

NetFlow Analytics for Splunk

User Manual

Version 3.5.x

March, 2016

Contents

Introduction	3
Overview	
Installation	0 4
Installing into a Single Solunk Server	4
Sten 1	6
Step 2	6
Installing into a Distributed Solunk Environment	0
Configuring Indexers	7
Configuring Universal Forwarders with NFI	<i>i</i>
Configure Universal Forwarder Output (Target Indexers)	0
Configure Universal Forwarder Input	0 Q
Receiving Systems Directly from NFI	0 9
Configuring Universal Forwarder with systog-ng or rsystog	9
Administration	10
Devices and SNMP polling	10
List of Devices	10
SNMP Integration	10
Configuration	10
Configuring Hunk 6.2	. 10
Dashboards	
Access the App NetFlow Analytics for Splunk	. 11
Default Dashboards	. 11
Dashboards navigation overview	. 12
Dashboard overview	. 12
NetFlow Logic > Traffic Overview dashboard	. 13
Bandwidth by Hosts	. 13
Traffic by Source IP dashboard	.13
Traffic by Destination IP dashboard	.14
Traffic by Protocol and Port	. 15
Traffic by Host Pairs dashboard	.15
Reports	. 16
Traffic by Subnets dashboard	. 16
Traffic by Protocol dashboard	. 17
Connections dashboards	. 18
Bandwidth by Network Devices	. 18
Top Devices by Traffic dashboard	. 18
Top Devices by Packet Rate dashboard	. 19
Interfaces Utilization dashboard	. 19
Watched Interfaces Utilization dashboard	.19
Interface Groups dashboard	.20
Services	. 20
Service Response Time dashboard	.20
Asset Access Monitor	.20

Security Events	21
Cyber Thread Statistics dashboard	21
DNS Security dashboard	22
Supplemental Traffic Statistics	22
TCP Health	22
GEO IP Monitor dashboard	22
Traffic by Autonomous Systems dashboard	23
Traffic by CBQoS dashboard	23
Search dashboard	24
Cisco ASA Monitor	24
Cisco Overview	24
Cisco Top Bandwidth Consumers	24
Cisco Top Destinations	25
Cisco Top Violators	25
Cisco Top Connectors	25
Palo Alto Networks	25
Palo Alto Networks Overview	25
Palo Alto Networks Top Bandwidth Consumers	25
Palo Alto Networks Top Destinations	26
Palo Alto Networks Top Violators	26
Palo Alto Networks Top Connectors	26
Top Applications	26
Top Applications and Users	26
Resources	27
FAQ	27
Getting help	27

Introduction

Overview

NetFlow Analytics for Splunk App is designed to deliver next generation, real-time, network resource management power to network and security analysts. NetFlow Integrator™ ("NFI") is a middleware that processes massive amount of flows to stream summarized and meaningful CIM ("Common Information Model") compliant syslog events into Splunk Enterprise, and, optionally, all original flow records to Hunk. The events are available for immediate indexing and correlation. NetFlow for Splunk App ("App") provides visualization and reporting capabilities. The operators benefit from detailed visibility to their entire network and being able to address many IT use cases including bandwidth monitoring, capacity planning, congestion troubleshooting, and cyber security using threat intelligence lists.

The App also includes Cisco ASA and Palo Alto Network firewall flow data dashboards which present bandwidth usage, users, applications, and violators etc, enabling the continual reinforcement of firewall policies.

This guide is intended for network and security analysts who use the App to monitor and investigate problems. For additional NFI information please visit <u>www.netflowlogic.com</u>.

Installation

App Indexes

NetFlow Analytics for Splunk App creates the following indexes during the installation and operation:

- 1) flowintegrator the main index for syslogs sent by NetFlow Integrator
- 2) flowintegrator_exp_ips a summary index which contains exporter IPs for populating Device drop-down
- 3) flowintegrator_pct_of_total a summary index filled with data to speed up calculations of "% of Total" fields on the dashboards

Pre-installation Steps

- 1) Download Technology Add-on for NetFlow from Splunkbase https://splunkbase.splunk.com/app/1838/
- 2) Download NetFlow Analytics for Splunk from Splunkbase https://apps.splunk.com/app/489/

Installing into a Single Splunk Server

 Depending on the OS of the server that is running Splunk, follow the installation recommendations from the Splunk website to install **both** Technology Add-on and NetFlow for Splunk application. Restart Splunk after installing the App.



2) Launch the App

splunk>	App: Search & Reporting \vee		Administrator \sim	Messages 🗸	Settings \backsim	Activity ~	Help \vee	Find
	App cor	figuration						
	The "NetFlo	w Analytics for Splunk" a	app has not been fully configu	red yet.				
	This app ha properties r	s configuration propertie nay or may not be requir	es that can be customized for ed.	this Splunk inst.	ce. Dependin	g on the app, t	hese	
					Conti	nue to app set	up page	

3) The first time you run the app from the web UI, you will be presented with a setup screen:

splu	unk> Apps ~	Administrator \sim	Messages \vee	Settings \sim	Activity \sim	Help \sim	Find
ne	tflow						
	Let's Get Started						
	Welcome to the Splunk App by NetFlow Logic!						
	If you need to alter the index, please follow these steps:						
	1. Create directory \$SPLUNK_ROOT/etc/apps/netflow/local/ if it doesn't e	xist					
	2. Create file \$SPLUNK_ROOT/etc/apps/netflow/local/macros.conf with f	ollowing lines:					
	<pre>[netflow_index] definition = index=your_index sourcetype=flowintegrator</pre>						
	3. Save \$SPLUNK_ROOT/etc/apps/netflow/local/macros.conf and restart	Splunk to changes take	effect				
	You can setup this app by following the steps below. Once you have reviewed	ed the setup steps, click	on the "Enable" but	tton.			
	Step 1						
	This App relies on NetFlow Integrator software. To download a free trial of N	NetFlow Integrator, pleas	e visit https://www	v.netflowlogic.co	m/downloads/	-	
	Step 2						
	Get more value out of NetFlow by enabling additional inline analytics in Net	Flow Integrator and enab	ling the correspon	ding Splunk App	panels under S	Settings > Co	nfiguration.
	Ready to continue or already have NetFlow Integrator software installed? Cl	ick on the "Enable" butto	n below.				
	questions or need assistance? We are here to help!						
	Enable						

If you need to alter the index, please follow these steps:

- a) Create directory \$SPLUNK_ROOT/etc/apps/netflow/local/ if it doesn't exist
- b) Create file \$SPLUNK_ROOT/etc/apps/netflow/local/macros.conf with following lines:

```
[netflow_index]
definition = index=your index sourcetype=flowintegrator
```

c) Save \$SPLUNK_ROOT/etc/apps/netflow/local/macros.conf and restart Splunk to changes take effect

You can setup this app by following the steps below. Once you have reviewed the setup steps, click on the "Enable" button.

NetFlow Analytics for Splunk App User Manual

NetFlow Logic Confidential

Step 1

This App relies on NetFlow Integrator software. To download a free trial of NetFlow Integrator, please visit <u>https://www.netflowlogic.com/download/</u> and don't forget to register to receive trial key.

Step 2

Get more value out of NetFlow by enabling additional inline analytics in NetFlow Integrator and enabling the corresponding Splunk App panels under Settings > Configuration.

