

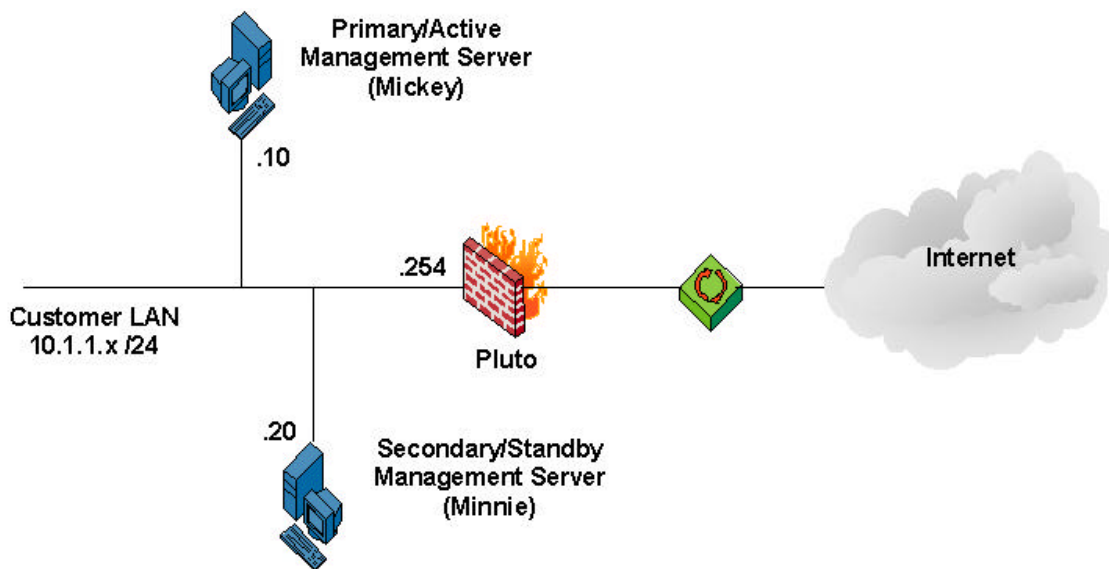


# **How to configure a Customer Logging Module in Check Point NG FP2**

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

This document assumes the following.

1. A working knowledge of Check Point NG in a distributed configuration (mgmt. separate from the module). This includes a working knowledge of SIC (Secure Internal Communication).
2. You have installed Check Point NG FP2 in a distributed configuration.
3. This guide details a distributed configuration. Organizations that have a manager managing multiple Firewalls are usually in need of a dedicated Customer Logging Module) CLM. The map below outlines the Network Setup used for this document.



Before configuring the CLM, 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 a CLM, make sure that it is reachable via IP connectivity. If you do not have IP connectivity, do not proceed.

*Note: SIC only functions when the management is able to reach the module and other components via name resolution. Configure your DNS or hosts file properly.*

If all of the components above are working, it's time to configure your CLM.

