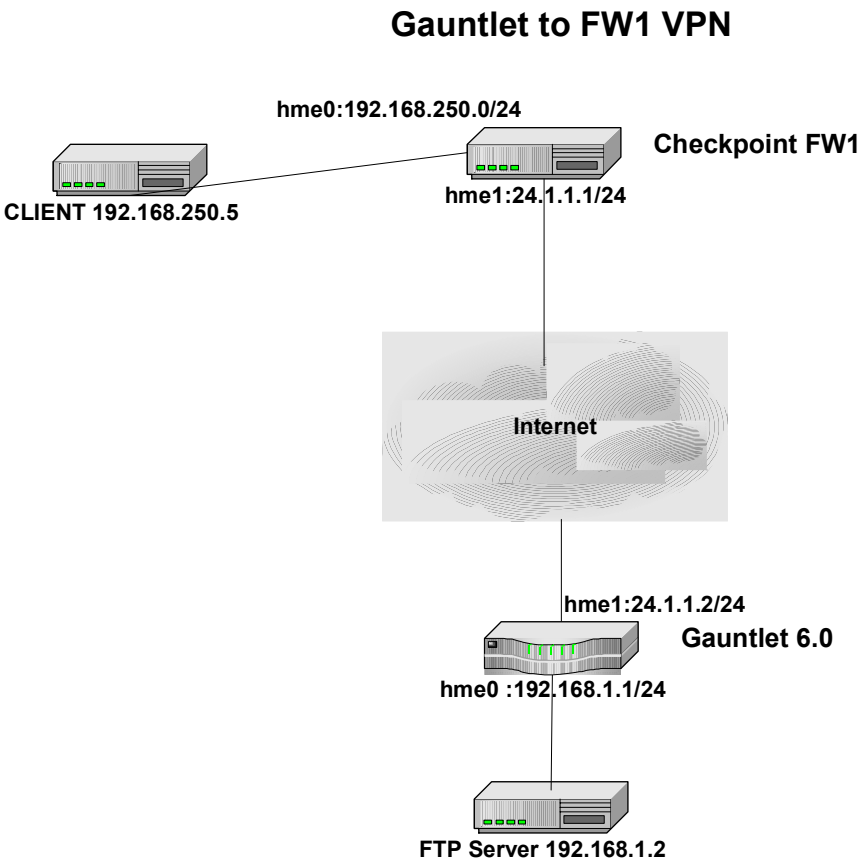
Gauntlet to Checkpoint VPN

Checkpoint Configuration

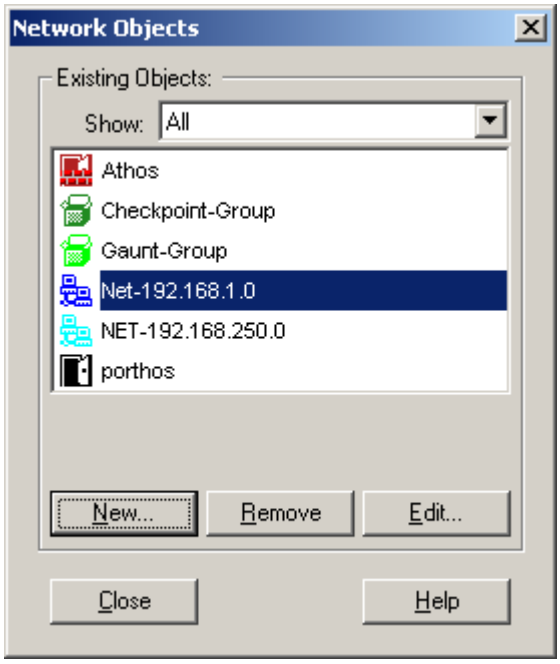
This test consisted of two networks one with a Gauntlet 6.0 Firewall on Solaris 8, and one with a Checkpoint 4.1(sp5) Firewall on Solaris 2.6. A crossover cable was set-up between the two firewalls, to represent the Internet connection.

1) The first step will be to configure the networks. You will need to know what internal IP addresses are going to be used for both sides. From the Gauntlet side we chose the 192.168.1.0/24 network. The internal network for the Checkpoint side is 192.168.250.0/24.

