Policy Hit Accounting Tool Guide

A guide to using the Policy Hit Accounting Tool to display a graphical representation of policy hits on the network

Introduction

Enterasys policy-enabled infrastructure devices, such as the Matrix N-series, provide the unique traffic management capabilities using port level multilayer classification. This allows the network administrator to granularly control the allocation of network resources to connecting devices directly at the point of entry to the network. NetSight Policy Manager, a management application in the NetSight suite, provides a centralized command and control for the definition of role-based network resource provisioning with single click policy enforcement.

With the deployment of policy on the network, the knowledge of which policies that are being hit by user traffic on which devices is invaluable to the network administrator for understanding how end systems are using the network and how policy is affecting the network's operation. The Policy Hit Accounting Tool allows a network administrator to graphically represent policy utilization on the network, specifically for Matrix N-series Platinum devices. Using this tool, a network administrator can capture policy hit information about a single device at a moment in time, or record network usage trending information by capturing policy hit statistics on several devices at continuously intervals over an extended period of time. The Policy Hit Accounting Tool makes it possible to see Secure Networks in action as policy discards malicious traffic before it enters the network and prioritizes mission critical traffic, yielding increased levels of network security and traffic optimitization.

Description

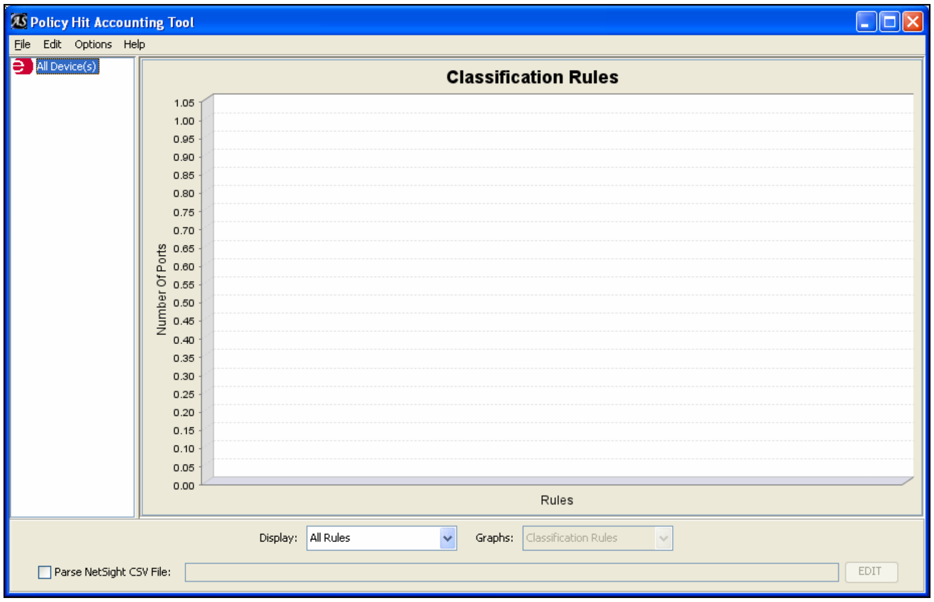
The Policy Hit Accounting Tool generates graphs of policy hits for a set of policy enabled devices. After NetSight Policy Manager is used to enforce a set of roles, services, and rules on a device, the tool can be used to generate a graph of these roles, services, and rules being hit by the traffic received on the switch. The Policy Hit Accounting Tool builds these graphs by using Simple Network Management Protocol (SNMP) to poll the *etsysPolicyRulePortTable* MIB on the switch (OID = 1.3.6.1.4.1.5624.1.2.6.11.7). Only the Matrix N-series Platinum platform currently supports this MIB out of all the Enterasys policy capable switches. As a result, this tool can only be used to graph policy hit information for Matrix N-series Platinum devices.

