

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

© 2003 IBM Corporation

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

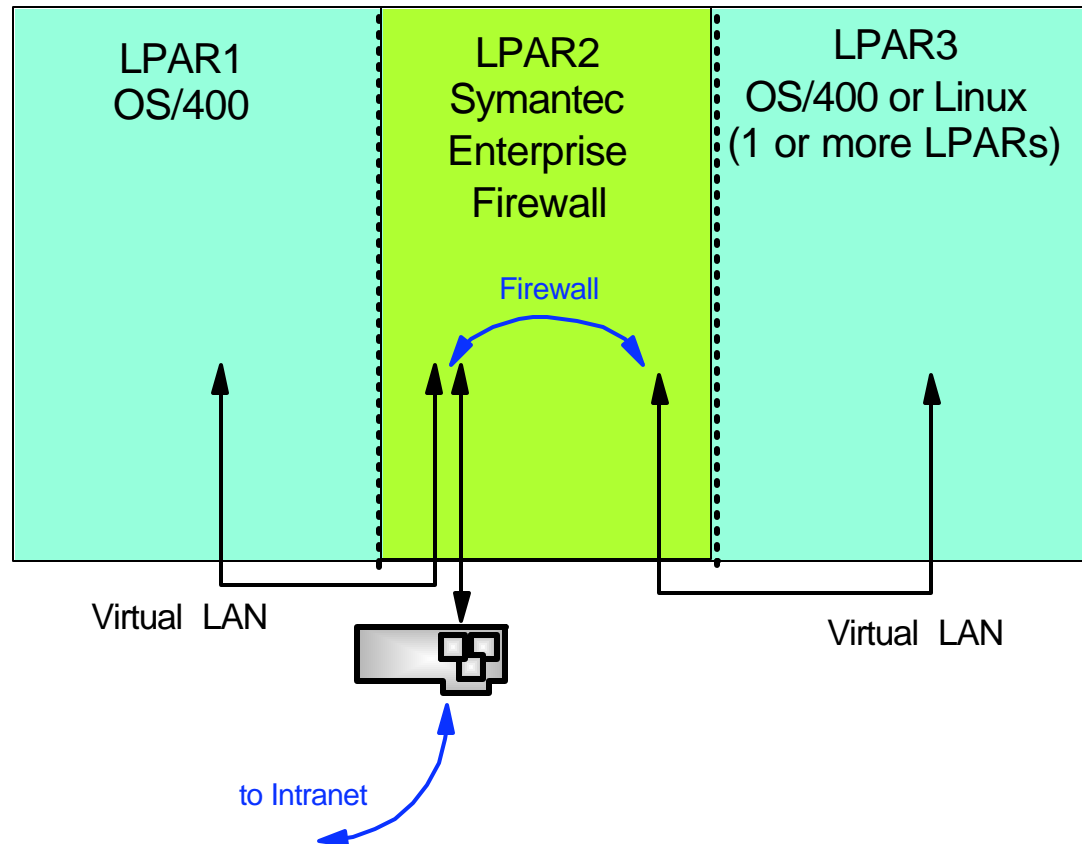


SEF for iSeries running Linux: Topologies

Topology 1



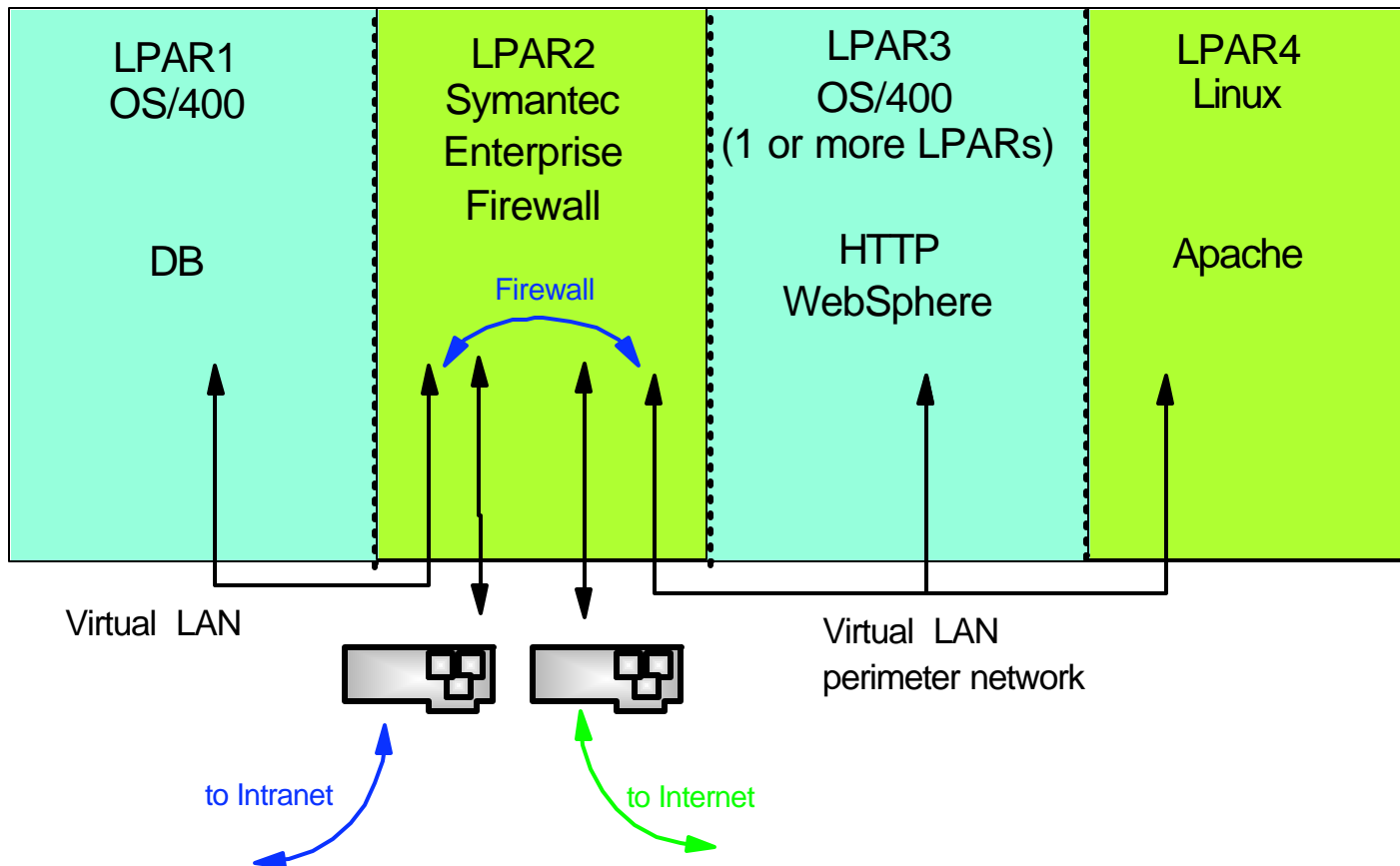
Symantec Enterprise Firewall with an Intranet



Topology 2



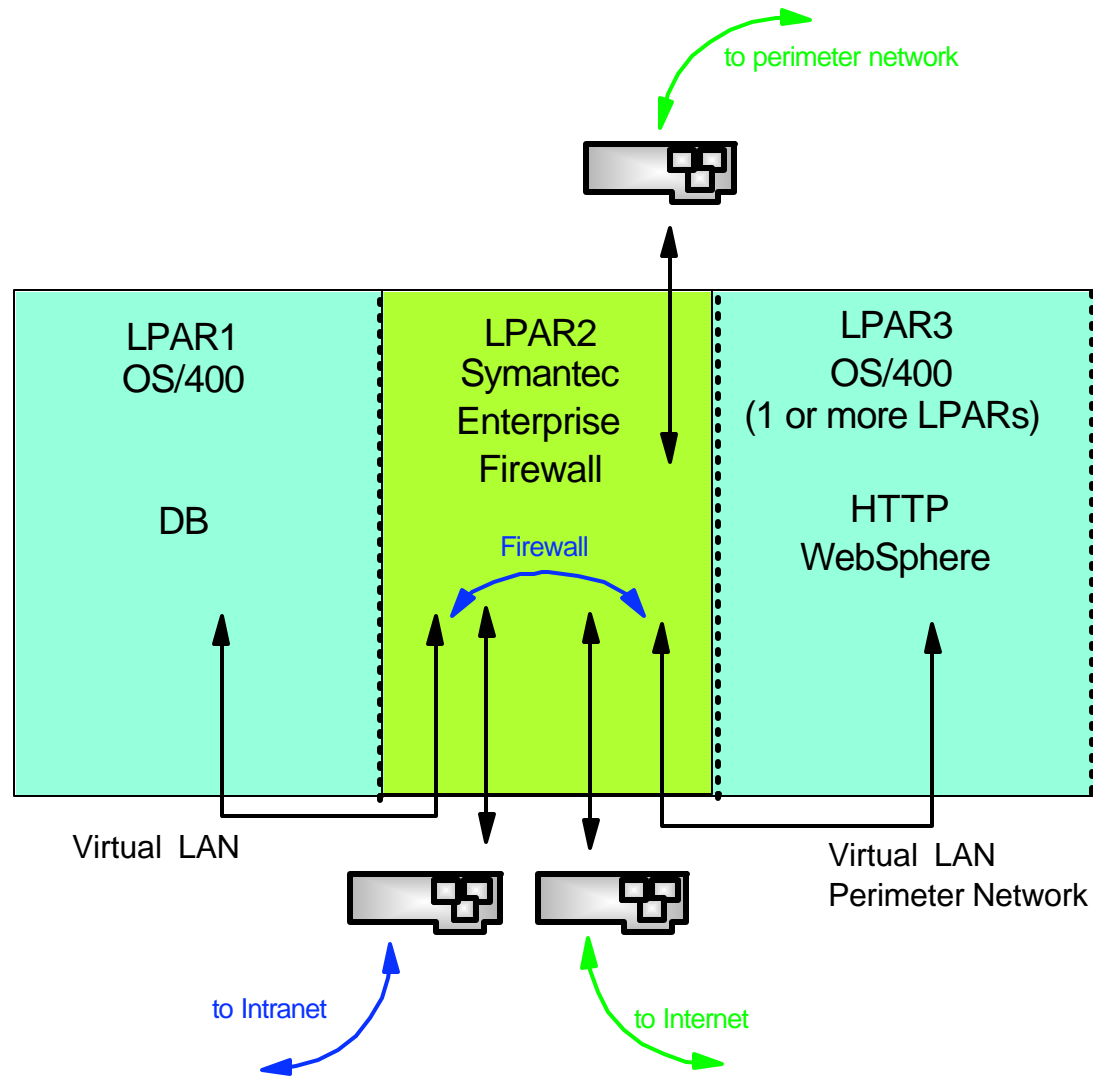
SEF with an Intranet and a virtual LAN perimeter network



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.)



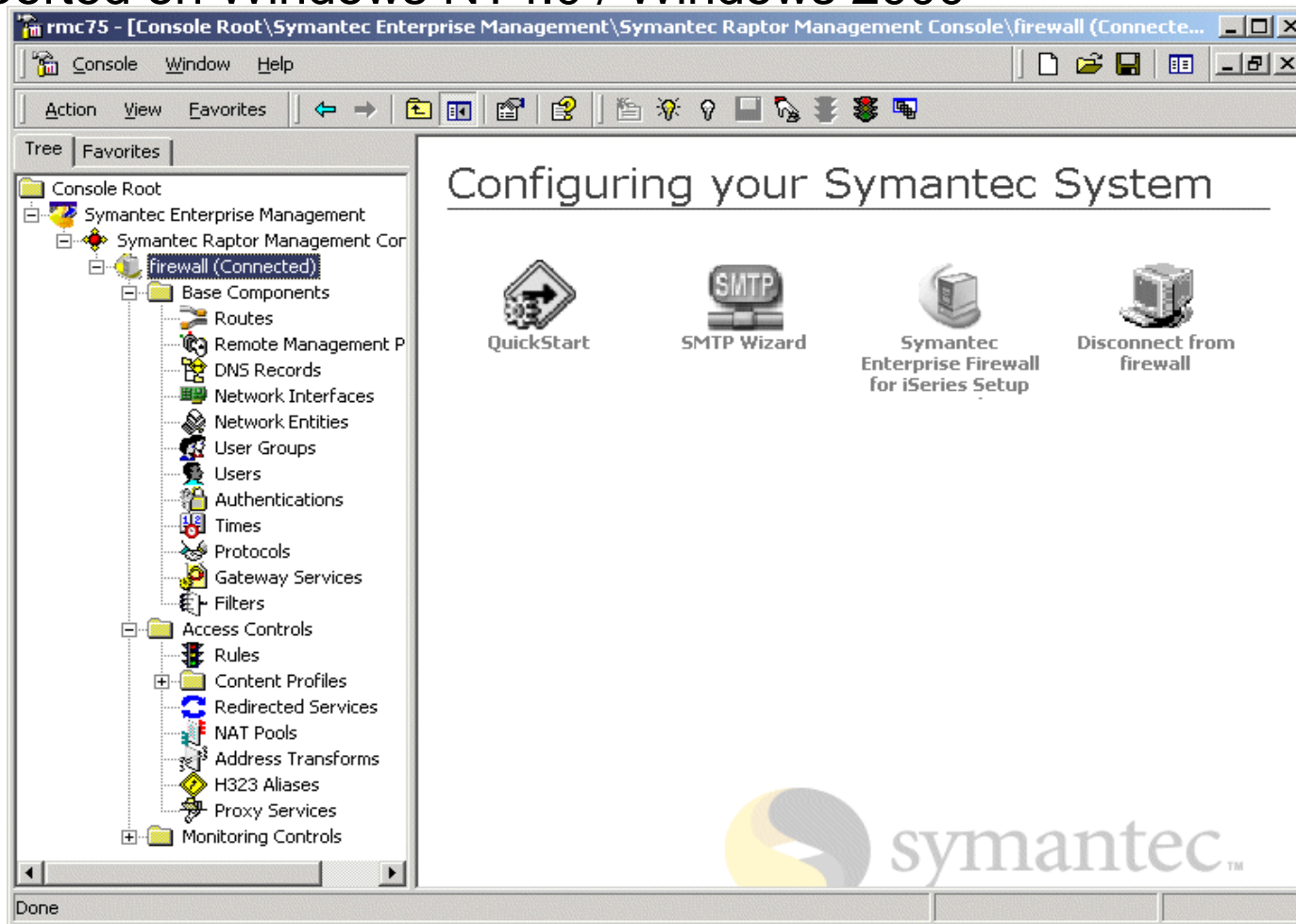
- ✓ Detailed logging facilities such as session duration, full URLs, user names and authentication methods
- ✓ Notification based on user defined events
- ✓ Diagnostic tools
- ✓ Web content filtering available with purchase of a license
- ✓ GUI configuration and easy to use setup wizards
- ✓ Remote management 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

