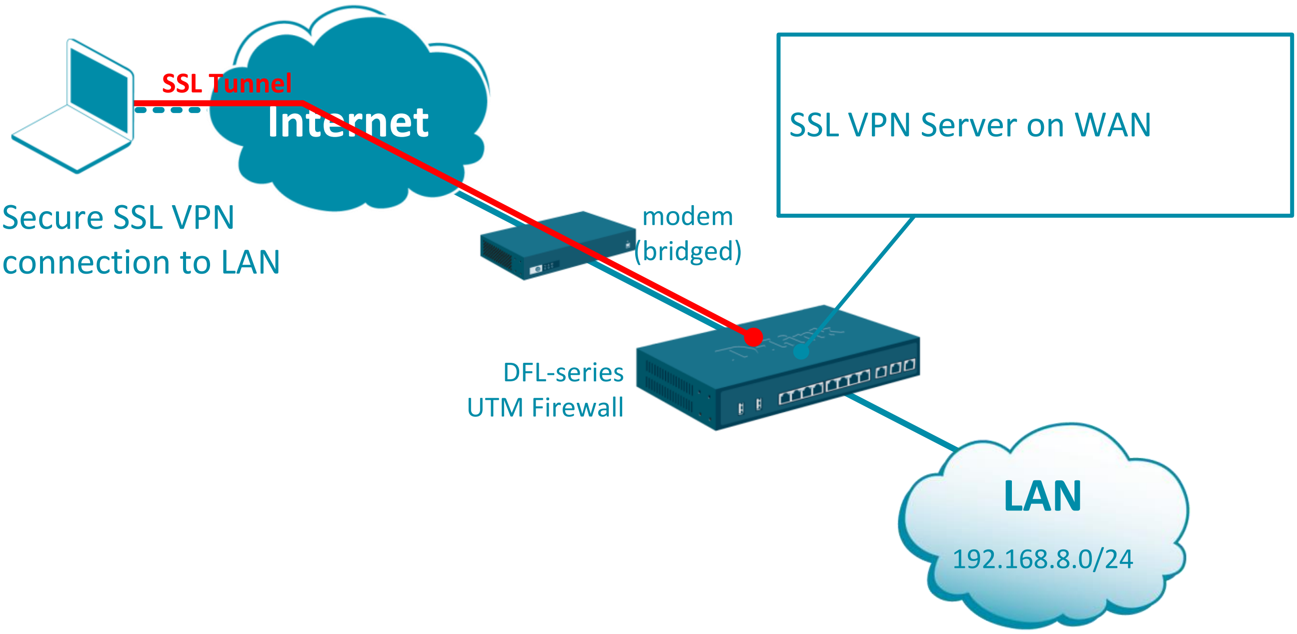
Configuration examples for the D-Link NetDefend Firewall series

Setting up SSL Server for remote access to LAN

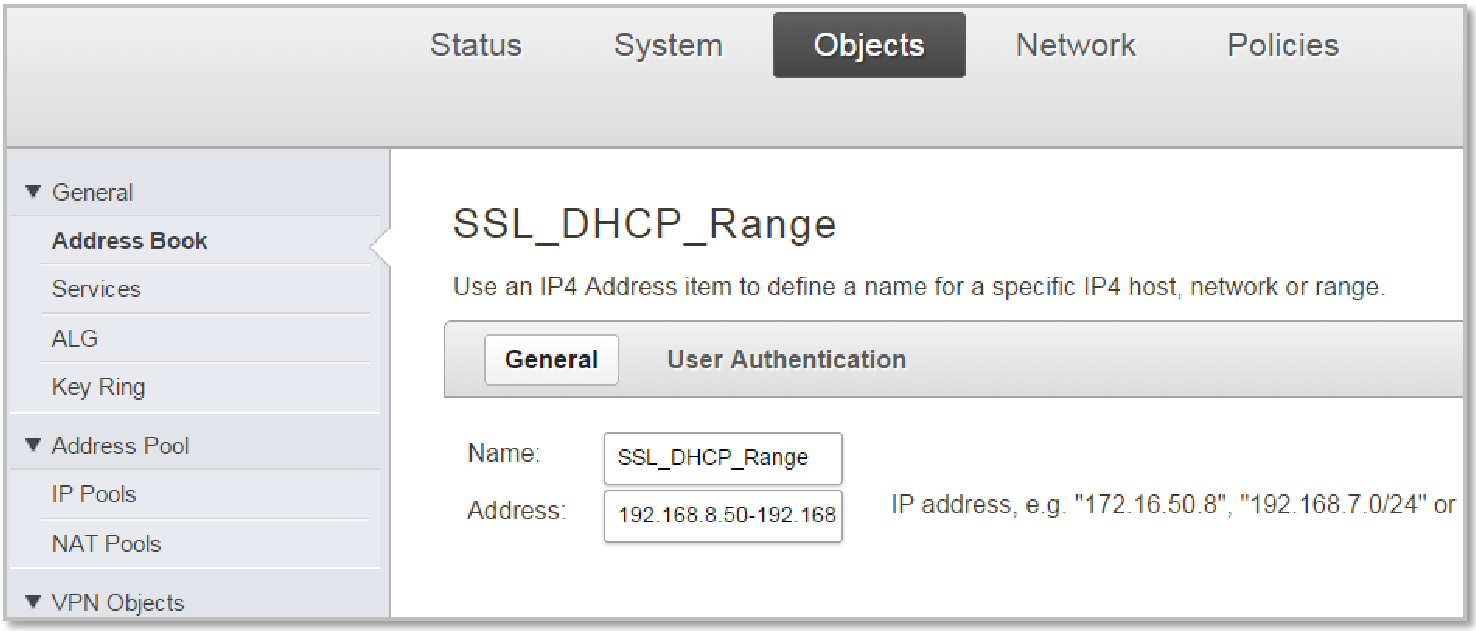
This configuration example is based on the following setup:



Step 1. Log into the firewall. The default access to LAN is via https://192.168.10.1. Default username is “admin” and password is “admin”.

