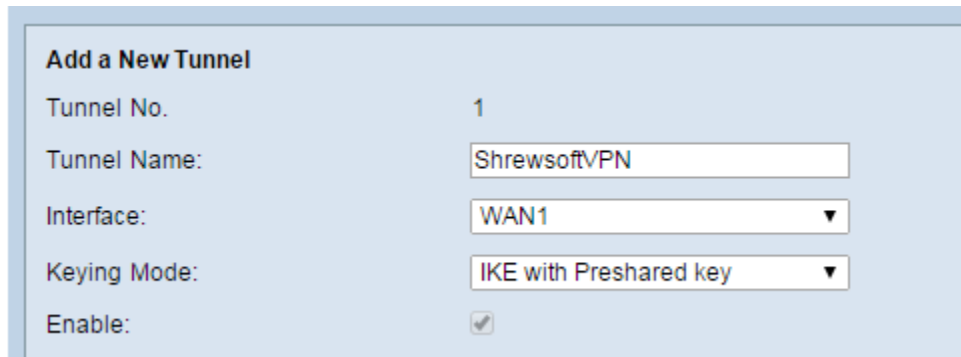


Rv320 and Shrew VPN

1- Enter a name for the tunnel.

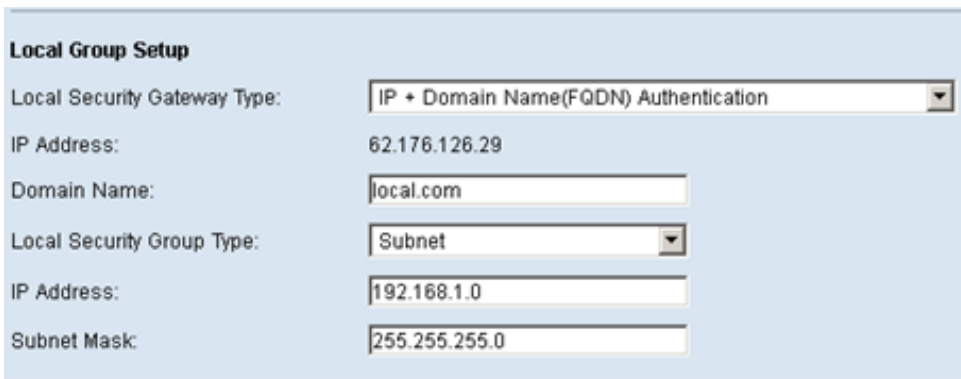
This should be Client to Gateway VPN since Shrewsoft is a Client.



The screenshot shows the 'Add a New Tunnel' configuration page. The fields are as follows:

Tunnel No.	1
Tunnel Name:	ShrewsoftVPN
Interface:	WAN1
Keying Mode:	IKE with Preshared key
Enable:	<input checked="" type="checkbox"/>

2- Enter local settings using IP+Domain Name.(local.com is just to make reference to the router, you can use something different)



The screenshot shows the 'Local Group Setup' configuration page. The fields are as follows:

Local Security Gateway Type:	IP + Domain Name(FQDN) Authentication
IP Address:	62.176.126.29
Domain Name:	local.com
Local Security Group Type:	Subnet
IP Address:	192.168.1.0
Subnet Mask:	255.255.255.0

3- For the Remote use dynamic IP + Domain Name(We don't know the Ip address for each remote client so that is why we use Dynamic), remote.com is only to make reference to the remote party but it could be something else.

Remote Client Setup

Remote Security Gateway Type:

Domain Name:

4- Specify phase 1 and 2 settings:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

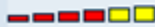
Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Advanced -

5- Check all the settings below:

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval 10 sec (Range: 10-999, Default: 10)
- Extended Authentication:

6- Specify if you want to use local database or something different like Active Directory or Radius from the dropdown menu(Be aware that you will need to create a Domain under user management if you want to use Active Dir or Radius and a user and password if you go with the Local database.

