## DFL-500 With Windows XP/2000 IPSec VPN Client Configuration Guide

### I. Configuring D-Link DFL-500 Firewall

- 1. Connect your computer to the internal port of the DFL-500 Firewall
- 2. Change the computer IP address to 192.168.1.100 255.255.255.0
- 3. In Internet Explorer address type: https://192.168.1.99
- 4. You will see the message with a Security Alert
- 5. Click "yes", you are in the Web Base Interface (WBI)
- 6. Type "admin" in the Name field and click "Login"

Status     Monitor       Status     Monitor       Status     Monitor       Status     Firmware Version:       DLINK-S00 2.27,build042,020808     Image: Comparison of the status of the stat	link –			Firewa	ll Appi	iance DFL-5	00 OLogow	t 🔍 Wizard	2
Soulig       rewall       PN       ID S       Firmware Version:     DLINK-S00 2.27,build042,020808       ID S       Antivirus:       Definitions       Yersion:       Story726/2002 14:01)       Yersion:       Serial Number:       FCT-S02801026300       System Settings:       Daveload       Uplead       Restart       Shutdown	im te ork	Status	Monitor						-1
IDS     Firmware Version:     DLTNK-S00 2.27,build0 42,020808       ntl-Virus     Antivirus Definitions:     3.5(07/26/2002 14:01)       reb Filter     Attack Definitions:     1.2(07/10/2002 15:40)       og&Report     Serial Number:     FGT-502801026300       System Settings:     Downlead     Uplead       Restore Factory Defaults     System:     Restore	9								
Antivitus: Definition:     3.5(07/26/2002 14:01)       /eb Filter     Version:       >g&Report     Attack Definitions Version:       Serial Number:     FGT-502801026300       System Settings:     Download       System:     Restore Factory Defaults       System:     Shutdown			Firmware Version:	DLINK-500	2.27,buil	ld042,020808	9		
Attack Definitions 1.2(07/10/2002 15:40)  Serial Number: FGT-502801026300 System Settings: Download Upload Restore Factory Defaults System: Restart Shutdown	/irus Filter		Antivirus Definitions Version:	3.5(07/26/	2002 14	:01)	<b>9</b>		
Serial Number:         FGT-502801026300           System Settings:         Download         Upload         Restore Factory Defaults           System:         Restart         Shutdown	Report		Attack Definitions Version:	1.2(07/10/	2002 15	:40)	9		
System Settings: <u>Downlead Upload Restore Factory Defaults</u> System: <u>Restart</u> Shutdown			Serial Number:	FGT-502801	1026300	)			
System: Restart Shutdown			System Settings:	Download	Upload	Restore Factor	Defaults		
			System:	Restart		Shutdown			

- 7. Click on "Network" under "System" menu
- 8. You will see "internal" and "external" interfaces
- 9. Click on Modify picture for "internal" interface
- 10. Put the ip address for the internal interface, for example 192.168.0.1 following the subnet mask 255.255.255.0 and press "**OK**". You will loose the connection to the firewall after you press "**OK**"
- 11. Now you can connect your firewall to switch or hub and connect your computer to that switch or hub
- 12. Make sure all the stations in the network (including your own computer) have the default address of your internal firewall interface, for example 192.168.0.1
- 13. Change the ip address of your computer to 192.168.0.100 255.255.255.0
- 14. Change the ip address in your Internet Explorer to https://192.168.0.1
- 15. Go to Systems/Network again and choose External interface
- Put the static IP address supplied by your internet provider, for example 202.129.97.105 255.255.255.0
- 17. Go to the Routing bookmark under System/Network and press "New"
- 18. Add the default route with the ip address supplied by your Internet prover. You create a default router by typing 0.0.0.0 for the destination network and destination network mask.
- 19. Go back to System/Network menu

