

# NetFlow Analyzer

Comprehensive network traffic and bandwidth management solution

# NetFlow Analyzer

Increased Visibility

+

Greater Control

ManageEngine NetFlow Analyzer is a standalone, full-featured bandwidth monitoring and network traffic analysis solution. It is a flow-based software that runs on both Windows and Linux machines and supports a wide range of flow formats and devices. NetFlow Analyzer monitors your network to provide in-depth visibility into your network devices, interfaces, applications, users, bandwidth usage, and network traffic. Now packed with new UI for increased visibility and better control, it takes bandwidth monitoring and traffic analytics to next level, with ease of monitoring.

# Leverages flow technology

NetFlow

sFlow

J-Flow

IPFIX

NetStream

AppFlow

NetFlow Analyzer collects and analyzes flows from major devices like Cisco, 3COM, Juniper, Foundry Networks, Hewlett-Packard, extreme and other leading vendors in the market.

# Key features

- Provides detailed visibility into your network to network traffic and bandwidth in real-time.
- Proactively monitors network traffic patterns to detect traffic spikes and anomalies.
- Helps analyze bandwidth usage trends to identify the root cause network traffic issues.
- Detects internal and external security threats such as DDoS/flash-crowd attacks, probes/scans, suspicious flows, etc
- Enables you to predict, plan, and optimize bandwidth usage to ensure priority of business-critical apps.
- Helps set real-time threshold-based alerts to reduce response time and enable faster troubleshooting.
- Helps enable comprehensive cloud traffic monitoring along with a range of home-grown and third-party integrations.
- Supports popular flow technologies, and devices by leading vendors.



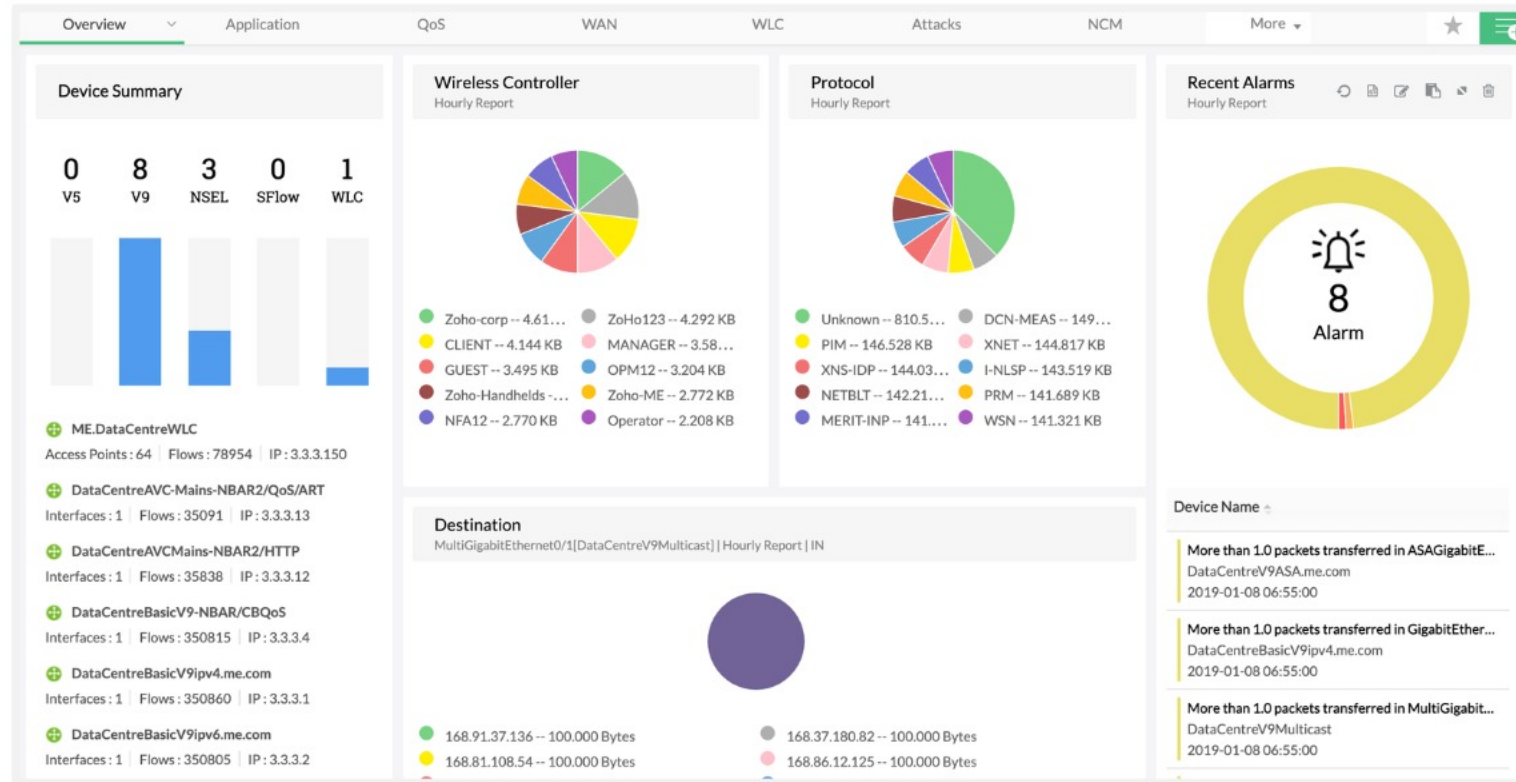
Real-time monitoring

# Know the who, when and what of your network traffic

Gain detailed visibility into traffic usage by

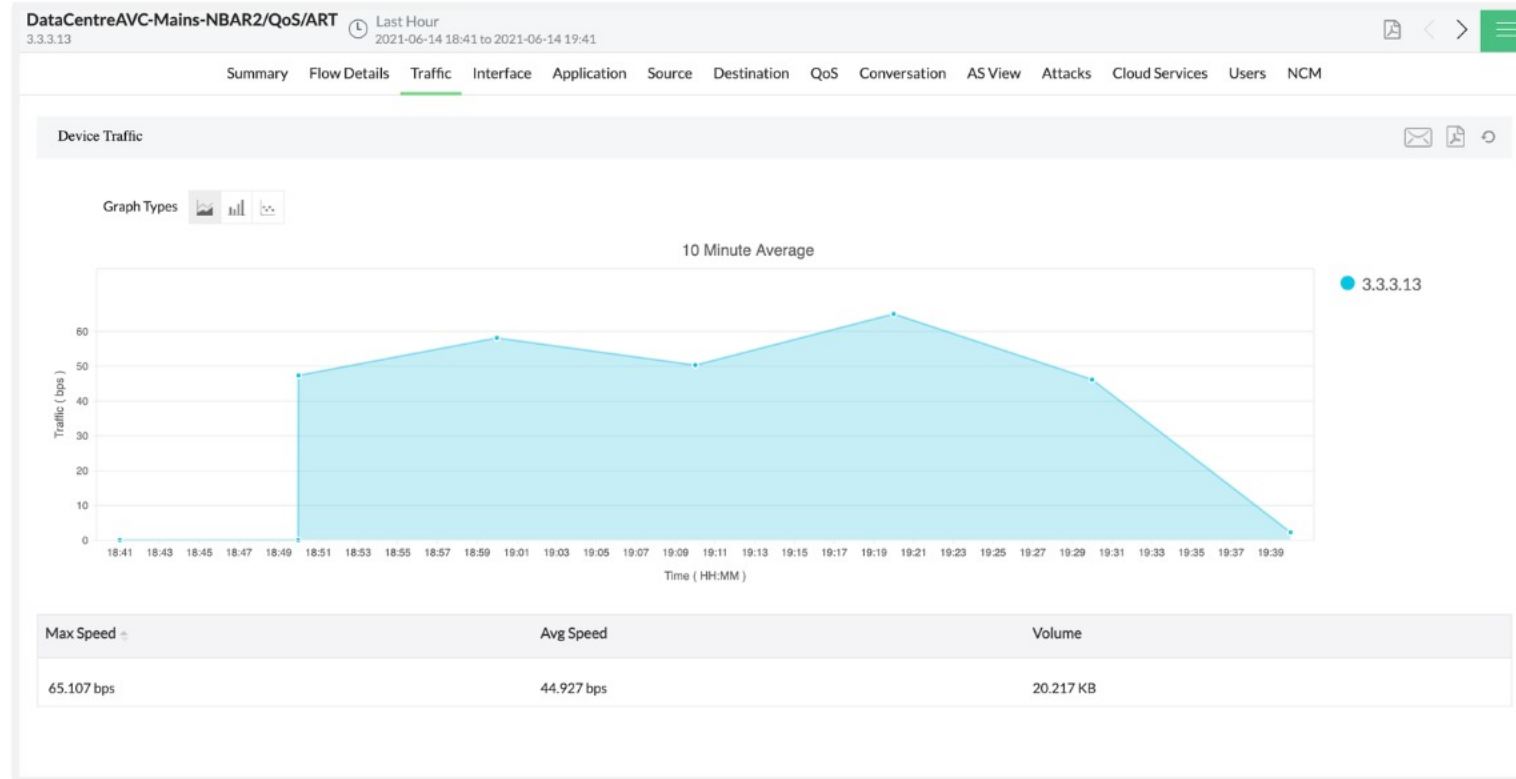
- Applications
- Protocols
- QoS
- Source
- Destination
- Conversation

# Dashboard



Dashboard provides summary of traffic details such as top applications, conversations, QoS, protocols, and alarms.

# Visibility into network traffic

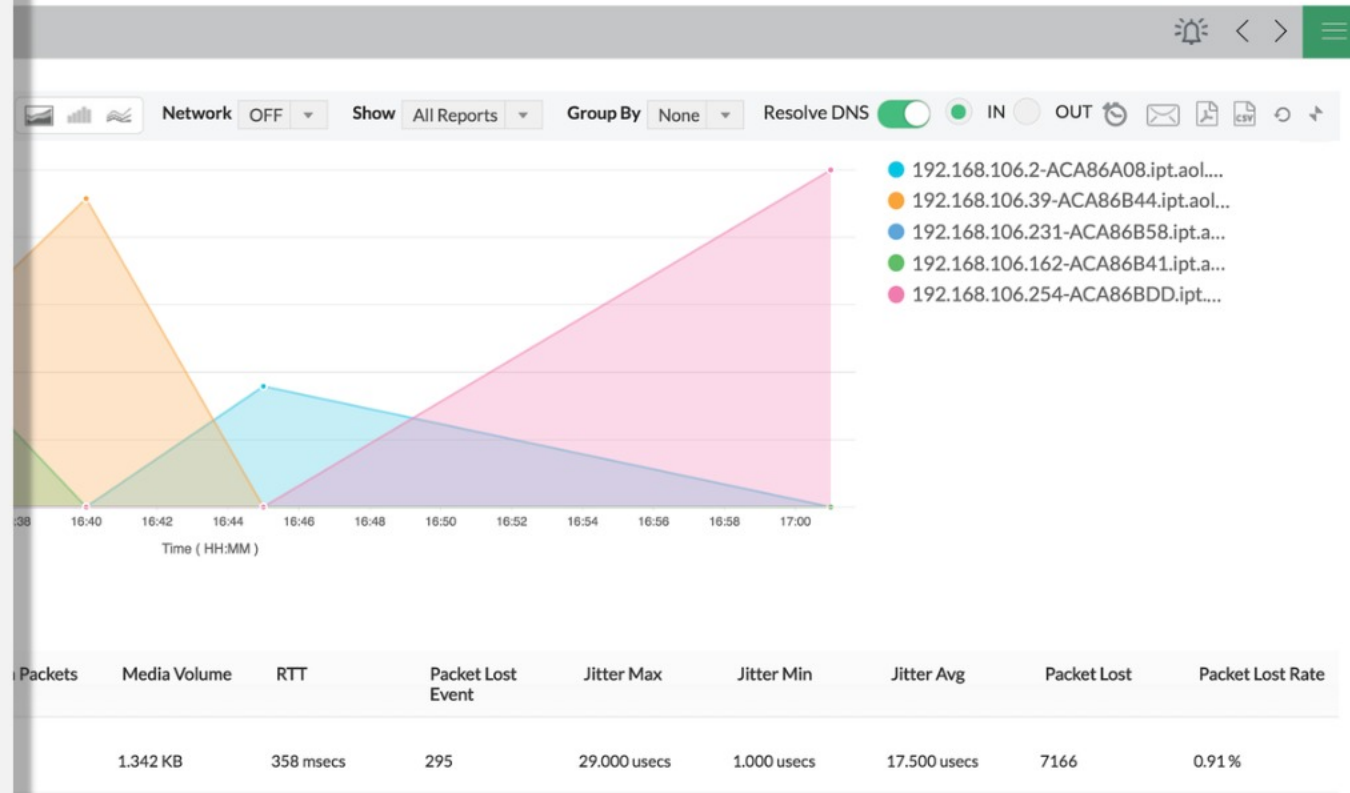


Get a detailed view of router/switch traffic to know the total bandwidth consumption by devices, its interface, applications, top source/destinations, QoS, and conversations from the Inventory.



