SSL VPN SecuExtender (4.0.0.1)

Supported Devices

ZyWALL 110 – Running firmware version 4.20 and newer
ZyWALL 310 – Running firmware version 4.20 and newer
ZyWALL 1100 – Running firmware version 4.20 and newer
USG40 – Running firmware version 4.20 and newer
USG40W – Running firmware version 4.20 and newer
USG60 – Running firmware version 4.20 and newer
USG60W – Running firmware version 4.20 and newer
USG110 – Running firmware version 4.20 and newer
USG210 – Running firmware version 4.20 and newer
USG310 – Running firmware version 4.20 and newer
USG1100 – Running firmware version 4.20 and newer
USG1900 – Running firmware version 4.20 and newer
USG20-VPN – Running firmware version 4.16 and newer
USG20W-VPN – Running firmware version 4.16 and newer

Supported Platforms

Windows XP
Windows 7 (32-bit and 64-bit)
Windows 8/8.1 (32-bit and 64-bit)
Windows 10 (32-bit and 64-bit)

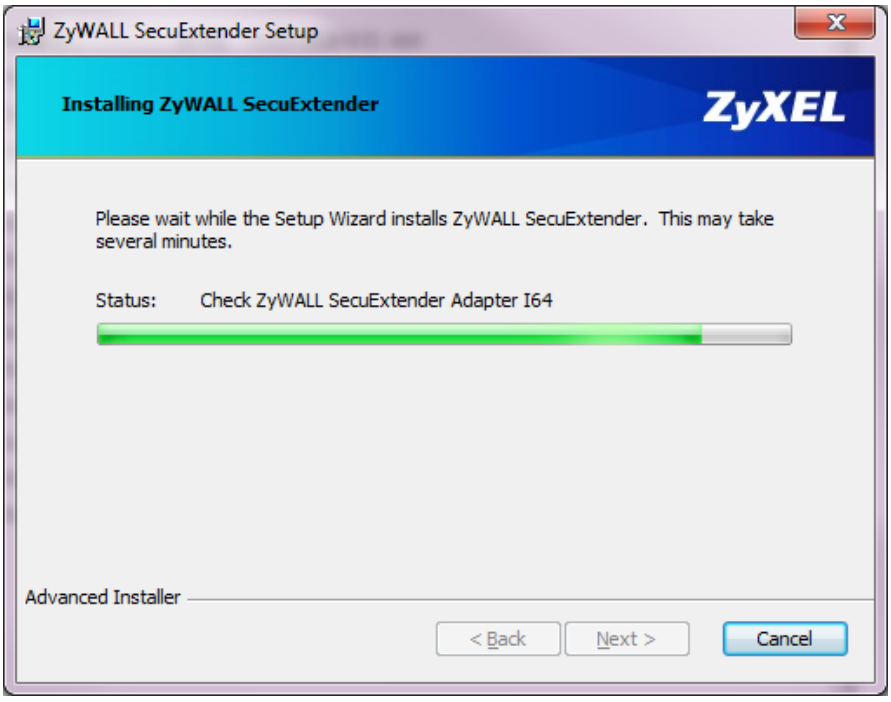
Overview

The SecuExtender client (4.0.0.1) is a tool used to establish an SSL VPN connection between a client PC and a ZyXEL security appliance. Once connected the user has access over the security appliance local network or can send all traffic, including internet, through the tunnel

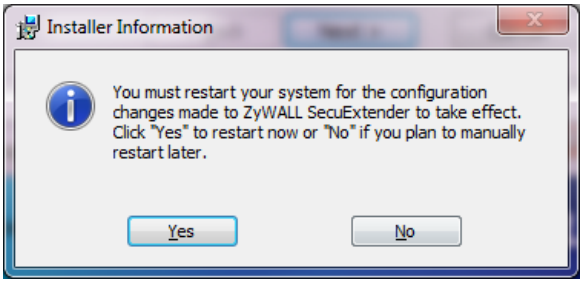
(depending on SSL VPN rule setup).

Installing SecuExtender

Please download the SecuExtender 4.0.0.1 client version from ftp://ftp.zyxel.com/SecuExtender/software/ to install on a compatible platform. Because different computer systems and user accounts have different permissions, it is recommended that the client be installed using an administrator account which has a higher privilege. Right-Click the SecuExtender installer and select "Run as administrator" to run the installation wizard.



