

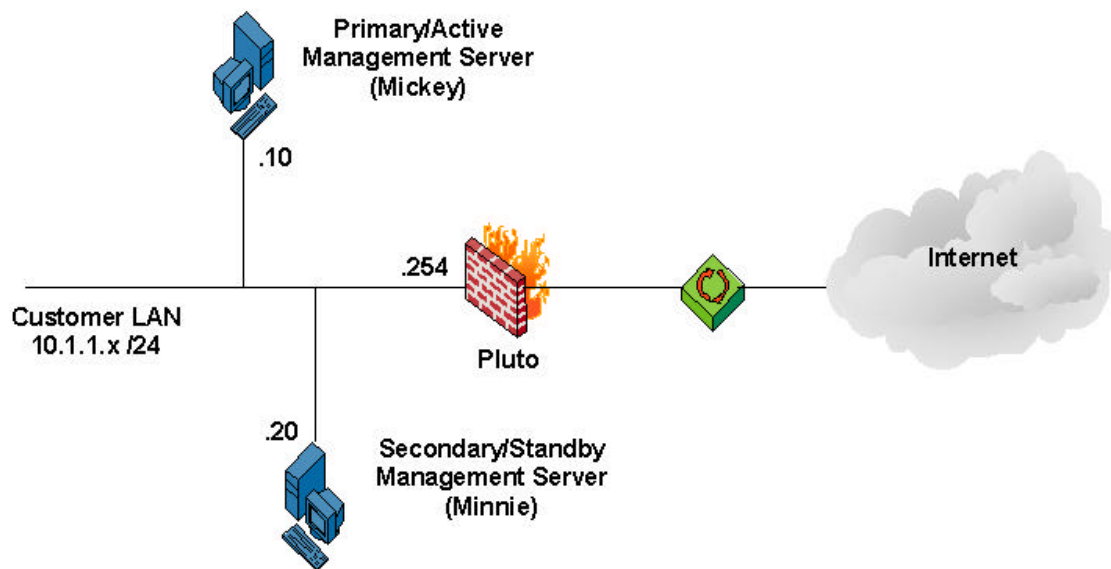


How to configure Management High Availability in Check Point NG FP-2

Author:
Joe Green
Security Engineer
Check Point Software Technologies, Inc.
5757 W. Century Blvd.
Los Angeles, CA 90045
jgreen@us.checkpoint.com

This document assumes the following.

1. A working knowledge of Check Point NG in a distributed configuration. This includes a working knowledge of Secure Internal Communication.
2. You have installed Check Point NG FP2 in a distributed configuration. For Management High Availability to be supported (and work), the Manager cannot reside on the FW-1/VPN-1 Module.
3. You will also need at least 3 physical computers for this configuration. The map below outlines the Network Setup.



Before configuring the secondary management, make sure that the primary management and the enforcement module are communicating via SIC. If SIC is not functioning, do not continue. Also, for the server that will be used as the secondary management server, make sure that it is reachable via IP connectivity.

Note: SIC only functions when the management is able to reach the module and other managers via name resolution.

If all of the components above are working, it's time to configure the secondary Management server.

Install the Check Point software on the secondary management server and select "Enterprise Secondary Management". See Fig 1.1 & 1.2

