

# NetFlow Analyzer

Solution complète de gestion du trafic réseau et de la bande passante

# NetFlow Analyzer

Visibilité Accrue

+

Meilleur Contrôle

NetFlow Analyzer, un outil complet d'analyse du trafic, exploite les technologies de flux pour offrir une visibilité en temps réel des performances de la bande passante du réseau. Il est désormais doté d'une nouvelle interface utilisateur pour une visibilité accrue et un meilleur contrôle. Il porte la surveillance de la bande passante et l'analyse du trafic à un niveau supérieur, avec une facilité de contrôle.

# Exploitation de la technologie des flux

NetFlow

sFlow

J-Flow

IPFIX

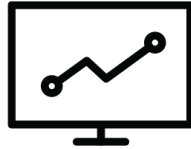
NetStream

AppFlow

NetFlow Analyzer collecte et analyse les flux provenant des principaux appareils tels que Cisco, 3COM, Juniper, Foundry Networks, Hewlett-Packard, extreme et d'autres fournisseurs leaders sur le marché.

# Fonctionnalités principales

- Offre une visibilité détaillée de votre réseau sur le trafic et la bande passante en temps réel.
- Surveillance de manière proactive les modèles de trafic réseau afin de détecter les pics de trafic et les anomalies.
- Aide à analyser les tendances d'utilisation de la bande passante pour identifier la cause première des problèmes de trafic réseau.
- Détecte les menaces de sécurité internes et externes telles que les attaques DDoS/flash-crowd, les sondes/scans, les flux suspects, etc.
- Permet de prévoir, de planifier et d'optimiser l'utilisation de la bande passante afin de garantir la priorité des applications critiques pour l'entreprise.
- Aide à définir des alertes en temps réel basées sur des seuils pour réduire le temps de réponse et permettre un dépannage plus rapide.
- Prend en charge les technologies de flux les plus courantes et les dispositifs des principaux fournisseurs.



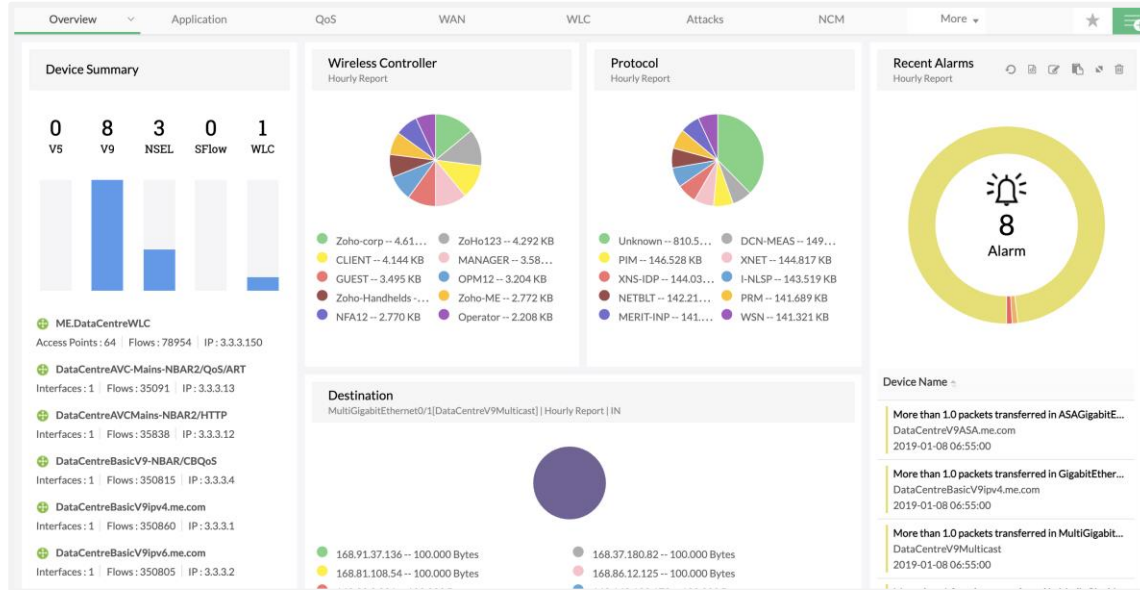
**Surveillance en temps réel**

# Connaître le qui, le quand et le quoi du trafic de votre réseau

Obtenez une visibilité détaillée de l'utilisation du trafic par

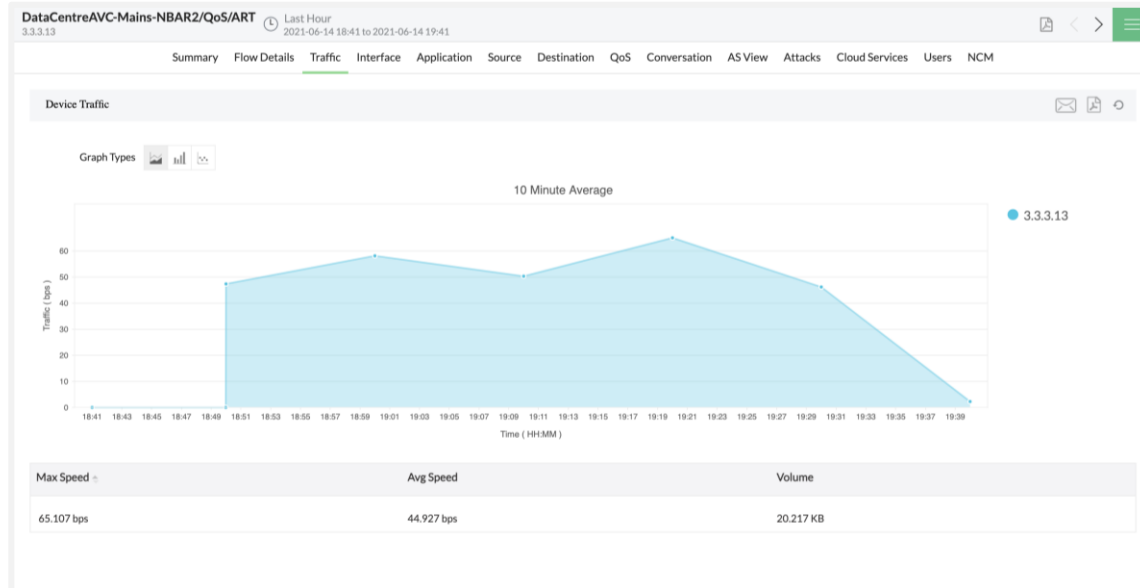
- Applications
- Protocoles
- QoS
- Source
- Destination
- Conversation

# Tableau de bord



Le tableau de bord fournit un résumé des détails du trafic tels que les principales applications, conversations, QoS, protocoles et alarmes.