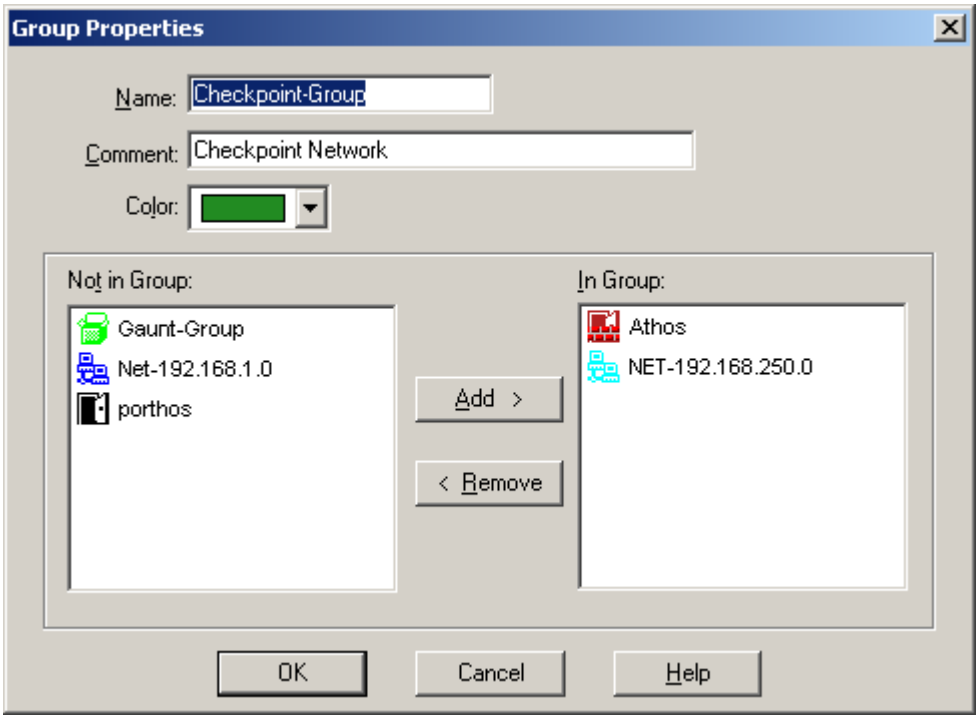
Test Network Diagram



2) To configure the networks in Checkpoint: Choose network under network objects, and create networks for each side. Note the below illustrated networks for NET-192.168.1.0 & NET-192.168.1.0.



3) Create Groups from the network objects and insert each network into its respective group.



You should have a group for each network. The above illustrates a Checkpoint group and a Gauntlet Group.

4) Create a rule base to mimic the following.

192.168.250.1 - Check Point Policy Editor

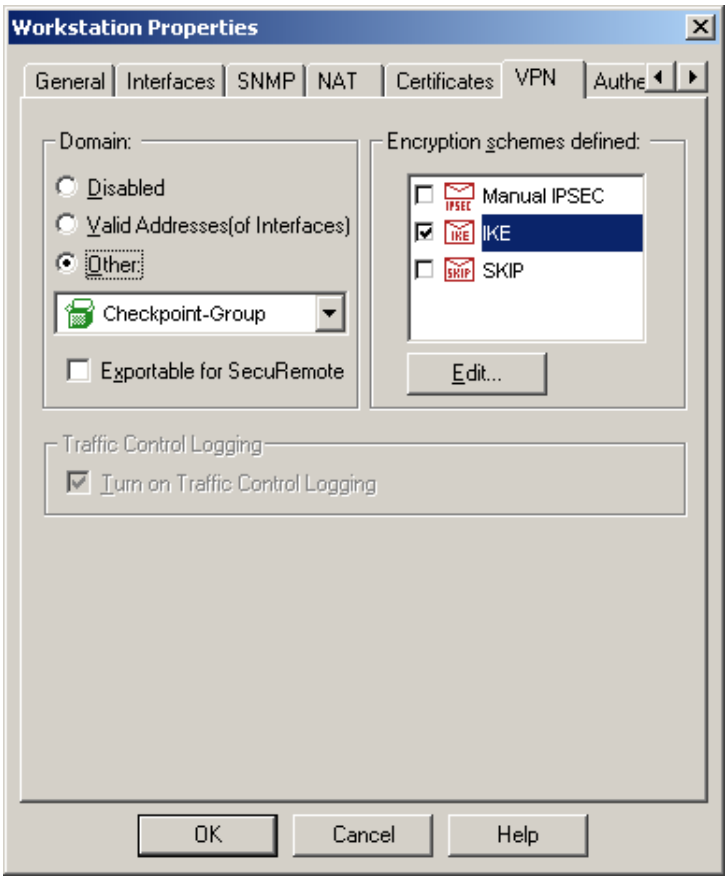
File Edit View Manage Policy Window Help

