Moschip Security Processor MCS1000

MCS1000 10/100 Secure NIC

Version 1.0

August, 2005

For more information contact : mcs1000spt@moschip.com

All information in this document is believed to be accurate as of the publish date.

VPNow™ is a registered trademark of Artec Group. ARM is a registered trademark of ARM Limited. All other brands or product names are the property of their respective holders.

Moschip Semiconductor products are not authorized for use as critical components in life support devices or systems without the express written approval of the president of Moschip Semiconductor, Ltd.

Moschip Semiconductor believes the information in this document to be accurate and reliable. However, it is subject to change without notice. No responsibility is assumed by Moschip Semiconductor for its use, nor for infringement of patent or other rights of third parties. No part of this document may be reproduced, or transmitted in any form or by any means without prior consent of Moschip Semiconductor, Ltd.

TABLE OF CONTENTS

MCS1000 10/100 Secure NIC

1. Introduction

MCS1000 is a fully featured 10/100 network Interface card with additional feature of hardware acceleration of the IPSec protocol. The MCs1000 can be used any windows and Linux operating systems and can add up to a maximum of 3-port NIC to the system. A simple driver needs to be installed on the operating systems and the integer intensive math IPSEC protocol will be offloaded to the NIC.

The MCS1000 can be programmed as a 1, 2, 3 port secure NIC card and can be modified for Optical Fiber Interface using an external PHY.

Below shown is the one port Copper and Fiber interface of MCS1000

Copper Media

Fiber Media

2. NIC Features

- 32 bit -33 MHz ,PCI 2.2 interface
- Ethernet interface (Copper or FIBER)
    - Compliant with IEEE 802.3 specification.
    - Supports 10/100 Mbps data transfer rates.
    - Supports both Full duplex /Half duplex operation.
    - Supports flow control for Full duplex Operation.
- Hardware offload engine.
    - IPSEC task offloading, compliant with Microsoft NDIS architecture (Windows).Secures sensitive data at wire speeds- with DES/3DES Encryption, MD5/SHA1 hashing, RFC-2402 and RFC2406 Authentication and upto 72 security Associations.
- Ethernet features
    - Addressing filtering modes are

    - § Unicast 48 bit address
    - § 64 hash filtered multicast addresses
    - § Pass all Multicast addresses
    - § Promiscuous mode
    - § Broadcast
  - o Optimized transmit and receive queues. Descriptor ring management hardware for transmit and receive.
  - o IEEE 802.3x compliant flow control support with software controllable pause time and threshold values.
- Management
  - o WMI (Windows Management Interface)

- Operating System support for Windows 2000/Xp/2003 server,Linux2.4

3. Installing and Connecting the NIC

This user guide explains how to install the MCS1000 10/100 Secure NIC in a computer running any of the following operating systems: • Windows 2003 Server • Windows XP • Windows 2000 • Linux 2.4 .

Minimum Installation Requirements

Your client computer or server must meet the following requirements before you can successfully install the MCS1000 Secure NIC:

• Processor (client or server) — Intel Pentium or above

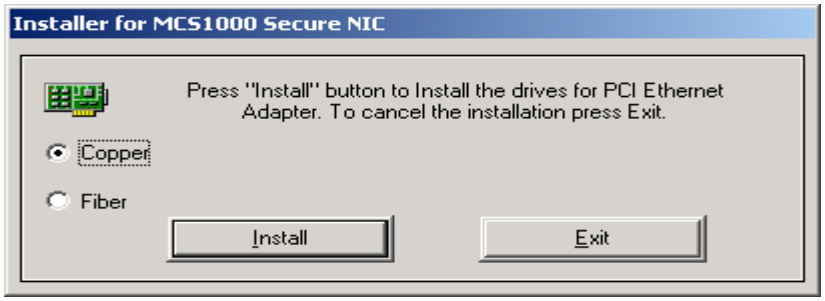
• Available bus-mastering PCI slot, conforming to PCI 32-bit specifications, revision 2.2
• CD-ROM drive

4. Windows 2003 Server Driver Installation

This Section explains the following tasks on a computer running Windows 2003 Server:

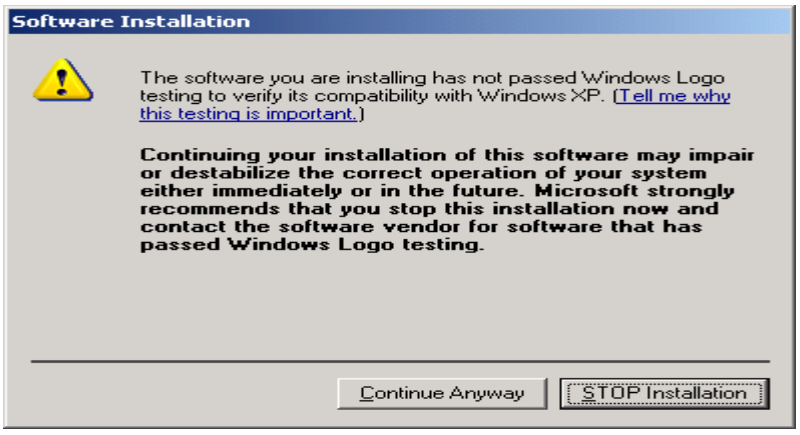
- To obtain the latest version of a driver, go to: http://www,moschip.com/downloadmatrix 1

- Click on the "Windows Secure NIC driver "under Product "MCS1000".and download the zip file on to PC.
- Unzip the folder and enter into the MCS1000_Windows_SecureNIC_drivers directory were the driver files are present.
- Run the MCS1000Setup.exe to install the driver on to the PC.

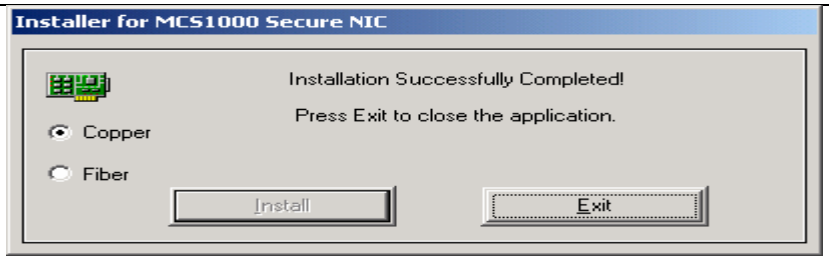


- Select "Copper" radio button, to install driver for Copper interface or select "Fiber" radio button for fiber Interface and click on Install to install the driver for MCS1000 secure NIC .

- A dialog pops up indicating the driver installed is not digitally signed .click on "Continue Anyway" to continue the installation.



- Click on Exit to complete the Installation.

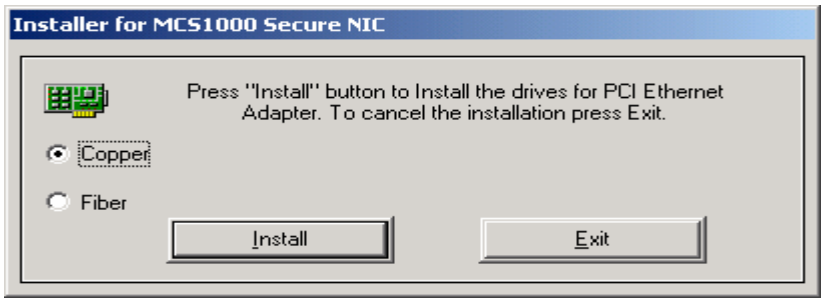


- Turn of the power to the computer.
- Make sure that the NIC is plugged into the PCI slot of the computer
- Turn on the power to the computer.
- The PC detects the MCS1000 Secure NIC card and “Found New Hardware “ window pops up.
- Make sure “Search for a suitable driver for my device (recommended)” is selected. Click on Next and so that the Operating System automatically searches for the driver until all the ports get installed.
- The Driver Files Search Results screen appears, then click on “Next” and the “Completing the Found New Hardware Wizard” screen appears with the name of the installed NIC.
- Click Finish. The driver is installed.
- Verify the NIC installation in Device Manager under Network Adapters.
- To verify successful NIC installation:
  Open the Windows Start menu, and then select Control Panel.
  Double click Network Connections.
  Check connections in the LAN or High-Speed Internet window. It will show “Moschip Secure NIC Adapter.