Application > And/ memory in a spalan in y memory cognition > Application > Applicatio		NetFlow LOGIC
Configuration	Edit ~ More Info ~	1.0
Step 2 Get more value or of NetFlow by enabling additional intere analytics in NetFlow Integrator and enabling the conseponding Splank App panels below. Place a checkbox for the selected panel and click on the "Saw" button below. Optor Thread Databoard Settings Image: Databoard Settings Image: Databoard Settings This stationard drows cyber Thread Databoard This stationard drows cyber Thread Databoard 1:0005 Democratic Command and Construction 0:0005 Democratic Command and Construction 1:0005 Democratic Democratic Detection 1:0005 Democratic Democr		
Clace ASA Monitor Settings Clace ASA Monitor Distributions Enable Clace ASA Monitor Distributions Enabled Clace ASA E		
Palo Alto Networks Settings Image Palo Alto Networks Dashboerds NetFlow inters are based on NetFlow data produced by Palo Alto Networks devices and converted to systig messages by 2nd party software - NetFlow Integrator. These dashboards who wattic based on Palo Alto Networks devices. Make sure you have the following Modules enabled. • Enable NetFlow Integrator Palo Alto Networks Modules (1000 mrough 1005) and Converter (2003)		
Network Treffic by CBQoS Settings © Enable DNS Security Dashboard This dashboard shows an average response time and top 10 users of each monitored DNS server. Make sure you have the following Module enabled: • 10004. DNS Monitor		
GEO IP Monitor Settings I Monitor Databased This distributed shows geographical locations of monitored hosts, and traffic statistics. Make sure you have the following Module enabled. I toldH Host Geographical Locations Monitor		
Asset Access Monitor Settings Image Asset Access Monitor Settings This Asset Access Monitor Dashboard This dashboard shows traffic from unautorized users to services (IP address, destination port, protocol) configured in the corresponding NFI Module. Make sure you have the following Module enabled and configured: • 10014. Asset Access Monitor		
TCP Health Settings I Enable TCP Health Gashboard This databloard dhows top houst TCP Resets. Make sure you have the following Module enabled 10005 TCP Health		
Wetched Interfaces Ig: Enable Watched Interfaces Utilization Dashboard Drate watched interfaces Utilization dashboard (see watched-interfaces on sample), when management, pris the management, pris the management prison and the device		
Interface Groups © Enable interface Groups Dathbard Orace interface-groups can be the interface focups dathbard Specify interface groups to view the aggregated traffic for grouped interfaces (see interface-groups cox sample), where management_p. It is the mane of the interface (neceed from SAMP poling) It groups is the mane of the interface belongs		
Devices, Management IPs, Device Groups Torse exponters-devices control for the management IPs to export IPs, and to groups devices (see exponters-devices control exponter) exp_0 is the management. Ps in the device the export IPs and to groups devices (see exponters-devices control exponter) management. Ps is the management IP address of the device the same as exp_0 if the device doesn't have extual immagement IP in device.group is the management IP address of the device the same as exp_0 if the device doesn't have extual immagement IP in device.group is the management IP address of the device belongs (this field is optional, input "" without quotes if the device shouldn't belong to any group) Tome		
https://lub.netflowlogic.com/8001/an-US/appinetflow/configuration/earliests/08statests#	© 2005-2015 Splunk Inc. All	rights reserved.

Installing into a Distributed Splunk Environment

If you have Splunk distributed environment (separate search heads / indexers / forwarders), install **both** Technology Add-on and NetFlow for Splunk App on Search Head. Install Technology Add-on on Indexers.



Install NetFlow Integrator (and optional syslog-ng or rsyslog) with Universal Forwarder.

Configuring Indexers

Make sure your Indexers are enabled to receive data from Universal Forwarder:

- 1. Log into Splunk Web as admin on the Indexer that will be receiving data from a forwarder
- 2. Click the Settings link at the top of the page
- 3. Select Forwarding and receiving in the Data area
- 4. Click Add new in the Receive data section
- 5. Specify which TCP port you want the receiver to listen on. Default value is 9997
- 6. Click Save. You must restart the instance to complete the process

Configuring Universal Forwarders with NFI

Configure Universal Forwarder Output (Target Indexers)

During the installation of the Universal Forwarders a Receiving Indexer can be configured, as it can be seen here:

🗒 UniversalForwarder Setup									
splunk>universal forwarder									
If you intend to use a Splunk receiving indexer to config specify the host or IP, and port (default port is 9997). T UniversalForwarder needs either a deployment server or anything. Receiving Indexer Hostname or IP	ure this UniversalForwarder, please his is an optional step. However, r receiving indexer in order to do								
10.1.0.100	: 9997								
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com	default is 9997								
Cancel	Back Next								

It is an optional step during the installation. If it was not configured or if load balancing is required, additional Receiving Indexers can be added later by adding to the %SPLUNK_HOME%/etc/system/local/outputs.conf file:

[tcpout]

defaultGroup = default-autolb-group

[tcpout:default-autolb-group]

server = 10.1.0.100:9997,10.1.0.101:9997

Restart Splunk Universal Forwarder

With a setup like this, load balancing is configured, the events are sent to 10.1.0.100:9997 and 10.1.0.101:9997

More info about load balancing:

http://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Setuploadbalancingd#How_load_balancing_works

Configure Universal Forwarder Input

The inputs can be configured in the following file:

%SPLUNK_HOME%/etc/system/local/inputs.conf

In general there are two options, either to listen directly for netflow events on a specific port or optionally to monitor files created by syslog-ng or rsyslog.

Receiving Syslogs Directly from NFI

inputs.conf file example (NFI sends data on a UDP port 10514):

[udp://10514]

sourcetype = flowintegrator

index = flowintegrator

Configuring Universal Forwarder with syslog-ng or rsyslog

In this scenario syslog-ng or rsyslog are configured to listen to syslogs sent by NFI on a UDP port 10514. Syslog-ng or rsyslog are usually writing the logs into configurable directories. In this example we assume that those are written to /var/log/netflow.

inputs.conf file example (NFI sends data on a UDP port 10514 to syslog-ng or rsyslog):

[monitor:///var/log/netflow]

sourcetype = flowintegrator

index = flowintegrator

N.B. It is very important to set sourcetype=flowintegrator and to point it to the index where Netflow Analytics for Splunk App is expecting it.

Administration

Under Settings you may find additional information about various options and configuration of the App.

Devices and SNMP polling

List of Devices

List of devices feature is introduced to improve performance of the App. Every 30 minutes a job runs to populate a summary index "flowintegrator_exp_ips", which is used to populate Device IP drop down on various dashboards in the App.

SNMP Integration

NetFlow records contain very limited information about network devices and interfaces. This application takes advantage of SNMP information provided by NFI special Module – SNMP Information Monitor, which poles the following information from network devices: device name, name of interfaces and their speed. Once this information is obtained by polling network devices, % of utilization of interfaces is computed and displayed to the users on the application dashboards.

Make sure that NFI SNMP Information Monitor Module is enabled.

Configuration

This screen allows you to enable additional dashboards in the App, and contains description of NFI Modules that need to be enabled to feed data to corresponding dashboards.

Configuring Hunk 6.2

1. In Hunk Web, select Manager > Virtual Indexes in the menu bar.

2. Click the Provider tab (if it is not already selected) and click New Provider.

3. Fill in the following fields:

Name – any string Java Home - /usr/lib/jvm/jre-1.7.0 Hadoop Home - /opt/Hadoop Hadoop Version – Hadoop 2.x (Yarn) File System – hdfs://%HDPIP%:8020 Resource Manager Address - %HDPIP%:8050 Resource Scheduler Address - %HDPIP%:8030 HDFS Working Directory - /user/root/splunkmr

4. Select Manager > Virtual Indexes in the menu bar.

5. Click the Virtual Index tab (if it is not already selected) and click New Virtual Index.

6. Fill in the following fields:

Name – any string Paths - /user/flume/netflow-syslog

7. Click Save to save your index and return to the Virtual Indexes page.

Dashboards

Access the App NetFlow Analytics for Splunk

This guide assumes that Splunk v6.x and NetFlow Analytics for Splunk App v3.5 have been installed on your organization and that you have been assigned a Splunk username and password. It also assumes that NFI and the App have been set up and configured. Contact your system administrators if they have not.

1. Log onto Splunk Web using your Splunk username and password.

2. Click on Splunk Home and click the NetFlow Analytics for Splunk App. You will see the Overview page. The Overview page presents a summary of your network. You can customize any dashboard. See Default Dashboard section.

3. Use the Hosts, Network Devices, Services, Security Events, Other Traffic Statistics, Cisco ASA Monitor, Palo Alto Network dashboards for detailed investigation, filtering and drill-downs.

All dashboards in this App are based on Splunk Web Framework using simple XML. Refer to <u>http://docs.splunk.com/Documentation/Splunk/latest/Viz/WebFramework</u> for an overview of Dashboards and Visualization.

Default Dashboards

When you install and enable the App, several dashboards are available by default. All these dashboards are based on data sent to Splunk by NFI Module 10067: Top Traffic Monitor. They are:

```
NetFlow Logic > Traffic Overview
Bandwidth by Hosts > Traffic by Source IP
Bandwidth by Hosts > Traffic by Destination IP
Bandwidth by Hosts > Traffic by Protocol and Port
Bandwidth by Hosts > Traffic by Protocol
Bandwidth by Hosts > Reports
```

```
Bandwidth by Network Devices > Top Devices by Traffic
Bandwidth by Network Devices > Interface Utilization
Search > Traffic Timeline
Settings
```

You can get more value out of the App by enabling additional dashboards. Go to Settings > Configuration, and place a checkbox for the selected dashboards. Please make sure that the corresponding NFI Modules are enabled and configured. Here are some of the dashboards you will be able to enable.



Dashboards navigation overview

The application navigation bar is displayed toward the top of the UI and offers drop-down menus.

splunk> App: NetFlow for Splunk by NetFlow Logic ~					
NetFlow Logic \sim Bandwidth by Hosts \sim Bandwidth by Network Devices $$ Services $$ Security Eve	nts \checkmark Supplemental Traffic Statistics \checkmark Search \checkmark Settings \checkmark				
Traffic Overview	TCP Health				
Device group Device Time Range	GEO IP Monitor				
* 🛛 v * 🕲 v Last 60 minutes 🗸 Submit	Traffic by Autonomous Systems				
	Network Traffic by CBQoS				
Update Device list					

Dashboard overview

Every dashboard has different filters at the top of the screen to enable further narrowing of the report. For example, the Traffic by Protocol and Port dashboard can be filtered by the device group, device, source IP/mask, destination IP/mask, protocol, source port, destination port, source DSCP, destination DSCP, input and output interfaces, and time range.



