Configuration Guide

How to Configure SSL VPN Features in DSR Series

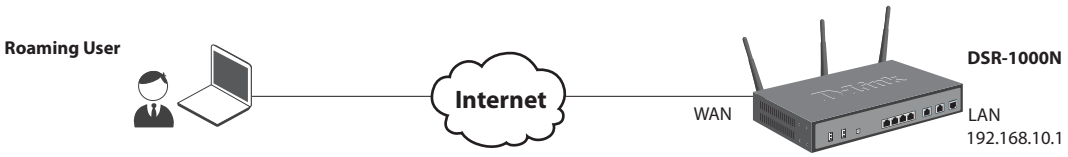
Overview

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.

D-Link®

Situation note

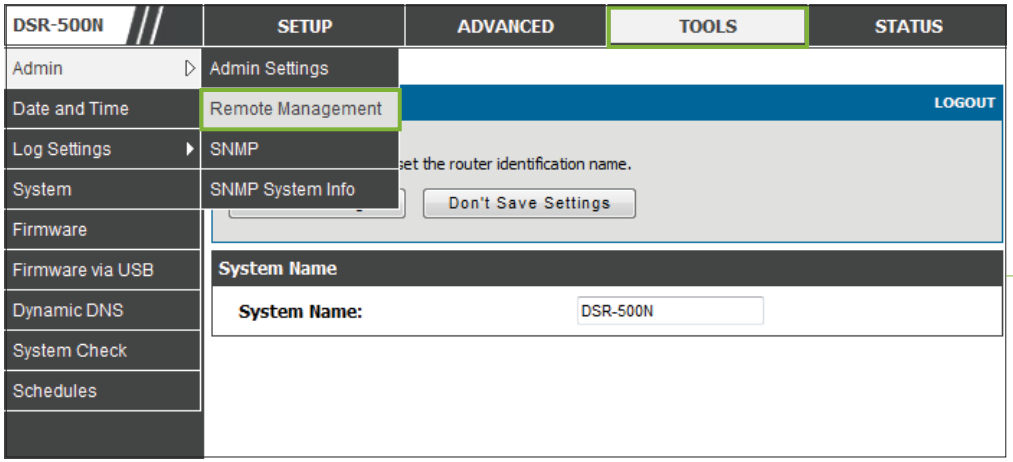
In this scenario, all application servers of headquarter are located in 192.168.10.0/24 subnet. We are going to configure DSR router which allows remote PCs to access application servers via this SSL VPN tunnel. This tunnel doesn't handle local Internet traffic of PCs in order to reduce traffic overhead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