Security Policy - Standard | Address Translation - Standard

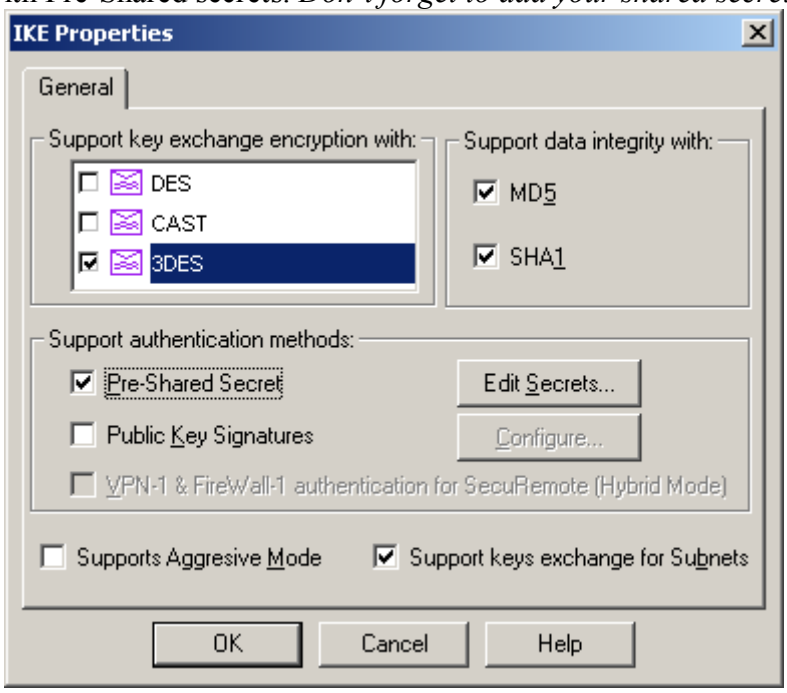
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Checkpoint-Group	Gaunt-Group	Any	Encrypt	Long	Gateways	Any	Allow any Encrypted traffic from the Checkpoint Group to the Gauntlet Group
2	Gaunt-Group	Checkpoint-Group	Any	Encrypt	Long	Gateways	Any	Allow any Encrypted traffic from the Gauntlett Group to the Checkpoint Group
3	NET-192.168.250.0	Any	Any	accept	Long	Gateways	Any	Allow ANY Local Traffic
4	Any	Any	Any	drop	Long	Gateways	Any	Drop all other Traffic

For Help, press F1 | 192.168.250.1 | Read/Write | NUM

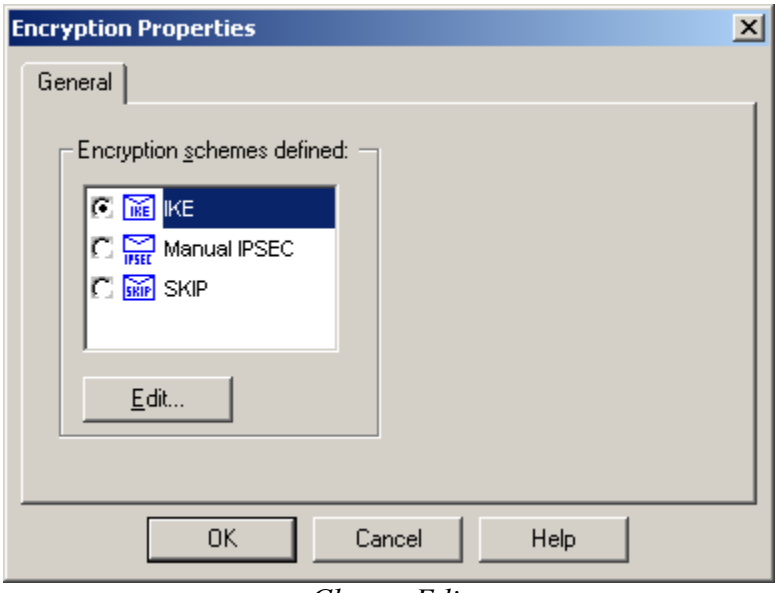
5) Configure the encryption scheme to use within the Firewall object. Choose the domain that will be allowed to use this service. For this test we chose IKE



6) Choose Triple DES with Pre-Shared secrets. *Don't forget to add your shared secret*.

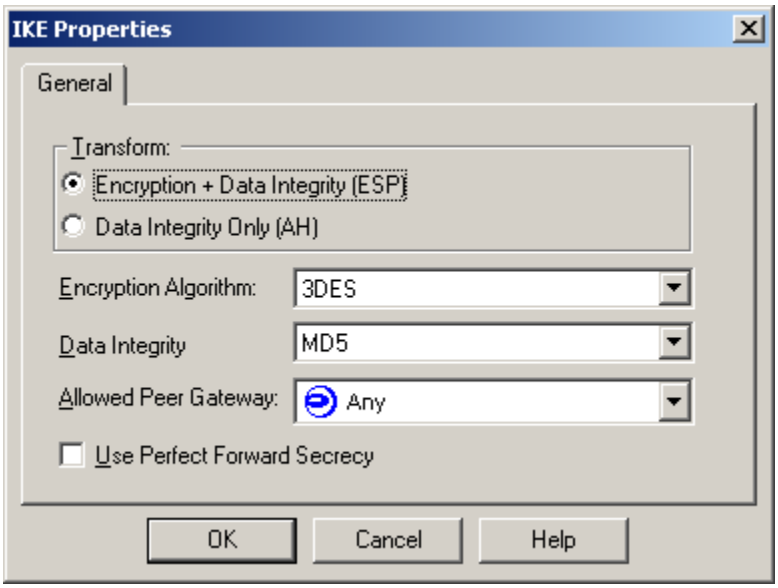


7) Edit the Encryption properties on the Action item of the ruleset. Right click on the Encrypt object, and edit properties.