Please note that source and destination IP/mask filters could be specified as subnets (IP/mask), as full IP addresses (199.45.1.45), or as a partial IP address (199.45.1.*).

NetFlow Logic > Traffic Overview dashboard

The Overview dashboard is the top view, aimed to provide a summary on traffic over a time period. The views can be filtered by the Device Group, Device and Time Range.

The panels show Top Traffic by Source IP, Top Traffic by Destination IP, Top Traffic by Protocol and Port, Top Traffic by Protocol, Top Traffic by Protocol, Top Devices by Traffic, Top Interfaces by Traffic by Device.



Bandwidth by Hosts

This section covers the dashboards and reports for monitoring traffic to and from hosts in your network, such as top talkers, top listeners, top host pairs, and many others.

Traffic by Source IP dashboard

The Traffic by Source IP dashboard (a.k.a. Top Talkers) monitors host which generate most traffic in your network. It is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic speed and volume, as well as packet rate and connections generated by each host.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Traffic by	Sourc	e IP													Edit 🗸	More Info 🗸 🛓 🗸
Device group		Device	Source IP/mask	Destination IP/mask	Protocol	Src. Port	Dest. Port	Src. DSCP	Dest. DSCP	Input Int.	Output Int.	Time Range				
All devices	0 -	All 🔘 🔹	•		•			•	•			Last 60 minutes	✓ Subm	uit .		
Traffic by S	ource IP															
20															199.45.0.18 (httf=ct01=	he hatf interne eat)
20															199.45.8.138 (sfo-isr01	enet.interop.net)
56 J											~				199.45.8.141 (sfo-lb-bi	gip1nteropnet.enet.interop.net)
							5								199.45.8.214 (vmw-sfo	vc01.enet.interop.net)
		12:40 PM		12:50 PM		1:00 PM			1:10 PM			1:20 PM	× .	1:30 PM	199.45.8.242 (NAME_NO	T_FOUND)
		Mon Sep 22													199.45.8.253 (NAME_NO	T_FOUND)
		2014				Tim									1/2	
9 1 1 0																
Source IP :		Source Host		Device 0	Average T	roffic Rate (To	tal Traffic)		Tre	ffic Line 🌣			Averane Park	et Bate (Total Packets)		Connections 0
45.0.2.70		NAME NOT FOUND		100.45.9.46	2.49 Mbo	e(1.04.CP)	tai manity -			and three to	~ ^~~		222 ppc/920 i	590)		920600
199.45.0.18		hstf.cr01.bn.bstf.interon.net		109.45.8.46	1.71 Mbr	(733 56 MR)			~	~~~~~		~	426 pps(059)	1.904)		1531004
199.45.8.195		NAME NOT FOUND		199.45.8.46	670.93 KP	ns/288 25 MR			14		40.44		62 nps(221 1)	R4)		221184
199 45 8 138		sfo-isr01 enet interon net		199.45.8.46	631 85 Kt	IOS(271 45 MR)		V	man	~~~~		69 pps(245 76	50)		245760
199.45.8.245		NAME_NOT_FOUND		199.45.8.46	413.65 Kt	ps(177.71 MB)			han	<u>л</u>		47 pps(167,93	36)		167936
199.45.8.214		vmw-sfo-vc01.enet.interop.net		199.45.8.46	367.06 Kt	ps(157.70 MB)			m		A.	37 pps(131,07	72)		131072
199.45.8.242		NAME_NOT_FOUND		199.45.8.46	345.14 Kt	IDS(148.28 MB)			man			39 pps(139,26	54)		139264
199.45.8.141		sfo-lb-bigip11-interopnet.enet.i	nterop.net	199.45.8.46	327.74 Kt	ps(140.81 MB)		-^	-1-1		_	36 pps(126,9)	76)		126976
199.45.8.253		NAME_NOT_FOUND		199.45.8.46	266.98 Kt	ps(114.70 MB)		~	mm	m	~	130 pps(466,9	944)		466944
199.45.8.146		sfo-services-vip-f5.enet.interop	o.net	199.45.8.46	256.63 Kt	ps(110.25 MB)		N	w-1			28 pps(98,304	4)		98304
														« prev 1 2	3 4 5 6	7 8 9 10 next »
9+10																
-210																

The Traffic by Source IP dashboard allows viewing talker traffic details – just click on the talker host IP or name, and drill down panel opens below showing all traffic destinations, including ports, network device interfaces, and traffic and packet rate details.

Traffic by Destination IP dashboard

The Traffic by Destination IP dashboard (a.k.a. Top Listeners) monitors host which receive most traffic in your network. As Traffic by Source IP, it is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic speed and volume, as well as packet rate and connections received by each host.



The Traffic by Destination IP dashboard allows viewing listener traffic details – just click on the listener host IP or name, and drill down panel opens below showing all traffic sources, including ports, network device interfaces, and traffic and packet rate details.

Traffic by Protocol and Port

The Traffic by Protocol and Port dashboard monitors traffic in your network by Service Name and Transport Protocol Port Number (a.k.a Destination port). The App is packaged with services.csv lookup file, which is used to display the service name and protocol, according to IANA:

(http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml).



Traffic by Host Pairs dashboard

The Traffic by Host Pairs dashboard shows consolidated **bidirectional** flows, sorted by traffic volume. You need to enable Module 10064: Top Pairs Monitor in order to see data in this dashboard. The Traffic by Host Pairs dashboard contains a timeline panel showing top 10 host pairs' traffic by volume, and the table showing top 100 host pairs with details, such as traffic volume and speed, packet rate, and connections count.

