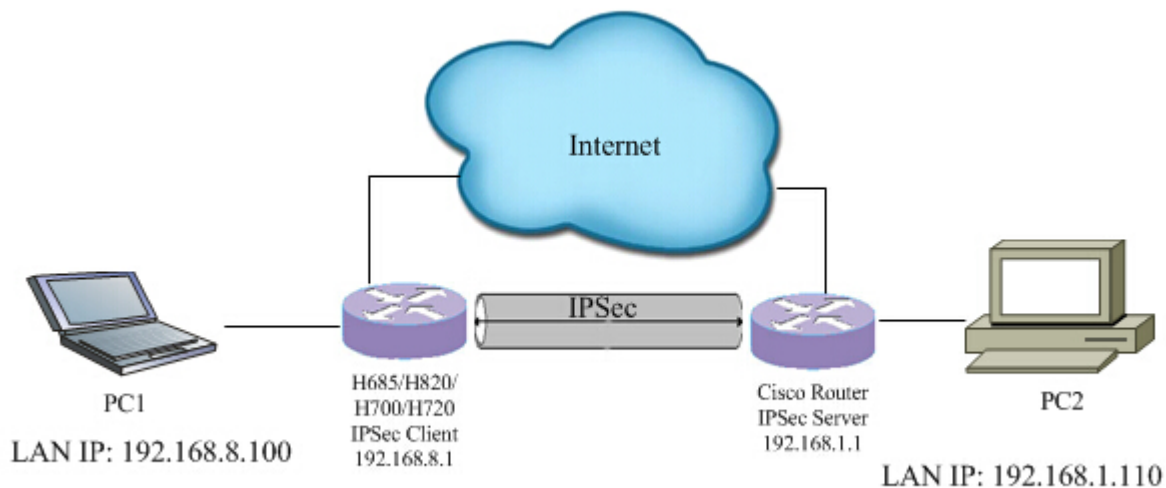


## H685/H820/H7X0 and Cisco RV180W with DDNS IPSec VPN in Main Mode

### 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	<input type="text" value="cwt201505.f3322.net"/>
Direction / Type	<input type="text" value="Both"/>
Exchange Mode	<input type="text" value="Main"/>
<b>Local</b>	
Identifier Type	<input type="text" value="Local WAN (Internet) IP"/>
Identifier	<input type="text" value="180.175.41.194"/>
<b>Remote</b>	
Identifier Type	<input type="text" value="Remote WAN (Internet) IP"/>
Identifier	<input type="text" value="101.91.99.246"/>
<b>IKE SA Parameters</b>	
Encryption Algorithm	<input type="text" value="3DES"/>
Authentication Algorithm	<input type="text" value="MD5"/>
Authentication Method	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key	<input type="text" value="ipsectest"/>
Diffie-Hellman (DH) Group	<input type="text" value="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	<input checked="" type="checkbox"/> 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	

## Advanced VPN Setup

### Add / Edit VPN Policy Configuration

Policy Name

Policy Type

Remote Endpoint

NETBIOS  Enable

### Local Traffic Selection

Local IP

Start Address

End Address

Subnet Mask

### Remote Traffic Selection

Remote IP

◀ This field is n

Start Address

End Address

Subnet Mask

Key-Out

**Auto Policy Parameters**

SA-Lifetime: 3600  
Seconds

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

PFS Key Group:  Enable  
DH-Group 2 (1024 bit)

Select IKE Policy: cwt201505.f3322.net

Auto Initiate:  Enable  
View

Save Cancel Back

### 3) set E-Lins router IPsec.

## IPSEC VPN

IPSEC	
Name (ID/FQDN)	cwt201505.f3322.net
Service Mode	Client
Exchange Mode	Main
Gateway	cwt20150529.f3322.net
Local Network Type	Subnet
Local IP	192.168.8.0 : 24
Remote Network Type	Subnet
Remote IP	192.168.1.0 : 24
Auth method	Pre Shared Key
Password	.....
Interface	WAN
	Advance

DPD Interval (sec)	60
DPD Maximum Failures	3
<b>Phase1</b>	
Proposal Check	obey ▼
Encryption Algorithm	3DES ▼
Hash Algorithm	MD5 ▼
DH Groups	modp1024/2 ▼
Phase1 Time (sec)	28800
<b>Phase2</b>	
Encryption Algorithm	3DES ▼
Hash Algorithm	MD5 ▼
DH Groups	modp1024/2 ▼
Phase2 Time (sec)	3600
Perfect Forward Secrecy	<input checked="" type="checkbox"/>

## System Command

Run a system command as root:

System command	
Command:	ping -l 192.168.8.1 192.168.1.1
<pre> PING 192.168.1.1 (192.168.1.1) from 192.168.8.1: 56 data bytes 64 bytes from 192.168.1.1: seq=0 ttl=64 time=75.800 ms 64 bytes from 192.168.1.1: seq=1 ttl=64 time=88.558 ms 64 bytes from 192.168.1.1: seq=2 ttl=64 time=79.634 ms 64 bytes from 192.168.1.1: seq=3 ttl=64 time=73.422 ms  --- 192.168.1.1 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 73.422/79.353/88.558 ms                     </pre>	

### 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.