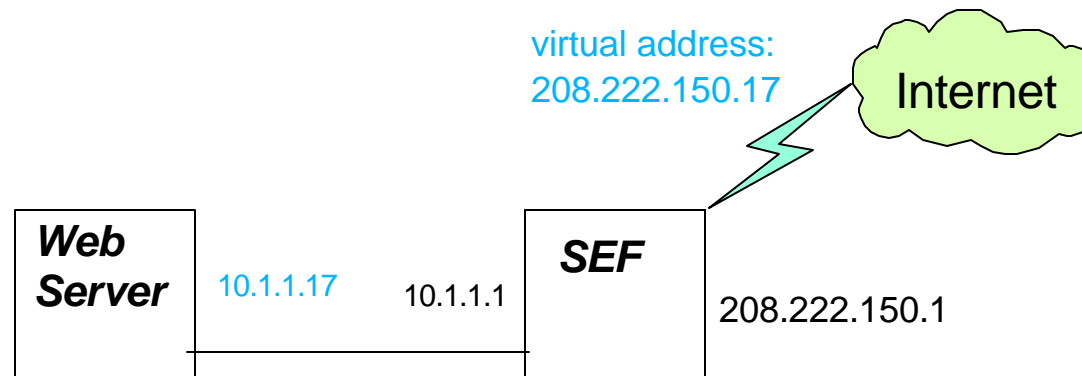
Features and Terminology



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



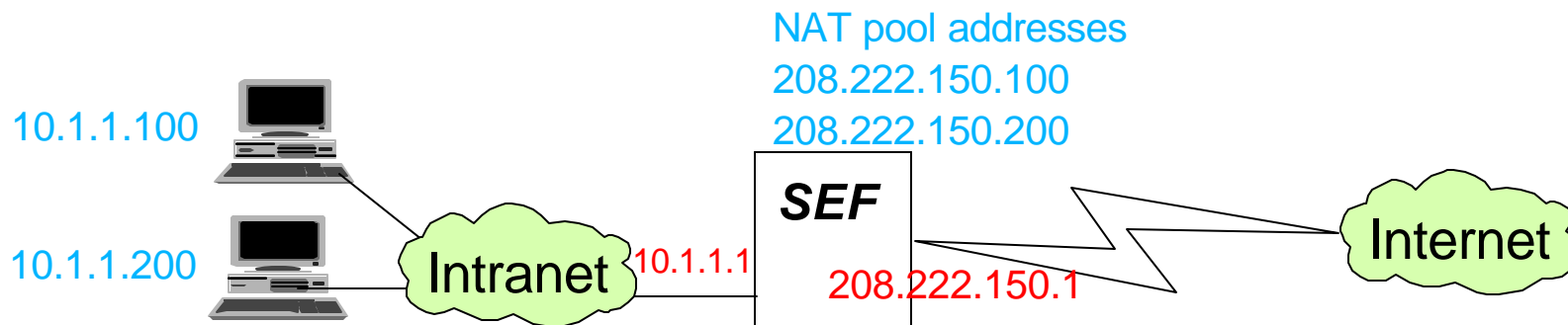
Features and Terminology



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



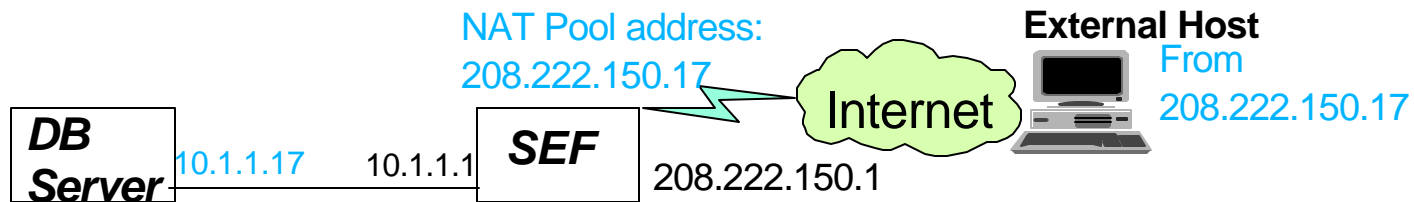
Features and Terminology



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:

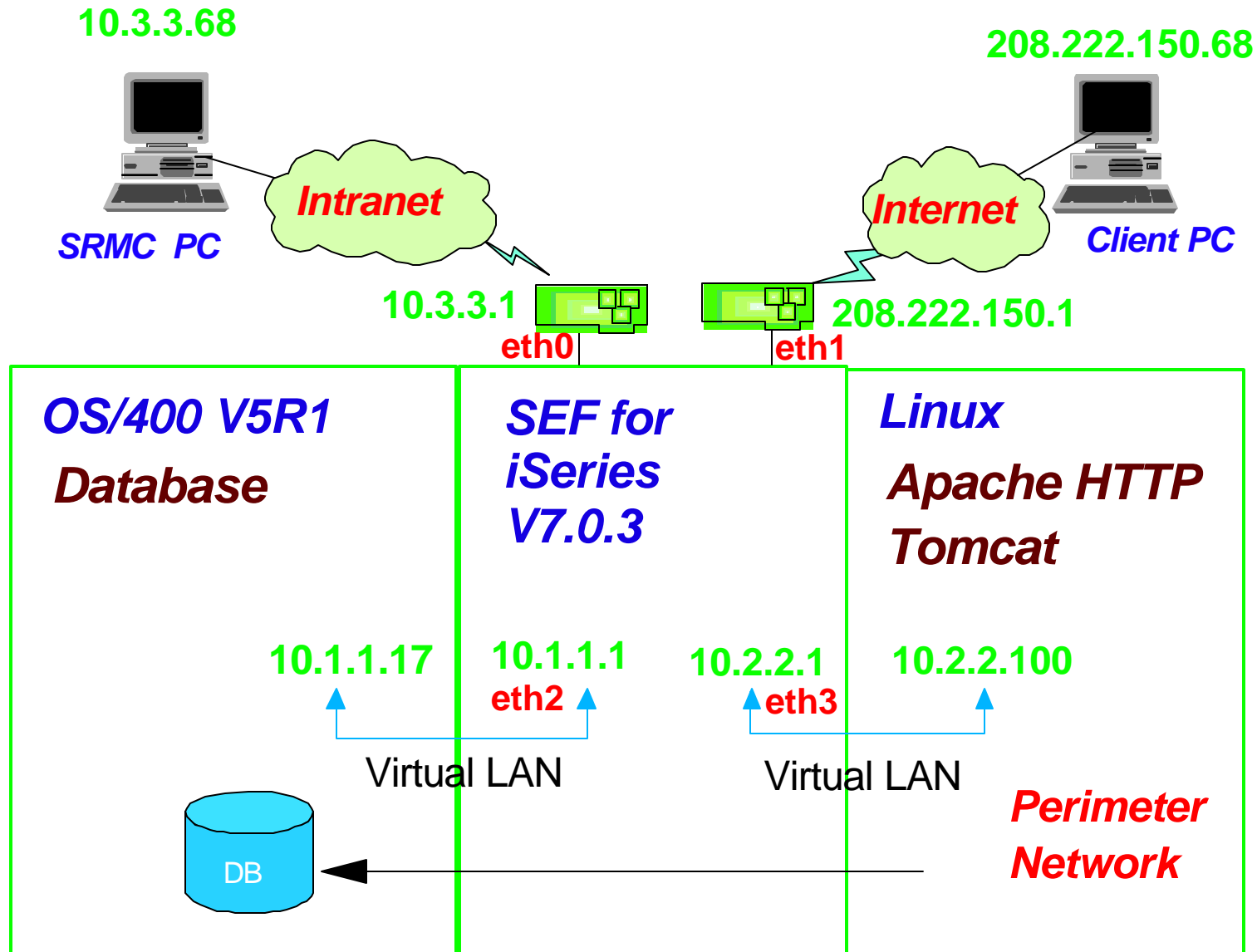
- FTP
- HTTP
- TELNET
- SMTP
- DNS
- NTP
- NNTP
- Ping
- CIFS
- GSPD
- NBDGRAM
- RTSP
- SQLNet
- H.32

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/series/vmlinux'
IPL parameters . . . . . : 'ks=file:/tmp/ks.cfg'
Text . . . . . : *BLANK
```

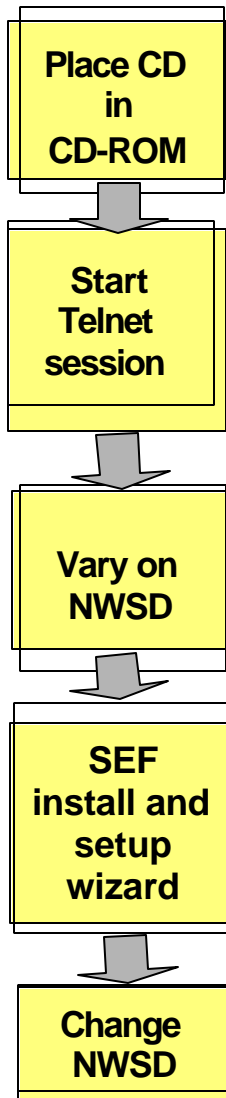
NWSD and NWSSTG



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



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

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 Enter

3. Vary on the NWSD object from a green screen

- 3a. Type WRKCFGSTS *NWS command
- 3b. Take Opt1 (Vary on)

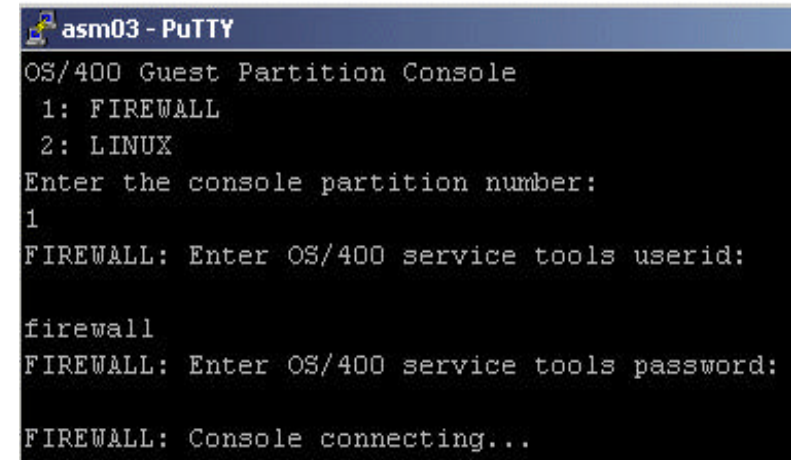
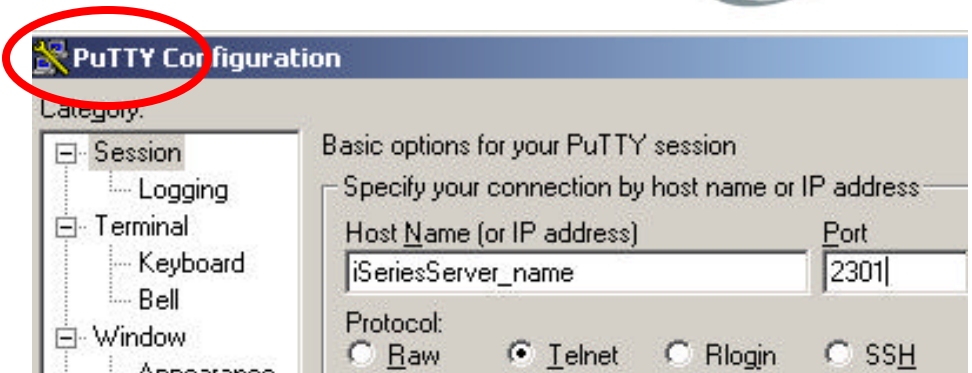
4. Setup wizard starts now. Follow the instructions.

- Configure network interface: IPaddress / Subnet mask
- Define the IP address and password for an SRMC client
- Reboot

5. Change NWSD

- 5a. Vary off the NWSD using Option 2 (Vary off) from WRKCFGSTS *NWS
- 5b. Change NWSD parameter as follows:

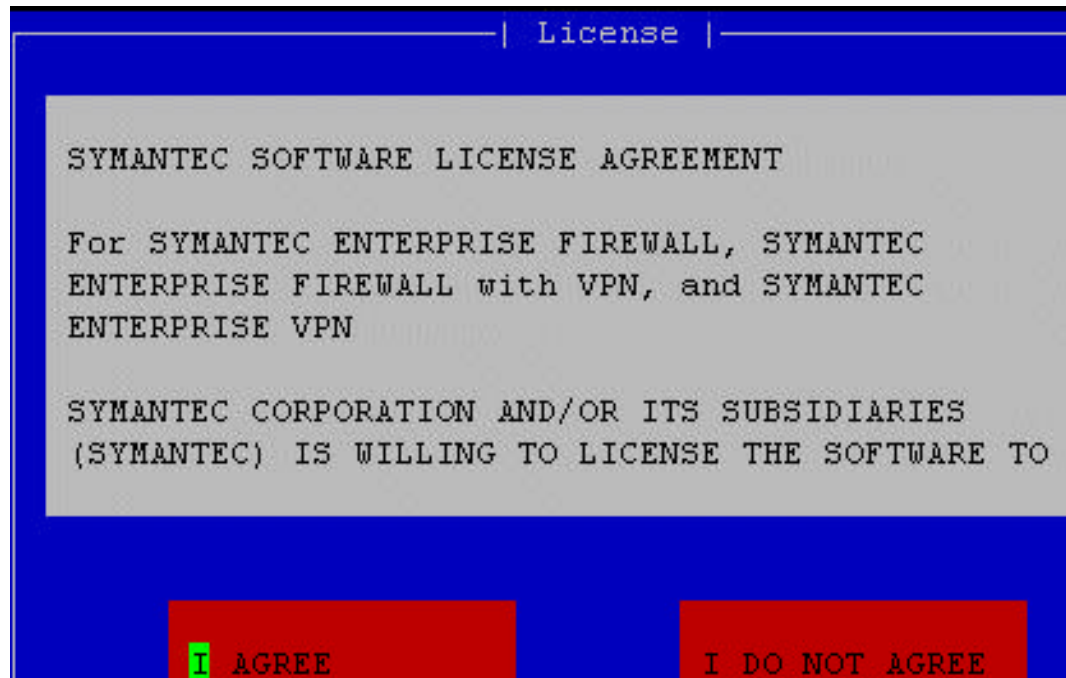
- IPL source: *NWSSTG / IPL stream file: *NONE / IPL parameters: *NONE



Step 1: Symantec SW License Agreement

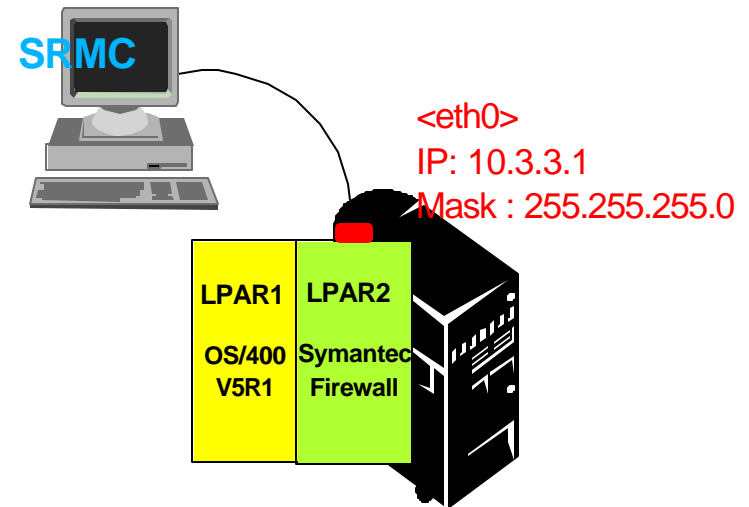
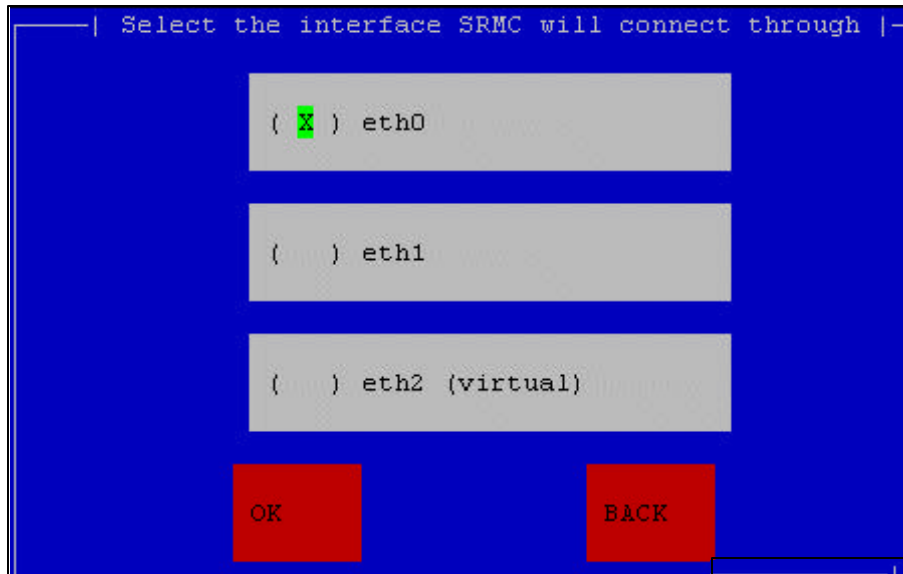


Varying on Firewall NWSD (Step 3 on previous chart) will automatically take you to this screen.



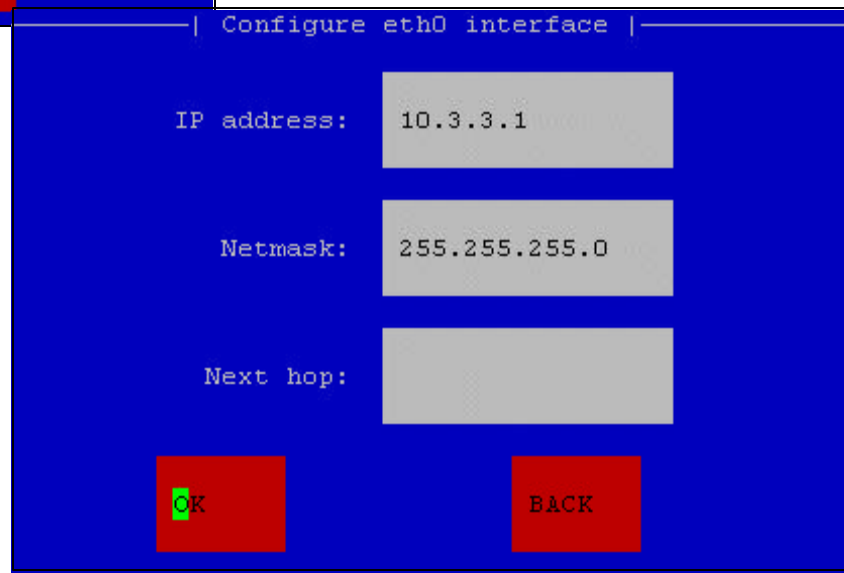
Read the license and choose your option. If you select I Agree, installation proceeds.

Step 2: Config Firewall Network Interface

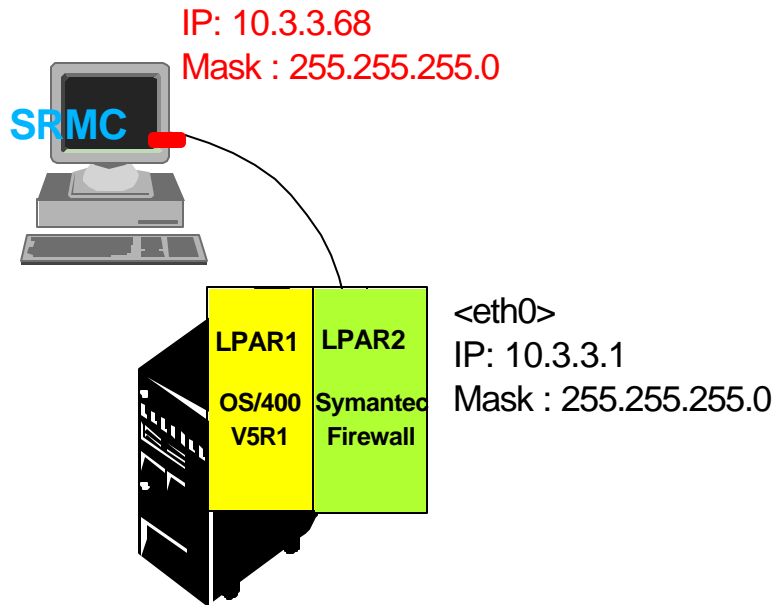


2a. Choose the interface the SRMC connects to.

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



Step 3: Config SRMC Network Interface



