هوالمحبوب

طریقه Block کردن IP ها و DNS ها توسط IPSEC

نویسنده : حسین عسگری

مقدمه :

در ویندوز های سری 2000/XP/2003 یک سیستم محافظتی پروتکل TCP/IP قرار داده شده است که به اختصار آن را IPSEC مینامند . (IP Security)

شرح کار کرد IPSEC بسیار گسترده میباشد که از جمله آنها می توان :

- آنالیز کزدن packet های IP ورودی و خروجی (برای حصول اطمینان از Normal بودن آنها
- Block کردن IP ها / Packet های ICMP به انواع و اقسام (Internet , Internet)
- Block کردن ترافیک برای هر پورت دلخواه و برای هر سیستم
- و .....

طریقه استفاده از آن در شکل های زیر همراه با توضیحی مختصر آمده است :

شروع (بلاک کردن IP مزاحم برای پورت ۸۰ و ٤٤٣) :

Start > Run > MMC

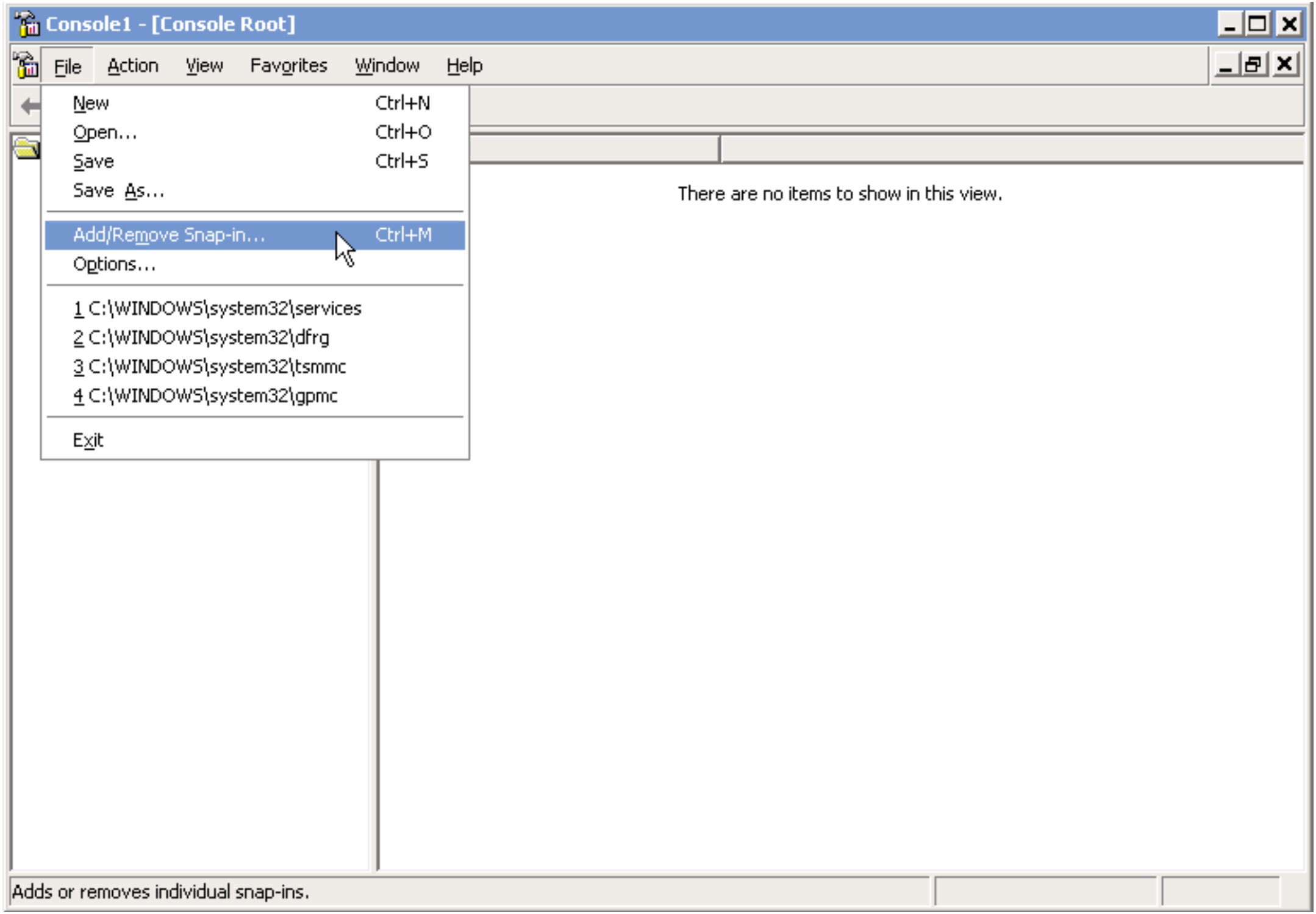
را اجرا کرده و با توجه به شکل های زیر ادامه کار را دنبال کنید .

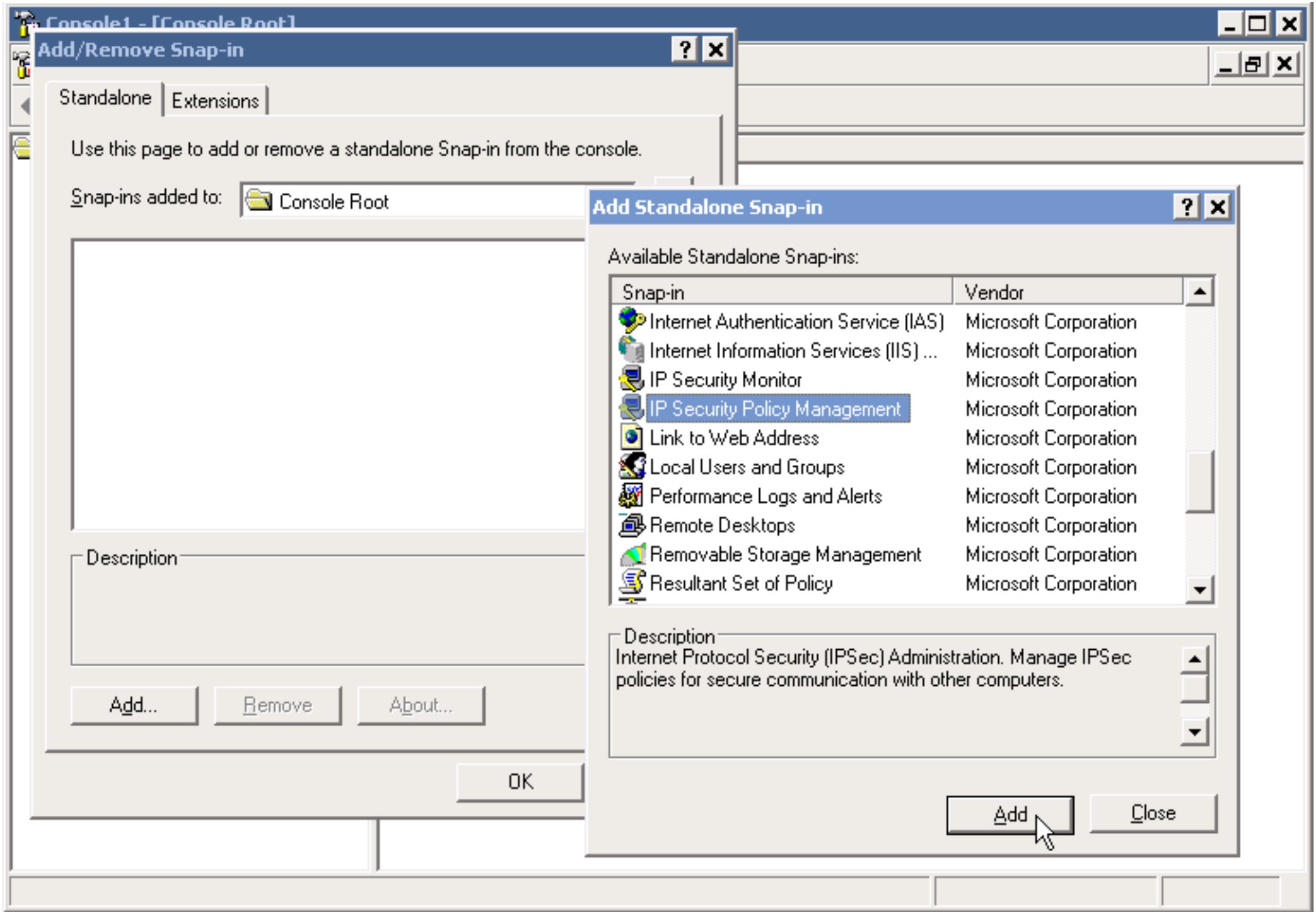
توجه : این یک آموزش برای Block کردن IP بر روپیورت های خاصی است . در صورت استفاده این روش در سرور لطفا این اعمال محدودیت برای تمامی پورت ها لحاظ شود :

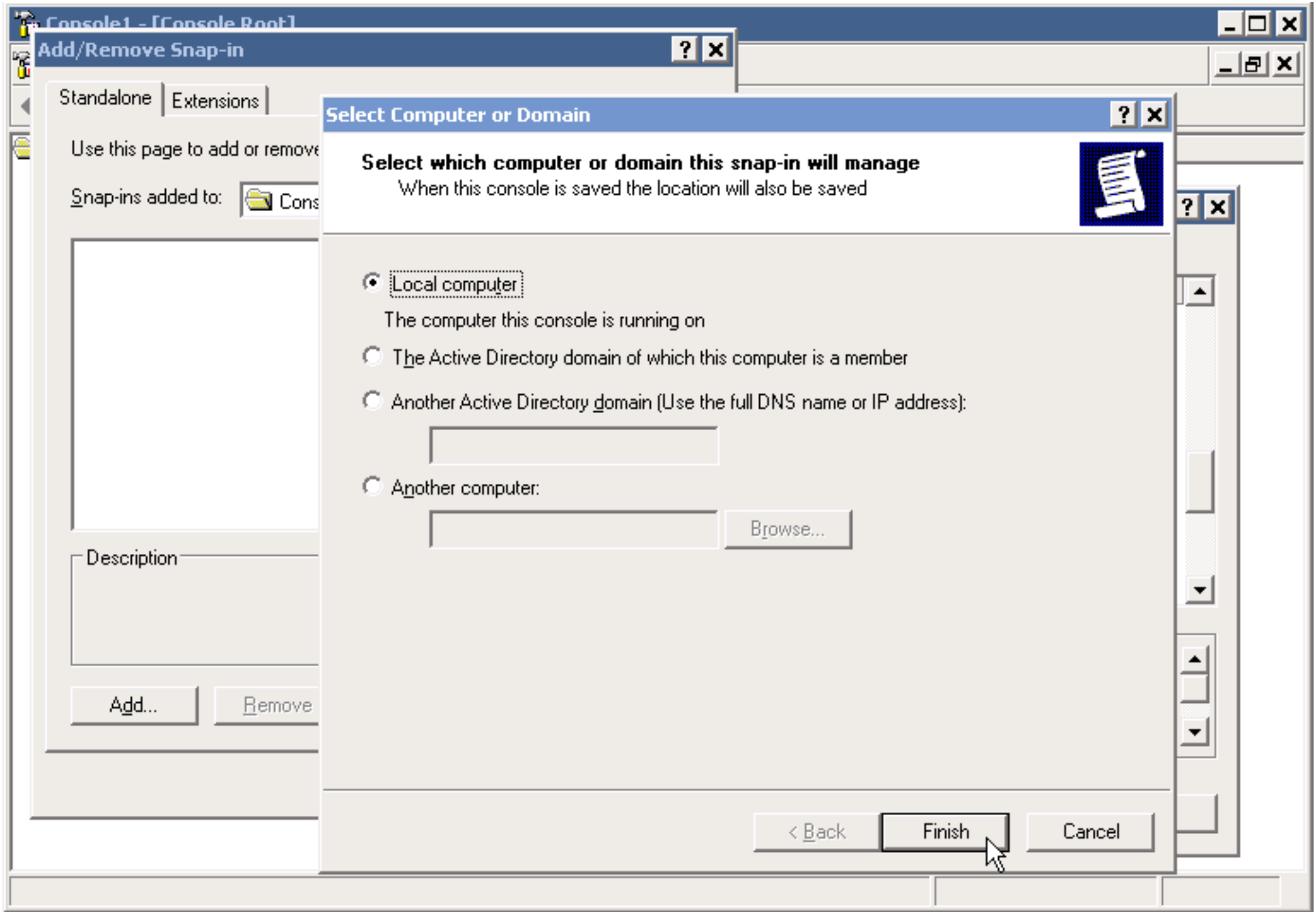
توجه ۲ : عکس های آموزشی فقط به محدود کردن دسترسی Local کامپیوتر میپردازد / برای اینکه Ip بلوک کنید میتوانید به جای Ip / Source Address کسی را که میخواهید به سرور دسترسی نداشته باشد یادداشت کنید .

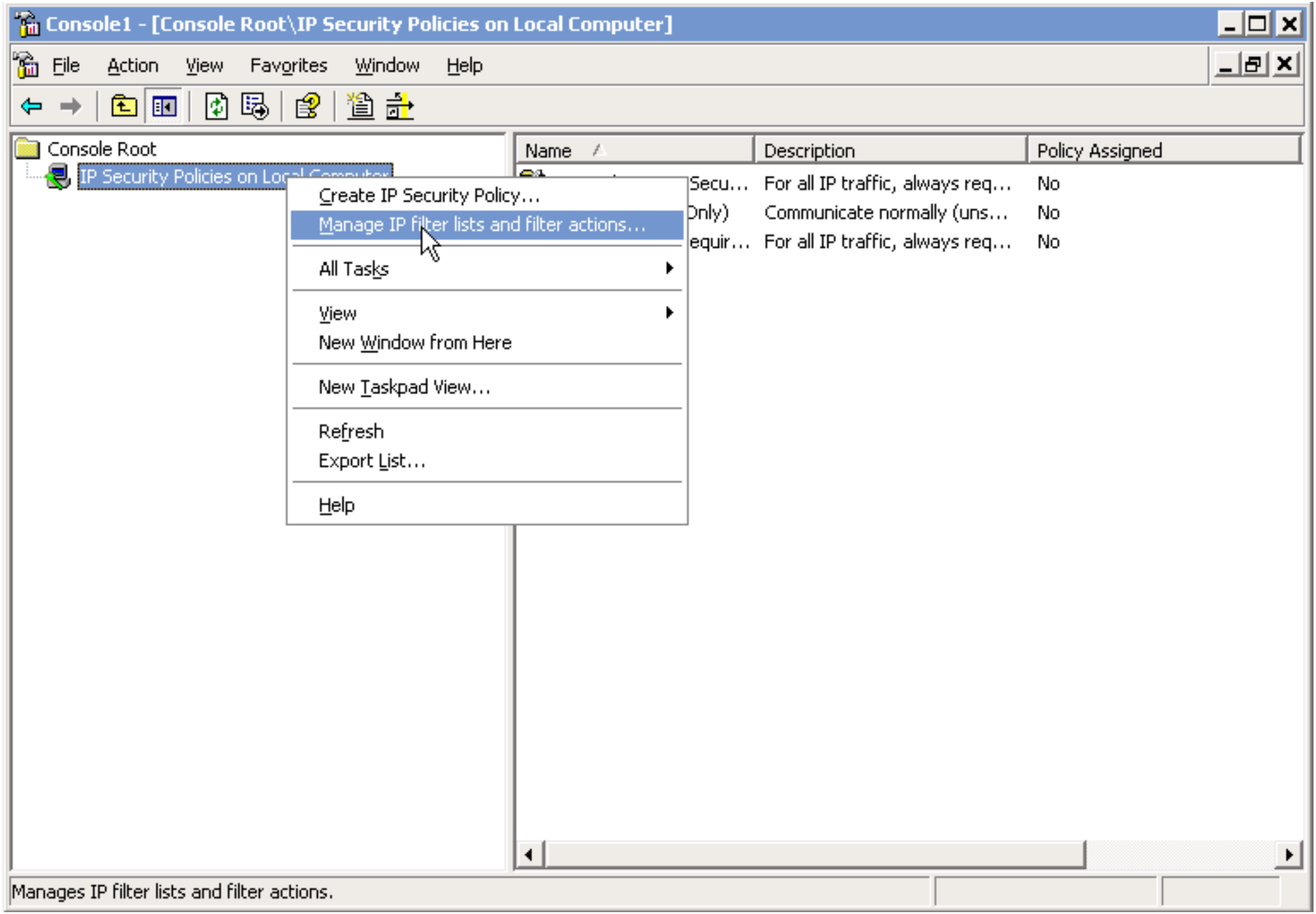
توجه ۳ : در صورت توضیحات بیشتر و آموزش غملی میتوانید به اینجانب مراجعه کنید .

