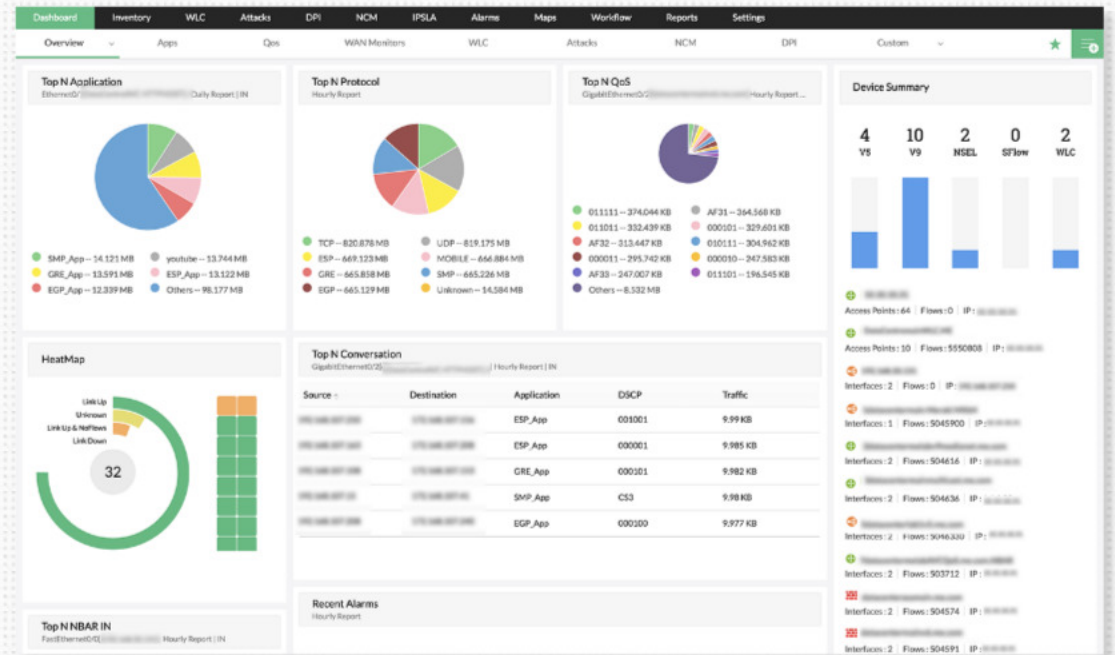


ManageEngine NetFlow Analyzer

Complete bandwidth monitoring and network traffic analysis solution for network admins.





The what and why of bandwidth monitoring

Bandwidth monitoring: The what and why

- Knowing the performance of your network
- Assessing each element's bandwidth usage
- Learning the bandwidth hogs and network strains
- Predicting the bandwidth capacity for future

“

If you can't measure it, you can't manage it"

- Peter Drucker

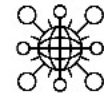
”



Why NetFlow Analyzer



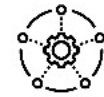
Flow-based traffic analysis



Support for distributed network traffic monitoring



Scalable to your network and customizable



Add-ons & multi-vendor support



Simple and easy-to-use UI

Bandwidth usage & speed

Medianet & Multicast

Traffic grouping

IP SLA monitoring

Cisco AVC monitoring

NBAR monitoring

WLC traffic monitoring

Security



Starting off with NetFlow monitoring!

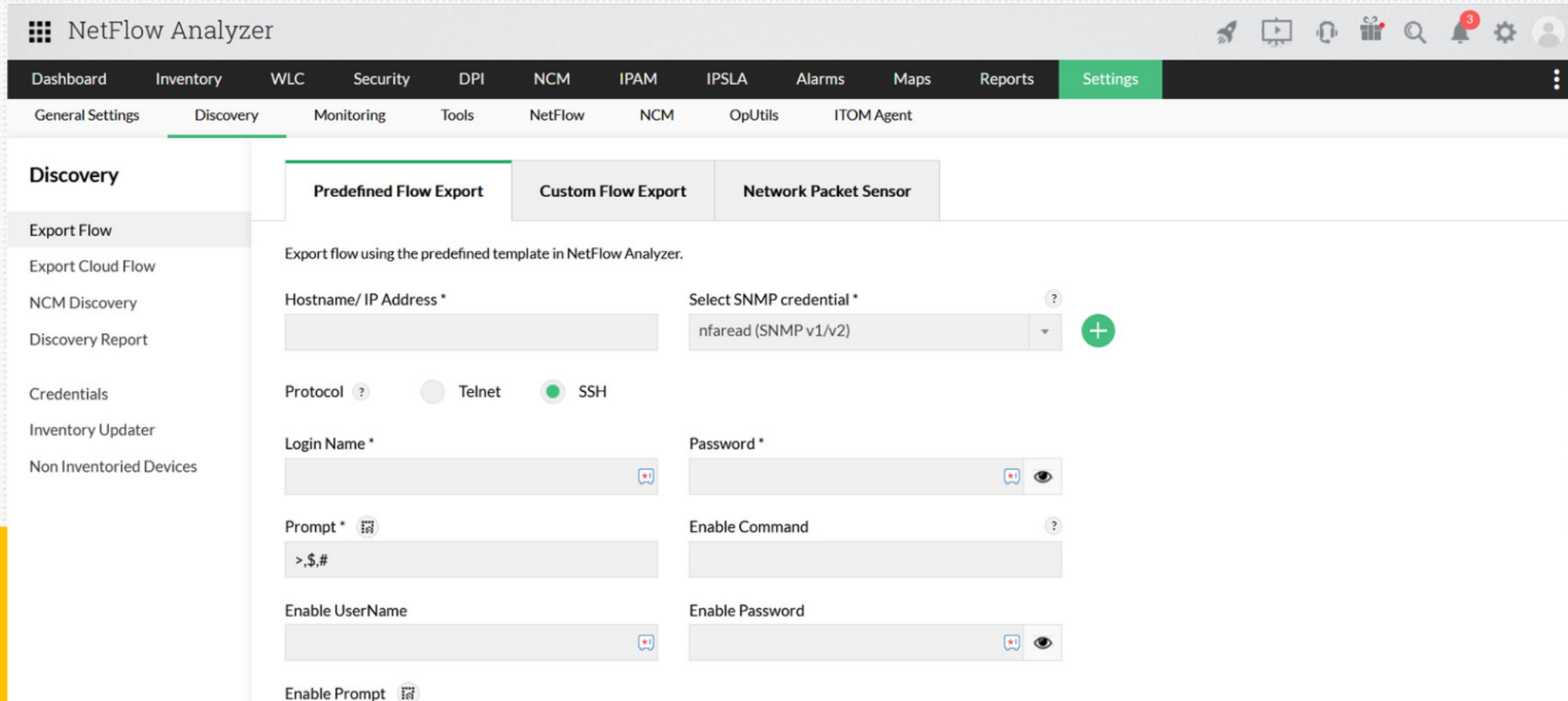
Flow export

Add Credentials 

Executing the commands 

Export flow 

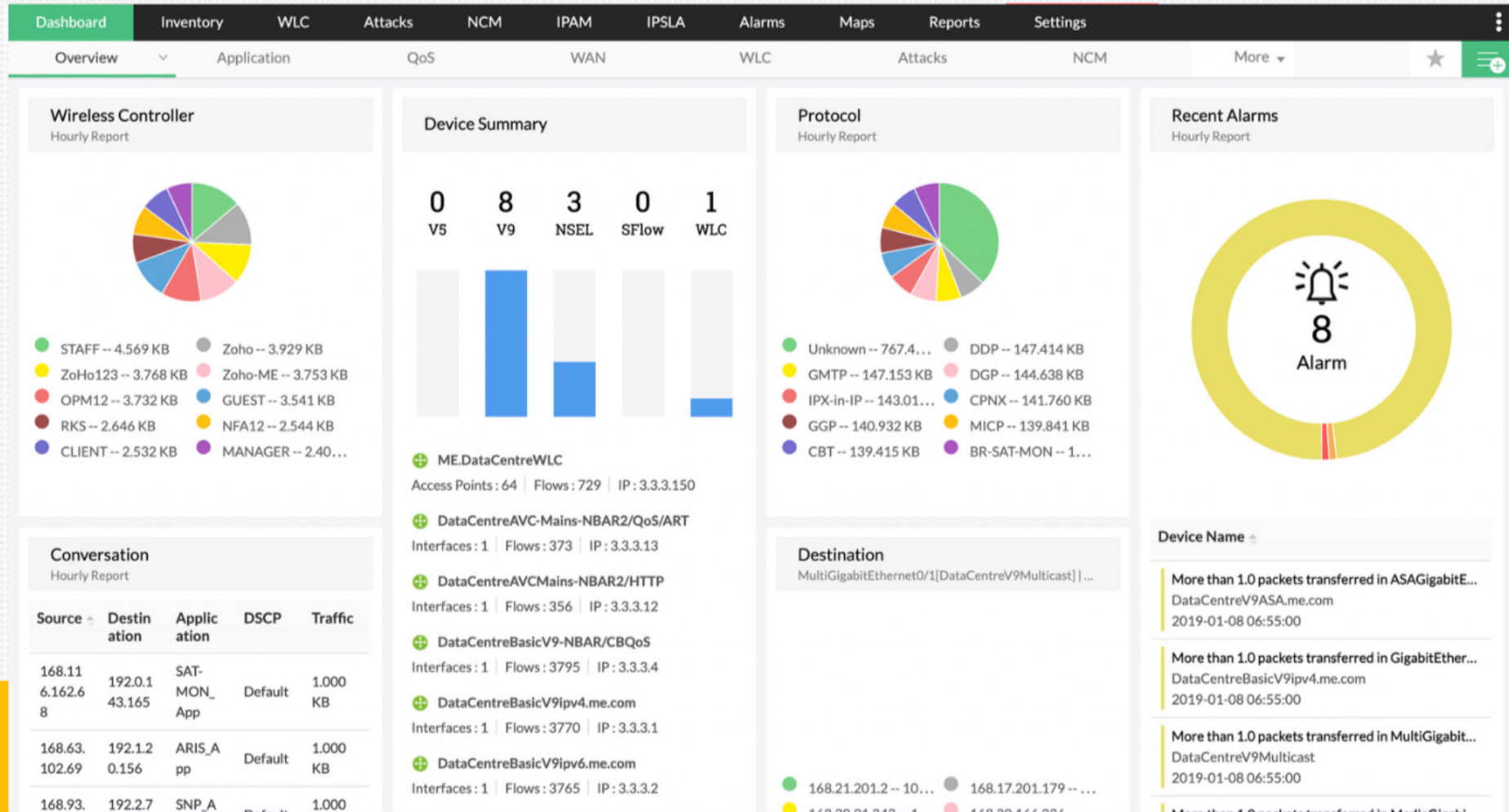
- i. Predefined
- ii. Custom
- iii. Network Packet Sensor



The screenshot shows the NetFlow Analyzer interface. The top navigation bar includes 'Dashboard', 'Inventory', 'WLC', 'Security', 'DPI', 'NCM', 'IPAM', 'IPSLA', 'Alarms', 'Maps', 'Reports', and 'Settings' (highlighted). Below this is a sub-menu with 'General Settings', 'Discovery' (highlighted), 'Monitoring', 'Tools', 'NetFlow', 'NCM', 'OpUtils', and 'ITOM Agent'. The left sidebar lists 'Discovery' and 'Export Flow' (highlighted). The main content area shows three tabs: 'Predefined Flow Export' (active), 'Custom Flow Export', and 'Network Packet Sensor'. The 'Predefined Flow Export' tab contains the following configuration fields:

- Export flow using the predefined template in NetFlow Analyzer.
- Hostname/ IP Address * (text input)
- Select SNMP credential * (dropdown menu with 'nfaread (SNMP v1/v2)' selected and a '+' icon)
- Protocol ? (radio buttons for 'Telnet' and 'SSH', with 'SSH' selected)
- Login Name * (text input with a help icon)
- Password * (text input with a help icon and an eye icon for visibility toggle)
- Prompt * (text input with a help icon, containing '>,\$,#')
- Enable Command (text input with a help icon)
- Enable UserName (text input with a help icon)
- Enable Password (text input with a help icon and an eye icon for visibility toggle)
- Enable Prompt (checkbox with a help icon)

Dashboard & NOC view



Wireless Controller

Hourly Report



- STAFF -- 4.569 KB
- ZoHo123 -- 3.768 KB
- OPM12 -- 3.732 KB
- RKS -- 2.646 KB
- CLIENT -- 2.532 KB
- Zoho -- 3.929 KB
- Zoho-ME -- 3.753 KB
- GUEST -- 3.541 KB
- NFA12 -- 2.544 KB
- MANAGER -- 2.40...