10000000000	y Host Pairs						Edit ~ More I	nto 🗸 🛓 🕯
rice group	Device	Server IP/mask	Client IP/mask Protocol	Time Range				
I devices	0 * Al 0 *		•	Last 60 minutes v Subm	a -			
Top 10 Hor	st Pairs							
sdqW	12.40 PM	12:50 PM	1:00 PM	110.04	1:20 PM	1:50 PM	154-J5.175.201 (undern2.7 170.178.191.18 (HAME276 199.45.8.174 (HAME_277 5.101.140.198 (HOT.J.) 5.101.140.198 (HOT.J.) 72.165.86.42 (Interparte82 94.125.182.255 (Hou at0.2.)	0 NAME_NOT_FOUND (NAME_NOT_FOUND) 01-hp.hatf.interop.net 0 (NAME_NOT_FOUND 3 (NAME_NOT_FOUND 0 (NAME_NOT_FOUND
	Mon Sep 22 2014	12.007	1.500 PM	Time	1.59 m	1.10 PM	55.69.246.66 (p=95-69-246-	sfo-isr01.enet.intero
9 1 1 0	b			Average Traffic Rate (Total Traffic)	Average Traffic Rate (Total Traffic)	Average Packet Rate (Total Packets)	Average Packet Rate (Total Packets)	
R ± I €	Server :	Server port	Client :	Average Traffic Rate (Total Traffic)	Average Traffic Rate (Total Traffic) Outbound 0	Average Packet Rate (Total Packets)	Average Packet Rate (Total Packets) Outbound :	Connections :
Q ± / € Device : 199.45.8.46	Server 0 199 45.0.18 (hstf-cr01-hp hstf interop.net)	Server port = 40000/udp (safetynetp)	Client : 199.45.8.174 (NAME_NOT_FOUND)	Average Traffic Rate (Total Traffic) Infound : 0 bps(0 Bytes)	Average Traffic Rate (Total Traffic) Outbound 3 824.45 Kbps(357.16 MB)	Average Packet Rate (Total Packets) Inbound 0 0 pps(0)	Average Packet Rate (Total Packets) Outbound : 212 pps(758,000)	Connections 768001
Device : 199.45.8.46 199.45.8.46	Server : 199 45 0.18 (httf-cr01-tip httf interop net) 199 45 8 138 (sto-iar0) enet interop net)	Server port : 40000/udp (safetynetp) 3389/tcp (ms-wbt- server)	Client : 199.45.8.174 (NAME_NOT_FOUND) 95.69.246.66 (i)p-35-69-246-56 airbites.net.ua)	Average Traffic Rate (Total Traffic) Inbound = 0 bps(0 Bytes) 2.39 Kbps(1.03 MB)	Average Traffic Rate (Total Traffic) Outbound © 824.45 Kbps(357.16 MB) 311.32 Kbps(134.87 MB)	Average Packet Rate (Total Packets) Inbound 0 0 pps(0) 7 pps(22,528)	Average Packet Rate (Total Packets) Outbound : 212 pps(768,000) 30 pps(106,496)	Connections 76800 12902
C + 1 C Device : 199.45.8.46 199.45.8.46	Server : 199.45.0.18 (httf-c01-tp:httf:interop.net) 199.45.0.18 (stof-su01 and:interiop.net) 199.45.8.245 (NAME_NOT_FOUND)	Server port 5 40000/udp (safetynetp) 3389/tcp (ms-wbt- server) 3389/tcp (ms-wbt- server)	Client : 199.45.8.174 (NAME_NOT_FOUND) 55.60.246.66 (p=5459-2456.66 airbites.net.ua) 95.60.246.66 (p=5569.246.66 airbites.net.ua)	Average Traffic Rate (Total Traffic) Inhound © D bps(D Bytes) 2.39 Kbps(1 03 MB) 5.77 Kbps(2.50 MB)	Average Traffic Rate (Total Traffic) Outbound © 824.45 Ktops(357.16.MB) 311.32 Ktops(134.87.MB) 204.94 Ktops(88.78.MB)	Average Packet Rate (Total Pickets) Inbound : 0 pps(0) 7 pps(22,558) 10 pps(22,768)	Average Packet Rate (Total Packets) Outbound 1 212 pps(748,000) 30 pps(106,496) 23 pps(81,920)	Connections 76800 12902 11468
Q ± 1 C Device : 199.45.8.46 199.45.8.46 199.45.8.46	Server : 199 45.018 (hotf-c01-tp.hstf.interp.net) 199 45.0.18 (hotf-c01-tp.hstf.interp.net) 199 45.0.25 (NAME_NOT_FOUND) 45.0.270 (NAME_NOT_FOUND)	Server port 5 40000/udp (safetymetp) 3389/tcp (ms-wbt- server) 3389/tcp (ms-wbt- server) 0/udp (other)	Clent : 199 45 8 17 (NAME_NOT_FOUND) 56 69 246 56 (95 567 246 66 (95 567 2	Average Traffic Rate (Total Traffic) Inbound : 0 best(0 Synes) 2.39 Kbps(1.03 MB) 5.77 Kbps(2.50 MB) 0 bps(0 Bytes)	Average Traffic Rate (Total Traffic) Outbound : 824 45 Kops(37 16 MB) 311 32 Kops(34 87 MB) 204 94 Kops(38 78 MB) 168 70 Kops(73 66 MB)	Average Packet Rate (Total Packets) inbornet 0 oper(0) 7 pex(22,528) 10 oper(0) 0 pes(0)	Average Packet Rate (Total Packets) Outbound 1 212 pps/(76,000) 30 pps/(106,496) 23 pps/(106,496) 23 pps/(15,200) 16 pps/(57,344)	Connections 76800 12902 114681 5734
Device : 199 45.8.46 199 45.8.46 199 45.8.46 199 45.8.46	Server : 199 45.018 (Inst c01-to-hast interop net) 199 45.8.138 (Inst c01-to-hast interop net) 199 45.8.245 (IAANE_NOT_FOUND) 199 45.8.242 (IAANE_NOT_FOUND) 199 45.8.242 (IAANE_NOT_FOUND)	Server port :: 40000/udg (safetynetp) 3389/tcp (ns-wbt- server) 3389/tcp (ns-wbt- server) 0/udg (other) 3389/tcp (ms-wbt- server)	Clent : 194 68 A7 (NAME_NOT_FOUND) 56 02 46 66 (p-55-59-246-66 arbites net ua) 05-56 72 46 66 (p-55-572-56 arbites net ua) 154 35 175 201 (undernet references) 05-69-246 66 (p-95-95-266 66 arbites net ua)	Average Traffic Rate (Total Traffic) Interunt 3 0 Detril Bytes) 2 39 Kbps(1 03 MB) 5 77 Kbps(2 50 MB) 0 Des(0 Bytes) 3 83 Kbps(1 66 MB)	Average Traffic Rate (Total Traffic) Outbound : 824.45 Xbpp(37-16 MB) 311.32 Xbpp(34.87 MB) 204.94 Xbpp(38.87 MB) 168.70 Kbpp(73.66 MB) 164.47 Xbpp(71.25 MB)	Average Packet Rate (Total Packets) intbornt Internet 0 oper(0) 7 pps/22,528) 10 pps/22,768) 0 oper(0) 0 pps/(0) 5 pps/(16,384) 5 pps/(16,384)	Average Packet Rate (Total Packets) Outbound 1 Outbound 1 212 popr(76,000) 30 pag1(06,496) 23 pog(15,20) 16 pog(57,344) 19 pog(05,536) 19	Connections 76800/ 12902/ 11468/ 5734/ 8192/
Q ± 1 C Device : 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46	Server : 199 4.6.0 8 (bit) c01-80 hotf merop net 198 4.8.133 (tof-sid) rest interop net 198 4.8.2.35 (NAME, NOT, FOUND) 45.0.27 (NAME, NOT, FOUND) 199 4.8.2.32 (NAME, NOT, FOUND) 45.0.27 (NAME, NOT, FOUND)	Server port = 40000/udp (safetynetp) 3389/tcp (ms-wbt- server) 0/udp (other) 3389/tcp (ms-wbt- server) 0/udp (other)	Client : 19.9 A5 17.4 (IAAME_NOT_FOUND) 56.9 246.6 66 (IP-59-67-246-66 attoles.net.ua) 56.9 246.6 6 (IP-59-67-246-66 attoles.net.ua) 10.43.3 17.5 201 (Indemit ethermholing net) 56.9 246.6 6 (IP-59-67-246-66 attoles.net.ua) 10.7 17.8 19.18 (IPAL-ROT_FOUND)	Average Traffic Rate (Total Traffic) biblioutel 0 bptil(0 ptres) 2 Jak Kbps(10 XMB) 5 77 Kbps(2 50 MB) 0 bptil(0 ptres) 3 JB Kbps(1 66 MB) 0 bptil(0 ptres)	Average Traffic Rate (Total Traffic) Outbould 0.4 824.45 K0pc(37:16 Me) 13.12 K0pc(37:16 Me) 204.94 K0pc(37:16 Me) 168.70 K0pc(73:36 Me) 164.70 K0pc(73:26 Me) 164.87 K0pc(72:26 Me)	Average Packet Rate (Total Packets) httound : Packets) 0 pps(0) 7 pps(22.528) 10 pps(0) 0 pps(0) 5 pps(15.384) 0 pps(0) 5 pps(15.384) 0 pps(0)	Average Packet Rate (Total Packets) Outcound : 212 pps(768,000) 30 pps(106,489) 23 pps(11920) 16 pps(57,344) 19 pps(65,336) 15 pps(53,248)	Connections 768001 12902- 1114681 5734 81921 5324
Q J I C Device 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46	Server : 199 4.5.0.18 (bitd c01-kp.huff.microp.net) 199 4.5.0.23 (plo-suc) met intersp.net) 199 4.5.2.45 (NAME_NOT_FOUND) 45.0.27 (NAME_NOT_FOUND) 199 4.5.2.22 (NAME_NOT_FOUND) 199 4.5.2.21 (mm ato- vot) met intersp.net)	Server port : 400001/dp (safetynetp) 3389/tp (ms-kbt- server) 3389/tp (ms-kbt- server) 01/dp (other) 3389/tp (ms-kbt- server) 3389/tp (ms-kbt- server)	Client : 19 / 4.5.174 (IAAME_NOT_FOUND) 56 / 24.6.66 (IP-55-67.24.66 at these net ua) 56 / 24.6.6 (IP-56-72.466 at these net ua) 10.143.3175.201 (Indemit ethermholing net) 56 / 24.6.6 (IP-56-72.466 das these net ua) 70.7178.19.118.404.6.017.FOUND) 96 / 66.24.6.6 (IP-55-67.246.66 at these net ua)	Average Traffic Rate (Total Traffic) biblioutel 0 bps(0 bptes) 2 38 kbps(1 00 MB) 5 77 kbps(2 50 MB) 0 bps(0 bptes) 3.83 kbps(1 66 MB) 0 bps(0 bptes) 1.10 kbps(488 kB)	Average Traffic Flate (Total Traffic) Outloom! 824.45 K0pc(37:16 Me) 31.32 K0pc(37:16 Me) 168.70 K0pc(37:36 Me) 164.70 K0pc(37:36 Me) 164.70 K0pc(37:36 Me) 164.47 K0pc(37:12 Me) 164.87 K0pc(37:16 Me) 164.87 K0pc(37:16 Me) 164.87 K0pc(37:16 Me)	Average Packet Rate (Total Packets) https://disease 0 pps(0) 7 pps(22,528) 10 pps(22,768) 0 pps(0) 5 pps(16,384) 0 pps(0) 3 pps(8,192)	Average Packet Rate (Total Packets) Outcound : 212 ppe(768,000) 30 pps(106,498) 23 pps(11920) 16 pps(57,344) 19 pps(65,336) 15 pps(53,248) 14 pps(49,152)	Connections 768000 129024 114688 57344 81920 53246 57344
Device C 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46	Server: : 199.45.018 (http://blanki.http://b	Server port : 40000.ubd (safetyneto) 338/h2p (ms-ebt- server) 338/h2p (ms-ebt- server) 0/udp (uts-ebt- server) 0/udp (uts-ebt- server) 161/udp (ump)	Client : 199.4 63 174 (NAME_NOT_FOUND) 96.6 246.6 66 (n9-55-672.466 antotes.net.ua) 96.6 246.6 6 (n9-55-672.466 antotes.net.ua) 10.453.5175 201 (noferent ethermhosting.net) 55.6 246.6 5 55.6 246.6 6 (n9-55-672.466 antotes.net.ua) 170.178.191.18 (NAME_NOT_FOUND) 96.6 248.6 6 (n9-55-472.466 antotes.net.ua) 171.218.68 44.2 (missensending.com)	Average Traffic Rate (Total Traffic) hotount : 0 bps(0 Bytes) 2,38 Kbps(1 03 MB) 5,77 Kbps(2,50 MB) 0 bps(0 Bytes) 2,88 Kbps(1 56 MB) 0 bps(0 Bytes) 1,18 Kbps(48 KB) 17,83 Kbps(7 64 MB)	Average Traffic Rate (Total Traffic) Outbound : Outbound : 82.4 45 Kbpc(557 16 MB) 311.32 Kbpc(13.487 MB) 204 54 Kbpc(13.67 MB) 104.70 Kbpc(13.06 MB) 164.70 Kbpc(17.25 MB) 104.47 Kbpc(17.25 MB) 164.87 Kbpc(72.56 MB) 11.32 X Kbpc(14.68 MB) 11.32 X Kbpc(16 MB) 11.37 Kbpc(49.25 MB)	Average Packet Rate (Total Packets) Inbound :: 0 pex(0) 7 pex(22,528) 10 ppx(22,768) 0 pex(0) 5 ppx(16,384) 0 pex(0) 3 ppx(1192) 19 ppx(27,584) 19 ppx(27,584)	Average Packet Rate (Total Packets) Outbound 1 212 popo(766,000) 30 pop(766,000) 22 popo(81,920) 16 pop(57,344) 19 pop(55,366) 15 pop(55,3248) 14 pop(41,922) 38 pop(135,168)	Connections 76800 12902 111468 5734 81920 5324 5734 20275
Device : 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46 199.45.8.46	Server :	Server port : 44000-bdp (safetynetp) 3380hdp (tra-beb- server) 3380hdp (tra-beb- server) 0/udp (cther) 3380hdp (tra-beb- server) 0/udp (cther) 161/udp (smap) 0/udp (cther)	Client : Client 1: 56 65 246 66 (1955 65 246 66 attests, not.us) 56 65 246 66 (1955 65 246 66 attests, not.us) 56 524 66 (1955 65 246 66 (1955 65 26 26 (1955 65 26) (1955 66 (1955 66 (1955 65 26) (19	Average Traffic Rate (Total Traffic) biburni 1: 0 bps(0 bytes) 2 Ja Ktops(1 00 MB) 5 77 Kbps(2 50 MB) 0 bps(0 bytes) 3 8 Kbps(1 66 MB) 0 bps(0 bytes) 1 10 Kbps(488 KB) 1 7 63 Kbps(7 64 MB) 0 bps(0 bytes)	Average Traffic Plate (Total Traffic) Ontonut 1 824.45 Kopo(587.16 MB) 31.32 Köps(34.87 MB) 264.95 Kopo(58.78 MB) 166.70 Köps(73.08 MB) 164.47 Köps(71.25 MB) 164.48 Köps(58.16 MB) 13.24 Köps(54.64 MB) 13.24 Köps(64.04 MB) 13.24 Köps(64.04 MB) 13.34 Köps(64.04 MB)	Average Packet Rate (Total Packets) httpom/d : 0 pps/0 7 pps(22,558) 10 pps(22,568) 0 pps(0) 5 pps(16,384) 0 pps(0) 3 pps(81,192) 19 pps(75,864) 0 pps(0)	Average Packet Rate (Total Packets) Outcound : 212 pp:(78,00) 30 pp:(106,496) 23 pp:(13,20) 16 pp:(5,7344) 19 pp:(65,536) 15 pp:(53,248) 14 pp:(41,152) 38 pp:(135,168) 11 pp:(132,122)	Connections 76800 12902 11468 5734 8192 5324 5734 20275 3891

