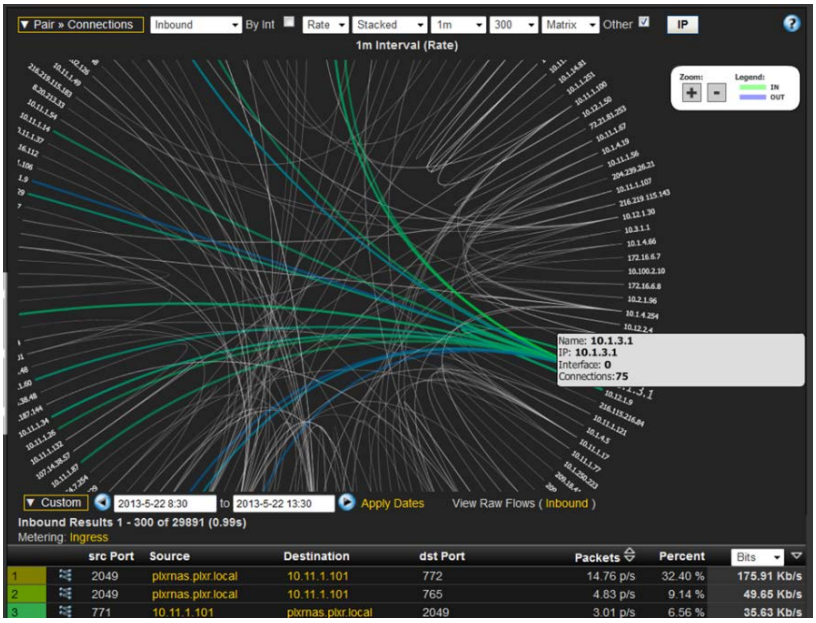
plixer International

Scrutinizer™ NetFlow & sFlow Analyzer

Cisco Catalyst 2960-X

NetFlow-Lite Solution Brief



CISCO DEVELOPER Registered

Table of Contents

Introduction

What is a Cisco Catalyst 2960x Switch?

Cisco Catalyst 2960-X Series Switches are the next generation of the world's most widely deployed access switches, providing Layer 2 and Layer 3 access features. Designed for operational simplicity to lower TCO, this platform also offers superior security capabilities. The switches deliver best-in-class energy efficiency, while preserving your investments through mixed stacking with existing Catalyst 2960-S and SF switches.

What is NetFlow-Lite?

Catalyst 2960-X Series Switches support NetFlow-Lite, which enables IT teams to understand the mix of traffic on their network and identify anomalies by capturing and recording specific packet flows. NetFlow Lite supports flexible sampling of the traffic, and exports flow data in the NetFlow Version 9 format for analysis on a wide range of Cisco and third-party collectors.

The 2960-X uses flow sampling without any form of packet capture. There are two types of possible NetFlow-Lite sampling configurations on the 2960-X:

1. Deterministic sampling: sample packets exactly as specified (I.e. the first flow out of every 100 flows). Deterministic samplers can only be applied on up to four interfaces.
2. Random sampling: samples a random flow out of every X flows. The maximum sample rate for both Deterministic and Random is 1 out-of 32. It is not limited to 4 interfaces like Deterministic sampling.

NetFlow-Lite is based on NetFlow v9 and is included on all Catalyst 2960-X and 2960-XR LAN Base and IP Lite models.

About this Document

This document describes the Flexible NetFlow configuration of NetFlow-Lite using Random Sampling on the Catalyst 2960-X. It also provides several reporting and threat detection examples.

Enabling NetFlow-Lite on the Catalyst 2960-X

In the configuration below, random sampling has been configured. It was added to all interfaces using a random sampler called "my-random-sampler" which was configured to randomly sample 1 out of every 100 flows on the interfaces it was applied to.

Setting up NetFlow-Lite on the 2960-X:

```
!
```

Step 1: Create a flow record

```
flow record flows
match datalink mac source address input
match datalink mac destination address input
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect transport tcp flags
collect interface input
collect flow sampler
! below I specified 'long' because the 2960x supports 64 bit counters
collect counter bytes long
collect counter packets long
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
!
```

Step 2: Create a flow exporter

```
flow exporter export-to-inside
description flexible NF v9
destination 10.1.1.1
```

```
source Vlan7
transport udp 2055
template data timeout 60
!
! lets export some cool option templates
option interface-table
option exporter-stats
option sampler-table
!
!
```

Step 3: Create a flow monitor

```
flow monitor nftest
record flows
exporter export-to-inside
cache timeout active 60
statistics packet protocol
!
! Below was used for the deterministic sampling configuration
! It was disabled in favor of Random Sampling
! sampler full
! mode deterministic 1 out-of 32
!
! Below is the random sampler configuration that I replaced the above with
sampler my-random-sampler
mode random 1 out-of 100
!
```

Step 4: Apply the flow monitor 'nftest' to each interface with

```
! the defined sampler 'my-random-sampler'
! input is for ingress.  Egress was not supported in this release…
interface GigabitEthernet1/0/1
ip flow monitor nftest sampler my-random-sampler input
!
interface GigabitEthernet1/0/2
ip flow monitor nftest sampler my-random-sampler input
!
```

```
interface GigabitEthernet1/0/3
ip flow monitor nftest sampler my-random-sampler input
!
The above is repeated thru 1/0/49

!
interface GigabitEthernet1/0/50
ip flow monitor nftest sampler my-random-sampler input
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
```

The above configuration will send the NetFlow-Lite off to Scrutinizer NetFlow and sFlow Analyzer. Scrutinizer passively listens on multiple configurable UDP ports including 2055 as configured above. After a few minutes, visit the Scrutinizer interface, click on the Status tab and navigate to the 2960-X to run reports.

