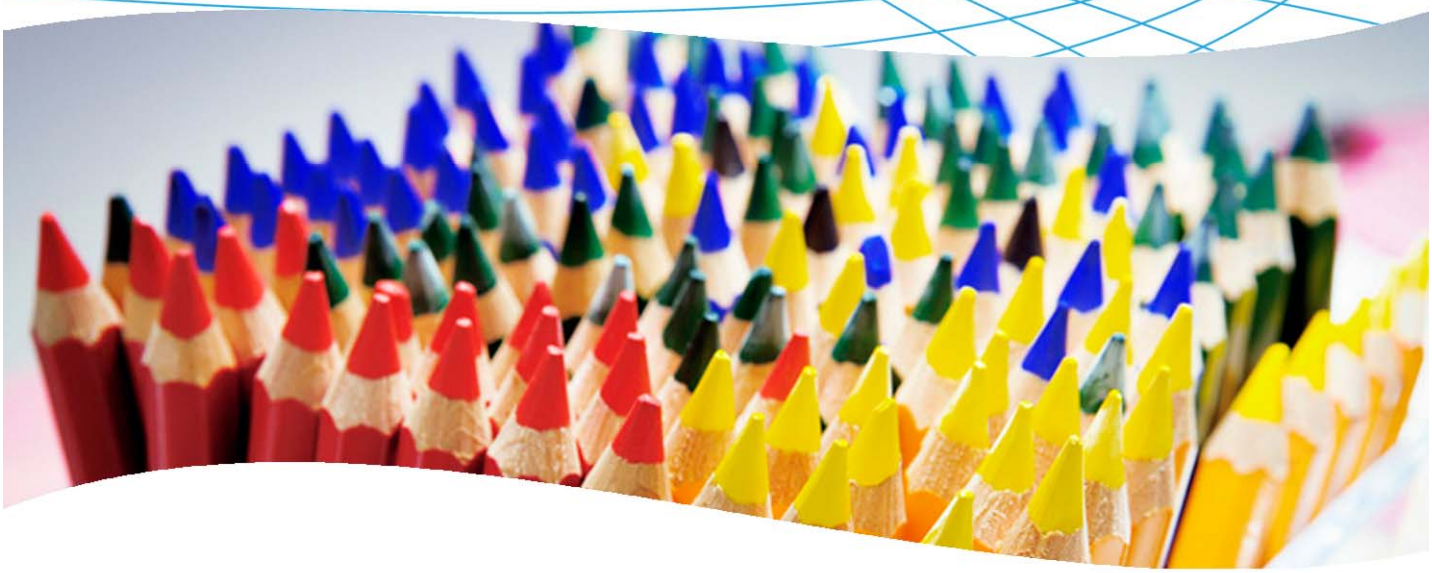
An HP ProCurve Networking Application Note

Automatic security policy enforcement with ProCurve Network Immunity Manager



Contents

1. Introduction

Along with ProCurve Manager (PCM) and Identity Driven Manager (IDM), ProCurve Network Immunity Manager (NIM) is a powerful tool that lets you enforce policy by configuring automatic actions to be performed upon detection of certain events. This application note explains how to set up some of these actions and check the results.

2. Prerequisites

This application note assumes you have a Windows Server 2003 installed, along with PCM, IDM and NIM. Examples are based on a configuration using a ProCurve Switch 5400zl and a ProCurve Switch 3500yl.

3. Network diagram

Figure 1 shows the network referenced in this application note.

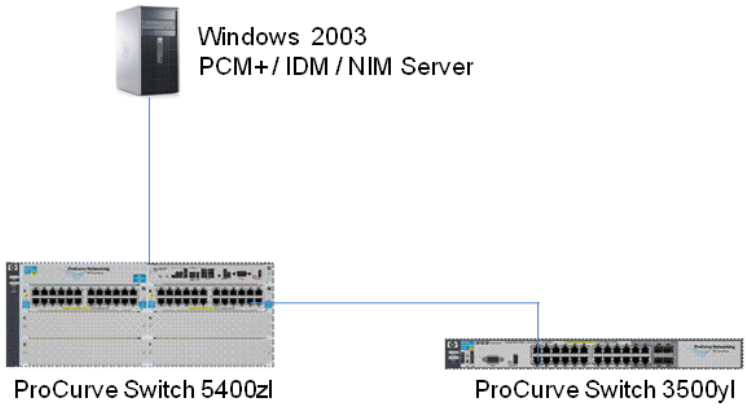


Figure 1. Network diagram used for these examples

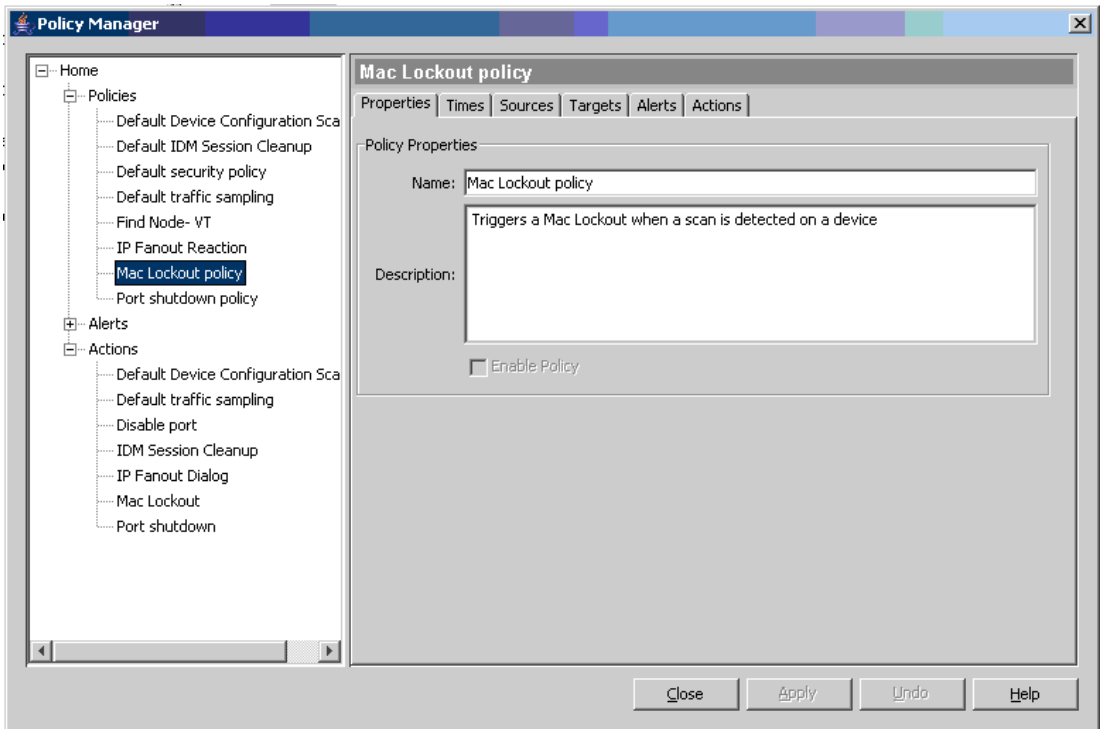
4. Instructions for automatically managing policy

This section explains the step-by-step instructions for managing policy with Network Immunity Manager. You create a couple of policies, then manage them with NIM.

