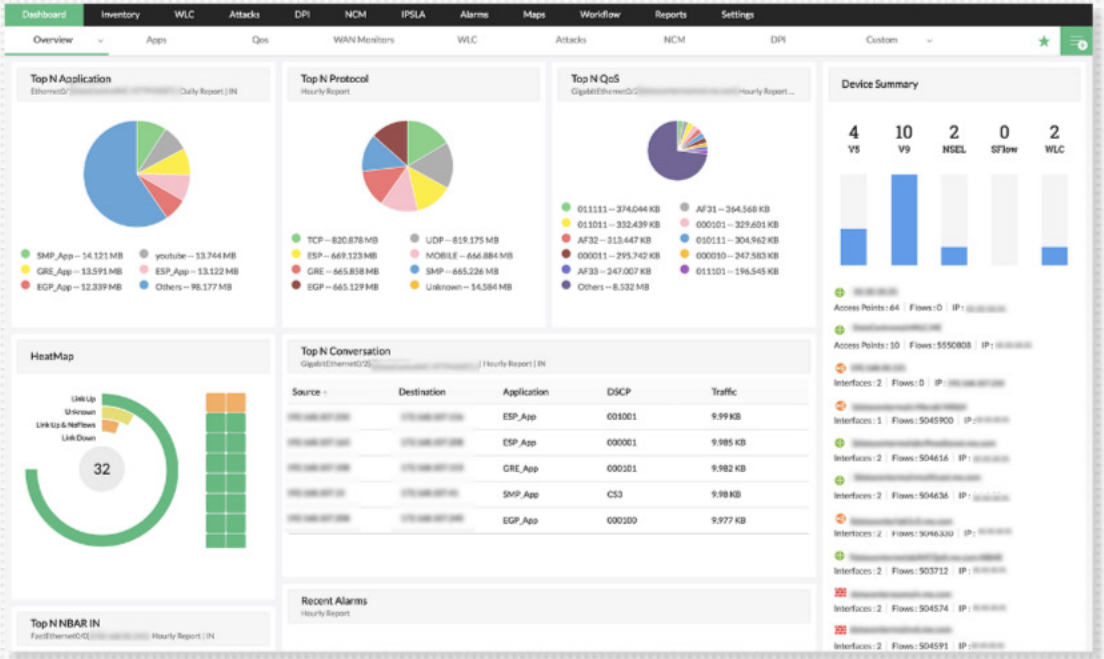
ManageEngine

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

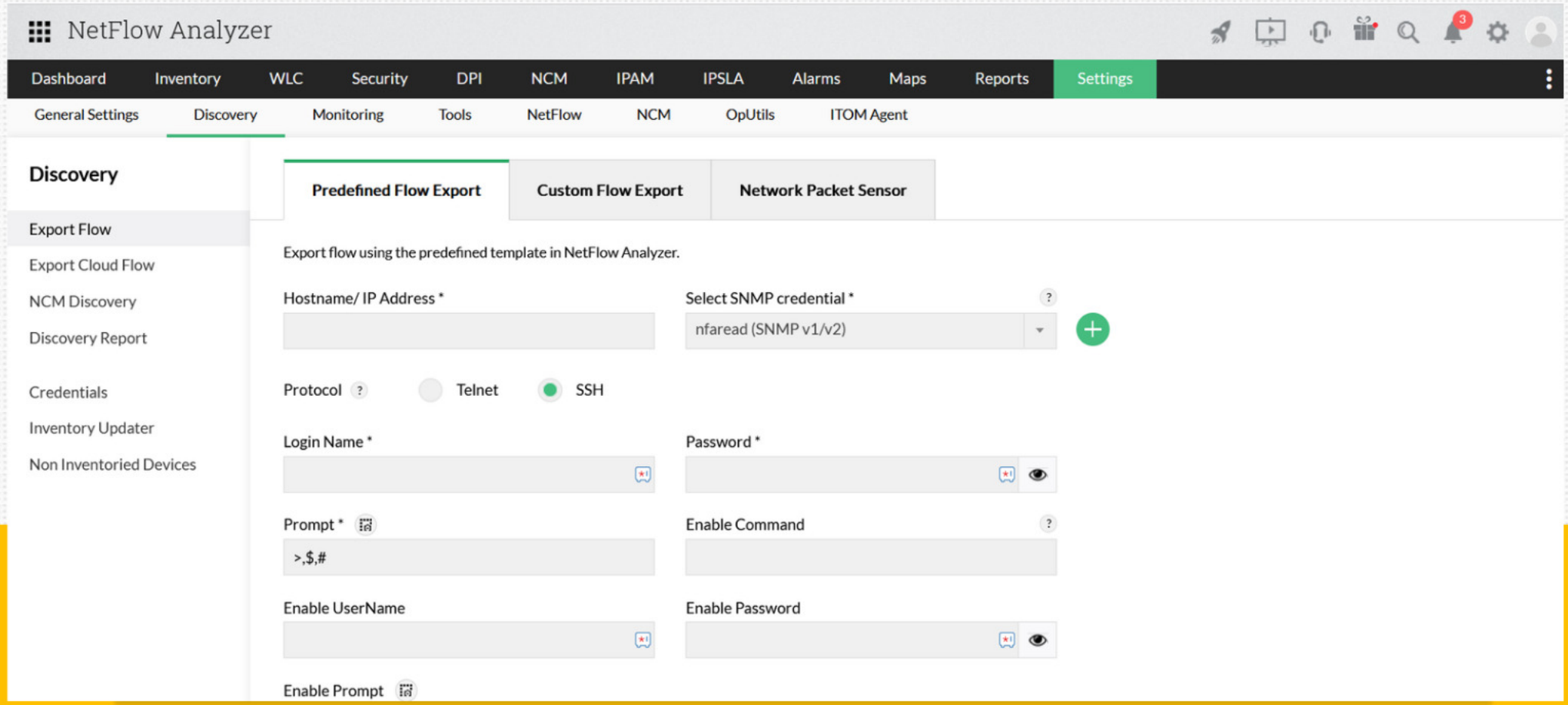
Security

Starting off with NetFlow monitoring!

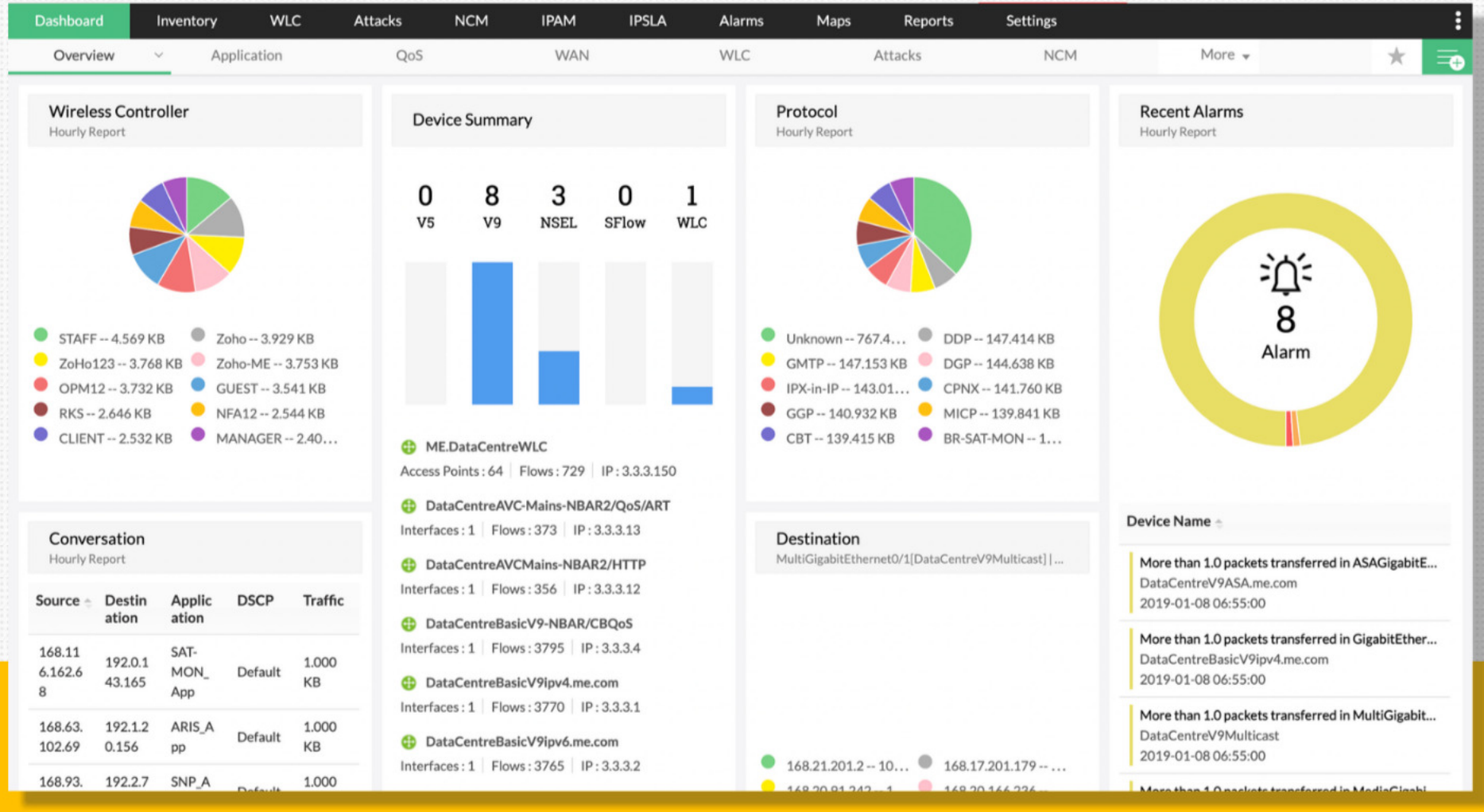
Flow export

Add Credentials → Executing the commands → Export flow

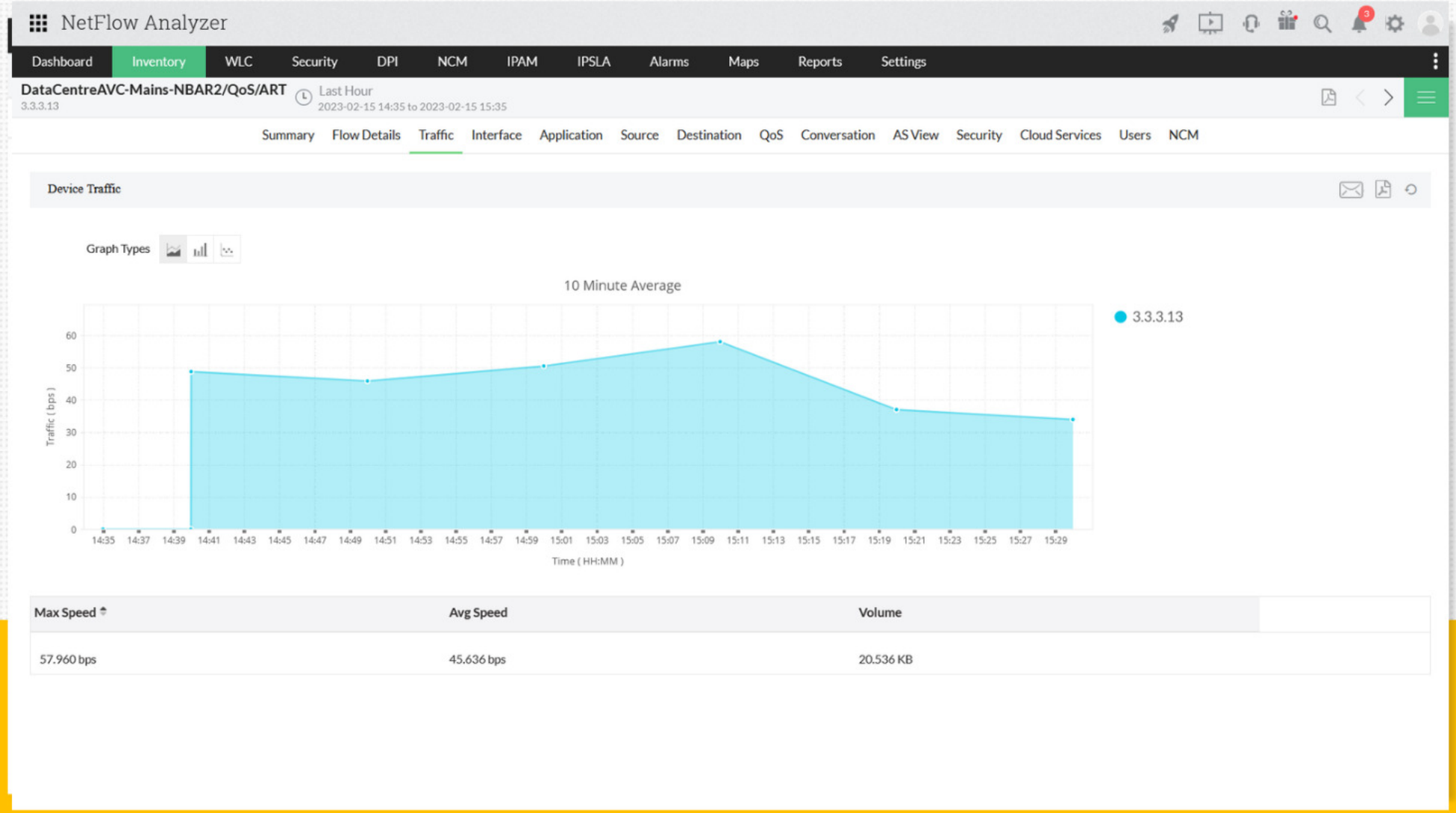
i. Predefined
ii. Custom
iii. Network Packet Sensor