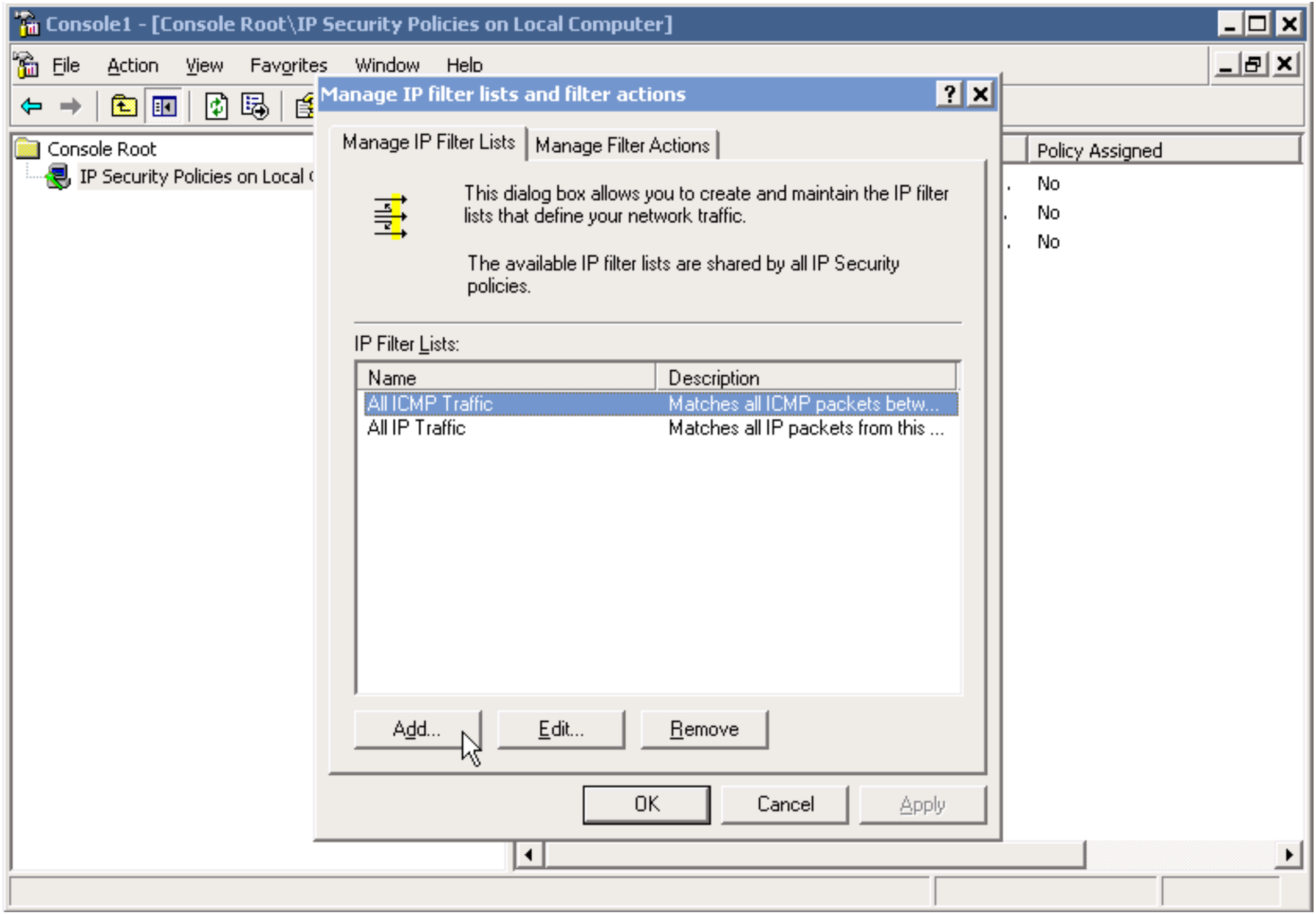
با تشکر : حسین عسگری

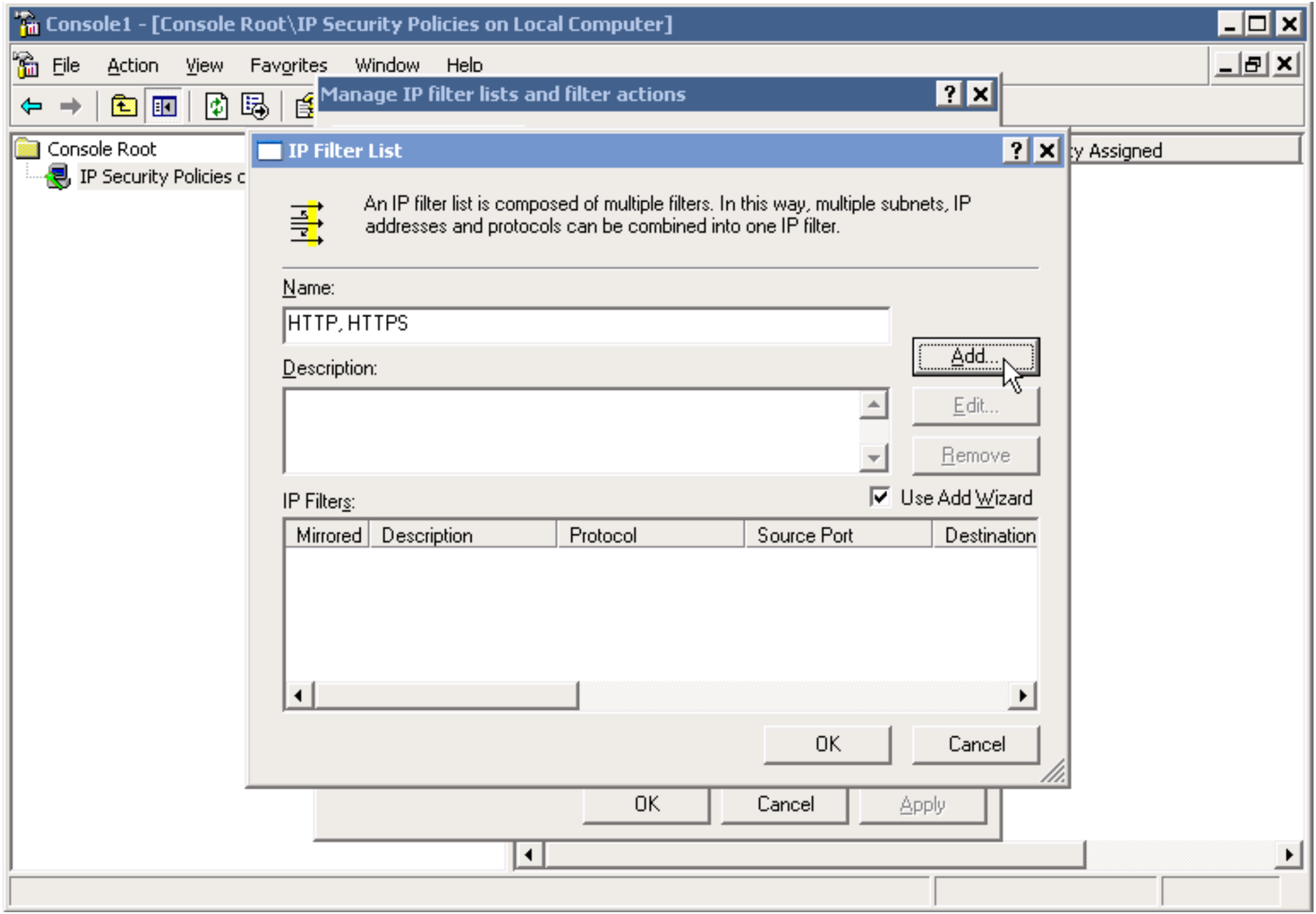

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\WINDOWS\system32\services
2 C:\WINDOWS\system32\dfrg
3 C:\WINDOWS\system32\tsmmc
4 C:\WINDOWS\system32\gpmc
Exit
There are no items to show in this view.
Adds or removes individual snap-ins.

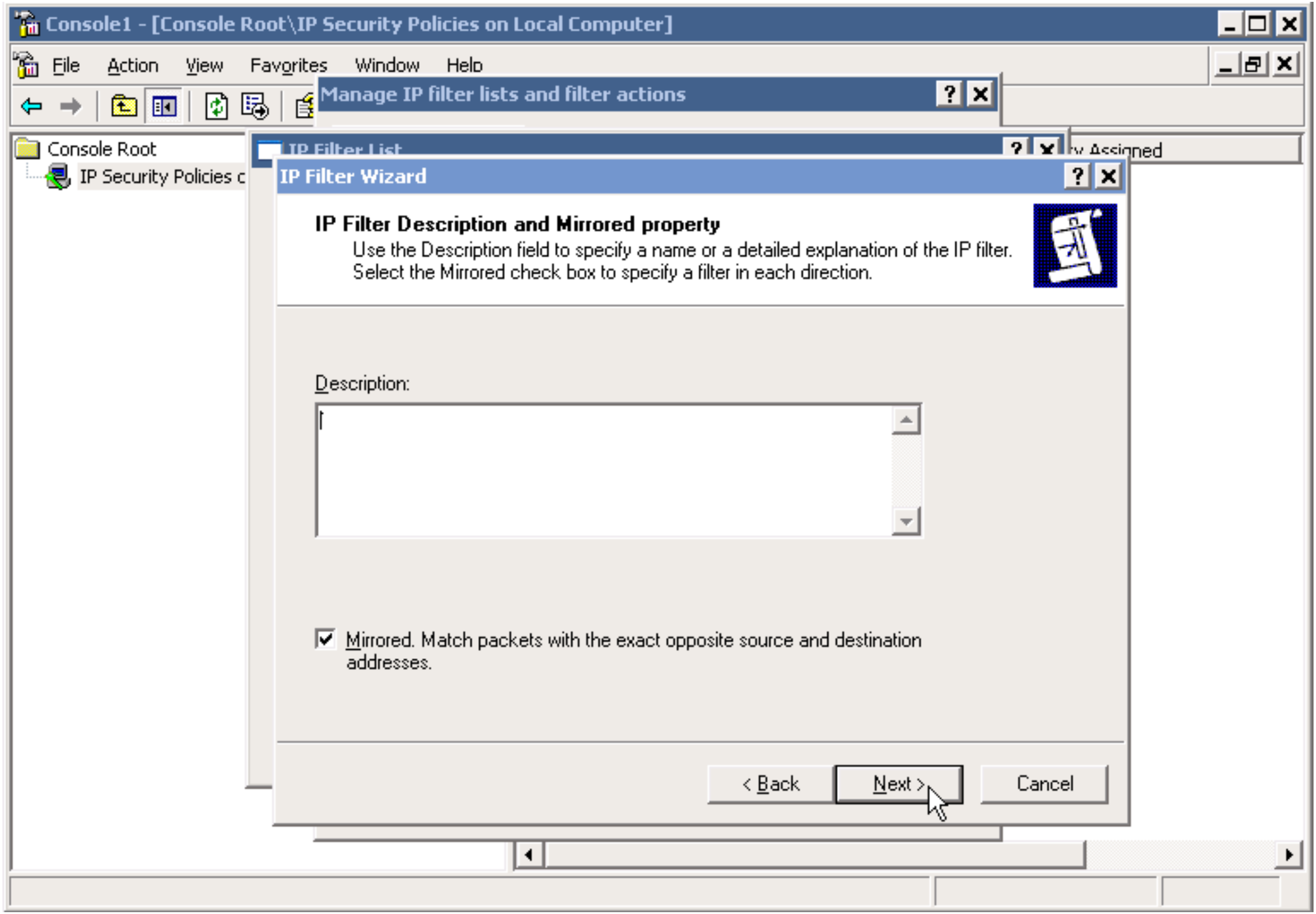

Console1 - [Console Root]
Add/Remove Snap-in
Standalone
Extensions
Use this page to add or remove a standalone Snap-in from the console.
Snap-ins added to:
Console Root
Description
Add...
Remove
About...
OK
Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in
Vendor
Internet Authentication Service (IAS)
Microsoft Corporation
Internet Information Services (IIS) ...
Microsoft Corporation
IP Security Monitor
Microsoft Corporation
IP Security Policy Management
Microsoft Corporation
Link to Web Address
Microsoft Corporation
Local Users and Groups
Microsoft Corporation
Performance Logs and Alerts
Microsoft Corporation
Remote Desktops
Microsoft Corporation
Removable Storage Management
Microsoft Corporation
Resultant Set of Policy
Microsoft Corporation
Description
Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.
Add
Close

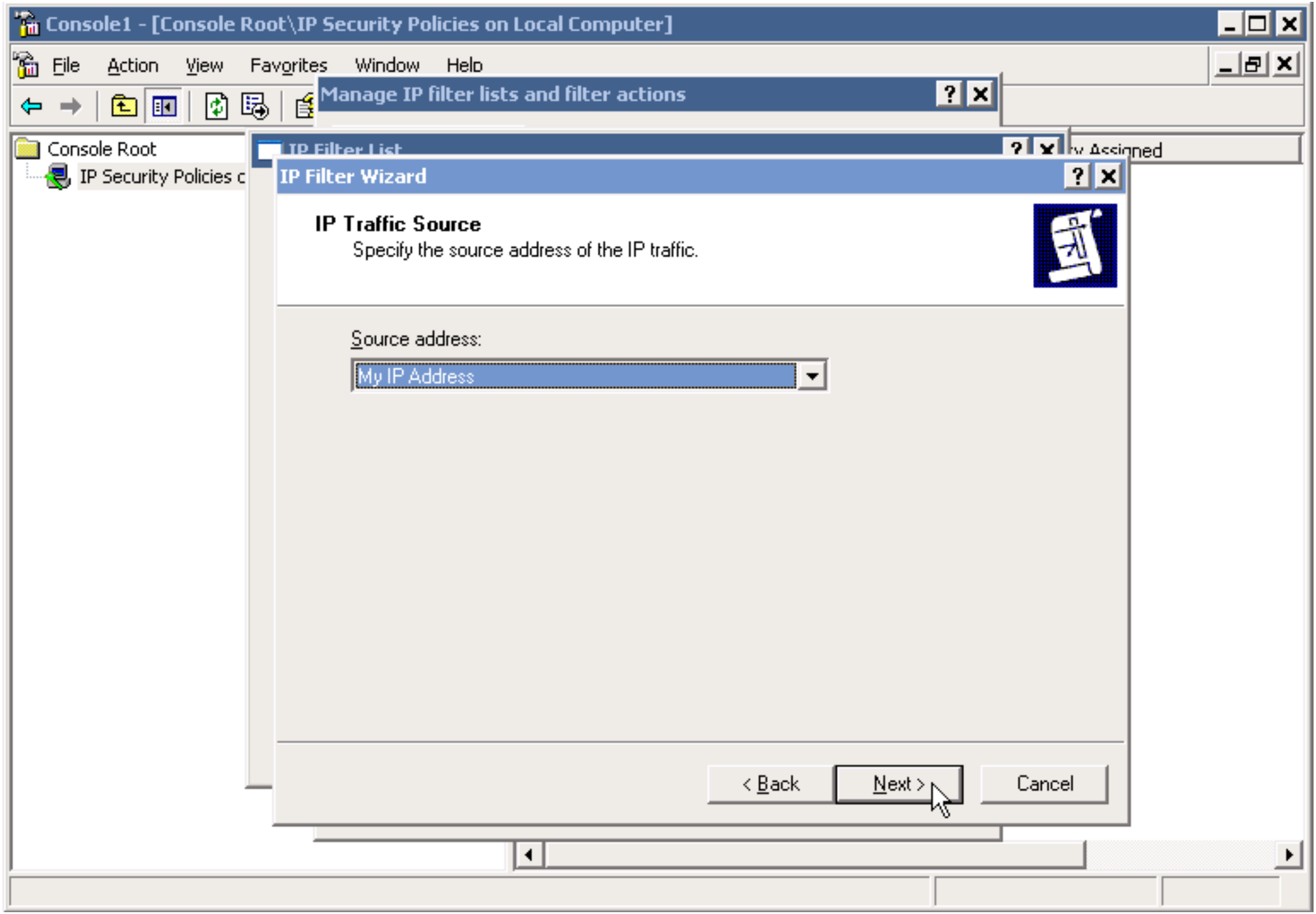

Console1 - [Console Root]
Add/Remove Snap-in
Standalone
Extensions
Use this page to add or remove
Snap-ins added to:
Description
Add...
Remove
Select Computer or Domain
Select which computer or domain this snap-in will manage
When this console is saved the location will also be saved
Local computer
The computer this console is running on
The Active Directory domain of which this computer is a member
Another Active Directory domain (Use the full DNS name or IP address):
Another computer:
Browse...
< Back
Finish
Cancel

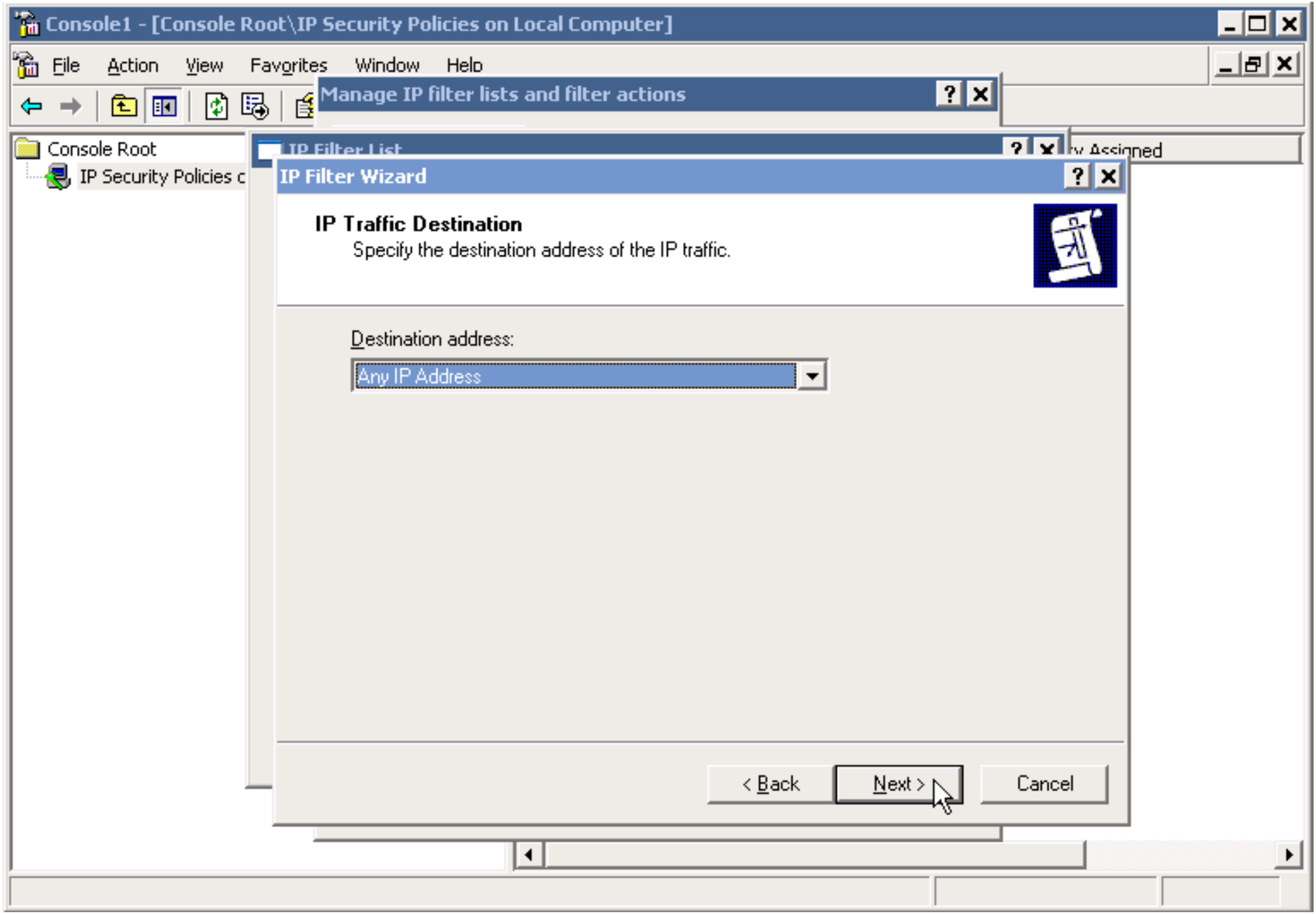

Console1 - [Console Root\IP Security Policies on Local Computer]
File
Action
View
Favorites
Window
Help
Console Root
IP Security Policies on Local Computer
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Name
Description
Policy Assigned
Secu...
For all IP traffic, always req...
No
Only)
Communicate normally (uns...
No
equir...
For all IP traffic, always req...
No
Manages IP filter lists and filter actions.