Reports

Reports section contains dashboards built to be printed or exported to PDF. The following reports are available today:

- Top Talkers
- Top Listeners
- Top Host Pairs

Traffic by Subnets dashboard

The Traffic by Subnets dashboard monitors subnets specified in NFI Module 10011: Network Subnets Monitor configuration. Please refer to NetFlow Integrator User Guide for details. The Traffic by Subnets dashboard is useful for real time and historical monitoring of bandwidth utilization in specified subnets.

The dashboard shows traffic In, Out, and in Both directions. Traffic for the top 10 by traffic volume monitored subnets is shown in timeline panels. The table below shows for each subnet such details as Source IP, Traffic speed and volume by direction, as well as packet rate information.



Traffic by Protocol dashboard

The Traffic by Protocol dashboard monitors traffic in your network by transport protocol, going through each of the network devices. It is useful for real time or historical monitoring of you traffic composition. The App is packaged with protocols.csv lookup file, which is used to display the protocol name and number, according to IANA: (http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml).

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

The Traffic by Protocol dashboard allows viewing traffic details for each protocol – just click on the protocol in the table below the graph, and drill down panel opens below showing all traffic details for the selected protocol, including source and destination hosts and port numbers, network device interfaces, and traffic speed and volume, packet rate, and connections.



Connections dashboards

Traffic dashboards described in the previous sections are based on NFI Modules that consolidated flow data and report top hosts by volume (Modules 10011, 10064, 10067 – default Module). Connections dashboards are based on NFI Module 10063, which reports top hosts by the number of connections regardless of traffic volume. There four dashboards to monitor host by connections.

- Connections by Source IP
- Connections by Destination IP
- Connections by Protocol and Port
- Connections by Protocol

These dashboards contain graphs and table with traffic details similar to corresponding Traffic dashboards.

Bandwidth by Network Devices

In comparison to Host dashboards, which are host centric, the Network devices dashboards are device (routers, firewalls, VLAN's) centric, tracking the ingress and egress traffic.

Top Devices by Traffic dashboard

The Top Devices by Traffic dashboard monitors network devices with most traffic in your network. It is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic speed and volume, as well as packet rate traversing each network device.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Top Devices by Traffic						Edit 🗸 More Info 🗸 🛓 🕹
Device group Device Source	e IP/mask Destination IP/mask	Protocol Src. Port Dest. Port Src. DS	CP Dest. DSCP Time Range			
All devices 🛛 👻 All 🗔 💌 *	•	x x x x	* Last 60 min	utes v Submit		
Top 10 Devices						
so						
8						10.0.5.110
₩ 25						10.0.5.21 (GW02.nfclab) 10.0.5.22
12:50 PM	1:00 PM	1:10 PM	1:20 PM	1:30 PM	1:40 PM	10.0.5.24 (HP-E2620-48-upper)
Mon Sep 22 2014						199.45.8.45
		Time				
Device 0	Average Traffic Rate 0	Traffic Line 0		Average Packet Rate 0	Packets Line 0	
199.45.8.46	21.95 Mbps	m		6.28 Kpps	m	
199.45.8.45	808.32 Kbps	mmmmm Mm		652 pps	withheren	
10.0.5.24 (HP-E2620-48-upper)	649.15 Kbps	mann		289 pps	······	
10.0.5.21 (GW02.nfclab)	8.18 Kbps	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		13 pps	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
10.0.5.22	143 bps	MMMM		1 pps	MMMM	
10.0.5.110	58 bps	M_M_LM_M_		1 pps	M_M_L_M	
1						

The Top Devices by Traffic dashboard allows viewing network traffic details – just click on one of the devices, and drill down panel opens below showing traffic composition by each interface. Further drilldown shows traffic speed statistics (Min, Max, Average, Standard Deviation, 95th Percentile), and hosts communicating over the selected interface.

Top Devices by Packet Rate dashboard

The Top Devices by Packet Rate dashboard is similar to Top Devices by Traffic dashboard, but the network devices are sorted by packet rate rather than traffic volume. You need to enable Module 10068: Top Packets Monitor in order to see data in this dashboard.