```
| Enter the SRMC IP address and password |
SRMC IP address: 10.3.3.68
SRMC Password: *****
Confirm SRMC password: *****
OK BACK
```

Enter IP address and password of the SRMC client.

Step 4: Set Password



```
| Set the root password for this system |
root Password: *****
Confirm root password: *****
OK BACK
```

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

4b. Set the SRL password.

```
| Set the SRL password for the firewall |
SRL Password: *****
Confirm SRL password: *****
OK BACK
```


Step 5: Save Configuration



```
| Save the setup |
Host ID           : 3d994134
Configured interface : eth0
IP Address        : 10.3.3.1
Netmask           : 255.255.255.0
Next hop          :
SRMC IP Address   : 10.3.3.68

SAVE             BACK
```

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.

```
asm03 - PuTTY
Symantec Enterprise Firewall V7.0.3 for iSeries
host login: █
```

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

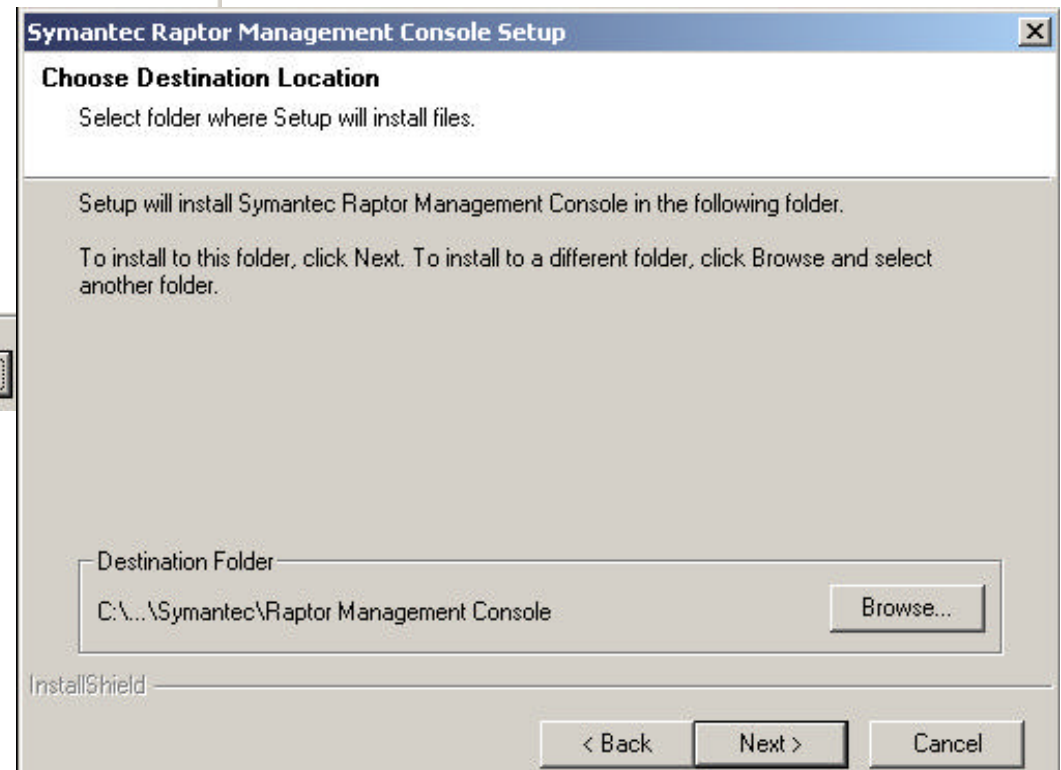
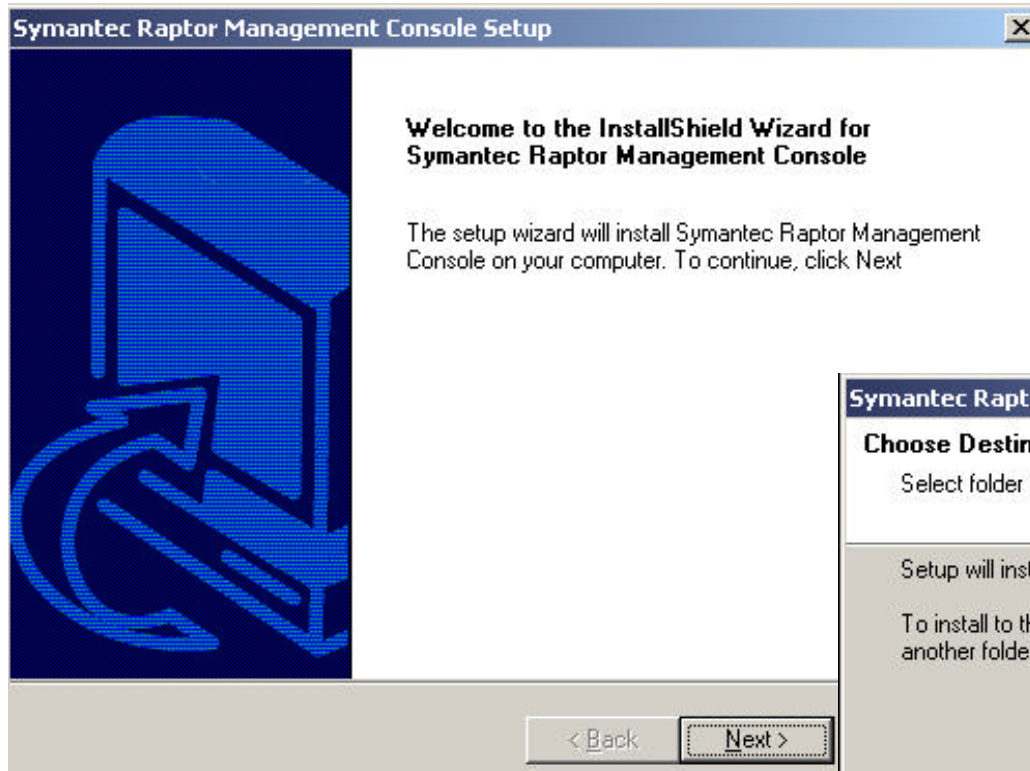
- Start the installation wizard by double clicking <ClientSoftware\SymantecRMC\Setup.exe> on the SEF installation CD
- Follow the installation wizard
- Start the SRMC by double clicking the icon on the desktop



★ To uninstall the SRMC, do the following:

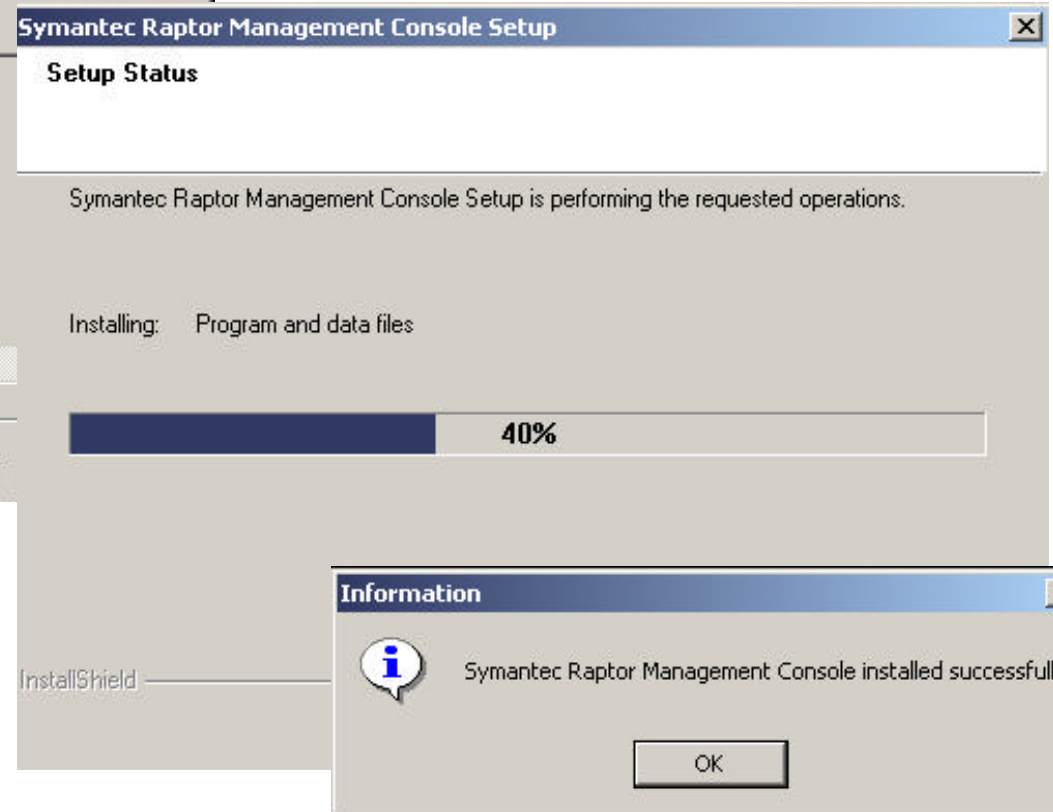
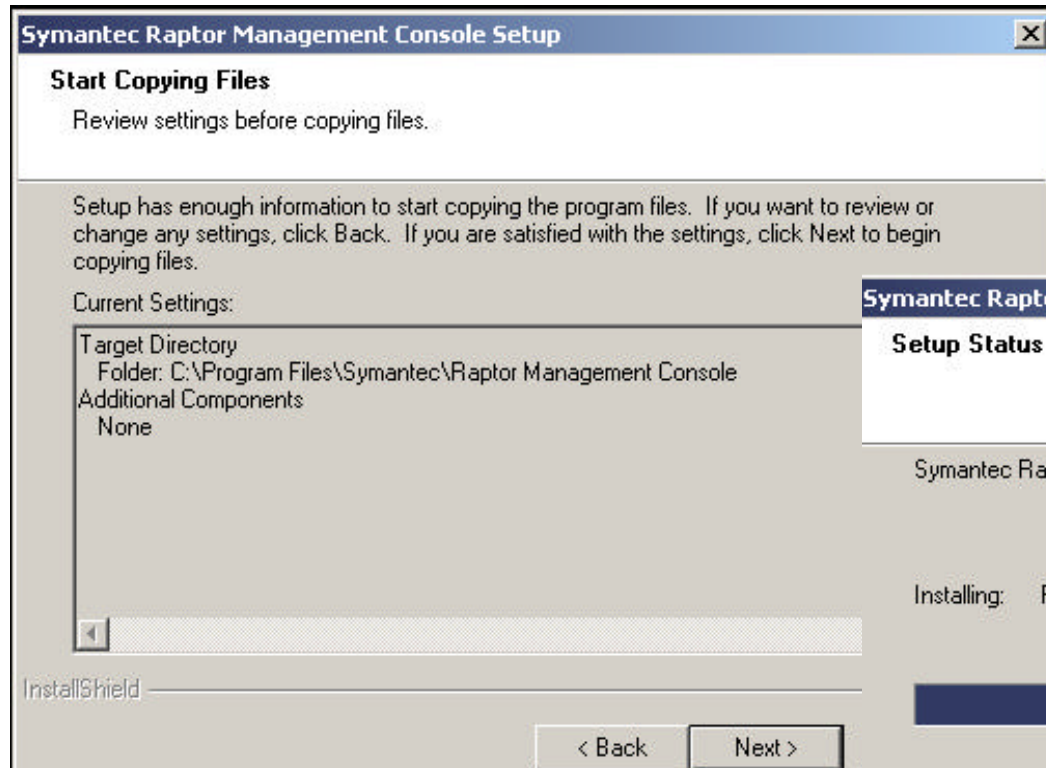
- Start -> Programs -> Symantec Raptor Management Console -> Uninstall Raptor Management Console
or
- Start -> Settings -> Control Panel -> Add/Remove Programs

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



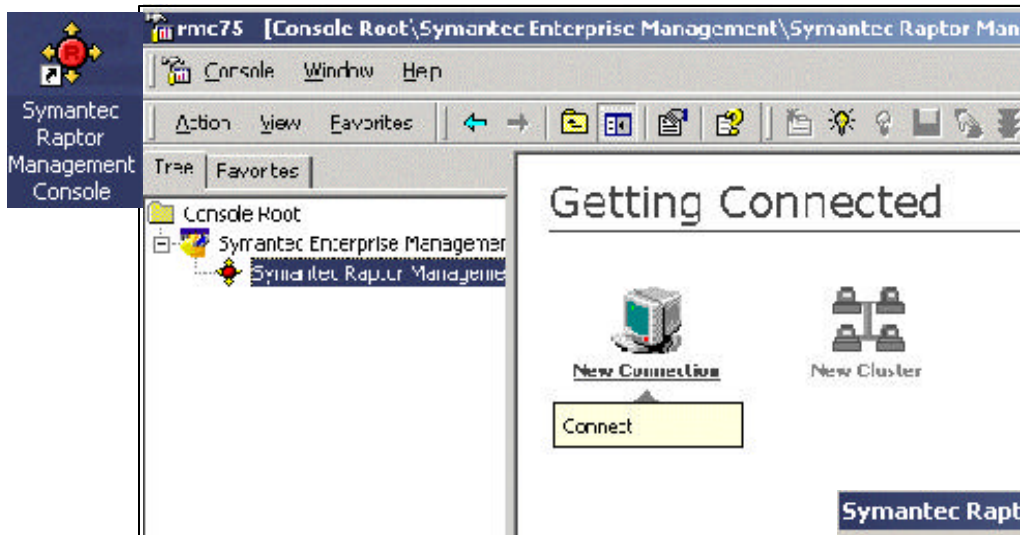
Connect the SRMC to the Firewall

- 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.

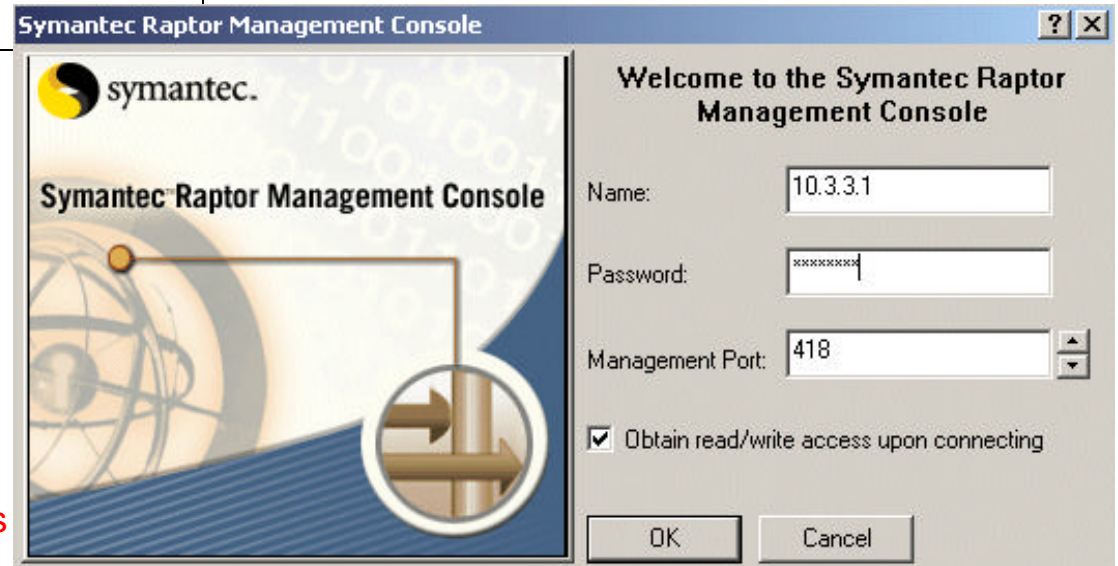
3. Sign on to the firewall.

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



The screenshot shows the Symantec Enterprise Management console interface. On the left is a tree view with 'firewall (Connected)' selected. The main area displays the 'Configuring your Symantec System' wizard with four icons: QuickStart, SMTP Wizard, Symantec Enterprise Firewall for iSeries Setup (circled in red), and Disconnect from firewall. A red arrow points from the text '1. Click Symantec Enterprise Firewall for iSeries Setup Wizard.' to the circled icon. Below this, a 'Setup Wizard' dialog box is open, titled 'Welcome to the Symantec Enterprise Firewall for iSeries Setup Wizard'. It contains instructions and a list of configuration items. A red circle highlights the 'Next >' button in the dialog's footer, with a red arrow pointing from the text '2. Click Next.' to it.

1. Click Symantec Enterprise Firewall for iSeries Setup Wizard.

2. Click Next.

SEF Basic Setup Wizard



Setup Wizard [X]

System Information
Specify the system information to be used by this system.

System name:

Domain name:

Default gateway IP:

License:

3. Type the system information.

4. Configure Network Interfaces.

Setup Wizard [X]

Network Interfaces
Specify the inside and outside network interfaces.

Network Interfaces:

Name	IP Address	Mask	Type	Description
eth0	10.3.3.1	255.255.255.0	Outside	Physical Interf...
eth1			Outside	Physical Interf...
eth2			Outside	Virtual Interface
eth3			Outside	Virtual Interface

Interface: IP address: Mask: Type:

Allow external ping to firewall

SEF Basic Setup Wizard



Setup Wizard [X]

Network Interfaces
Specify the inside and outside network interfaces.

Network Interfaces:

Name	IP Address	Mask	Type	Description