Step 2. Set your firewall’s WAN settings as per Internet provider requirements.
In our example WAN is set with a static IP address.

Step 3. Add a new object into the Address Book: “SSL IP Range”.
Specify the range of IP addresses which will be assigned to the clients connecting via SSL. These addresses should be from the IP subnet used on your LAN. Make sure this range does not conflict with the range used by the DHCP Server on your LAN.



SSL_DHCP_Range

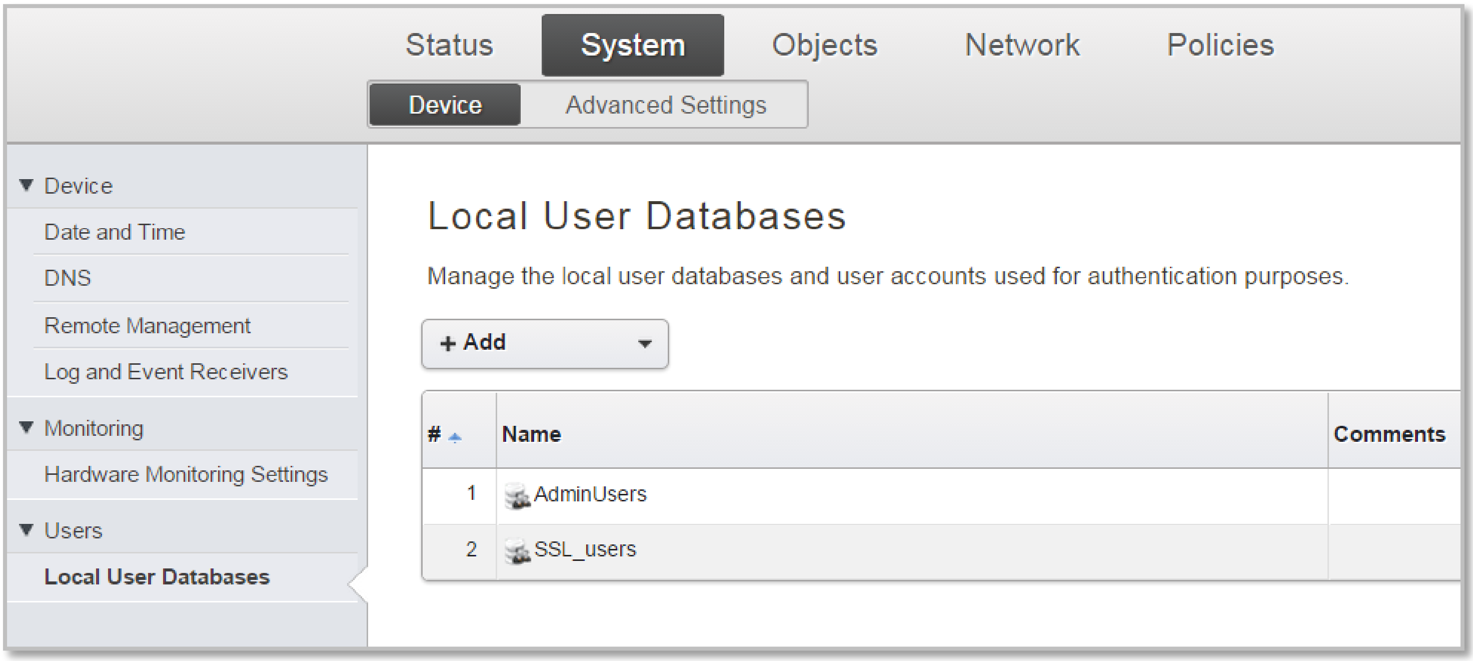
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: SSL_DHCP_Range

Address: 192.168.8.50-192.168

IP address, e.g. "172.16.50.8", "192.168.7.0/24" or

Step 4. Go to System > Device > Local User Databases.
Add new Local User Database for the SSL users.

