

Configuration Guide



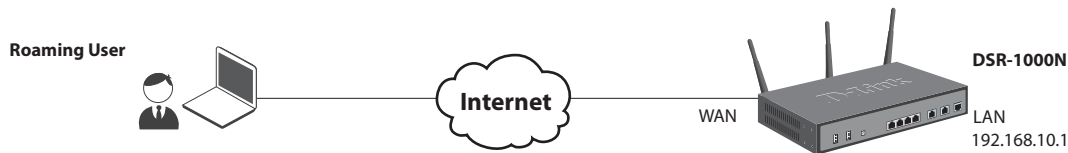
How to Configure SSL VPN Features in DSR Series

Overview

This document describes how to configure D-Link DSR-500N to enable SSL VPN feature. An SSL VPN is a form of VPN that can be used with a standard Web browser. SSL VPN doesn't require the installation of specialized client software on end users' computers, and is ideal for applications including file sharing, remote backup and remote system management.

Situation note

In this scenario, all application servers of headquarter are located in 192.168.10.0/24 subnet. We are going to configure DSR router which allows remote PCs to access application servers via this SSL VPN tunnel. This tunnel doesn't handle local Internet traffic of PCs in order to reduce traffic overhead for the tunnel.



Firmware version
1.03B12_WW

Configuration Step

1. Before SSL configuration, please enable remote management feature via [Tools -> Admin -> Remote Management](#).

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS
Admin	Admin Settings			
Date and Time	Remote Management			LOGOUT
Log Settings	SNMP			
System	SNMP System Info			
Firmware				
Firmware via USB				
Dynamic DNS				
System Check				
Schedules				

System Name

System Name:

Don't Save Settings

Make sure the **Enable Remote Management** option is enabled and keep the Port Number in 443.

REMOTE MANAGEMENT		LOGOUT
<p>From this page a user can configure the remote management feature. This feature can be used to manage the box remotely from WAN side.</p> <p> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p>		
Remote Management Enable		
Enable Remote Management:	<input checked="" type="checkbox"/>	
Access Type:	All IP Addresses	▼
From:	<input type="text"/>	
To:	<input type="text"/>	
IP Address:	<input type="text"/>	
Port Number:	443	
Enable Remote SNMP:	<input type="checkbox"/>	

2. Go to SETUP -> VPN Settings -> SSL VPN server -> Portal Layouts

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	<p>INTERNET CONNECTION LOGOUT</p> <p>This page will guide you through common configuration tasks such as changing the password, timezone and setting up of your internet connection.</p>			
Internet Settings	<p>Internet Connection Setup Wizard</p> <p>our easy to use Web-based Wizards to assist you in connecting your new D-Link internet, click on the button below.</p> <p><input type="button" value="Internet Connection Setup Wizard"/></p>			
Wireless Settings	<p>are you have followed all steps outlined in the Quick</p>			
Network Settings	<p>SSL VPN Server</p>			
DMZ Setup	<p>Portal Layouts</p>			
VPN Settings	<p>IPsec</p>			
USB Settings	<p>PPTP</p>			
VLAN Settings	<p>L2TP</p>			
	<p>SSL VPN Client</p>			
	<p>Manual Internet Con</p>			
	<p>Resources</p>			
	<p>Port Forwarding</p>			
	<p>If you would like to config your new D-Link Systems Router manually, then click on the button below.</p> <p><input type="button" value="Manual Internet Connection Setup"/></p>			

Follow below parameter to add a portal layout.