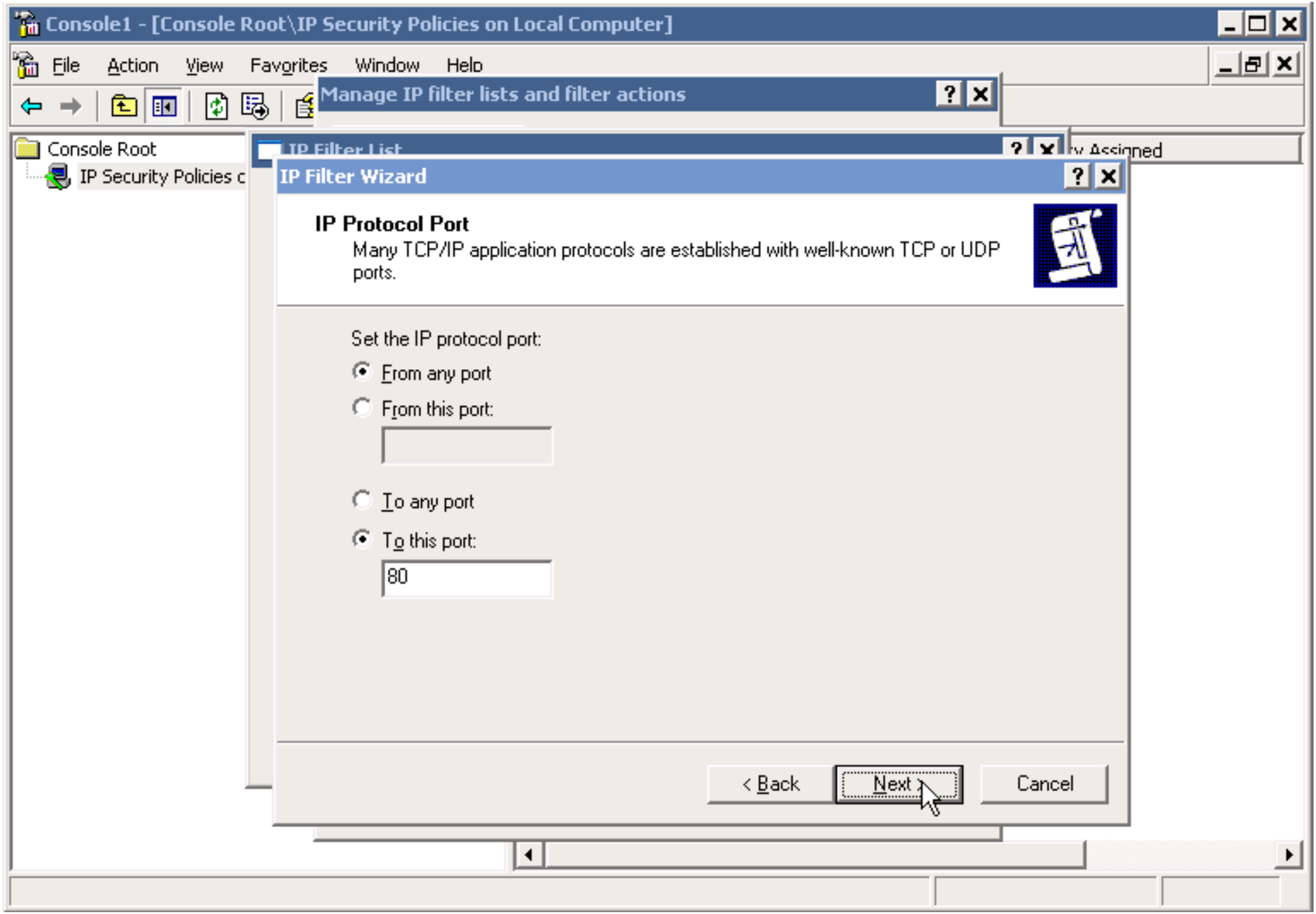

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Policy Assigned
No
No
No
Manage IP filter lists and filter actions
Manage IP Filter Lists
Manage Filter Actions
This dialog box allows you to create and maintain the IP filter lists that define your network traffic.
The available IP filter lists are shared by all IP Security policies.
IP Filter Lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
Add...
Edit...
Remove
OK
Cancel
Apply

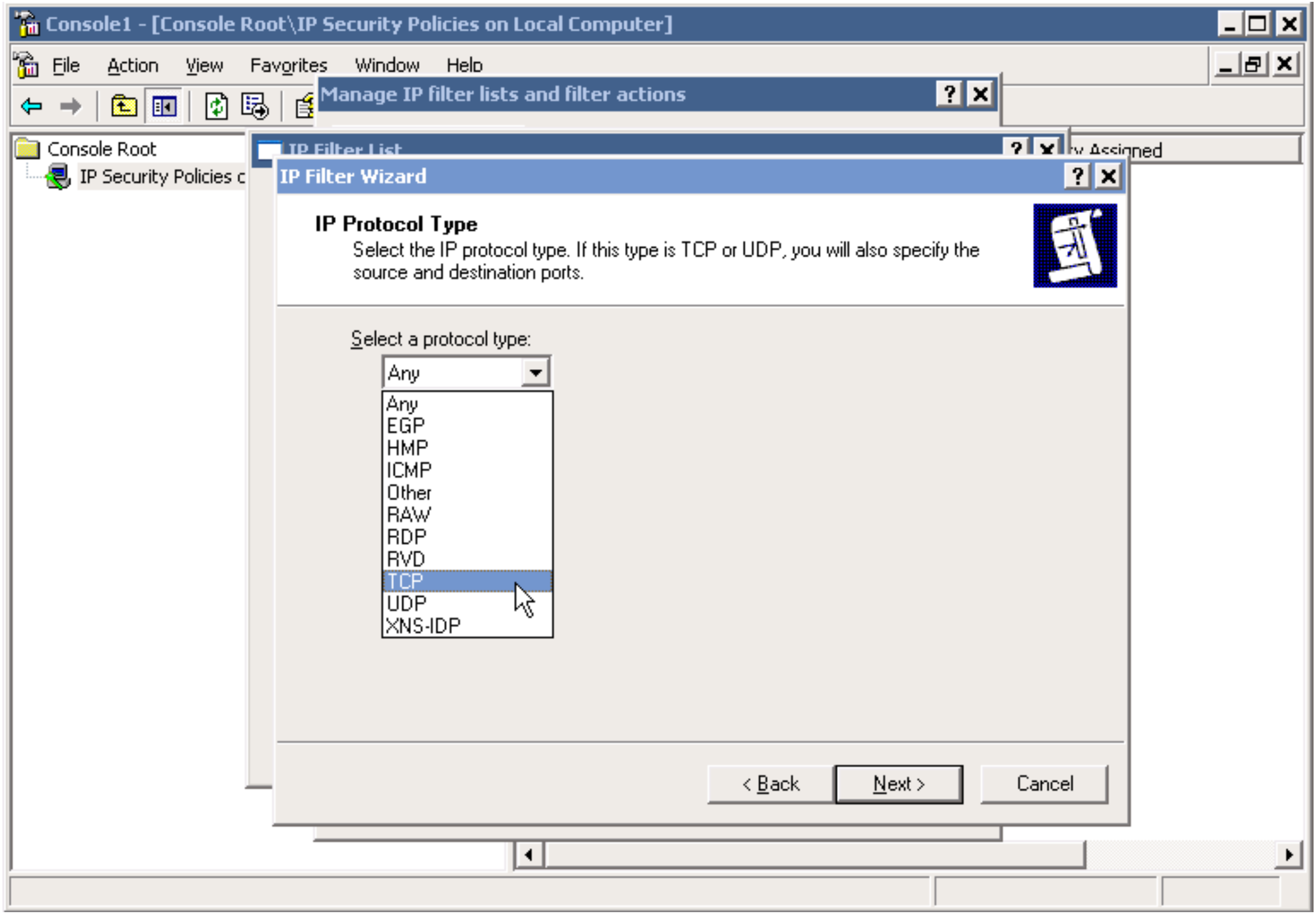

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
HTTP, HTTPS
Description:
Add...
Edit...
Remove
IP Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
OK
Cancel
OK
Cancel
Apply

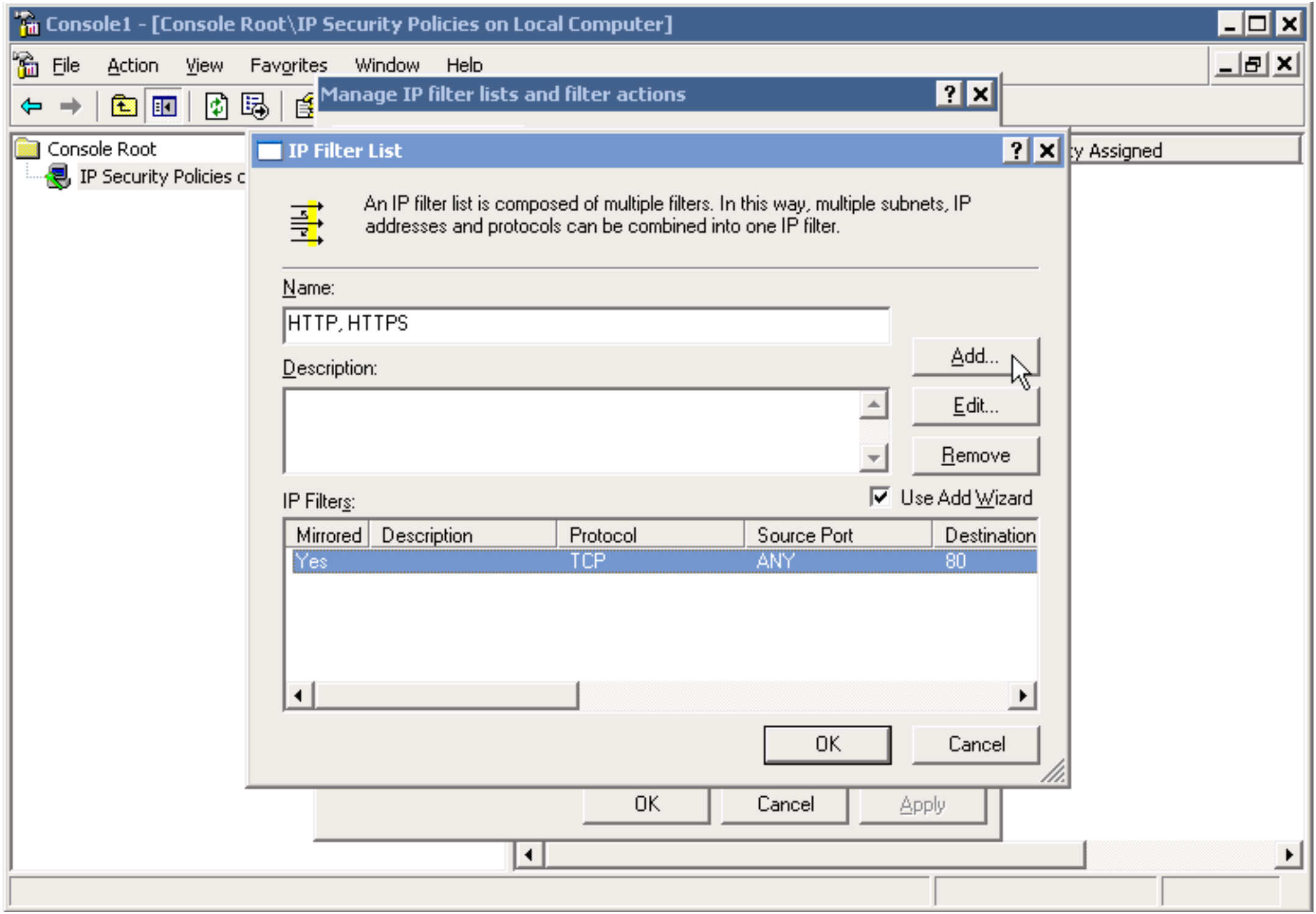

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
IP Filter Wizard
IP Filter Description and Mirrored property
Use the Description field to specify a name or a detailed explanation of the IP filter.
Select the Mirrored check box to specify a filter in each direction.
Description:
Mirrored. Match packets with the exact opposite source and destination addresses.
< Back
Next >
Cancel

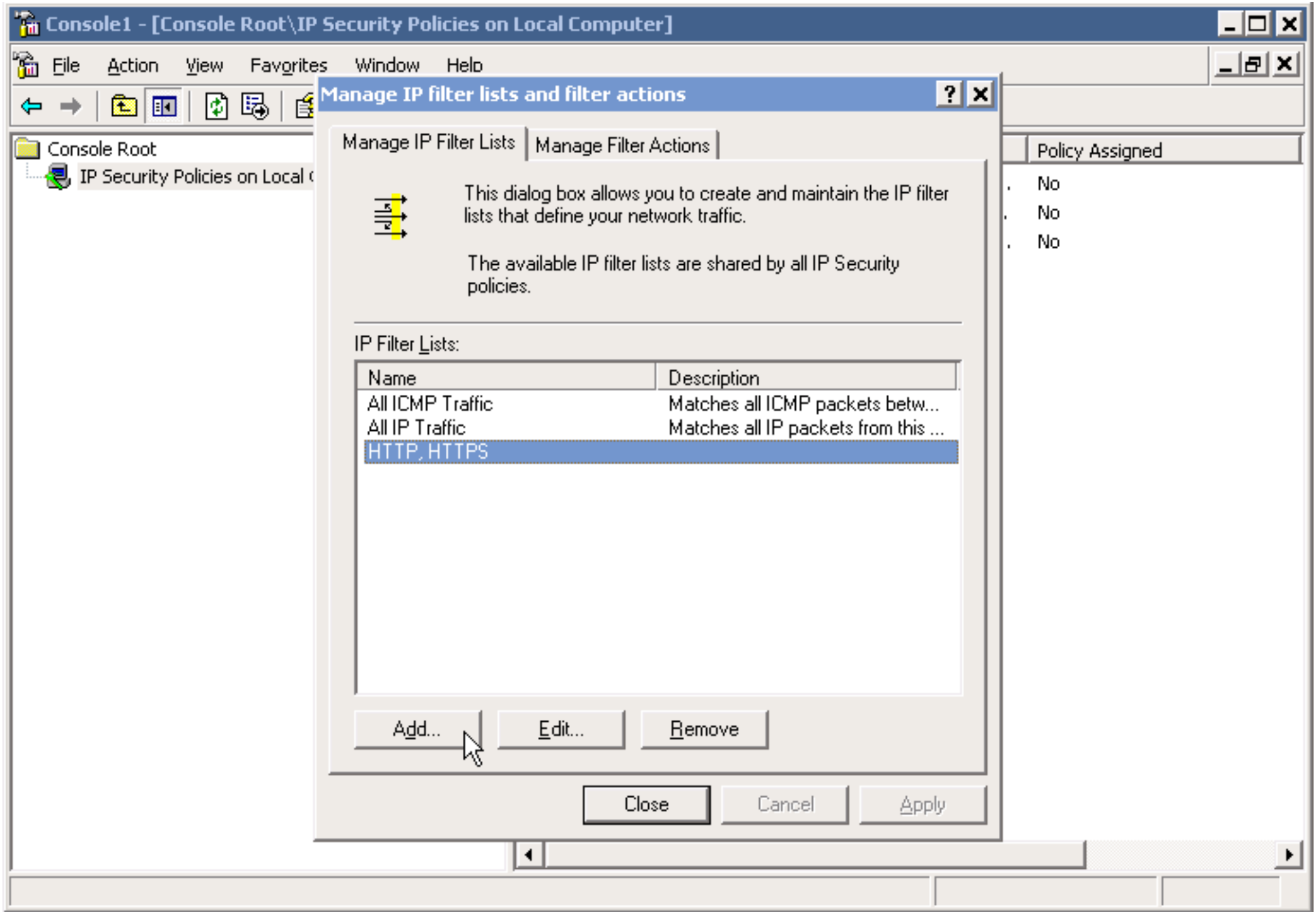

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
IP Filter Wizard
IP Traffic Source
Specify the source address of the IP traffic.
Source address:
My IP Address
< Back
Next >
Cancel

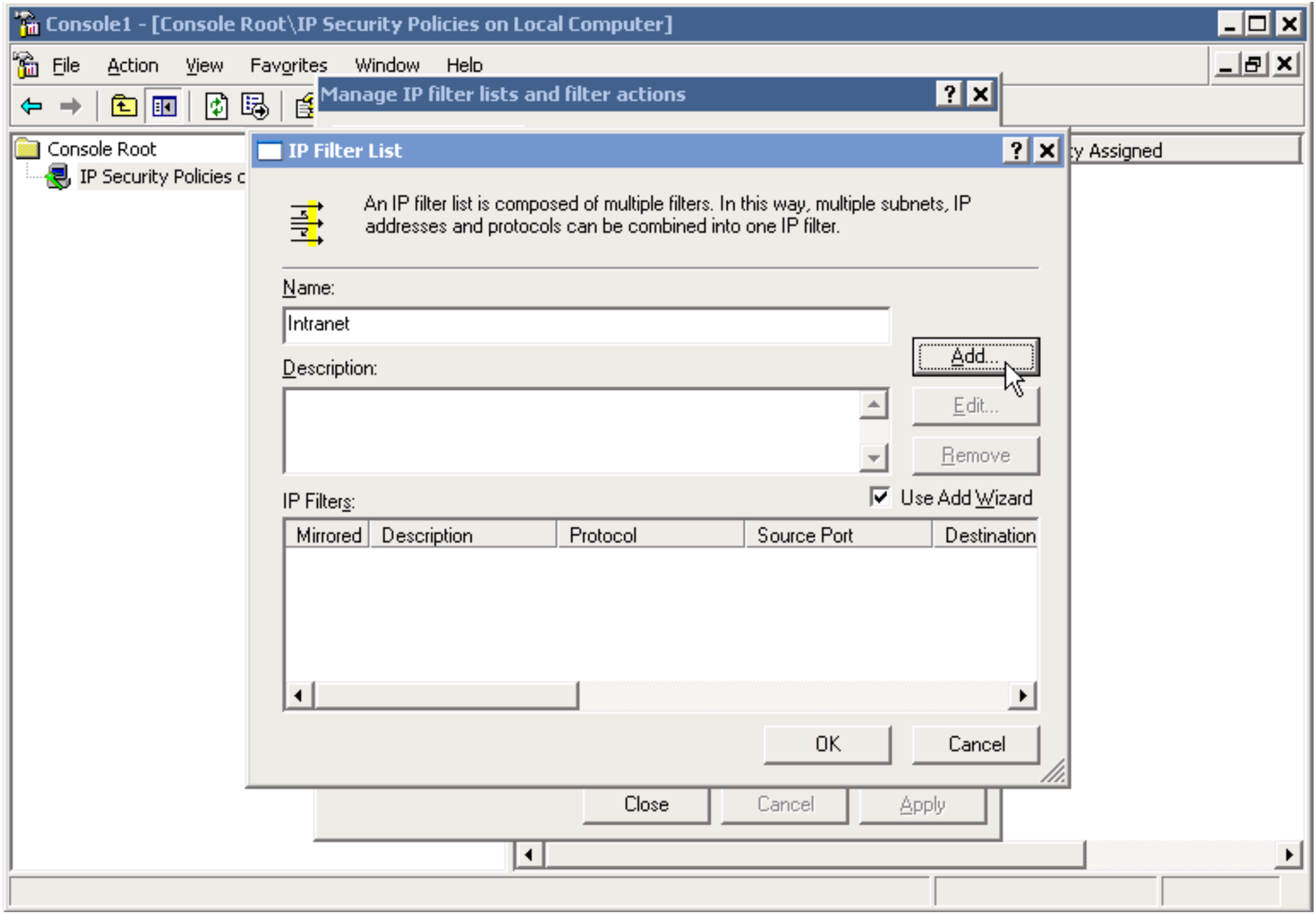

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
IP Filter Wizard
IP Traffic Destination
Specify the destination address of the IP traffic.
Destination address:
Any IP Address
< Back
Next >
Cancel

