# DFL-600 With Windows XP IPSec VPN Configuration Procedures

Beta version of the setup, please note the IP address's used are example use only.

### I. Configuring D-Link DFL-600 VPN Router

#### **DFL-600 Settings:**

This is the page you need to go into to change the IP, once you have change it make sure your PC has the same subnet.

Remember to Access the unit with the default IP 192.168.0.1:8081 In the below the IP was changed.







# **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.

Please change DI-804V to DFL-600 in the below shots.

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

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

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

🚡 Co	nsole1 - [Console Root]			_ 8 ×
1 🛸	<u>C</u> onsole <u>W</u> indow <u>H</u> elp		. D 😂 🖬 🛛	I _ 8 ×
<u>A</u> r Tre∈	New Open Save	Ctrl+N Ctrl+O Ctrl+S	3	
	Save As			
	Add/Remove Snap-in Options	Ctrl+M		
	1 D:\WINNT\System32\Inetsrv\ii 2 D:\WINNT\system32\devmgmt	s		
	Exit			

3.Click "Add"

Add/Remove Snap-i	in	? ×
Standalone Extensi	ons	
Use this page to ad	d or remove a standalone Snap-in from the conso	ile.
<u>S</u> nap-ins added to:	Console Root	•
Description		
	<u>R</u> emove <u>Ab</u> out	
	ОК	Cancel

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



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

Local cor	nputer			
The comp	uter this console is rur	nning on		
C <u>M</u> anage	domain policy for this o	computer's do	main	
C Manage	domain policy for anot	her <u>d</u> omain:		
C Another r	:omputer:			
			Browne	
I.			DIDAASe	

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	
Recurity Policies on Local Machine	
Description	
Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.	
Add <u>R</u> emove <u>Ab</u> out	
OK Cancel	



#### 8.Click "Next"

IP Security Policy Wizard	?×
	Welcome to the IP Security Policy wizard.
	This wizard helps you create an IP Security Policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.
	To continue, click Next.
	< Back Next> Cancel

9.Enter the details below and click "Next"

IP Security Policy Wizard	? ×
IP Security Policy Name Name this IP Security policy and provide a brief description	ļ
Na <u>m</u> e:	
DI804V with XP	
Description:	
D1804V communicates with XP	
	<b>v</b>
< <u>₿</u> ack <u>N</u> ext >	Cancel

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

Security Policy Wizard	? ×
Requests for Secure Communication Specify how this policy responds to requests for secure communication.	Ē
The default response rule responds to remote computers that request security other rule applies. To communicate securely, the computer must respond to re secure communication.	), when no equests 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 based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.
	A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.
	Security actions:
	Authentication methods
	- Filter actions
	To continue, click Next.
	< Back Cancel

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



\* If your client gets IP address dynamically click to "This rule does not specify a tunnel".

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

	,		
Security Rule Wizard			? ×
Network Type The security rule must be applied to a netwo	ork type.		<u>[</u> ]
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

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

ecurit	y Rule Wizard			?
Aut	nentication Method To add multiple authentication me IP Security rule wizard.	thods, edit the security rule	after completing the	
	Set the initial authentication metho	od for this security rule:		
	C Active Directory default (Kerbe	eros V5 protocol)		
Use a certificate from this certification authority (CA):				
			Browse	
	Use this string to protect the k	ey exchange (preshared ke	ey):	
	1234567			4
				<b>_</b>
	,			_

#### 17.Select "Add"

Security Rule Wizard							
IP Filter List Select the IP filter list for the type of IP traffic to which this security rule applies.							
If no IP filter in the following list matches your needs, click Add to create a new one.							
Name	Description	Add					
O <mark>I All ICMP Traffic</mark> O All IP Traffic	Matches all ICMP packets bet Matches all IP packets from t	Edit					
<u> &lt; B</u> ack <u>N</u> ext > Cancel							

#### 18.Enter a filter name then click "Add"

📑 IP Filte	er List			? ×
t d h t	An IP filter list is compose addresses and protocol	sed of multiple filters. In s can be combined into	this way, multiple sub one IP filter.	onets, IP
<u>N</u> ame:				
XP to D	1804V			
Descript	ion:			<u>A</u> dd
Make a	filter from XP to D1804V		<u>^</u>	<u>E</u> dit
			-	<u>R</u> emove
Filters:			<b>V</b> (	Jse Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
			OK	Cancel