eth0	10.3.3.1	255.255.255.0	Inside	Physical Interf...
eth1	208.222.150.1	255.255.255.0	Outside	Physical Interf...
eth2	10.1.1.1	255.255.255.0	Inside	Virtual Interface
eth3	10.2.2.1	255.255.255.0	Inside	Virtual Interface

Interface: IP address: Mask: Type:

Allow external ping to firewall

Setup Wizard [X]

System's Date and Time
Set Date and Time of the system

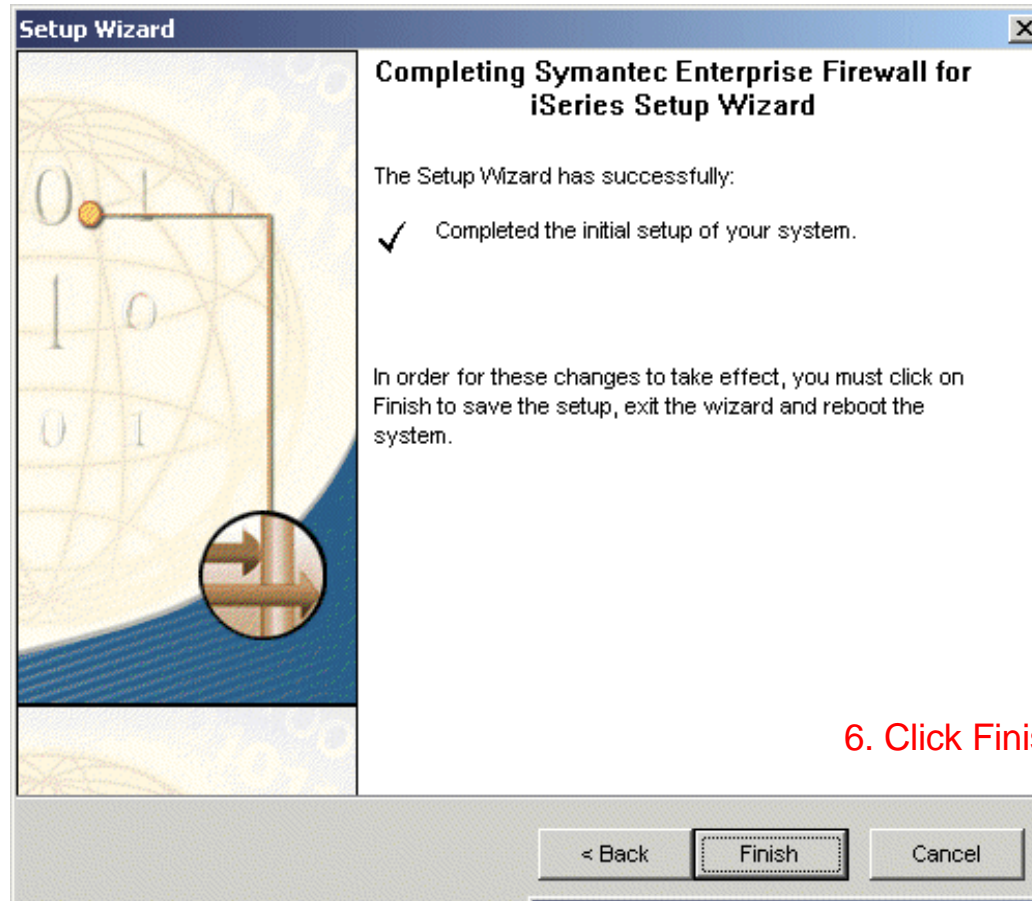
Set Date and Time

Date and Time:

Timezone:

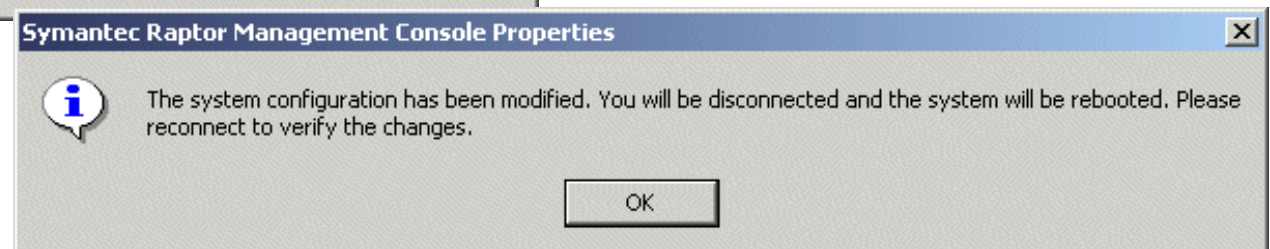
5. Set system's date and time

SEF Basic Setup Wizard

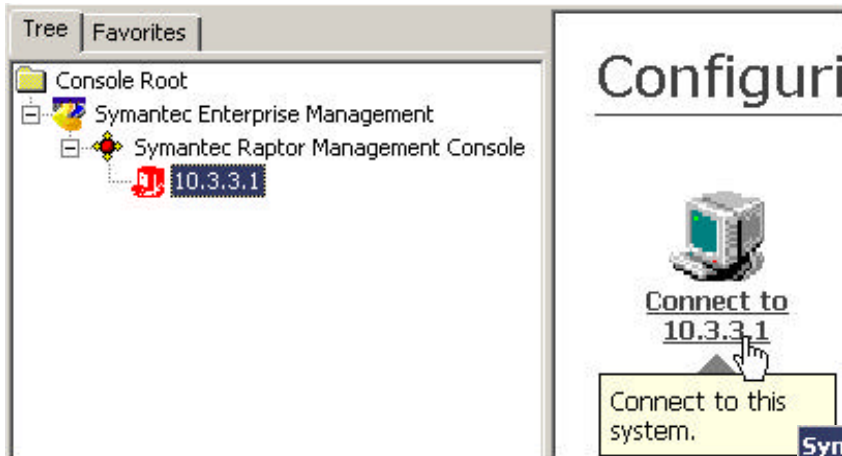


6. Click Finish.

7. The SEF reboots automatically.

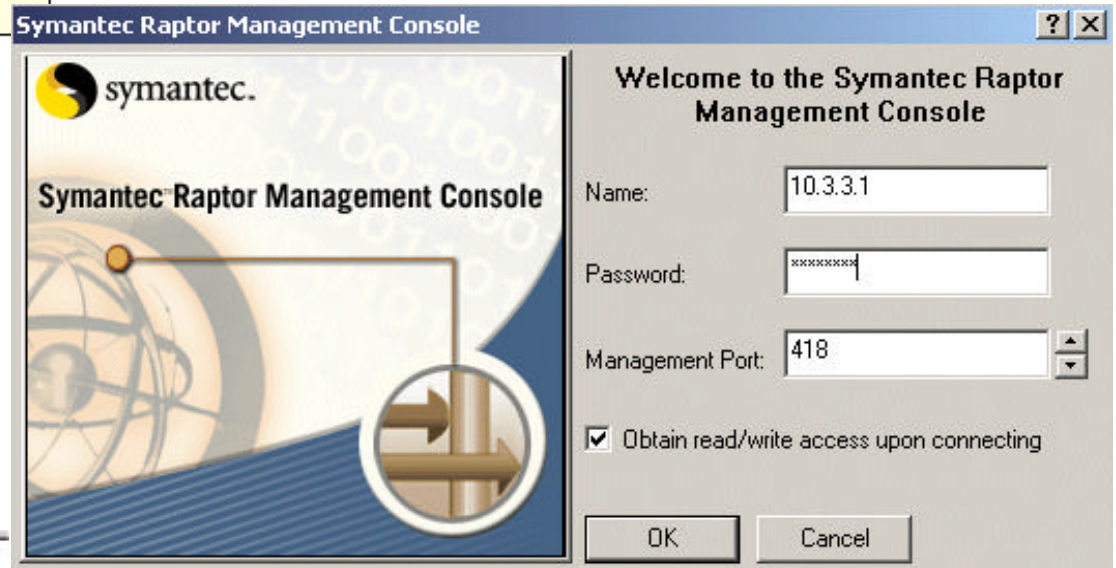


Connect to SEF

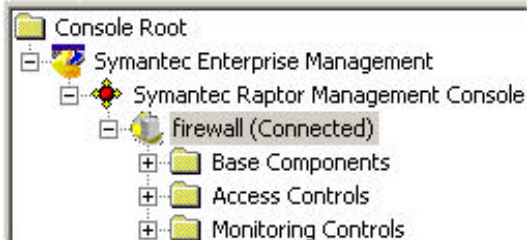


The Connection appears.
1. Click the created connection.

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



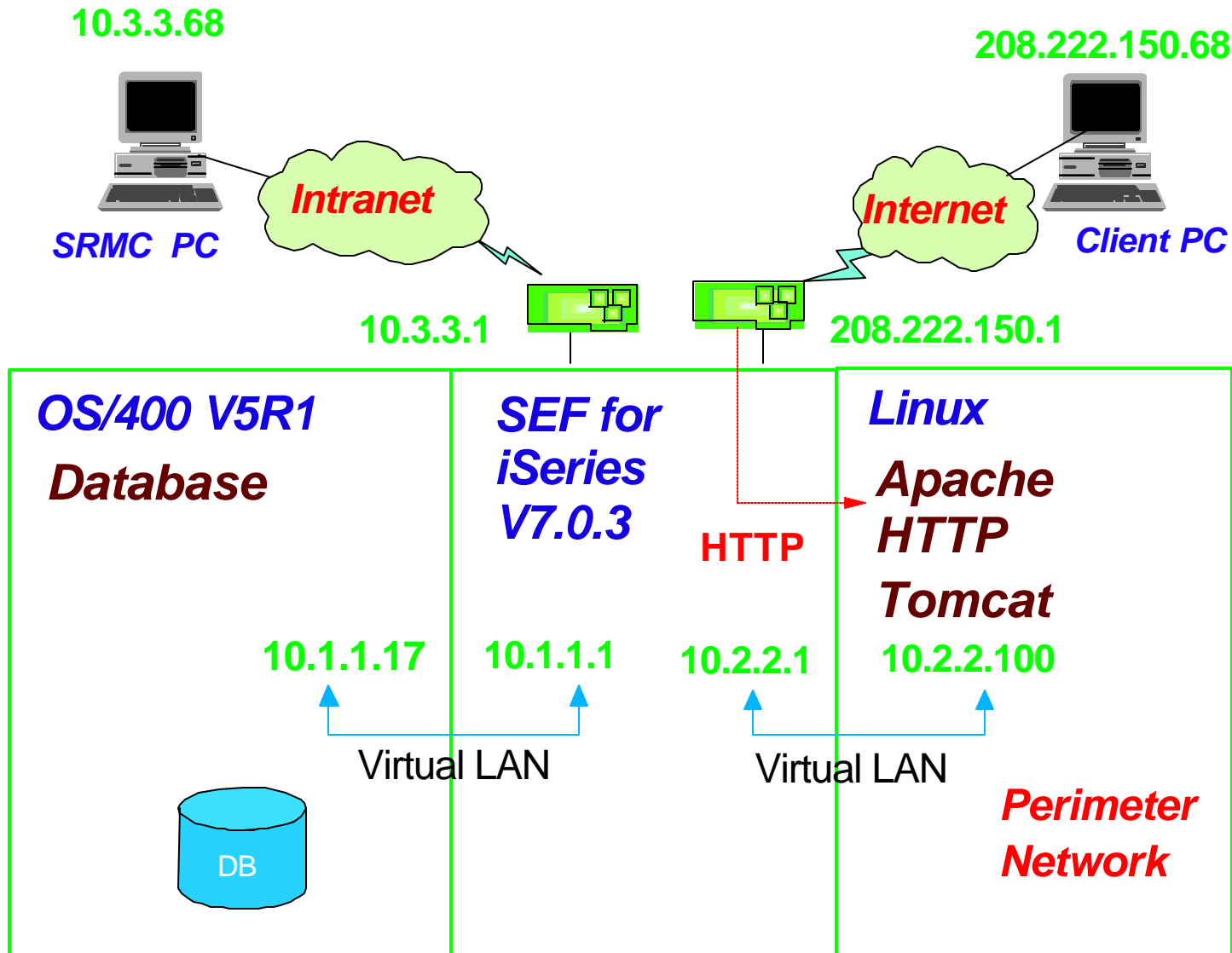
3. The SEF system accepts the connection, the folders appear on the SRMC screen.



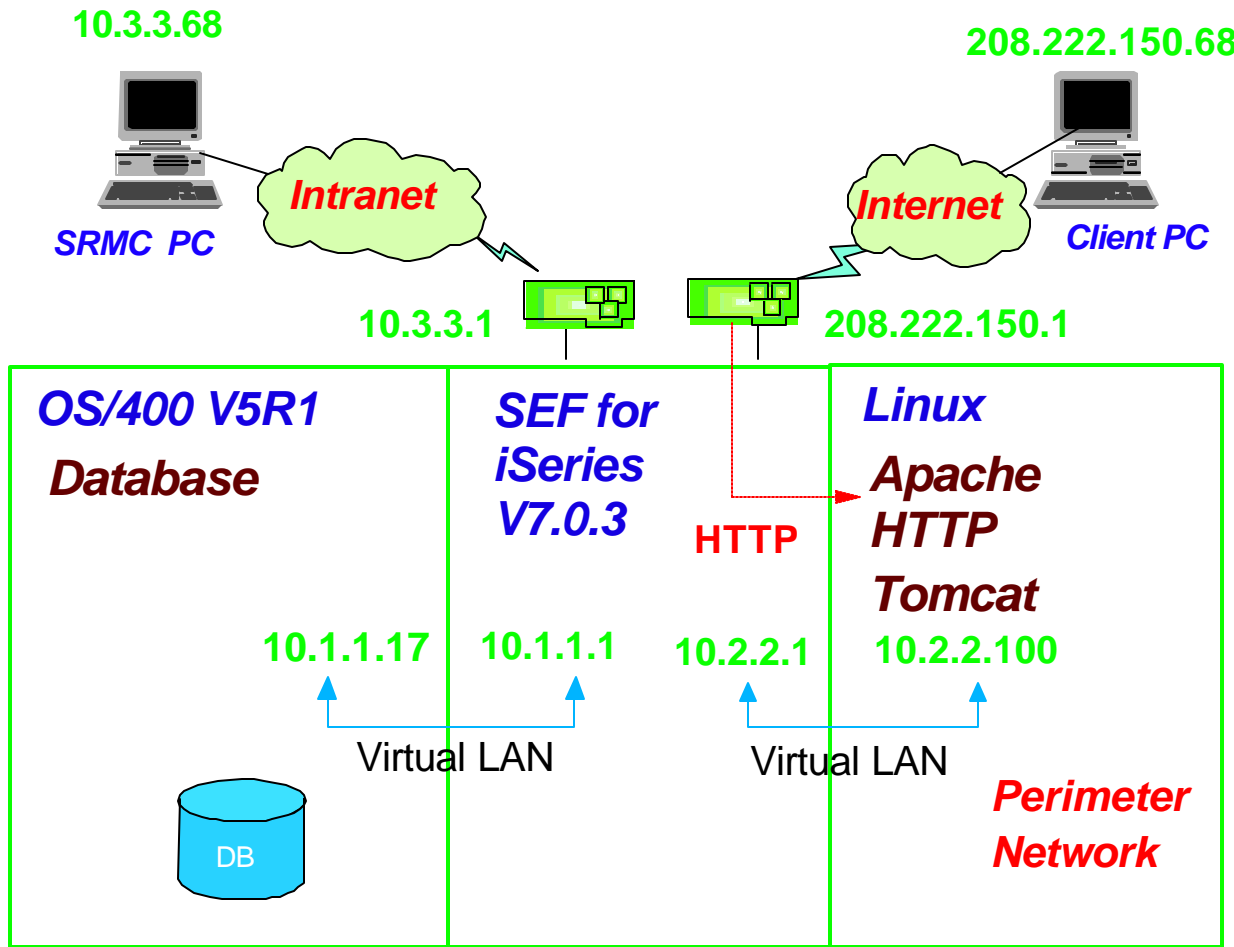


SEF for iSeries: Configuration Examples

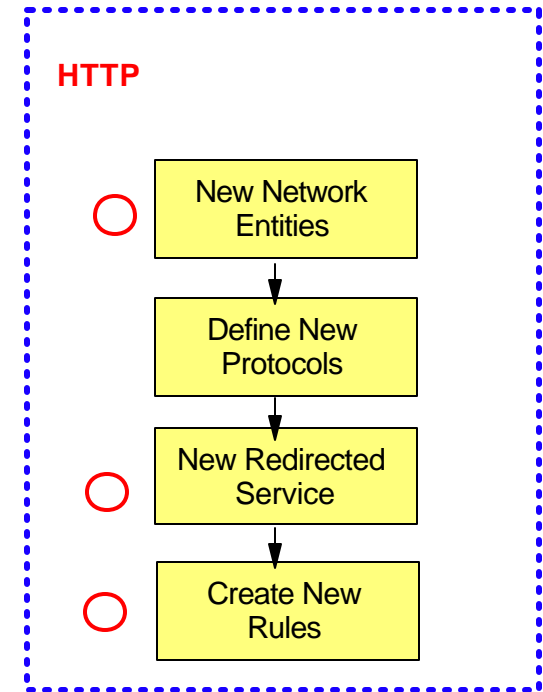
Configuration Example 1: HTTP



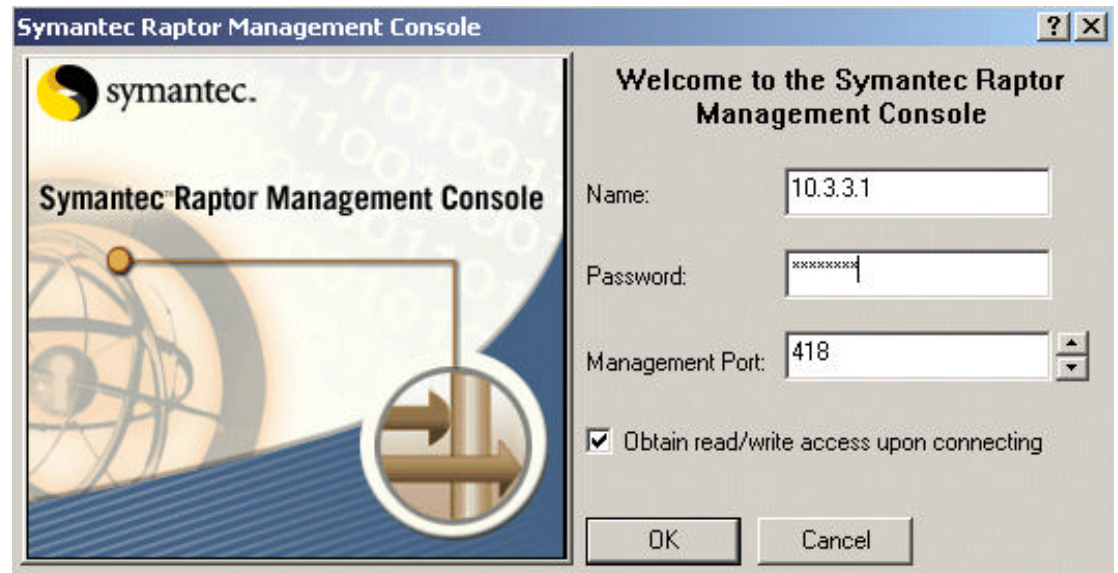
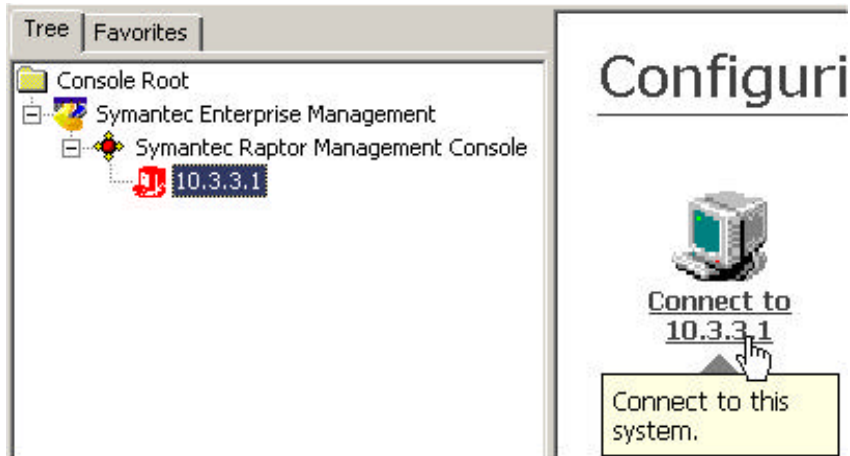
Configuration Example 1: HTTP



Steps:



First, Starting SRMC



Starting SRMC...continued



The screenshot shows the Symantec Raptor Management Console interface. The title bar reads "rmc75 - [Console Root\Symantec Enterprise Management\Symantec Raptor Management Console\firewall (Connecte...". The menu bar includes "Console", "Window", and "Help". The toolbar contains various icons for navigation and actions. On the left, a tree view shows the hierarchy: Console Root > Symantec Enterprise Management > Symantec Raptor Management Cor > Firewall (Connected). Under "Firewall (Connected)", the "Network Entities" folder is circled in red. The main pane displays "Configuring your Symantec System" with four icons: QuickStart, SMTP Wizard, Symantec Enterprise Firewall for iSeries Setup, and Disconnect from firewall. The Symantec logo is visible at the bottom right of the main pane.

Creating New Network Entities

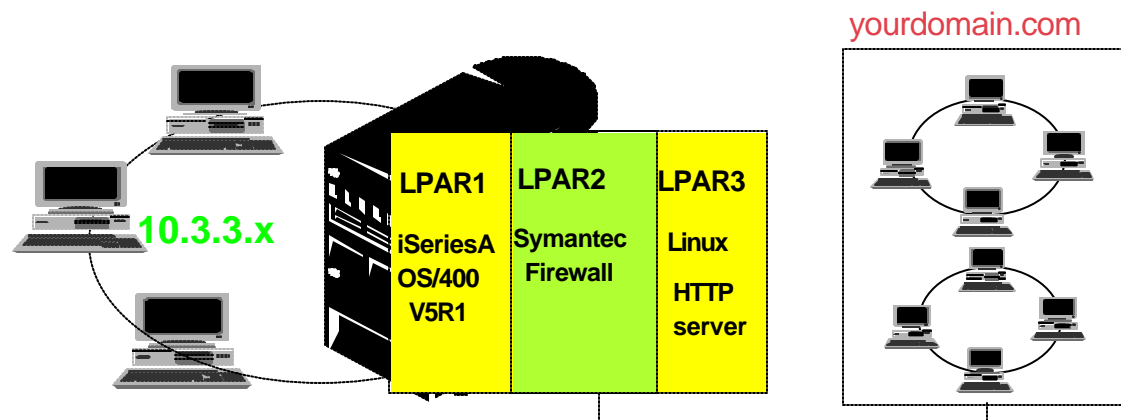
Step 1: Creating New Network Entity



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

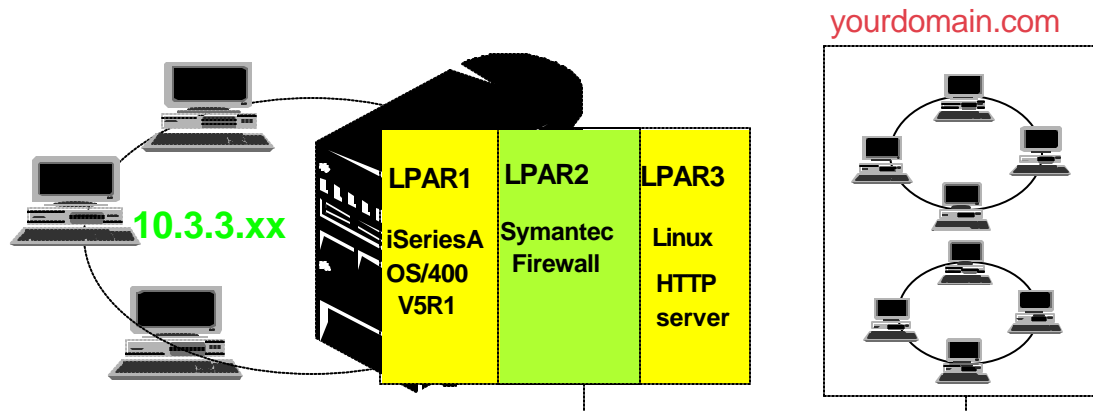


Step 1: Creating New Network Entity



Needed Network Entities for Configuration Example 1

- Host Entity: for Linux partition



Step 1: Creating New Network Entity



The screenshot shows the Symantec Raptor Management Console interface. The left pane displays a tree view of the management hierarchy, with 'Network Entity' selected. A context menu is open over 'Network Entity', showing options: 'New', 'All Tasks', 'View', 'New Window from Here', 'New Taskpad View...', 'Export List...', and 'Help'. The 'New' sub-menu is expanded, showing 'Host', 'Subnet', 'Domain', and 'Group'. The main pane displays a table with one entry:

Name	Type	Description	Address	Mask
Universe*	Host		0.0.0.0	

At the bottom of the console, a status bar reads: "Adds a new network entity."

Step 1: Creating New Network Entity



Creating Host type Network Entity for Linux partition

A screenshot of a Windows-style dialog box titled "firewall\Network Entity\Linux Properties". The dialog has three tabs: "General", "Address", and "In Use By", with "General" selected. Below the tabs is a printer icon and the text "Please enter a name and description and select the Network Entity type." There are three input fields: "Name:" with the text "Linux", "Description:" with the text "Linux partition with Apache and Tomcat", and "Type:" with a dropdown menu. The dropdown menu is open, showing a list of options: "Host" (which is highlighted with a blue background), "Subnet", "Domain", and "Group". A mouse cursor is pointing at the "Host" option.