The graphs generated by the Policy Hit Accounting Tool display either the classification rule, the service, or the policy role on the x-axis and the number of ports on which the rule, service, or role was hit on the y-axis. (Note that the y-axis does ***not*** indicate the number of times the rule, service, or role was hit.) Therefore, the network administrator may leverage this tool to understand how users assigned to a specific role are utilizing the network. While policy configured on Enterasys switches protects the network from attacks by discarding malicious traffic before ingress, the Policy Hit Accounting Tool empowers the network administrator with the ability to identify network misuse, such as the use of peer-to-peer applications, or network abuse, such as worms and viruses. For example, the *Threat Management* service is defined in *demo.pmd* in NetSight Policy Manager as a container for classification rules that drop malicious traffic before it enters the network. While classification rules of the *Threat Management* service protect the network, the network administrator can use the Policy Hit Accounting Tool to monitor if the classification rules of the *Threat Management* service are being hit, identifying end systems that are attempting to abuse the network. Furthermore, as new threats emerge, simply updating the *Threat Management* service to account for new attack vectors and enforcing these changes with NetSight Policy Manager to the policy-enabled network will allow the further monitoring of new threats while ensuring the network is protected.

In summary, the Policy Hit Accounting Tool has a number of features and functions that improve visibility into the operation of the network from a security and traffic optimization perspective. The remainder of the document discusses how to configure these features and recommended implementation scenarios for this tool in illustrating the power of Secure Networks with policy.

Download and Installation Instructions

The Policy Hit Accounting Tool can be downloaded at the following link; http://www.enterasys.com/support/tools.html. After the download of the tool is complete, execute the *.exe* file to begin the installation (note that the *.exe* file is used to install this tool on a Windows platform). After following the steps of the installation wizard, the tool can be started, as shown in Figure 1, through *Start→Programs→Enterasys Networks→Policy Hit Accounting Tool* from the Microsoft taskbar.



Display: All Rules

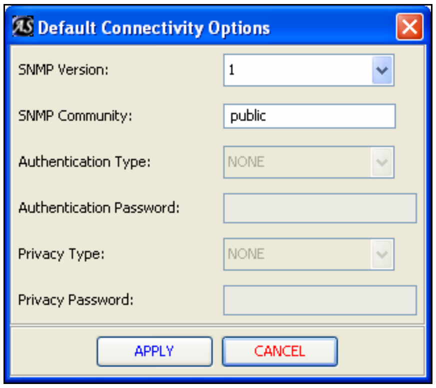
Graphs: Classification Rules

□ Parse NetSight CSV File:

Figure 1. Policy Hit Accounting Tool interface

Adding a Device

Before adding a device to the Policy Hit Accounting Tool, the *Edit* drop menu can be used to specify the default SNMP connectivity settings for switches to be added to the tool, as shown in Figure 2. If SNMPv1 is selected, only a community string needs to be specified, defaulting to *public* (Enterasys switches default to SNMPv1 with community string *public*), while SNMPv3 requires the configuration authentication and encryption credentials.

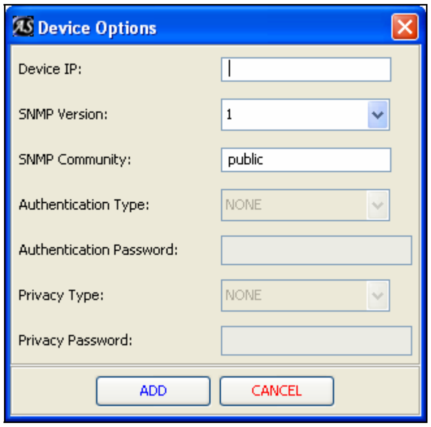


SNMP Version: 1
SNMP Community: public
Authentication Type: NONE
Authentication Password:
Privacy Type: NONE
Privacy Password:

Figure 2. Default SNMP connectivity setting

Devices that will be monitored for policy hit accounting can be added to the tool by right clicking on the *All Devices* icon in the left pane. Two methods exist for adding devices:

- Each device can be added one at a time by selecting the *Add Device* option after right clicking on the *All Devices* icon in the left pane. For each device, the IP address must be entered along with SNMP credentials, as shown in Figure 3, if different from the default SNMP connectivity settings previously configured.