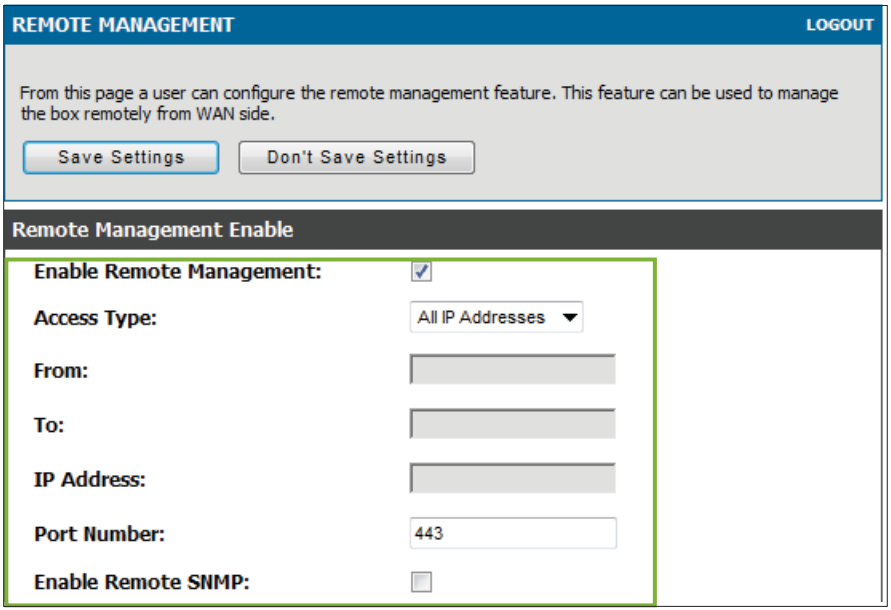
Firmware version 1.03B12_WW

Configuration Step

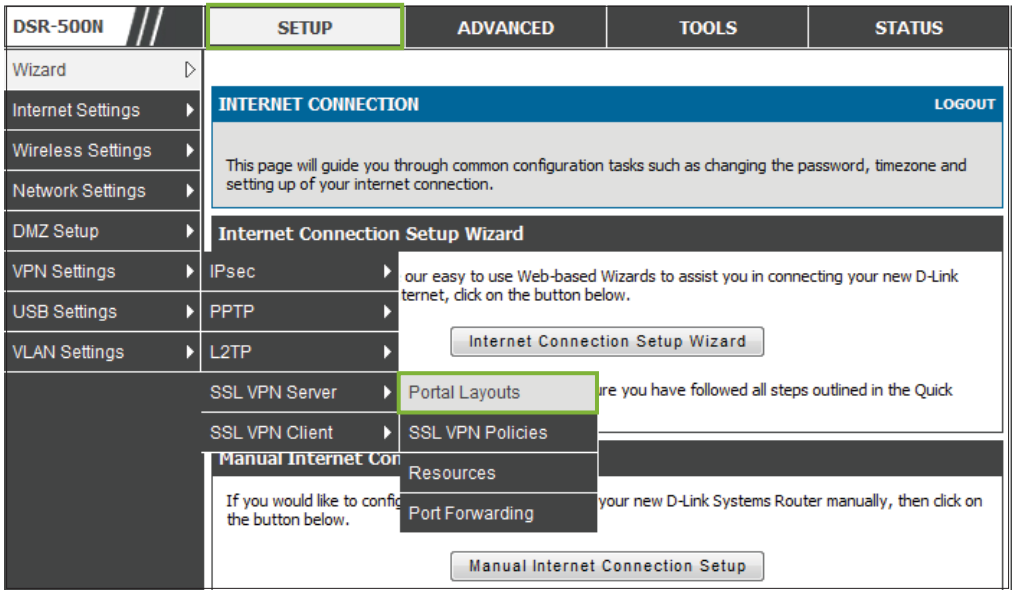
1. Before SSL configuration, please enable remote management feature via Tools -> Admin -> Remote Management.



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



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



Follow below parameter to add a portal layout.

Portal Layout Name: **test**

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

Banner Title (optional): **test**

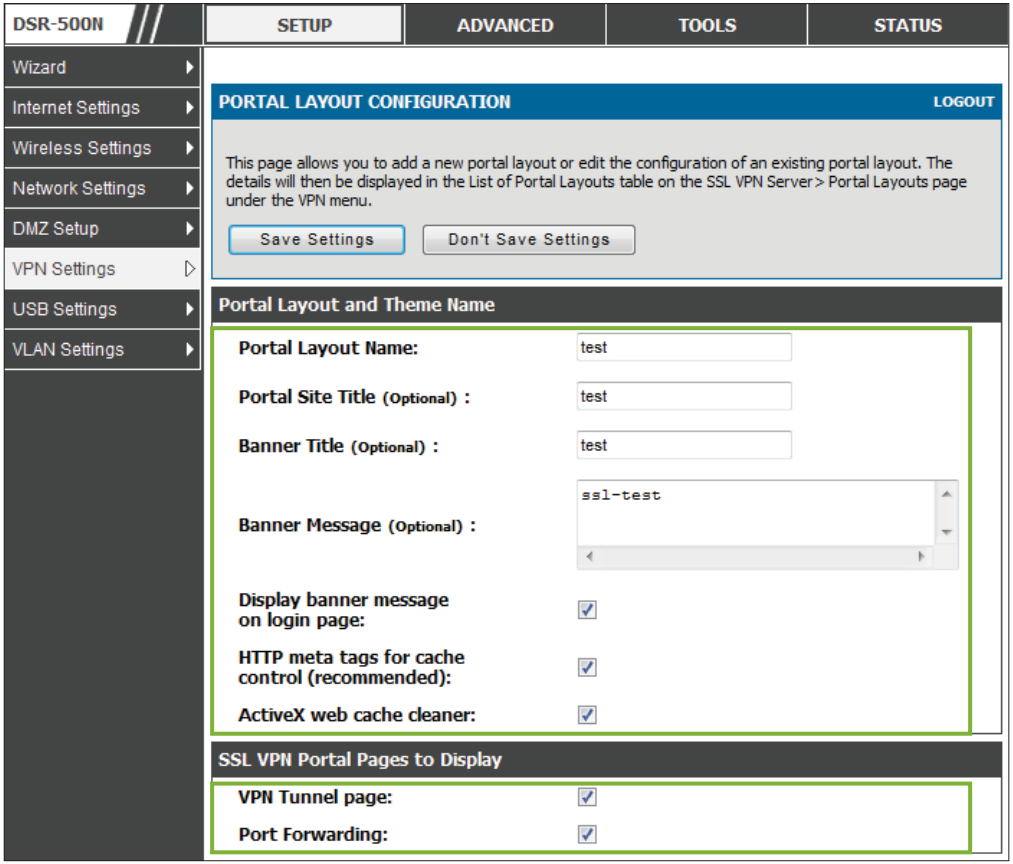
Display banner message on login page: **Enabled**