Portal Layout Name: **test**

Portal Site Title (optional): **test**

Banner Title (optional): **test**

Display banner message on login page: **Enabled**

HTTP meta tags for cache control (recommended): **Enabled**

ActiveX Web cache cleaner: **Enabled**

VPN tunnel page: **Enabled**

Port Forwarding: **Enabled**

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS
Wizard				
Internet Settings				
Wireless Settings				
Network Settings				
DMZ Setup				
VPN Settings	<div style="border: 1px solid black; padding: 5px;"> <p>PORTAL LAYOUT CONFIGURATION LOGOUT</p> <p>This page allows you to add a new portal layout or edit the configuration of an existing portal layout. The details will then be displayed in the List of Portal Layouts table on the SSL VPN Server > Portal Layouts page under the VPN menu.</p> <p style="text-align: center;"> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p> </div>			
USB Settings	<div style="border: 1px solid black; padding: 5px;"> <p>Portal Layout and Theme Name</p> <p>Portal Layout Name: <input type="text" value="test"/></p> <p>Portal Site Title (Optional) : <input type="text" value="test"/></p> <p>Banner Title (Optional) : <input type="text" value="test"/></p> <p>Banner Message (Optional) : <input type="text" value="ssl-test"/></p> <p>Display banner message on login page: <input checked="" type="checkbox"/></p> <p>HTTP meta tags for cache control (recommended): <input checked="" type="checkbox"/></p> <p>ActiveX web cache cleaner: <input checked="" type="checkbox"/></p> </div>			
VLAN Settings	<div style="border: 1px solid black; padding: 5px;"> <p>SSL VPN Portal Pages to Display</p> <p>VPN Tunnel page: <input checked="" type="checkbox"/></p> <p>Port Forwarding: <input checked="" type="checkbox"/></p> </div>			

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS												
Wizard	<p>PORTAL LAYOUTS LOGOUT</p> <p>The table lists the SSL portal layouts configured for this device and allows several operations on the portal layouts.</p>															
Internet Settings	<p>List of of Layouts</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Layout Name</th> <th>Use Count</th> <th>Portal URL</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>SSLVPN*</td> <td>1</td> <td>https://0.0.0.0/portal/SSLVPN</td> </tr> <tr> <td><input type="checkbox"/></td> <td>test</td> <td>0</td> <td>https://0.0.0.0/portal/test</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Set Default"/> <input type="button" value="Add"/> </p>				<input type="checkbox"/>	Layout Name	Use Count	Portal URL	<input type="checkbox"/>	SSLVPN*	1	https://0.0.0.0/portal/SSLVPN	<input type="checkbox"/>	test	0	https://0.0.0.0/portal/test
<input type="checkbox"/>	Layout Name	Use Count	Portal URL													
<input type="checkbox"/>	SSLVPN*	1	https://0.0.0.0/portal/SSLVPN													
<input type="checkbox"/>	test	0	https://0.0.0.0/portal/test													
Wireless Settings																
Network Settings																
DMZ Setup																
VPN Settings																
USB Settings																
VLAN Settings																

The GUI page will look like above screenshot when you finish to add a portal layout.

3. Go to **ADVANCED** -> **Users** -> **Domains**, create a new Domain for SSL VPN users.

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS																						
Application Rules	<p>APPLICATION RULES LOGOUT</p> <p>The table lists all the available port triggering rules and allows several operations on the rules.</p>																									
Website Filter	<p>List of Available Application Rules</p> <table border="1"> <thead> <tr> <th rowspan="2"><input type="checkbox"/></th> <th rowspan="2">Name</th> <th rowspan="2">Enable</th> <th rowspan="2">Protocol</th> <th rowspan="2">Interface</th> <th colspan="2">Outgoing Ports</th> <th colspan="2">Incoming Ports</th> </tr> <tr> <th>Start Port</th> <th>End Port</th> <th>Start Port</th> <th>End Port</th> </tr> </thead> <tbody> <tr> <td colspan="9" style="text-align: center;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add"/> </td> </tr> </tbody> </table>				<input type="checkbox"/>	Name	Enable	Protocol	Interface	Outgoing Ports		Incoming Ports		Start Port	End Port	Start Port	End Port	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add"/>								
<input type="checkbox"/>	Name	Enable	Protocol	Interface						Outgoing Ports		Incoming Ports														
					Start Port	End Port	Start Port	End Port																		
<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add"/>																										
Firewall Settings																										
Wireless Settings																										
Advanced Network																										
Routing																										
Certificates																										
Users	<ul style="list-style-type: none"> Get Users DB <li style="background-color: #e0e0e0;">Domains Groups Users 																									
IP/MAC Binding																										
IPv6																										
Radius Settings																										
Switch Settings																										

Follow below parameters on Domains Configuration page.