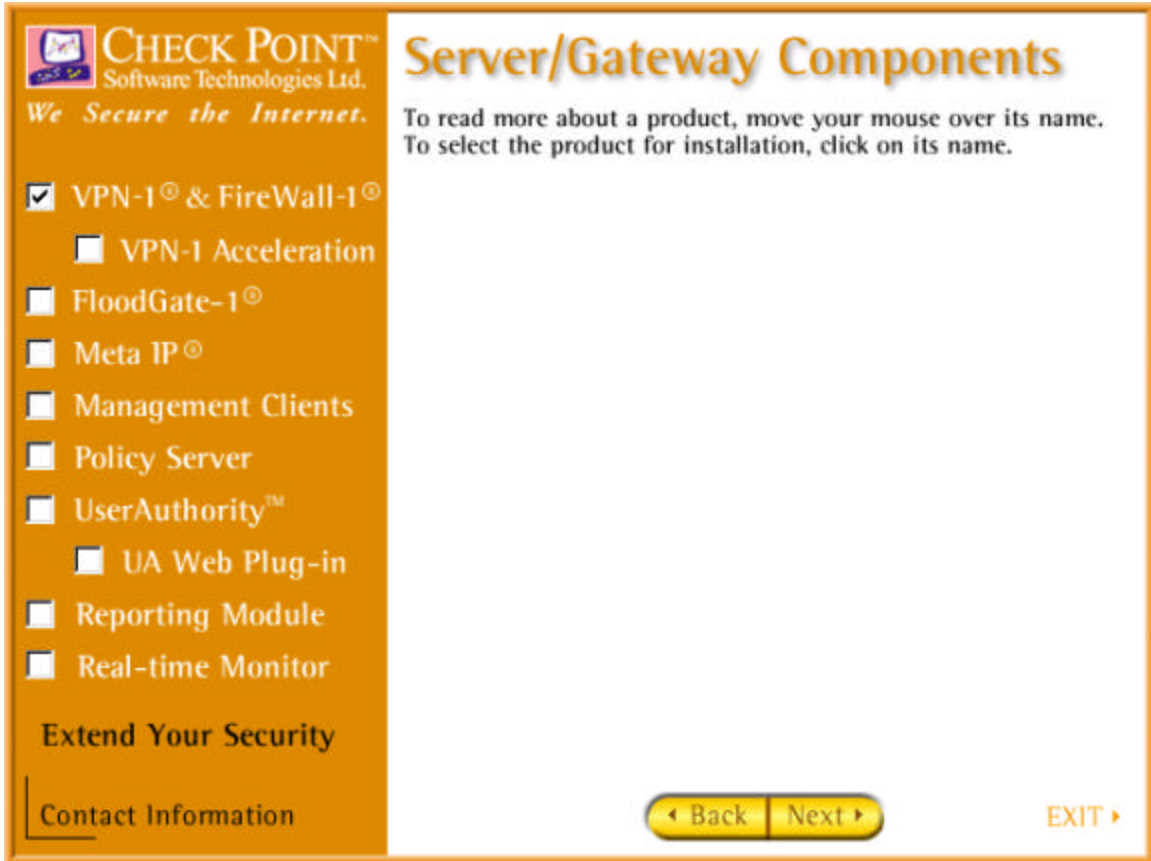


Fig. 1.1 Component Selection

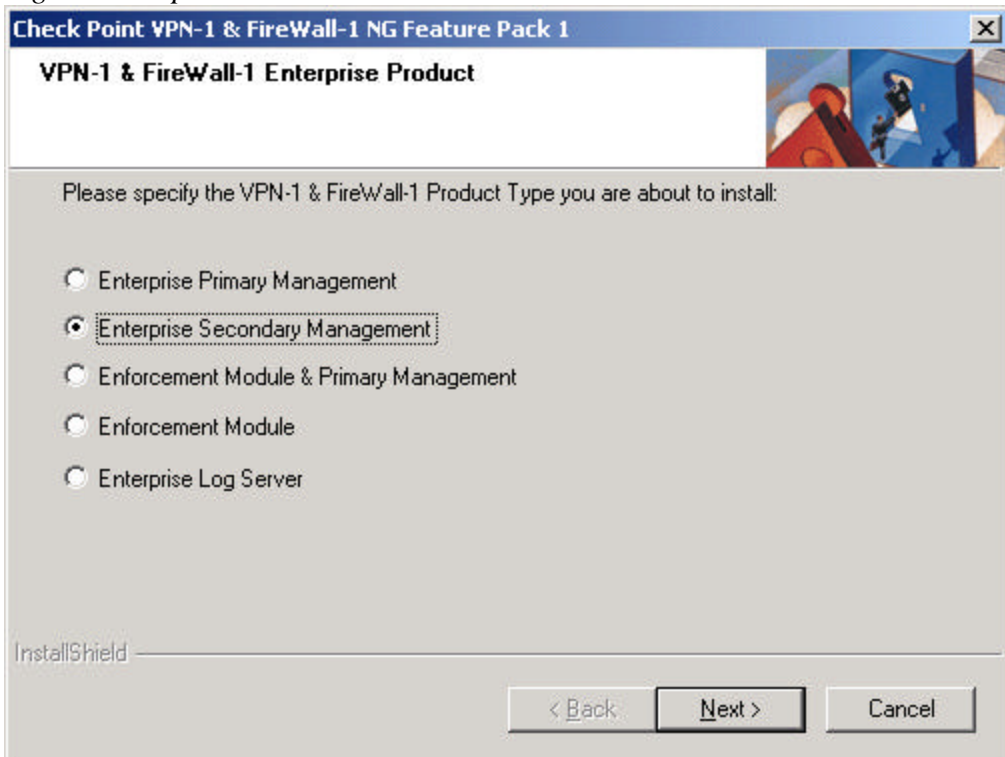


Fig 1.2 Product Selection

Check Point Next Generation Feature Pack 2

Set the SIC password and reboot. Next, log into the Primary Management server and create a new “Check Point Host”.