Edge Device Default - Local Database Edit

Mode Configuration

7- You can create the user and Domain from user management.

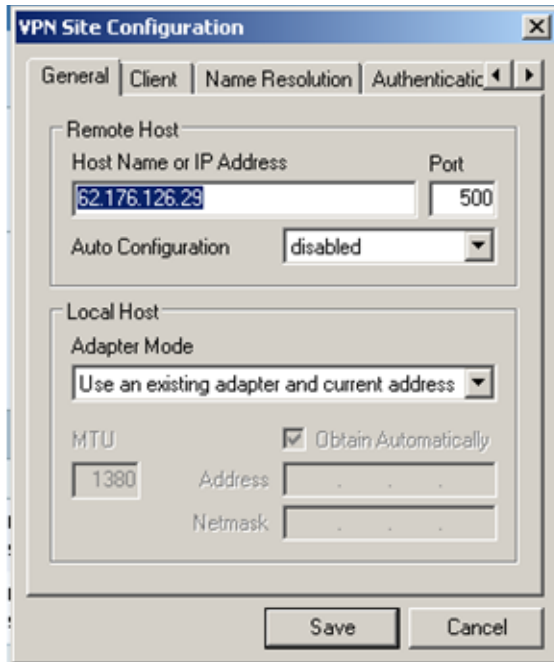
User Management

Domain Management Table			
Domain Name	Authentication Type	Authentication Server IP	
<input checked="" type="radio"/> Default	Local Database	N/A	
Add...	Edit...	Delete	

User Management Table			
<input type="checkbox"/> Username	Password	Group	Domain
<input checked="" type="checkbox"/> cisco	*****	Administrator	Default

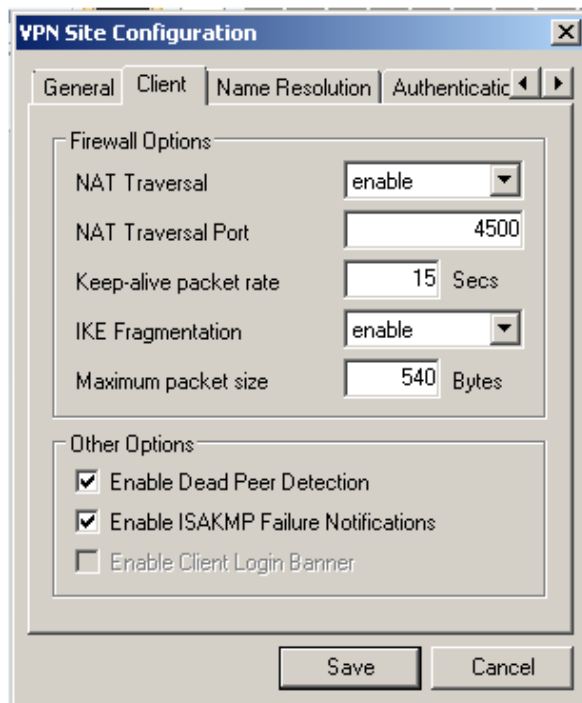
Shrew Client configuration:

- 1- Install Shrewsoft as Standard.
- 2- Click on Add.
- 3- Enter the public IP that is configured on the RV320 and make sure you match the settings here.



The screenshot shows the 'VPN Site Configuration' dialog box with the 'General' tab selected. The 'Remote Host' section has 'Host Name or IP Address' set to '62.176.126.29' and 'Port' set to '500'. The 'Auto Configuration' dropdown is set to 'disabled'. The 'Local Host' section has 'Adapter Mode' set to 'Use an existing adapter and current address'. The 'MTU' is set to '1380', and the 'Obtain Automatically' checkbox is checked. The 'Address' and 'Netmask' fields are empty.