Device IP:
SNMP Version: 1
SNMP Community: public
Authentication Type: NONE
Authentication Password:
Privacy Type: NONE
Privacy Password:

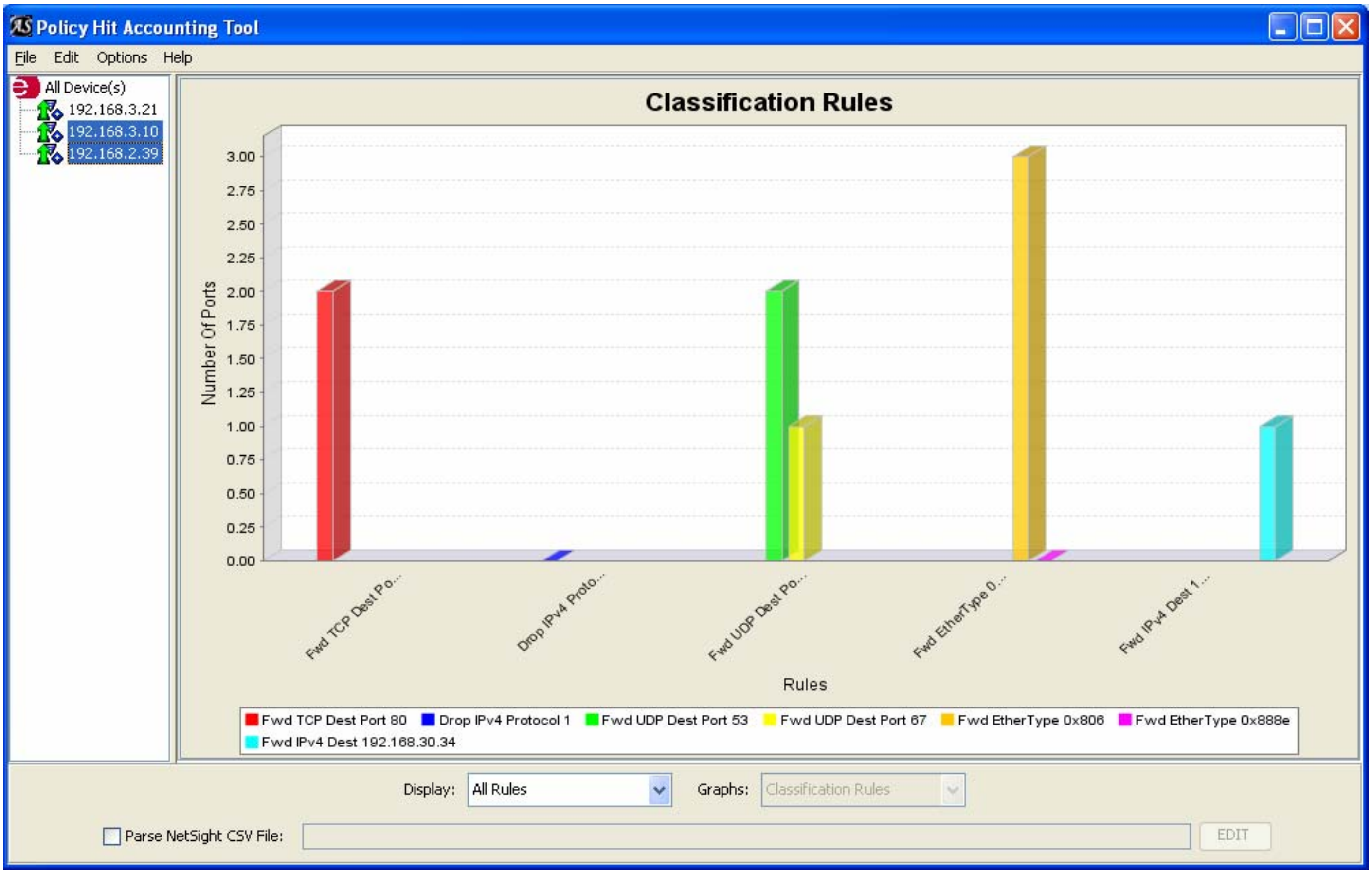
Figure 3. Adding a device

- A group of devices can be added to the tool at one time by selecting *Load NetSight .ngf file* after right clicking on the *All Devices* icon in the left pane. This will load the entire list of devices specified in the *.ngf* file using the SNMP credentials indicated in the *.ngf* file. To create an *.ngf* file of devices to import into the tool, choose the *Device List→Export* option from the *File* drop down menu in NetSight Console.

<u>Generating a Graph</u>

After the devices are added to the Policy Hit Accounting Tool, a graph of policy hits can be generated for all devices, a set of selected devices, or a single device.

- To generate a graph for all devices, right click on the *All Devices* icon in the left pane and select *Run All* to display the cumulative policy hit information across all devices.
- To generate a graph for only selected devices, hold down the *Ctrl* button and left click on the devices for selection in the left pane. Then, right click on these devices and select *Run* to display the cumulative policy hit information for the selected devices, as shown in Figure 4.
