## Configuring VPN connection using SSH Sentinel VPN Client and D-Link DI -804V VPN Router

## 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:



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 202.129.97.105 255.255.255.0 for our WAN interface and the default gateway of 202.129.97.1 255.255.255.0. 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:



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:

Service Advances for all these actions for a	Rings - Photosoff Educated Explorer		ALC:
Ne Edit Wow Revented Tindo Halp			
- O Z Antone 🐑 LENNER	1.00.5 Livin japantings have		- D -
D. Fault	VPN Router OI	8047	
D'Link	MAR MAR MANAGE STATES	ana -	
Main manu			
ISP SETTINGS	- Static IP Settings		
1. Solect the IS	Settings List below		
State P Saling			
IP assigned I	oy year 189: 282 128 07 , 105		
US BETTINGS	billion mask: 295 256 295 0		
NUMER			
STTTINGS DSP-Gatum	ay Addresse: [282 ] [129 ] [27 ] [1		
2. Elick Neut to	and your request to the Cable/aDSI. Broadba	nd	
Bautor.	CONTRACT DATA		
	Contraction and Contraction		
Capacity (C. 2040		•	
0		1104 5724	🔮 internet
Start e Setap Visced - 197 HL.	nhes Mai - delovenik . 🛛 💌 Sile VMs06-0041.4x	A Disk.	

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 Would - Tel	ne bettings - Phonoidi Inform	et Englisere			a Mix
	Andreas (100 Mage 7152 A00.5)	Det_VPMMs			- 0 -
D-Link	arthullos - H2RA	VPN Route MNG SPMMER	r DI-BOAY		
Main reaso	VPN BETTUNGR				
	Consecution Name				
DEVICE IF	cantena ann				
	Road to Anna Anna	sand there are a second p	role: the converse &		
SETTINGS					
STORM.					
NOTION OF		- DACK NO	CHT IN		
CHINE C 100100					
1.1.1.		14-15-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	111.		-
Statt Status	Wound - Time	tal - chelonetik	000 doc 0000	1 9 Wite	- 58 1404

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 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 leave Remote Gateway field blank. Otherwise, you must specify the static IP address of your client. If your client gets the IP dynamically, than you should also leave this field blank.

Let's look at what we have got:

Noting Without - 1975 No	etangs - Microsoft Tableviel In	a pilor re	1813
-0-364	100 Migori 198 1.00 S. Dw	e, VN Julter	- 0 -
D-Link	ettilition tettilit	VPN Router 01-8041 NNS NEWYICE NEET MAR	
DEVICE IF	Canvection Name Lecal IPSEC Monthier Romote IPSEC Monthier	MPN_Cloud	
NODEN	Hermote IP Hetwork Researce IP Hermote Researce Gateway IP Hermote Satescoy IP	ETE 1/23 (97 0) ESE 1025 (925 0) FRE 1255 (107 HEI WANNET HER REFET T	
	Senare Resociation Partiect Forward Secure Encryption Protocol PolyShared Key	R Men Wade C Aggetone C Mennel R Exotive C Disolet Soci5 M Period 2	
	Key Life RE Life Time	900 Seconds 2800 Seconds	
	Inable States	Load DBAC 20 - Pressin PERC 22. Surveyord	
europhi () 2000			
1000			Storet .
Start C Tetap Vice	wed - WHER 💕 Pales (Mai	- chelonenik . 🗮 750++99+06-0091.doz	- 🗰 - 🛤 2.00 Mit

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.