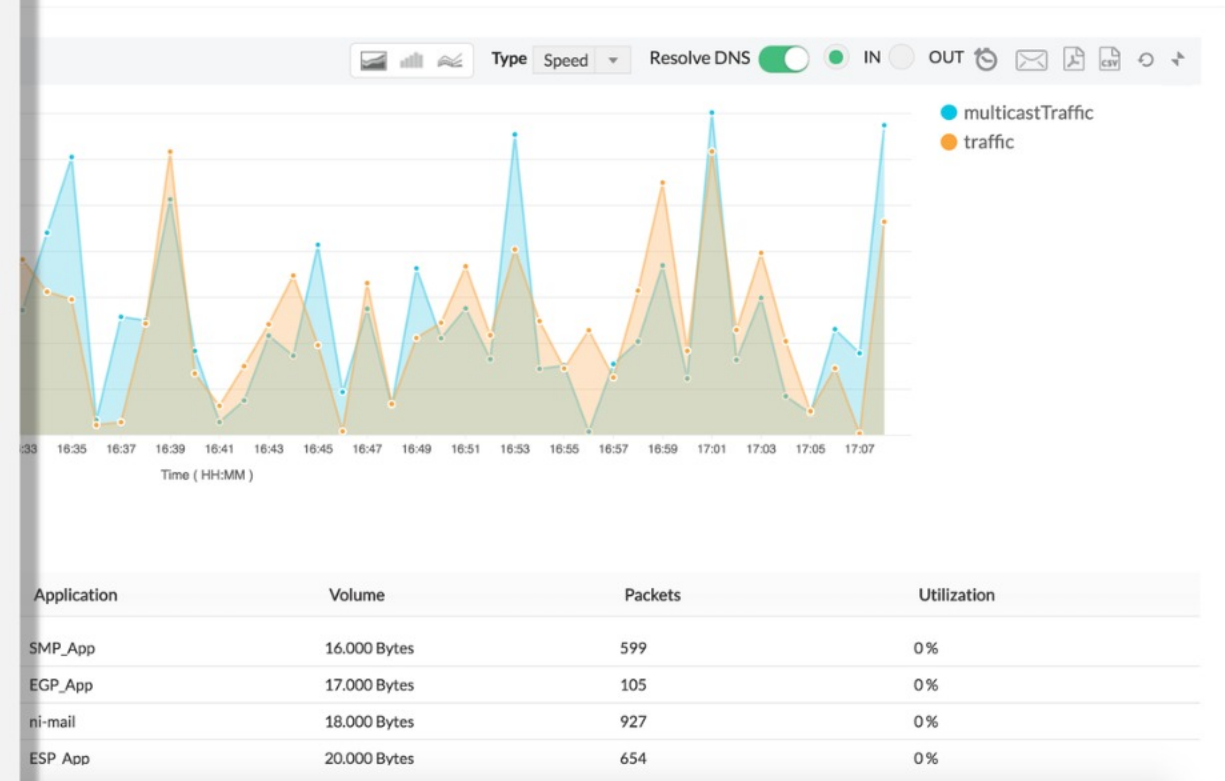
# Medianet traffic monitoring

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

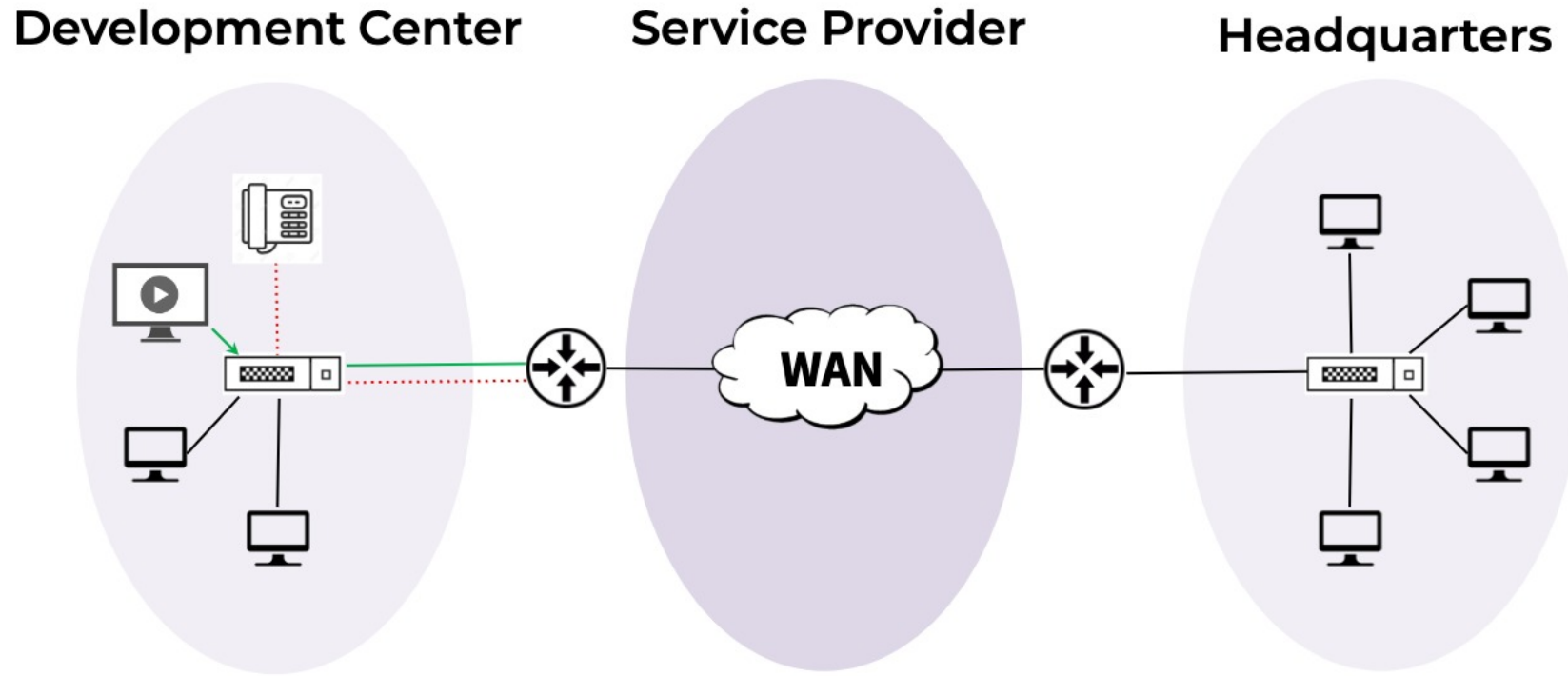


# Multicast traffic monitoring

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



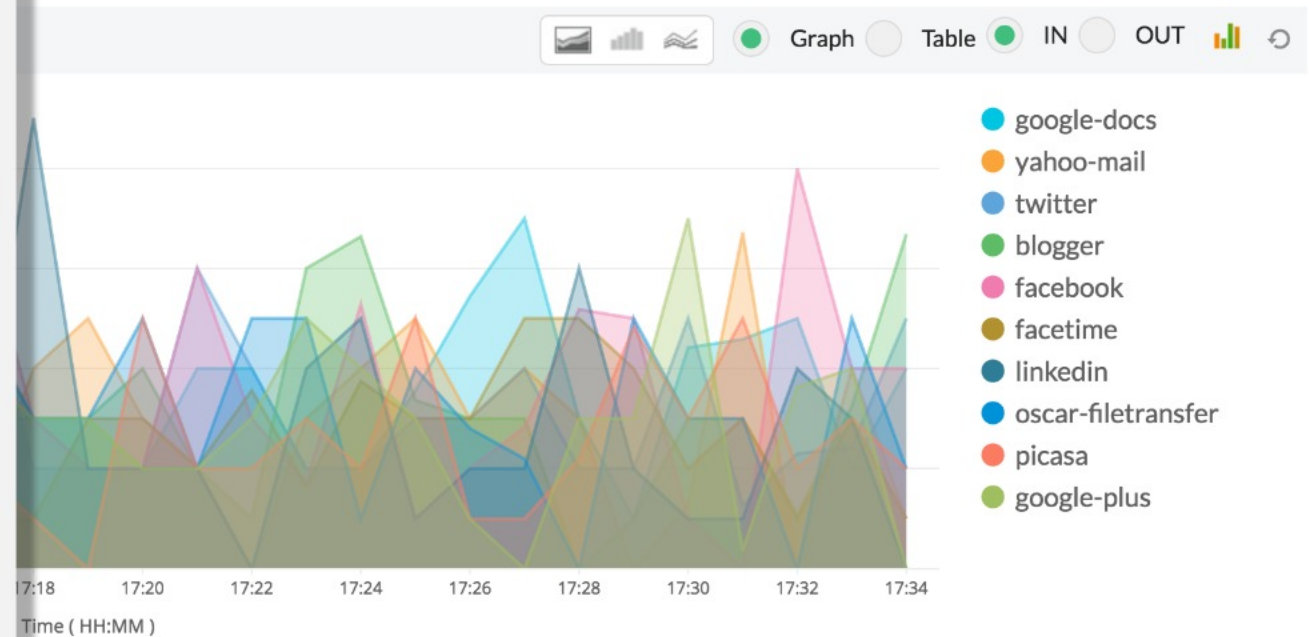
# IP SLA Monitoring



Get real-time visibility into your VoIP, WAN, and video traffic.