See Fig. 1.3

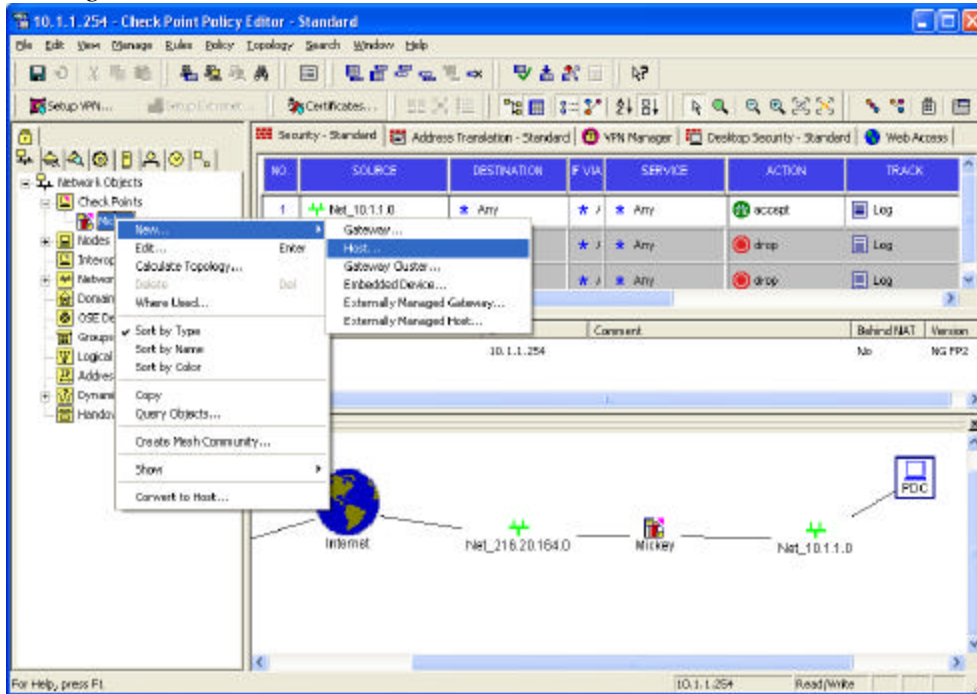


Fig 1.3 New Check Point Host

From there, define the parameters for the secondary management host. See Fig 1.4

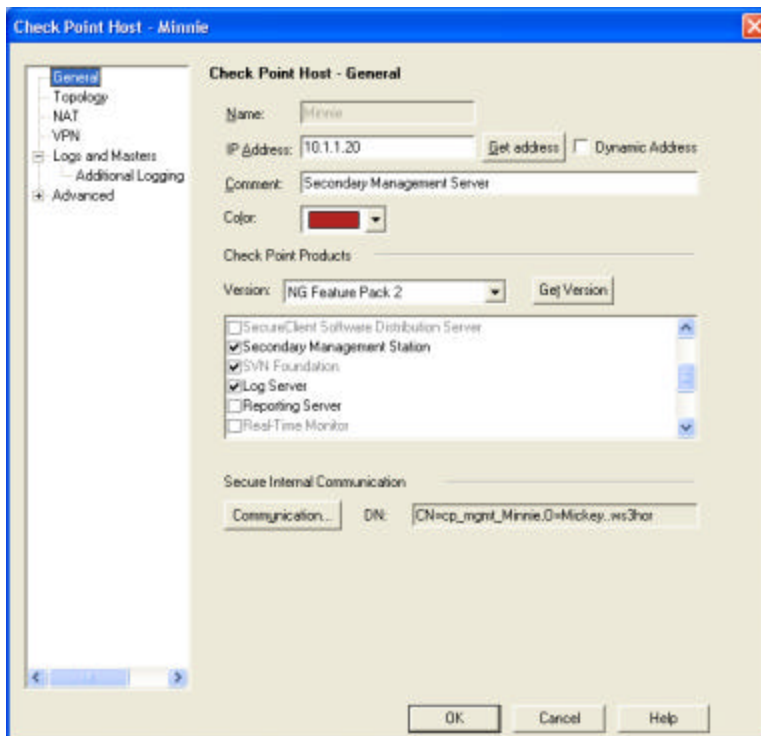


Fig. 1.4 Host Configuration

Check Point Next Generation Feature Pack 2

Make sure that you have checked all the boxes for the components installed on the secondary management server.

Initialize the Secure Internal Communication and make sure that the secondary can communicate with the primary management server. At this point, make sure the correct license is applied to both management servers and reboot the secondary manager. Then, install the current rule base to all modules.

Now, login and go to the “Policy” menu of the Check Point Policy editor and click on the “Management High Availability...” menu. *See Fig. 1.5*

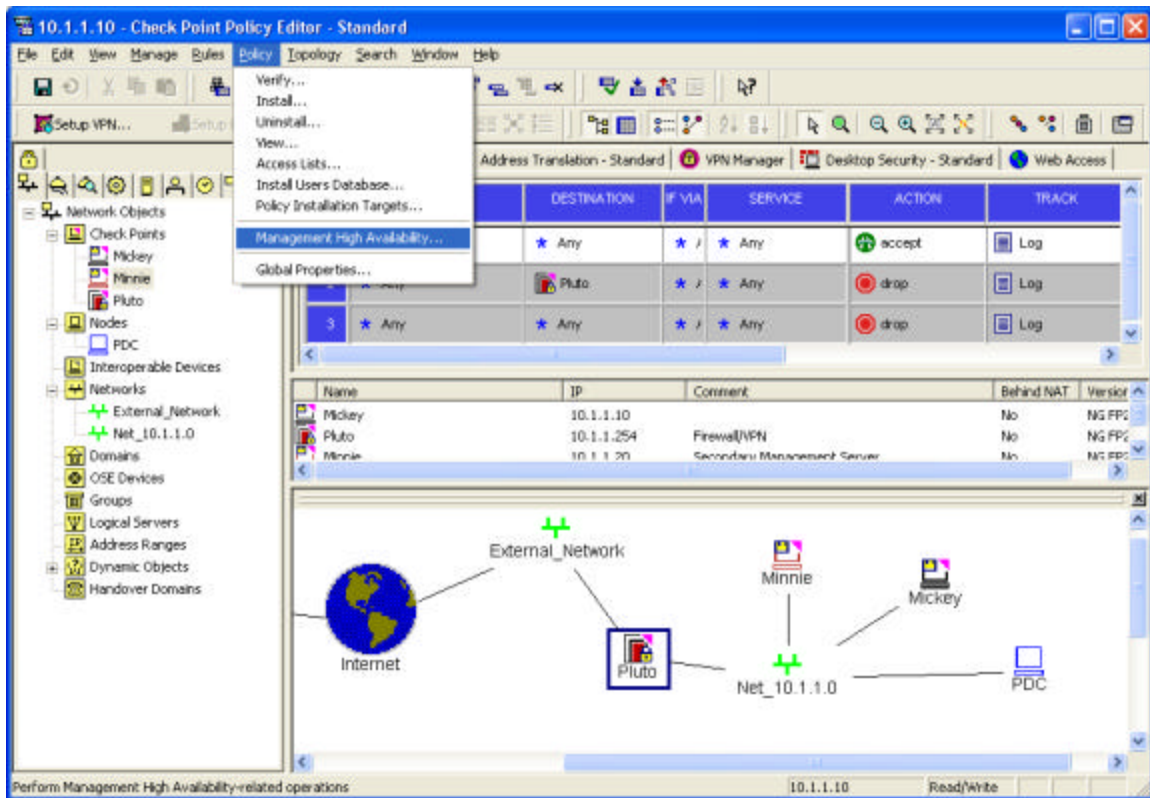


Fig. 1.5 Configuring Management HA

From the Management High Availability screen, synchronize the gateways. *See Fig. 1.6*

