Configuring SSH Sentinel VPN client and D-Link DFL-500 Firewall

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"

-Link			Firewall Appliance	0
System Statue Update Notwork Correg Firewall VPN NIDS Anti-Virus Web Filter Log&Report	Status	Firmware Version: Antiview Definitions Version: Attack Definitions Version: Serial Number: System Settings: System:	DLINK-500 2.27,build042,020808 3.5(07/26/2082 14:01) 1.2(07/10/2082 15:40) FGT-502801026300 Develoed Develoed Usload Restart Shutclown	

🐮 Skart 🧔 🕹 🌮 题 Document) - Microsoft 💽 D-Link Finansii - Micro-

- 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 192.1680.1
- 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
- 16. 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 router with the ip address supplied by your internet prover.

19. Go back to System/Network menu

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

0.24	dokess 💽 https://140.166.0.1864	melijnde:/login=i				
)-Link			Firewall Appli	ance DFL-500	OLegost Oldizard	0
Status	Interface	Enuling	DHCP			
Update Network	Name	19	Netmesk	Access	Medify	
Config	internal	192.168.0.1 202.129.97.105	255.255.255.0	HTTPS,PING PING	8	-
irewall					1200	
'PN						
IDS						
nti-Virus						
Veb Filter						
og&Report						
						-14
					A blue	
1	I Day					A 10

21. Go to Firewall menu and choose Addresses

- 22. In the Internal submenu press "New"
- 23. 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
- 24. Go to External submenu and press "New"
- 25. Type the name of the VPN client, for example "Client" and put the ip address of the client, for example 202.129.97.101 255.255.255.0. If you want to allow any VPN client to connect leave all 0s for the ip address
- 26. Go to VPN menu and choose IPSec submenu
- 27. Choose Autokey IKE bookmark and click "New"
- 28. You will see the following screen:

D-Link DFL-500 Upper Interest Inter	an kaz taku Havanasi Toox Helip) - 🕐 💽 🛣 Address 🔞 hitu	or (/192.165.0.1)themes jinder Program		
System Partice Autokey IKE Masual Key Datus Manites Firewall VPN Immed Name Immed Name PERC Form Formed Rame 0.0.0.0 P1 Propesal Encryption: DES F 3DES Anti-Virue P1 Propesal Encryption: F DES Web Filter P2 Propesal F MAI F DES Log&Report 2 DES HWAC-HDS F HMAC-HAI F Enable perfect forward secret/(PFS). Replice detection F Enable perfect forward secret/(PFS). Replice detection Miter State OK Cancel	D-Link		Firewall Appliance	78 () (61)
VPN New VEW Tunnel PREC Famel Name Propesal Brorybon: NIDS Axthentication: Anti-Virue P Propesal Web Filter P Not Log&Report P Remote Gateway Participation: P Not P Propesal P Not P Propesal P Not P Propesal P Not P Sectors P HMA P Sectors P Sectors	System P.	Autokey IKE	Masual Key Dial-up Monitor	
PSEC Famel Name Parter Remote Galeway NIDS P1 Propesal Anti-Virue P2 Propesal Web Filter P2 Propesal Log&Report P1 Propesal Web Filter P2 Propesal P2 Propesal P MAC-MDS P MAC-MDS P MAC-SHA1 P DES-HNAC-MDS P DES-HNAC-SHA1 P DES-HNAC-MDS P DES-HNAC-MDS P SDES-HNAC-SHA1 P DES-HNAC-SHA1 P mable replay detection P Enable perfect forward secretry(PF6). Rewrife: 300 Methedication Key (Fre-shared Key) Francel OK Cancel	VPN		New VPN Tunnel	
Authendication: V MOS V SHAI Keylfe: [28800] Web Filter Log&Report Anti-Virue Web Filter Log&Report Authendication: V MOS V SHAI Keylfe: [28800] V MAL-NDS V MMAC-SHAI V DESHMAC-MDS V DESHMAC-SHAI V DESHMAC-MDS V DESHMAC-SHAI V DESHMAC-MDS V DESHMAC-SHAI V DESHMAC-MDS V DESHMAC-SHAI V DESHMAC-MDS V DESHMAC	IPSEC PETP L2TP RADIUS	Tannel Name Remote Gateway P1 Propasal	0.0.0.0 Encryption: IP DES IP SDES	
Web Filter FMAC-MDS FMAC-MDS Log&Report FMAC-MDS FMAC-MDS State State State Patter State State	NIDS	92 Proposal	Authentication P MD5 P SHA1 Keylife: 208000 (seconds)	
Cancel Concel Concel Concel Concel Concel	Web Filter Log&Report	F2 Fightin	KAII KOES F HVAC-NDS F HVAC-SHA1 F DESHMAC-MDS F DESHMAC-MDS F DESHMAC-SHA1 F DES	
Astheaticotion Key (Fre-shared Key) Incomig NAT			Finable replay detection Finable portext forward secrecy(PF6). Keylfe: 300 (seconds) Proxy ID: IP Subret	
OK		Asthentication Key (Fre-shared Key) Incoming NAT		
		OK	Cancel	