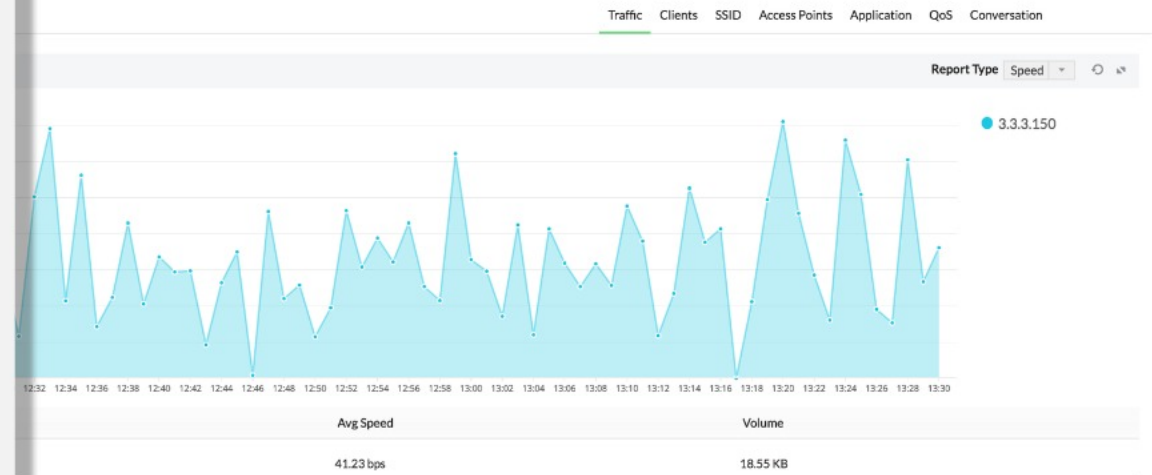
# Application Visibility and Control

- Gain visibility into NBAR2 applications with Cisco AVC monitoring (Application Visibility and Control).
- Advanced NBAR is used to identify web traffic, URLs, 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 LAN traffic monitoring

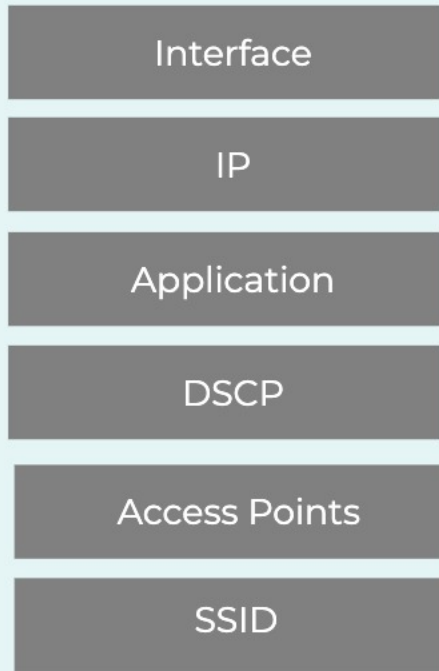
- Monitor Cisco WLAN controllers.
- Find the top traffic users by access points, SSIDs, applications, clients etc.
- Group WLANs by SSIDs.
- Troubleshoot bandwidth spikes by identifying consumption by SSIDs, finding its top clients and complete conversation details for the selected time period.





# Customizing NetFlow Analyzer to fit your network

# Sort traffic usage by Groups



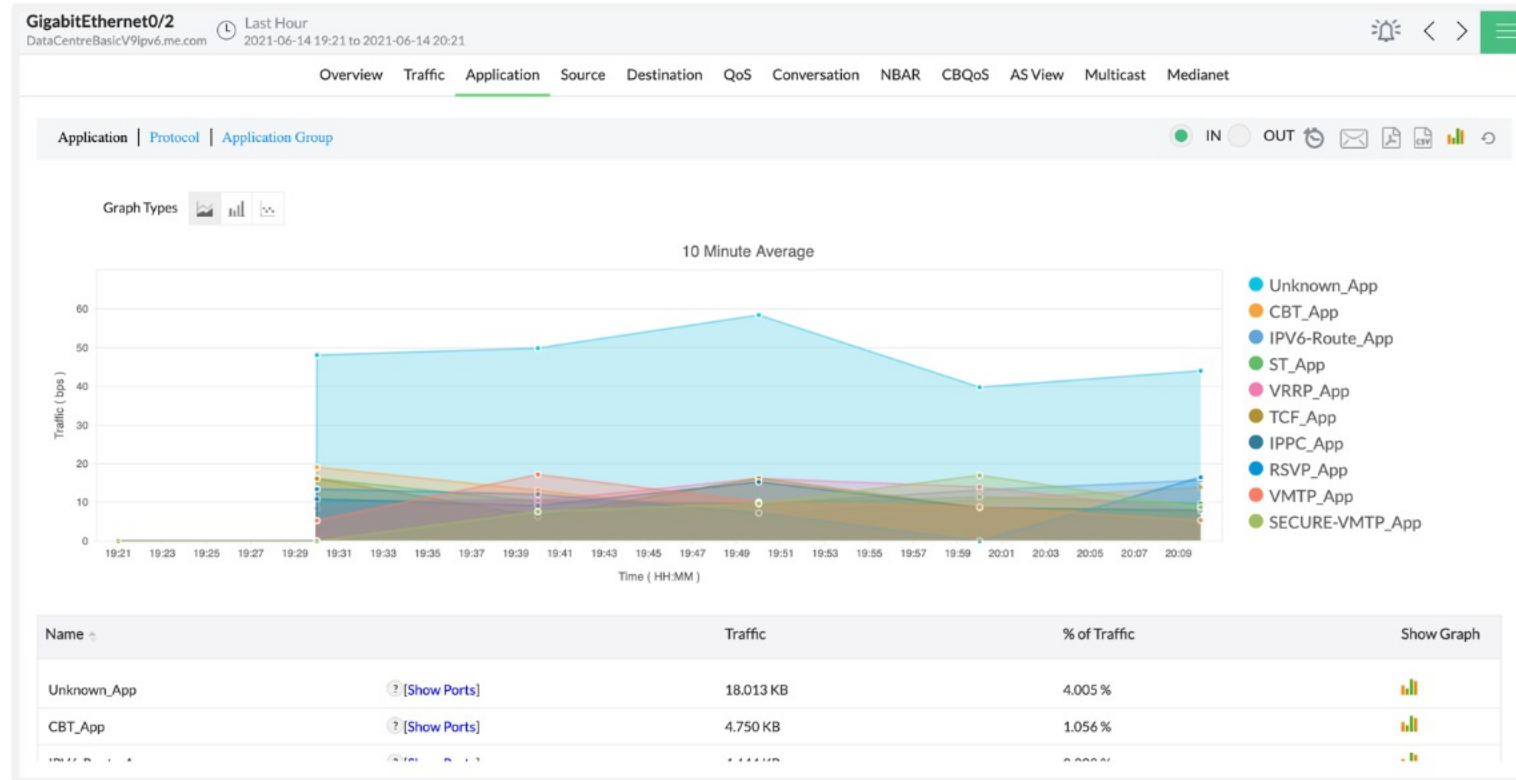
Types of groups

## Benefits of creating groups:

- Categorize traffic by department, subnets, branches, related apps, VLANs, etc
- Monitor combined bandwidth usage to get better picture of traffic consumption.
- Provide access to operators based on groups.
- Provide better visibility to improve troubleshooting.



# Map and monitor custom applications



Define custom application names based on Port & Protocol and get detailed insights on their usage.



# UserName-IP Mapping

- Manual Mapping:

Manual Mapping uses manually imported UserName-IP Mapping data to resolve and assign user names to IP addresses.

- Active Directory:

The Active Directory (AD) mapping feature automatically fetches UserName-IP Mapping configurations from Active Directory Proxy servers to assign user and host names to their corresponding IP addresses.

Port Number	Protocol Name	Actions
<input type="text"/>	<input type="text"/>	
3091	TCP	
3091	UDP	
629	TCP	
629	UDP	
2391	TCP	
2391	UDP	
5264	TCP	
5264	UDP	
5265	TCP	
5265	UDP	
1742	TCP	
1742	UDP	
106	TCP	
106	UDP	
2339	TCP	

# 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

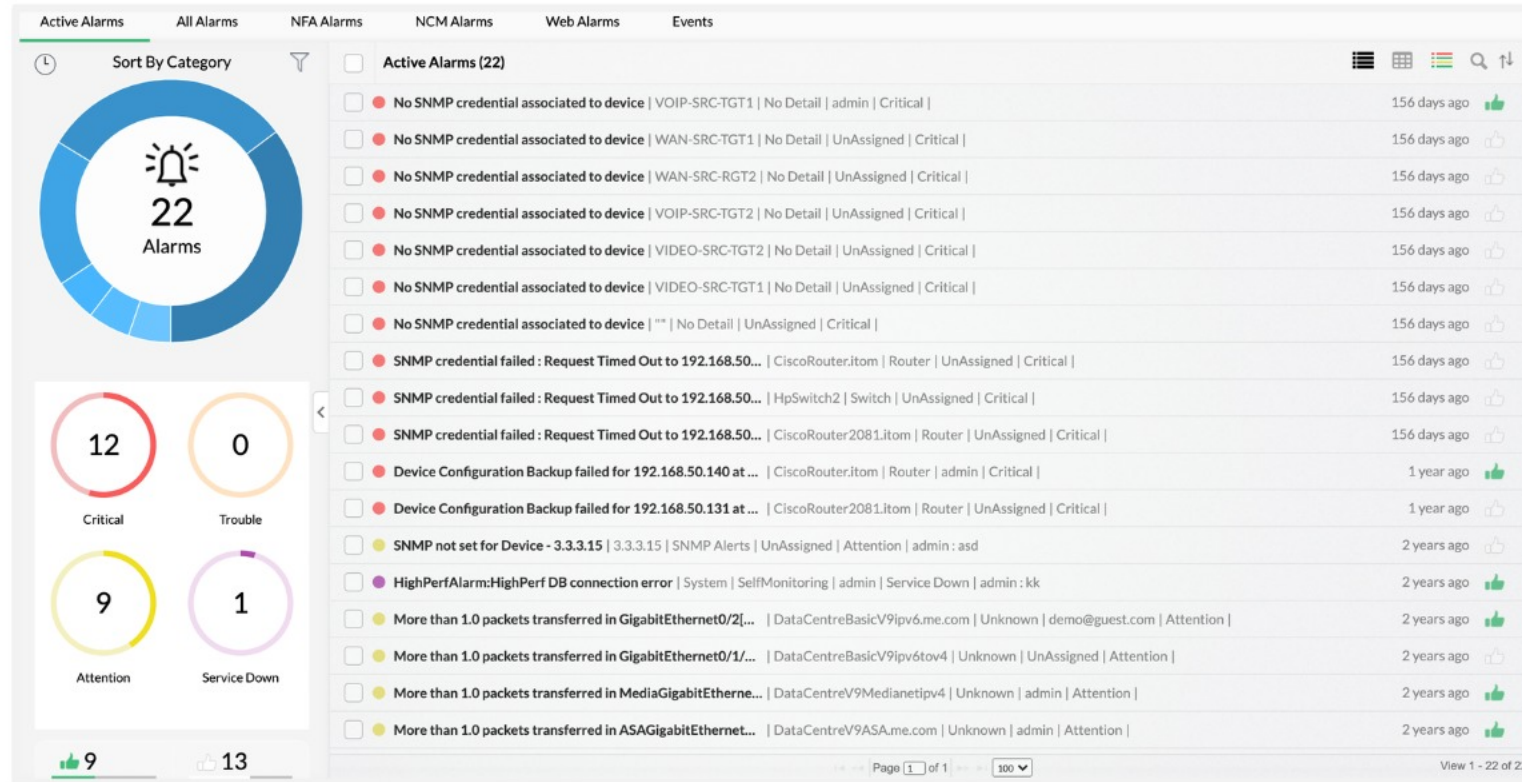
**Application**   **Services**   **DSCP**   **AS View**   **Cloud Services**

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.xxx.xx	104.16.203.xx	2019-12-18	
SugarSync	File Sharing	208.94.xxx.xx	208.94.4.xx	2018-12-17	
Office 365	File Sharing	40.84.xxx.xx	40.84.199.xx	2015-03-12	
4shared	File Sharing	204.155.xxx.xx	204.155.149.xx	2018-05-29	
Sendspace	File Sharing	69.31.xxx.xx	69.31.136.xx	2015-03-12	
Hightail	File Sharing	35.165.xxx.xx	35.165.148.xx	2019-09-27	
Carbonite	Online Storage	45.60.xxx.xx	45.60.171.xx	2019-09-27	
CrashPlan	Online Storage	216.17.xxx.xx	216.17.8.xx	2015-03-12	
Mozy	Online Storage	52.170.xxx.xx	52.170.7.xx	2019-07-10	
Flickr	Arts and Entertainment	13.35.xxx.xx	13.35.209.xx	2019-12-18	
Photobucket	Photo Sharing	209.17.xxx.xx	209.17.68.xx	2015-03-12	
Shutterfly	Photo Sharing	136.179.xxx.xx	136.179.236.xx	2015-03-12	
Pintrest	Photo Sharing	72.52.xxx.xx	72.52.10.xx	2015-03-12	

Recognize, categorize, monitor, and manage internet cloud services in your network custom-defined based on IP ranges.