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

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

Source address:					-		
A specific IP Address				-			
<u>I</u> P Address:	202	. 1	29	. 97	. 1	01	
Subnet <u>m</u> ask:	255	. 2	55	255	. 2	55	

\* 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										? X
IP Traffic Destination Specify the destination add	lress of th	ie IF	<sup>o</sup> traffic							đ
Destination address:										
A specific IP Subnet						•				
IP add <u>r</u> ess:	192	•	168	•	0	•	0			
Subnet mas <u>k</u> :	255	•	255		255	•	0			
				< [	<u>B</u> ack		<u>N</u> ext	>	Can	icel

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





24.Click "Ok"

IP Filter	List			? ×
	An IP filter list is compose addresses and protocol	sed of multiple filters. In Is can be combined into	this way, multiple one IP filter.	e subnets, IP
<u>N</u> ame:				
XP to DI	804V			
Descriptio	on:			<u>A</u> dd
Make a f	ilter from XP to D1804V		k	<u>E</u> dit
				<u>R</u> emove
Filters:			I	✓ Use Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY
		-		
			OK	Cancel
				/

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

Security Rule Wizard		? ×
IP Filter List Select the IP filter list for the t	ype of IP traffic to which this security rule	applies.
If no IP filter in the following li	st matches your needs, click Add to creat	e a new one.
<u>I</u> P filter lists:		
Name	Description	<u>A</u> dd
O All ICMP Traffic	Matches all ICMP packets bet	
O All IP Traffic	Matches all IP packets from t	<u>E</u> dit
⊙ XP to DI804V	Makes a filter from XP to D180	<u>R</u> emove
1		
	< <u>B</u> ack <u>N</u> ext	> Cancel

#### 26.Click "Add"

Security	Rule Wizard		? ×
Filter 9	r Action Select the filter action for this secu	rity rule.	Ē
li c	f no filter actions in the following lis one. Select Use Add Wizard to cre	st matches your needs, click Add to ate a filter action.	i create a new
F	ilter A <u>c</u> tions:	V	Use Add <u>W</u> izard
[	Name	Description	Add
	Permit     Request Security (Optional)     Require Security	Permit unsecured IP packets t Accepts unsecured communi Accepts unsecured communi	Edit
		< <u>B</u> ack <u>N</u> ext	Cancel

#### 27.Click "Next"

Filter Action Wizard	<u>?</u> ×				
	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 transfer. These requirements are specified in a list of security methods contained in the filter action.				
	Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.				
	To continue, click Next.				
	< <u>₿</u> ack <b>Next&gt;</b> Cancel				

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

Filter Action Wizard	? ×
Filter Action Name Name this filter action and optionally give a brief description	1691
Name:  3DES_MD5	
Description:  3DES_MD5	<u> </u>
	Y
< <u>B</u> ack <u>N</u> ext >	Cancel

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

ilter Action General Options 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"

.

cer Action wizard				- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1
Communicating wit Communicating w network to securi	h computers that do ith computers that do no ty risks.	not support IP t support IPSec m	Sec Nay expose your	1001
Do you want to al	low communication with	computers the do	not support IPSe	c?
Do not commit	unicate with computers t	hat do not support	t IPSec.	
C Fall back to <u>u</u>	nsecured communication	1.		
Use this optio Communicatio to security risk	n if there are computers n with computers that do .s.	that do not suppor o not support IPSe	rt IPSec on your n c may expose you	etwork. .r network
		< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Security Method Wizard	2 X
IP Traffic Security Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard.	
This filter action requires at least one security method for IP traffic.	
<ul> <li>High (Encapsulated Secure Payload)         Data will be encrypted, authenticated, and unmodified.         Medium (Authenticated Header)         Data will be authentic and unmodified, but will not be encrypted.     </li> <li>Custom         Settings     </li> </ul>	
< <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	<u>? ×</u>
Specify the settings for this custom sec	urity method.
Data and address integrity without o	encryption ( <u>A</u> H) :
MD5	
Data integrity and encryption (ESP)	:
Encryption algorithm:	
Generate a new key every:	Gene <u>r</u> ate a new key every 3600 <u>s</u> econds
	OK Cancel

