ProCurve VPN Client and ProCurve Secure Router 7000dl Series

Introduction

Customers today work from a variety of locations and settings; this is the *mobile worker*. Equipped with laptop and access to a Hotpoint, or in a hotel with high-speed Internet, they continuing the day's tasks taking advantage of flexibility these technologies afford. Working on sensitive and private information within a public setting requires secure technologies. The ProCurve VPN Client provides such security with industry standard IPSec tunneling capabilities that form the virtual private network (VPN) to your ProCurve Secure 7000dl series router.

The IT professional who configures such a solution for the employees in their company can use this application note to understand the configuration of such access. This application note will explain how to configure a VPN tunnel between a ProCurve 7000dl series router, running SROS J.01.02B or greater, using the ProCurve VPN client software (version 10.3). This configuration approach utilizes "Mode config", and simplifies client configuration by dynamically assigning the VPN client an IP address for VPN traffic. "Mode config" allows the administrator to import the same security policy to each VPN client.

Included on this document are:

- Step by step instructions to configure VPN in on the ProCurve 7000dl series router.
- Full sample configuration of the ProCurve 7000dl series with firewall and VPN.
- Step by step instructions, with screen shots, to configure ProCurve VPN client on your laptop or PC.

This application note assumes the ProCurve 7000dl series router is already installed and has connectivity to a network. The Internet is shown in Figure 1 as an example. It is further assumed that the ProCurve VPN client software is already installed on the user's PC and the PC has access to the network or Internet.

Note: It is very important to verify with your ISP that they will allow ESP traffic (protocol 50) and AU (protocol 51) through their network. ESP is the protocol that carries the encrypted data of your VPN across the Internet. Some ISPs require a corporate or business class of service before they will allow ESP through.

In Figure 1 on the right is a user requiring access to the remote network (10.24.25.0/24). The ProCurve 7000dl router and ProCurve VPN client software will be setup using "mode config". "Mode config" allows the ProCurve 7000dl series to dynamically assign an IP address to the VPN client. (This is not address assigned to the client manually or DHCP but an additional address for the tunnel.) The dynamic IP address range for this example will be 192.168.4.1 through 192.168.4.5. On the right is a ProCurve 7000dl router with a WAN IP address of 172.16.1.2 and a mask of 255.255.255.252. The LAN network behind the ProCurve 7000dl router is also a private network 192.168.100.0 with a mask of 255.255.255.0.

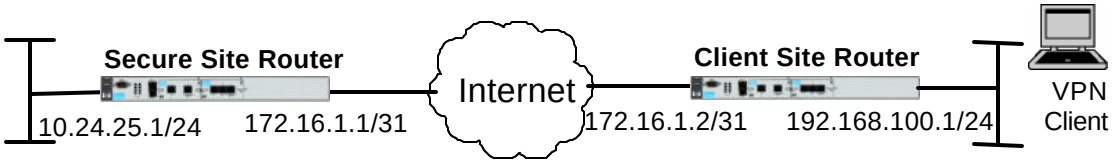

Figure 1 Sample network diagram

ProCurve 7000dl series configuration (Client Site Router)

1. Reset Router to Factory Defaults

A) Open a VT-100 session with the ProCurve Secure Router. Use the HyperTerminal icon on your desktop with the following settings:

(1) Baud Rate = 9600
(2) Parity = None
(3) Data Bits = 8
(4) Stop Bits = 1
(5) Flow Control = None

B) Press <Enter> on the keyboard and the access prompt should appear. Enter into Enable Mode by typing 'enable' and factory default the ProCurve Secure Router using the following commands:

```
ProCurveSR7102dl# erase startup-config      // Erase start-up configuration file
ProCurveSR7102dl# reload                    // Reload/reboot the router
```

C) Enter <n> for 'no' when asked if wanting to save system configuration.

D) Enter <y> for 'yes' when asked if wanting to reboot system.

E) Re-establish the connection and log back in to the Enable Mode.

2. Configure the Ethernet Interface 0/1

A) Type 'enable' to enter the enable mode, the 'config t' to enter the Global Configuration Mode.

B) Type 'hostname CleintSiteRouter' to change the host name on the ProCurve Secure Router.

C) Type 'interface ethernet 0/1' to access the configuration parameters for the Ethernet port located on the front panel of the router.

D) Type 'ip address 192.168.100.1 255.255.255.0' to assign an IP address to the ethernet port using a 24 bit subnet mask.

E) Type ‘no shutdown’ to activate the interface to pass data.
F) Type ‘exit’ to return to the Global Configuration mode.

3. Configure the T-1 Interface 1/1

A) Type ‘interface t1 1/1’ to enter configuration of the T1 interface on slot 1 port 1
B) Type ‘tdm-group 1 timeslots 1-24’ to map channels 1 through 24 on the T1 to a TDM group number 1
C) Type ‘no shutdown’ to active the T-1 interface
D) Type ‘exit’ to exit back to the Global Configuration Mode
E) Type ‘interface ppp 1’ to create a PPP interface number 1
F) Type ‘ip address 172.16.1.2 /31’ to assign an IP address to the ppp interface using a 31 bit subnet mask.
G) Type ‘no shutdown’ to activate the PPP interface.
H) Type ‘exit’ to return back to the Global Configuration Mode the type ‘bind 1 t1 1/1 1 ppp 1’ to create a bind name 1 and bind the t-1 1/1 interface with TDM group number 1 to the PPP 1 interface.
I) Type ‘exit’ to return to the Enable Mode then type ‘write memory’ to save the configuration to non-volatile memory.