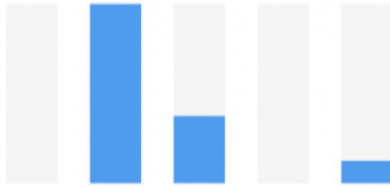
Conversation

Hourly Report

Source	Destination	Application	DSCP	Traffic
168.11 6.162.6 8	192.0.1 43.165	SAT- MON_ App	Default	1,000 KB
168.63. 102.69	192.1.2 0.156	ARIS_A pp	Default	1,000 KB
168.93.	192.2.7	SNP_A	Default	1,000

Device Summary

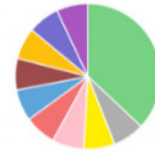
0 V5 8 V9 3 NSEL 0 SFlow 1 WLC



- ME.DataCentreWLC
Access Points: 64 | Flows: 729 | IP: 3.3.3.150
- DataCentreAVC-Mains-NBAR2/QoS/ART
Interfaces: 1 | Flows: 373 | IP: 3.3.3.13
- DataCentreAVCMains-NBAR2/HTTP
Interfaces: 1 | Flows: 356 | IP: 3.3.3.12
- DataCentreBasicV9-NBAR/CBQoS
Interfaces: 1 | Flows: 3795 | IP: 3.3.3.4
- DataCentreBasicV9ipv4.me.com
Interfaces: 1 | Flows: 3770 | IP: 3.3.3.1
- DataCentreBasicV9ipv6.me.com
Interfaces: 1 | Flows: 3765 | IP: 3.3.3.2

Protocol

Hourly Report



- Unknown -- 767.4...
- GMTP -- 147.153 KB
- IPX-in-IP -- 143.01...
- GGP -- 140.932 KB
- CBT -- 139.415 KB
- DDP -- 147.414 KB
- DGP -- 144.638 KB
- CPNX -- 141.760 KB
- MICP -- 139.841 KB
- BR-SAT-MON -- 1...

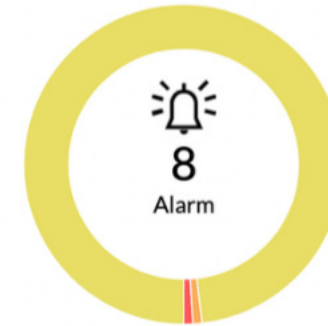
Destination

MultiGigabitEthernet0/1[DataCentreV9Multicast] | ...

- 168.21.201.2 -- 10...
- 168.20.1.242 -- 1
- 168.17.201.179 -- ...
- 168.20.166.236

Recent Alarms

Hourly Report



Device Name

- More than 1.0 packets transferred in ASAGigabit...
DataCentreV9ASA.me.com
2019-01-08 06:55:00
- More than 1.0 packets transferred in GigabitEther...
DataCentreBasicV9ipv4.me.com
2019-01-08 06:55:00
- More than 1.0 packets transferred in MultiGigabit...
DataCentreV9Multicast
2019-01-08 06:55:00
- More than 1.0 packets transferred in MultiGigabit...

Device and Interface Traffic




NetFlow Analyzer

Dashboard **Inventory** WLC Security DPI NCM IPAM IPSLA Alarms Maps Reports Settings

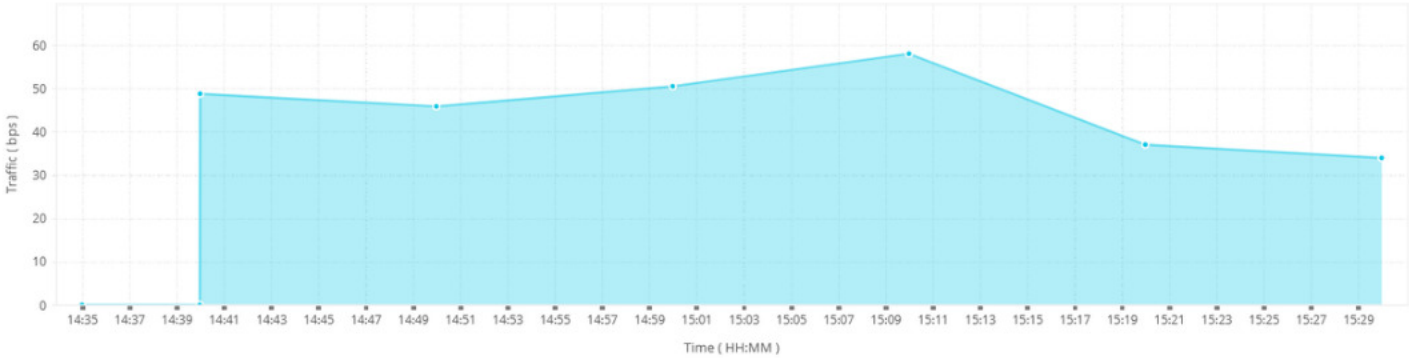
DataCentreAVC-Mains-NBAR2/QoS/ART Last Hour
3.3.3.13 2023-02-15 14:35 to 2023-02-15 15:35

Summary **Flow Details** Traffic Interface Application Source Destination QoS Conversation AS View Security Cloud Services Users NCM

Device Traffic

Graph Types   

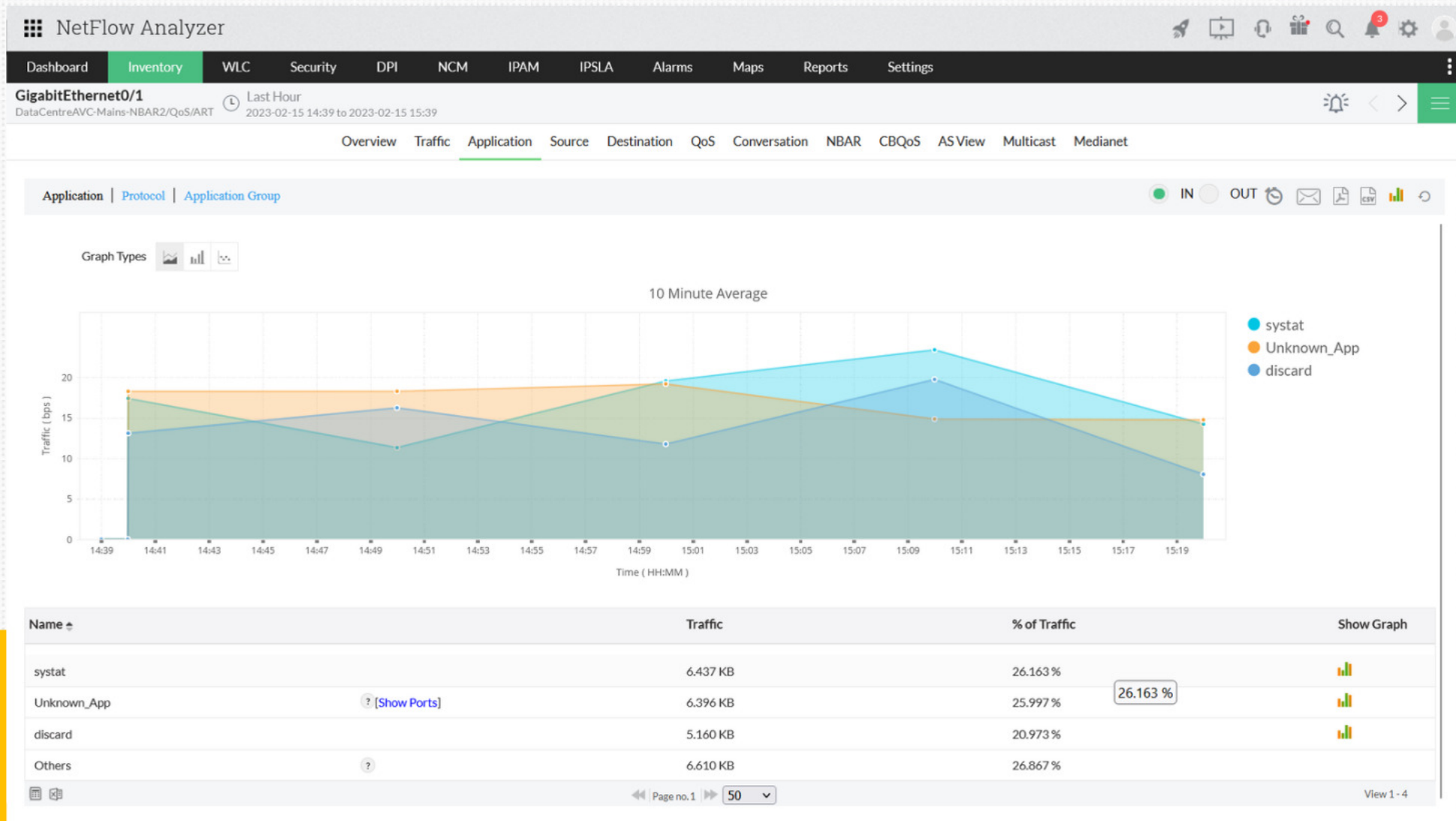
10 Minute Average



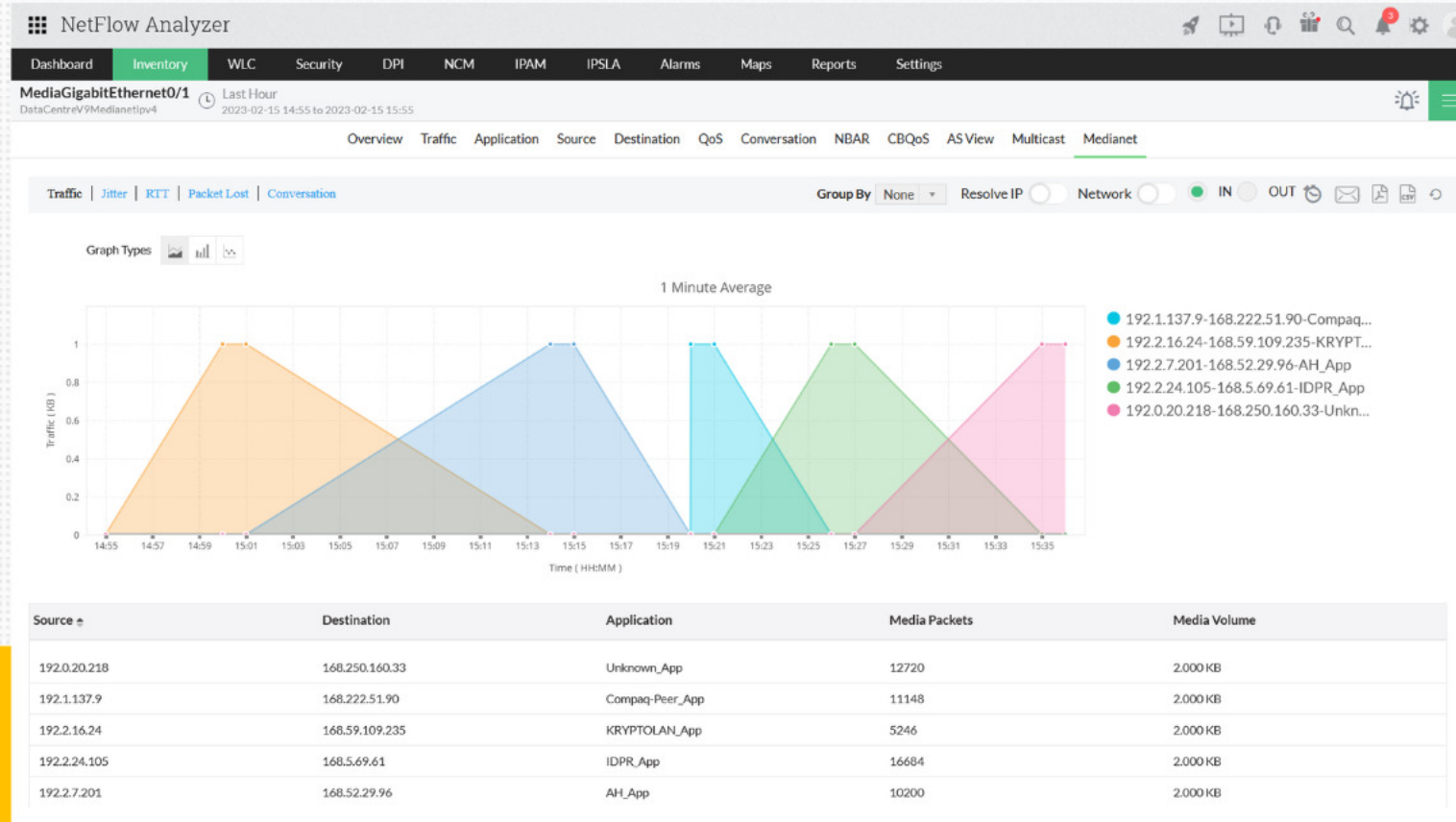
Time (HH:MM)	Traffic (bps)
14:35	0
14:37	0
14:39	0
14:41	48
14:43	47
14:45	46
14:47	45
14:49	44
14:51	45
14:53	46
14:55	47
14:57	48
14:59	49
15:01	50
15:03	51
15:05	52
15:07	53
15:09	58
15:11	55
15:13	50
15:15	45
15:17	40
15:19	38
15:21	37
15:23	36
15:25	35
15:27	34
15:29	34

