# DI-804V With Windows XP IPSec VPN Configuration Procedures

## I. Configuring D-Link DI-804V VPN Router

First of all you should login into your D-Link VPN Router. Please connect your PC to any of the Ethernet ports of the VPN Router.

By default the IP address of DI-804V is 192.168.0.1 255.255.255.0, thus you should configure your PC, so it would be in the same subnet as VPN router. For example, you can configure it for the IP address of 192.168.0.2 255.255.255.0 and default gateway of 192.168.0.1. The default gateway should always point to VPN Router. You can also use the dynamic IP settings on your PC, so VPN Router will give you the address automatically.

Try to ping the VPN Router to check if your PC can communicate with VPN Router. If ping is unsuccessful, that probably means that your VPN Router is configured with some other IP address. In order to get the Router back to default settings press Factory Reset button on the back of unit. After resetting, the IP address of the unit will be 192.168.0.1 255.255.255.0.

Now you should open your Internet Explorer and type http://192.168.0.1 in the Address bar. The login prompt will appear. You should use the login name "admin" and leave the password blank. You can set up the password later on. If you cannot log into the Router with blank password, that means that the password was changed. You should Factory Reset the unit in order to login into it. After you have logged in, you will see the following screen:



| Now, let's go to the Device | Information. | You will see | the following | screen there: |
|-----------------------------|--------------|--------------|---------------|---------------|
|-----------------------------|--------------|--------------|---------------|---------------|

| - C) - 🖹 🖹   | Address a) http://192.168.0.1/d info.htm              | • 🗗 |
|--------------|---|-----|
| Link         | VPN Router DI-804V                                    |     |
| tain menu    | DI-004V VPN Router                                    |     |
|              | Device Name: DF804V                                   |     |
|              | IP Address: 192.168.0.1                               |     |
|              | Private LAN Mac Address: 00:05:50:F0:31:88            |     |
|              | Public WAN (Cable/DSL) Mac Address: 00.05.5D:F0:31:BC |     |
|              | Firmware Version: C4.73 (2002/09/20)                  |     |
|              |   |     |
|              |   |     |
|              |   |     |
| right © 2000 |   |     |
|              |   |     |
|              |   |     |
|              |   |     |
|              |   |     |
|              |   |     |
|              |   |     |
|              |   |     |
|              |   |     |

You will see the device name, IP address of the unit, Private and Public MAC addresses as well as firmware version. It is always recommended that you use the latest firmware available. By the time of this writing the latest firmware version available is 4.73.

Now you should go to the Basic Setup menu and configure Cable/DSL ISP Settings. It can be a Static IP, PPPoE, PPTP or Telstra. For PPPoE, PPTP and Telstra you must specify the user name and the password. Let's configure a static IP for our example. We will use the IP address of 202.129.97.105 255.255.255.254 for our WAN interface and the default gateway of 202.129.97.1 255.255.255.254. For DNS server we use 202.129.97.124. Your Internet service provider must give your IP address, default gateway address and DNS server address. When you are done with Static IP configuration, you will see the following screen:

| Basic Setup - Microsoft Internet Ex | plorer  | <br>     |
|-------------------------------------|---|----------|
| C - C - R 2 Address 1005            | p://192.168.0.1/wiz_basic.htm                           |          |
| D-Link                              | VPN Router DI-804V<br>DEVICE BASIC ADVANCED SYSTEM HELP |          |
| Main menu Basic Se                  | etup - Cable/DSL ISP Settings                           |          |
| TIME SETTINGS<br>Computer           | Name DI-804V  |          |
| DEVICE IP<br>SETTINGS Domain Na     | ume   |          |
| ISP SETTINGS ISP Settin             | ngs etings  |          |
| ISP ADDITIONAL<br>SETTINGS IP subm  | ned by your ISP 202                                     |          |
| SETTINGS ISP Gate                   | eway Address 202 . 129 . 97 . 1                         |          |
|                                     | c DNS @ Static DNS                                      |          |
| DNS1<br>DNS2                        | 202 129 97 124  |          |
|                                     | GANGEL BAVEGREETART                                     |          |
| Copyright © 2000                    |   |          |
|                                     |   |          |
|                                     |   |          |
|                                     |   |          |
|                                     |   |          |
|                                     |   |          |
| Done                                |   | internet |

Click Save & Restart, so the unit will save the new ISP settings. After the unit is restarted, go to the Basic Setup again. Choose ISP Settings, you will see the following screen:

| Setup Wizard - ISP SETTINGS-Static IP Settings - Microsoft Internet Explorer |           |
|--|-----------|
| le Edit Yew Fgvorites Iools Help   |           |
| C - X 2 Address Dhttp://192.168.0.1/wiz_ispsettings.htm                      | 💌 🔁 Go    |
| VPN Router DI-804V   |           |
| D-Link project project and any any system                                    |           |
| INFORMATION STATUS SETUP SETTINGS TOOLS HELP                                 |           |
| Main menu<br>ISP SETTINGS - Static IP Settings                               |           |
| ME SETTINGS  |           |
| 1. Select the ISP Settings List below  |           |
| DEVICE IP<br>SETTINGS Static IP Settings V                                   |           |
|  |           |
| SP SETTINGS IP assigned by your ISP: 202 . 129 . 97 . 105                    |           |
| P ADDITIONAL IB Subpat Mark: 255 255 255 224                                 |           |
|  |           |
| SETTINGS ISP Gateway Address: 202 . 129 . 97 . 1                             |           |
| VPN  |           |
| 2. Click Next to send your request to the Cable/xDSL Broadband Router        |           |
| VE & RESTART   |           |
|  |           |
| yright © 2000  |           |
|  |           |
|  |           |
|  |           |
|  |           |
|  |           |
|  |           |
|  |           |
|  |           |
|  |           |
|  | Dinternet |

Click Next, so your VPN Router will to access Cable/xDSL Broadband Router. The connection is established now and we can go to the next step. If you have problems with the connection, check the IP (PPPoE, PPTP, Telstra) settings with your Internet service provider.

Let's go to VPN settings menu now:

| Setup Wizard - Time Settings - Microsoft Internet Explorer          | _ <i>8</i> × |
|---|--------------|
| le Edit View Figwarites Iools Help                                  | 27           |
| ) = 🕘 - 🖹 👔 Address 🕘 http://192.168.0.1/wiz_VPN.htm                | 💌 🔁 Go       |
| VPM Router DI-8044  | ×            |
| Main menu VPN SETTINGS  |              |
| Sevice IP   |              |
| ISP SETTINGS Enable Williams Local IPSEC ID Remote IPSEC ID Command |              |
| NODEM<br>BETTINGS<br>VPN<br>SETTINGS                                |              |
| AVE & RESTART   |              |
|   |              |
|   |              |
|   |              |
|   |              |

Type the name of your new VPN connection and click Add. We will use VPN\_Client for our example. In the next menu, you will be asked for Remote IP settings. Put the IP address of Remote IP Network, i.e. the network from which the clients will be connecting. If you want many clients from the same network to connect to your VPN Router, then put all zeros in Remote Gateway field. Otherwise, you must specify the static IP address of your client. If your client gets the IP dynamically, than you should also use 0.0.0.0 address. If you want to allow any client to connect, then put 0.0.0.0 for Remote IP Network, Remote IP Network, Remote IP Netwark, and Remote Gateway.