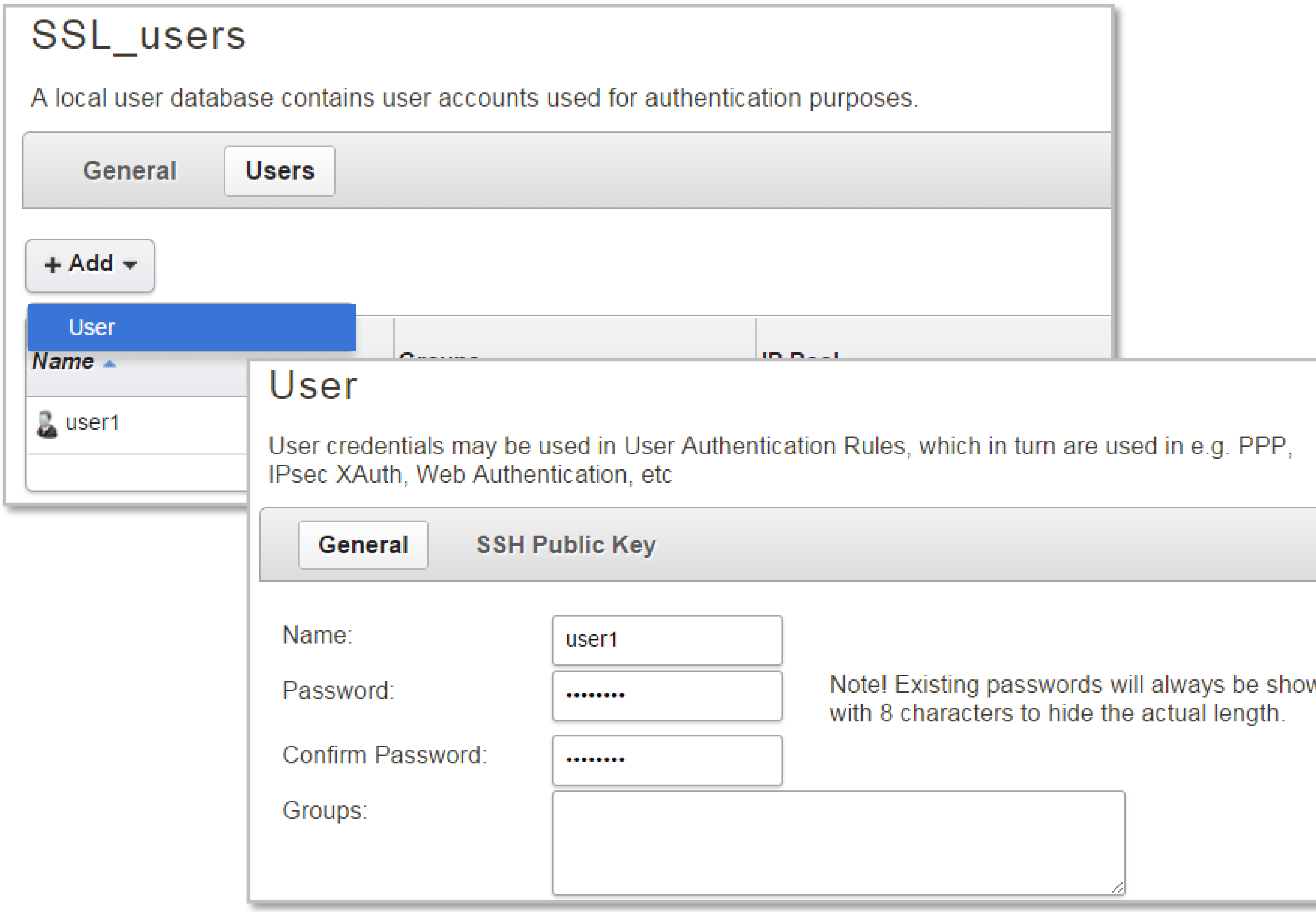


Local User Databases

Manage the local user databases and user accounts used for authentication purposes.

#	Name	Comments
1	AdminUsers	
2	SSL_users	

Open the newly created User Database and add your VPN users. Specify Username and Password for each remote user.



SSL_users

A local user database contains user accounts used for authentication purposes.