Top 10 CVTOCUS DY 1 Clock 11 Click Extended and the second of the se	Ton Devic	res by Packet I	Rate											Ertit v More Info v 1
Device grapp Device Brunes Protocol Sc. Port Det Per Sc. DCP Det Det Per Sc. DCP Det DCP Time Range It devices Top 10 Devices Terre Device : Average Traffic faite : Traffic faite : Traffic faite : Postest faite : Poste	TOP Devic	CS Dy I doket I	late											Lon · more mo · L ·
All everys •	Device group	Device	So	ource IP/mask	Destination IP/mask	Protocol	Src. Port	Dest. Port	Src. DSCP	Dest. DSCP	Time Range			
Top 10 Devices 10 10 100.5110 100.5110 10 100.5110 100.5110 100.5110 100.521 (0002.rds8b) 100.522 100.522 100.522 100.52 (0002.rds8b) 100.5110 100.521 (0002.rds8b) 100.522 100.52 (0002.rds8b) 100.52 100.523 (0002.rds8b) 100.523 (0002.rds8b) 100.52 (0002.rds8b) 100.52 100.52 (0002.rds8b) 100.52 (0002.rds8b) 100.52 (0002.rds8b) 100.752 (0002.rds8b) 100.52 (0002.rds8b) 100.52 (0002.rds8b) 100.52 (0002.rds8b) 200 (1002.rds8b) 200 (1002.rds8b) 100.52 (0002.rds8b) 100.52 (0002.rds8b) 200 (1002.rds8b) 100.rds8b 100.rds8b 100.52 (0002.rds8b) 200 (1002.rds8b) 100.rds8b 100.rds8b<	All devices	O • All	• •		•	•	•	•	•	•	Last 60 minutes	 Submit 		
Top 10 Devices Image: Spin Spin Spin Spin Spin Spin Spin Spin														
Image: Second	Top 10 Devi	ces												
Image: Second	10													
B I	~													10.0.5.110
Is 25 PM bit 25 OPM 2014 Is 00 PM Is 10 PM Is 20 PM Is 30 PM Is 30 PM Is 20 PM 2014 Is 00 PM Is 20 PM Is 20 PM Is 30 PM Is 30 PM Device : Average Traffic Rate : Time Time Is 30 PM	d 5									_				= 10.0.5.21 (GW02.nfclab)
I 25 0FM Mos 5g 22 2014 I 30 PM														10.0.5.22
Mos Sep 22 2014 Ime 199-35.8-5 [199-35.8-6] Device : Average Traffic Rate : Tarfic Line : Average Packet Rate : Packets Line : Device : Average Traffic Rate : Tarfic Line : Average Packet Rate : Packets Line : 199-458.45 10.73 Mogs		12:50 PM		1:00 PM		1:10 PM			1:20 P	м		1:30 PM	1:40 PM	10.0.5.24 (HP-E2620-48-upper)
Time Time Device : Average Traffic Rate : Traffic Time : Average Traffic Rate : Packets Line : Packets Line : 199.458.46 107.73 Magis		Mon Sep 22 2014												199.45.8.45
Device : Average Traffic Rate : Traffic Line : Average Packet Rate : Packets Line : 199.458.86 10.72 Mitps 3.10 Kips								Time						
Device : Average Traffic Rate : Traffic Line : Average Packet Rate : Packets Line : 199.458.46 10.73 Mps 3.10 Kpps														
Device : Average Traffic Fate : Traffic Line : Average Packet Rate : Packet Line : 199.45.8.66 18.72 Mpc 31.0 Kpps 31.0 Kpps														
Decic: Average Traffic Rate : Traffic Life : Average Traffic Rate : Protest Life : 199.458.46 10.77 Mbps 310 Kpps														
19458.45 197.21Mgs 3.10 kgss 19458.45 287.01 kgss 3.10 kgss 19458.45 287.01 kgss 3.22 gps 105.52 kftps: 144 pps 105.52 kftps: 144 pps 105.52 kftps: 144 pps 105.52 kftps: 13 pps 105.52 kftps: 0.000 kftps: 105.55 kftps: 0.000 kftps: 105.55 kftps: 0.000 kftps: 105.55 kftps: 0.000 kftps: 105.55 kftps: 0.000 kftps: <	Device 0			Average Traffic	c Rate 0	Trai	ffic Line 0				Aver	age Packet Rate 🌣	Packets Line 0	
199.458.45 298.70 Kbps 223.pps Vm/Vm/Vm/ 100.524 (PF Z502)-48-upper) 320.45 Kbps 144.pps Vm/Vm/Vm/ 100.521 (WW2.niclub) 8.04 Kkps Vm/Vm/Vm/ 13 pps Vm/Vm/Vm/ 100.510 (W2.niclub) 229 ps 0.46 A A A A 1 tops A	199.45.8.46			10.73 Mbps		~			Λ		3.10	Kpps		
106524(#FE26044-spon) 3204 Kbps 144 pps 106523 (WW2-McLab) 8.04 Kaps ゲーゲゲーゲー 13 pps 1065210 22 bps Λρ. Λρ. Λρ. Λρ. 13 pps	199.45.8.45			398.70 Kbps		~	·····	m	~		323	pps	mon	
105.510 22 (2002.setals) 8.84 Raps V V V 1 13 pps V V V V V 1 10 20 20 20 20 20 20 20 20 20 20 20 20 20	10.0.5.24 (HP-	E2620-48-upper)		320.43 Kbps		~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	n -		144	pps	manny	
10.05.110 29 bos A A A A A 1 pos A A A A A	10.0.5.21 (GW	02.nfclab)		8.04 Kbps		~	~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	٦		13 p	ps	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
	10.0.5.110			29 bps		A		~~~~			1 pp	s	M_M_L_L_L_	
10.0522 147 bps M.M.M.M. 1pps M.M.M.M.	10.0.5.22			147 bps		A	www	LAN	L		1 pp	s	Minini	

Interfaces Utilization dashboard

The Interfaces Utilization dashboard shows interfaces across your entire data center, with most loaded interfaces first. This dashboard works the best when the App is integrated with SNMP (see SNMP Integration on page 10).

As in Top Devices dashboards, Interfaces Utilization allows drill down to examine traffic details going over the selected interface. Click on an interface, and panels below will show traffic speed statistics, and hosts communicating over the selected interface.

Interfaces Utilization				Edit V More Info V 🛓 💰
Device group Device	Time Range			
All devices 😋 👻 All 📢	3 • Last 60 minutes • Submit			
Interfaces by % of Use				Tm ego
Device/Interface 0	Average Traffic Rate Both/% of Usage Both 0	Traffic Line 0	Average Packet Rate 0	Packets Line 0
10.0.5.24 (HP-E2620-48-upper)/29	148.89 Kbps/0.15%	mmmmM	56 pps	munt
10.0.5.24 (HP-E2620-48-upper)/9	92.71 Kbps/0.09%	mmmmm.	26 pps	monorm
10.0.5.24 (HP-E2620-48-upper)/2	90.23 Kbps/0.09%	M	47 pps	mannen
10.0.5.24 (HP-E2620-48-upper)/28	71.58 Kbps/0.07%	ummuch	25 pps	Lummunh
10.0.5.24 (HP-E2620-48-upper)/6	60.72 Kbps/0.06%	Marchan	23 pps	mmmmm
10.0.5.24 (HP-E2620-48-upper)/7	30.55 Kbps/0.03%	homenon	13 pps	mmmmm
10.0.5.24 (HP-E2620-48-upper)/21	23.62 Kbps/0.02%	mmmmm	9 pps	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
10.0.5.24 (HP-E2620-48-upper)/22	23.62 Kbps/0.02%	mmmmm	9 pps	mont
10.0.5.24 (HP-E2620-48-upper)/8	20.03 Kbps/0.02%	mmmmm	9 pps	m Mun m
10.0.5.24 (HP-E2620-48-upper)/15	9.51 Kbps/0.01%	~mmmmmmm	16 pps	month
				« prev 1 2 3 4 next »

Watched Interfaces Utilization dashboard

The Watched Interfaces Utilization dashboard is very similar to Interface Utilization, but shows only the interfaces specified in watched-interfaces.csv lookup CSV file. Please see Watched Interfaces section at the bottom of App's Settings > Configuration page for more details.

W	Watched Interfaces Utilization												
De	Device group Device Time Range All devices O • All O • Last 60 minutes v Submit												
Ľ	Interfaces by % of Use												
	Device/Interface 0	Average Traffic Rate Both/% of Usage Both 0	Traffic Line 0	Average Packet Rate 0	Packets Line 0								
	10.0.5.21 (GW02.nfclab)/FastEthernet0/1	6.30 Kbps/0.01%	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	11 pps	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~								
	10.0.5.21 (GW02.nfclab)/FastEthernet0/0.2	1.02 Kbps/0.00%		2 pps	7								

Interface Groups dashboard

This dashboard shows consolidated information for Interface Groups. Interface Groups are defined in interface-groups.csv lookup CSV file. Please see Interface Groups section at the bottom of App's Settings > Configuration page for more details.

Interface Groups			Edit V More Info V
Device group Device Time Range All devices O * All O * Last 60 minutes V Submit			
Interface Groups			7m ego
Interface Group 0	Traffic 0	Packets 0	
cisco device	3.15 MB	42,272	

Services

Services dashboards enable users to monitor performance and traffic statistics of selected services in your datacenter. You need to enable corresponding NFI Modules in order to see data in these dashboards.