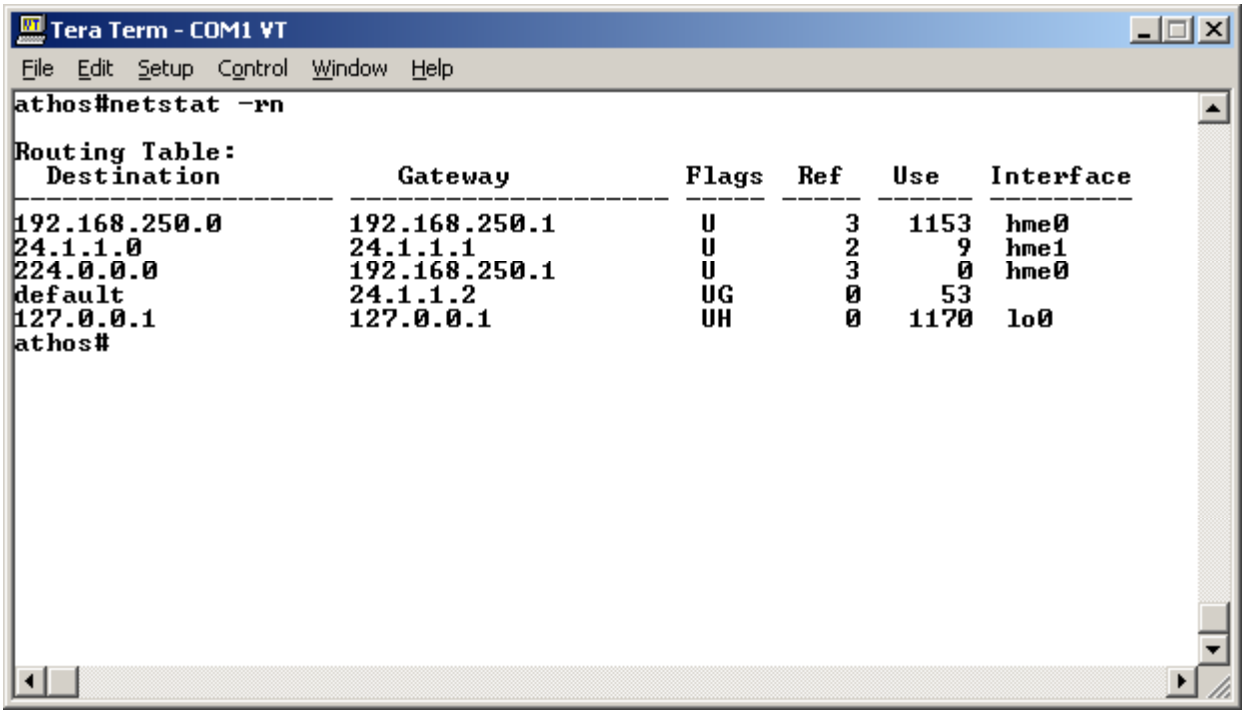
Choose Edit

7) Continued…..



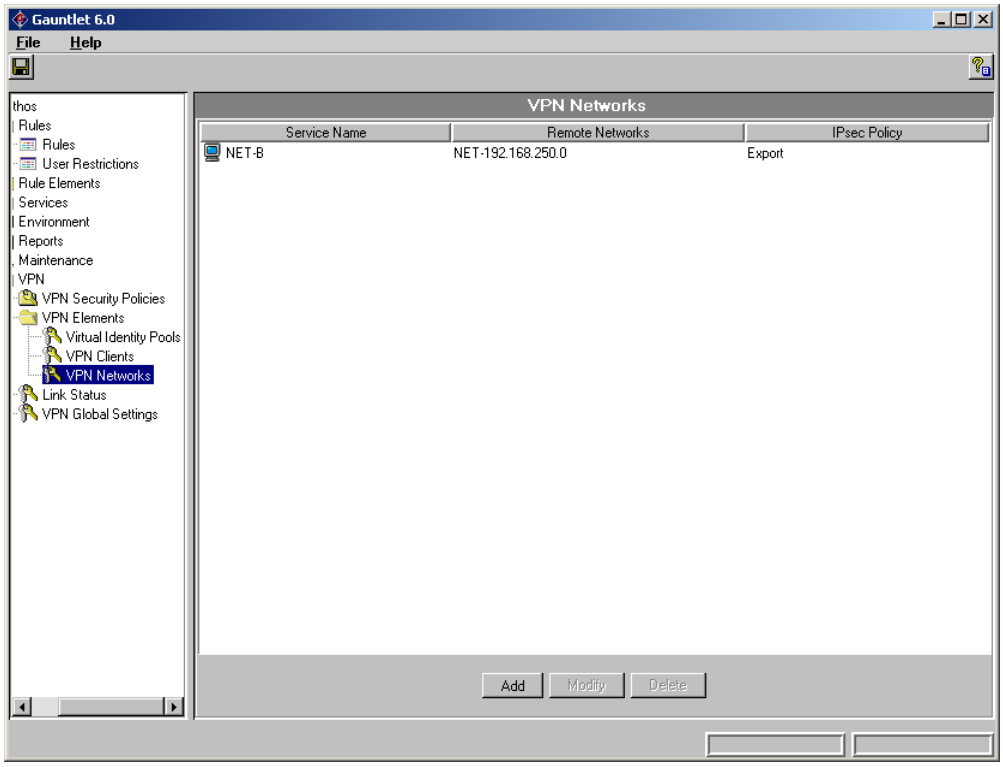
Choose the Algorithm & Integrity.