Catalyst 2960-X NetFlow-Lite Reports

Hundreds of reporting combinations are possible with the NetFlow-Lite export. The following examples demonstrate only a few of the types of reports possible when the flows are exported to Scrutinizer NetFlow and sFlow Analyzer from Plixer.

Host Flows

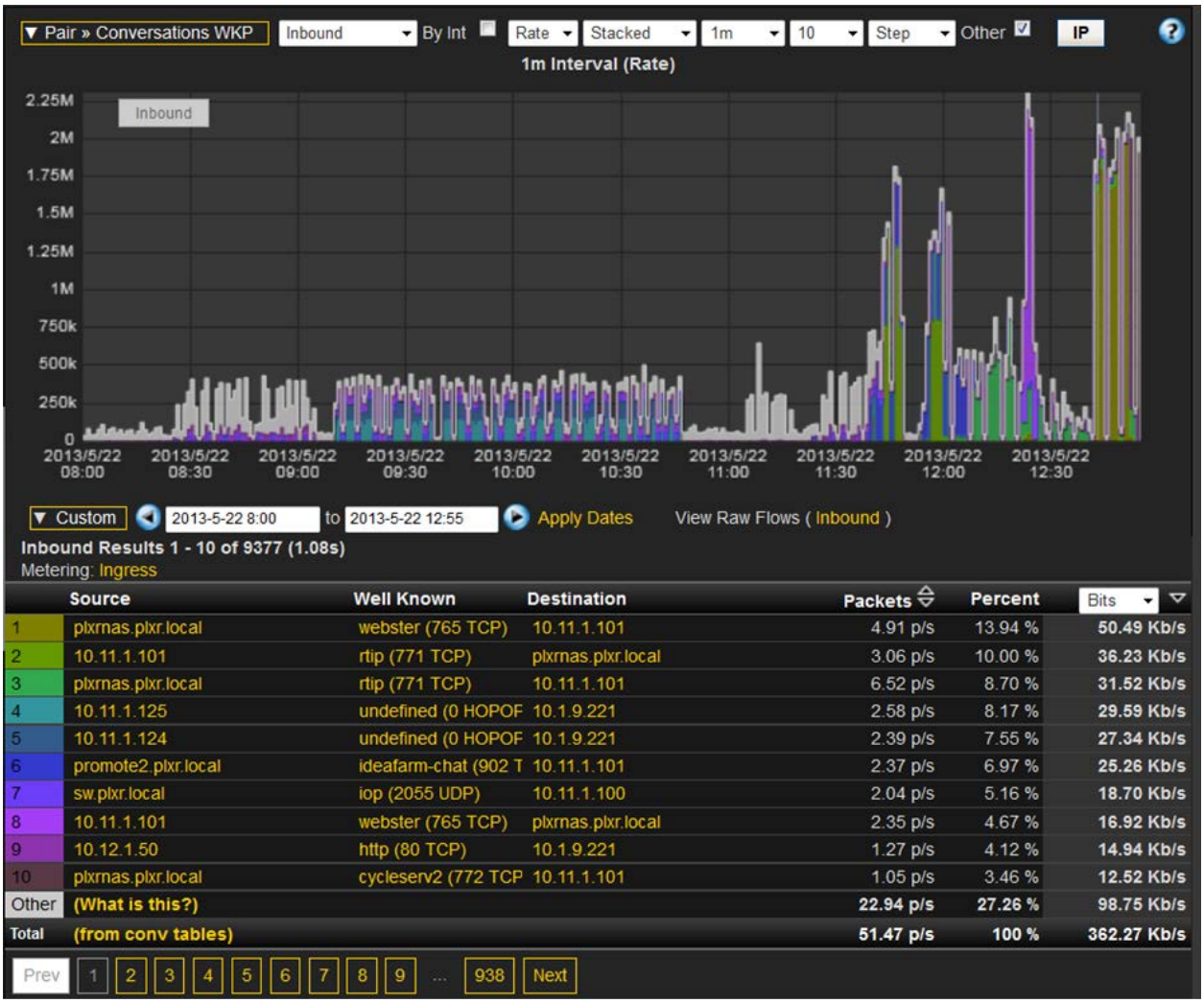
The Host Flows report can group by source or destinations hosts. Below on the left, the "cisco-2960x.plxr.local" devices has been selected and the report type "Source >> Host Flows" has been run. The first column groups by unique Source host. The second column "Dest Hosts" displays the number of unique destination IP addresses the source host connected to for the selected time frame. The third and fourth columns are counts of the total packets and unique flows between the Source and Destination hosts.

NOTE: This data is based on sampled flows.

Conversations WKP

The Conversations WKP (Well Known Port) displays the source and destination IP addresses as well as the primary port being used to communicate. Clicking on a Source, Well Known or Destination entry will prompt the user for a menu to report specifically on the selected entry. This behavior is one way to create a filter.