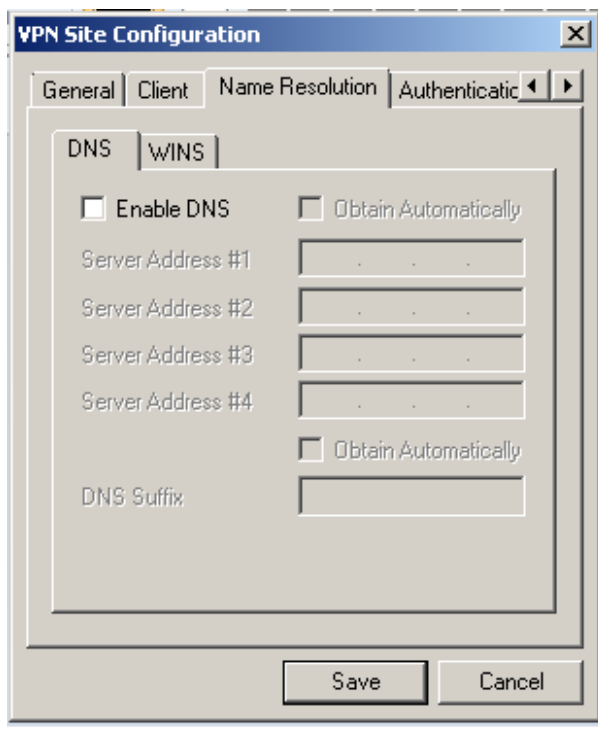
Field	Value
Host Name or IP Address	62.176.126.29
Port	500
Auto Configuration	disabled
Adapter Mode	Use an existing adapter and current address
MTU	1380
Obtain Automatically	<input checked="" type="checkbox"/>
Address	
Netmask	



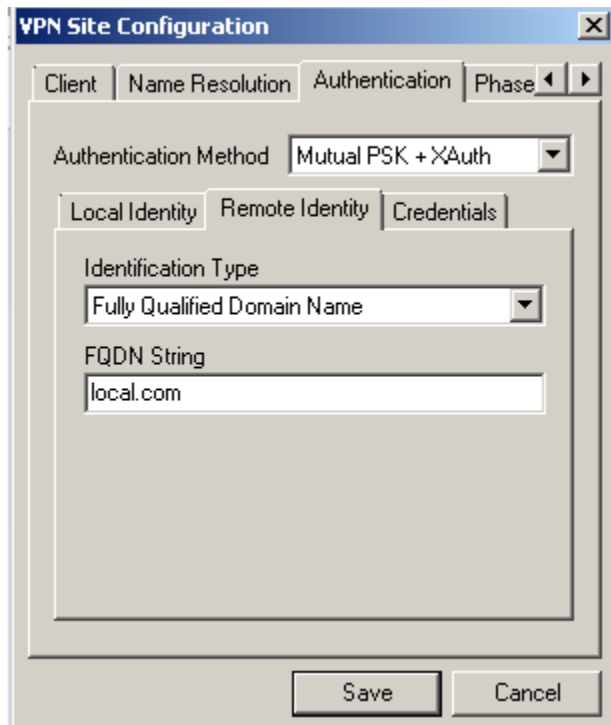
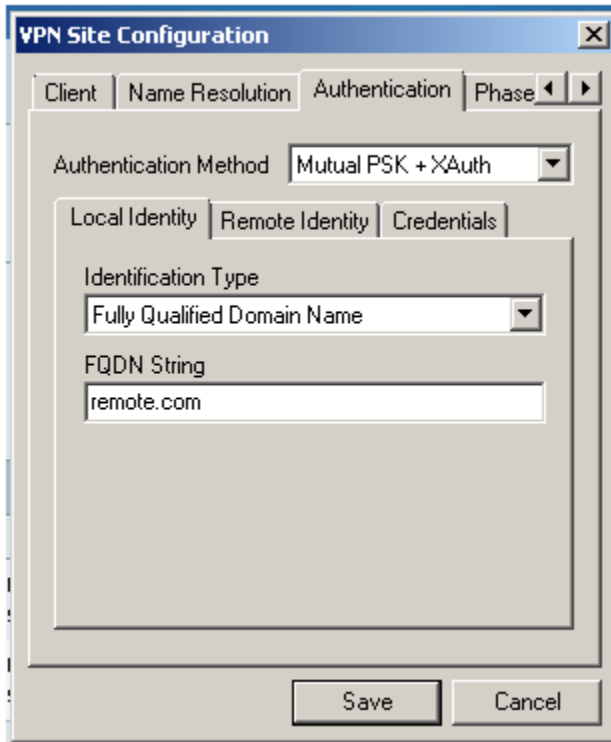
The screenshot shows the 'VPN Site Configuration' dialog box with the 'Client' tab selected. The 'Firewall Options' section has 'NAT Traversal' set to 'enable', 'NAT Traversal Port' set to '4500', 'Keep-alive packet rate' set to '15 Secs', 'IKE Fragmentation' set to 'enable', and 'Maximum packet size' set to '540 Bytes'. The 'Other Options' section has 'Enable Dead Peer Detection', 'Enable ISAKMP Failure Notifications', and 'Enable Client Login Banner' checkboxes.