Max Speed	Avg Speed	Volume
57.960 bps	45.636 bps	20.536 KB

Application traffic

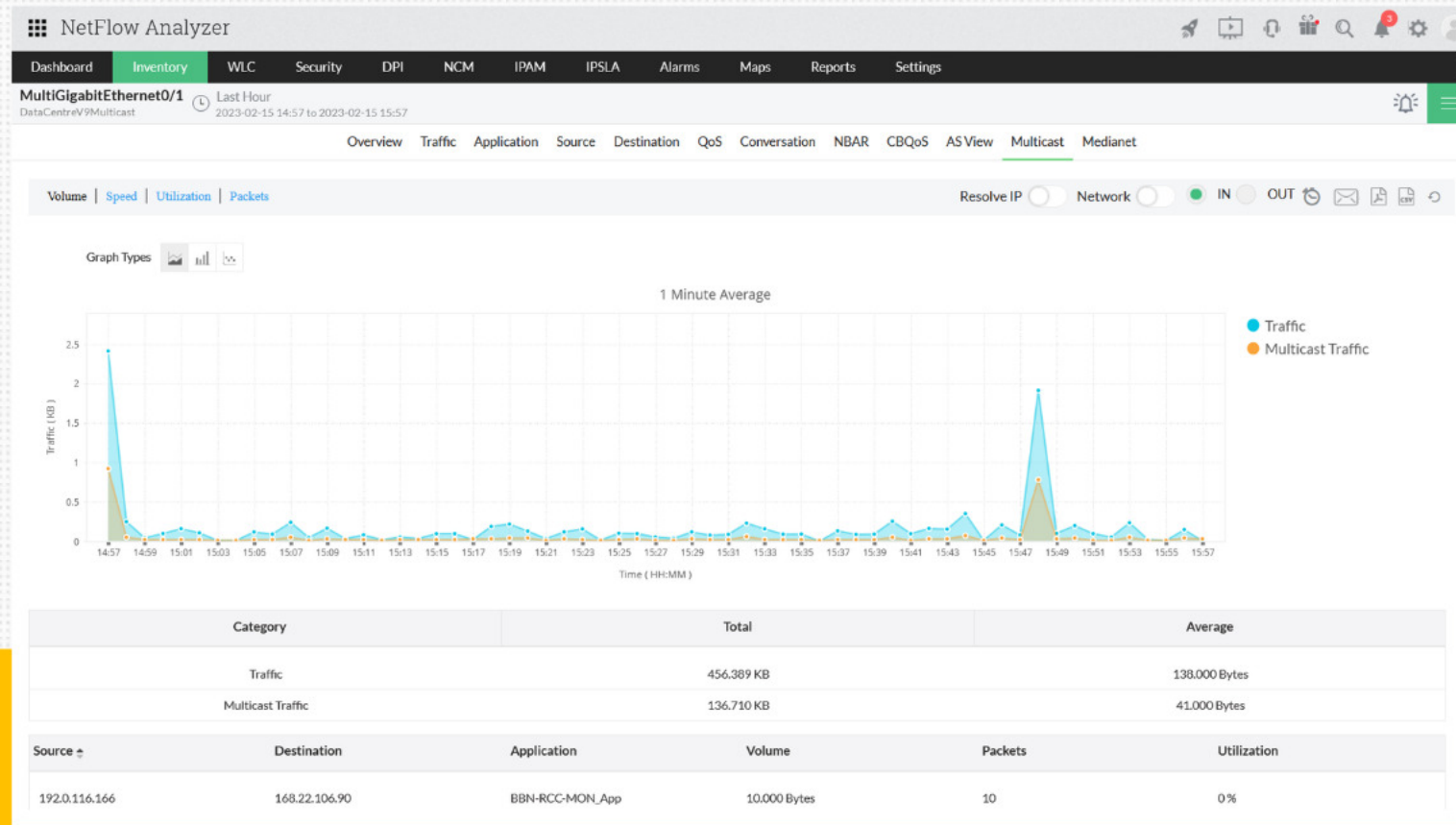


Medianet traffic monitoring



- Monitor media-rich traffic such as voice and video traffic for improving QoE.
- Measure performance statistics such as Jitter, Packet Loss, & RTT.

Multicast traffic monitoring



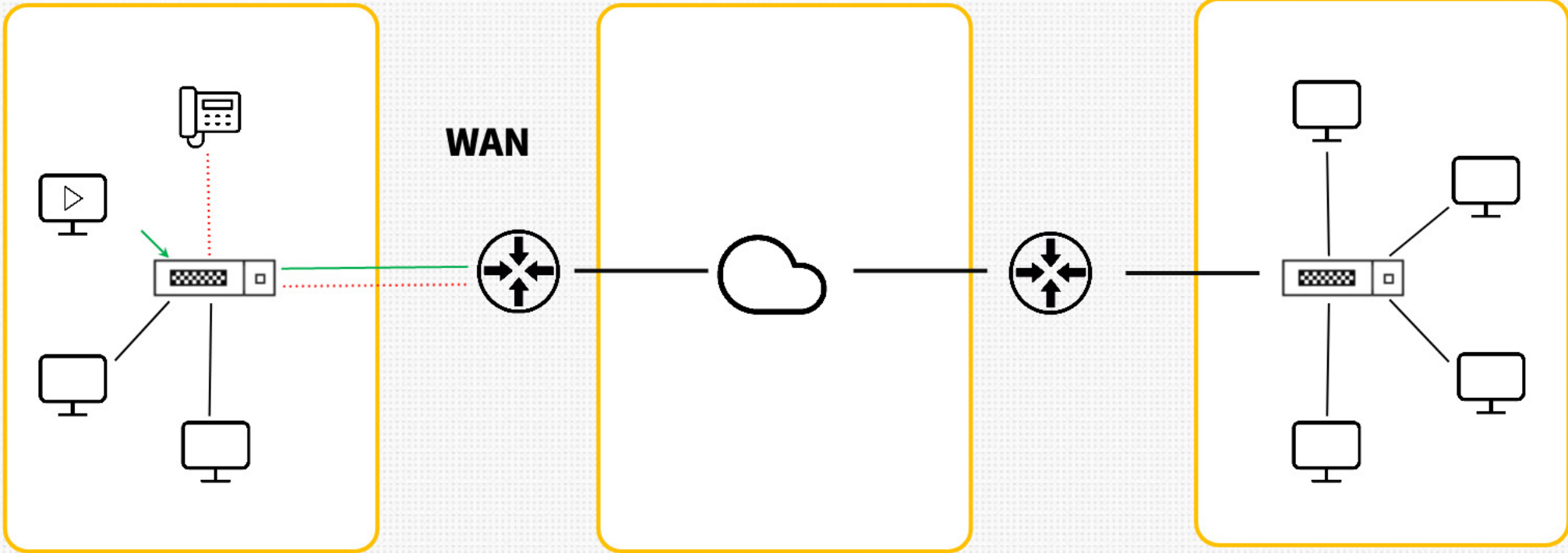
- IP Multicasting allows a host to send packets to a specific group of hosts.
- Monitor multicast traffic by usage & speed.

IPSLA Monitoring

Development Center

Service Provider

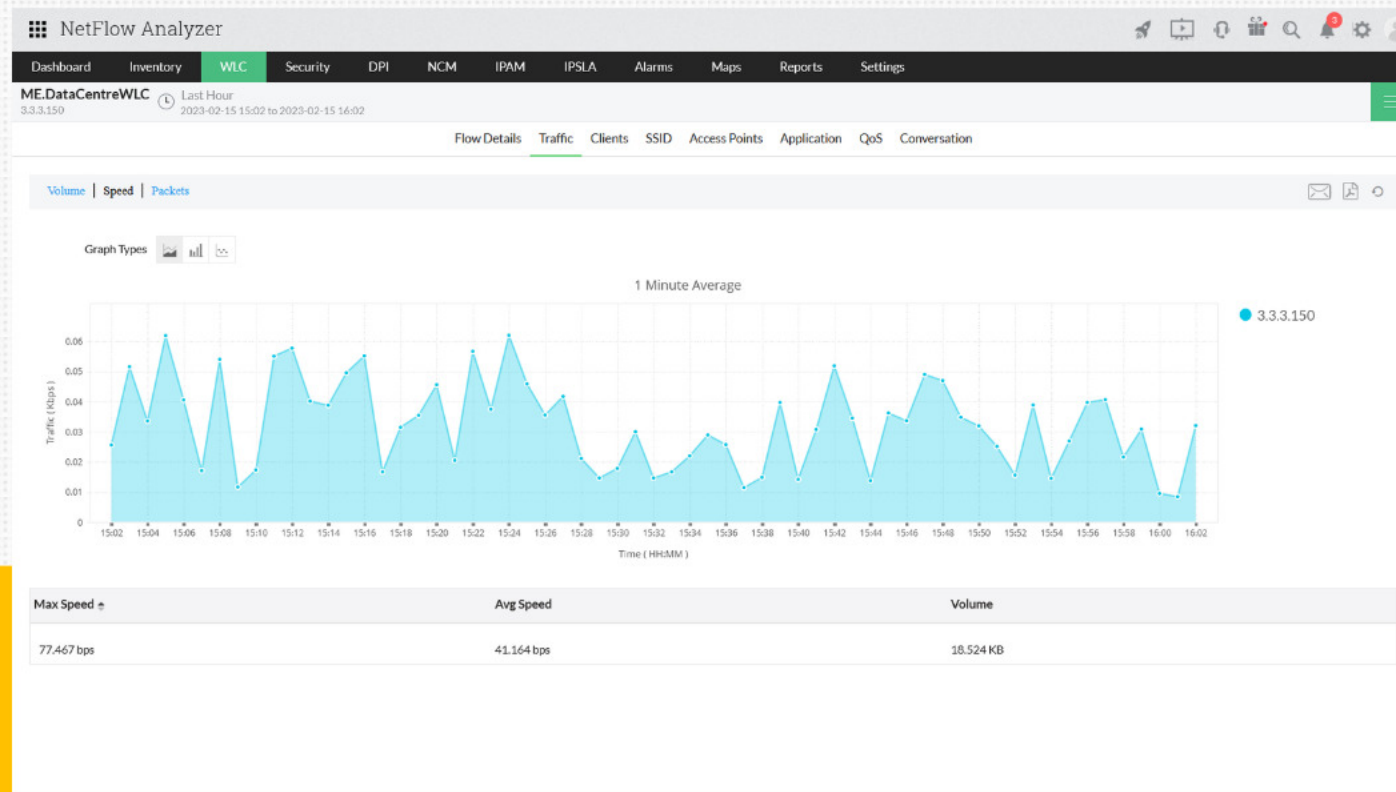
Headquarters



Application Visibility and Control

- Gain visibility into NBAR2 applications with Cisco AVC monitoring (Application Visibility and Control).
- Advanced NBAR is used to identify web traffic, URL's, file sharing and random port application.
- View NBAR2 application, URL hit count (HTTP host report), QoS class hierarchy and application response time monitoring reports(ART monitoring).
- How to enable: Needs additional fields to be configured during exporting flow.