5. Windows XP Driver Installation

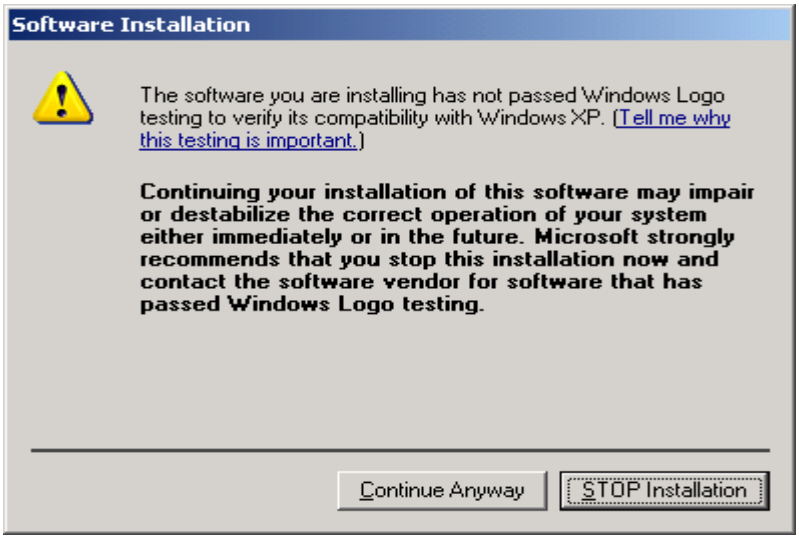
This Section explains the following tasks on a computer running Windows XP:

- To obtain the latest version of a driver, go to: http://www,moschip.com/downloadmatrix 1
- Click on the “Windows Secure NIC driver “under Product “MCS1000”.and download the zip file on to PC.
- Unzip the folder and enter into the MCS1000_Windows_SecureNIC_drivers directory were the driver files are present.
- Run the MCS1000Setup.exe to install the driver on to the PC.

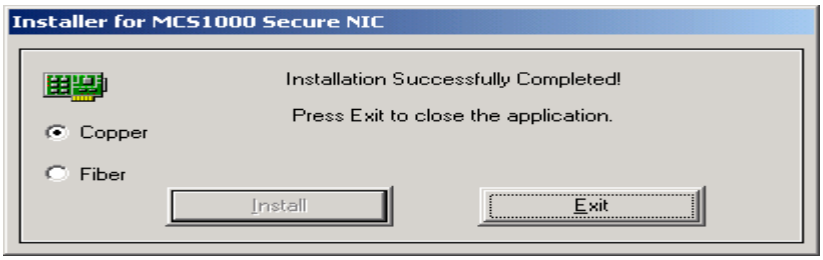


- Select “Copper” radio button, to install driver for Copper interface or select “Fiber” radio button for fiber Interface and click on Install to install the driver for MCS1000 secure NIC.

- A dialog pops up indicating the driver installed is not digitally signed .click on “Continue Anyway” to continue the installation.



- Click on Exit to complete the Installation.



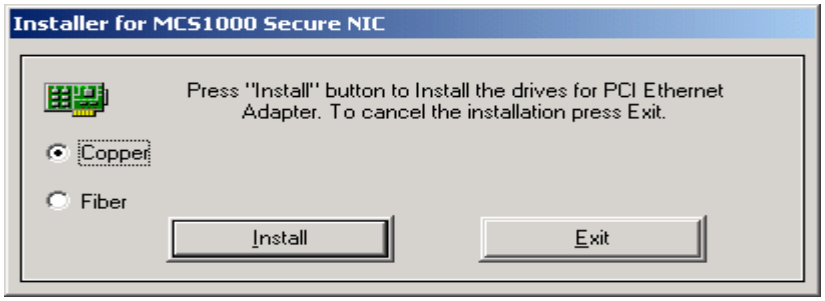
- Turn of the power to the computer.
- Make sure that the NIC is plugged into the PCI slot of the computer
- Turn on the power to the computer.
- The PC detects the MCS1000 Secure NIC card and "Found New Hardware "window pops up.
- Make sure "Search for a suitable driver for my device (recommended)" is selected. Click on Next and so that the Operating System automatically searches for the driver until all the ports get installed.
- The Driver Files Search Results screens appears and then click on "Next" and the "Completing the Found New Hardware Wizard" screen appears with the name of the installed NIC.
- Click Finish. The driver is installed.
- Verify the NIC installation in Device Manager under Network Adapters.
- To verify successful NIC installation:
  Open the Windows Start menu, and then select Control Panel.
  Double click Network Connections.
  Check connections in the LAN or High-Speed Internet window. It will show "Moschip Secure NIC Adapter.

6. Windows 2000 Driver Installation

This section explains the following tasks on a computer running Windows 2000

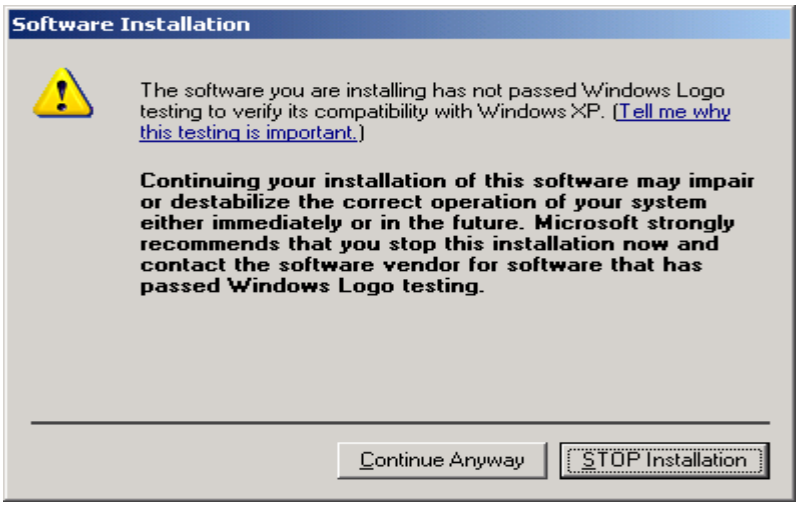
- To obtain the latest version of a driver, go to: http://www,moschip.com/downloadmatrix 1

- Click on the “Windows Secure NIC driver “under Product “MCS1000”.and download the zip file on to PC.
- Unzip the folder and enter into the MCS1000_Windows_SecureNIC_drivers directory were the driver files are present.
- Run the MCS1000Setup.exe to install the driver on to the PC.

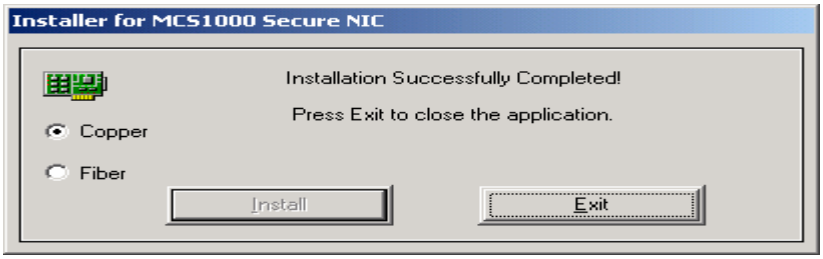


- Select “Copper” radio button, to install driver for Copper interface or select “Fiber” radio button for fiber Interface and click on Install to install the driver for MCS1000 secure NIC.

- A dialog pops up indicating the driver installed is not digitally signed .click on “Continue Anyway” to continue the installation.



- Click on Exit to complete the Installation.



- Turn of the power to the computer.
- Make sure that the NIC is plugged into the PCI slot of the computer
- Turn on the power to the computer.
- The PC detects the MCS1000 Secure NIC card and "Found New Hardware "window pops up.
- Make sure "Search for a suitable driver for my device (recommended)" is selected. Click on Next and so that the Operating System automatically searches for the driver until all the ports get installed.
- The Driver Files Search Results screens appears and then click on "Next" and the "Completing the Found New Hardware Wizard" screen appears with the name of the installed NIC.
- Click Finish. The driver is installed.
- Verify the NIC installation in Device Manager under Network Adapters.
- To verify successful NIC installation:
  Open the Windows Start menu, and then select Control Panel.
  Double click Network Connections.
  Check connections in the LAN or High-Speed Internet window. It will show "Moschip Secure NIC Adapter.

7. Linux 2.4 Driver Installation

This chapter explains how to install the network driver on a computer running Linux 2.4.
To obtain the latest version of a driver, go to
http://www.moschip.com/htmls/download_matrix1.htm

1) Linux requirement:

This development is made for Linux 2.4.20-8 kernel that comes with the Redhat 9 distribution.

2) Configuring the kernel:

The user is suggested to make copy of Linux source located at /usr/src

For example: /usr/src/linux2.4.20-8-IPSECcopy.

There are two patches that need to be applied to make the Linux kernel to support offloading of IPsec tasks and work with openswan and MCS1000 card. The patches are present in the /MCS1000_Linux/kernel_patch/ directory of the Driver disk

The two patches are named as follows in the Driver tar file .In kernel_patch directory.