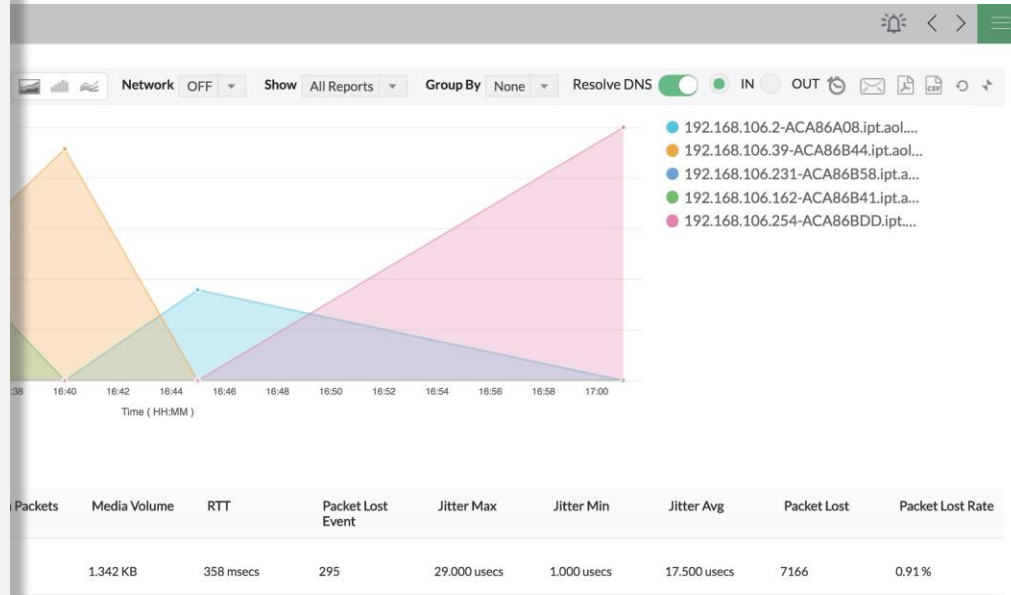
# Visibilité sur le trafic réseau



Obtenez une vue détaillée du trafic des routeurs/commutateurs pour connaître la consommation totale de bande passante par les appareils, leurs interfaces, les applications, les principales sources/destinations, la QoS et les conversations de l'inventaire.

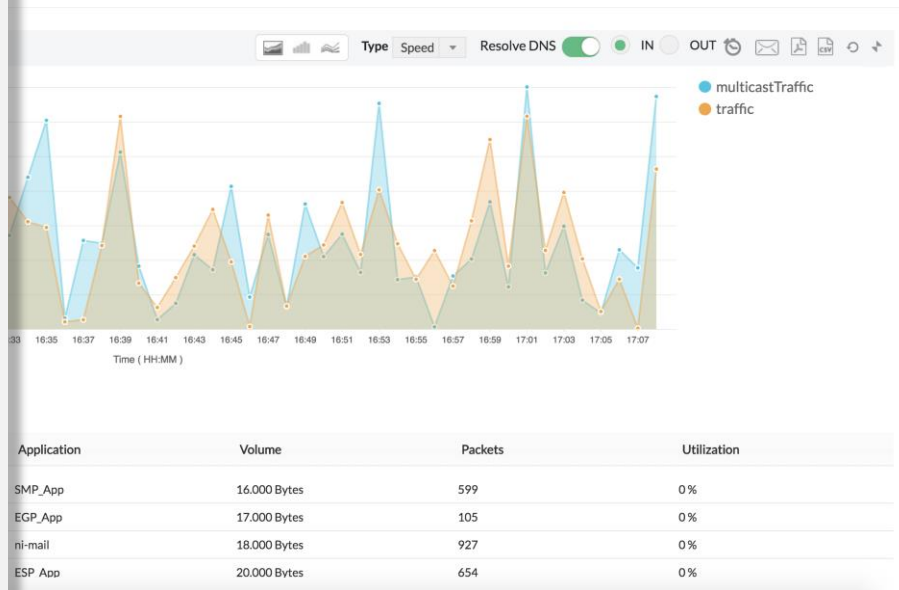
# Supervision du trafic Medianet

- Surveillez le trafic riche en médias comme le trafic vocal et vidéo pour améliorer la qualité d'expérience.
- Mesurez les statistiques de performance telles que la gigue, la perte de paquets et le temps de parcours.

