# NetFlow vs. sFlow:

**A Technical Review** 





# Table of Contents

Abstract	3
Introduction	3
NetFlow	3
sFlow	3
Lab Configuration	4
Hardware	4
Collection and Analysis	4
Utilization Measurements	4
Top Hosts Don't Match Up	5
Strictly Speaking IP	6
Flow Volumes Back To The Collector	8
Historical Differences	9
Conclusion	11
Related Articles	12

# Abstract

In an effort to gain more insight into large scale networks where packet probes are not feasible, NetFlow and sFlow capable routers and switches are being utilized. NetFlow & sFlow are technologies supported by most major router and switch vendors whereby packet analyzer like details are pushed to a collector. This paper provides technical insight into the differences between the two.

## Introduction

NetFlow Vs. sFlow is not so much a question of which is better, it is more of an architecture question of: Where should each be deployed? NetFlow (i.e. IP FIX) is a standard developed by Cisco and is generally software based. However, there are hardware implementations (e.g. Enterasys). Inmon is the developer of sFlow, which is hardware based.

#### NetFlow

When NetFlow version 5 is enabled on an interface, it caches conversations between hosts and exports the conversations in a configurable interval, which is typically every 60 seconds for TCP and immediately for UDP. The packets between host A and host B are summarized into a single record in a NetFlow datagram. A single NetFlow packet can contain up to 30 records where each represents potentially thousands of packets. Because of its aggregation method, it normally results in a less than a 1% increase in network traffic. Vendors supporting NetFlow can be found here:

http://www.plixer.com/products/scrutinizer\_activate-netflow.php

## sFlow

SFlow is a packet sampling technology. Some implementations can only sample every 100th packet per interface while others, such as Foundry, can sample every other packet. Although sFlow can provide more details than NetFlow, such as errors per interface, sFlow generally is not as accurate when measuring total traffic between two hosts. This is only true in pure IP environments. Vendors supporting sFlow can be found here:

http://www.sflow.org/products/network.php

Developments in NetFlow v9 allow it to sample similar to sFlow.



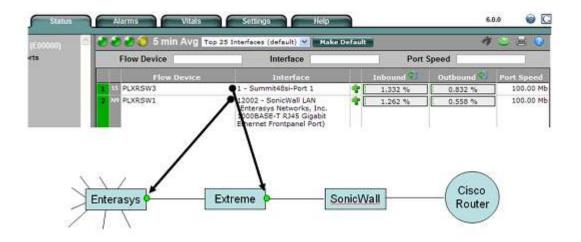
# Lab Configuration

#### Hardware

In the lab, an Extreme Summit sFlow switch running v7.6 firmware was inserted between the Enterasys switch running Rev 05.42.04 and the firewall (SonicWall). The Enterasys switch supported NetFlow v9 and the Extreme switch supported sFlow v5. The sampling rate on the Extreme was configured to sample every packet. The lab technician wasn't confident that the Extreme Summit switch could sample every packet, but the switch didn't complain after entering the command.

#### Collection and Analysis

For flow collection, Scrutinizer NetFlow & sFlow Analyzer v6 was used, which is pictured below. PLXRSW3 (sFlow) is the Summit switch and PLXRSW1 (NetFlow) is the Enterasys Switch.

