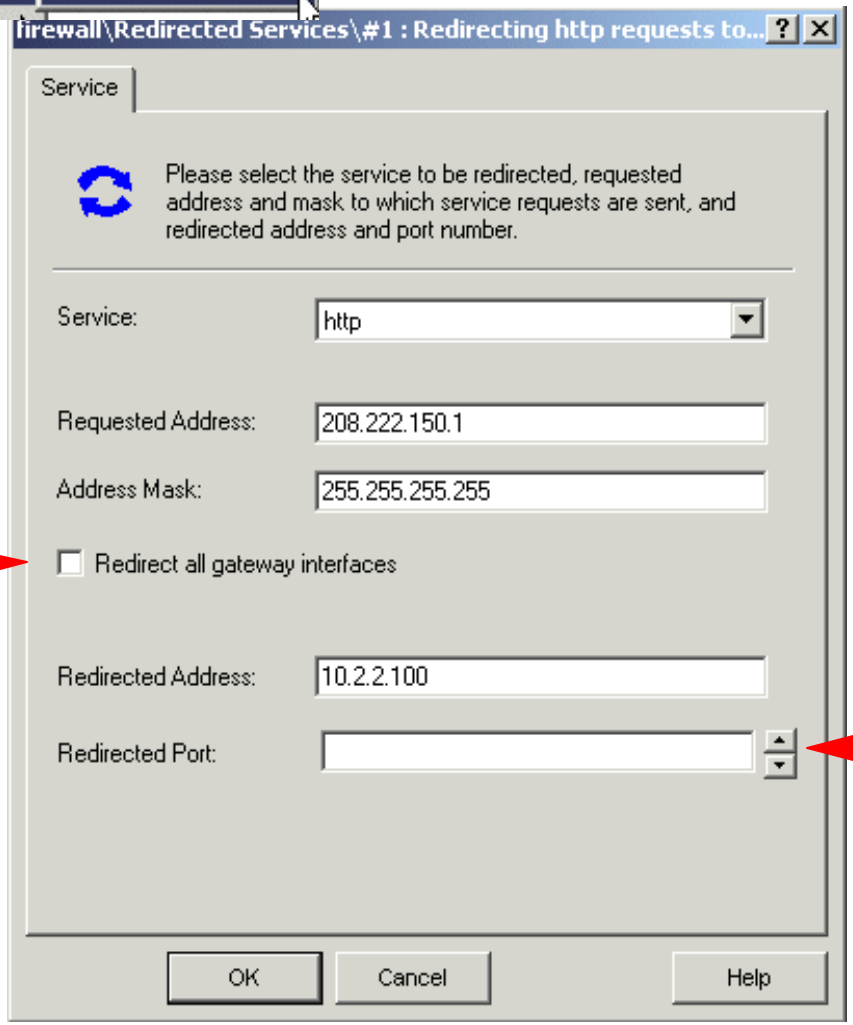
- Right-click the protocol which you want to clone and edit it.

Step 3: Creating Redirected Services



Define Redirected Services

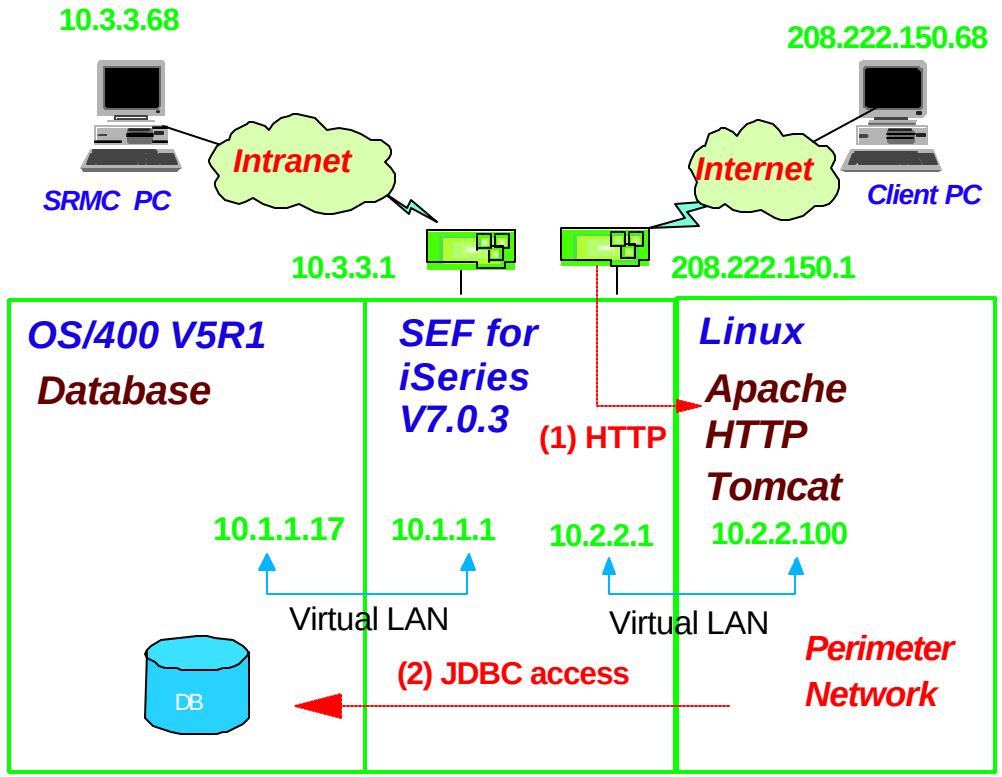
(1) HTTP



You can redirect the requested service from any gateway to the specific IP address.