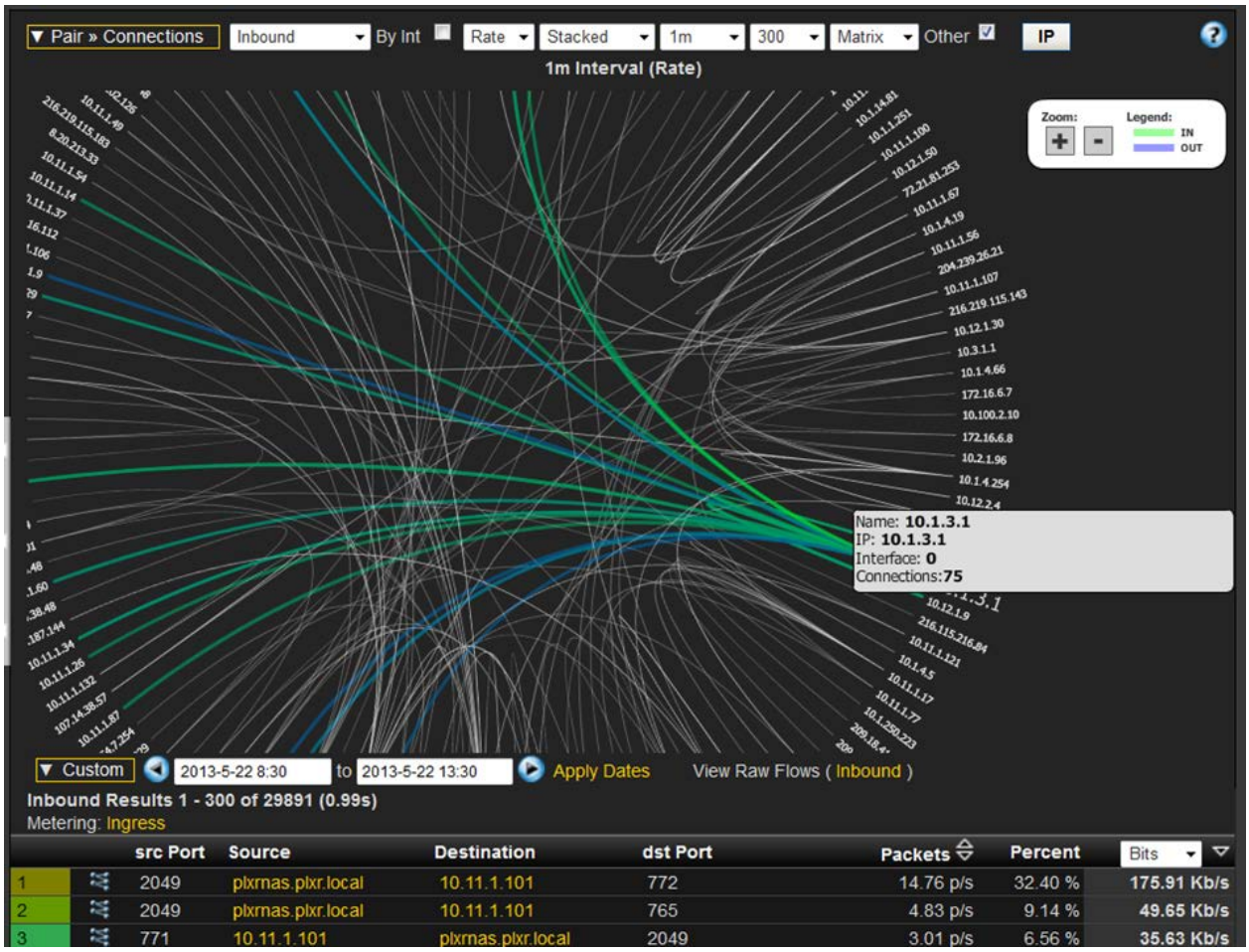
Notice the pagination at the bottom '938'. Scrutinizer provides 100% access to all the flows (I.e. not just the top 1000). To view the raw flow data used to create the report, click on 'Inbound' after "View Raw Flows".



	Source	Well Known	Destination	Packets	Percent	Bits
1	plxrnas.plxr.local	webster (765 TCP)	10.11.1.101	4.91 p/s	13.94 %	50.49 Kb/s
2	10.11.1.101	rtip (771 TCP)	plxrnas.plxr.local	3.06 p/s	10.00 %	36.23 Kb/s
3	plxrnas.plxr.local	rtip (771 TCP)	10.11.1.101	6.52 p/s	8.70 %	31.52 Kb/s
4	10.11.1.125	undefined (0 HOPOF	10.1.9.221	2.58 p/s	8.17 %	29.59 Kb/s
5	10.11.1.124	undefined (0 HOPOF	10.1.9.221	2.39 p/s	7.55 %	27.34 Kb/s
6	promote2.plxr.local	ideafarm-chat (902 T	10.11.1.101	2.37 p/s	6.97 %	25.26 Kb/s
7	sw.plxr.local	iop (2055 UDP)	10.11.1.100	2.04 p/s	5.16 %	18.70 Kb/s
8	10.11.1.101	webster (765 TCP)	plxrnas.plxr.local	2.35 p/s	4.67 %	16.92 Kb/s
9	10.12.1.50	http (80 TCP)	10.1.9.221	1.27 p/s	4.12 %	14.94 Kb/s
10	plxrnas.plxr.local	cycleserv2 (772 TCP	10.11.1.101	1.05 p/s	3.46 %	12.52 Kb/s
Other	(What is this?)			22.94 p/s	27.26 %	98.75 Kb/s
Total	(from conv tables)			51.47 p/s	100 %	362.27 Kb/s