4.1 Create a policy: MAC lockout

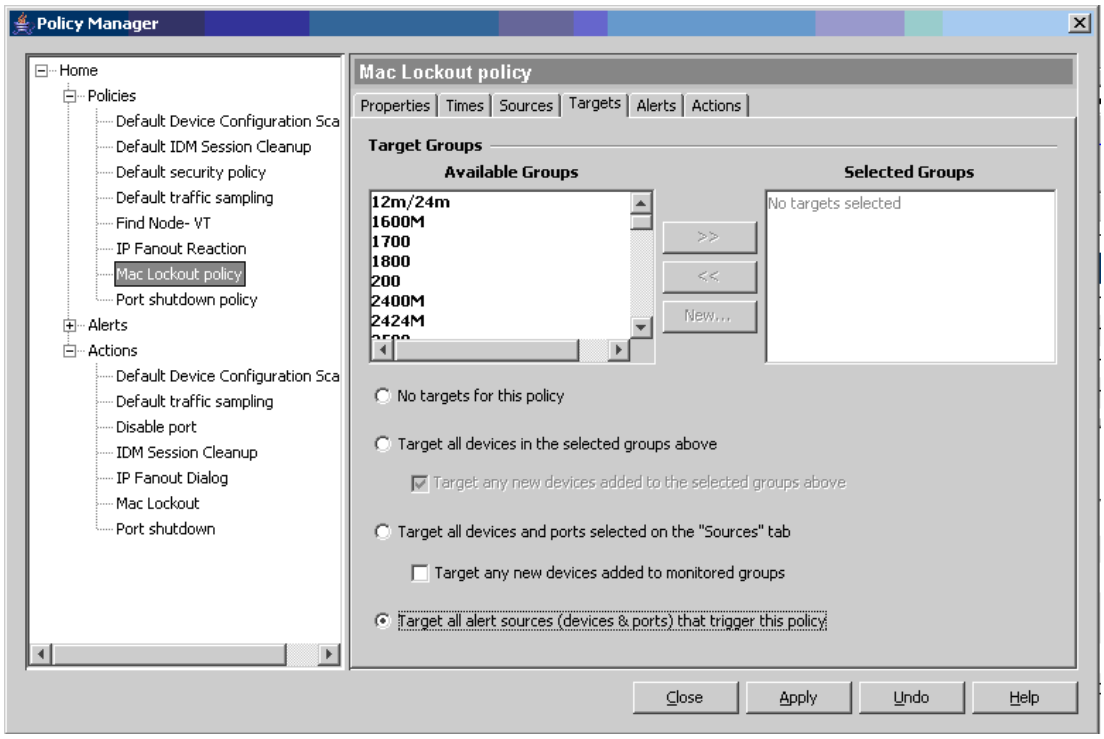
First, create a policy for locking out MAC addresses. To create the policy:

1. In PCM, go to the Policy Manager (use the  icon) to launch the Policy Configuration Manager window.
2. Select the Policies node in the navigation tree to display the Manage Policies panel, then click New to launch the Create Policy dialog. Create a new policy called Mac Lockout policy. (Or simply read through the different steps of policy creation if this policy already exists.) In the Properties tab enter the Name and Description; for example:



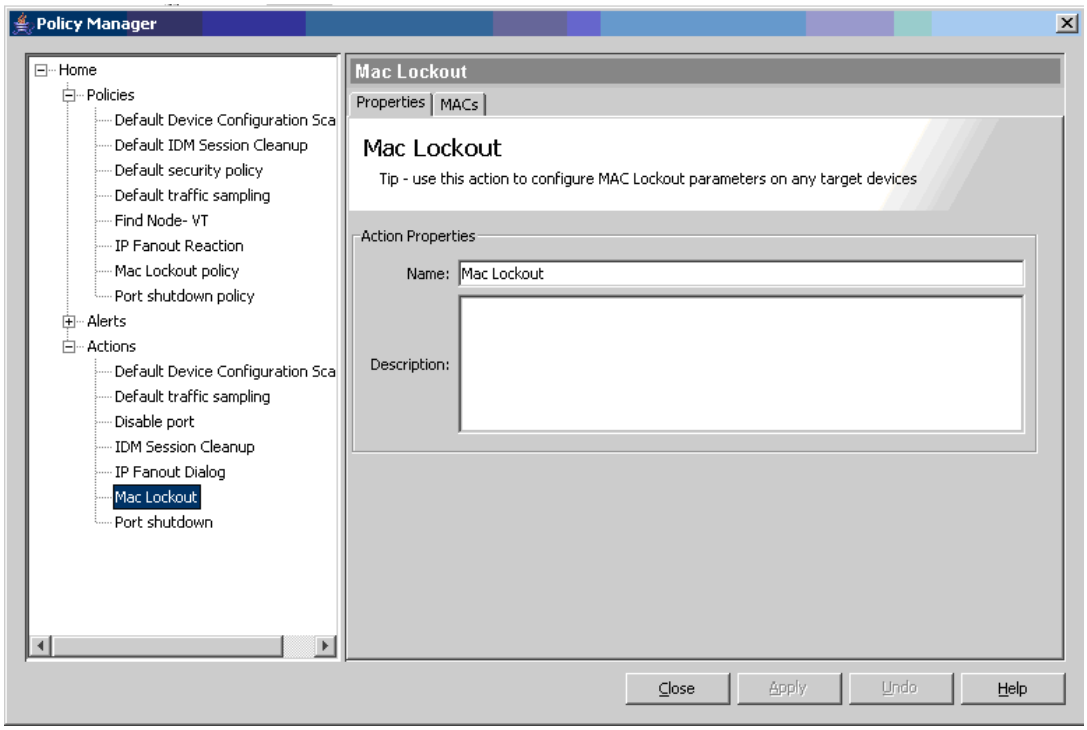
3. Leave the Times tab as it is.
4. In the Sources tab, leave the Selected Groups column set to No Groups selected. (In this case, the policy will accept events from any source.)

5. In the Targets tab, enable the radio button for Target all alert sources (devices & ports) that trigger this policy:



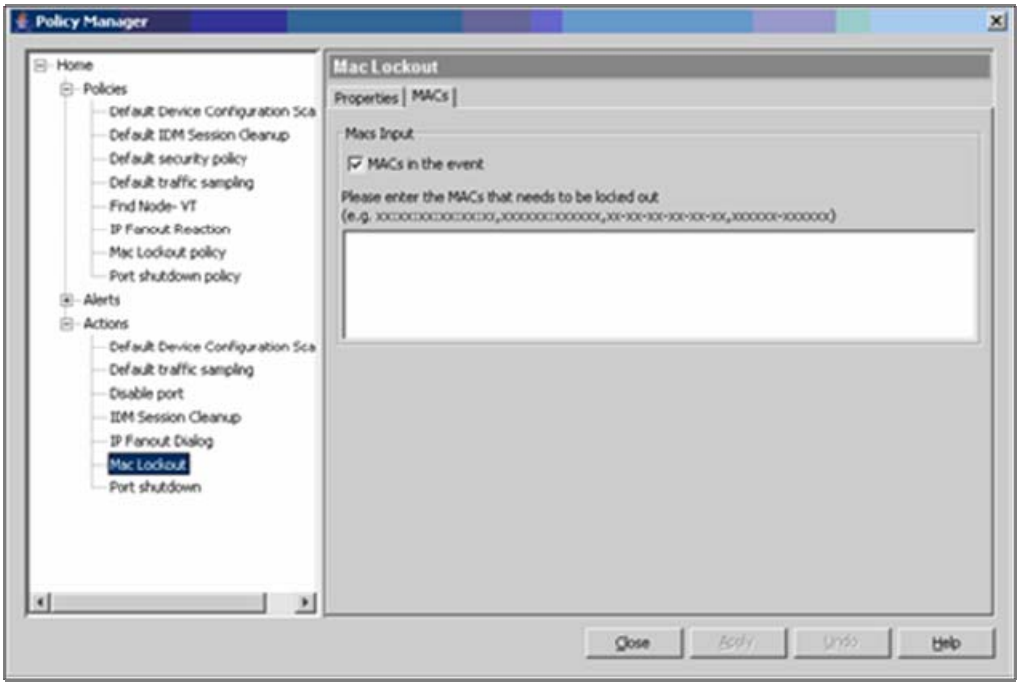
6. In the Alerts tab, select Default IP-Fanout, Default TCP/UDP-Fanout, and Default protocol anomaly, then click the right arrow (>>) to move them to the Selected Groups column on the right.