Wireless traffic monitoring

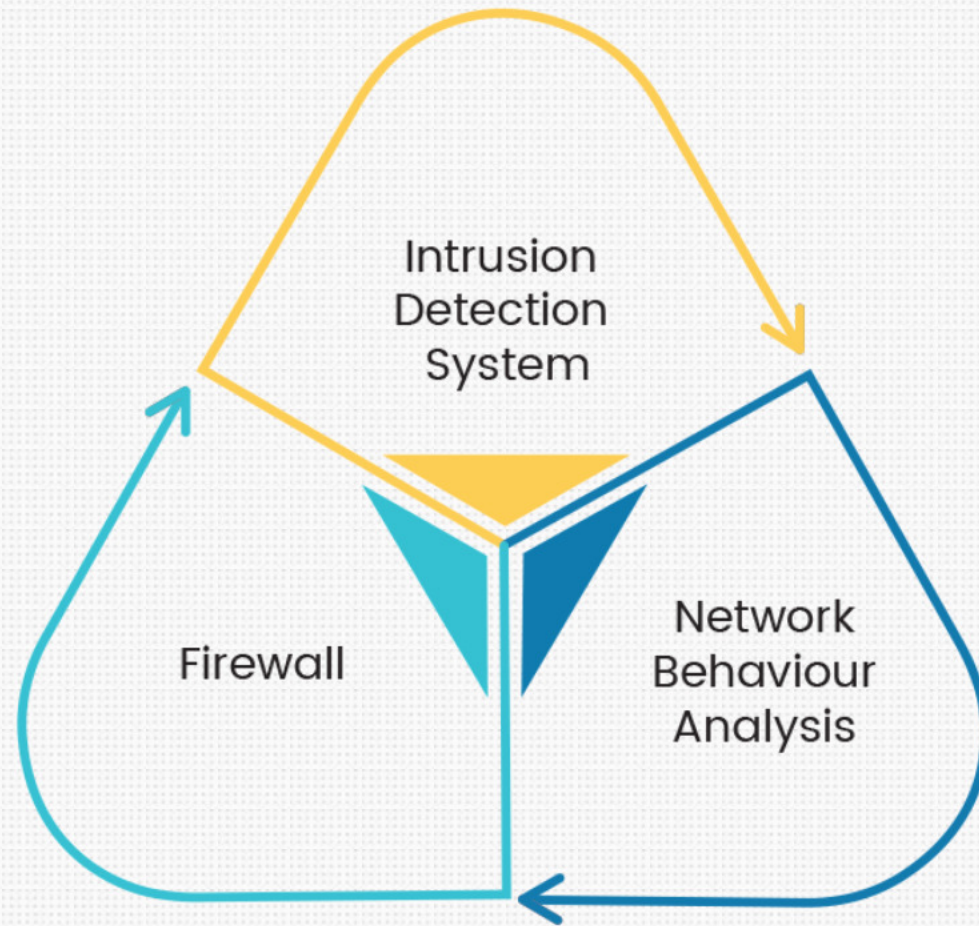


- Monitor Cisco WLAN controllers.
- Find the top traffic usage by access points, SSIDs, applications, clients etc.
- Group WLANs by SSIDs.
- Troubleshoot bandwidth spikes by identifying consumption by SSIDs, finding its top clients and complete conversation details for the selected time period.



Security, beyond basic NTA

Behavior analysis



How does NetFlow Analyzer help?

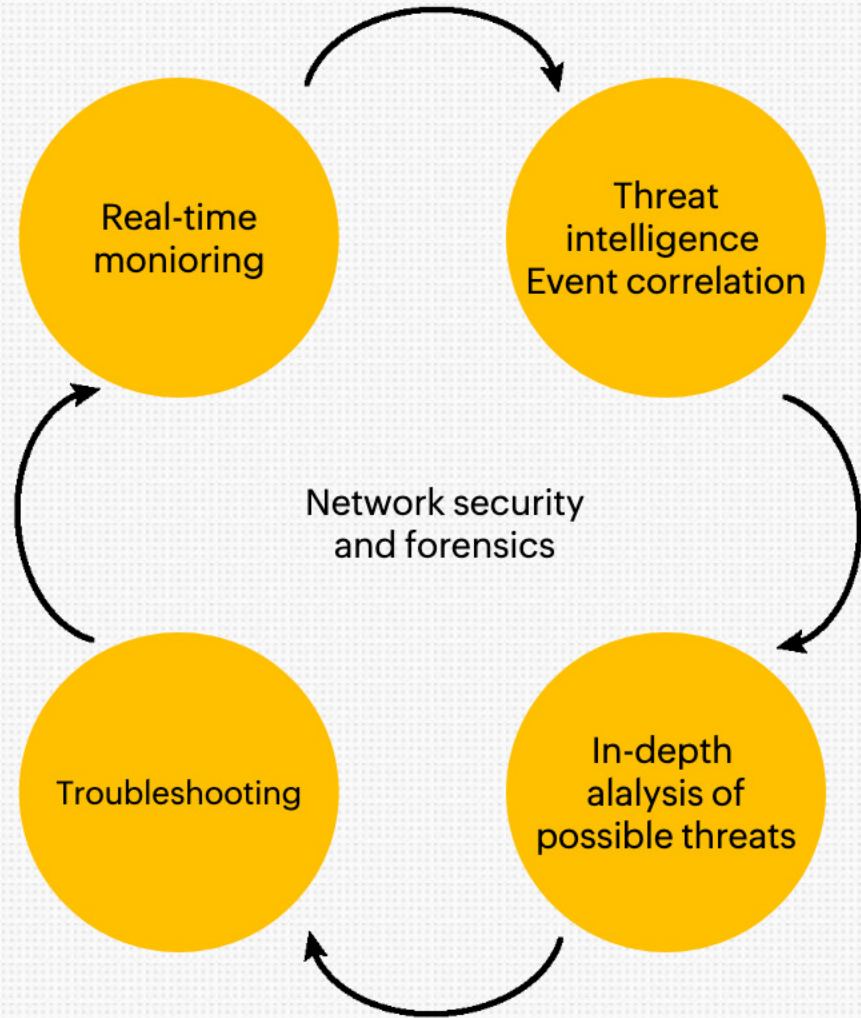


Network Forensics



Security Module

Network forensics



- Better visibility
- Ease of identifying issues in the network infrastructure, overall performance, and bandwidth usage
- Better troubleshooting response

Network forensics

Forensics

Device Type : Interface WLC Device

Select Device : Router140.ITOM

Select Interface : GigabitEthernet0/0

Define Criteria :

Source Address Include

From : 2019-11-12 Date 00 Hrs 07 Mns

To : 2019-11-12 Date 01 Hrs 07 Mns

Note :
Generated from raw data and may take longer, especially for large time intervals.

- Get more granular traffic statistics using raw data
- Drill down to identify which users, applications, and protocols are consuming the most bandwidth at a specific time
- Troubleshoot accurately by defining multiple criteria to filter required traffic

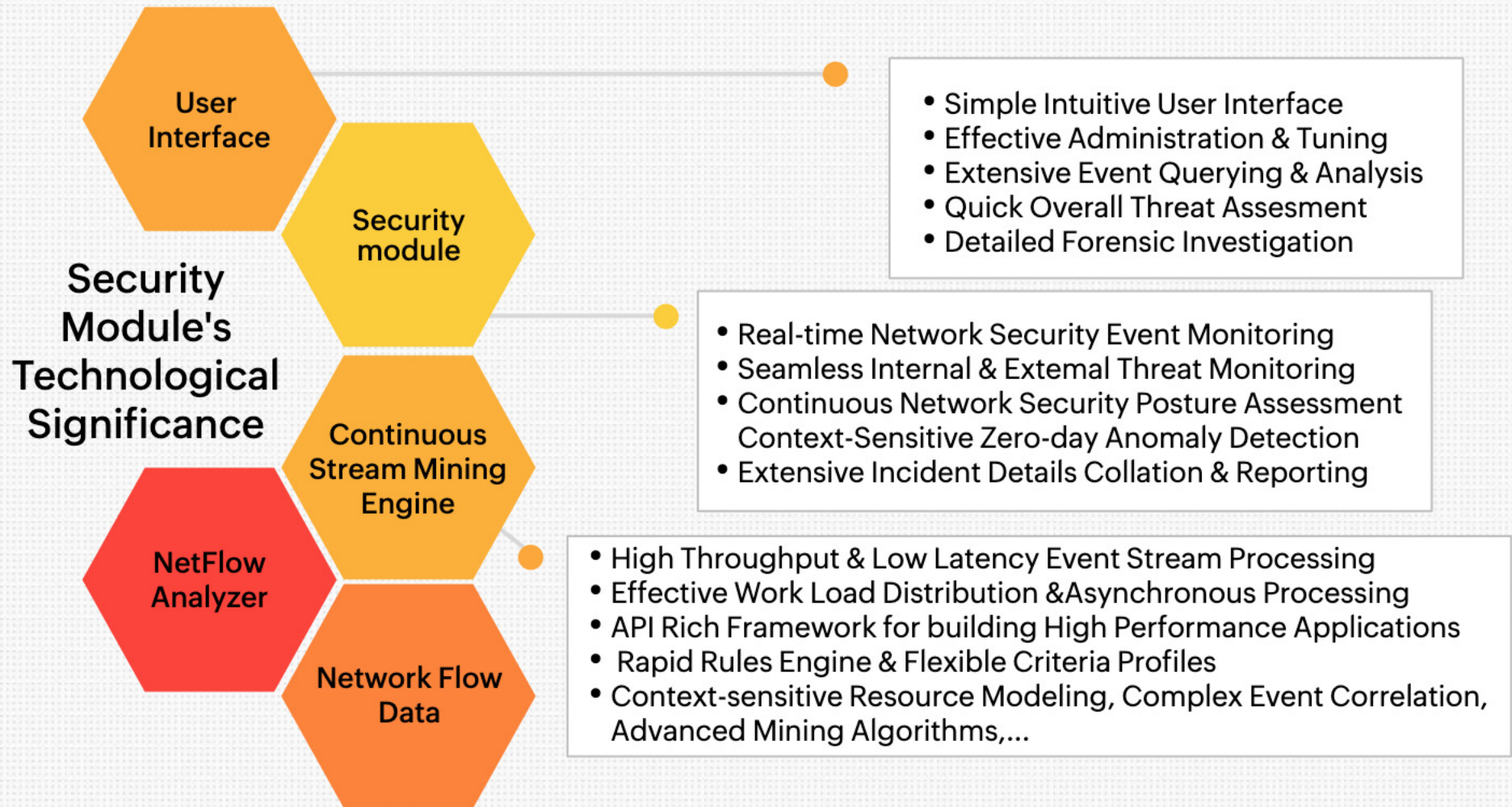
Security analytics

DDOS

Scan / Probes












Botnets

What is the Security Module?



Detect attacks with flow-based security analytics module

- Identify junk/malicious traffic using advanced mining algorithm.
- Security module classifies traffic as suspect flows, bad source and destination, DDoS, and scans /probes.

	Problem	Offenders	Routed Via	Targets	Time	Hits	Severity
<input type="radio"/>	 TCP Fin Host Scan(Reverse)	60	2	58	Today 07 : 23 PM, IST	63	Warning
<input type="radio"/>	 Malformed UDP Packets	75	10	92	Today 06 : 56 PM, IST	100	Major
<input type="radio"/>	 TCP Syn_Fin Host Scan	60	2	60	Today 06 : 46 PM, IST	63	Warning
<input type="radio"/>	 Malformed TCP Packets	80	11	94	Today 06 : 37 PM, IST	100	Major
<input type="radio"/>	 TCP Syn_Fin Violations	82	14	91	Today 06 : 37 PM, IST	100	Major
<input type="radio"/>	 Malformed TCP Packets	79	11	93	Today 06 : 37 PM, IST	100	Major
<input type="radio"/>	 TCP Fin Violations	84	14	92	Today 06 : 36 PM, IST	100	Major
<input type="radio"/>	 TCP Fin Violations	81	14	91	Today 06 : 36 PM, IST	100	Major
<input type="radio"/>	 TCP Syn_Fin Violations	77	14	91	Today 06 : 36 PM, IST	100	Major
<input type="radio"/>	 Malformed IP Packets	83	10	95	Today 06 : 31 PM, IST	100	Major
<input type="radio"/>	 Malformed IP Packets	87	10	94	Today 06 : 31 PM, IST	100	Major

Reports

Reports

Search report

Search specific traffic details by the associated application, protocol, host, or IP

Compare report

Compare bandwidth usage at different time intervals

Consolidated report

Track top talkers and conversations with a complete report

Inventory report

Visualize the combined traffic usage of all interfaces

Reports

Percentile report

Generate traffic reports by 90th and 95th percentile values for interfaces, IP groups

Geolocation report

Identify the region-based information of source and destination traffic

Scheduled report

Get bandwidth usage reports automatically on daily, weekly, monthly basis

LAN-WAN report

Track the traffic between your LAN IPs and LAN and WAN



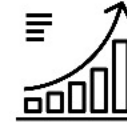
Capacity Planning: Reporting and predicting bandwidth needs

