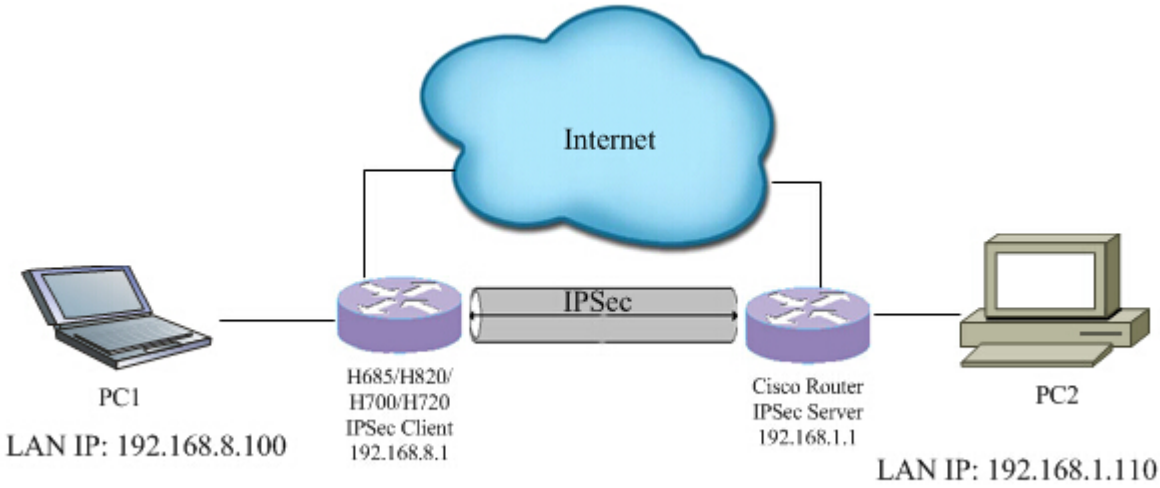
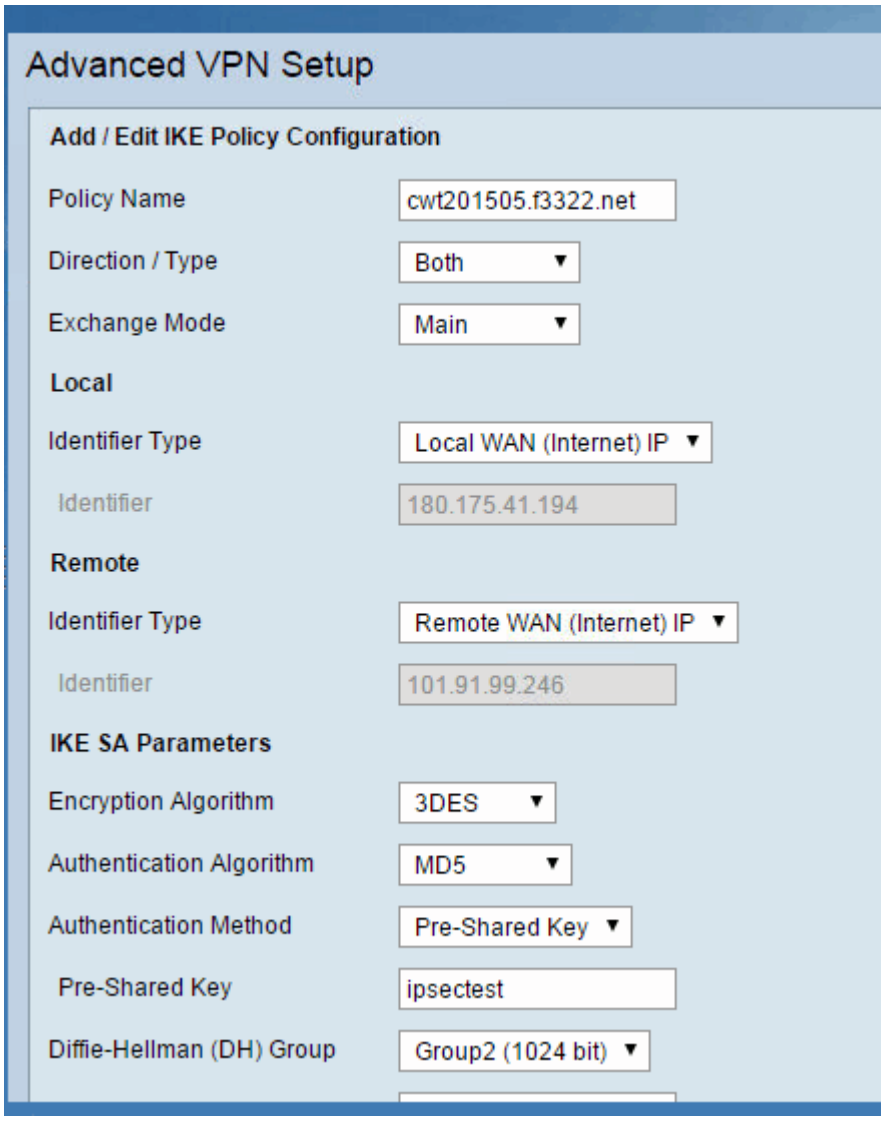
H685/H820/H7X0 and Cisco RV180W with DDNS IPSec VPN in Main Mode