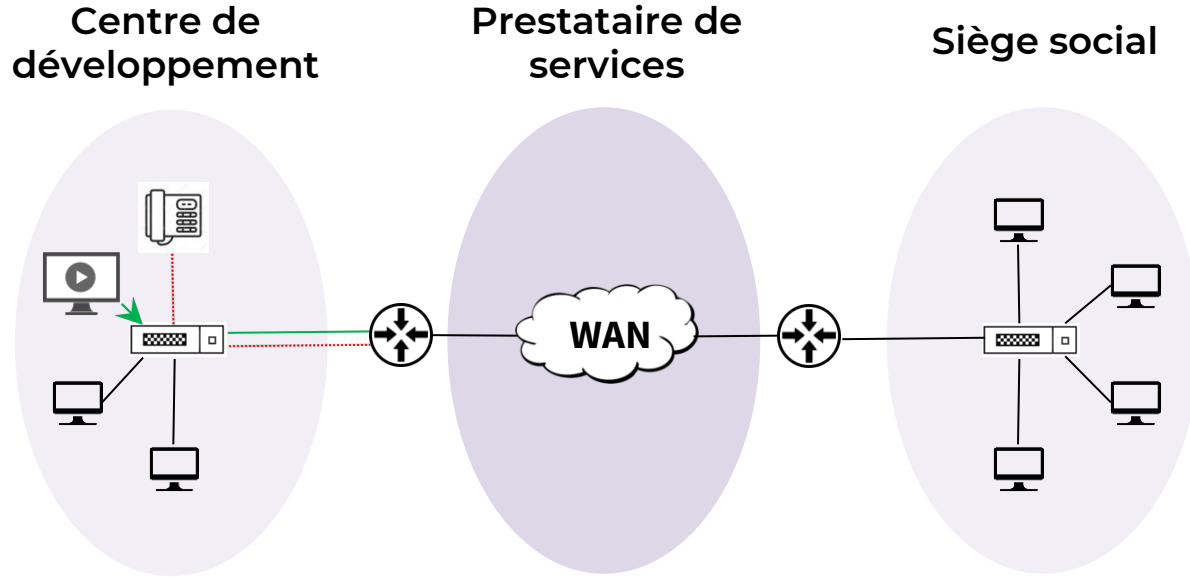


# Supervision du trafic Multicast

- La multidiffusion IP permet à un hôte d'envoyer des paquets à un groupe spécifique d'hôtes.
- Surveillez le trafic de multidiffusion en fonction de son utilisation et de sa vitesse.



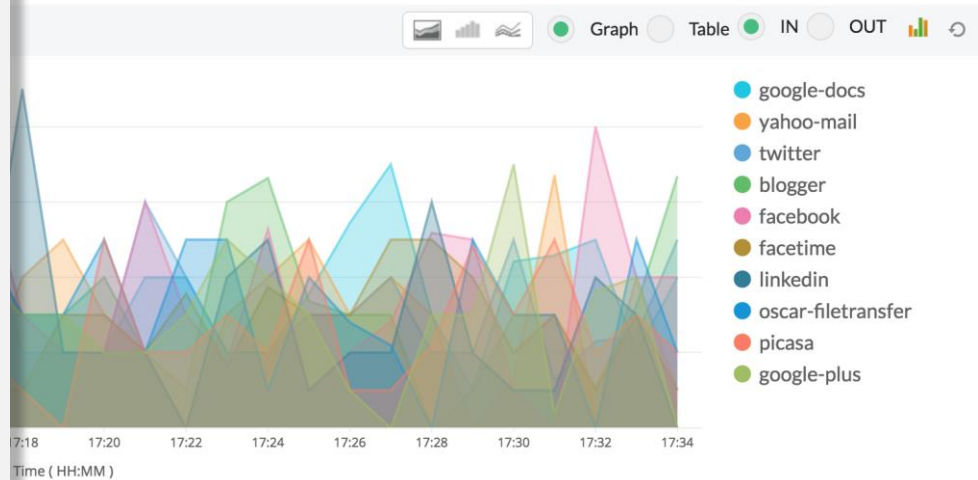
# Supervision IP SLA



Obtenez une visibilité en temps réel de votre trafic VoIP, WAN et vidéo.

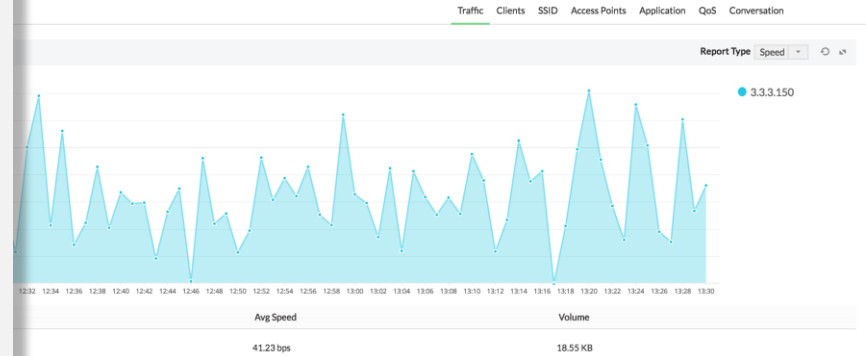
# Visibilité et contrôle des applications

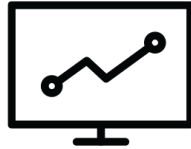
- Obtenez une visibilité sur les applications NBAR2 grâce à la supervision Cisco AVC (Application Visibility and Control).
- NBAR avancé est utilisé pour identifier le trafic Web, les URL, le partage de fichiers et les applications à port aléatoire.
- Visualisez l'application NBAR2, le nombre d'occurrences d'URL (rapport sur les hôtes HTTP), la hiérarchie des classes de QoS et les rapports de surveillance du temps de réponse des applications (surveillance ART).
- Comment l'activer: Des champs supplémentaires doivent être configurés pendant l'exportation du flux.



# Supervision du trafic LAN sans fil

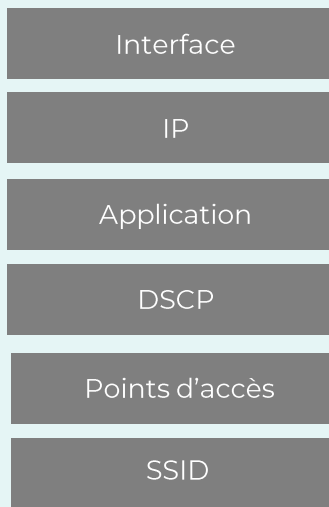
- Surveillez les contrôleurs WLAN Cisco.
- Trouvez les principaux utilisateurs du trafic par points d'accès, SSID, applications, clients, etc.
- Regroupez les réseaux locaux sans fil par SSID.
- Dépannez les pics de bande passante en identifiant la consommation par SSID, en trouvant ses principaux clients et les détails complets de la conversation pour la période sélectionnée.





