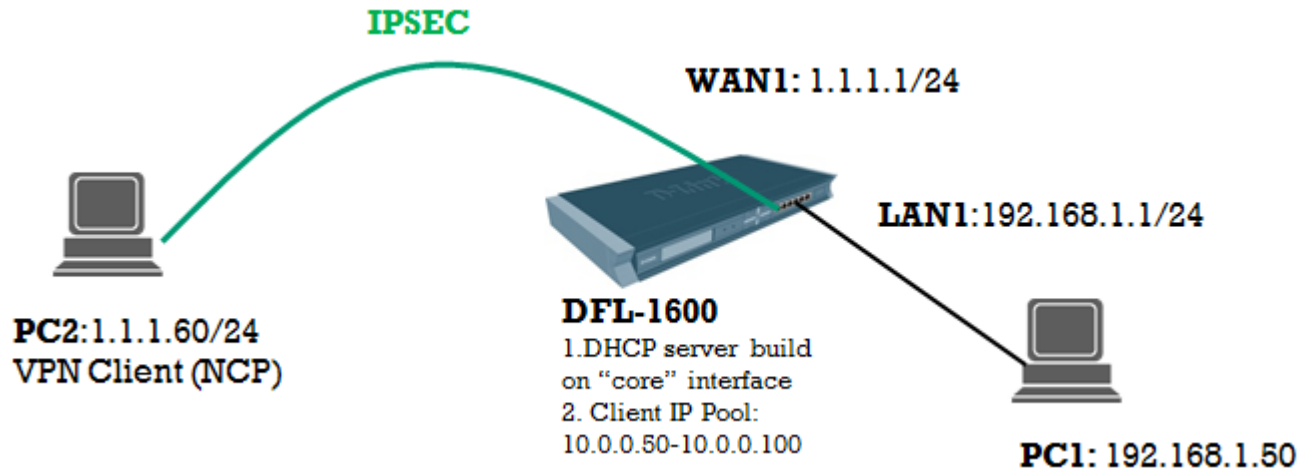


In current scenario, we have to build up a dynamic IPSEC VPN server in Netdefend series for roaming users(the provided software is NCP VPN client). The roaming users have to dynamically get IP address from DHCP server of firewall during the IKE-phase2, it's so-called "IKE-Config-mode".



[Solution]

The settings of DFL-1600

=====

```
set Interface Ethernet wan1 DHCPEnabled=No
set Address IP4Address InterfaceAddresses/wan1_ip Address=1.1.1.1
set Address IP4Address InterfaceAddresses/wan1net Address=1.1.1.0/24
add Address IP4Address dhcp-server-ipsec Address=127.0.0.1
add PSK ipsec-psk Type=ASCII PSKAscii=testtest
```

```
add Interface IPsecTunnel ipsec-if IKEAlgorithms=Medium IPsecAlgorithms=Medium
LocalNetwork=InterfaceAddresses/lan1net RemoteNetwork=all-nets AuthMethod=PSK PSK=ipsec-
psk AutoInterfaceNetworkRoute=No AddRouteToRemoteNet=Yes
```

```
add DHCPServer dhcp-on-ipsec Interface=core IPAddressPool=10.0.0.50-10.0.0.100
Netmask=255.255.255.0 LogEnabled=Yes
```

```
add IPPool ippool-for-ike Interface=core DHCPSType=ServerIP ServerIP=dhcp-server-ipsec
add ConfigModePool IPPoolType=PreDefined IPPool=ippool-for-ike
set Interface IPsecTunnel ipsec-if IKEConfigModePool=ConfigModePool
add Interface InterfaceGroup ipsec-lan1 Members=ipsec-if,lan1
```

```
add IPRule Action=Allow SourceInterface=ipsec-lan1 SourceNetwork=all-nets
DestinationInterface=ipsec-lan1 DestinationNetwork=all-nets Service=all_services Index=1
LogEnabled=Yes Name=ipsec-lan1-allow
```