Domain name: **test**, select portal: **test**

DSR-500N // SETUP ADVANCED TOOLS STATUS

Application Rules ▶
Website Filter ▶
Firewall Settings ▶
Wireless Settings ▶
Advanced Network ▶
Routing ▶
Certificates ▶
Users ▶
IP/MAC Binding ▶
IPv6 ▶
Radius Settings ▶
Switch Settings ▶

DOMAINS LOGOUT

This page allows a user to add a new domain.

Save Settings Don't Save Settings

Domains Configuration

Domain Name: test

Authentication Type: Local User Database ▼

Select Portal: test ▼

Authentication Server 1: [Text Field]

Authentication Server 2: [Text Field] (Optional)

Authentication Server 3: [Text Field] (Optional)

Timeout: 360 (Seconds)

Retries: 5

DSR-500N // SETUP ADVANCED TOOLS STATUS

Application Rules ▶
Website Filter ▶
Firewall Settings ▶
Wireless Settings ▶
Advanced Network ▶
Routing ▶
Certificates ▶
Users ▶
IP/MAC Binding ▶
IPv6 ▶
Radius Settings ▶
Switch Settings ▶

DOMAINS LOGOUT

This page shows the list of added domains to the router. The user can add, delete and edit the domains also.

List of Domains

<input type="checkbox"/>	Domain Name	Authentication Type	Portal Layout Name
<input type="checkbox"/>	SSLVPN *	Local User Database	SSLVPN
<input type="checkbox"/>	test	Local User Database	test

Edit Delete Add

The GUI page will look like above screenshot when you finish to add a new domain.

4. Go to **ADVANCED** -> **Users** -> **Users**, add a new user account for SSL VPN connection belong to the **test** domain.

User Name	Group	Type	Authentication Domain	Login Status
admin *	SSLVPN	Administrator	Local User Database	Enabled (LAN and WAN)
test	SSLVPN	Guest	Local User Database	Disabled

Follow below parameters on Users Configuration page:

User Name: **test1**

First Name: **test1**

Last Name: **test1**

User Type: **SSL VPN user**

Password: **<Here please input a password>**

Confirm Password: **<Here please input a same password again>**

Idle Timeout: **30 Minutes**

Users Configuration

User Name: test1

First Name: test1

Last Name: test1

User Type: SSL VPN User

Select Group: SSLVPN

Password: •••••

Confirm Password: •••••

Idle Timeout: 30 (Minutes)

Operation succeeded

USERS LOGOUT

This page shows a list of available users in the system. A user can add, delete and edit the users also. This page can also be used for setting policies on users.

List of Users

<input type="checkbox"/>	User Name	Group	Type	Authentication Domain	Login Status
<input type="checkbox"/>	admin *	SSLVPN	Administrator	Local User Database	Enabled (LAN and WAN)
<input type="checkbox"/>	guest *	SSLVPN	Guest	Local User Database	Disabled
<input type="checkbox"/>	test1	SSLVPN	SSL VPN User	Local User Database	Enabled (LAN and WAN)

The GUI page will look like above screenshot when you finish to add a new user belong to test domain.

- Go to **SETUP** -> **VPN Settings** -> **SSL VPN Client** -> **SSL VPN Client**, in this page, administrator is able to configure what IP address range, DNS information will be dispensed to SSL VPN clients .

INTERNET CONNECTION LOGOUT

This page will guide you through common configuration tasks such as changing the password, timezone and setting up of your internet connection.

Internet Connection Setup Wizard

our easy to use Web-based Wizards to assist you in connecting your new D-Link Internet, click on the button below.

