

**Check Point Software Technologies LTD.**

***VPN-1 Version 4.1  
Gateway to Gateway  
IKE Encryption Failover  
Quick Reference Guide***

**Authored By:** David Goodman  
**Date:** October 5, 1999  
**Purpose:** To describe and Document how to configure IKE Failover within Checkpoint VPN-1 Version 4.1

**Check Point Software Technologies LTD.**

---

**VPN-1 Version 4.1 Gateway to Gateway IKE Encryption Failover Quick Reference**

This document describes how to setup gateway to gateway Single Entry Point (SEP) IKE VPN fault tolerance with Check Point VPN-1 Version 4.1. It assumes a basic knowledge of Check Point distributed architecture, and that a functional implementation of this architecture has been previously configured as shown in Figure 1 below. For more information on how to install and configure Check Point VPN-1 Version 4.1, please see the associated documentation in the VPN-1 User's Guides version 4.1 dated July 1999.

In addition to the Check Point VPN-1 software, SEP implementations must also include a method for dynamic failover or clustering of multiple physical machines. This particular example employs the StoneBeat High Availability Software from StoneSoft to accomplish this goal. For other OPSEC (Open Platform for Security) certified failover or clustering options, please see: <http://www.checkpoint.com/opsec/framework.html#High Availability>

Consider the following diagram. Access to the main business network (192.32.42.0) is considered mission critical and a loss of connectivity is unacceptable. Single point of failure for this network is mitigated by configuring dual redundant VPN-1 modules at the perimeter of the network (primary and secondary), managed by a management console at 192.32.42.10. Both the primary and secondary gateways are physically connected to the internal and external networks. They are also connected via a dedicated "heartbeat network" (192.32.52.0) which is used by the StoneBeat software to poll the health of its peer, and the Check Point software to share state (connection) information. The management console at 192.32.42.10 is also responsible for management (policy creation and logging) of the remote gateway 192.32.32.1. **Note: The SEP configuration can be duplicated on the remote network, and a separate management console can manage the remote gateway. These configurations are not covered in this document.**

In this example, the primary VPN gateway is responsible for all traffic and the secondary gateway is in hot standby mode. In the event of a failure of the primary, the StoneBeat Software reconfigures the secondary gateway (in a matter of seconds) with the mac address and IP address of the internal and external interfaces of the primary and brings the primary off line. In this scenario, an IKE encrypted communication between the internal network and the remote network (negotiated by the primary VPN gateway and the remote VPN gateway), can continue without interruption through the secondary gateway. This connection failover is possible because both gateways have identical rulebases, and are sharing encrypted connection state information through the use of Check Point's State Synchronization capabilities. **Note: The SEP configuration can be applied to two or more live gateways in a load sharing scenario. While configuration parameters for this design are similar to those defined in this document, this configuration is not specifically detailed in this document.**

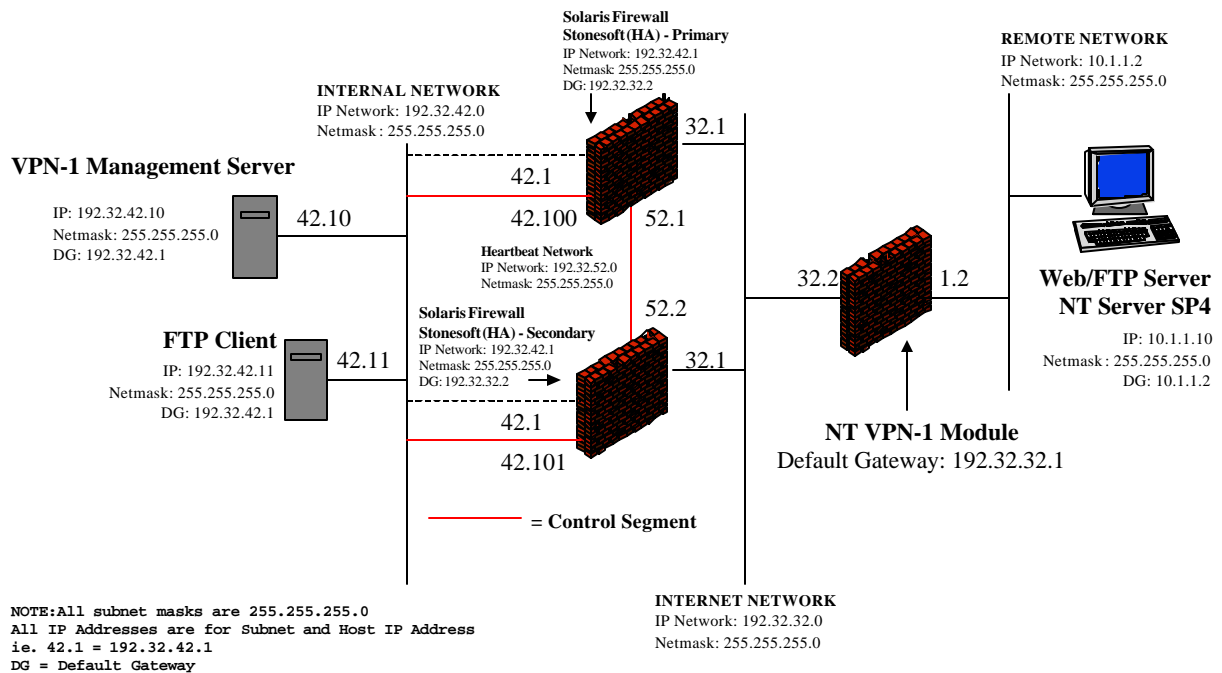


Figure 1 Network Diagram

In order to configure a SEP fault tolerant gateway to gateway VPN, we will perform the following steps:

1. Define the workstation objects that represent the VPN gateways. The following three gateway objects with their parameters will be created:

#### Primary Gateway

- Name - "fw1-a"
- IP address - "192.32.52.1" (**Note: The heartbeat network interface address is selected for use as the gateway object IP address because it is not modified by the StoneBeat software**)
- Location - "Internal"
- Type - "Gateway"
- Modules Installed - "VPN-1 & Firewall-1"
- Version - "4.1"

#### Secondary Gateway

- Name - "fw1-b"
- IP address - "192.32.52.2" (**Note: The heartbeat network interface address is selected for use as the gateway object IP address because it is not modified by the StoneBeat software**)
- Location - "Internal"
- Type - "Gateway"
- Modules Installed - "VPN-1 & Firewall-1"
- Version - "4.1"

#### Remote Gateway

- Name - "ntfw1"
- IP address - "192.32.32.2"
- Location - "Internal"
- Type - "Gateway"
- Modules Installed - "VPN-1 & Firewall-1"
- Version - "4.1"

2. Define the network objects that represent the internal and remote networks. The following two network objects with their parameters will be created:

#### Internal Network

- Name - "internal-network"
- IP address - "192.32.42.0"
- Net Mask - "255.255.255.0"
- Location - "Internal"
- Broadcast - "Allowed"

#### Remote Network

- Name - "remote-network"
- IP address - "10.1.1.0"
- Net Mask - "255.255.255.0"
- Location - "Internal"
- Broadcast - "Allowed"

3. Enable Gateway Clusters in **Policy → Properties → High Availability Options**
4. Define a cluster object which logically represent the primary and secondary VPN-1 gateways. This object will have the following parameters:
  - Name - "ipsec\_cluster"
  - IP address - "192.32.32.1"
  - Location - "Internal"
  - VPN-1 & Firewall-1 installed version - "4.1"
5. Modify the "fw1-a" & "fw1-b" objects to be a cluster members
6. Define a group object that represents the internal network's encryption domain
  - Name - "internal\_enc\_domain"
  - In Group - "internal\_network" & "ipsec\_cluster"
7. Define a group object that represents the remote network's encryption domain
  - Name - "remote\_enc\_domain"
  - In Group - "remote\_network" & "ntfw1"
8. Modify the VPN parameters of the "ipsec\_cluster" object as follows:
  - Domain - "internal\_enc\_domain" (internal encryption domain group object)
  - Encryption Schemes Defined "IKE"
  - Key Negotiation Encryption Method - "3DES"
  - Hash Method - "MD5" & "SHA1"
  - Authentication Method - "Pre-Shared Secret"

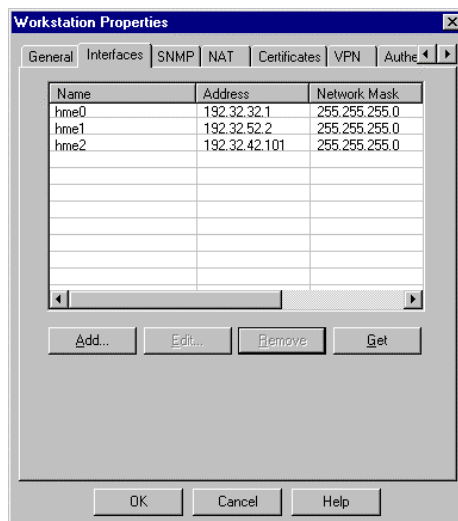
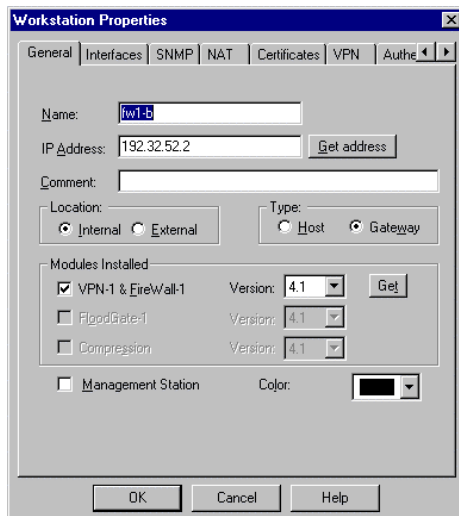
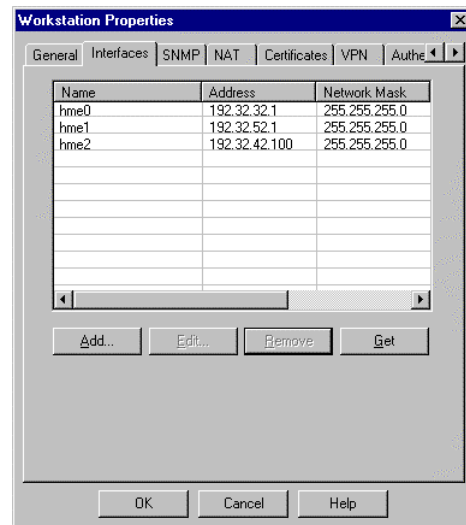
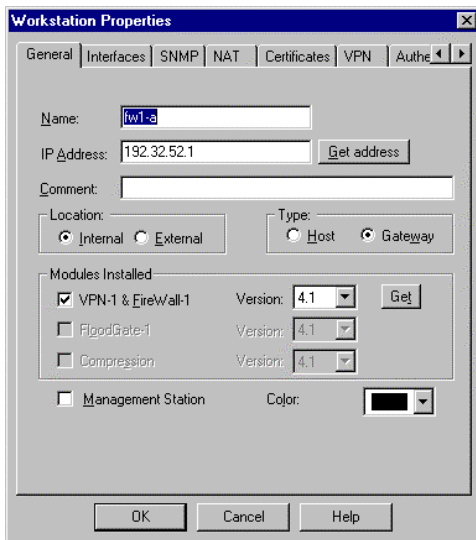
9. Modify the VPN parameters of the “ntfw1” object as follows:

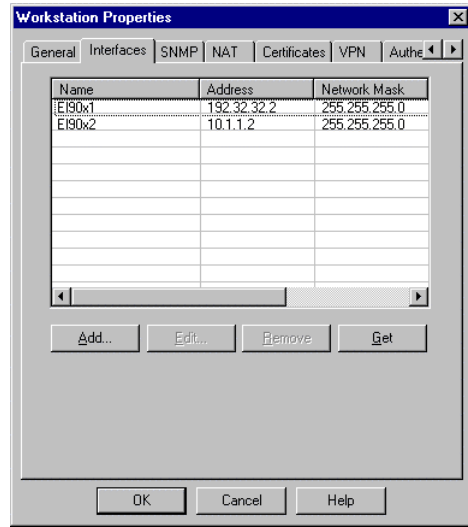
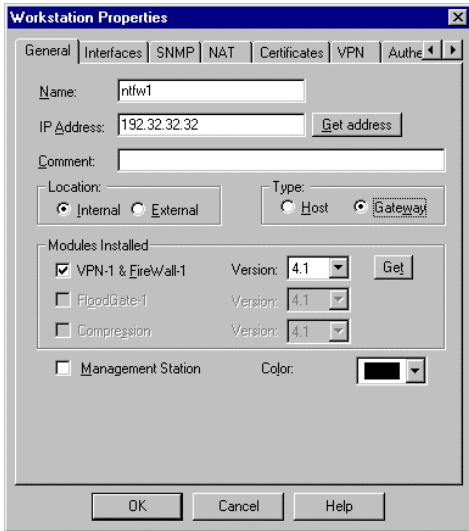
- Domain - "remote\_enc\_domain" (remote encryption domain group object)
- Encryption Schemes Defined “IKE”
- Key Negotiation Encryption Method – “3DES”
- Hash Method – “MD5” & “SHA1”
- Authentication Method - “Pre-Shared Secret”
- Member of the Shared Secret list “ipsec\_cluster”
- Shared Secret for ipsec\_cluster “test123”
- VPN-1 & Firewall-1 installed version - “4.1”

10. Create a rule enabling encryption between the internal network and the remote network

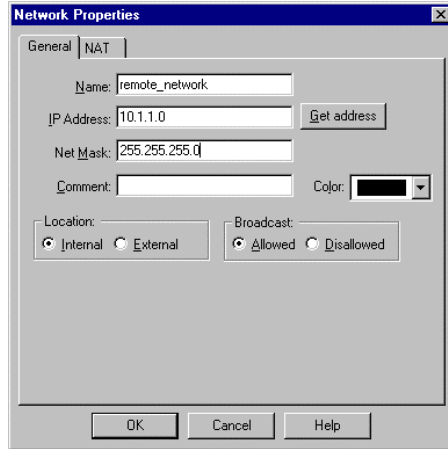
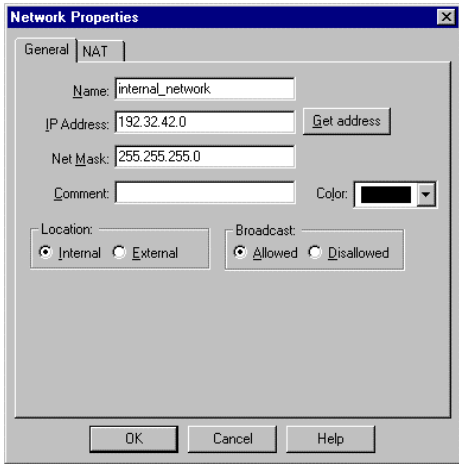
11. Test the configuration

**Step 1** Define the workstation objects that represent the VPN gateways. In the main Policy Editor window select **Manage** → **network Objects** → **New** → **Workstation** and create three objects with the following parameters:

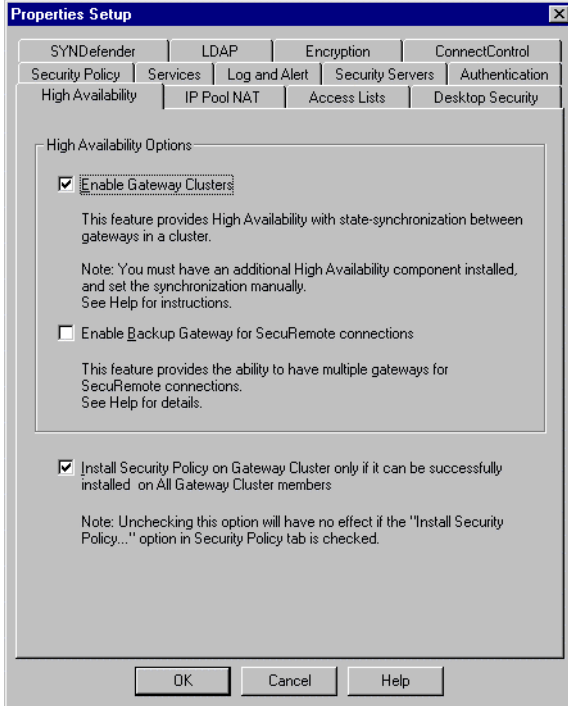




**Step 2** Define the network objects that represent the internal and remote networks. In the main Policy Editor window select **Manage** → **network Objects** → **New** → **Network** and create two objects with the following parameters:

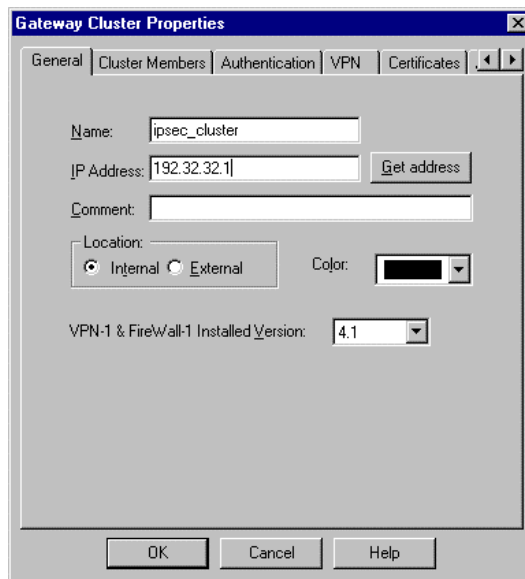


**Step 3** Enable Gateway Clusters in Policy → Properties → High Availability Options

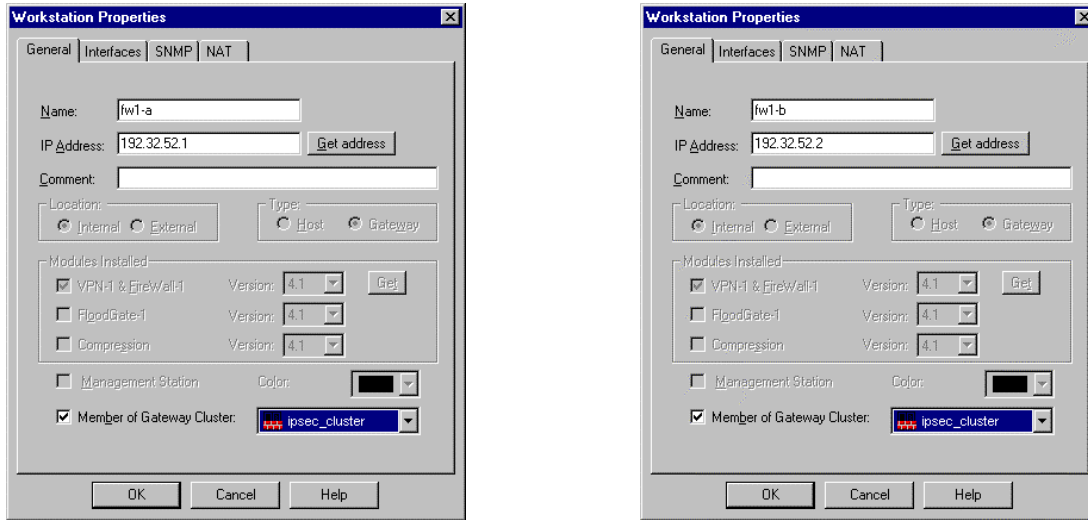


**NOTE:** Selecting “Install Security Policy on Gateway Cluster only if it can be successfully installed on ALL Gateway Cluster Members” will install the Security Policy either on all of the members of a gateway cluster or on none of them. This option is important if disparate policies on cluster members is undesirable.

**Step 4** Define a cluster object which logically represent the primary and secondary VPN-1 gateways. In the main Policy Editor window select **Manage → network Objects → New → Gateway Cluster** and create an object with the following parameters

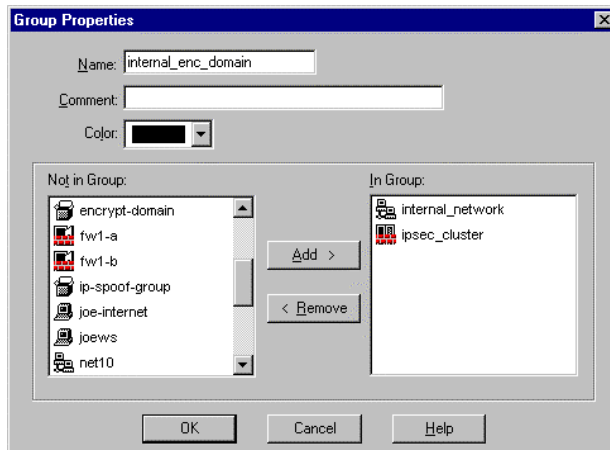


**Step 5** Modify the “fw1-a” & “fw1-b” objects to be a cluster members. Make them members of the “ipsec\_cluster” cluster.