- To generate a graph for a single device, right click on the device and select *Run* to display the policy hit information for the selected device.



Display: All Rules

Graphs: Classification Rules

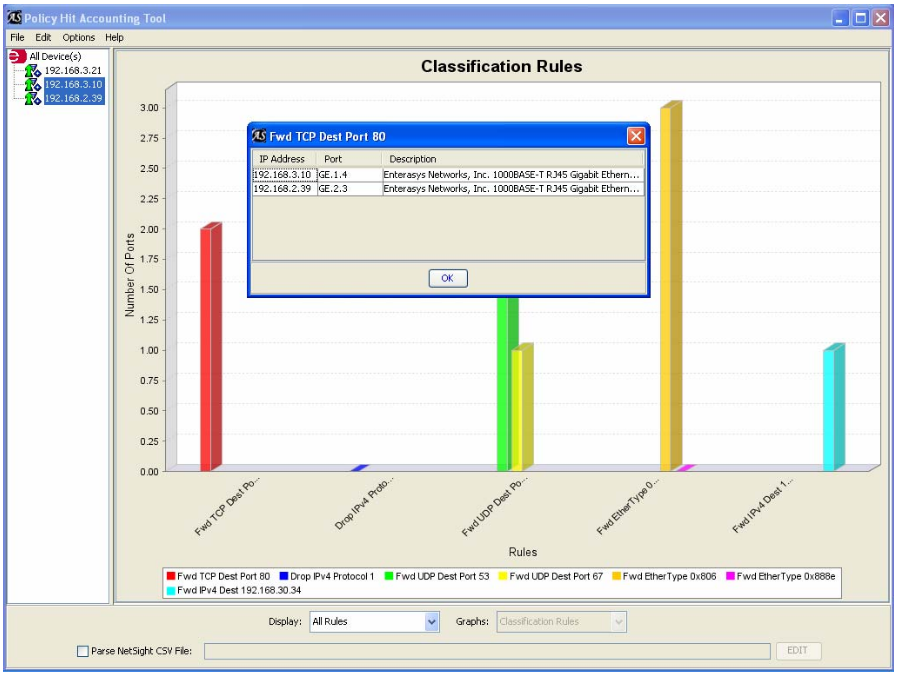
□ Parse NetSight CSV File:

Figure 4. Displaying policy hits for selected devices

Description of the Graph

The x-axis of the graph defaults to the classification rules configured on the selected devices, and the y-axis represents the number of ports that have received classifications rules hits. Note that classification rules are displayed on the x-axis in accordance with the action and traffic attribute being classified on for the specific classification rule. For example in Figure 4, the first classification rule displayed is *Fwd TCP Dest Port 80*, represented by the red bar, which forwards packets with a layer 4 TCP destination port of 80. This classification rule was hit on two ports, as indicated on the y-axis. The legend at the bottom of the graph should be used when the classification rule description is too long to display on the graph's x-axis, or when the spacing of the classification rules on the x-axis is too close to display a label for each bar.