1. patch-netdevice
2. patch-skbuff

Copy both patches to /usr/src/linux2.4.20-8-IPSECcopy directory and apply the patches in the same directory.
The patches can be applied using the following commands;

```
patch -p1 include/linux/netdevice.h <  patch-netdevice
patch -p1 include/linux/skbuff.h < patch-skbuff
```

After successfully applying the patch the user should recompile the kernel.

Go to /usr/src/linux2.4.20-8-IPSECcopy .

Commands to recompile the kernel:

1. make clean
2. make mrproper
3. make menuconfig:
   Select <File Systems> and select the <ext3> for built-in kernel support.

User should select 'Exit' and then select 'Yes' for saving the current configuration.
4. make dep
5. make modules
6. make modules_install
7. make bzImage

Once this process is over, we will have this kernel image in
/usr/src/linux.xxx/arch/i386/boot/bzImage and copy this image file into
/boot/XXXXXXXX.

Now open the file /etc/grub.conf
this should look like the follows

```
title Red Hat Linux-up (2.4.20-8)
root (hd0,1)
kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
initrd /initrd-2.4.20-8.img
```

Now we need to add a new entry for kernel and with the some title and kernel with the path of bzImage.

```
title Red Hat Linux (2.4.20-8-IPSEC)
root (hd0,1)
kernel /XXXXXXXXX ro root=LABEL=/
initrd /initrd-2.4.20-8.img
```

Reboot the system with the new Kernel "Red Hat Linux (2.4.20-8-IPSEC)"

Check point : After you reboot check whether you are in the newly compiled enviroment by typing "uname -a" , it should show linux2.4..xxxcustom.

3) Compiling Openswan:

Download the tar file from location
http://www.openswan.org/download/openswan-2.3.0.tar.gz

untar the file with command
tar -xzvf filename.tar
now we will have a directory openswan.2.3.0

Compilation:

We need replace some files in the openswan directory.
Copy the following files present in the "Openswan" directory of the Driverdisk to openswan-2.3.0/linux/net/ipsec .

```
ipsec_esp.c
```

ipsec_rcv.c
ipsec_xmit.c
ipsec_sa.c
MOS_OFFLOAD_SA.h
pfkey_v2_parser.c

Copy the file ipsec_sa.h to openswan-2.3.0/linux/include/openswan

In the directory openswan-2.3.0, execute

make KERNELSRC=/usr/src/linux-2.4.xxx module minstall programs install

This will install openswan related files in the system.
To start the IPSEC, execute
#ipsec setup start
More details are in the man pages of ipsec.

4) Loading MCS1000 Linux Network driver .

Go to the directory "network_driver" where the driver files are present and execute
#./load.sh

To install the driver execute

make install (Installing the Network Driver)

to Uninstall the Network Driver execute the command

make remove (Uninstalling the Network Driver)

Note: Before Uninstalling the Network Driver stop ipsec by issuing the command "ipsec setup stop".

Note:
1) This script will install the MCS1000 as eth1 device. This will work when there is only one more network card present in the system (which is required for a tunnel mode setup).

2) The ipsec.conf file generated by the Openswan uses "eth1" as the device to be used for security tasks. Make sure that this is the same as MCS1000 card.
refer to man pages of "ipsec.conf" and "ipsec.secrets" file for more details on setting up security.

8. Installing and Configuring Data Encryption Offloads

The MCS1000 Secure NIC performs data encryption processing offloads in Windows 2003, Windows XP, and Windows 2000.
Encryption processing is handled entirely by the NIC. The NIC enables true end-to-end network security at the data capacity of the connected network cable, without sacrificing performance. This chapter provides instructions for configuring IPSec in Windows 2003, Windows XP, and Windows 2000 environments.

Overview Internet Protocol Security (IPSec) is a framework of open standards for ensuring secure private communications over IP networks. IPSec ensures confidentiality, integrity, access control, and authenticity of data communications across a public IP network.

Offloading Encryption Processing You can configure any two (or more) computers running Windows 2003, Windows XP, or Windows 2000 to perform IPSec encryption by changing the Local Security Setting in the operating system. With most non-MCS1000 Secure NICs, all the IPSec processing is done by the host central processing unit (CPU), which significantly diminishes CPU performance. The MCS1000 Secure NIC can offload all the encryption processing from the host CPU, thereby freeing the CPU to work on other tasks.

9. Selecting Basic or Strong Encryption Processing

The MCS1000 Secure NIC provides Data Encryption Standard (DES) 56-bit encryption processing and 3DES (3DES 168-bit) encryption processing. You can configure the MCS1000 Secure NIC to process data packets encrypted with either DES (basic) or 3DES (strong) algorithms. DES and 3DES are IPSec bulk encryption algorithms for coding data. DES encrypts 64-bit data blocks using a 56-bit key. DES can be applied in several modes. 3DES (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys. 3DES is also known as 168-bit data encryption.

10. Configuring IPSec in Windows 2003, Windows XP, and Windows 2000

The MCS1000 Secure NIC accelerates IP security (IPSec) data encryption from supported operating systems that provide this offload capability. This feature is currently available in the Windows 2003, Windows XP, and Windows 2000 operating systems. IPSec primarily consists of two parts: • encryption/decryption • authentication To send or receive encrypted data with a MCS1000 Secure NIC installed, you must first create a security policy, and then enable encryption on the NIC. The security policy establishes and defines how encrypted network traffic between your computer and a specified server occurs. Authentication enables the receiver to verify the sender of a packet by adding key

fields to a packet without altering the packet data content. The following table shows the available levels of encryption

11.Creating a Security Policy

The process you use to create and enable a security policy depends on your network environment requirements. The following is an example of one approach to creating a security policy. Encryption Type Encryption Level Description AH Medium Authentication only ESP High Authentication and encryption Custom Varies Provides encryption and an extra authentication that includes the IP header. Custom allows you to select options for both AH and ESP, such as MD5/SHA-1 and DES/3DES. And you can select the rate at which new keys are negotiated. Microsoft uses IKE key exchange to renew keys every x seconds or y bytes. For more information, refer to the Microsoft documentation about creating IPSec flows. NOTE: You must complete all of the sequences in this section to establish and enable a security policy for transmitting and receiving encrypted data over the network.

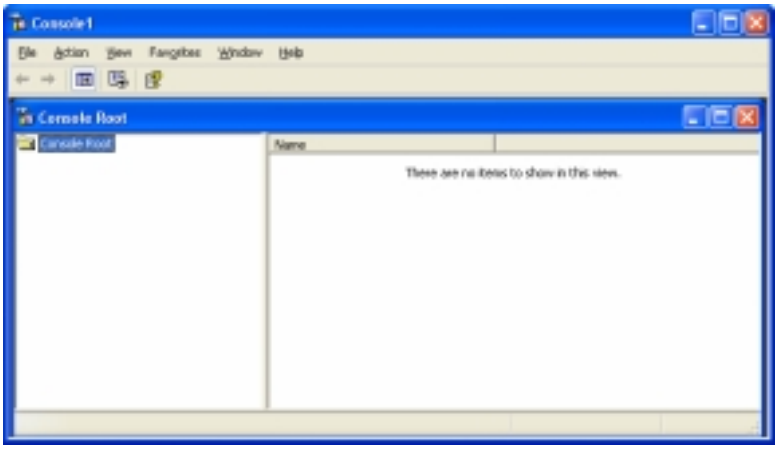
A. Defining the Console

This sequence establishes the Console and defines its parameters.

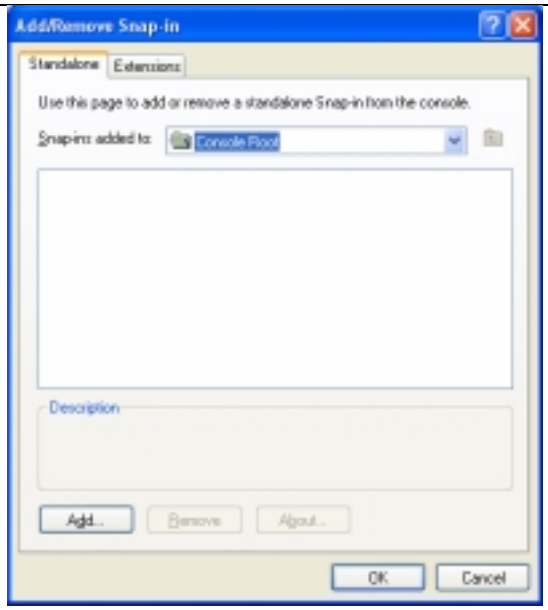
To define the Console:

1) In the Windows taskbar, click Start, Programs, Accessories, and then Command Prompt.