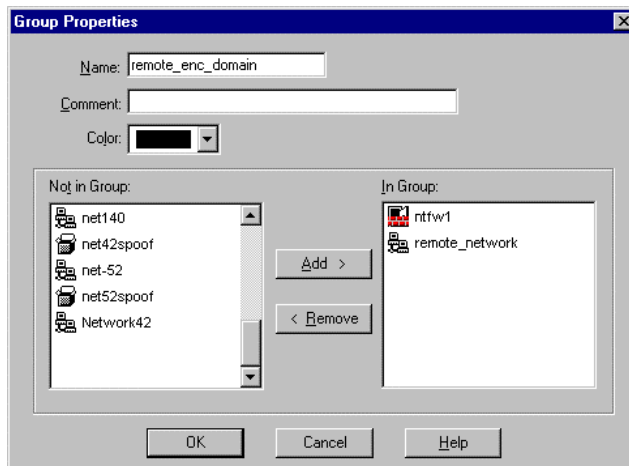


**Note** the existence of the “Member of Gateway Cluster” field that is not present in Step 1. This field is enabled by the “enable gateway clusters” selection in Step 3.

**Step 6** Define a group object that represents the internal network’s encryption domain. Select **Manage** → **network Objects** → **New** → **Group** and create a group object called internal\_enc\_domain by adding the “ipsec\_cluster” object and the “internal\_network” object



**Step 7** Define a group object that represents the internal network's encryption domain. Select **Manage** → **network Objects** → **New** → **Group** and create a group object called remote\_enc\_domain by adding the "ntfw1" object and the "remote\_network" object. Select **OK** in all windows until the network objects window is reached to complete the object modification



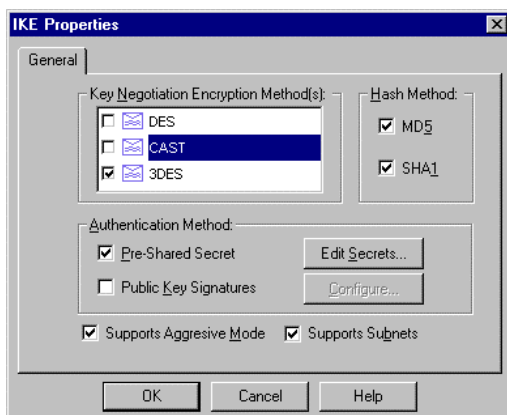
**Step 8** Modify the VPN parameters of the "ipsec\_cluster" object as follows:



Domain - "internal\_enc\_domain" (internal encryption domain group object)  
Encryption Schemes Defined Select "IKE"

Highlight IKE and Select **Edit**

The IKE Properties window will appear

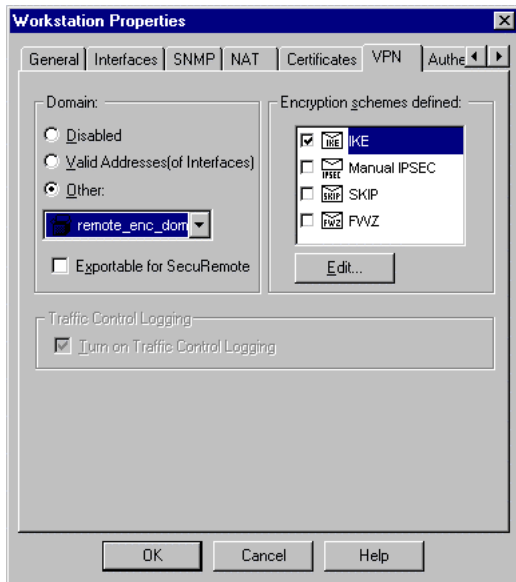


Select Key Negotiation Encryption Method – "3DES"  
Select Hash Method – "MD5" & "SHA1"  
Select Authentication Method - "Pre-Shared Secret"  
Select **OK** in all windows until the network objects window is reached to complete the object modification

**Note: The Pre-Shared Secrets will be edited all at once in the next step with the definition of the ntfw1 VPN properties**

**Note: Support for subnets facilitates interoperability with other vendors who implement this by default. The VPN device will setup the security associations (SAs) for the entire IP Subnet that is behind the VPN Gateway device. All IP addresses on this subnet will use two SAs that are defined for the subnet, one inbound and one outbound. Since only two SAs are need for the entire subnet, this simplifies the configuration as opposed to having two SAs per each IP Host.**

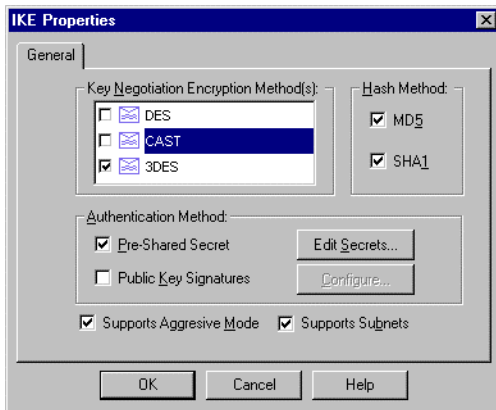
**Step 9** Modify the VPN parameters of the “ntfw1” object as follows:



Domain - "internal\_enc\_domain" (internal encryption domain group object)  
Encryption Schemes Defined Select “IKE”

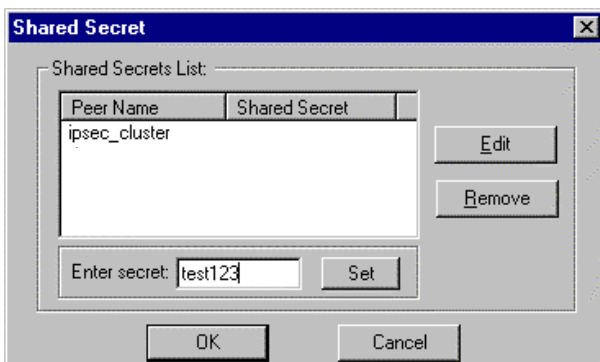
Highlight IKE and Select **Edit**

The IKE Properties window will appear



Select Key Negotiation Encryption Method – “3DES”  
Select Hash Method – “MD5” & “SHA1”  
Select Authentication Method - “Pre-Shared Secret”  
Select **Edit Secrets**