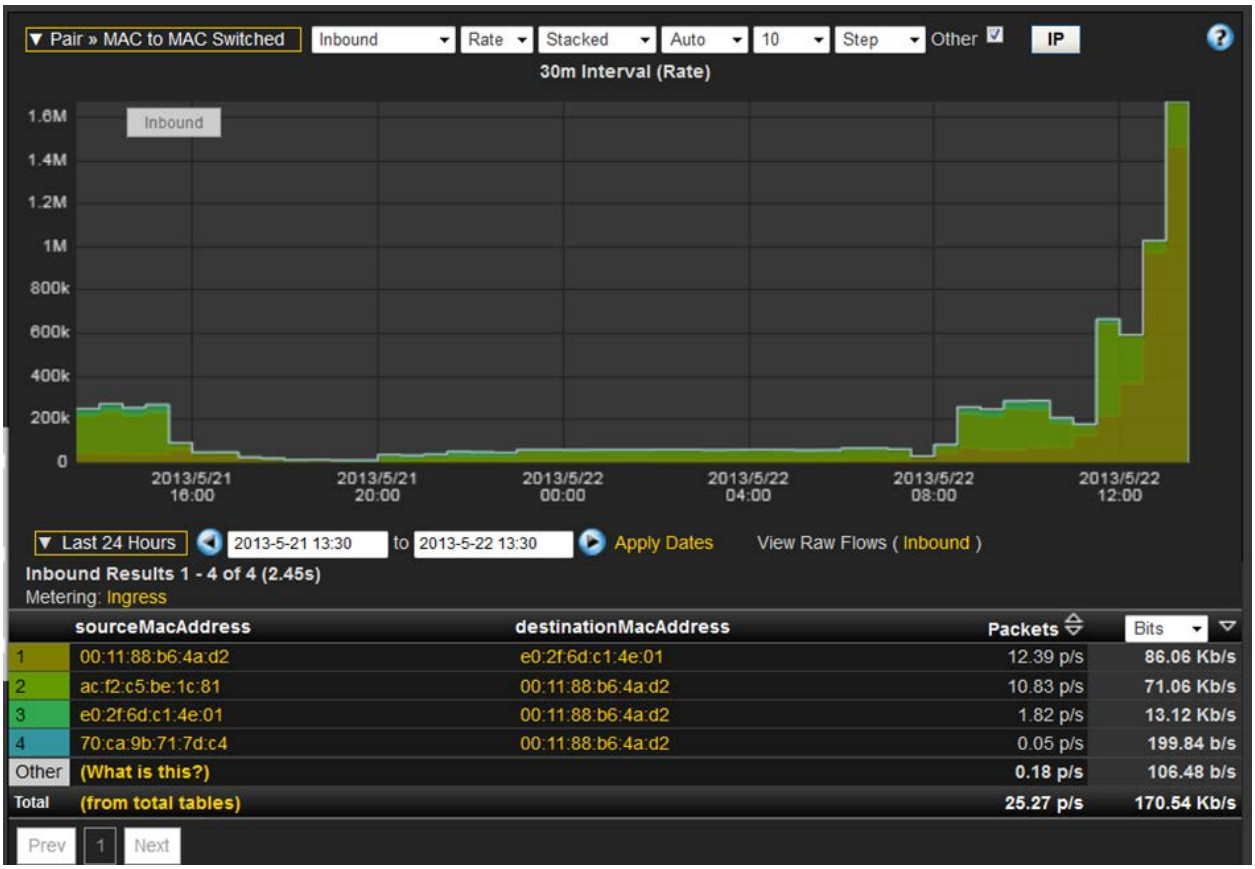
Connections

The Connections report displays the source and destination IP address and ports. By default, this report displays a trend. In the example below the 'Matrix' graph type was selected to demonstrate one of several methods included in Scrutinizer to display the data. The Matrix view is useful when trying to understand the propagation of certain types of malware such as worms.