#### 20. You will get the following configuration:

Interface         Nome         PC         Nome         Modely	D-Link Firewall - Microso	ilt Internet Explorer				
Control       Addees       Model	le Edit View Favorites	s Tools Help				
System       OFL-500       Oracest Control       Offlow       Off	) - 🗇 - 💌 🔊 🐔 -	Address 🕘 https://192.168.0	0.1/theme1/index?login=1			
System     Interface     DHS     Reuting     DHCP       Values     Values     Internal     192.168.0.1     255.255.255.0     HTTPS,PINO     Image: Control of the state of the	D-Link			Firewall Appl	iance DFL-500	- OLOgout Owizard On
Update     Name     IP     Network     Access     Modify       Config     internal     192.168.0.1     255.255.255.0     HTTPS,PING     dd/       Firewall     202.129.97.105     255.255.255.0     PING     dd/       VPN     NIDS     Anti-Virus     dd/     Biologia       Web Filter     Log&Report     Log&Report     Image: Control of the pice of the	System Status	Interface	DNS Routing	DHCP		
Config         internal         192.168.0.1         255.255.255.0         PTINS         BF           Firewall         202.129.97.105         255.255.255.0         PTINS         BF           Anti-Virus         Web Filter         Log&Report         E         E         E	Update Network	Name	IP	Netmask	Access	Modify
VPN NIDS Anti-Virus Web Filter Log&Report	Config	internal externa	192.168.0.1 202.129.97.105	255.255.255.0 255.255.255.0	HTTPS,PING PING	167 167
VPN NIDS Anti-Virus Web Filter Log&Report	Firewall					
Anti-Virus Web Filter Log&Report	VPN					
Anti-Virus Web Filter Log&Report	NIDS					
Done	Anti-Virus					
	Web Filter					
	Log&Report					
	Dooe					A Internat
		Department Minnesoft	D. Link France B., Mars			Incernec

- 21. Go to Firewall menu and choose Addresses
- 22. If your XP/2000 IPSec client has a dynamically assigned IP address, you need to skip steps 23 26!
- 23. In the Internal submenu press "New"
- 24. Type the name of your internal network, for example "**D-Link**" and put the ip address of the internal network, for example 192.168.0.0 255.255.255.0. You will see the following screen:

🙄 - 💌 🌒 Address 🧃	https://192.168.0.95/theme1/index?login=1		2 2
-Link		Firewall Appliance	Logout Swizard 📀
System	Internal External		
Firewall			
Mode	Name	IP/Netmask	Modify
Policy	Internal_All	0.0.0.0/0.0.0	
Address	DHLink	192.168.0.0/255.255.255.0	
Scherbile	A laws		
Users	New		
Virtual IP			
Port Forward			
IP/MAC Binding			
VPN			
NIDS			
Anti-Virus			
Web Filter			
.og&Report			

#### 25. Go to External submenu and press "New"

26. Type the name of the VPN client, for example "**Client**" and put the ip address of the client, for example 202.129.97.101 255.255.255.255. You will see the following screen:

D-Link Firewall - Microsoft Internet Explorer		- 6
Col. New Parones 100s hep     Col. New Parones 100s hep     Address III https://192.168.0.95/theme1/index/login=1		-] 🖪 🤅
D-Link	Firewall Appliance	- <mark>2</mark> ) Rel
System Internal External	1	
Firewall		
Policy External_All Address Client	19/Netmask Modily 0.0.0.0/0.0.0.0 S 202.129.97.101/255.255.255 *	
Schedule New Users		
Virtual IP Port Forward URMAC Bindian		
VPN		
Apti-Virus		
Web Filter		
Log&Report		

- 27. Go to VPN menu and choose IPSec submenu
- 28. Choose Autokey IKE bookmark and click "New"
- 29. You will see the following screen:

		Firewall Appliance
System	Policy Autokey IKE	Manual Key Dial-up Monitor
Firewall		
VPN		New VPN Tunnel
IPSEC	Tunnel Name	
PPTP	Remote Gateway	0.0.0.0
RADIUS	P1 Proposal	Encryption: 🔽 DES 🔽 3DES
NIDS		Authentication: 🔽 MD5 🛛 🧮 SHA1
		Keylife: 28800 (seconds)
Anti-Virus	P2 Proposal	R Null R DES
Web Filter		HMAC-MDS HMAC-SHA1
L and Damast		DES-HMAC-MD5 R DES-HMAC-SHA1
Logakeport		V 3DES V 3DES-HMAC-MD5
		Enable replay detection
		Keylife: 200 (seconds) - Draw ID: 10 Subast V
	Authentication Kou	Keyite: Jauu (seconds) Proxy ID: [IP subnet
	(Pre-shared Key)	
	Incoming NAT	
	ОК	Cancel