#### Let's look at what we have got:

| Setup Wizard - VPN         | Settings - Microsoft Internet Exp                 | lorer                                 | X        |
|----------------------------|---|---------------------------------------|----------|
| G - C - N 2                | Address and http://192.168.0.1/wiz                | WN_ke.htm                             |          |
| D-Link                     | DEVICE DEVICE                                     | VPN Router DI-804V                    | *        |
| Main menu                  | VPN SETTINGS                                      |                                       |          |
| TIME SETTINGS              | Connection Name                                   | XP                                    |          |
| DEVICE IP<br>SETTINGS      | Local IPSEC Identifier<br>Remote IPSEC Identifier |                                       |          |
| ISP SETTINGS               | Remote IP Network                                 | 202 129 97 .101                       |          |
| ISP ADDITIONAL<br>SETTINGS | Remote Gateway IP                                 | 202                                   |          |
| SETTINGS                   | Network Interface                                 | WANETHERNET ▼                         |          |
| SETTINGS                   | Perfect Forward Secure<br>Encryption Protocol     | Enabled C Disabled                    |          |
| SAVE & RESTART             | PreShared Key                                     | 1234567                               |          |
|                            | IKE Life Time                                     | 28800 Seconds Bave                    |          |
|                            | Enable Connection L                               | ocal IPSEC ID Ramota IPSEC ID Command |          |
|                            |   | C Bank Bany >                         |          |
| Copyright © 2000           |   |                                       | <u>v</u> |
| Done                       |   |                                       | Internet |

You should type in the PreShared Key, which is going to be used by remote Client as well. So, don't forget the key, you will use it later, while configuring the remote Client. Be sure to remember the Key Life and IKE Life Time settings as well, they must be the same on your VPN Router and VPN Client. You may change them to whatever amount is suitable for you, but be sure to use equal settings for your client.

You can use Main, Aggressive and Manual modes for Secure Association, but be sure to use the same mode on the VPN Client. The default mode is a Main mode for VPN Router as well as for VPN Client. You have two choices for the Encryption Protocol: 3DES or DES in Main mode, you can choose Key Group in Aggressive mode and Authentication protocol in Manual mode, as well as Encryption and Authentication Keys. Once again, make sure to use equal settings for you VPN Client and VPN Router.

| Now, when we are done with VPN settings | , you may safely click on Save. |
|---|---------------------------------|
|---|---------------------------------|

| 🗿 Setup Wizard - Time Settlings - Microsoft Internet Explorer                                     | _ @ ×    |
|---|----------|
| Ele Lidt Yew Favorites Iools Help   |          |
| 3 - 3 - 8 a Address B Phtp://192.168.0.1/wkz_MPN.htm  | 💌 🄁 Go   |
| D-Link VPN Router BI-804V   | *        |
| Main menu<br>VPN SETTINGS   |          |
| Connection Name   |          |
| INP ADDITIONAL DEVELOPMENT CACALIFIEC ID Remote IPECC ID Command<br>DP ADDITIONAL DE XDP Edit Del |          |
| SETTINGS  |          |
| STTINGS   |          |
| SAVE & ROSYART  |          |
|   |          |
|   |          |
|   |          |
|   | ×        |
| http://192.160.0.1/wiz_save-restart.htm   | Internet |

You will see the Connection we have just created. You can add more connections if you would like a client with another IP address or from the other remote network to access your internal network. The maximum amount of clients, which are supported by D-Link DI-804V VPN Router is 8.

Now you can either click on Save & Restart in the left bottom corner of the screen, or you can click Next and the system will offer you to Save & Restart the router itself. Your VPN Router is ready to get the VPN Client request.

# **II. Configuring Windows XP IPSec Client**

<u>Technical Requirement:</u> Customer is required to understand their network and the Windows XP well for this configuration. Please consult Microsoft certified professional if unsure. The information provided here is for your reference only. D-Link will not be held responsible for any consequences arise from it.

1.Click "Start", then "Run" and type "mmc". Click "OK"

| Run   | <u>?×</u>  |
|-------|--|
|       | Type the name of a program, folder, document, or<br>Internet resource, and Windows will open it for you. |
| Open: | mmc  |
|       |  |
|       | OK Cancel <u>B</u> rowse   |

#### 2.Select "Add/Remove Snap-in"

| Console Window Help New Crit+N Open Save As Add/Remove Snapin Crit+M Oploins 1 D:/WINVT/System32(Inetsrvilis 2 D:/WINVT/System32(Idewingint Exit  | Console1 - [Console Root]                            |                  |      |  |       | _ 8 |
|---|--|------------------|------|--|-------|-----|
| New     Ctrl-N       Save     Ctrl-S       Save As     Ctrl-M       Adjferenove Snap-in     Ctrl-M       Options     Ctrl-M       1 D:\UMINNT/System32\Unetsrviis       2 D:\UMINNT/System32\devmgmt       Exit | Console <u>W</u> indow <u>H</u> elp                  |                  |      |  | 🗋 🚅 🖬 |     |
| Open     CtH-0       Save     CtH-5       Add/fremove Snap-in     CtH-M       Options     CtH-M       I     D:\WINNTSystem32\lanksrv\is       2     D:\WINNTsystem32\lanksrv\is       Exit     Exit             | A New  | Ctrl+N           | l 19 |  |       |     |
| Save S Add/Remove Snap-In Ctrl+M Options 1 D:\/WINNTSystem32\Inetsrv\iis 2 D:\/WINNTSystem32\Idevrogmt Ext  | Open   | Ctrl+O           |      |  |       |     |
| Add/femoreSnap-in Ctrl+M<br>Options<br>1 D:\WINNTSystem32\Linetsrv\is<br>2 D:\WINNTsystem32\Linetsrv\is<br>Exit   | Save As  | Ctri+5           |      |  |       |     |
| Addytemove Shapin<br>Options<br>1 D:\VIINT\System32\Inetsrvlis<br>2 D:\VIINT\System32\Idevmgmt<br>Exit  |  | at h t           |      |  |       |     |
| 1 D:\WINNT\System32\Intersrviiis       2 D:\WINNT\System32\devmgmt       Exit   | Add/Remove Snap-In<br>Onlinns                        | Ctri#M           |      |  |       |     |
| 2 D1/WINVTSystem32(dewngmt Exit   |  |                  |      |  |       |     |
|   | 1 D:\WINNT(System32)Inet<br>2 D:\WINNT(system32)devr | .srv\iis<br>mamt |      |  |       |     |
|   |  |                  |      |  |       |     |
|   | Exit   |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |
|   |  |                  |      |  |       |     |

#### 3.Click "Add"

| 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 <u>R</u> emove <u>About</u>                                       |       |
| ОК Са   | ancel |

## 4.Select and Add "IP Security Policy Management"

| Snap-in  | Vendor                                     |
|--|--|
| FrontPage Server Extensions  |  |
| 🕵 Group Policy   | Microsoft Corporation                      |
| Service Service  | Microsoft Corporation, I                   |
| Internet Authentication Service (IAS)  | Microsoft Corporation                      |
| Internet Information Services  | Microsoft Corporation                      |
| 🛃 IP Security Policy Management  |  |
| Link to Web Address  |  |
| 🚾 Local Users and Groups   | Microsoft Corporation                      |
| 🕎 Performance Logs and Alerts  | Microsoft Corporation                      |
| 💐 QoS Admission Control  | Microsoft Corporation                      |
| Description  |  |
| Description  |  |
| Internet Protocol Security (IPSec) Admin<br>policies for secure communication with o | istration. Manage IPSec<br>ther computers. |
|  |  |
|  |  |

# 5.Select "Local computer", then click "Finish"

| ect Computer  |  | <u>?</u> |
|---|--|----------|
| Select which computer this Snap-in v<br>When this console is saved the location | <b>will manage</b><br>n will also be saved |          |
| Local computer     The computer this console is running on                      |  |          |
| Manage domain policy for this computer  | s domain                                   |          |
| C Manage domain policy for another doma   | in:  |          |
|   |  |          |
| C Another computer:   |  |          |
|   | Browse                                     |          |
|   |  |          |
|   |  |          |
|   |  |          |
|   |  |          |
|   |  |          |
|   |  |          |
|   | < Back Finish                              | Cancel   |
|   |  |          |

# 6.Click "**OK**"

| Add/Remove Snap-in   | ? ×  |
|--|------|
| Standalone Extensions  |      |
| Use this page to add or remove a standalone Snap-in from the console.  |      |
| Snap-ins added to:   |      |
| IP Security Policies on Local Machine  |      |
|  |      |
|  |      |
|  |      |
|  |      |
|  |      |
| Description  |      |
| Internet Protocol Security (IPSec) Administration. Manage IPSec polici<br>for secure communication with other computers. | ies  |
| Add <u>R</u> emove <u>Ab</u> out   |      |
| OK Ca  | ncel |



#### 8.Click "Next"



#### 9.Enter the details below and click "Next"

| IP Security Policy Wizard   | <u>?</u> × |
|---|------------|
| IP Security Policy Name<br>Name this IP Security policy and provide a brief description | Ē          |
| Name:<br>D1804V with XP<br>Description:<br>D1804V communicates with XP                  | ×          |
| < <u>B</u> ack <u>N</u> ext>  | Cancel     |