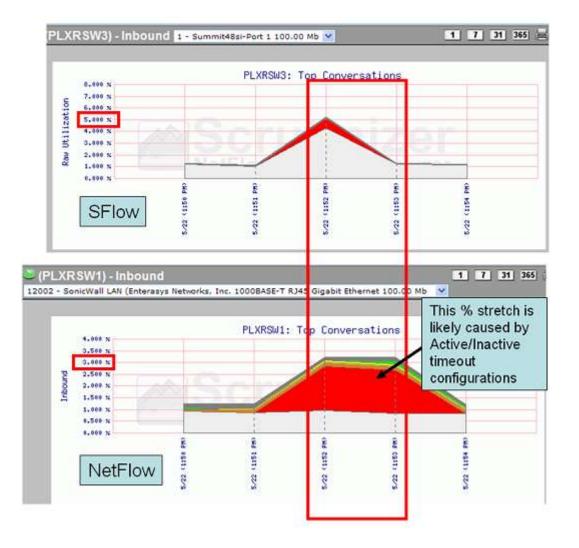


#### Utilization Measurements

The above configuration displayed traffic rates of the same live traffic using NetFlow and sFlow collection. Notice above that the Inbound and Outbound - five minute traffic averages don't match for exactly the same traffic volumes. The Extreme Summit = 1.332 % and the Enterasys = 1.262 % for Inbound utilization. The lab technician believes this was likely caused by many things including the fact that sFlow samples tend to be exported closer to real time. NetFlow, on the other hand, has to deal with active and inactive timeout configurations (http://www.plixer.com/products/scrutinizer\_activate-netflow.php). Because of this, an sFlow switch would likely reflect a sudden spike in utilization quicker than a NetFlow switch.

At times both switches would be as much as 1% different from one another, but for the most part they were pretty much the same. Below is an example:





# Top Hosts Don't Match Up

The test was left to run for a few days. Scrutinizer sat there collecting away. Every so often the top ten talkers reported were compared for the same time frame. They seldom matched up when looking at trends for the last 5 minutes or the last 24 hours:



14532		ys -		30. 4385	tre		ne - SFlow
15	~	Int	Source	15	*	Int	Source
1		12002	66.186.184.219		-	1	66.186.184.219
2		12002	10.1.1.64	2	-	1	66.151.115.139
		12002	66.151.115.139	3	-	1	208.80.52.80
		12002	10.1.3.252		~	1	66.186.184.220
5		12002	66.186.184.220	5		1	79.32.128.227
		12002	78.48.224.164		~	1	66.186.184.202
		12002	72.36.152.206			1	80.185.209.3
8		12002	79.32.128.227 💕	8		1	81.222.204.131
9			137.226.34.232	9		1	87.98.130.166
-	-			1	)	1	81.217.109.35

As expected, since the Extreme Summit is sampling packets, the total host bit count is below what the Enterasys Switch is reporting for the same host for the same time frame:

ns Hosts	Enterasys - NetFlo		s
Source	Application	Theorem in the	Total bits
66.186.184.219	ssh (TCP 22)	10.1.69.1 12028	57.69 % 225.44 Mb
	and the second sec		
oons Hosts	Extreme - SFlow	Qos	AS
uons Hosts	Extreme - SFlow	Qos	AS Total bits

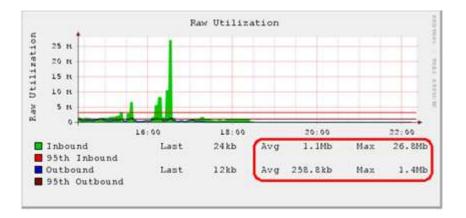
## Strictly Speaking IP

When looking at purely IP traffic, NetFlow has the advantage of collecting nearly everything; hence the 4 fold increase over the sFlow interface above. On the other hand, unlike NetFlow, sFlow is not limited to IP traffic and results in more accurate overall utilization. Notice below that the same Outbound traffic reported by NetFlow is under that which is stated by sFlow.

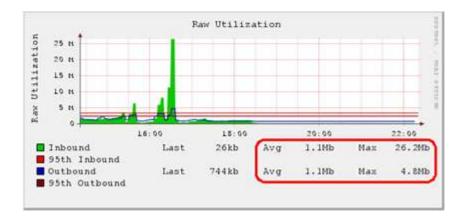




NetFlow Trend:



### sFlow Trend:



Regarding the above, sFlow reports on non IP traffic as well as broadcasts that are not exported by NetFlow.



"The Enterasys Matrix N-Series switches collect NetFlow statistics for every packet in every flow without sacrificing performance based on the nTERA ASIC capabilities," said Trent Waterhouse - Marketing VP for Enterasys.