**Personnalisez NetFlow Analyzer  
pour l'adapter à votre réseau**

# Trier l'utilisation du trafic par groupes

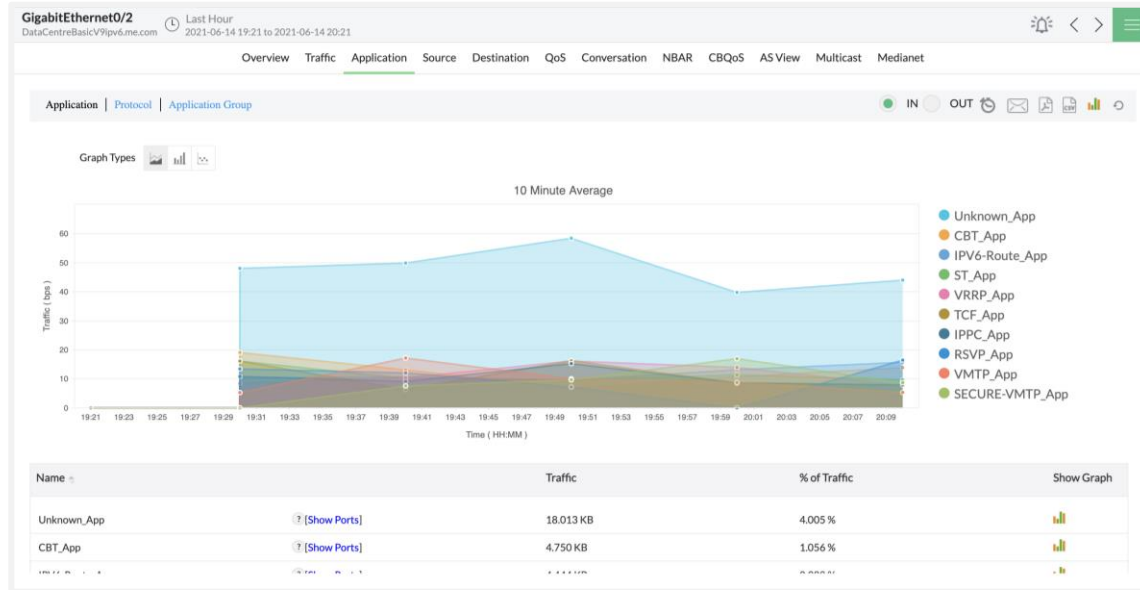


Types de groupes

Avantages de la création de groupes :

- Classez le trafic par département, sous-réseaux, branches, applications connexes, VLAN, etc.
- Surveillez l'utilisation combinée de la bande passante pour obtenir une meilleure image de la consommation du trafic.
- Fournir un accès aux opérateurs en fonction des groupes.
- Fournir une meilleure visibilité pour améliorer le dépannage.

# Cartographier et surveiller les applications personnalisées



Définissez des noms d'applications personnalisées en fonction du port et du protocole et obtenez des informations détaillées sur leur utilisation.

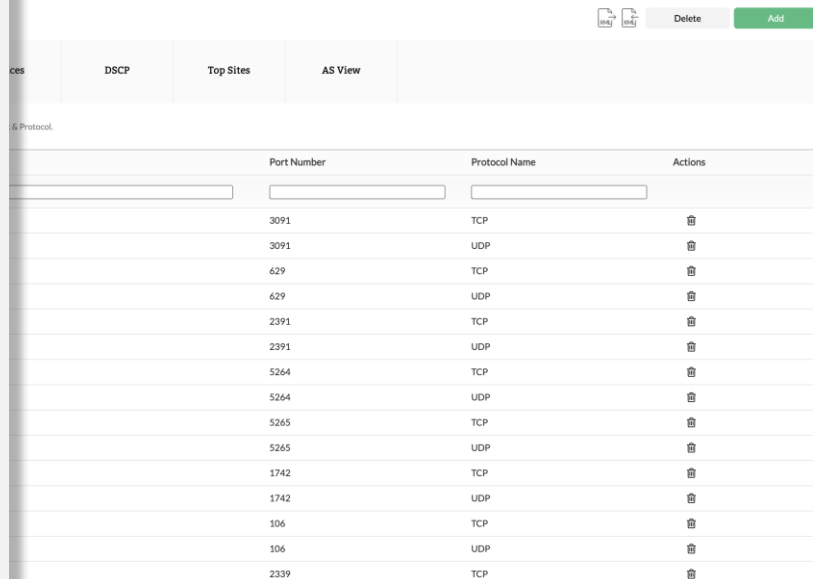
# Cartographie UserName-IP (Nom d'utilisateur-IP)

- Cartographie manuelle :

Le mappage manuel utilise des données de cartographie UserName-IP importées manuellement pour résoudre et attribuer des noms d'utilisateur à des adresses IP.

- Active Directory :

La fonction de mappage d'Active Directory (AD) récupère automatiquement les configurations de cartographie de noms d'utilisateurs et d'adresses IP à partir des serveurs proxy d'Active Directory pour affecter les noms d'utilisateurs et d'hôtes aux adresses IP correspondantes.



The screenshot shows a web interface with a table of network configurations. At the top right, there are icons for 'Add' and 'Delete', and a green 'Add' button. Below the table, there are input fields for 'Port Number' and 'Protocol Name'. The table contains the following data:

Port Number	Protocol Name	Actions
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	

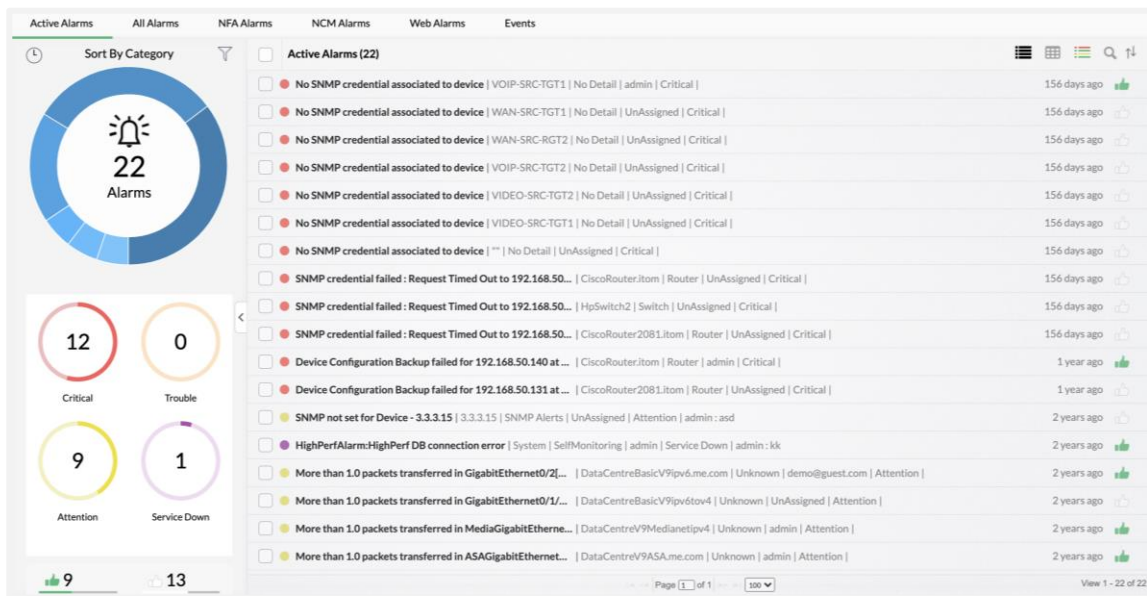
# Services Cloud

The screenshot displays the 'Map' section of a NetFlow management interface. On the left is a sidebar with navigation options: 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, and WAAS Settings. The main area is titled 'Map' and contains a tabbed interface with 'Cloud Services' selected. Below the tabs is a table of cloud services with columns for Name, Category, Network Start, Network End, Add Date, and Actions. An 'Add' button is visible in the top right corner.

