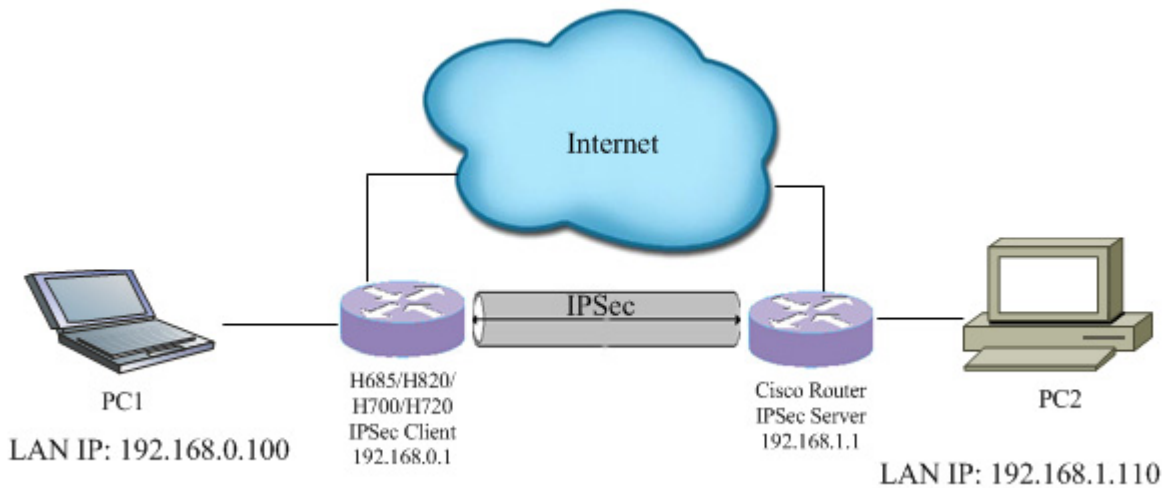


# H685/H820/H7X0 and Cisco IPSec VPN in Main Mode

## Typical Simple Diagram



### 1) check for Cisco router WAN IP and LAN IP

### 2) set IKE Cisco router IPSec

Select Tunnel Entry:

IPSec VPN Tunnel:  Enable  Disable

Tunnel Name:

---

**Local Group Setup**

Local Security Gateway Type:

IP address:

Local Security Group Type:

IP Address:

Subnet Mask:

**Remote Group Setup**

Remote Security Gateway Type:    
 This Gateway accepts requests from any IP address.

Remote Security Group Type:

IP Address:

Subnet Mask:

**IPSec Setup**

Keying Mode:

**Phase 1:**

Encryption:

Authentication:

Group:

Key Lifetime:  sec

**Phase 2:**

Encryption:

Authentication:

Perfect Forward Secrecy:

Preshared Key:

Group:

Key Lifetime:  sec

**Status**

Up

---

**Advanced**

Aggressive Mode

NetBios Broadcast

---

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

Name (ID/FQDN)	test
Service Mode	Client ▾
Exchange Mode	Main ▾
Gateway	112.95.34.154
Local Network Type	Subnet ▾
Local IP	192.168.0.0 : 24
Remote Network Type	Subnet ▾
Remote IP	192.168.1.0 : 24
Auth method	Pre Shared Key ▾
Password	••••
Interface	WAN ▾
	Advance
NAT Traversal	<input checked="" type="checkbox"/>
DPD Check	<input checked="" type="checkbox"/>
DPD Interval (sec)	60
DPD Maximum Failures	3
<b>Phase1</b>	
Proposal Check	obey ▾
Encryption Algorithm	3DES ▾
Hash Algorithm	MD5 ▾
DH Groups	modp1024/2 ▾
Life Time (sec)	28800
<b>Phase2</b>	
Encryption Algorithm	3DES ▾
Hash Algorithm	MD5 ▾
DH Groups	modp1024/2 ▾
Life Time (sec)	3600
Perfect Forward Secrecy	<input type="checkbox"/>

**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.