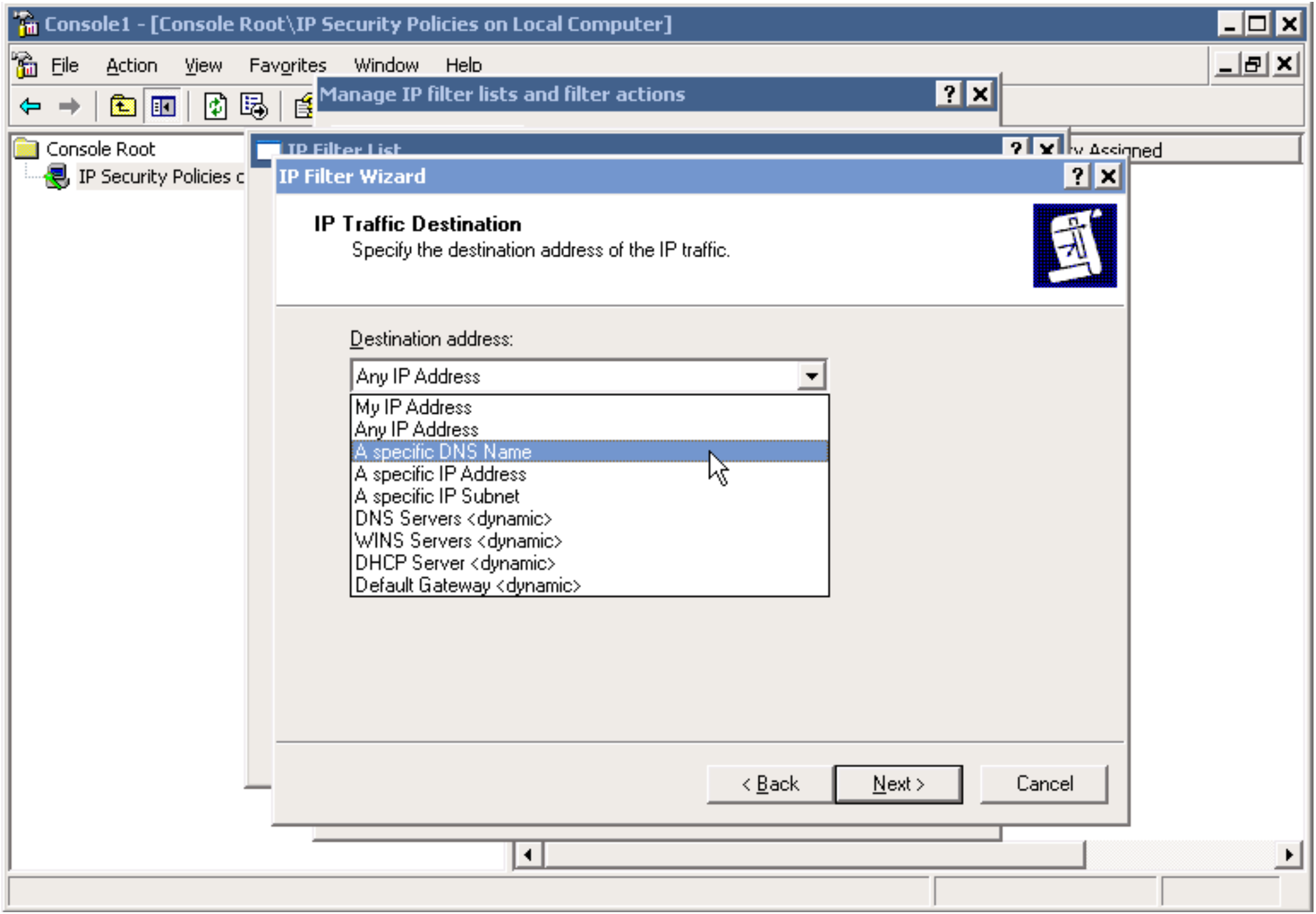

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
IP Filter Wizard
IP Protocol Port
Many TCP/IP application protocols are established with well-known TCP or UDP ports.
Set the IP protocol port:
From any port
From this port:
To any port
To this port:
80
< Back
Next >
Cancel

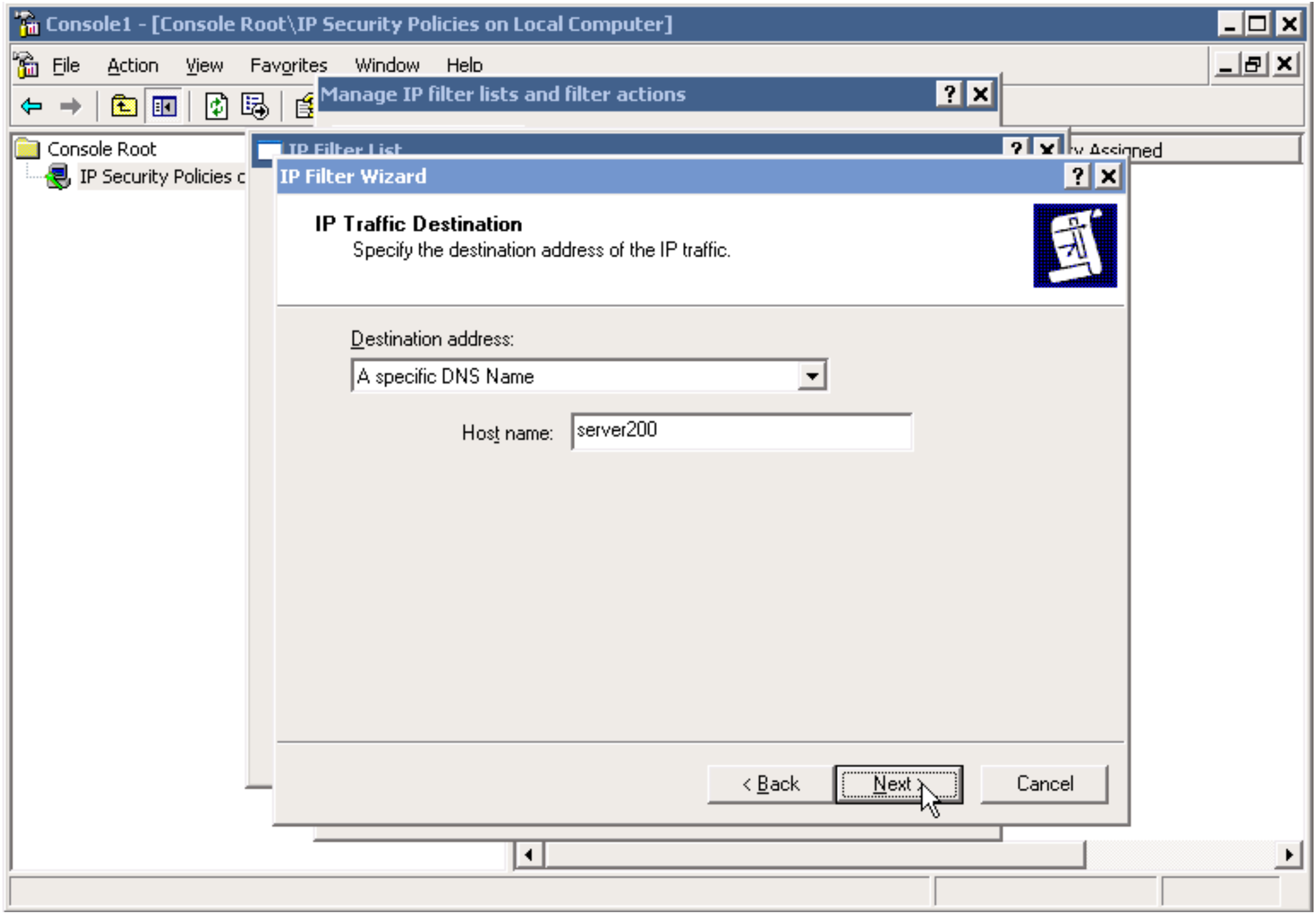

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
IP Filter Wizard
IP Protocol Type
Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.
Select a protocol type:
Any
Any
EGP
HMP
ICMP
Other
RAW
RDP
RVD
TCP
UDP
XNS-IDP
< Back
Next >
Cancel

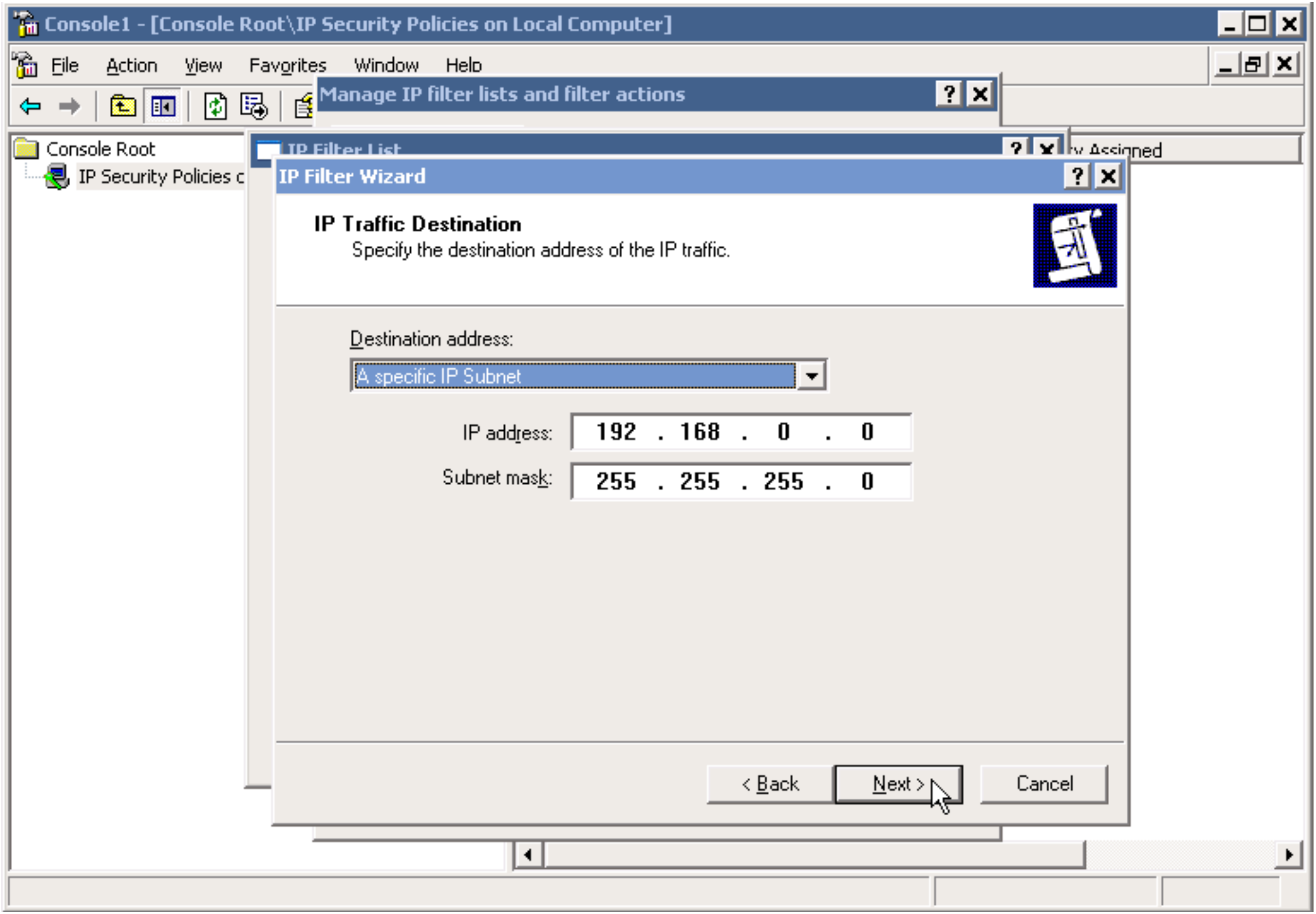

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
HTTP, HTTPS
Description:
Add...
Edit...
Remove
IP Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
Yes
TCP
ANY
80
OK
Cancel
OK
Cancel
Apply

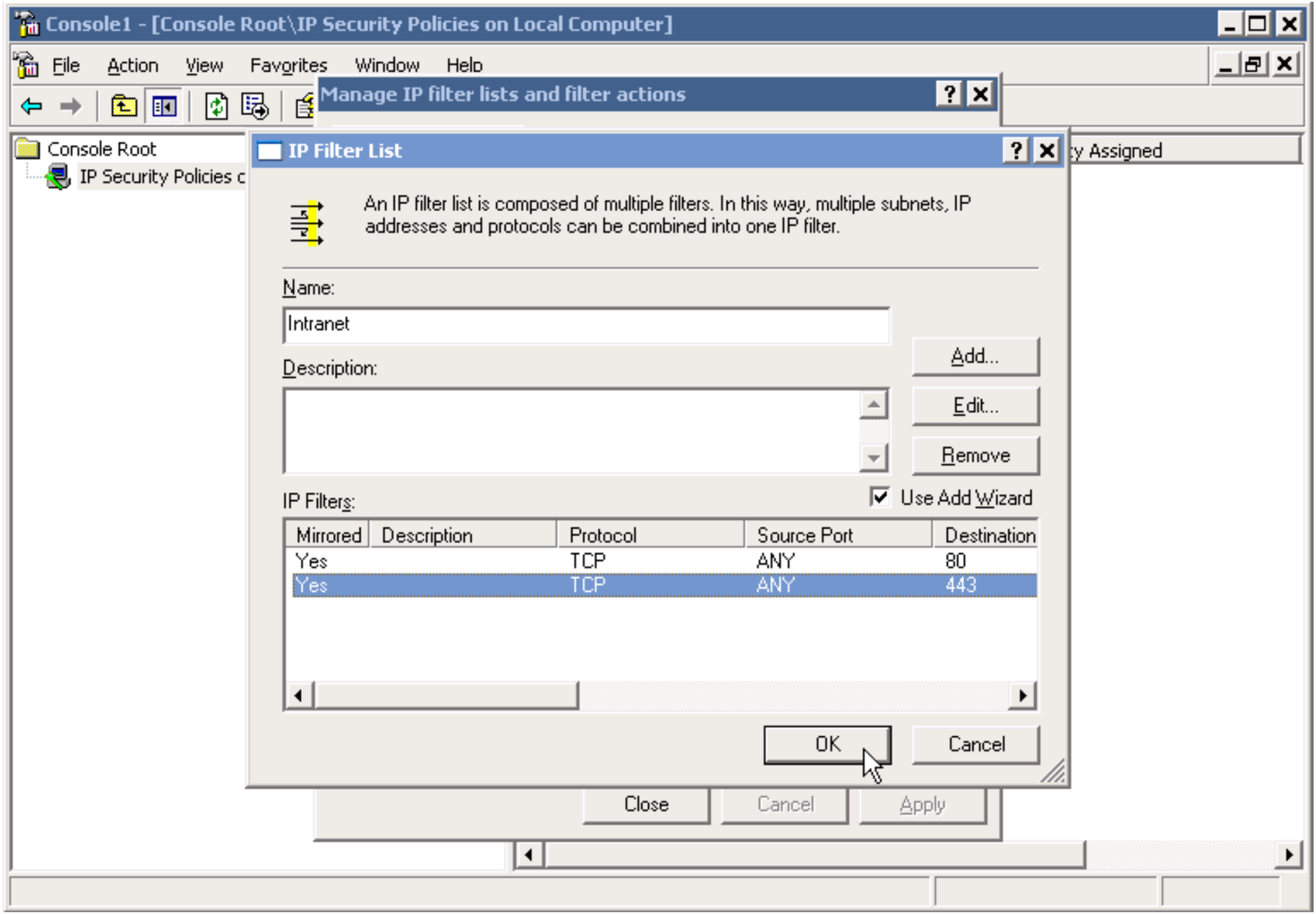

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Policy Assigned
No
No
No
Manage IP filter lists and filter actions
Manage IP Filter Lists
Manage Filter Actions
This dialog box allows you to create and maintain the IP filter lists that define your network traffic.
The available IP filter lists are shared by all IP Security policies.
IP Filter Lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
HTTP, HTTPS
Add...
Edit...
Remove
Close
Cancel
Apply

