


## Configuration on RV130



Small Business  
cisco 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

Server Enable:

NAT Traversal: Enabled [Edit](#)

**Phase 1 Configuration**

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:

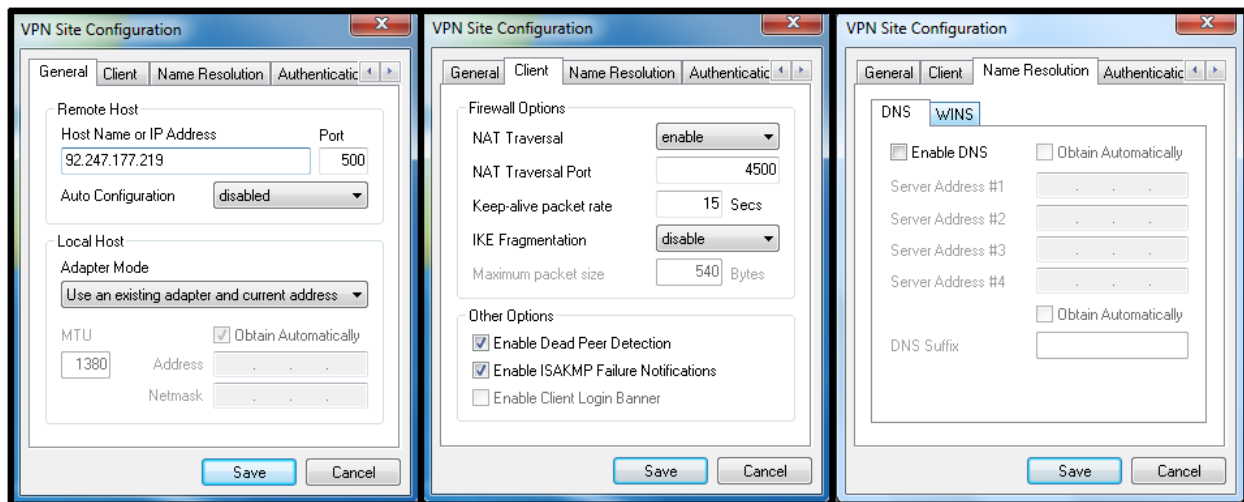
PFS Key Group:  Enable

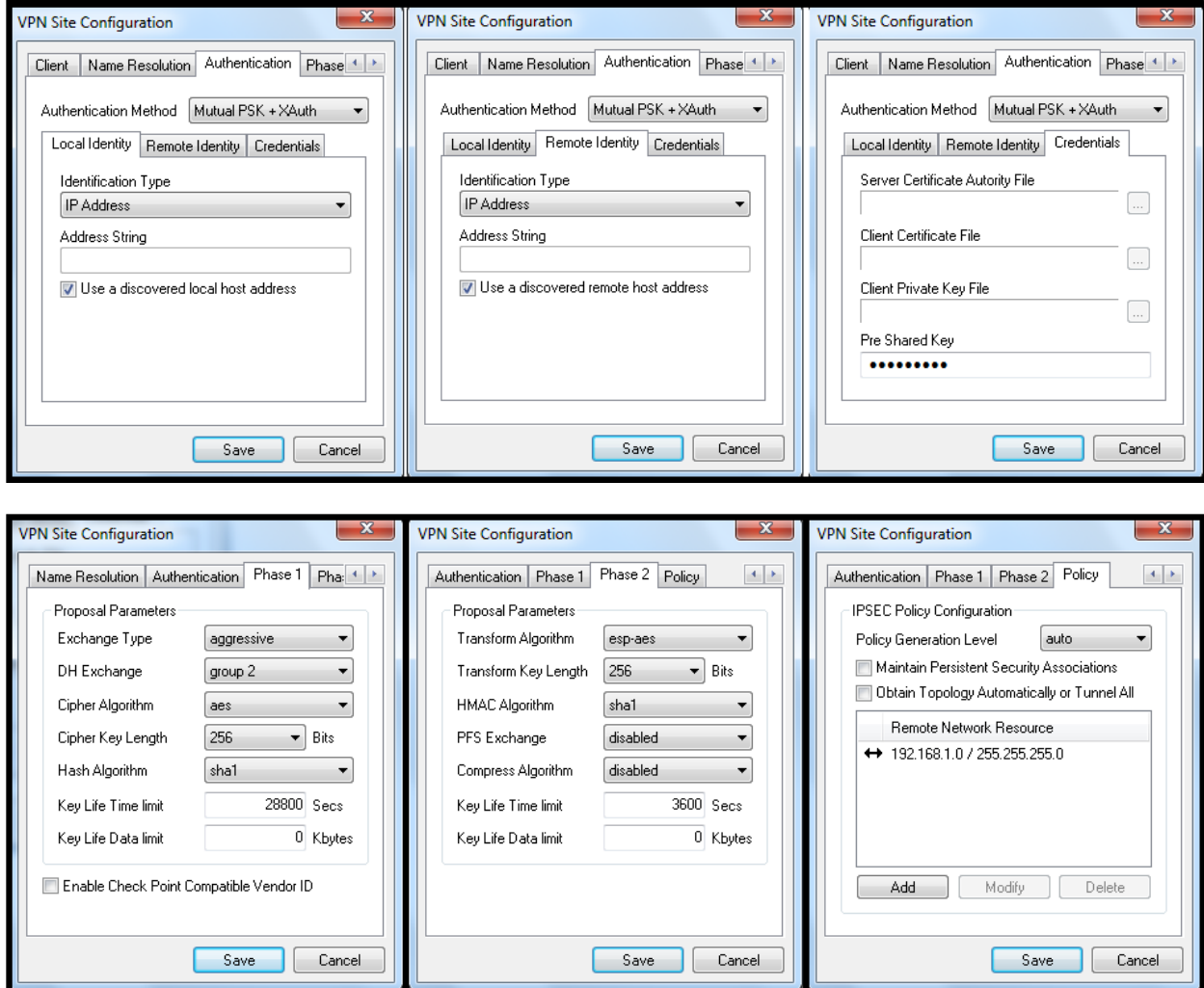
DH Group:

- User configuration on RV130W :



## Shrew-VPN configuration example





The image displays six screenshots of the VPN Site Configuration interface, arranged in two rows of three. The top row shows the 'Authentication' tab for three different VPN sites, all configured with 'Mutual PSK + XAuth' authentication. The first two sites are configured for local identity (IP Address), while the third is configured for remote identity (IP Address). The bottom row shows the 'Phase 1' and 'Policy' tabs for three different VPN sites. The first two sites show proposal parameters such as Exchange Type (aggressive), DH Exchange (group 2), Cipher Algorithm (aes), and Key Life Time limit (28800 Secs). The third site shows the IPSEC Policy Configuration, including Policy Generation Level (auto) and Remote Network Resource (192.168.1.0 / 255.255.255.0).