# Real-time alerts



Generate real-time and aggregated threshold-based alerts to get notified via email, SMS, log a ticket, chat, run a program, web alarm, syslog and trap profiles

# Notification Templates

The screenshot displays the NetFlow Analyzer web interface. The top navigation bar includes tabs for General Settings, Discovery, Monitoring, Tools, NetFlow (which is active), NCM, and OpUtils. On the left, a sidebar lists various configuration categories, with 'Notification Templates' highlighted. The main content area is titled 'Notification Template Types' and includes a sub-header: 'Choose the template type you would like to receive any fault in your network or devices.' Below this, there are nine selectable notification template options arranged in a 3x3 grid:

- 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.

NetFlow Analyzer seamlessly integrates with ManageEngine ServiceDesk Plus/ServiceNow, JIRA Service Desk, and Slack to create and manage custom notification templates for frequently used alert types.



Reports

# Network traffic 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

Billing

Measure bandwidth usage to verify your ISP billing and create bill plans

# Inventory report

The screenshot shows a web interface for NetFlow reports. The main content area is titled 'Inventory Report' and is filtered for 'Last Hour'. The report is organized into columns for Router Name, Interface Name, and traffic statistics. The traffic statistics are further divided into IN and OUT categories, each with sub-columns for Traffic, Max, Min, Avg, and Link Speed.

Router Name	Interface Name	IN					OUT				
		Traffic	Max	Min	Avg	Link Speed	Traffic	Max	Min	Avg	Link Speed
DataCentreA VC-Mains- NBAR2/QoS/ ART	GigabitEther net0/1	22.180 KB	644.000 Bytes	157.000 Bytes	363.607 Bytes	10.000 Kbps	23.185 KB	730.000 Bytes	202.000 Bytes	380.082 Bytes	10.000 Kbps
DataCentreA VC-Mains- NBAR2/HTT P	GigabitEther net0/1/1	4.275 KB	128.000 Bytes	21.000 Bytes	70.082 Bytes	10.000 Kbps	4.438 KB	129.000 Bytes	27.000 Bytes	72.754 Bytes	10.000 Kbps
DataCentreB asicV9- NBAR/CBQo S	GigabitEther net0/1/1	452.799 KB	8.571 KB	6.358 KB	7.423 KB	10.000 Kbps	231.370 KB	4.781 KB	2.708 KB	3.793 KB	1.000 Kbps
DataCentreB asicV9ipv4.m e.com	GigabitEther net0/1/2	455.543 KB	8.680 KB	5.712 KB	7.468 KB	20.000 Kbps	460.550 KB	8.560 KB	6.353 KB	7.550 KB	20.000 Kbps
DataCentreB asicV9ipv6.m e.com	GigabitEther net0/2	466.188 KB	8.558 KB	6.568 KB	7.642 KB	1.000 Kbps	461.258 KB	8.450 KB	6.401 KB	7.562 KB	1.000 Kbps
DataCentrei pV4Bi-ASA	GigabitEther net0/1/2	6.871 MB	126.971 KB	80.404 KB	112.636 KB	8.000 Kbps	6.867 MB	124.097 KB	83.169 KB	112.574 KB	8.000 Kbps













Generate Inventory reports with the option to demarcate In/Out data of your entire network based on traffic type.



# Save and Schedule Reports

Report Profiles

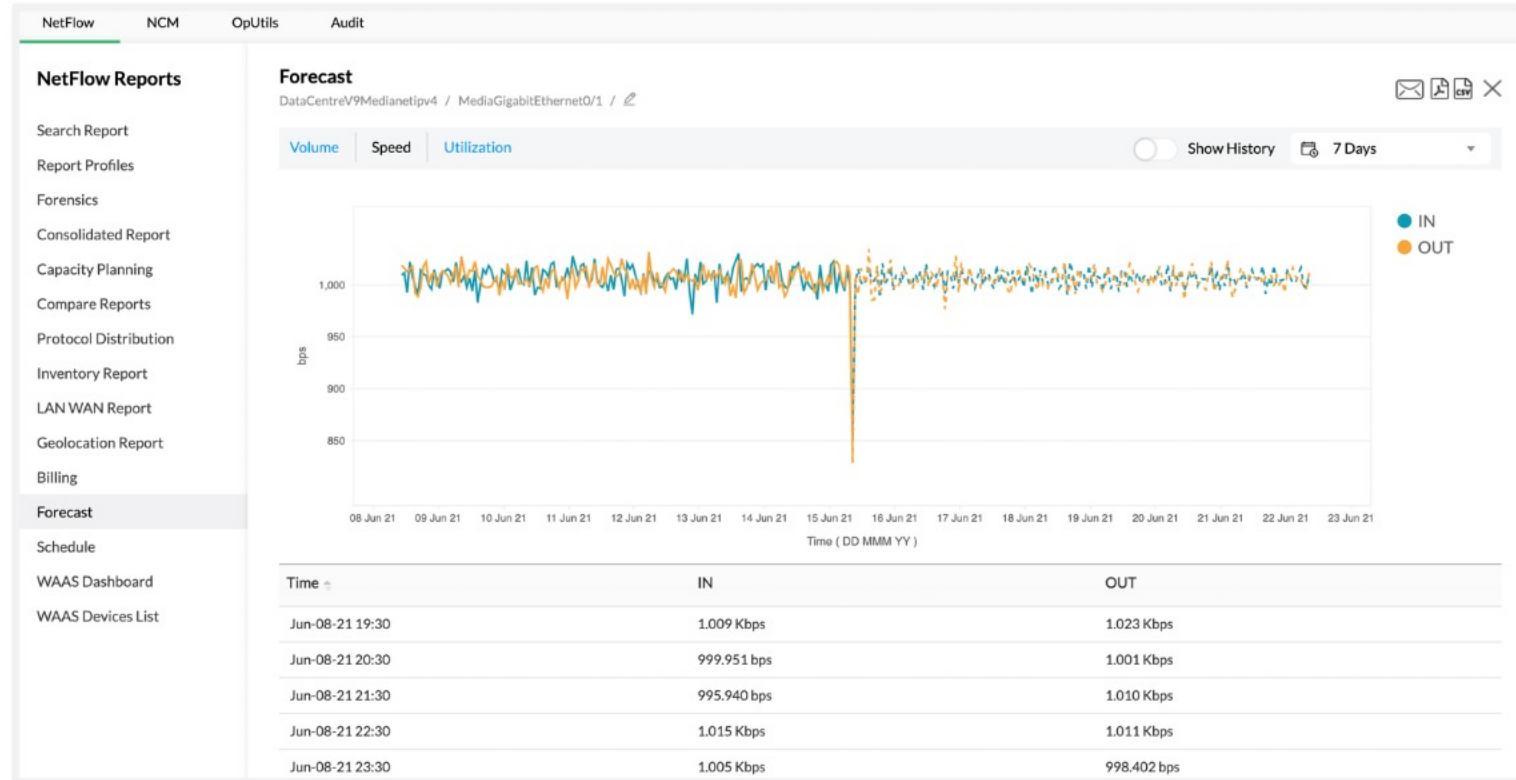
Profile Filter Add Profile

Profile Name	Time Period	Reports	Copy	Edit	Delete	Q
<input type="text"/>	<input type="text"/>					
▶ Non Critical	Last Hour	<a href="#">View Reports</a>				
▶ Application last 7 days	Last 7 Days	<a href="#">View Reports</a>				
▶ Top Protocols	Last Hour	<a href="#">View Reports</a>				
▶ Critical Profile	Last Hour	<a href="#">View Reports</a>				

- **Report profile:** Create and save your criteria based reports and view them at any time.
- **Schedule report:** Add a schedule - daily, weekly or monthly to get notified via email.



# Forecast reports



Forecast bandwidth utilization of any device and application usage across your network for any device.

# Capacity planning reports

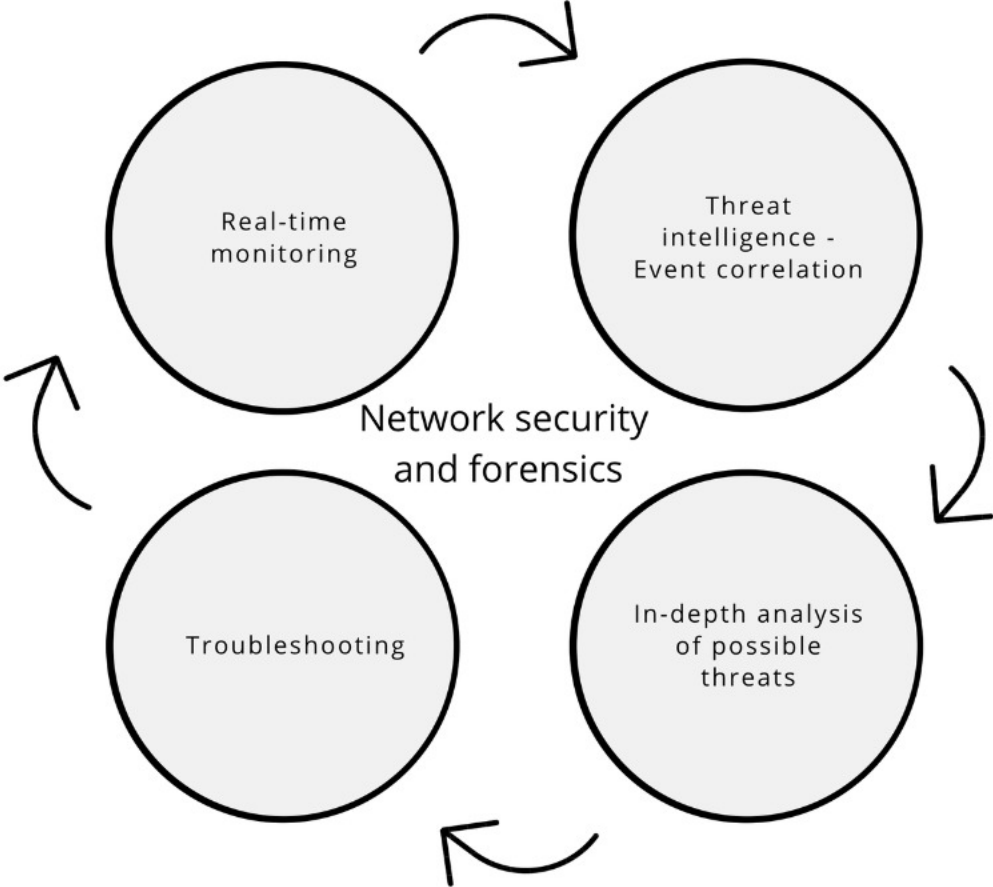


Measure and manage your bandwidth usage, identify application usage and growth patterns over any period of time.



