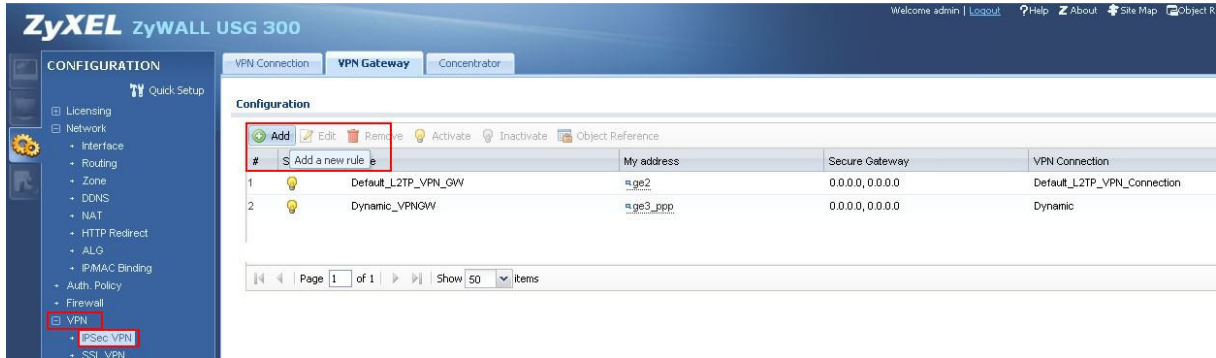


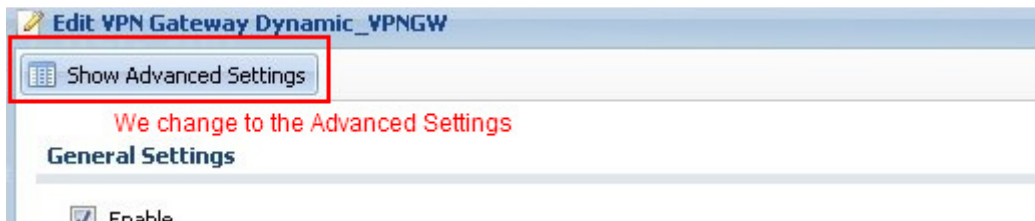
VPN connection between Shrew IPSEC Client (V2.1.7) and ZyWALL USG

First we must create a Dynamic Gateway Policy on the USG:

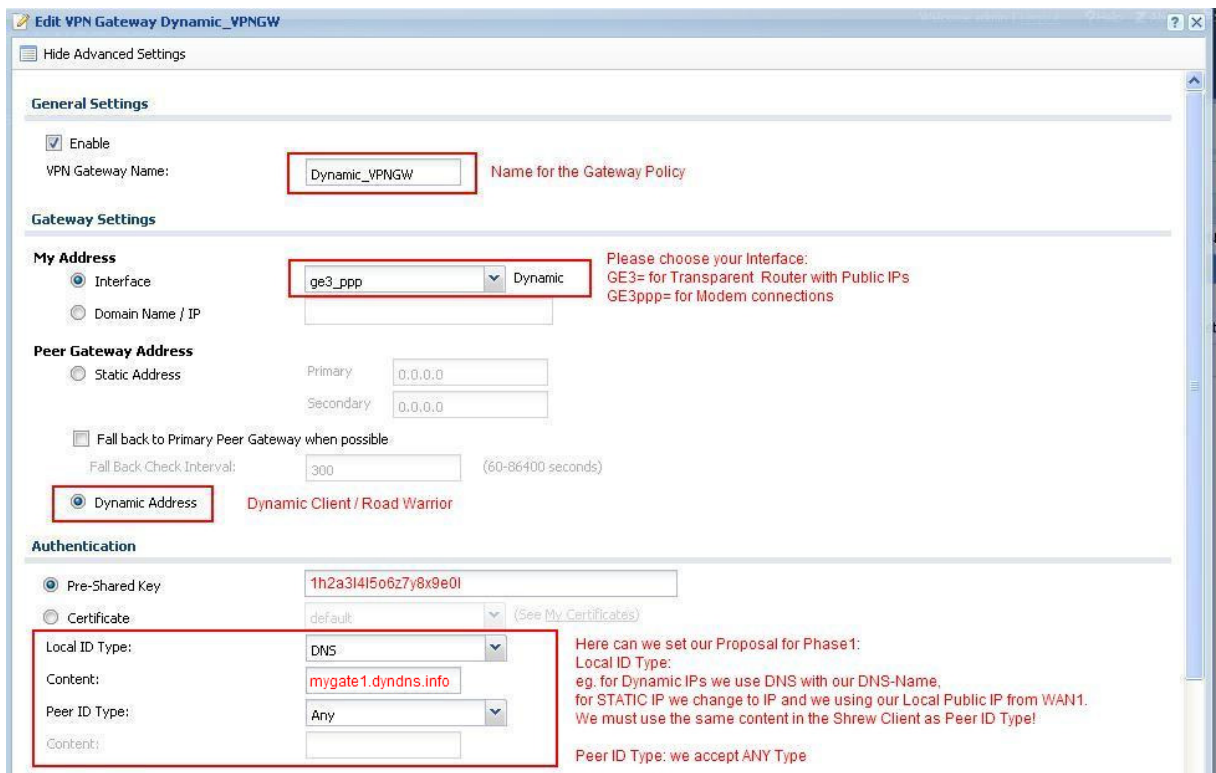
CONFIGURATION -> VPN -> IPsecVPN -> VPN Gateway, we click on ADD