First, install the Check Point software on your CLM. See Fig. 1.1 and Fig. 1.2



Fig. 1.1 Component Selection

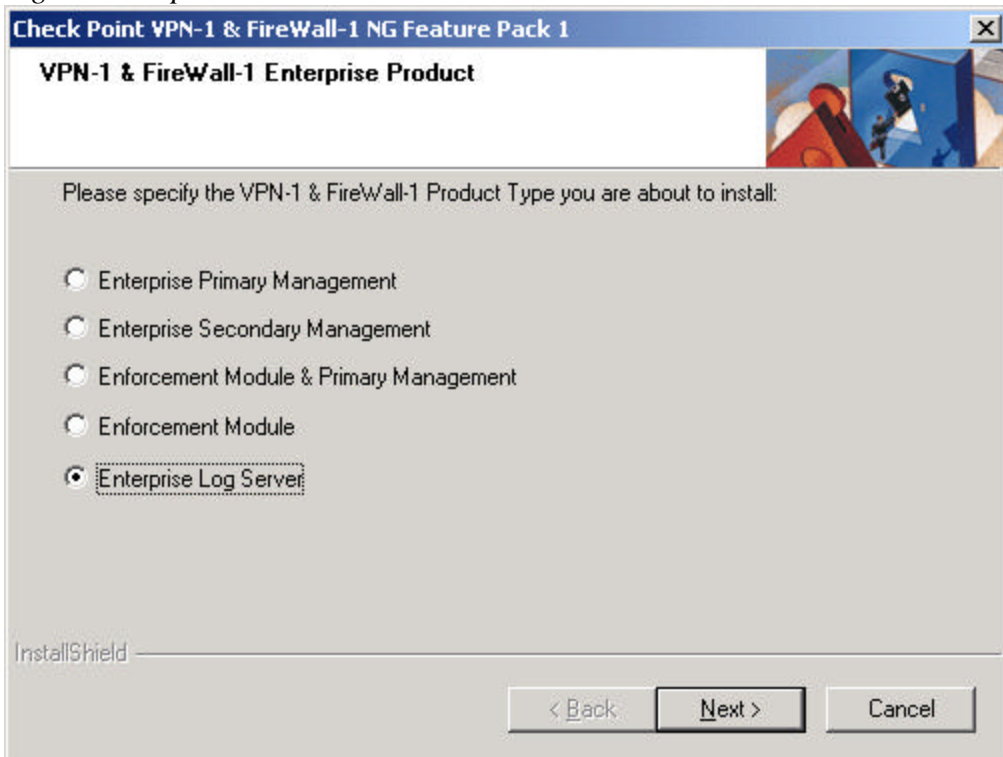
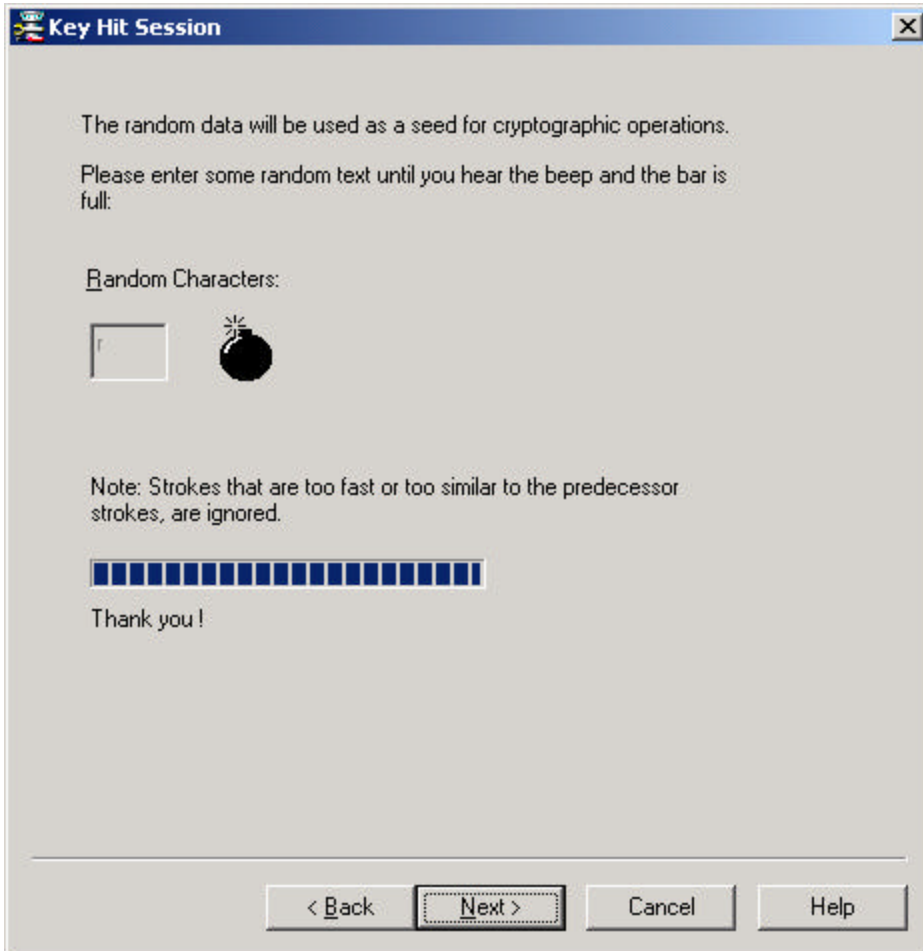


Fig. 1.2 Product Selection

*Check Point Next Generation Feature Pack 2*

During installation you will generate the random seed and set the one time password for Secure Internal Communication. *See Fig. 1.3 and .1.4* You also need to specify what GUI clients will be allowed to connect to the CLM. After installation is complete reboot the module.