8) Make sure you have the correct routes set up on the Checkpoint firewall.

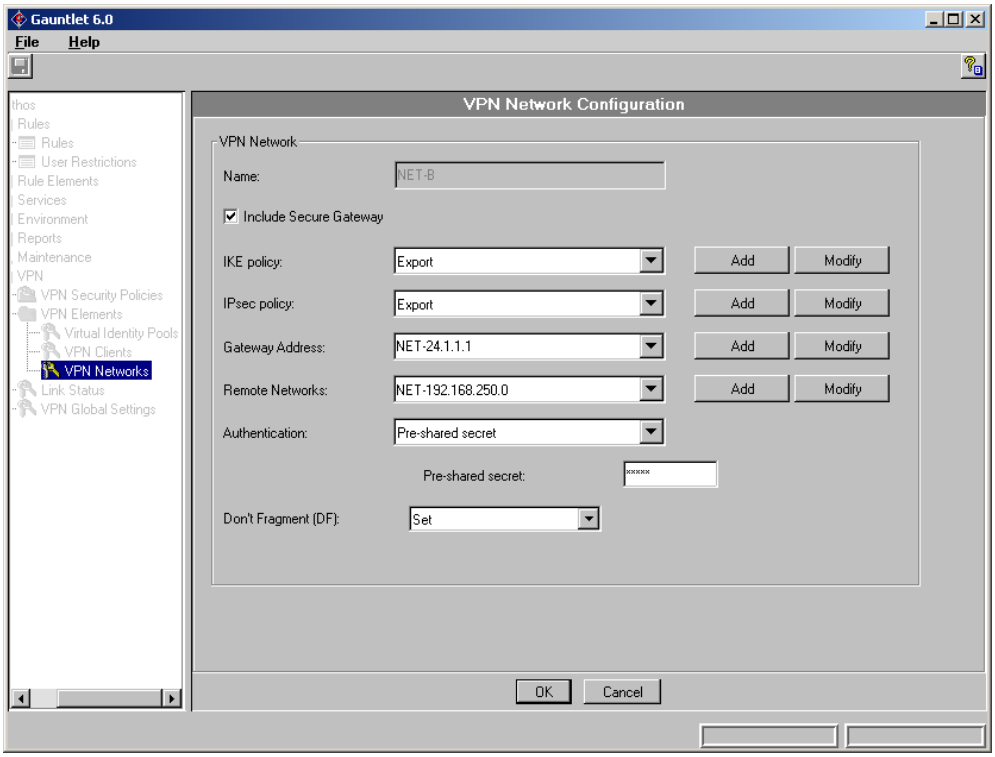


Gauntlet Configuration

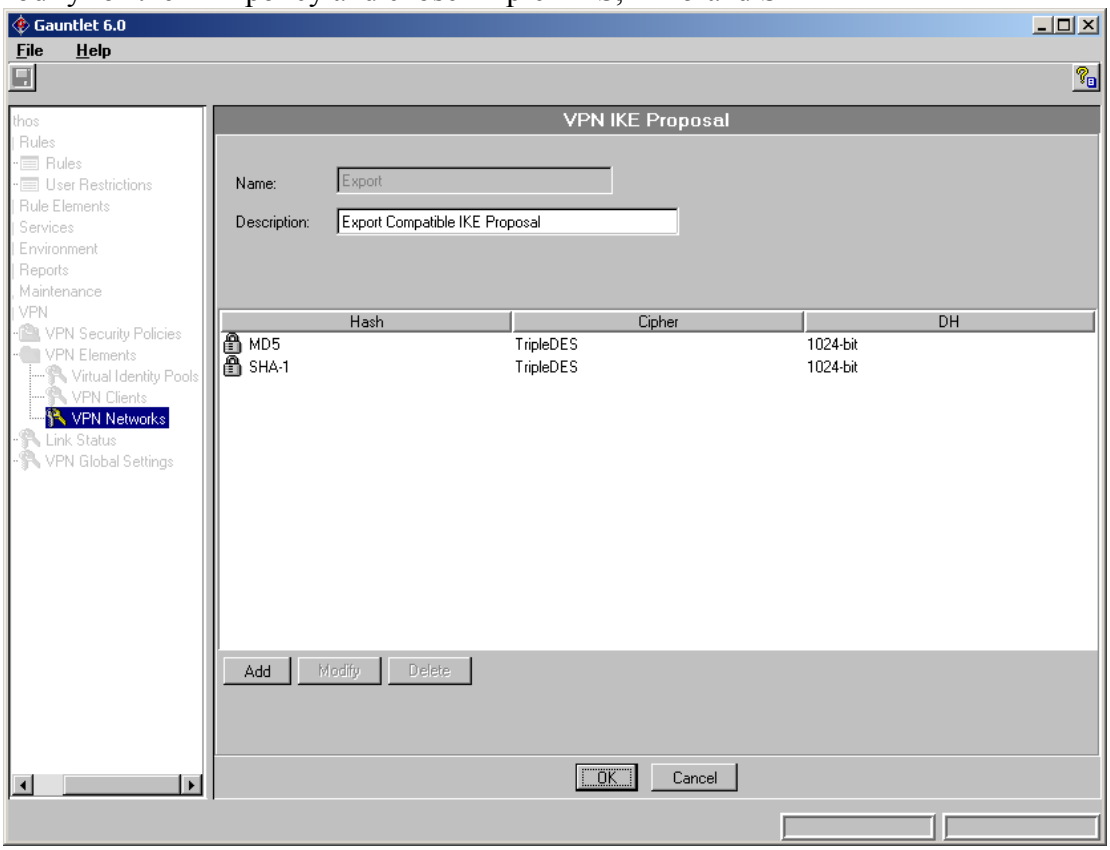
The Gauntlet Configuration consists of the following.