#### 10.Uncheck "Activate the default response rule" and click "Next"

| ecurity Policy Wizard  |   | ?                            |
|--|---|------------------------------|
| Requests for Secure Communication<br>Specify how this policy responds to requ                                | lests for secure communication.   | Ē                            |
| The default response rule responds to re<br>other rule applies. To communicate secu<br>secure communication. | mote computers that request securi<br>arely, the computer must respond to | ity, when no<br>requests for |
| Activate the default response rule.  |   |                              |
|  |   |                              |
|  |   |                              |
|  |   |                              |
|  |   |                              |
|  | < <u>B</u> ack <u>N</u> ext >   | Cancel                       |

#### 11.Check below and click "Finish"



### 12.Select "Add"



#### 13.Click "Next"

| Security Rule Wizard | <u>?×</u>   |
|----------------------|---|
|                      | Welcome to the Create IP Security Rule Wizard.  |
|                      | A security rule governs how and when security is invoked<br>based upon criteria, such as the source, destination, and type<br>of IP traffic, in the security rule's IP filter list. |
| 10=                  | A security rule contains a collection of security actions that<br>are activated when a communication matches the criteria in<br>the IP filter list.                                 |
|                      | Security actions:   |
|                      | IP tunneling attributes     Authentication methods  |
|                      | - Filter actions  |
|                      |   |
|                      | To continue, click Next.  |
|                      |   |
|                      |   |
|                      |   |
|                      | < <u>B</u> ack <u>Next</u> Cancel   |

# 14. Input the IP Address into "**The tunnel endpoint specified by this IP address:**" (Eg. DI-804V WAN IP Address), "**Next**"

| Security Rule Wizard   | ? ×  |
|--|------|
| Tunnel Endpoint<br>The tunnel endpoint is the tunneling computer closest to the IP traffic destination,<br>as specified by the security rule's IP filter list. | Ē    |
| An IPSec tunnel allows packets to traverse a public or private internetwork with the<br>security level of a direct, private connection between two computers.  |      |
| Specify the tunnel endpoint for the IP Security rule:  |      |
| ○ <u>I</u> his rule does not specify a tunnel  |      |
| The tunnel endpoint is specified by this <u>IP</u> address:  |      |
| 202 . 129 . 97 . 105   |      |
| <u> &lt; B</u> ack <u>N</u> ext > Car  | ncel |

#### 15.Select "All network connections", then click "Next"

| Security Rule Wizard  |                |                | ? ×    |
|---|----------------|----------------|--------|
| Network Type<br>The security rule must be applied to a network  | type.          |                | 圓      |
| Select the network type:<br>C All network <u>connections</u><br>C Local area network (LAN)<br>C <u>R</u> emote access |                |                |        |
|   | < <u>B</u> ack | <u>N</u> ext ≻ | Cancel |

# 16.Select "Use this string to protect the key exchange (preshared key)" (Eg. DI-804V preshared key) then click "Next"

| ecurity Rule Wizard                                     |  |                          |                     | ?        |
|---|--|--------------------------|---------------------|----------|
| Authentication M<br>To add multiple<br>IP Security rule | ethod<br>authentication methods<br>wizard. | , edit the security rule | after completing th | •        |
| Set the initial au                                      | thentication method for                    | this security rule:      |                     |          |
| C Active Direc  | ctory <u>d</u> efault (Kerberos V          | 5 protocol)              |                     |          |
| ⊂ Use a <u>c</u> ertifi                                 | icate from this certificatio               | on authority (CA):       |                     |          |
|   |  |                          | Blow                | se       |
| Use this stri   | ng to protect the key ex                   | change (preshared ke     | y):                 |          |
| 1234567   |  |                          |                     | <b>A</b> |
|   |  |                          |                     |          |
|   |  |                          |                     |          |
|   |  |                          |                     | <b>_</b> |
|   |  |                          |                     |          |
|   |  |                          |                     |          |
|   |  |                          |                     |          |
|   |  | ( Deals                  | Maula               | Connel   |

#### 17.Select "Add"



18.Enter a filter name (XP to DI-804V) then click "Add"

| IP Filter         | r List  |  |  | ? ×                    |
|-------------------|---|--|--|------------------------|
| t diet            | An IP filter list is compos<br>addresses and protocol | ed of multiple filters. In<br>s can be combined into | this way, multiple sub<br>one IP filter. | nets, IP               |
| <u>N</u> ame:     |   |  |  |                        |
| XP to DI          | 804V  |  |  |                        |
| Descriptio        | on:   |  |  | <u>A</u> dd            |
| Make a I          | filter from XP to D1804V                              |  | <u>^</u>                                 | <u>E</u> dit           |
|                   |   |  | 7  | <u>R</u> emove         |
| Filter <u>s</u> : |   |  | ν.                                       | Jse Add <u>W</u> izard |
| Mirrored          | d Description   | Protocol   | Source Port                              | Destination            |
| •                 |   |  |  | Þ                      |
|                   |   |  | ОК                                       | Cancel                 |



| IP Filter Wizard |  | <u>? ×</u> |  |  |  |  |
|------------------|--|------------|--|--|--|--|
|                  | Welcome to the IP Filter Wizard.   |            |  |  |  |  |
|                  | This wizard helps you provide the source, destination, and<br>traffic-type information needed to filter IP traffic.  |            |  |  |  |  |
|                  | This wizard creates "mirrored" filters that match on both<br>incoming and outgoing IP traffic.   |            |  |  |  |  |
| N                | You can add multiple filters to build an IP Filter List that<br>matches on IP packets for multiple source or destination<br>machines, or for many different traffic types. |            |  |  |  |  |
|                  | To continue, click Next.   |            |  |  |  |  |
|                  | < Back Next> Cancel  |            |  |  |  |  |

20.Select "A specific IP Address" and input the Source address, then "Next" to continue (Eg. Windows XP IP) \*\_\_\_\_\_

|     |     |       |                               |                                   | _                                 |  |  |  |
|-----|-----|-------|-------------------------------|-----------------------------------|-----------------------------------|--|--|--|
|     |     |       |                               |                                   | -                                 |  |  |  |
| 202 |     | 129   |                               | 97                                |                                   | 101  |  |  |
| 255 |     | 255   |                               | 255                               |                                   | 255  |  |  |
|     |     |       |                               |                                   |                                   |  |  |  |
|     |     |       |                               |                                   |                                   |  |  |  |
|     |     |       |                               |                                   |                                   |  |  |  |
|     |     |       |                               |                                   |                                   |  |  |  |
|     |     |       |                               |                                   |                                   |  |  |  |
|     | 202 | 202 . | <b>202 . 129</b><br>255 . 255 | <b>202 . 129 .</b><br>255 . 255 . | 202 . 129 . 97<br>255 . 255 . 255 | ▼<br>202 . 129 . 97 .<br>255 . 255 . 255 . | 202     . 129     . 97     . 101       255     . 255     . 255     . 255 | 202     .     129     .     97     .     101       255     .     255     .     255     .     255 |

\* If your client gets IP address dynamically choose "My IP address".