The Shared Secrets List window will appear



Select “ipsec\_cluster”

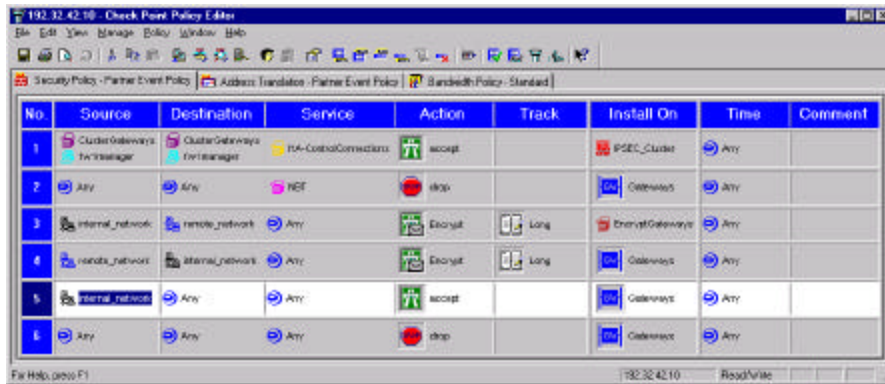
Select **Edit**

Enter the shared secret of **test123**

Select **Set**

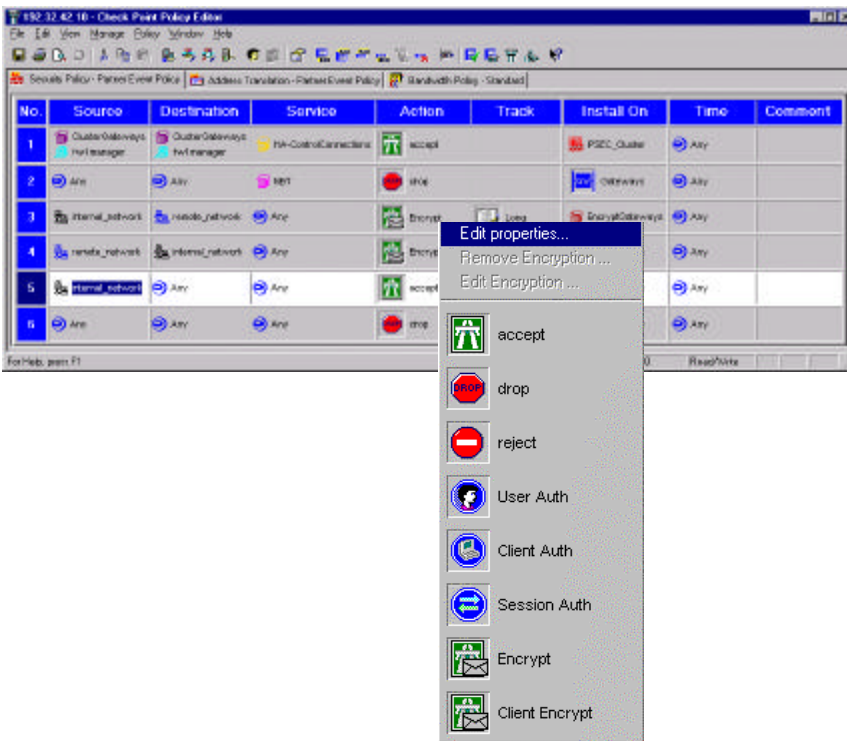
Select **OK** in all windows until the network objects window is reached to complete the object modification

**Step 10** In the Check Point Policy editor create a rule enabling encryption between the internal network and the remote network.

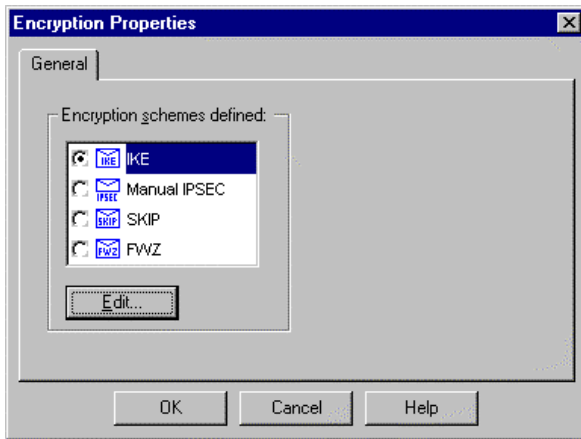


Rules three and four govern the encryption between sites Rule one enables communication between the cluster gateway and the management console

Once the rule is created, click the right mouse button in the action field. The action drop down menu will appear.



Select  
**Edit properties**

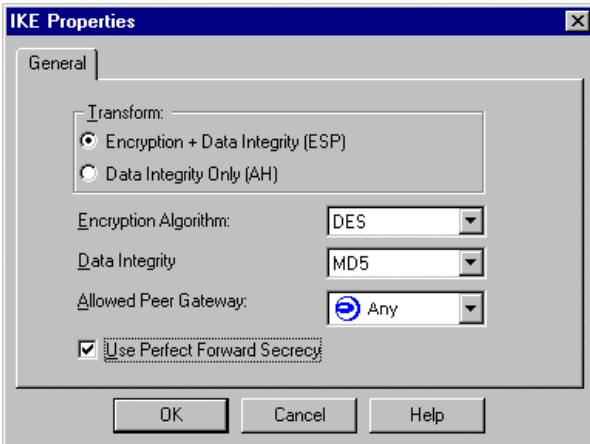


The Encryption properties window will appear.