By double-clicking on a bar in the graph, a listing of the ports the classification rule was hit on is displayed. In the example shown in Figure 5, the *Fwd TCP Dest Port 80* classification rule was hit on port ge.1.4 on device 192.168.3.10 and port ge.2.3 on device 192.168.2.39.



Fwd TCP Dest Port 80

IP Address	Port	Description
192.168.3.10	GE.1.4	Enterasys Networks, Inc. 1000BASE-T RJ45 Gigabit Ethern...
192.168.2.39	GE.2.3	Enterasys Networks, Inc. 1000BASE-T RJ45 Gigabit Ethern...

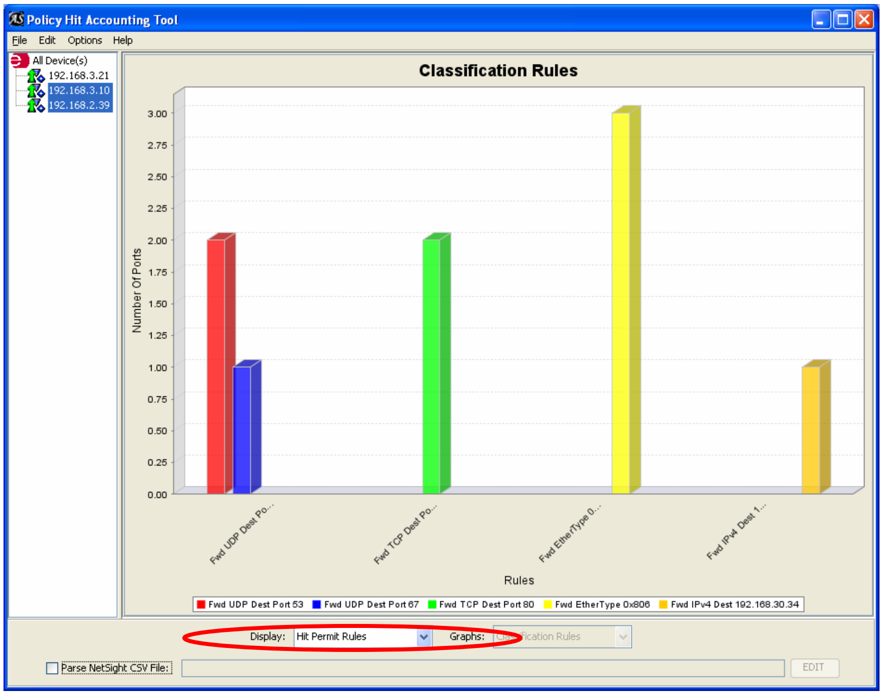
Display: All Rules

□ Parse NetSight CSV File:

Figure 5. Displaying the ports where *Fwd TCP Dest Port 80* classification rule was hit

Options in Displaying Classification Rules

The *Display* drop down menu at the bottom of the Policy Hit Accounting Tool allows the user to control of whether all classification rules are displayed or only "hit" classification rules are shown. Furthermore, in union with this option, it is also possible to select the display of only permit or discard classification rules. For example, the graph shown in Figure 6 displays all permit classification rules that were hit on devices 192.168.3.10 and 192.168.2.39.