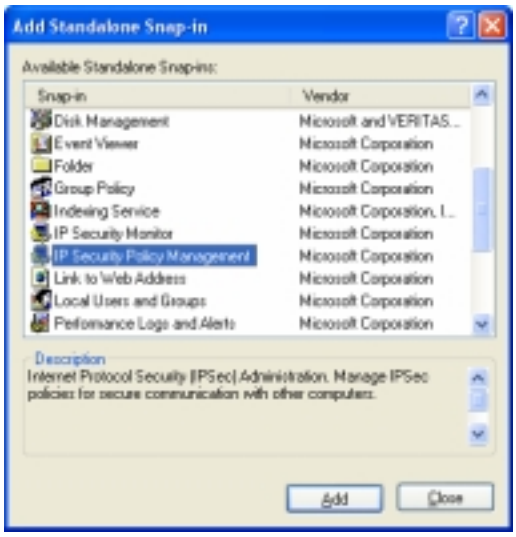
2) At the DOS prompt, enter: MMC The Console1 screen appears.



3) In the menu click Console, and then Add/Remove Snap-in. The Add/Remove Snap-in screen appears.

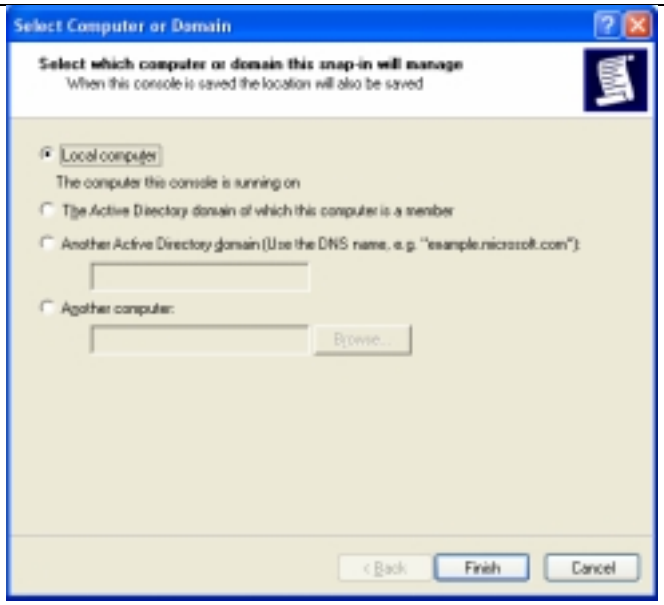


4) Click Add. The Add Standalone Snap-in screen appears.



5) Select IP Security Policy Management, and then click Add. The Select which computer this Snap-in will manage screen appears.

6) Enable the Local computer option.

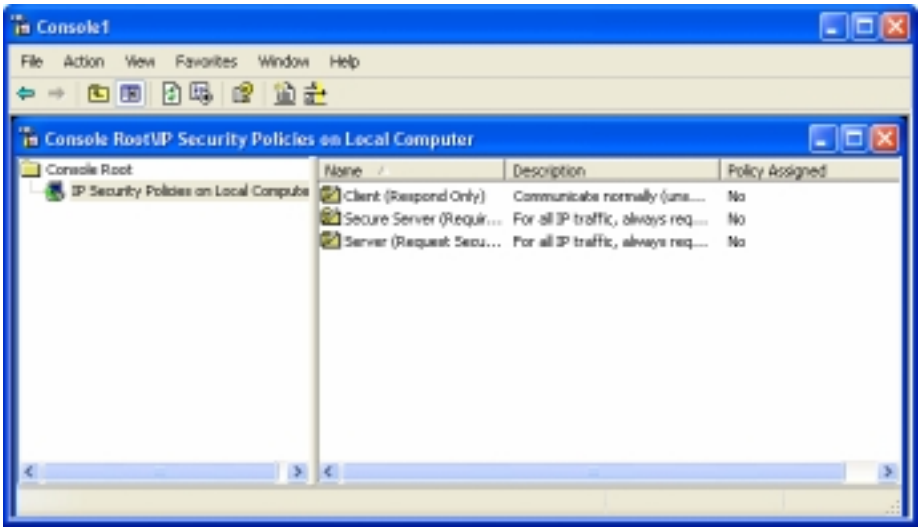


7) Click Finish, Close, and then OK.

B. Creating the Policy

This sequence creates and names the new security policy.
The Console1 and Console Root screen appears with IP Security Policies on Local Machine displayed in the list.

1. In the left pane, click IP Security Policies on Local Machine.

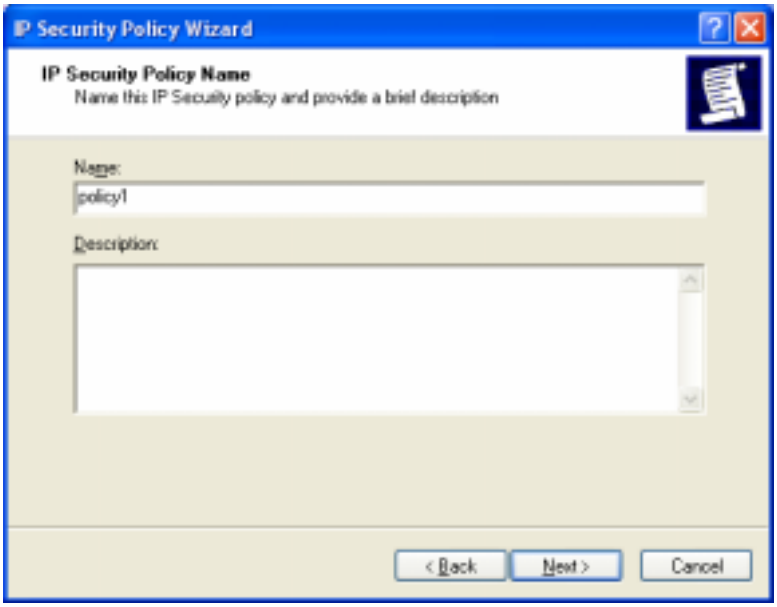


2. Right-click inside the right pane below the list items.

3. From the pop-up menu, select Create IP Security Policy. The IP Security Policy Wizard starts

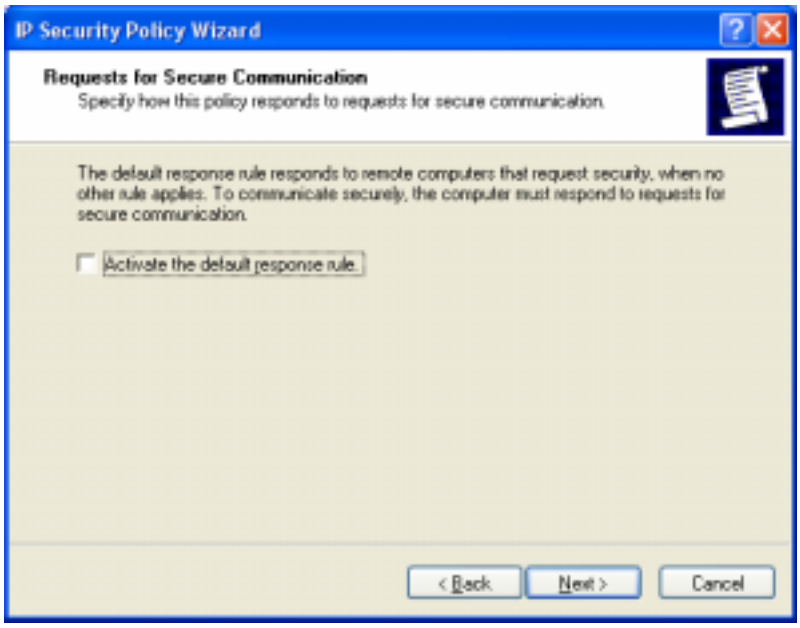
4. Click Next. The IP Security Policy Name screen appears.

5. Enter a name for the new security policy that you are creating. You can enter a description to help you identify this policy.