Create a VPN network



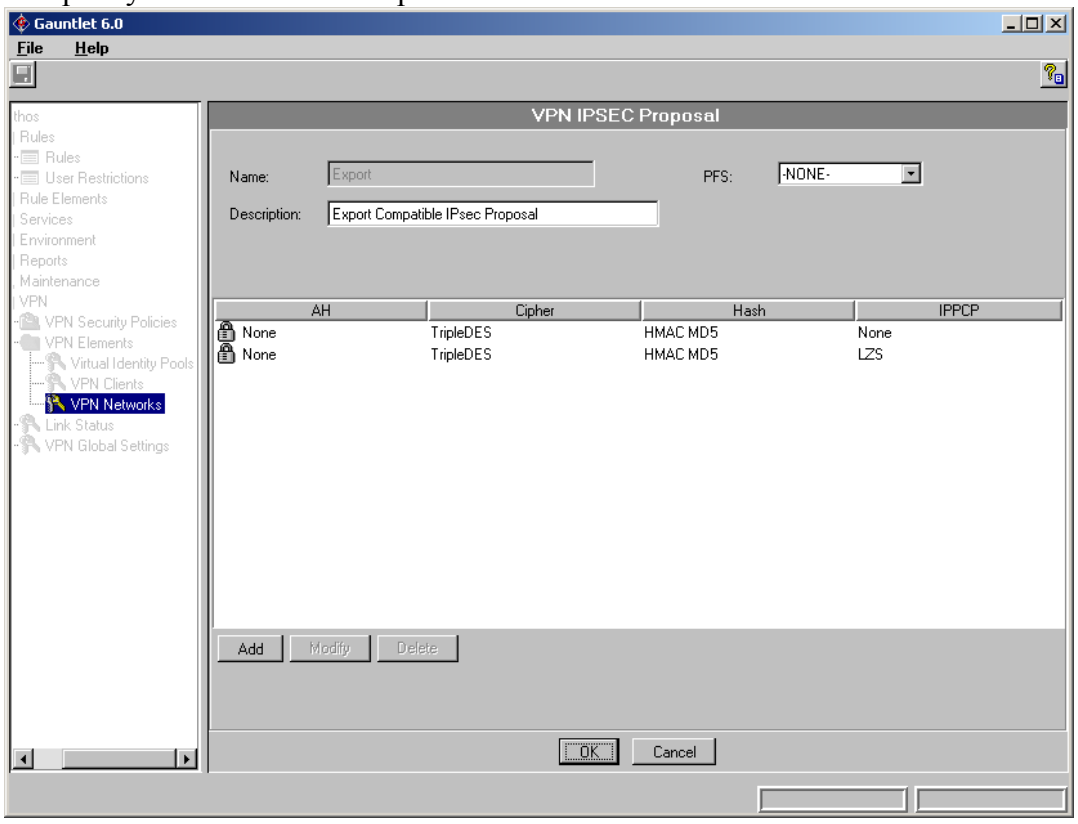
1) Add the Gateway address and the internal network of the Checkpoint firewall. Set the Pre-shared secret to be the same as on the Checkpoint set-up.