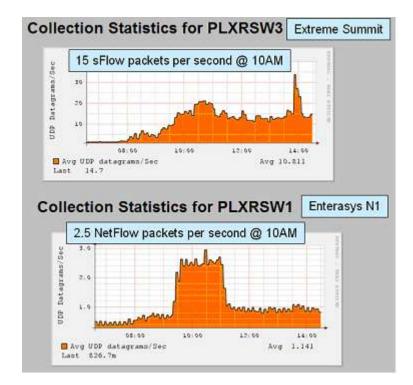


"Although we have considered the recent IPFIX solution (based on NetFlow v9), ProCurve currently favors sFlow for unification of our wired and wireless ... "

".... the NetFlow feature is an important transition technology for the "refresh" and we do have plans in our next software release to support NetFlow in our WAN router products." See: Blog with Paul: http://www.networkworld.com/community/node/23982

## Flow volumes back to the collector

When the lab technician reviewed the volume of sFlow traffic being sent by the Extreme Summit switch back to the Scrutinizer collector, the results were again interesting. The Extreme sFlow volume was 6 times that of the NetFlow sending Enterasys switch. This is because Plixer configured the Extreme switch to sample as much as possible, which generally isn't necessary. See below:



Note that many believe that sFlow is a 1:1 ratio of 1 packet per 1 sample. This is not true. As Wireshark points out below in the packet trace, a single sFlow packet had 8 packet samples in it:

8	-	ex.	8	-	Ð		×	** 2	3	9	Þ Þ	Ø	<b>4</b>			•	9	Q,		100	$\otimes$	15	×
(beri		_	_		~					•	Erpress	on ç	Jear Apply										
io	D	Ne .			Source	4			Dest	nation			Protocol	Info									
_	11	145	:35.	5269	66.1	86.184	.180		66.	186.1	4.202		SFlow	V5.	actent	10.1	2.20.	sub	acent	10	0. 5	eg 92	08/17
						80.184					34.202		SELOW			10.1.							
						96.184					34.202		sF)ow			10.1							
						86.184					34.202		SFlow			10.1							
						86.184					\$4,202		SETOW			10.1							
						86.184					14,202		SFlow			10.1							
						86.184 86.184					34.202		SFlow			10.1							
						86.184 86.184					34.202		SFTOW			10.1							
						7.215					54.202		SFlow			72.3							
						86.184					34,202		SFlow			10.1							
						86.184					34.202		SFlow			10.1							
						86.184					34.202		sFlow			10.1							
						86.184					4,202		SElow			10.1							
						86.184					34,202		sFlow			10.1							
		1451	36.1	179236	66.1	86.184	.180		66.	186.13	34:202		SFlow	V5.	agent	10.1	2.20.			ID.	0, 5	eq 92	08233
	16 14	с II,	. Sr	c; Sor	ricwa1	_0c:1	9:09		:61:0	)c:18:	69), O		e11_38:t	5:10 (0	0:18:	85:38:	65:10	sub		10	0, si 	eq 92	08233
	16 14 hernet er bat fon si dat ag igent Sub-at sequent sysup trow	t II, t Pro tagna flow ram v addr gent hce r time: time: VS S	vers ress ID: Numb : 45 St 8	t; Sor ol, se rotoce ion: 1 ; 10.1 0 er: 9 268534 165 (j	11 cwal c: 66 11 ≤ 2,20 208218 6 11 ease	_0c:1) .186.; c Port (10.: ;	8:89 184,11 1: 10 1.2,2 1.2,2	80 (66 24 (10 0)	1611( ,186, 24),	0c:18: 184.1 DST P	89), 0 80), 0 ort: 6	st: 6 243 (	ell_38:t	5:10 (0	0:18:	85:38:	65:10	sub		: 10	0. 5	eq 92	08230
	16 1- bernet ternet ton si dat agent sub-ar teque tequer teque tequer tequer tequer tequer tequer teque teq teque teque teque teque teque teque teque te	t II, t Pro lagra tlow addr gent hce f time: toles vo s	vers to: ress to: st 8 sano	c; Son ol, Se rotoco ion: 1 ; 10.1 0 er: 9; 268534 Tes (;	1 Cwa 1 c: 60 1 2 2, 20 208218 6 1 ease 20 0	_0c:1 .186.: c Port ( (10.: ; writ: 2 00	9:69 184,11 1: 10 1.2,2 1.2,2 e and 01 00	80 (66 24 (10 0) contr	16110 ,186 24), 1601	c:18: 184.1 DST P : code 14 6a	89), 0 80), 0 ort: 6	st: 6 243 (	e11_38:1 6.186.1 6343)	5:10 (0	0:18:	85:38:	65:10	sub		: 10	0. 5	eq 92	0823
10 US 10	16 1- bernet ternet ton si dat agent sub-ai tequer bysup tequer bysup tequer bysup tequer bysup tequer bysup	t II, t Pro lagra t low addr gent hce f t inte t inte t inte 2 200 0 000	vers ress ID: numb : 45 Salo	c; Sor pl, sr rotoc; ion; ! ; 10.1 0 er; 9; 26853- (65.02 (65.02 00.02	11 cwa 1 c: 60 1 2.20 08218 6 108218 6	_0c:1 .186.: c Port (10.: u (10.: u writ: 0 00 0 00	8:69 184,11 1:10 1.2,2 1.2,2 1.2,2 1.2,2	60 (66 24 (10 0) contr	16110 .186 24), 16010	c:18: 184.1 DST P c code	to di	st; 6 343 () ssect	e11_38:1 6.186.1 6343)	5:10 (0	0:18:	85:38:	65:10	sub		: 10	0. 5	eq 92	0823)
In US In 10	16 14 bernet ernet ar Dat don si dat ag ugent sub-a su	t II, t Pro tagno tagno tagno addr gent hce f time toles vo : 2 000 f 00	ver's ress ID: 45 31 8 31 9 00	c; Sor ol, Se rotoci ion: 1 o er: 9 ces3a res ( 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 Civia I c: 60 1 S 08218 6 1 ease 00 0 00 0	_0c:1 .186.: c Port (10.: u (10.: u writ: 0 00 0 00	8:69 184,11 1:10 1.2,2 1.2,2 1.2,2 1.2,2	60 (66 24 (10 0) contr	16110 .186 24), 16010	c:18: 184.1 DST P c code	to di	st; 6 343 () ssect	e/1_38;t 6.186.18 6343) them!) 	5:10 () 4,202 (	0:18:	85:38:	65:10	sub		10	0. 5	eq 92	0623)
1n 15 1n 40 50 60 70	16 14 bernet er bat dat agent sub-as sequen bysup friow 6e 2 55 a 31 7 00 0	t II, t Pro taora taora tlow addr gent hce f time toles 2 80 0 00 f 00 4 00	vers ress to: st 8 salio 00 00 00	c; Sor ol, Sr rotocr ion: 1 ; 10.1 0 er: 9; c68534 00 02 00 02 00 02 00 02 00 02 00 02	1 Cital C: 66 1 S 08218 6 1 ease 1 ease 00 0 00 0 00 0 00 0 00 0	_0ct1 .186.) c Port (10.) (10.) ( writ) 0 00 0 00 0 00 0 00 0 00 0 00	8:89 184,11 1:10 1.2,2,2 1.2,2,2 1.2,2,2 1.2,2,2 1.2,2,2 1.2,2,2 1.2,2,2,2 1.2,2,2,2,2 1.2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,	contr 00 00 1a 00 100 00 100 00 100 00 100 00 100 00	16110 .186. 24), 16010 194 94 94 94 012	c:18: 184.1 Dst P code 14 6a 00 co 00 00 00 00 3f 13	to di	st: 6 243 () ssect	e11_38:1 6.186.1 6343)	5:10 () 4,202 (	0:18:	85:38:	65:10	sub		10	0. 5	eq 92	0823)
