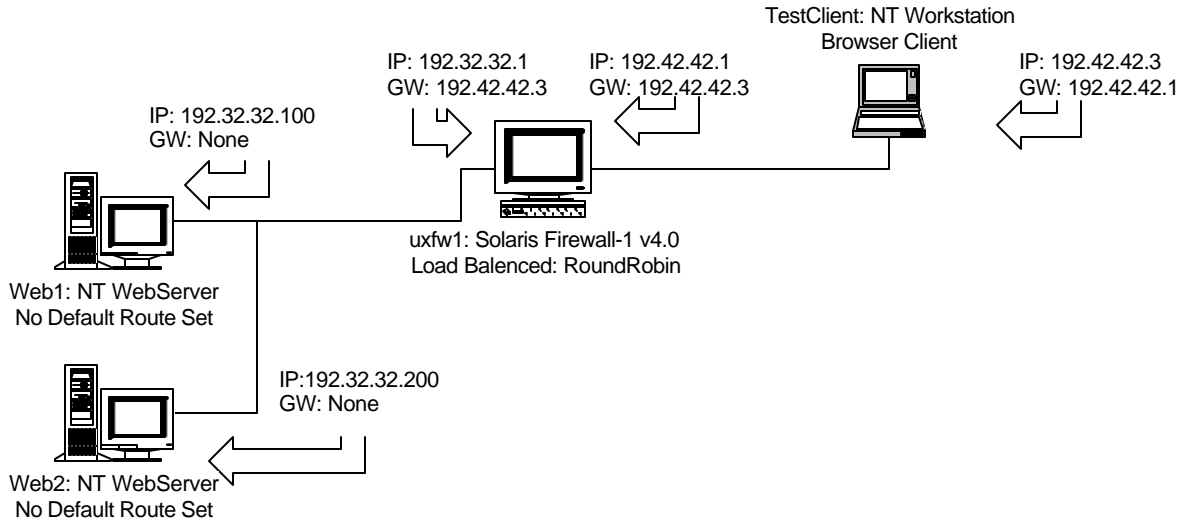


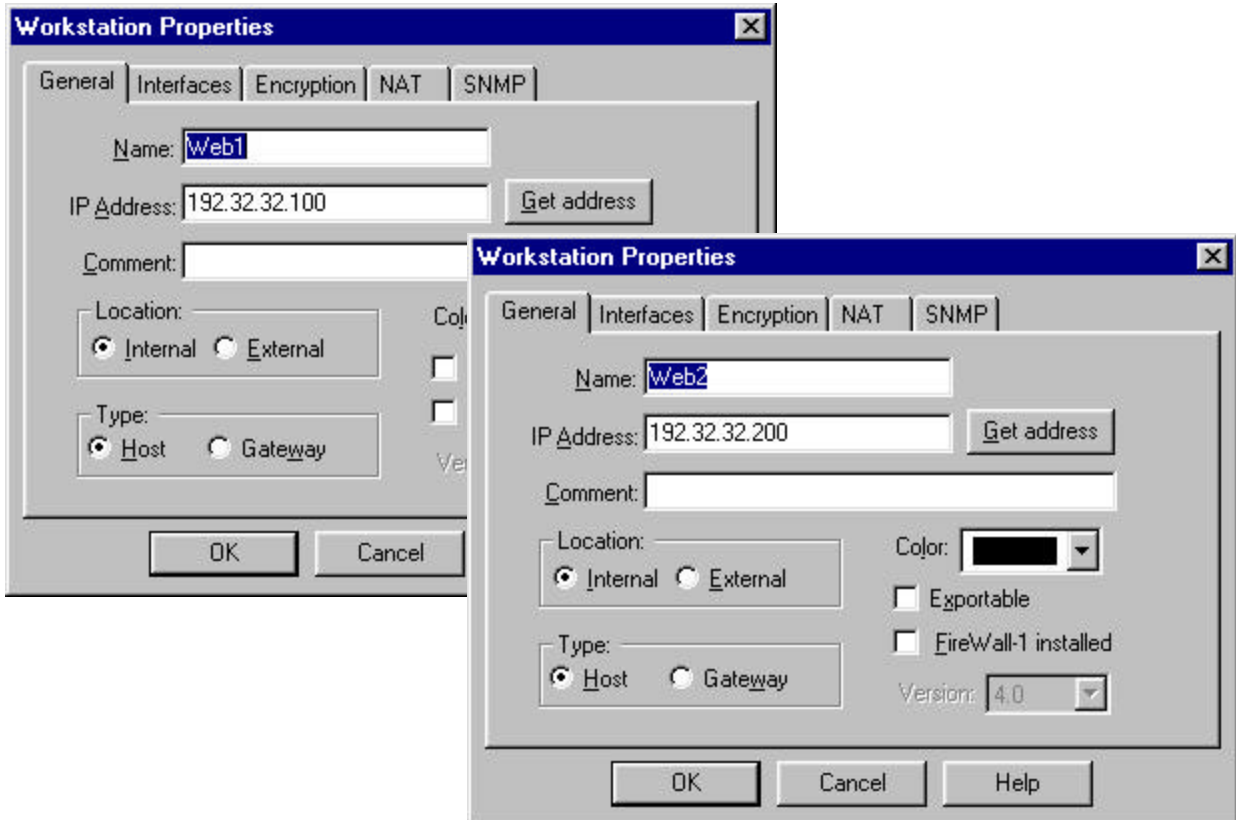
Connect Control with Address Translation:

By combining Connect Control with NAT you can configure your web servers in the cluster to default route out of another gateway for redundancy, or have them configured with no default gateway at all. This example has 2 web servers in a web farm with no default routes set. This means that by default there is no return path to the Internet to respond to clients.

NOTE: that the Web servers in my farm have no default route set at all, they have no IP route to the TestClient system on the other side of the gateway/load balance. There is no IP connectivity between the web servers and the TestClient system.

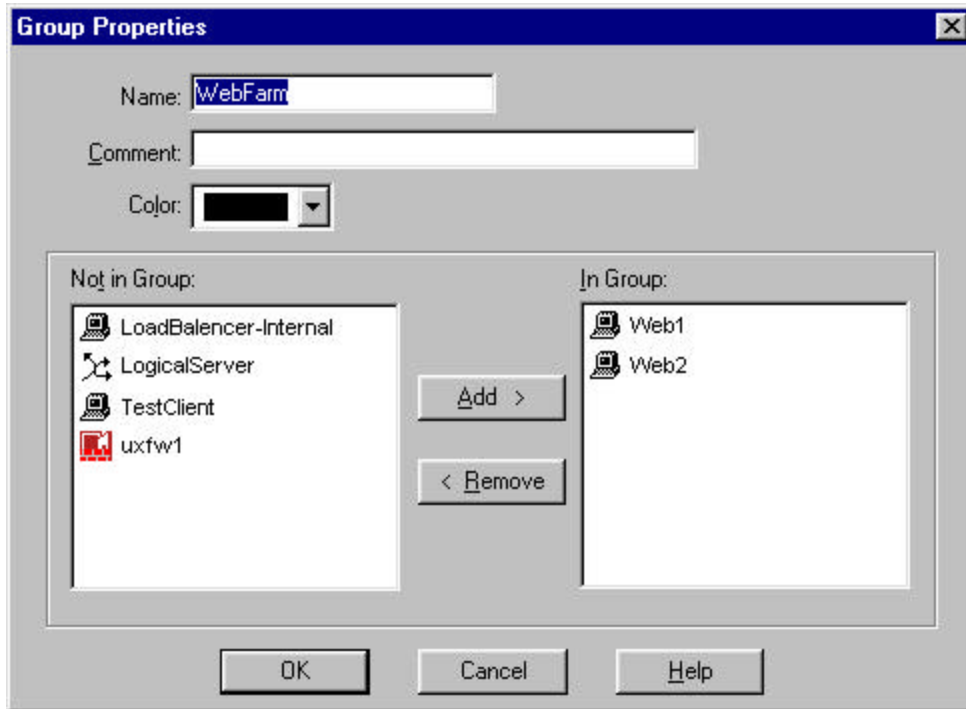


First create 2 objects for Web Servers 1 & 2:

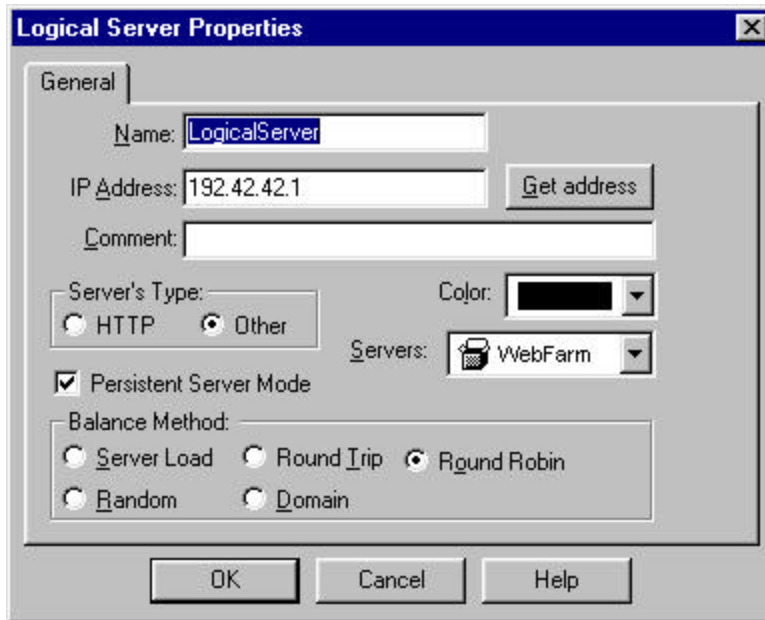


Check Point Software Inc.

Next create a Group Object for the load balance configuration.

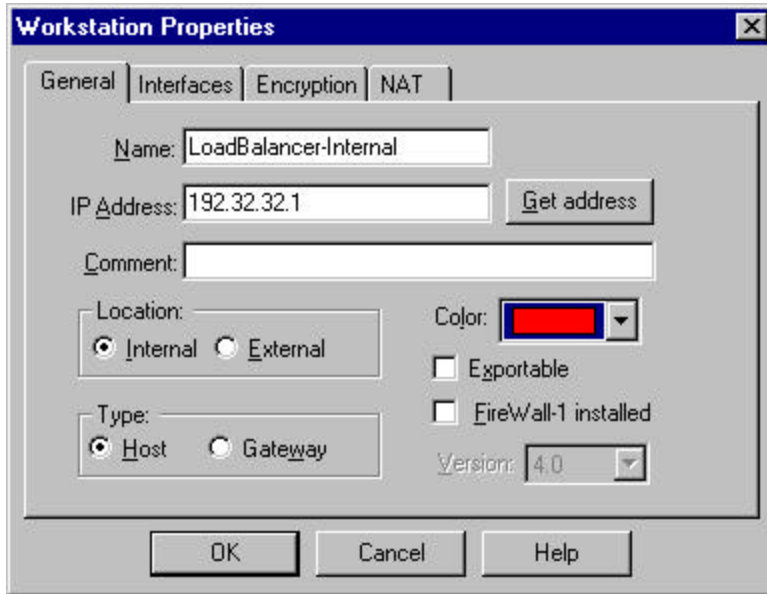


Next build a Logical Server Object pointing to the Internet address of the Firewall:

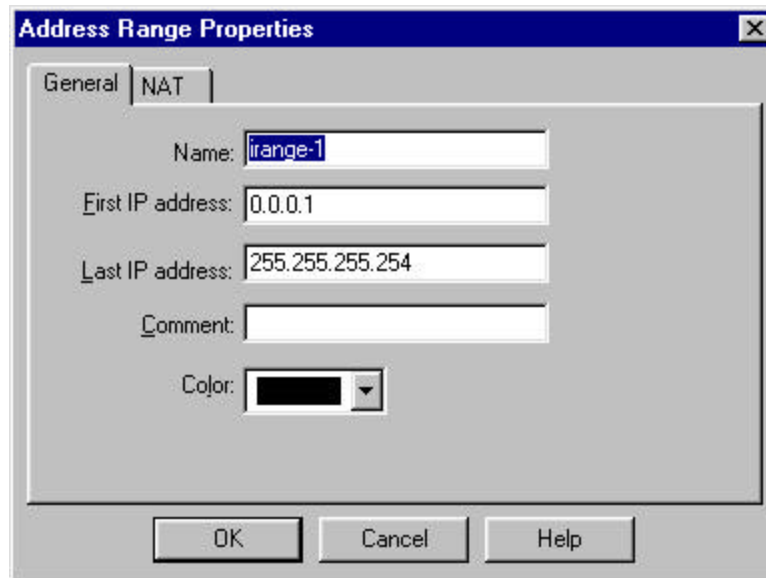


NOTE: In this example I am using the Firewall's external address for the Connect Control address i.e. the address that internet users will connect to. If you have **Sealth Rules** (i.e. **Any Any Firewall Drop Alert**), this will also block the Connect Control connections from Internet users. You may want to use another address in the valid external range for the Connect Control address and have the Firewall Proxy Arp for it.