Capacity planning and performance forecasting reports



Capacity planning

Device and application usage trends and growth trends to plan proactive measures



Forecast Reports

Predictive analysis based on historical growth and utilization trends

Capacity trend reports

NetFlow NCM OpUtils Audit

NetFlow Reports

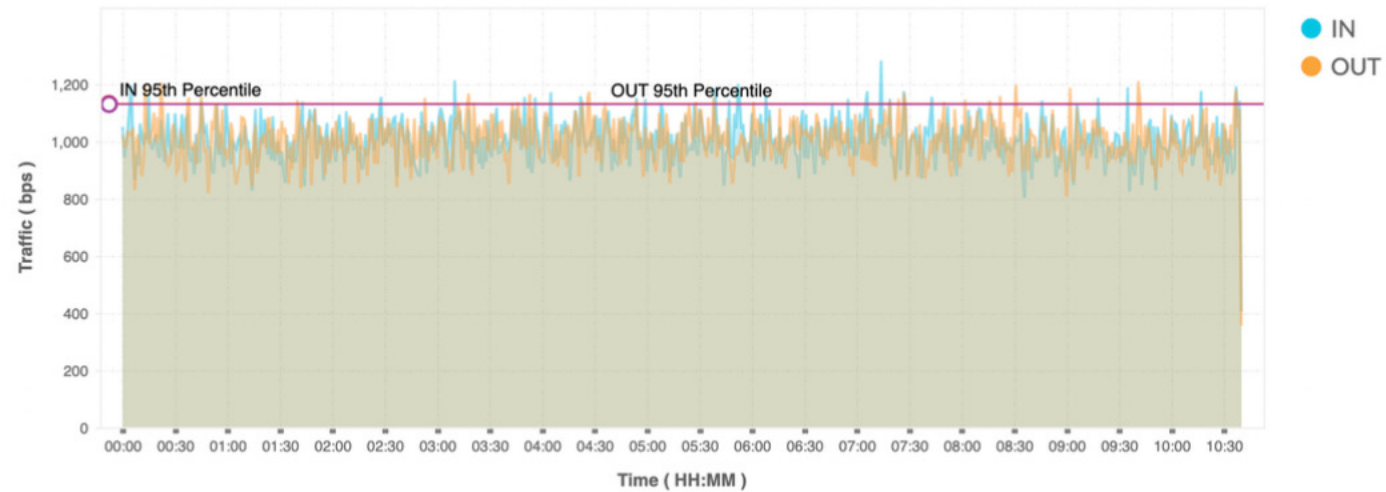
- Search Report
- Report Profiles
- Forensics
- Favorite Reports
- Consolidated Report
- Capacity Planning**
- Compare Reports
- Protocol Distribution
- Inventory Report
- Percentile Report
- LAN WAN Report
- Geolocation Report
- Billing
- Forecast
- Schedule
- WAAS Dashboard
- WAAS Devices List

Capacity Planning

DataCentreV9Medianetipv4 (MediaGigabitEthernet0/1) | Today[2022-02-24 00:00 -- 2022-02-24 10:40] | [Generate Bill](#)



1 Minute Average



Category	Total	Maximum	Minimum	Average	Standard Deviation	95th Percentile
Traffic IN	4.842 MB	1.283 Kbps	405.200 bps	1.007 Kbps	75.778 bps	1.132 Kbps

Forecast report

NetFlow NCM OpUtils Audit

NetFlow Reports

- Search Report
- Report Profiles
- Forensics
- Favorite Reports
- Consolidated Report
- Capacity Planning
- Compare Reports
- Protocol Distribution
- Inventory Report
- Percentile Report
- LAN WAN Report
- Geolocation Report
- Billing
- Forecast**
- Schedule
- WAAS Dashboard
- WAAS Devices List

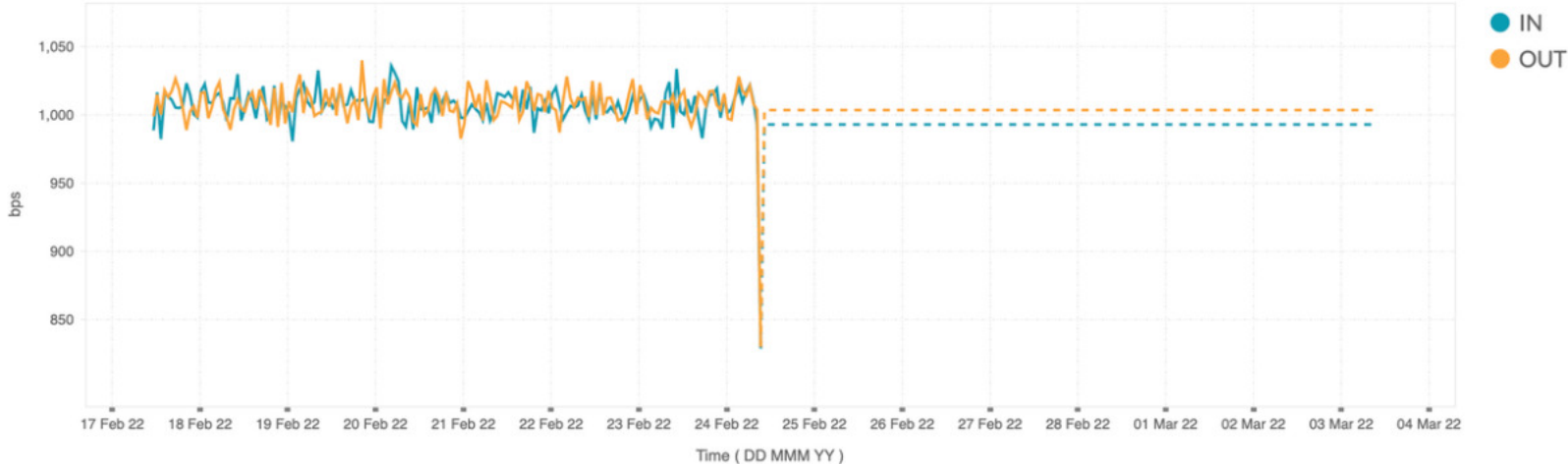
Forecast

DataCentreV9Medianetipv4 / MediaGigabitEthernet0/1 / [🔗](#)



Volume
Speed
Utilization

 Show History
 📅 7 Days



Time ↕	IN	OUT
Feb-17-22 21:30	1.014 Kbps	1.002 Kbps
Feb-17-22 22:30	1.000 Kbps	1.006 Kbps
Feb-17-22 23:30	997.696 bps	997.684 bps

Billing report

The image shows a screenshot of a billing report interface. On the left, there is a sidebar with navigation options: Netflow Reports, Billing, Capacity Planning, Compare Reports, Consolidated Report, Forensics, IPGroup Consolidated, Protocol Distribution, Report Profiles, Schedule, Search Report, WAAS Dashboard, and WAAS Devices List. The main area displays a 'Bill List' table with columns for Name, Type, and Time Zone. A modal window titled 'Billing Reports' is open on the right, showing summary details and a table of report entries.

Netflow Reports
Billing
Capacity Planning
Compare Reports
Consolidated Report
Forensics
IPGroup Consolidated
Protocol Distribution
Report Profiles
Schedule
Search Report
WAAS Dashboard
WAAS Devices List

Bill List

Name	Type	Time Zone

Billing Reports

Plan Name : Basic plan **Bill Type** : Volume
Last Report Time : 02/20/19 11:28 **Time Zone** : Asia/Calcutta
Bill Period : 1st of every month

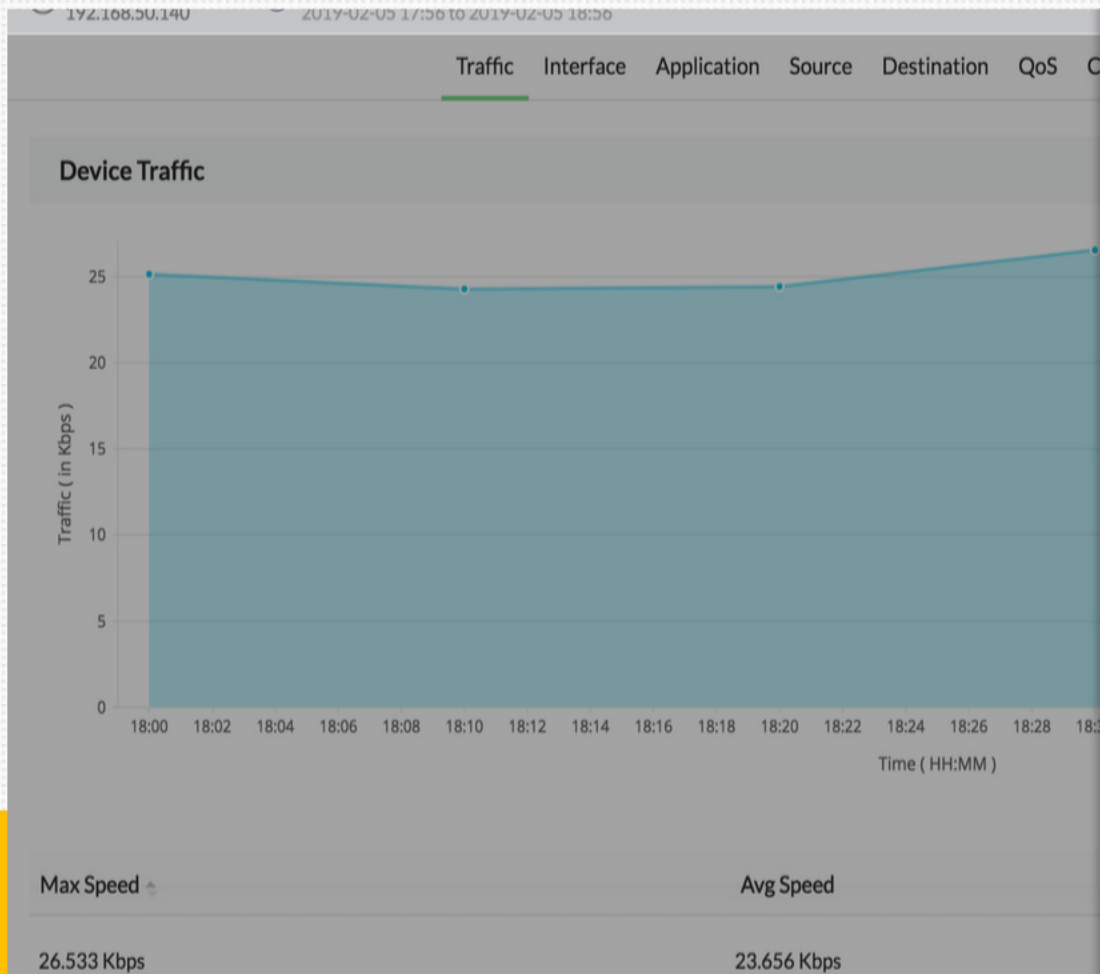
Report Time	Base Volume	Base Cost	Additional Volume	Additional Cost
01/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
02/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
03/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
04/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
05/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
06/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
07/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
08/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
09/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
10/01/18 19:05	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD
11/01/18 02:09	399.000 Bytes	10.0 USD	20.000 Bytes	50.0 USD

+ Quick links



**Prioritizing data and traffic
shaping: Optimization made
easy**

Filter out excess router traffic by blocking or restricting IPs / IP networks with ACL



Add ACL

Type: Standard Extended

Access: Permit Deny

Criteria:

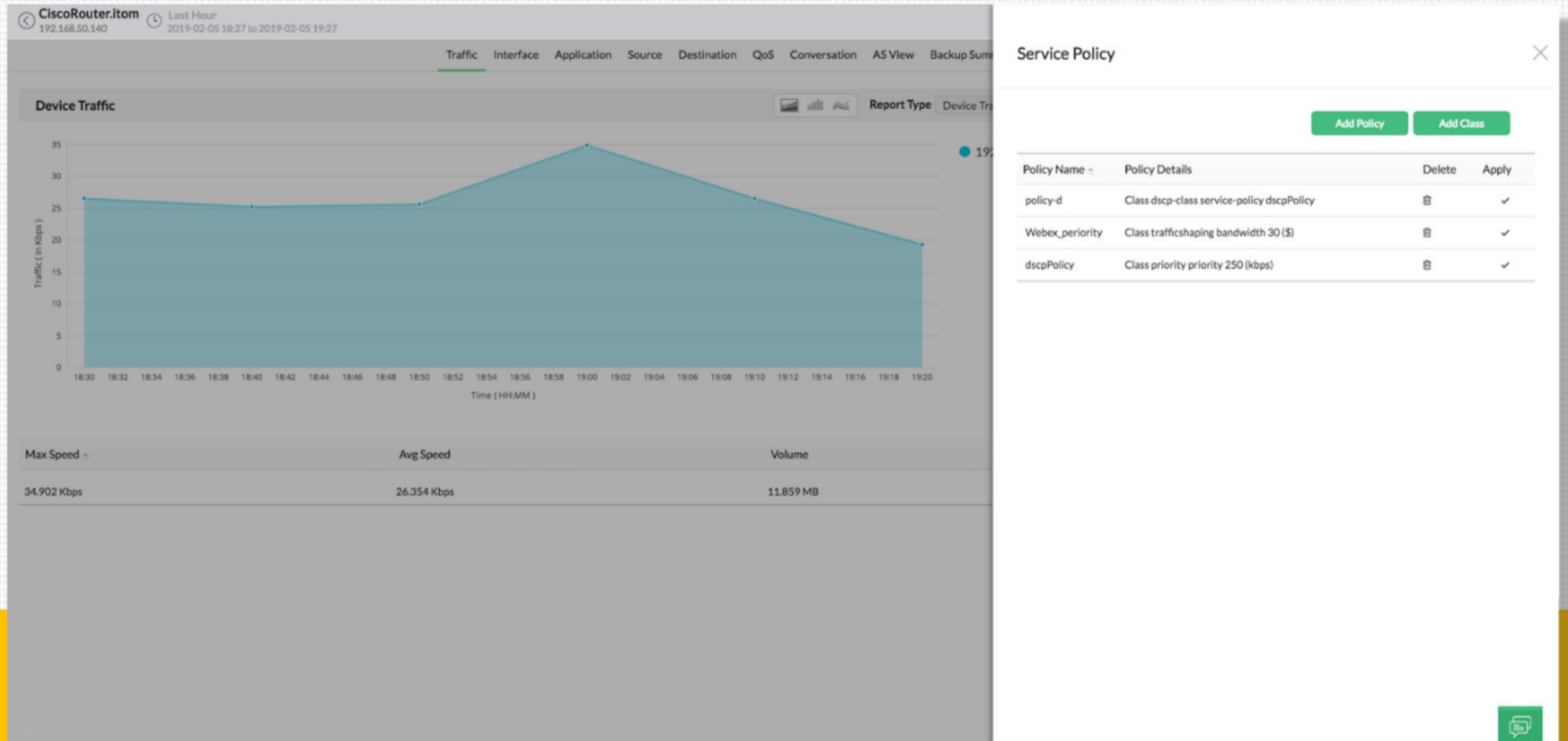
- Source Host: IP Address
- Destination Host: IP Address