Cloud Service Name	Category	Network Start	Network End	Add Date	Actions
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	
Shutterstock	Photo Sharing	136.179.xxx.xx	136.179.236.xx	2015-03-12	
Pinterest	Photo Sharing	72.52.xxx.xx	72.52.10.xx	2015-03-12	

Reconnaissez, catégorisez, surveillez et gérez les services Internet en cloud dans votre réseau, définis de manière personnalisée en fonction des plages d'adresses IP.

# Alertes en temps réel



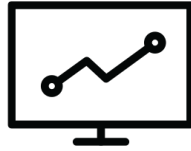
Générer des alertes en temps réel et agrégées basées sur des seuils pour être notifié par e-mail, SMS, enregistrement d'un ticket, chat, exécution d'un programme, alarme web, syslog et profils de piège.

# Modèles de notification

The screenshot displays the 'NetFlow' configuration page in a management console. The top navigation bar includes 'General Settings', 'Discovery', 'Monitoring', 'Tools', 'NetFlow' (selected), 'NCM', and 'OpUtils'. On the left, a sidebar lists various settings categories under 'NetFlow', including Basic Settings, Storage Settings, Groups Settings, Mappings, UserName-IP Mapping, LAN IP Settings, Alert Profiles, Notification Templates, NBAR, CBQoS, Attacks, NetFlow Generator, License Management, WLC License Management, Attacks License Management, Flow Filter Settings, Network Mapping, Data Unit, and WAAS Settings. The main content area is titled 'Notification Template Types' and contains the instruction: 'Choose the template type you would like to receive any fault in your network or devices.' Below this, there are nine selectable options, each with an icon and a brief description:

- 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 s'intègre de manière transparente à ManageEngine ServiceDesk Plus/ServiceNow, JIRA Service Desk et Slack pour créer et gérer des modèles de notification personnalisés pour les types d'alertes fréquemment utilisés.



# Rapports

# Rapports sur le trafic réseau

Rapport de recherche

Recherche de détails spécifiques sur le trafic par application, protocole, hôte ou IP associés.

Rapport de comparaison

Comparer l'utilisation de la bande passante à différents intervalles de temps

Rapport consolidé

Suivez les principaux interlocuteurs et les principales conversations grâce à un rapport complet.

Facturation

Mesurez l'utilisation de la bande passante pour vérifier la facturation de votre FAI et créer des plans de facturation.

# Rapport d'inventaire

The screenshot shows a web-based interface for network management. The main menu includes 'NetFlow', 'NCM', 'OpUtils', and 'Audit'. The 'NetFlow Reports' section is active, with a sidebar listing various report types. The 'Inventory Report' is selected, showing a table of interface traffic data. The table is filtered for the 'Last Hour' and displays columns for Router Name, Interface Name, and traffic statistics (Traffic, Max, Min, Avg, Link Speed) for both IN and OUT directions.

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 asicV9/pip4.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 asicV9/pip6.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 pV4B/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
DataCentrei	GigabitEther					100.000					100.000

Générer des rapports d'inventaire avec la possibilité de délimiter les données d'entrée/sortie de l'ensemble de votre réseau en fonction du type de trafic.

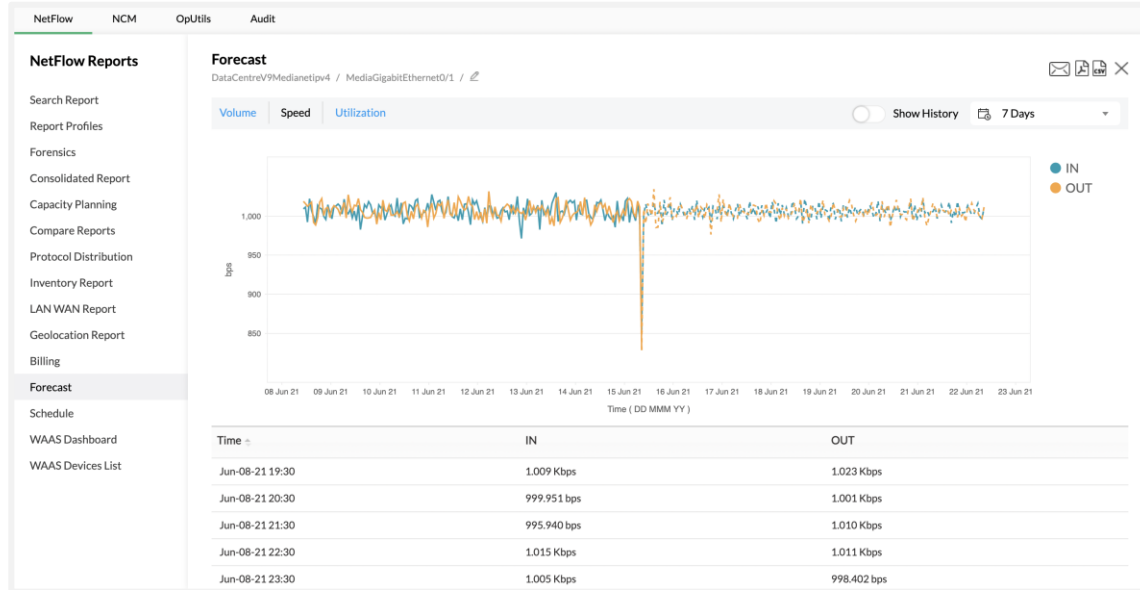
# Sauvegarde et programmation des rapports