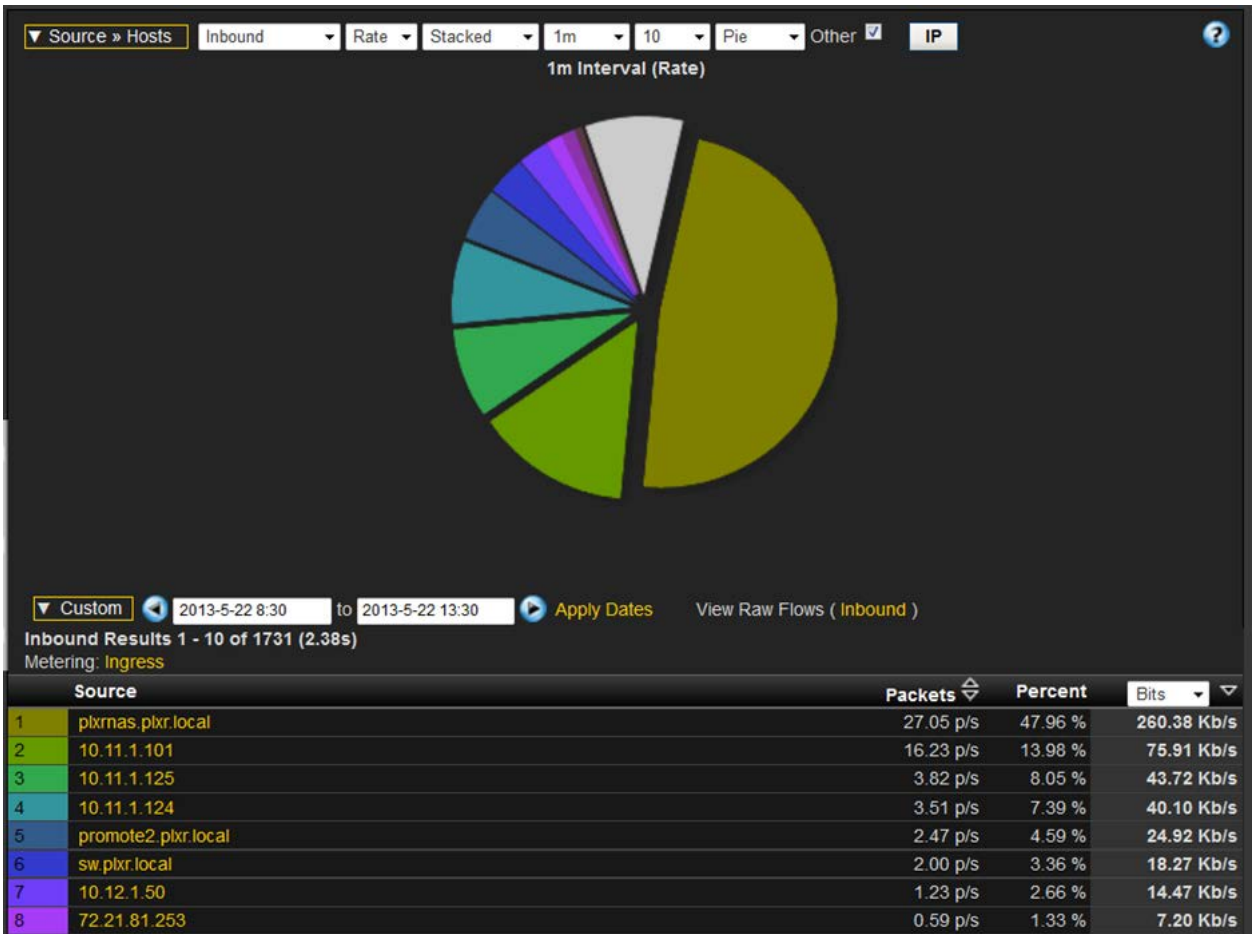
MAC to MAC Switched

Because the Flexible NetFlow configuration was setup to export MAC address, Scrutinizer can report on these Layer 2 details. Filtering can be applied to include/exclude individual addresses or a portion of the address such as the first 3 bytes representing the vendor ID.



Hosts

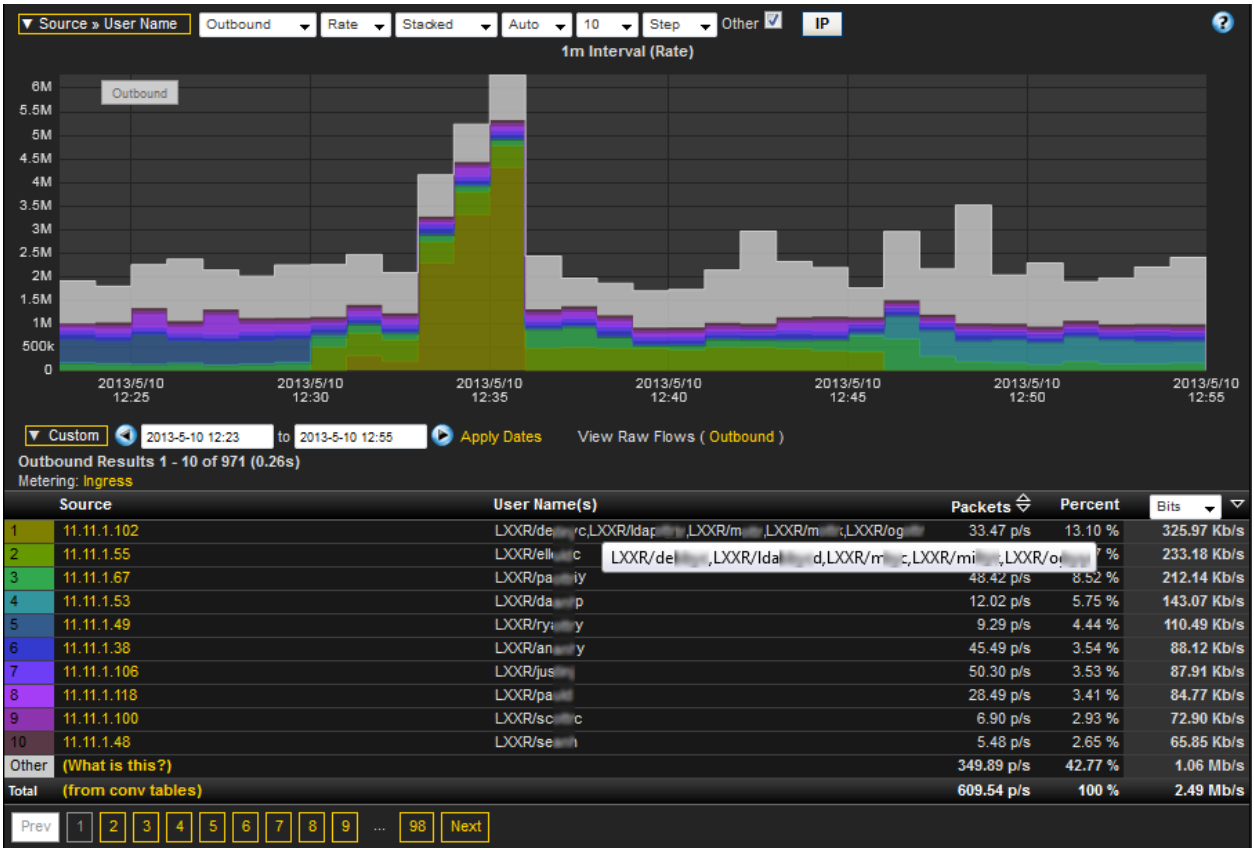
The Hosts report below demonstrates that Scrutinizer can display pie charts as well.



	Source	Packets	Percent	Bits
1	plxrnas.plxr.local	27.05 p/s	47.96 %	260.38 Kb/s
2	10.11.1.101	16.23 p/s	13.98 %	75.91 Kb/s
3	10.11.1.125	3.82 p/s	8.05 %	43.72 Kb/s
4	10.11.1.124	3.51 p/s	7.39 %	40.10 Kb/s
5	promote2.plxr.local	2.47 p/s	4.59 %	24.92 Kb/s
6	sw.plxr.local	2.00 p/s	3.36 %	18.27 Kb/s
7	10.12.1.50	1.23 p/s	2.66 %	14.47 Kb/s
8	72.21.81.253	0.59 p/s	1.33 %	7.20 Kb/s

Usernames

Scrutinizer can integrate with Microsoft Directory Services, Cisco ISE or any other network authentication system to gain access to usernames for IP address to actual login account correlation. Notice below that the top IP address has been authenticated onto the network with multiple user names during the time frame selected.



Dashboards

Dashboards are customizable views specific to individual account profiles. All reports created in Scrutinizer including those with filters can be placed into customizable dashboards.