*Fig. 1.3 Seed Generation*

Check Point Next Generation Feature Pack 2

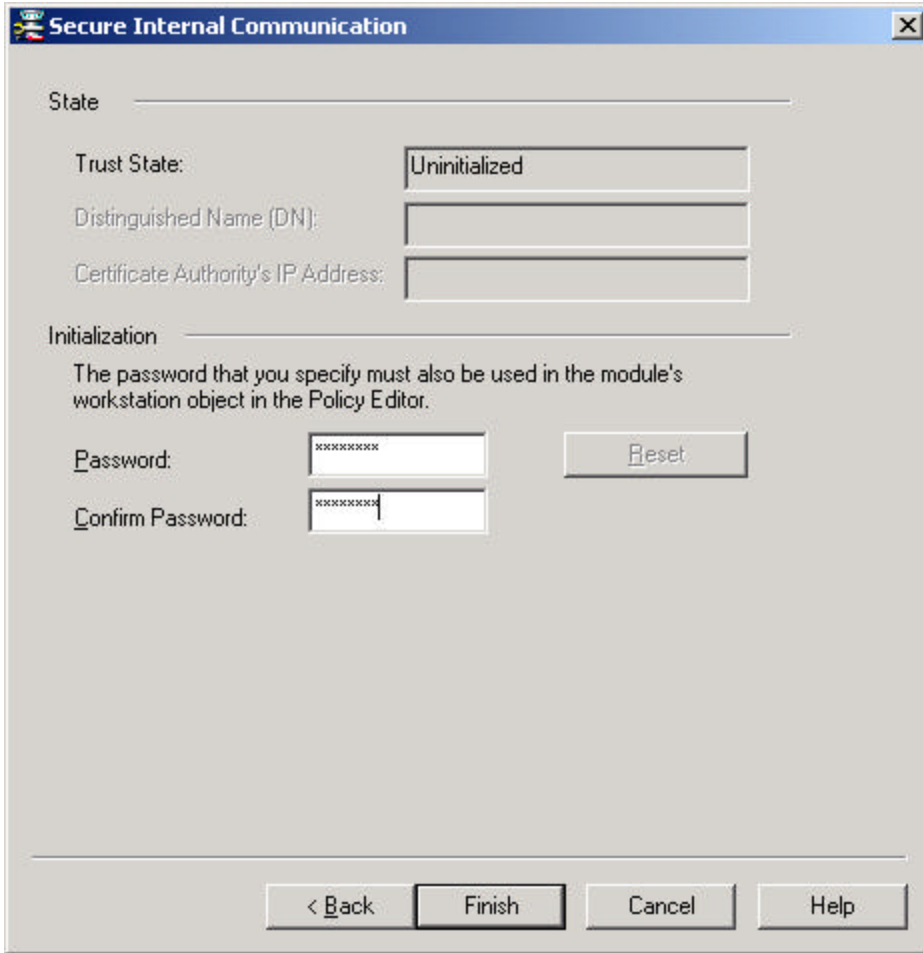


Fig. 1.4 SIC Password

The rest of the configuration is done from the Primary Management Server. Once logged in, you need to create an object that represents the CLM. See Fig. 1.5 and Fig 1.6