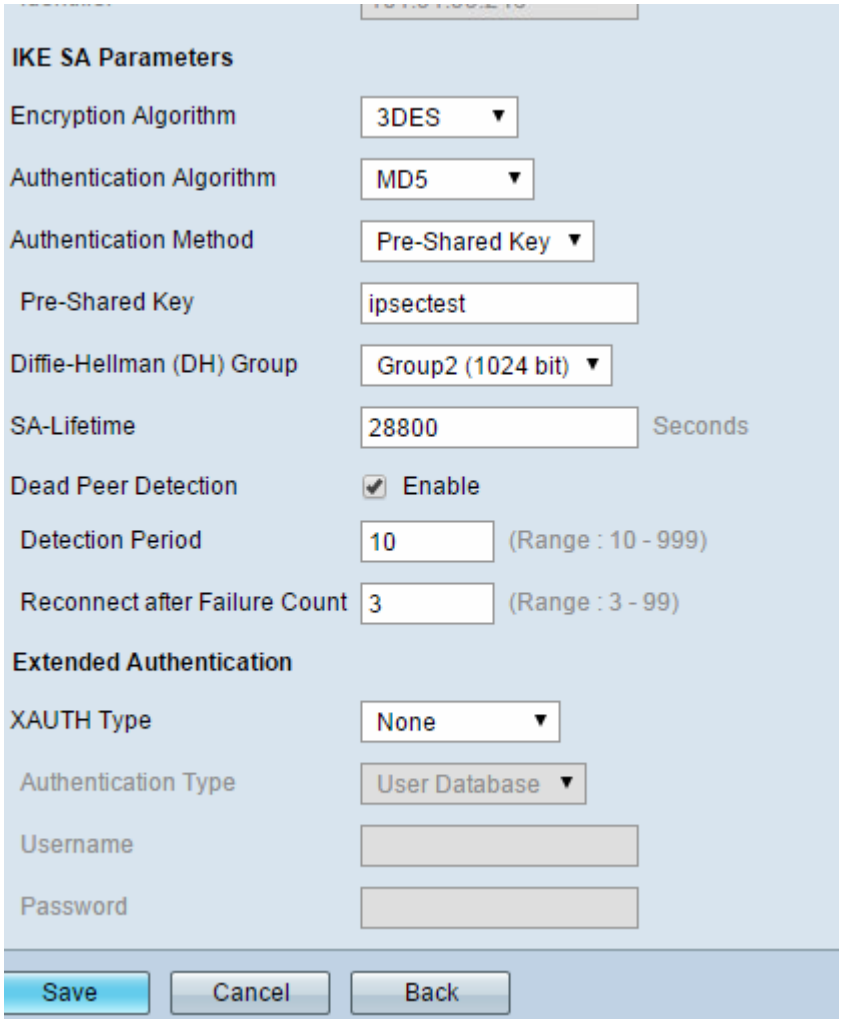
Typical Simple Diagram

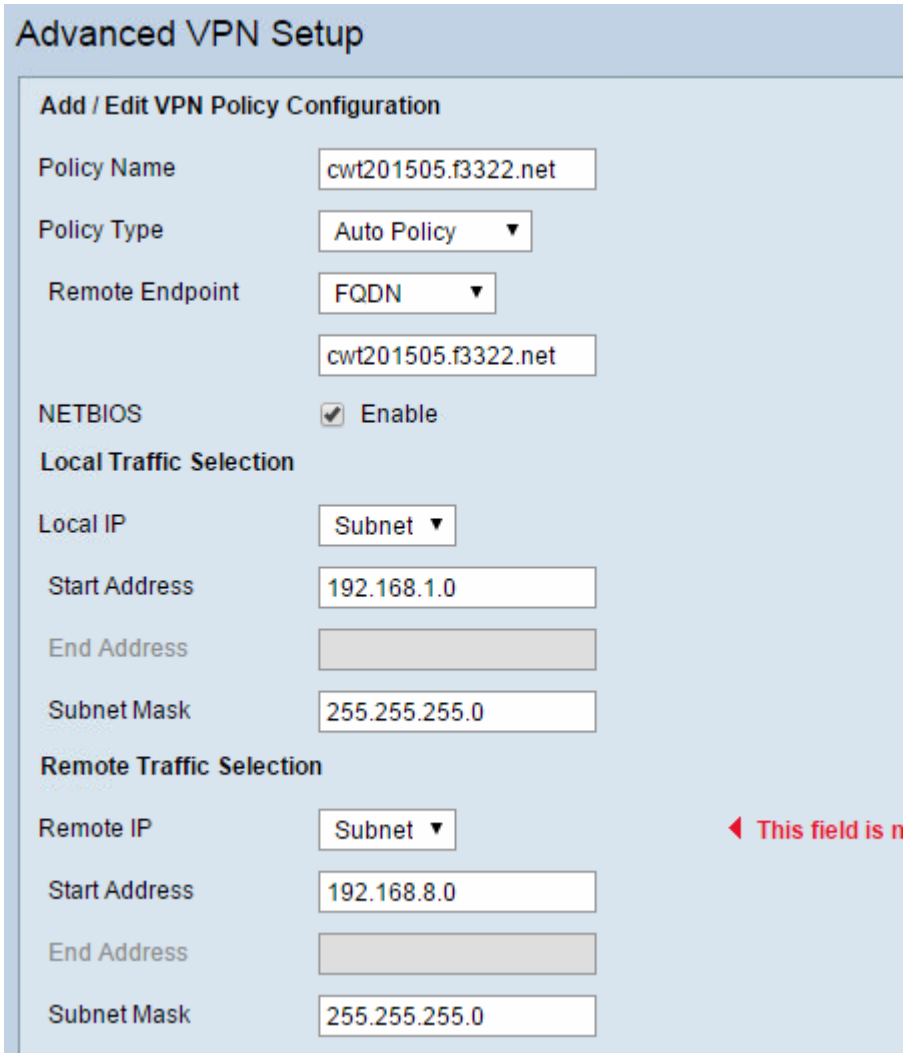