#### 33.Click "Next"

	110/11			
Securi	ity Method Wizard			? ×
IP	Traffic Security Specify a security method for IP traffic. To add filter action after completing the wizard.	multiple secu	rity methods edit t	he 🛒
	This filter action requires at least one security m	ethod for IP t	raffic.	
	High (Encapsulated Secure Payload)     Data will be encrypted, authenticated, and     Medium (Authenticated Header)     Data will be authentic and unmodified, but w     Lustom     Settings	unmodified. will not be en	crypted.	
		< <u>B</u> ack	<u>N</u> ext >	Cancel

#### 34.Click "Finish"

Filter Action Wizard	<u>? ×</u>
	Completing the IP Security filter action Wizard You have successfully completed the IP Security Policy wizard. To edit your filter action now, select the Edit properties 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 Select the filter action for this secu	rity rule.	Ē
If no filter actions in the following lis one. Select Use Add Wizard to cre	st matches your needs, click Add to 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>E</u> dit
O Request Security (Optional) O Require Security	Accepts unsecured communi Accepts unsecured communi	<u>R</u> emove
	< <u>B</u> ack <u>N</u> ext	t> Cancel

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

3DES_MD5 Pr	operties			<u> </u>
Security Meth	nods General			
<ul> <li>Permit</li> <li>Block</li> <li>Negotia</li> <li>Security Meta</li> </ul>	te security: thod preference o	order:		
Туре	AH Integrity	ESP Confident	ial ES	A <u>d</u> d
Custom	<none></none>	3DES	MC .	<u>E</u> dit <u>R</u> emove Move <u>up</u> Move d <u>o</u> wn
<ul> <li>✓ Accept</li> <li>✓ Allow ur</li> <li>✓ Session</li> </ul>	unsecured commi nsecured commun key <u>P</u> erfect Forw	unication, but alv ication <u>w</u> ith non ard Secrecy	vays respond u IPSec-aware o	ising <u>I</u> PSec computer
		OK	Cancel	

#### 37.Click "Next"



#### 38.Click "Finish'



#### 39.Click "Add"





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

Security Rule Wizard	<u>?</u> ×
Tunnel Endpoint The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.	Ī
An IPSec tunnel allows packets to traverse a public or private internetwork with the 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 . 105	
< <u>B</u> ack Next > C	ancel

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



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

=y.	DI-604 V preshared key) then click <b>Next</b>
	Security Rule Wizard
	Authentication Method To add multiple authentication methods, edit the security rule after completing the 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):
	BTowse***
	O Use this string to protect the key exchange (preshared key):
	1234567
	< <u>B</u> ack <u>N</u> ext > Cancel

#### 44. Click "Add"

Security Rule Wizard		? ×
IP Filter List Select the IP filter list	for the type of IP traffic to which this security rule	e applies.
If no IP filter in the foll IP filter lists:	owing list matches your needs, click Add to crea	te a new one.
Name	Description	<u>A</u> dd
All ICMP Traffic     All IP Traffic     All IP Traffic     XP to D1804V	Matches all ICMP packets bet Matches all IP packets from t Makes a filter from XP to D180	<u>E</u> dit <u>R</u> emove
	< <u>B</u> ack <u>N</u> ext	> Cancel

#### 45. Enter a filter name then click on "Add"

IP Filter List			? ×
An IP filter	list is composed of multiple filte and protocols can be combine	rs. In this way, multiple sub d into one IP filter.	nets, IP
Name:			
DI804V to XP			
Description:			<u>A</u> dd
Make a filter from DI	804V to XP	<u>~</u>	<u>E</u> dit
		<b>V</b>	<u>R</u> emove
Filter <u>s</u> :		V L	Jse Add <u>W</u> izard
Mirrored Descripti	on Protocol	Source Port	Destination
4		ОК	▶ Cancel



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

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

lter Wizard								?
IP Traffic So Specify th	p <b>urce</b> e source address	of the IP	traffic.					Ē
<u>S</u> ource ad	ldress:							
A specific	: IP Subnet				•			
	IP Address:	192	. 168	. 0	•	0		
	Subnet <u>m</u> ask:	255	. 255	. 255		0		
	,							
				< <u>B</u> ack		Next :	>	Cancel