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

A screenshot of a Windows-style dialog box titled "firewall\Network Entity\Linux Properties". It has three tabs: "General", "Address", and "In Use By". The "Address" tab is selected. Below the tabs, there is a small icon of a computer and a text box containing the instruction: "Please enter the IP address or DNS name, and optional MAC address for this Host. Entering a MAC address will associate the IP address with a specific network card." Below this instruction, there are two input fields. The first is labeled "Address:" and contains the text "10.2.2.100". The second is labeled "MAC Address:" and is currently empty.

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

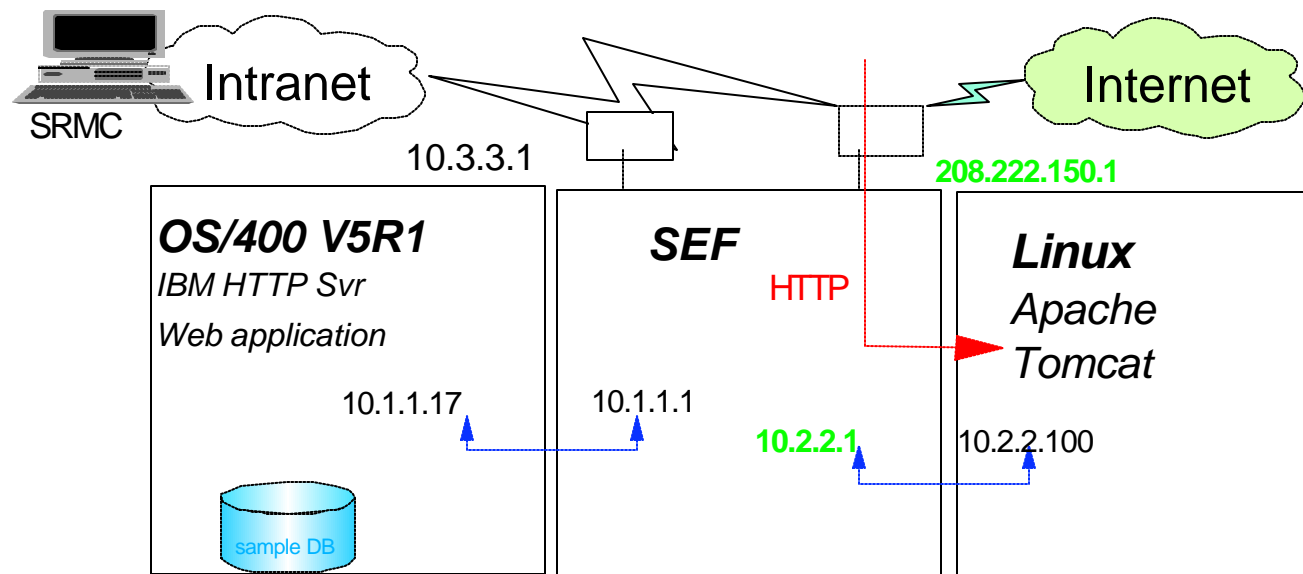
- You don't need to create new protocol.

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

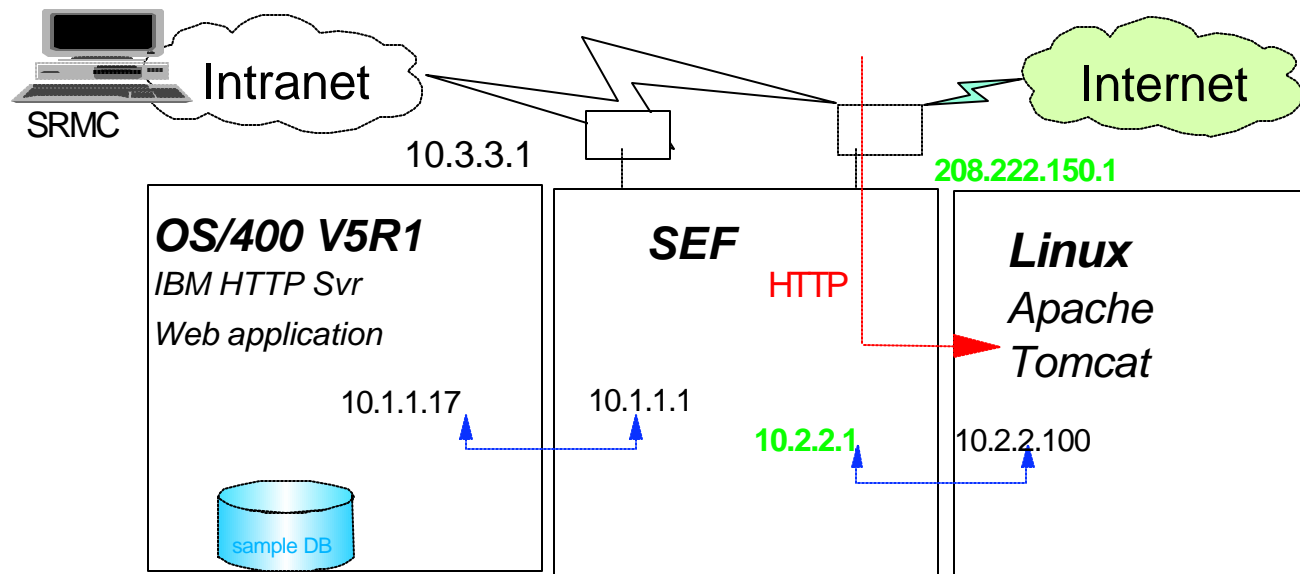


Step 3: Creating Redirected Service



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



The screenshot shows the Symantec Raptor Management Console interface. The left pane displays a tree view of the firewall configuration. The right pane shows a table with columns for ID, Requested Address, Mask, Service, and Redirected Address. A context menu is open over the 'Redirected Services' folder in the tree, with the 'New' option selected and a sub-menu showing 'Redirected Service' as the chosen option.

ID	Requested Address	Mask	Service	Redirected Address
----	-------------------	------	---------	--------------------

Step 3: Creating Redirected Service



firewall\Redirected Services\#6 : Redirecting All Services Pro... ? x

Service

Please select the service to be redirected, requested address and mask to which service requests are sent, and redirected address and port number.

Service: http

Requested Address: 208.222.150.1

Address Mask: 255.255.255.255

Redirect all gateway interfaces

Redirected Address: 10.2.2.100

Redirected Port:

OK Cancel Help

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** field.

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



firewall\Rule\Rule #5 Properties (New)

Alert Thresholds Miscellaneous Advanced Services
General Services Time Authentication

Please enter a description and select the Source, Destination and Access type.

Description:
Allow HTTP from the Internet to the Linux partition

For connections coming in via: eth1(208.222.150.1) From source: Universe*

Destined for: Linux Coming out via: eth3(10.2.2.1)

Rules can be written to allow or deny access to services:
 Allow Access To Services
 Deny Access To Services

OK Cancel Help

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.

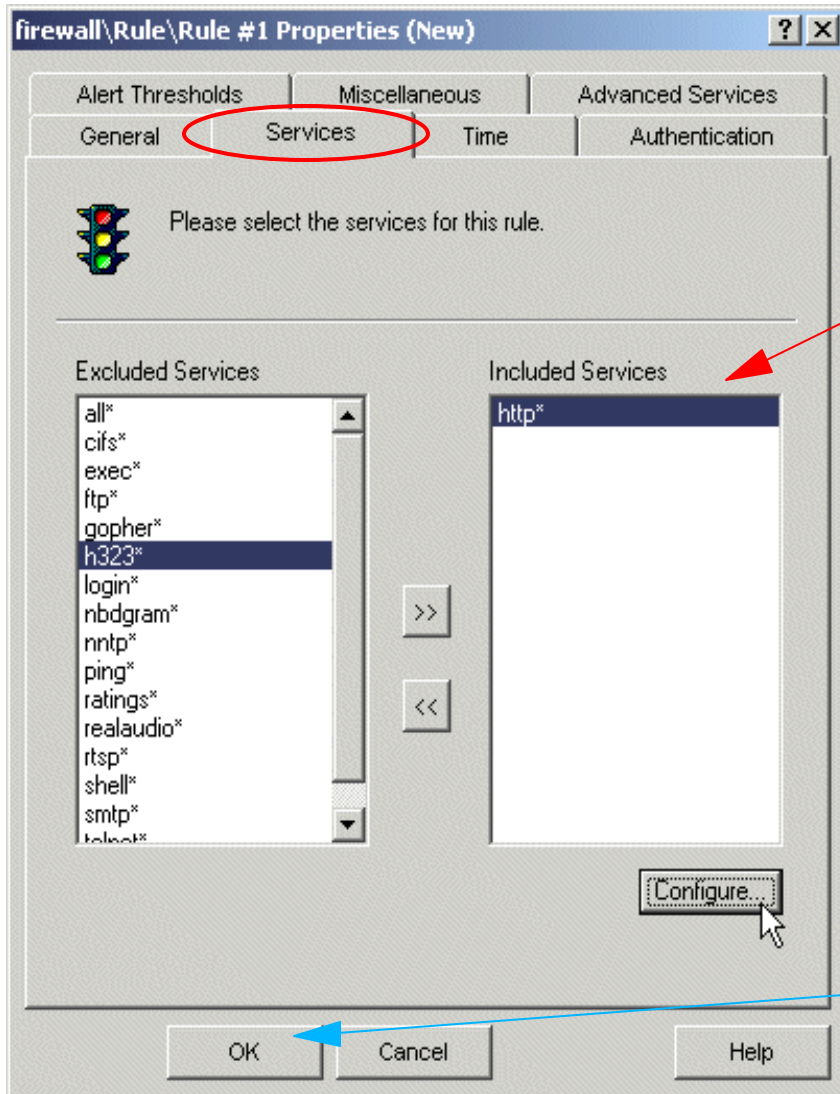
4c. Select **Universe*** for source field.

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.

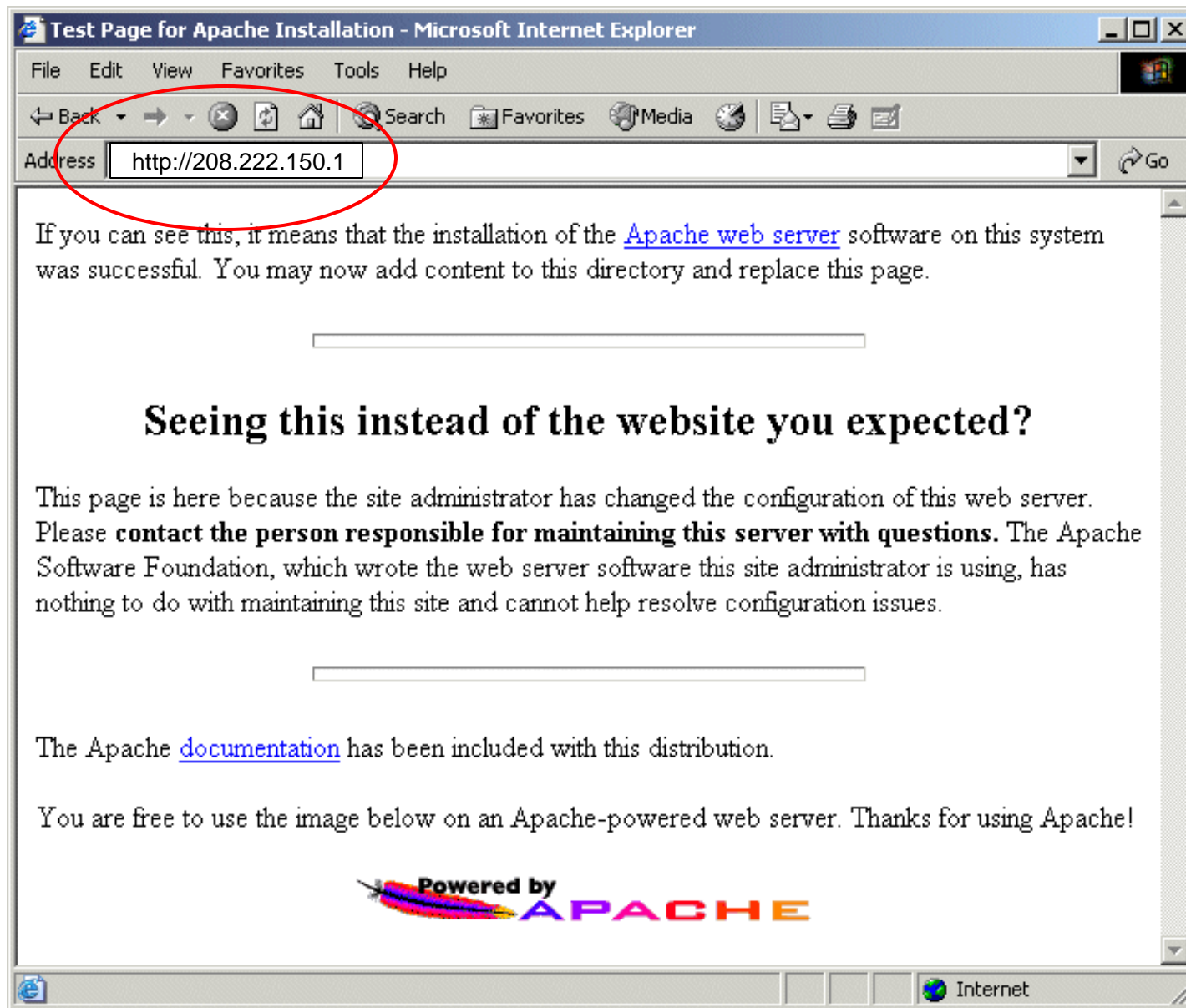
Saving Changes



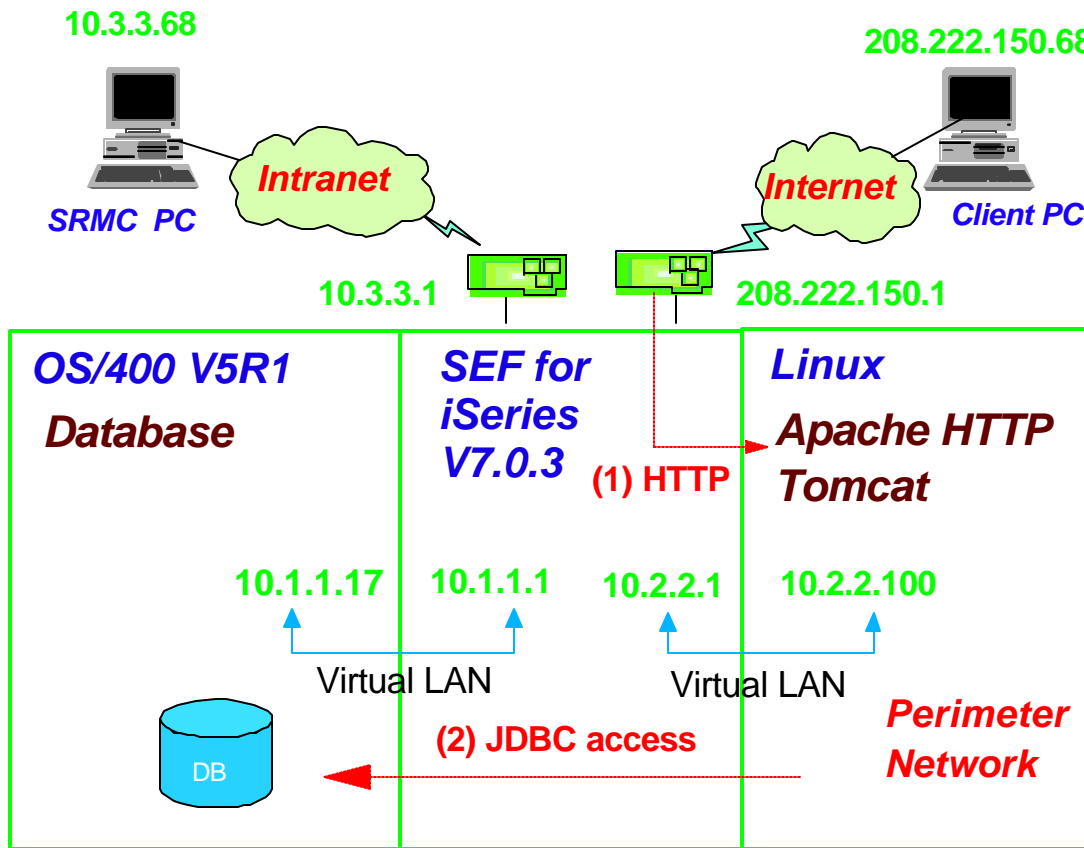
The screenshot shows the Symantec Raptor Management Console interface. The title bar reads "rmc75 - [Console Root\Symantec Enterprise Management\Symantec Raptor Management Console\firewall (Connecte...". The menu bar includes "Console", "Window", and "Help". The toolbar contains various icons, with a red circle highlighting the "Save and reconfigure" icon (a floppy disk with a refresh symbol). The left pane shows a tree view of the configuration hierarchy, with "Rules" selected under "Access Controls". The right pane displays a table of firewall rules.