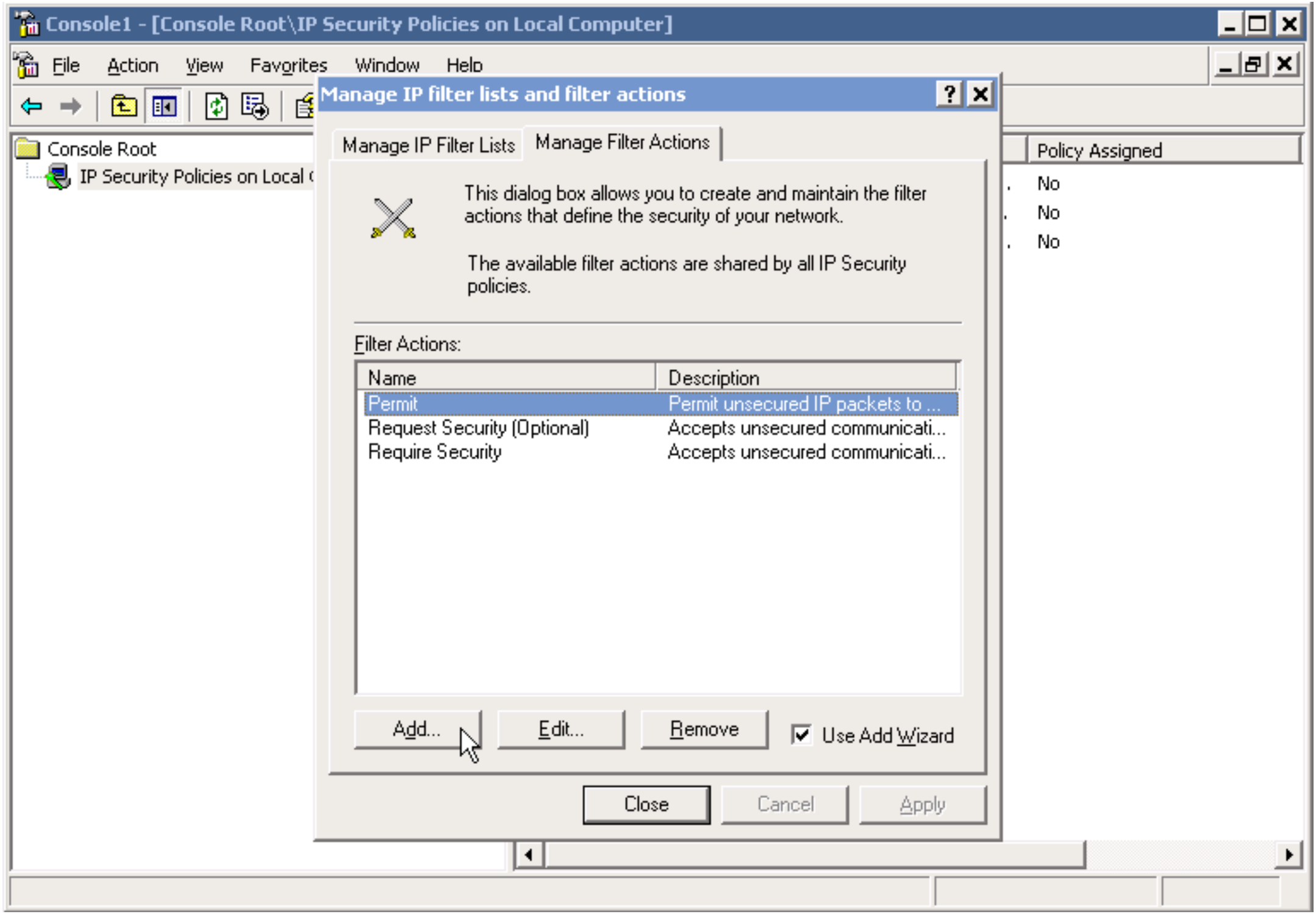

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
Intranet
Description:
Add...
Edit...
Remove
IP Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
OK
Cancel
Close
Cancel
Apply

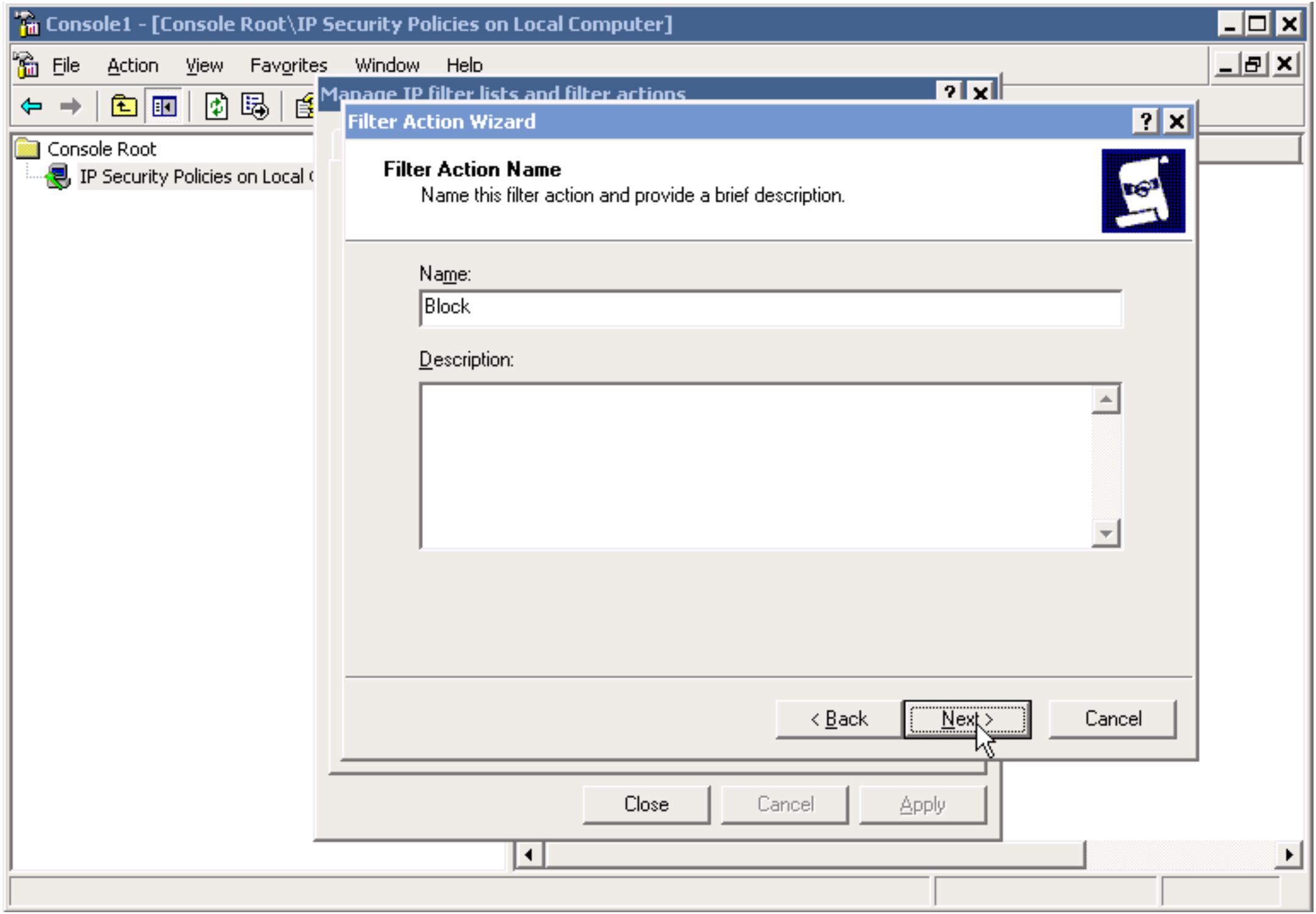

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
IP Filter Wizard
IP Traffic Destination
Specify the destination address of the IP traffic.
Destination address:
Any IP Address
My IP Address
Any IP Address
A specific DNS Name
A specific IP Address
A specific IP Subnet
DNS Servers <dynamic>
WINS Servers <dynamic>
DHCP Server <dynamic>
Default Gateway <dynamic>
< Back
Next >
Cancel

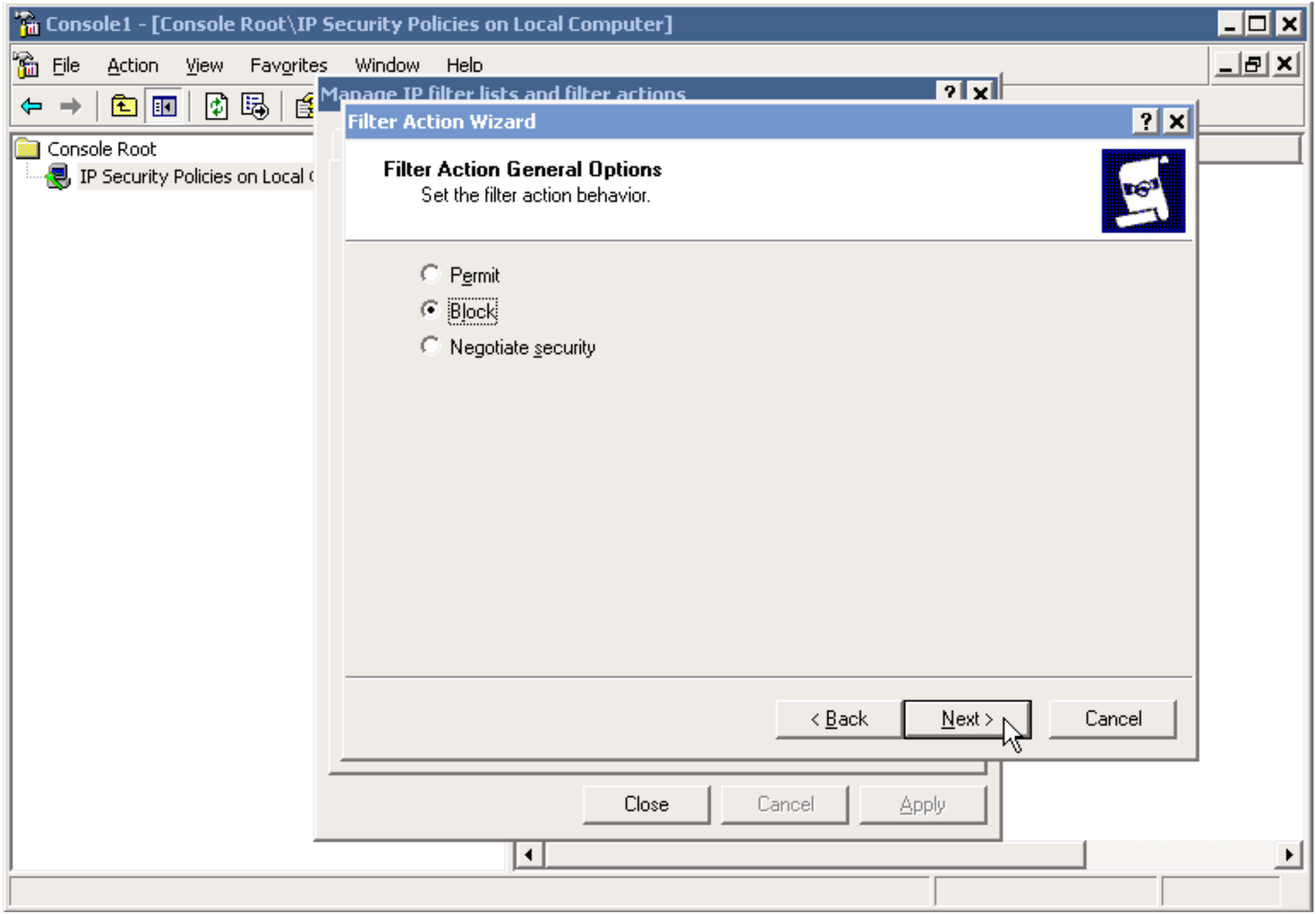

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
IP Filter Wizard
IP Traffic Destination
Specify the destination address of the IP traffic.
Destination address:
A specific DNS Name
Host name:
server200
< Back
Next >
Cancel

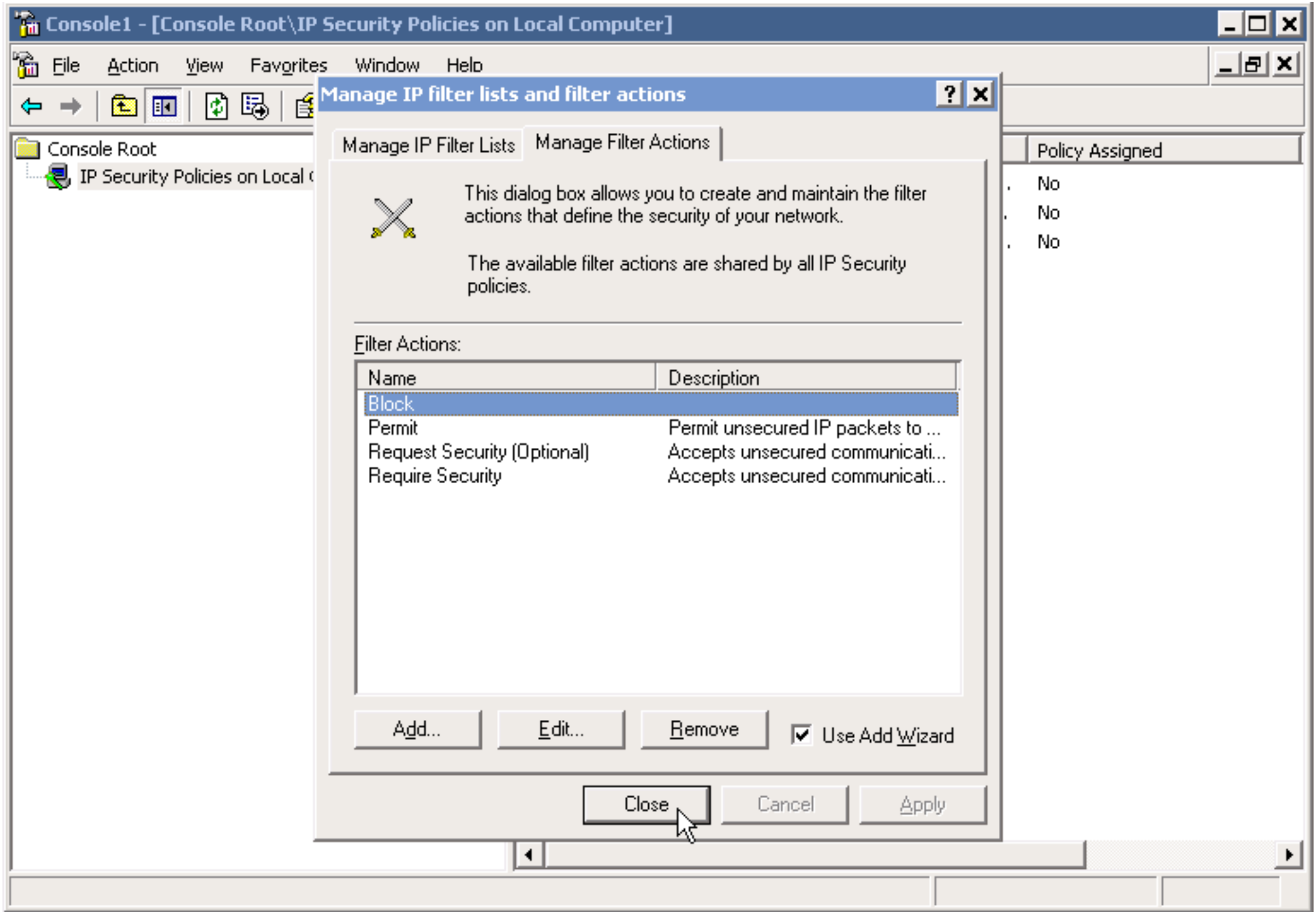

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
IP Filter Wizard
IP Traffic Destination
Specify the destination address of the IP traffic.
Destination address:
A specific IP Subnet
IP address: 192 . 168 . 0 . 0
Subnet mask: 255 . 255 . 255 . 0
< Back
Next >
Cancel

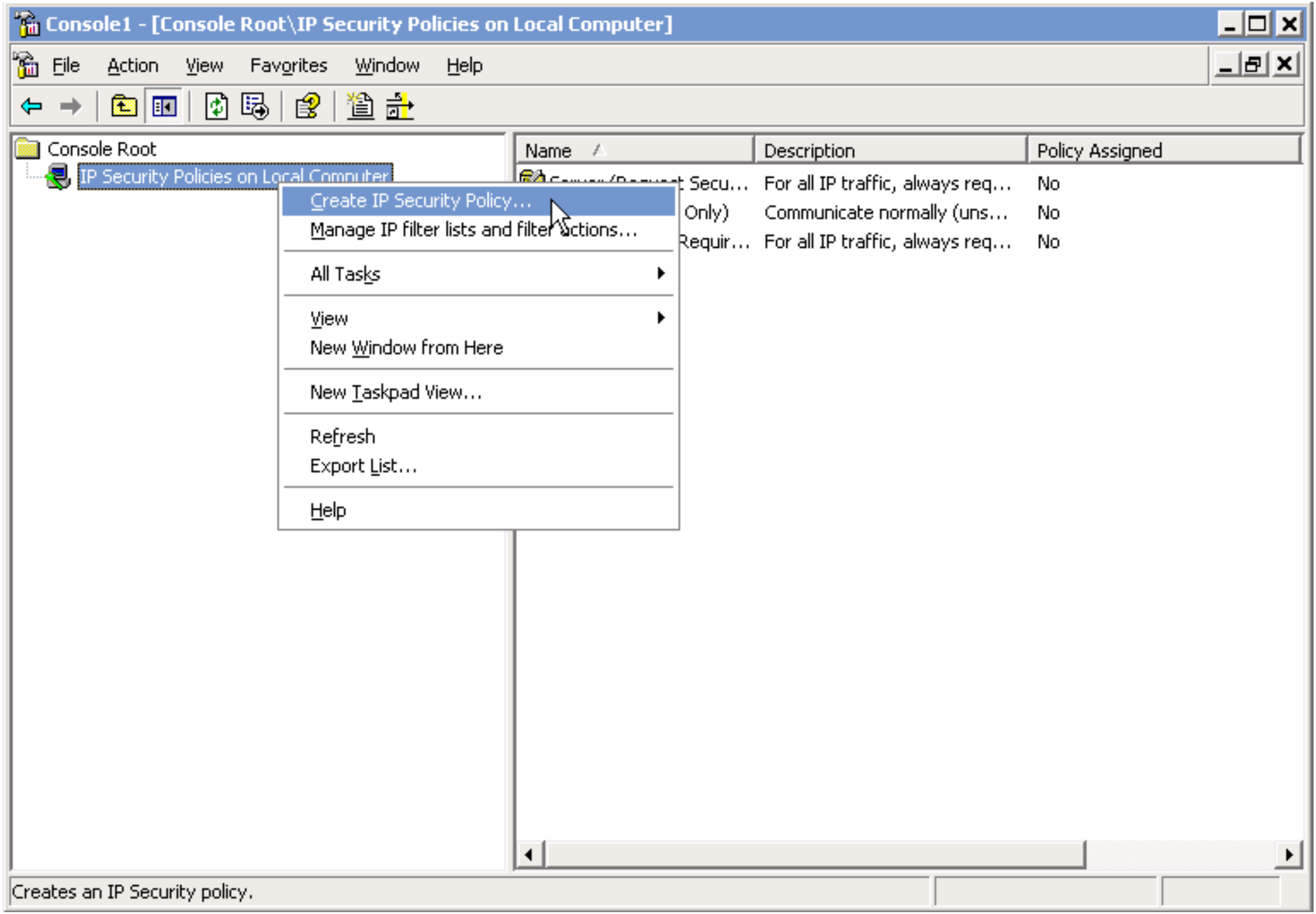

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Manage IP filter lists and filter actions
Console Root
IP Security Policies c
IP Filter List
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
Intranet
Description:
Add...
Edit...
Remove
IP Filters:
Use Add Wizard
Mirrored Description Protocol Source Port Destination
Yes TCP ANY 80
Yes TCP ANY 443
OK
Cancel
Close
Cancel
Apply