Check Point Next Generation Feature Pack 2

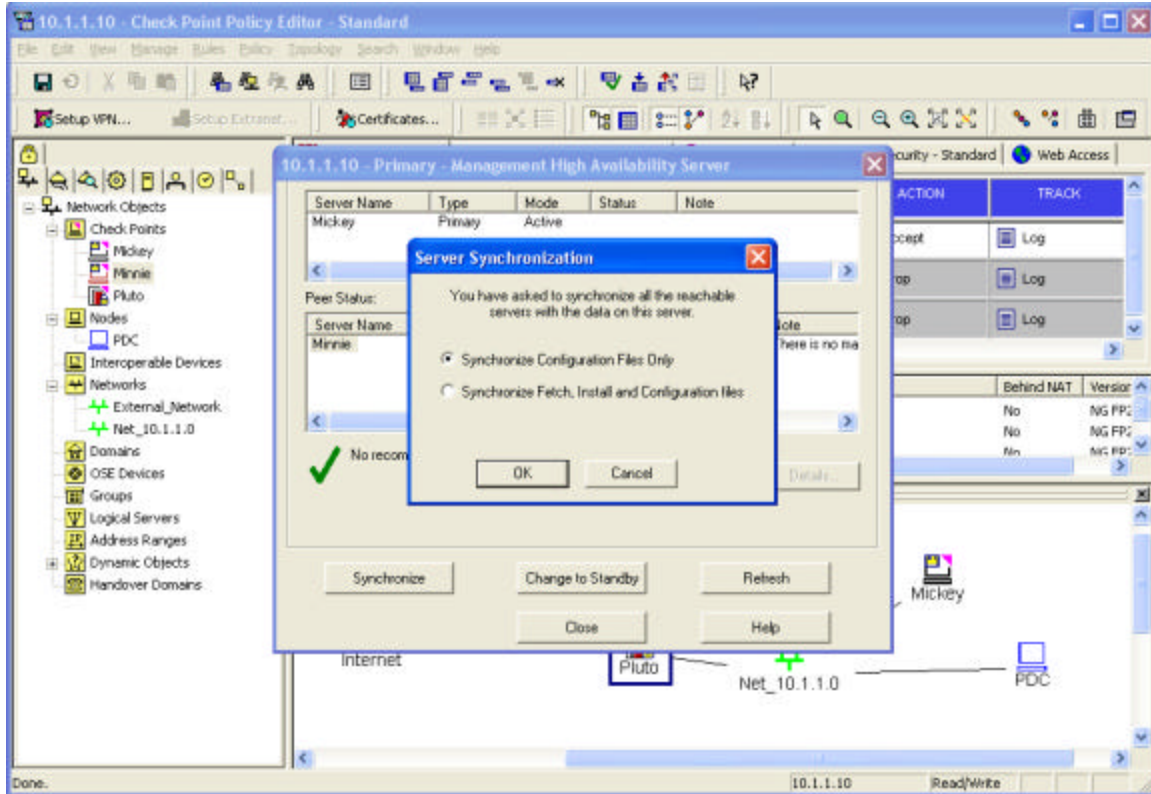


Fig 1.6 Dialogue Box with Status

The two configuration options presented in the screen above are,

1. “Synchronize Configuration Files Only”. This will synchronize only the database and configuration files.
2. “Synchronize Fetch, Install and Configuration Files”. In addition to the above, the fetch and install files will be synchronized. This will enable the modules to fetch their policy from the secondary management if it is defined as a master.

It is recommended to perform a full synchronization at this point. E.g. “Synchronize Fetch, Install and Configuration Files”. After the sync is done, you should see the following. See Fig 1.7

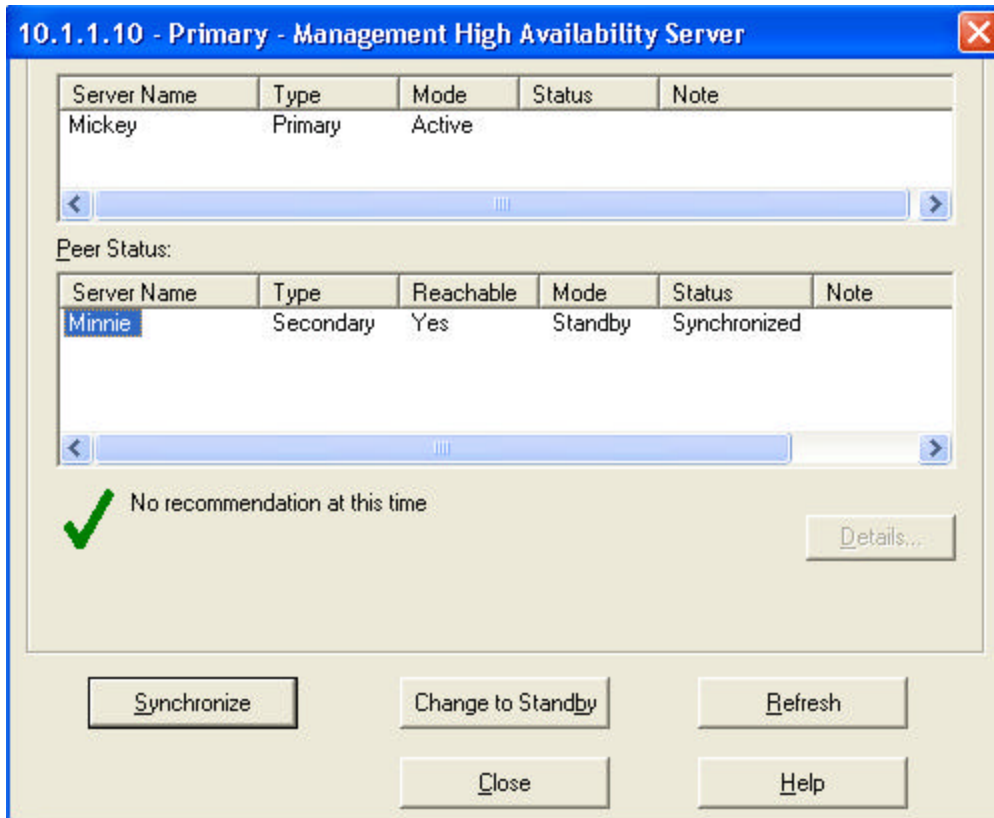


Fig 1.7 Synchronization Status

After the servers have been synchronized manually, you can automate the synchronization process. See Fig. 1.8