Now create a Workstation object to represent the internal interface of the Firewall to perform the Hide;

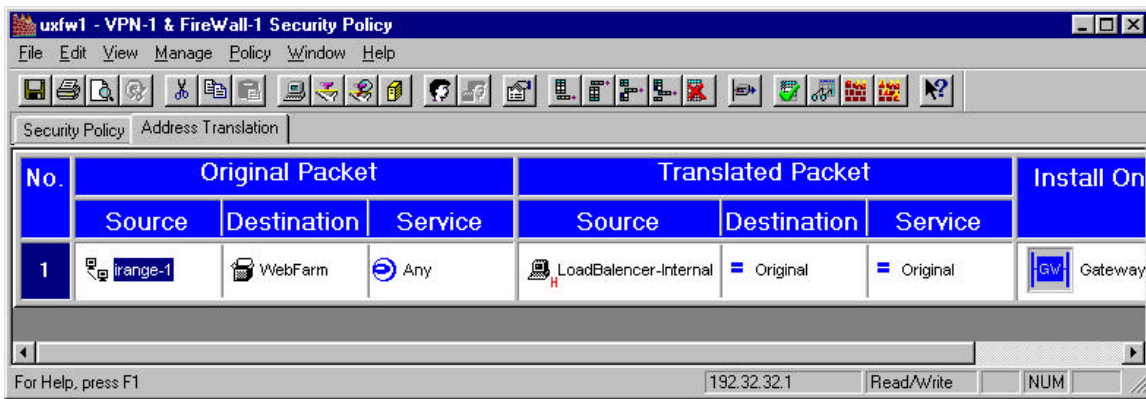
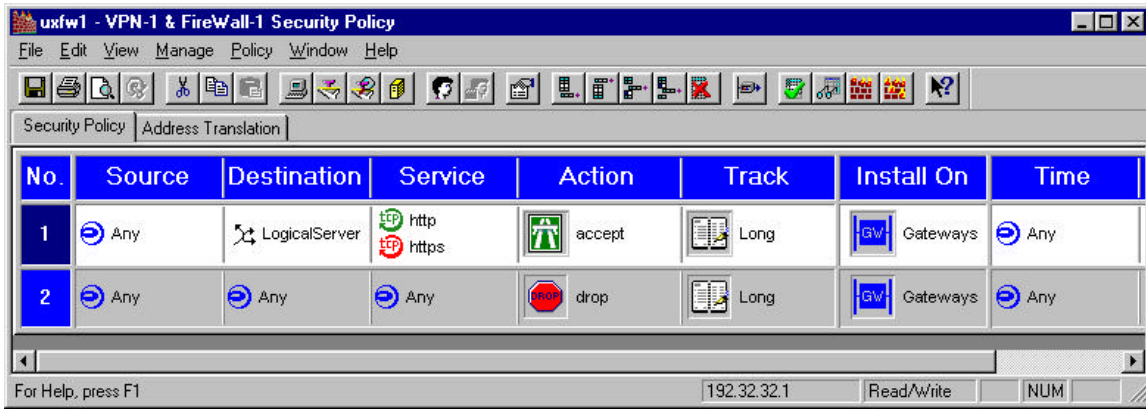


Now create a Network Address Range object to represent the Internet clients source addresses coming in. You need to know the source address of a packet to do a dynamic HIDE so we must represent all possible addresses.



NOTE: The Destination of WebFarm in the NAT rule is critical and will keep the gateway from performing NAT on packets destined for other services. All packets destined for the WebFarm will be NAT'ed behind the internal interface so no default routes are required. Now when a packet comes into the Firewall the DST is changed by the Connect Control Module to whatever server is next in the load balance scheme, and the Source is hidden behind the internal interface of the gateway. The 2 web servers could have a default route to another gateway i.e. a production internet firewall or no default route at all.

Now create Security and NAT rulebase's;



Here is the NAT log output;