Display: Hit Permit Rules

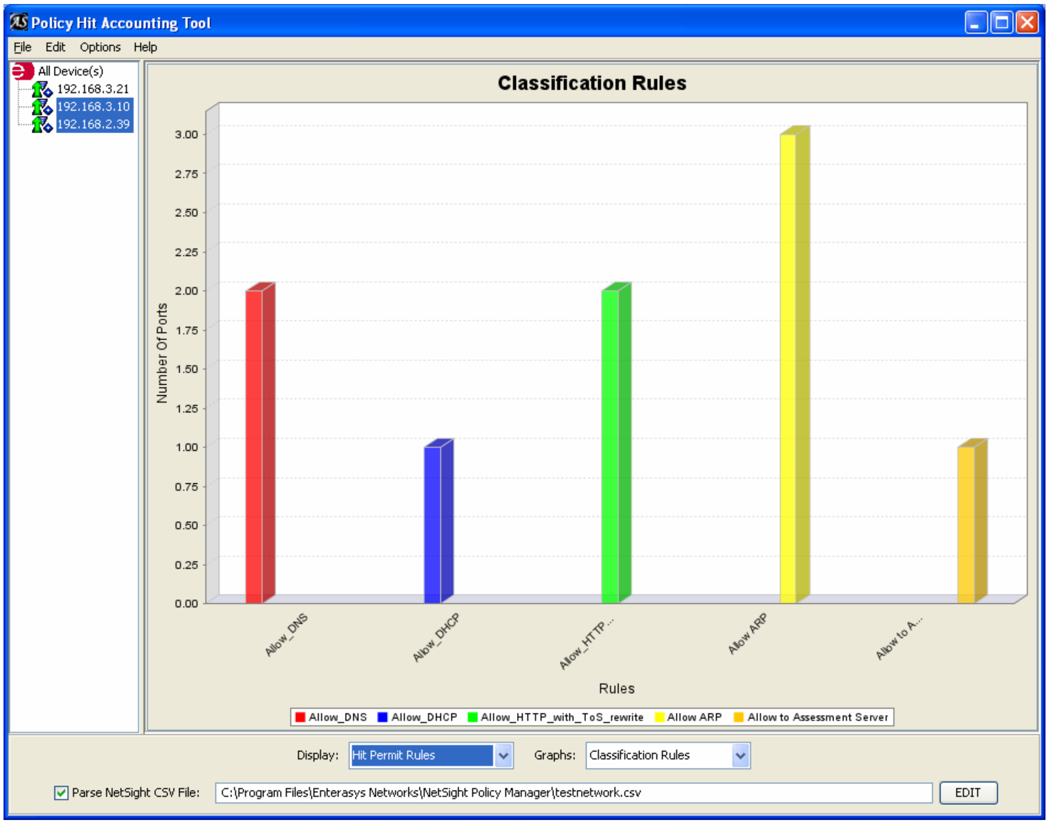
□ Parse NetSight CSV File:

Figure 6. Displaying only permit classification rules that were hit

Importing NetSight Policy Manager Configuration

The Policy Hit Accounting Tool can also be used to graph out classification rules hits using the names of the classification rules, as defined in NetSight Policy Manager, (e.g. *Drop ICMP* for a classification rule that drops packets with an IP Protocol field of *1*) and display classification rule hits for the corresponding services and roles. Yet, the names of the classification rules are stored only in NetSight Policy Manager and not configured on the switches themselves. Furthermore, the services assigned to the roles in NetSight Policy Manager are also not configured on the switches. However, the Policy Hit Accounting Tool supports the generation of graphs that display classification rule names, as well as corresponding services and roles, on the x-axis; requiring the importing of the NetSight Policy Manager configuration as described below.

To display the classification rules on the x-axis by the classification rule name, the Policy Hit Accounting Tool parses the *.csv* file created by NetSight Policy Manager when a *.pmd* file is saved. To generate the *.csv* file for a policy configuration in NetSight Policy Manager 2.0, select the *Export to file* option from the *File* drop down menu and save the current policy configuration as a *.pmd* file. In the same directory where the *.pmd* file was saved, a corresponding *.csv* file is also created with the same file name. To configure the Policy Hit Accounting Tool to parse this file, check the *Parse NetSight CSV* file checkbox at the bottom of the tool's interface, and click on the adjacent *Edit* button navigating to the created *.csv* file. After selecting the *.csv* file, note that the x-axis labels for the classification rules now show the name of each classification rule, as configured in NetSight Policy Manager, rather than details about the traffic attribute and action of the classification rule, as shown in Figure 7. For example, the *Fwd TCP Dest Port 80* classification rule is now displayed as *Allow HTTP* in the Policy Hit Accounting Tool giving a more intuitive display of the configured classification rules on the network.

