

Configuration on RV130

Small Business
RV130W Wireless-N VPN Firewall

Getting Started

- ▶ Status
- ▶ Networking
- ▶ Wireless
- ▶ Firewall
- VPN**
 - ▶ Site-to-Site IPSec VPN
 - IPSec VPN Server
 - Setup**
 - User
 - PPTP Server
 - VPN Passthrough
 - ▶ QoS
 - ▶ Administration

Phase 1 Configuration

Server Enable:

NAT Traversal: Enabled [Edit](#)

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group: Enable

DH Group:

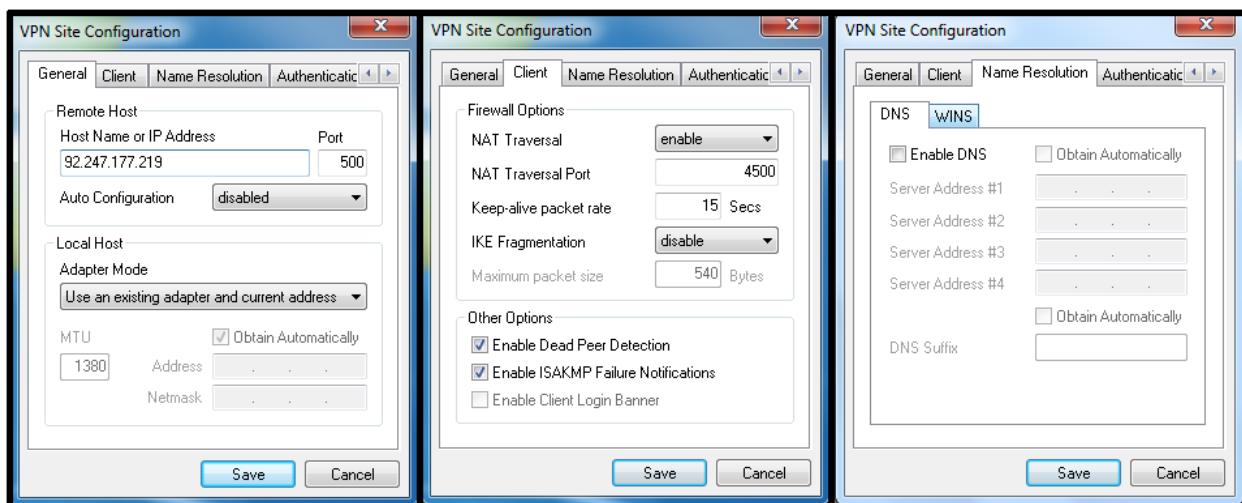
- User configuration on RV130W :



The screenshot shows the 'User' configuration page on the RV130W. The left sidebar menu is expanded to show the 'VPN' section, with 'User' selected. The main area displays a 'User Account Table' with one entry: 'Cisco-user' with a password of '*****'. There are buttons for 'Add Row', 'Edit', 'Delete', and 'Import'. At the bottom are 'Save' and 'Cancel' buttons.