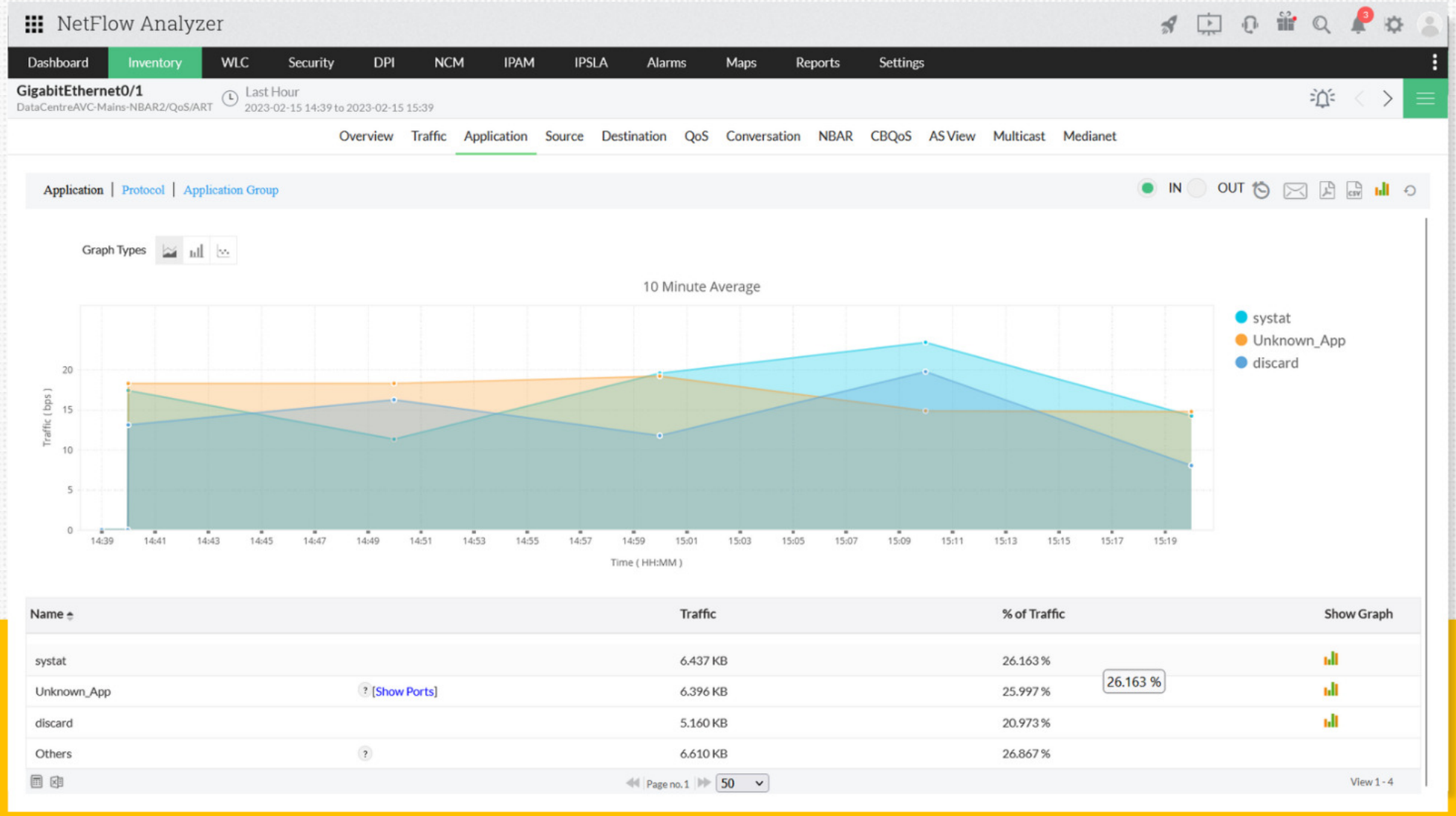
Dashboard & NOC view



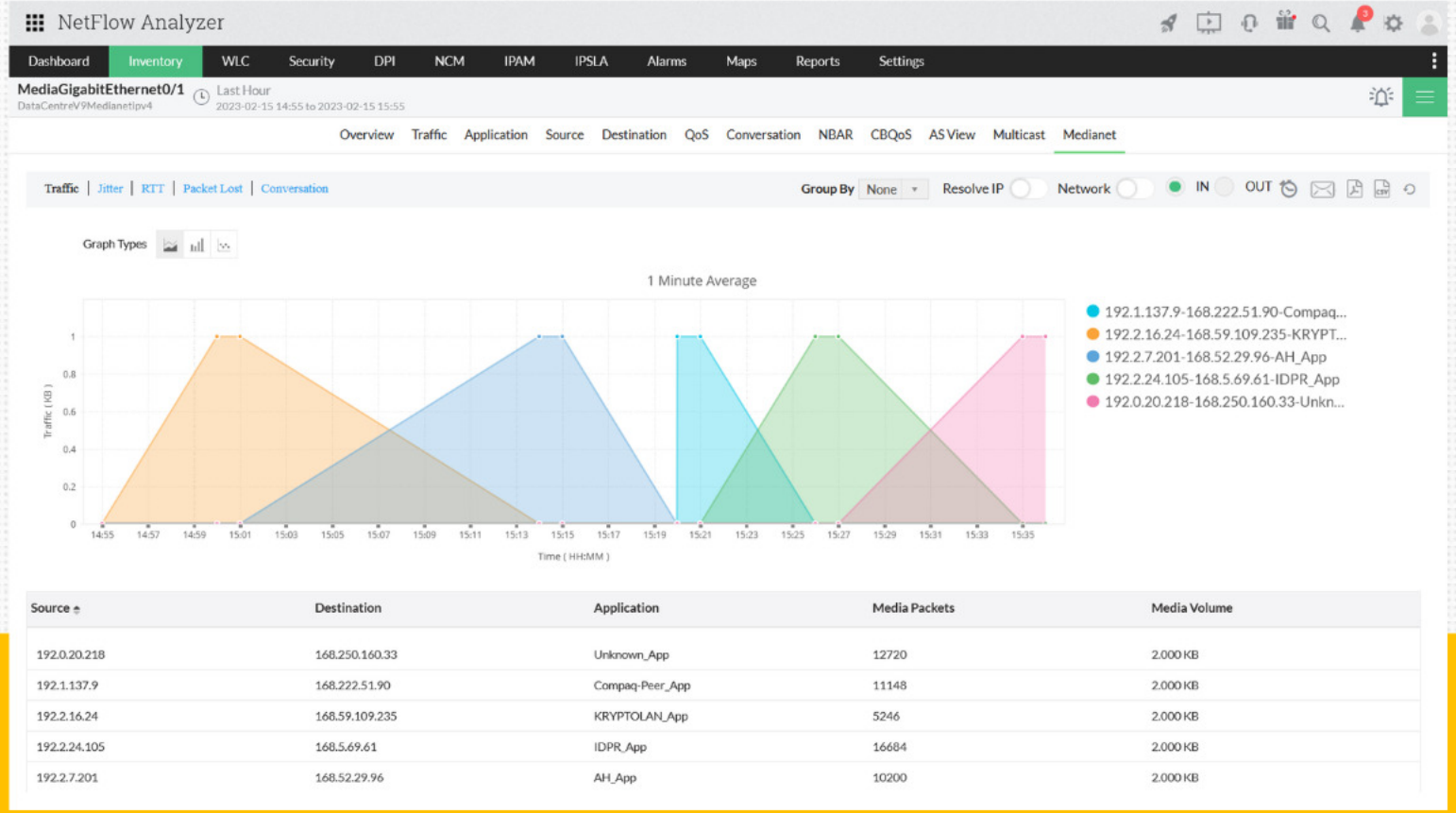
Device and Interface Traffic



Application traffic

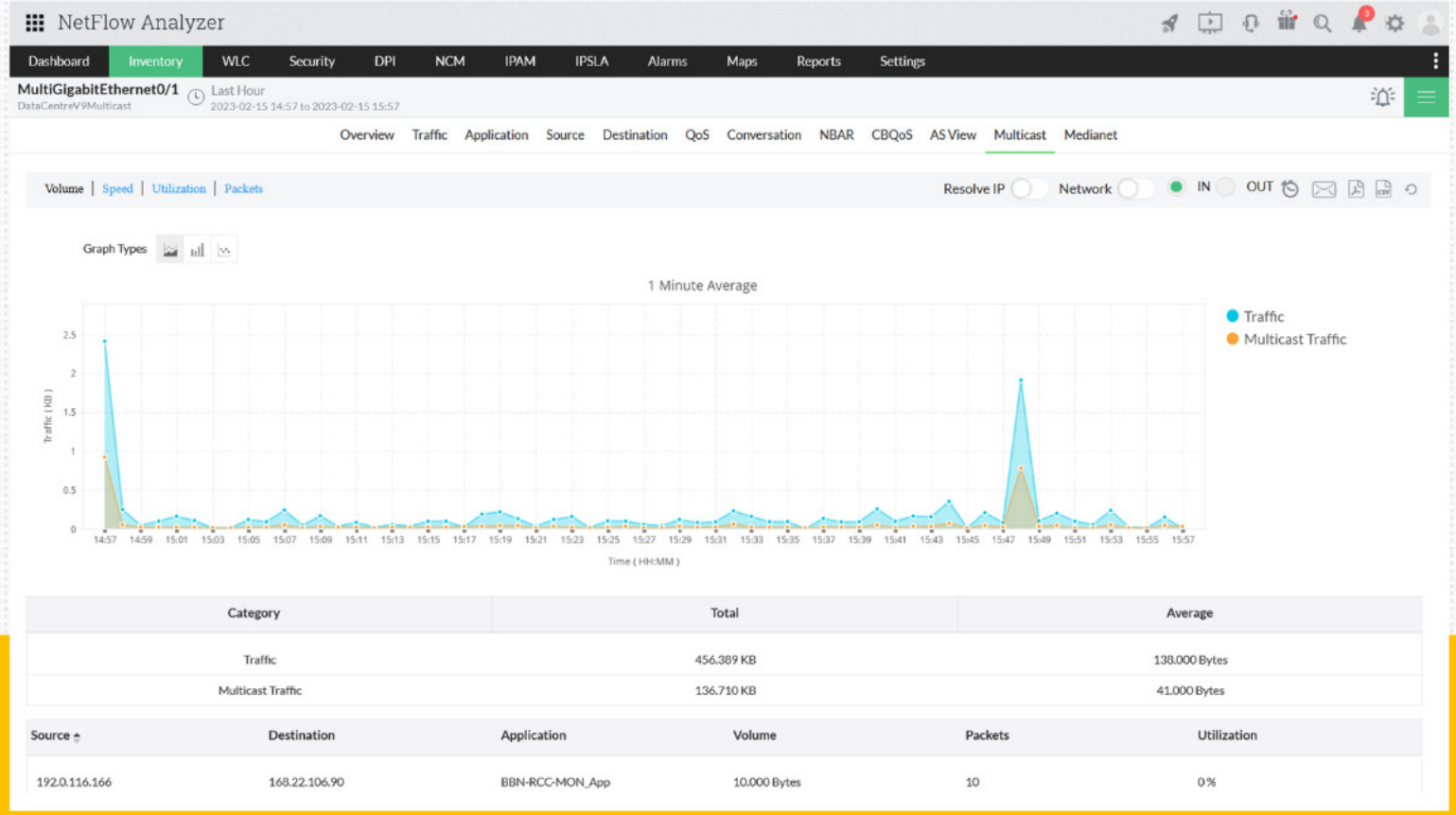


Medianet traffic monitoring



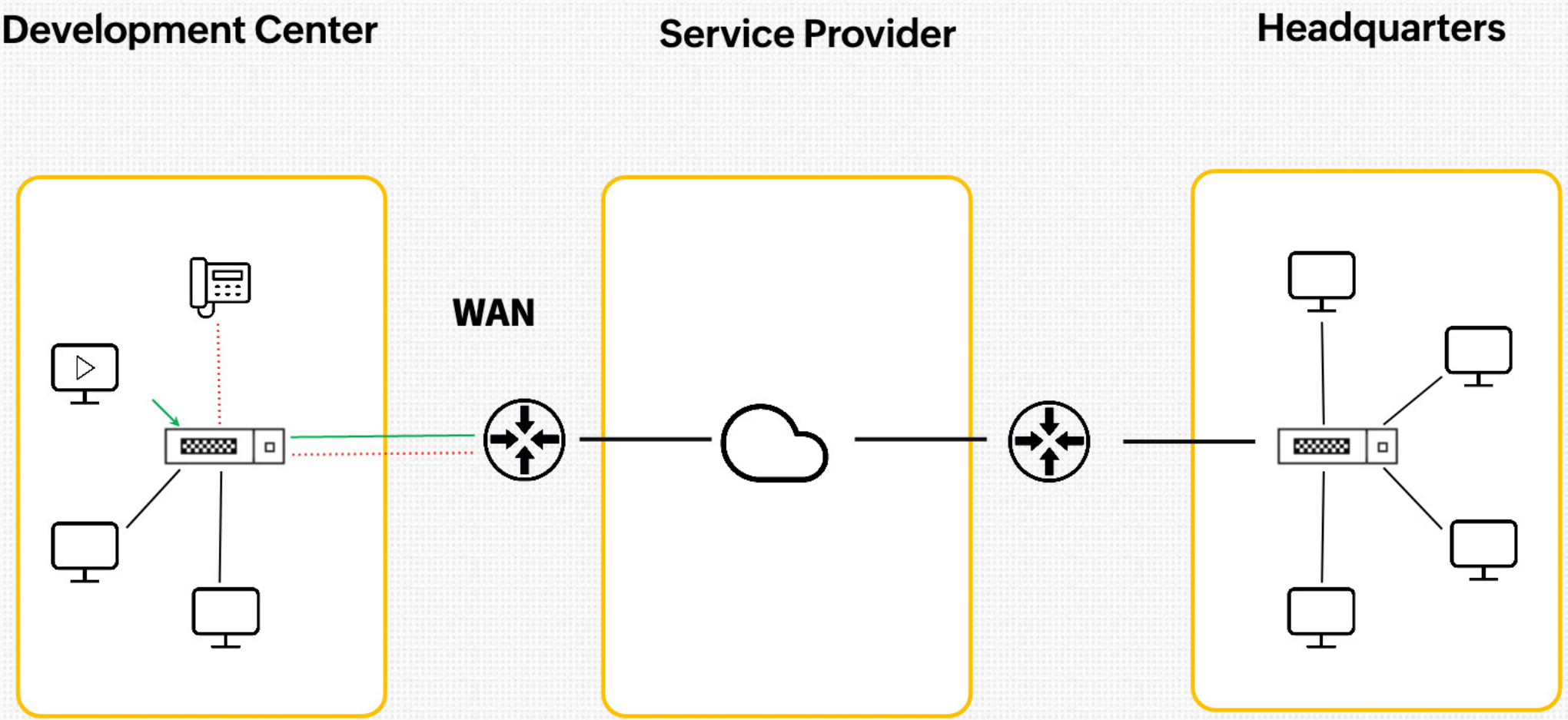
- Monitor media-rich traffic such as voice and video traffic for improving QoE.
- Measure performance statistics such as Jitter, Packet Loss, & RTT.