In US In 10 10 10 10 10 10 10 10 10 10 10 10 10	16 14 bernet ternet ton si dat agent sub-as tequer tysup friow 66 2 55 a 31 7 00 0 56 0	t 11, t Pro addr addr addr gent hc2 f time t 100 2 300 f 00 f 00 f 00 f 00 d 00 f 00 d 00	, Sr otoc an P ress ID: 10: 145 5370 00 00 00 00 00 00	c; Sor ol, Se rotoco ion: 1; ion: 0; o er: 0; 268534 ies (; 00.0200000000	1 CH 1 C; 60 1 2 2,20 08215 6 1 ease 00 0 00 0 00 0 00 0 00 0	_0c:1 .186.; c Port (10.: writ) 0 00 0 00 0 00 0 00 0 00 0 00 0 00 0	8:69 184,11 1:10: 1.2.2.2 1.2.2.2 1.2.2.2 1.2.2 1.2.2 1.2.2 1.2.2 1.2.2 1.2.2 1.2.2 1.2.2 1.2.2 1.2.2	contr 00 00 1a 00 100 0 100 0 100 0 100 0	161:0 .186. 24), 160. 194. 94. 94. 94. 94. 94. 94. 94. 94. 94.	c:18: 184.1 ost P ost P 14 6a 00 co 00 co 3f 13 05 fc	to di 0	ssect	e11_38;t 6.186.11 6343) them!) t. 6. 	5:1d () 4,202 (	0:18:	85:38:	65:10	sub		10	0. 5	eq 92	06233
In US In 40 500 70 80 90 80	16 14 bernet ernet ton si dat ag igent sub-as leques bysup friow 66 2 55 a 31 7 00 0 00 0 05 a b 06 a b	t 11, t Pro ladr ladr addr addr addr addr addr time t 1 0 00 f 00 d 00 f 00 d 00 f 00 d 00 d 00	, Sri otoc att P vers to: ress to: ress to: sato 00 00 00 00 00 00 00	c; Son ol, So notoc: ion: 1 o er: 9; 26853- ic: 0 00 02 00 02 00 4c 00 3c 45 00 cf b0	1 cval c: 66 1 se 08218 6 1 ease 00 0 00 0 00 0 00 0 00 0 00 0 00 0 00	   	8:89 184.10 1:10. 1.2.2 1.2.2 1.2.2 1.2.2 1.0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	eo (e6 24 (10 0) 0) 00 00 10 00	161:0 .186 24), 160 100 100 100 100 100 100 100	c:18: 184.1 Dst P 14 6a 00 c0 00 00 3f 13 05 fc c8	to di 0 0 0 0 0 0 0 0.	st: 6 243 () ssect	e11_38:1 6.186.18 6343) then!) 	5:10 () 4.202 (	0:18:	85:38:	65:10	sub		: 10	0. 5	eq 92	
In US In 40 50 60 70 80 90 80 90	16 14 berneternet ernet ar bai dat agent soub-au tequer variant friow 66 2 55 a 31 7 00 0 5a b 03 b	t 11, t Prot addr pent f time f v 2 200 t 00 t 00 t 00 t 00 t 00 t 00 t 0	, Sr otoc at P vers ID: numb : 45 sato 00 00 00 00 00 00 00 00 00	c: Son ol, Se rotos: 1 on: 1 c: 10.1 0 er: 92 c:	1 CWA1 C: 66 1 2 .2, 20 08218 6 1 ease 00 0 00 0 0	    	8:89 184.11 1:10 1.2.2.2 1.2.2.2 1.2.2.2 1.2.2.2 1.2.2.2.2	80 (66 24 (10 0) contr 10 0 10 0 10 0 10 0 10 0 10 0 10 0 10	(b1;) (b1;)(	c:18: 184.1 pst P st code 14 6a 00 co 00 00 3f 13 65 fc 16 c8 00 00	to di 0.100 0.0000 0.000 0.00000 0.000000	ssect	ell_38;t 6.186,18 6343) them:) t. 	5:10 (( 4,202 )	0:18:	85:38:	65:10	sub		: 10	0. 5	eq 92	
100 100 100 100 100 100 100 100 100 100	16 14 berne erne tron sk dan sk dan sk dan sk dat ag gent sequen sy upsa from sy upsa from sy upsa from sy upsa from sy upsa from sk dat ag gent from sk dat ag sk dat ag sk dat ag sk dat ag sk dat ag sk dat sk dat ag sk dat ag sk sk dat ag sk sk sk sk dat ag sk sk sk sk sk sk sk sk sk sk sk sk sk	t 11, t Prot addr addr pent time t 100 t 00 f 00 f 00 f 00 f 00 f 00 f 00 f	, SF otoc an P ver's ress ress ress sano 00 00 00 00 00 00 00 00 00 00 00 00 00	c; Son ol, So notoc: ion: 1 o er: 9; 26853- ic: 0 00 02 00 02 00 4c 00 3c 45 00 cf b0	1 CWA1 C: 60 1 2 2,20 08218 6 1 ease 00 0 00 0 0 00 0 00 0 00 0	_0c:1) .186.: c Port (10.: c vrit) 0 00 0 00 0 00 0 00 0 00 0 00 0 00 0	8:89 1:84,11 1:10, 1:2,2 1	eo (e6 24 (10 0) 0) 00 00 10 00	1801:0 186 24), 186 24), 186 24), 186 24), 190 190 10 10 10 10 10 10 10 10 10 10 10 10 10	c:18: 184.1 pst P st code 14 6a 00 co 00 00 3f 13 65 fc 16 c8 00 00	to di 0.100 0.0000 0.000 0.00000 0.000000	ssect	e11_38:1 6.186.18 6343) then!) 	5:10 (( 4,202 )	0:18:	85:38:	65:10	sub		: 10	0. 5	92	0823