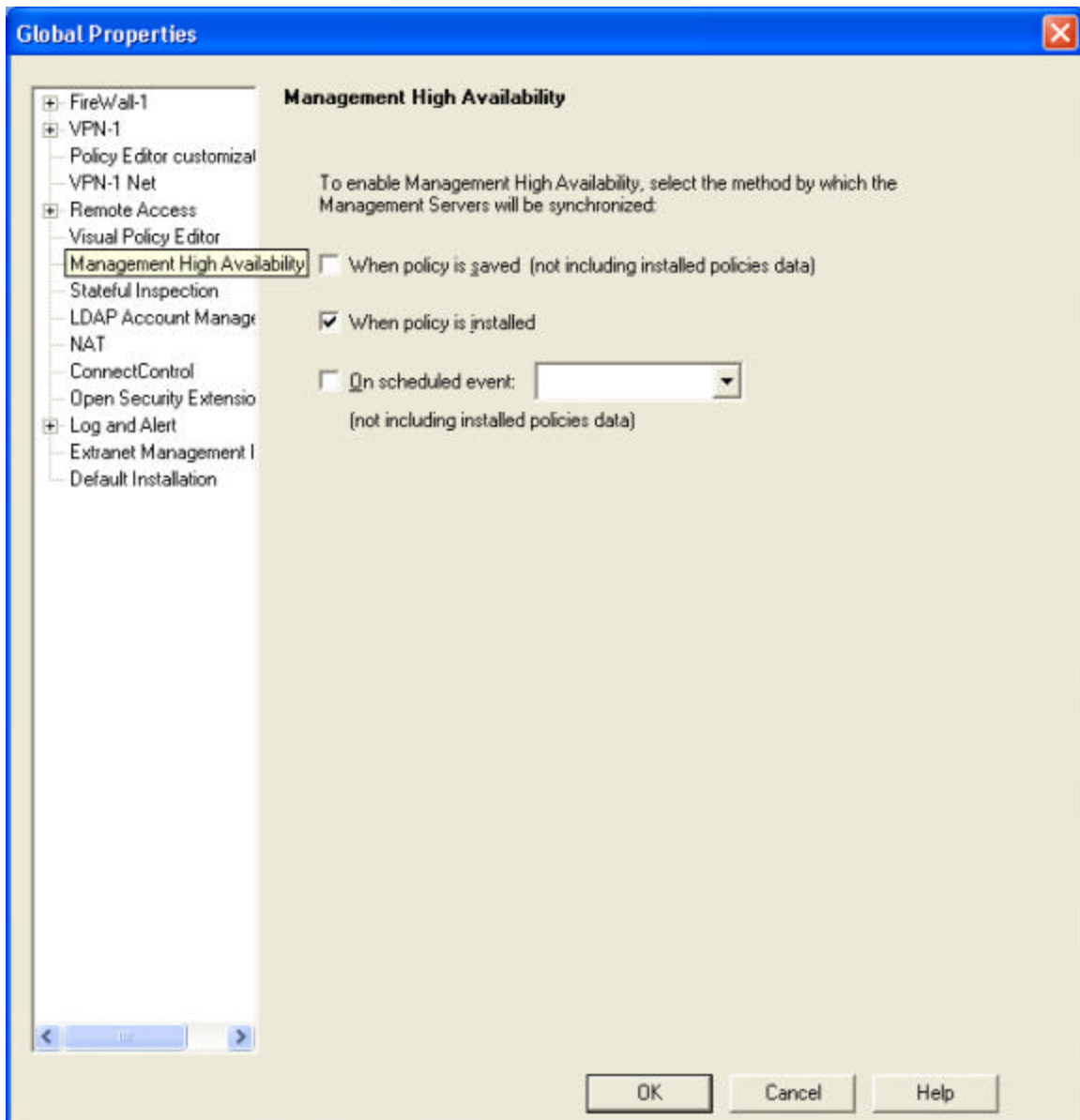
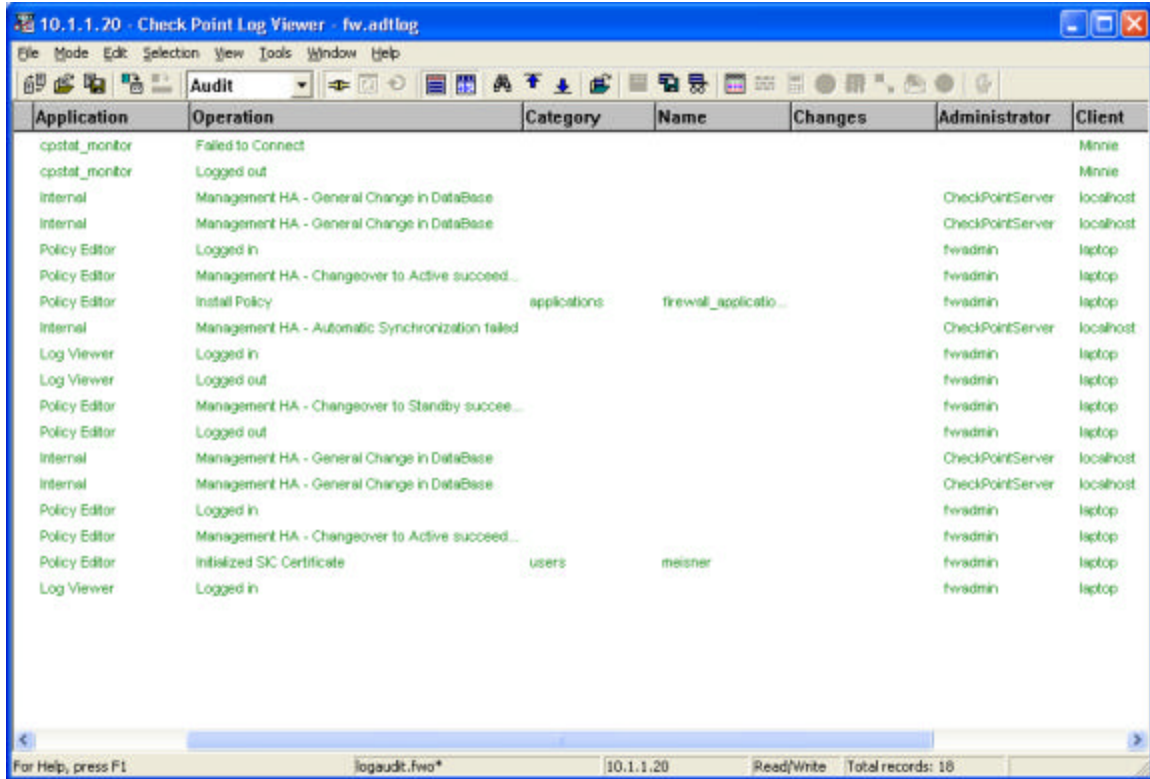


Fig. 1.8 Automating Synchronization

The log viewer should now show the events that have transpired. See fig. 1.9

Check Point Next Generation Feature Pack 2



The screenshot shows the 'Check Point Log Viewer' application window. The title bar reads '10.1.1.20 - Check Point Log Viewer - fw.adflog'. The menu bar includes 'File', 'Mode', 'Edit', 'Selection', 'View', 'Tools', 'Window', and 'Help'. The toolbar contains various icons for file operations and viewing. The main area displays a table of audit log entries. The status bar at the bottom shows 'logaudit.fwo*', '10.1.1.20', 'Read/Write', and 'Total records: 18'.