29. Put in the Tunnel Name, for example "VPN\_Client"

In "**Remote Gateway**" field type the ip address of the client, for example 202.129.97.101. Type 0.0.0.0, if your XP/2000 IPSec client has a dynamically assigned IP address!

- 30. Choose the encryption and authentication algorithms you would like to you or leave it as default
- 31. Put the "Authentication Key", it can be any key, but it is better to use meaningless combination of digits and characters. Don't forget the key, you will use it later.
- 32. Check "Incoming NAT" and press OK

- 33. If your XP/2000 IPSec client has a dynamically assigned IP address, you need to skip steps 34 37!
- 34. You will get the following screen:

D-Link Firewall - Microsoft Int	ernet Explorer						_ <i>8</i> ×
File Edit View Favorites To	ools Help						27
😋 = 😳 - 💽 😰 🐔 🛛 Add	tress 🕘 https://192.168.0.1/t/	eme1/index?login=1					*
D-Link	_		Firewall Ap	opliance	L-500 - Oto	gout 💽 Wizard	Help
System	Policy	Autokey IKE	Manual Key	Dial-up Mor	litor		
Prevail VPN IPSEC PPTP L2TP RADIUS NIDS Anti-Virus Web Filter Log&Report	Tunnel Name VPN_Client New	Remote Gatsway 202.120.97.101	Lifetime(seconds) 300	Status Down	Timeout O	Modify 19	
Done	unt Manute [@]Dur	k Graunik - Mercarel				🔒 🔮 Internet	1.00 004
🚾 avan 🦉 🚯 🚳 🖉 pocus	P-Un	n reerial - Pacrosof				1	1:20 PT

- 35. Choose "Policy" submenu in VPN/IPSec menu
- 36. Press "New" and choose "D-Link" for source, "Client" for destination and "VPN\_Client" for VPN Tunnel name and press "OK":

Link Firewall - Microsoft Inter	rnet Explorer					
Edit View Favorites Tool	ls Help					
• 🗇 - 💌 🔊 🎧 🛛 Addre	HSS and https://192.168.0	0.1/theme1/index?login=1				
)-Link			Firewall Ap	opliance DFL-500	Ogout Swizard	<u>-</u> Он
System	Policy	Autokey IKE	Manual Key	Dial-up Monitor		
Firewall						
VPN	Order	Source	Destination	VPN Tunnel	Modify	
IPSEC	1	D-Link	Client	VPN_Client	1 19	
PPTP		-				
RADIUS	New					
IIDS						
oti-Virus						
Web Filter						
.og&Report						
		IPSEC Pass T	Through PPTP Pa	ss Through. Apply		
					🔒 🔮 Internet	
art 🥭 🚯 🏈 🖪 Docume	nt1 - Microsoft 🧧	D-Link Firewall - Micr			🧭 🗞 🖬	1:2

37. The DFL-500 Firewall configuration is finally ready.

## **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.

The configuration is very similar to the one with DI-804V, that's why you will see DI-804V in screenshot examples. You will have DFL-500 in your setup though.