# Network security

# Network forensics

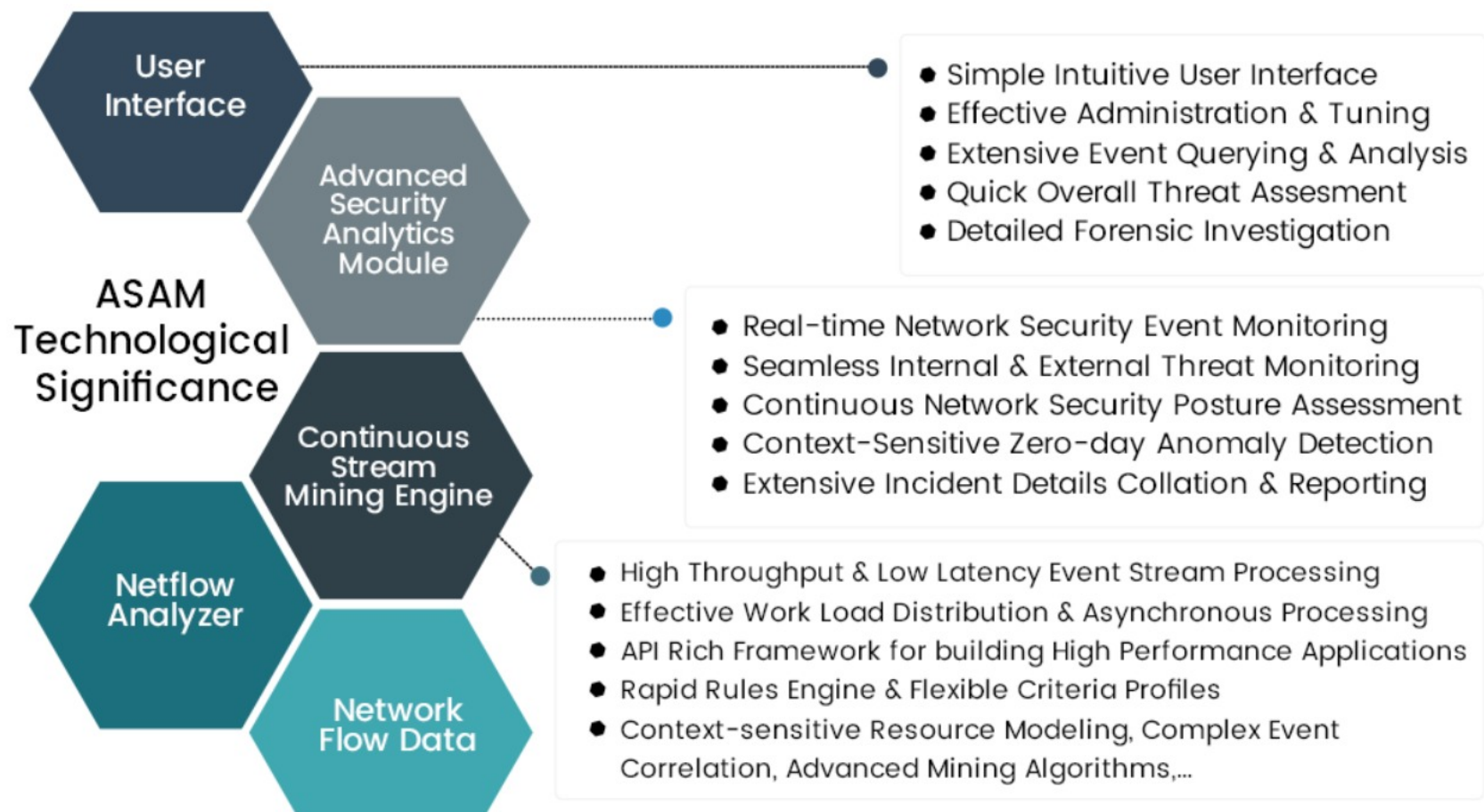


# Forensics reports



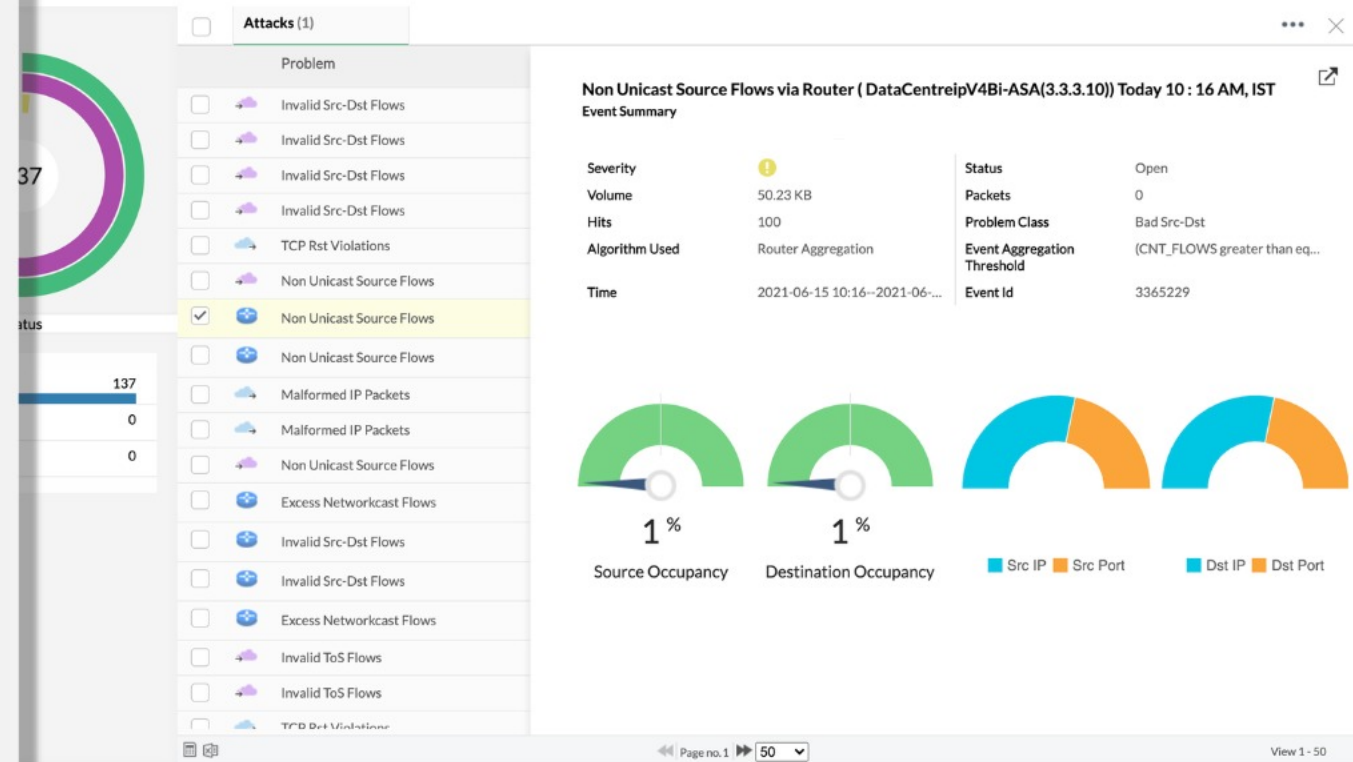
Proactively identify network traffic issues and anomalies, and monitor network infrastructure, overall performance, and bandwidth usage.

