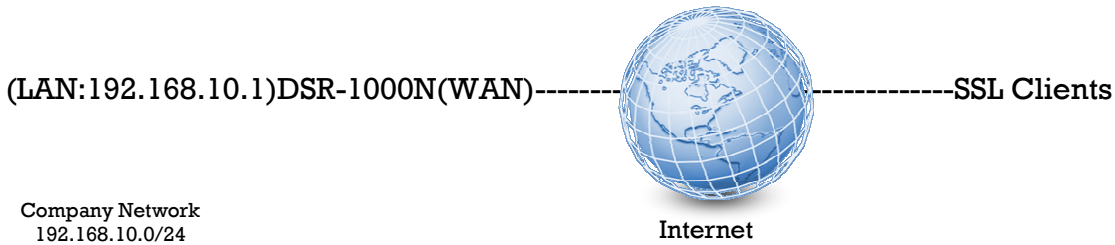


How to create SSL VPN server for users in DSR-1000N?

[Scenario]



Here we're trying to build up a SSL VPN server on the DSR-1000N for users are able to remotely connect into the resource of company network.

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

[Procedure]

1. Go to SETUP→VPN Settings→SSL VPN server→Portal Layouts.

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01B31

D-Link

DSR-1000N // **SETUP** ADVANCED TOOLS STATUS HELP

Wizard

Internet Settings ▶ **INTERNET CONNECTION** LOGOUT

Wireless Settings ▶

Network Settings ▶

DMZ Setup ▶

VPN Settings ▶ IPsec ▶ our easy to use Web-based Wizards to assist you in connecting your new D-Link internet, click on the button below.

USB Settings ▶ PPTP ▶

VLAN Settings ▶ L2TP ▶

SSL VPN Server ▶ **Portal Layouts** ▶ If you have followed all steps outlined in the Quick

SSL VPN Client ▶ SSL VPN Policies

Manual Internet Con ▶ Resources

Port Forwarding

Manual Internet Connection Setup

UNIFIED SERVICES ROUTER

Helpful Hints...
If you are new to networking and have never configured a router before, click on Internet Connection Setup Wizard and the router will run you through a few simple steps to get your network up and running.
If you consider yourself an Advanced user and have configured a router before, click Manual Internet Connection Setup to input all the settings manually.
More...

2. Add a custom portal.

PORTAL LAYOUTS

LOGOUT

The table lists the SSL portal layouts configured for this device and allows several operations on the portal layouts.

List of of Layouts

<input type="checkbox"/>	Layout Name	Use Count	Portal URL
<input type="checkbox"/>	SSLVPN*	1	https://0.0.0.0/portal/SSLVPN
<input type="checkbox"/>	fortest	1	https://0.0.0.0/portal/fortest
<input type="checkbox"/>	test2	1	https://0.0.0.0/portal/test2

Edit

Delete


Set Default

Add 

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.

Save Settings 

Don't Save Settings

Portal Layout and Theme Name

Portal Layout Name: **1**

test_custom_portal

Portal Site Title (Optional) :

Test_Portal_Title

Banner Title (Optional) :

Test_Banner_Title

Banner Message (Optional) :

Test Banner message

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:



3. Go to ADVANCE→Users→Domains, create a domain object.



DSR-1000N // **SETUP** **ADVANCED** TOOLS STATUS HELP

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

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"/>	fortest	Local User Database	fortest
<input type="checkbox"/>	fortest2	Local User Database	test2

Helpful Hints...
The Domain determines the authentication method for a VPN or GUI user. For SSL VPN connections, the domain sets the portal layout and corresponding SSL VPN features. You must create a Domain first, and then a new Group can be created and assigned to the Domain. The last step is to add specific SSL VPN users to an already-configured Group.
[More...](#)

UNIFIED SERVICES ROUTER

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"/>	fortest	Local User Database	fortest
<input type="checkbox"/>	fortest2	Local User Database	test2

This page allows a user to add a new domain.