If you use the different port number from the default port of the service you select, you must define Redirected port.

Step 4: Defining Rules

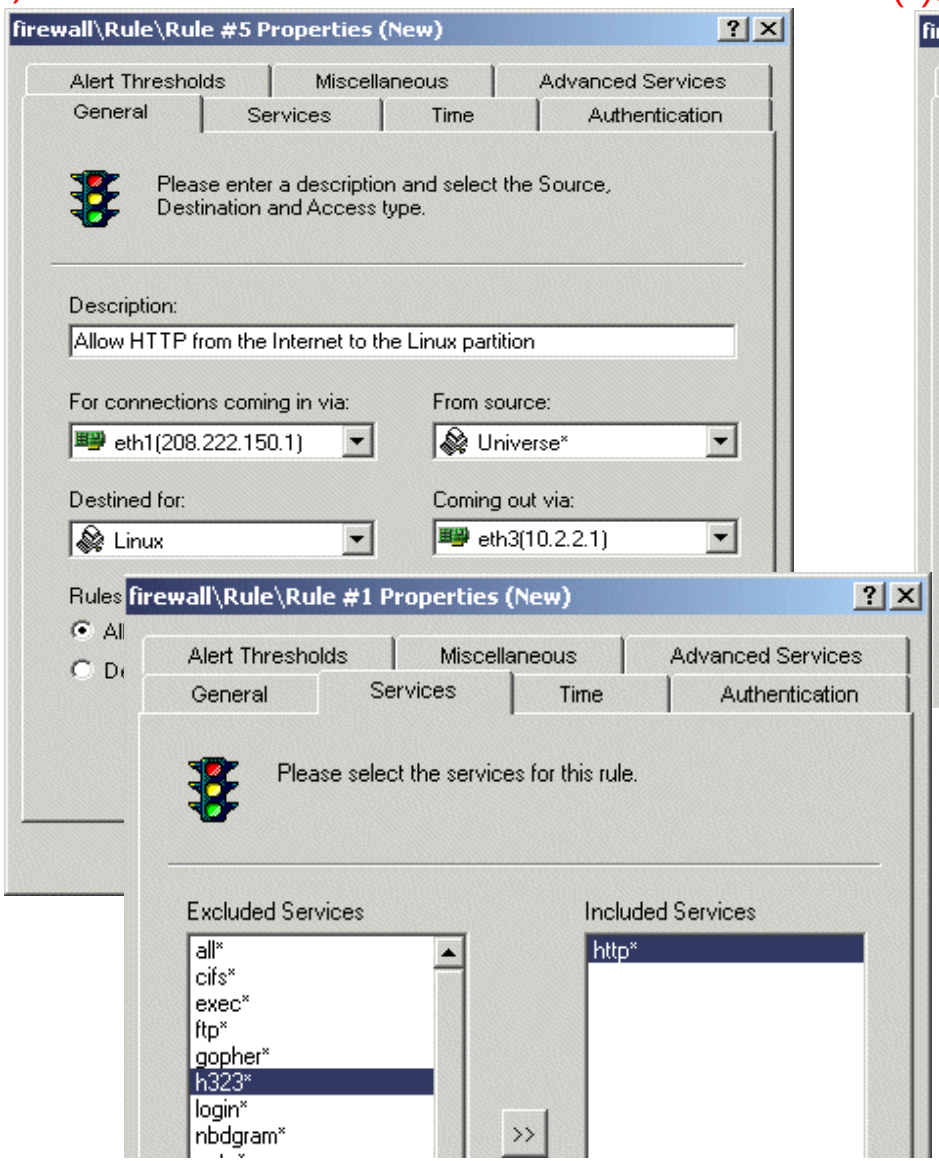


Allow/Deny	Interface coming in	From which entity	To which entity	Interface going out	Services
Allow (1)	208.222.150.1	anybody	Linux	10.2.2.1	HTTP
Allow (2)	10.2.2.1	Linux	iSeriesServer	10.1.1.1	JDBC access