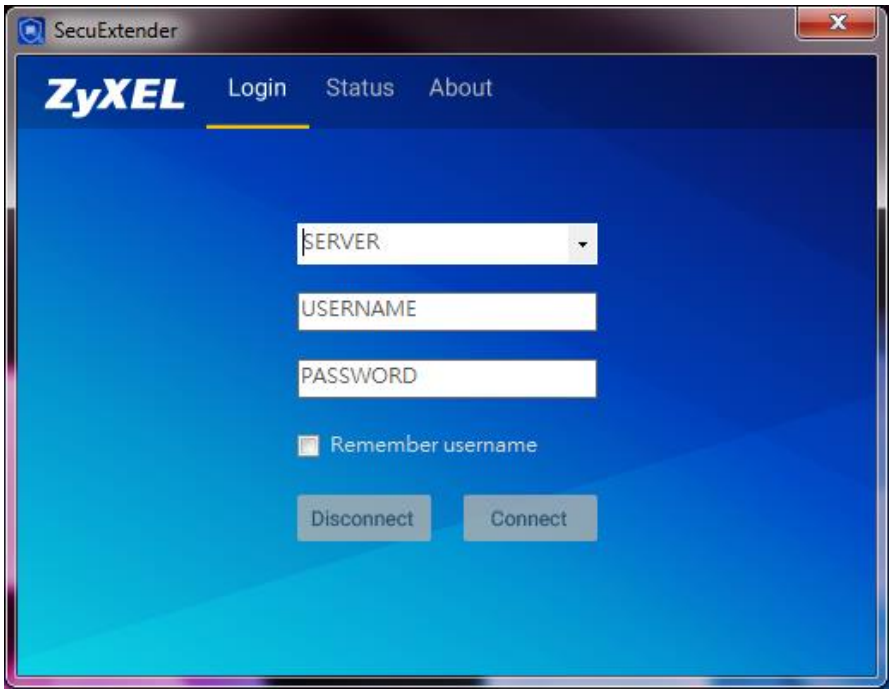
After the installation is complete the computer will need to be rebooted to finish installing all components necessary by the SecuExtender client. When the pop-up below appears (after installation wizard is complete) please click the **Yes** button to restart the computer.



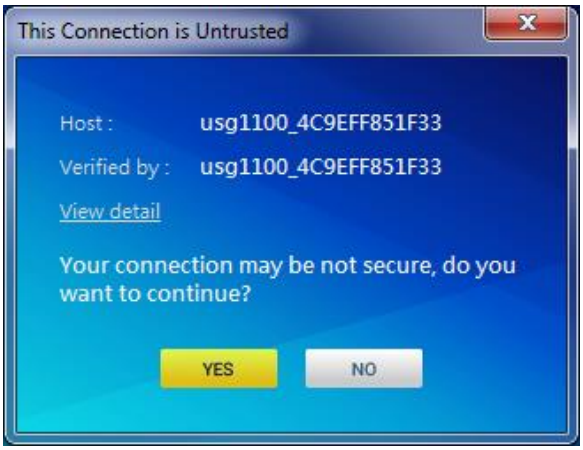
SecuExtender Client

Launch the SecuExtender client to establish an SSL VPN connection to a compatible ZyXEL appliance. Provide the following info to initiate the connection.