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"



#### 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	
Description	
Add	
ОКС	ancel



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

ect Computer	?
Select which computer this Snap-in will manage When this console is saved the location will also be saved	Ē
Local computer     The computer this console is running on <u>Manage</u> domain policy for this computer's domain	
C Manage domain policy for another domain:	
C Another computer:	
< <u>B</u> ack 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: 🔄 Console Root 💌 💼
IP Security 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>About</u>
OK 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 l	orief description		Ē
Na <u>m</u> e: DI804V with XP			
Description:			
D1804V communicates with XP			×
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

IP Security Policy Wizard	<u>? ×</u>
Requests for Secure Communication Specify how this policy responds to requests f	for secure communication.
The default response rule responds to remote other rule applies. To communicate securely, I secure communication.	e computers that request security, when no the computer must respond to requests for
C Activate the default response rule.	
1	< <u>B</u> ack <u>N</u> ext > Cancel

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



#### 12. Select "Add"



Security Rule Wizard	<u>? ×</u>
Security Rule Wizard	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:  IP tunneling attributes Authentication methods Filter actions  To continue, click Next.
	< <u>₿</u> ack. [ <u>Next&gt;</u> ] Cancel

14. Input the IP Address into "**The tunnel endpoint specified by this IP address:**" (Eg. DFL-500 WAN IP Address), "**Next**"

Security Rule Wizard	? ×
Tunnel Endpoint The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.	Ţ
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 I his rule does not specify a tunnel C I has here and which its end size the security for the terms of terms of the terms of terms o	
202 . 129 . 97 . 105	
< <u>B</u> ack <u>N</u> ext > Ca	ancel

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

Security Rule Wizard			? ×
<b>Network Type</b> The security rule must be applied to a netwo	ork type.		Ē
Select the network type:			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

# 16. Select "**Use this string to protect the key exchange (preshared key)**" (Eg. DFL-500 preshared key) then click "**Next**"

Security Rule Wizard		?
Authentication Method To add multiple authentication m IP Security rule wizard.	ethods, edit the security rule after completing	the
Set the initial authentication meth	nod for this security rule:	
C Active Directory default (Kerb	eros V5 protocol)	
O Use a <u>c</u> ertificate from this cer	tification authority (CA):	
	Bg	owse
<ul> <li>Use this string to protect the l</li> </ul>	key exchange (preshared key):	
1234567		×

#### 17. Select "Add"



18. Enter a filter name (XP to DFL-500) then click "Add"

. . .

IP Filte	er List			<u> </u>
	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.	inets, IP
<u>N</u> ame:				
XP to D	)1804V			
Descript	tion:			<u>A</u> dd
Make a	a filter from XP to D1804V		<u>^</u>	<u>E</u> dit
			<b>v</b>	<u>R</u> emove
Filter <u>s</u> :			Γ ι	Jse Add <u>W</u> izard
Mirrore	ed Description	Protocol	Source Port	Destination
•				▶
			OK	Cancel

IP Filter Wizard		<u>?</u> ×		
Ĩ	Welcome to the IP Filter Wizard. This wizard helps you provide the source, destination, and			
	trainc-type information needed to niter in trainc. 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:				т	
A specific IP Address			·	1	
IP Address:	202	. 129	. 97	. 101	
Subnet <u>m</u> ask:	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. DFL-500 Private network)

Filter Wizard										? ×
IP Traffic Destination Specify the destination add	lress of th	e IF	<sup>o</sup> traffic.							Ð
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	>	Car	icel

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





24. Click "**Ok**"

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

#### 25. Now, select "XP to DFL-500" then click "Next"

Security Rule Wizard		<u>?</u> ×					
IP Filter List Select the IP filter list for the typ	e 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.							
<u>I</u> P filter lists:							
Name	Description	<u>A</u> dd					
All ICMP Traffic All IP Traffic	Matches all ICMP packets bet Matches all IP packets from t	<u>E</u> dit					
XP to DI804V	Makes a filter from XP to D180	<u>R</u> emove					
	< <u>B</u> ack <u>N</u> ext	> Cancel					

#### 26. Click "Add"

	710101		
Securit	y Rule Wizard		? ×
Filt	er Action Select the filter action for this secu	rity rule.	
	If no filter actions in the following lis one. Select Use Add Wizard to cre	st matches your needs, click Add to 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 Accepts unsecured communi 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 transfer. These requirements are specified in a list of security methods contained in the filter action.			
000	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>B</u> ack [ <u>Next&gt;</u> ] Cancel			

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

Filter Action Wizard	<u>? ×</u>
Filter Action Name Name this filter action and optionally give a brief description	169
Name:  3DES_MD5  Description:	
	×
< <u>₿</u> ack <u>N</u> ext >	Cancel