"NetFlow is much more accurate for IP statistics however, sFlow is more than a substitute for NetFlow. It offers many more statistics than NetFlow does. Flexible NetFlow looks to take smart ideas from sFlow like sampling packets."

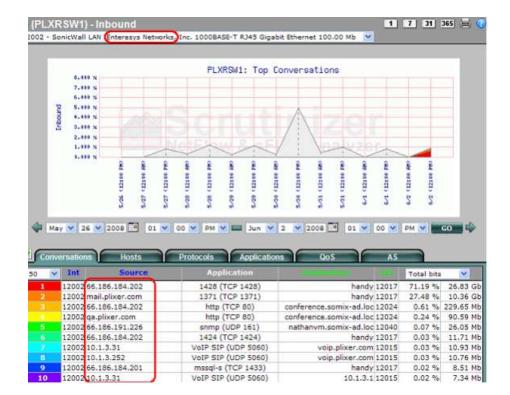


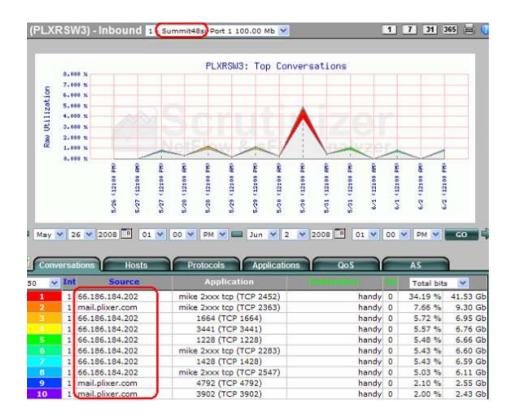
Marc Bilodeau - CTO, Plixer International, Inc.

#### **Historical Differences**

One would think that even with sampling that, statistically, the same top talkers would result with either technology over time and they didn't. Below is based on a 6 day trend on both switches. Although the overall interface utilization trends look the same, the top hosts were inconsistent:

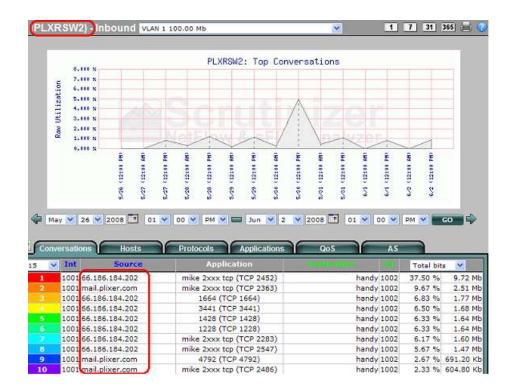








After comparing the first two switches reporting on the same traffic and seeing inconsistent top 10 host results, plixer decided to review sFlow from a 3rd switch (i.e. the backup plan) looking at the same traffic. The 3rd switch made by Alcatel PLXRSW2 was sampling at a much lower rate, but the top ten hosts were consistent with the Extreme sFlow switch:



# Conclusion

Both technologies have their benefits. Because of the cost involved with engineering NetFlow on a switch and the readily available sFlow chips from Inmon, sFlow is the prevailing technology on switches. On routers, NetFlow seems to be the more popular technology.

In extremely high traffic volume environments, sampling is the only alternative as no collector can handle the volume of flows generated by even a single router. Even Cisco recommends sampling albeit with NetFlow v9.



## **Related Articles:**

Cisco toe stepper HP ProCurve deftly hoofs over Cisco NetFlow http://www.networkworld.com/community/node/23982

Cisco's NetFlow vs. Inmon's sFlow: Which will prevail? http://www.networkworld.com/community/node/22667

NetFlow or sFlow: which is the open standard? http://www.networkworld.com/community/node/23739