These wizards, please make sure you have followed all steps outlined in the Quick Start in the package.

Manual Internet Connection Setup

If you would like to configure your new D-Link Systems Router manually, then click on the button below.

Follow below parameters to configure on SSL VPN Client page:

Enable Split Tunnel Support: **Enabled**

Client Address Range Begin: **192.168.251.1**

Client Address Range end: **192.168.251.254**

LCP Timeout: **60 Minutes**

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS
Wizard Internet Settings Wireless Settings Network Settings DMZ Setup VPN Settings USB Settings VLAN Settings	<div style="text-align: right;">LOGOUT</div> <h3>SSL VPN CLIENT</h3> <p>An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this device. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address, DNS and WINS settings is automatically created, which allows local applications to talk to services on the private network without any special network configuration on the remote SSL VPN client machine.</p> <p> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p> <h4>Client IP Address Range</h4> <p>Enable Split Tunnel Support: <input checked="" type="checkbox"/></p> <p>DNS Suffix (Optional) : <input type="text"/></p> <p>Primary DNS Server (Optional) : <input type="text"/></p> <p>Secondary DNS Server (Optional) : <input type="text"/></p> <p>Client Address Range Begin: <input type="text" value="192.168.251.1"/></p> <p>Client Address Range End: <input type="text" value="192.168.251.254"/></p> <p>LCP Timeout: <input type="text" value="60"/> (Seconds)</p>			

- Go to **SETUP -> VPN Settings -> SSL VPN Client -> Configured Client Routes** to add a static route, since we enabled the feature of "Split Tunnel Support" at previous step. Therefore, administrator is able to manually alter the routing entries for each SSL user.

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	SSL VPN CLIENT LOGOUT			
Internet Settings	An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this device. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address, DNS and WINS settings is automatically created, which allows local applications to talk to services on the private network without any special network configuration on the remote SSL VPN client machine.			
Wireless Settings	<input type="button" value="Don't Save Settings"/>			
Network Settings	IPsec			
DMZ Setup	PPTP			
VPN Settings	L2TP			
USB Settings	SSL VPN Server	Split Tunnel Support: <input checked="" type="checkbox"/>		
VLAN Settings	SSL VPN Client	<input type="text"/> <input type="text"/> <input type="text"/>		
	Primary DNS Server	Configured Client Routes		
	Secondary DNS Server	SSL VPN Client Portal		
	Client Address Range Begin:	192.168.251.1		
	Client Address Range End:	192.168.251.254		
	LCP Timeout:	60 (Seconds)		

Note: DSR router would not allow you to add Client Routes if you didn't enable the Split Tunnel Support at previous step.

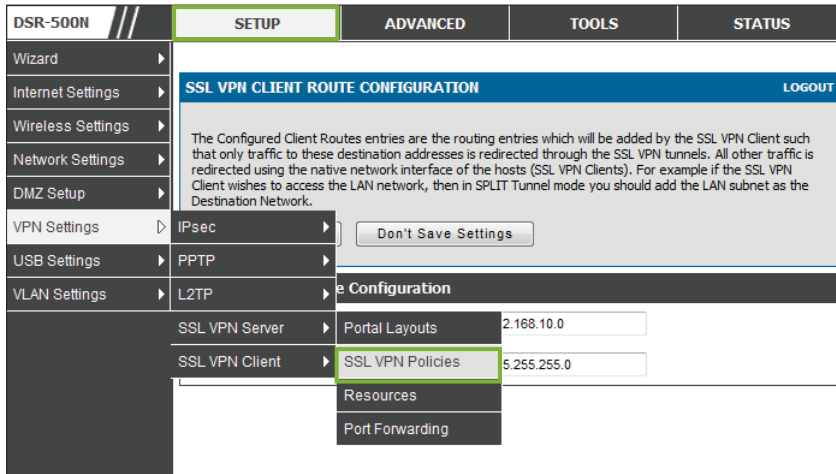
Following parameters are routing information of remote network for SSL VPN client.