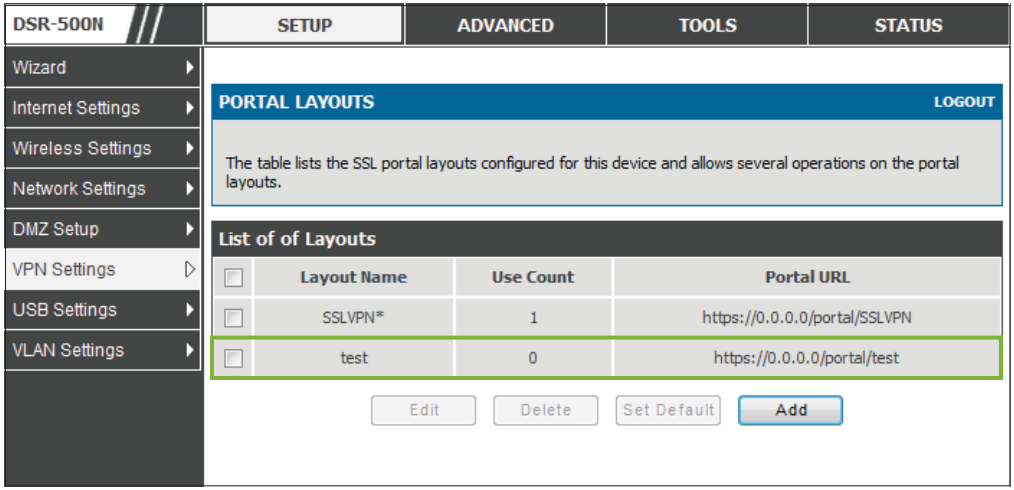
HTTP meta tags for cache control (recommended): **Enabled**

ActiveX Web cache cleaner: **Enabled**

VPN tunnel page: **Enabled**

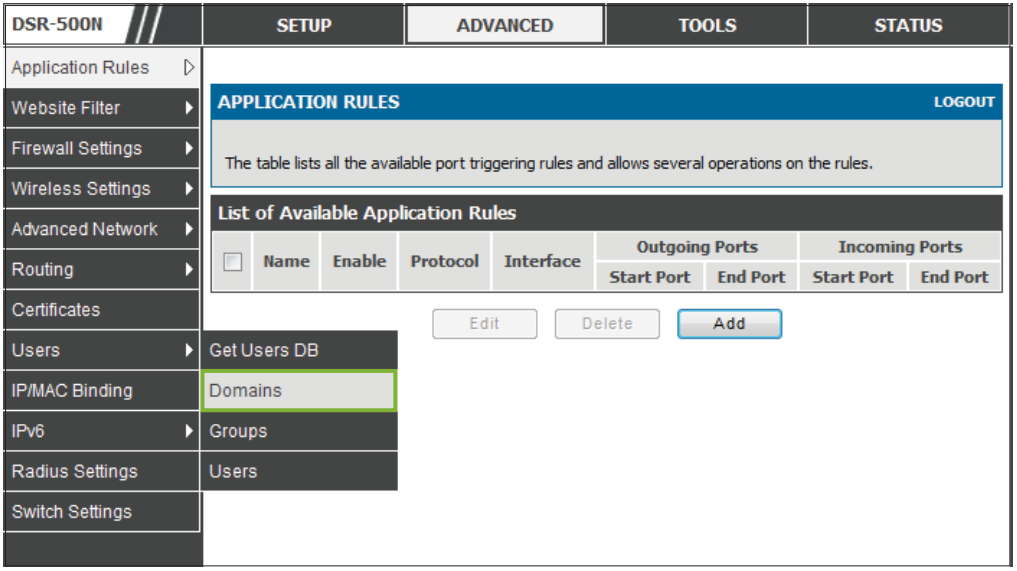
Port Forwarding: **Enabled**





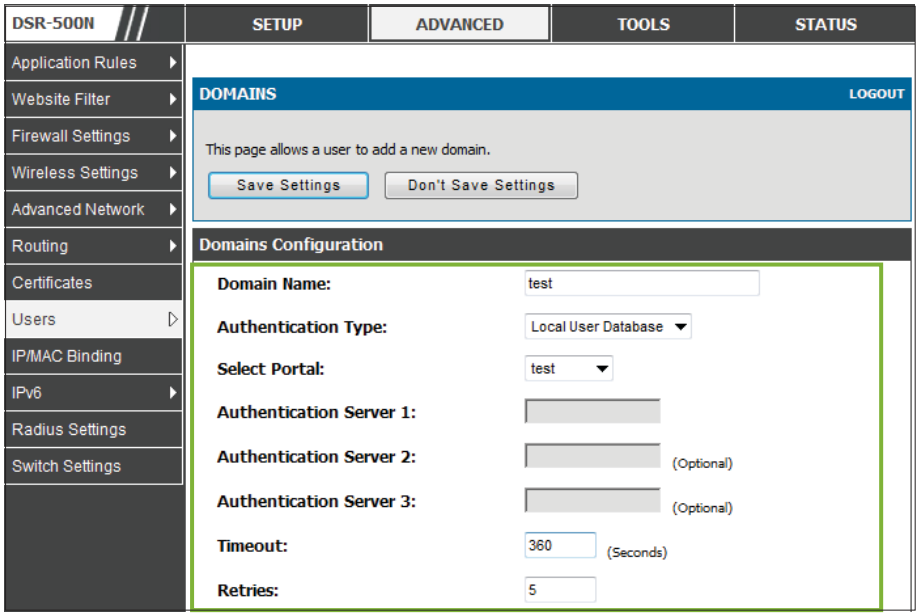
The GUI page will look like above screenshot when you finish to add a portal layout.