4. Create a Static Route to the Secure Site Router

A) From the Global Configuration Mode type ‘ip route 10.24.25.0 255.255.255.0 ppp 1’ to create a static route to the internal network on the secure site router and attach it to the PPP 1 interface.

ProCurve 7000dl series configuration (Secure Site Router)

1. Reset Router to Factory Defaults

A) Open a VT-100 session with the ProCurve Secure Router. Use the HyperTerminal icon on your desktop with the following settings:
   (1) Baud Rate = 9600
   (2) Parity = None
   (3) Data Bits = 8
   (4) Stop Bits = 1
   (5) Flow Control = None

B) Press <Enter> on the keyboard and the access prompt should appear. Enter into Enable Mode by typing ‘enable’ and factory default the ProCurve Secure Router using the following commands:

```
ProCurveSR7102dl# erase startup-config      // Erase start-up configuration file
ProCurveSR7102dl# reload                    // Reload/reboot the router
```

C) Enter <n> for ‘no’ when asked if wanting to save system configuration.
D) Enter <y> for ‘yes’ when asked if wanting to reboot system.
E) Re-establish the connection and log back in to the Enable Mode.

2. Configure the Ethernet Interface 0/1

A) Type ‘enable’ to enter the enable mode, the ‘config t’ to enter the Global Configuration Mode.

B) Type 'hostname SecureSiteRouter' to change the host name on the ProCurve Secure Router.
C) Type 'interface ethernet 0/1' to access the configuration parameters for the Ethernet port located on the front panel of the router.
D) Type 'ip address 10.24.25.1 255.255.255.0' to assign an IP address to the ethernet port using a 24 bit subnet mask.
E) Type 'no shutdown' to activate the interface to pass data.
F) Type 'exit' to return to the Global Configuration mode.

3. Configure the T-1 Interface 1/1

A) Type 'interface t1 1/1' to enter configuration of the T1 interface on slot 1 port 1
B) Type 'tdm-group 1 timeslots 1-24' to map channels 1 through 24 on the T1 to a TDM group number 1
C) Type 'no shutdown' to active the T-1 interface
D) Type 'exit' to exit back to the Global Configuration Mode
E) Type 'interface ppp 1' to create a PPP interface number 1
F) Type 'ip address 172.16.1.1 /31' to assign an IP address to the ppp interface using a 31 bit subnet mask.
G) Type 'no shutdown' to activate the PPP interface.
H) Type 'exit' to return back to the Global Configuration Mode the type 'bind 1 t1 1/1 1 ppp 1' to create a bind name 1 and bind the t-1 1/1 interface with TDM group number 1 to the PPP 1 interface.
I) Type 'exit' to return to the Enable Mode then type 'write memory' to save the configuration to non-volatile memory.

4. Create a Static Route to the Secure Site Router

A) From the Global Configuration Mode type 'ip route 192.168.100.0 255.255.255.0 ppp 1' to create a static route to the internal network on the Client site router and attach it to the PPP 1 interface.

ProCurve 7000dl series VPN configuration

1. Configuration mode (Secure Site Router)

From the SecureSiteRouter> prompt, enter into priveliged mode by typying **enable**. If an enable password has been set, you will be prompted to enter it. You should now be at the enable prompt: SecureSiteRoute#. Next you will need to enter into configuration mode by typeing **config t**. **Once in configuration mode, you will need to activate the VPN process by using the command *ip crypto*.**

```
SecureSiteRouter> enable
SecureSiteRouter # config t
SecureSiteRouter(config)# ip crypto
```

Figure 2 Enabling VPN process

Note: not all configuration steps are covered in this document. Please reference the CLI output to determine any other steps not central to this topic.

Configuring IKE client configuration pool

a) The IKE client configuration pool contains the options to be passed to the client during IKE negotiation. Each pool must be given a label so that it may be referenced later in the IKE policy. The example below creates a configuration pool called “vpn_users”.

```
SecureSiteRouter(config)#  crypto ike client configuration pool vpn_users
```

Figure 3

b) Once a pool is created, enter the properties of that pool. The command **ip-range** is used to specify a block of address that will be assigned to remote clients when they negotiate a VPN connection. The command **dns-server** will set the IP address of the DNS server for remote clients. The command **netbios-name-server** is used to set the IP address of the Windows Internet Naming Service (WINS) server. If you wish to configure a secondary DNS or WINS server, the secondary address may be added directly after the primary address. The example below shows a DNS entry with both a primary and secondary server specified and a single WINS server configured.