	UserName	Password
<input type="checkbox"/>	Cisco-user	*****

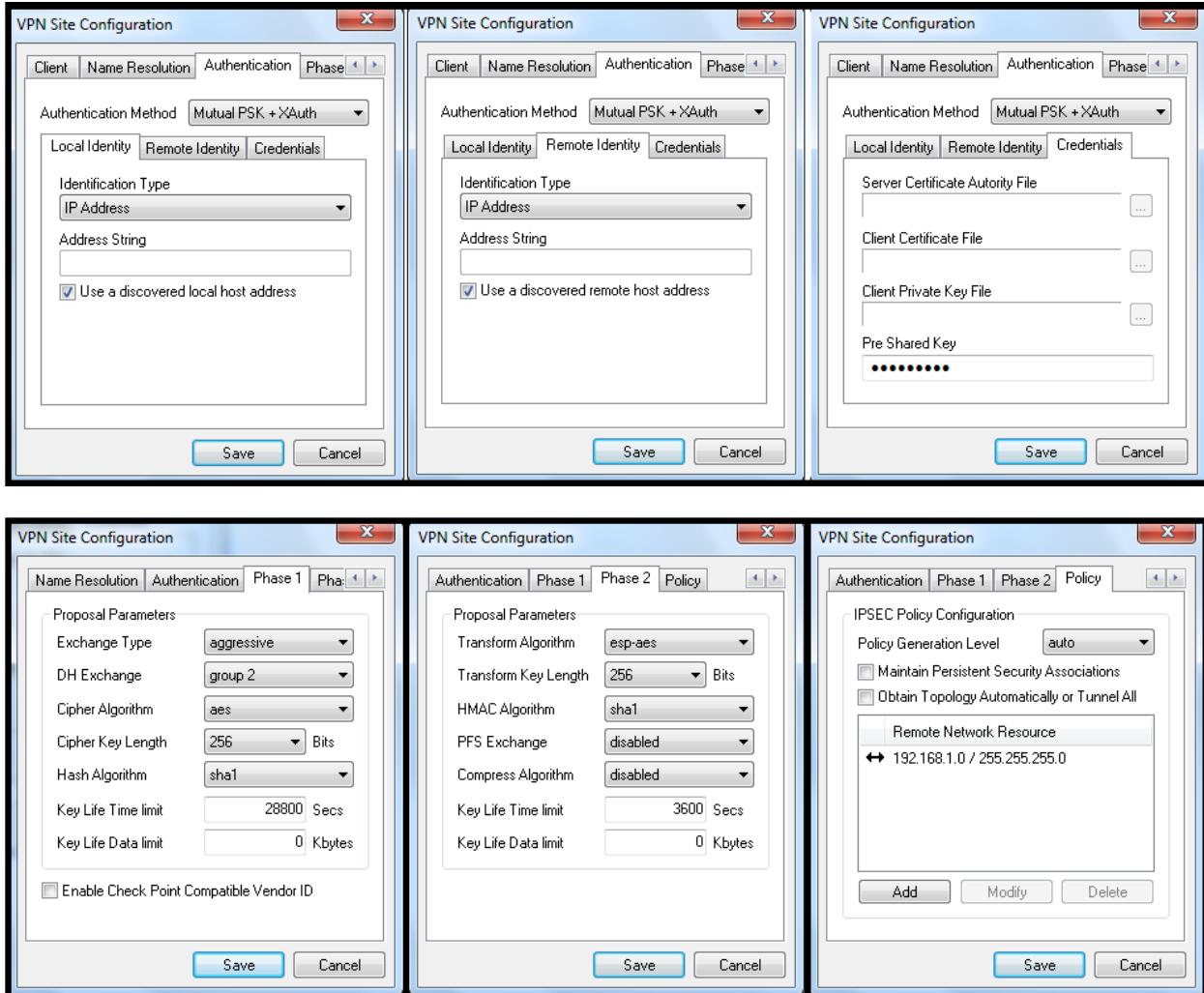
Shrew-VPN configuration example



The three screenshots show the 'VPN Site Configuration' software interface:

- General Tab:** Shows 'Remote Host' settings with 'Host Name or IP Address' set to '92.247.177.219' and 'Port' set to '500'. 'Auto Configuration' is set to 'disabled'. 'Local Host' settings include 'Adapter Mode' set to 'Use an existing adapter and current address'. 'MTU' is set to '1380'. 'Address' and 'Netmask' fields are partially visible. Buttons for 'Save' and 'Cancel' are at the bottom.
- Client Tab:** Shows 'Firewall Options' with 'NAT Traversal' set to 'enable' and port '4500'. 'Keep-alive packet rate' is '15 Secs'. 'IKE Fragmentation' is 'disable'. 'Maximum packet size' is '540 Bytes'. Under 'Other Options', 'Enable Dead Peer Detection' and 'Enable ISAKMP Failure Notifications' are checked. Buttons for 'Save' and 'Cancel' are at the bottom.
- WINS Tab:** Shows 'DNS' and 'WINS' sections. Under 'DNS', 'Enable DNS' is checked. Under 'WINS', 'Server Address #1' through '#4' are listed with 'Obtain Automatically' checkboxes. A 'DNS Suffix' field is also present. Buttons for 'Save' and 'Cancel' are at the bottom.

ShrewVPN configuration with RV130



The screenshots illustrate the configuration of a ShrewVPN site on an RV130 router using the Cisco SBSC Center. The configuration is divided into six panels across three rows:

- Row 1:** Shows the initial configuration steps for Phase 1. The first panel (Client tab) sets the Authentication Method to "Mutual PSK + XAuth" and the Local Identity to "IP Address". The second panel (Authentication tab) also sets the Authentication Method to "Mutual PSK + XAuth" and the Local Identity to "IP Address". The third panel (Phase tab) specifies the Server Certificate Authority File, Client Certificate File, Client Private Key File, and Pre Shared Key.
- Row 2:** Shows the detailed proposal parameters for Phase 1. The first panel (Name Resolution tab) includes fields for Exchange Type (aggressive), DH Exchange (group 2), Cipher Algorithm (aes), Cipher Key Length (256 Bits), Hash Algorithm (sha1), Key Life Time limit (28800 Secs), and Key Life Data limit (0 Kbytes). The second panel (Authentication tab) includes fields for Transform Algorithm (esp-aes), Transform Key Length (256 Bits), HMAC Algorithm (sha1), PFS Exchange (disabled), Compress Algorithm (disabled), Key Life Time limit (3600 Secs), and Key Life Data limit (0 Kbytes).
- Row 3:** Shows the IPSEC Policy Configuration for Phase 1. The third panel (Policy tab) includes fields for Policy Generation Level (auto), Maintain Persistent Security Associations (unchecked), Obtain Topology Automatically or Tunnel All (unchecked), and a Remote Network Resource entry for 192.168.1.0 / 255.255.255.0.