# Security Module - Advanced security analytics



# Detect attacks with the Security Module

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

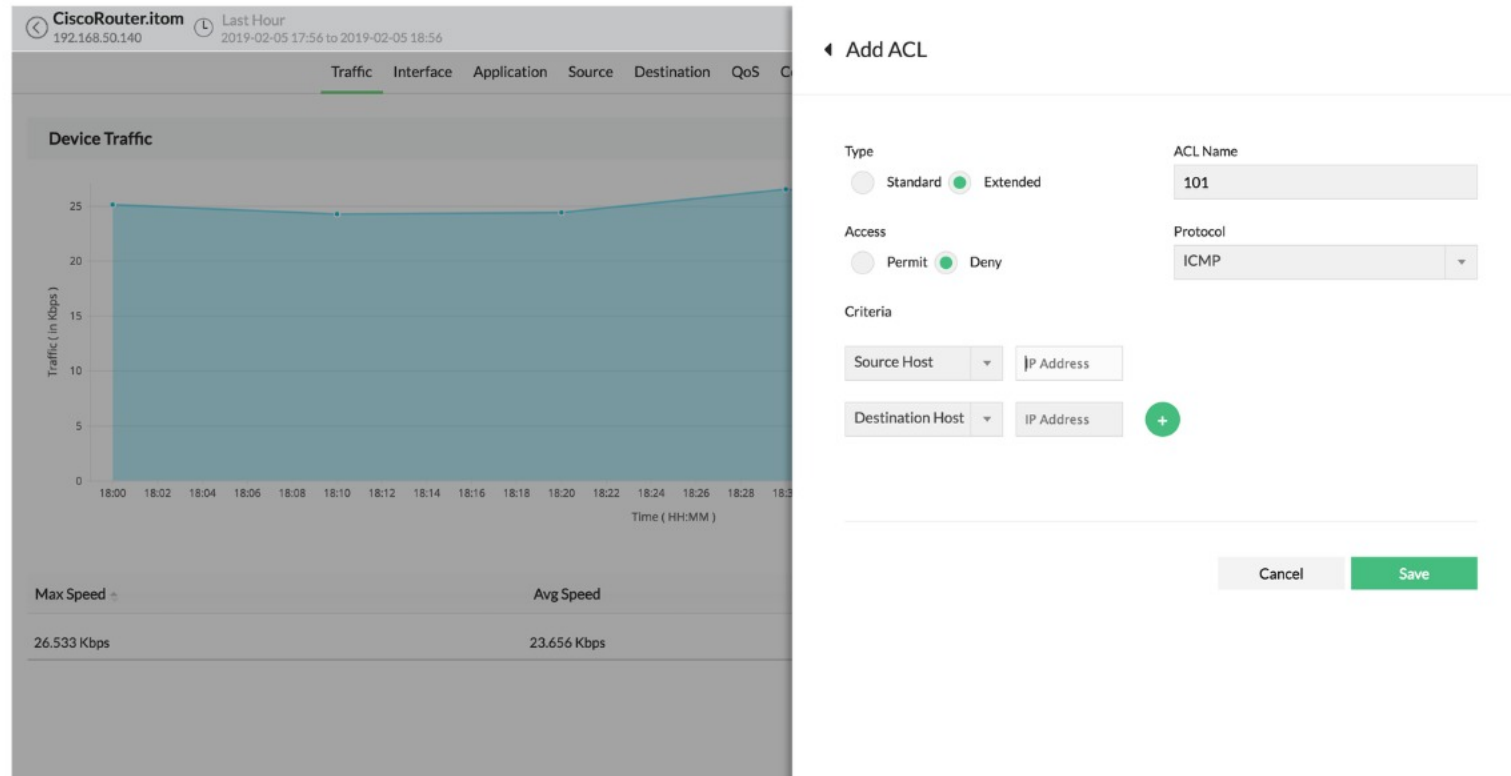




# Traffic Shaping

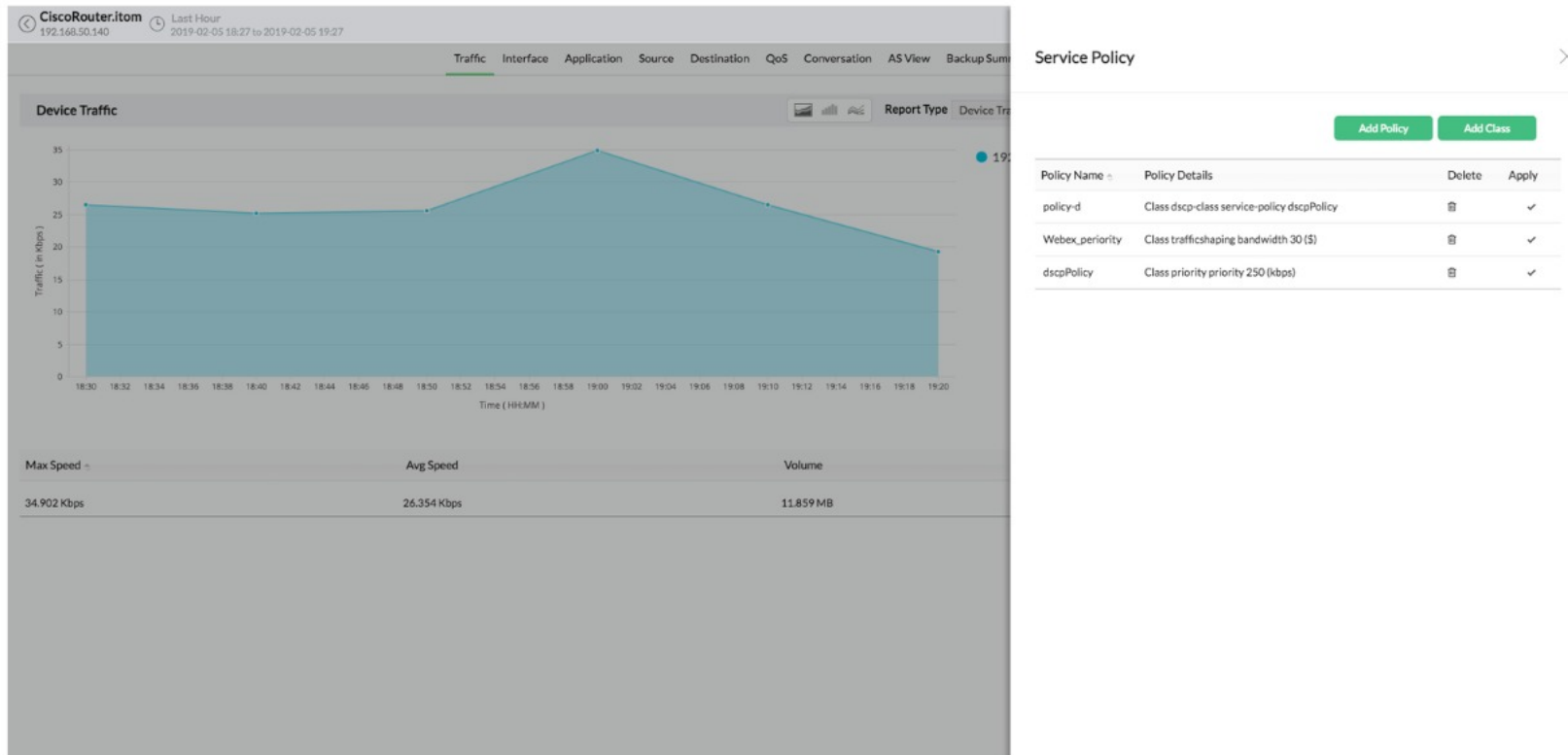


# Access control list (ACL)



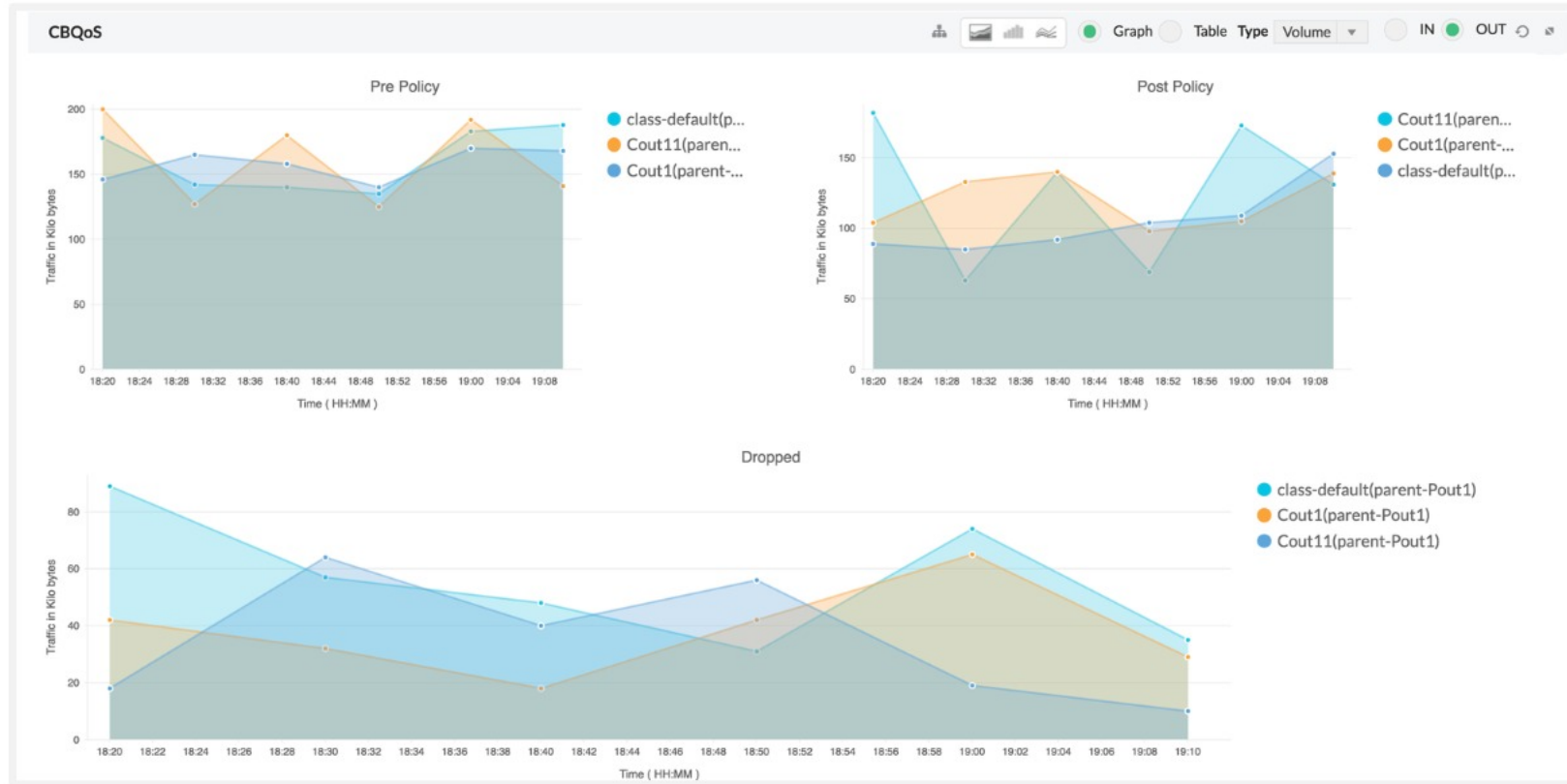
Filter out excess router traffic by blocking or restricting IPs/ IP networks.

# Service Policy



Manage your service policies and limit access to apps based on priority.

# Validate QoS policies with CBQoS



Monitor the pre-policy and post-policy performance with the CBQoS for various time periods and compare their efficiency.



# Integrations

# Applications Manager Integration

Map and monitor business application servers and help ensure business-critical applications meet end-user requirements.

## 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  : 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

# OpUtils Integration

The screenshot displays the OpUtils web interface for managing IP addresses. The left sidebar shows a tree view of the network structure under 'Your Company', including folders for 'Default Group', 'DHCP Servers', 'Discovered Subnets', 'Discovered v6 Hosts', and a series of 'OpUtils' folders (OpUtils201 through OpUtils2011). The main content area is titled 'Your Company > OpUtils202 > 172.20.2.0/24' and features a 'Subnet Summary' tab. The summary table lists the following details:

Subnet Address	172.20.2.0
Subnet Name	
Subnet Mask	255.255.255.0
Subnet Size	254
Subnet Usage	0.0%
VLAN Name	
Location	
Last Scan Time	27 Jul 20, 02:12 PM
Description	
Scan Status	Scanned

Below the table, there are two circular gauges. The 'IP Availability' gauge shows a large orange circle representing 254 transient IP addresses. The 'DNS Status' gauge shows a large red circle representing 254 N/A (Not Available) status. A legend at the bottom of the gauges defines the colors: Used (red), Available (green), Transient (orange), Not Scanned (blue), Success (green), Rev. Lookup Failed (blue), Fwd. Lookup Failed (yellow), Fwd. Lookup IP Mismatch (purple), and N/A (red).

Manage IP addresses and switch ports better.

# Network Configuration Manager - What is it?

ManageEngine's Network Configuration Manager is a configuration, change and compliance management software to manage network devices such as switches, routers, firewalls to simplify the job of IT admins.



Configuration backups

Change management



Configlets

Compliance audit



Extensive reports

Disaster management



# ServiceDesk Plus Integration

The screenshot displays the 'ServiceDesk Plus - Configuration' page within a web application. The top navigation bar includes 'General Settings', 'Discovery', 'Monitoring', 'Tools', 'NetFlow', 'NCM', and 'OpUtils'. The left sidebar lists various settings categories such as 'Mail server settings', 'SMS Server Settings', 'Proxy Server Settings', 'User Management', 'Server Settings', 'System Settings', 'Rebranding', 'REST API', 'Device Snapshot Settings', 'Security Settings', 'Privacy Settings', 'Third Party Integrations', 'Self Monitoring', and 'SSH Settings'. The main content area is titled 'ServiceDesk Plus - Configuration' and features a 'Download' button in the top right corner. Below the title, there is a section 'Integrate NetFlow Analyzer with ServiceDesk Plus' with a descriptive paragraph. The 'Product Type' section has two radio buttons: 'ServiceDesk Plus' (selected) and 'ServiceDesk Plus-MSP'. The 'Server IP/DNS Name' field is a text input with a dropdown menu set to 'http' and a 'Port' field. The 'Technician Key' field is a text input with a help icon. The 'Ticket Settings' section has two radio buttons: 'Create new ticket' (selected) and 'Re-open closed ticket'. At the bottom, there is a checkbox for the license agreement and three buttons: 'Back', 'Reset', and 'Save'.

**General Settings**

Discovery Monitoring Tools NetFlow NCM OpUtils

**ServiceDesk Plus - Configuration** [Download](#)

**Integrate NetFlow Analyzer with ServiceDesk Plus**

ServiceDesk Plus is a web-based HelpDesk and Asset Management software. Integrating NetFlow Analyzer with ServiceDesk Plus will help you to automatically log NetFlow Analyzer alarms as tickets in ServiceDesk Plus.

**Product Type**

ServiceDesk Plus  ServiceDesk Plus-MSP

**Server IP/DNS Name**

http Server IP/DNS Name Port

**Technician Key** ?

**Ticket Settings**

If alert re-occurs  Create new ticket  Re-open closed ticket

By clicking Save, you acknowledge that you have read & accepted the [License Agreement of ServiceDesk Plus](#).