Figure 4

```
SecureSiteRouter(config-ike-client-pool)# ip-range 192.168.4.1 192.168.4.5
SecureSiteRouter(config-ike-client-pool)# dns-server 192.168.100.2 192.168.100.3
SecureSiteRouter(config-ike-client-pool)# netbois-name-server 192.168.100.4
```

2. Configuring IKE policy

In order to use IKE negotiation, an IKE policy must be created. Within the system, a list of IKE policies is maintained. Each IKE policy is given a priority number in the system. That priority number defines the position of that IKE policy within the system list. When IKE negotiation is needed, the system searches through the list, starting with the policy with the lowest priority, looking for a match to the peer IP address.

The following IKE policy is configured to use any peer IP address since it is assumed the dial-up users will all have differing IP addresses. This IKE policy is set not to initiate a tunnel but respond to main or aggressive mode, use 3DES encryption and SHA1 hash. A pre-shared key will be used for authentication, Diffie-Hellman Group 1 and an IKE lifetime in seconds of 600.

```
SecureSiteRouter(config)#  crypto ike policy 10
SecureSiteRouter(config-ike)# peer any
SecureSiteRouter(config-ike)# no initiate
SecureSiteRouter(config-ike)# respond anymode
SecureSiteRouter(config-ike)# client configuration pool vpn_users
SecureSiteRouter(config-ike)# attribute 10
SecureSiteRouter(config-ike-attribute)# encryption 3des
SecureSiteRouter(config-ike-attribute)# hash sha
SecureSiteRouter(config-ike-attribute)# authentication pre-share
SecureSiteRouter(config-ike-attribute)# group 1
SecureSiteRouter(config-ike-attribute)# lifetime 600
```

Figure 5 Creating IKE policy

The **crypto ike remote-id** command is used to specify the remote-id information for a peer connecting to the system. This command is also used to specify the preshared-key associated with the specific remote-id. The VPN client will identify itself as remote.com and also have a pre-shared key of “ProCurve_Networking”.

```
SecureSiteRouter(config)# crypto ike remote-id fqdn remote.com preshared-key ProCurve_Networking
```

Figure 6 Setting remote-id information

3. IPSec transform

A transform-set defines the encryption and authentication algorithms to be used to secure the data transmitted over the VPN tunnel. In this example, a transform-set named “highly_secure” has been created. This transform-set defines ESP with Authentication to be implemented using 3DES encryption and SHA1 hash algorithm for authentication.

```
SecureSiteRouter(config)# crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac
SecureSiteRouter(cfg-crypto-trans)# mode tunnel
```

Figure 7 Creating IPSec attributes

4. Access Control List

An Extended Access Control List (ACL) is used to specify which traffic needs to be sent securely over the VPN tunnel. The entries in the list are defined with respect to the local system. For this sample configuration, the source is the LAN IP network behind the ProCurve 7000dl is 192.168.100.0. The destination is the vpn pool IP network (192.168.4.0) specified in the “client configuration pool vpn_users”

```
SecureSiteRouter(config)# ip access-list extended vpn_traffic
SecureSiteRouter(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 192.168.4.0 0.0.0.255
```

Figure 8 Specifying traffic to encrypt

6. Create Crypto Map

A Crypto Map is used to define a set of encryption schemes to be used for a given interface. A crypto map entry has a unique index within the crypto map set. This crypto map will encrypt traffic that matches access-list vpn_traffic, use the highly_secure transform, set the IPSec lifetime seconds to 1800 and will not use perfect forward secrecy.

```
SecureSiteRouter(config)#  crypto map corporate_vpn 1 ipsec-ike
SecureSiteRouter(config-crypto-map)# match address vpn_traffic
SecureSiteRouter(config-crypto-map)# set security-association lifetime seconds 1800
SecureSiteRouter(config-crypto-map)# no set pfs
```

Figure 9 Creating crypto map

7. Apply Crypto Map

The **crypto map** should be applied to the interface that will transmit the encrypted traffic to the remote peer. The example below shows the crypto map being applied to interface PPP 1. If your WAN protocol is frame-relay, you would apply the crypto map to the frame-relay interface.

```
SecureSiteRouter(config)#  interface ppp 1
SecureSiteRouter(config-ppp)# crypto map corporate_vpn
```

Figure 10 Applying crypto map to interface

8. Allow Traffic Through Firewall

a) If the firewall feature is enabled on the ProCurve 7000dl router, then Extended ACLs will need to be added to the configuration. IP access-list extended vpn_lan will use the following permit statement:

```
SecureSiteRouter(config)#  ip firewall
SecureSiteRouter(config)#  ip access-list extended VPN_to_LAN
SecureSiteRouter(config-ext-nacl)# permit ip 192.168.4.0 0.0.0.255 192.168.100.0 0.0.0.255
```