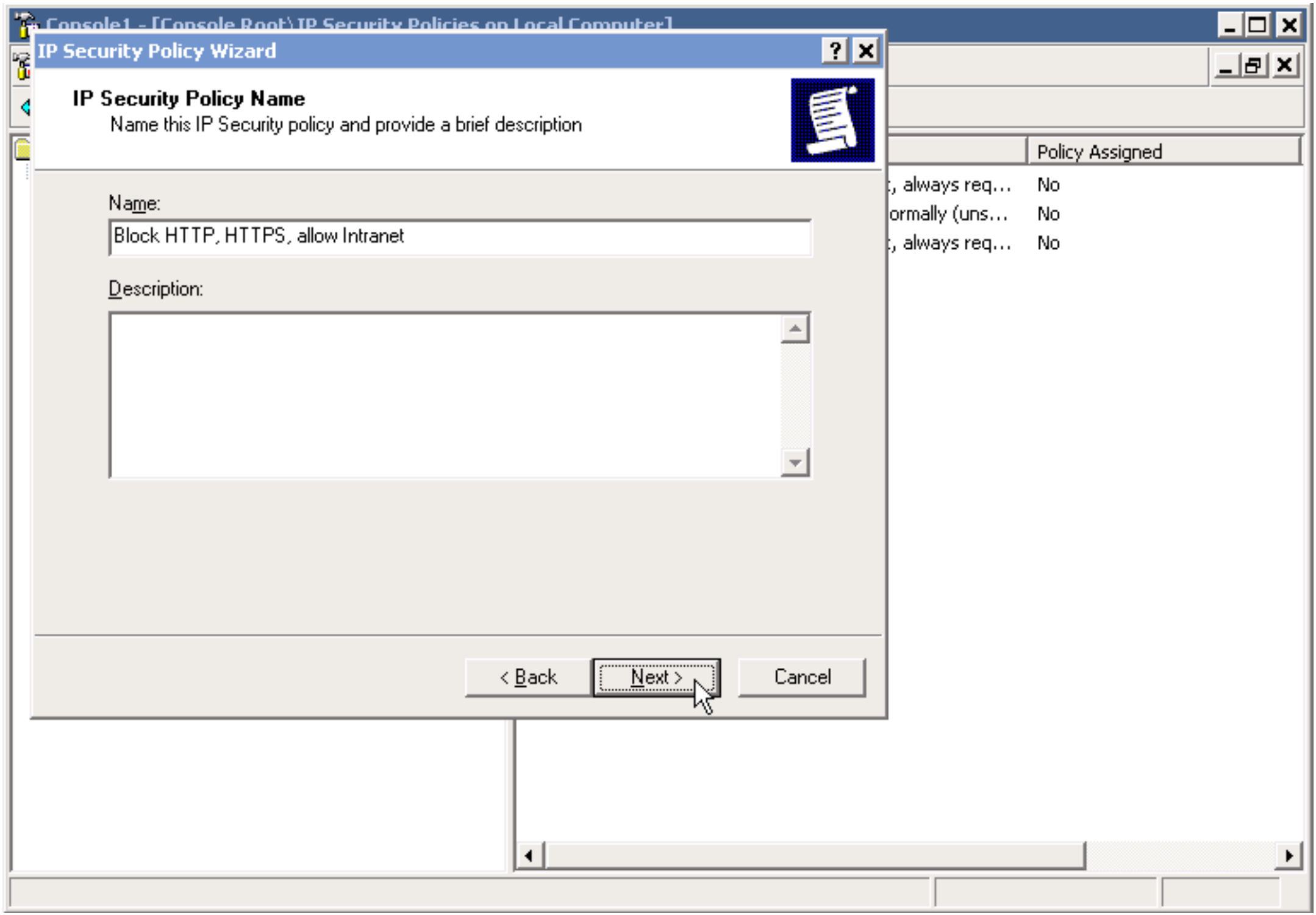

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Policy Assigned
No
No
No
Manage IP filter lists and filter actions
Manage IP Filter Lists
Manage Filter Actions
This dialog box allows you to create and maintain the filter actions that define the security of your network.
The available filter actions are shared by all IP Security policies.
Filter Actions:
Name
Description
Permit
Permit unsecured IP packets to ...
Request Security (Optional)
Accepts unsecured communicati...
Require Security
Accepts unsecured communicati...
Add...
Edit...
Remove
Use Add Wizard
Close
Cancel
Apply

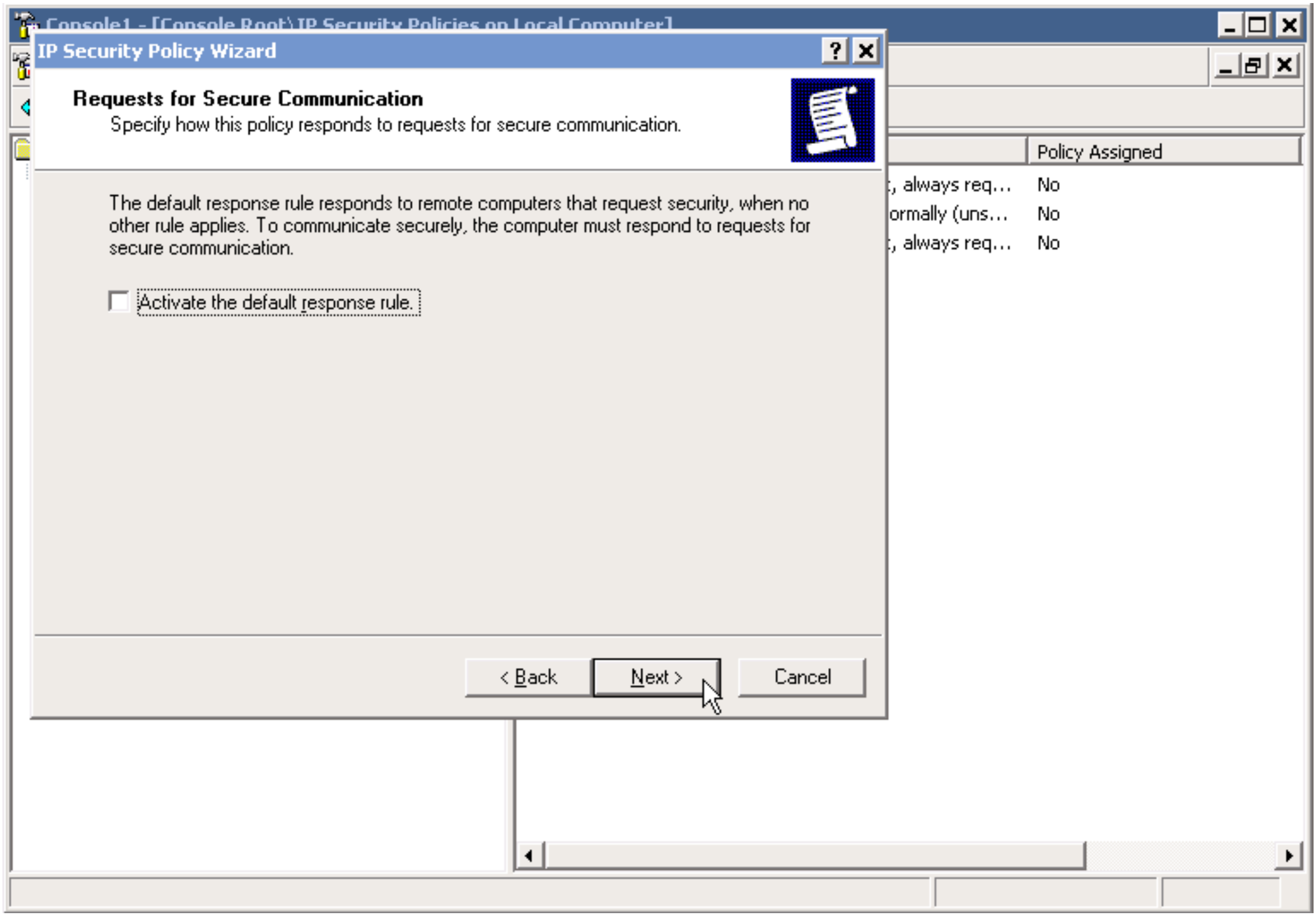

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Manage IP filter lists and filter actions
Filter Action Wizard
Filter Action Name
Name this filter action and provide a brief description.
Name:
Block
Description:
< Back
Next >
Cancel
Close
Cancel
Apply

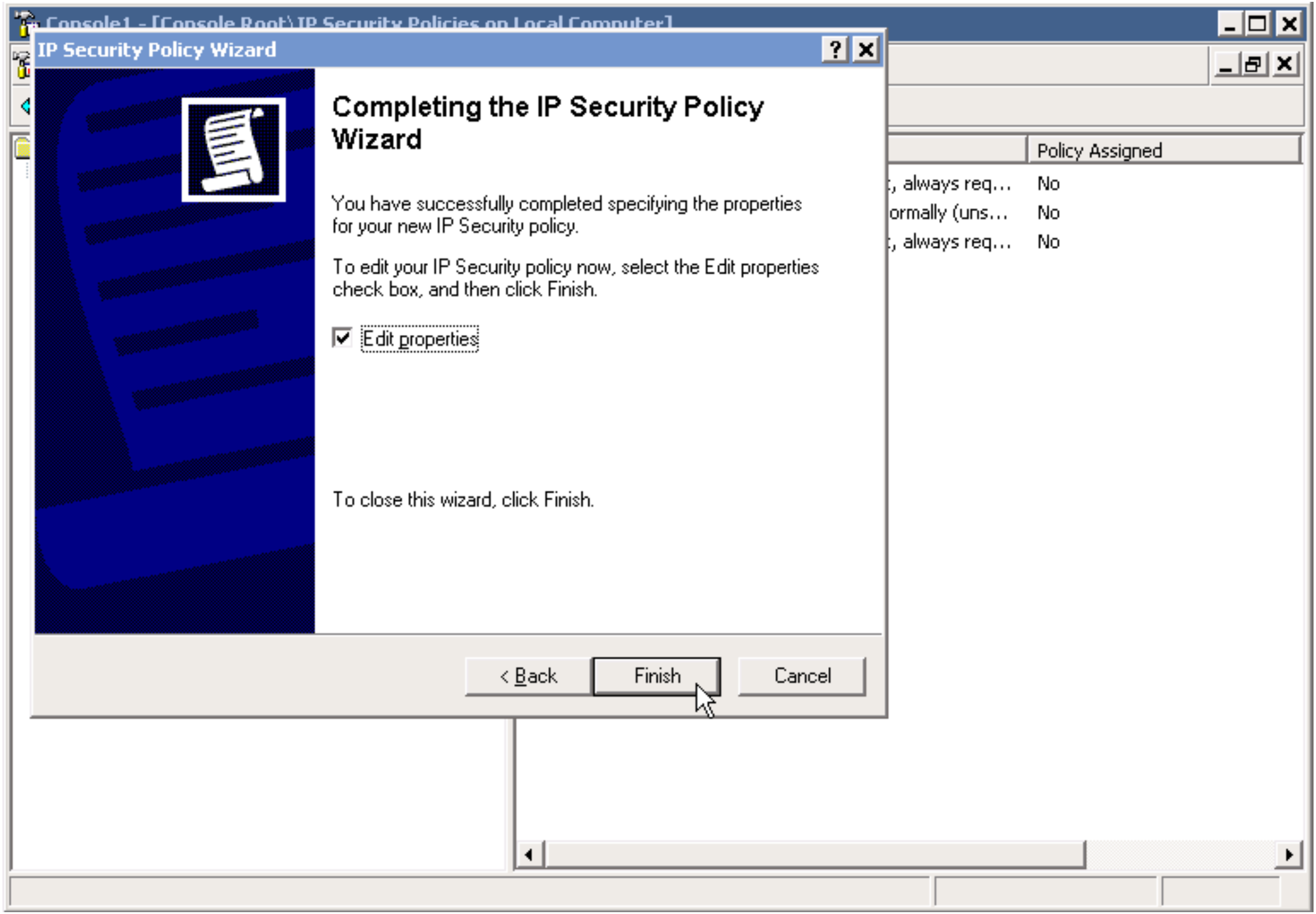

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Manage IP filter lists and filter actions
Filter Action Wizard
Filter Action General Options
Set the filter action behavior.
Permit
Block
Negotiate security
< Back
Next >
Cancel
Close
Cancel
Apply

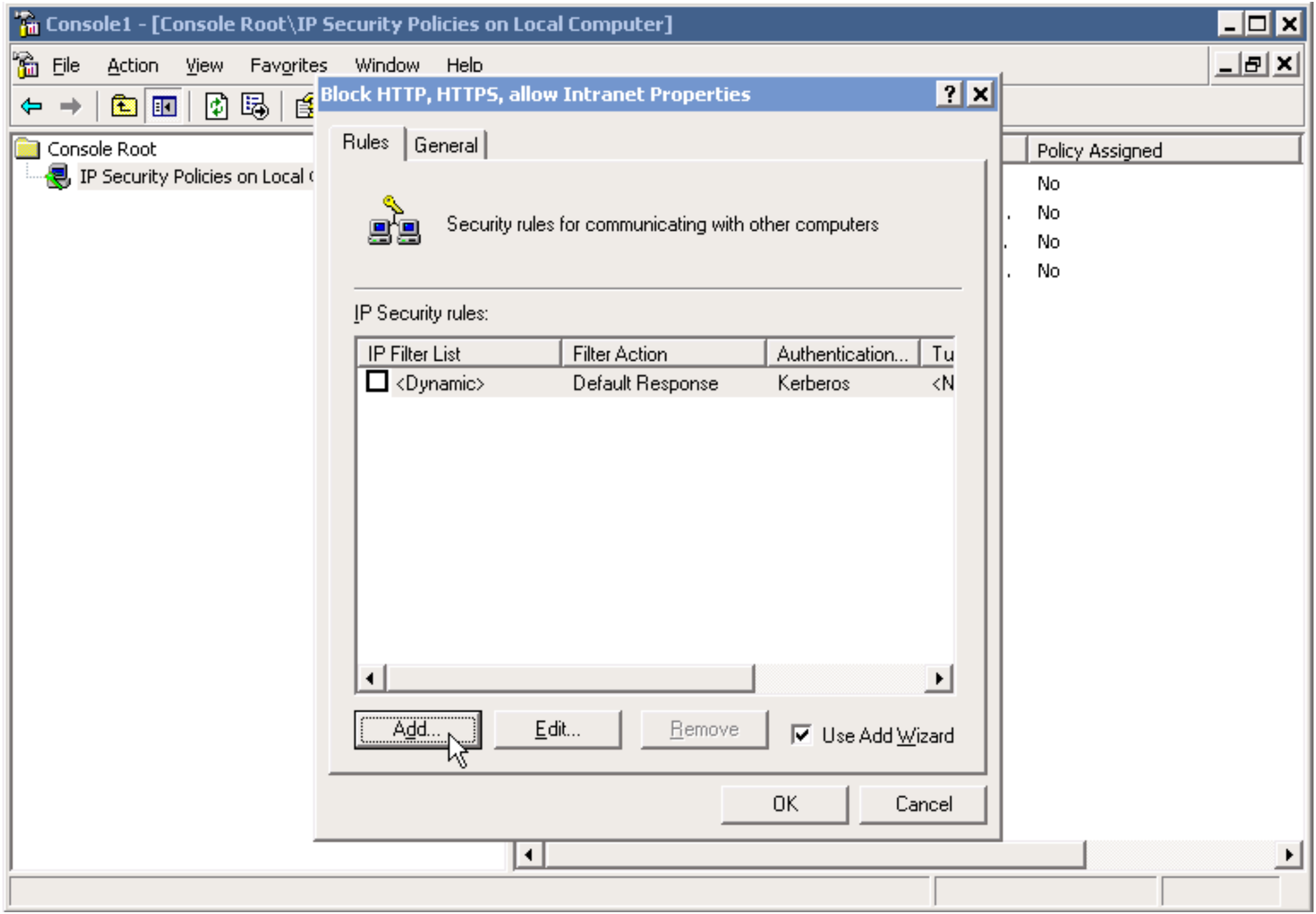

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Policy Assigned
No
No
No
Manage IP filter lists and filter actions
Manage IP Filter Lists
Manage Filter Actions
This dialog box allows you to create and maintain the filter actions that define the security of your network.
The available filter actions are shared by all IP Security policies.
Filter Actions:
Name
Description
Block
Permit
Permit unsecured IP packets to ...
Request Security (Optional)
Accepts unsecured communicati...
Require Security
Accepts unsecured communicati...
Add...
Edit...
Remove
Use Add Wizard
Close
Cancel
Apply

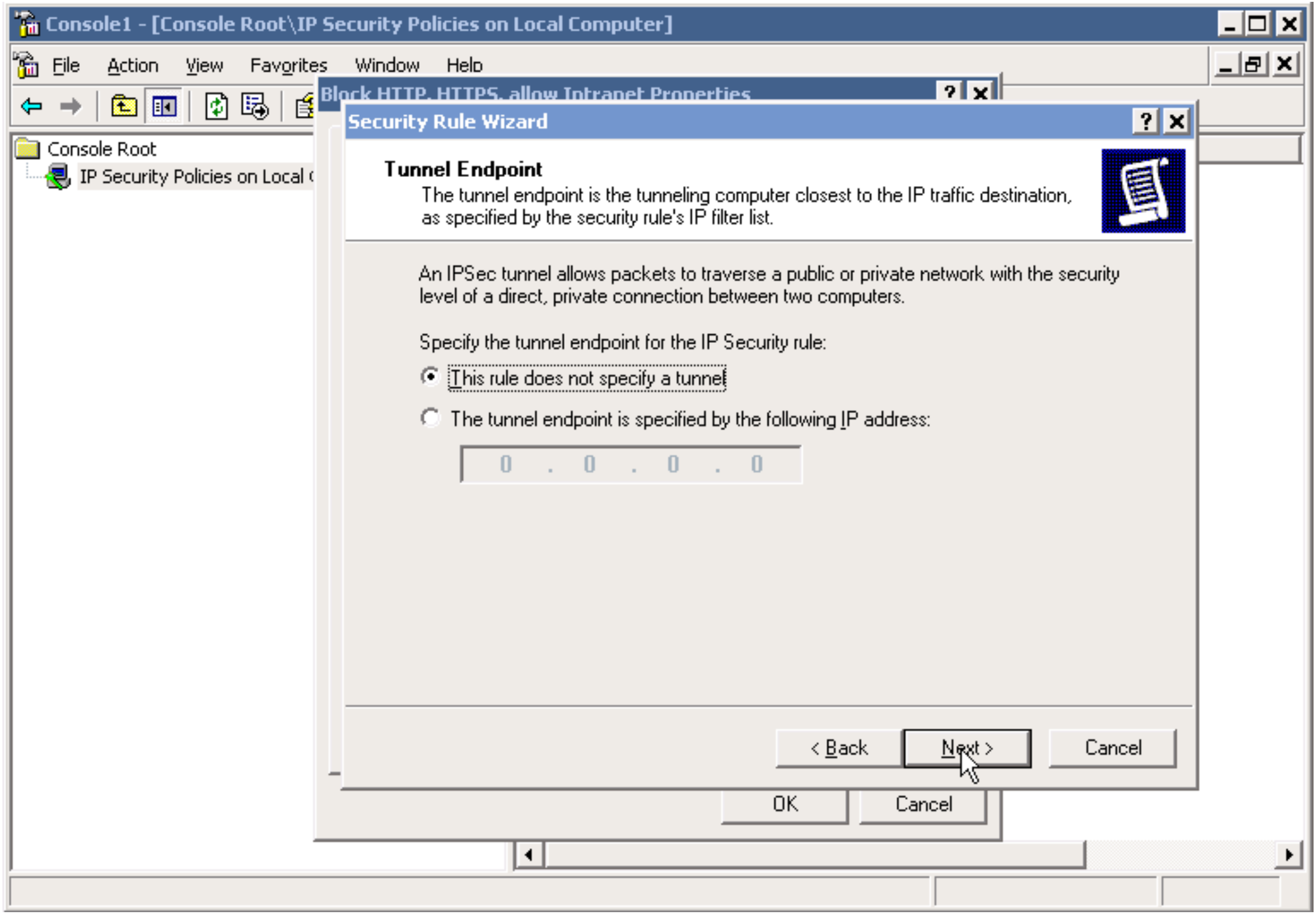

Console1 - [Console Root\IP Security Policies on Local Computer]
File
Action
View
Favorites
Window
Help
Console Root
IP Security Policies on Local Computer
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Name
Description
Policy Assigned
For all IP traffic, always req...
No
Communicate normally (uns...
No
For all IP traffic, always req...
No
Creates an IP Security policy.