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

Traffic Destination Specify the destination add	lress of th	e IP trai	fic.					Ē
A specific IP Address					•			
IP add <u>r</u> ess:	202	. 12	9.	97		101		
Subnet mas <u>k</u> :	255	. 25	5.	255		255		
							_	

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





#### 51.Click on "Close"

IP Filter List			?
An IP filter list is comp addresses and protoc	oosed of multiple filter ols can be combined	s. In this way, multiple su Linto one IP filter.	bnets, IP
Name:			
DI804V to XP			
<u>D</u> escription:			<u>A</u> dd
Make a filter from D1804V to XP	D	<u> </u>	<u>E</u> dit
		-	<u>R</u> emove
Filter <u>s</u> :		<b>V</b>	Use Add <u>W</u> izard
Mirrored Description	Protocol	Source Port	Destination
Yes	ANY	ANY	ANY
•			Ŀ
		ок	Cancel

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

Security Rule Wizard		<u>? ×</u>
<b>IP Filter List</b> Select the IP filter li	t for the type of IP traffic to which this security rule	applies.
If no IP filter in the fi	ollowing list matches your needs, click Add to creat	ie a new one.
Name	Description	Add
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets bet Matches all IP packets from t	<u> </u>
OI804V to XP XP to DI804V	Make a filter from D1804V to XP Makes a filter from XP to D180	<u>R</u> emove
	< <u>B</u> ack <u>N</u> ext	> Cancel

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

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

#### 54.Click "Finish"

Security Rule Wizard		<u>? ×</u>
	Completing the New Rule Wizard You have successfully completed specifying the properties for your new rule. To edit your security rule now, select the Edit properties check box, and then click Finish.	
	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 rul	les for communicating with o	ther 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
•	Edit Bemove	1 🖬 📖 🗛 🗛 🖉	
		Close Ca	ncel

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

Rule Properties	?
Authentication Methods Tur IP Filter List	nnel Setting Connection Type Filter Action
The selected IP filter lis affected by this rule.	t specifies which network traffic will be
IP Filter <u>L</u> ists:	
Name	Description
O All ICMP Traffic	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
⊙ XP to DI804V	Makes a filter from XP to D1804V
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
01	Cancel Apply

#### 57.Click "Edit"

📑 IP Filte	r List			? ×
	An IP filter list is compose addresses and protocol	ed of multiple filters. In l s can be combined into	his way, multiple sub one IP filter.	onets, IP
<u>N</u> ame:				
XP to D	1804V			
<u>D</u> escript	ion:			<u>A</u> dd
Makes	a filter from XP to D1804V		<u> </u>	<u>E</u> dit
			<b>v</b>	<u>R</u> emove
Filter <u>s</u> :				Jse Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY
•				F
			ОК	Cancel

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

lter Properties								?
Addressing Protocol Descri	iption							
<u>Source address:</u>								
A specific IP Address						•		
<u>I</u> P Address:	202	•	129	•	97	•	101	1
Subnet <u>m</u> ask:	255		255	•	255		255	
	·							
A specific IP Subnet		_				•		
IP add <u>r</u> ess:	192	•	168	•	0	•	0	
Subnet mas <u>k</u> :	255	·	255	•	255	•	0	
Mirrored. Also match pack destination addresses.	kets with	the	exact o	)pp	osite sc	ourc	e and	
					OK.	1	Car	ncel

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

#### 59.Click "Close"

📑 IP Filte	r List			? ×
	An IP filter list is compo- addresses and protocol	sed of multiple filters. In is can be combined into	this way, multiple sub one IP filter.	nets, IP
<u>N</u> ame:				
XP to D	1804V			
Descript	ion:			<u>A</u> dd
Makes	a filter from XP to D1804V		<u>^</u>	<u>E</u> dit
			<b>V</b>	<u>R</u> emove
Filter <u>s</u> :			V U	se Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY
				<u> </u>
			OK	Cancel