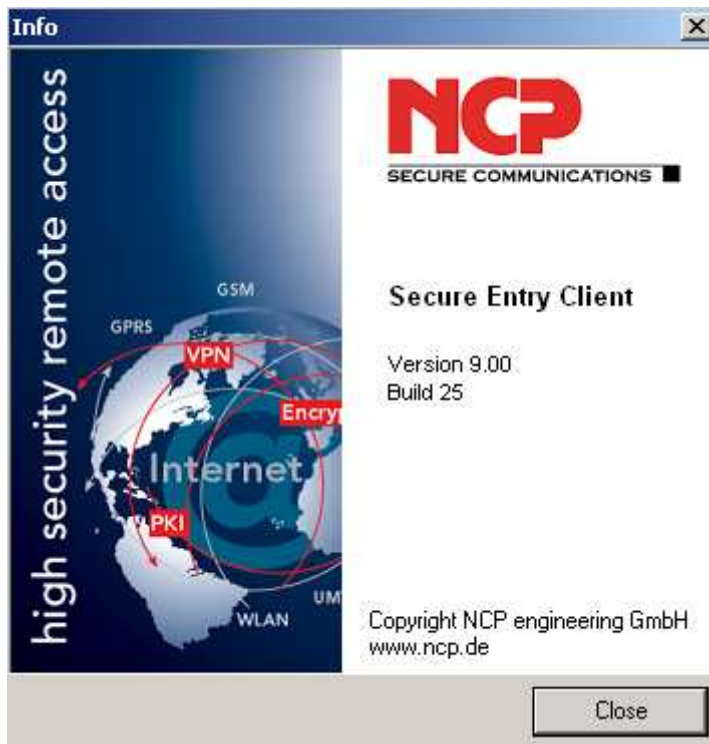
```
set IPRule 2(ping_fw) SourceInterface=ipsec-lan1 SourceNetwork=all-nets LogEnabled=Yes
```

=====

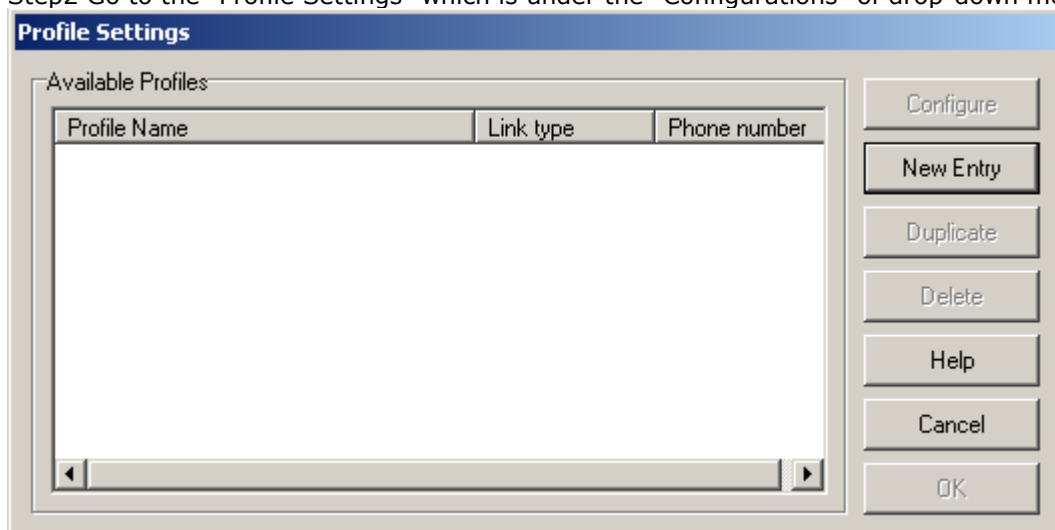
The settings of NCP

=====

Step1. Make sure the NCP software version you have is the same with the current scenario.(NCP.9.00)



Step2 Go to the "Profile Settings" which is under the "Configurations" of drop-down menu.



Step3 Create a New Entry and select the "Connection Type" to the first option below:

**Assistant for new profile** ✕

**Connection Type**  
Define type of connection **NCP**

**Link to Corporate Network using IPSec**  
Create a link to the corporate network over a Virtual Private Network (VPN) secured by IPSec.