Make sure the Encryption properties are set to IKE

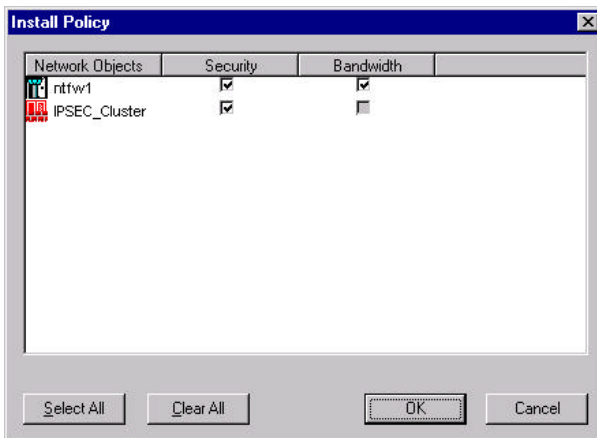
Select **Edit**

The IKE properties window will appear



Make sure the IKE properties are set as shown

Select **OK**

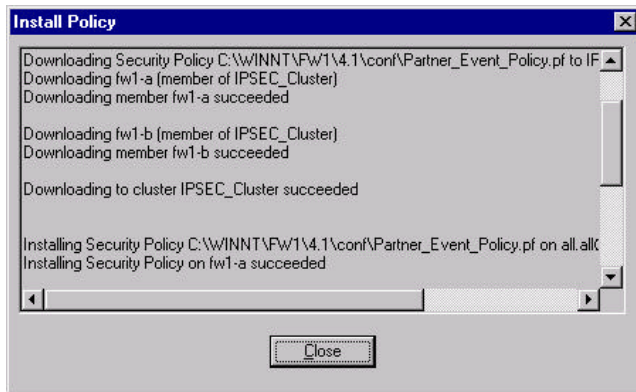


Select **Policy** → **Install** from the policy editor window.

Select **OK**

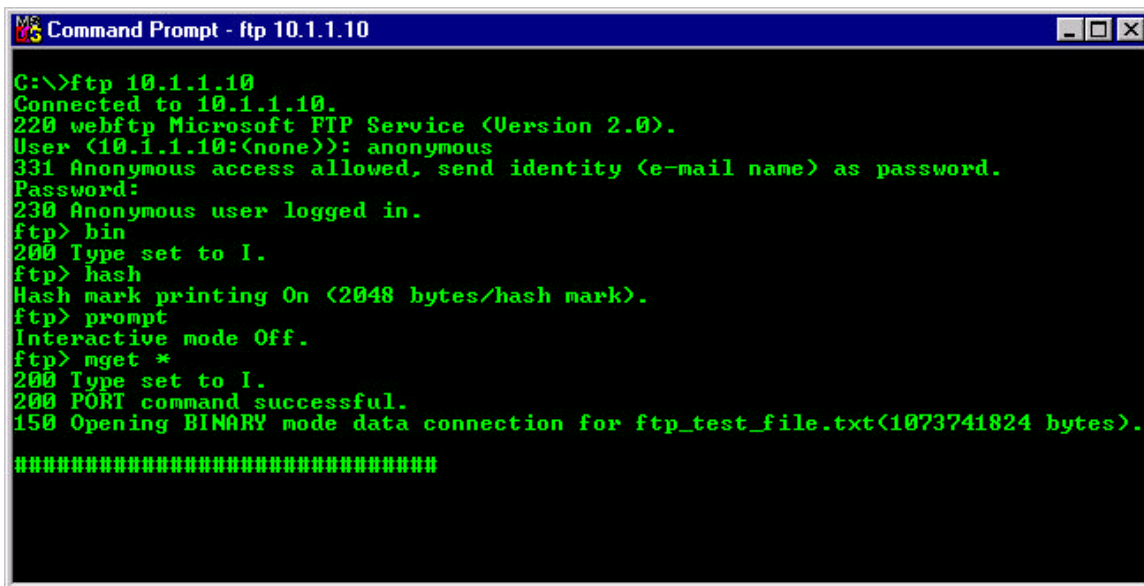
The rule base will be compiled and installed on all VPN gateways.

**Note:** ntfw1 is configured with Floodgate-1 Bandwidth Management and therefore the object appears different, and the option to install a bandwidth policy is enabled.