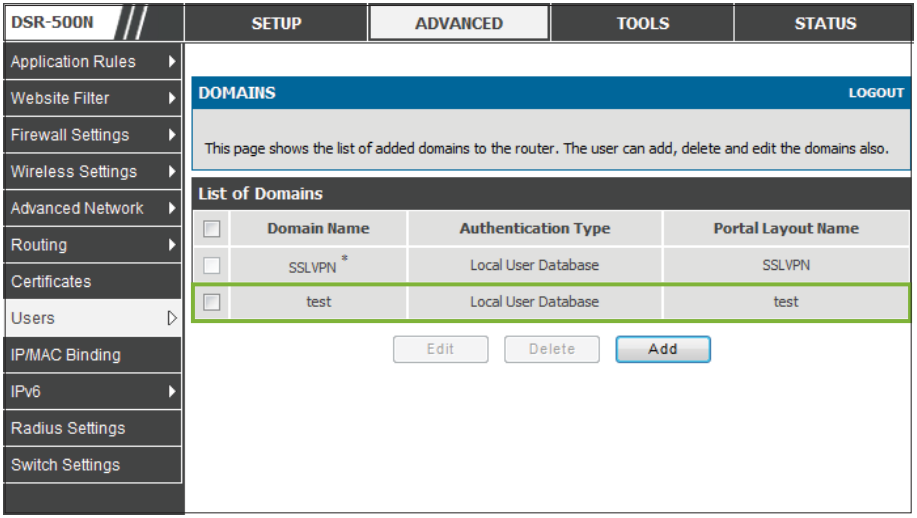
3. Go to ADVANCED -> Users -> Domains, create a new Domain for SSL VPN users.



Follow below parameters on Domains Configuration page.

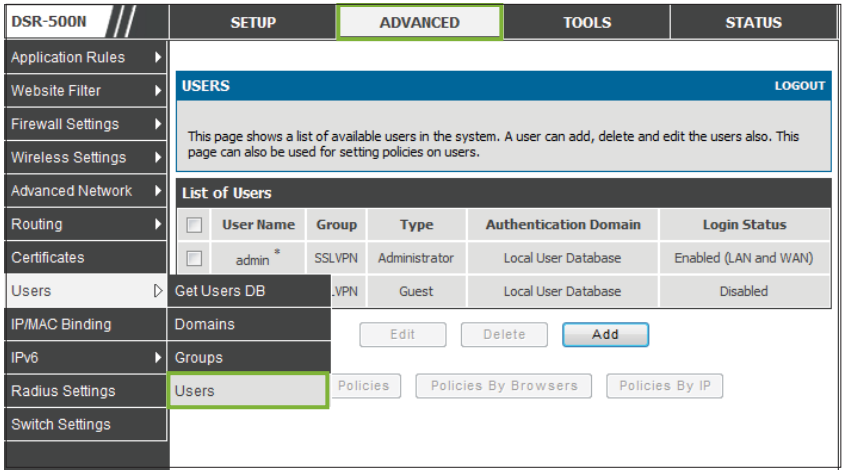
Domain name: **test**, select portal: **test**





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.



Follow below parameters on Users Configuration page:

User Name: **test1**

First Name: **test1**

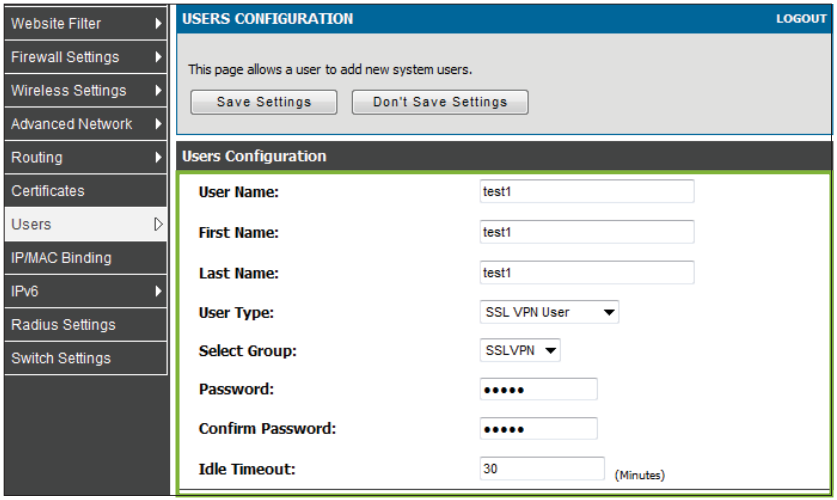
Last Name: **test1**

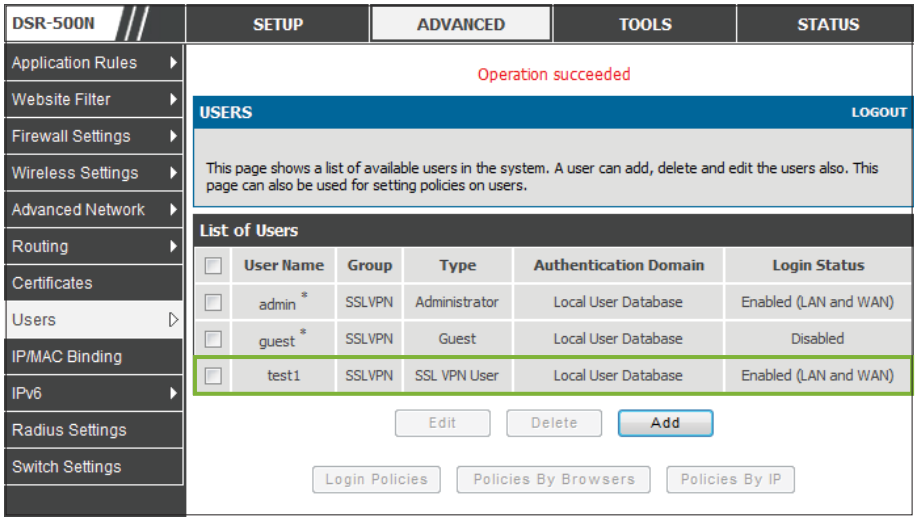
User Type: **SSL VPN user**

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

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

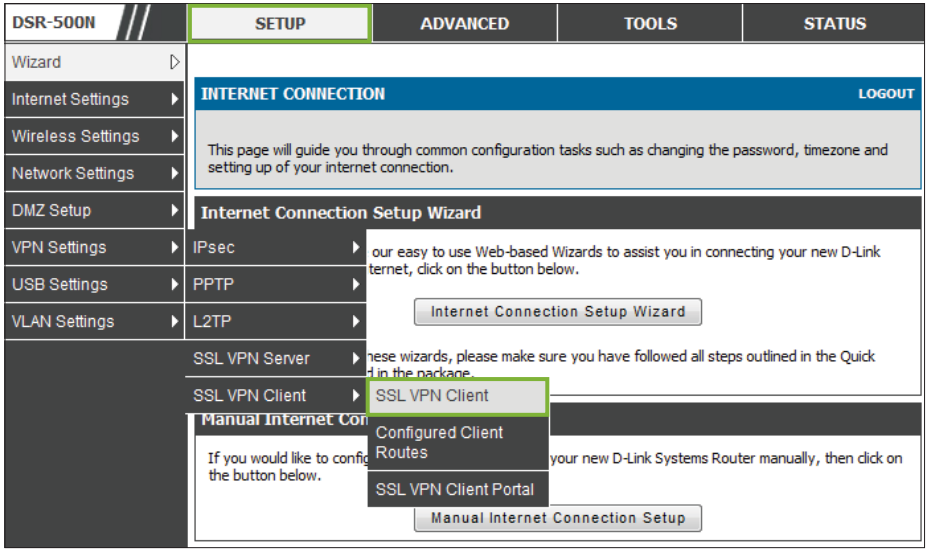
Idle Timeout: **30 Minutes**





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

5. 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 .



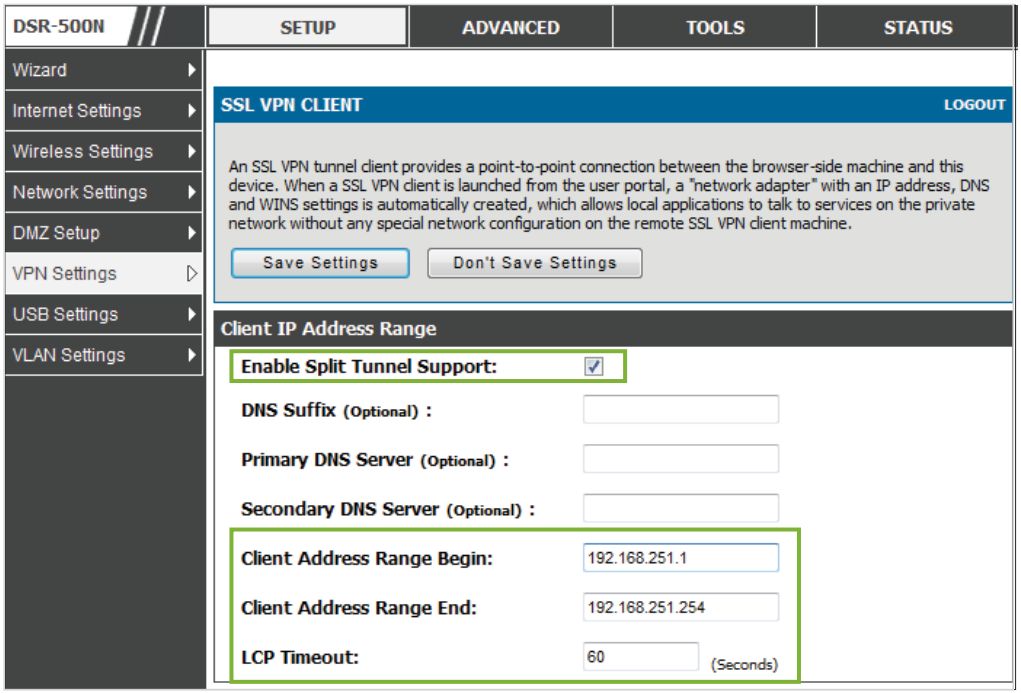
Follow below parameters to configure on SSL VPN Client page:

Enable Split Tunnel Support: **Enabled**

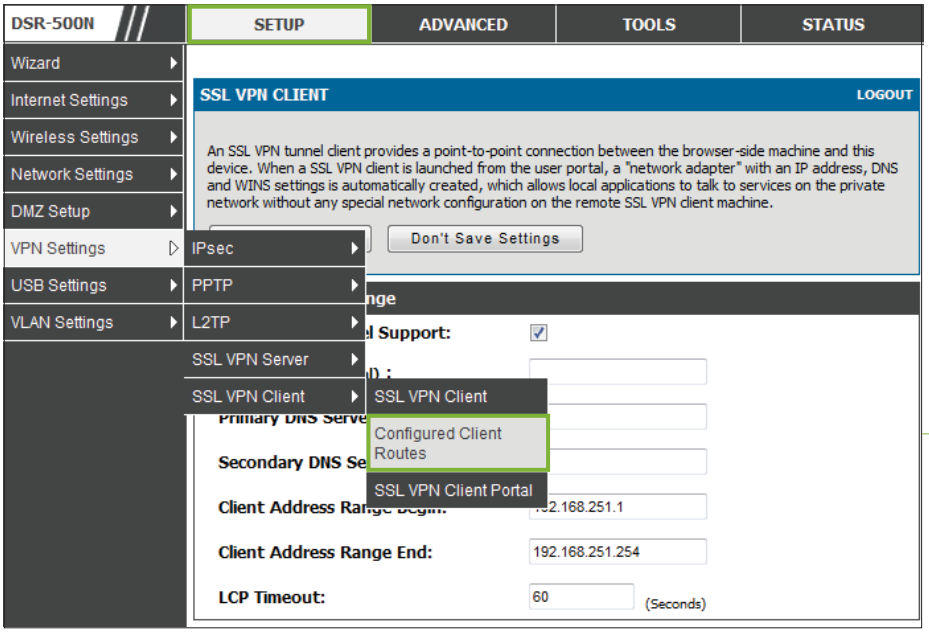
Client Address Range Begin: **192.168.251.1**

Client Address Range end: **192.168.251.254**

LCP Timeout: **60 Minutes**



6. 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.

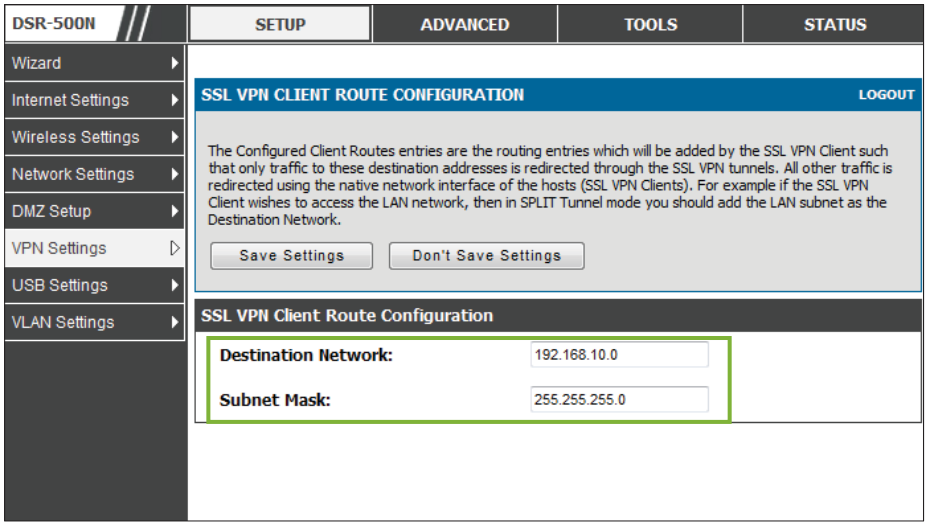


Note: DSR router would not allow you to add Client Routes if you didn't enable the Split Tunnel Support at previous step.