**Link to the Internet**  
Create a connection to the Internet (No VPN).

Step4 Name the current profile.

**Assistant for new profile** ✕

**Connection Name**  
Enter the name of the connection **NCP**

The connection may be given a descriptive name; enter a name in the following field.


 **Name of the connection :**

Step5 Select the "Communication Media".

**Assistant for new profile** ✕

**Link type (Dial up configuration)**  
Select the media type of the connection. **NCP**

Determine how the connection to the corporate network should be established. If the Internet is to be used via modem, set the communication media to "modem" and then select the appropriate modem.


 Communication media :

Step6 Set the IP address of VPN server, in current case the value shall be filled in 1.1.1.1.


**Assistant for new profile** ✕

**VPN gateway parameters**  
To which VPN gateway should the connection be established? **NCP**

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.  
Using Extended Authentication (XAUTH) you can enter the Username and Password for the authentication. If no authentication data are entered they will be requested when establishing the connection.


 Gateway :

Use extended authentication (XAUTH)


 Username :


Password : 
                     Password (Confirm) :

Step7 Set the "Exchange mode" to "Main Mode" and none PFS feature enable.

**Assistant for new profile** X

**IPSec Configuration**  
Configure the basic IPSec parameters **NCP**

The basic IPSec parameters can be specified here. The IPSec negotiations will use "automatic mode" which are pre-defined (default) proposals. In the event that uniquely defined IKE- / IPSec policies are to be used, these can then be defined and assigned using the Policy Editor under IPSec Generally Settings.

 Exchange mode :

PFS group :

Use IP compression


Step8 Set the value of "Pre-shared key", in current case the value is "testtest".

**Assistant for new profile** X


**Pre-shared key**  
Common secret for data encryption **NCP**

A shared secret or pre-shared key is used to encrypt the connection; this then needs to be identically configured on both sides (VPN client and VPN gateway).

Enter the appropriate value for the IKE ID according to the selected ID type.

 Pre-shared key \_\_\_\_\_

Shared secret :  Confirm secret :

 Local identity \_\_\_\_\_

Type :

ID :


Step9 Set "Use IKE Config Mode" here.

**Assistant for new profile** X


**IPSec Configuration - IP addresses**  
Assigning the IP address to the client **NCP**

Specify which IP address the client is going to use. By selecting "Use IKE Config Mode" the client's IP address is dynamically assigned by the VPN gateway.

Furthermore, define where the DNS / WINS servers (if used) can be found.

 IP address assignment

IP address :  Subnet mask :


 DNS / WINS servers  
 DNS server :  WINS server :

Step10 No firewall enable.

**Assistant for new profile** X

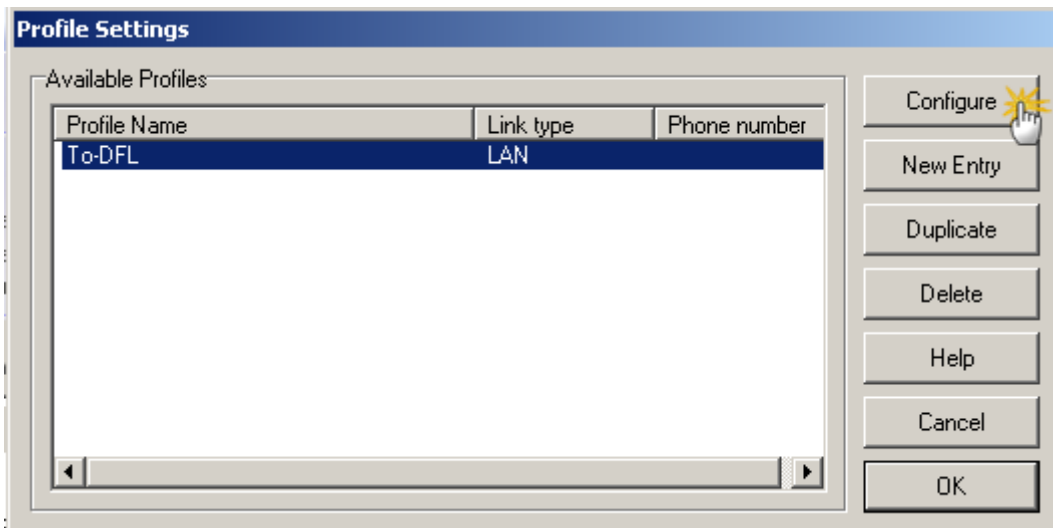
**Firewall Settings**  
Select and enable different firewall features **NCP**