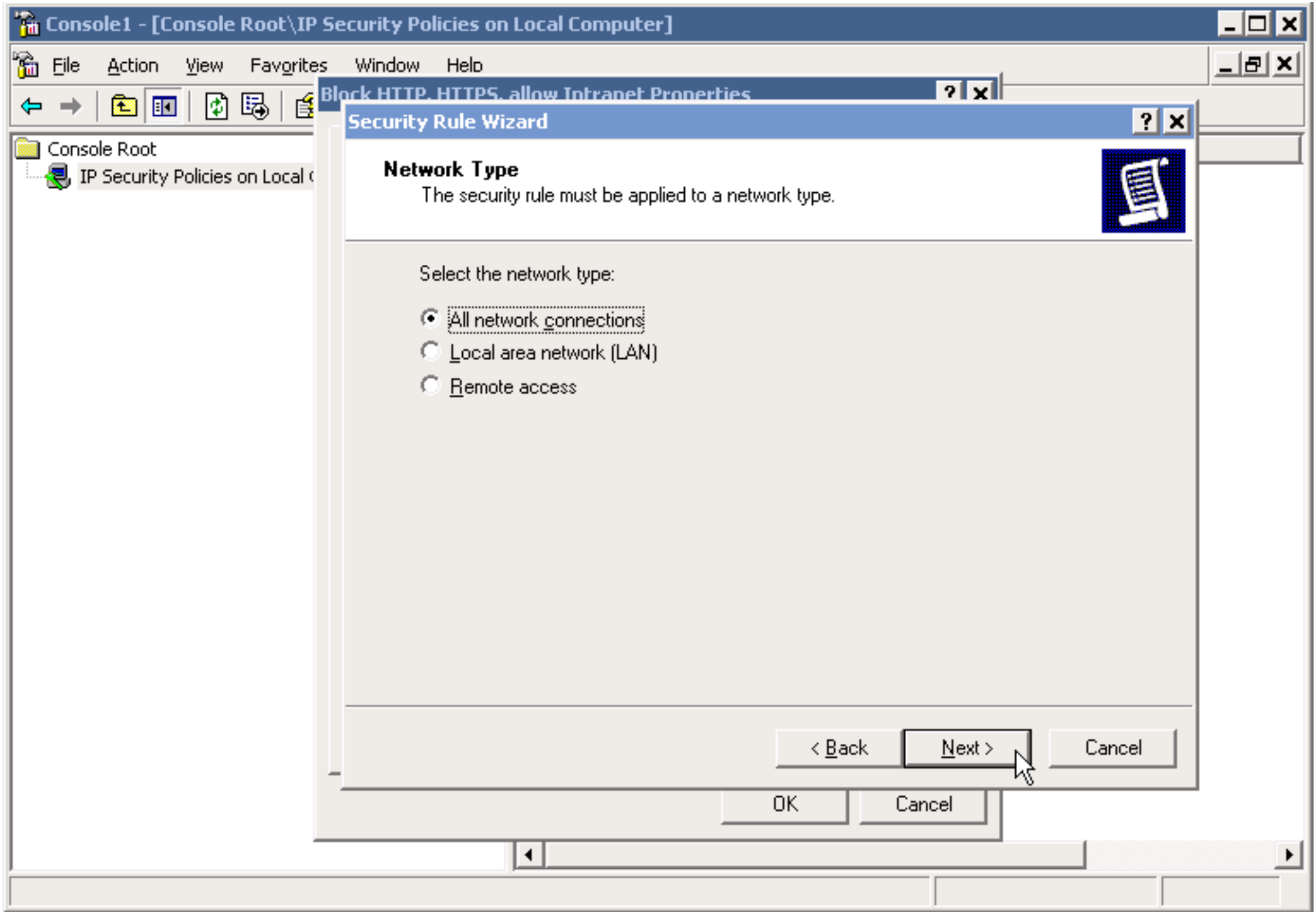

Console1 - [Console Root\IP Security Policies on Local Computer]
IP Security Policy Wizard
IP Security Policy Name
Name this IP Security policy and provide a brief description
Name:
Block HTTP, HTTPS, allow Intranet
Description:
< Back
Next >
Cancel
Policy Assigned
, always req...
No
ormally (uns...
No
, always req...
No

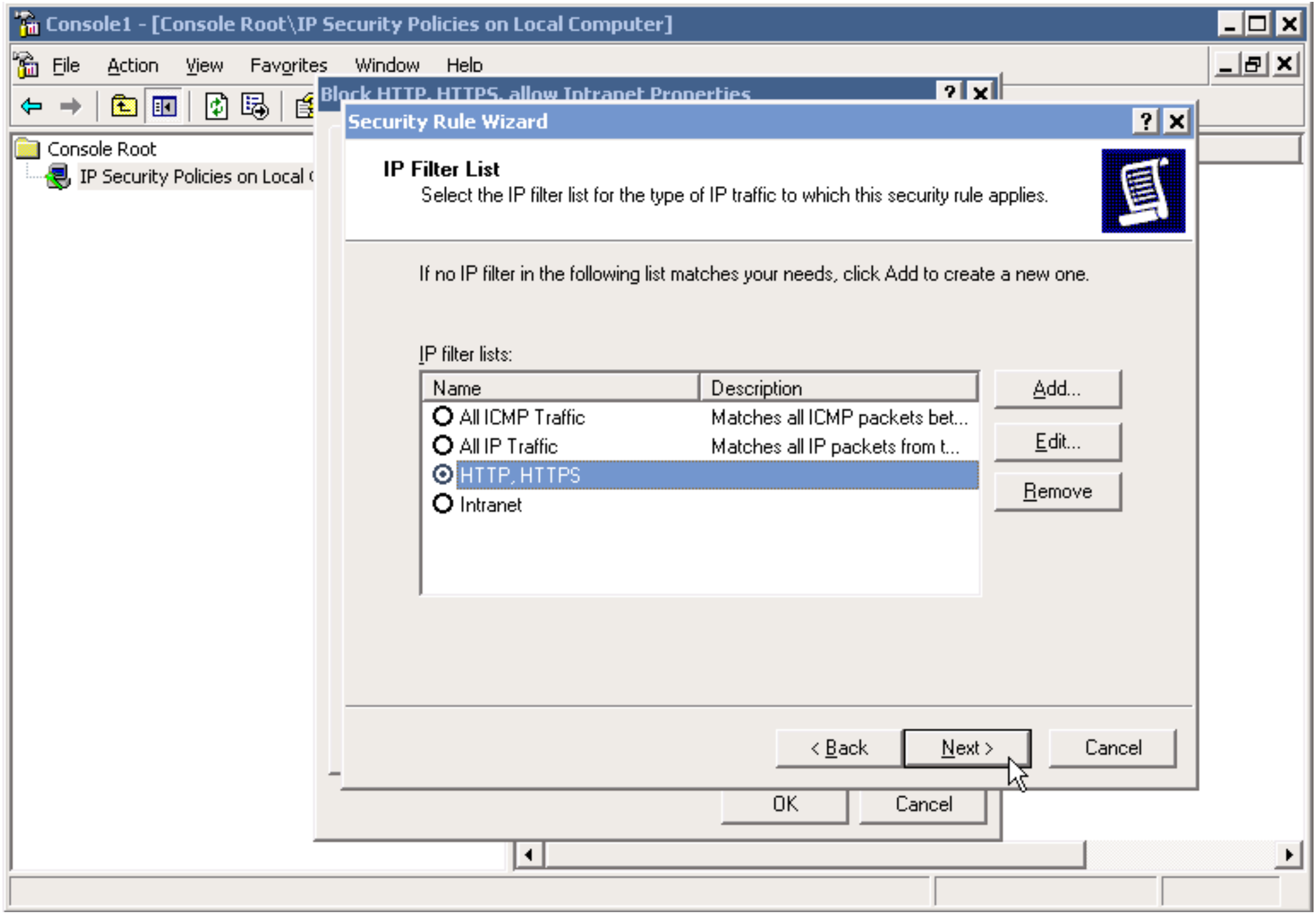

Console1 - [Console Root\IP Security Policies on Local Computer]
IP Security Policy Wizard
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
Activate the default response rule.
< Back
Next >
Cancel
Policy Assigned
, always req...
No
ormally (uns...
No
, always req...
No

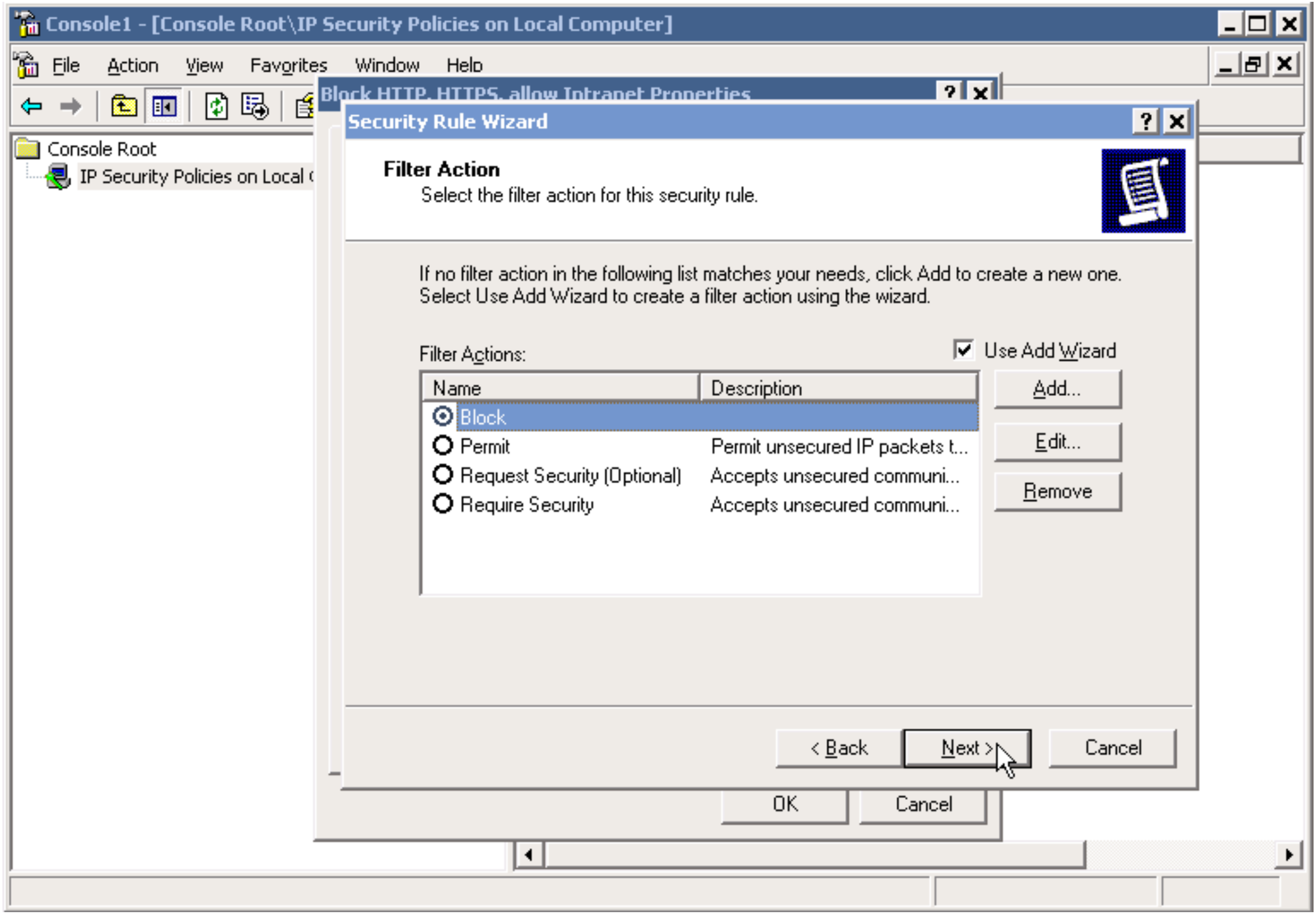

Console1 - [Console Root\IP Security Policies on Local Computer]
Policy Assigned
, always req...
No
ormally (uns...
No
, always req...
No
IP Security Policy Wizard
Completing the IP Security Policy Wizard
You have successfully completed specifying the properties for your new IP Security policy.
To edit your IP Security policy now, select the Edit properties check box, and then click Finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel

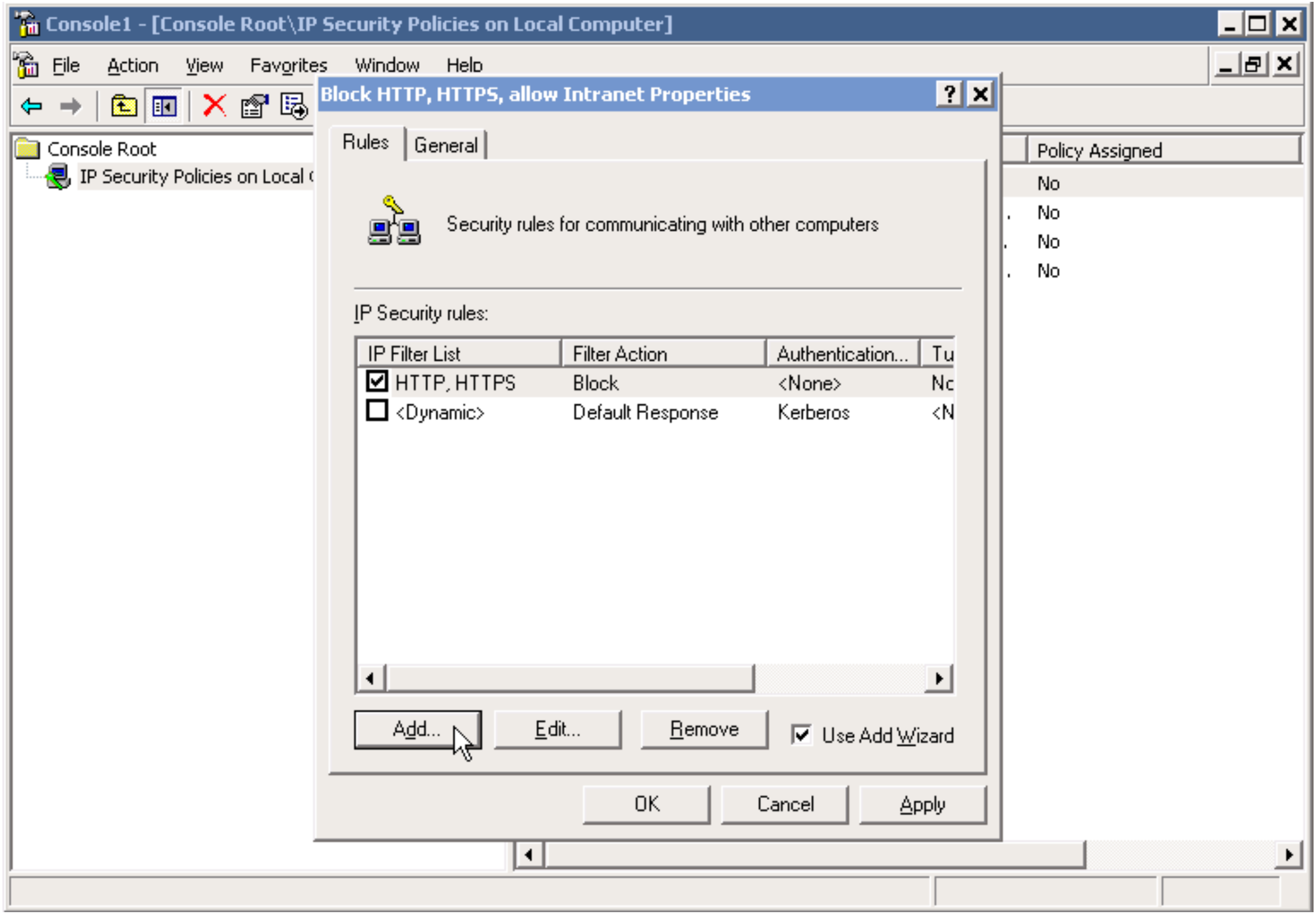

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Policy Assigned
No
No
No
No
Block HTTP, HTTPS, allow Intranet Properties
Rules
General
Security rules for communicating with other computers
IP Security rules:
IP Filter List
Filter Action
Authentication...
Tu
<Dynamic>
Default Response
Kerberos
<N
Add...
Edit...
Remove
Use Add Wizard
OK
Cancel