websp Would - White becauge - Microsoft In	dever at heplaners	-1813
The Edit Move Persentage Tools (19/18		
🕽 - 🖸 - 🛃 🗶 Address 🌒 Maps/1997	1005.046.996.940.800	- 🔁 😁
D-Link	VPN Router 01-804V	
Hein menu VPN SETTINGS		
THE SETTINGS	a DOM Close	
Local IPSEC No	ether	
Remote IPSEC In	antiller	
Benote IP Bene Benote IP Bene	est 212 121 117 10 est 295 255 256 0	
Report Colervy	P 22 12 97 10	
Botwork Intertee	VIVANETHERNET	
Secure Associate	an 🦉 Main Mado C Aggressie C Mariaal Secure 🤗 Enabled C Disabled	
Encryption Prote	101 1025 -	
Forskered Koy Kay Life	2800 Secondo	
HE LTP Time	Second Back	
D UDA	See Contract Contract Contract	
C. Status	100 See	
	Contract Contraction	-
(present document RE, Same astantic)	1.844 C.S.	internet
Statt States Vised - White I	ahas (Mail-stationestic.)	

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

You will see the Connection at the bottom on the screen. This is 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. Now your VPN Router is ready to get the VPN Client request.

## II. Configuring SSH Sentinel Client<sup>1</sup>

Please install the SSH Sentinel to your system. Please you the official SSH Sentinel Manual if you have problems while installing it. If you installed the SSH Sentinel client successfully and restarted your computer, the client would start automatically, the SSH Sentinel taskbar sign would appear in your taskbar in the right bottom corner of your Desktop. Move your mouse to the SSH Sentinel sign at the taskbar and press the right mouse button. Choose Run Policy Editor and click on it.

You will get into the following menu:

SSH Sentinel Policy Editor	<u>? ×</u>
Security Policy   Key Management	
Policy : 🔝 Defeut	- 🖬 🖼 🔛
Profileso Inter     Barrentons     And Proceedings     Barrentons     Alow all trains	and examines and
Dencription SSH Sentinettni/Version 1.3.2 build 21 Windows XP Version 5.1 (Build 2000.)	eriec Damenton
OK	Cancel Early

<sup>&</sup>lt;sup>1</sup> The SSH Sentinel official manual can be found at www.ssh.com. The material, which is presented in this chapter is not an official SSH manual. D-Link does NOT guarantee that the configuration changes you make to SSH Sentinel according to this manual are correct and has no responsibilities for any misconfiguration or misuse of SSH products.

Choose Key Management bookmark:

incurity Policy Key I	lansgement		
Co- Co Trusted Po	ALC: NO.		
Add.	Historia Historia Historia Historia Historia Historia Historia Martina	4	
	lienare 🛔 1	coster]	<u>y</u> ea.

Go to My Keys and press "Add":



Choose "Create Pre-Shared Key" and click "Next":



Give a name to the key and put exactly the same key you used in "Authentication Key" field of DLink DI-804V VPN Router, press "Finish". The key is now created and you can go back to the "Security Policy" bookmark. Choose "VPN Connections" and press "Add":

SSH Sentinel Policy Editor	<u>?</u> ×
Security Policy   Key Management	
Policy : 🔛 Default	• • • • •
Po-PSec File     VPU Connections     VPU Connections     VSu Connections     Secured Connections     Secured Networks     Secured Networks     Secured Networks     Secured Networks     Volume Secure Secure     Alow al traffic	Arment routine armen
Add. Berrove Br Description Add anule.	ornes <u>Biographies</u>
DK _	Cancel

On the "Gateway IP address" field press "IP" and put the external IP address of your VPN Router, for example 202.129.97.105:

1	Galemay IP address:	202 . 129 . 97 . 105	वा
*3	Remote network:	ay 💽	1
	Authentication key	🚧 seige certificate	٠
		🗐 Use legacy proposal	
Diago	ostics. Doperties	OK Cano	e

Press "..." button in "Remote Network" field. Press "New" and create a network with your internal network address, for example 192.168.0.0 255.255.255.0:

Nane	IP add	dreee	Subnet	mask	
any D-Link	192.1	660.0	255.25	5 255.0	
		Ne	w ]	Herro	ve
letwork manuel	D-Link.	Ne	<u> </u>	Berro	~
ietwork manie Pladdress:	0 Link 192	<u>N</u> e	w	<u>H</u> emo	

Press "OK" and select "key" in "Authentication Key" field:



Check on "Use legacy proposal" and press "OK". The VPN Connection is now created. Choose the VPN connection, we have just created and press "Properties". You will get the following menu:

le Prop	erties		?
ieneral	Advanced		
Renola	endpoint		
	Security gateway:	<b>OK</b> . 129 .	97 . 105 JP
	Renote network	DLink	*
PSec /	IKE proposal		
-	Authentication keys	- key	-
* (	Proposal template:	lagacy	-
			Setings.
T Acc	pire virtual IP address	-	- participation of the second
₽ <b>8</b>	A urtual IP address is the internal network.	an address from	Settings
E EM	ended authentication This VPN gatemay ma XAwth, RADIUS or Ch	g require IKE IAP authentication.	Setings
Desci	liplian	ļ	Diarge
_		OK	Cancel

Click "Settings" under the "Proposal template" field, you will get this:

Encyption algorithm	3DES	
Integrity function:	MD5	-
(KE mode	main mode	*
(KE group:	MODP 1024 ( group 2	*
PSep process		
Encyption algorithm	3DES	-
Integrity function:	HMAC-MD5	-
IPSec mode:	band	2
PFS group:	MODP 1024 ( group 2 )	

Choose the IKE and IPSec modes you would like to use and click "OK". Choose "Advanced" bookmark and press "Settings":

Rule Prop	orties	<u>? X</u>
General	Advanced	
Securit	y association lifetimes	
<b>3</b>	Set the Batimes of IPSec and IKE security associations.	Settings.
Audito	pton	
1	R Audithia nale	
Advanc	ced options	
5	<ul> <li>□ Apply IP compression</li> <li>□ Biscover path gissioun iterater u</li> <li>□ Ernable <u>Natives</u> Address Translatio</li> <li>□ Open on statisticp</li> </ul>	vi (FMTU) an Trixennal (NAT-T)
		Cancel

Choose lifetime, so it would correspond to the lifetime specified in DI-804V configuration. The defaults for DI-804V are 28800 seconds for Phase 1 (IKE) and 3600 seconds for Phase 2 (IPSec):



Go back to the main "Security Policy" window and press "Apply" and "OK" again. Don't forget to "Apply" every time you change your VPN connection properties or security policy. The basic configuration of SSH Sentinel VPN client is now over. You can check you Pre-IPSec and Post-IPSec Filters to be sure that all the ports needed for your work are opened and the rest of the ports are closed. SSH Sentinel VPN client is actually working as a firewall on the client side. Now you are ready to connect your client to the office network.

## **III. Connecting SSH Sentinel VPN Client to the Office network**

Make sure your client has a connection to the Internet. In SSH Sentinel Policy Editor choose the VPN connection you have created and press "Diagnostics".

tolicy : 🔛 Defeut	- 🖬 🖻 📓
Pre-IPSeo Filter     WPN Connections     WPN Connections     Add     Add     Socured Connections     Socured Networks     Socured Networks     Add     Add	anna na martaine casas
Add. <u>Bernove Pr</u> Deutsiption (no description)	peter. Disperie.

You will see the client trying to connect to D Link DI-804V VPN Router. If the diagnostics is successful, you will see the following message:



Click on "Details" to check which authentication and encryption modes are chosen for IKE and IPSec:



Now you can connect your client to your office network. Click right mouse button on SSH Sentinel taskbar sign and choose "Select VPN". Select the connection you have created, for example 202.129.97.105 (D-Link) and click on it, you will see the following window:



When the connection is done, you will see the follow message:



The message disappears in a few seconds, that means that you VPN connection is now established (Not Responding is normal here, since Sentinel closes the window itself). Now you can open Command Prompt from Start/Programs/Accessories menu in Windows. Check if you have a connection to your office network by "pinging" of the office computers:



If you get the replies from your office computer that means that the VPN connection to your office network works and you can start using the office network as you are connected directly to it.

Congratulations! You have successfully created the VPN Connection from SSH Sentinel VPN Client to your Office network through D-Link DI-804V VPN Router!