Threat Detection

Beyond the native threat detection capabilities of the Catalyst 2960-X additional behavior analysis can be performed on the flows it exports. NetFlow and IPFIX solutions like Scrutinizer are well suited for organizations trying to identify threats for several reasons:

- They constantly compare IP addresses found in flows to a routinely updated host reputation databases
- They can be used to perform investigations on traffic to determine who a potentially infected host has been communicating with, when and for how long.

"DPS (or deep packet inspection) is our #1 security defense; **NetFlow is a very close #2**"

Gavin Reid, Director Threat Research at Cisco Systems

IP Host Reputation

One of the features that sets threat detection solutions apart is the integration of an IP reputation system that performs rigorous research and analysis. Reliable reputation lists require direct observation to identify threats that are placed into context and it requires advanced IP forensics to categorize the results. It must also deliver actionable updates on an hourly basis.

"We've learned that NetFlow can tell us who is talking to who across our network, but how can we tell who is a bad actor? By checking the **reputation of the IP addresses** at both ends of the conversation."

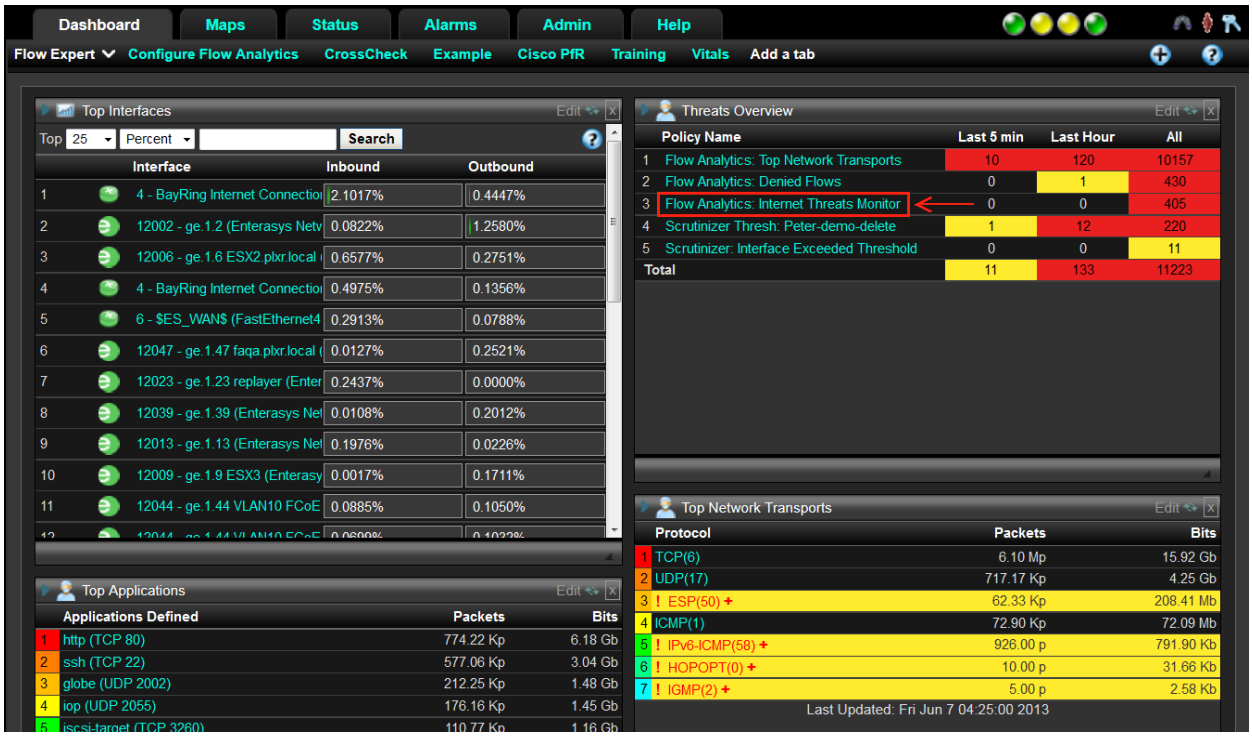
Mike Schiffman at Cisco Systems

Scrutinizer passes the NetFlow-Lite received through dozens of algorithms which scour the flows for various suspicious behavior patterns. In the dashboard on the next page, the "Internet Threats Monitor" leverages a constantly updated host reputation database.

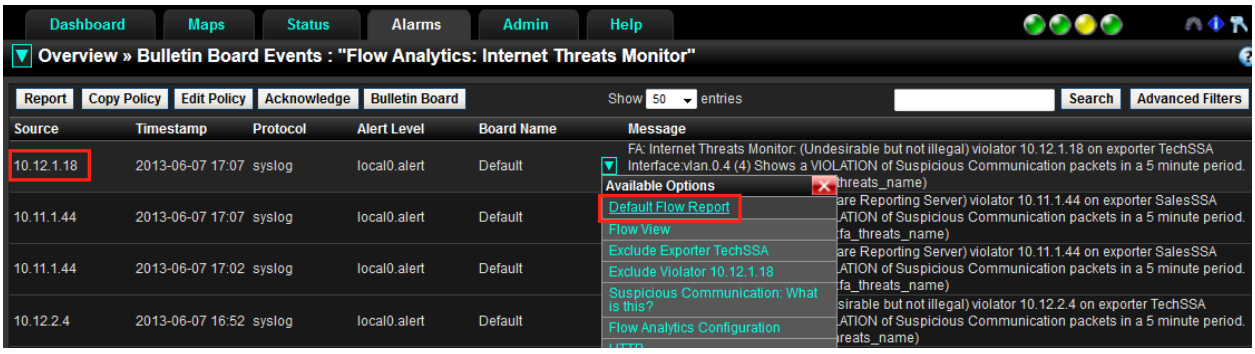
Positive IP address reputation matches are placed into the alarm table as described in the next section.