Domains Configuration

Domain Name:	<input type="text" value="Domain_for_test_custom_portal"/>
Authentication Type:	<input type="text" value="Local User Database"/> ▼
Select Portal:	<input type="text" value="test_custom_portal"/> ▼
Authentication Server 1:	<input type="text"/>
Authentication Server 2:	<input type="text"/> (Optional)
Authentication Server 3:	<input type="text"/> (Optional)
Timeout:	<input type="text" value="360"/> (Seconds)
Retries:	<input type="text" value="5"/>
Authentication Secret:	<input type="text"/>
Authentication Secret2:	<input type="text"/>
Workgroup:	<input type="text"/>
Second Workgroup:	<input type="text"/> (Optional)
LDAP Base DN:	<input type="text"/>
Second LDAP Base DN	<input type="text"/> (Optional)
Active Directory Domain:	<input type="text"/>
Second Active Directory Domain	<input type="text"/> (Optional)

4. Go to ADVANCE→Users→Users, create a test user then apply the previous created domain object on.



DSR-1000N // **SETUP** **ADVANCED** **TOOLS** **STATUS** **HELP**

Application Rules ▶ Operation succeeded

Website Filter ▶ **DOMAINS** **LOGOUT**

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

Wireless Settings ▶

Advanced Network ▶ **List of Domains**

<input type="checkbox"/>	Domain Name	Authentication Type	Portal Layout Name
<input type="checkbox"/>	SSLVPN *	Local User Database	SSLVPN
<input type="checkbox"/>	Get Users DB	test	Local User Database
<input type="checkbox"/>	Domains	test2	Local User Database
<input type="checkbox"/>	Groups	t_custom_portal	Local User Database

Routing ▶

Certificates

Users ▶ **Users**

IP/MAC Binding

IPV6 ▶

Radius Settings

Power Saving

UNIFIED SERVICES ROUTER

Helpful Hints...

The Domain determines the authentication method for a VPN or GUI user. For SSL VPN connections, the domain sets the portal layout and corresponding SSL VPN features. You must create a Domain first, and then a new Group can be created and assigned to the Domain. The last step is to add specific SSL VPN users to an already-configured Group.

[More...](#)

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	fortest	SSL VPN User	Local User Database	Enabled (LAN and WAN)
<input type="checkbox"/>	dlink	SSLVPN	Administrator	Local User Database	Enabled (LAN and WAN)
<input type="checkbox"/>	test2	fortest2	SSL VPN User	Local User Database	Enabled (LAN and WAN)

USERS CONFIGURATION LOGOUT

This page allows a user to add new system users.

Users Configuration

User Name:
First Name:
Last Name:
User Type:
Select Group:
Password:
Confirm Password:
Idle Timeout: (Minutes)

5. Go to TOOLS→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 DSR by TCP port 443.

D-Link

DSR-1000N // **SETUP** **ADVANCED** **TOOLS** **STATUS** **HELP**

Remote Management Enable

Enable Remote Management:
Access Type:
From:
To:
IP Address:
Port Number:
Enable Remote SNMP:

UNIFIED SERVICES ROUTER

Helpful Hints...
Both HTTPS and telnet access can be restricted to a subset of IP addresses. Administrator and Guest users are permitted to login to the GUI, and User Login Policies will allow remote management over HTTPS to take place as configured.
[More...](#)

REMOTE MANAGEMENT
LOGOUT

From this page a user can configure the remote management feature. This feature can be used to manage the box remotely from WAN side.

Remote Management Enable

Enable Remote Management:

Access Type: All IP Addresses ▼

From:

To:

IP Address:

Port Number:

Enable Remote SNMP:

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-1000N	SETUP	ADVANCED	TOOLS	STATUS	HELP
Wizard	SSL VPN CLIENT LOGOUT				Helpful Hints... An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this router. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address from the corporate subnet, DNS and WINS settings is automatically created. The IP addresses of the client's network interfaces (Ethernet, Wireless, etc.) cannot be identical to the router's IP address or a server on the corporate LAN that is being accessed through the SSL VPN tunnel. More...
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	Client Support: <input checked="" type="checkbox"/>				
DMZ Setup	Client Address Range: <input type="text"/>				
VPN Settings	Primary DNS Server: <input type="text"/>				
USB Settings	Secondary DNS Server: <input type="text"/>				
VLAN Settings	Client Address Range Begin: <input type="text" value="192.168.251.1"/>				
	Client Address Range End: <input type="text" value="192.168.251.254"/>				
	LCP Timeout: <input type="text" value="60"/> (Seconds)				
UNIFIED SERVICES ROUTER					

SSL VPN CLIENT LOGOUT

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.