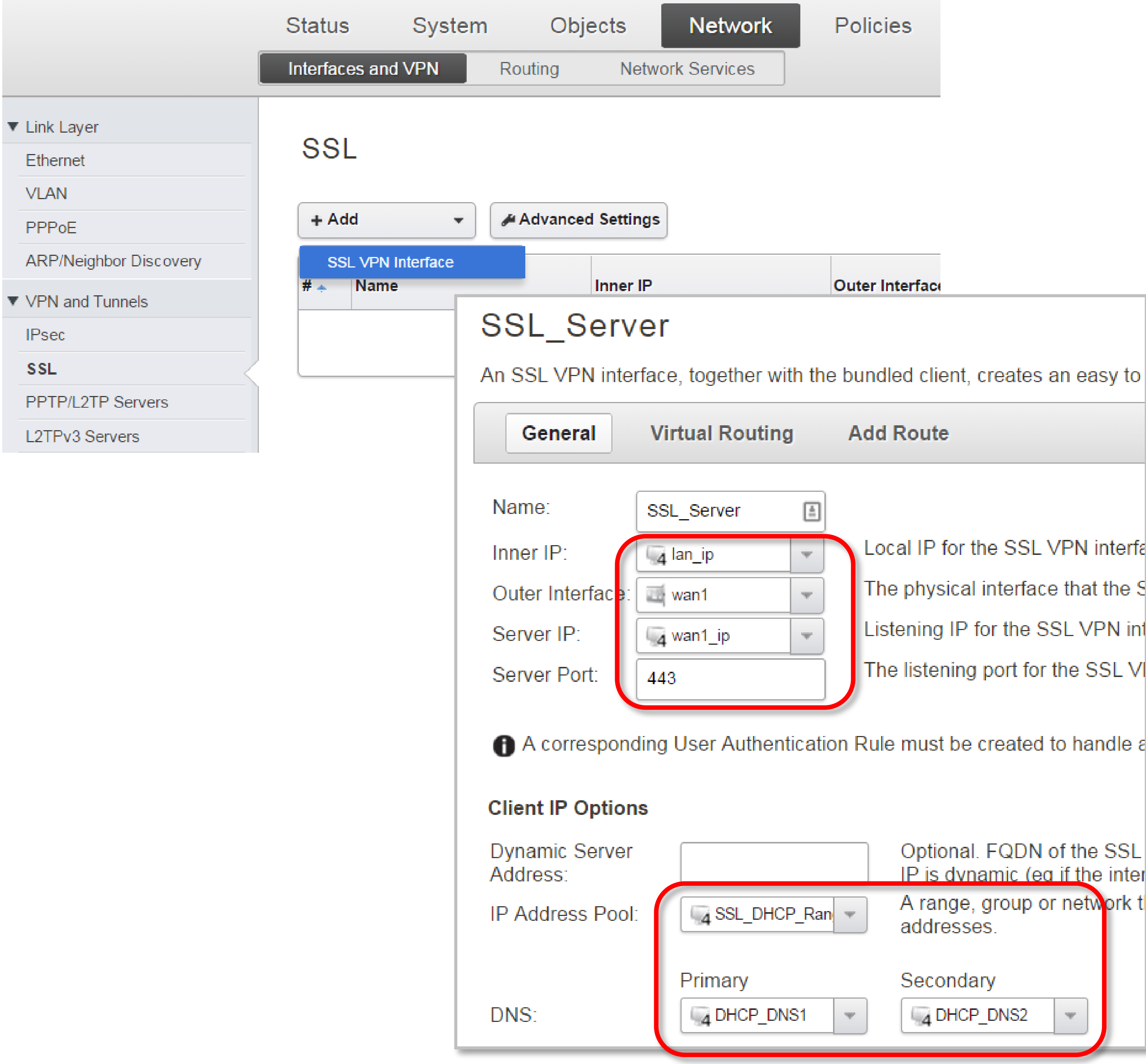
User

User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authentication, etc

Name:	user1
Password:	••••••••
Confirm Password:	••••••••
Groups:	

Note! Existing passwords will always be show with 8 characters to hide the actual length.

Step 5. Go to Network> SSL. Add a new SSL VPN Interface.
Inner IP Address – set as "LAN_IP".
Outer Interface – "WAN" (or if WAN is set with PPPoE select the PPPoE interface).
Server Port – set as "443" (i.e. access via HTTPS).
Specify the IP address pool and DNS assignment for SSL users.