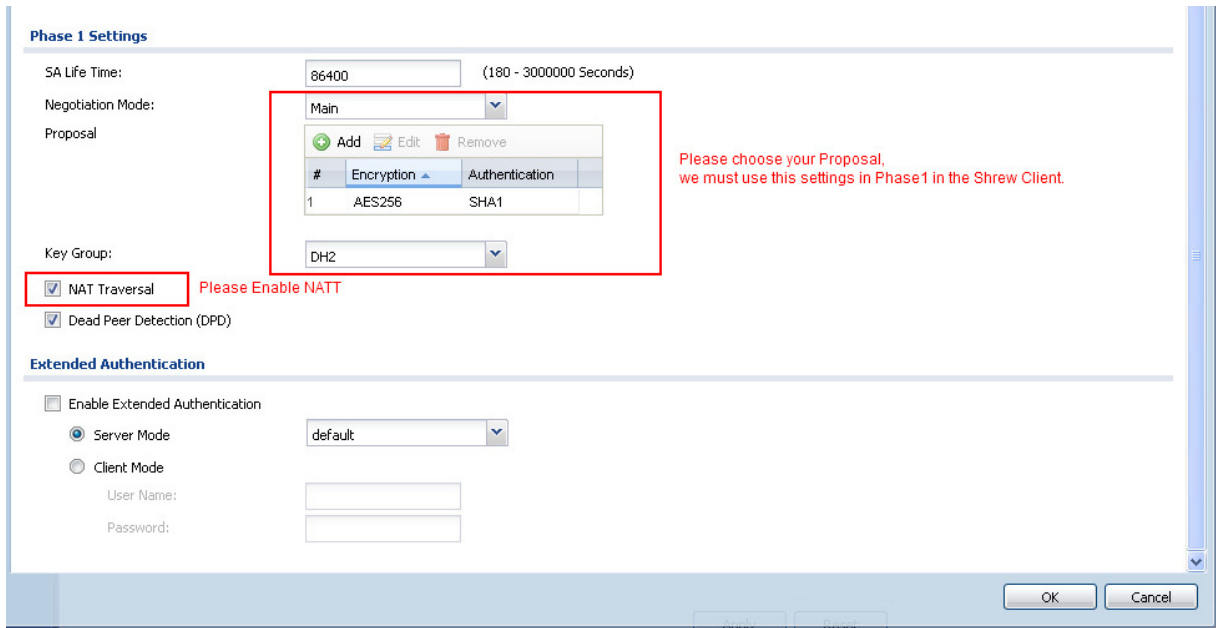


We change to the Advanced Settings:



Now we create the Phase1 on ZyWALL USG:

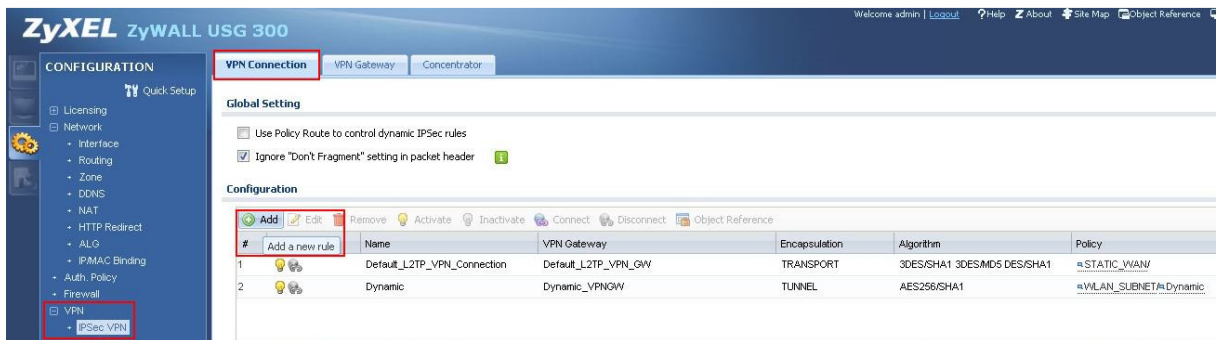




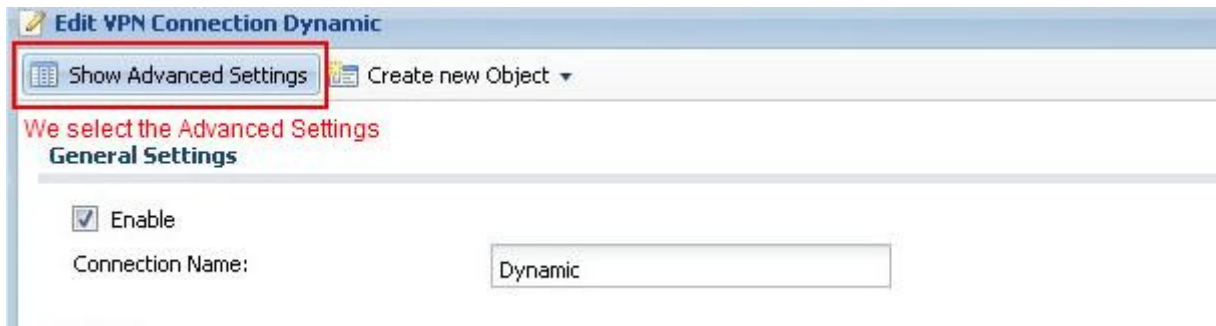
We submit with OK and Phase1 was successfully created.

Now we must create Phase2:

CONFIGURATION -> VPN -> IPsecVPN -> VPN Connection, click on ADD:



We change to Advanced Settings:



We create Phase2 on ZyWALL USG

Edit VPN Connection Dynamic

Hide Advanced Settings

General Settings

Enable
Connection Name: *Name of the connection*

Nailed-Up
 Enable Replay Detection
 Enable NetBIOS broadcast over IPsec

VPN Gateway

Application Scenario

Site-to-site
 Site-to-site with Dynamic Peer
 Remote Access (Server Role)
 Remote Access (Client Role)

VPN Gateway: *Binding to Phase1 "Gateway Policy"*

Manual Key

Manual Key

My Address:
Secure Gateway Address:
SPI: (256 - 4095)
Encapsulation Mode:
Active Protocol:
Encryption Algorithm:
Authentication Algorithm:
Encryption Key:
Authentication Key:

Policy

Local policy: *Local Policy, here e.g. WLAN Subnet*

Remote policy: *Object for Dynamic HOST*

Policy Enforcement

Phase 2 Settings

SA Life Time: (180 - 3000000 Seconds)

Active Protocol:
Encapsulation:

Proposal

#	Encryption	Authentication
1	AES256	SHA1

Here we can make the proposal for Phase2 SA Life, Encryption etc.