Application	Operation	Category	Name	Changes	Administrator	Client
cpstat_monitor	Failed to Connect					Minnie
cpstat_monitor	Logged out					Minnie
Internal	Management HA - General Change in DataBase				CheckPointServer	localhost
Internal	Management HA - General Change in DataBase				CheckPointServer	localhost
Policy Editor	Logged in				fwadmin	laptop
Policy Editor	Management HA - Changeover to Active succeed...				fwadmin	laptop
Policy Editor	Install Policy	applications	firewall_applicatio...		fwadmin	laptop
Internal	Management HA - Automatic Synchronization failed				CheckPointServer	localhost
Log Viewer	Logged in				fwadmin	laptop
Log Viewer	Logged out				fwadmin	laptop
Policy Editor	Management HA - Changeover to Standby succeed...				fwadmin	laptop
Policy Editor	Logged out				fwadmin	laptop
Internal	Management HA - General Change in DataBase				CheckPointServer	localhost
Internal	Management HA - General Change in DataBase				CheckPointServer	localhost
Policy Editor	Logged in				fwadmin	laptop
Policy Editor	Management HA - Changeover to Active succeed...				fwadmin	laptop
Policy Editor	Initialized SIC Certificate	users	meisner		fwadmin	laptop
Log Viewer	Logged in				fwadmin	laptop

Fig. 1.9 Audit Log Displaying Status

Now, make sure that the enforcement points properties are configured for management HA. See Fig. 1.10 and 1.11

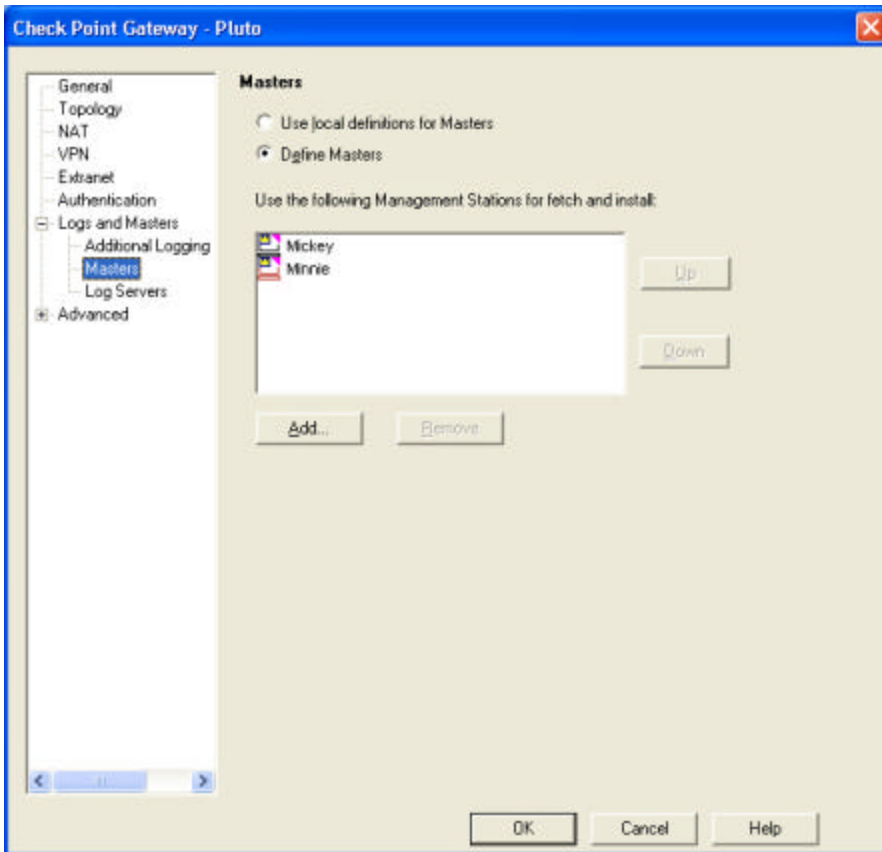


Fig 1.10 Masters

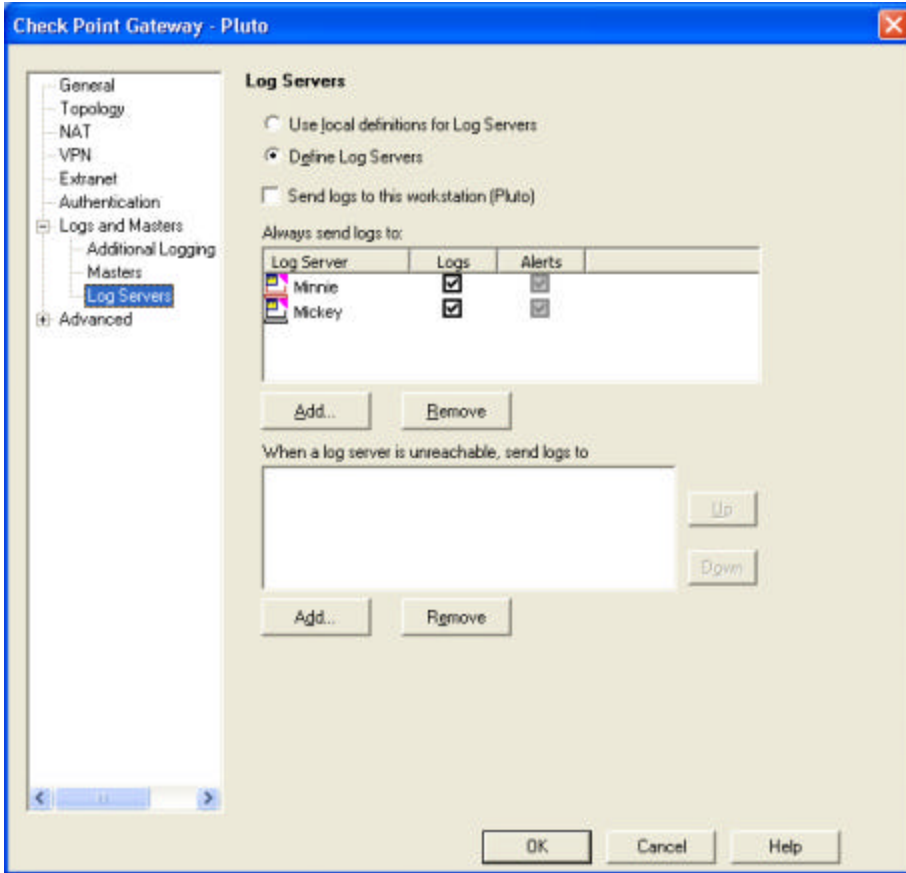


Fig. 1.11 Log Servers

At this point, Management HA is now in place and you can test the fail over capabilities.