ACL Name: 101

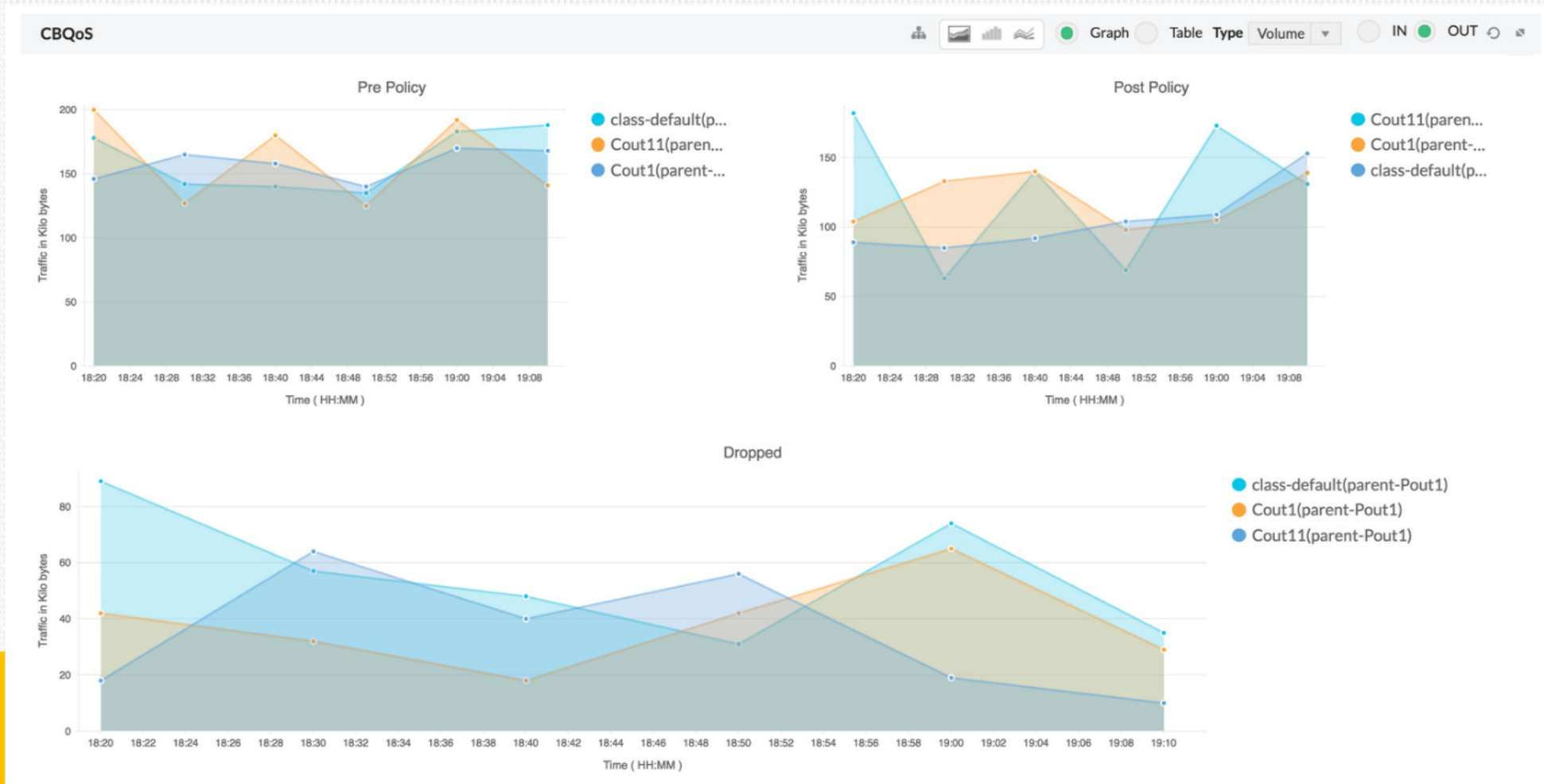
Protocol: ICMP

Buttons: Cancel, Save

Manage your service policies and limit access to apps based on priority with Service Policies



Validate QoS policies with CBQoS





**Cumulative traffic
monitoring: Enhancing
bandwidth management**

Categorizing traffic usage

Department

Branches

Network subnet

Related apps

VLAN

Sort traffic usage by Groups

Interface

IP

Application

DSCP

SSID

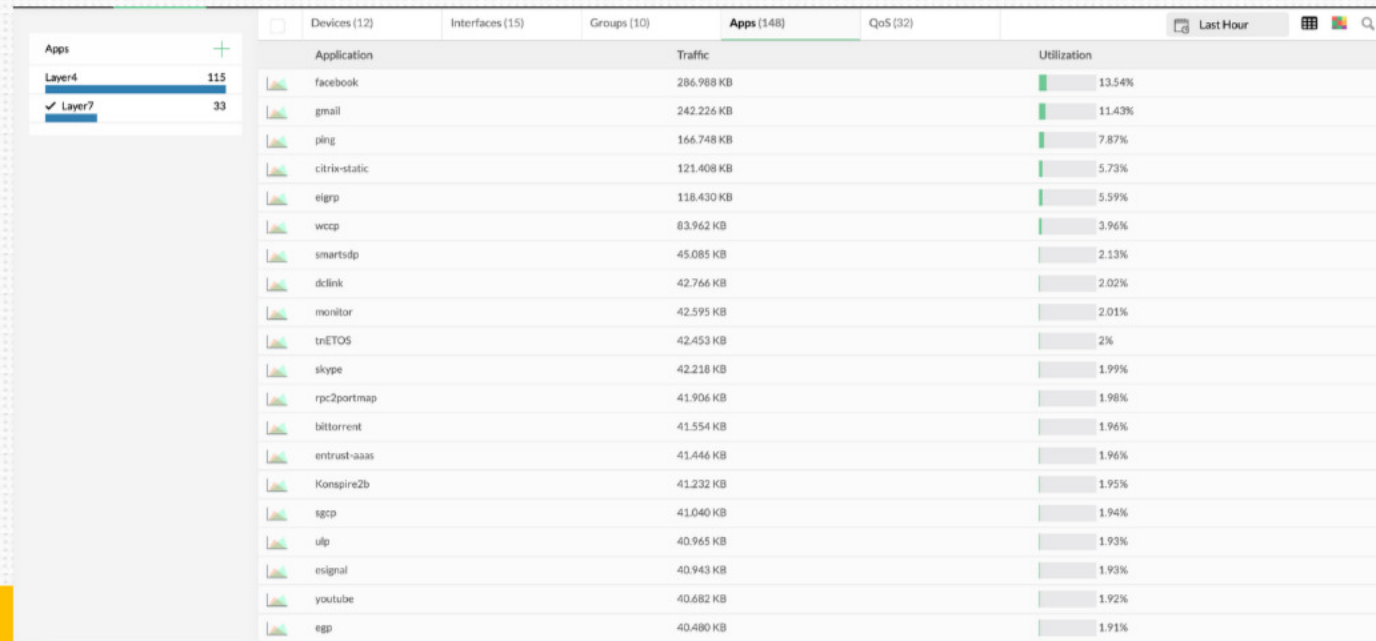
SSID

Monitor combined bandwidth usage to get better picture of traffic consumption.

Provide access to operators based on groups.

Provide better visibility to improve troubleshooting.

Monitor custom applications



The screenshot displays a network monitoring dashboard with a sidebar on the left and a main table. The sidebar shows 'Apps' with a plus sign, 'Layer4' with 115 items, and 'Layer7' with 33 items. The main table has tabs for 'Devices (12)', 'Interfaces (15)', 'Groups (10)', 'Apps (148)', and 'QoS (32)'. The 'Apps (148)' tab is active, showing a table with columns for 'Application', 'Traffic', and 'Utilization'. The 'Utilization' column includes a green progress bar and a percentage value.

Application	Traffic	Utilization
facebook	286.988 KB	13.54%
gmail	242.226 KB	11.43%
ping	166.748 KB	7.87%
citrix-static	121.408 KB	5.73%
elgrp	118.430 KB	5.59%
wccp	83.962 KB	3.96%
smartsdp	45.085 KB	2.13%
dclink	42.766 KB	2.02%
monitor	42.595 KB	2.01%
tnETOS	42.453 KB	2%
skype	42.218 KB	1.99%
rpc2portmap	41.906 KB	1.98%
bittorrent	41.554 KB	1.96%
entrust-aaas	41.446 KB	1.96%
Konspire2b	41.232 KB	1.95%
sgcp	41.040 KB	1.94%
ulp	40.965 KB	1.93%
esignal	40.943 KB	1.93%
youtube	40.682 KB	1.92%
egp	40.480 KB	1.91%

➤ Application mapping for _App

Interface > Application > _App > Show port (show port needs raw data enabled).

Map application and define IP address/ IP network/ IP range.

➤ Application mapping for custom apps

Settings > NetFlow > Mapping > Application List > Add

Username - IP Mapping

NetFlow

Basic Settings

Storage Settings

Groups Settings

Mappings

IP Mapping

LAN IP Settings

Alert Profiles

Notification Templates

NBAR

CBQoS

Attacks

NetFlow Generator

License Management

Flow Filter Settings

Network Mapping

Data Unit

WAAS Settings

IP Mapping

Disable DHCP Mapping





Import

Active Directory

Manual Mapping

DHCP

Import IP address - Name configurations from DHCP servers logs to assign names to IP addresses.

Profile Name	Assigned Devices	Status	Imported Time	Schedule Details	Actions	View List	Q
maha-Dhcp	192.168.43.121	Import of log file completed	02 Jul 2021 15:40:59	-	  		

- AD Mapping
- Manual
- Mapping
- DHCP

Cloud Services

NetFlow

Basic Settings

Storage Settings

Groups Settings

Mappings

UserName-IP Mapping

LAN IP Settings

Alert Profiles

NBAR

CBQoS

Attacks

NetFlow Generator

License Management

WLC License Management

Attacks License Management

Flow Filter Settings

Data Unit

WAAS Settings

Map

Add

Application



























Services

DSCP

AS View

Cloud Services

Define custom Cloud Services based on IP and monitor critical Cloud Services running in your network.

Cloud Service Name	Category	Network Start	Network End	Add Date	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
MediaFire	File Sharing	104.16.xx.xx	104.16.203.xx	2019-12-18	 
SugarSync	File Sharing	208.94.xx.xx	208.94.4.xx	2018-12-17	 
Office 365	File Sharing	40.84.xx.xx	40.84.199.xx	2015-03-12	 
4shared	File Sharing	204.155.xx.xx	204.155.149.xx	2018-05-29	 
Sendspace	File Sharing	69.31.xx.xx	69.31.136.xx	2015-03-12	 
Hightail	File Sharing	35.165.xx.xx	35.165.148.xx	2019-09-27	 
Carbonite	Online Storage	45.60.xx.xx	45.60.171.xx	2019-09-27	 
CrashPlan	Online Storage	216.17.xx.xx	216.17.8.xx	2015-03-12	 
Mozy	Online Storage	52.170.xx.xx	52.170.7.xx	2019-07-10	 
Flickr	Arts and Entertainment	13.35.xx.xx	13.35.209.xx	2019-12-18	 
Photobucket	Photo Sharing	209.17.xx.xx	209.17.68.xx	2015-03-12	 
Shutterfly	Photo Sharing	136.179.xx.xx	136.179.236.xx	2015-03-12	 
Pinterest	Photo Sharing	72.52.xx.xx	72.52.10.xx	2015-03-12	 



Proactive management

Setting up Alerts

Real - time alerts

Aggregated alerts

- Preconfigured alerts (Link down / No flow)
- Threshold based alerts

- **Get notified via Email, SMS, tickets, Email-based SMS, Chat, Run a Program, Syslog Profile, Trap Profile, Web Alarm**

Create and manage Notification Templates to receive E-mail / SMS alerts, web alarms, log tickets or SNMP traps / syslogs.