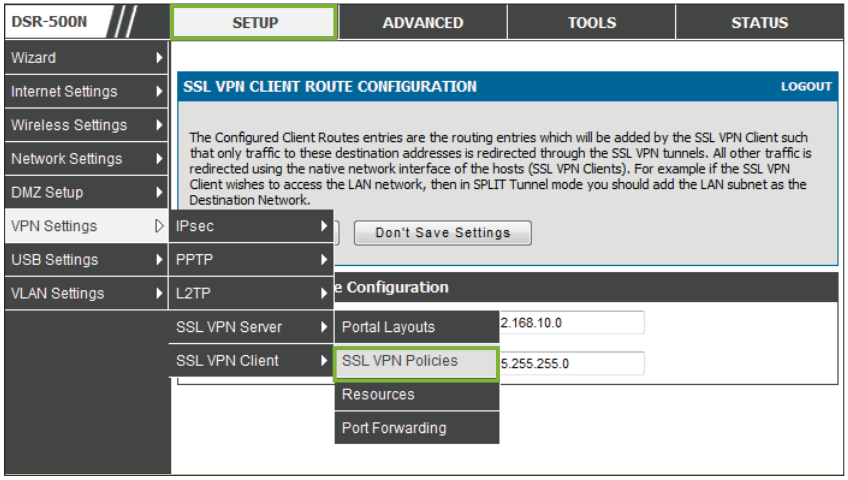
Following parameters are routing information of remote network for SSL VPN client.

