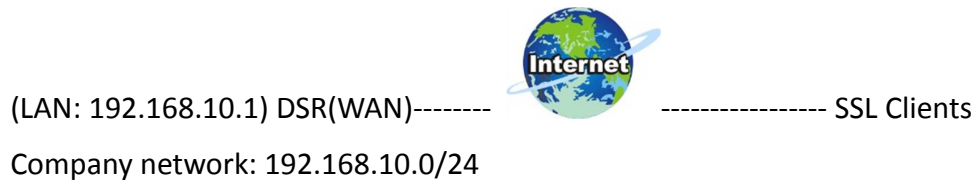


## How to create SSL VPN server for users in DSR



In this scenario, the traffic of SSL clients send to the network 192.168.10.0/24 will be forwarded via SSL VPN, and the normal internet traffic will be sent through their local ISP, it's so called the "split tunnel" in VPN terminology.

(1) Go to SETUP->VPN Settings->SSL VPN server->Portal

The screenshot shows the router's configuration page for the DSR-500N. The 'SETUP' tab is selected. Under 'VPN Settings', 'SSL VPN Server' is expanded, and 'Portal Layouts' is highlighted with a red box. Other options visible include 'IPsec', 'PPTP', 'L2TP', 'SSL VPN Client', 'Manual Internet Conn', and 'Port Forwarding'. A 'Helpful Hints...' sidebar is visible on the right.

(2) Add a custom portal.

The screenshot shows the 'PORTAL LAYOUTS' configuration page. It contains a table with the following data:

	Layout Name	Use Count	Portal URL
<input type="checkbox"/>	SSLVPN*	1	https://218.210.16.29/portal/SSLVPN
<input type="checkbox"/>	test	1	https://218.210.16.29/portal/test

The 'test' row is highlighted with a red box. Below the table are buttons for 'Edit', 'Delete', 'Set Default', and 'Add'.

Product Page: DSR-500N Hardware Version: A1 Firmware Version: 0.0.5\_WW

# D-Link®

DSR-500N
SETUP
ADVANCED
TOOLS
STATUS
HELP

- Wizard
- Internet Settings
- Wireless Settings
- Network Settings
- DMZ Setup
- VPN Settings
- USB Settings
- VLAN Settings

### PORTAL LAYOUT CONFIGURATION LOGOUT

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.

---

**Portal Layout and Theme Name**

Portal Layout Name:

Portal Site Title (Optional):

Banner Title (Optional):

Banner Message (Optional):

Display banner message on login page:

HTTP meta tags for cache control (recommended):

ActiveX web cache cleaner:

---

**SSL VPN Portal Pages to Display**

VPN Tunnel page:

Port Forwarding:

**Helpful Hints...**

When remote users want to access the private network through an SSL tunnel (either using the Port Forwarding or VPN tunnel service), they logn through the client ports. This portal provides the authentication fields to provide the appropriate access levels and privileges as determined by the router.

[More...](#)

UNIFIED SERVICES ROUTER

Copyright © 2010 D-Link Corporation.

(3)Go to ADVANCE->Users->Domains, create a domain object.

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

### APPLICATION RULES LOGOUT

The table lists all the available port triggering rules and allows several operations on the rules.

List of Available Application Rules								
☐	Name	Enable	Protocol	Interface	Outgoing Ports		Incoming Ports	
					Start Port	End Port	Start Port	End Port
<div style="display: flex; justify-content: center; gap: 20px;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add"/> </div>								

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

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.

**Domains Configuration**

**Domain Name:**

**Authentication Type:**

**Select Portal:**

**Authentication Server 1:**

**Authentication Server 2:**  (Optional)

**Authentication Server 3:**  (Optional)

**Timeout:**  (Seconds)

**Retries:**

(4) Go to ADVANCE->Users->Users, create a test user then apply the previous created Domain object on.