Notification Template Types

Choose the template type you would like to receive any fault in your network or devices.



Email

Get notified by an email alert when an alarm is generated.



Email based SMS

Get notified by an email alert when an alarm is generated.



SMS

Get notified by SMS alert when an alarm is generated.



Chat

Get notified by slack when an alarm is generated.



Run Program

Lets you execute a script/ program automatically when there is an alarm.



Log a Ticket

Lets you log trouble tickets in ServiceDesk Plus/ ServiceNow when an alarm is generated.



Web Alarm

Get notified with a sound alert when a critical alarm is generated.



SysLog Profile

Get notified by SysLog messages when this profile is triggered based on the configured criteria.



Trap Profile

This profile allows you to receive SNMP traps when it is triggered based on the configured criteria.

Third Party Integrations

General Settings

- Mail server settings
- SMS Server Settings
- Proxy Server Settings
- User Management
- Authentication
- Server Settings
- System Settings
- Rebranding
- Device Snapshot Settings
- Security Settings
- Privacy Settings
- Third Party Integrations**
- Self Monitoring
- SSH Settings
- Mobile App

Third Party Integrations



ServiceDesk Plus

This integration automates alarm to ticket creation, asset synchronization, and maintenance scheduling. When NetFlow Analyzer raises an alarm, a corresponding ticket is auto-generated in ServiceDesk Plus. [Learn more](#)

Help Desk

[+ Configure](#)



ServiceDesk Plus Cloud

Cloud version of ServiceDesk Plus. Automate ticket creation and asset synchronization. On configuring this integration, alarms from NetFlow Analyzer will automatically be created as tickets in ServiceDesk Plus.

Help Desk

[+ Configure](#)



ServiceNow

Streamline ITOM with NetFlow Analyzer's out-of-the-box integration with ServiceNow. Automatic incident logging and bi-directional data synchronization between NetFlow Analyzer and ServiceNow ensures effortless, real-time alert management. [Learn more](#)

Help Desk

[+ Configure](#)



Slack

This integration helps IT teams customize alert handling tasks while reducing downtime. Once integrated with NetFlow Analyzer, Slack alerts can be configured in a notification profile, or as a step in a Workflow. [Learn more](#)

Chat

[+ Configure](#)



Applications Manager

With the Applications Performance Management integration in NetFlow Analyzer, you can proactively monitor business application servers and help businesses ensure their revenue-critical applications meet end-user requirements. [Learn more](#)

Monitoring

[+ Configure](#)



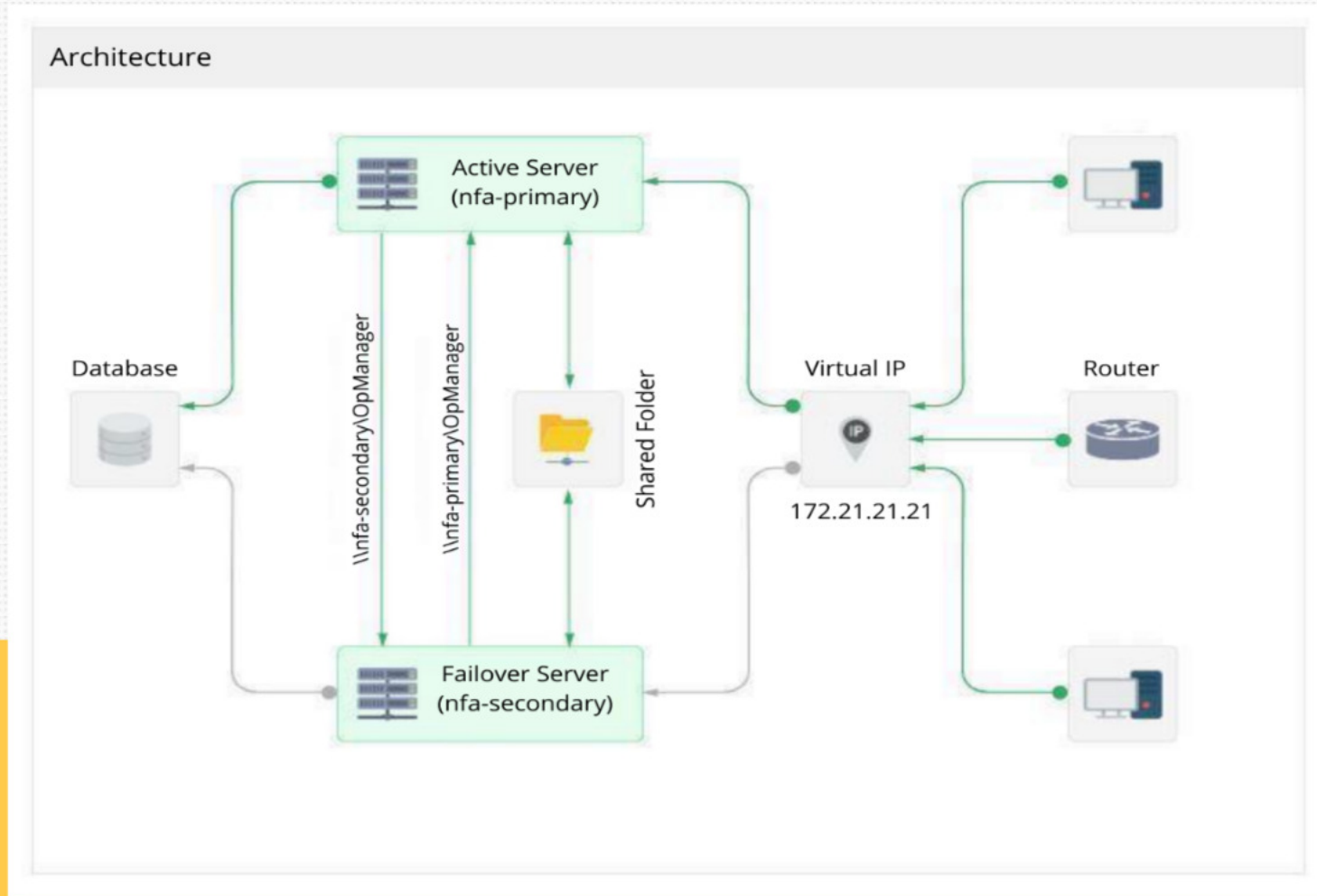
Jira Service Desk(On-Premise)

This integration enables users to receive alerts from NetFlow Analyzer and register them as issues in Jira Service Desk, the comprehensive service request management solution.

Help Desk

[+ Configure](#)

Ensure your network is always monitored with NetFlow Analyzer's Failover





New Updates and Integrations

Applications Manager Integration

Application Manager - Configuration

Applications Manager Integration

ManageEngine Applications Manager is a server and application performance monitoring software. It helps monitor the performance of various components of an application and helps troubleshoot production issues quickly. With Applications Manager, you get a holistic view of your IT resources while ensuring more responsive applications.

APM - Server Details

http IP Address/Server Name : 9090

API Key

Fetch Services Fetch DNS Names

Fetch details from the APM server every 24 hours

By clicking Save, you acknowledge that you have read & accepted the [Privacy Statement](#) of ManageEngine.

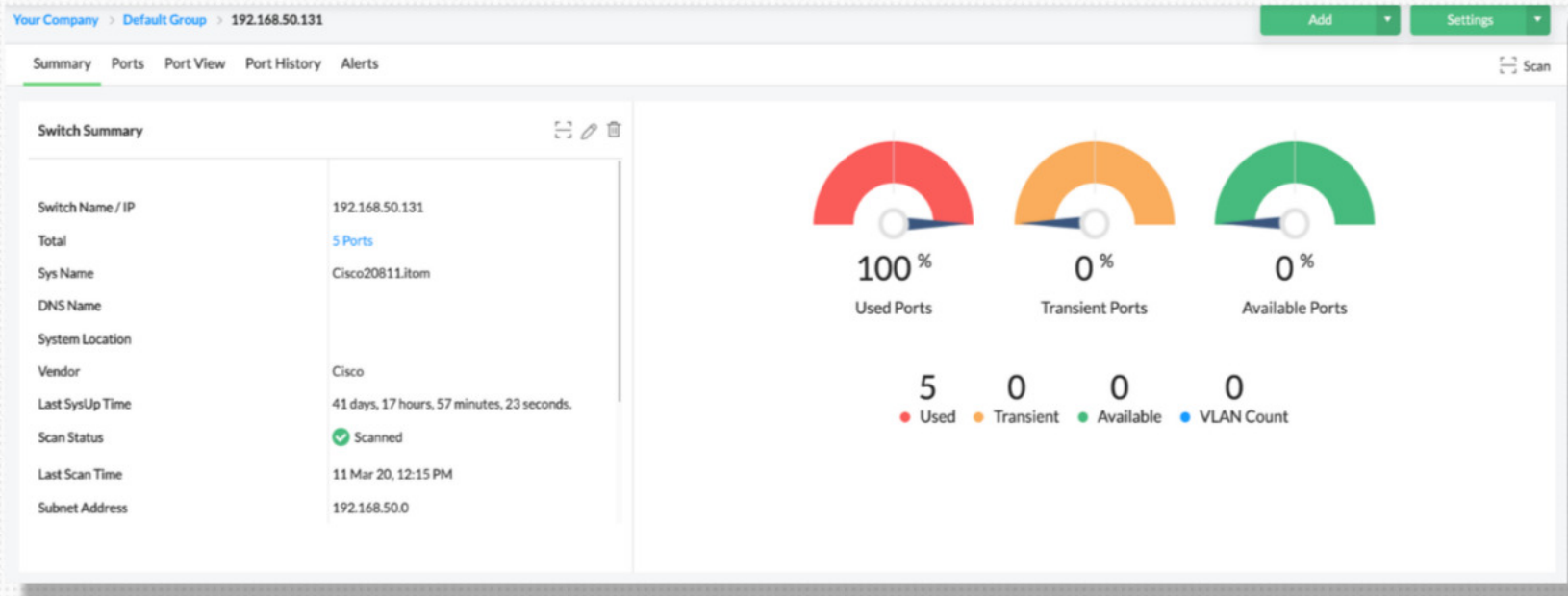
Sync now

Back

Save

- Synchronizing application details (Port, Protocol, IP)
- Categorize these critical applications separately
- Monitor application traffic by to Source, Destination, Byte & more.

OpUtils Integration



- Visibility into network ports
- Ability to inspect IP addresses
- Intuitive widgets

Cloud Traffic Monitoring - Monitor and manage AWS resources and virtual private clouds in your network.

Discovery

- Export Flow
- Export Cloud Flow
- NCM Discovery
- Discovery Report
- Credentials
- Inventory Updater
- Non Inventoried Devices

AWS credentials

Monitor AWS interfaces and analyze their traffic in your network using AWS credentials.