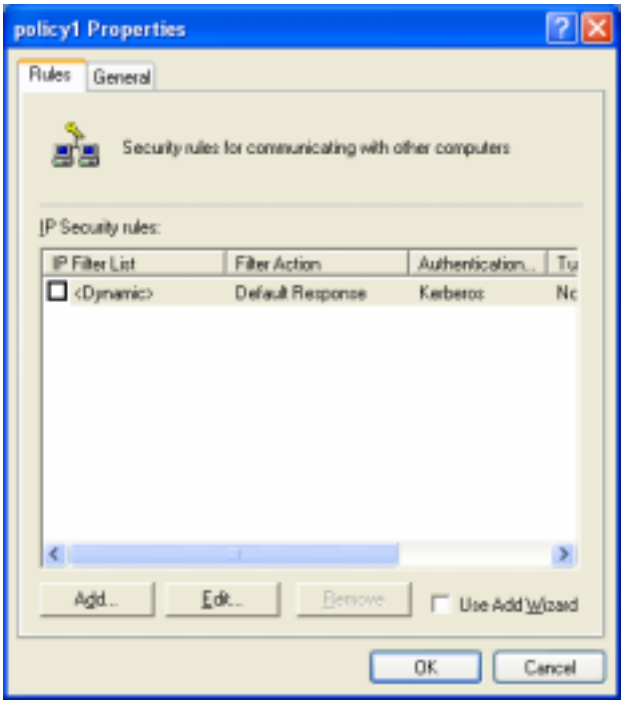
6. Click Next. The Requests for Secure Communication screen appears.

7. Clear the Activate the default response rule check box.



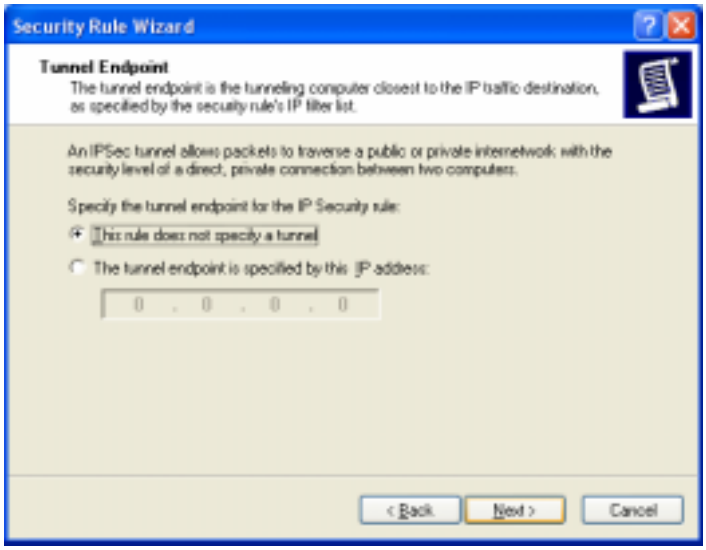
8. Click Next and then Finish.

9. A screen appears with the name of the new security policy in the title bar.

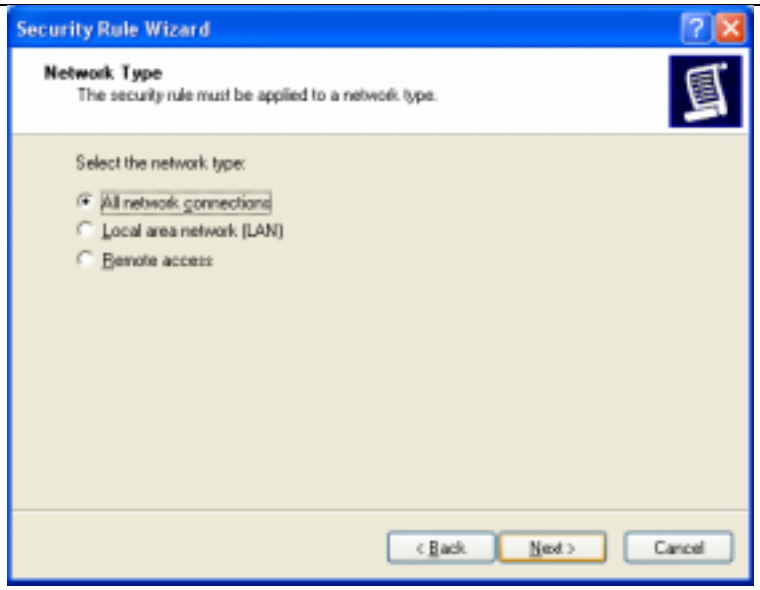


10. Click Add. The Security Rule Wizard starts.

11. Click Next. The Tunnel Endpoint screen appears.

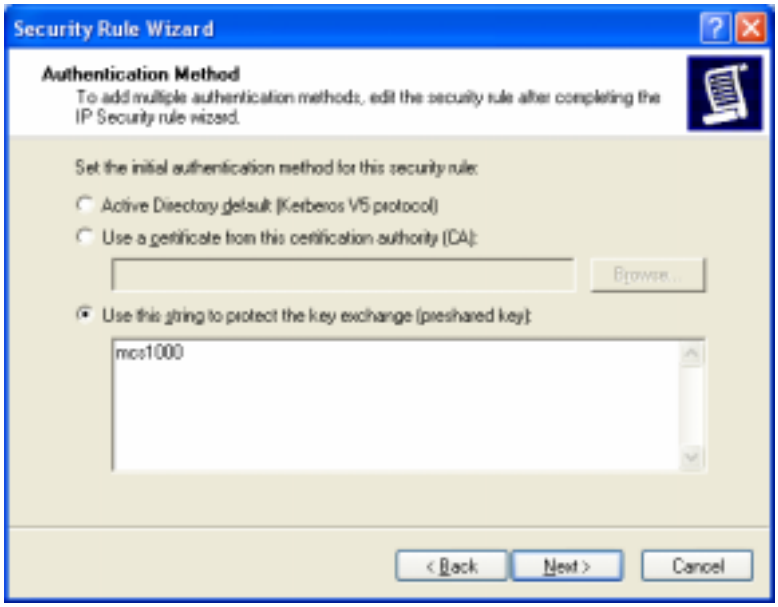


12. Enable the default option This rule does not specify a tunnel, and then click Next. The Network Type screen appears.



13. Enable the default option All network connections, and then click Next.

14. The Authentication Methods screen appears.

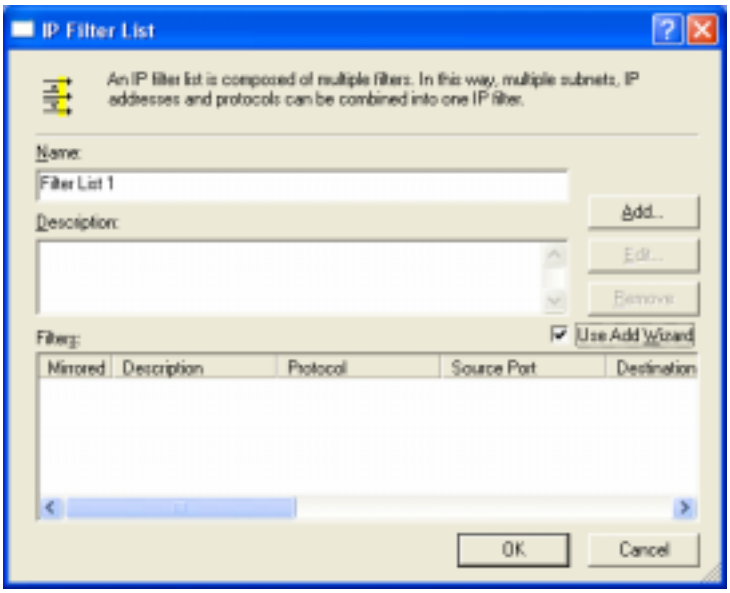


15. Enable the Use this string to protect the key exchange (Preshared key): option, type the appropriate string text in the entry field, and then click Next.

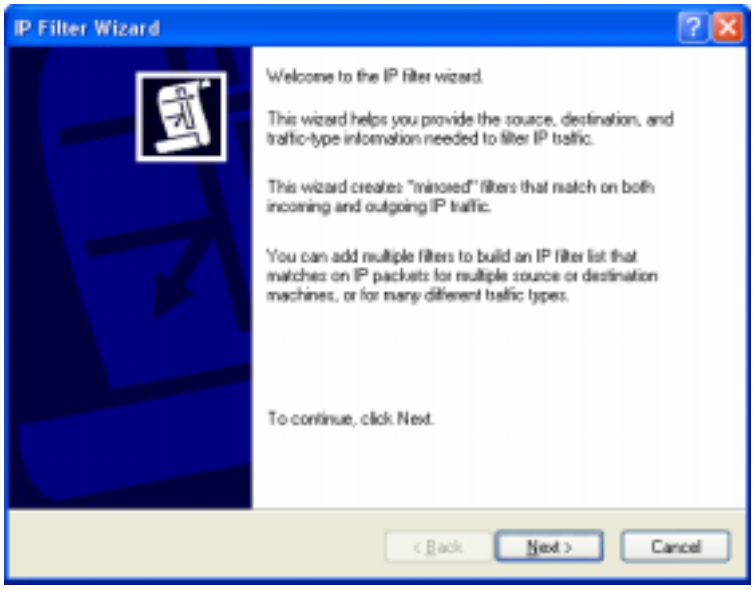
C. Creating a Filter

This sequence creates a filter for the policy. The IP Filter List screen appears.