Figure 11 Permiting remote LAN traffic into local ProCurve 7000dl series

b) The Extended ACL must be added to the appropriate policy-class before they take affect. **NOTE: Policy-class names are case sensitive. The policy-class names below may need to be changed based on the current policy-class nomencalature. If a discard list MATCHALL statement is in the policy class be sure to remove it by using the no form of the command. Re-enter the discard list MATCHALL statement after entering new statements.** The UNTRUSTED policy class is used for traffic coming from the internet. This policy-class is attached to interface ppp 1. Figure 12 gives an example of the commands.

```
SecureSiteRouter(config)#  ip policy-class UNTRUSTED
SecureSiteRouter(config-ext-nacl)# no discard list MATCHALL (optional, see above text)
SecureSiteRouter(config-ext-nacl)# allow list VPN_to_LAN
SecureSiteRouter(config-ext-nacl)# discard list MATCHALL
```

Figure 12 Allow traffic specified by ACL into UNTRUSTED interface

c) An allow statement must be added to the TRUSTED policy class allowing vpn-traffic through the firewall to be encrypted. **NOTE: Policy-class names are case sensitive. The policy-class names below may need to be changed based on the current policy-class nomencalature. If a nat source list MATCHALL statement is in the policy-class be sure to remove it by using the no form of the command. Re-enter the nat source list MATCHALL statement after entering new statements.** The policy-class TRUSTED is attached to interface ethernet 0/1 interface.

```
SecureSiteRouter(config)#  ip policy-class TRUSTED
SecureSiteRouter(config-policy-class)# no nat source list MATCHALL interface ppp 1 overload
SecureSiteRouter(config-policy-class)# allow list vpn_traffic
SecureSiteRouter(config-policy-class)# nat source list MATCHALL interface ppp 1 overload
```

Figure 13 Allow traffic specified by ACL into TRUSTED interface

d) Finally, the UNTRUSTED policy class must be attached to the ppp 1 interface.

```
SecureSiteRouter(config)#  interface ppp 1
SecureSiteRouter(config-ppp 1)# access-policy UNTRUSTED
```

The “Secure Site” ProCurve 7000dl series router configuration used in the sample network is listed below:

```
!
hostname "SecureSiteRouter"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
ip firewall
!
!
!
!
!
!
ip crypto
!
crypto ike client configuration pool vpn_users
  ip-range            10.24.44.1       10.24.44.5
  dns-server          10.24.3.10
  netbios-name-server 192.168.100.4
!
crypto ike policy 10
  no initiate
  respond anymode
  peer any
  client configuration pool vpn_users
  attribute 10
    encryption 3des
    authentication pre-share
    lifetime 600
!
crypto ike remote-id fqdn remote.com preshared-key
ProCurve_Networking
!
crypto ipsec transform-set highly_secure esp-3des
esp-sha-hmac
  mode tunnel
!
crypto map corporate_vpn 1 ipsec-ike
  match address vpn_traffic
  set transform-set highly_secure
  set security-association lifetime seconds 1800
!
interface eth 0/1
  ip address  10.24.25.1  255.255.255.0
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
interface t1 1/1
  clock source line
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  clock source through
  shutdown
!
interface ppp 1
  ip address  172.16.1.1  255.255.255.0
  access-policy UNTRUSTED
  crypto map corporate_vpn
  peer default ip address 172.16.1.2
  no shutdown
  bind 1 t1 1/1 1 ppp 1
!
!
ip access-list standard MATCHALL
  permit any
!
ip access-list extended VPN_to_LAN
  permit ip 10.24.44.0 0.0.0.255  10.24.25.0
0.0.0.255
!
ip access-list extended vpn_traffic
  permit ip 10.24.25.0 0.0.0.255  10.24.44.0
0.0.0.255
!
ip policy-class TRUSTED
  allow list vpn_traffic
  nat source list MATCHALL interface ppp 1 overload
!
ip policy-class UNTRUSTED
  allow list VPN_to_LAN
  discard list MATCHALL
!
ip route 192.168.100.0 255.255.255.0 ppp 1
!
no ip tftp server
ip http server
ip http secure-server
ip snmp agent
no ip ftp agent
!
line con 0
  login local-userlist
!
line telnet 0 4
  login local-userlist
  password pnb
!
end
```

Configuring the ProCurve VPN Client Software

1. Configure new connection

a) Start the Security Policy Editor by double-clicking on the ProCurve VPN Client icon in the Taskbar. Then select **Edit > Add > Connection** to create a New Connection.
b) Select **Secure** from the **Connection Security** list**.**
c) For **ID Type** choose **IP Subnet**. Then enter **10.24.25.0** and **255.255.255.0** for the **Subnet** and **Mask** (ProCurve 7000dl router's Private LAN network).
d) Check **Connect using** and Select **Secure Gateway Tunnel**.
e) Under **ID type** select Any and **Gateway IP Address** and below enter the WAN IP address of the ProCurve 7000dl series router.