Perfect Forward Secrecy (PFS):

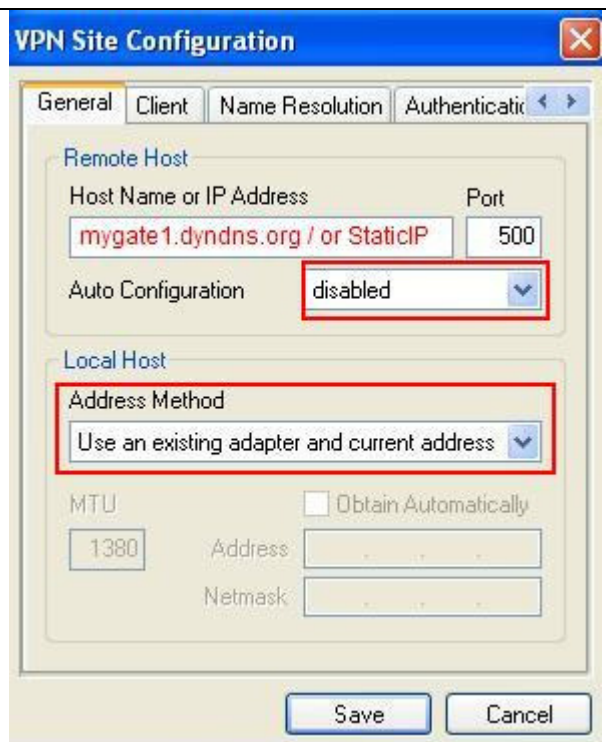
Connectivity Check

Enable Connectivity Check

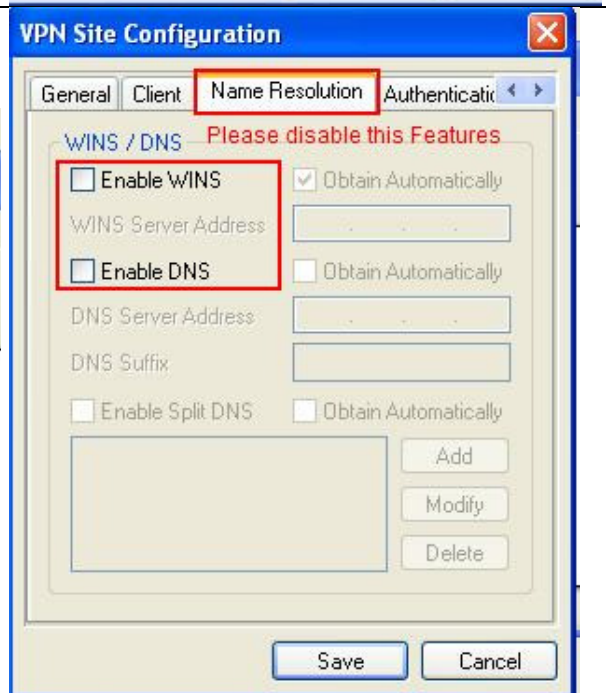
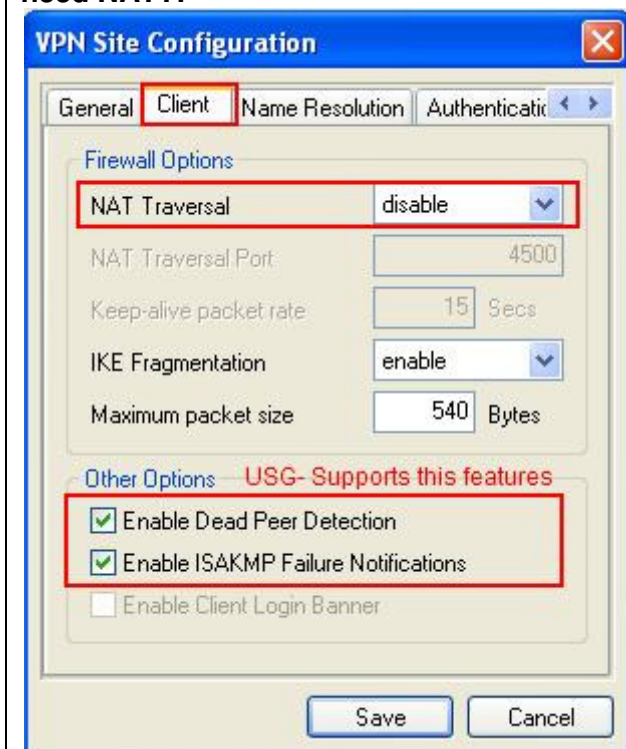
Check Method:
Check Period: (5-30 Seconds)
Check Timeout: (1-10 Seconds)
Check Fail Tolerance: (1-10)
 Check This Address Domain Name or IP Address
 Check the First and Last IP Address in the Remote Policy
 Log