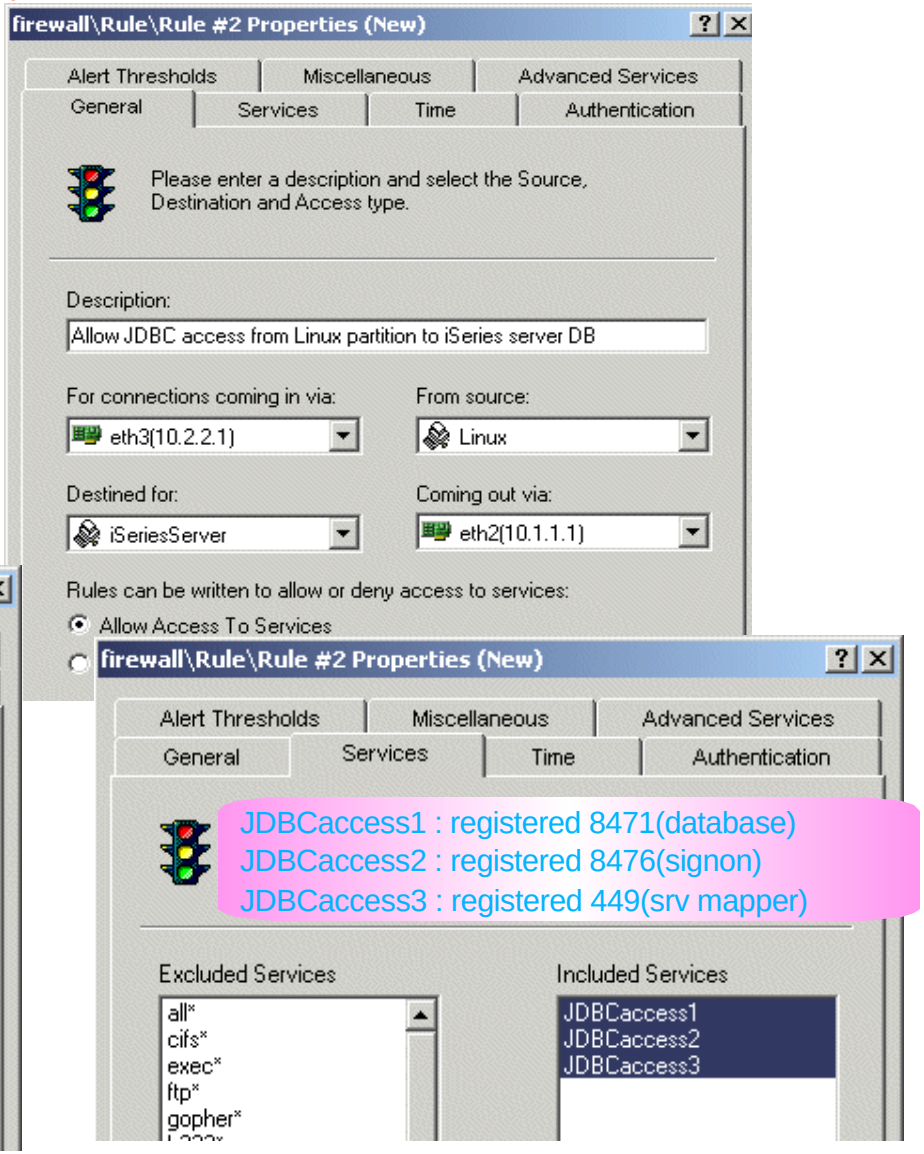
*In this case, JDBC access needs database(8471), sigh on(8476), server mapper(449)

Step 4: Defining Rules

(1)HTTP



(2)JDBC access

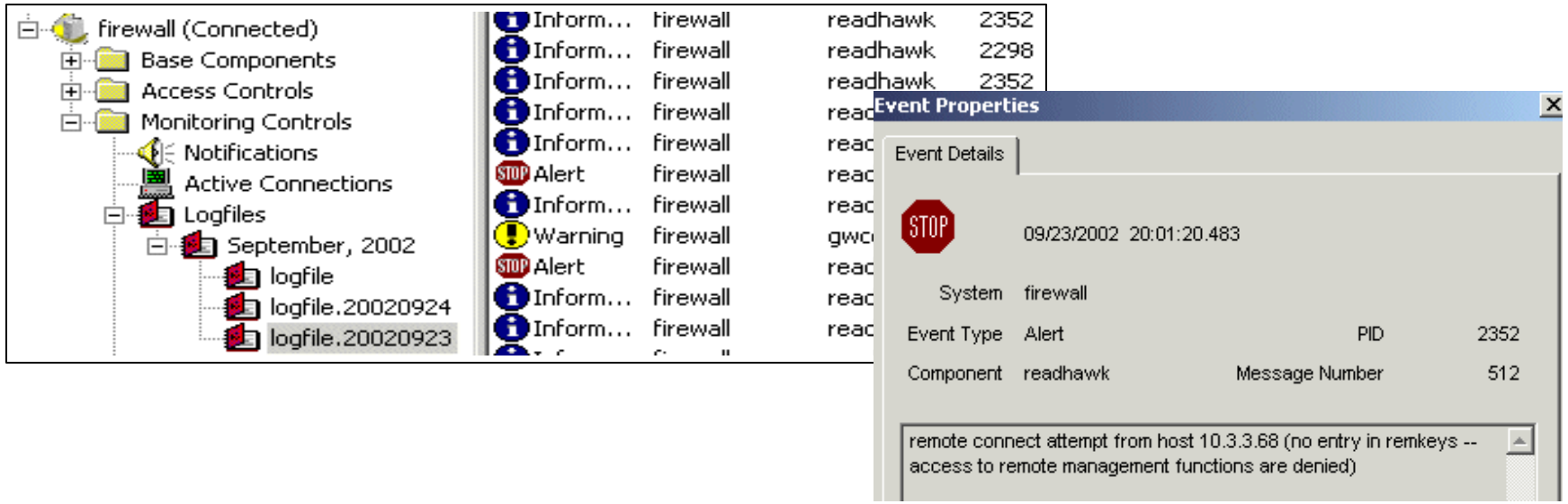


SEF for iSeries: Administration

Logfiles

Logfile:

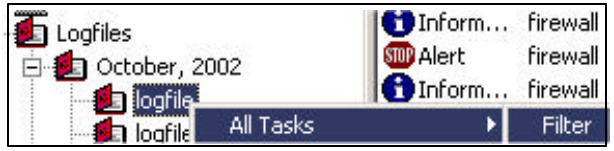
- Information that the system logs about all connections and connection attempts
- You can look for malicious traffic such as:
  - ✓ denial of service attacks
  - ✓ port scans
  - ✓ attempts to access protected services
  - ✓ etc.



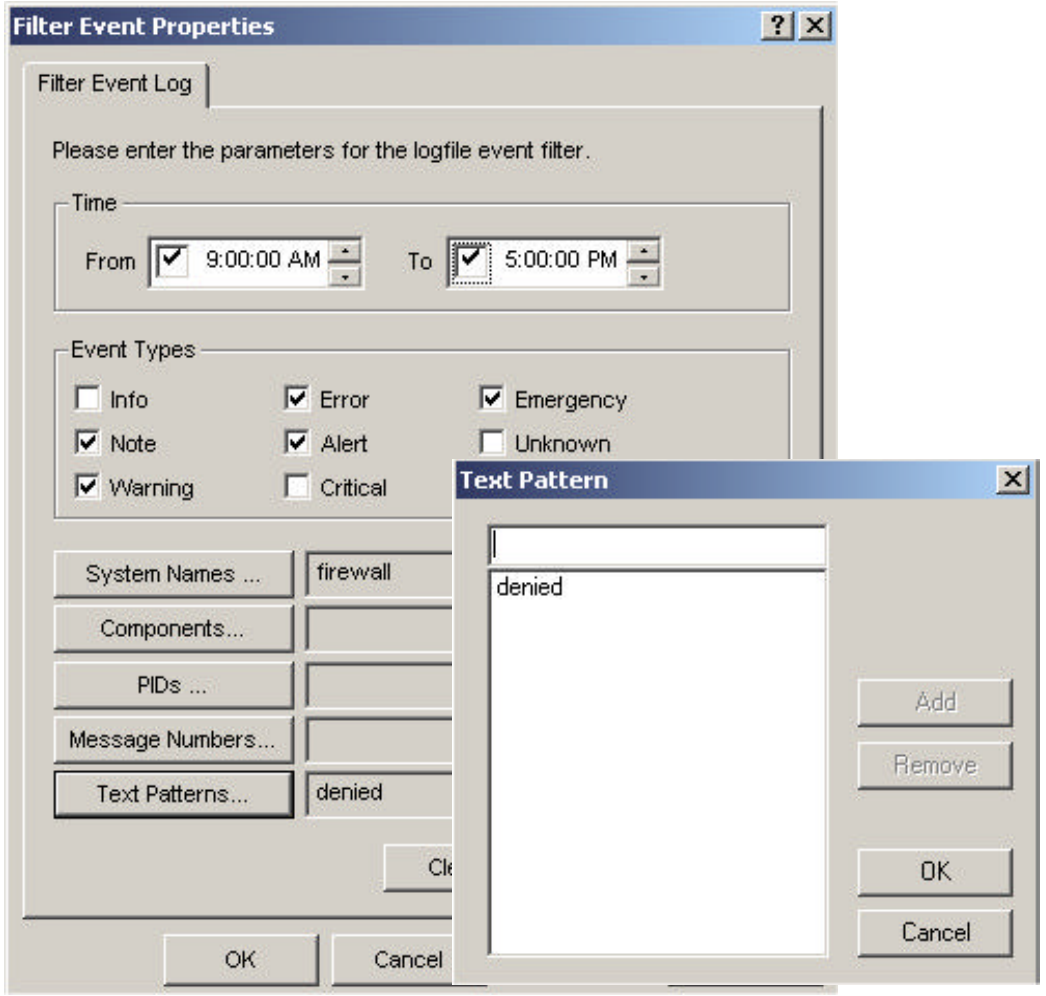
Logfiles (cont.)