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

Edit Rule Properties	<u>? ×</u>
Authentication Methods Tu IP Filter List	nnel Setting Connection Type   Filter Action   t specifies which network traffic will be
IP Filter Lists:	
Name	Description
O All ICMP Traffic	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 hiter from XP to D18U4V
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
Clo	se Cancel <u>Apply</u>

## 61.Click "Edit"

🗌 IP Filte	r List			? ×
   	An IP filter list is compo- addresses and protocol	sed of multiple filters. In Is can be combined into	this way, multiple one IP filter.	subnets, IP
<u>N</u> ame:				
D1804V	to XP			
, <u>D</u> escript	ion:			<u>A</u> dd
Make a	filter from D1804V to XP		_	<u>E</u> dit
			-	<u>R</u> emove
Filters:			R	Vise Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY
•				Þ
			OK	Cancel

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

ilter Properties							<u>?</u> >
Addressing Protocol Descr	iption						
<u>Source address:</u>							
A specific IP Subnet					•		
<u>I</u> P Address:	192	. 16	8.	0		0	
Subnet <u>m</u> ask:	255	. 25	5.	255	•	0	
	,						
A specific IP Address					•		
IP add <u>r</u> ess:	202	. 12	9.	97	•	101	
Subnet mas <u>k</u> :	255	. 25	5.	255	÷	255	
Mirrored. Also match pactination addresses.	kets with I	the exac	t opp	oosite si	ourc	e and	
		[		ОК		Car	ncel

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

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

<u>? ×</u>
e filters. In this way, multiple subnets, IP nbined into one IP filter.
<u>A</u> dd
<u> </u>
<u> </u>
🔽 Use Add <u>W</u> izard
Source Port Destination
ANY ANY
Ľ
OK Cancel

### 64.Click "Close"

Rule Properties				?
Authentication Methods   IP Filter List	Tur	nnel Setting	Connection Ty Filter Action	pe
The selected IP fil affected by this rul	ter list le.	specifies whi	ch network traffic will	be
P Filter <u>L</u> ists: Name		Description		_
O All ICMP Traffic		Matches all I	CMP packets betw	
O All IP Traffic		Matches all I	P packets from this .	··
O DI804V to XP		Make a filter	from DI804V to XP	
Add Edit		<u>R</u> emove		
	Clos	xe (	ancel App	ly -

P with DI804¥ Prope	rties	
Rules General		
Security n	ules for communicating with	other computers
IP Security rules:	Filter Action	Authentication
XP to DI804V	3DES_MD5	Preshared Key
DI804V to XP	3DES_MD5	Preshared Key
Oynamic>	Default Response	Kerberos
Add	Edit Remove	🔽 🛛 🖉 🗸 🗸 🗸

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

Console1 - [Console Root\IP Secu	urity Policies on Local Cor	nputer]			_ # ×
🚡 File Action View Favorites V	Window Help				_161 ×
← → 🗈 🖬 🗙 🕾 🖳 🔮	2 🖻 📩 🖻 🖉				
Console Root	Name /	Description	Policy Assigned		
Sourty Pokes on Local Comp	Bit Care Respond (PP) Bit Source Server (Inequini Bit Source Server (Inequini Bit Source Server (Inequini Bit Source (Inequinit Source)	Consuricate normally (und . For all IP traffic, always reg For all IP traffic, always reg	No No Po Al Tasks Celeis Properties Help		
Assign this policy, attempt to make it active	0				

67.Do a **PING** to a valid machine on the Remote private network on the Dos Command Prompt (to bring up the IPSec tunnel) (Eg. ping 192.168.0.101 –t)

ex 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.	
Reply from $192.168.0.101$ : bytes=32 time=4ms TTL=127	
Reply from 192.168.0.101: bytes=32 time=4ms TTL=122	
Reply from 192.168.0.101: bytes=32 time=4ms IIL=127	
Reply from 192.168.0.101: Dytes=32 time=3ms 11L=127	
Reply from 192.106.0.101. bytes $-52$ time $-4$ ms 11L-127	
Reply from 192.168.0.101: bytes 32 time 4ms TTL=127	
Reply from 192.168.0.101: bytes=32 time=4ms TTL=127	
Reply from 192.168.0.101: bytes=32 time=3ms $TTL=127$	
Reply from $192.168.0.101$ : bytes=32 time=4ms TTL=127	
Reply from 192.168.0.101: bytes=32 time=4ms IIL=127	
Reply from 172.168.0.101: bytes=32 time=4ms IIL=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 DFL-600 VPN Router Device Status Monitor. Let's go to the VPN server menu first and check out the VPN Connection status. Go to Advanced, then click VPN-IPSec then IPSec Status. You should see something like the below.