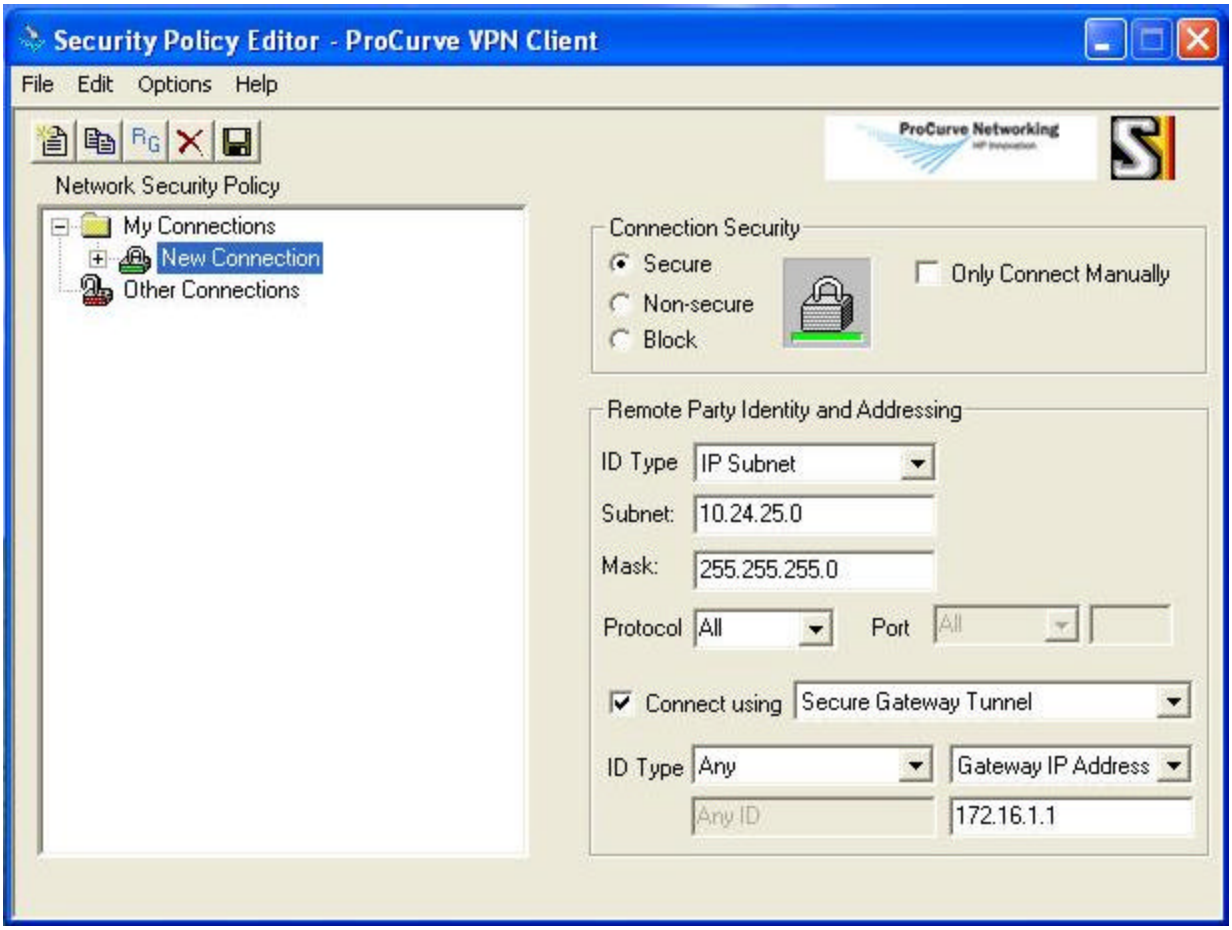

Figure 1

2. Configure Security Policy

a) Next, select Security Policy and under Security Policy select Aggressive Mode. (we are using “Aggressive Mode” in this simple example, but “Main Mode” should be the most common choice when combined with use of a “pre-shared” key. See Figure 2.