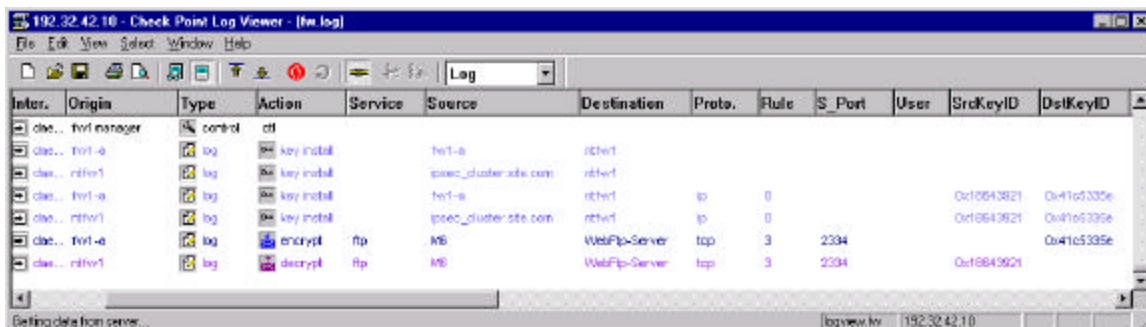


Notice the policy is downloaded to each member of the cluster

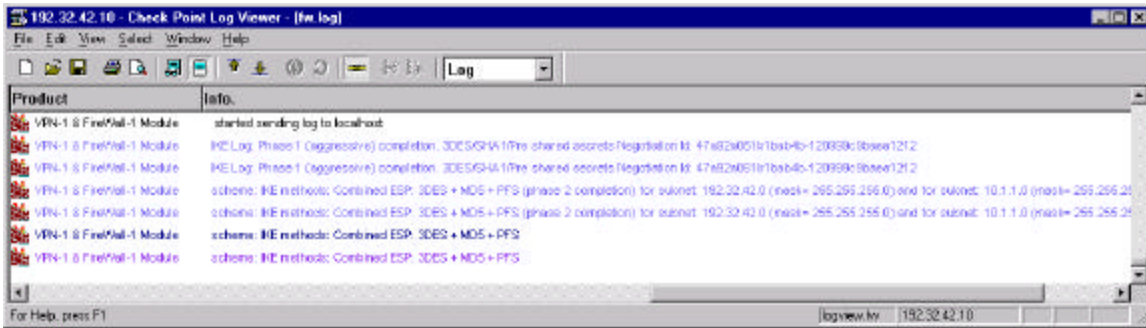
**Step 11** Test the configuration by initiating an FTP session from 192.32.42.11 to 10.1.1.10. Set the FTP parameters to show hash marks during an FTP session by issuing the command **hash**. FTP a large file from 10.1.1.10 by using the command **mget ftp\_test\_file.txt**



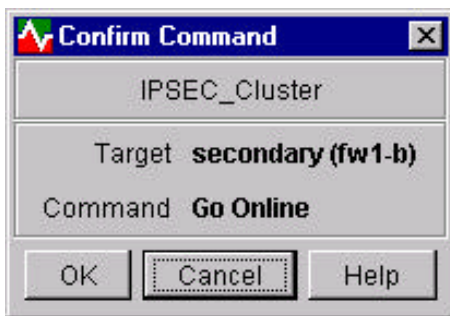
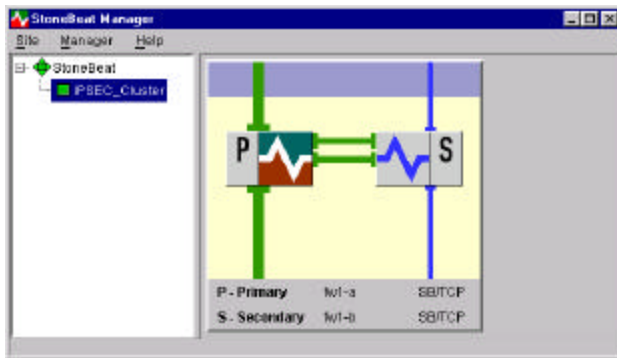
Open the Log view and note the successful IKE phase 1 and phase 2 key negotiation between the primary (fw1-a) and ntfw1. Also note the ftp encrypt & decrypt between fw1-a and ntfw1. Note – log viewer fields in this document are segregated into two screen captures because of window size constraints.



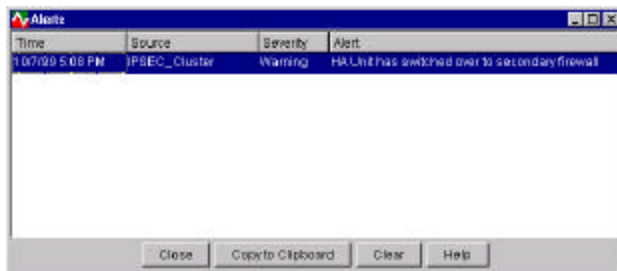
In the info field, note that the phase two completion is conducted for the subnets of 192.32.42.0 & 10.1.1.0.



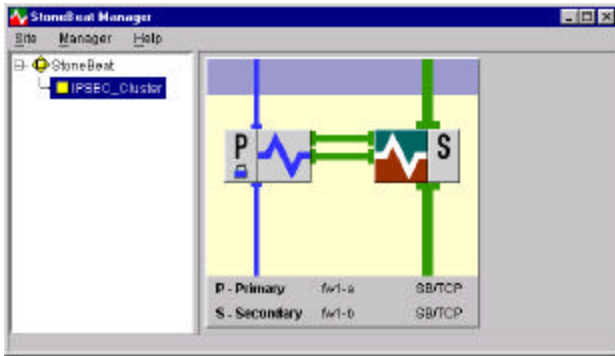
We can now test the IKE failover. For this configuration we have used StoneBeat for failover. The StoneBeat manager shows fw1-a as the primary, and that the primary is active. To fail over to the secondary, Click the right mouse button over the secondary symbol and select **Go Online**.



The Confirm Command window will appear, select **OK**



The Alerts window will indicate that the HA unit has switched to the secondary



The StoneBeat manager will highlight the secondary (fw1-b) as now being active.



Notice that the FTP has continued with minimal interruption.

Notice also that fw1-b and ntfw1 have automatically performed a successful IKE Phase 2 negotiation