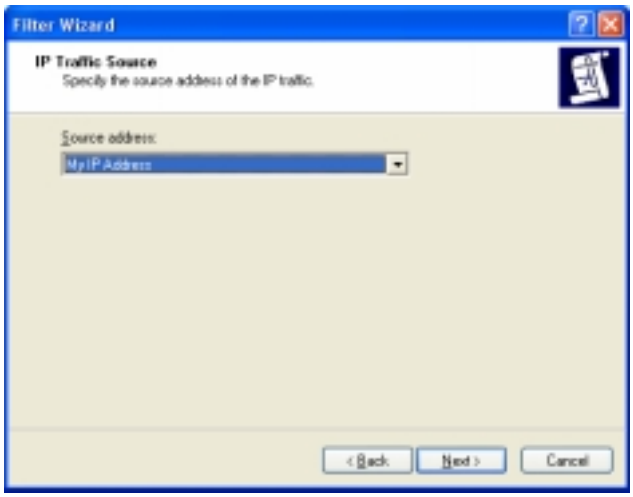
1) Click Add. A new IP Filter List screen appears.



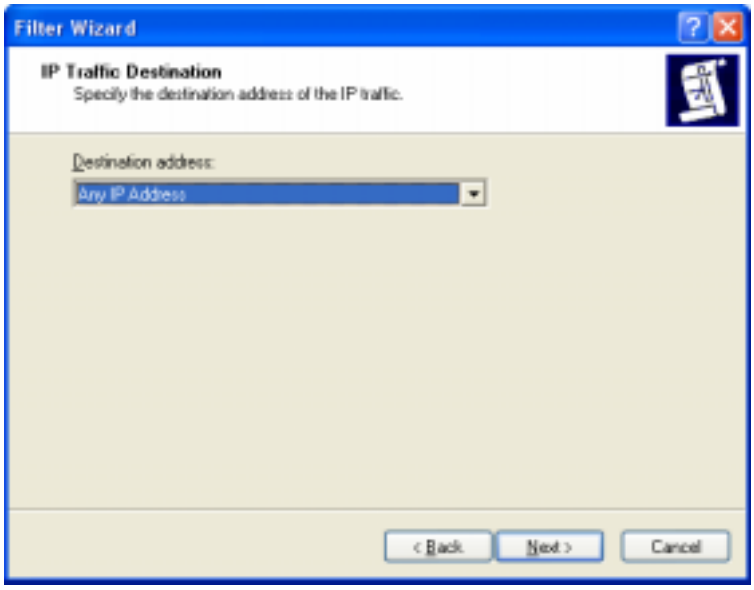
2) Enter a name for the filter, and then click Add. The IP Filter Wizard starts.



3) Click Next. The IP Traffic Source screen appears.

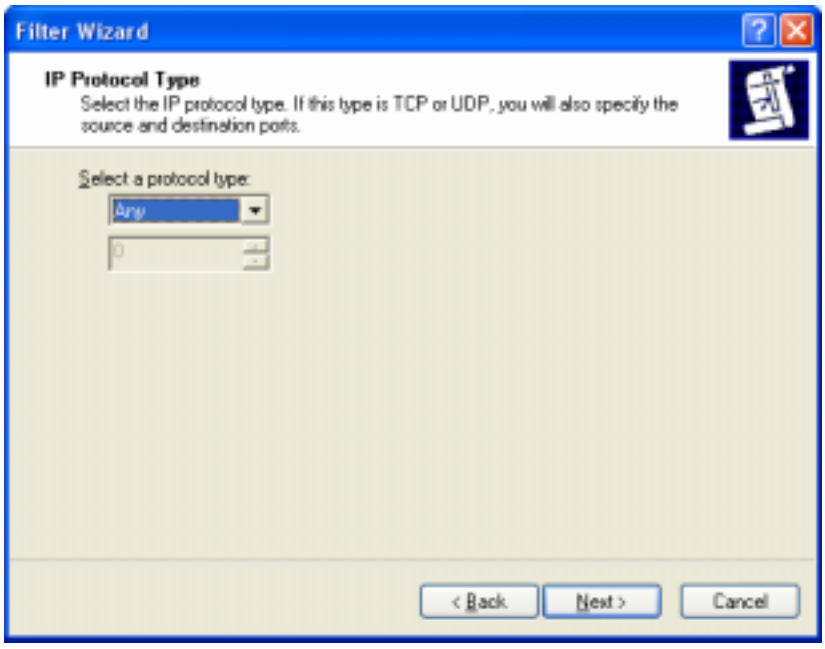


4) Click Next. The IP Traffic Destination screen appears.

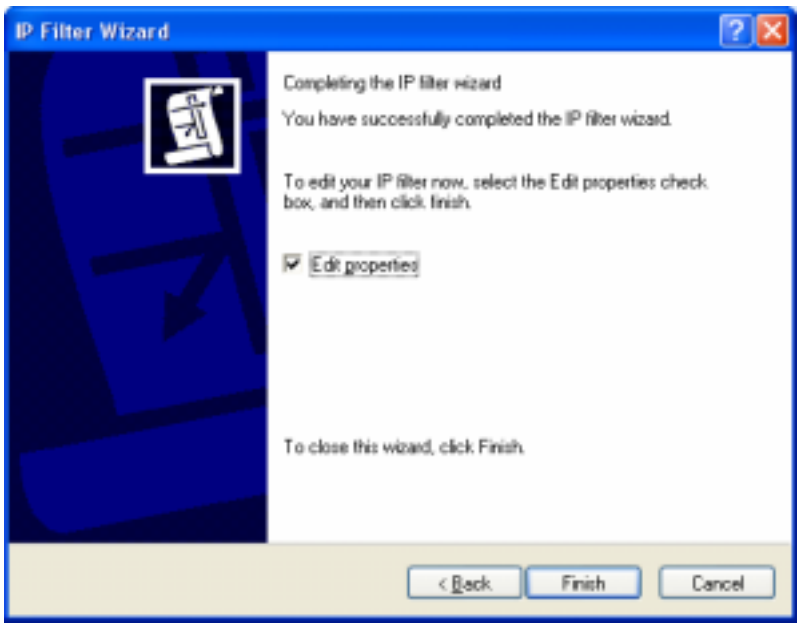


5) Select A Specific IP Address in the pull-down list. The IP Address entry box appears on the IP Traffic Destination screen.

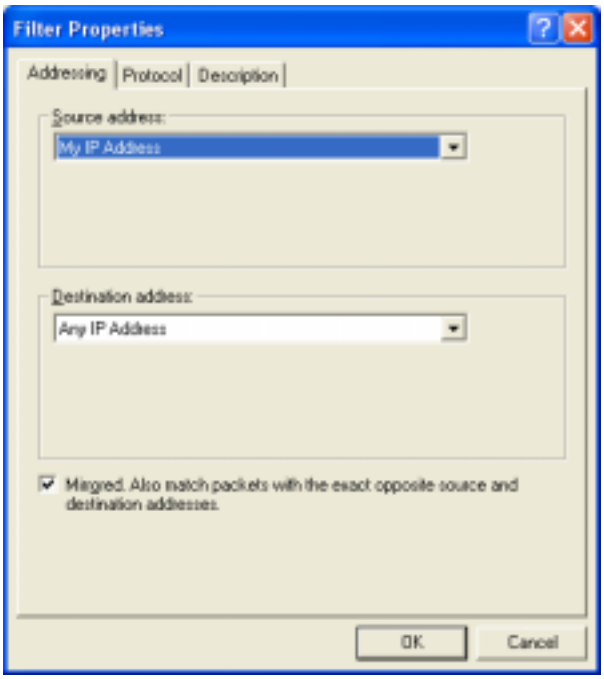
6) Enter destination IP address, and then click Next. The IP Protocol Type screen appears.



7) Accept the default, and then click Next.



8) Click Finish to close the IP Filter Wizard.