Filtering the logfile:

- Sort through the data collected in a logfile



- Easy to locate information based on criteria you define, such as:
  - Event type:
    - Emergency
    - Alert
    - Error
    - Warning
    - Critical
    - etc.
  - Time
  - System names
  - Text patterns

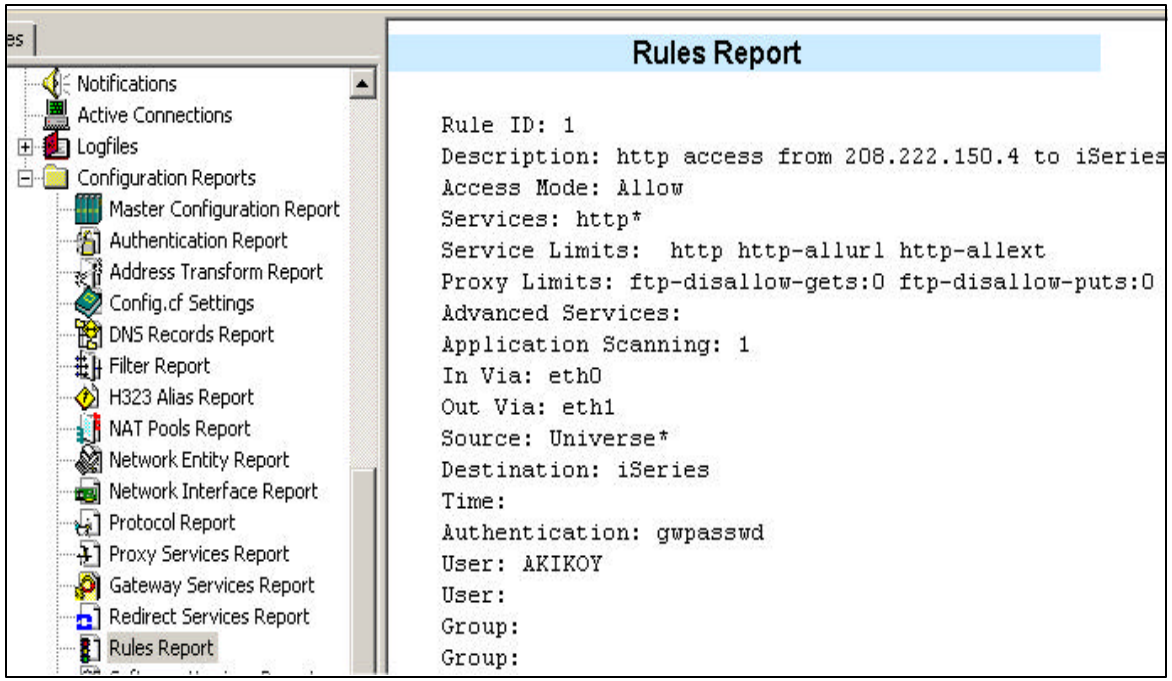


Configuration Reports

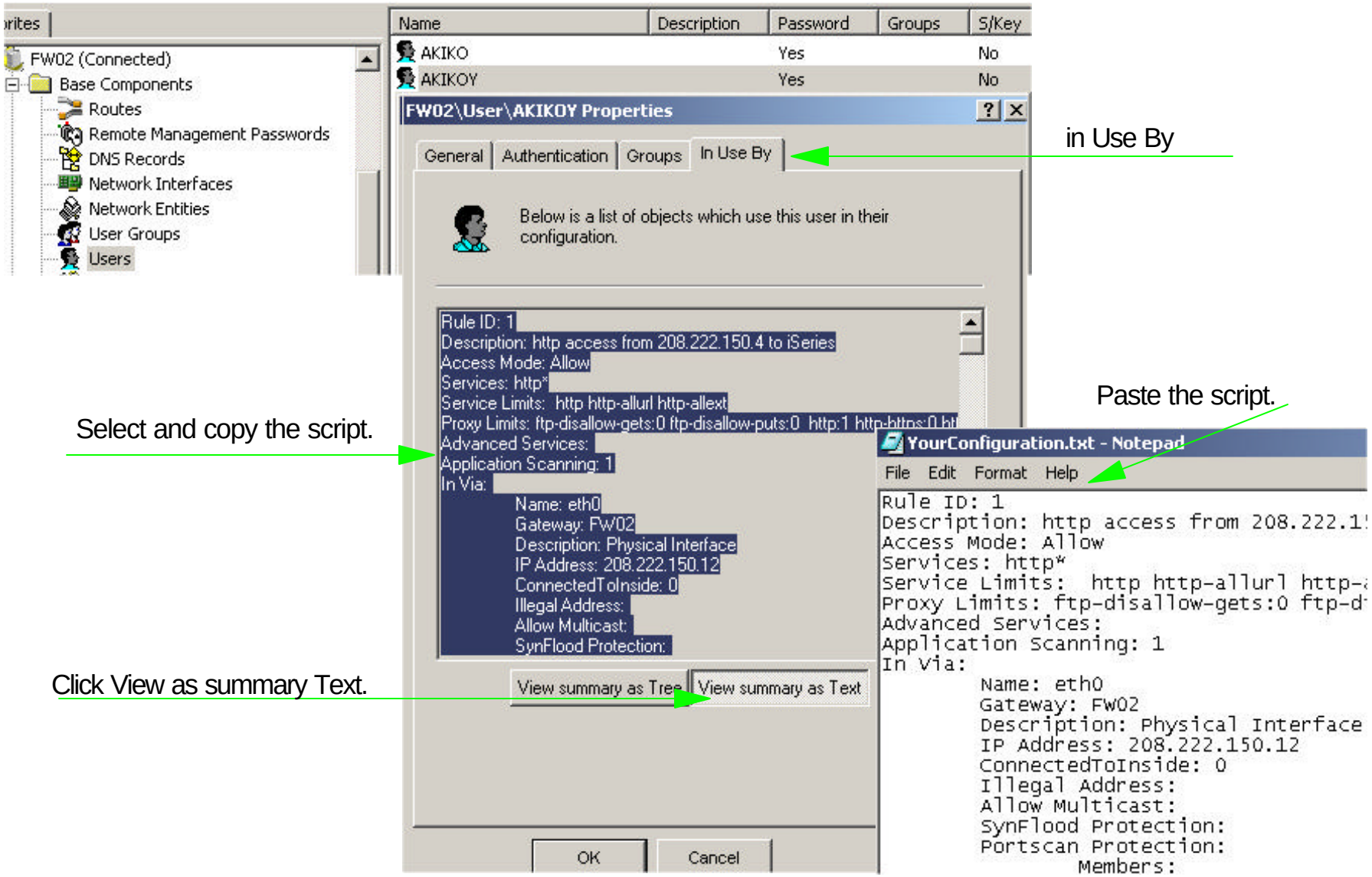
Let other administrators know your configuration easily