Multicast traffic monitoring



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

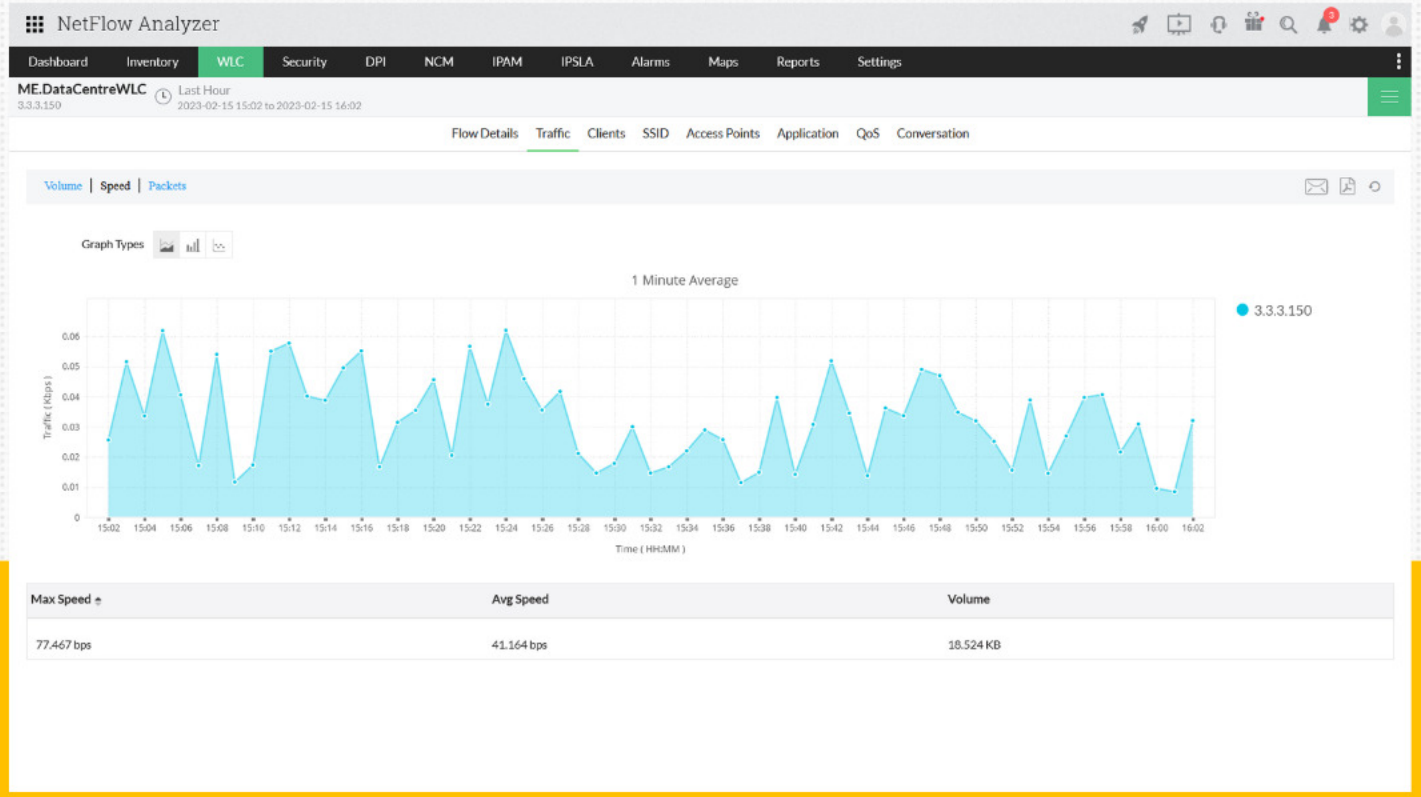
IPSLA Monitoring



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.

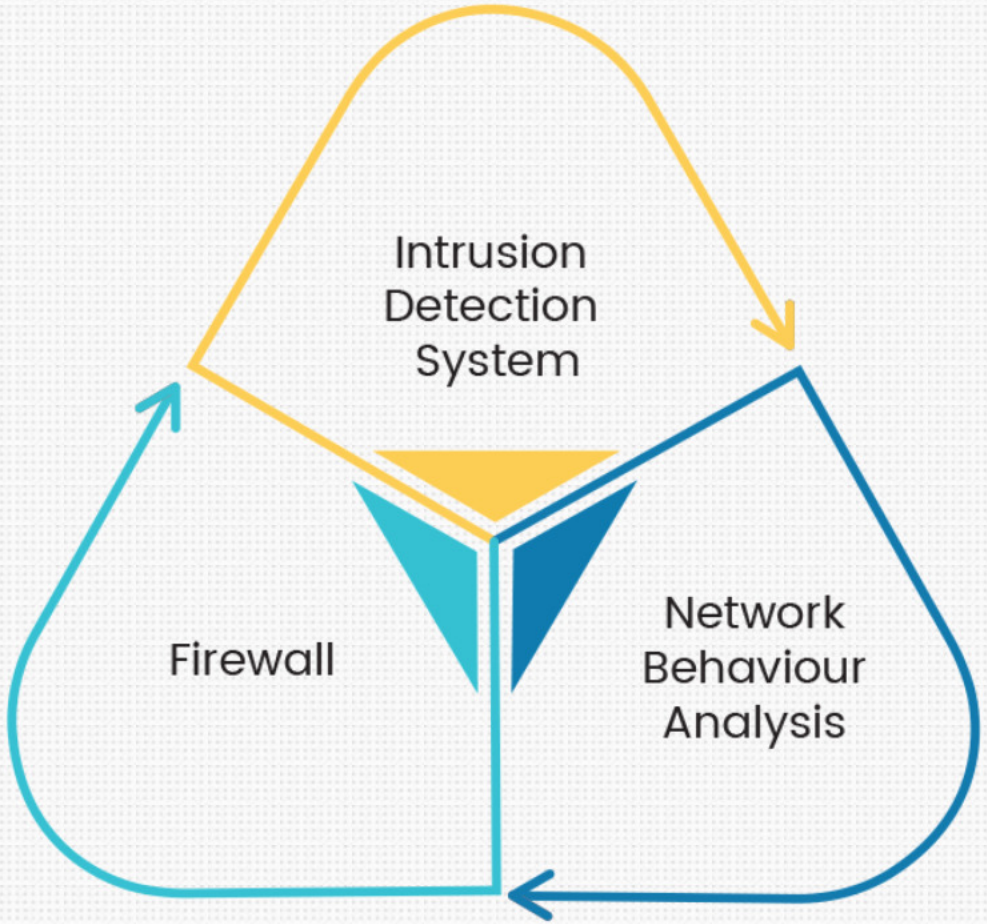
Wireless traffic monitoring



- 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

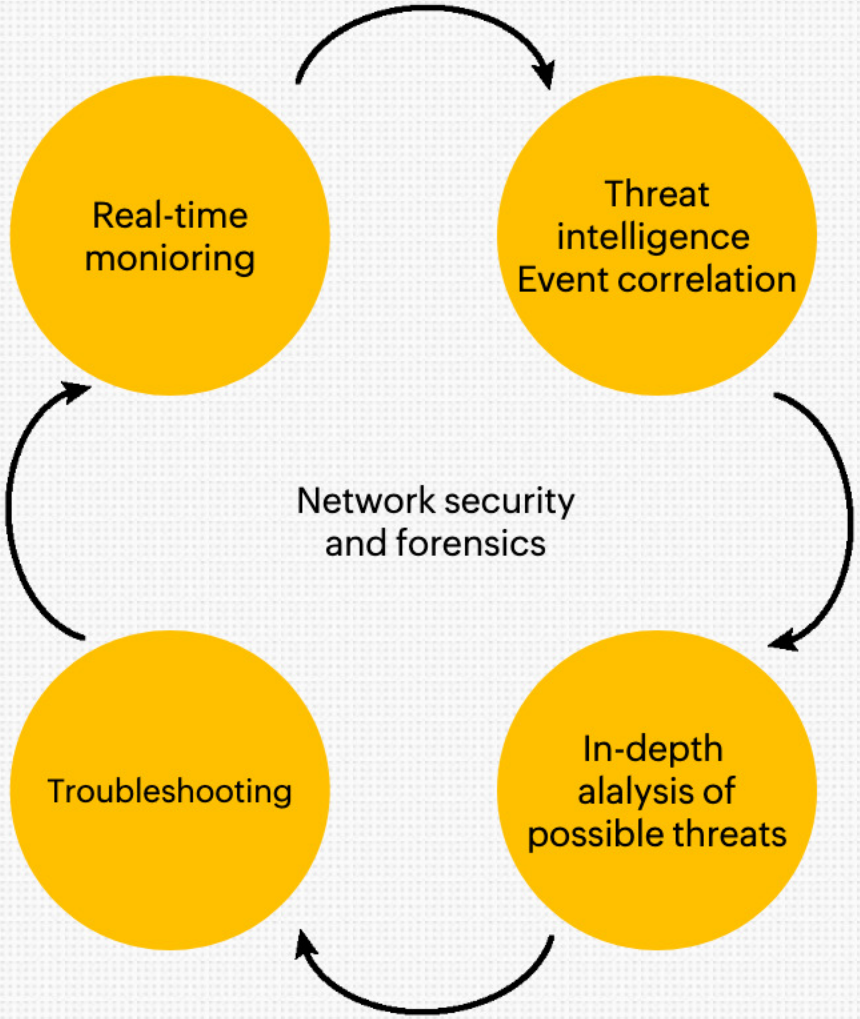


How does NetFlow Analyzer help?

Network Forensics

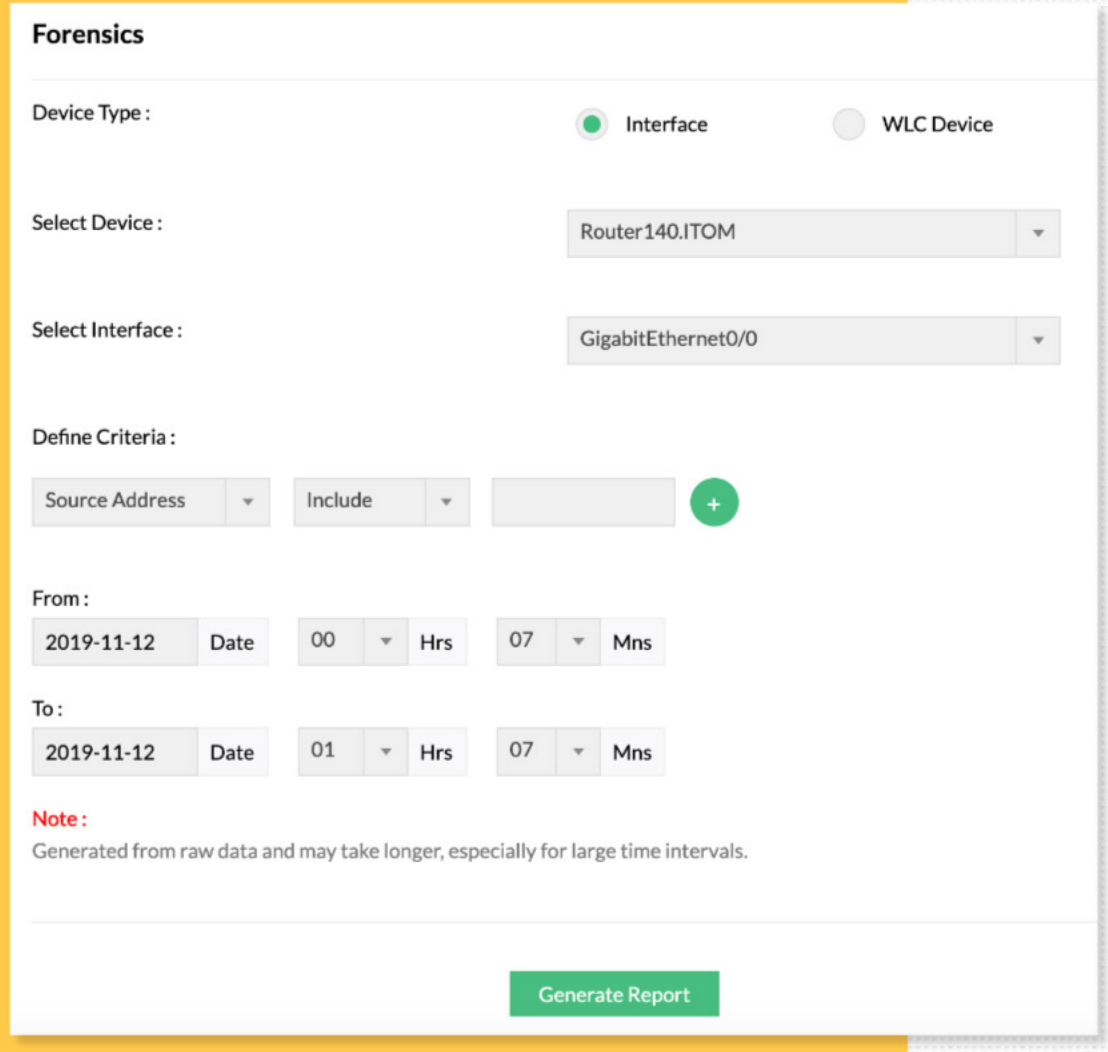
Security Module

Network forensics



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

Network forensics



- 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

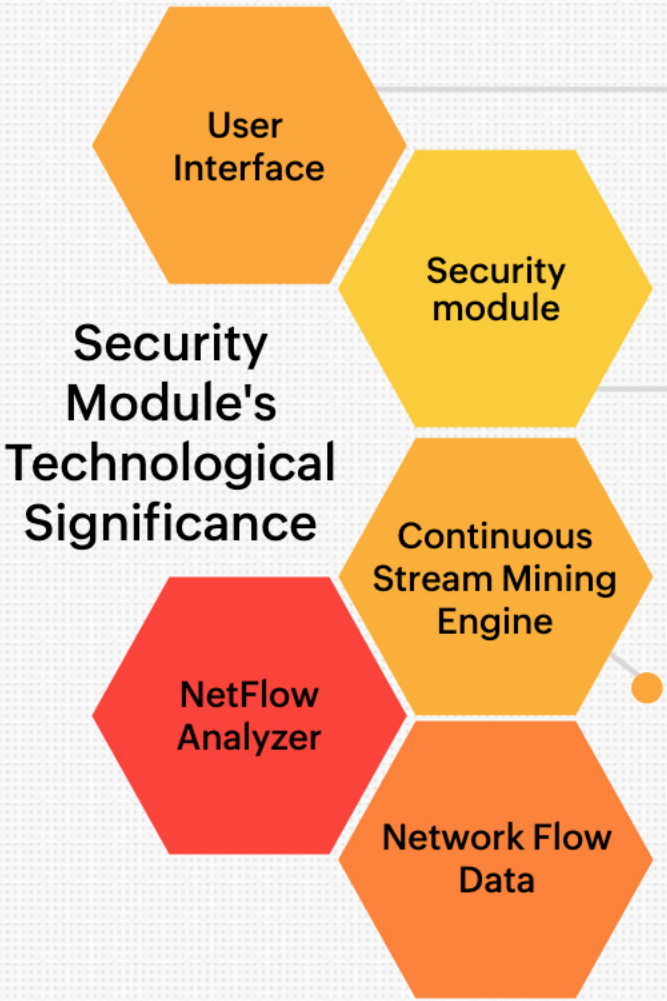
Security analytics

DDOS

Scan / Probes

Botnets

What is the Security Module?



