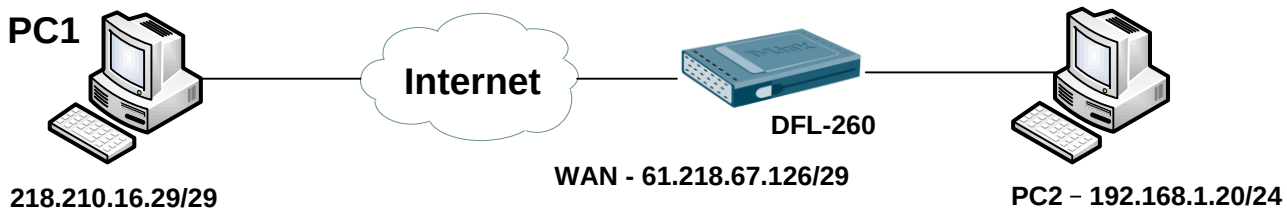
How to set up IKE Config Mode VPN

[Foreword]

1) Use IKE Config Mode to create VPN tunnel.

[Topology]



[Setup]

1. Create Interface Addresses Objects

   Objects > Address Book > InterfaceAddresses

#	Name	Address	User Auth Groups	Comments
1	wan_ip	61.218.67.126		IPAddress of interface wan
2	wannet	61.218.67.120/29		The network on interface wan
3	wan_gw	61.218.67.121		Default gateway for interface wan.
4	wan_dns1	0.0.0.0		Primary DNS server for interface wan.
5	wan_dns2	0.0.0.0		Secondary DNS server for interface wan.
6	lan_ip	192.168.1.1		IPAddress of interface lan
7	lannet	192.168.1.0/24		The network on interface lan
8	dmz_ip	172.17.100.254		IPAddress of interface dmz
9	dmznet	172.17.100.0/24		The network on interface dmz
10	IPSec_Pool	192.168.1.200-192.168.1.220		
11	LAN_Mask	255.255.255.0		
12	Google_DNS	8.8.8.8		
13	HiNet_DNS	168.95.1.1		