Destination Network: **192.168.10.0**

Subnet Mask: **255.255.255.0**

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	SSL VPN CLIENT ROUTE CONFIGURATION LOGOUT			
Internet Settings	The Configured Client Routes entries are the routing entries which will be added by the SSL VPN Client such that only traffic to these destination addresses is redirected through the SSL VPN tunnels. All other traffic is redirected using the native network interface of the hosts (SSL VPN Clients). For example if the SSL VPN Client wishes to access the LAN network, then in SPLIT Tunnel mode you should add the LAN subnet as the Destination Network.			
Wireless Settings	<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>			
Network Settings	SSL VPN Client Route Configuration			
DMZ Setup	Destination Network:	192.168.10.0		
VPN Settings	Subnet Mask:	255.255.255.0		
USB Settings				
VLAN Settings				

7. Go to **SETUP -> VPN Settings -> SSL VPN Server -> SSL VPN Policies**, create a policy that allow the SSL VPN users to access remote network.



Add a SSL VPN policy and follow below parameters on SSL VPN Policy Configuration Page.

Policy For: **Global**

Apply Policy to: **All Addresses**

Policy Name: **Allow_all_address**

Begin: **0**

End: **65535**

Service: **All**

Permission: **Permit**

When you click save settings, a SSL VPN policy has been created like following screenshot.

The screenshot shows the DSR-500N web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, and STATUS. The left sidebar lists various settings: Wizard, Internet Settings, Wireless Settings, Network Settings, DMZ Setup, VPN Settings, USB Settings, and VLAN Settings. The main content area shows a red message "Operation succeeded". Below this is the "SSL VPN POLICIES" section with a "LOGOUT" link. A descriptive text explains that policies are used to permit or deny access to network resources. The "Query" section allows filtering by "View List of SSL VPN Policies For:" (Global), "Available Groups:" (SSLVPN), and "Available Users:" (admin). A "Display" button is present. Below the query section is a table titled "List of SSL VPN Policies" with columns for Name, Service, Destination, and Permission. One policy is listed: "Allow_all_address" with Service "All", Destination "0.0.0.0/0-65535", and Permission "Permit". At the bottom are "Edit", "Delete", and "Add" buttons.

Name	Service	Destination	Permission
Allow_all_address	All	0.0.0.0/0-65535	Permit

8. Now, you have finished all settings in DSR routers. When you successfully connect to DSR router via SSL VPN \ tunnel, You can check that there will be two default gateway in your client PC.

For Internet traffic, it will be routed to 172.17.5.254.

For company network traffic, it will be routed to 192.168.251.1.

The screenshot shows a Windows desktop environment. On the left, a command prompt window titled "系統管理員: C:\Windows\system32\cmd.exe" displays the IPv4 routing table. The table lists various network destinations, their associated interfaces, and metrics. Two rows are highlighted with red boxes: the first row shows the default route (0.0.0.0) pointing to the Microsoft ISATAP Adapter #2, and the second row shows a specific route (192.168.251.0) pointing to the Teredo Tunneling Pseudo-Interface.

On the right, a status window titled "D-link-SSLVPN-Tunnel Connection Status" is open. It displays connection details for the "D-link-SSLVPN-Tunnel" interface. The "Status" is "Connected" with a duration of "00:01:34". The "Interfaces" section shows the "IF Address" as "192.168.251.2" and the "Server IP" as "218.210.16.29". The "Activity" section shows "Bytes Sent" as 7165 and "Bytes Received" as 670. A "Status Message" at the bottom reads "D-link-SSLVPN-Tunnel Connected".

The taskbar at the bottom shows the system clock as "上午 11:33" on "2011/2/11".

D-Link[®]

Visit our website for more information
www.dlink.com

D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries.
All other third party marks mentioned herein are trademarks of the respective owners.

Copyright © 2011 D-Link Corporation. All Rights Reserved.