Destination Network: **192.168.10.0**

Subnet Mask: **255.255.255.0**



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**

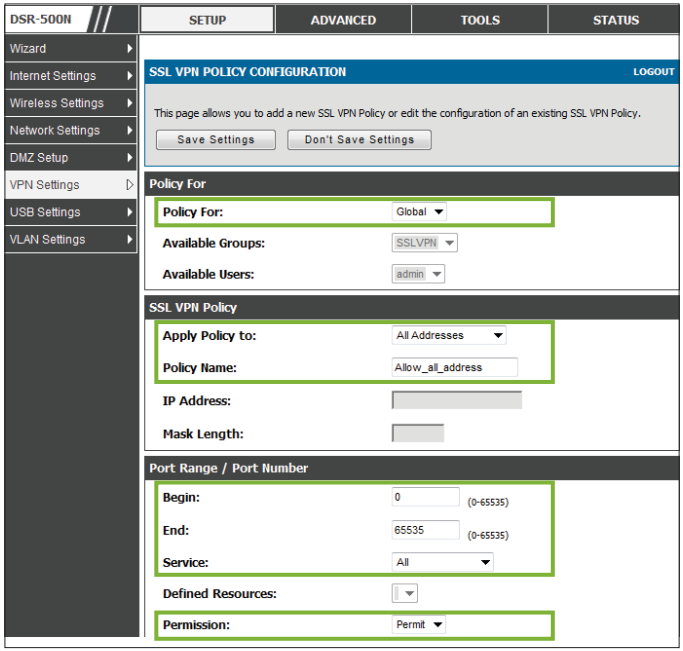
Policy Name: **Allow_all_address**

Begin: **0**

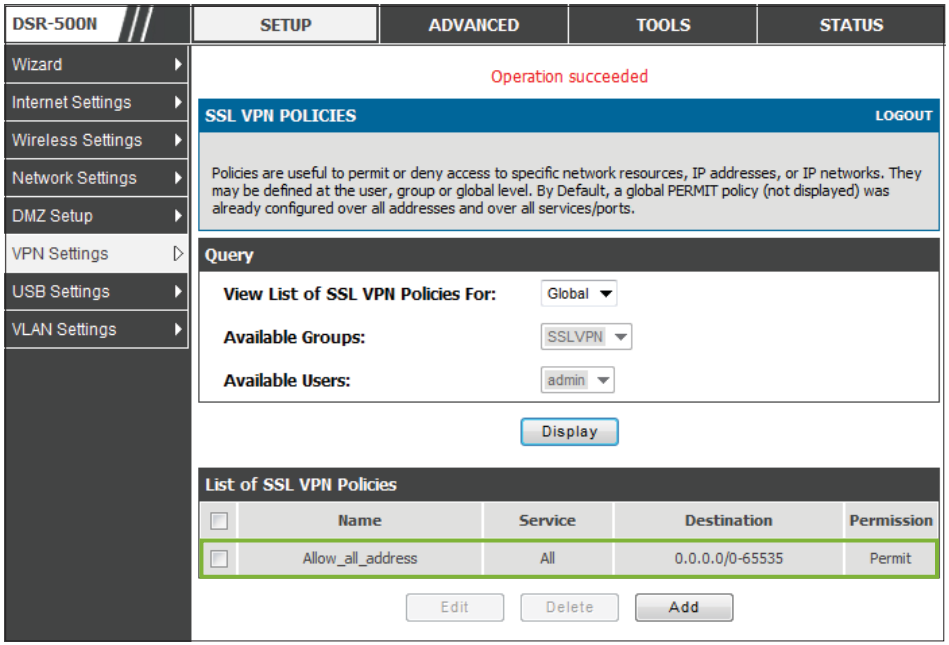
End: **65535**

Service: **All**

Permission: **Permit**

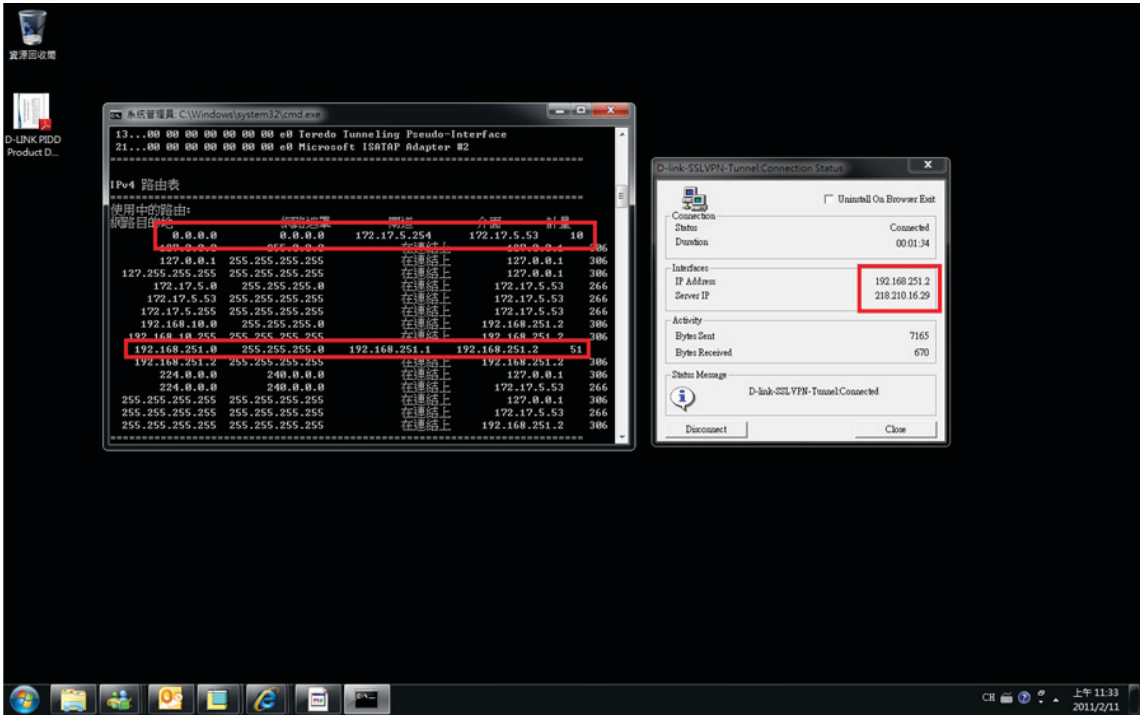


When you click save settings, a SSL VPN policy has been created like following screenshot.



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.


資源回收筒
D-LINK PIDD Product D...
系統管理員: C:\Windows\system32\cmd.exe
13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
21...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
IPv4 路由表
使用中的路由:
0.0.0.0 0.0.0.0 172.17.5.254 172.17.5.53 10
127.0.0.1 255.255.255.255 在連結上 127.0.0.1 306
127.255.255.255 255.255.255.255 在連結上 127.0.0.1 306
172.17.5.0 255.255.255.0 在連結上 172.17.5.53 266
172.17.5.53 255.255.255.255 在連結上 172.17.5.53 266
172.17.5.255 255.255.255.255 在連結上 172.17.5.53 266
192.168.10.0 255.255.255.0 在連結上 192.168.251.2 306
192.168.251.0 255.255.255.0 192.168.251.1 192.168.251.2 51
192.168.251.2 255.255.255.255 在連結上 192.168.251.2 306
224.0.0.0 240.0.0.0 在連結上 127.0.0.1 306
224.0.0.0 240.0.0.0 在連結上 172.17.5.53 266
255.255.255.255 255.255.255.255 在連結上 127.0.0.1 306
255.255.255.255 255.255.255.255 在連結上 172.17.5.53 266
255.255.255.255 255.255.255.255 在連結上 192.168.251.2 306
D-link-SSLVPN-TunnelConnection Status
Uninstall On Browser Exit
Connection
Status Connected
Duration 00:01:34
Interfaces
IP Address 192.168.251.2
Server IP 218.210.16.29
Activity
Bytes Sent 7165
Bytes Received 670
Status Message
D-link-SSLVPN-TunnelConnected
Disconnect
Close
CH 上午 11:33 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.