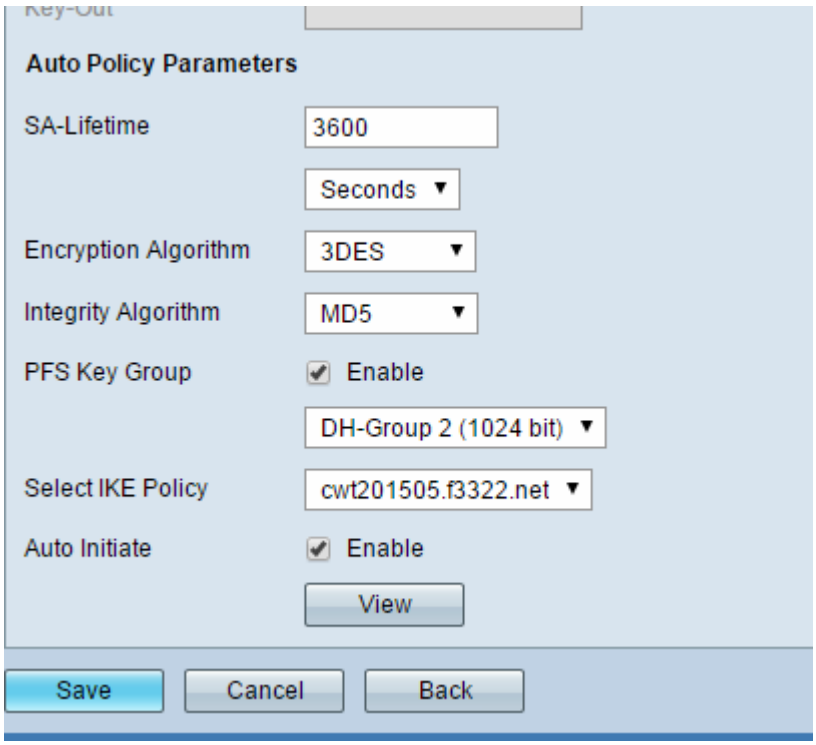
1) Make sure the Cisco router and E-Lins router' DDNS are working.