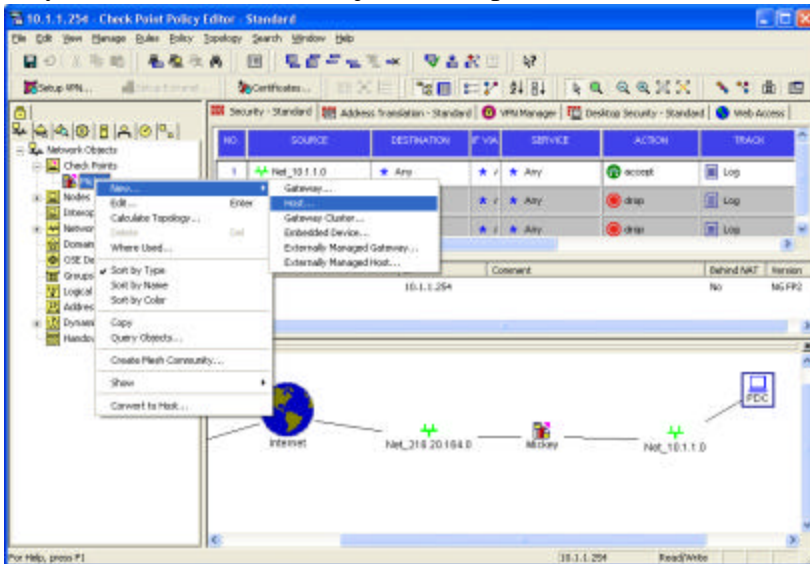


Fig. 1.5 New Host Creation

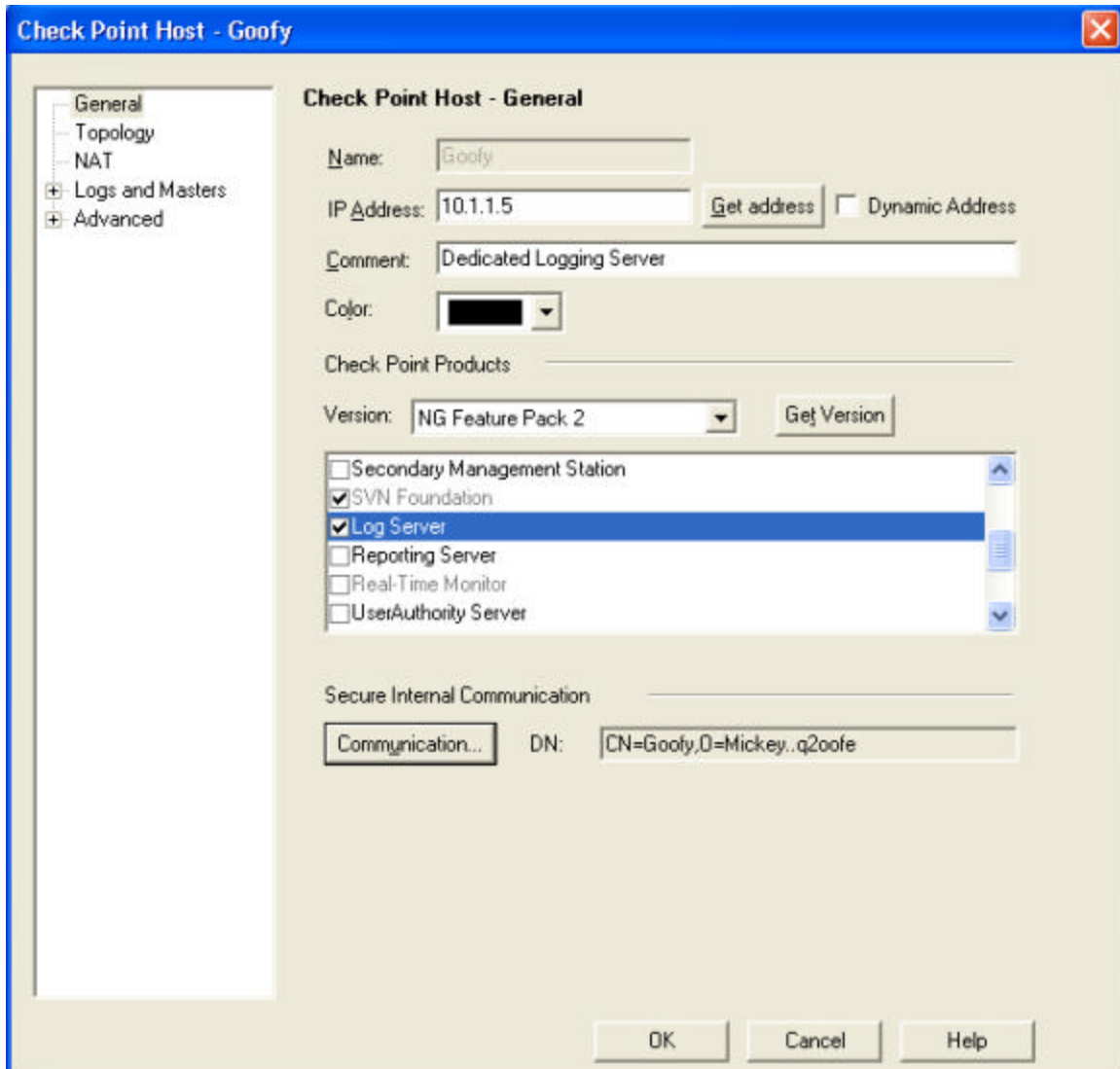


Fig. 1.6 New Host Configuration (CLM)

Make sure that the manager can resolve the host name of the new CLM or initializing the SIC may fail. Also, make sure that you check the box to signify that it is a Log Server.

Now, the remote modules need to be configured to take advantage of the new CLM. From the Firewall Modules properties (Mickey), go to the “Log and Masters” section and select its logging destinations. See Fig. 1.7