- Simple Intuitive User Interface
- Effective Administration & Tuning
- Extensive Event Querying & Analysis
- Quick Overall Threat Assesment
- Detailed Forensic Investigation

- Real-time Network Security Event Monitoring
- Seamless Internal & Extemal Threat Monitoring
- Continuous Network Security Posture Assessment
  Context-Sensitive Zero-day Anomaly Detection
- Extensive Incident Details Collation & Reporting

- High Throughput & Low Latency Event Stream Processing
- Effective Work Load Distribution &Asynchronous Processing
- API Rich Framework for building High Performance Applications
- Rapid Rules Engine & Flexible Criteria Profiles
- Context-sensitive Resource Modeling, Complex Event Correlation, Advanced Mining Algorithms,...

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
TCP Fin Host Scan(Reverse)	60	2	58	Today 07 : 23 PM, IST	63	Warning
Malformed UDP Packets	75	10	92	Today 06 : 56 PM, IST	100	Major
TCP Syn_Fin Host Scan	60	2	60	Today 06 : 46 PM, IST	63	Warning
Malformed TCP Packets	80	11	94	Today 06 : 37 PM, IST	100	Major
TCP Syn_Fin Violations	82	14	91	Today 06 : 37 PM, IST	100	Major
Malformed TCP Packets	79	11	93	Today 06 : 37 PM, IST	100	Major
TCP Fin Violations	84	14	92	Today 06 : 36 PM, IST	100	Major
TCP Fin Violations	81	14	91	Today 06 : 36 PM, IST	100	Major
TCP Syn_Fin Violations	77	14	91	Today 06 : 36 PM, IST	100	Major
Malformed IP Packets	83	10	95	Today 06 : 31 PM, IST	100	Major
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

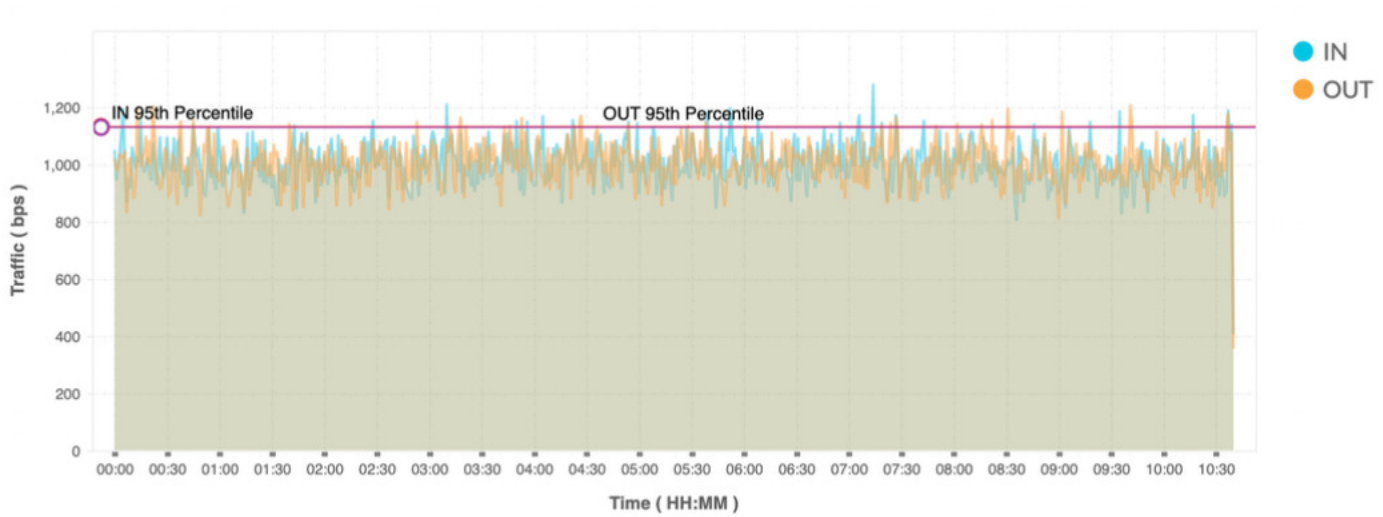
NetFlow Reports

- 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

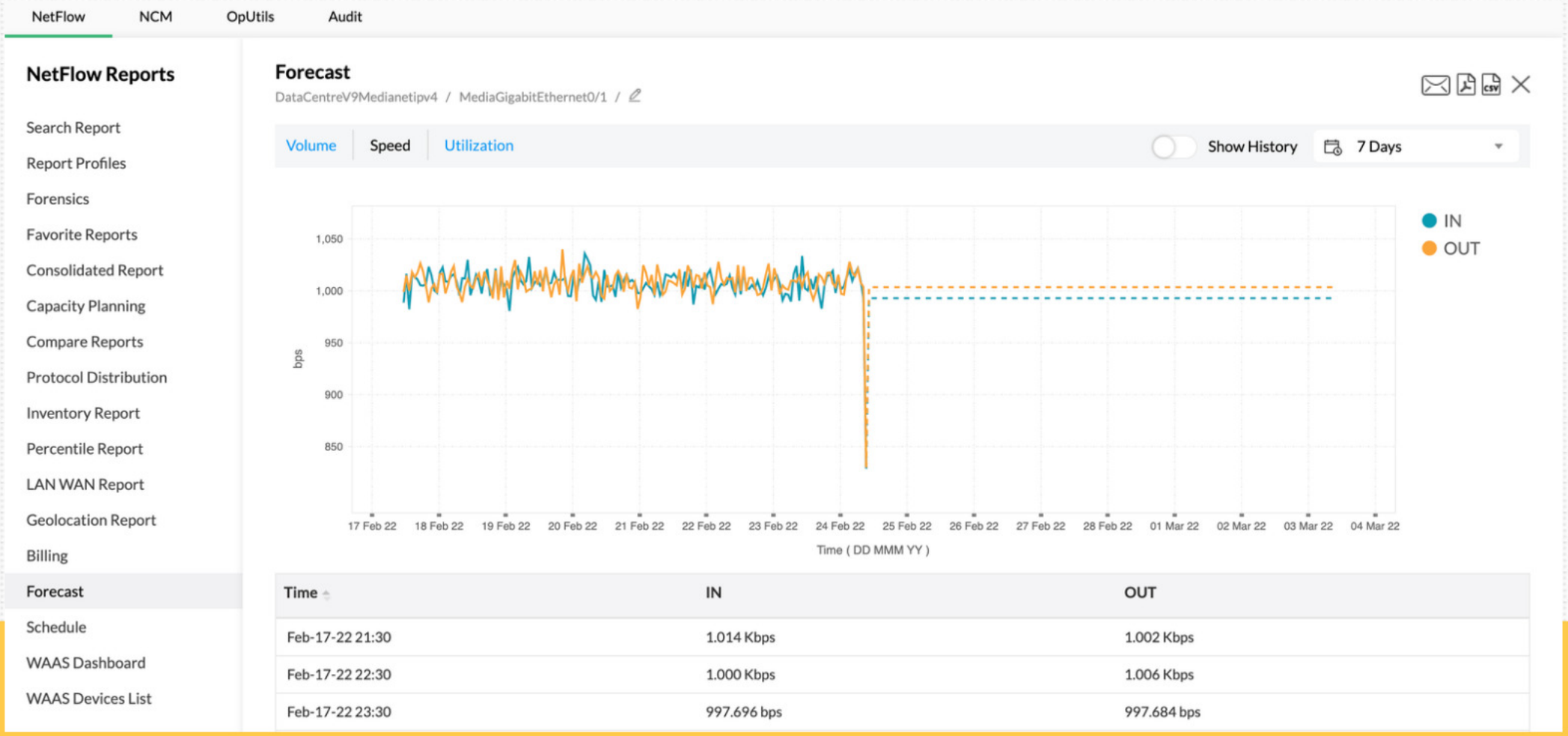
DataCentreV9Medianetipv4 (MediaGigabitEthernet0/1) | Today[2022-02-24 00:00 -- 2022-02-24 10:40] | Generate Bill

1 Minute Average



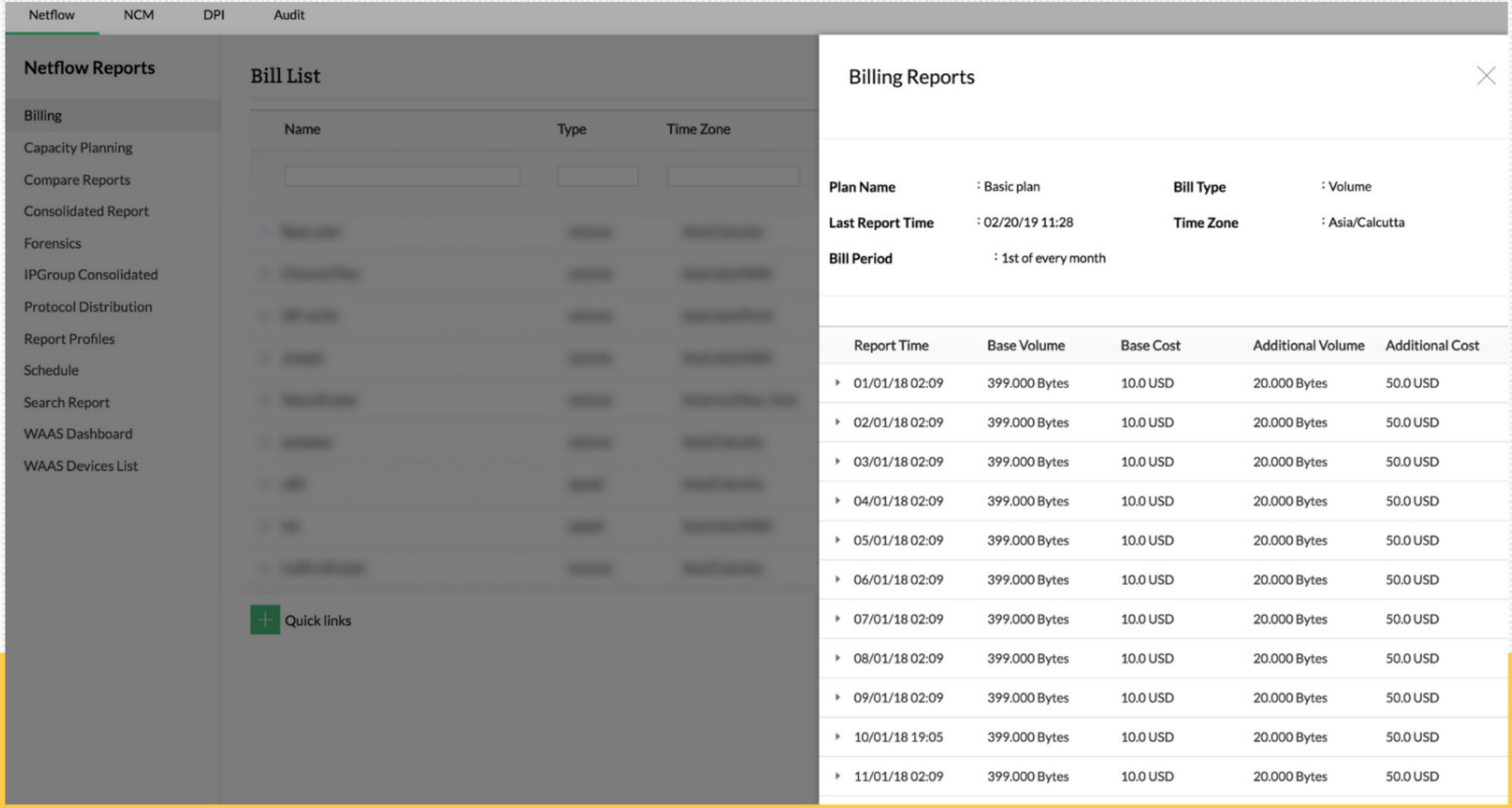
Category	Total	Maximum	Minimum	Average	Standard Deviation	95th Percentile
Traffic IN	4.842 MB	1.283 Kbps	405.200 bps	1.007 Kbps	75.778 bps	1.132 Kbps

Forecast report



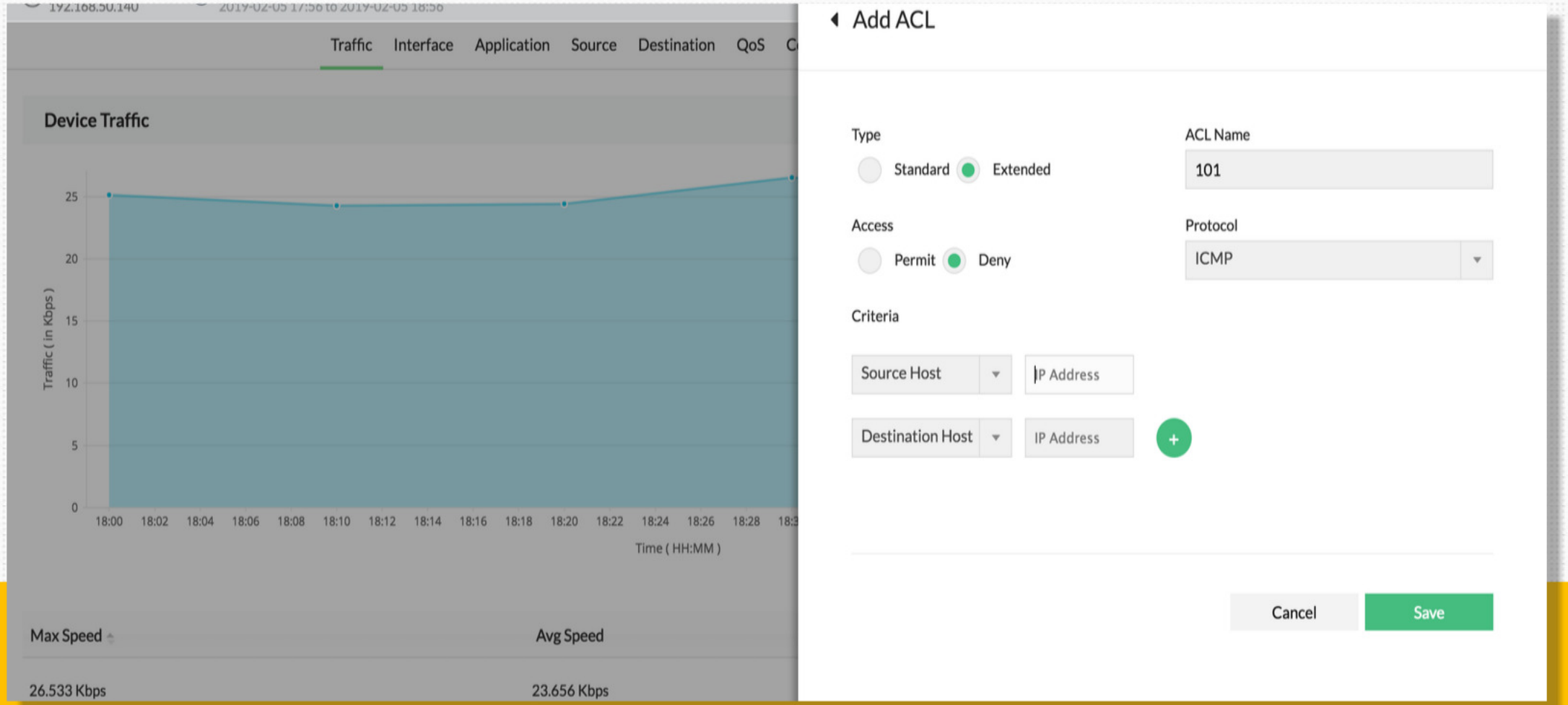
Time	IN	OUT
Feb-17-22 21:30	1.014 Kbps	1.002 Kbps
Feb-17-22 22:30	1.000 Kbps	1.006 Kbps
Feb-17-22 23:30	997.696 bps	997.684 bps