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

coloci nogotiato cocality		ITOAL	
Filter Action			<u>?</u> ×
Filter Action General Options Set the filter action behavior.			161
C P <u>e</u> rmit			
O Bjock			
Negotiate security:			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Com	municating with computers that do not support IPSec Communicating with computers that do not support IPSec may expose your network to security risks.
I	Do you want to allow communication with computers the do not support IPSec?
	Do not communicate with computers that do not support IPSec.
	S Fall back to unsecured communication.
	Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.
	< <u>B</u> ack <u>N</u> ext > Cancel

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

Security Method Wizard	? ×
IP Traffic Security Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard.	1
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.</li> <li>Medium (Authenticated Header) Data will be authentic and unmodified, but will not be encrypted.</li> <li>Custom</li> <li>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 security method.			
Data and address integrity without er Integrity algorithm:	ncryption (AH) :		
<ul> <li>Data integrity and encryption (ESP):</li> <li>Integrity algorithm:</li> <li>MD5</li> <li>Encryption algorithm:</li> <li>3DES</li> </ul>			
Session Key Settings: <u>G</u> enerate a new key every: 1000000 <u>K</u> bytes	Generate a new key every           3600         seconds		
	OK Cancel		

#### 33. Click "Next"

Security Method Wizard	<u>?</u> ×
IP Traffic Security Specify a security method for IP traffic. To add multipl filter action after completing the wizard.	le security methods edit the
This filter action requires at least one security method	for IP traffic.
<ul> <li>High (Encapsulated Secure Payload) Data will be encrypted, authenticated, and unmod</li> <li>Medium (Authenticated Header) Data will be authentic and unmodified, but will not</li> <li>Custom</li> <li>Settings</li> </ul>	ilfied. : be encrypted.
<u> </u>	ick <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		? ×
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)	Accepts unsecured communi	Remove
O Require Security	Accepts unsecured communi	
	< <u>B</u> ack <u>N</u> ext	t> Cancel

36. Select the following and check "Session key Perfect Forward Secrecy" then click "OK" 3DE5\_MD5 Properties





38. Click "Finish'



39. Click "Add"



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: IP tunneling attributes Authentication methods Filter actions
	To continue, click Next.
	< Back Cancel

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 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:			
Ihis rule does not specify a tunnel			
The tunnel endpoint is specified by this IP address:			
202 . 129 . 97 . 101			
< <u>B</u> ack <u>N</u> ext > C	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"

Security Rule Wizard			? ×
Network Type The security rule must be applied to a netwo	ork type.		Ī
Select the network type: All network <u>connections</u> Local area network (LAN) <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. DFL-500 preshared key) then click "Next"

rity Rule Wizard		
Authentication Method To add multiple authentication meth IP Security rule wizard.	ods, edit the security rule after comp	oleting the
Set the initial authentication method	for this security rule:	
C Active Directory default (Kerbero	s V5 protocol)	
C Use a <u>c</u> ertificate from this certific	ation authority (CA):	
		Browse
Use this string to protect the key	exchange (preshared key):	
1234567		Ă

#### 44. Click "Add"



45. Enter a filter name (DFL-500 to XP) then click on "Add"

Name:	An IP filter list is composed addresses and protocole	ed of multiple filters. In s can be combined into	this way, multiple subn one IP filter.	ets, IP
Description	x.			<u>A</u> dd
Make a fill	ter from DI804V to XP			Edit <u>R</u> emove
Mirrored	Description	Protocol	Source Port	Destination
•			ОК	▶ Cancel

IP Filter Wizard	?	<			
	Welcome to the IP Filter Wizard.				
E	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.				
M	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. DFL-500 Private network)

Filter Wizard								? ×
IP Traffic Source Specify the source address	of the IP	traffic.						Ē
Source address:								
A specific IP Subnet					•			
<u>I</u> P Address:	192	. 16	8.	0	•	0		
Subnet <u>m</u> ask:	255	. 25	5.	255	•	0		
				: <u>B</u> ack		<u>N</u> ext	>	Cancel