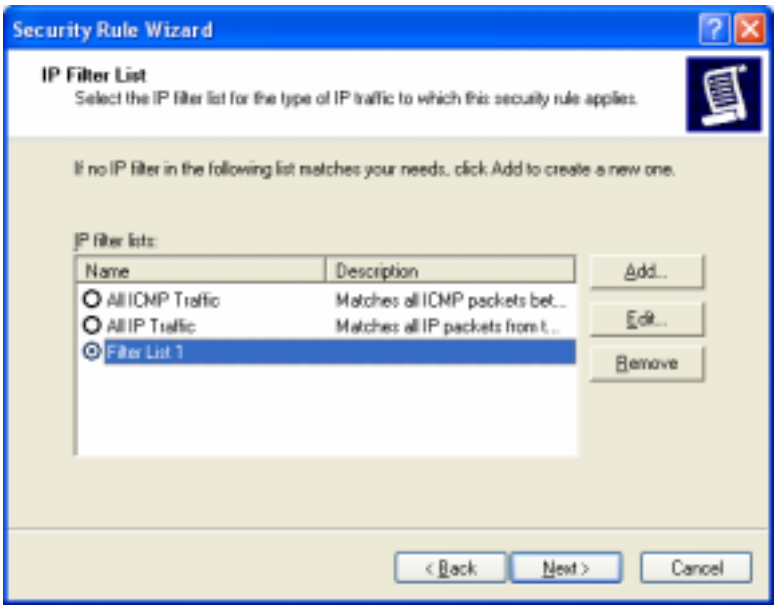
9) Click Close to close the IP Filter List screen.

D. Binding the Filter

This sequence attaches the new filter to the policy.

The IP Filter List screen appears.

1. Enable the option for the new filter name and make sure that the new filter name is selected.

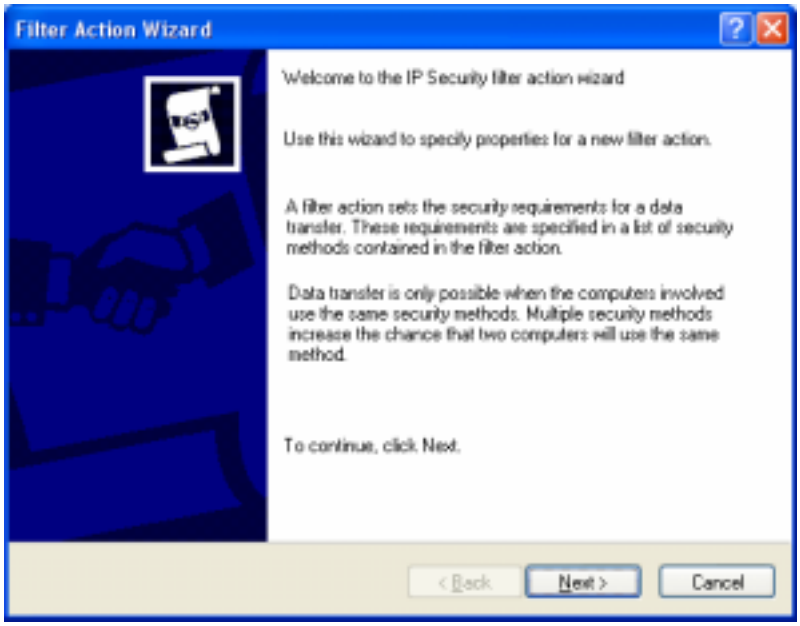


2. Click Next.

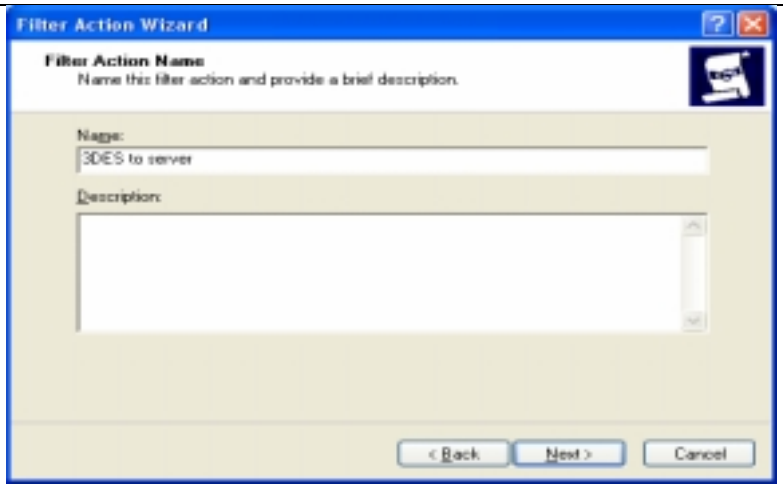
E .Creating the Filter Action

This sequence defines how the filter acts on the policy. The Filter Action screen appears.

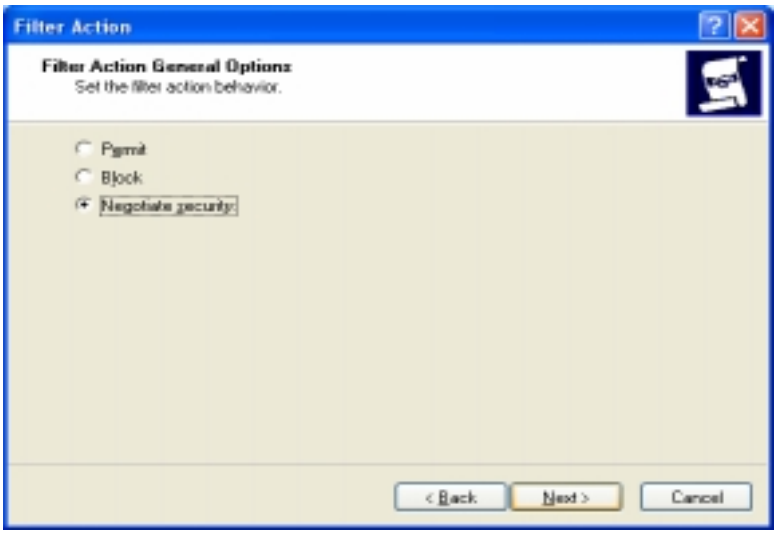
1. Click Add. The Filter Action Wizard starts.



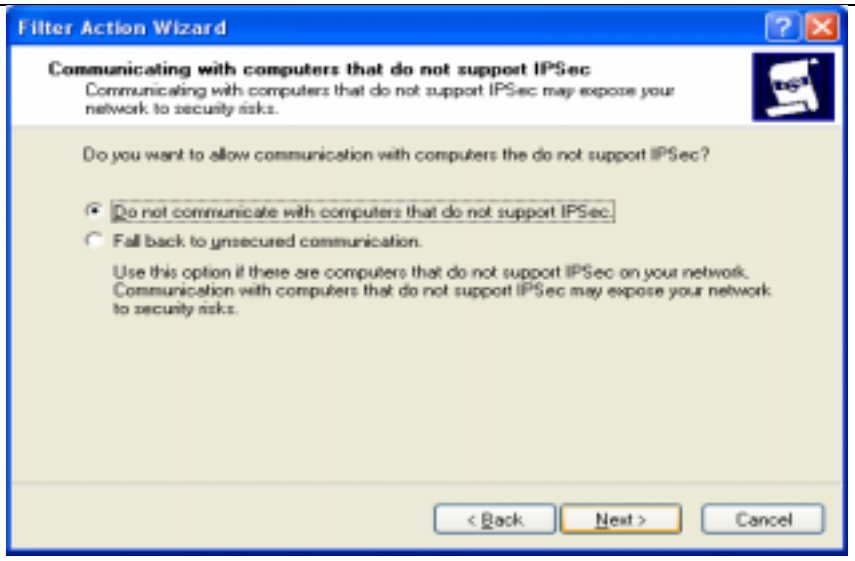
2. Click Next. The Filter Action Name screen appears.



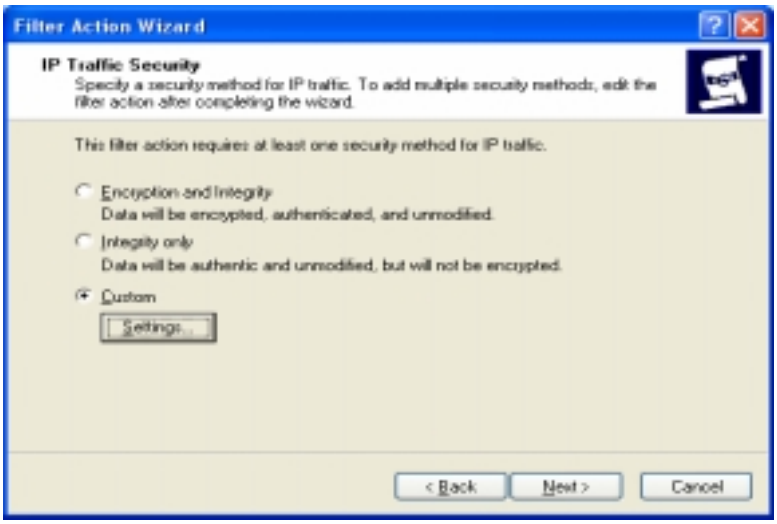
3. Enter a name (for example: 3DES to the Server), and then click Next. The Filter Action General Options screen appears.