2) set IKE Cisco router IPSec

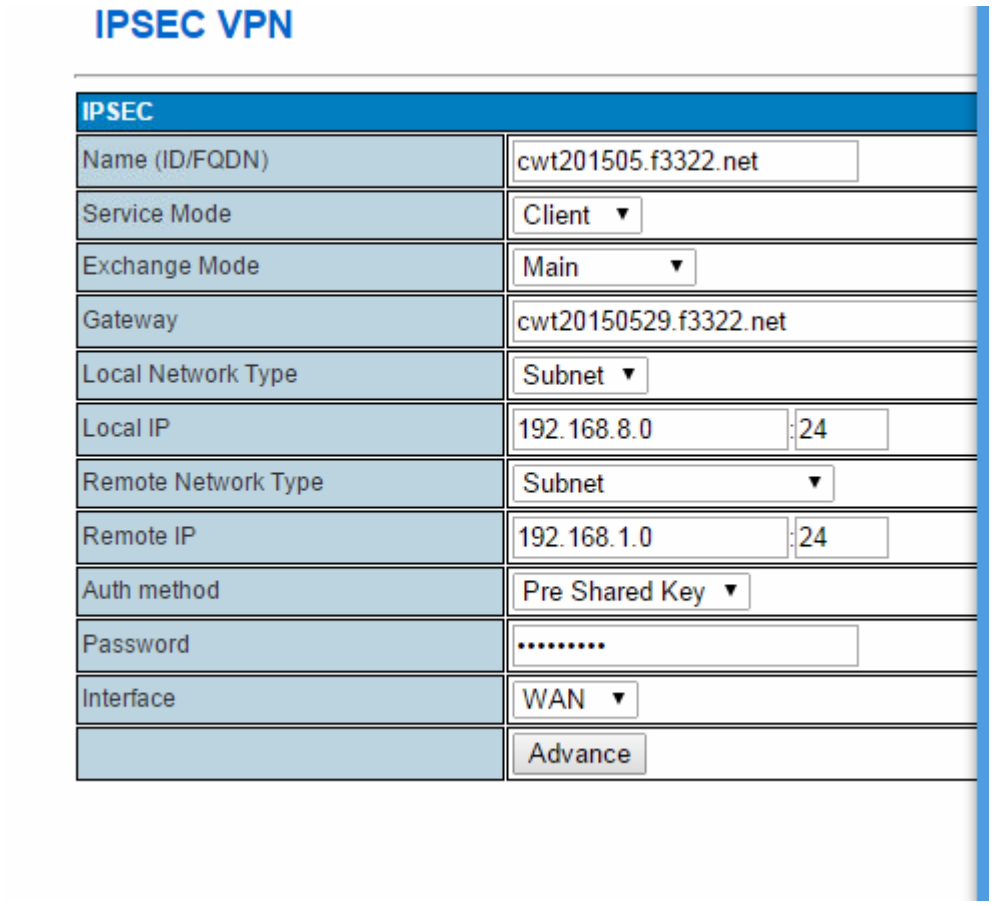

Advanced VPN Setup
Add / Edit IKE Policy Configuration
Policy Name
cwt201505.f3322.net
Direction / Type
Both
Exchange Mode
Main
Local
Identifier Type
Local WAN (Internet) IP
Identifier
180.175.41.194
Remote
Identifier Type
Remote WAN (Internet) IP
Identifier
101.91.99.246
IKE SA Parameters
Encryption Algorithm
3DES
Authentication Algorithm
MD5
Authentication Method
Pre-Shared Key
Pre-Shared Key
ipsectest
Diffie-Hellman (DH) Group
Group2 (1024 bit)