Service Response Time dashboard

To see data in this dashboard enable and configure Module 10017: Service Performance Monitor. Please refer to NetFlow Integrator User Guide for details. Use Watch List parameter in this Module to specify the services you want to monitor (Service Destination IP, Destination Port, and Transport protocol).

Asset Access Monitor

To see data in this dashboard enable and configure Module 10014: Asset Access Monitor. Please refer to NetFlow Integrator User Guide for details.

This dashboard shows top services with most unauthorized connections - traffic from unauthorized users to services (IP address, destination port, protocol configured in the NFI Module 10014: Asset Access Monitor) and top peers with most unauthorized connections – traffic to peers (IP address and subnet mask also configurable in NFI Module 10014 section).



Security Events

Cyber Thread Statistics dashboard

The Cyber Threat Statistics dashboard enables your organization to analyze and prioritize network security event traffic. Using this dashboard you will be able to see geo location of top hosts, network traffic to and from known suspicious hosts. Out of the box we support geo county database from MaxMind and threat intelligence from Emerging Threats and Alienvault. A corporation can also integrate its own watch-list.

To see data in this dashboard enable Security Module Set: 10040, 10050, 10052, 10053 and install and setup the four utilities for each Module, create the required data sets and add them to the NetFlow Integrator Modules.



DNS Security dashboard

To see data in this dashboard enable Module 10004: DNS Monitor. Please refer to NetFlow Integrator User Guide for details. It is useful to monitor average response time of all DNS servers used in your network. The right panel also shows top DNS users.

DNS Monit Exporter group All exporters	Exporter	Time Range O • Date time range •	Search					Edit - h	lore Info 🔹 🛓 🕹
Average Resp 75,000 50,000 25,000 455 756 756 756 756 756 756 756 756	PM 5:00 PM	Ver 510 PM 520 PM Time	5.30 PM 5.40 Pb	-lm sge 198.153.192.1 199.180.63 199.187.164.1 199.187.164.1 199.187.264.1 199.187.264.1 2716.199.549 2716.199.549 2716.199.549 2716.199.549 2716.199.549	Top 10 DNS Users 45,0,4,17 20442,2533 45,0,427 45,0,427 45,0,427 45,0,427 45,0,427 45,0,427 45,0,427 45,0,427 45,0,427 45,0,427 45,0,417 45,0,	50,000 100,000 150,000	200,000 250,000 Connections	300,000 350,	<1m spo
				soge m1>					lm ago
Exporter 0	DNS Server 0	Average Resp. Time 🗧	Traffic received 0	Traffic sent 0	Exporter 0	DNS user 0			Connections 0
45.0.6.17	199.212.0.63	9.77 sec	87 bps(38 KB)	24 bps(10 KB)	45.0.6.17	45.0.4.12			407280
45.0.6.17	45.0.8.125	7.96 sec	1 bps(40 Bytes)	1 bps(44 Bytes)	45.0.6.17	184.105.139.77			15002
45.0.6.17	45.0.8.126	7.30 sec	1 bps(120 Bytes)	1 bps(132 Bytes)	45.0.6.17	204.42.253.2			11484
45.0.6.17	199.45.8.171	6.90 sec	1 bps(40 Bytes)	1 bps(44 Bytes)	45.0.6.17	45.0.42.21			4653
45.0.6.17	63.110.90.52	5.66 sec	2 bps(739 Bytes)	2 bps(821 Bytes)	45.0.6.17	45.0.100.20			4018
45.0.6.17	199.180.180.63	5.65 sec	130 bps(57 KB)	16 bps(7 KB)	45.0.6.17	45.1.105.138			2127
45.0.6.17	196.15.157.162	5.35 sec	1 bps(60 Bytes)	1 bps(71 Bytes)	45.0.6.17	45.0.34.53			1766
45.0.6.17	199.187.164.1	3.15 sec	30 bps(13 KB)	35 bps(15 KB)	45.0.6.17	45.0.50.42			1736
45.0.6.17	64.68.200.200	3.10 sec	7 bps(3 KB)	3 bps(1 KB)	45.0.6.17	45.0.8.126			1456
45.0.6.17	219.133.0.2	2.94 sec	3 bps(1015 Bytes)	5 bps(2 KB)	45.0.6.17	45.0.24.66			1394
			« prev 1 2 3 4 5	6 7 8 9 10 next »			« prev 1 2 3	4 5 6 7	8 9 10 next »

Supplemental Traffic Statistics

TCP Health

To see data in this dashboard enable and configure Module 10060: TCP Health. Please refer to NetFlow Integrator User Guide for details.

The TCP Health dashboard monitors and detects top hosts with the most TCP Resets.

Top hosts are defined by percent of TCP resets to the total number of Resets for definitive NetFlow exporter or by percent of TCP resets to the total number of host's connections.

The TCP Health dashboard shows top hosts with most count of failed TCP connections and top hosts with largest share of failed TCP connections.

GEO IP Monitor dashboard

The GEO IP dashboard shows geographical locations of Source IP for inbound traffic and Destination IP for outbound traffic. You need to enable Module 10040: Visitors by country.

GEO IP Monito	F at 24 hours											Edit	✓ More Info ✓ ± ♣
Inbound Traffic							Outbound Traffic						
•	Vinitation Via OR Em Pareitos CA Ecs.Argele	MT WY UT Denv CC AZ NM	ND SD NE White State OK TX Na Mutgerey	MN IA ates MO AR LA	ON Chenge R N OH PA N FV VA TN NO MS AL DA FL FL Auni	Na re Na Aa	-	Vandener WA OR D San Fascher CA Las Acyster	MT WY UT Deev O AZ NM	ND SD NE KS OK TX H Moderny	MN IA Tates MC AF	ON W M To N C M PA N K V VA TN OH PA N Weiningen KS All CA FL FL Marti	M Na Te Ni Ni Au
Inbound Traffic							Outbound Traffic						
Device 0	Source IP 0	Dest. IP 0	cc o Fi	Num. of A Flows 0 T	Nverage Traffic Rate (Total 'raffic) ಂ	TrafficLine 0	Device 0	Source IP 0	Dest. IP 0	cc o	Num. of Flows 0	Average Traffic Rate (Total Traffic) 0	TrafficLine 0
10.0.5.24 (HP-E2620-48-	211.143.243.35	255 255 255 255	CN	8 1	bps(2 KB)	λ	10.0.5.21 (GW02.nfclab)	255.255.255.255	217.79.179.106	DE	88	1 bps(7 KB)	1.
10.0.5.24 (HP-E2620-48-	212.129.11.247	255 255 255 255	FR	2 1	bps(106 Bytes)	A	10.0.5.24 (HP-E2620-48- upper)	255 255 255 255	178.16.145.98	RU	137	1 bps(8 KB)	mmm
10.0.5.24 (HP-E2620-48-	218.2.0.132	255.255.255.255	CN	2 1	bps(312 Bytes)		10.0.5.24 (HP-E2620-48- upper)	255.255.255.255	211.143.243.35	CN	10	1 bps(3 KB)	/
upper) 10.0.5.24 (HP-E2620-48-	60.173.11.22	255.255.255.255	CN	95 2	2 bps(18 KB)	^_	10.0.5.24 (HP-E2620-48- upper)	255.255.255.255	217.79.179.106	DE	3	1 bps(228 Bytes)	_//
10.0 5 24 (HP-E2620-48-	61.174.51.213	255 255 255 255	CN	1.1	bps(156 Bytes)	٨	10.0.5.24 (HP-E2620-48- upper)	255.255.255.255	218.2.0.132	CN	4	1 bps(238 Bytes)	
upper) 10.0.5.24 (HP-E2620-48-	61.174.51.214	255.255.255.255	CN	8 1	bps(1 KB)	A	10.0.5.24 (HP-E2620-48- upper)	255.255.255.255	60.173.11.22	CN	109	2 bps(19 KB)	^

Traffic by Autonomous Systems dashboard

The Traffic by Autonomous Systems (AS) dashboard monitors traffic by AS. To see data in this dashboard enable and configure Module 10066: Autonomous Systems Monitor.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results. Select if you want to see incoming or outgoing traffic by AS. Indicate if you want to see statistics for IPv4 or IPv6 or both.