- 29. Put in the Tunnel Name, for example "VPN_Client"
- 30. In "Remote Gateway" field type the ip address of the client, for example 202.129.97.101 or leave it all zeros, if you want to allow any client to connect
- 31. Choose the encryption and authentication algorithms you would like to you or leave it as default
- 32. 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.
- 33. Check "Incoming NAT" and press OK
- 34. You will get the following screen:

D-Link						
D-Link	enep https://190.160.0.1Mternelljir	ndeo/Rogin=t				-
Dunk						
			Firewall Ap	opliance	Legost	Wizard Ulicip
9 92 92 P.				18	30	
System	Policy	utokey IKE	Menual Key	Dial-up Mentter		
Firewall	-					
VPN	Tunnel Name Rema MRN Client 202	te Geteway Lif	ann	Status	Timeout 15	odify 197
PPTP						
RADIUS	New					
NIDS						
Anti-Virus						
Web Filter						
Log&Report						
						1.5
Dane	a di tana in					Internet
25 Choose "Del	Mcrosoft	in in VDN	/IDCoo m			S 1:26 PM
26 Dragg "Now"	ley subment		for sour		"for dection	ation and
50. Press new	and choose	D-LIIIK	TOF SOUR		, for desum	ation and
VPIN_CIIER		unner na	me and p	ress OK	:	ule xi
File Edit View Flavosities Tools	нф					
		where Merceleural				
Address Address	https://192.168.0.48bere.1jr	Marringo-L				-
D-Link	😰 https://190.168.0.1/theresile	Managare -	Firmual Ar	DFL-	500 Olegent	ar Annare Oneige
D-Link	💼 https://190.160.0.18herestik		Firewall Ap	opliance DFL-	500 - O Legent	Niceri Olicip
D-Link	C https://190.100.0.1kherestin	nan ny	Firewall Ap	opliance DFL-	500 - Olagorat	Witzerd Officip
D-Link System	Policy	atokay IKE	Firewall Ap	Opliance OFL-	500 OLegovit	Wizard Officip
D-Link System Firewall	Policy Conter Sour	atokay IKE	Firewall Ap	Diance DFL-	500 - O Legovi - C	altzeri Olitiya
D-Link System Firewall VPN IPSEC	Policy Conder Source	atokay IKE	Firewall Ap	Disl-up Manitor VPN Tussed VPN_Ciert	500 Otsour	atzard Officip
System Firewall VPN IPSEC Perp L2TP	Policy Code Code	ntohay ISE nos Dr	Firewall Ay Massail Ray Initiation Client	OPL-I Clai-up Manifer VPN Tussel VPN_Clark	SDD Otsport	atzer Officip
System Firowall VEN IPSEC AZTP RADIUS	Policy Could be a series of the series of th	ntokay IKE nce Dr	Firewall Ay Messael Key estimation Client	DFL-I Dial-up Manifer VPN Tunnal VPN_Clime	SDO OLegori O Medify R S	ntzeri 🖓 ikip
Addees D-Link System Firowall VFN IPSC Perip L2TP RADUS NIDS Addees	Policy Content of the second s	ntokey IKE	Firewall Ay Manual Key atlantion Client	DFL-I Dial-up Manitar VPN Tunnal VPN_Client	SOO OLegent O	ntzeri Olinip