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

er Wizard						? ×
IP Traffic Destination Specify the destination add	ess of the	e IP traffic.				Ĩ
Destination address:						
A specific IP Address			ľ	•		
IP add <u>r</u> ess:	202	. 129	. 97	. 101		
Subnet mas <u>k</u> :	255	. 255	. 255	. 255	1	
			Z Back	Nev		Cancel
			1 Dark	<u>Tiex</u>		

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



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



51. Click on "Close"

IP Filter	List			<u>?</u> ×
	An IP filter list is compos addresses and protocol:	ed of multiple filters. In l s can be combined into	this way, multiple s one IP filter.	subnets, IP
<u>N</u> ame:				
D1804V 6	io XP			
<u>D</u> escriptio	on:			( <u>A</u> dd
Make a f	ilter from DI804V to XP		<b>A</b>	<u>E</u> dit
			-	<u>R</u> emove
Filter <u>s</u> :				Use Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY
•				▶
			OK	Cancel

#### 52. Select "DFL-500 to XP" then click "Next"

	? ×
t for the type of IP traffic to which this security rule	applies.
illowing list matches your needs, click Add to creat	e a new one.
Description	Add
Matches all ICMP packets bet Matches all IP packets from t	
Make a filter from DI804V to XP Makes a filter from XP to DI80	<u>R</u> emove
< <u>B</u> ack <u>N</u> ext	> Cancel
	st for the type of IP traffic to which this security rule allowing list matches your needs, click Add to creat Description Matches all ICMP packets bet Matches all IP packets from t Make a filter from DI804V to XP Makes a filter from XP to DI80

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

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 eate a filter action.	ocreate a new
Filter Actions:		Use Add <u>W</u> izard
Name	Description	Add
3DES_MD5     O Permit     O Request Security (Optional)     O Require Security	3DES_MD5 Permit unsecured IP packets t Accepts unsecured communi Accepts unsecured communi	<u>E</u> dit <u>R</u> emove
	C Back Moul	Canada

#### 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 DFL-500" then click on "Edit"

with DI804¥ Proper	ties		3
ules General			
Security rule	es for communicating with o	ther computers	
P Security rules:	Ether Ander	A dia anti- ation - 1	T
	Filter Action	Authentication	10
XP to DI804V	3DES_MD5	Preshared Key	20
	JUES_MUS	Preshared Key	20
•			Þ
A <u>d</u> d	Edit <u>R</u> emove	Use Add <u>W</u> i	zaro
		Close Car	nce

56. Select "XP to DFL-500" then click on "Edit"

t Rule Properties	<u> </u>
Authentication Methods Tur	nnel Setting Connection Type
The selected IP filter list affected by this rule.	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 DI804V
1	
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
40	Cancel Apply

#### 57. Click "Edit"

📑 IP Filte	r List			<u>? ×</u>
	An IP filter list is compose addresses and protocol	sed of multiple filters. In s can be combined into	this way, multiple su one IP filter.	bnets, IP
<u>N</u> ame:				
XP to D	1804V			
<u>D</u> escripti	ion:			<u>A</u> dd
Makesa	a filter from XP to D1804V		<u> </u>	<u>E</u> dit
			<b>T</b>	<u>R</u> emove
Filter <u>s</u> :			V	Use Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY
•				
			ОК	Cancel

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

Addressing       Protocol       Description         Source address:
Source address:         A specific IP Address:         IP Address:         202       129         97       101         Subnet mask:       255         Destination address:         A specific IP Subnet         IP address:       192         192       168       0
A specific IP Address         IP Address:         202       129       97       101         Subnet mask:       255       255       255         Destination address:       Image: Compare the second s
IP Address:       202 . 129 . 97 . 101         Subnet mask:       255 . 255 . 255 . 255         Destination address:
Subnet mask:         255         255         255         255           Destination address:         A specific IP Subnet         Image: s
Destination address: A specific IP Subnet IP add <u>r</u> ess: 192 . 168 . 0 . 0
IP address: 192 . 168 . 0 . 0
Subnet mask: 255 . 255 . 255 . 0
Mirrored. Also match packets with the exact opposite source and destination addresses.
OK Cancel