Activate the desired firewall options. Enabling Stateful Inspection will discard packets from other hosts. Optionally, NetBIOS over IP can also be enabled.

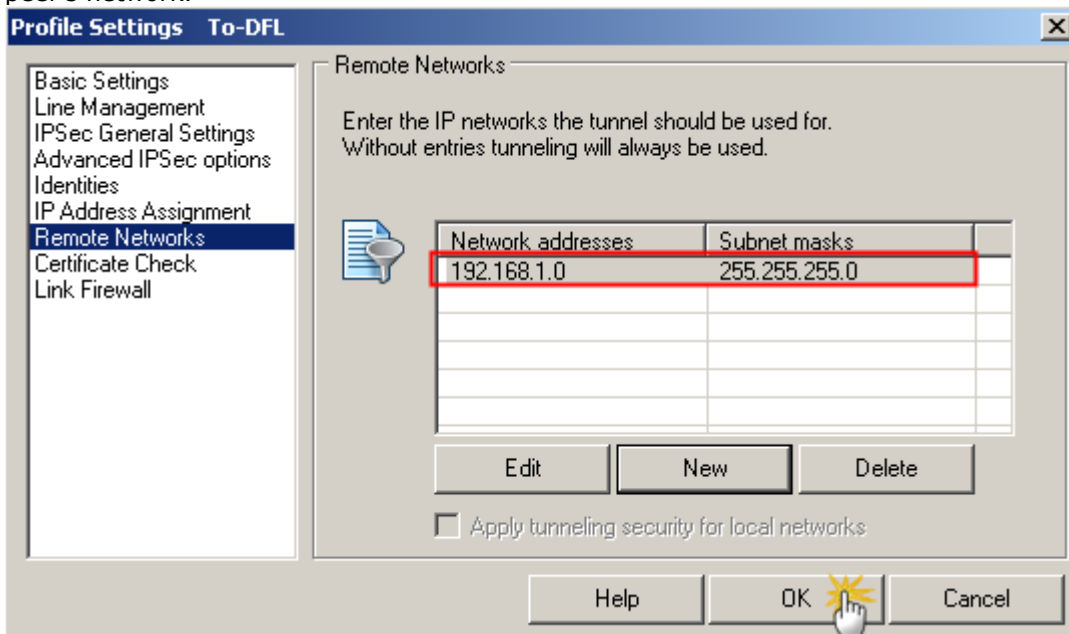
 Firewall  
 Enable Stateful Inspection :

Only communication within the tunnel permitted  
 Enable NetBIOS over IP

Step11 Enter into the created object: "To-DFL" in order to set the "Remote network".