Billing report

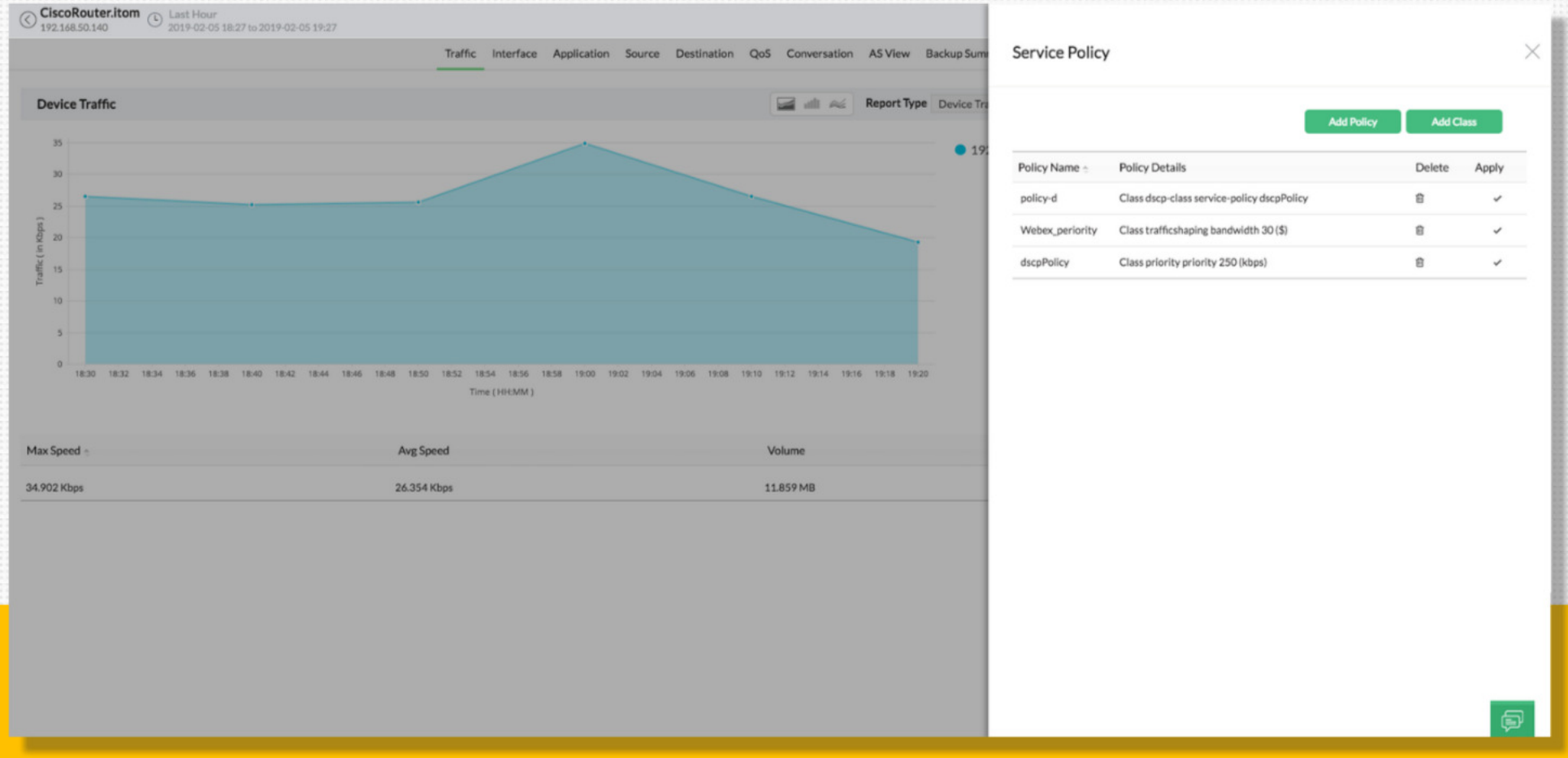


Prioritizing data and traffic shaping: Optimization made easy

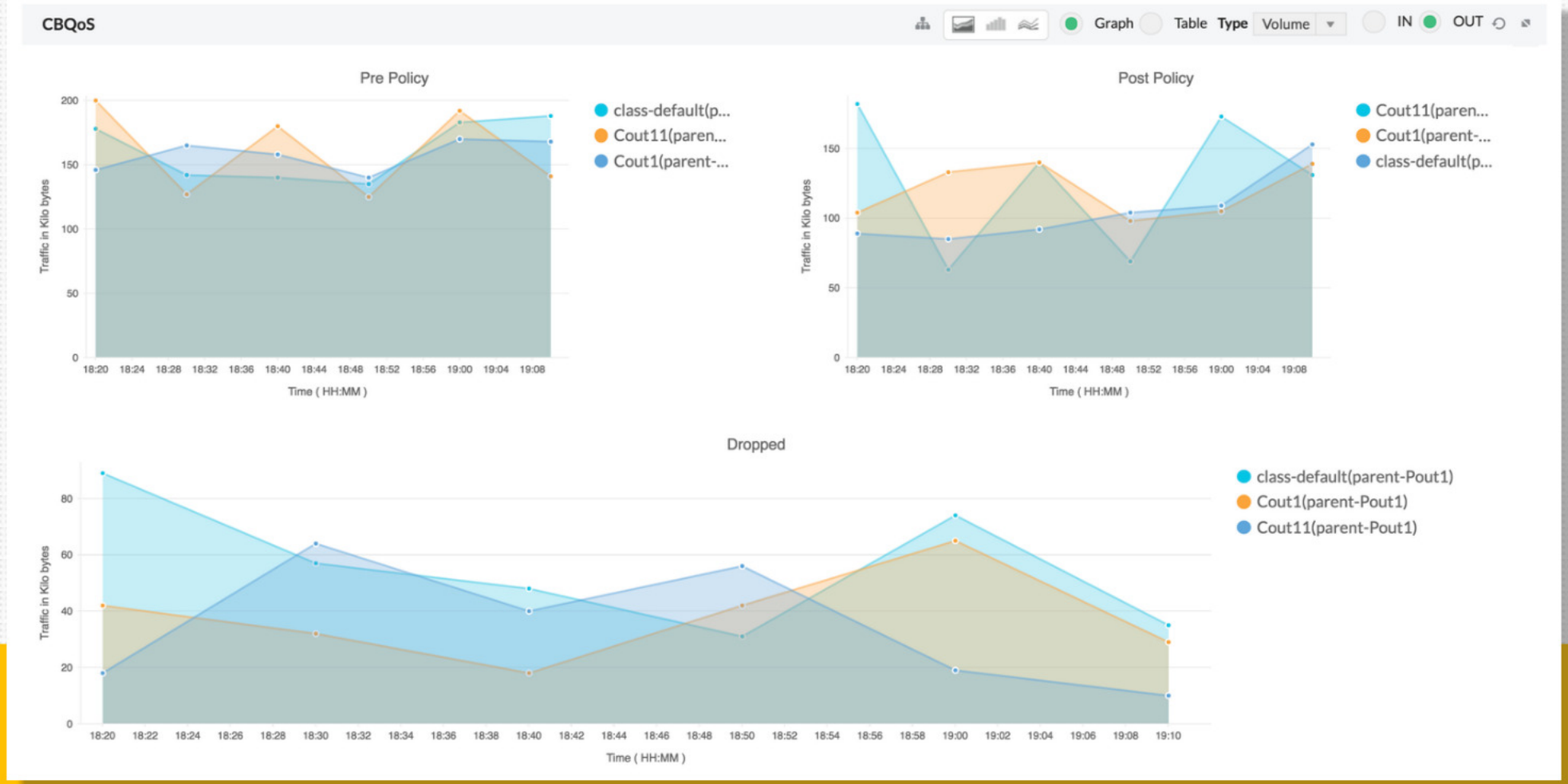
Filter out excess router traffic by blocking or restricting IPs / IP networks with ACL



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

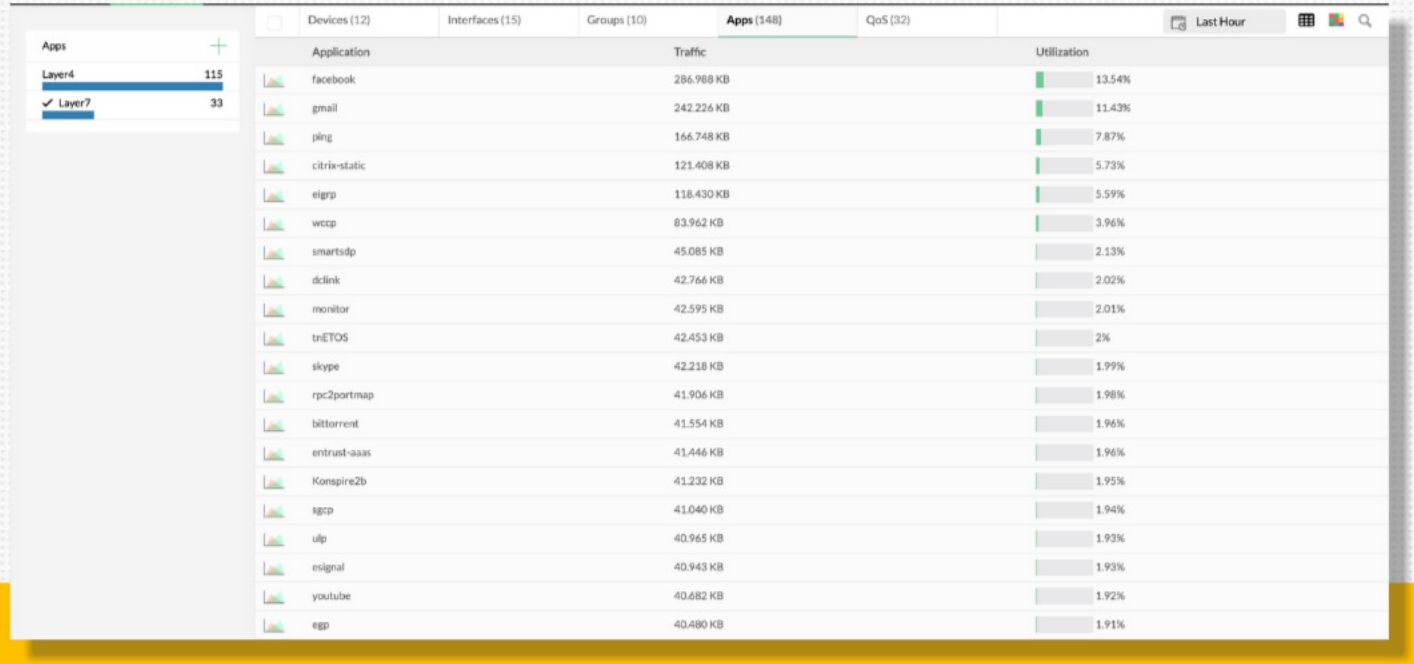
- Interface
- IP
- Application
- DSCP
- SSID
- SSID

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



- **Application mapping for _App**

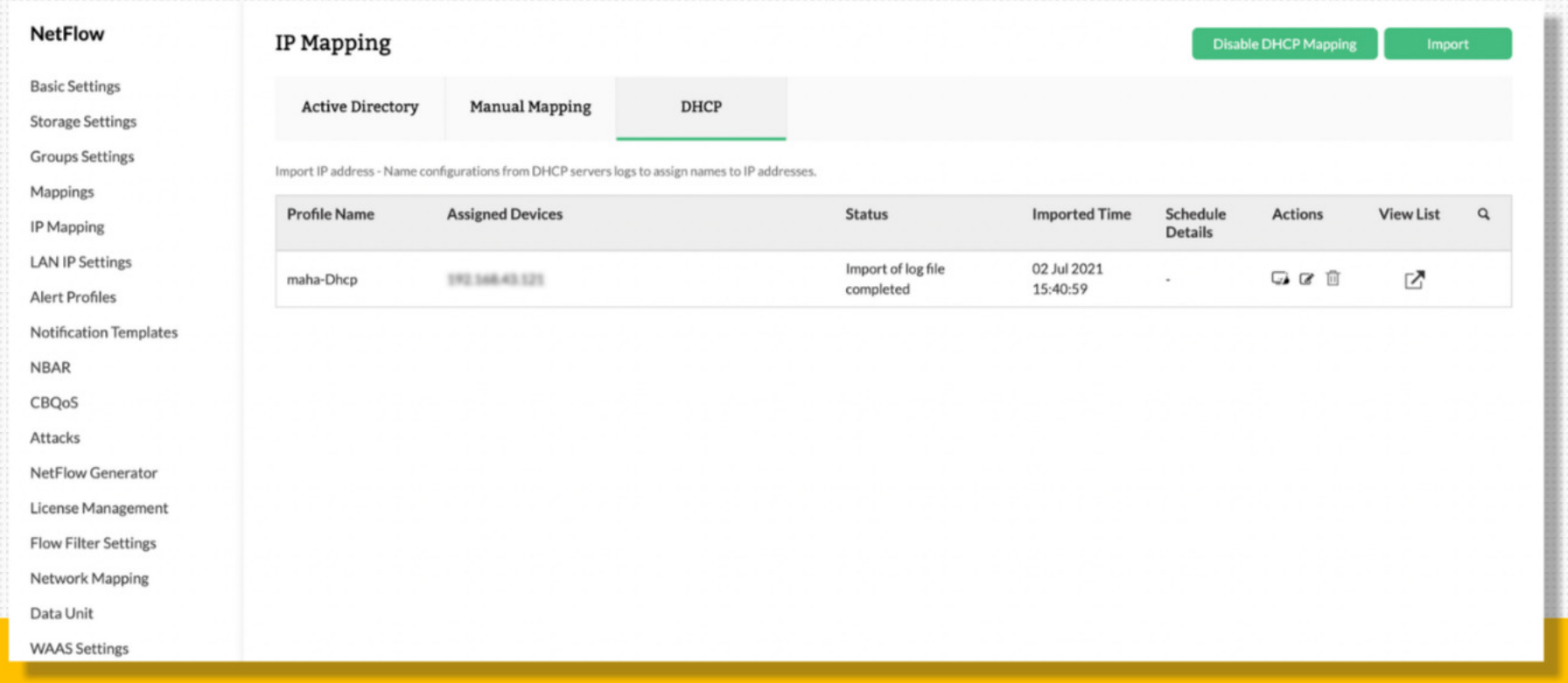
  Interface >Application > _App > Show port (show port needs raw data enabled).