Name	Description	In Via	Source	Destination	Out Via
Rule #1 : Universe* - Linux ...	Allow HTTP...	eth1	Univer...	Linux	eth3

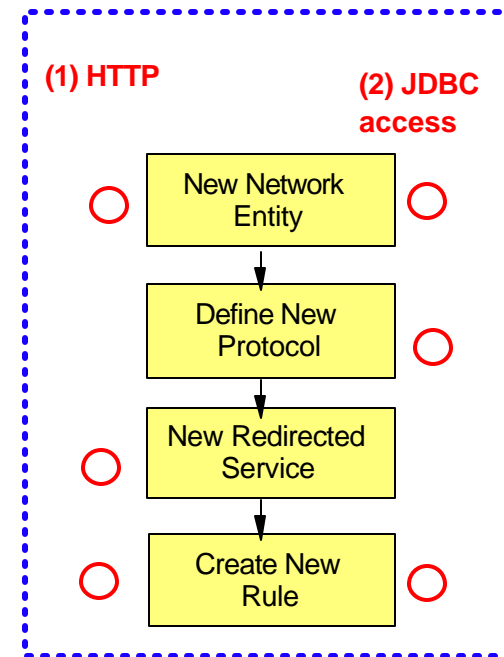
Test New Configuration Changes



Configuration Example 2: JDBC Access



Steps:



Step 1: Creating New Network Entities



firewall\Network Entity\Linux Properties

General | Address | In Use By

Please enter a name and description and select the Network Entity type.

Name: Linux

Description: Linux partition with Apache and Tomcat

Type: Host

- Host
- Subnet
- Domain
- Group

firewall\Network Entity\Linux Properties

General | Address | In Use By | **Host**

Please enter the IP address or DNS name, and optional MAC address for this Host. Entering a MAC address will associate the IP address with a specific network card.

Address: 10.2.2.100

Enter IP address

firewall\Network Entity\NewDomain Properties (New)

General | Name | In Use By | **Domain**

Please enter the DNS domain name for this domain.

Domain Name: yourdomain.com

Enter Domain name.

firewall\Network Entity\intranet Properties

General | Address | In Use By | **Subnet**

Please enter the details to describe the addressing of this Subnet.

Address: 10.3.3.0

Network Mask: 255.255.255.0

Enter the address and subnet mask.

- On General tab,
1. Enter name (entity name).
 2. Select type: Host / subnet / domain / group.

Step 1: Creating New Network Entities



firewall\Network Entity\NewHost Properties (New)

General | Address | In Use By

Please enter a name and description and select the Network Entity type.

Name:

Description:

Type:

(1) HTTP

Define Linux as a host entity.

firewall\Network Entity\NewHost Properties (New)

General | Address | In Use By

Please enter the IP address or DNS name, and optional MAC address for this Host. Entering a MAC address will associate the IP address with a specific network card.

Address:

MAC Address:

(2) JDBC access

Define iSeries as a host entity.

firewall\Network Entity\NewHost Properties (New)

General | Address | In Use By

Please enter a name and description and select the Network Entity type.

Name:

Description:

Type:

firewall\Network Entity\NewHost Properties (New)

General | Address | In Use By

Please enter the IP address or DNS name, and optional MAC address for this Host. Entering a MAC address will associate the IP address with a specific network card.

Address:

MAC Address:

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



The image shows a sequence of three screenshots from a firewall configuration interface. The first screenshot shows the 'New Protocol Properties (New)' dialog box on the 'General' tab. The 'Name' field is 'NewProtocol', 'Description' is 'creating new protocol', and 'Base Protocol' is set to 'TCP'. A dropdown menu is open, showing 'IP', 'TCP', 'UDP', and 'ICMP'. The second screenshot shows the 'Number' tab, where the 'Protocol Number' is set to '8'. The third screenshot shows the 'Message Type' tab, where the 'Message Type' is set to '8'. Green text annotations are present: 'in the case of IP' above the second dialog, 'in the case of TCP or UDP' above the third dialog, and 'in the case of ICMP' above the third dialog. Text annotations on the right side of each dialog provide instructions: 'Enter protocol number.', 'Enter destination port number and source port number.', and 'Enter message type.'