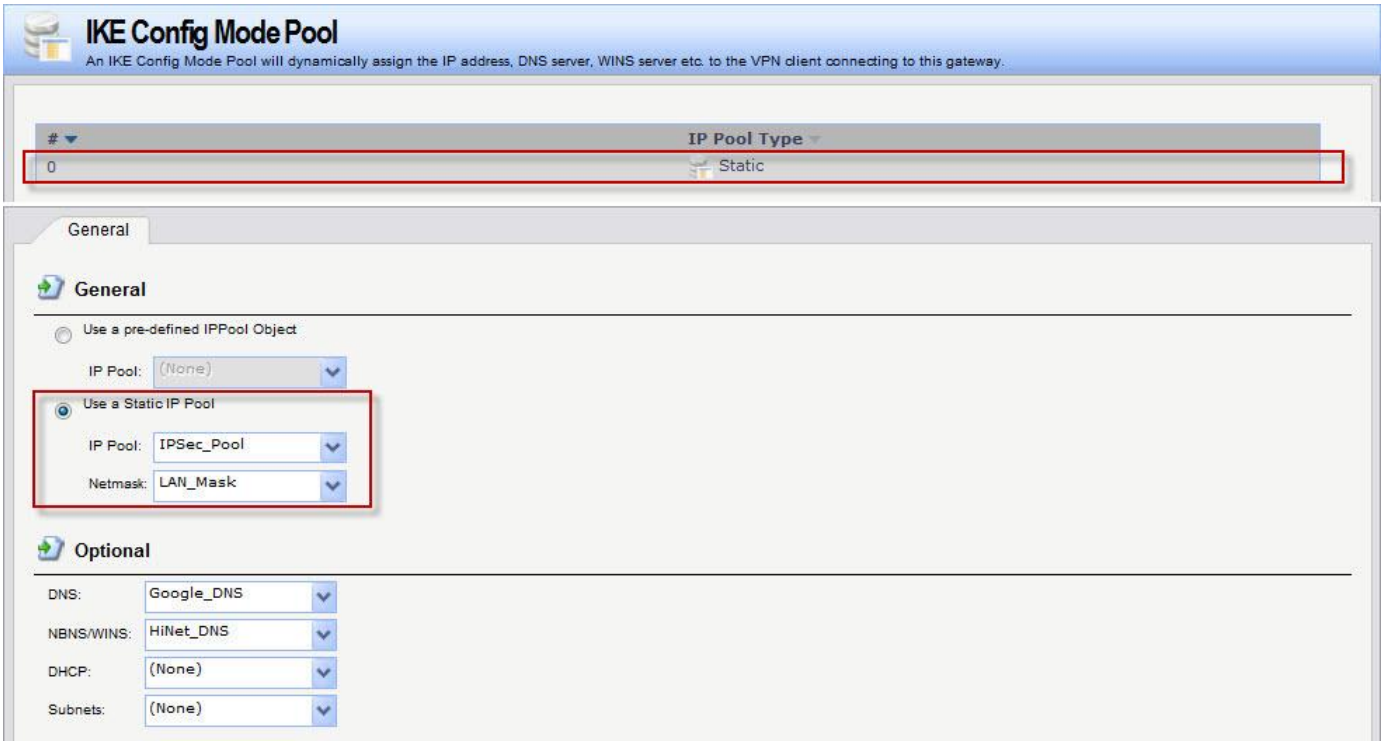
2. Create Authentication Objects

   Objects > Authentication Objects

#	Name	Type	Type	Comments
1	HTTPSAdminCert	Certificate	Local	
2	Key	Pre-Shared Key	ASCII	

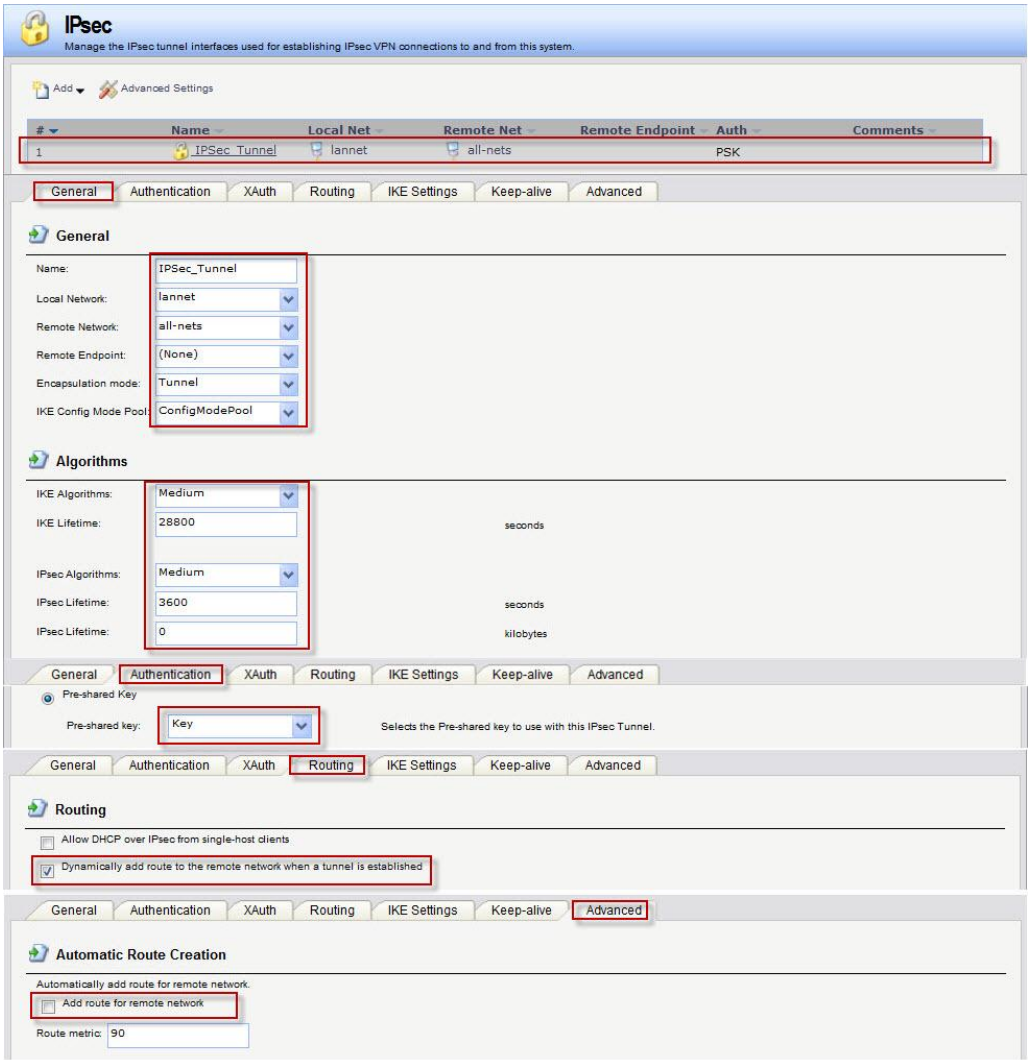
3. Create VPN Objects for IKE Config Mode Pool