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

- **Application mapping for custom apps**

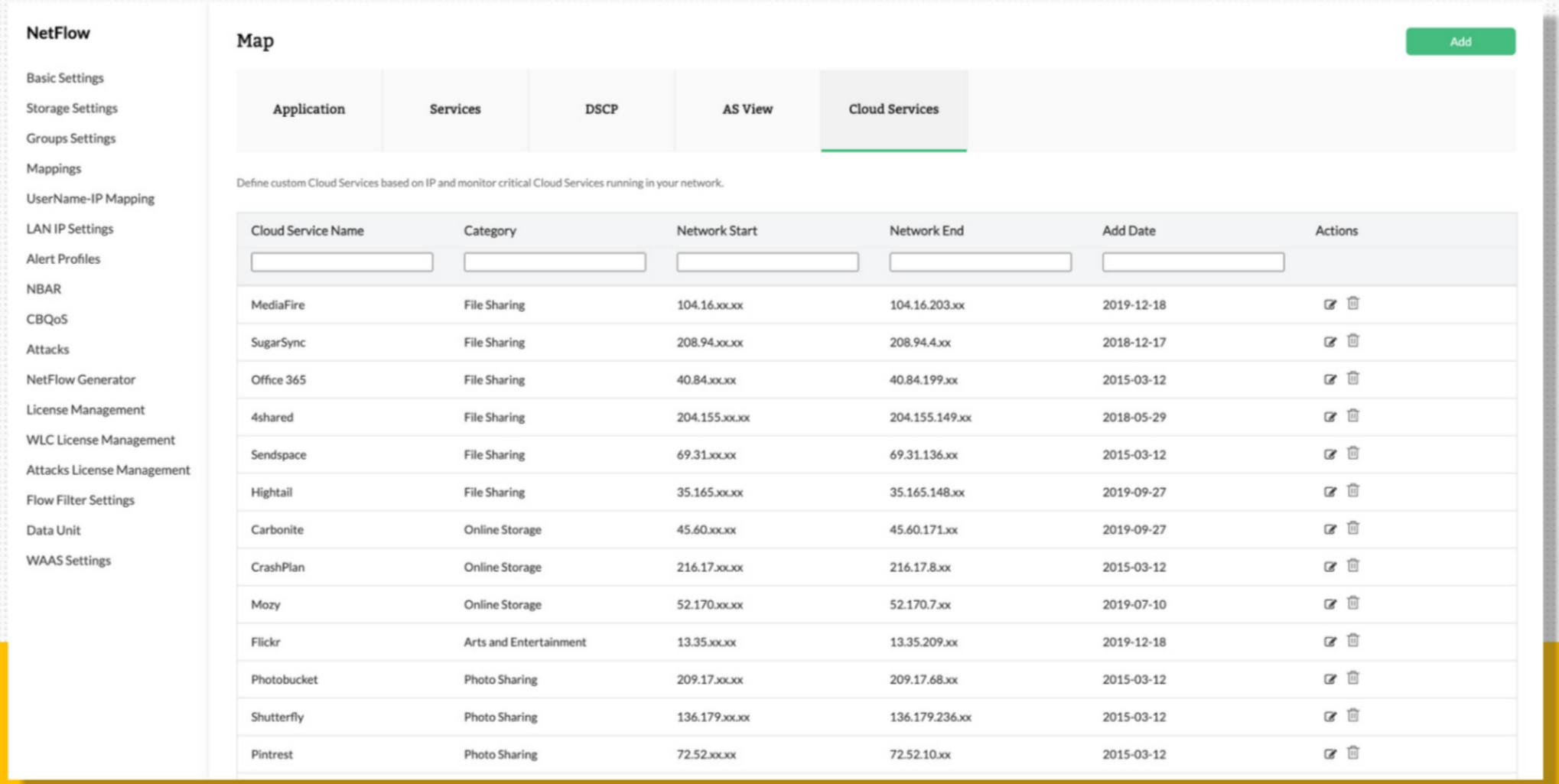
  Settings > NetFlow > Mapping > Application List > Add

Username - IP Mapping



- AD Mapping
- Manual
- Mapping
- DHCP

Cloud Services



Proactive management

Setting up Alerts

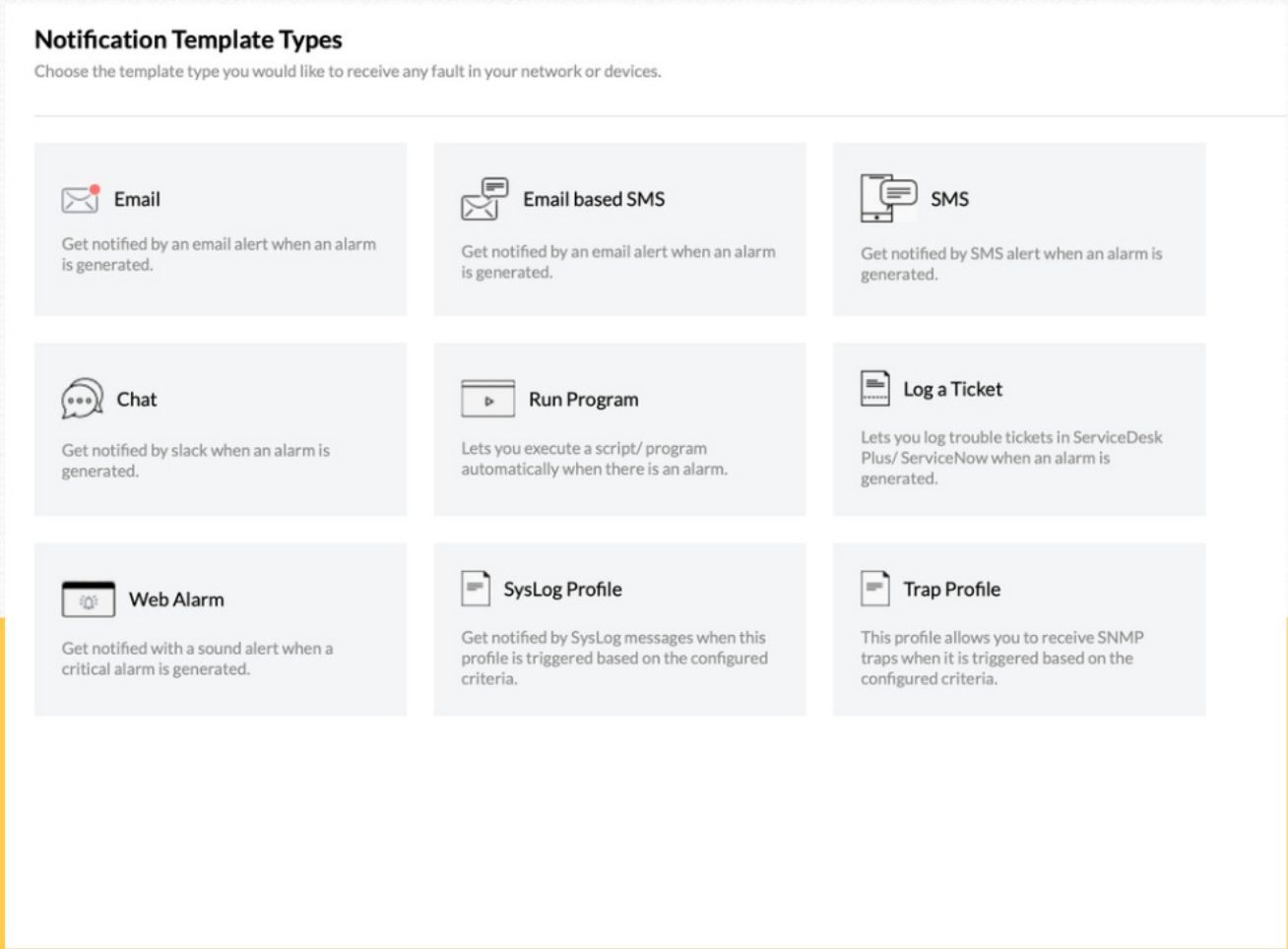
Real - time alerts

Aggregated alerts

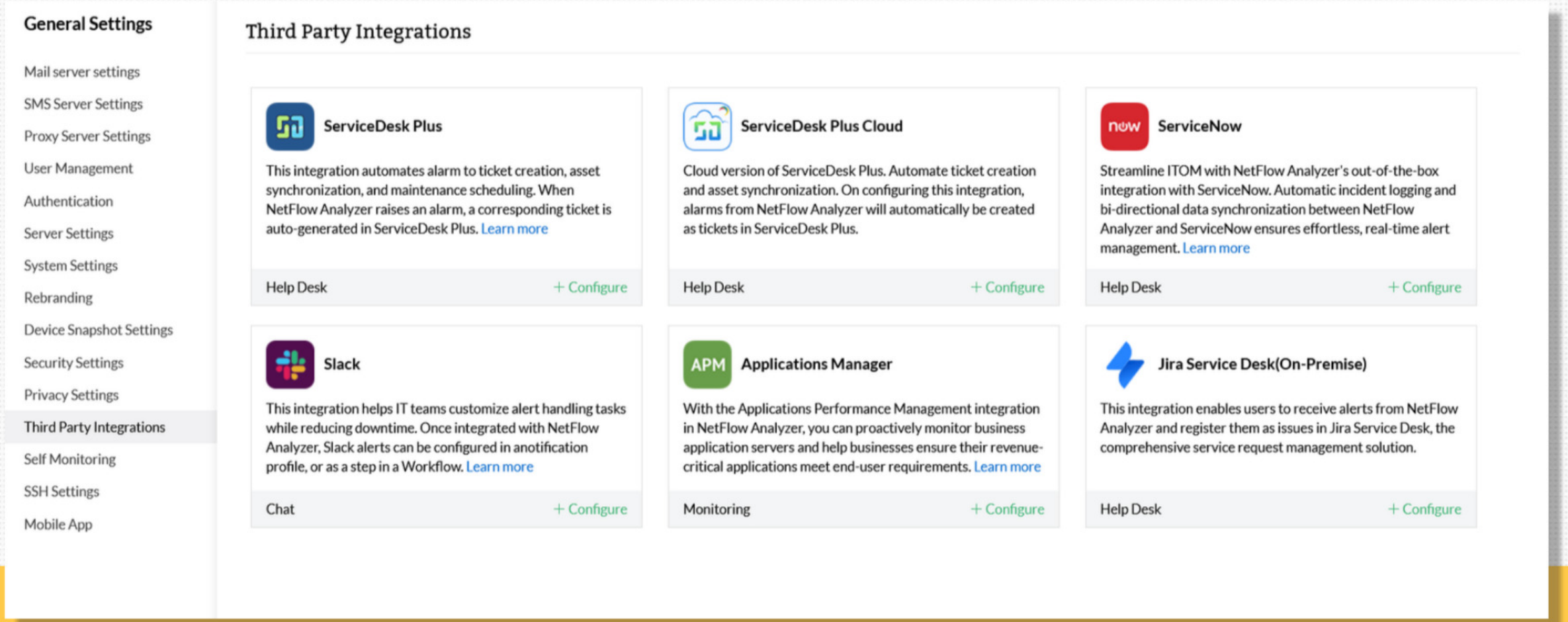
- Preconfigured alerts (Link down / No flow)
- Threshold based alerts

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

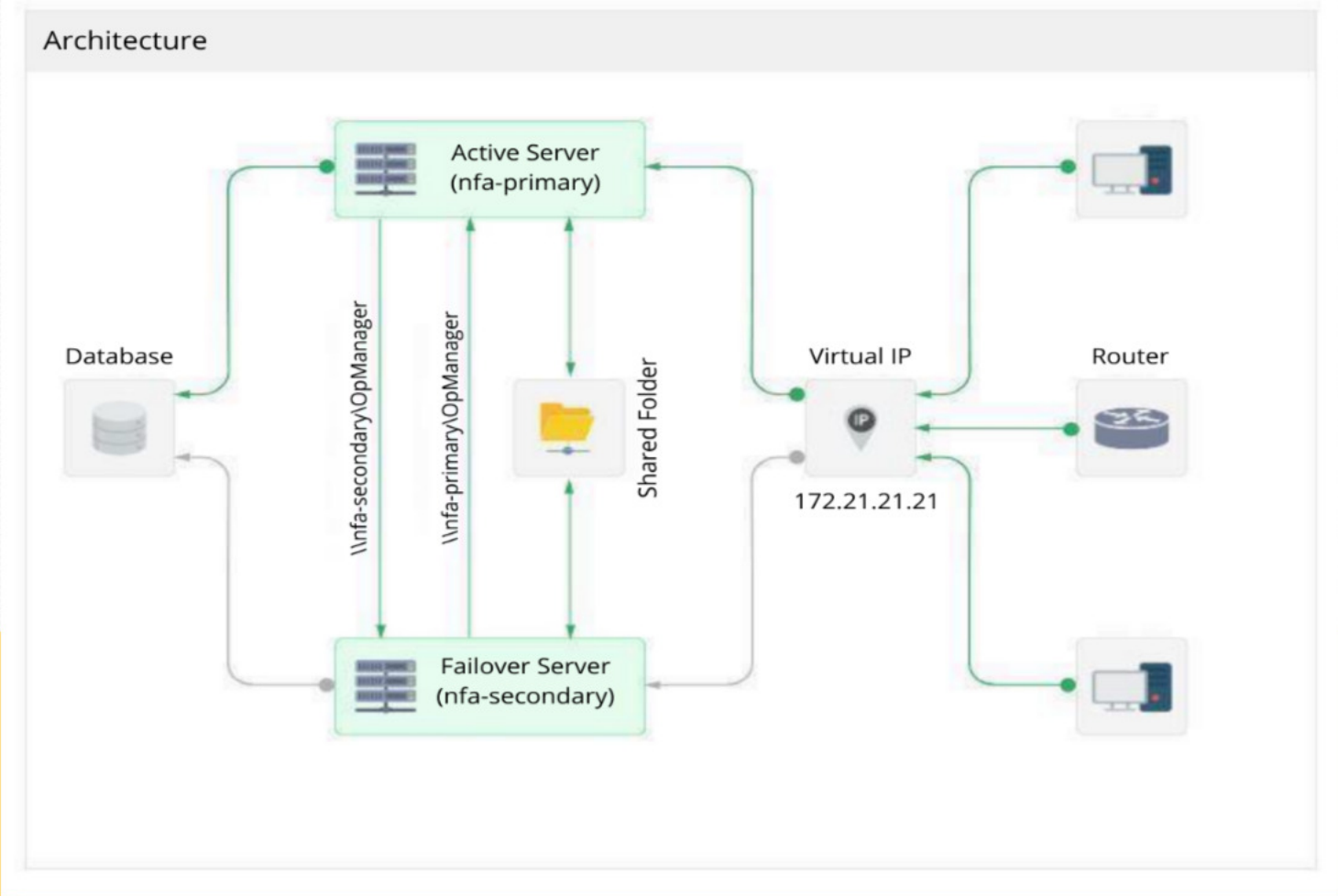
Create and manage Notification Templates to receive E-mail / SMS alerts, web alarms, log tickets or SNMP traps / syslogs.