Traffic by	Auton	omous Sy	/stems				Edit 🗸 More Info 🖌 🛓 👼
Device group		Device	Direction	IPv4/IPv6	Time Range		
All devices	0 -	All	😔 🔹 🛛 In	O ▼ IPv4	🛚 🔹 Last 60 minutes 🗸 Submit		
Autonomo	us System	Statistics					
	-	_					
500000 -	Keserved AS-						10.0.5.110
e l							10.0.5.22
- :0 Auto	Reserved AS-						10.0.5.24 (HP-E2620-48-upper)
		0			2		199.45.8.45
					GB		
Autonomous	System 0		Device 0		Average Traffic Rate (Total Traffic) 0	Average Packet Rate (Total Packets) ©	Connections 0
65535: -Reser	ved AS-		199.45.8.46		6.72 Mbps(2.85 GB)	1.90 Kpps(6,936,576)	6948864
65535: -Reser	ved AS-		199.45.8.45		216.82 Kbps(94.29 MB)	166 pps(602,112)	602112
65535 -Beser	ved AS-		10.0.5.24 (HP-E26	J20-48-upper)	138.89 Kbps(60.40 MB)	57 pps(207,300)	207400
	IC.		10.0.5.21 (GW02.)	afclab)	4.04 Kbps(1.76 MB)	7 pps(23,418)	486
0: -Reserved /	10.						
0: -Reserved / 0: -Reserved /	us-		10.0.5.22		74 bps(33 KB)	1 pps(24)	24

Traffic by CBQoS dashboard

The Traffic by CBQoS dashboard enables your organization to analyze and prioritize network traffic by Quality of Service (QoS). Using this dashboard you will be able to see how QoS policy is applied in each of your network device where it is enabled and reported, and if necessary tweak Type of Service (TOS) settings. To see data in this dashboard enable Module 10066: CBQoS Monitor.

Network Traffic by	CBQoS							Edit ~ More Info	v ×] ∓ 😜
Device group Devic All devices O • All	se S	iource IP/mask Destination IF	Protocol Src.	Port Dest. Port Src. 0	DSCP Dest. DSCP Time Range * Last 60 minu	ntes 🗸 Submit			
Inbound Traffic	D PM 2:20 PM	230 PM 240 PM Time	2:50 PM	0 (C50) 10 (Unknowode Point) 1000 (C51) 1010 (AF21) 1010 (AF21) 110000 (C54)	Outbound Traffic	2:10 PM 2:20 PM	2:30 PM 2: Time	NO PM 2:50 PM	0 (CS0)
Device 0	Source Diff. Services 0	Average Traffic Rate (Total Traffic) 0	Average Packet Rate (Total Packet	ets) Connections	Device 0	Destination Diff. Services	Average Traffic Rate (Total Traffic) 0	Average Packet Rate (Total Packets)	Connections 0
199.45.8.46	0 (CS0)	6.66 Mbps(2.82 GB)	1.87 Kpps(6,801,408)	6801408	199.45.8.46	0 (CS0)	6.75 Mbps(2.86 GB)	1.92 Kpps(6,975,488)	6975488
199.45.8.45	0 (CS0)	222.27 Kbps(96.39 MB)	163 pps(591,872)	591872	199.45.8.45	0 (CS0)	222.63 Kbps(96.55 MB)	164 pps(595,968)	595968
10.0.5.24 (HP-E2620-48-upper)	0 (CS0)	139.59 Kbps(60.54 MB)	56 pps(203,100)	203100	10.0.5.24 (HP-E2620-48-upper)	0 (CS0)	140.81 Kbps(61.07 MB)	58 pps(208,500)	208500
199.45.8.46	10 (Unknown Code Point)	66.33 Kbps(28.77 MB)	15 pps(51,200)	51200	10.0.5.21 (GW02.nfclab)	0 (CS0)	4.08 Kbps(1.77 MB)	7 pps(23,589)	484
199.45.8.46	1000 (CS1)	12.25 Kbps(5.31 MB)	20 pps(69,632)	69632	10.0.5.22	0 (CS0)	71 bps(31 KB)	1 pps(23)	23
199.45.8.46	10010 (AF21)	4.28 Kbps(1.86 MB)	10 pps(34,816)	34816	10.0.5.110	0 (CS0)	14 bps(6 KB)	1 pps(27)	27
10.0.5.21 (GW02.nfclab)	0 (CS0)	3.95 Kbps(1.71 MB)	7 pps(23,016)	429					
199.45.8.46	1010 (AF11)	3.52 Kbps(1.53 MB)	6 pps(18,432)	18432					
10.0.5.24 (HP-E2620-48-upper)	110000 (CS6)	1.17 Kbps(519 KB)	2 pps(5,200)	5200					
199.45.8.45	10010 (AF21)	361 bps(160 KB)	2 pps(4,096)	4096					
				« prev 1 2 next »					

Search dashboard

This screen opens a Search dashboard within the App, with search criteria set to macro `netflow_search_traffic_rules`.

To see all output from NFI enter "index=flowintegrator" in search area. To filter search results to a specific NFI Module, please add the corresponding Module output ID to your search, for example:

"index=flowintegrator nfc_id=20067"

You can add additional filters or any other Splunk search commands to narrow your search results and / or see various statistics. You can also save your custom searches there.

Cisco ASA Monitor

Cisco ASA Monitor dashboards show the output from NetFlow Integrator Cisco ASA Module set, which in its turn designed to handle Cisco ASA NSEL.

Cisco Overview

The Cisco Overview dashboard aimed to provide a summary on traffic over the last 24 hours.

The panels show Geo location of hosts on the map, Top Bandwidth Consumers, Top Destinations, Top Violators, and Top Connectors.

Cisco Top Bandwidth Consumers

This dashboard (a.k.a. Top Talkers) monitors host which generate most traffic in your network. It is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic volume and connections count (created and denied) generated by each host.

Cisco Top Destinations

This dashboard (a.k.a. Top Listeners) monitors host which receive most traffic. The top of the dashboard has a map showing geographical locations of top destinations of the traffic in your network. It is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic volume and connections count (created and denied) received by each host.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Cisco Top Violators

This dashboard show hosts with most traffic of denied flows. It could be useful to reinforce Cisco ASA firewall policies.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Cisco Top Connectors

This dashboard monitors host which generate most connections in your network. It is useful for identifying hosts that make most connections, but could be omitted from top bandwidth consumers because of the small packets they send, e.g. port scanners. The dashboard shows connections created by each host.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Palo Alto Networks

Palo Alto Networks dashboards show the output from NetFlow Integrator Palo Alto Networks Module set, which in its turn designed to handle Palo Alto Network proprietary NetFlow v9 fields.

Palo Alto Networks Overview

The Palo Alto Networks Overview dashboard aimed to provide a summary on traffic over selected period time.

The panels show Top Bandwidth Consumers, Top Destinations, Top Violators, Top Connectors, Top Applications, and Top Applications and Users.

Palo Alto Networks Top Bandwidth Consumers

This dashboard (a.k.a. Top Talkers) monitors host which generate most traffic in your network. It is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic volume and connections count (created and denied) generated by each host.

Palo Alto Networks Top Destinations

This dashboard (a.k.a. Top Listeners) monitors host which receive most traffic. It is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic volume and connections count (created and denied) received by each host.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Palo Alto Networks Top Violators

This dashboard show hosts with most traffic of denied flows. It could be useful to reinforce Palo Alto Networks firewall policies.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Palo Alto Networks Top Connectors

This dashboard monitors host which generate most connections in your network. It is useful for identifying hosts that make most connections, but could be omitted from top bandwidth consumers because of the small packets they send, e.g. port scanners. The dashboard shows connections generated by each host.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Top Applications

This dashboard monitors traffic by Application as identified by Palo Alto Network devices. It is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic volume and connections attributed to each application recognized by Palo Alto Networks devices.

Use the filtering options and time picker at the top of the dashboard to select the time interval and narrow down your search results.

Top Applications and Users

This dashboard monitors traffic by Application and Users as identified by Palo Alto Network devices. It is useful for real time or historical network utilization and bandwidth monitoring. The dashboard shows traffic volume and connections attributed to each application recognized by Palo Alto Networks devices, and allows to drill down to see users of each reported application.

Resources

FAQ

What is the default UDP Data Input the app uses?

Once the app is installed the default Data Input 10514 is created with the index=flowintegrator and the manual sourcetype=flowintegrator

How do I setup the app to work with SNMP?

This application is automatically integrated with SNMP. See SNMP Integration section on page 10.

How do I change the default index where NetFlow data is stored?

Once the app is installed the default index=flowintegrator is created, If you need to alter the index, please follow these steps:

- 1. Create directory \$SPLUNK_ROOT/etc/apps/netflow/local/ if it doesn't exist
- 2. Create file \$SPLUNK_ROOT/etc/apps/netflow/local/macros.conf with following lines:

```
[netflow_index]
definition = index=your_index sourcetype=flowintegrator
```

Save \$SPLUNK_ROOT/etc/apps/netflow/local/macros.conf and restart Splunk to changes take effect.

Getting help

NetFlow Logic provides many resources for help with the NetFlow Analytics for Splunk App.

NetFlow Analytics for Splunk App download: https://apps.splunk.com/app/489/

Technology Add-on for NetFlow download: https://splunkbase.splunk.com/app/1838/

NetFlow Logic Support: https://www.netflowlogic.com/connect/support/