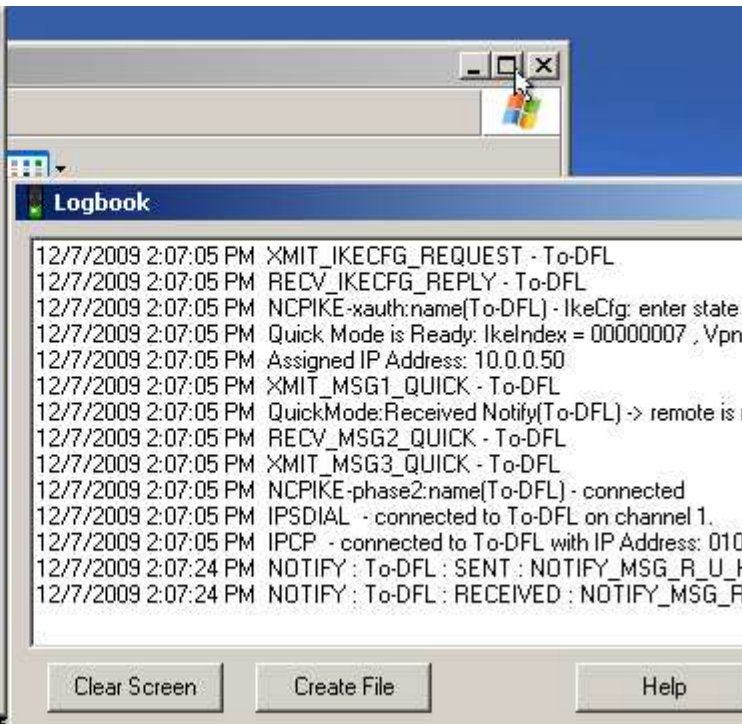
Step12 Go to the setting page of "Remote Networks", and add a new entry which points to remote peer's network.



Step13 After end of above settings, try to build up a VPN tunnel to firewall.



Step14 Tunnel has been built.



=====  
 [Troubleshooting]  
 Via CLI in DFL:  
 =====  
**Before the tunnel establish.**

```

DFL-1600:/> ippool -show -verbose
ippool-for-ike:
  In progress:
    0 instances

```



```

Free maintained in pool:
 10.0.0.50/255.255.255.0 (00-00-00-00-00-00) (BCAST:10.0.0.255)
 10.0.0.53/255.255.255.0 (00-00-00-00-00-00) (BCAST:10.0.0.255)
 10.0.0.52/255.255.255.0 (00-00-00-00-00-00) (BCAST:10.0.0.255)
 10.0.0.51/255.255.255.0 (00-00-00-00-00-00) (BCAST:10.0.0.255)
Used by subsystems:

```

```
DFL-1600:/> dhcpserver -show
```

```
Active DHCP sessions:
```

Rule	Iface	Client MAC	Client IP	Expire
1	core	*00-00-00-00-00-00	10.0.0.50	85978
1	core	*00-00-00-00-00-00	10.0.0.51	85980
1	core	*00-00-00-00-00-00	10.0.0.52	85980
1	core	*00-00-00-00-00-00	10.0.0.53	85980

**After tunnel established.**

```
DFL-1600:/> routes -verbose
```

Flags	Network	Iface	Gateway	Local IP	Metric
D	10.0.0.50	ipsec-if		0	
	Originator: IPsec interface with automatically added client routes				
	1.1.1.0/24	wan1		100	
	192.168.120.0/24	wan2		100	
	172.17.100.0/24	dmz		100	
	192.168.1.0/24	lan1		100	
	192.168.2.0/24	lan2		100	
	192.168.3.0/24	lan3		100	
	0.0.0.0/0	wan1		100	

```
DFL-1600:/> ippool -show -verbose
```

```
ippool-for-ike:
```

```
In progress:
```

```
0 instances
```

```
Free maintained in pool:
```

```
 10.0.0.53/255.255.255.0 (00-00-00-00-00-00) (BCAST:10.0.0.255)
```

```
 10.0.0.52/255.255.255.0 (00-00-00-00-00-00) (BCAST:10.0.0.255)
```

```
 10.0.0.51/255.255.255.0 (00-00-00-00-00-00) (BCAST:10.0.0.255)
```

```
Used by subsystems:
```

```
10.0.0.50/255.255.255.0 (00-00-00-00-00-00) (BCAST:10.0.0.255)
```

```
DFL-1600:/> dhcpserver -show
```

```
Active DHCP sessions:
```

Rule	Iface	Client MAC	Client IP	Expire
1	core	*00-00-00-00-00-00	10.0.0.50	85415
1	core	*00-00-00-00-00-00	10.0.0.51	85417
1	core	*00-00-00-00-00-00	10.0.0.52	85417
1	core	*00-00-00-00-00-00	10.0.0.53	85417

```
DFL-1600:/>
```

```
=====
```