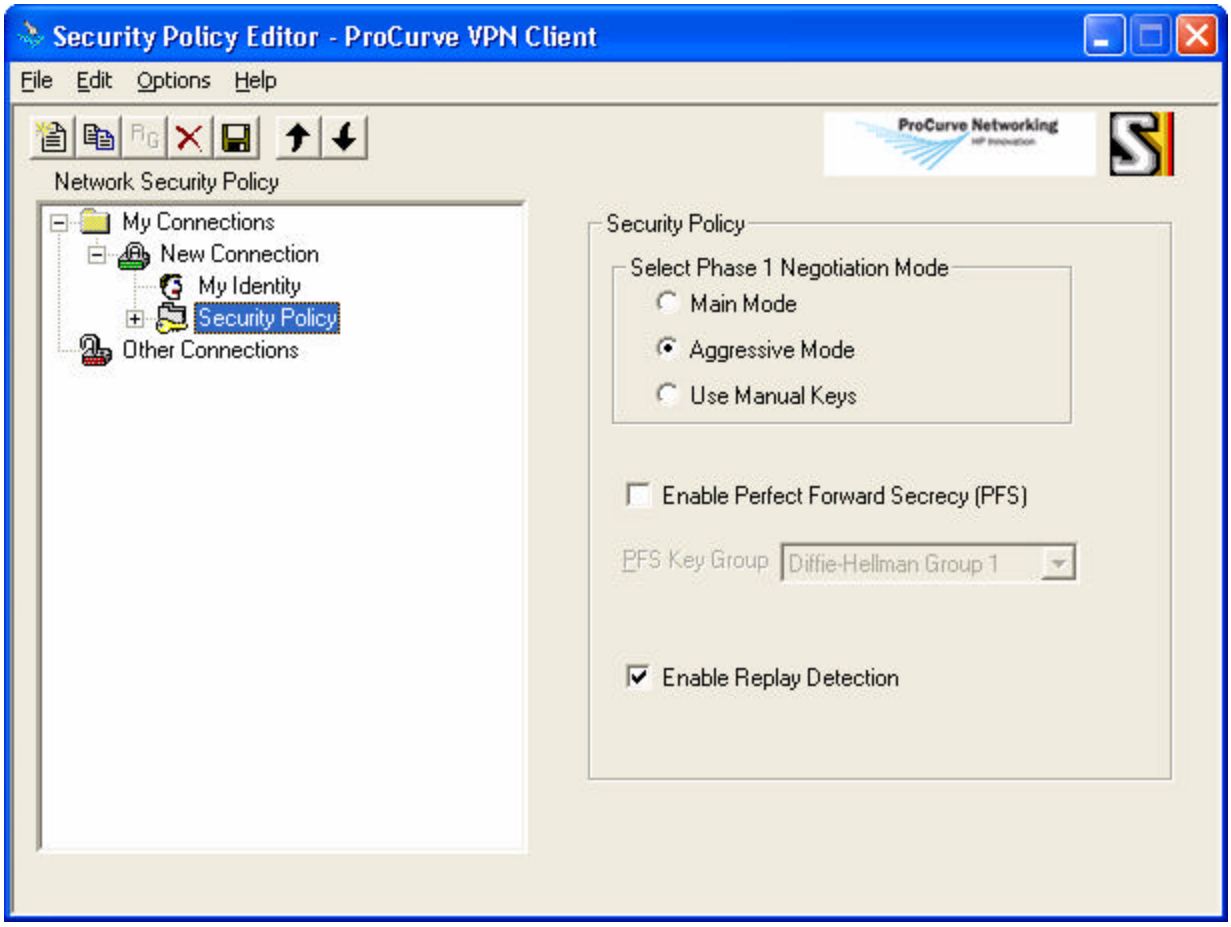

Figure 2

3. Set My Identy Parameters

Select **My Identity**. Under **ID Type** select **Domain Name** and type in the local ID (remote.com). This local ID data will be the ProCurve 7000dl series remote ID information. Select **Pre-Shared Key** and enter same key as entered into the ProCurve 7000dl router (ProCurve_Networking). Select **Disabled** for **Virtual Adapter**. See Figure 3.