Field	Value
NAT Traversal	enable
NAT Traversal Port	4500
Keep-alive packet rate	15 Secs
IKE Fragmentation	enable
Maximum packet size	540 Bytes
Enable Dead Peer Detection	<input checked="" type="checkbox"/>
Enable ISAKMP Failure Notifications	<input checked="" type="checkbox"/>
Enable Client Login Banner	<input type="checkbox"/>

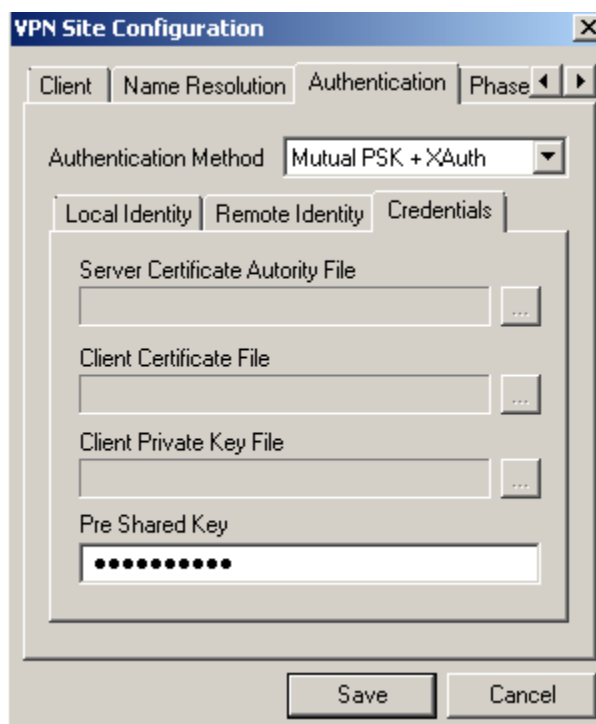
Disable both DNS and WINS



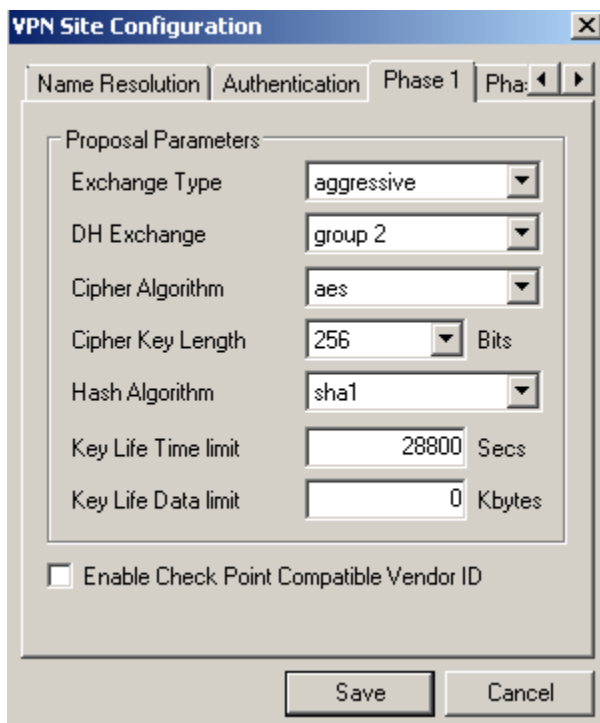
Here the local.com and remote.com will be inverted (The PC is the remote and the Rv320 is the local):