21. Select "**A specific IP Subnet**" and input the Destination subnet address, then "**Next**" to continue (Eg. DI-804V Private network)

| Filter Wizard   |             |           |     |                |   |              |   | ? ×    |
|---|-------------|-----------|-----|----------------|---|--------------|---|--------|
| IP Traffic Destination<br>Specify the destination add | lress of th | e IP traf | ïc. |                |   |              |   | Ē      |
| Destination address:                                  |             |           |     |                |   |              |   |        |
| A specific IP Subnet                                  |             |           | _   |                | • |              |   |        |
| IP add <u>r</u> ess:                                  | 192         | . 16      | в.  | 0              | • | 0            |   |        |
| Subnet mas <u>k</u> :                                 | 255         | . 25      | 5.  | 255            |   | 0            |   |        |
|   |             |           |     |                |   |              |   |        |
|   |             |           |     |                |   |              |   |        |
|   |             |           |     |                |   |              |   |        |
|   |             |           |     |                |   |              |   |        |
|   |             |           |     |                |   |              |   |        |
|   |             |           | <   | : <u>B</u> ack |   | <u>N</u> ext | > | Cancel |

#### 22.Select the following and click "Next"





#### 24.Click "Ok"

| IP Filter List       |                                     |  |  | ? ×                    |
|----------------------|-------------------------------------|--|--|------------------------|
| An IP filter         | r list is compos<br>s and protocols | ed of multiple filters. In<br>can be combined into | this way, multiple s<br>o one IP filter. | ubnets, IP             |
| <u>N</u> ame:        |                                     |  |  |                        |
| XP to DI804V         |                                     |  |  |                        |
| Description:         |                                     |  |  | <u>A</u> dd            |
| Make a filter from X | P to DI804V                         |  | <b>A</b>                                 | <u>E</u> dit           |
|                      |                                     |  | <b>v</b>                                 | <u>R</u> emove         |
| Filter <u>s</u> :    |                                     |  | <b>v</b>                                 | Use Add <u>W</u> izard |
| Mirrored Descrip     | tion                                | Protocol   | Source Port                              | Destination            |
| Yes                  |                                     | ANY  | ANY                                      | ANY                    |
| 4                    |                                     |  |  | Þ                      |
|                      |                                     |  | OK                                       | Cancel                 |

#### 25.Now, select "XP to DI-804V" then click "Next"

| Security Rule Wizard                                    |   | <u>?</u> ×     |
|---|---|----------------|
| IP Filter List<br>Select the IP filter list for the typ | pe of IP traffic to which this security rule                    | applies.       |
| If no IP filter in the following list                   | matches your needs, click Add to creat                          | e a new one.   |
|   |   |                |
| IP filter lists:  |   |                |
| Name  | Description   | <u>A</u> dd    |
|   | Matches all ICMP packets bet                                    | Edit           |
| O AILIP Traffic   | Matches all IP packets from t<br>Makes a filter from XP to D180 |                |
|   | Makes a file from Air to Pros                                   | <u>R</u> emove |
|   |   |                |
|   |   |                |
|   |   |                |
|   |   |                |
|   | < <u>B</u> ack <u>N</u> ext                                     | > Cancel       |

#### 26.Click "Add"

| Securi | ity Rule Wizard   |   | ? ×                    |
|--------|---|---|------------------------|
| Fil    | ter Action<br>Select the filter action for this secu                          | urity rule.   | Ĩ                      |
|        | If no filter actions in the following li<br>one. Select Use Add Wizard to cre | st matches your needs, click Add to<br>eate a filter action.                            | i create a new         |
|        | Filter Actions:   | V   | Use Add <u>W</u> izard |
|        | Name  | Description   | <u>A</u> dd            |
|        | Permit     Request Security (Optional)     Require Security                   | Permit unsecured IP packets t<br>Accepts unsecured communi<br>Accepts unsecured communi | Edit                   |
|        |   | < <u>B</u> ack <u>N</u> ext   | Cancel                 |

### 27.Click "Next"

| Filter Action Wizard | ?  X  |
|----------------------|---|
|                      | Welcome to the IP Security Filter Action Wizard   |
| 161                  | Use this wizard to specify properties for a new filter action.  |
|                      | A filter action sets the security requirements for a data<br>transfer. These requirements are specified in a list of security<br>methods contained in the filter action.                      |
|                      | Data transfer is only possible when the computers involved<br>use the same security methods. Multiple security methods<br>increase the chance that two computers will use the same<br>method. |
|                      | To continue, click Next.  |
|                      | < <u>B</u> ack <u>Next</u> Cancel   |

#### 28. Enter a filter action name then click "Next"

| Filter Action Wizard  | <u>?</u> × |
|---|------------|
| Filter Action Name<br>Name this filter action and optionally give a brief description | 163        |
| Na <u>m</u> e:<br> 3DES_MD5<br>Description:   |            |
| SDES_MDS  | ×          |
| < <u>B</u> ack <u>N</u> ext>  | Cancel     |

29.Select "Negotiate security" then click "Next'

| ilter Action General Options<br>Set the filter action behavior. |  |
|---|--|
| O Permit  |  |
| C Block   |  |
| Negotiate security  |  |
|   |  |
|   |  |
|   |  |
|   |  |
|   |  |
|   |  |
|   |  |
|   |  |
|   |  |

30.Select "Do not communicate with computer that do not support IPSec" then click "Next"



#### 31. Select "Custom" then click on "Settings"

| Security Method Wizard   | <u>? ×</u> |  |  |
|--|------------|--|--|
| IP Traffic Security<br>Specify a security method for IP traffic. To add multiple security methods edit the<br>filter action after completing the wizard. | 1997       |  |  |
| This filter action requires at least one security method for IP traffic.   |            |  |  |
| <u>High</u> (Encapsulated Secure Payload)     Data will be encrypted, authenticated, and unmodified.     Medium (Authenticated Header)                   |            |  |  |
| Data will be authentic and unmodified, but will not be encrypted.  |            |  |  |
| © <u>Custom</u><br>Settings  |            |  |  |
|  |            |  |  |
| < <u>B</u> ack <u>N</u> ext >  | Cancel     |  |  |

# 32.Check "Data integrity and encryption (ESP)", select the "Integrity algorithm (MD5)" and "Encryption algorithm (3DES)" then click "OK"

| Custom Security Method Settings  | ? ×       |
|--|-----------|
| Specify the settings for this custom security method.                        |           |
| Data and address integrity without encryption (AH) :<br>Integrity algorithm: |           |
| MD5  |           |
| Data integrity and encryption (ESP): Integrity algorithm:                    |           |
| Encryption algorithm:  |           |
| - Session Key Settings:  |           |
| 🔽 🖸 Generate a new key every: 🗖 Gene <u>r</u> ate a new                      | key every |
| 100000 <u>K</u> bytes 3600 <u>s</u> ec                                       | onds      |
|  |           |
| ОК   | Cancel    |

#### 33.Click "Next"

| Security Method W   | izard   |  |                      | ? ×    |
|---|---|--|----------------------|--------|
| IP Traffic Secu<br>Specify a sec<br>filter action af                | <b>rrity</b><br>:urity method for IP traffic. To<br>ter completing the wizard.                                    | add multiple secu                      | rity methods edit th |        |
| This filter action  | on requires at least one secu   | rity method for IP t                   | raffic.              |        |
| C High (Enc<br>Data will t<br>C Medium (<br>Data will t<br>C Lustom | apsulated Secure Payload)<br>e encrypted, authenticated,<br>Authenticated Header)<br>ae authentic and unmodified, | and unmodified.<br>but will not be end | sypted.              |        |
|   |   | < <u>B</u> ack                         | <u>N</u> ext >       | Cancel |

#### 34.Click "Finish"

| Filter Action Wizard | <u>? ×</u>   |
|----------------------|--|
|                      | Completing the IP Security filter action Wizard<br>You have successfully completed the IP Security Policy<br>wizard.<br>To edit your filter action now, select the Edit properties<br>checkbox, then click Finish. |
|                      | To close this wizard, click Finish.  |
|                      | < <u>B</u> ack Finish Cancel   |

### 35.Select "3DES\_MD5" then click "Edit"

| Security Rule Wizard   |  | <u>? ×</u>             |
|--|--|------------------------|
| Filter Action<br>Select the filter action for this secu                        | rity rule.   | Ē                      |
| If no filter actions in the following lis<br>one. Select Use Add Wizard to cre | t matches your needs, click Add to<br>ate a filter action. | create a new           |
| Filter Actions:  | $\checkmark$   | Use Add <u>W</u> izard |
| Name   | Description  | Add                    |
| O 3DES_MD5   | 3DES_MD5   |                        |
| O Permit   | Permit unsecured IP packets t                              | <u> </u>               |
| O Request Security (Optional)<br>O Require Security                            | Accepts unsecured communi<br>Accepts unsecured communi     | <u>R</u> emove         |
|  |  |                        |
|  |  |                        |
|  | < <u>B</u> ack <u>N</u> ext                                | :> Cancel              |