**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>				

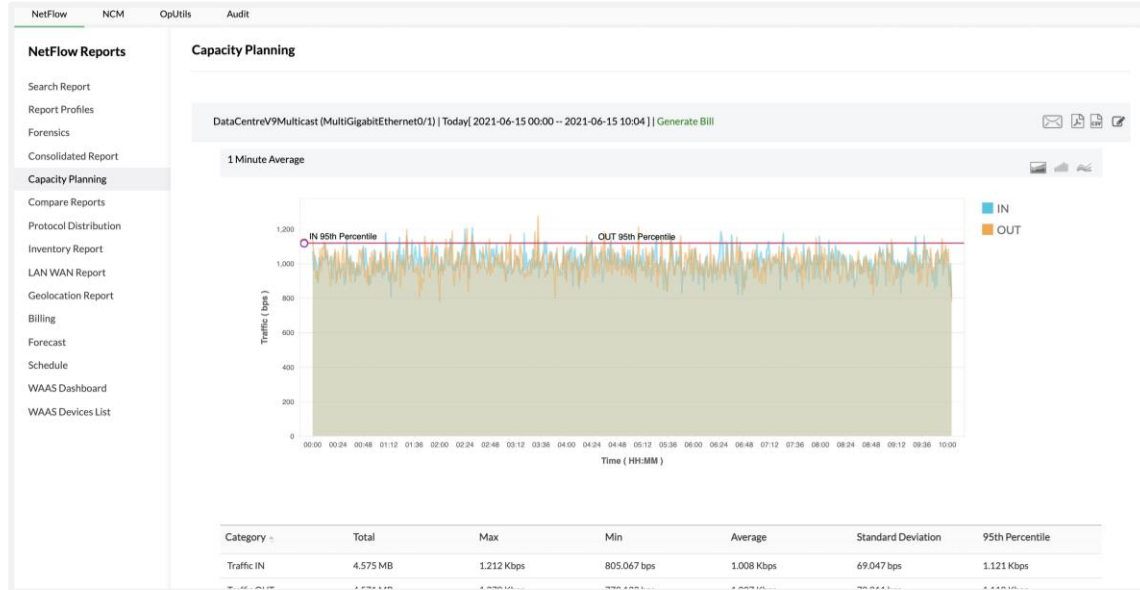
- **Profil de rapport:** Créez et enregistrez vos rapports basés sur des critères et consultez-les à tout moment.
- **Programmation des rapports:** Ajoutez un planning - quotidien, hebdomadaire ou mensuel - pour recevoir une notification par e-mail.

# Rapports prévisionnels



Prévoyez l'utilisation de la bande passante de tout appareil et l'utilisation des applications sur votre réseau pour tout appareil.

# Rapports de planification des capacités

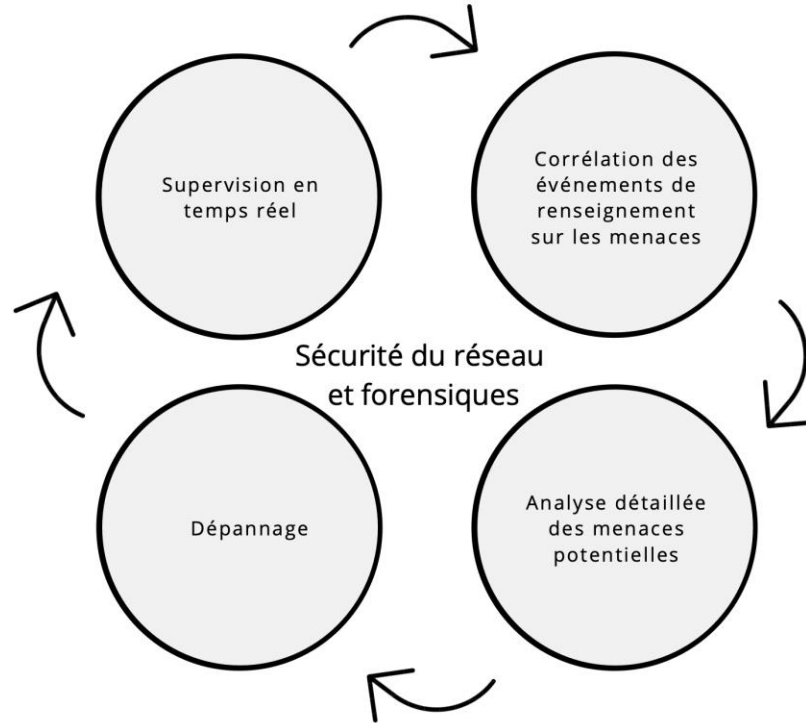


Mesurez et gérez l'utilisation de votre bande passante, identifiez l'utilisation des applications et les modèles de croissance sur une période donnée.