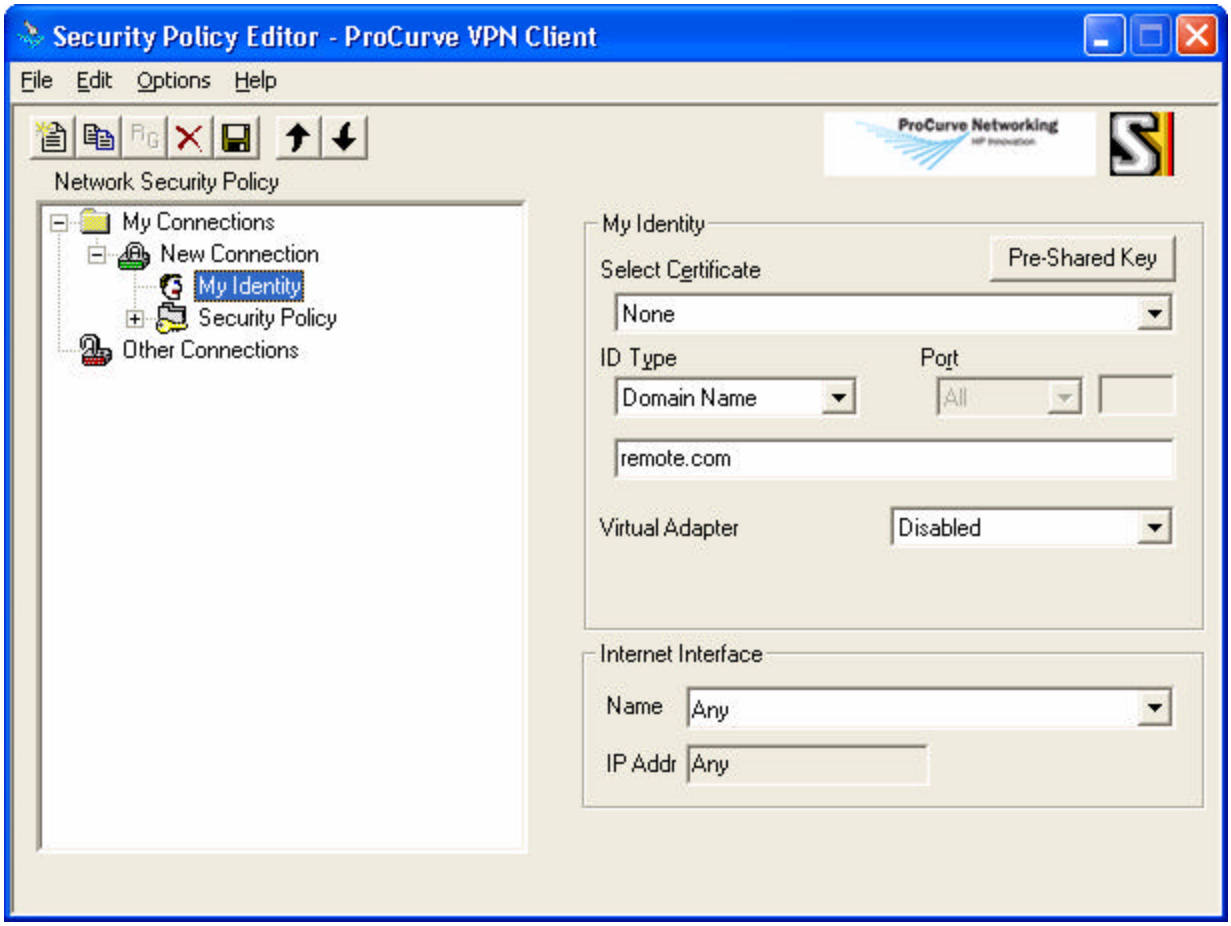

Figure 3

4. Configure IKE Parameters

Click on the plus **(+)** sign by **Security Policy**. Then click on the plus **(+)** sign by **Authentication (Phase 1)**. Click on **Proposal 1**. Select **Pre-Shared Key** for the **Authentication Method**. Select **Triple DES** for the **Encrypt Alg**. Select **SHA1** for **Hash Alg**. Select **Seconds** for **SA Life** and enter **1800** (The IKE policy timeout from the ProCurve 7000dl router). Select **Diffie-Hellman Group 1** for **Key Group**. See Figure 4.