36.Select the following and check "Session key Perfect Forward Secrecy" then click "OK"

| 3DES_MD5 Properties  |                            |                  | <u> </u>           |
|--|----------------------------|------------------|--------------------|
| Security Methods General   |                            |                  |                    |
| <ul> <li>Permit</li> <li>Block</li> <li>Negotiate security:</li> <li>Security Method preference</li> </ul> | e order:                   |                  |                    |
| Type AH Integrity  | ESP Confider               | ntial ES         | Add                |
| Custom <none></none>   | 3DES                       | МЕ               |                    |
|  |                            | _                | <u>E</u> dit       |
|  |                            |                  | <u>R</u> emove     |
|  |                            |                  | Move <u>up</u>     |
| •  |                            |                  | Move d <u>o</u> wn |
| Accept unsecured com   | munication, but al         | ways respond us  | sing <u>I</u> PSec |
| Allow unsecured comm   | unication <u>w</u> ith nor | n IPSec-aware co | omputer            |
| 🔽 Session key <u>P</u> erfect Fo   | rward Secrecy              |                  |                    |
|  |                            |                  |                    |
|  |                            |                  |                    |
|  |                            |                  |                    |
|  | OK                         | Cancel           | Apply              |
|  |                            |                  |                    |

#### 37.Click "Next"



#### 38.Click "Finish'



#### 39.Click "Add"





41. Enter the IP Address detail into "**The tunnel endpoint specified by this IP address:**" (Eg. Windows XP IP Address)\*

| Security Rule Wizard   | <u>?</u> × |
|--|------------|
| Tunnel Endpoint<br>The tunnel endpoint is the tunneling computer closest to the IP traffic destination,<br>as specified by the security rule's IP filter list. | Ī          |
| An IPSec tunnel allows packets to traverse a public or private internetwork with the<br>security level of a direct, private connection between two computers.  |            |
| Specify the tunnel endpoint for the IP Security rule:  |            |
| C Ihis rule does not specify a tunnel  |            |
| The tunnel endpoint is specified by this <u>IP</u> address:  |            |
| 202 . 129 . 97 . 101   |            |
| <u>≺B</u> ack <u>N</u> ext > Ca  | ancel      |

\* If your client gets IP address dynamically, put the dynamic IP address here! You will have to change this setting every time you connect to the Internet. Unfortunately, this is the limitation of XP/2000 IPSec client. If your XP/2000 IPSec client is connected to the Internet through the router, use the private IP of your computer, NOT the public IP address of the router!

42. Select "All network connections" then click "Next"

| Network Type<br>The security rule must be applied to a | a network type. |               |        |
|--|-----------------|---------------|--------|
| Select the network type:                               |                 |               |        |
| All network connections                                |                 |               |        |
| C Local area network (LAN)                             |                 |               |        |
| C <u>R</u> emote access                                |                 |               |        |
|  |                 |               |        |
|  |                 |               |        |
|  |                 |               |        |
|  |                 |               |        |
|  |                 |               |        |
|  |                 |               |        |
|  |                 |               |        |
|  |                 |               |        |
|  | < <u>B</u> ack  | <u>N</u> ext> | Cancel |

# 43. Select "**Use this string to protect the key exchange (preshared key)**" (Eg. DI-804V preshared key) then click "**Next**"

| .y. | DI-004 V preshared key) then click <b>Next</b>   |
|-----|--|
|     | Security Rule Wizard   |
|     | Authentication Method<br>To add multiple authentication methods, edit the security rule after completing the<br>IP Security rule wizard. |
|     | Set the initial authentication method for this security rule:  |
|     | C Active Directory default (Kerberos V5 protocol)  |
|     | O Use a certificate from this certification authority (CA):  |
|     | Browse   |
|     | <ul> <li>Use this string to protect the key exchange (preshared key):</li> </ul>   |
|     | 1234567  |
|     |  |
|     | < <u>B</u> ack <u>N</u> ext> Cancel  |

#### 44. Click "Add"



45. Enter a filter name (DI-804V to XP) then click on "Add"

|                   | An IP filter list is compos<br>addresses and protocol: | ed of multiple filters. In<br>s can be combined into | this way, multiple subn<br>one IP filter. | ets, IP              |
|-------------------|--|--|---|----------------------|
| <u>N</u> ame:     |  |  |   |                      |
| DI804V to         | ×P   |  |   | Add 1                |
| Description       | 1:   |  |   |                      |
| Make a fil        | ter from DI804V to XP                                  |  | <u> </u>                                  | <u>E</u> dit         |
|                   |  |  | <b>_</b>                                  | <u>R</u> emove       |
| Filter <u>s</u> : |  |  | 🔽 Us                                      | e Add <u>W</u> izard |
| Mirrored          | Description  | Protocol   | Source Port                               | Destination          |
| •                 |  |  |   |                      |
|                   |  |  | ОК  | Cancel               |



| IP Filter Wizard | <u>? ×</u>   |  |  |  |  |  |
|------------------|--|--|--|--|--|--|
| I                | Welcome to the IP Filter Wizard.<br>This wizard helps you provide the source, destination, and<br>traffic-type information needed to filter IP traffic.                    |  |  |  |  |  |
|                  | This wizard creates "mirrored" filters that match on both<br>incoming and outgoing IP traffic.   |  |  |  |  |  |
|                  | You can add multiple filters to build an IP Filter List that<br>matches on IP packets for multiple source or destination<br>machines, or for many different traffic types. |  |  |  |  |  |
|                  | To continue, click Next.   |  |  |  |  |  |
|                  | < Back Cancel  |  |  |  |  |  |

47. Select "**A specific IP Subnet**" and input the Source subnet address then click "**Next**" (Eg. DI-804V Private network)

| to nothony                                      |           |       |       |               |   |     |       |        |
|---|-----------|-------|-------|---------------|---|-----|-------|--------|
| ilter Wizard                                    |           |       |       |               |   |     |       | ?      |
| IP Traffic Source<br>Specify the source address | of the IF | , tra | ffic. |               |   |     |       | E      |
| Source address:                                 |           |       |       |               |   |     |       |        |
| A specific IP Subnet                            |           |       |       |               | • |     |       |        |
| <u>I</u> P Address:                             | 192       |       | 168   | . 0           |   | . 0 |       |        |
| Subnet <u>m</u> ask:                            | 255       |       | 255   | . 25          | 5 | . 0 | _     |        |
|   |           |       |       |               |   |     |       |        |
|   |           |       |       |               |   |     |       |        |
|   |           |       |       |               |   |     |       |        |
|   |           |       |       |               |   |     |       |        |
|   |           |       |       |               |   |     |       |        |
|   |           |       |       |               |   |     |       | 1      |
|   |           |       | _     | < <u>B</u> ac | k | Ne  | ext > | Cancel |

48. Select "**A specific IP Address**" and input the Destination address then click "**Next**" (Eg. Windows XP IP address)\*

| Wizard<br>Traffic Destination |             | ID to still |        |         |         | <u>י</u><br>ה |
|-------------------------------|-------------|-------------|--------|---------|---------|---------------|
| Specify the destination add   | ress of the | IP traffic. |        |         |         | 괵             |
| Destination address:          |             |             |        |         |         |               |
| A specific IP Address         |             |             |        | -       |         |               |
| IP add <u>r</u> ess:          | 202         | . 129       | . 97   | . 101   |         |               |
| Subnet mas <u>k</u> :         | 255         | . 255       | . 255  | . 255   |         |               |
|                               |             |             |        |         |         |               |
|                               |             |             |        |         |         |               |
|                               |             |             |        |         |         |               |
|                               |             |             |        |         |         |               |
|                               |             |             |        |         |         |               |
|                               |             |             |        | <b></b> |         |               |
|                               |             |             | < Back | Next >  | > 📔 Can | cel           |

\* If your client gets IP address dynamically choose "My IP Address".