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:

Console1 - [Console Root /IP Sect	anty Policies on Local Con	iputer]				그린 스
🚡 File Action View Favorites V	Window Help					@_×
← → 🗈 📧 🗙 🕾 🚱	🖹 📩 🕷 🖪					
Console Root	Name /	Description		Policy Assigned		
Security Policies on Local Comp	Client (Respond Only)	Communicat	e normaliv (uns	No		
	DI804V with XP	Г	I be analysis	Yes		
	Secure Server (Requir	For all IP tr	Un-assign	No		
	Server (Request Secu	For all IP tr	All Tasks 🕨	No		
			Delete			
			Rename			
		1	Properties			
			нер			
		-		-		
× ×						
Un-assign this policy, attempt to make it in	active					

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:

Add Standalone Snap-in		? ×
Available Standalone Snap-ins:		
Snap-in	Vendor	
🚮 Group Policy	Microsoft Corporation	
📔 🎦 Indexing Service	Microsoft Corporation, I	
🖶 IP Security Monitor	Microsoft Corporation	
lP Security Policy Management	Microsoft Corporation	
💽 Link to Web Address	Microsoft Corporation	
🔣 Local Users and Groups	Microsoft Corporation	
👹 Performance Logs and Alerts	Microsoft Corporation	
Premovable Storage Management	Microsoft Corporation	
🚮 Resultant Set of Policy	Microsoft Corporation	
📴 Security Configuration and Analysis	Microsoft Corporation	-
The IP Security monitor snap-in is used to	monitor the IP Security statu	JS.
Г		-
L	<u>A</u> dd <u>C</u> lose	

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:

Console 1 - [Console Root/JP Security Monitor/SERGE/Main Mode/Generic Filters]							_8 X
🚡 Elle Action Yew Favgrites y	Window Help						_8×
← → 🗈 🖬 🗡 🕄 😼	2						
Console Root	Name	Source	Destination	IKE Policy	Authentication Methods	Interface Type	
P Security Policies on Local Comp	<b>#</b> 11	Me	202.129.97.101	5	Preshared Key	All connections	
B SECURY MONITOR	12	Me	202.129.97.105	5	Preshared Key	All connections	
Good States     Good Stat	<b>T</b>	70	200.127197-105	2	Heward Key	AI COPIECTOR	
	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 Authentica	ation Methods			
	Source: Address: Me Destination: Address: 202 Interface Type: Create Mirror:	.129.97.105 M. All connections Yes	ask: 255.255.	255.255	
	Policy Name:	5			
	The <u>s</u> pecific main r	node filters expande	ed from this ge	neric filter:	
	Source	Destination	Direction	Weight	
	202.129.97.105 202.129.97.101	202.129.97.101 202.129.97.105	Inbound Outbound	69206 69206	
		ОК		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 Pr	operties				? ×
G	eneral				
	1				1
	Offers of this IK	E policy:			
	Encryption	Integrity	Diffie-Hellman	Quick Mode Limit	Key Lif
	3DES	SHA1	Medium (2)	0	0/2880
	3DES DES	MD5 SHA1	Medium (2)	0	0/2880
	DES	MD5	Low (1)	0	0/2880
	•				<u> </u>
_					
			OK	Cancel	Apply

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

02.129.97.101 Prop	erties			?
General				
Me: 202.129.97.1	01	Peer:	202.129.97.10	15
Authentication: Pr	eshared Key			
IKE Policy: 5				
The Selected Offe	r			
Encryption:		3DES	6	
Integrity:		SHA	1	
Diffie Hellman Gro	up:	Medi	um (2)	
Key Lifetimes (KB)	'Sec):	0/28	800	
Uuick Mode SAs es	Destination Add	5A: dress	Source Port	Destination F
•				
	01		Cancel	Applu
			Cancor	OPPly

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.

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.

~ End of Document ~