- Create reports on SEF configuration
  - ✓ SEF provides reports for all parts of your configuration includding:
    - Master configuration report
    - Authentication report
    - Address transform report
    - DNS records report
    - NAT pools report
    - Network entities report
    - Protocols report

You can copy and paste the reports, and create text files (.txt) for sending to other administrators or for printing.



Create reports on specific objects

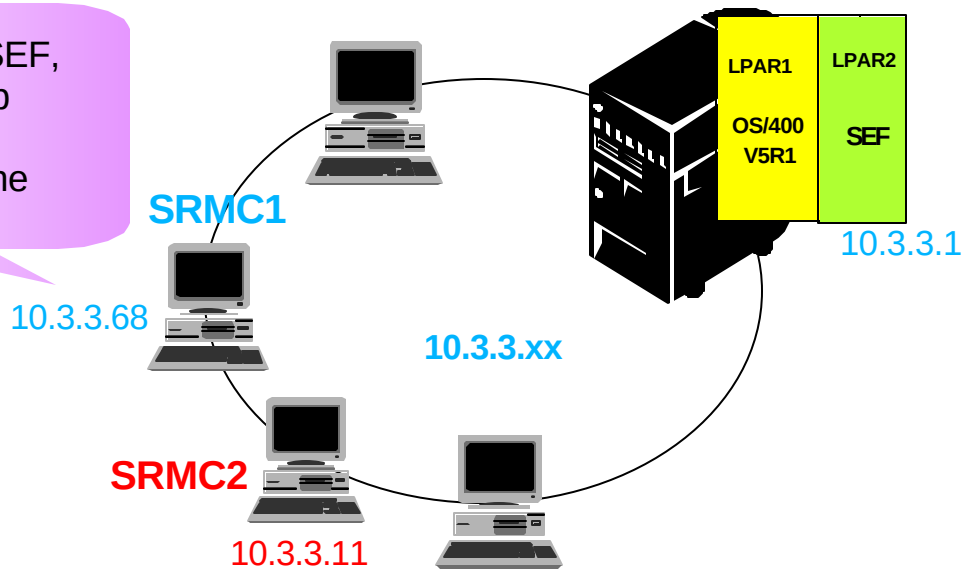


Configuring additional SRMC clients

Administer SEF system with additional SRMC clients

- SRMC remote management types
  - Remote Management
  - Read Only
  - Logfile Retrieval
  - Log Event Submission
  - Intrusion Detection

