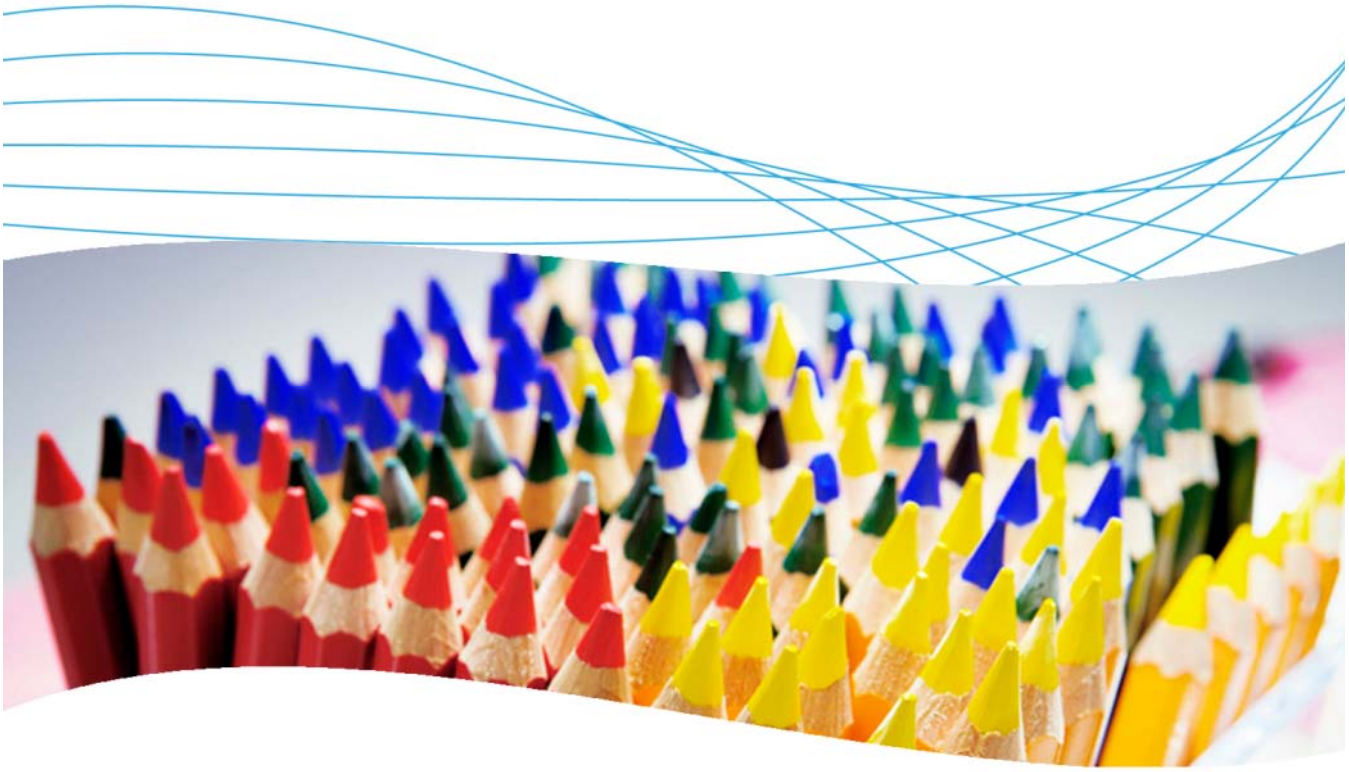
An HP ProCurve Networking Application Note

How to configure NBAD on ProCurve switches



Contents

1. Introduction

This application note explains how to configure NBAD on a ProCurve switch.

Network behavior anomaly detection (NBAD) is the continuous monitoring of a network for unusual events or trends. NBAD is an integral part of network behavior analysis (NBA), which offers security in addition to that provided by traditional anti-threat applications such as firewalls, antivirus software and spyware-detection software.

2. Prerequisites

To perform the tasks in this application note, you will need to have Windows Server 2003 installed, along with ProCurve Manager Plus (PCM+) 2.2, Identity Driven Manager (IDM), and Network Immunity Manager (NIM). NIM interacts with the IDM server and client to get information on the user connected to ports where an attack is detected. The example here uses an HP ProCurve 5400zl switch.

3. Network diagram

Figure 1 details the hardware configuration referenced in this application note.