7. In the Actions tab, create a new action called Mac Lockout, and in the Actions list choose Mac Lockout:

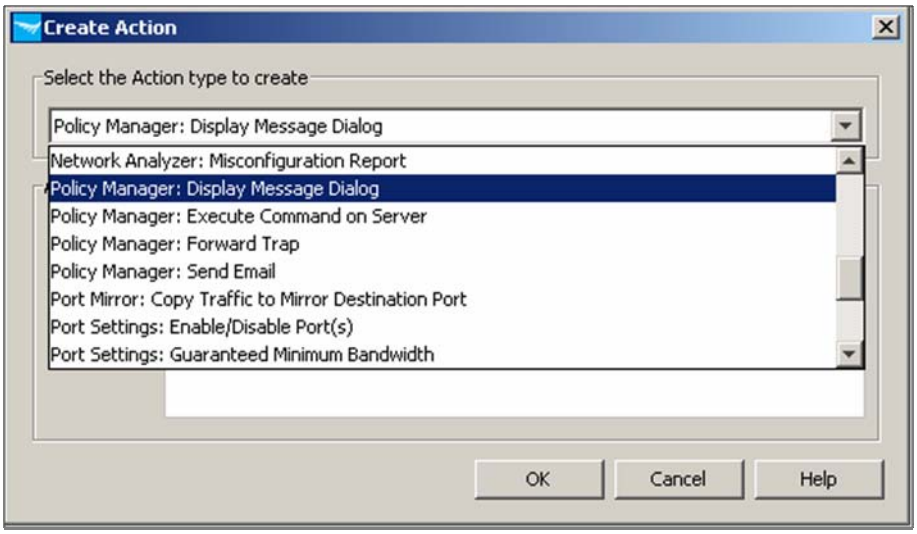


This configures actions the policy will take when it is executed.

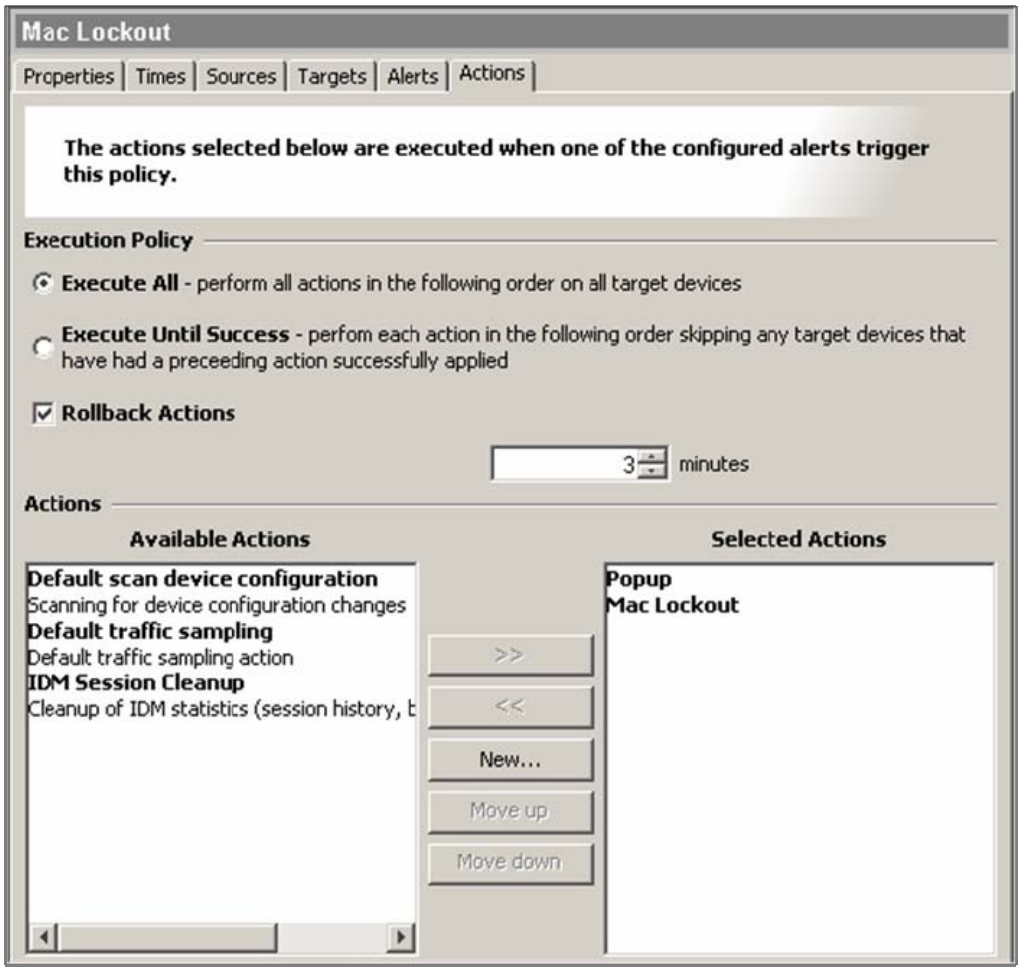
8. On the MACs tab, choose MACs in the event. This will enable NIM to block MAC addresses detected as offenders in the scans:



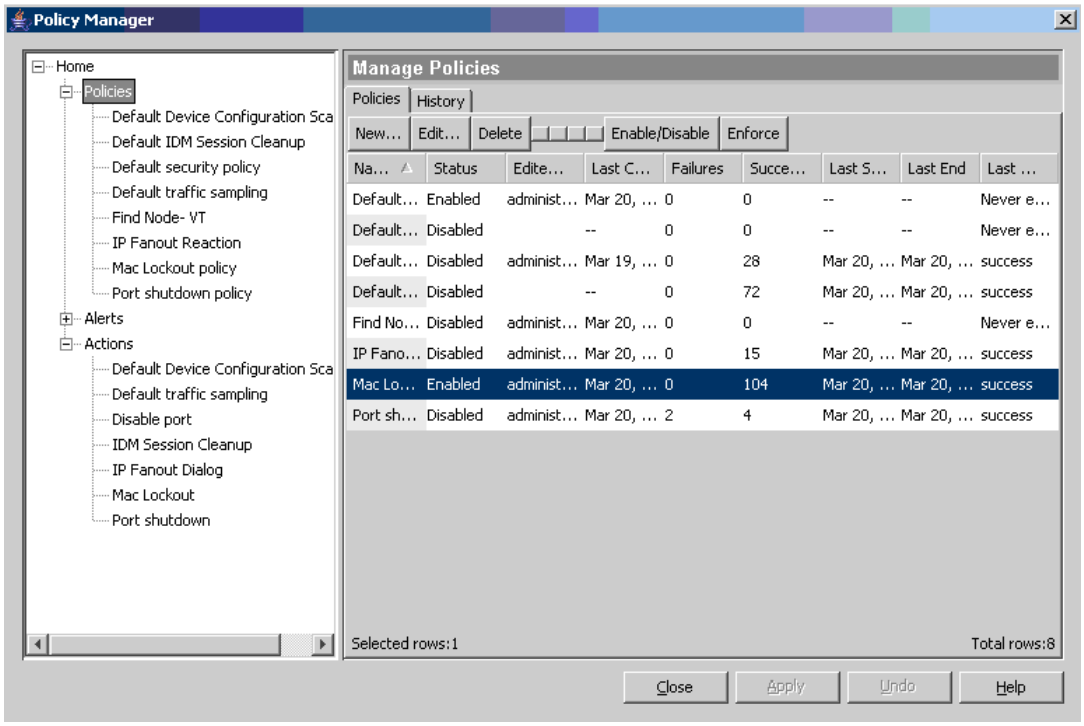
9. Also create an action called Popup, and use the Create Action window to indicate that it will display a message dialog:



10. On the Actions tab, choose Popup and Mac Lockout in the list of Available Actions and move them into the Selected Actions column. Click the Execute All radio button. Also, put a check in the box next to Rollback Actions, and set the time to 3 minutes. This will enable the policy to automatically unlock the blocked MAC address after 3 minutes:



11. Finally, in the Manage Policies window, disable all default policies and enable the Mac Lockout policy:

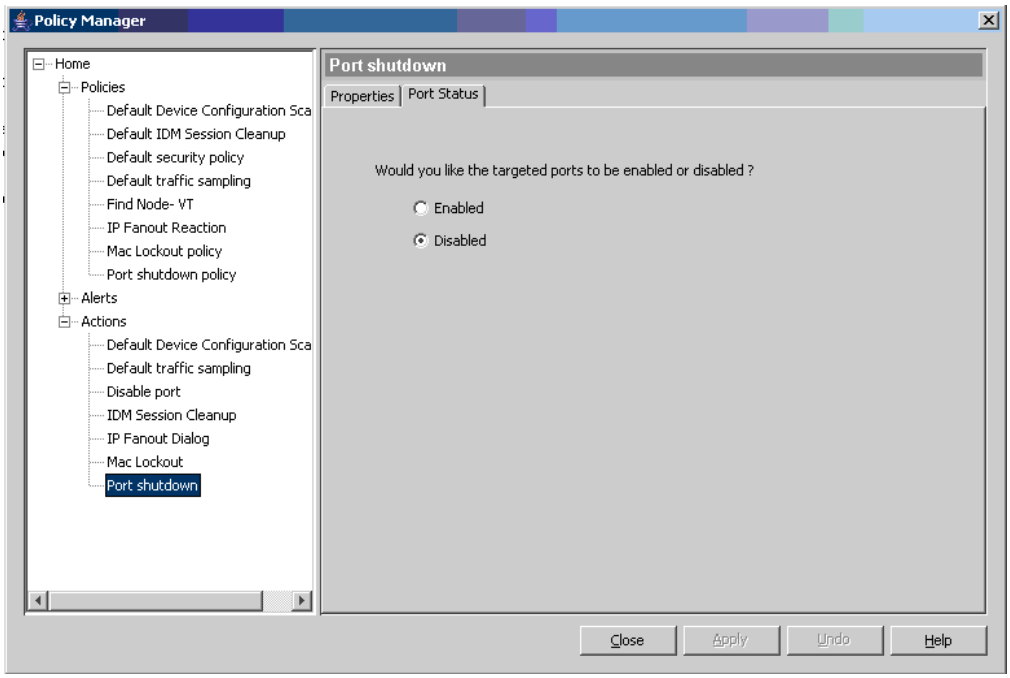


With this procedure you have configured a Mac Lockout policy. The policy will lock out the Mac address of the offender each time a TCP/UDP or IP fanout event is detected by NBAD (network behavior anomaly detection) in Network Immunity Manager.

4.2 Create another policy: port shutdown

Now create another policy.

1. Create the policy Port shutdown, using the same procedure as for Mac Lockout. Specify the following parameters:
    - **Targets**: Select Target all alert sources (devices & ports) that trigger this policy.
    - **Alerts**: Select Default TCP/UDP-Fanout, Default IP-Fanout, and Default protocol anomaly.
    - **Actions**: Create a new action, Port shutdown.
2. From the list of pre-configured actions, select Port shutdown; and in the Port Status tab of this action choose Disabled.



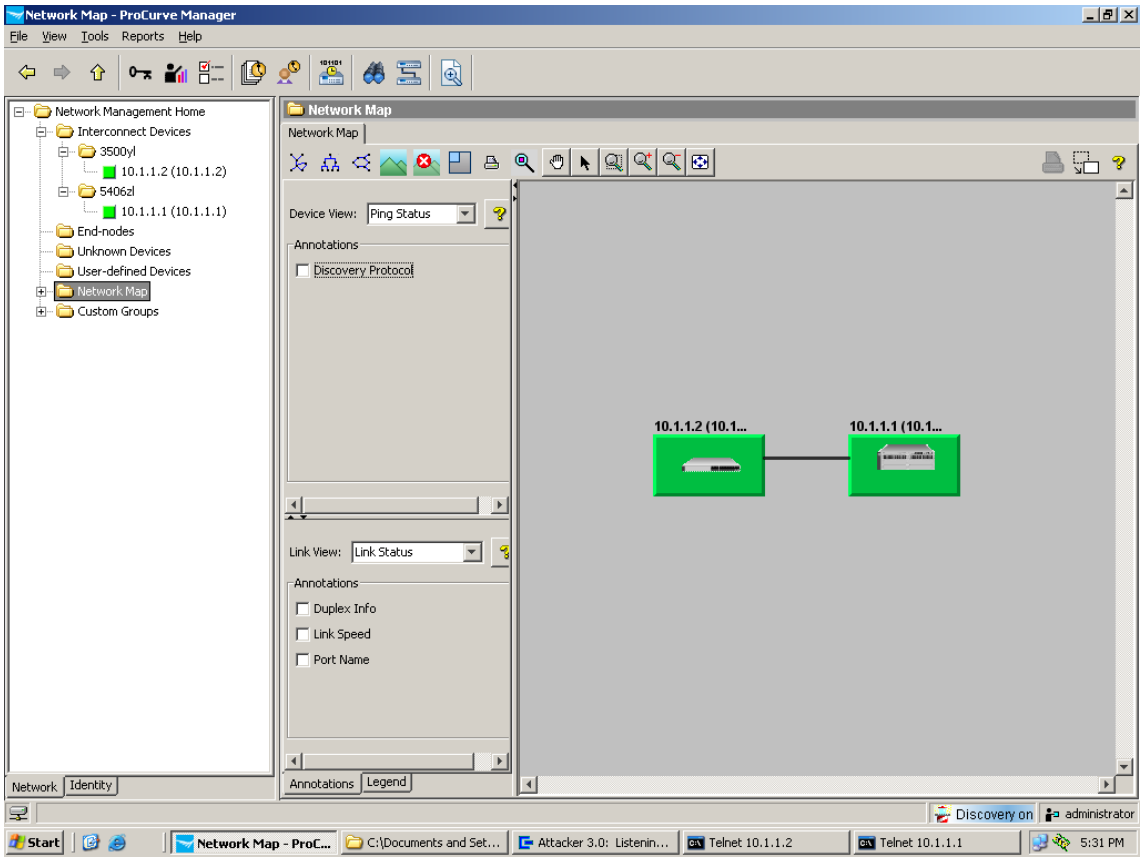
3. Enable this policy and disable the Mac Lockout policy.

4.3 View a security heatmap

The Network Maps window in PCM also provides an overview of the security state of the managed network based on data from NI Manager. It can display the security totals by category and severity.

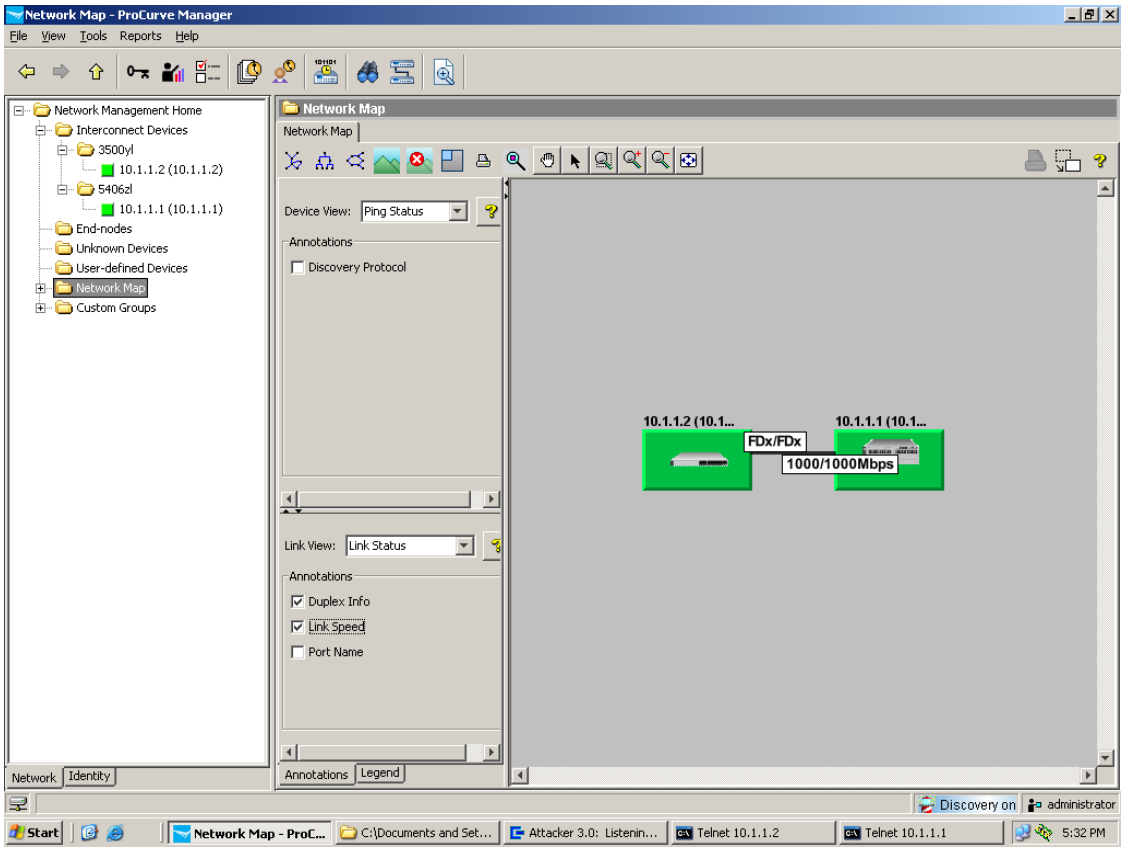
To view a security heatmap:

1. In PCM, click on the Network Map node in the navigation tree to display the network map.
2. In the Device View pulldown menu choose Ping Status (the default) to see the devices that are operational:

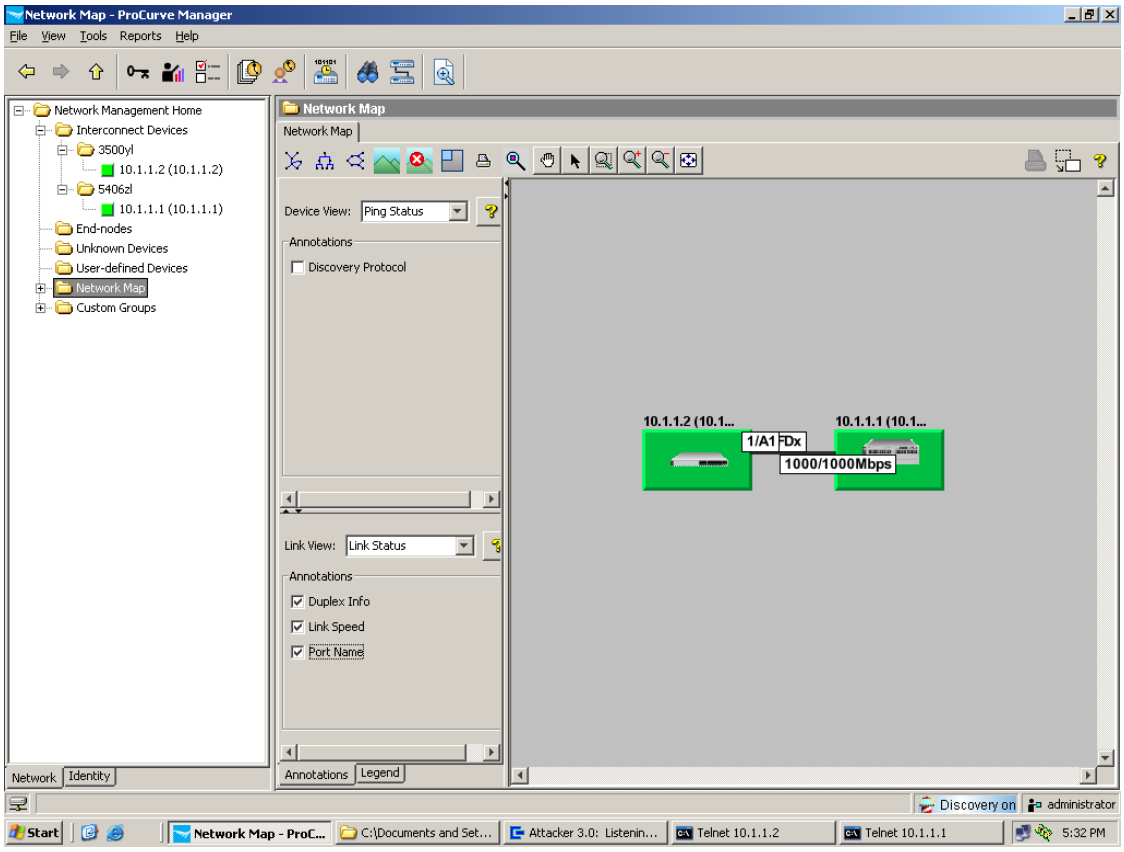


3. In the Link View area, enable Duplex Info. You see that the link between the devices is in FDX on both sides.

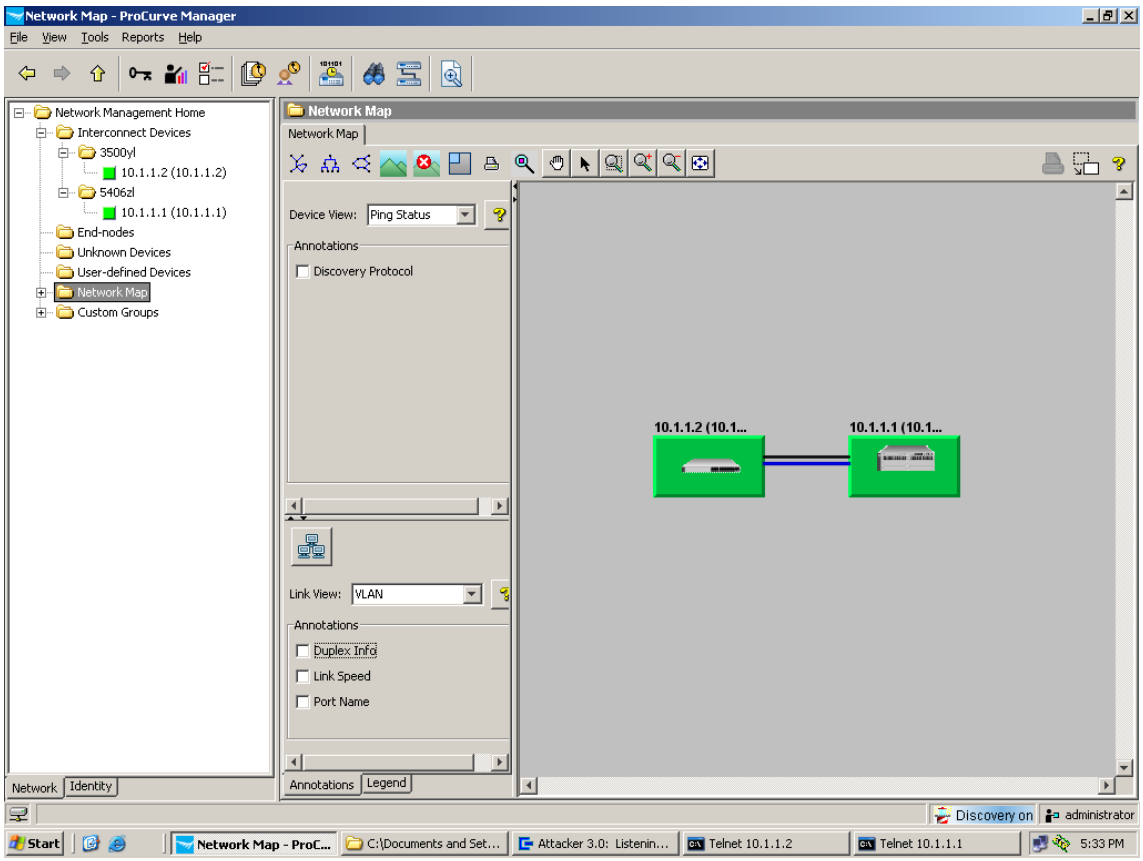
4. Also, enable Link Speed to show the speed of the link between the 5400 switch and the 3500 switch:



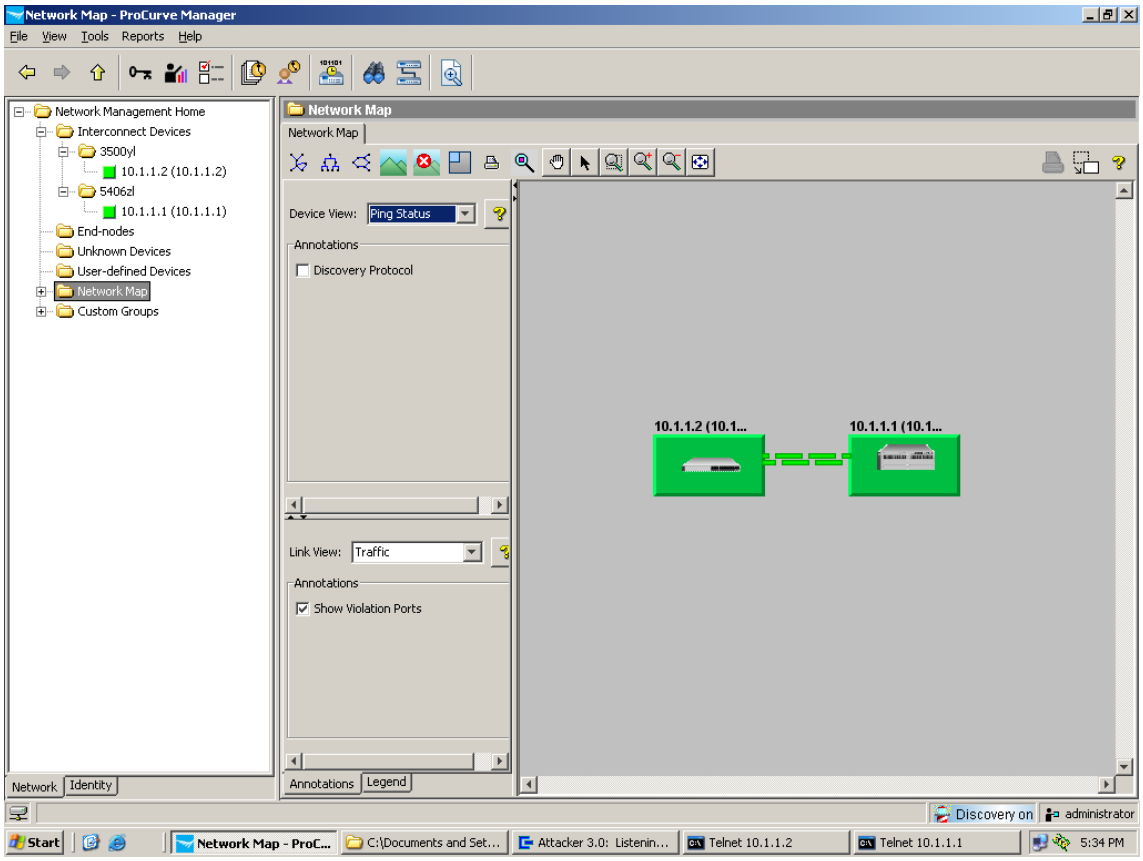
5. Finally, enable Port Name to show which ports are interconnected:



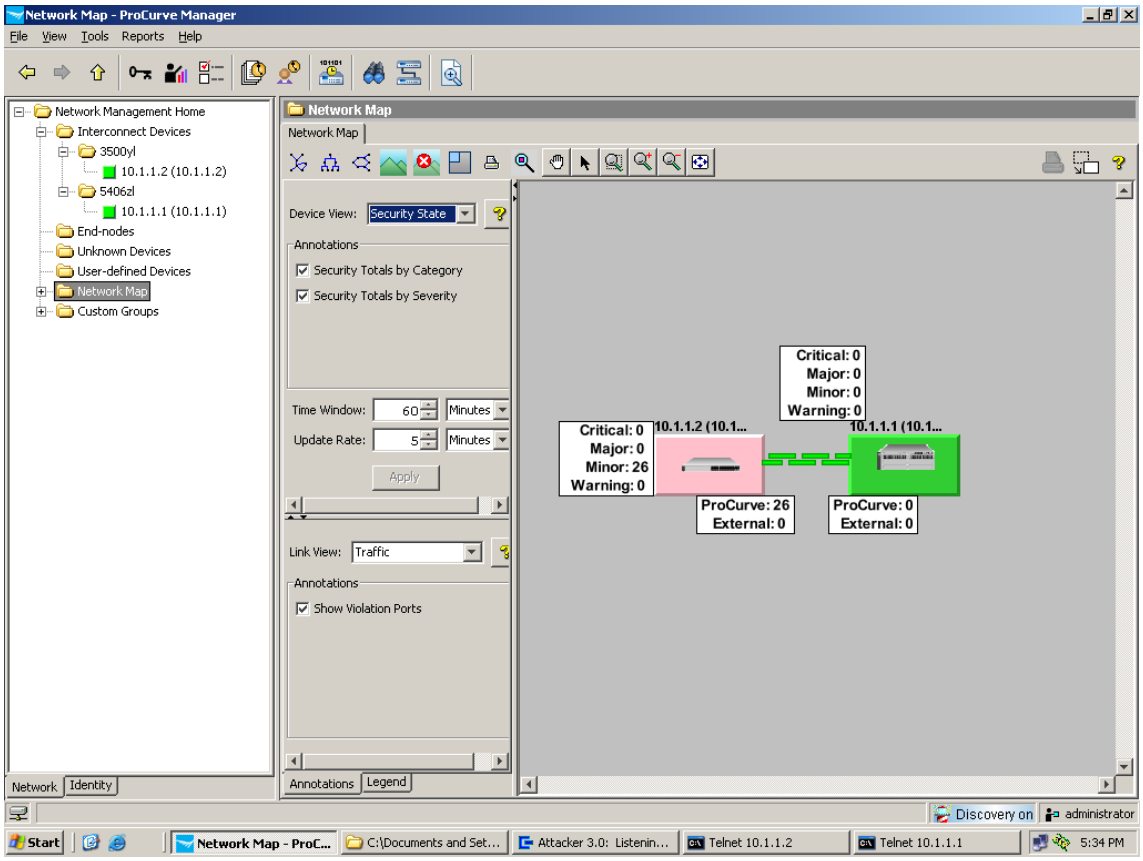
6. Now change the Link View from Link Status to VLAN. The network map displays the different VLANs that are tagged on the link between the two switches:



7. Change the Link View to Traffic. You can see the traffic between the two devices appears in green, which means the link is not busy:



8. Now change the Device View to Security State. You see the ProCurve Switch 3500 now appears pink, indicating that security events were detected on it.



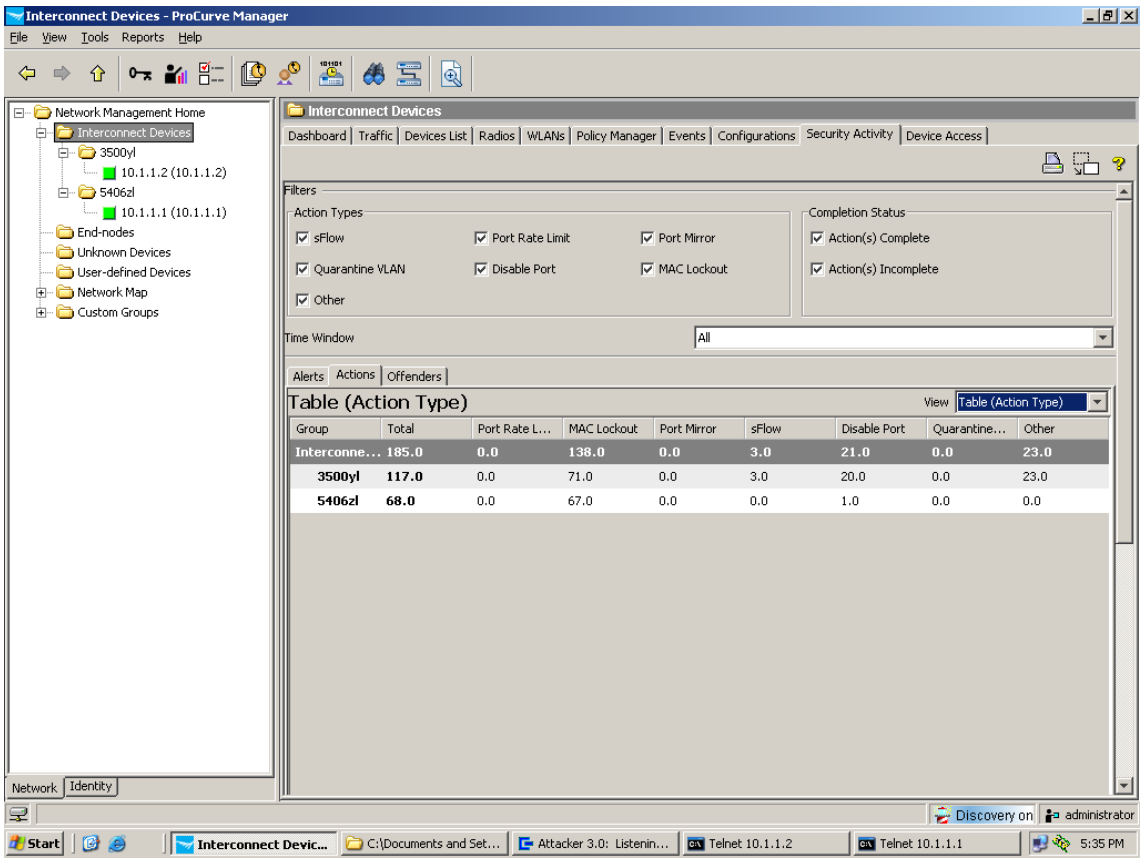
You can display the number of events per switch by category (Security Totals by Category). The two categories are ProCurve, for the events detected by the switches or NIM; and External for events coming from a third-party IDS/IPS or UTM. You can also display events according to severity (Security Totals by Severity).