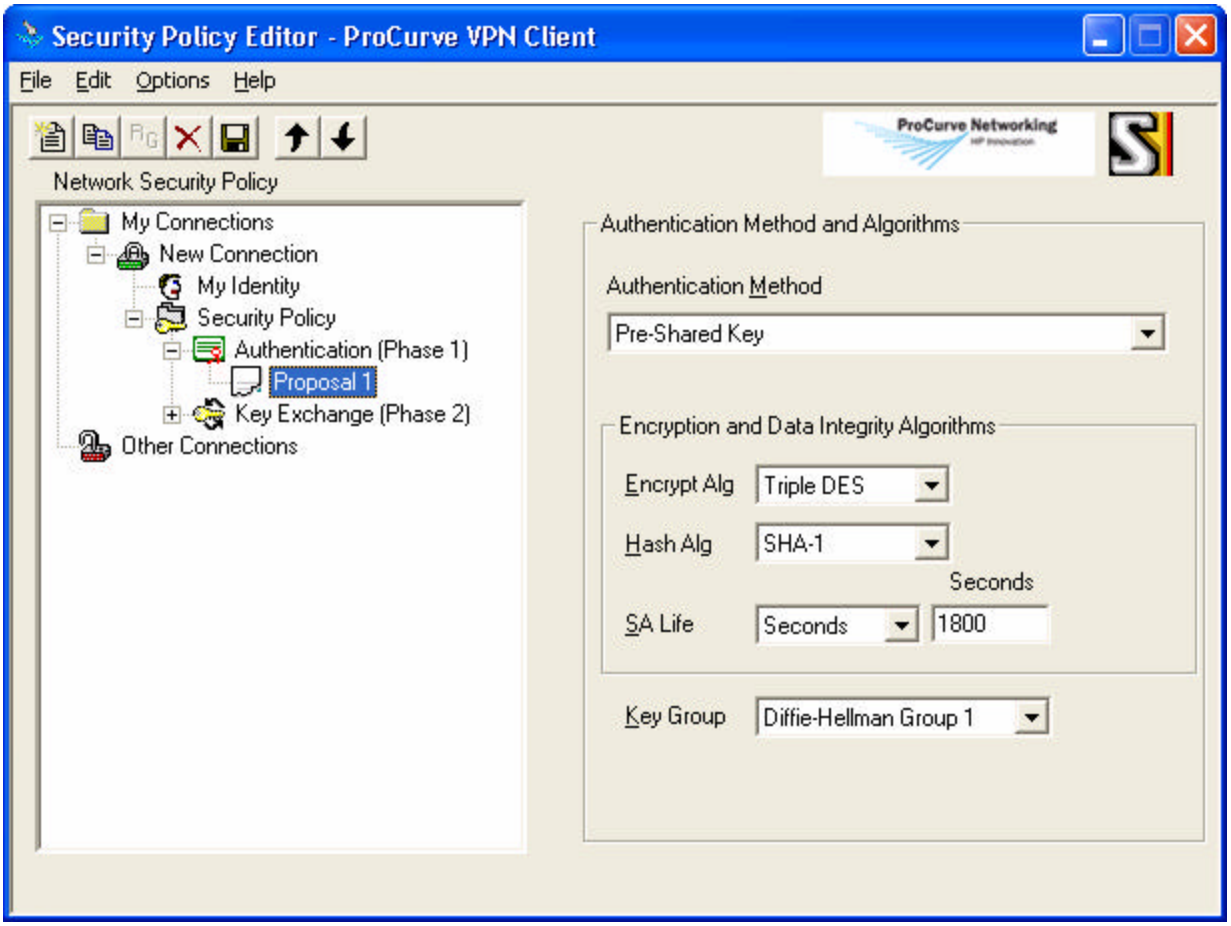

Figure 4

5. Configure IPSec Parameters

Click on the plus **(+)** sign by **Key Exchange (Phase 2)**. Then click on **Proposal 1.** Under **IPSec Protocols**, select **Seconds** for **SA life.** For **Seconds** enter **600** (The IPSec Lifetime Secs of the ProCurve 7000dl router). Check **Encapsulation Protocol (ESP)**. Select **Triple DES** for the **Encrypt Alg, SHA1** for the **Hash Alg** and **Tunnel** for the **Encapsulation**. See Figure 5.

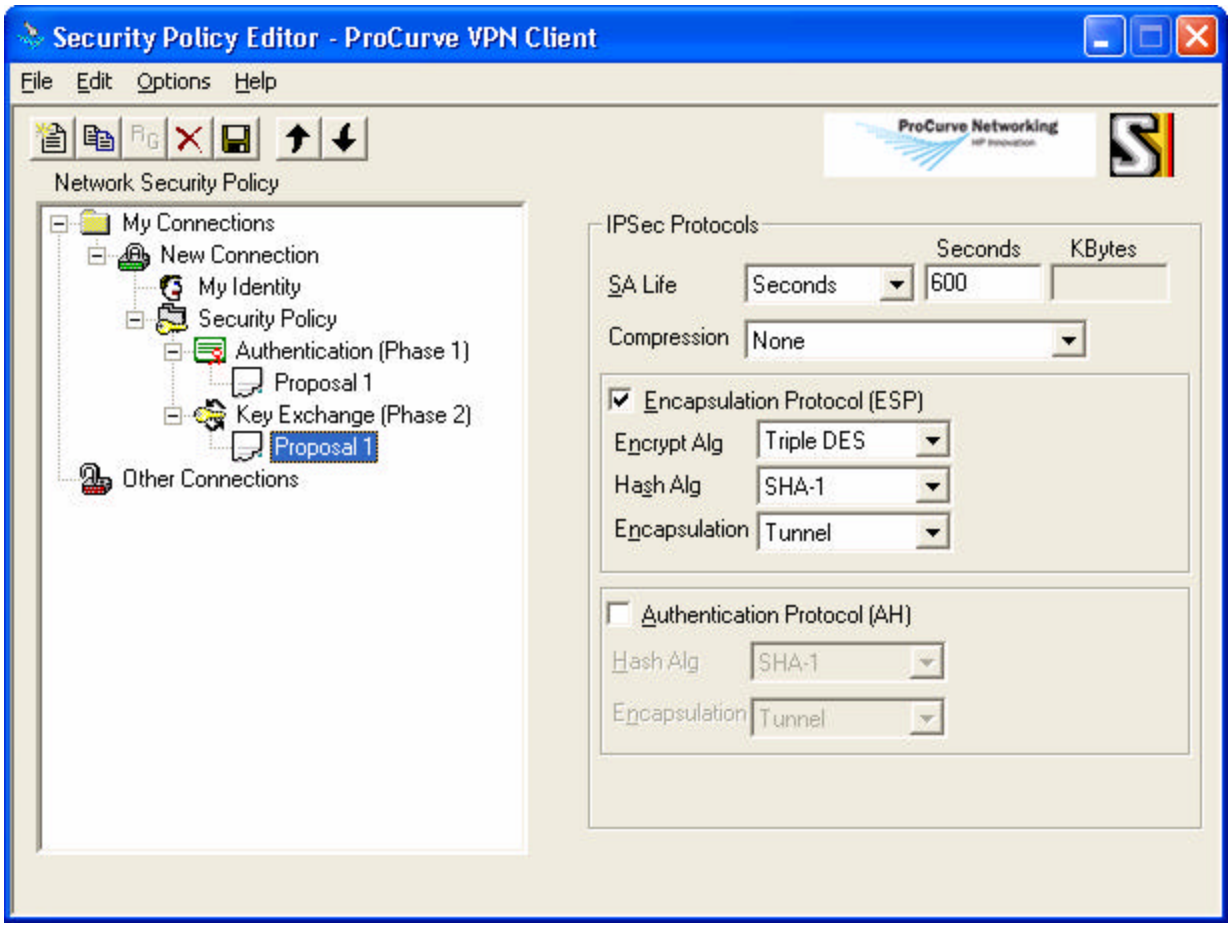

Figure 5

6. Save and Reload new Policy

Finally, click on **File** and then **Save**. Right-click on the ProCurve VPN Client icon and select **Reload Security Policy**. On the PC, open up a DOS prompt and type **ping 10.24.25.1**. This should activate the tunnel and you should get replies from 10.24.25.1