Addees D-Link System Firewall VEN IPSEC PETP L2TP MADUS NIDS Anti-Virus Web Ellier	Policy Conternation	ntokay IKE nce Di	Firewall Ay Messed Key attinution Client	DFL-i Diance Dian-up Manifer VPN-Tunnel VPN_Ciert	SOO OLegent Medify T	ntzeri Olinip
D-Link System Firewall VPN IPSEC Petr RADIUS NIDS Anti-Virus Web Filter LooßReport	Policy Conternation	atakay is.E na Du	Firewall Ag	Deliance Dal-us Manitor VPN_Client	SOO Creport	nitzeri Okolp
D-Link System Firewall VPN IPSEC Petr RADIUS NIDS Anti-Virus Web Filter Log&Report	Policy A Order Source 1 D-la Now	atokay is:E ns Di nk	Firewall Ay	Deplicance Dial-up Manifer VPN, Tunned VPN_Cisere	SOO Creport	attard O follow
Addex D-Link System Firewall VEN IPSEC PETP RADIUS NIDS Anti-Virus Web Filter Log&Report	Policy A Order Score 1 D-42 Nox	atokey isz na Di	Firewall Ay Manual Key Interaction Client	OFL-I Clai-up Menthe VPN Tuesed VPN_Client	SOO Creport	
Addex D-Link System Firewall VPN IPSEC revtP L2TP RADUS NIDS Anti-Virus Web Filter Log&Report	Policy A Corder Soul I D-42 Now	atobey ISE na Di	Firewall As Messel Key Interaction Client	OPL-I Dal-up Menter VPN Tussed VPN_Cierc	SOO OLegont	atterd O Rep
Addex D-Link System Firewall VPN IPSEC PerfP ADDUS NIDS Anti-Virus Web Filter Log&Report	Policy A Corder Sout I D-42 Now	atobay ISE na Do	Firewall As Messel Key estimation Client	VPN_Ciert	SOO O Legout	Interd O Help
Addex D-Link System Firewall VPN IPSEC Perte C2TP RADUS NIDS Anti-Virus Web Filter Log&Report	Policy A Corder South I D-iz Now	ntokey IKE ree Dr rk	Firewall As Messal Key etilection Client	VPN_Clert	SOO OLegont	ntzeri Olitop
System Firowall VEN IPSEC PETP L2TP RADIUS NIDS Anti-Virus Web Filter Log&Report	Policy A Order Sour	ntokay IKE Di	Firewall As Messal Key atlantion Client	VPN, Tunnel VPN, Cliert	500 € Legent Meetify T S7	ntzeri Olimija
D-Link System Firewall VEN IPSEC PETP ADDUS NIDS Anti-Virus Web Filter Log&Report	Policy A	ntokey IKE Do	Firewall As Messed Key Interation Client	Depliance DFL-4	SOO Cuspont	
D-Link System Firewall VFN IPSEC PPTP RADIUS NIDS Anti-Virus Web Filter Log&Report	Policy A	otokoy IKE Do ne Do nk	Firewall As Messed Key Interation Client	Depliance DFL-4	SOO Cuspont	
D-Link System Firewall VFN IPSEC PETP RADIUS NIDS Anti-Virus Web Filter Log&Report	Policy A	otobey ISE res Dr rk:	Firewall Ag	Sophiance OFL-I	SOO Corport	

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

II. Configuring SSH Sentinel Client

- 1. After you installed the SSH Sentinel client and restarted your computer, the client will start automatically, the SSH Sentinel taskbar sign will appear
- 2. Move your mouse to the SSH Sentinel sign at the taskbar and press the right mouse button
- 3. You will see the following menu:



3. Choose Run Policy Editor and click on it

Security Po	licy Key	Managemen	t	
Policy :	💼 Defau	lt	•	🗉 🛅 💆
	Pre-IPSec VPN Conn Secured C Secured N Default Re Post-IPSec Allow all tra	Filter ections connections letworks esponse a Filter affic	<u>.</u>]	RULE EVALUATION DROSE 🕥
Add. Descrip SSH Se Window	tion ntinel(tm) \ s XP Vers	<u>Remove</u> Version 1.3.2 ion 5.1 (Build	Eroperties (build 2) (2600:)	Diagnostics

5. Choose Key Management bookmark:

SSH Sentinel Polic	ty Editor		?
Security Policy Key	Management		
Trusted Pc Trusted Pc Trusted Cc P Remot Directory S My Keys Second	vicy Servers artificates ation Authorities e Hosts iervices ey rge certificate id reshared key	5	
Add Description You can share a s under trusted polic	<u>H</u> emove ecurity policy is: y servers.	Eroperties	⊻iew ity listed
	ОК	Cancel	Apply
	17		1 122
Go to My	Keys an	d press "A	\dd´´:
SSH Sentinel Polic	cy Editor		?
Security Policy Key	Management		
Trusted Po Trusted Ce Certific Remot Directory S My Keys Add	slicy Servers ertificates :ation Authoritie: e Hosts iervices ey rge certificate Id	5	
Add	<u>Bemove</u>	Eroperties	⊻iew

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



- 8. Give a name to the key and put exactly the same key you used in "Authentication Key" field of D-Link DFL-500 Firewall, press "Finish"
- 9. The key is now created and you can go back to the "Security Policy" bookmark
- 10. Choose "VPN Connections" and press "Add":

SSH Sentinel Policy Editor	?
Security Policy Key Management	
Policy : E Default	- 🖬 🐚 👲
Pre-IPSec Filter VPN Connections Add. Secured Connections Secured Networks Oefault Response Post-IPSec Filter Milow all traffic	RULE EVALUATION DROER
Add <u>Bernove</u> <u>Bropert</u> Description Add a rule.	ies <u>Diagnostics</u>
OK C.	ancel Apply

11. On the "Gateway IP address" field press "IP" and put the external ip address of your firewall, for example 202.129.97.105

Add VPN Conne	ection	? ×
Gatev	vay IP address: 202 . 129 . 97 . 1	105 JP
Remo	ote network: any	▼
Authe	ntication key: 🛛 🐖 serge certificate	
	🔲 Use legacy proposal	
Diagnostics	Properties OK Ca	ancel
12. Press "	" button in "Remote Net	work" field
13. Press "	New" and create a network	with your internal network address, for
exampl	e 192.168.0.0 255.255.255	.0:
Network Editor		? ×
Give	enetworks and subnetworks custom names. Jater use the names when creating rules	You
	iako	
News		
any	0.0.0.0 0.0.0.0	
D-Link	192.168.0.0 255.255.255.0	
	<u>N</u> ew <u>R</u> emo	ve
Mahurahaan	D-Link	
Network nam		
IP address:	192 . 168 . U . U	
Subnet mask	255 . 255 . 255 . 0	
-3		
	OK Car	ncel
14. Press "	OK" and select "key" in "/	Authentication Key" field:
Add VPN Conne	ection	? ×
. Calu		05 10
Hemo	ite network: JD-Link	
Authe	ntication key: Key	
	I⊻ Use legacy proposal	
Diagnostics	Properties OK Ca	ancel
	nan yan kes	

- 15. Check on "Use legacy proposal" and press "OK"
- 16. The VPN Connection is now created
- 17. Choose the VPN connection, we have just created and press "Properties"

18. You will get the following menu:

ule Prop	erties		2
General	Advanced		
Remote	e endpoint		
	Security gateway:	202 . 129 .	97 . 105 IP
Simu	Remote network:	D-Link	▼
IPSec /	/IKE proposal		
`	Authentication key:	🐖 key	•
×	Proposal template:	legacy	-
			Settings
C Ac	quire virtual IP address		
- P	A virtual IP address is the internal network.	an address from	Settings
□ Ext	ended authentication		
	The VPN gateway ma XAuth, RADIUS or CH	y require IKE AP authentication.	Settings
Desc	ription		
			<u>C</u> hange
		ОК	Cancel