SSL_Server

An SSL VPN interface, together with the bundled client, creates an easy to

Name: SSL_Server

Inner IP: lan_ip — Local IP for the SSL VPN interfa

Outer Interface: wan1 — The physical interface that the S

Server IP: wan1_ip — Listening IP for the SSL VPN int

Server Port: 443 — The listening port for the SSL V

A corresponding User Authentication Rule must be created to handle a

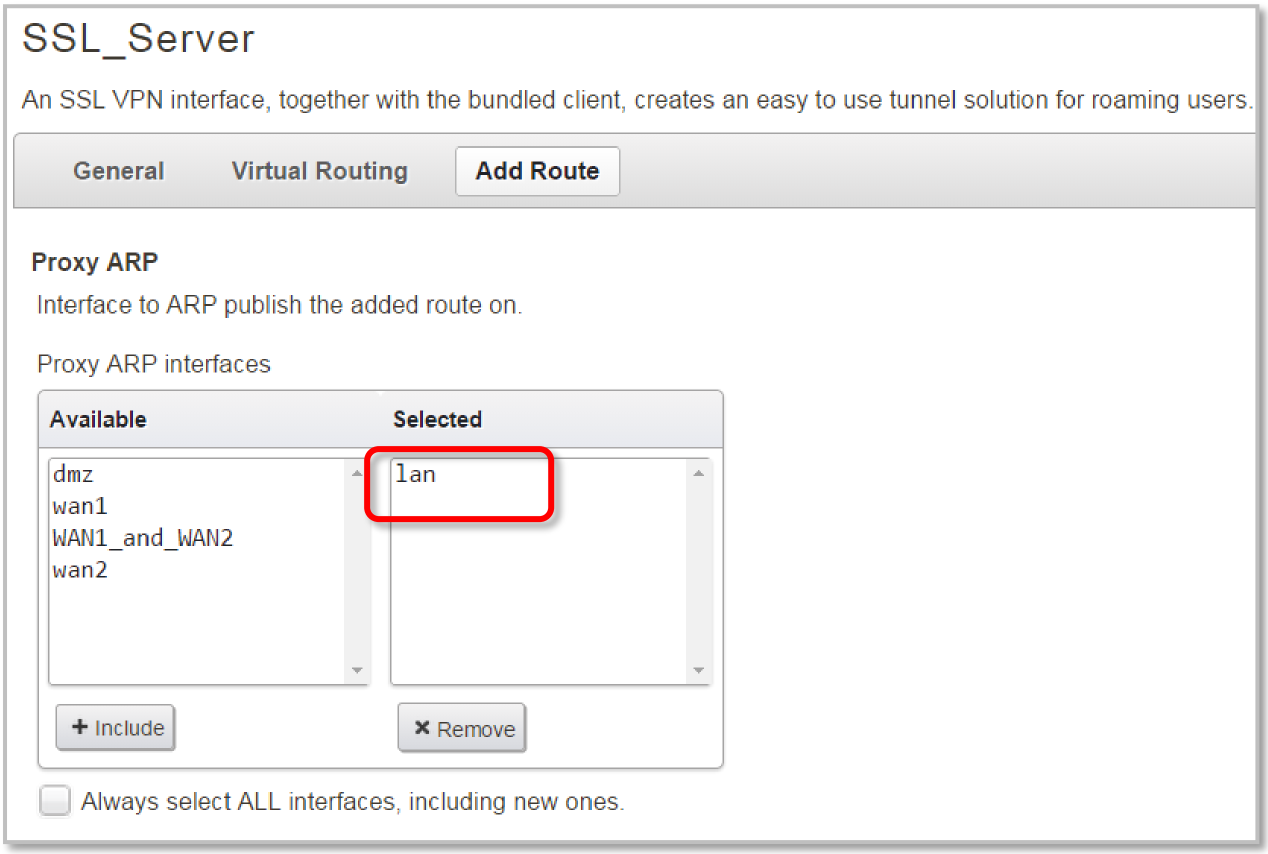
Client IP Options

Dynamic Server Address: — Optional. FQDN of the SSL IP is dynamic (eg if the inter

IP Address Pool: SSL_DHCP_Ran — A range, group or network t addresses.

DNS: Primary DHCP_DNS1 — Secondary DHCP_DNS2

Click on the **Add Route** tab and add “LAN” interface under Proxy ARP.



SSL_Server

An SSL VPN interface, together with the bundled client, creates an easy to use tunnel solution for roaming users.

Proxy ARP

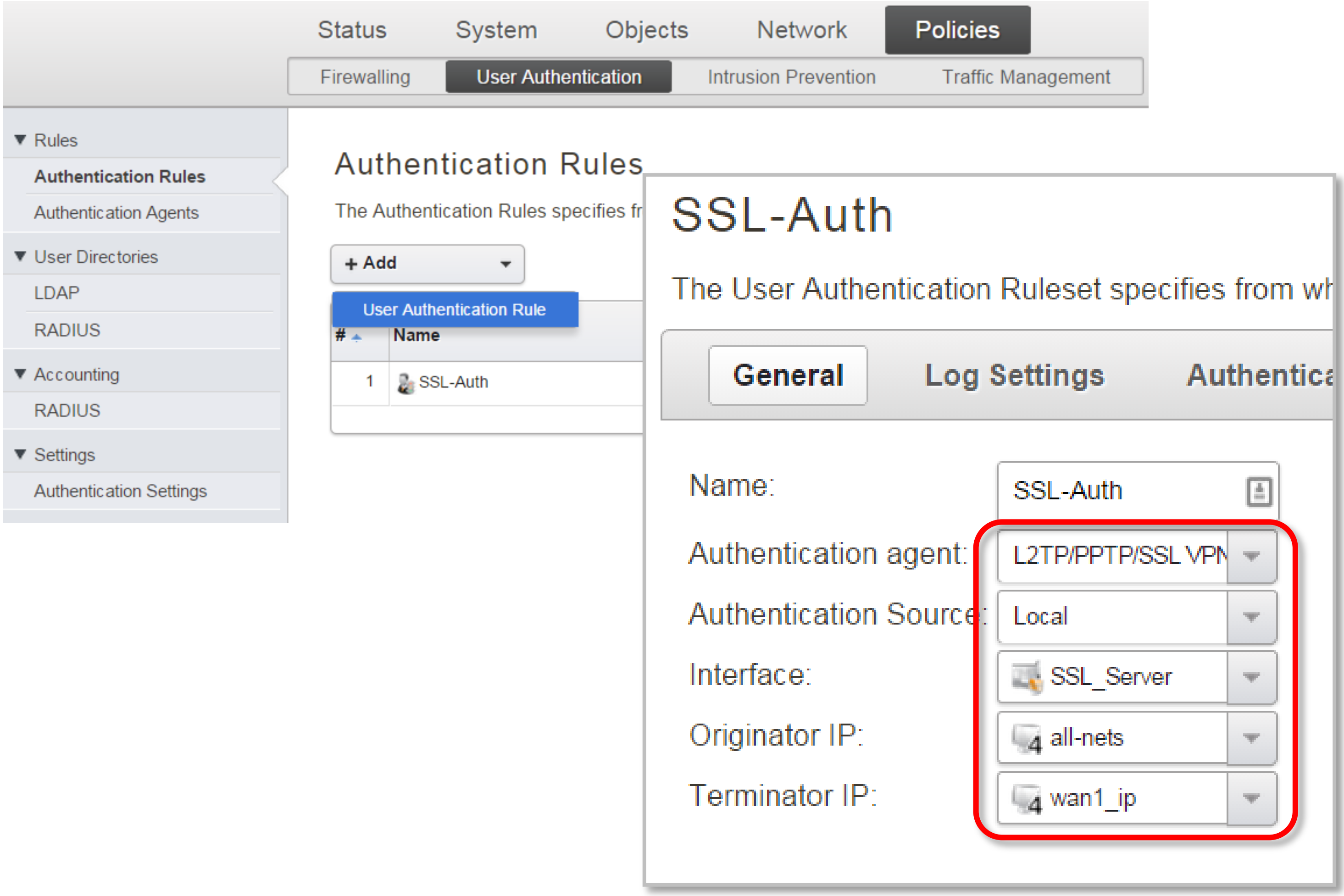
Interface to ARP publish the added route on.

Proxy ARP interfaces

Available	Selected
dmz wan1 WAN1_and_WAN2 wan2	lan

□ Always select ALL interfaces, including new ones.

Step 6. Go to Policies > User Authentication > User Authentication Rules. Add a new rule. Set Agent as “L2TP/PPTP/SSL”, Authentication as “Local”, Interface – “SSL-Server”.