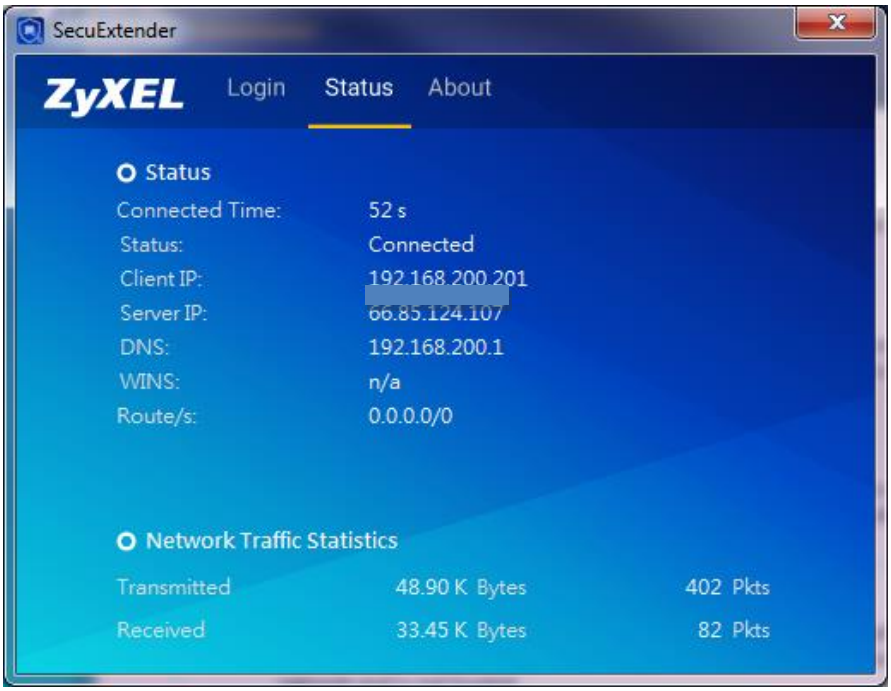
- SERVER – Provide the domain name, ddns hostname or public IP address of the ZyXEL appliance you wish to establish a connection with. (if the management port has been changed from TCP:443, please specify the new SSL port by adding a ":" <colon> and the port number. Ex: <Public_IP>:8443)
- USERNAME – Provide an allowed user account
- PASSWORD – Provide the password for the allowed user account
- Remember username – Check the box to store connection server and credentials on client memory
- Disconnect – Press the Disconnect button to end the SSL VPN session
- Connect – Press the Connect button to initiate an SSL VPN session



The pop-up below appears when establishing a connection. Verify the certificate being used to encrypt the SSL VPN connection is correct and click **YES** to trust the connection.

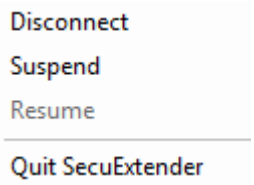


The clients *Status* tab shows information regarding the connection such as amount of time connected, IP address provided by the ZyXEL appliance to the client and traffic statistics.



Right-Click on any of the SecuExtender tab windows for options to disconnect, suspend, resume and quit the client.

- Disconnect – Ends the SSL VPN session
- Suspend – Stops routing traffic through the SSL VPN, session is still active
- Resume – Resume sending traffic through SSL VPN from suspend mode
- Quit SecuExtender – Disconnects the SSL VPN session and stops all client components

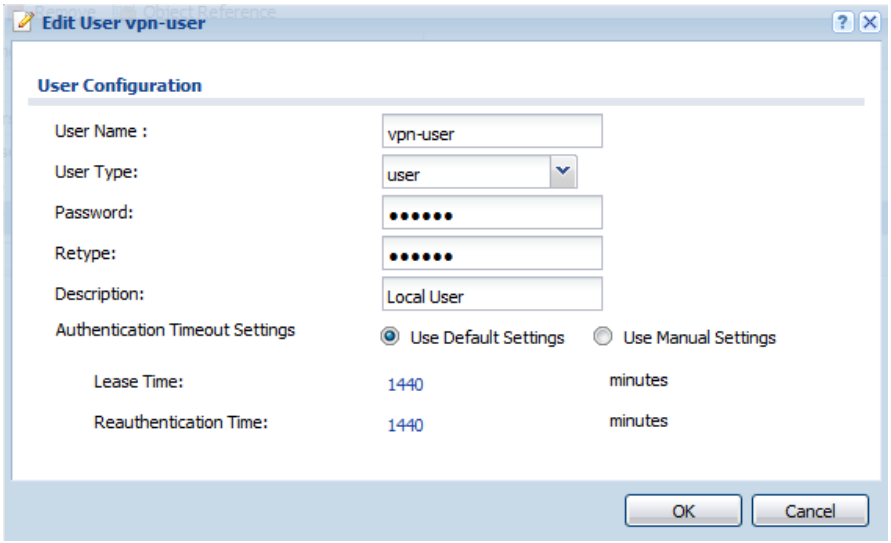


SSL VPN Rule

SSL VPN allows remote users to establish a VPN connection to the ZyWALL firewall router. A VPN can provide access to resources on the ZyWALL firewall routers local network or allow you to tunnel your internet traffic from hotspot/public networks to protect your traffic from potential man-in-the-middle discovery. Creating an SSL VPN rule gives you the ability to establish an SSL VPN tunnel as well as provide privileges to allowed users, computers and/or resources.

