Topology:

PC 1 ------SSL client (Remote User)

Setup:

(1) Check firmware. You need to use 2.30.01.06 or later.

DFL-260E DFL-260E System Dipots Dipots Dipots Dipots Dipots	Image: System Status				
Interfaces Routing	Model: DFL-260E				
F. DP / IPS	System Time: 2011-11-15 11:58:37				
	Uptime: 0 days, 01:38:39				
🗄 🕞 Traffic Management	Configuration: Version 14				
	Firmware Version: 2.30.01.08-15905 May 12 2011				
	Last Restart: 2011-11-15 11:22:25: Activating configuration changes				
	IDP Signatures Last updated -				
	AV Signatures: 0 Signatures Last updated -				

(2) If you have not setup your PPPoE Internet connection yet - add a new PPPoE interface.

DFL-260E	Setup PPP (Point-to	Point Protocol) tunnels over	Ethernet interfaces.					
Dipets	Add 🗸							
- minterfaces	# 🕶	Name 🔻	Physical Interface 🗸	Remote Network 👻	Service Name 🔻	Username 🔻	Dial-on-demand	Comments 🗸
Ethernet	1	PPPOE	3 wan	🖁 all-nets		ac01575479	No	
PSec							() R	ight-click on a row for additional options.

(3) Add a new SSL VPN interface. Inter IP and IP address pool – they must be in the same subnet.

Outer interface: PPPoE

Server IP: pppoe_ip

	The SSL-VPN						
DFL-260E	An SSL VPN interface, together with the bundled client, creates an easy to use tunnel solution for roaming users.						
± System	General Add Boute						
	General Add Route						
E G Interfaces							
	Name: SSL-VPN						
🔤 VLAN							
	Inner IP: 10.10.10.254 V Local IP for the SSL VPN interface						
	Outer Interface: PPPOE V The physical Interface that the SSL VPN Interface will listen on						
	Server IP: PPPOE in V Listening IP for the SSI VPN interface						
PPTP/L2TP Servers							
PPTP/L2TP Clients	Server Port: 443 The listening port for the SSL VPN interface						
SSL VPN Interface							
Switch Management	(1) A corresponding User Authentication Rule must be created to handle authentication of SSL VPN users.						
ARP	n Client IP Ontions						
E 🚱 Routing							
🗄 🖓 🚺 🖾 🖉	Dynamic Server Address: Ontional FODN of the SSI VPN server riven to clients, en: (ssivun example com) Only needed if the Server IP is dynamic (
User Authentication	cytanin deret reactor.						
	IP Address Pool: 10.10.10.1-10.10.1 A range, group or network that will be the IP pool from which the SSL VPN clients will receive their IP addresses.						
	Primary Secondary						
	DNS: 168.95.1.1 V (None) V						

Note:

Inner IP

This is the IP number within the tunnel that SSL VPN clients will connect to.

All clients that connect to the SSL VPN object interface are allocated an IP from the SSL VPN interface's *IP Pool*. All the pool addresses as well as the *Inner IP* must belong to the same network and these define the relationship between the firewall and the connecting clients.

A private IP network should be used for this purpose. The *Inner IP* itself must not be one of the *IP Pool* addresses that can be handed out to connecting SSL VPN clients.

• IP Pool

As described above, client IP addresses for new SSL VPN connections are handed out from a pool of private IPv4 addresses. This pool is specified by an IP address object defined in the NetDefendOS address book. It is *not* the same as an *IP Pool* object used with IPsec.

The pool addresses do not need to be a continuous range but must belong to the same network. The *Inner IP* listed above must also belong to this network but must not be one of the pool IPs.

About more SSL VPN information, please read "NetDefendOS_2.40.00_Firewall_UserManual". (4) Add a new SSL VPN user "dlink".



Add 🗸		
Name 🔻	Groups 👻	IP Pool
admin	administrators	

- (5) Go to "User Authentication rules".
 - Interface: SSL-VPN

Originator IP: all-nets

Terminator IP: PPPOE_ip

	S auth			
GDFL-260E	The User Authent	tication Ruleset specifies	from w	here users are allowed to authenticate to the system, and how.
E Columb	General	Settings Author	aticatio	n Options Accounting Agent Options Pestrictions
	Contrai	Autici	nication	Recounting Agent options Restrictions
Rules	A Course			
E Interfaces	General			
Ethernet	Name:	auth		
····· 🕎 VLAN	Authorities for another			
···· 😚 IPsec	Autnentication agent:	L2TP/PPTP/SSL VF	^	
	Authentication Source:	Local	~	
😥 PPPoE	Interface:	SSL-VPN	~	
PPTP/L2TP Servers				
PPTP/L2TP Clients	Originator IP:	all-nets	× .	For XAuth and PPP, this is the tunnel originator IP.
SSL VPN Interface	Terminator IP:	PPPOE_ip	~	
Switch Management				
	Comments			
ARP	Comments			
🗄 🖓 Routing	Comments:			
🗄 🖓 🏹 IDP / IPS				
User Authentication				
🗄 🖓 🔂 Local User Databases				
AdminUsers				
External User Databases				
Accounting Servers				
User Authentication Rules				
Authentication Settings				

	General Log Settings Authentication Options Accounting Agent Options Restrictions
DFL-260E	彭 General
🗄 🖓 📁 Objects	Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.
🗄 📲 🙀 Rules	RADIUS servers
E-Galaces	Available Selected
WLAN	
GRE	
PPTP/L2TP Servers	
PPTP/L2TP Clients	
SSL VPN Interface	Move up Move down
Switch Management	
Interface Groups	1010
ARP	LUAF Servers
+ Routing	Avanadie Selected
E-R Local User Databases	
	<<
Accounting Servers	
Ser Authentication Rules	Move up Move down
Authentication Settings	
Traffic Management	
E By trans management	RADIUS Method: Unencrypted password (PAP)
	Local User DB: AdminUsers

(6) Add 2 IP rules for SSL VPN user.

DFL-260E	B IP Rules	d to filter IP-based network traffic	In addition, they provide n	neans for address translation as	well as Server Load Balancing.			
Dijects	Add 🗸							
E- 8 IP Rules	#-	Name	Action	Sec If -	Src Net -	Dest If -	Dest Net -	Service -
ian_to_wan	1	\$ in	Allow	SSL-VPN	😌 all-nets	🔝 lan	🤤 all-nets	🗑 all_services
Access	2	\$ out	TAT NAT	SSL-VPN	🗟 all-nets	PPPOE	🗟 all-nets	all_services
- interfaces	3	<pre>g ping_fw</pre>	Allow	🔯 any	🖁 all-nets	Si core	🖁 lan_ip	ping-inbound
Ethernet	4	诸 lan_to_wan						
Charles Charl							Đ.	Right-Slick on a row for additional opti

- (7) Save the firewall's configuration.
- (8) Remote user needs to open a web browser and enter the firewall's WAN IP address (or DynDNS address). Enter SSL username and password. Accept the download and installation of SSL thin client. Remote user can now use this thin client to connect.

Connect - D-Link SSL VPN Clie	nt 🗆 🔍 🗙
D-Link	_
User name:	
No verification of the server certiin when custom server is selected	ficate can be done
Specify Custom Server	
<u>A</u> ddress:	Po <u>r</u> t:
company.dyndns.com	443
Connec	t <u>C</u> ancel