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

 Proposal Parameters

enerypaon algonam.	JUES	
Integrity function:	MD5	•
IKE mode:	main mode	-
IKE group:	MODP 1024 (group 2)	•
^o Sec proposal		
Encryption algorithm:	3DES	-
Integrity function:	HMAC-MD5	-
IPSec mode:	tunnel	-
PFS group:	MODP 1024 (group 2)	•

20. Choose the IKE and IPSec modes you would like to use and click "OK"21. Choose "Advanced" bookmark and press "Settings":



22. Choose lifetime, so it would correspond to the lifetime specified in DFL-500 configuration. The defaults for DFL-500 are 28800 seconds for Phase 1 (IKE) and 300 seconds for Phase 2 (IPSec):

	1.02	5500	iat	ion	Life	etin	nes						
0>	Tł	he si	ettin	gs a	ffec	st th	is co	onne	ectic	on ru	le on	ly.	
KE s	ecu	rity a	asso	ciat	ion	_							
Life	time	in n	ninul	tes:									
-			— J							-	Г	480 r	nin
i					l						1		2020
Life	time	in n	nega	abyte	es:						_		
1	10	a.	51	102	$\hat{\mathbf{r}}_{i}$	×.	87	16	a.			0 1	ИB
PSe	c se	curil	tv as	soc	iatio	on –							
PSe Life	c se time	curil	ty as	soc	iatio	on-							
PSe Life	c se time	curil in n	ty as ninul	soc tes:	iatio	on-					_	5	nin
PSe Life	c se time	curil in n	ty as ninul	soc tes:	iatic ,	on ,	1	1	1			5 r	nin
PSe Life '}	c se time ,	icuril in n	ty as ninul ,	soc tes: ,	iatio , es:	on-	1	1	1		F	5 1	nin
PSe Life 1	c se time time	in n	ty as ninul , nega	soc tes: - abyte	iatic , es:	on	,	•	ı			5 r 400 ł	nin VIB
PSe Life Life	c se time , time	in n in n	ty as ninul nega	soc tes: abyte	iatio • es:	on-	•	1	•			5 r 400 t	min v1B
PSe Life 1/- Life	c se time time	in n in n in n	ty as ninul nega	soc tes: abyte	iatio • •	on ,	,	1	•		Г Г	5 r 400 t	nin VIB

- 23. 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
- 24. The basic configuration of SSH Sentinel VPN client is now over
- 25. 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
- 26. Now you are ready to connect your client to the office network

III. Connecting SSH Sentinel VPN Client to the Office network

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



- 3. You will see the client trying to connect to D-Link DFL-500 Firewall
- 4. If the diagnostics is successful, you will see the following message:



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

parame	ers, click Details.		lection
		Detai	ls Close
	Connection	Properties	
Remote: Vendor ID:	202.129.97.105		
Virtual IP	Not assigned		
a service	IKE SA	A	- Second
Auth.:	pre-shared key	Mode:	main
Encryption:	3des-cbc (168 bits)	Group:	MODP 1024
Hash:	md5	Lifetime:	0MB/14400s
NAT-T:	disabled		
	IPSec	SA	
Protocol:	ESP	Mode:	tunnel
Encryption:	3des (168 bits)	PFS group:	MODP 1024
	have a staff OC	l ifatima:	400MB/3600a

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

VPN Connection Status	×			
Opening the VPN connection to 202.129.97.105 (D-Link)				
	Cancel			
9. When the connection is done, y	ou will see the follow message:			
VPN Connection Status (Not Responding)	×			
The VPN connection established succesfully.				
	Close			

10. 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).

- 11. Now you can open Command Prompt from Start/Programs/Accessories menu in Windows
- 12. Check if you have a connection to your office network by "pinging" of the office computers:



- 13. 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
- 14. Congratulations! You have successfully created the VPN Connection from SSH Sentinel VPN Client to your Office network through D-Link DFL-500 Firewall!