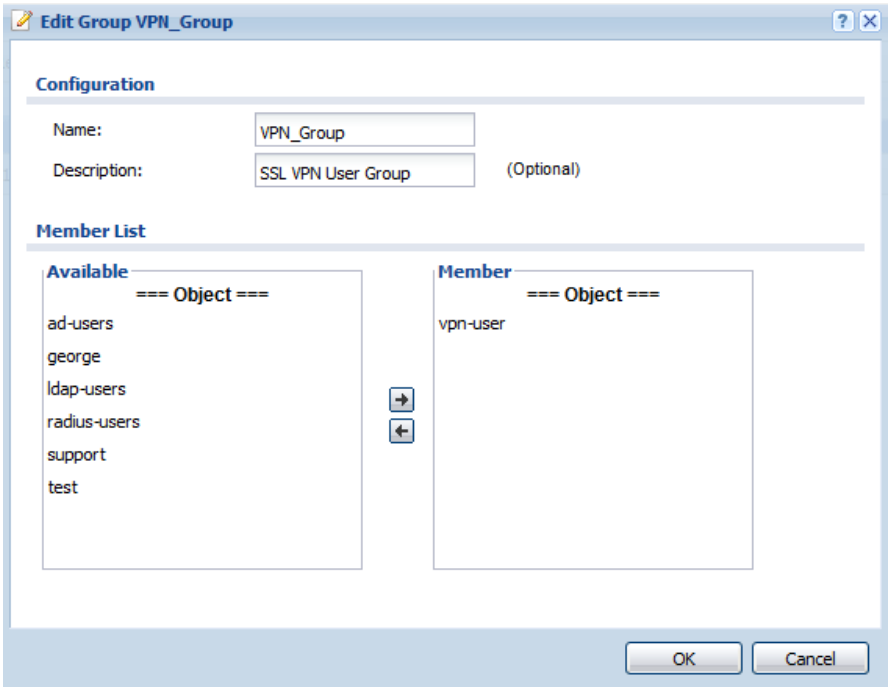
Step 1 – User Account Setup

Login to the ZyXEL router and go to menu, **Configuration → Object → User/Group**. Click the **Add** button to insert user accounts for SSL VPN access. SSL VPN users CANNOT be administrator account "User Type".



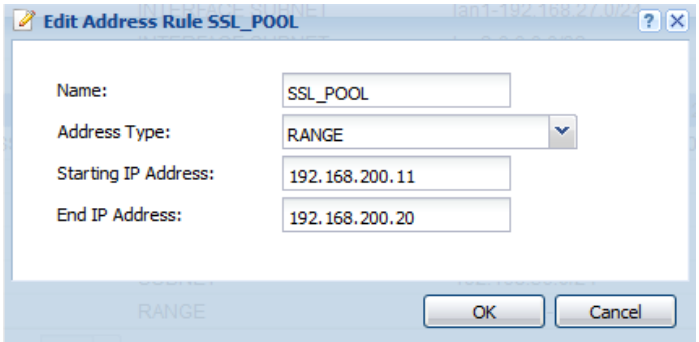
Step 2 – User Group Setup

If you have created multiple user accounts you may want to group them all together to keep all settings as simple as possible. You may skip this step if you only have about three user accounts. To create a user group, click the "*User Group*" tab in the **Configuration → Object → User/Group** menu. Add all the users which will have SSL VPN privilege to the group.