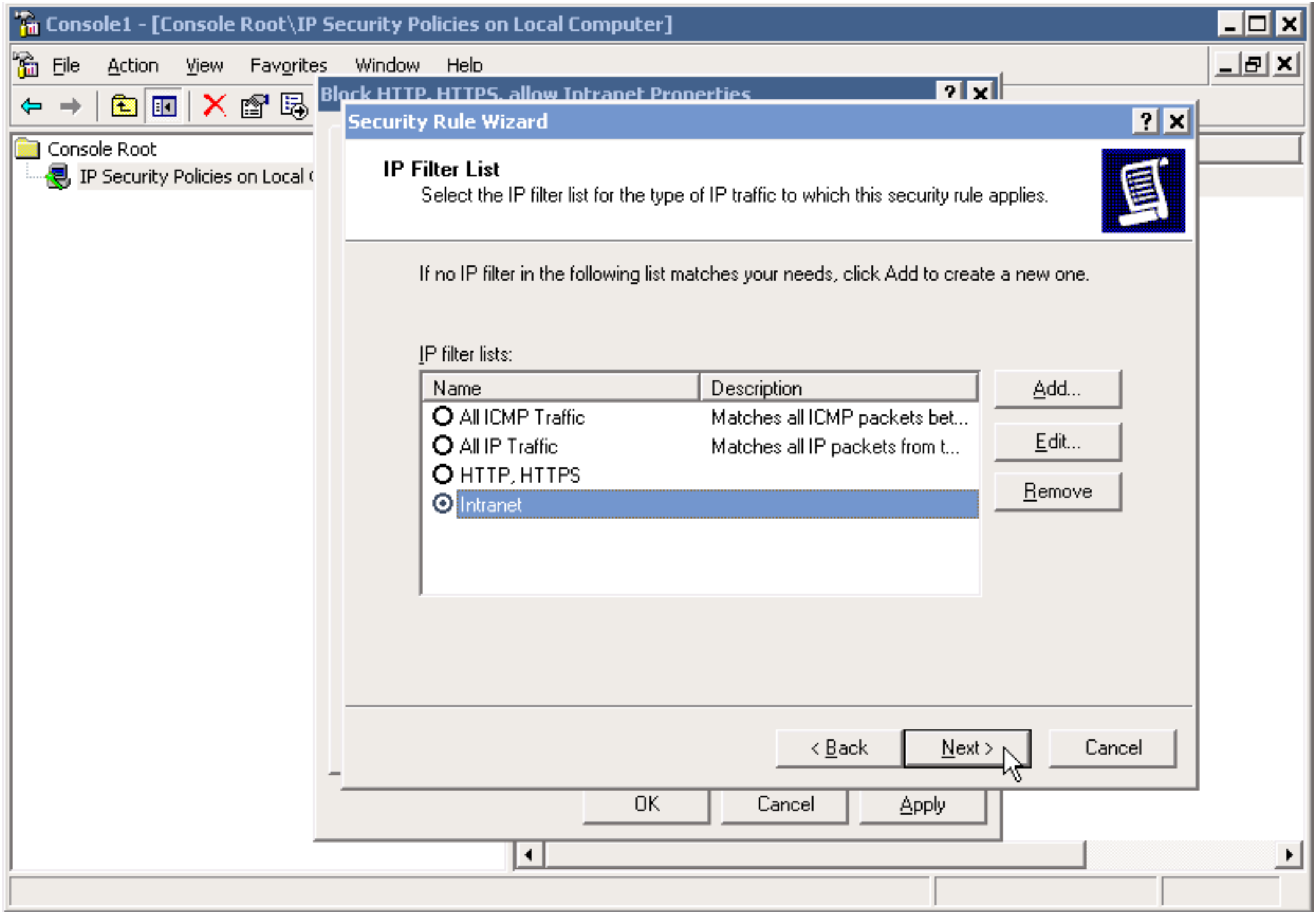

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Block HTTP, HTTPS, allow Intranet Properties
Security Rule Wizard
Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.
An IPSec tunnel allows packets to traverse a public or private network with the security level of a direct, private connection between two computers.
Specify the tunnel endpoint for the IP Security rule:
This rule does not specify a tunnel
The tunnel endpoint is specified by the following IP address:
0 . 0 . 0 . 0
< Back
Next >
Cancel
OK
Cancel

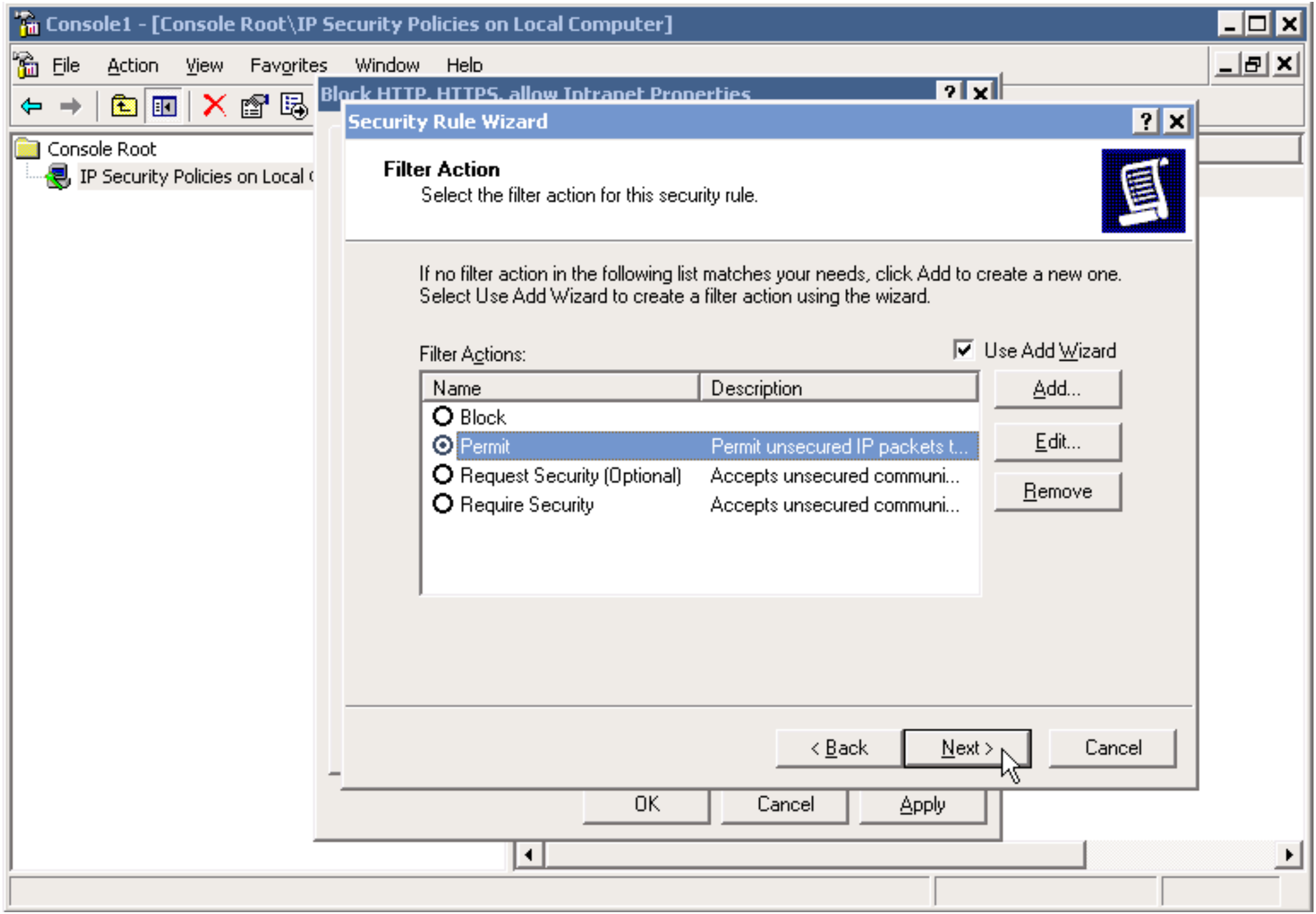

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Block HTTP, HTTPS, allow Intranet Properties
Security Rule Wizard
Network Type
The security rule must be applied to a network type.
Select the network type:
All network connections
Local area network (LAN)
Remote access
< Back
Next >
Cancel
OK
Cancel

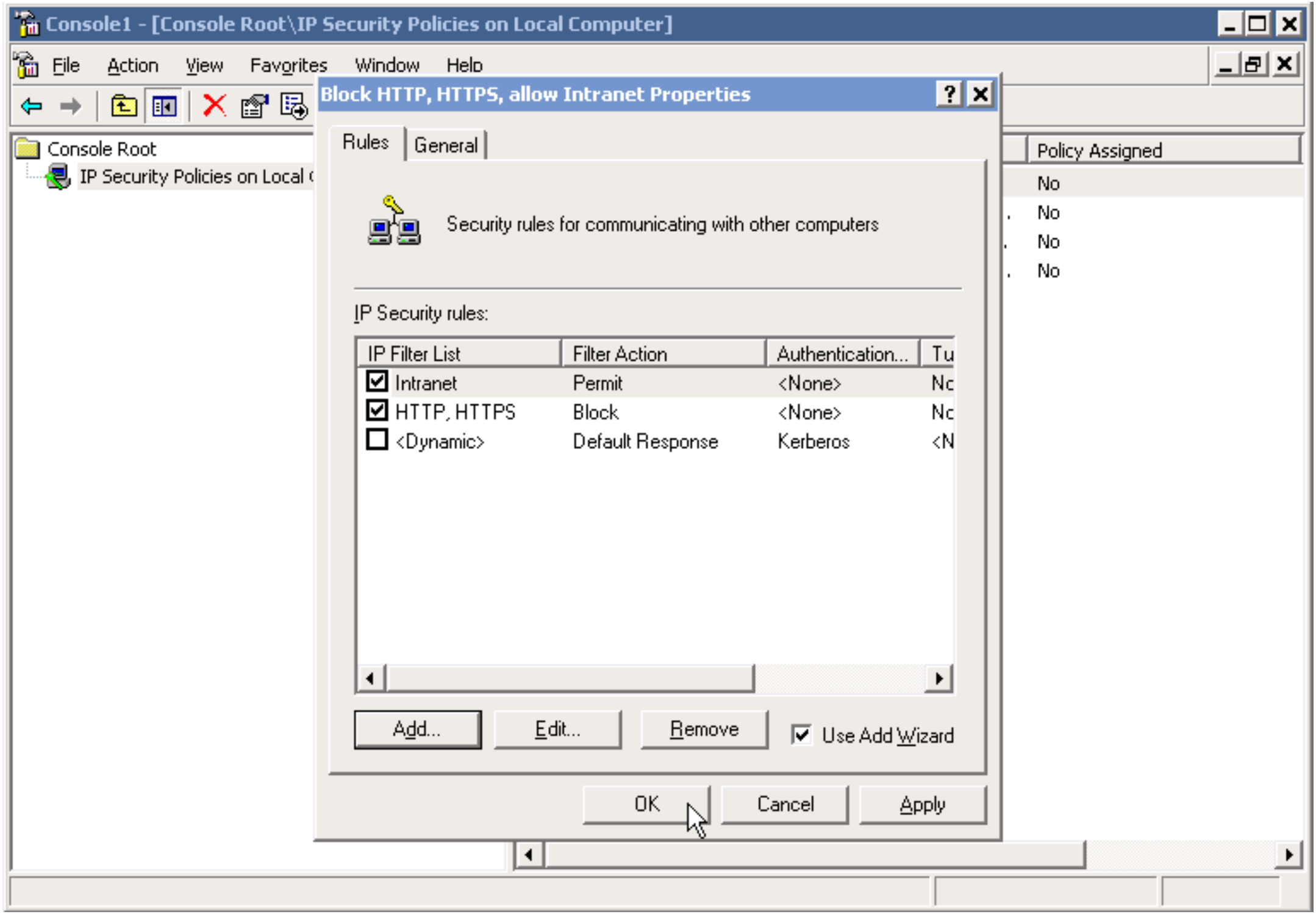

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Block HTTP, HTTPS, allow Intranet Properties
Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
HTTP, HTTPS
Intranet
Add...
Edit...
Remove
< Back
Next >
Cancel
OK
Cancel

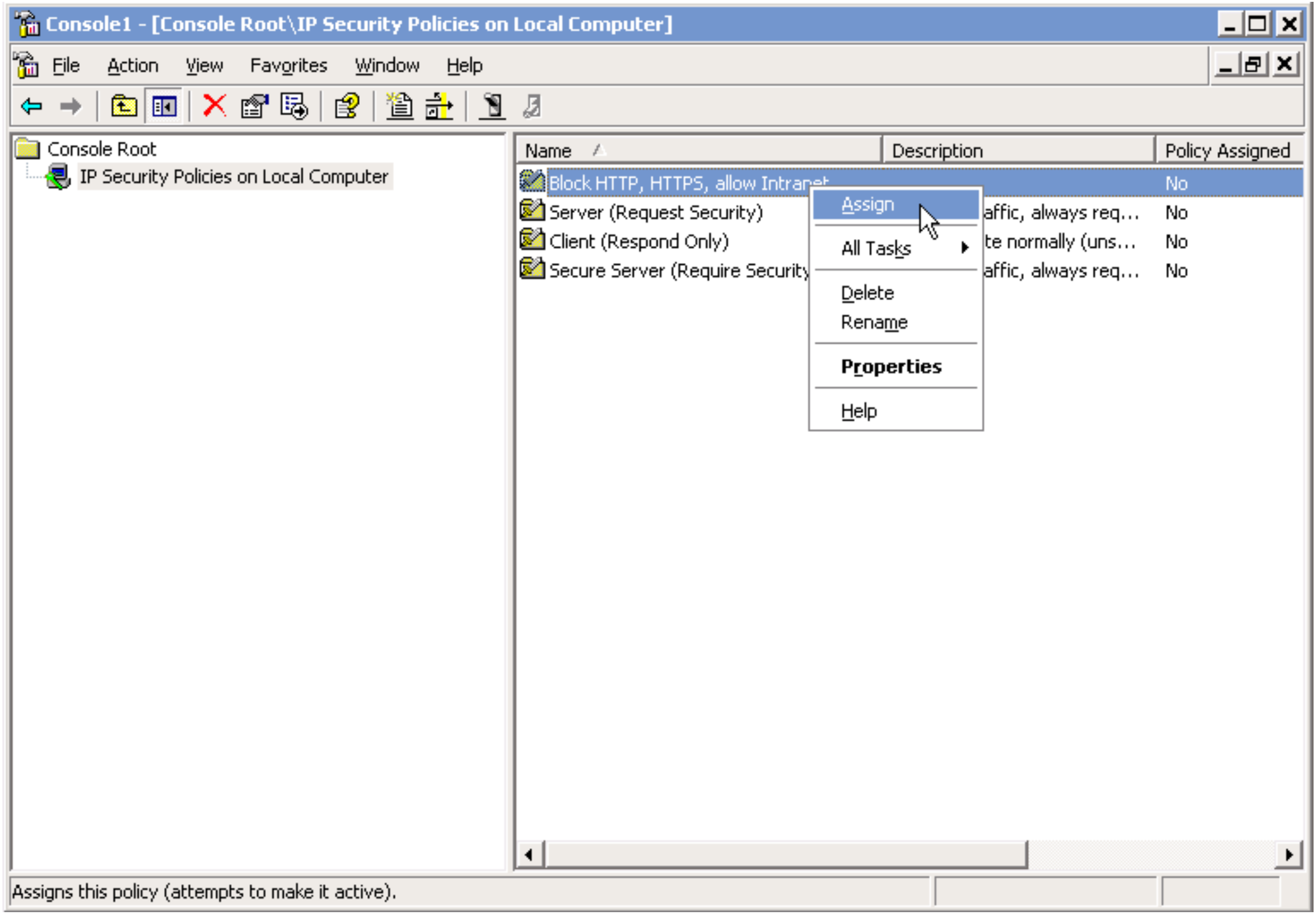

Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Block HTTP, HTTPS, allow Intranet Properties
Security Rule Wizard
Filter Action
Select the filter action for this security rule.
If no filter action in the following list matches your needs, click Add to create a new one.
Select Use Add Wizard to create a filter action using the wizard.
Filter Actions:
Use Add Wizard
Name
Description
Block
Permit
Permit unsecured IP packets t...
Request Security (Optional)
Accepts unsecured communi...
Require Security
Accepts unsecured communi...
Add...
Edit...
Remove
< Back
Next >
Cancel
OK
Cancel


Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Policy Assigned
No
No
No
No
Block HTTP, HTTPS, allow Intranet Properties
Rules
General
Security rules for communicating with other computers
IP Security rules:
IP Filter List
Filter Action
Authentication...
Tu
HTTP, HTTPS
Block
<None>
Nc
<Dynamic>
Default Response
Kerberos
<N
Add...
Edit...
Remove
Use Add Wizard
OK
Cancel
Apply


Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Block HTTP, HTTPS, allow Intranet Properties
Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
HTTP, HTTPS
Intranet
Add...
Edit...
Remove
< Back
Next >
Cancel
OK
Cancel
Apply


Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Block HTTP, HTTPS, allow Intranet Properties
Security Rule Wizard
Filter Action
Select the filter action for this security rule.
If no filter action in the following list matches your needs, click Add to create a new one.
Select Use Add Wizard to create a filter action using the wizard.
Filter Actions:
Use Add Wizard
Name
Description
Block
Permit
Permit unsecured IP packets t...
Request Security (Optional)
Accepts unsecured communi...
Require Security
Accepts unsecured communi...
Add...
Edit...
Remove
< Back
Next >
Cancel
OK
Cancel
Apply


Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local
Policy Assigned
No
No
No
No
Block HTTP, HTTPS, allow Intranet Properties
Rules
General
Security rules for communicating with other computers
IP Security rules:
IP Filter List
Filter Action
Authentication...
Tu
Intranet
Permit
<None>
Nc
HTTP, HTTPS
Block
<None>
Nc
<Dynamic>
Default Response
Kerberos
<N
Add...
Edit...
Remove
Use Add Wizard
OK
Cancel
Apply


Console1 - [Console Root\IP Security Policies on Local Computer]
File
Action
View
Favorites
Window
Help
Console Root
IP Security Policies on Local Computer
Name
Description
Policy Assigned
Block HTTP, HTTPS, allow Intranet
No
Server (Request Security)
affic, always req...
No
Client (Respond Only)
te normally (uns...
No
Secure Server (Require Security
affic, always req...
No
Assign
All Tasks
Delete
Rename
Properties
Help
Assigns this policy (attempts to make it active).