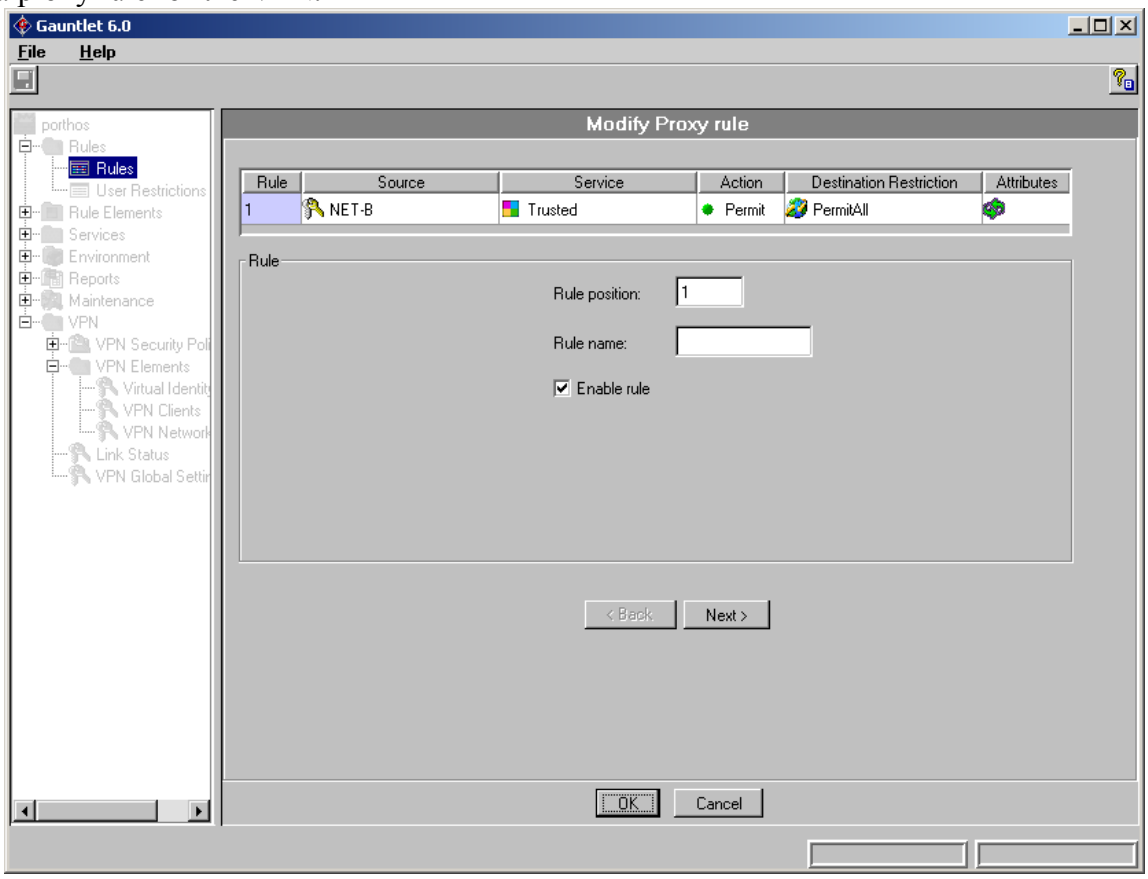
2) Choose Modify for the IKE policy and chose Triple DES, MD5 and SHA-1



3) For the IPSEC policy we chose to use Triple DES. Choose NONE for PFS.