SSL-Auth

The User Authentication Ruleset specifies from wh

Name: SSL-Auth

Authentication agent: L2TP/PPTP/SSL VPN

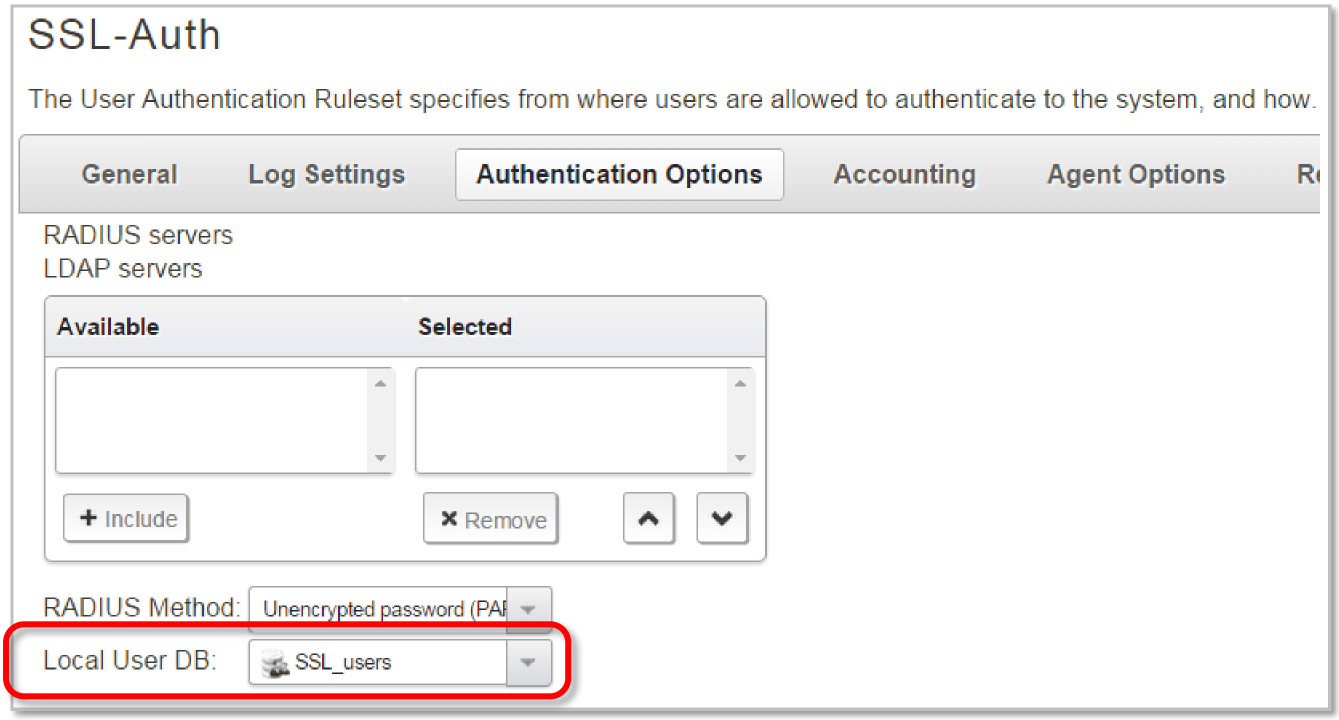
Authentication Source: Local

Interface: SSL_Server

Originator IP: all-nets

Terminator IP: wan1_ip

Click on the **Authentication Options** tab. Make sure that under Local User DB you have your User Database selected.



SSL-Auth

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

RADIUS servers

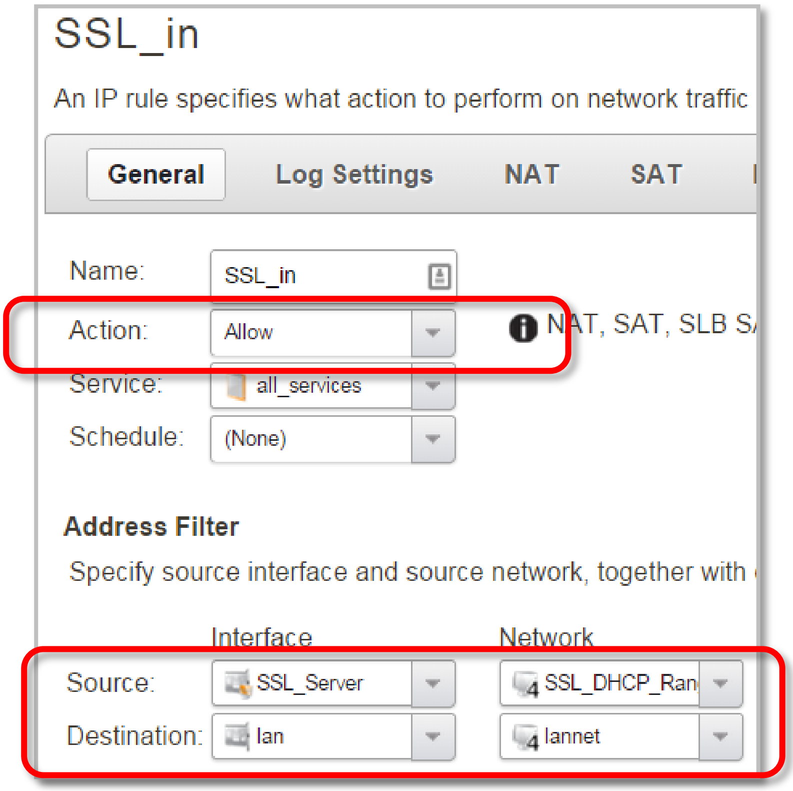
LDAP servers

RADIUS Method: Unencrypted password (PAP

Local User DB: SSL_users

Step 7. Go to Policies > Main IP Rules. Create two IP Rules:

1. To allow SSL users to communicate with LAN (Allow rule).
2. To allow SSL users to access the Internet through the firewall (NAT rule).