#### 50.Click "**Finish**" IP Filter Wizard



#### 51.Click on "Close"

| IP Filter I       | List   |  |   | ? >                    |
|-------------------|--|--|---|------------------------|
|                   | An IP filter list is compos<br>addresses and protocols | ed of multiple filters. In<br>s can be combined into | this way, multiple su<br>one IP filter. | ibnets, IP             |
| Name:             |  |  |   |                        |
| DI804V to         | XP   |  |   |                        |
| Description       | 1:   |  |   | <u>A</u> dd            |
| Make a fil        | ter from DI804V to XP                                  |  | <b>A</b>                                | <u>E</u> dit           |
|                   |  |  | ~                                       | <u>R</u> emove         |
| Filter <u>s</u> : |  |  | $\checkmark$                            | Use Add <u>W</u> izard |
| Mirrored          | Description  | Protocol   | Source Port                             | Destination            |
| Yes               |  | ANY  | ANY                                     | ANY                    |
| •                 |  |  |   | Þ                      |
|                   |  |  | ОК                                      | Cancel                 |

#### 52.Select "DI-804V to XP" then click "Next"

| uritu Dulo Wizard                   |  | 2             |
|-------------------------------------|--|---------------|
| IP Filter List                      |  |               |
| Select the IP filter list for the I | type of IP traffic to which this security rule | e applies.    |
| If no IP filter in the following li | st matches your needs, click Add to crea       | te a new one. |
|                                     |  |               |
| IP hilter lists:                    | Description                                    | Add           |
|                                     | Matches all ICMP packets bet                   | <u></u> dd    |
|                                     | Matches all IP packets from t                  | <u>E</u> dit  |
| O DI804V to XP                      | Make a filter from DI804V to XP                | Bomouro       |
| O XP to DI804V                      | Makes a filter from XP to D180                 |               |
|                                     |  |               |
|                                     |  |               |
|                                     |  |               |
|                                     |  |               |
|                                     |  |               |
|                                     | < <u>B</u> ack <u>N</u> ext                    | > Cancel      |
|                                     |  |               |

### 53. Select "3DES\_MD5" then click "Next"

| ecurity Rule Wizard  |   | ? >                    |
|--|---|------------------------|
| Filter Action<br>Select the filter action for this secu  | irity rule.   | <u></u>                |
| If no filter actions in the following li<br>one. Select Use Add Wizard to cre                                | st matches your needs, click Add to<br>eate a filter action.  | create a new           |
| Filter Actions:  | <b>V</b>  | Use Add <u>W</u> izard |
| Name   | Description   | Add                    |
| <ul> <li>i3DES_MD5</li> <li>Permit</li> <li>Request Security (Optional)</li> <li>Require Security</li> </ul> | 3DES_MD5<br>Permit unsecured IP packets t<br>Accepts unsecured communi<br>Accepts unsecured communi | Edit                   |
| 1  | < <u>B</u> ack <u>N</u> ext   | :> Cancel              |

#### 54.Click "Finish"

| Security Rule Wizard |   | <u>? ×</u> |
|----------------------|---|------------|
|                      | Completing the New Rule Wizard<br>You have successfully completed specifying the properties<br>for your new rule.<br>To edit your security rule now, select the Edit properties<br>check hox, and then click Finish |            |
|                      | Edit properties   |            |
|                      | To close this wizard, click Finish.   |            |
|                      | < <u>B</u> ack Finish Can   | cel        |

#### 55.Select "XP to DI-804V" then click on "Edit"

| P with DI804¥ Proper | ties                        |                | ? >       |
|----------------------|-----------------------------|----------------|-----------|
| Rules General        |                             |                |           |
| Security rule        | es for communicating with o | her computers  |           |
| IP Security rules:   |                             |                |           |
| IP Filter List       | Filter Action               | Authentication | Tu        |
| XP to DI804V         | 3DES_MD5                    | Preshared Key  | 20        |
| DI804V to XP         | 3DES_MD5                    | Preshared Key  | 20        |
| Oynamic>             | Default Response            | Kerberos       | Nc        |
| Add                  | Edit                        | Use Add Wi     | ►<br>zard |
|                      |                             | Close Ca       | ncel      |

56.Select "XP to DI-804V" then click on "Edit"

| Edit Rule Properties                                 | <u>? ×</u>                                      |  |  |
|--|---|--|--|
| Authentication Methods Tur<br>IP Filter List         | nnel Setting Connection Type  <br>Filter Action |  |  |
| The selected IP filter lis<br>affected by this rule. | t specifies which network traffic will be       |  |  |
| IP Filter <u>L</u> ists:                             |   |  |  |
| Name   | Description                                     |  |  |
|  | Matches all ICMP packets betw                   |  |  |
| O All IP Traffic                                     | Matches all IP packets from this                |  |  |
| O DI804V to XP                                       | Make a filter from DI804V to XP                 |  |  |
| O XP to DI804V                                       | Makes a filter from XP to DI804V                |  |  |
| Add., Edit., 1                                       | Remove  |  |  |
|  | Cancel Apply                                    |  |  |
|  |   |  |  |

#### 57.Click "Edit"

| 📑 IP Filte             | r List   |  |   | ? ×                    |
|------------------------|--|--|---|------------------------|
| TalleT                 | An IP filter list is compose<br>addresses and protocol | ed of multiple filters. In l<br>s can be combined into | ihis way, multiple su<br>one IP filter. | bnets, IP              |
| <u>N</u> ame:          |  |  |   |                        |
| XP to D                | 1804V  |  |   |                        |
| ,<br><u>D</u> escripti | ion:   |  |   | <u>A</u> dd            |
| Makesa                 | a filter from XP to D1804V                             |  | <u> </u>                                | <u>E</u> dit           |
|                        |  |  | 7                                       | <u>R</u> emove         |
| Filter <u>s</u> :      |  |  | $\checkmark$                            | Use Add <u>W</u> izard |
| Mirrore                | d Description  | Protocol   | Source Port                             | Destination            |
| Yes                    |  | ANY  | ANY                                     | ANY                    |
| •                      |  |  |   | Þ                      |
|                        |  |  | OK                                      | Cancel                 |

58.Uncheck "Mirrored. Also match packets with exact opposite source and destination address" then click "OK" \*

| essing   Protocol   Descri                          | ption    |     |         |    |          |      |        |
|---|----------|-----|---------|----|----------|------|--------|
| ource address:                                      |          |     |         |    |          | 7    |        |
| A specific in Address                               |          |     |         |    |          | · _  |        |
| <u>I</u> P Address:                                 | 202      | •   | 129     | •  | 97       | •    | 101    |
| Subnet <u>m</u> ask:                                | 255      | •   | 255     | •  | 255      | •    | 255    |
| estination address:                                 |          |     |         |    |          |      |        |
| A specific IP Subnet                                |          |     |         |    |          | •    |        |
| IP add <u>r</u> ess:                                | 192      | •   | 168     | •  | 0        | •    | 0      |
| Subnet mas <u>k</u> :                               | 255      | •   | 255     | ·  | 255      | •    | 0      |
| Mirrgred. Also match pack<br>destination addresses. | ets with | the | exact o | pp | osite sc | ouro | ce and |
|   |          |     |         |    |          |      |        |

\* If your client gets IP address dynamically you will see "My IP Address" in Source address field.

| 59.0 | Click " <b>Clo</b>       | se"  |  |                                    |          |                    |
|------|--------------------------|--|--|------------------------------------|----------|--------------------|
|      | 🔲 IP Filter I            | List   |  |                                    |          | ? ×                |
|      |                          | An IP filter list is compos<br>addresses and protocol: | ed of multiple filters. In 1<br>s can be combined into | his way, multipl<br>one IP filter. | le subne | ts, IP             |
|      | Name:                    |  |  |                                    |          |                    |
|      | XP to DI8                | 04V  |  |                                    |          |                    |
|      | ,<br><u>D</u> escriptior | n:   |  |                                    |          | <u>A</u> dd        |
|      | Makes a f                | ilter from XP to D1804V                                |  |                                    |          | <u>E</u> dit       |
|      |                          |  |  |                                    | -        | <u>R</u> emove     |
|      | Filter <u>s</u> :        |  |  |                                    | 🔽 Use    | Add <u>W</u> izard |
|      | Mirrored                 | Description  | Protocol   | Source Port                        |          | Destination        |
|      | No                       |  | ANY  | ANY                                |          | ANY                |
|      | I                        |  |  |                                    |          | Þ                  |
|      |                          |  |  | ОК                                 |          | Cancel             |