   Objects > VPN Objects > IKE Config Mode Pool

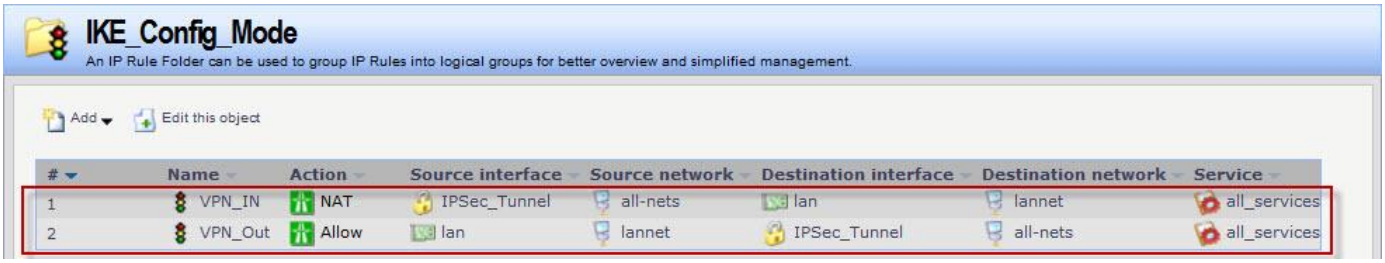


4. Create IPsec Interfaces

   Interfaces > IPsec



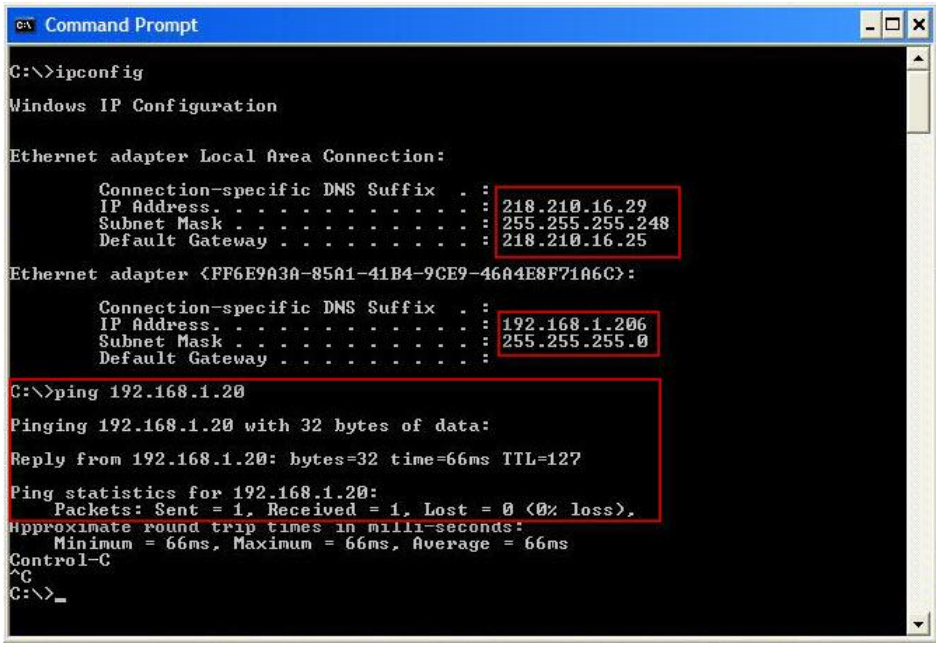
5. Create IP Rules



[Test & Confirm]