Third Party Integrations

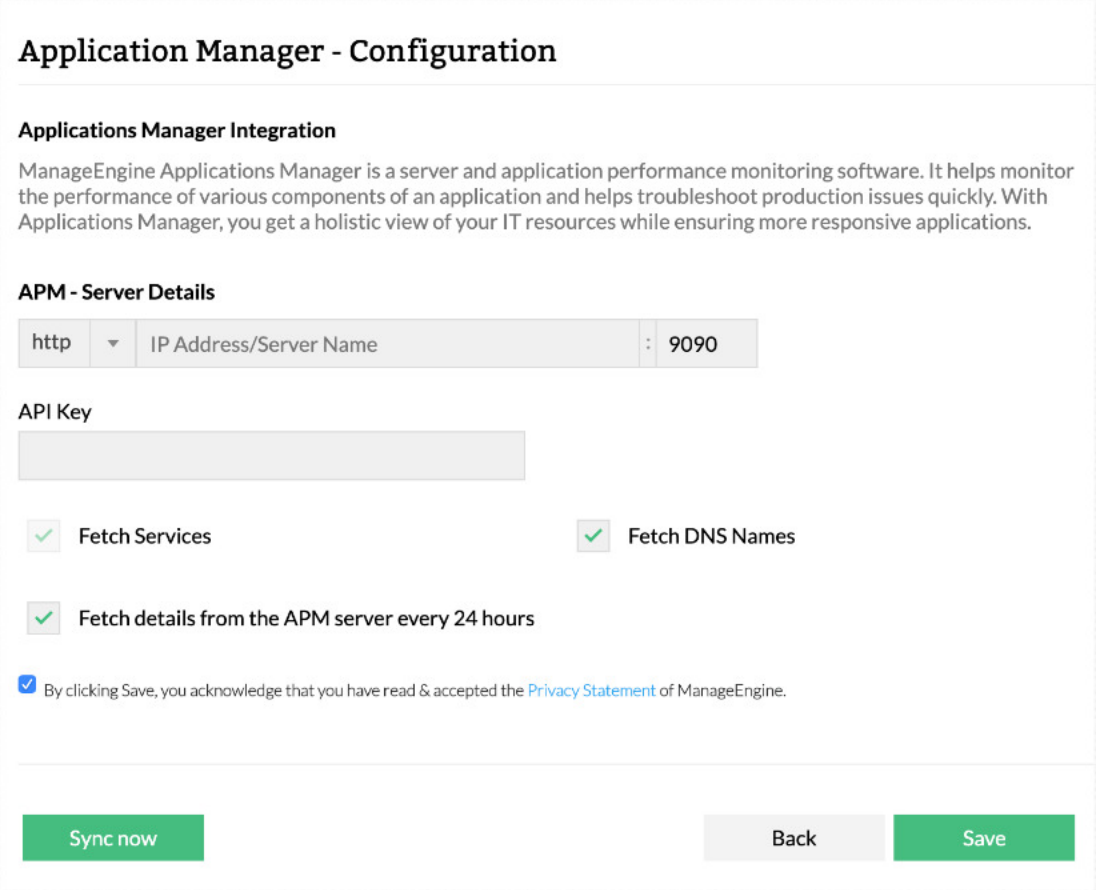


Ensure your network is always monitored with NetFlow Analyzer's Failover



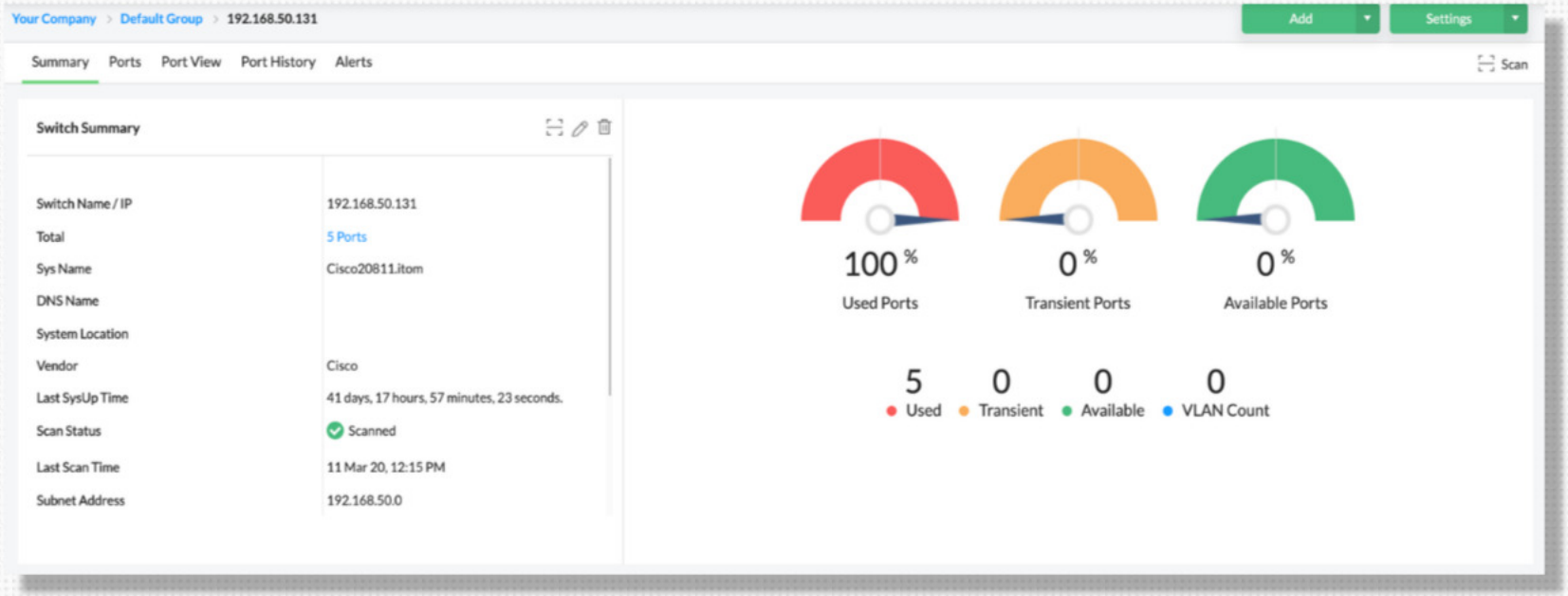
New Updates and Integrations

Applications Manager Integration



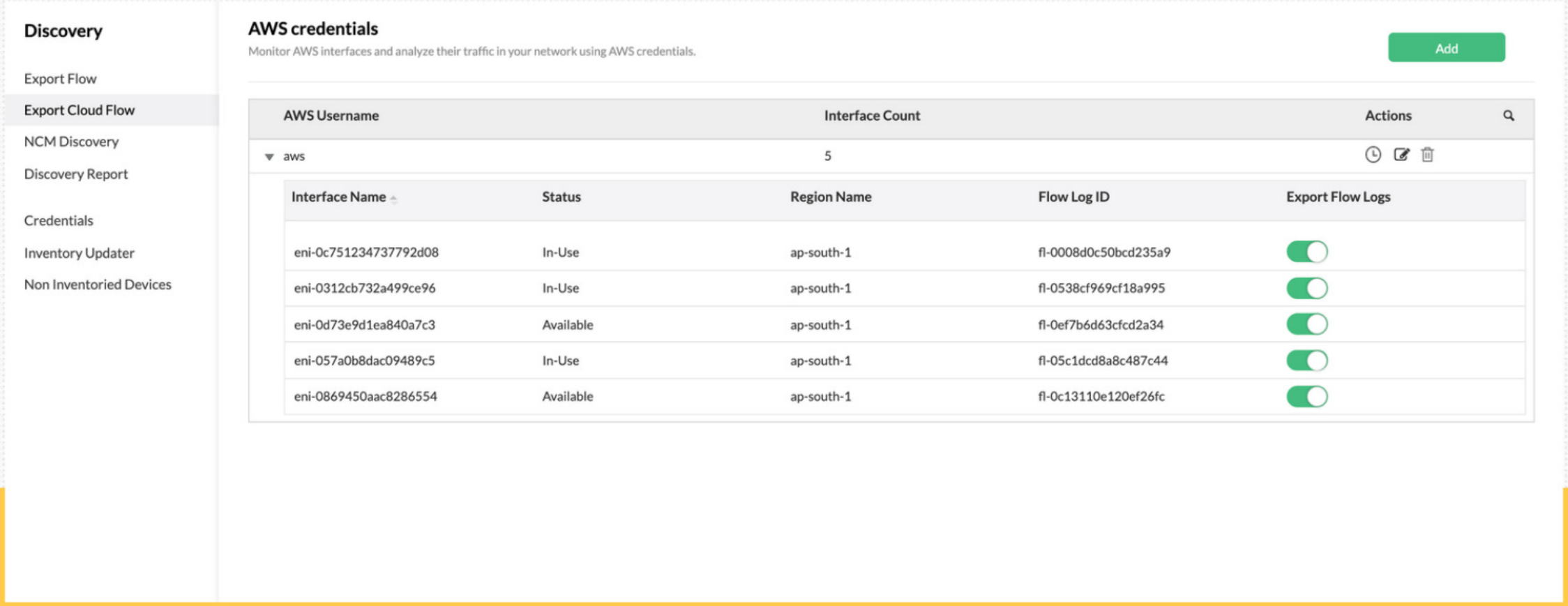
- Synchronizing application details (Port, Protocol, IP)
- Categorize these critical applications separately
- Monitor application traffic by to Source, Destination, Byte & more.

OpUtils Integration

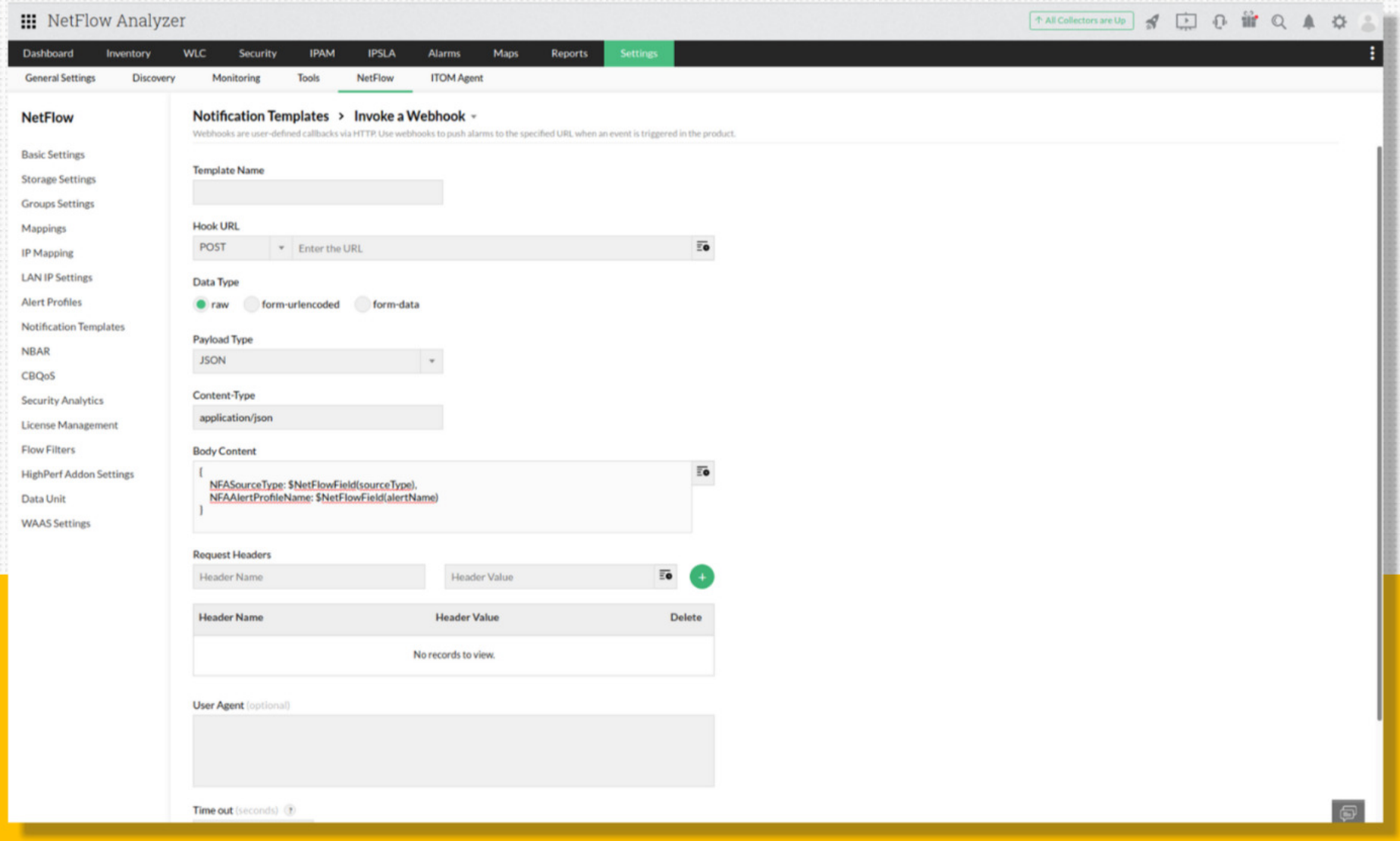


- Visibility into network ports
- Ability to inspect IP addresses
- Intuitive widgets