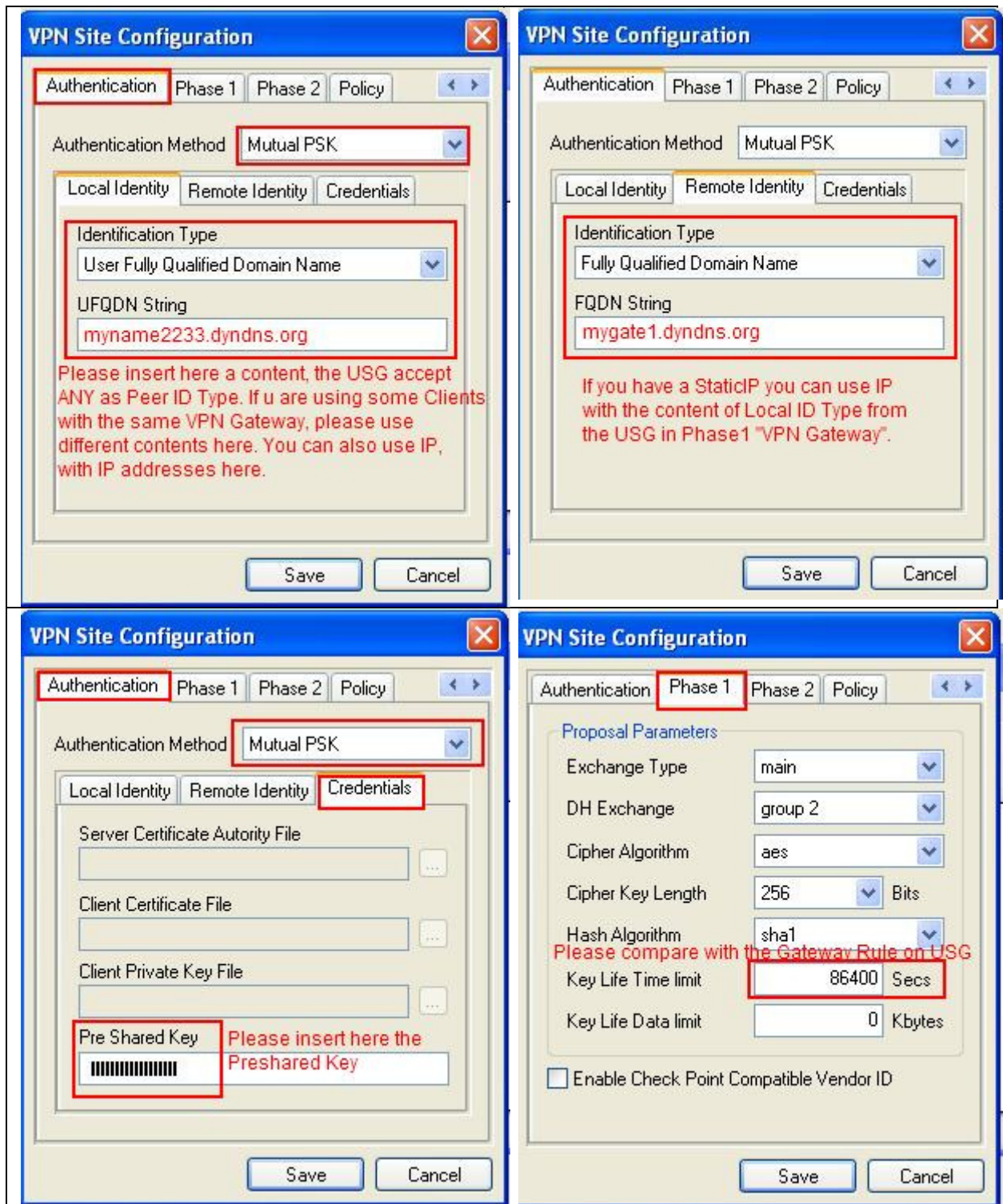
We submit with OK and Phase2 was successfully created. USG is ready for VPN use.