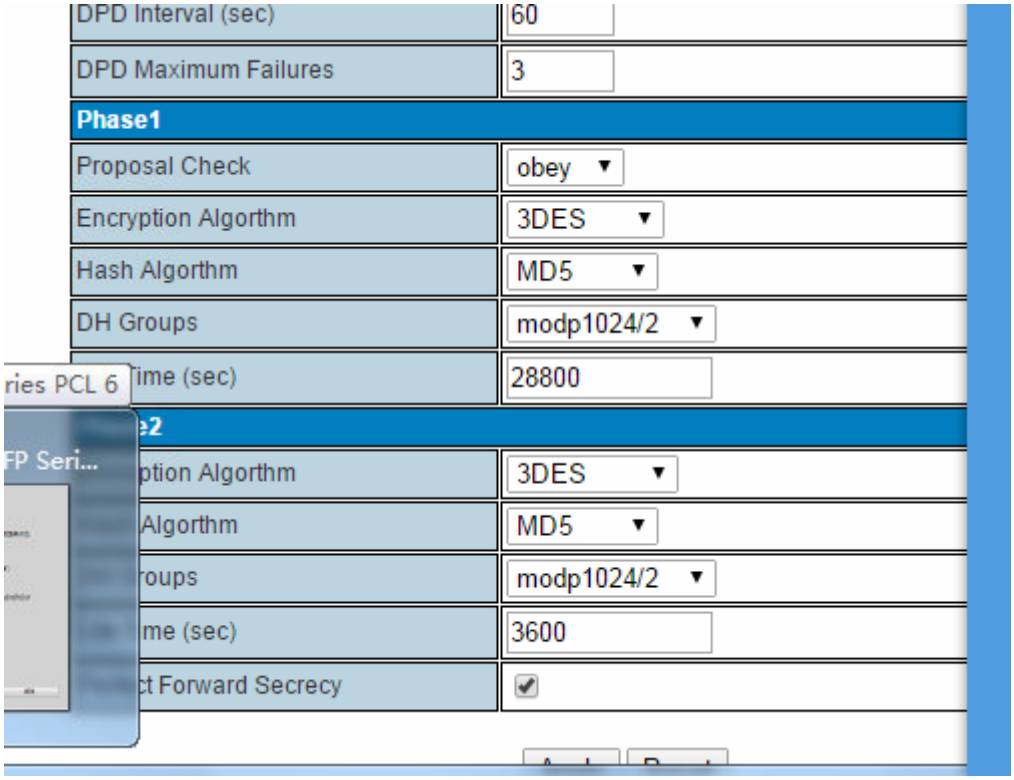

IKE SA Parameters
Encryption Algorithm
3DES
Authentication Algorithm
MD5
Authentication Method
Pre-Shared Key
Pre-Shared Key
ipsectest
Diffie-Hellman (DH) Group
Group2 (1024 bit)
SA-Lifetime
28800
Seconds
Dead Peer Detection
Enable
Detection Period
10
(Range : 10 - 999)
Reconnect after Failure Count
3
(Range : 3 - 99)
Extended Authentication
XAUTH Type
None
Authentication Type
User Database
Username
Password
Save
Cancel
Back

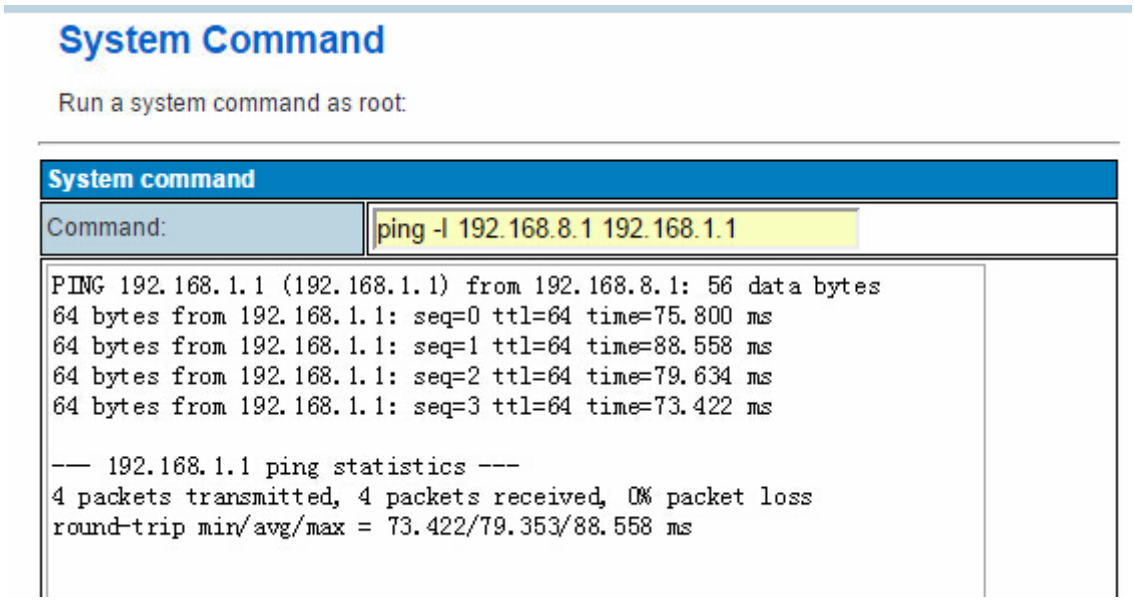

Advanced VPN Setup
Add / Edit VPN Policy Configuration
Policy Name
cwt201505.f3322.net
Policy Type
Auto Policy
Remote Endpoint
FQDN
cwt201505.f3322.net
NETBIOS
Enable
Local Traffic Selection
Local IP
Subnet
Start Address
192.168.1.0
End Address
Subnet Mask
255.255.255.0
Remote Traffic Selection
Remote IP
Subnet
This field is n
Start Address
192.168.8.0
End Address
Subnet Mask
255.255.255.0



3) set E-Lins router IPSec.







Notes:

1) If sometimes the settings are correct but IPSec VPN cannot connect, try to re-start the IPSec settings.
2) The IP should be correct for settings. If your IP is dynamic, please double check this.
3) If PC1 and PC2 cannot be through, check the PC firewall if it's closed.
4) For main mode, the both sides' WAN IP should be visit each other. And ID/FQDN should use IP instead of name if cannot connect.