[Back](#) [Reset](#) [Save](#)

Automate alarm to ticket creation, asset synchronization, and maintenance scheduling.



# Service Now Integration

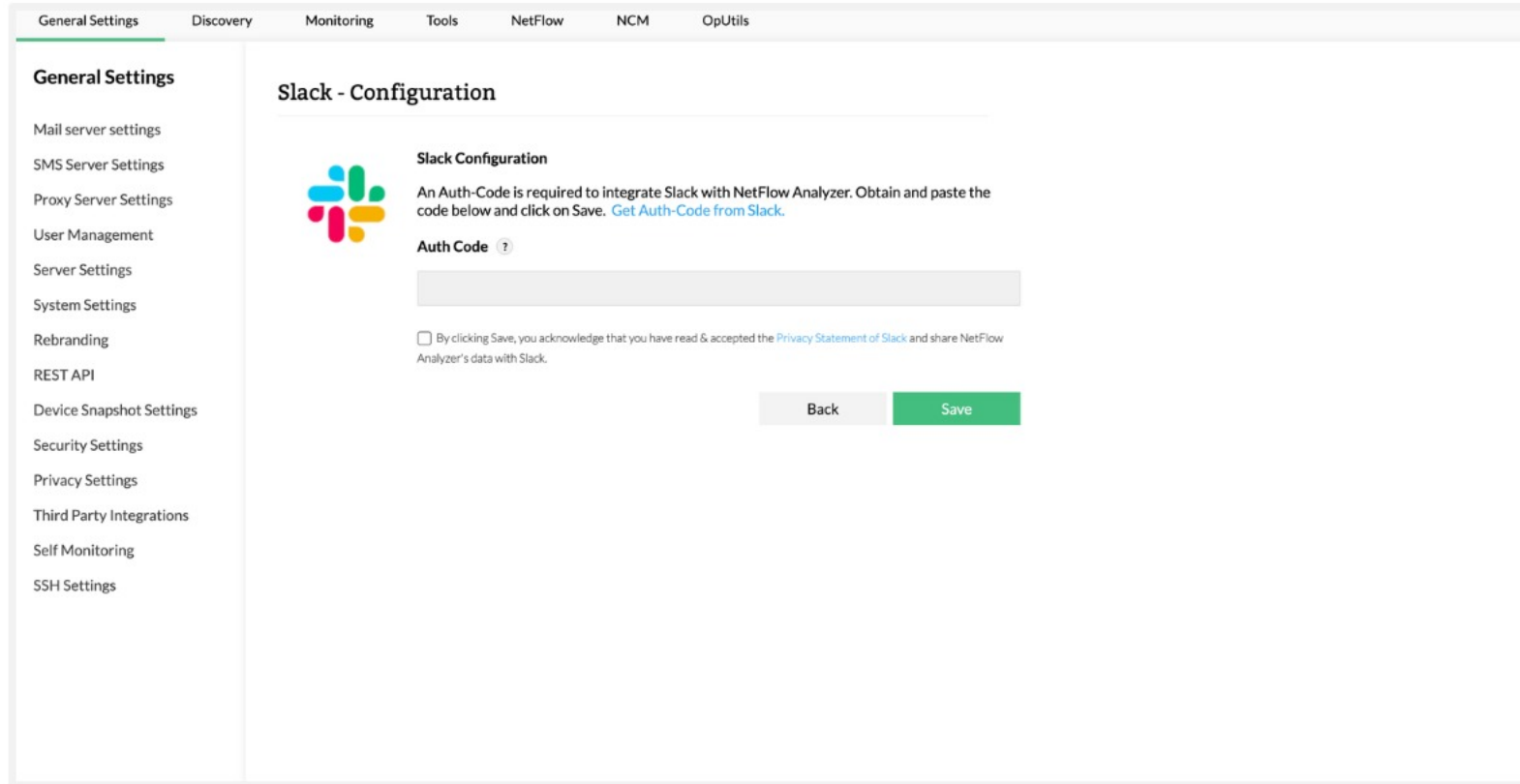
The screenshot shows a web interface for configuring ServiceNow integration. The top navigation bar includes 'General Settings', 'Discovery', 'Monitoring', 'Tools', 'NetFlow', 'NCM', and 'OpUtils'. The left sidebar lists various settings categories: 'General Settings', 'Mail server settings', 'SMS Server Settings', 'Proxy Server Settings', 'User Management', 'Server Settings', 'System Settings', 'Rebranding', 'REST API', 'Device Snapshot Settings', 'Security Settings', 'Privacy Settings', 'Third Party Integrations', 'Self Monitoring', and 'SSH Settings'. The main content area is titled 'ServiceNow - Configuration' and contains the following fields and options:

- ServiceNow Instance URL:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- Ticket Settings:**
  - If alert re-occurs:** Radio buttons for 'Create new ticket' (selected) and 'Re-open closed ticket'.
  - Clear alarm in NetFlow Analyzer when an Incident is closed/resolved in ServiceNow:** A toggle switch.
  - By clicking Save, you acknowledge that you have read & accepted the [Privacy Statement of ServiceNow](#) and share NetFlow Analyzer's data with ServiceNow.

At the bottom of the configuration area, there are three buttons: 'Back', 'Reset', and 'Save'.

Ensure effortless, real-time alert management with the automatic incident logging and bi-directional data synchronization this integration offers.

# Slack Integration



The screenshot shows a web interface with a navigation menu on the left and a main content area. The navigation menu includes: General Settings (highlighted), Discovery, Monitoring, Tools, NetFlow, NCM, and OpUtils. Under General Settings, there are sub-items: Mail server settings, SMS Server Settings, Proxy Server Settings, User Management, Server Settings, System Settings, Rebranding, REST API, Device Snapshot Settings, Security Settings, Privacy Settings, Third Party Integrations, Self Monitoring, and SSH Settings.

The main content area is titled "Slack - Configuration". It features the Slack logo and the following text: "Slack Configuration" followed by "An Auth-Code is required to integrate Slack with NetFlow Analyzer. Obtain and paste the code below and click on Save. [Get Auth-Code from Slack.](#)". Below this is a text input field labeled "Auth Code" with a help icon. At the bottom, there is a checkbox with the text: "By clicking Save, you acknowledge that you have read & accepted the [Privacy Statement of Slack](#) and share NetFlow Analyzer's data with Slack." Two buttons, "Back" and "Save", are located at the bottom right of the configuration area.

Customize alert handling tasks while reducing downtime with Slack alerts that can be configured in a notification profile, or as a step in a Workflow

# Cloud Traffic Monitoring

## 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	Q	
▼ 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"/>

Monitor and manage AWS resources and virtual private clouds in your network

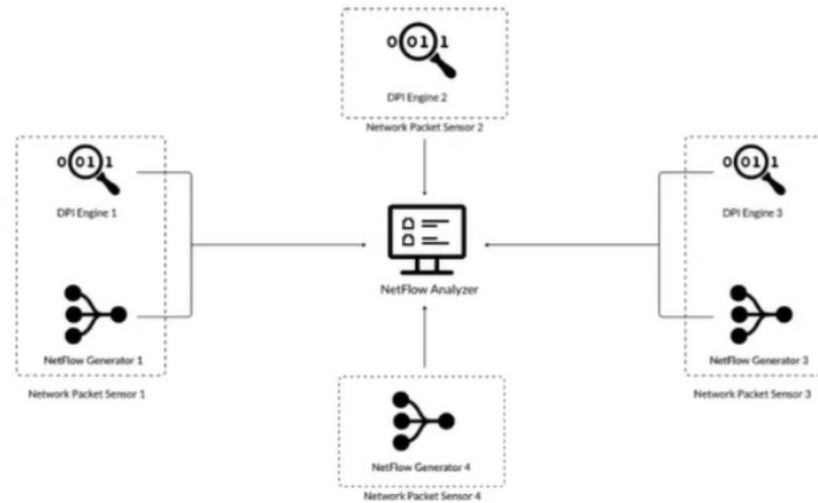
# Network Packet Sensor (NPS)

## 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.

## Network Packet Sensor Installation Key

97A7\*\*\*\*\*295C



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](#)



Get deeper insights about your network traffic with NetFlow Generator and deep packet inspection



# Other Highlights

# One-click flow export

Add  
Credentials



Executing the  
commands



Export flow



i. Predefined  
ii. Custom  
iii. NetFlow Generator

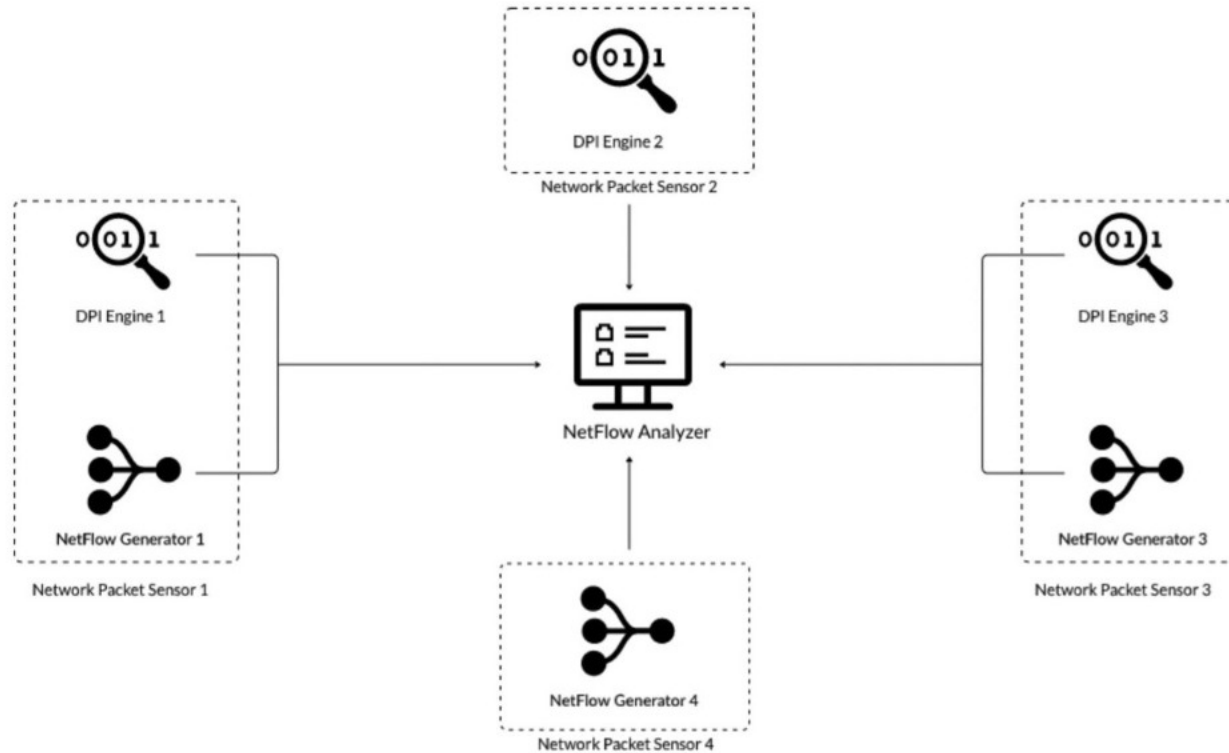
The screenshot shows a web interface for 'Predefined Flow Export'. The left sidebar contains a 'Discovery' menu with items like 'Export Flow', 'NCM Discovery', 'Discovery Report', 'Credentials', 'Inventory Updater', and 'Non Invented Devices'. The main content area has three tabs: 'Predefined Flow Export' (selected), 'Custom Flow Export', and 'NetFlow Generator'. Under 'Predefined Flow Export', there is a 'Flow export's status:' section with a green checkmark and the text 'Commands are executed. Flows are received.' Below this is an 'Execution Output:' section containing a terminal window with the following configuration commands:

```
Config t
Enter configuration commands, one per line. End with CNTL/Z.
CiscoRouter(config)#
CiscoRouter(config)#
%Exceeded maximum export destinations
CiscoRouter(config)#
ip flow-export source GigabitEthernet0/2:
ip flow-export source GigabitEthernet0/2
CiscoRouter(config)#
ip flow-export version 5:
ip flow-export version 5
CiscoRouter(config)#
ip flow-export version 5 origin-as:
ip flow-export version 5 origin-as
CiscoRouter(config)#
ip flow-cache timeout active 1:
ip flow-cache timeout active 1
CiscoRouter(config)#
ip flow-cache timeout inactive 15:
ip flow-cache timeout inactive 15
CiscoRouter(config)#
Snmp-server ifindex persist:
Snmp-server ifindex persist
CiscoRouter(config)#
Interface Backplane-GigabitEthernet0/3:
interface Backplane-GigabitEthernet0/3
```

At the bottom of the terminal window, there is a 'Note: In case of any errors in the output of command execution, contact netflowanalyser-support@managengine.com' and two buttons: 'Back' and 'Close'.