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

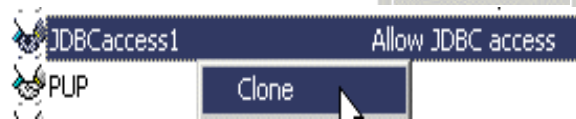


(1) **HTTP:** You don't need to configure protocol for HTTP because SEF provides it by default.

(2) **JDBC access**

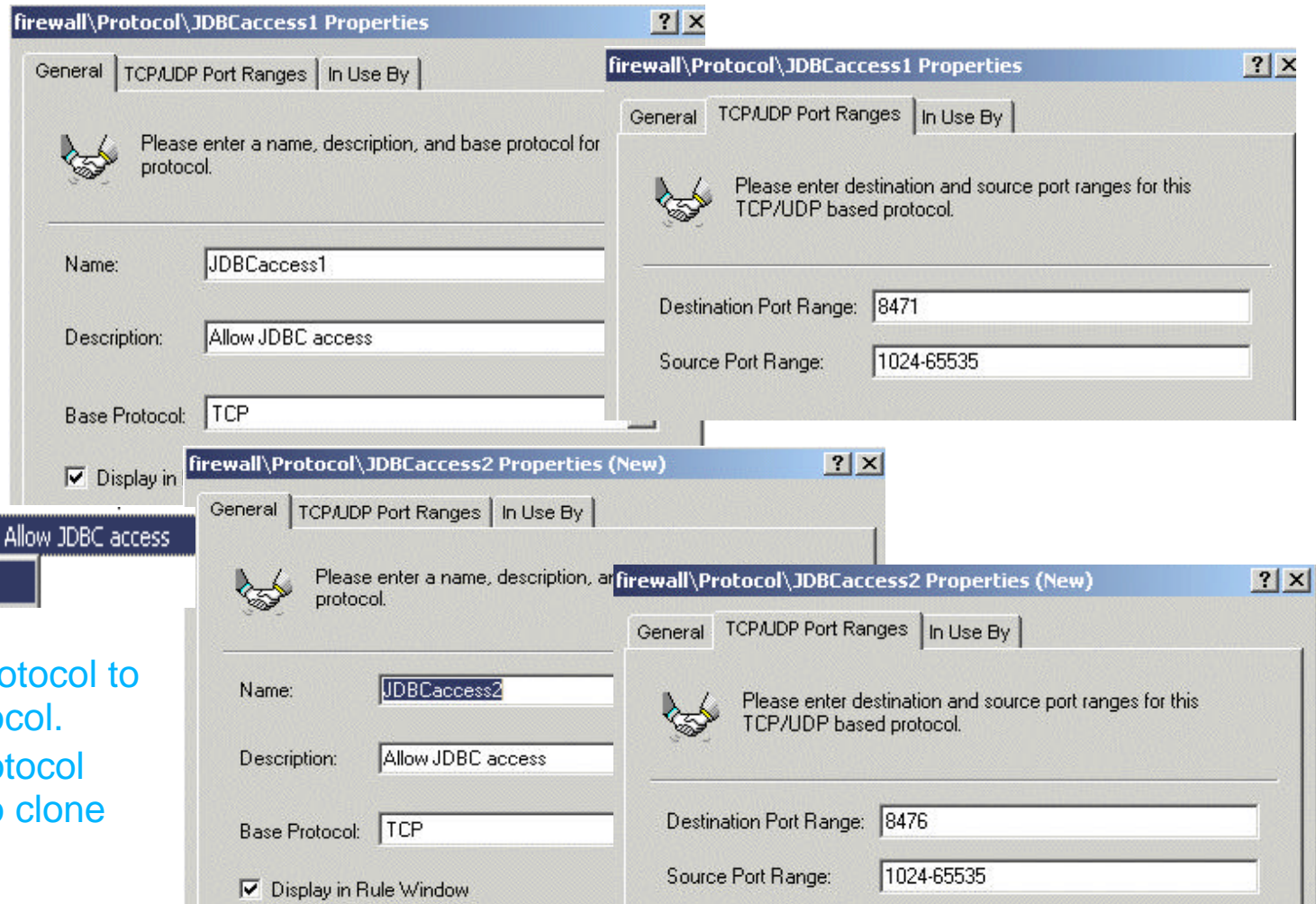
Define protocols
JDBC access
uses.

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

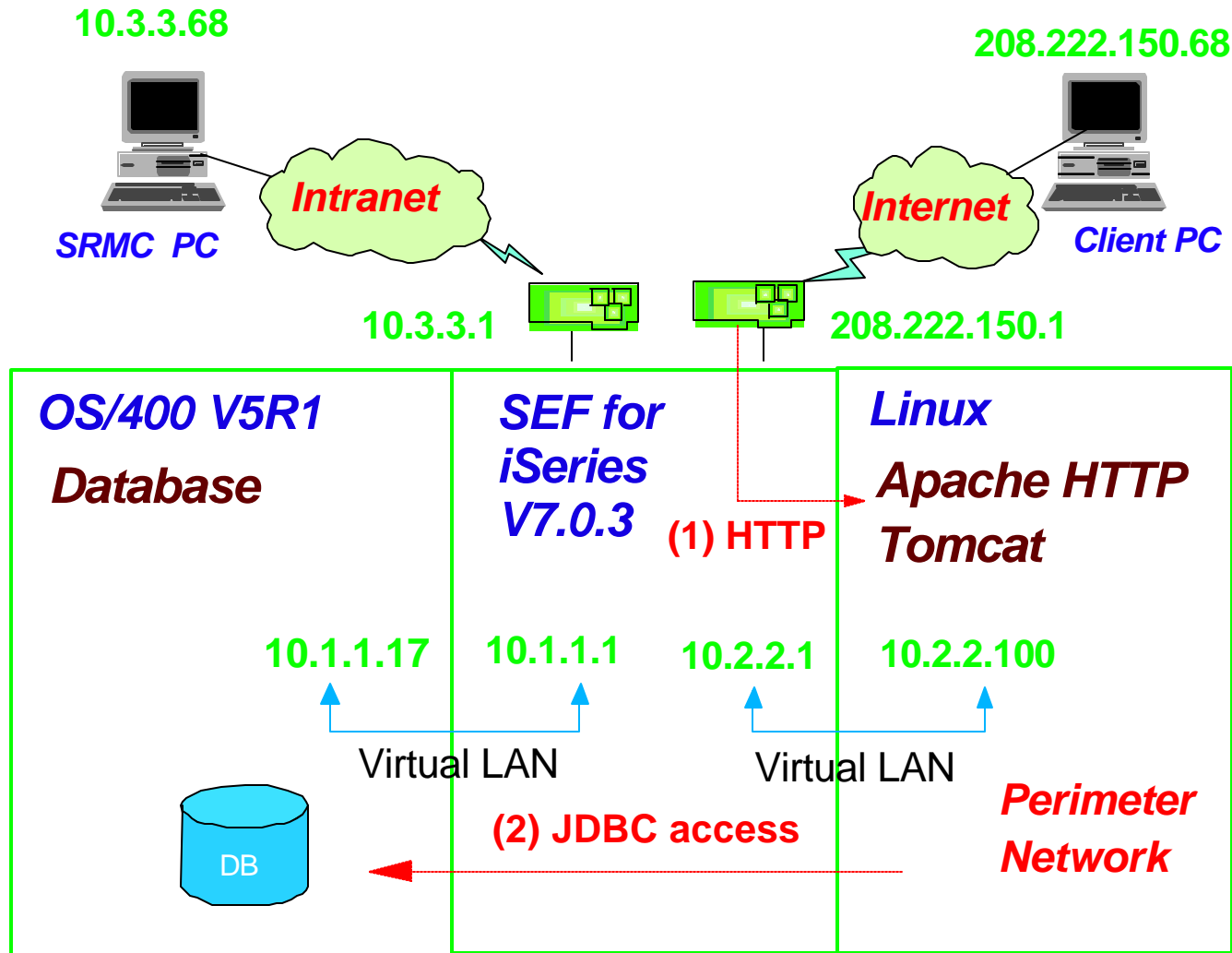


You can clone the protocol to create a similar protocol.

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



Step 3: Creating Redirected Services



Define Redirected Services

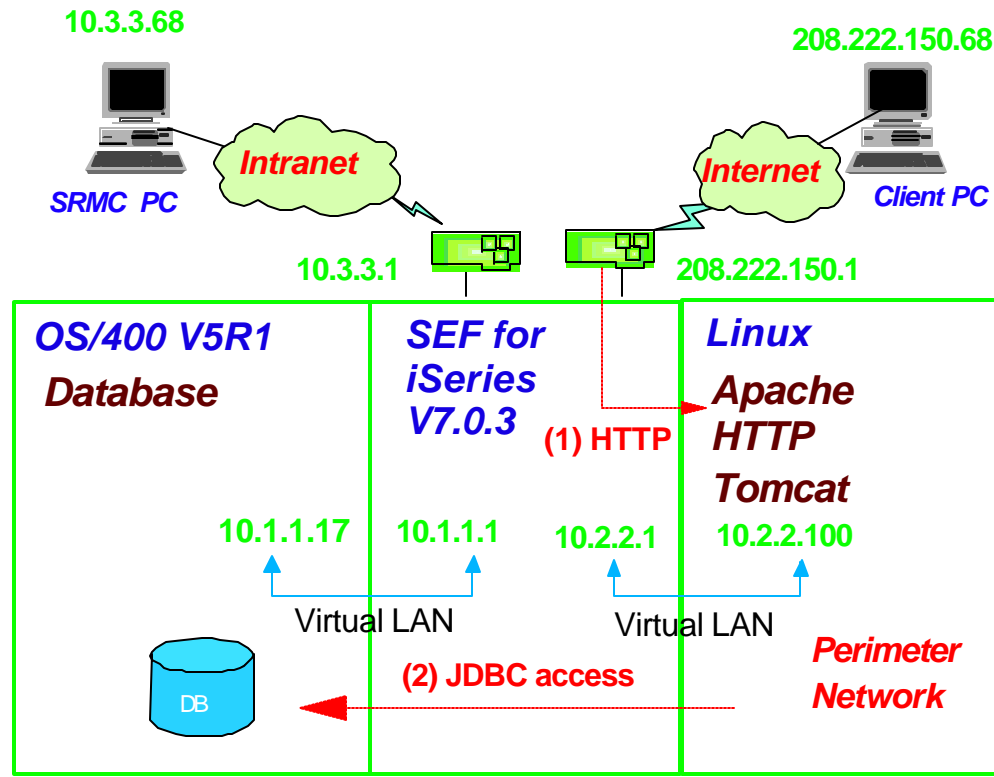


(1) HTTP

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

The screenshot shows the configuration for Rule #5. The description is "Allow HTTP from the Internet to the Linux partition". The source is "Universe*" and the destination is "Linux". The rule is applied to the "Services" tab, where "http*" is selected in the "Included Services" list.

(2) JDBC access

The screenshot shows the configuration for Rule #2. The description is "Allow JDBC access from Linux partition to iSeries server DB". The source is "Linux" and the destination is "iSeriesServer". The rule is applied to the "Services" tab, where "JDBCAccess1", "JDBCAccess2", and "JDBCAccess3" are selected in the "Included Services" list.



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.

The screenshot shows the Windows Firewall Logfiles folder in the Windows Explorer. The left pane shows the folder structure: firewall (Connected) > Base Components > Access Controls > Monitoring Controls > Notifications > Active Connections > Logfiles > September, 2002 > logfile, logfile.20020924, logfile.20020923. The right pane shows a list of log entries with columns for icon, description, source, and PID. An 'Event Properties' dialog box is open over the list, showing details for an 'Alert' event.

Icon	Description	Source	PID
Information	Inform...	firewall	readhawk 2352
Information	Inform...	firewall	readhawk 2298
Information	Inform...	firewall	readhawk 2352
Information	Inform...	firewall	readhawk 2352
Information	Inform...	firewall	readhawk 2352
Information	Inform...	firewall	readhawk 2352
Alert	Alert	firewall	readhawk 2352
Warning	Warning	firewall	gwc...
Alert	Alert	firewall	readhawk 2352
Information	Inform...	firewall	readhawk 2352
Information	Inform...	firewall	readhawk 2352

Event Properties

Event Details

STOP 09/23/2002 20:01:20.483

System: firewall

Event Type: Alert PID: 2352

Component: readhawk Message Number: 512

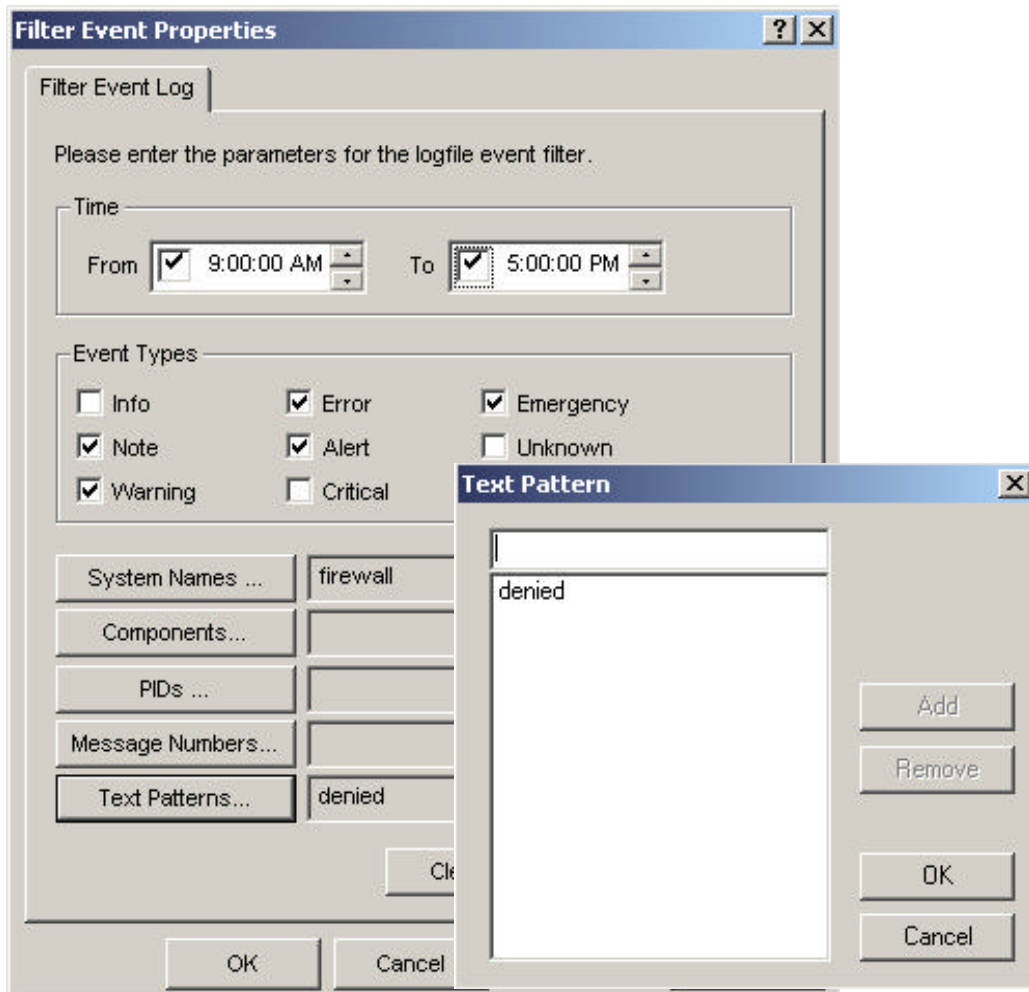
remote connect attempt from host 10.3.3.68 (no entry in remkeys -- access to remote management functions are denied)

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 including:
 - ▶ 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.

The screenshot shows the SEF Configuration Reports interface. On the left is a tree view with the following items: Notifications, Active Connections, Logfiles, Configuration Reports (expanded), Master Configuration Report, Authentication Report, Address Transform Report, Config.of Settings, DNS Records Report, Filter Report, H323 Alias Report, NAT Pools Report, Network Entity Report, Network Interface Report, Protocol Report, Proxy Services Report, Gateway Services Report, Redirect Services Report, and Rules Report. On the right is a detailed view of the Rules Report for Rule ID: 1. The details are as follows:

```
Rule ID: 1
Description: http access from 208.222.150.4 to iSeries
Access Mode: Allow
Services: http*
Service Limits: http http-allurl http-allext
Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
Advanced Services:
Application Scanning: 1
In Via: eth0
Out Via: eth1
Source: Universe*
Destination: iSeries
Time:
Authentication: gpasswd
User: AKIKOY
User:
Group:
Group:
```


Create reports on specific objects



The screenshot shows a network management console with a tree view on the left containing 'FW02 (Connected)', 'Base Components', 'Routes', 'Remote Management Passwords', 'DNS Records', 'Network Interfaces', 'Network Entities', 'User Groups', and 'Users'. A table at the top lists users:

Name	Description	Password	Groups	S/Key
AKIKO		Yes		No
AKIKOY		Yes		No

The 'FW02\User\AKIKOY Properties' dialog box is open, with the 'In Use By' tab selected. It displays a list of objects using this user:

```

Rule ID: 1
Description: http access from 208.222.150.4 to iSeries
Access Mode: Allow
Services: http*
Service Limits: http http-allurl http-allext
Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0 http:1 http-https:0 ht
Advanced Services:
Application Scanning: 1
In Via:
  Name: eth0
  Gateway: FW02
  Description: Physical Interface
  IP Address: 208.222.150.12
  ConnectedToInside: 0
  Illegal Address:
  Allow Multicast:
  SynFlood Protection:
  
```

A Notepad window titled 'YourConfiguration.txt - Notepad' is open, showing the copied script:

```

Rule ID: 1
Description: http access from 208.222.150.4 to iSeries
Access Mode: Allow
Services: http*
Service Limits: http http-allurl http-allext
Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0 http:1 http-https:0 ht
Advanced Services:
Application Scanning: 1
In Via:
  Name: eth0
  Gateway: FW02
  Description: Physical Interface
  IP Address: 208.222.150.12
  ConnectedToInside: 0
  Illegal Address:
  Allow Multicast:
  SynFlood Protection:
  
```

Annotations with green arrows point to the 'In Use By' tab, the selected script text, the 'View summary as Text' button, and the Notepad window.

Select and copy the script.

in Use By

Paste the script.

Click View as summary Text.

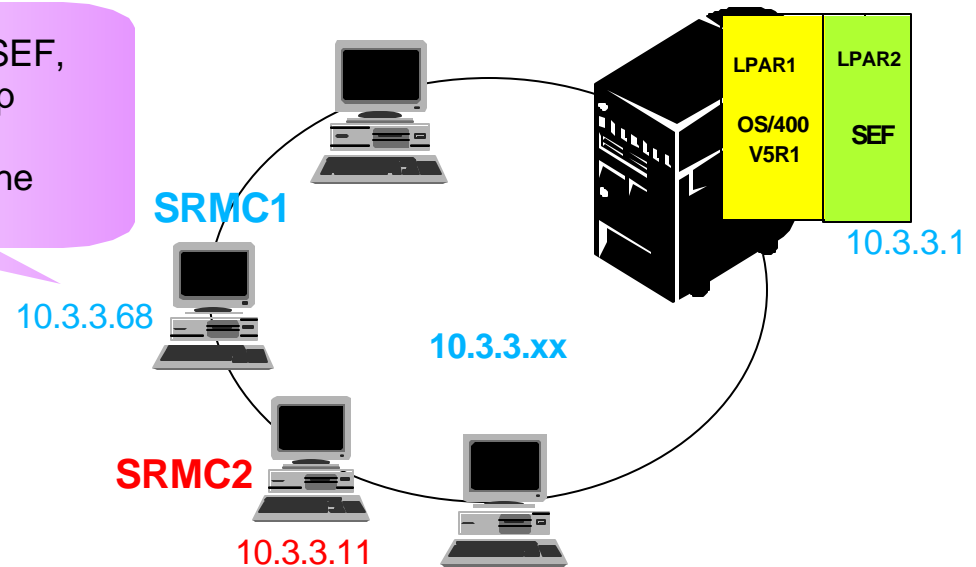
Configuring additional SRMC clients



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 : *****

A screenshot of a Windows dialog box titled "firewall\Remote Management Password\ Properties (New)". The dialog box has a tab labeled "Remote Management Password". Below the tab is a small icon of a mouse cursor pointing at a red padlock, followed by the text "Specify remote management type, system and password." The dialog box is divided into several sections. The first section is "Remote Management Type", which contains five radio buttons: "Remote Management" (selected), "Log Event Submission", "Intrusion Detection", "Logfile Retrieval", and "Read Only". Below this section is an "Intrusion Detection" section with two input fields: "Port Number:" with the value "426" and "Blacklist Timeout (minutes):" with the value "1440". The next section is "Remote Management System" with a text input field containing "10.3.3.11". The final section is "Remote Management Password" with a text input field containing "*****".

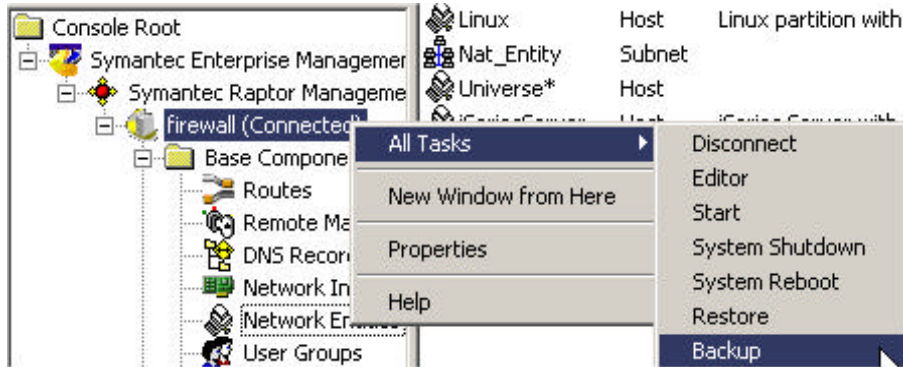
Backup and Recovery



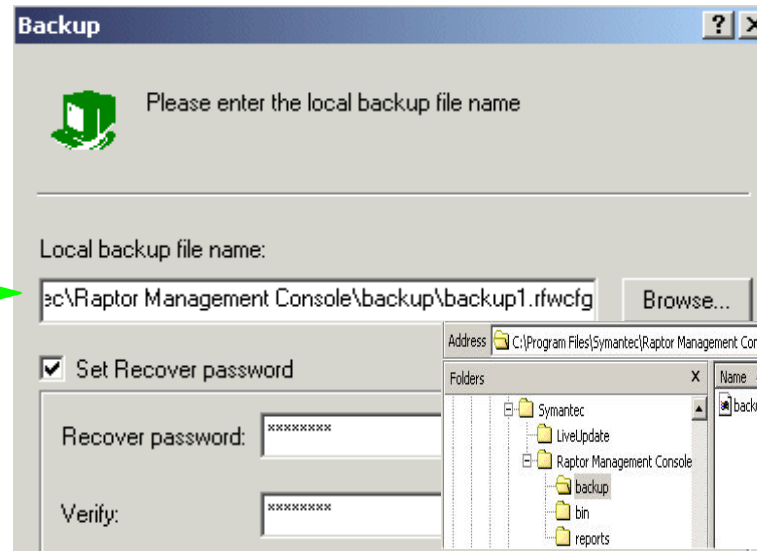
Two Ways for backup and recovery:

- 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



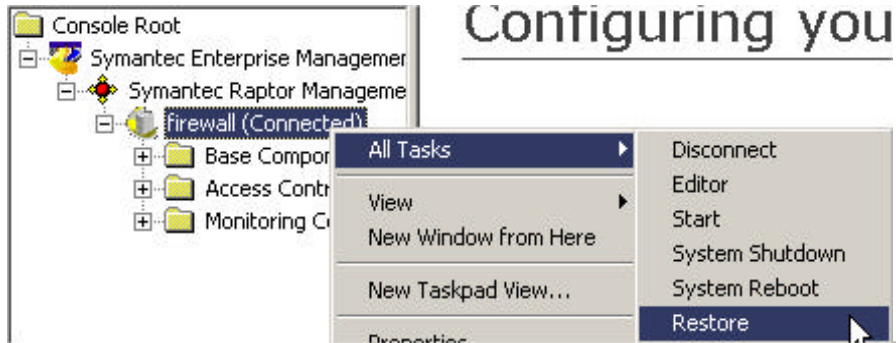
1. Right click any SRMC component and select All Tasks -> Backup.



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



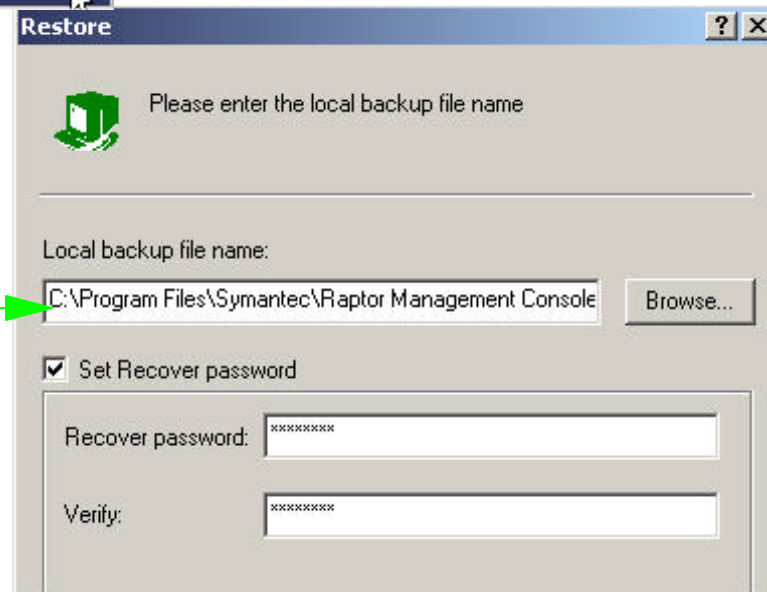
Configuring you

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

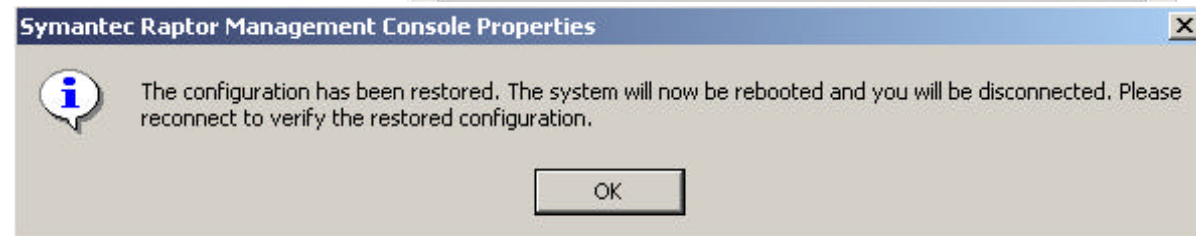
2. Browse to an existing filename or type in the backup file name.

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>