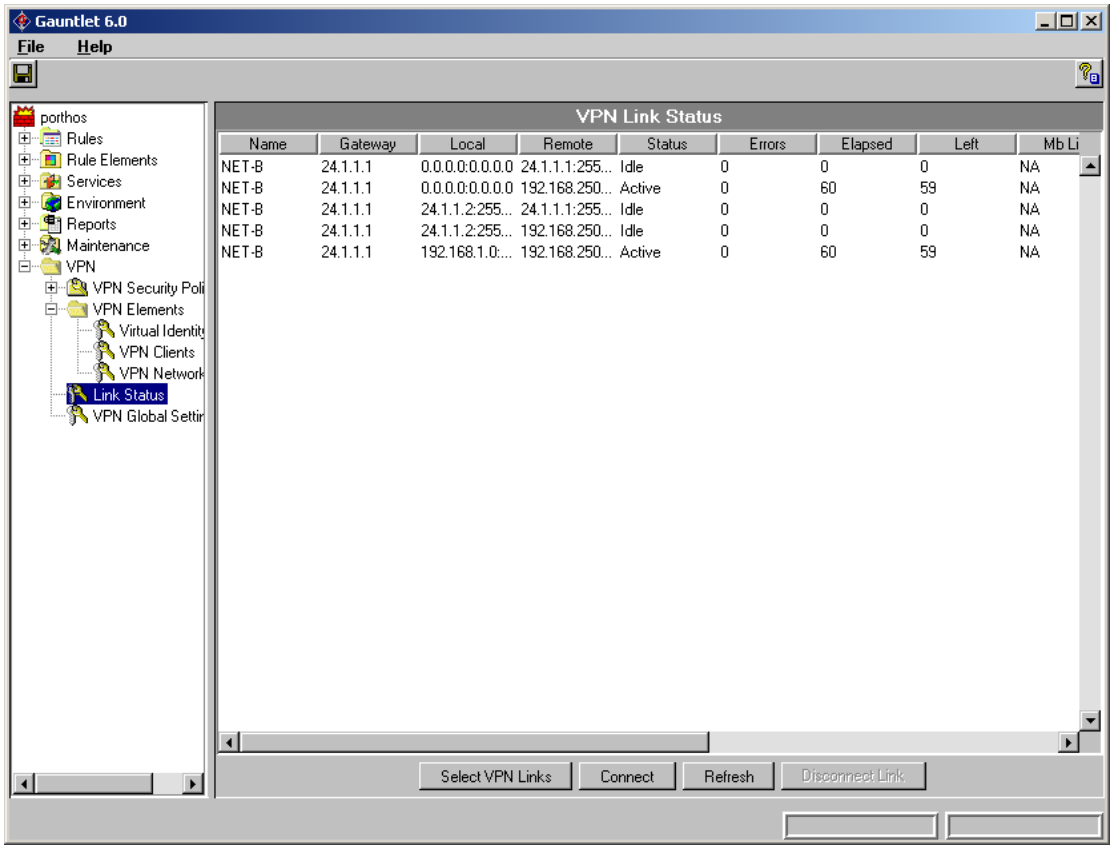


4) Create a proxy rule for the VPN.

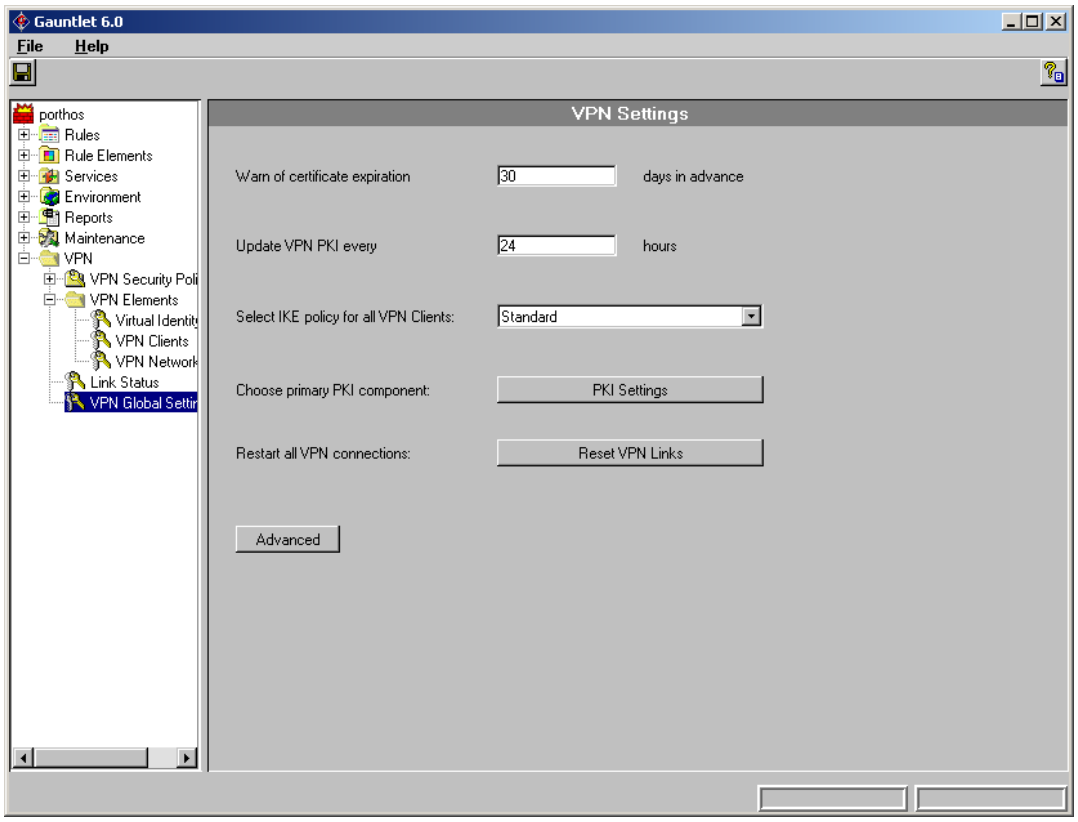


5) Save and Apply your configuration

6) Go to the Link Status under VPN Elements. You should see something similar to the following.



7) If you do not see anything Active, and all the numbers are 0's then choose VPN Global Settings and Reset VPN Links.



8) If you are still having problems, check your configurations for typos. Check the routes on both firewalls, and look at the checkpoint logs for errors. From the Gauntlet you can also run the ipe command to get VPN status information. Type *ipe?* for help.