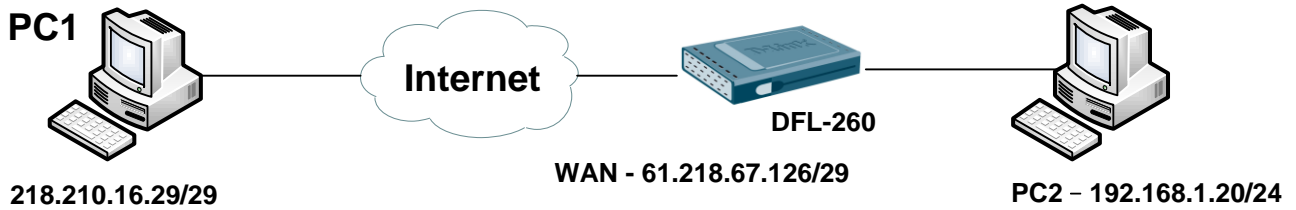


## How to set up IKE Config Mode VPN

[Foreword]

1) Use IKE Config Mode to create VPN tunnel.

[Topology]



[Setup]

1. Create Interface Addresses Objects

Objects > Address Book > InterfaceAddresses

The screenshot shows the 'InterfaceAddresses' configuration page. The page title is 'InterfaceAddresses' and it contains a table of address objects. A red box highlights rows 10 through 13.

#	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

The screenshot shows the 'Authentication Objects' configuration page. The page title is 'Authentication Objects' and it contains a table of authentication objects. A red box highlights row 2.

#	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

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	VPN_IN	NAT	IPSec_Tunnel	all-nets	lan	lannet	all_services
2	VPN_Out	Allow	lan	lannet	IPSec_Tunnel	all-nets	all_services

[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.

```

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 218.210.16.29
    Subnet Mask . . . . . : 255.255.255.248
    Default Gateway . . . . . : 218.210.16.25

Ethernet adapter <FF6E9A3A-85A1-41B4-9CE9-46A4E8F71A6C>:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.206
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time=66ms TTL=127

Ping statistics for 192.168.1.20:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 66ms, Maximum = 66ms, Average = 66ms
Control-C
^C
C:\>_
  
```

3. Check Firewall route states.

Status > Routes

Flags	Network	Interface	Gateway	Local IP	Metric
D	192.168.1.208	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

In the "Flags" field of the routing tables, the following letters are used:  
 O: Learned via OSPF    X: Route is Disabled  
 M: Route is Monitored    A: Published via Proxy ARP  
 D: Dynamic (from e.g. IPsec, L2TP/PPTP servers, etc.)

#### 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