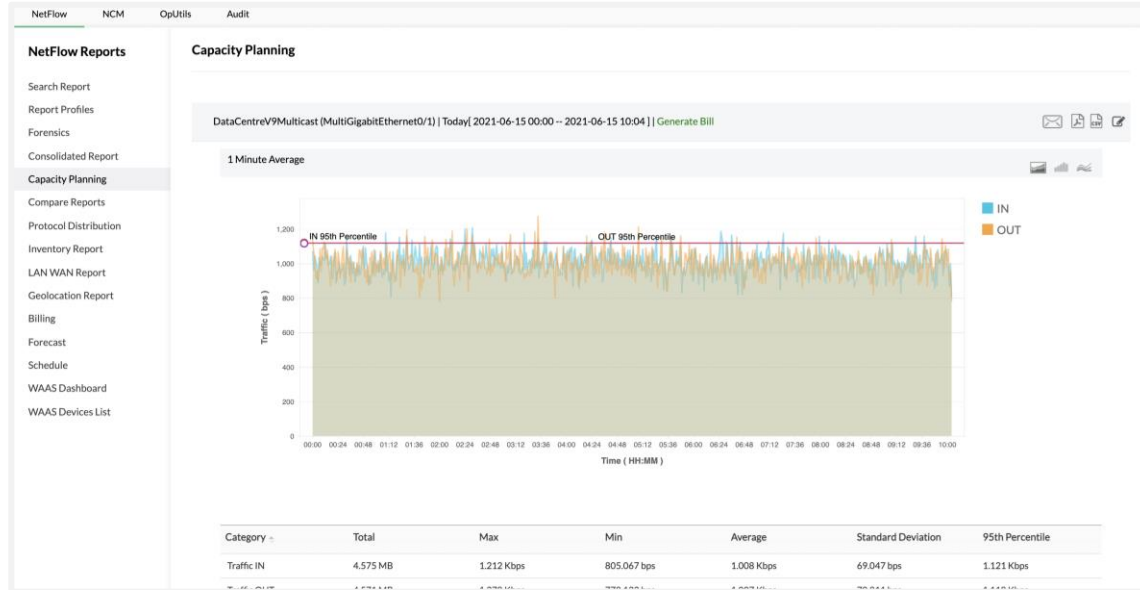


# Sécurité des réseaux

# Analyse des réseaux

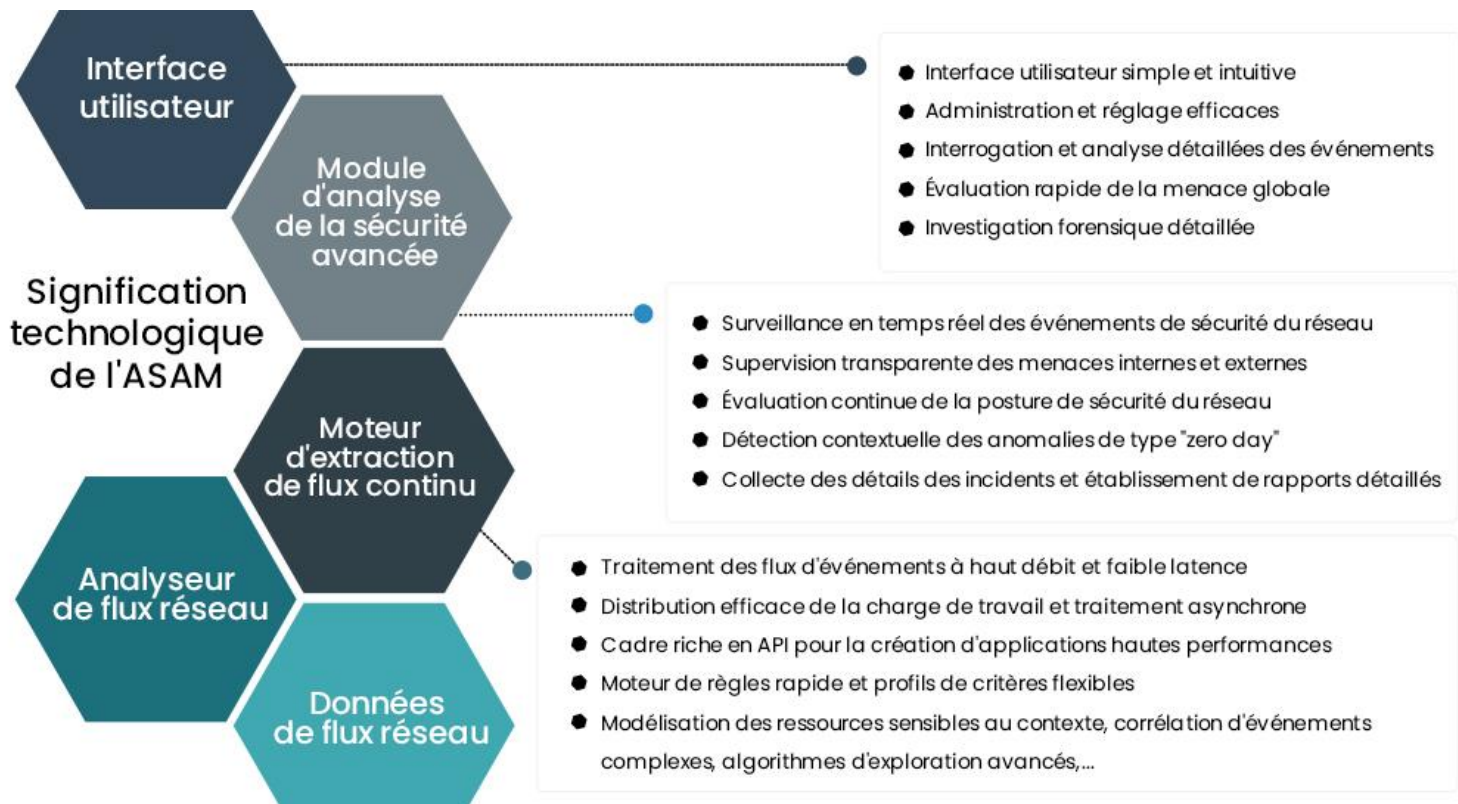


# Rapports forensiques



Identifiez de manière proactive les problèmes et les anomalies du trafic réseau, et surveillez l'infrastructure du réseau, les performances globales et l'utilisation de la bande passante.