SSL_in

An IP rule specifies what action to perform on network traffic

Name: SSL_in

Action: Allow

NAT, SAT, SLB S

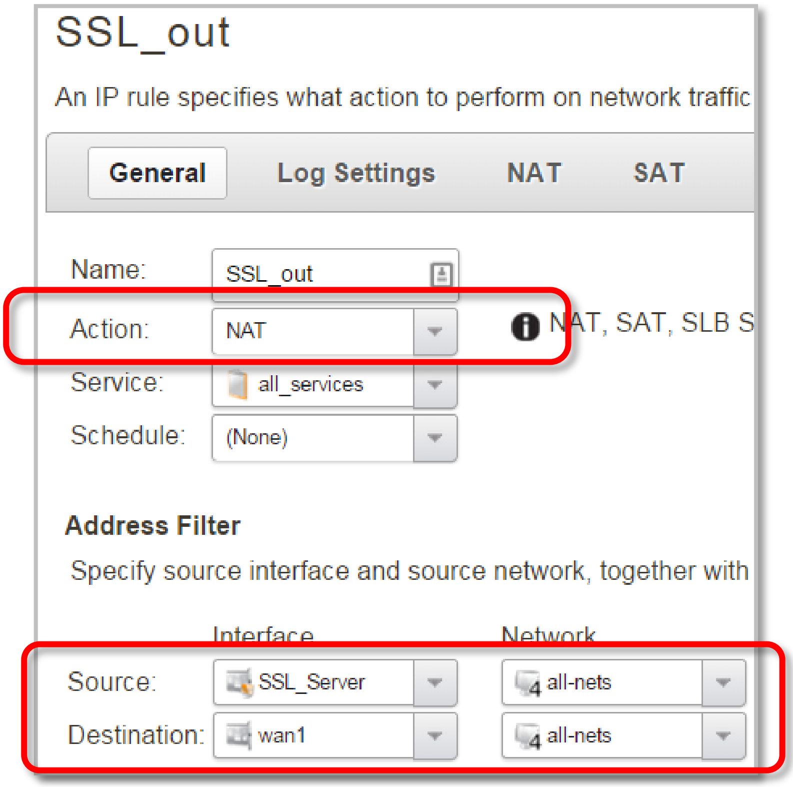
Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, together with

	Interface	Network
Source:	SSL_Server	SSL_DHCP_Ran
Destination:	lan	lannet



SSL_out

An IP rule specifies what action to perform on network traffic

Name: SSL_out

Action: NAT

NAT, SAT, SLB S

Service: all_services

Schedule: (None)

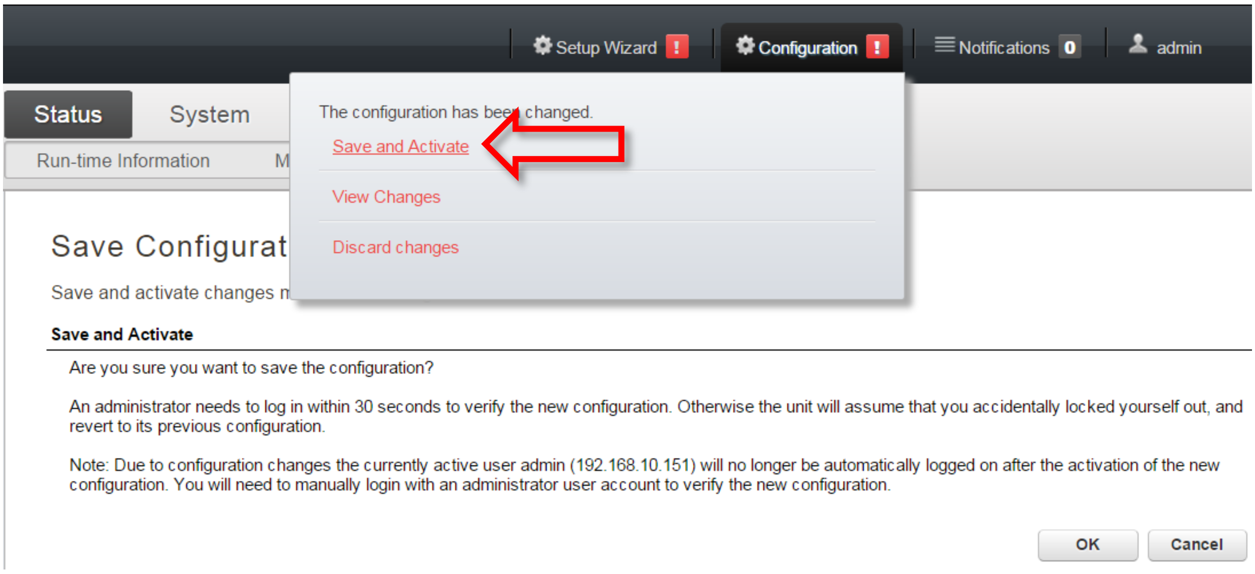
Address Filter

Specify source interface and source network, together with

	Interface	Network
Source:	SSL_Server	all-nets
Destination:	wan1	all-nets

Step 8. After the configuration is done, click “Configuration” in main bar and select “Save and Activate”. Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.