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

#### 59. Click "Close"

📑 IP Filter	List			? ×
	An IP filter list is compose addresses and protocol	sed of multiple filters. In t s can be combined into	this way, multiple sub one IP filter.	nets, IP
Name:				
XP to DI	804V			
, <u>D</u> escriptio	on:			<u>A</u> dd
Makes a	filter from XP to D1804V		<u>^</u>	<u>E</u> dit
			<b>T</b>	<u>R</u> emove
Filter <u>s</u> :			🔽 l	lse Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY
1				F
			OK	Cancel

### 60. Select "DFL-500 to XP" then click on "Edit"

Edit Rule Properties	<u>? ×</u>
Authentication Methods Tur IP Filter List	nnel Setting Connection Type   Filter Action
The selected IP filter list	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
O XP to DI804∨	Makes a filter from XP to D1804V
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			<u>? ×</u>
	An IP filter list is compose addresses and protocol	sed of multiple filters. In s 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 DI804V to XP		_	<u>E</u> dit
			-	<u>R</u> emove
Filter <u>s</u> :			R	Use Add Wizard
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	. 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 pac destination addresses.	kets with I	the exact (	opposite so	ource and	
			ОК	Ca	incel

\* 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>
Talle1	An IP filter list is compo- addresses and protocol	sed of multiple filters. In Is can be combined into	this way, multiple su one IP filter.	ubnets, IP
<u>N</u> ame:				
D1804V	to XP			
<u>D</u> escripti	ion:			<u>A</u> dd
Make a	filter from DI804V to XP		<u></u>	Edit
			<b>v</b>	<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 IP Filter List	Tunnel Setting Connection Type Filter Action
The selected IP filte	er list specifies which network traffic will be
IP Filter <u>L</u> ists:	
	Description
O AILICMP Traffic	Matches all ICMP packets betw
O AILIP Trathc	Matches all IP packets from this
	Make a filter from DI804V to XP
A <u>d</u> d	<u>R</u> emove
	Close Cancel Apply

65. <b>(</b>	Click "Close"			
	XP with DI804¥ Propertie	s		? ×
	Rules General			
	Security rules 1	for communicating with ot	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
	L <dynamic></dynamic>	Default Response	Kerberos	Nc
	▲ [ A <u>d</u> dEdi	t <u>R</u> emove	Use Add <u>W</u> iz	> ard
		(	Close Car	rcel

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

Console1 - [Console Root\IP Sec	curity Policies on Local Computer]	X
The Action View Favorites	Window Help	_161 ×1
← → 🗈 🖬 🗙 🗗 🖳 🖆	2 1 1 2 3	
Console Root	Name A Description Policy Assigned	
IP Security Policies on Local Comp	P 🛍 Client (Respond Only) Communicate normally (uns No	
	DIBO4V with XP No	
	Secure Server (Requir For all IP traffic, always req No Assign	
	Server (Request Secu For all IP traffic, always req No All Tasks	
	Calata	
	Rename	
	Broowline	
	Propercies	
	Help	
< >	1	
Assign this policy, attempt to make it activ	ve l	

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	<u>- 🗆 ×</u>
C:\Documents and Settings\Serge>ping 192.168.0.101 -t	<b></b>
Pinging 192.168.0.101 with 32 bytes of data:	
Negotiating IP Security. Negotiating IP Security. Negotiating IP Security. Negotiating IP Security. Negotiating IP Security. Negotiating IP Security. Negotiating IP Security.	
Reply from 192.168.0.101: bytes=32 time=4ms TIL=127 Reply from 192.168.0.101: bytes=32 time=4ms TIL=127 Reply from 192.168.0.101: bytes=32 time=4ms TIL=127 Reply from 192.168.0.101: bytes=32 time=3ms TIL=127 Reply from 192.168.0.101: bytes=32 time=4ms TIL=127 Reply from 192.168.0.101: bytes=32 time=4ms TIL=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	