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

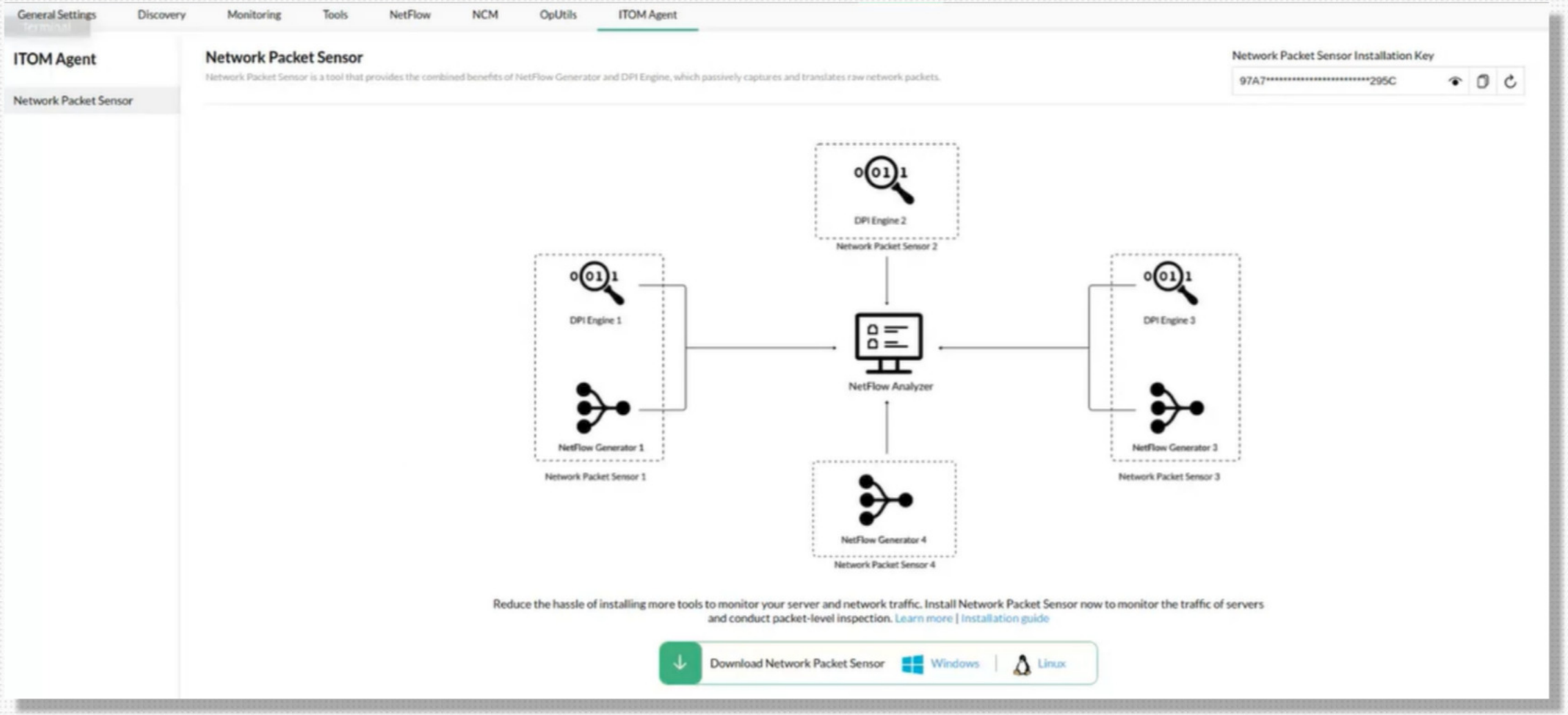


Webhook Integration with NetFlow Analyzer

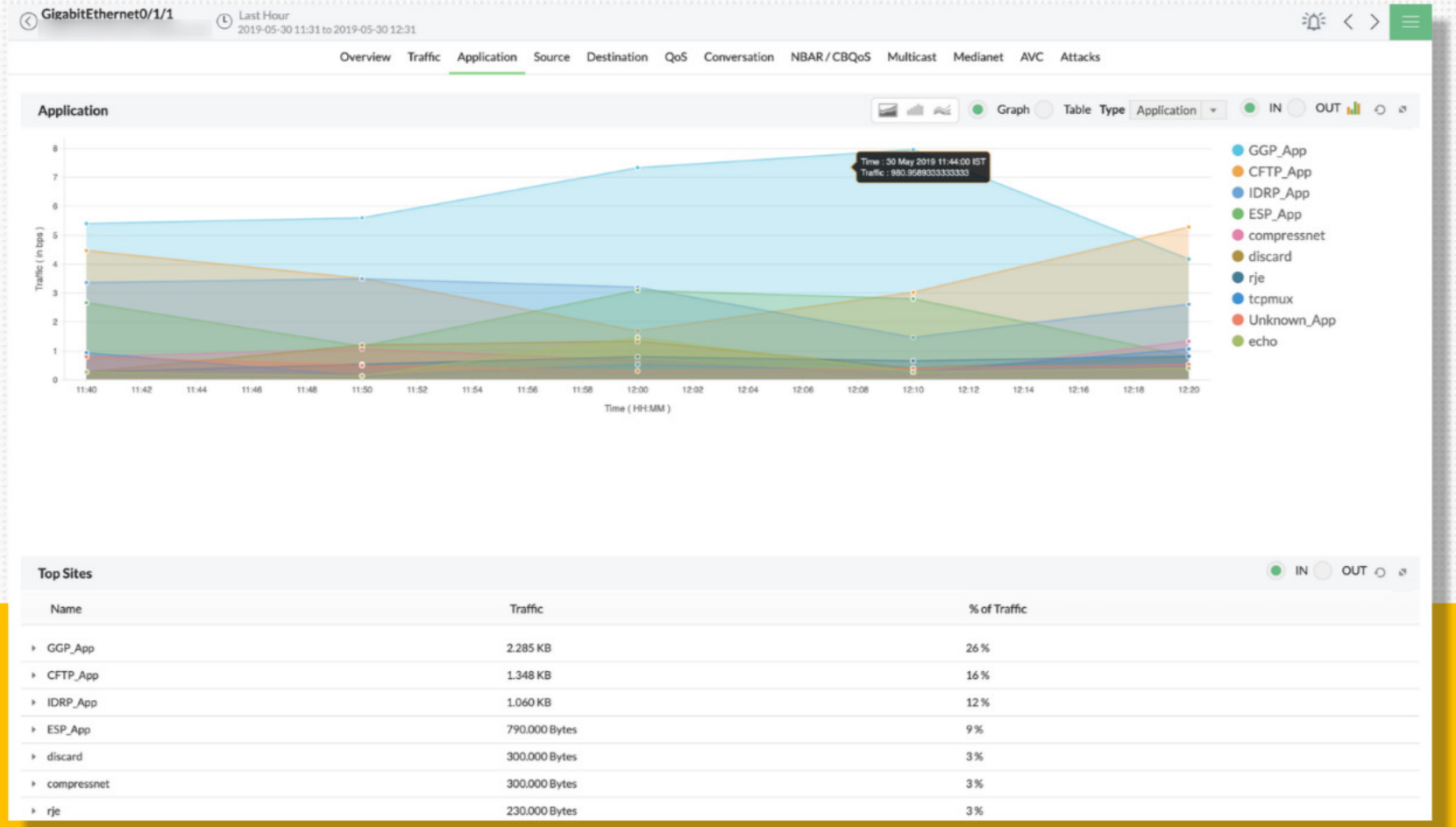


Network Packet Sensor

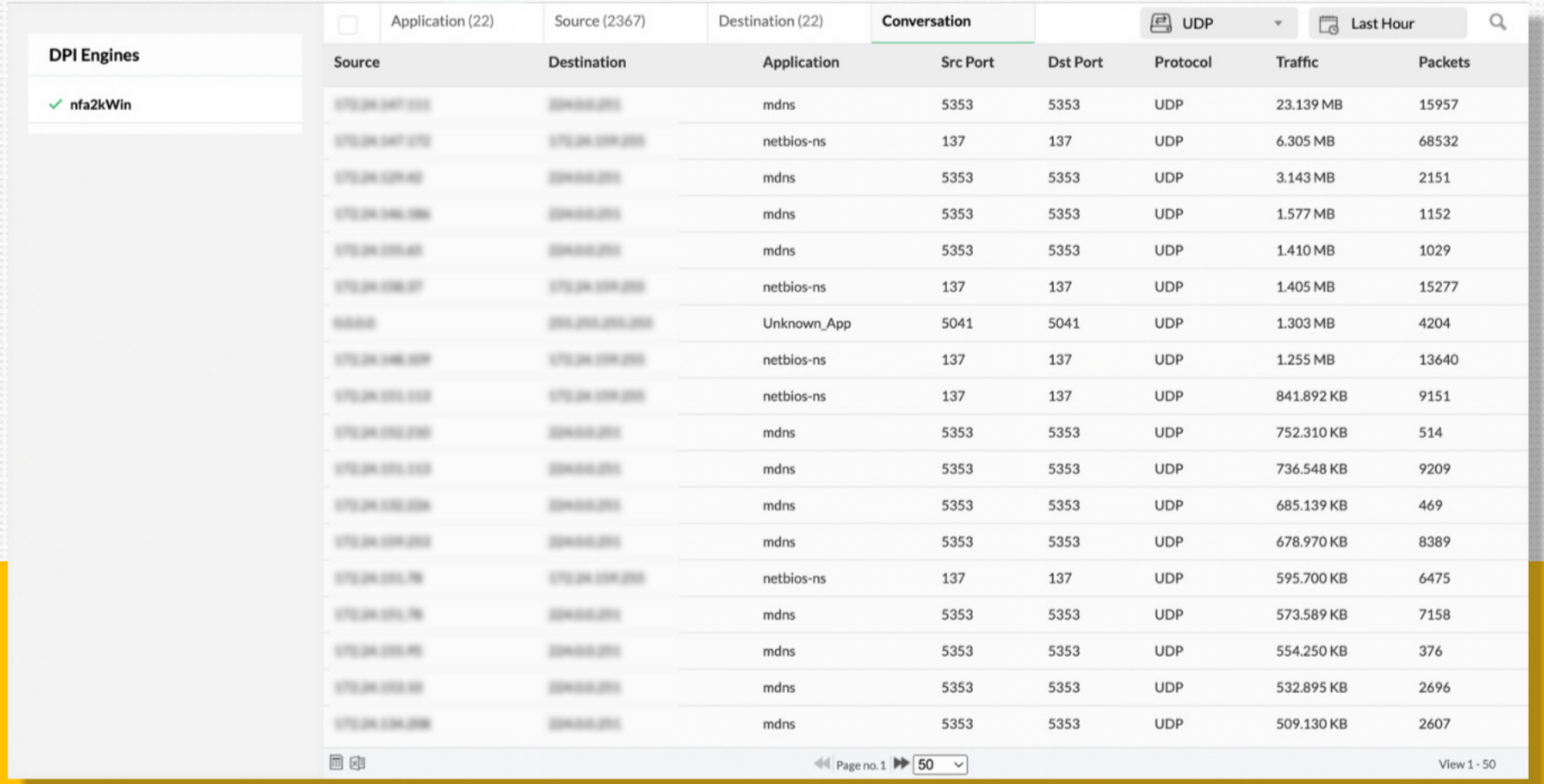
Network Packet Sensor (NPS)



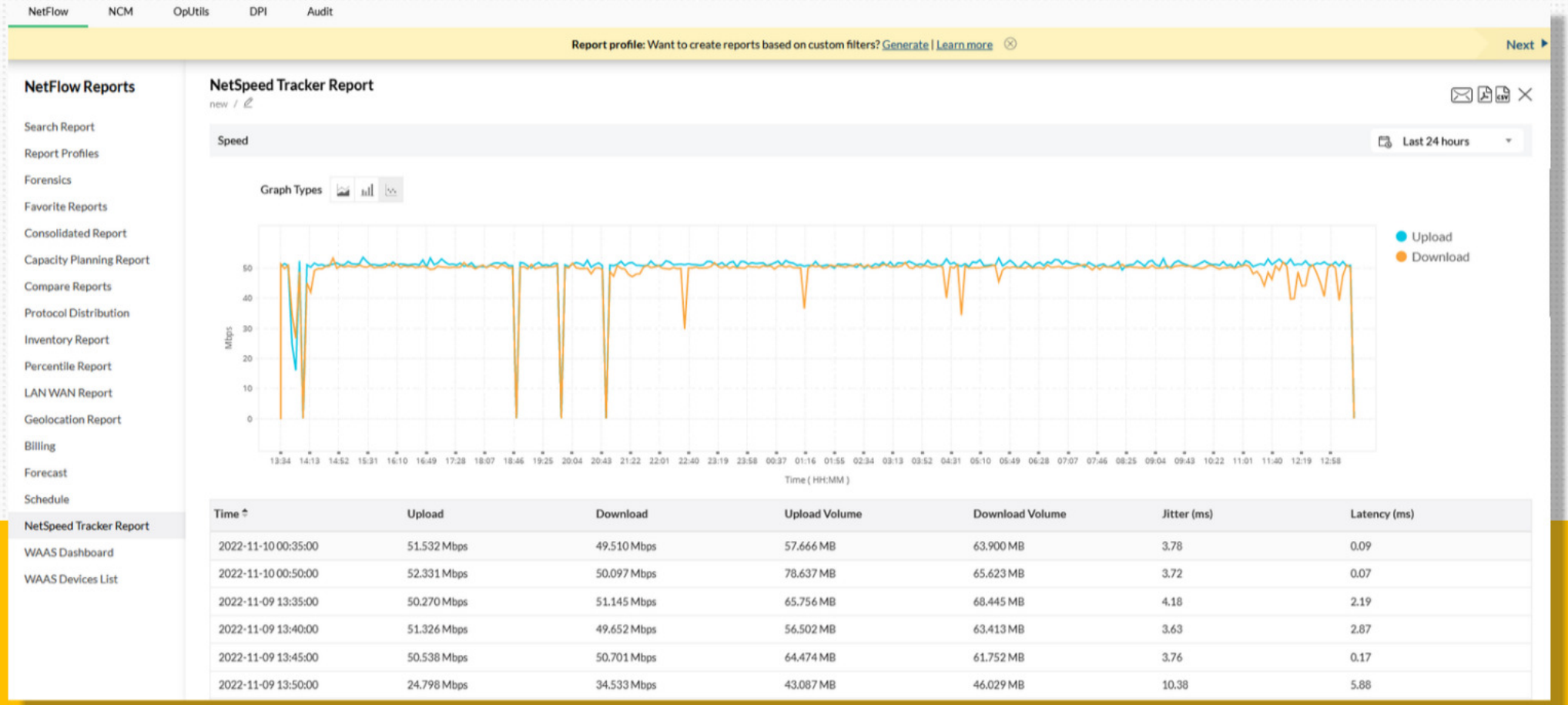
NetFlow Generator



Deep Packet Inspection



NetSpeed Tracker



Time	Upload	Download	Upload Volume	Download Volume	Jitter (ms)	Latency (ms)
2022-11-10 00:35:00	51.532 Mbps	49.510 Mbps	57.666 MB	63.900 MB	3.78	0.09
2022-11-10 00:50:00	52.331 Mbps	50.097 Mbps	78.637 MB	65.623 MB	3.72	0.07
2022-11-09 13:35:00	50.270 Mbps	51.145 Mbps	65.756 MB	68.445 MB	4.18	2.19
2022-11-09 13:40:00	51.326 Mbps	49.652 Mbps	56.502 MB	63.413 MB	3.63	2.87
2022-11-09 13:45:00	50.538 Mbps	50.701 Mbps	64.474 MB	61.752 MB	3.76	0.17
2022-11-09 13:50:00	24.798 Mbps	34.533 Mbps	43.087 MB	46.029 MB	10.38	5.88

ManageEngine

YouTube

youtube.com/opmanagertechvideos

ManageEngine PitStop

forums.manageengine.com/netflowanalyzer

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/