NOTE: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.



The configuration has been changed.

Save Configurat

Save and activate changes m

Save and Activate

Are you sure you want to save the configuration?

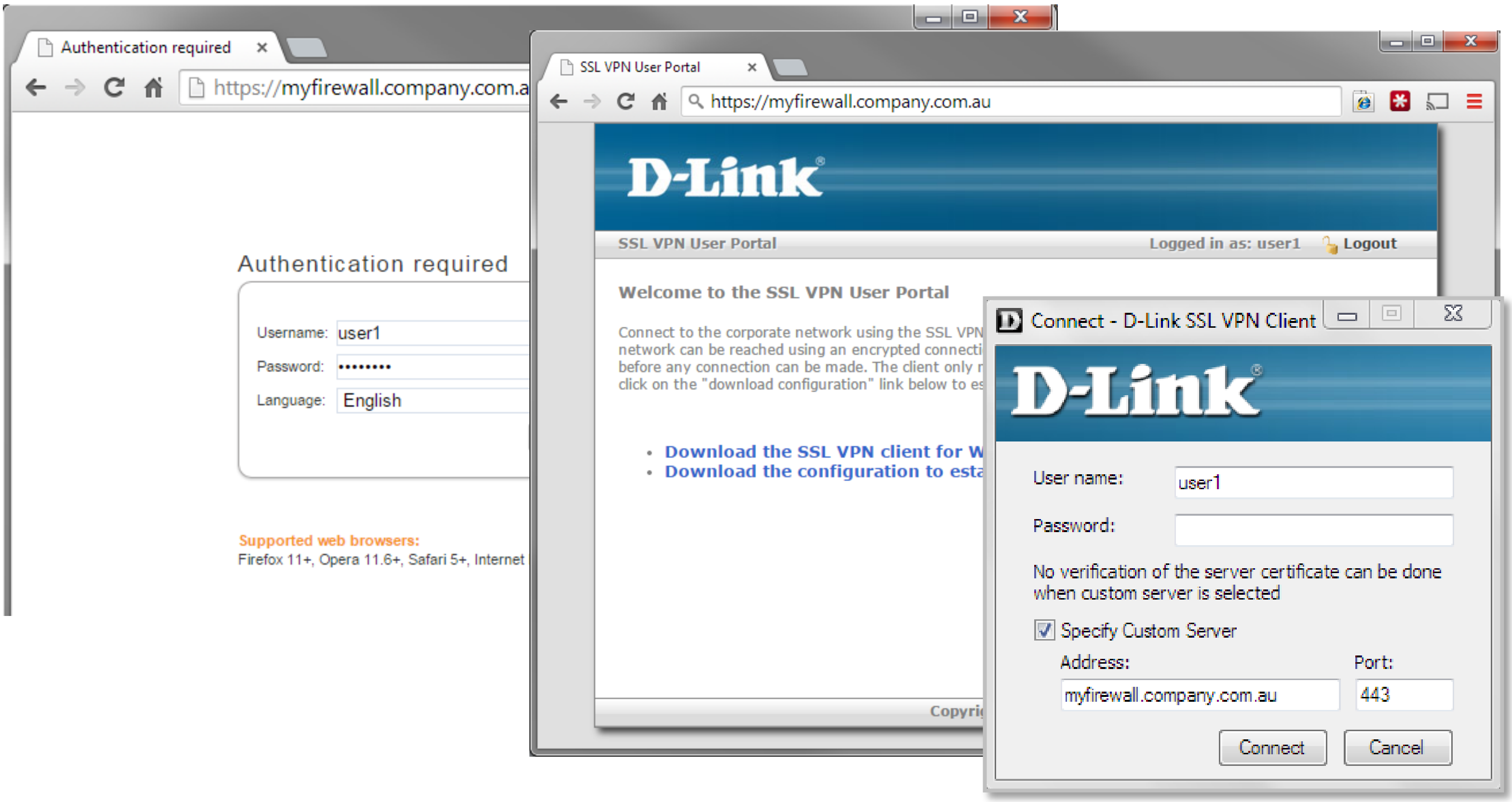
An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Note: Due to configuration changes the currently active user admin (192.168.10.151) will no longer be automatically logged on after the activation of the new configuration. You will need to manually login with an administrator user account to verify the new configuration.

To connect via SSL VPN a Remote User needs to open a Web Browser and type in the firewall’s WAN address or URL (https://myfirewall.company.com).

Login using SSL username/password.

Download thin SSL client and connect via SSL.



https://myfirewall.company.com.a

Authentication required

Username: user1

Password: ••••••••

Language: English

Supported web browsers:
Firefox 11+, Opera 11.6+, Safari 5+, Internet

https://myfirewall.company.com.au

Logged in as: user1

Welcome to the SSL VPN User Portal

Connect to the corporate network using the SSL VPN network can be reached using an encrypted connecti before any connection can be made. The client only r click on the "download configuration" link below to es

- Download the SSL VPN client for W
- Download the configuration to esta

User name: user1

Password:

No verification of the server certificate can be done when custom server is selected

☑ Specify Custom Server

Address: myfirewall.company.com.au

Port: 443