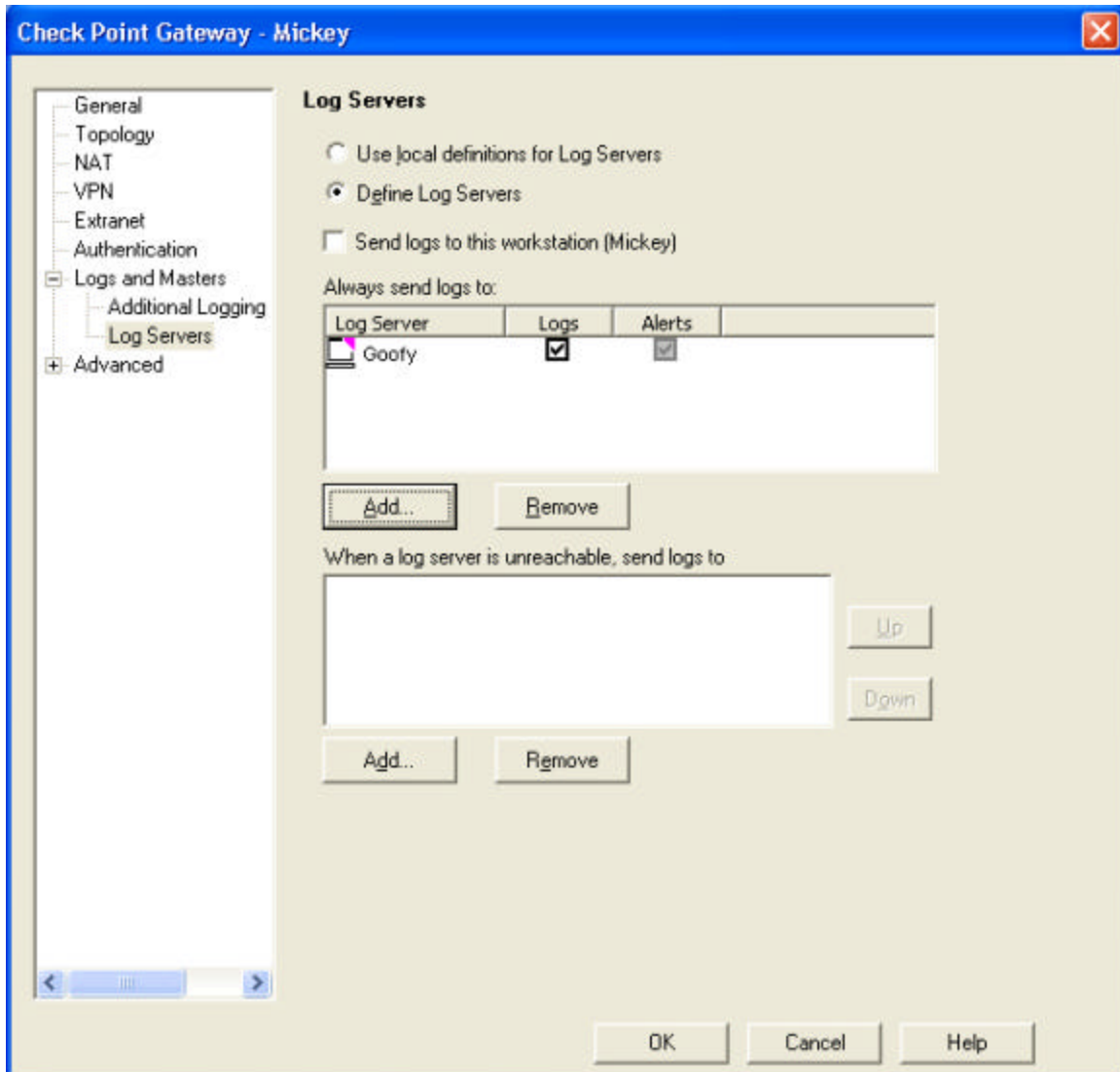


Fig 1.7 Log Server Definition

Install your policy and that's it! Below is a screen shot of the GUI with all the components configured. See Fig. 1.8

## Check Point Next Generation Feature Pack 2