# 60. Select "DI-804V to XP" then click on "Edit"

| t Rule Properties                                     | ?   |
|---|---|
| Authentication Methods   Tur<br>IP Filter List        | nnel Setting Connection Type<br>Filter Action |
| The selected IP filter list<br>affected by this rule. | t specifies which network traffic will be     |
| IP Filter <u>L</u> ists:                              |   |
| Name  | Description                                   |
| O AILICMP Traffic                                     | Matches all ICMP packets betw                 |
| O All IP Traffic                                      | Matches all IP packets from this              |
| O DI804V to XP  | Make a filter from D1804V to XP               |
| C XP to DI804V  | Makes a filter from XP to DI804∨              |
| A <u>d</u> d <u>E</u> dit                             | <u>R</u> emove                                |
| Clo   | se Cancel <u>Apply</u>                        |

## 61.Click "Edit"

I

| 📑 IP Filte        | r List  |  |   | <u>?</u> ×             |
|-------------------|---|--|---|------------------------|
|                   | An IP filter list is compo-<br>addresses and protocol | sed of multiple filters. In<br>Is can be combined into | this way, multiple su<br>one IP filter. | bnets, IP              |
| <u>N</u> ame:     |   |  |   |                        |
| D1804V            | to XP   |  |   |                        |
| ,<br>Descript     | ion:  |  |   | <u>A</u> dd            |
| Make a            | filter from D1804V to XP                              |  | <b>A</b>                                | <u>E</u> dit           |
|                   |   |  | -                                       | <u>R</u> emove         |
| Filter <u>s</u> : |   |  |   | Use Add <u>W</u> izard |
| Mirrore           | d Description   | Protocol   | Source Port                             | Destination            |
| Yes               |   | ANY  | ANY                                     | ANY                    |
|                   |   |  |   |                        |
|                   |   |  |   | F                      |
|                   |   |  | ОК                                      | Cancel                 |

62. Uncheck "Mirrored. Also match packets with exact opposite source..." then click "OK" \*

| ilter Properties                                    |             |            |             |          | <u>?</u> × |
|---|-------------|------------|-------------|----------|------------|
| Addressing Protocol Descri                          | ption       |            |             |          |            |
| <u>Source address:</u>                              |             |            |             |          |            |
| A specific IP Subnet                                |             |            |             | •        |            |
| <u>I</u> P Address:                                 | 192         | . 168      | . 0         | . 0      |            |
| Subnet <u>m</u> ask:                                | 255         | . 255      | . 255       | . 0      |            |
|   |             |            |             |          |            |
| A specific IP Address                               |             |            |             | •        |            |
| IP add <u>r</u> ess:                                | 202         | . 129      | . 97        | . 101    |            |
| Subnet mas <u>k</u> :                               | 255         | . 255      | . 255       | . 255    |            |
| Mirrored. Also match pack<br>destination addresses. | kets with t | he exact o | opposite so | urce and |            |
|   |             |            | ОК          | Ca       | ncel       |

\* If your client gets IP address dynamically you will see "My IP Address" in Destination address field.

## 63.Click "**Ok**"

| 🗌 IP Filte            | r List  |   |   | <u>? ×</u>             |
|-----------------------|---|---|---|------------------------|
| [d]b]                 | An IP filter list is compo-<br>addresses and protocol | sed of multiple filters. In<br>s can be combined into | this way, multiple su<br>one IP filter. | ubnets, IP             |
| <u>N</u> ame:         |   |   |   |                        |
| D1804V                | to XP   |   |   |                        |
| ,<br><u>D</u> escript | ion:  |   |   | <u>A</u> dd            |
| Make a                | filter from D1804V to XP                              |   | <u>_</u>                                | []                     |
|                       |   |   | 7                                       | <u>R</u> emove         |
| Filter <u>s</u> :     |   |   | V                                       | Use Add <u>W</u> izard |
| Mirrore               | d Description   | Protocol  | Source Port                             | Destination            |
| No                    |   | ANY   | ANY                                     | ANY                    |
| 1                     |   |   |   | Þ                      |
|                       |   |   | ОК                                      | Cancel                 |

### 64.Click "Close"

| Rule Properties                                      | ?   |
|--|---|
| Authentication Methods Tu<br>IP Filter List          | nnel Setting Connection Type<br>Filter Action |
| The selected IP filter lis<br>affected by this rule. | t specifies which network traffic will be     |
| IP Filter <u>L</u> ists:                             | Description                                   |
|  | Matches all ICMP packets betw                 |
|  | Matches all IP packets from this              |
| ODI804V to XP  | Make a filter from DI804V to XP               |
| O XP to D1804V                                       | Makes a hiter from XP to D1804V               |
| Add  | <u>R</u> emove                                |

| P with DI804¥ Prope | rties                      |                 |
|---------------------|----------------------------|-----------------|
| Rules General       |                            |                 |
| Security ru         | les for communicating with | other computers |
| IP Security rules:  |                            |                 |
| IP Filter List      | Filter Action              | Authentication  |
| XP to DI804V        | 3DES_MD5                   | Preshared Key   |
| DI804V to XP        | 3DES_MD5                   | Preshared Key   |
|                     |                            |                 |
|                     |                            | 1               |
|                     | Edit Remove                | J               |

66.Right-click on the below and select "Assign"

| Console1 - [Console Root\IP Security Policies on Local Computer]   | _ 8 X |
|--|-------|
| Ele Action View Favorites Window Help  | 6 ×   |
|  |       |
| Console Root Name / Description Policy Assigned  |       |
| SP Security Policies on Local Comp Collect (Respond Only) Communicate normally (uns No   |       |
| D1804V with top No   |       |
| Caseure Server (Requir For all IP traffic, always req No Assion  |       |
| Convertige of the second secon |       |
| Delete   |       |
| Rename   |       |
| Properties   |       |
|  |       |
| nep  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
|  |       |
| Assign this policy, attempt to make it active  |       |

67. On XP/2000 IPSec client machine do a **PING** to a valid machine (which HAS the default gateway pointing to DFL-500 internal IP address and NO anti-virus or ANY other blocking software installed) on the Remote private network in the Dos Command Prompt: "ping 192.168.0.101 –t"

| 📾 Command Prompt - ping 192.168.0.101 -t   | - 🗆 🗵 |
|--|-------|
| C:\Documents and Settings\Serge>ping 192.168.0.101 -t  |       |
| Pinging 192.168.0.101 with 32 bytes of data:   |       |
| Negotiating IP Security.<br>Negotiating IP Security.<br>Negotiating IP Security.<br>Negotiating IP Security.<br>Negotiating IP Security.<br>Negotiating IP Security.<br>Negotiating IP Security.<br>Reply from 192.168.0.101: bytes=32 time=4ms TIL=127<br>Reply from 192.168.0.101: bytes=32 time=4ms TIL=127 |       |
| Reply from 192.168.0.101: bytes=32 time=4ms IIL=127<br>Reply from 192.168.0.101: bytes=32 time=4ms TTL=127   |       |
| Reply from 192.168.0.101: bytes=32 time=4ms TTL=127  | -     |

# **III. Monitoring and managing the VPN connection**

You can use two tools to monitor your VPN connection. It is Microsoft IP Security Monitor and D-Link DI-804V VPN Router Device Status Monitor. Let's go to the VPN Client menu first and check out the VPN Connection status. Go to Device Status, then click VPN Status in the bottom left corner of the screen:



You will see the connection, which we have just created:

| 🚰 YPN Status - Microsoft Internet Explorer |            |                    |                |                  |                 |      | <br>Ľ |            |            |         |      |   |
|--|------------|--------------------|----------------|------------------|-----------------|------|-------|------------|------------|---------|------|---|
|  | VPN STATUS |                    |                |                  |                 |      |       |            |            | 4       |      |   |
| IPS  | ec Co      | nnection           | Status         |                  |                 |      |       |            |            |         |      |   |
|  | Status     | Connection<br>Name | Remote IP      | Virtual Network  | Interface       | Туре | State | Tx<br>Pkts | Rx<br>Pkts | UpTime  | Drop |   |
|  | Inactive   | XP                 | 202.129.97.101 | 202.129.97.96/27 | WAN<br>Ethernet |      | Idle  | 0          | 0          | 0 0:0:0 | Drop |   |
|  |            |                    |                |                  |                 |      |       |            |            |         |      |   |
|  |            |                    |                |                  |                 |      |       |            |            |         |      |   |
| Сор  | yright 20  | 00                 |                |                  |                 |      |       |            |            |         |      |   |
|  |            |                    |                |                  |                 |      |       |            |            |         |      |   |
|  |            |                    |                |                  |                 |      |       |            |            |         |      |   |
|  |            |                    |                |                  |                 |      |       |            |            |         |      |   |
|  |            |                    |                |                  |                 |      |       |            |            |         |      |   |
|  |            |                    |                |                  |                 |      |       |            |            |         |      | - |
| 1 🛃  | 0 seconds  | left until page    | e refresh!     |                  |                 |      |       |            |            | 🥑 Inter | met  |   |

The status of the connection is Inactive or Idle, it means, that there is no active VPN connections at this time, however the VPN connection itself is created. Later on, you will be able to drop the unnecessary or suspecting connections by clicking Drop button. You can also drop the connection by clicking the right-mouse button in Microsoft Management Concole (MMC), while pointing onto the active connection:



Now let's go back to Microsoft Management Console. We need to add one more Snap-in there. Go to File, then to Add/Remove Snap-in and choose IP Security Monitor:



You have a choice of Generic Filters, Specific Filters, IKE Policies and Security Associations in Quick and Main modes.