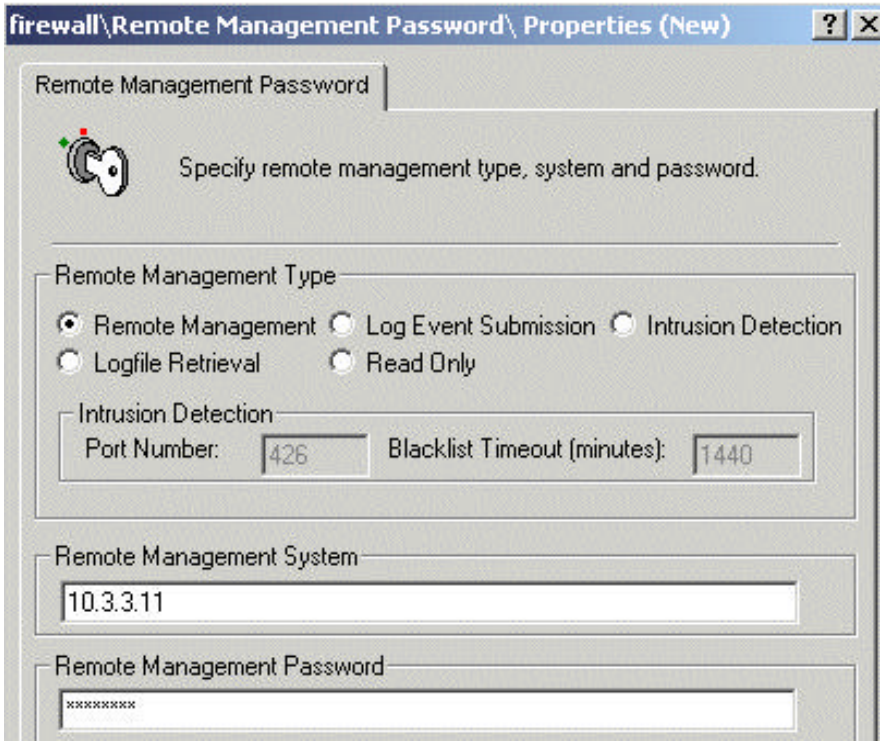
- To allow SRMC2 (10.3.3.11) to administer the SEF, in addition to SRMC1 (10.3.3.68) that was setup during the SEF install, we must configure an additional Remote Management Password on the SEF from SRMC1.



Define Remote Management Console

Configuring additional SRMC

- Configure a new Remote Management Password to allow an SRMC connection from 10.3.3.11 from existing SRMC
  - IP address : 10.3.3.11
  - Password : **********

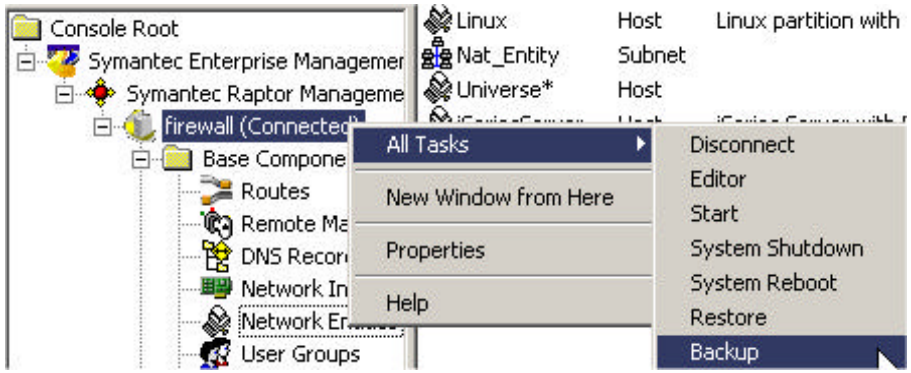


Backup and Recovery

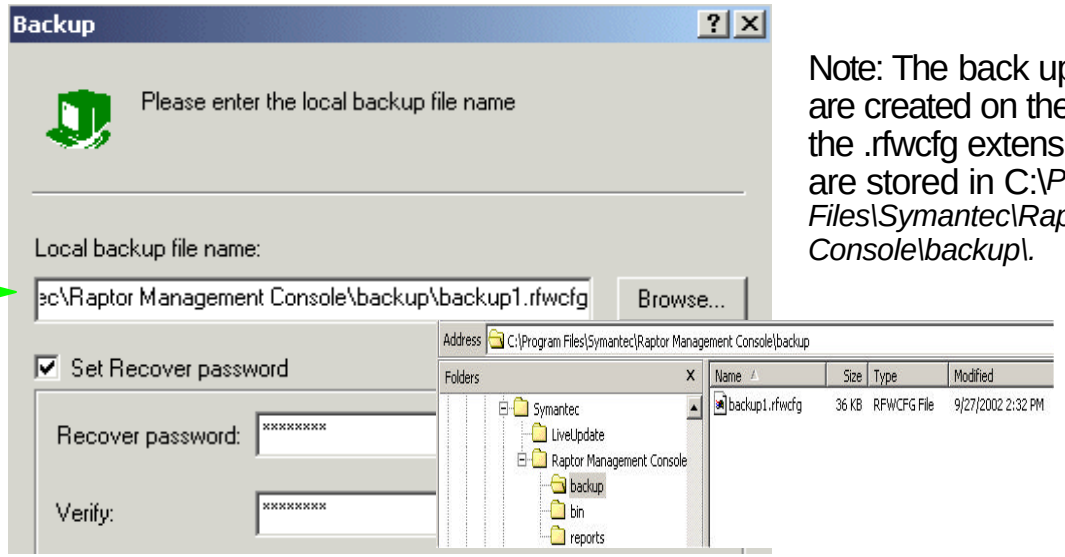
Two Ways for backup and recovery:

- Save NWSSTG object on iSeries
  - ✓ NWSSTG exists on IFS
    - ➢ /QFPNWSSTG/XXXX (NWSSTG name)
    - ➢ SAV DEV('.../.../...') OBJ(('qfpnwsstg/NWSSTG_name'))
    - ➢ SAV DEV('qsys.lib/qgpl.lib/firewall.savf') OBJ(('qfpnwsstg/fw_stg'))
    - ➢ SAV DEV('tap01') OBJ(('qfpnwsstg/fw_stg'))
    - ➢ RST DEV('.../.../...') OBJ(('qfpnwsstg/NWSSTG_name'))
    - ➢ RST DEV('qsys.lib/qgpl.lib/firewall.savf') OBJ(('qfpnwsstg/NWSSTG_name'))
    - ➢ RST DEV('tap01') OBJ(('qfpnwsstg/fw_stg'))
- Save SEF configuration files from a SRMC client
  - ✓ The backup configuration file is stored locally on the SRMC client.