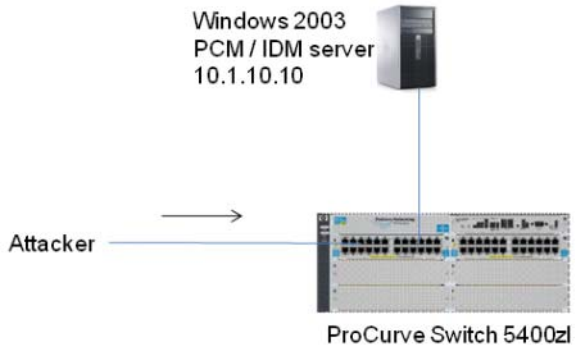


Figure 1. Setup for configuring NBAD on a ProCurve switch

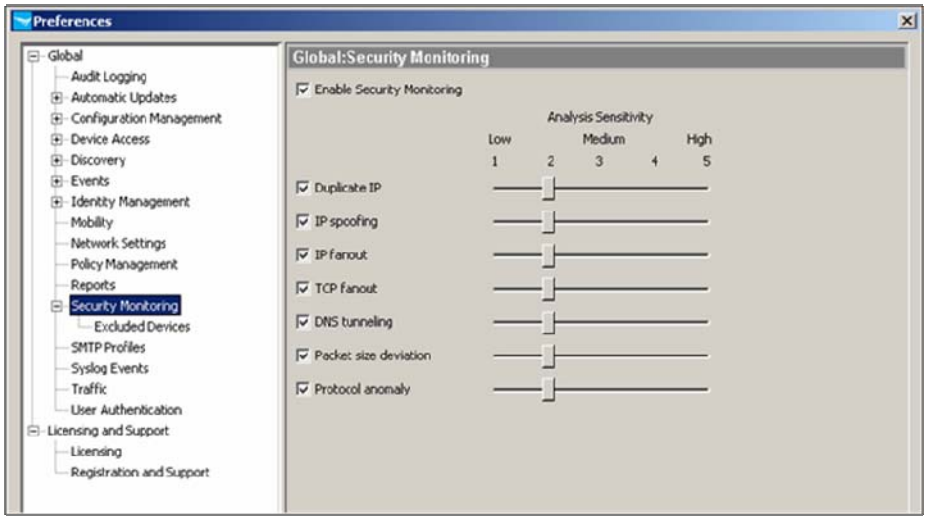
4. Configuring NBAD

The Preferences feature in PCM provides the tools to control and adjust the NBAD detection sensitivity and manage the NBAD options to fit your particular environment.

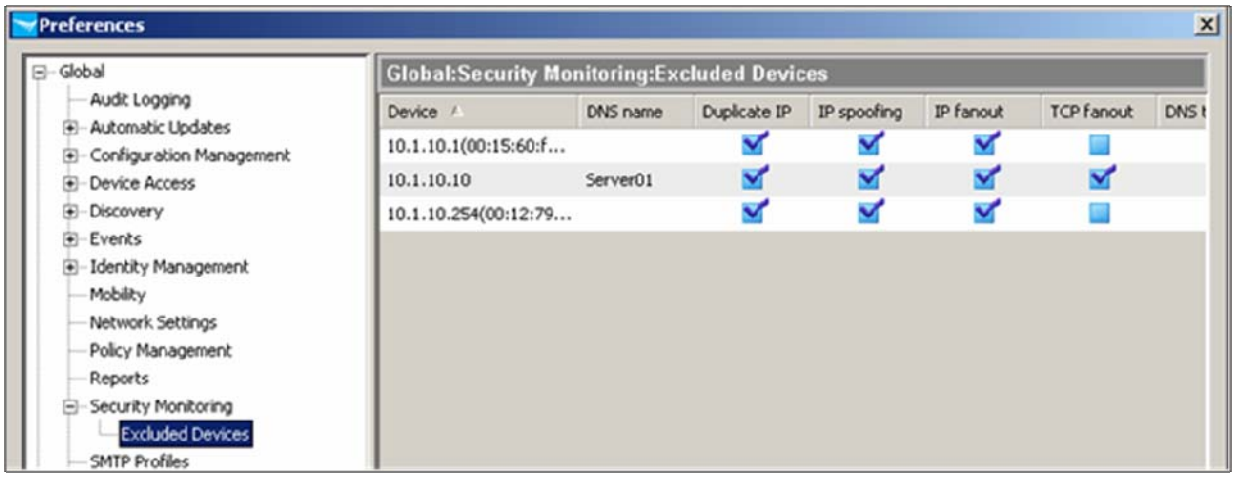
4.1 Configure the security monitoring preferences

To configure Security Monitoring Preferences for Network Immunity Manager:

1. In NIM, go the Preferences menu and select the Security Monitoring option. You see the Security preferences configuration window. In this window, ensure that Analysis Sensitivity has been adjusted to level 2 for all types of alerts:

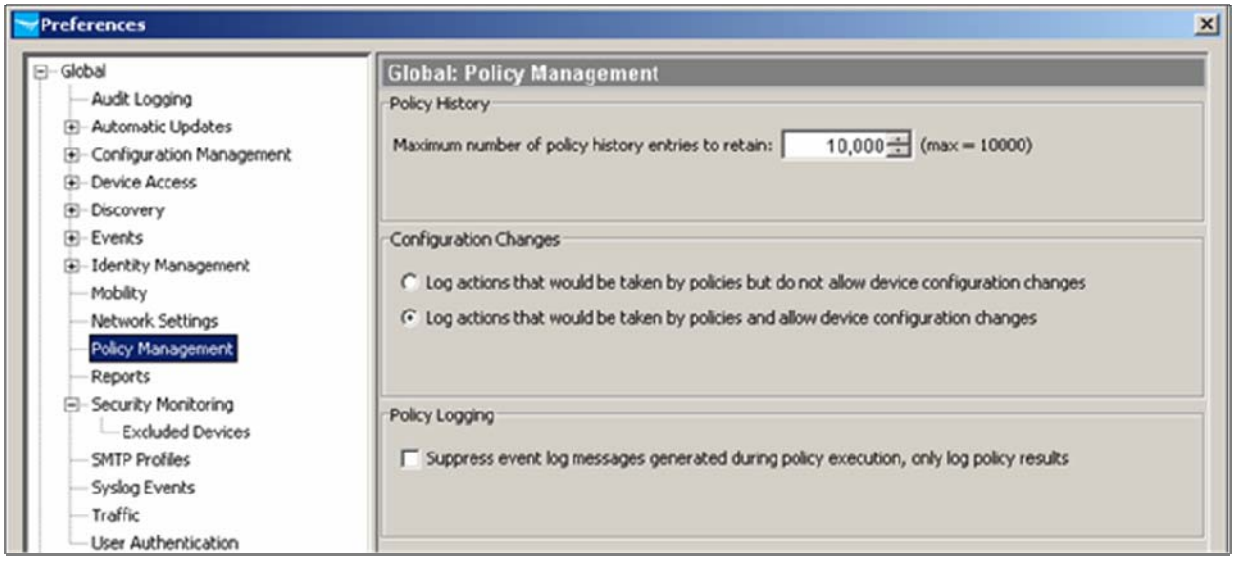


2. Under Security Monitoring, select Excluded Devices. You see a list of excluded devices. The PCM/IDM server (here, 10.1.10.10) has automatically been excluded from all alerts. Routers have been excluded from Duplicate IP, IP spoofing, and IP fanout alerts.



3. Go to the Global: Policy Management window. By default, the Configuration Changes setting is Log actions that would be taken by policies but *do not allow* device configuration changes. This allows you to test policies, while not enforcing any actions, before applying the policies in a real production mode.

   Here you want to show actions, so choose the option to Log actions that would be taken by policies and *allow* device configuration changes:



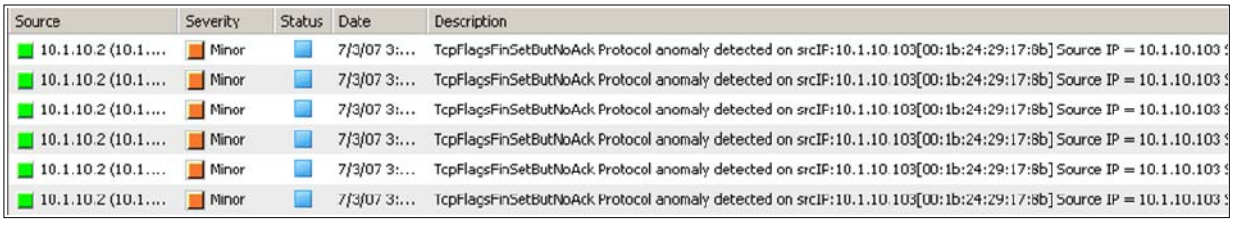
4.2 Simulate an attack

To simulate and monitor an attack:

1. Connect the attacker to port 5 on the HP ProCurve 5400zl.

2. Use Nmap to launch an Xmas scan to the entire subnet:
   - Target: **10.1.10.0/24**
   - Options: **-p 0-65535 -sX**

   After a few seconds, you see the scan appear under Network Management Home in the Events window of PCM+, with source NBAD. You see the source IP address (10.1.10.x), the source MAC address, and the event description (TCPFlagsFinSetButNoAck Protocol anomaly…).



5. Reference documents

This concludes the procedure for configuring network behavior anomaly detection (NBAD) on ProCurve switches.

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

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

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

- For ProCurve Switch 2610 series manuals:
  http://www.hp.com/rnd/support/manuals/2610.htm

For further information, please visit www.procurve.eu

4AA2-1724EEE, July 2008