[Add](#)

AWS Username	Interface Count	Actions		
▼ aws	5			
Interface Name	Status	Region Name	Flow Log ID	Export Flow Logs
eni-0c751234737792d08	In-Use	ap-south-1	fl-0008d0c50bcd235a9	<input checked="" type="checkbox"/>
eni-0312cb732a499ce96	In-Use	ap-south-1	fl-0538cf969cf18a995	<input checked="" type="checkbox"/>
eni-0d73e9d1ea840a7c3	Available	ap-south-1	fl-0ef7b6d63cfd2a34	<input checked="" type="checkbox"/>
eni-057a0b8dac09489c5	In-Use	ap-south-1	fl-05c1dcd8a8c487c44	<input checked="" type="checkbox"/>
eni-0869450aac8286554	Available	ap-south-1	fl-0c13110e120ef26fc	<input checked="" type="checkbox"/>

Webhook Integration with NetFlow Analyzer

The screenshot displays the NetFlow Analyzer web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'WLC', 'Security', 'IPAM', 'IPSLA', 'Alarms', 'Maps', 'Reports', and 'Settings' (which is highlighted). Below this, a secondary navigation bar shows 'General Settings', 'Discovery', 'Monitoring', 'Tools', 'NetFlow' (highlighted), and 'ITOM Agent'. The left sidebar lists various settings categories: 'NetFlow', 'Basic Settings', 'Storage Settings', 'Groups Settings', 'Mappings', 'IP Mapping', 'LAN IP Settings', 'Alert Profiles', 'Notification Templates', 'NBAR', 'CBQoS', 'Security Analytics', 'License Management', 'Flow Filters', 'HighPerf Addon Settings', 'Data Unit', and 'WAAS Settings'. The main content area is titled 'Notification Templates > Invoke a Webhook'. It includes a descriptive text: 'Webhooks are user-defined callbacks via HTTP. Use webhooks to push alarms to the specified URL when an event is triggered in the product.' The configuration fields are: 'Template Name' (text input), 'Hook URL' (text input with a dropdown set to 'POST' and a 'Enter the URL' placeholder), 'Data Type' (radio buttons for 'raw' (selected), 'form-urlencoded', and 'form-data'), 'Payload Type' (dropdown set to 'JSON'), 'Content-Type' (text input set to 'application/json'), 'Body Content' (text area containing a JSON template:

```
{  "NFASourceType": $NetFlowField(sourceType),  "NFAAlertProfileName": $NetFlowField(alertName)} 
```

), 'Request Headers' (a table with columns 'Header Name', 'Header Value', and 'Delete', currently empty with a 'No records to view.' message), 'User Agent (optional)' (text area), and 'Time out (seconds)' (text input).

Network Packet Sensor

Network Packet Sensor (NPS)

General Settings | Discovery | Monitoring | Tools | NetFlow | NCM | OpUtils | **ITOM Agent**

ITOM Agent

Network Packet Sensor

Network Packet Sensor Installation Key: 97A7*****295C

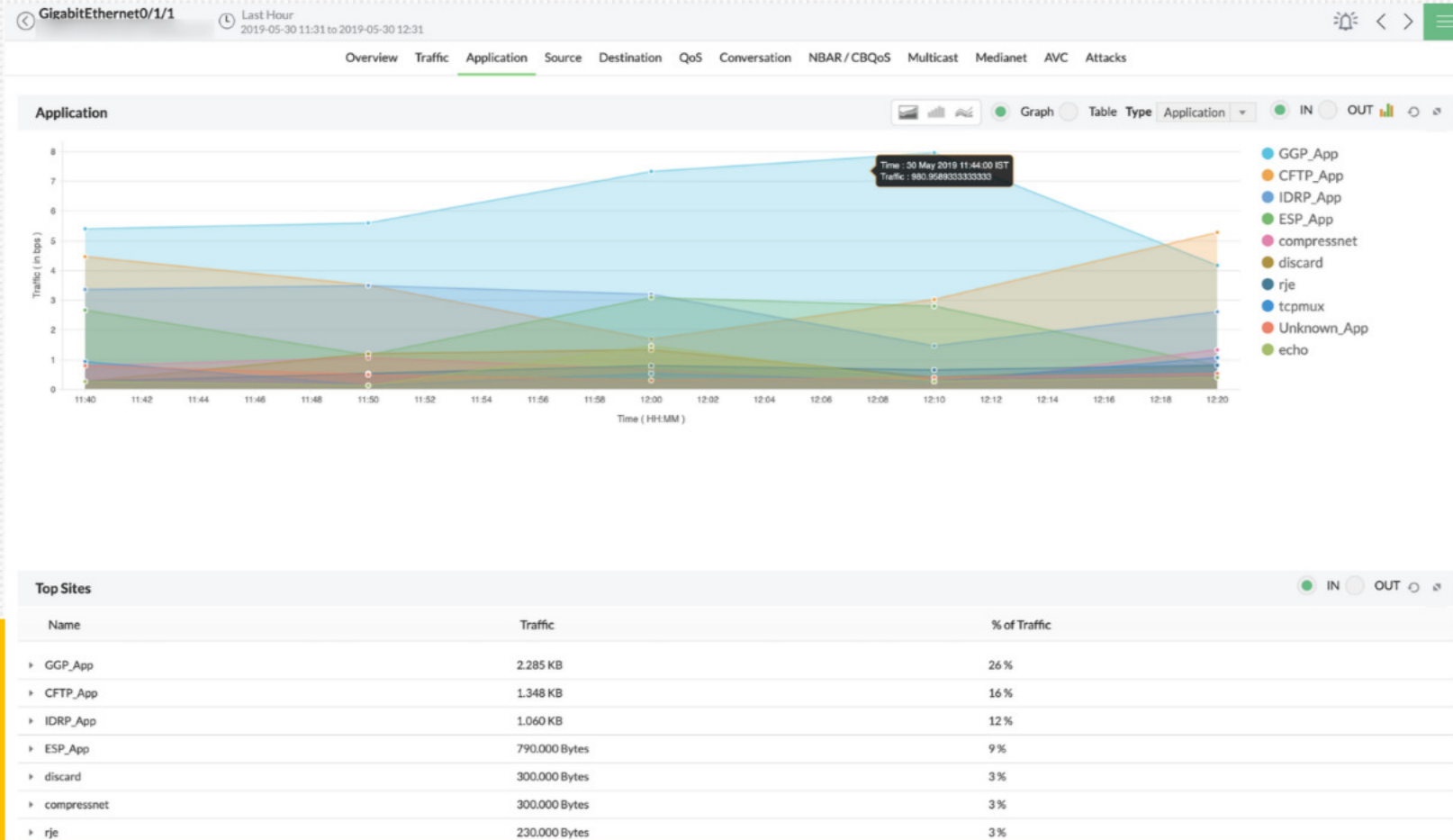
Network Packet Sensor
Network Packet Sensor is a tool that provides the combined benefits of NetFlow Generator and DPI Engine, which passively captures and translates raw network packets.

```
graph TD; subgraph NPS1 [Network Packet Sensor 1]; NG1[NetFlow Generator 1]; DE1[DPI Engine 1]; end; subgraph NPS2 [Network Packet Sensor 2]; DE2[DPI Engine 2]; end; subgraph NPS3 [Network Packet Sensor 3]; NG3[NetFlow Generator 3]; DE3[DPI Engine 3]; end; subgraph NPS4 [Network Packet Sensor 4]; NG4[NetFlow Generator 4]; end; NG1 --> NFA[NetFlow Analyzer]; DE1 --> NFA; DE2 --> NFA; NG3 --> NFA; DE3 --> NFA; NG4 --> NFA;
```

Reduce the hassle of installing more tools to monitor your server and network traffic. Install Network Packet Sensor now to monitor the traffic of servers and conduct packet-level inspection. [Learn more](#) | [Installation guide](#)

Download Network Packet Sensor Windows | Linux

NetFlow Generator

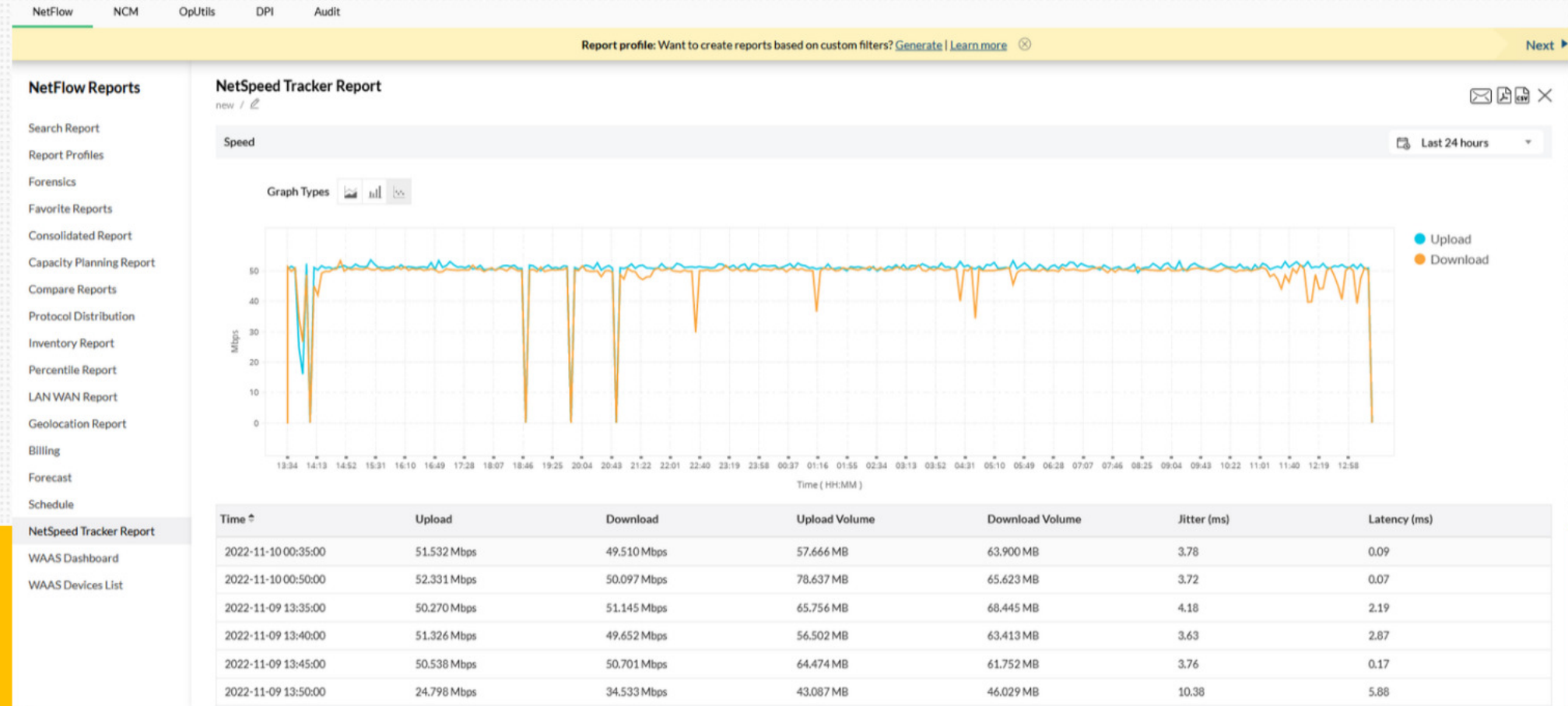


Deep Packet Inspection

DPI Engines		Application (22)	Source (2367)	Destination (22)	Conversation	UDP	Last Hour	
Source	Destination	Application	Src Port	Dst Port	Protocol	Traffic	Packets	
✓ nfa2kWin	172.24.147.112	224.0.0.251	mdns	5353	5353	UDP	23.139 MB	15957
	172.24.147.172	172.24.139.200	netbios-ns	137	137	UDP	6.305 MB	68532
	172.24.139.42	224.0.0.251	mdns	5353	5353	UDP	3.143 MB	2151
	172.24.144.184	224.0.0.251	mdns	5353	5353	UDP	1.577 MB	1152
	172.24.139.48	224.0.0.251	mdns	5353	5353	UDP	1.410 MB	1029
	172.24.139.27	172.24.139.200	netbios-ns	137	137	UDP	1.405 MB	15277
	8.8.8.8	201.201.201.201	Unknown_App	5041	5041	UDP	1.303 MB	4204
	172.24.146.109	172.24.139.200	netbios-ns	137	137	UDP	1.255 MB	13640
	172.24.151.112	172.24.139.200	netbios-ns	137	137	UDP	841.892 KB	9151
	172.24.152.200	224.0.0.251	mdns	5353	5353	UDP	752.310 KB	514
	172.24.151.112	224.0.0.251	mdns	5353	5353	UDP	736.548 KB	9209
	172.24.152.204	224.0.0.251	mdns	5353	5353	UDP	685.139 KB	469
	172.24.139.200	224.0.0.251	mdns	5353	5353	UDP	678.970 KB	8389
	172.24.151.76	172.24.139.200	netbios-ns	137	137	UDP	595.700 KB	6475
	172.24.151.76	224.0.0.251	mdns	5353	5353	UDP	573.589 KB	7158
	172.24.151.92	224.0.0.251	mdns	5353	5353	UDP	554.250 KB	376
	172.24.152.88	224.0.0.251	mdns	5353	5353	UDP	532.895 KB	2696
	172.24.139.200	224.0.0.251	mdns	5353	5353	UDP	509.130 KB	2607



NetSpeed Tracker





youtube.com/opmanagertechvideos



forums.manageengine.com/netflow-analyzer



<http://www.netflowanalyzer.com/help>



netflowanalyzer-support@manageengine.com



+1 (888) 720-9500 / +1 (408) 916 - 9400



THANK YOU

<https://www.manageengine.com/products/netflow/>

© 2023, Zoho Corp., ManageEngine - All rights reserved.