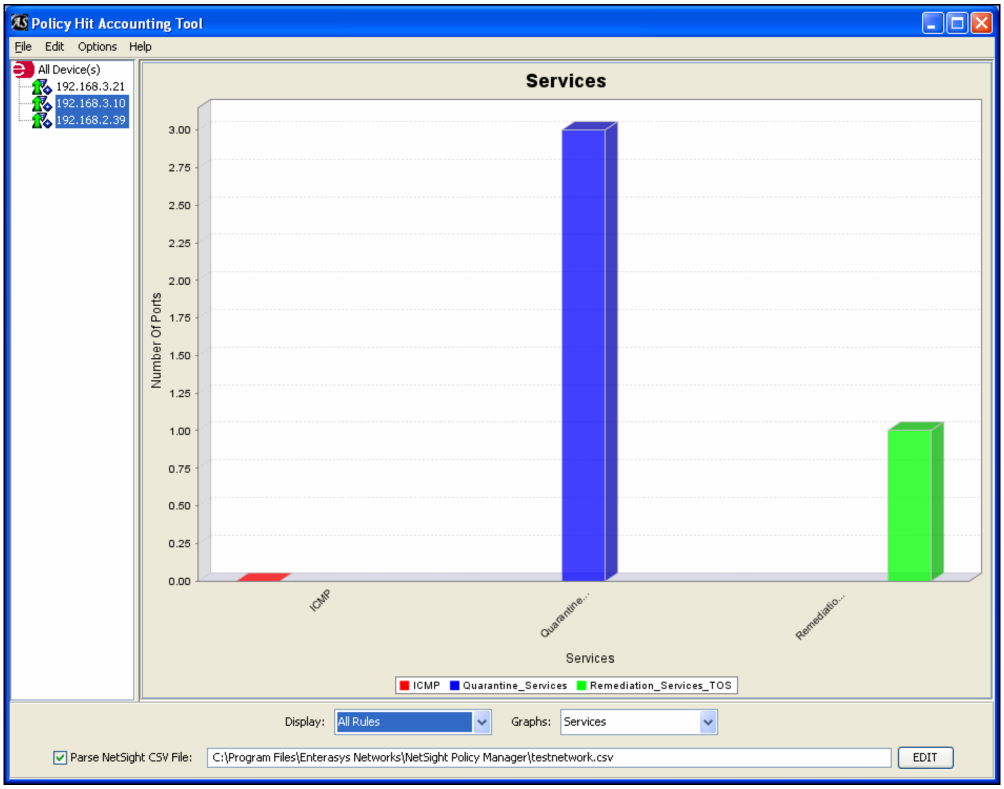


Display: Hit Permit Rules   Graphs: Classification Rules

☑ Parse NetSight CSV File: C:\Program Files\Enterasys Networks\NetSight Policy Manager\testnetwork.csv

Figure 7. Displaying classification rule names by importing NetSight Policy Manager configuration

Furthermore, by parsing the NetSight *.csv* file that corresponds to the policy configuration on the device, it is also possible to change the x-axis to display the corresponding service or policy role where the classification rule was hit. This is accomplished by using the *Graphs* drop down menu at the bottom of the Policy Hit Accounting Tool. The example shown in Figure 8 displays the services specified in the NetSight Policy Manager configuration indicating which services' classification rules were hit on the selected infrastructure devices. Double-clicking on a bar will again display the specific ports on which the service's classification rules were hit.