The screenshot shows the 'Domains Configuration' page in the DSR-500N interface. The 'ADVANCED' tab is active. The left sidebar has 'Users' highlighted. The main content area shows the following configuration:

- Domain Name:** test
- Authentication Domain:** Local User Database
- Group:** test
- Authentication Server 1:** [Empty field]
- Authentication Server 2:** [Empty field] (Optional)
- Authentication Server 3:** [Empty field] (Optional)
- Timeout:** 360 (Seconds)

The screenshot shows the 'Users' page in the DSR-500N interface. The 'ADVANCED' tab is active. The left sidebar has 'Users' highlighted. The main content area shows the 'List of Users' table:

<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"/>	tes1t	test	SSL VPN User	Local User Database	Enabled (LAN and WAN)

Below the table are buttons for 'Edit', 'Delete', and 'Add'. At the bottom, there are buttons for 'Login Policies', 'Policies By Browsers', and 'Policies By IP'.

Website Filter	<b>USERS CONFIGURATION</b> <span style="float: right;">LOGOUT</span>																				
Firewall Settings	<p>This page allows a user to add new system users.</p> <p style="text-align: center;"> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p>																				
Wireless Settings	<b>Users Configuration</b>																				
Advanced Network	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"><b>User Name:</b></td> <td><input type="text" value="tes1t"/></td> </tr> <tr> <td><b>First Name:</b></td> <td><input type="text" value="test1"/></td> </tr> <tr> <td><b>Last Name:</b></td> <td><input type="text" value="test1"/></td> </tr> <tr> <td><b>User Type:</b></td> <td><input type="text" value="SSL VPN User"/></td> </tr> <tr> <td><b>Select Group:</b></td> <td><input type="text" value="test"/></td> </tr> <tr> <td><b>Check to Edit Password:</b></td> <td><input type="checkbox"/></td> </tr> <tr> <td><b>Enter Current Logged in Administrator Password:</b></td> <td><input type="text"/></td> </tr> <tr> <td><b>New Password:</b></td> <td><input type="text"/></td> </tr> <tr> <td><b>Confirm New Password:</b></td> <td><input type="text"/></td> </tr> <tr> <td><b>Idle Timeout:</b></td> <td><input type="text" value="30"/> (Minutes)</td> </tr> </table>	<b>User Name:</b>	<input type="text" value="tes1t"/>	<b>First Name:</b>	<input type="text" value="test1"/>	<b>Last Name:</b>	<input type="text" value="test1"/>	<b>User Type:</b>	<input type="text" value="SSL VPN User"/>	<b>Select Group:</b>	<input type="text" value="test"/>	<b>Check to Edit Password:</b>	<input type="checkbox"/>	<b>Enter Current Logged in Administrator Password:</b>	<input type="text"/>	<b>New Password:</b>	<input type="text"/>	<b>Confirm New Password:</b>	<input type="text"/>	<b>Idle Timeout:</b>	<input type="text" value="30"/> (Minutes)
<b>User Name:</b>	<input type="text" value="tes1t"/>																				
<b>First Name:</b>	<input type="text" value="test1"/>																				
<b>Last Name:</b>	<input type="text" value="test1"/>																				
<b>User Type:</b>	<input type="text" value="SSL VPN User"/>																				
<b>Select Group:</b>	<input type="text" value="test"/>																				
<b>Check to Edit Password:</b>	<input type="checkbox"/>																				
<b>Enter Current Logged in Administrator Password:</b>	<input type="text"/>																				
<b>New Password:</b>	<input type="text"/>																				
<b>Confirm New Password:</b>	<input type="text"/>																				
<b>Idle Timeout:</b>	<input type="text" value="30"/> (Minutes)																				
Routing																					
Certificates																					
Users																					
IP/MAC Binding																					
IPv6																					
Radius Settings																					
Switch Settings																					

(5)Go to TOOL->Admin->Remote Management, check the checkbox of “Enable the Remote Management”, it’s used for users are able to build up SSL VPN tunnel with TCP port 443.