Client IP Address Range

Enable Split Tunnel Support:

DNS Suffix (Optional) :

Primary DNS Server (Optional) :

Secondary DNS Server (Optional) :

Client Address Range Begin:

Client Address Range End:

LCP Timeout: (Seconds)

7. Go to ADVANCE→VPN Settings→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.

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.01B31

D-Link

DSR-1000N // **SETUP** **ADVANCED** **TOOLS** **STATUS** **HELP**

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

IPsec
 PPTP
 L2TP
 SSL VPN Server
SSL VPN Client
 SSL VPN Client Portal

Configured Client Routes LOGOUT
 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, and all other traffic is redirected using the hosts (SSL VPN Clients) native network interface. The table shows the destination routes that will be configured on the SSL VPN client. 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 subnet on this

Destination Network	Subnet Mask
192.168.10.0	255.255.255.0

Helpful Hints...
 For split tunnel SSL VPN client support, client routes must be configured to direct the SSL VPN client to a LAN resource.
[More...](#)

UNIFIED SERVICES ROUTER

CONFIGURED CLIENT ROUTES

LOGOUT

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, and all other traffic is redirected using the hosts (SSL VPN Clients) native network interface. The table shows the destination routes that will be configured on the SSL VPN client. 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 subnet on this device.

Configured Client Routes

<input type="checkbox"/>	Destination Network	Subnet Mask
<input type="checkbox"/>	192.168.10.0	255.255.255.0


Delete

Add 

SSL VPN CLIENT ROUTE CONFIGURATION

LOGOUT

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.

Save Settings 

Don't Save Settings

SSL VPN Client Route Configuration

Destination Network:

Subnet Mask:

8. Go to VPN Settings→SSL VPN Server→SSL VPN Policies, create a policy that allows the SSL users access into internal network.

The screenshot shows the configuration interface for a DSR-1000N device. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', and 'STATUS'. A sidebar on the left contains various settings categories: Wizard, Internet Settings, Wireless Settings, Network Settings, DMZ Setup, VPN Settings, USB Settings, and VLAN Settings. The 'VPN Settings' category is expanded, showing sub-options: IPsec, PPTP, L2TP, SSL VPN Server, and SSL VPN Client. 'SSL VPN Server' is further expanded to show 'Portal Layouts' and 'SSL VPN Policies', which is highlighted with a red box. The main content area displays a message: 'Please Enable Remote Management to activate SSL VPN Configurations.' Below this is the 'SSL VPN POLICY CONFIGURATION' section with a 'LOGOUT' link and a brief description: 'This page allows you to add a new SSL VPN Policy or edit the configuration of an existing SSL VPN Policy.' Two buttons, 'Save Settings' and 'Don't Save Settings', are visible.

The screenshot shows the 'SSL VPN POLICIES' configuration page. At the top, there is a 'LOGOUT' link. Below the header, a text block explains: 'Policies are useful to permit or deny access to specific network resources, IP addresses, or IP networks. They may be defined at the user, group or global level. By Default, a global PERMIT policy (not displayed) was already configured over all addresses and over all services/ports.' A 'Query' section contains three dropdown menus: 'View List of SSL VPN Policies For:' (set to 'Global'), 'Available Groups:' (set to 'SSLVPN'), and 'Available Users:' (set to 'admin'). A 'Display' button is located below these dropdowns.

The screenshot shows a table titled 'List of SSL VPN Policies'. The table has four columns: 'Name', 'Service', 'Destination', and 'Permission'. Below the table, there are three buttons: 'Edit', 'Delete', and 'Add'. The 'Add' button is highlighted with a red box.

Name	Service	Destination	Permission

This page allows you to add a new SSL VPN Policy or edit the configuration of an existing SSL VPN Policy.

Policy For

Policy For:

Available Groups:

Available Users:

SSL VPN Policy

Apply Policy to:

Policy Name:

IP Address:

Mask Length:

Port Range / Port Number

Begin: (0-65535)

End: (0-65535)

Service:

Defined Resources:

Permission:

End of document.