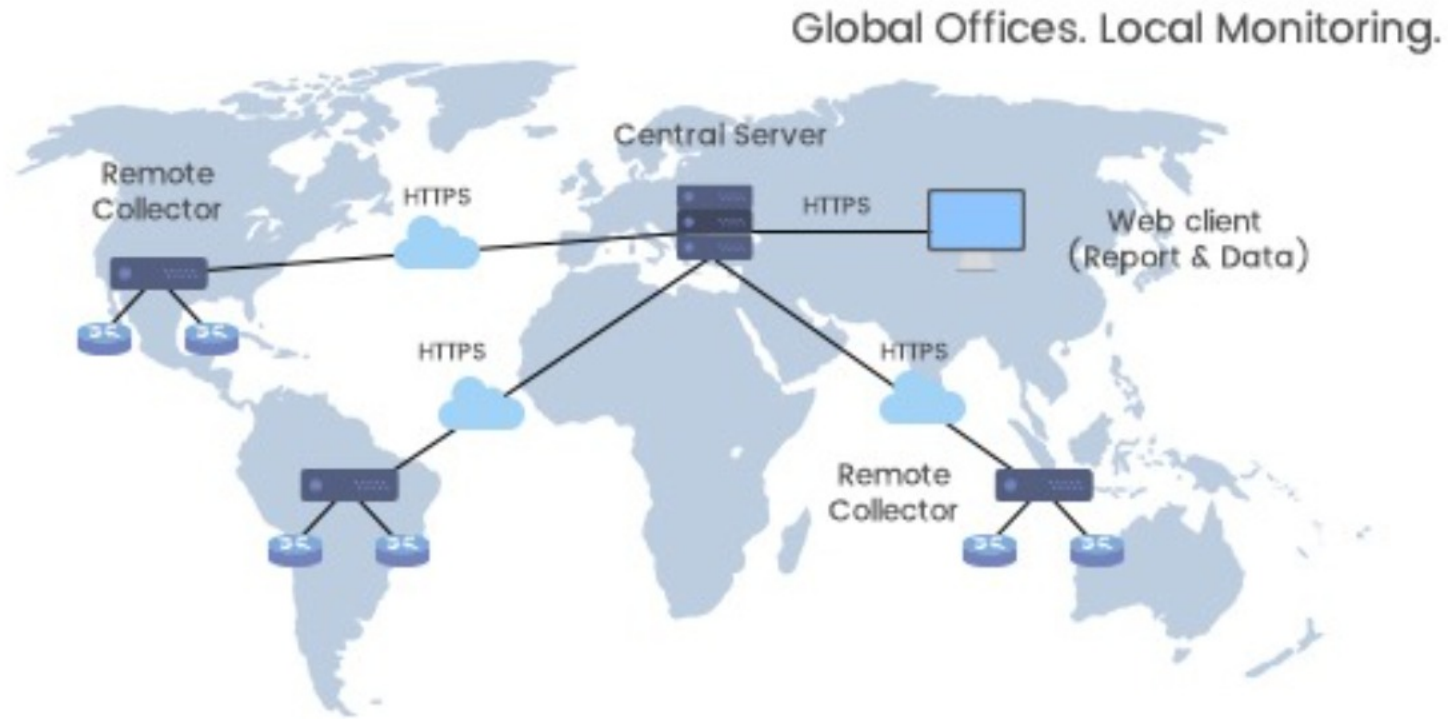
Export flows using predefined templates or custom configuration directly from the UI.

# NetFlow Generator



The Network Packet Sensor combines the functions of NetFlow Generator and deep packet inspection (DPI). The Network Packet Sensor can either be configured as a NetFlow Generator, a deep packet inspection engine, or both depending on your requirements.

# Enterprise Edition for Distributed Monitoring



High scalability and Centralized console for monitoring



# Distributed Monitoring

**Configuration**

- Storage Settings
- Mappings
- Groups Settings
- Alert Profiles
- NBAR
- CBQoS
- Attacks
- License Management
- WLC License Management
- Attacks License Management
- Flow Filter Settings
- Network Mapping
- HighPerf Reporting Engine
- Data Unit
- WAAS Settings
- Distributed Monitoring**

## Distributed Monitoring

Enable Distributed Mode

https port for Central Server  
443

Internal Collector name  
Collector1

**\* Requires Server Restart**

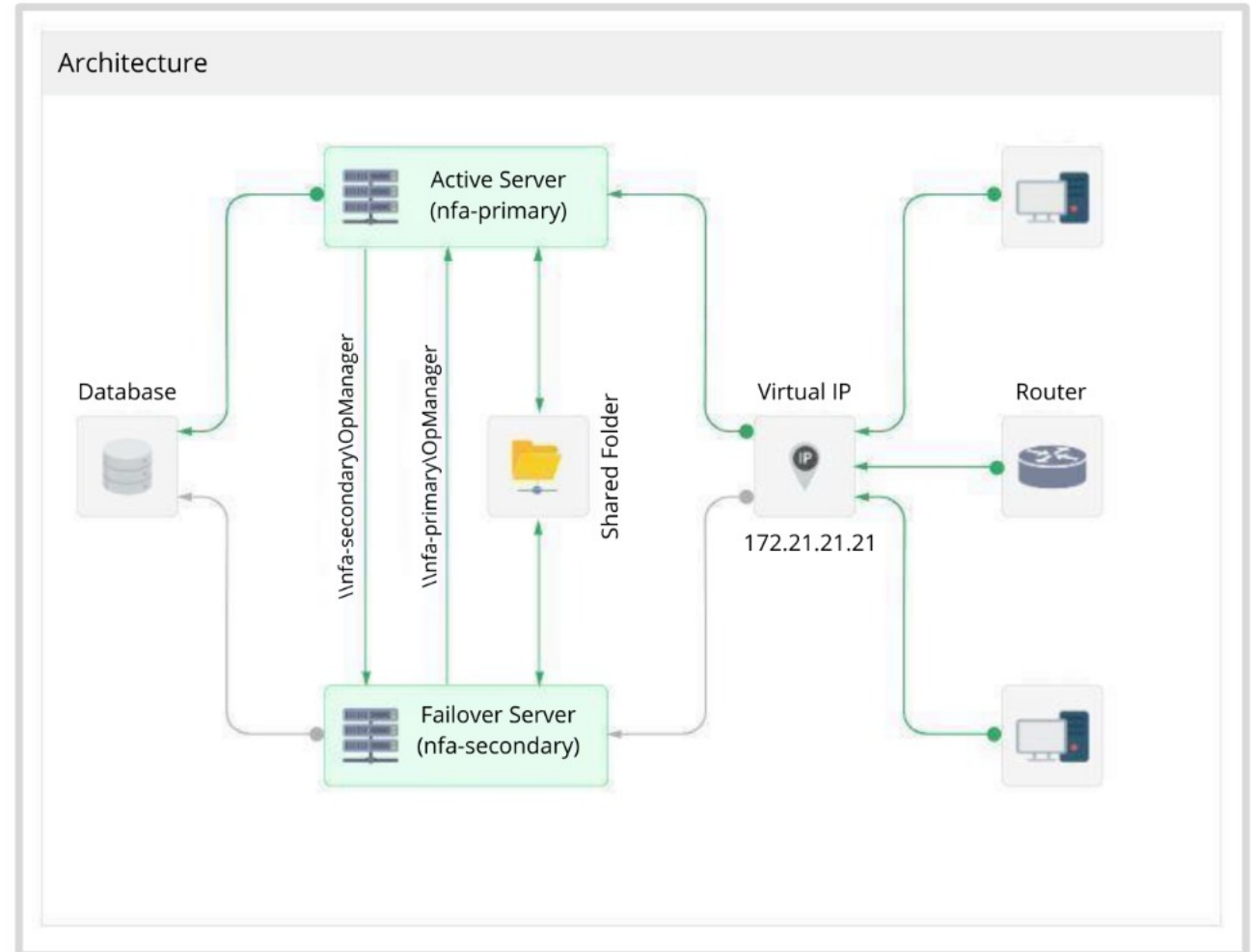
\* Note: On clicking the enable button, the product converts from Essential Edition to Distributed Edition and the process becomes irreversible.

[Enable](#)

Switch to Enterprise Edition in a single click.

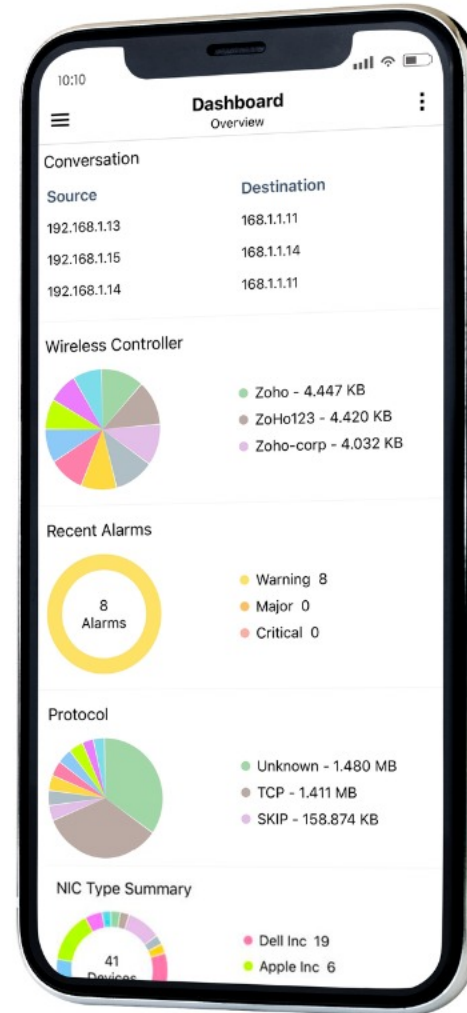
# Failover

Ensure your network is always monitored with NetFlow Analyzer's Failover. Failover offers hot-standby secondary server support for high availability.



# Mobile application

Monitor your network devices on-the-go with the NetFlow Analyzer iOS and Android apps.



# Need more help?



[youtube.com/opmanagertechvideos](https://www.youtube.com/opmanagertechvideos)



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



[forums.manageengine.com/netflowanalyzer](https://forums.manageengine.com/netflowanalyzer)



[netflowanalyzer-support@manageengine.com](mailto:netflowanalyzer-support@manageengine.com)



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

# Thank you

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