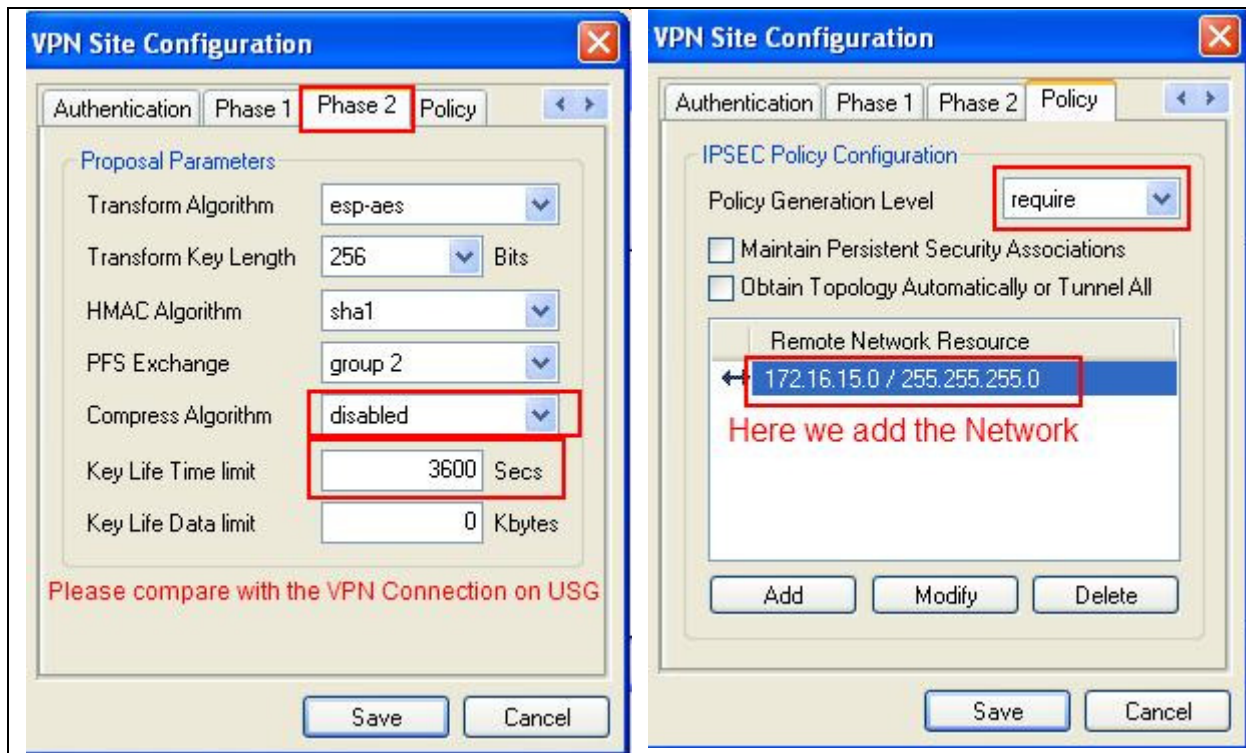
Client Configuration:



Please check if you need NATT, if your Client is behind another NAT Router u need NATT!