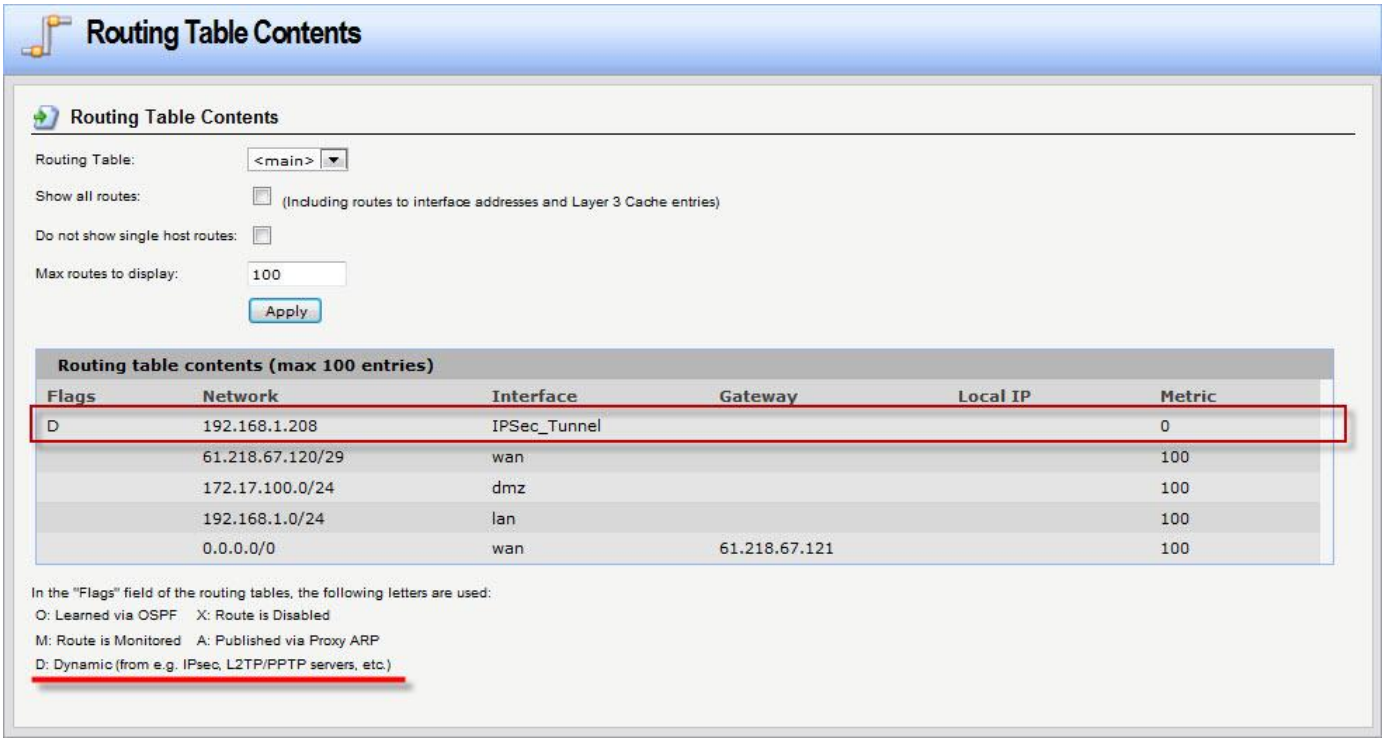
If PC1 connection success to firewall. You can follow those notices to check VPN tunnel.

1. PC1 ping PC2
2. Use ipconfig command on PC1. Check PC1 isn't it use IP-Pool range IP.



3. Check Firewall route states.

   Status > Routes



4. Firewall command line

```
DFL-260:/> ikesnoop

Ike snooping is not active
DFL-260:/> ikesnoop -on -verbose

Ike snooping is active - verbose mode; snooping address *
DFL-260:/>
```

When PC1 connection VPN. Use same command in firewall. (ikesnoop –on –verbose) (ikesnoop -off)

```
    Notification : DPD R-U-THERE-ACK

2011-08-10 09:37:07: IkeSnoop: Received IKE packet from 218.210.16.29:500
Exchange type  : Informational
ISAKMP Version : 1.0
Flags          : E (encryption)
Cookies        : 0xd48162bc1b55e46f -> 0x5a61d8726081a629
Message ID     : 0x23e51c1a
Packet length  : 80 bytes
# payloads     : 2
Payloads:
  HASH (Hash)
    Payload data length : 16 bytes
  N (Notification)
    Payload data length : 28 bytes
    Protocol ID  : ISAKMP
    Notification : DPD R-U-THERE
```

Use routes command

```
routes
Flags Network            Iface          Gateway         Local IP        Metric
----- ------------------ -------------- --------------- --------------- ------
D     192.168.1.207      IPSec_Tunnel                                   0
      61.218.67.120/29   wan                                            100
      172.17.100.0/24    dmz                                            100
      192.168.1.0/24     lan                                            100
      0.0.0.0/0          wan            61.218.67.121                   100
```

END