Threat Dashboards

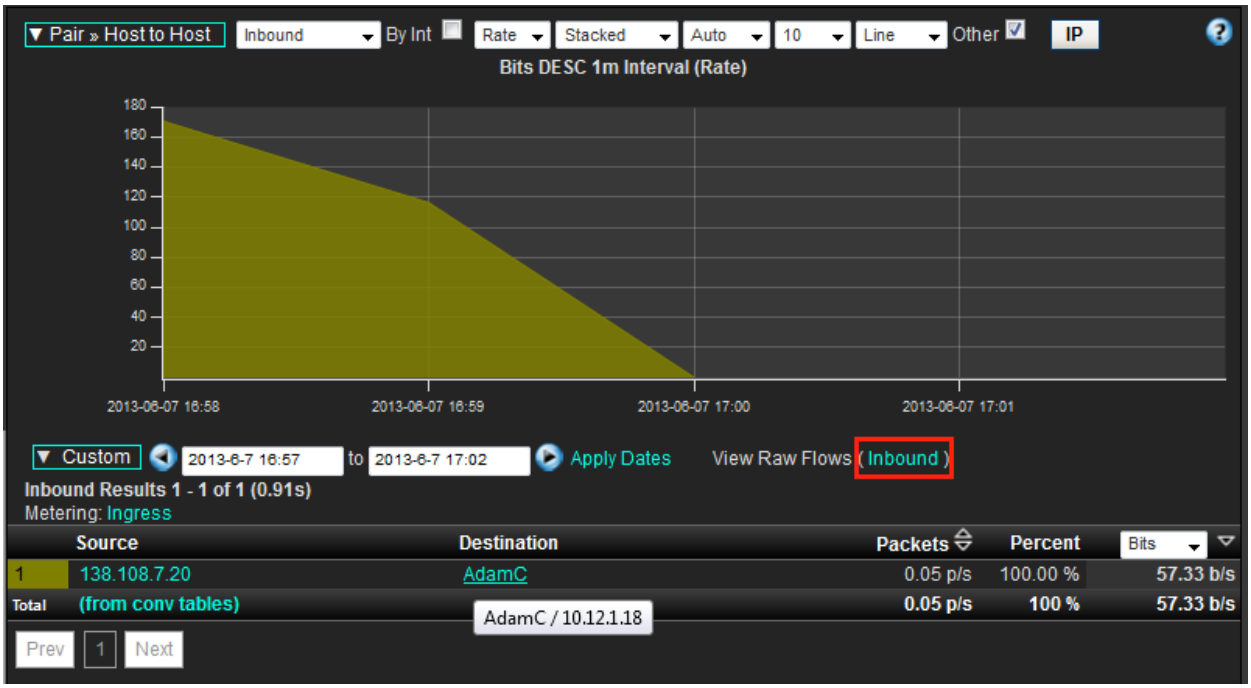
In the upper right corner of the dashboard below, the threats overview lists the Internet Threats Monitor which is triggered by a host reputation match.



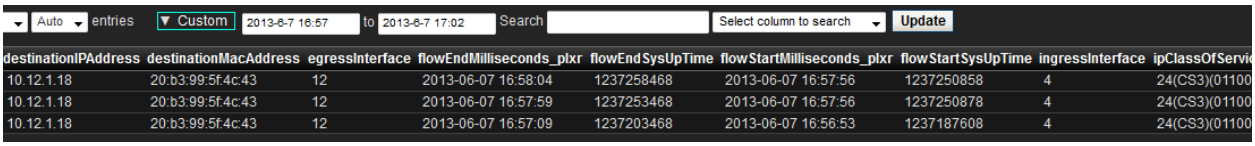
When you click on the entry above, (outlined in red) the window below pops up with details specific to the alarm. Click again for details on the flows for a specific host.



Selecting 'Default Flow Report' in the above menu will bring up the Host to Host report below with the filter sourceIPAddress=10.12.1.18.



To observe the details behind the above report, click on the "View Raw Flows (Inbound)" link. This will launch the Flow View shown below:



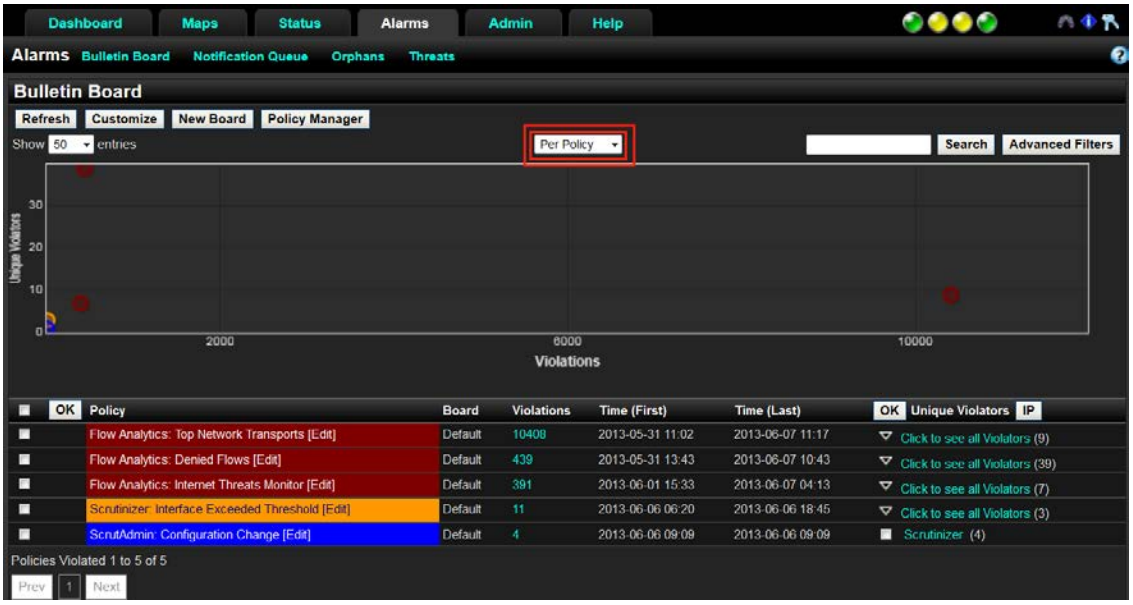
The ability to drill in for the details allows you to access the Wireshark like details of the flow exported by the Catalyst 2960-X.