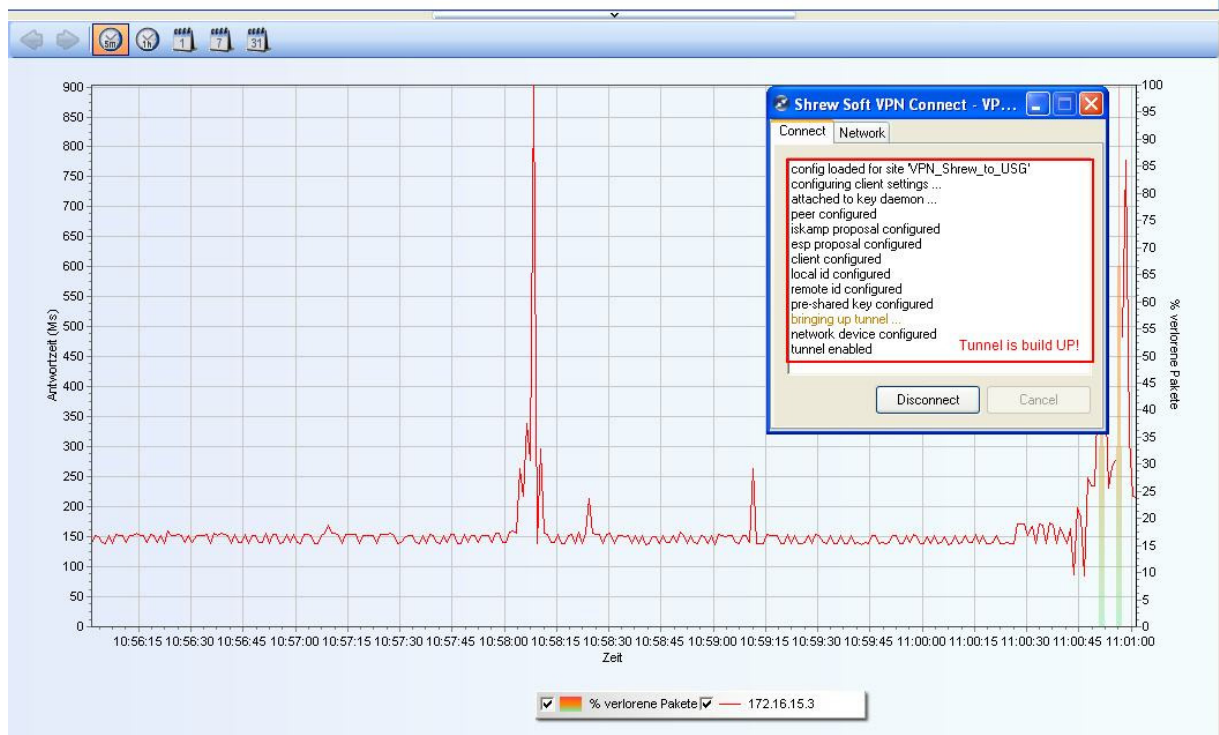




And now we can make a try if the VPN connection works:

Tunnel is build up successfully and we can Ping Clients in the 172.16.15.0/24 Network.

Statut	Host			Antwortzeit (Ms)				Pakete		
	Name	IP	DNS Name	Letzte	Durchschnitt	Min.	Max.	Gesendet	Verloren	% Verloren
▶	172.16.15.1	172.16.15.1		216	84	72	903	588	2	0
▶	172.16.15.3	172.16.15.3		216	130	83	903	581	2	0



THX & Finish!