Backup Configuration Files



1. Right click any SRMC component. and select All Tasks -> Backup.



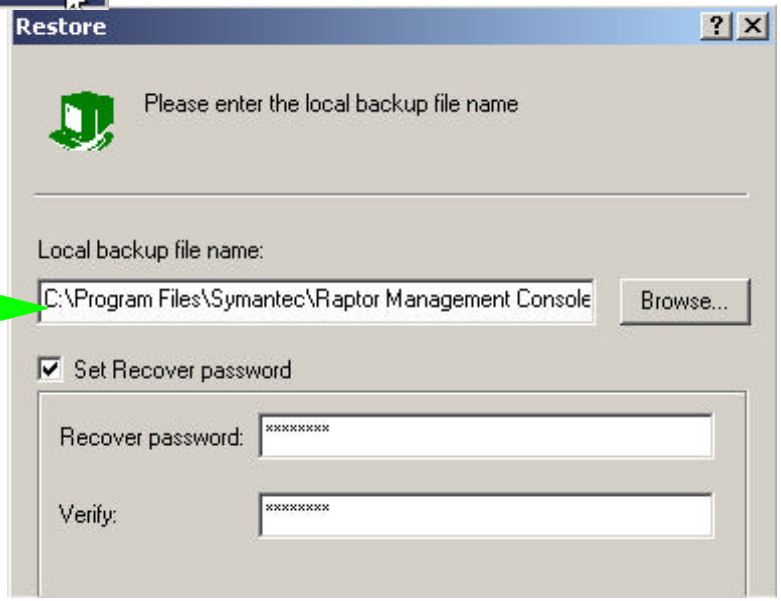
2. Enter the backup file name.

If you want to restore the configuration to another SEF, you need to set a recover password. Otherwise it is optional.

Note: The back up configuration files are created on the SRMC PC with the .rfwcfg extension and by default are stored in C:*Program Files\Symantec\Raptor Management Console\backup*.

Restore configuration files

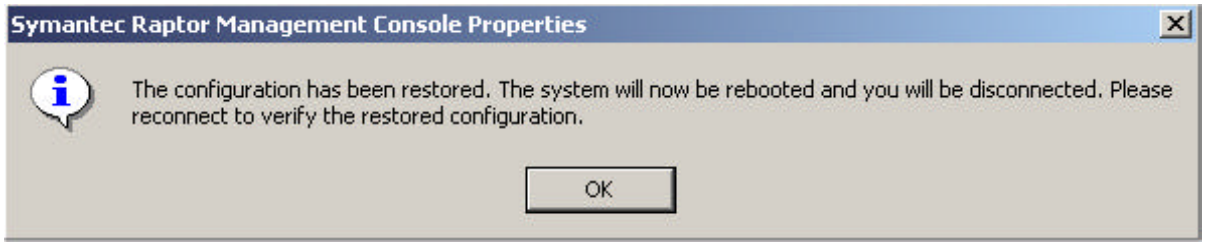
1. Right click any component and select All Tasks -> Restore.



2. Browse to an existing filename or type in the backup file name.

3. Type in a recover password if needed.

4.Click OK to restore.



5. Click OK on the SRMC properties dialog to reboot the SEF. After rebooting, the configuration is restored.

Summary

Summary

- Easy installation from CD
  - ✓ Install SEF on iSeries, Install SRMC on PC
- GUI configuration and easy to use setup wizards
- Remote management
  - ✓ Symantec Raptor Management Console(SRMC)
- Logging facilities
  - ✓ Such as user names, session duration, authentication methods
- Full-applicaiton packet inspection
  - ✓ Rules, Filters
- Network address translation and address hiding
  - ✓ Redirected address, NAT pools, Address transform
- Backup and recovery
  - ✓ Backup and recover configuration files using the SRMC or backup the NWSSTG from the iSeries server using the SAV command.

References

Symantec

- http://www.symantec.com
- On SEF installation CD
  - ✓ SEF_Config.pdf
  - ✓ SEF_Install.pdf
  - ✓ SEFVPN_Ref.pdf

Redbooks and Redpieces

- Symantec Enterprise Firewall on Linux for iSeries (book# SG24-6872)
- Linux on the IBM eServer iSeries
  - ✓ http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg246232.pdf
- LPAR Configuration and Management Working with IBM eServer iSeries Logical Partitions
  - ✓ http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg246251.pdf