To test the fail over, perform the following procedure:

Shut down the Primary Management Server. Then, through the standard Check Point Policy editor, log into the secondary management server by specifying it's IP in the "Management Server" field of the login screen. The following screen should appear upon login. See Fig. 1.12

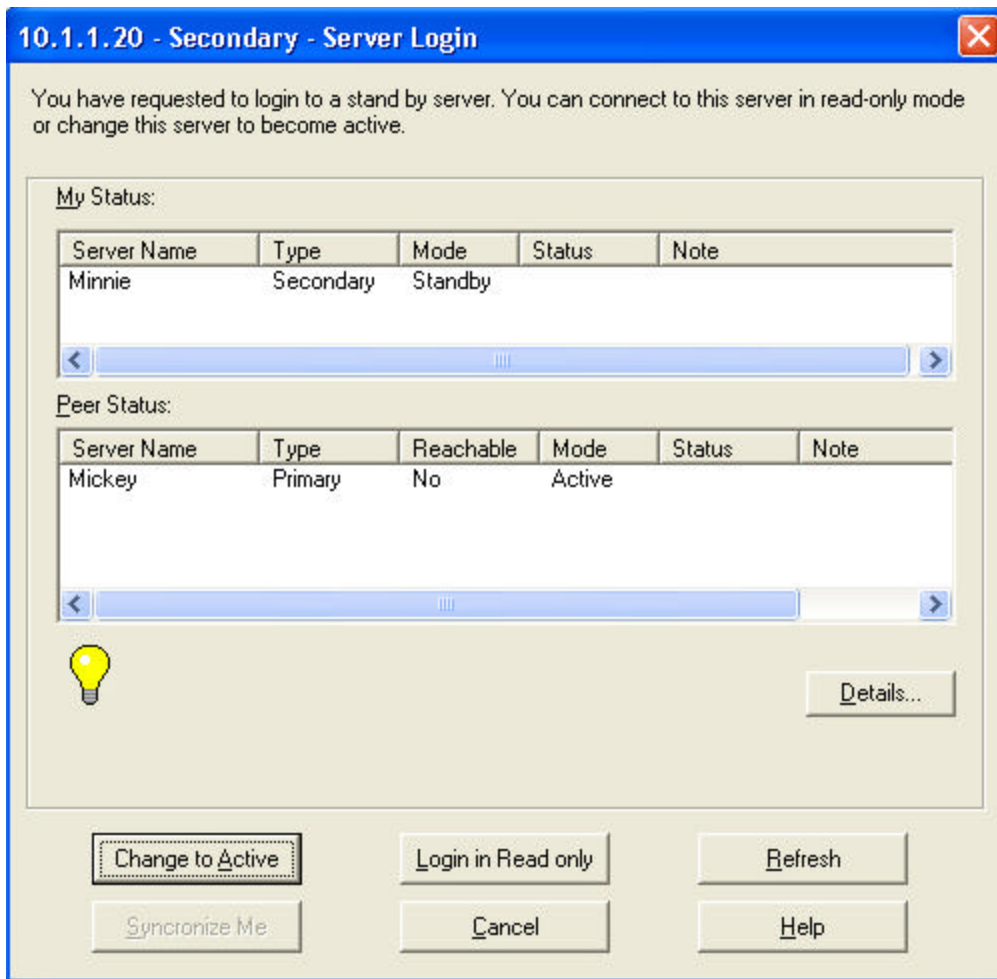


Fig. 1.12 Log in to Secondary

Click on the button titled “Change to Active”. The following screen will appear. See Fig 1.13