9. Click on one of the switches in the Network Map. You get to the Interconnect Devices level, where you can see the Security Activity tab with a list of actions executed by the Policy Manager on each switch.

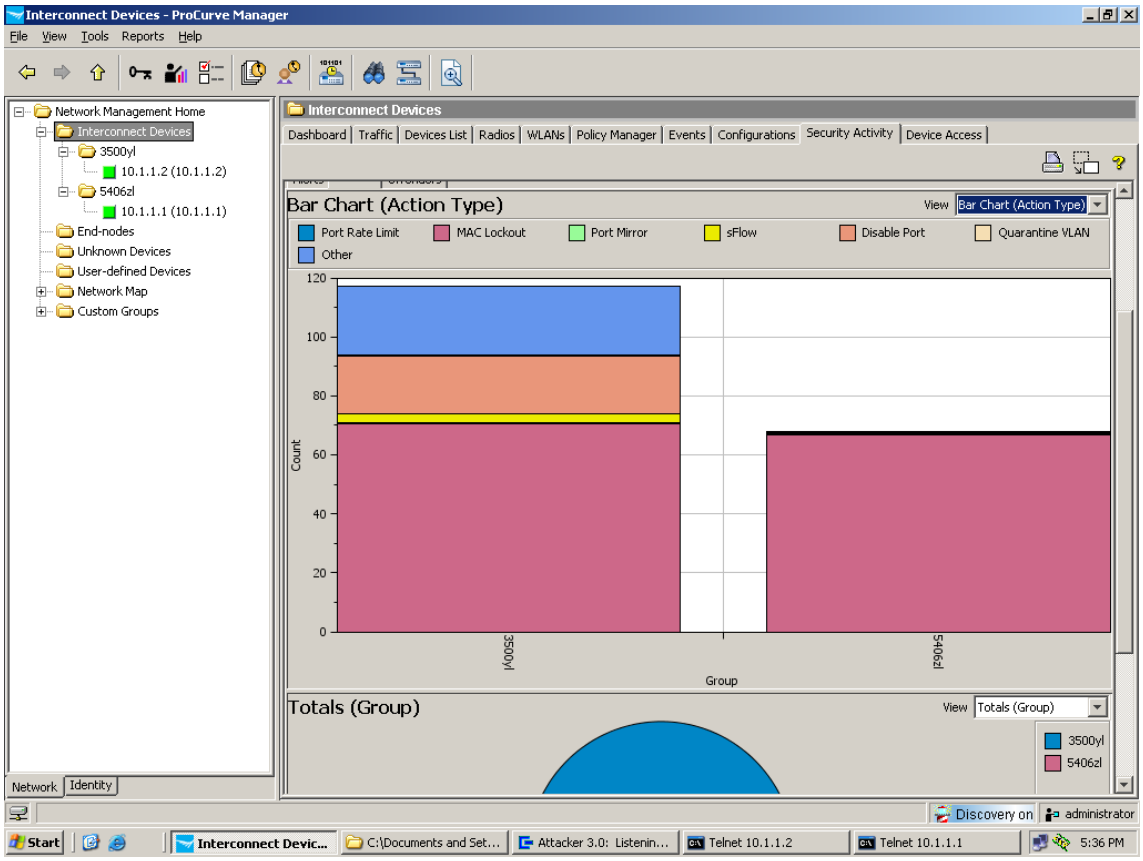
   At this level, you have the choice of three tabs, depending on how you want to see security events organized:

   - **Alerts**: ProCurve or External
   - **Actions**: By type of action performed by the policy manager in response to the attacks
   - **Offenders**: By IP address of the attacker

   Choose the Actions tab to see the actions (e.g., Mac Lockout, Disable Port) performed in response to attacks:



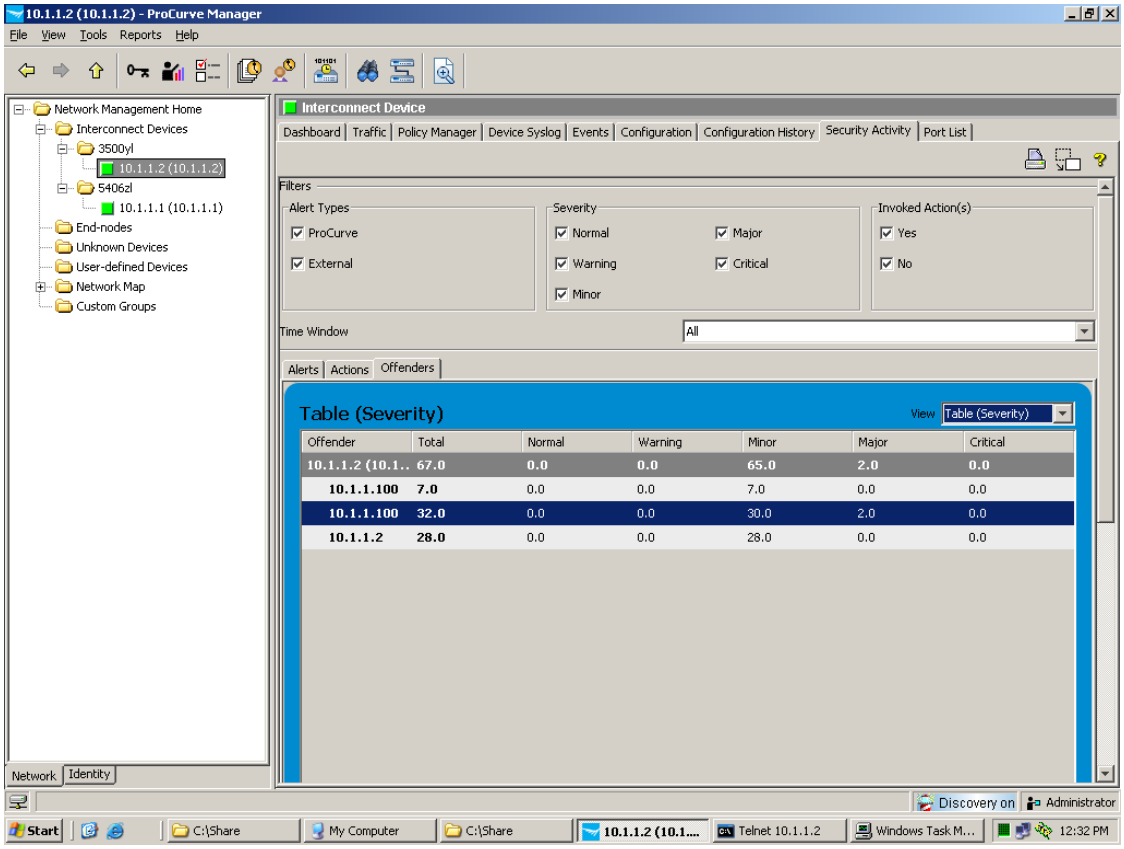
10. To see this Security Activity as a bar chart, change the View to Bar Chart (Action Type). You see a chart with a different color for each type of action:



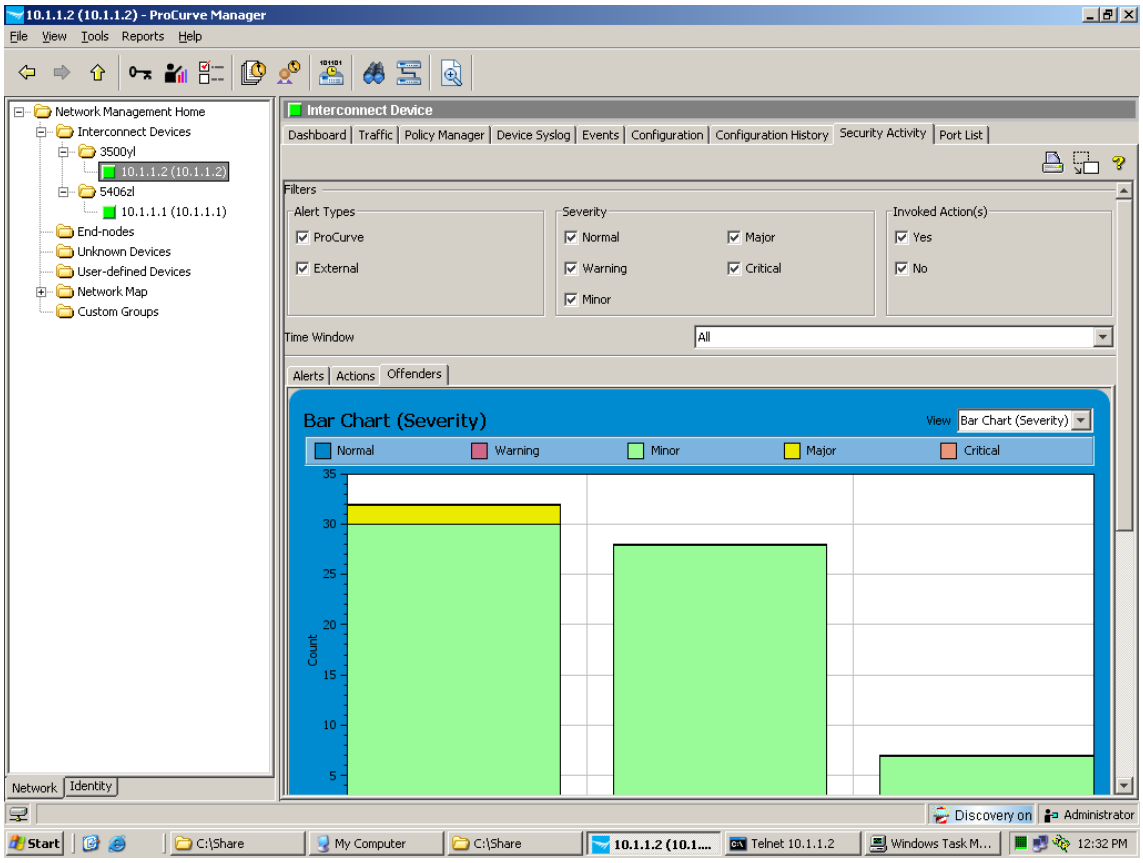
4.4 Track offenders

Another feature of Network Immunity Manager is offender tracking. To see offender tracking:

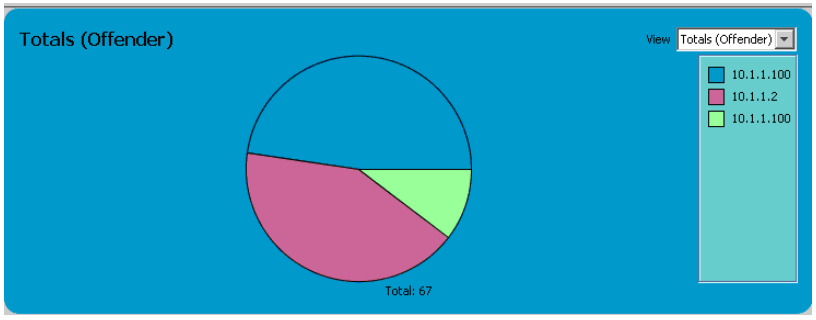
1. Go to the switch or Interconnect Devices level, and select the Security Activity tab.
2. Click on the Offenders tab, and ensure all Filters are enabled. By default, you see a table with the list of Offenders, and for each one, the number of events received in each severity category (Normal, Warning, Minor, Major, Critical):



3. To see the offenders and their statistics as a bar chart, change the View to Bar Chart (Severity):



4. To see the proportion of attacks per offender (listed by IP address), change the View to Totals (Offender):



5. Double-click on an offender's section of the chart and you can obtain a history of security events and policies associated with this offender's IP address.
6. Click on one of the lines of the Policy History to obtain the details of the event and policy.

   In the Properties section you can view the following information:

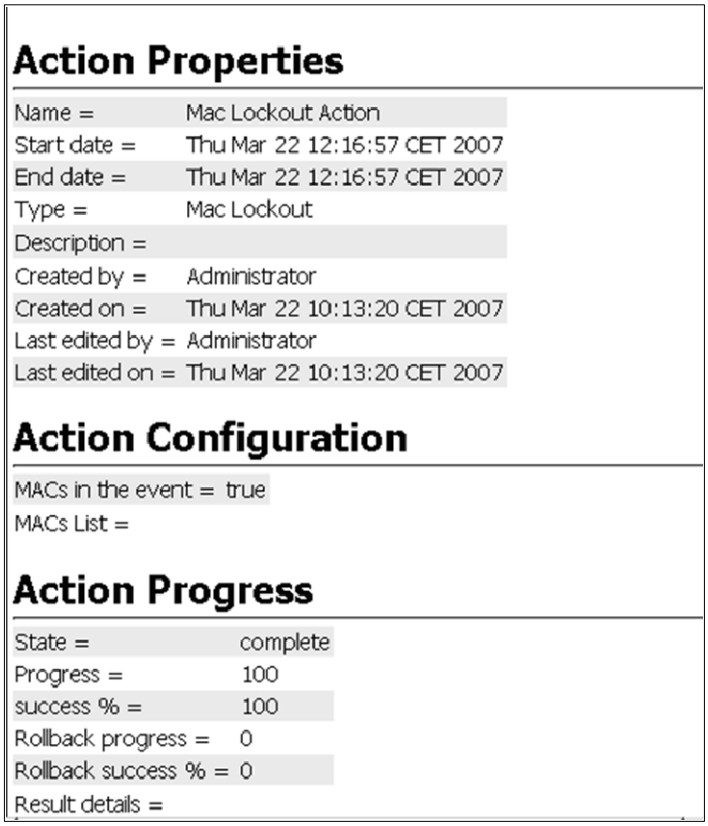
   - Name, type, description of the alert
   - Offender's IP, MAC address, connected device, and port
   - Result of the alert: enforcement of a policy

   The Configuration section shows the threshold (number of events over a given period) that were necessary to generate the security alert.

Then, if an action was applied by this policy, you can see an Action Properties section, including:

- Name and type of the action
- Start and end date of creation, last edition, and who created it
- Start and end date of enforcement

You also can view the Action Configuration and Action Progress, showing the level of success of enforcement:



Action Properties

Name =	Mac Lockout Action
Start date =	Thu Mar 22 12:16:57 CET 2007
End date =	Thu Mar 22 12:16:57 CET 2007
Type =	Mac Lockout
Description =	
Created by =	Administrator
Created on =	Thu Mar 22 10:13:20 CET 2007
Last edited by =	Administrator
Last edited on =	Thu Mar 22 10:13:20 CET 2007

Action Configuration

MACs in the event =	true
MACs List =	

Action Progress

State =	complete
Progress =	100
success % =	100
Rollback progress =	0
Rollback success % =	0
Result details =	

5. Reference documents

This concludes the example procedures for using ProCurve Manager, Identity-Driven Manager, and Network Immunity Manager to automatically enforce policy on ProCurve switches.

For further information about how to configure ProCurve switches to support security, please refer to the following links:

- For user manuals for ProCurve 3500yl-5400zl-8212zl switches:
  http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm

- For PCM, IDM, and NIM manuals:
  http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm
  http://www.hp.com/rnd/support/manuals/IDM.htm
  http://www.hp.com/rnd/support/manuals/NIM.htm

For further information, please visit www.procurve.eu

4AA2-1971EEE, July 2008