Let's look at Generic Filters in Main mode:

| Console1 - [Console Root\IP Secu   | urity Monitor\SERGE\/ | Main Mode\Generic Filte | rs]            |            |                        |                 | _ # X |
|------------------------------------|-----------------------|-------------------------|----------------|------------|------------------------|-----------------|-------|
| Ble Action Yew Favgrites y         | ₩indow Help           |                         |                |            |                        |                 | _@×   |
| ← → 💼 🖪 🗙 🕄 😫                      | 2                     |                         |                |            |                        |                 |       |
| Console Root                       | Name                  | Source                  | Destination    | IKE Policy | Authentication Methods | Interface Type  |       |
| IP Security Policies on Local Comp | 11 III                | Me                      | 202.129.97.101 | S          | Preshared Key          | All connections |       |
| - SERGE                            | 3, 12                 | Me                      | 202.129.97.105 | 5          | Preshared Key          | All connections |       |
| 🖂 🚞 Main Mode                      |                       |                         |                |            |                        |                 |       |
| Constitution Street                |                       |                         |                |            |                        |                 |       |
| - IKE Policies                     |                       |                         |                |            |                        |                 |       |
| - Security Associations            |                       |                         |                |            |                        |                 |       |
| Quick Mode     Generic Elberr      |                       |                         |                |            |                        |                 |       |
| - Specific Filters                 |                       |                         |                |            |                        |                 |       |
| - Negotiation Policies             |                       |                         |                |            |                        |                 |       |
| Security Associations              |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
|                                    |                       |                         |                |            |                        |                 |       |
| · · ·                              | 1                     |                         |                |            |                        |                 |       |

You can see two connections there: one with a destination of 202.129.97.105 and another one with a destination of 202.129.97.101. Those are our "XP to DI804V" and "DI804V to XP" connections. Now click on to the one with 202.129.97.105 connection. You will see the following:

| 12 Properties   |                                     |                     |                | <u>?</u> × |  |  |  |  |
|---|-------------------------------------|---------------------|----------------|------------|--|--|--|--|
| General Authentic   | ation Methods                       |                     |                |            |  |  |  |  |
| Source:<br>Address: Me<br>Destination:<br>Address: 202.129.97.105 Mask: 255.255.255.255 |                                     |                     |                |            |  |  |  |  |
| Create Mirror:  | Yes                                 |                     |                |            |  |  |  |  |
| Policy Name:  | 5                                   |                     |                |            |  |  |  |  |
| The specific main mode filters expanded from this generic filter:                       |                                     |                     |                |            |  |  |  |  |
| Source  | Source Destination Direction Weight |                     |                |            |  |  |  |  |
| 202.129.97.105<br>202.129.97.101  | 202.129.97.101<br>202.129.97.105    | Inbound<br>Outbound | 69206<br>69206 |            |  |  |  |  |
|   | OK                                  | Ca                  | ancel          | Apply      |  |  |  |  |

It basically tells you the source and destination of connections as well as a weight of the connection.

Now click on Authentication Methods:



What you see there is the Preshared Key used in this connection. In Specific Filters, we basically see the same information, but in a bit different order:



In IKE Policies you can see the authentication and encryption modes available:

| 5 Pi | operties                   |           |                |                  | ? ×     |  |  |  |  |
|------|----------------------------|-----------|----------------|------------------|---------|--|--|--|--|
| G    | eneral                     |           |                |                  |         |  |  |  |  |
|      | Offers of this IKE policy: |           |                |                  |         |  |  |  |  |
|      | Encryption                 | Integrity | Diffie-Hellman | Quick Mode Limit | Key Lif |  |  |  |  |
|      | 3DES                       | SHA1      | Medium (2)     | 0                | 0/2880  |  |  |  |  |
|      | 3DES 🛛                     | MD5       | Medium (2)     | 0                | 0/2880  |  |  |  |  |
|      | DES                        | SHA1      | Low (1)        | 0                | 0/2880  |  |  |  |  |
|      | DES                        | MD5       | Low (1)        | 0                | 0/2880  |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |
|      |                            |           | ОК             | Cancel           | Acoly   |  |  |  |  |
|      |                            |           |                |                  |         |  |  |  |  |

And finally, in the Security Associations you will see the following:

| 202.129.97.101 Prop | erties               |                      | <u>?</u> ×    |  |  |  |
|---------------------|----------------------|----------------------|---------------|--|--|--|
| General             |                      |                      |               |  |  |  |
| Me: 202.129.97.1    | D1 Peer              | Peer: 202.129.97.105 |               |  |  |  |
| Authentication: Pr  | eshared Key          | ,                    |               |  |  |  |
| IKE Policy: 5       |                      |                      |               |  |  |  |
| ⊢ The Selected Offe | r                    |                      |               |  |  |  |
| Encryption:         | 3DE:                 | S                    |               |  |  |  |
| Integrity:          | SHA                  | 1                    |               |  |  |  |
| Diffie Hellman Gro  | up: Medi             | Medium (2)           |               |  |  |  |
| Key Lifetimes (KB/  | 'Sec): 0/28          | 0/28800              |               |  |  |  |
| Quick Mode SAs es   | ablished on this SA: |                      |               |  |  |  |
| Source Address      | Destination Address  | Source Port          | Destination F |  |  |  |
| •                   |                      |                      | Þ             |  |  |  |
|                     | OK                   | Cancel               | Apply         |  |  |  |

What we see here is the encryption and integrity algorithms, which were actually chosen from the options we had in IKE Policy window. The algorithms are chosen during the negotiation phase. In our example, we have a IKE Policy 5 chosen. You can also see the Key Lifetimes here.

Now let's go back to VPN Router and check the VPN Status there:

| 🚈 VPN Status - Microsoft Internet Explorer   |   |  |  |  |  |  |  |  |  |
|--|---|--|--|--|--|--|--|--|--|
| VPN STATUS   |   |  |  |  |  |  |  |  |  |
| IPSec Connection Status  |   |  |  |  |  |  |  |  |  |
| Status         Connection<br>Name         Remote IP         Virtual Network         Interface         Type         State         Tx<br>Pkts         Rx<br>Pkts         UpTime         Drop |   |  |  |  |  |  |  |  |  |
| Active XP 202.129.97.101 202.129.97.96/27 WAN Ethernet CBC CBC Stab. 70 1806 0:37:2  |   |  |  |  |  |  |  |  |  |
|  |   |  |  |  |  |  |  |  |  |
| Copyright 2000   | - |  |  |  |  |  |  |  |  |
|  |   |  |  |  |  |  |  |  |  |
|  |   |  |  |  |  |  |  |  |  |
| 17. seconds left until name refrecht   |   |  |  |  |  |  |  |  |  |

What you see now is that the VPN connection is active. You can also see the Encryption and Integrity modes used. The state of the VPN Connection is M->Q-Established. You can also see the amount of packets received and send as well as up time. As previously told, you can drop the connection by clicking Drop on the VPN Router, or Un-assigning the IPSec policy in XP MMC.

That's basically it and now you can use your VPN connection with ease.