Step 3 – SSL VPN Address Pool

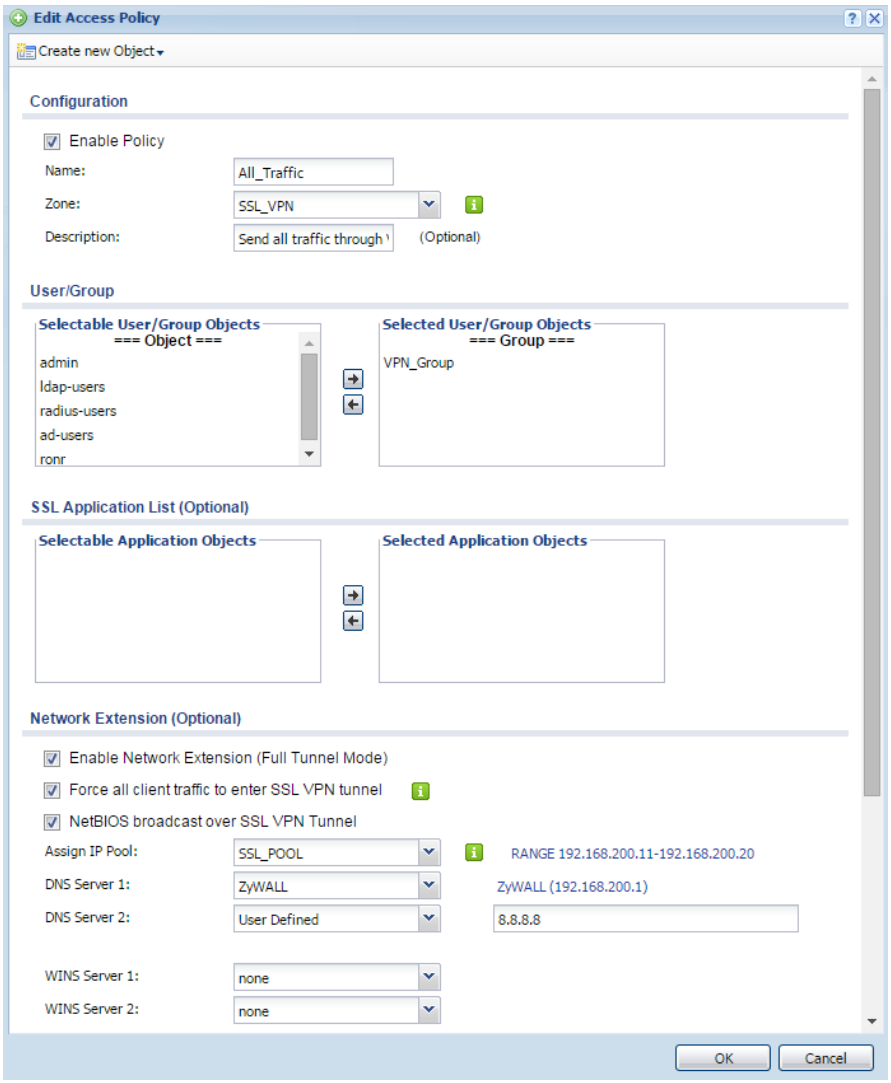
Create an address object for a pool of IP addresses which will be used by the connected SSL VPN user. Go to **Configuration → Object → Address** and click the **Add** button to insert the SSL VPN IP address pool. By default 192.168.200.X IP scheme is reserved for SSL VPN connections.



Step 4 – SSL VPN Policy

Now that the VPN users and IP pool have been created we can begin creating the SSL VPN policy. Go to menu **Configuration → VPN → SSL VPN** and click the **Add** button to insert an SSL VPN policy to allow the specified users access to the network.

- Make sure the "Enable Policy" checkbox is checked
- Provide a name for the SSL VPN policy
- The rule must be part of the **SSL_VPN** zone
- From the "Selectable User/Group Objects" find the user account or user group and move it over to the "Selected User/Group Objects"
- Scroll down to the "Network Extension" option and check the box to "Enable Network Extension (Full Tunnel Mode)"
- Check the box to "Force all client traffic to enter SSL VPN tunnel"
- For the "Assign IP Pool" dropdown select the object you have created for the SSL VPN IP Pool
- Provide DNS server entries, "User Defined" can be selected to manually enter the DNS server the SSL VPN users will use for their DNS queries, "ZyWALL" can be selected to have the SSL VPN users point all DNS queries to the ZyXEL router
- Click the **OK** button to apply the settings


Edit Access Policy
Create new Object
Configuration
Enable Policy
Name:
All_Traffic
Zone:
SSL_VPN
Description:
Send all traffic through
(Optional)
User/Group
Selectable User/Group Objects
=== Object ===
admin
ldap-users
radius-users
ad-users
ronr
Selected User/Group Objects
=== Group ===
VPN_Group
SSL Application List (Optional)
Selectable Application Objects
Selected Application Objects
Network Extension (Optional)
Enable Network Extension (Full Tunnel Mode)
Force all client traffic to enter SSL VPN tunnel
NetBIOS broadcast over SSL VPN Tunnel
Assign IP Pool:
SSL_POOL
RANGE 192.168.200.11-192.168.200.20
DNS Server 1:
ZyWALL
ZyWALL (192.168.200.1)
DNS Server 2:
User Defined
8.8.8.8
WINS Server 1:
none
WINS Server 2:
none
OK
Cancel