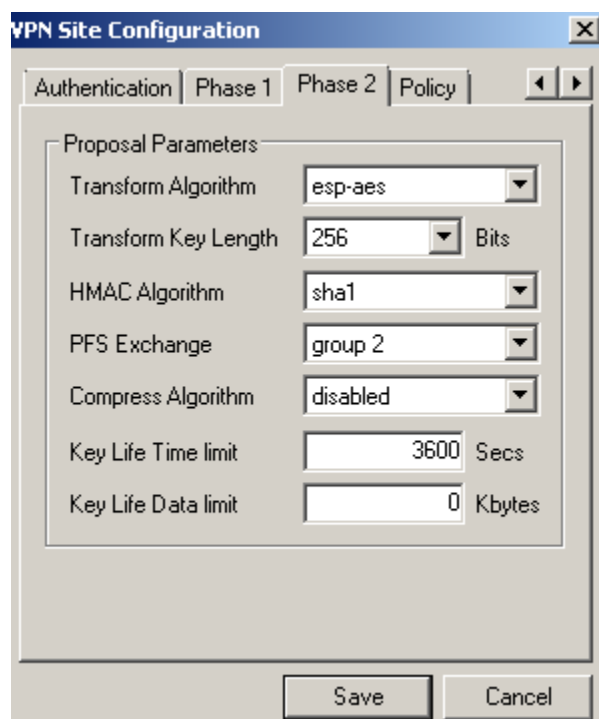


Here use Mutual PSK +XAuth and enter the pre shared key we put on the router:

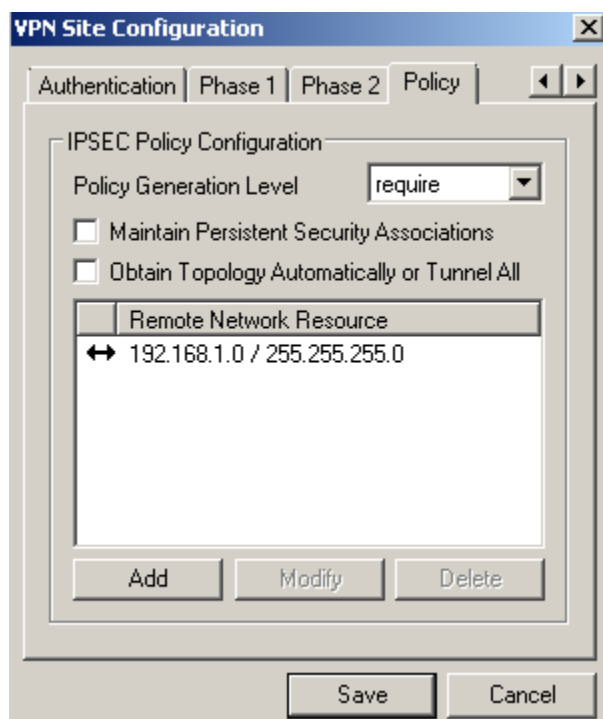


Match phase 1 and phase 2 on the router:





Here you need to make sure to add the remote network 192.168.1.0/24 but keep in mind not all the time the router is using the default network and it might be different, also make sure the LAN on the client side is different than the one behind the router RV320.



We are done, just save and run the VPN client and click on connect, and you will be ask to enter the username and password in this example cisco cisco.