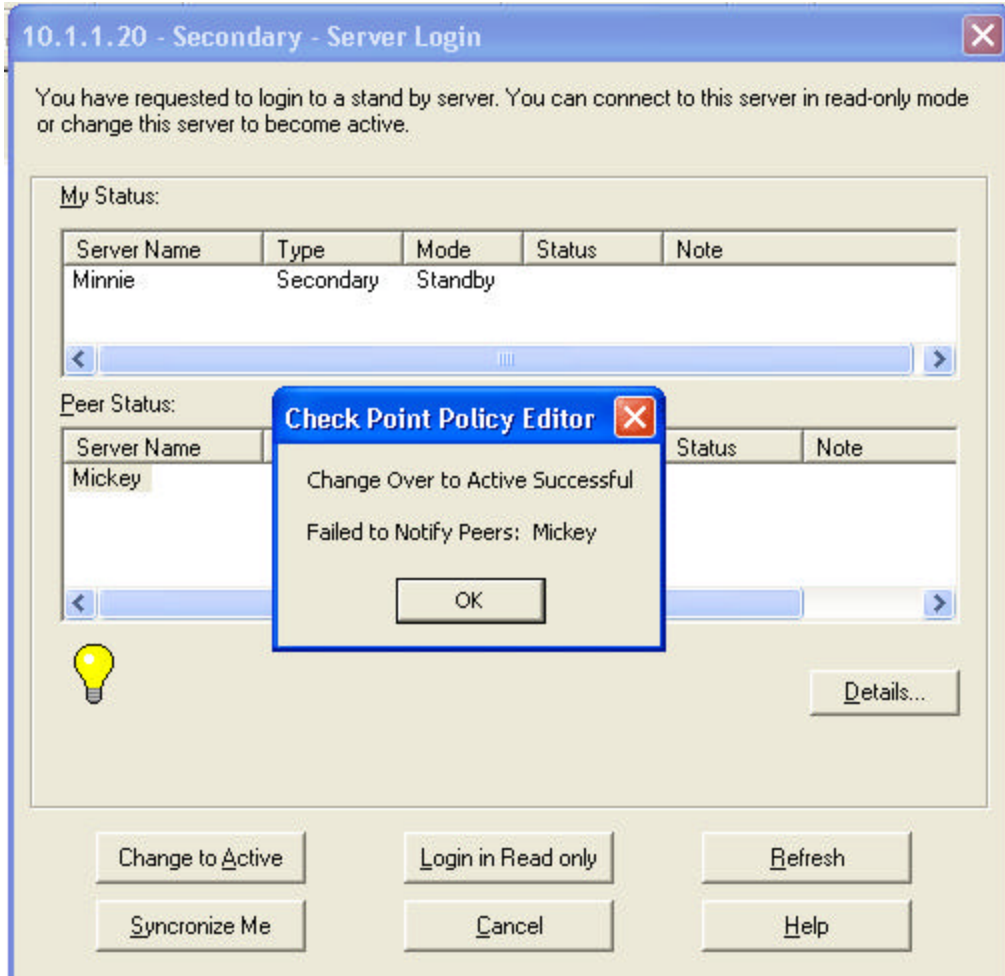


Fig. 1.13 Failover Notification

Now, install a policy from the secondary management server. See Fig. 1.14

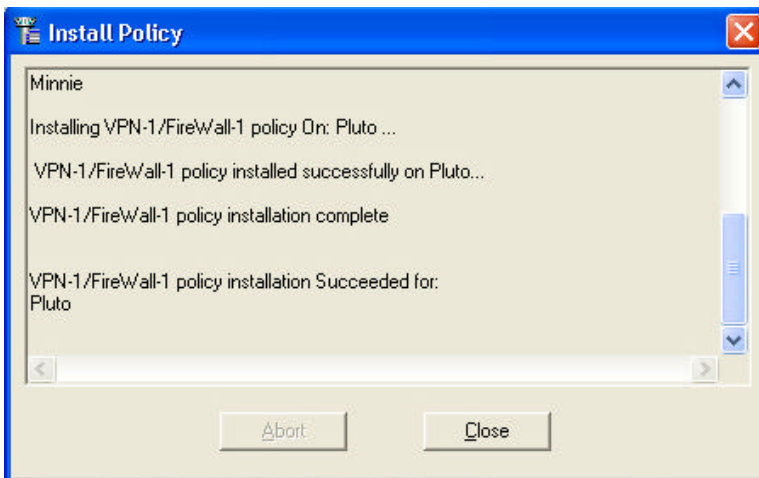


Fig. 1.14 Policy Installation

Check Point Next Generation Feature Pack 2

At this point, you can bring the Primary Management Server back on line or continue with the Secondary as the Active.

If you choose to bring the primary back online, change the secondary server's status to "Stand By". See Fig. 1.15

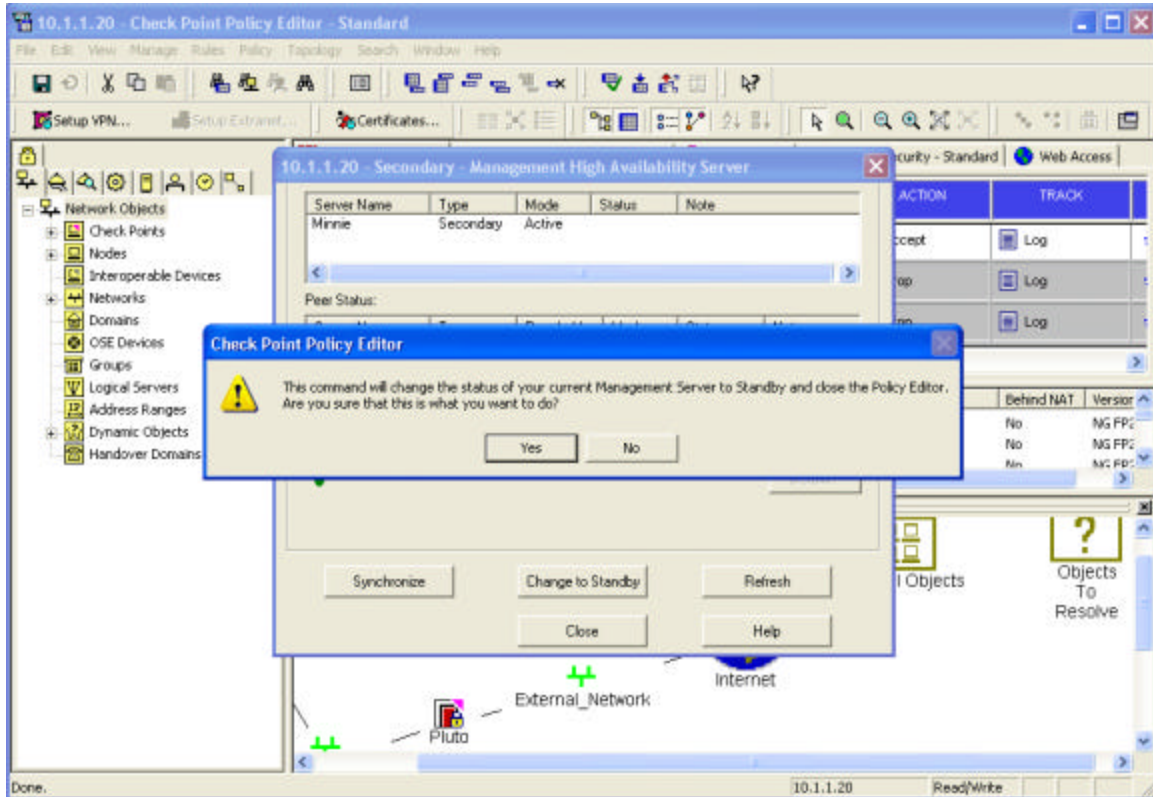


Fig. 1.15 Changing Primary back to Secondary

This will change the server to standby and you can now log back into the Primary Management server.

Further documentation can be found in the Check Point Management guide.