4. Accept the default, and then click Next. The screen, communicating with computers that do not support IPsec, appears.



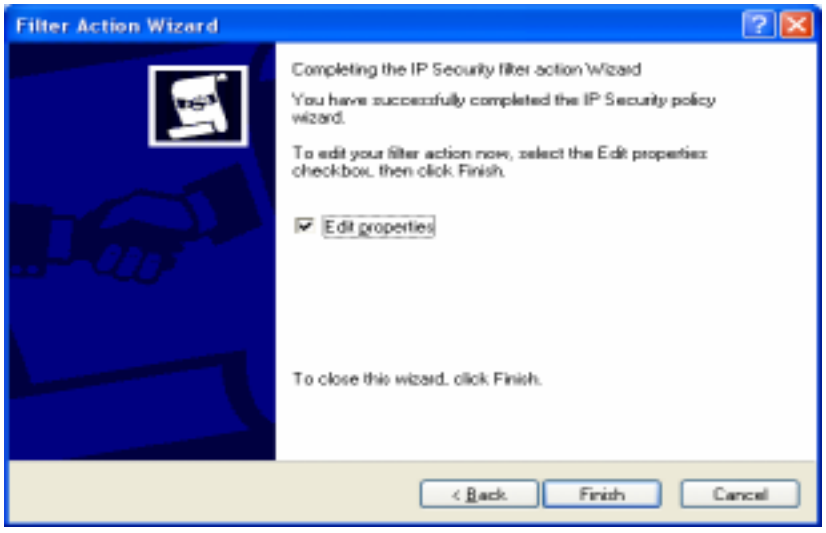
5. Accept the default value, and then click Next. The IP Traffic Security screen appears.



6. Select Custom, and then click Settings. The Custom Security Method Settings screen appears.

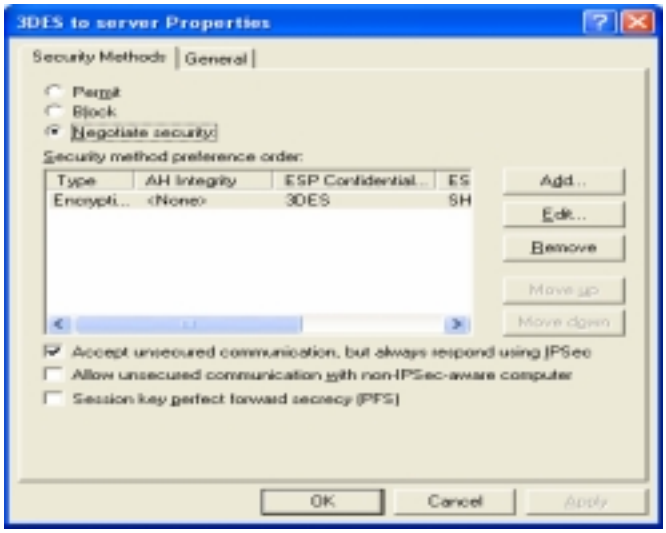
7. Enable the Data integrity and encryption (ESP): check box, and then make the appropriate selections in the Integrity and algorithms list boxes.

8. Click OK, Next, and then Finish.

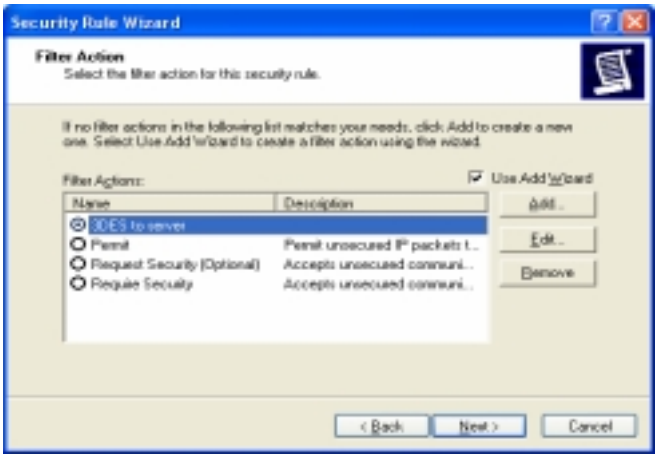


F. Binding the Filter Action

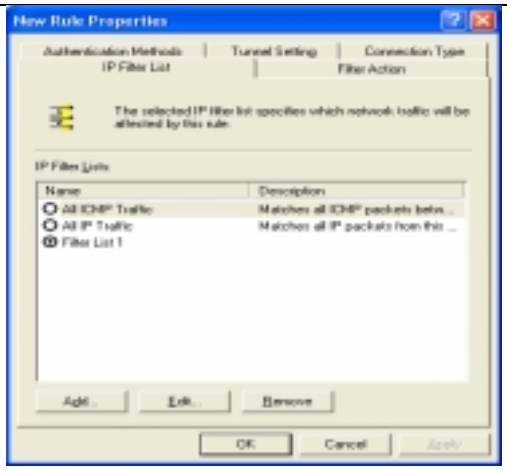
This sequence attaches the new filter action to the filter and policy. The Filter Action screen appears.



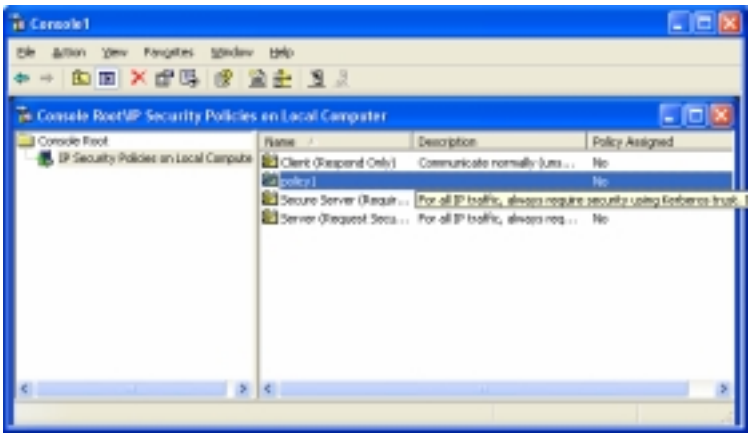
I. Enable the filter action option and make sure that the filter name is selected. (In this example, we used the filter name: 3DES to the Server.)



II. Click Next, Finish, and then Close.



III. The newly created policy appears in the right pane of the Console Root\IP Security Policies on Local Machine screen.



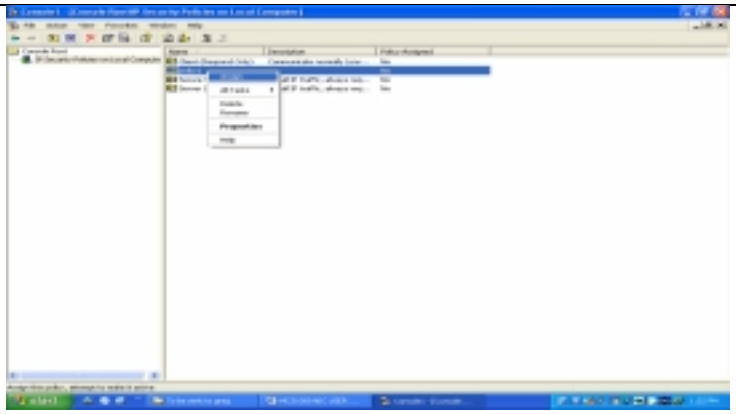
IV. Exit this screen and, when prompted, save the new policy information. Use a meaningful name for future reference. You can modify this security policy by double clicking the icon that is created when you save the policy in the previous step.

G.Enabling Encryption

An encryption policy must exist in the Console Root\IP Security Policies on the Local Machine screen before you can enable encryption on the MCS1000 Secure NIC.

To enable encryption:

Right-click the desired policy icon in the right pane of the screen.



2 Select Assign.

3 A green plus (+) symbol appears on the policy icon to indicate that encryption is toggled on.

H. Disabling Encryption

An encryption policy must exist in the Console Root\IP Security Policies on the Local Machine screen, and be enabled, before you can disable encryption on the MCS1000 Secure NIC. To disable encryption:

1 Right-click the desired policy icon in the right pane of the screen.

2 Select Un-assign. The absence of a green plus (+) symbol on the policy icon indicates that encryption is toggled off.

General Information

If you have any questions regarding the MCS1000 or Moschip Semiconductor, please contact the Moschip Support Group at e-mail mcs1000spt@moschip.com.

Appendix A. Full Schematic.

The Full schematic can be requested from mcs1000spt@moschip.com.

Appendix B. PCB Fabrication Drawing.

The PCB Fabrication Drawing and Gerber can be requested from mcs1000spt@moschip.com

Appendix C. Bill of Materials.

The complete BOM can be requested from mcs1000spt@moschip.com