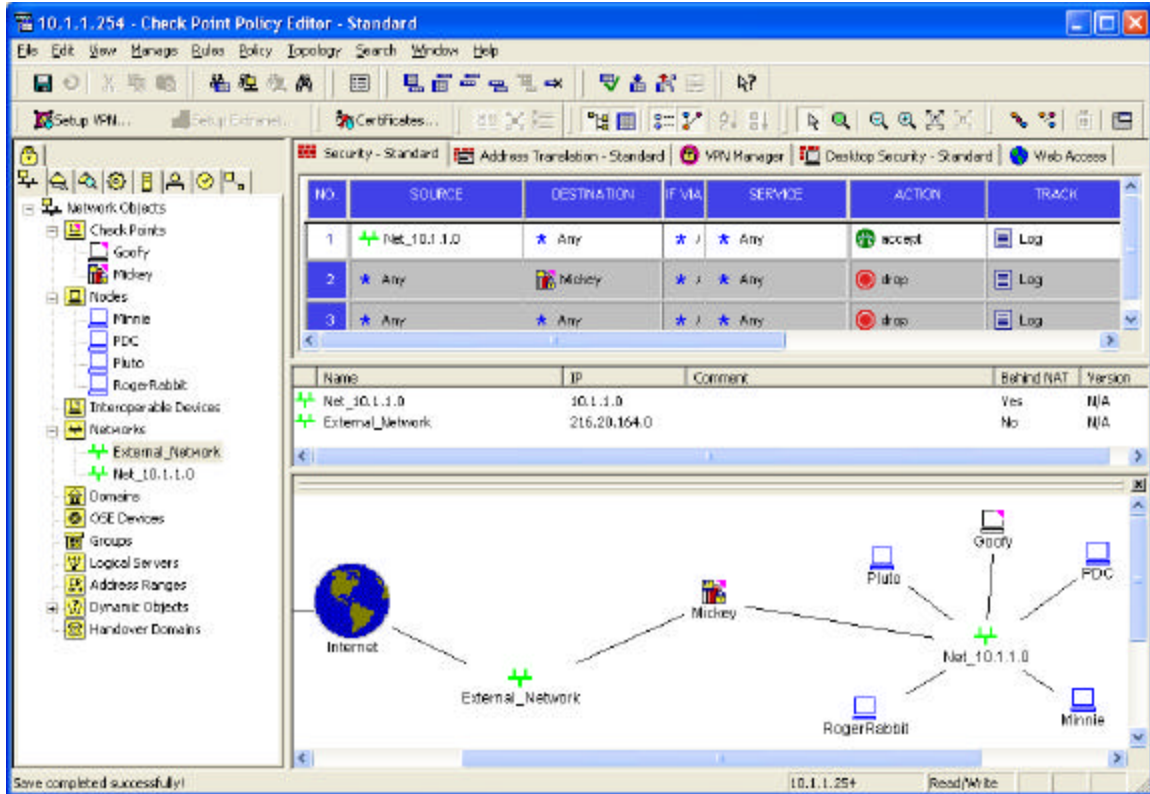


Fig 1.8 GUI Client

Notes:

Licensing:

You need a license for the Manger, the Module, and a CLM license. All licenses are bound to the Management server in NG and pushed out using Secure Update.