Display: All Rules

Graphs: Services

☑ Parse NetSight CSV File: C:\Program Files\Enterasys Networks\NetSight Policy Manager\testnetwork.csv

Figure 8. Display of services

<u>Additional Options</u>

The Policy Hit Accounting Tool also supports other options, as listed below:

- The graph can be saved or printed by right clicking on the graph itself and selecting the appropriate option.
- The format of the graph, such as font and axis labeling, can be controlled by right clicking on the graph and selecting the appropriate option.
- Polling can be enabled for the tool where the graph will be automatically refreshed at a specified interval. The *Options* drop down menu is used to enable this feature.
- Logging can be enabled for the tool where the results of each poll are stored to a file. The *Options* drop down menu is used to enable this feature.

Recommended Usage Scenarios

The Policy Hit Accounting Tool provides invaluable information to a network administrator that has deployed policy on Enterasys switches in the network. While policy protects the network from malicious traffic and prioritizes business critical applications, the network administrator has the capability to granularly monitor the usage of the network by leveraging the abilities of Enterasys policy capable switches.

Furthermore, it is also possible to use the Policy Hit Accounting Tool to validate how the implementation of policy would increase the security and efficiency of operation of a network composed purely of 3rd party infrastructure devices, without impacting the existing network. By displaying policy in action as it is hit by the various applications on the network, the Policy Hit Accounting Tool can clearly illustrate the need for port level granular network resource allocation for any network. The following procedure can be used to illustrate the power of Enterasys Secure Networks with policy on a 3rd party infrastructure:

1. Position a Matrix N-series device (e.g. NSA, Matrix N1) inline between an 3rd party access layer device and a 3rd party distribution layer device.
    - As a less intrusive alternative, the Matrix N-series can also be connected to a port on a 3rd party access layer device, and the 3rd party access layer device can be configured to mirror traffic from an uplink port(s) over to the Matrix N-series device.
2. Using NetSight Policy Manager, open *demo.pmd*. Configure all "discard" and "CoS" classification rules grouped into the services that are assigned to the *Enterprise User* policy role to forward traffic without rate limiting using the following procedure:
    - Under the **Services** tab of NetSight Policy Manager, select the *Deny Spoofing & other Administrative Protocols* service in the left pane and configure all classification rules under this service with the action of *Permit Traffic* instead of *Deny Traffic*.
    - Repeat this process for the *Threat Management* service.
    - Under the **Classes of Service** tab, navigate to the *Rate Limits* folder under the *CoS Components* folder in the left pane. Delete all rate limiters by right clicking on the rate limiter and selecting *Delete*.
3. Add the Matrix N-series device to the **Network Elements** tab.
4. Enforce the policy configuration to the Matrix N-series device using the *Enforce* button.
5. Using the **Network Elements** tab, assign *Enterprise User* to the port connected to the 3rd party access layer device, by selecting the Matrix N-series device in the left pane and clicking on the **Details View** tab in the right pane. Right click on the specific port under the **Details View** tab and set the default role to *Enterprise User*.

The Policy Hit Accounting Tool can then be used to poll the Matrix N-series device for policy hits. Importing the NetSight *.csv* into the tool allows for the display of which services' classification rules are being hit. If classification rules in the *Deny Spoofing & other Administrative Protocols* service, *Limit Exposure to DoS Attacks* service, or *Threat Management* service are being hit, it is possible that the network is under attack allowing the transmission of malicious traffic through the network. If the edge device was a policy capable Enterasys switch, this malicious traffic could be discarded before it even entered the network.

Conclusion

The Policy Hit Accounting Tool allows a network administrator to graphically represent the implementation of policy on the network specifically for Matrix N-series Platinum platform. Using this tool, a network administrator can view Secure Networks in action as policy discards malicious traffic before it enters the network and prioritizes mission critical traffic for end to end QoS, yielding increased levels of network security and traffic optimitization. Please contact askthecto@enterasys.com for any questions, comments, and enhancement suggestions about the tool. Please contact enet-as@enterasys.com for any issues with the tool's operation.