Alarming

Alarm logs in the threat detection industry have been plagued with voluminous amounts of events. Many detections are false positives resulting in alarm boards being ignored. Scrutinizer addresses this problem by taking multiple approaches. Alarms are displayed in two different tables: Per Policy and Per Violator. Each view provides a threat heat map with the most significant threats being placed high and to the right.

Per Policy

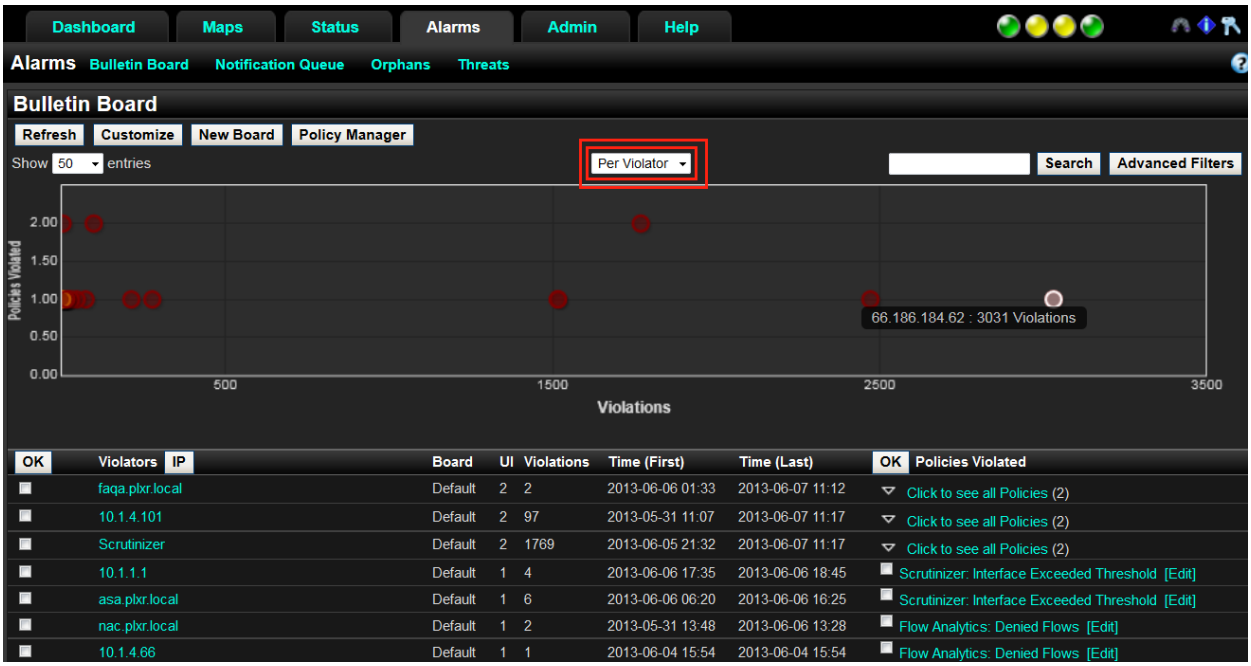
This is a list of all the policies or algorithms being violated. Each algorithm lists the Violation count and can be expanded to view the hosts which triggered the violations. Policies are plotted based on the number of unique hosts violating them (Y axis) and the count of violations (X axis). Clicking on the dots brings up the list of events which can be clicked on for further details.



Drilling in on the above "Flow Analytics: Internet Threats Monitor" policy will display the 391 individual events. Clicking to the right on "Click to see all Violators" will display the seven hosts that have violated the policy.

Per Violator

This is a list of all the hosts that have violated one or multiple policies (I.e. Algorithms). Each host is plotted based on a UI (Unique Index) and a Violation count. Clicking on the dots brings up the list of events which can be clicked on for further details. Similar to the Per Policy view, entries high and to the right should be investigated first.



Drilling in on a host above leads to a view which provides quick access to the specific flows which triggered the events.

Every violation should be taken seriously however; the reality is that threats cloak themselves as legitimate traffic. By addressing the hosts high and to the right first, the heat map will auto scale bringing the next most significant issue to your attention.

Summary

The addition of NetFlow-Lite to the Catalyst 2960-X line of switches demonstrates continued support of flow technologies across nearly the entire product line. In partnership with Cisco Systems, Plixer engineered support for this exciting new export and has clearly demonstrable functionality.

Scrutinizer's effectiveness as a complete NetFlow solution is enhanced when the exports are scoured for abnormal behaviors and the IP addresses within the flows are compared to host reputation databases. Scrutinizer was the first solution to report on these unique exports and continues to work directly with the Catalyst 2960-X engineers at Cisco Systems.

"For the last 6 years I have been working with Cisco's NetFlow engineering team, customers as well as many network management system vendors. Plixer is one of the industry's premier thought leaders. It is clear to me that Michael and the team at Plixer are passionate when it comes to anything NetFlow and IPFIX related. This is a company that is on the bleeding edge of NetFlow/IPFIX processing and has much to share with industry."

Aamer Akhter, Technical Leader & Architect for Network Management Solutions at Cisco Systems

NetFlow and IPFIX exporting routers, switches and servers provide a form of electronic video surveillance by providing historical visibility into 100% of all traffic passing through their systems. The Scrutinizer NetFlow collector uses behavioral logic to detect threats and stores 100% of the data for future reference.