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS
Admin	Admin Settings			
Date and Time	Remote Management			LOGOUT
Log Settings	SNMP	<p>set the router identification name.</p> <p style="text-align: center;"> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p>		
System	SNMP System Info			
Firmware				
Firmware via USB				
Dynamic DNS				
System Check				
Schedules				

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		
<b>Enable Remote Management:</b>	<input checked="" type="checkbox"/>	
<b>Access Type:</b>	All IP Addresses	
<b>From:</b>	<input type="text"/>	
<b>To:</b>	<input type="text"/>	
<b>IP Address:</b>	<input type="text"/>	
<b>Port Number:</b>	443	
<b>Enable Remote SNMP:</b>	<input type="checkbox"/>	

(6)Go to SETUP->VPN Settings->SSL VPN Client->SSL VPN Client, in this page, administrator is able to dispense the IP range/DNS/DNS Suffix to SSL clients.

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

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	<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><b>Enable Split Tunnel Support:</b> <input checked="" type="checkbox"/></p> <p><b>DNS Suffix (Optional) :</b> <input type="text"/></p> <p><b>Primary DNS Server (Optional) :</b> <input type="text"/></p> <p><b>Secondary DNS Server (Optional) :</b> <input type="text"/></p> <p><b>Client Address Range Begin:</b> <input type="text" value="192.168.251.1"/></p> <p><b>Client Address Range End:</b> <input type="text" value="192.168.251.254"/></p> <p><b>LCP Timeout:</b> <input type="text" value="60"/> (Seconds)</p>			
Internet Settings				
Wireless Settings				
Network Settings				
DMZ Setup				
VPN Settings				
USB Settings				
VLAN Settings				



(7) Go to SETUP->VPN Settings->SSL VPN Client->SSL VPN Client->Configured Client Routes, since we've enabled the feature of "Split Tunnel Support", therefore administrator is able to manually alter the routing entries for each SSL user.

The screenshot shows the 'SSL VPN CLIENT' configuration page. The 'SETUP' tab is active. The left sidebar has 'Configured Client Routes' highlighted. The main content area includes a 'Split Tunnel Support' checkbox which is checked, and a 'Don't Save Settings' button. Below this, there are fields for 'Primary DNS Server', 'Secondary DNS Server', 'Client Address Range Begin' (192.168.251.1), 'Client Address Range End' (192.168.251.254), and 'LCP Timeout' (60 seconds).

The screenshot shows the 'CONFIGURED CLIENT ROUTES' page. The 'SETUP' tab is active. The left sidebar has 'Configured Client Routes' highlighted. The main content area includes a table with the following data:

Destination Network	Subnet Mask
192.168.10.0	255.255.255.0

Below the table are 'Delete' and 'Add' buttons.

(8) Go to SETUP->VPN Settings->SSL VPN Server->SSL VPN Policies, create a policy that allow the SSL users access into internal network.

The screenshot shows the configuration interface for a DSR-500N device. The 'SETUP' tab is selected. The left sidebar contains a tree view with 'VPN Settings' expanded to 'SSL VPN Client', where 'SSL VPN Policies' is highlighted. The main content area shows 'CONFIGURED CLIENT ROUTES' with an 'Add' button.

Destination Network	Subnet Mask
	255.255.255.0

The screenshot shows the 'SSL VPN POLICIES' configuration page. It includes a 'Query' section with filters for 'View List of SSL VPN Policies For:', 'Available Groups:', and 'Available Users:'. Below the filters is a 'Display' button. The 'List of SSL VPN Policies' table shows a single policy named 'allow' with 'All' service and '0.0.0.0/0-65535' destination.

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

**Policy For**

Policy For: Global

Available Groups: SSLVPN

Available Users: admin

---

**SSL VPN Policy**

Apply Policy to: All Addresses

Policy Name: allow

IP Address: [ ]

Mask Length: [ ]

---

**Port Range / Port Number**

Begin: 0 (0-65535)

End: 65535 (0-65535)

Service: All

Defined Resources: [ ]

Permission: Permit

(9)When you connect SSL VPN successfully. You will see two default gateway. Internet traffic will go to 172.17.5.254. Company network traffic will go to 192.168.251.1