# Analyses de sécurité avancées

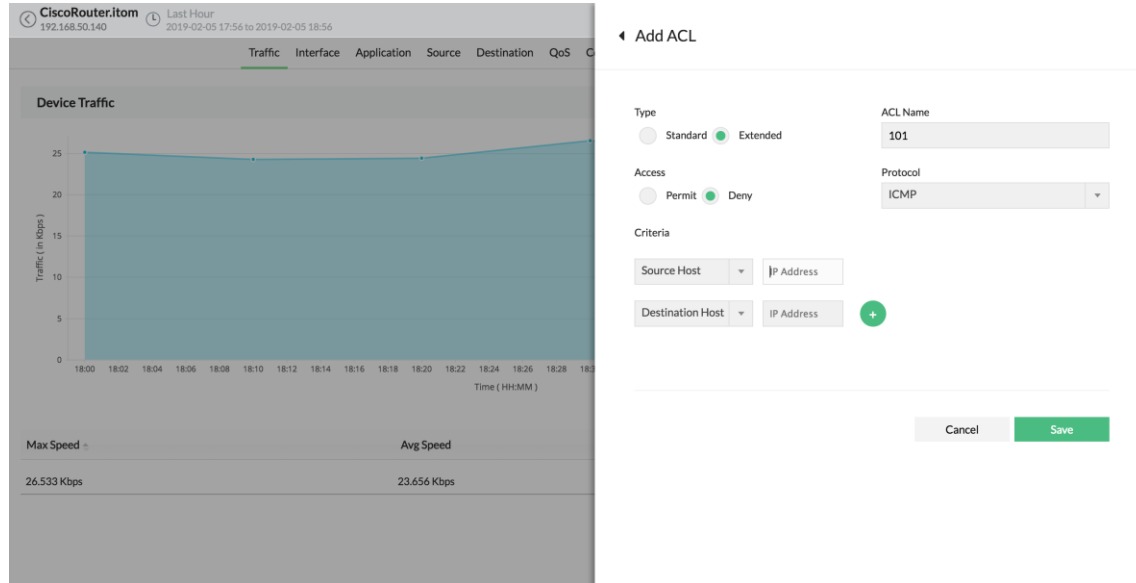






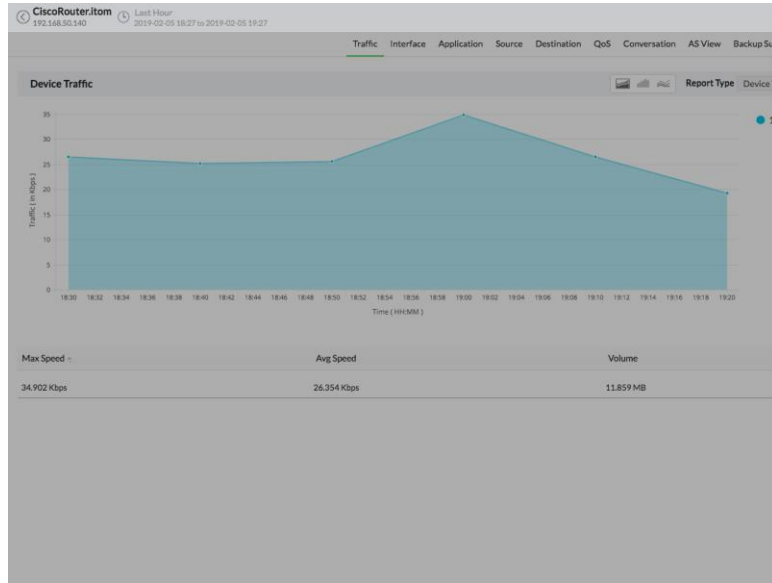
# Modélisation du trafic

# Liste de contrôle d'accès (ACL)



Filtrez le trafic excessif du routeur en bloquant ou en restreignant les IP/réseaux IP.

# Politique de service



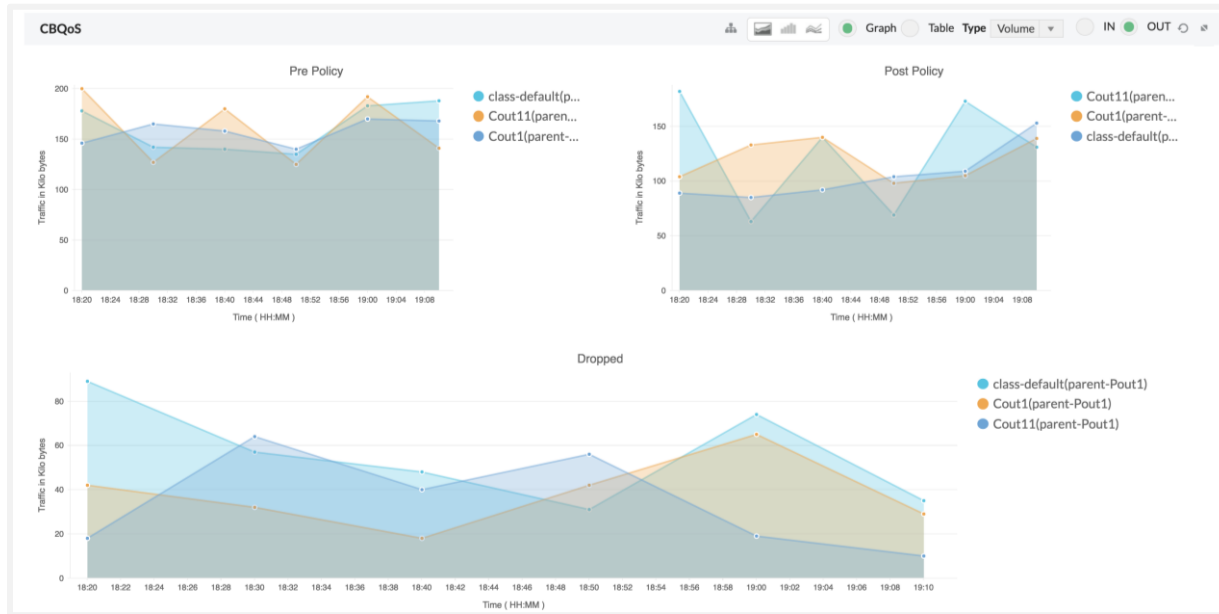
Service Policy

[Add Policy](#) [Add Class](#)

Policy Name	Policy Details	Delete	Apply
policy-d	Class dscp-class service-policy dscpPolicy	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Webex_priority	Class trafficshaping bandwidth 30 (S)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
dscpPolicy	Class priority priority 250 (kbps)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Gérez vos politiques de service et limitez l'accès aux applications en fonction des priorités.

# Valider les politiques de QoS avec CBQoS



Surveillez les performances de la pré-politique et de la post-politique avec la CBQoS pour différentes périodes de temps et comparez leur efficacité.



# Intégrations

# Intégration d'Applications Manager

Cartographier et superviser les serveurs d'applications d'entreprise et contribuer à garantir que les applications critiques pour l'entreprise répondent aux exigences des utilisateurs finaux.

## 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.

# Intégration d'OpUtils

The screenshot displays a network management interface with a sidebar on the left and a main content area on the right. The sidebar, titled 'Tree View', shows a hierarchy starting with 'Your Company' and 'Default Group', followed by 'DHCP Servers', 'Discovered Subnets', and 'Discovered v6 Hosts'. Under 'Discovered Subnets', there is a list of subnets from 'OpUtils201' to 'OpUtils2011'. The main content area is titled 'Your Company > OpUtils202 > 172.20.2.0/24' and includes 'Add' and 'Settings' buttons. Below the breadcrumb is a navigation bar with 'Subnet Summary', 'IP Details', 'History', and 'Alerts'. The 'Subnet Summary' tab is active, showing a table of subnet details and two donut charts. The table lists: Subnet Address (172.20.2.0), Subnet Name (with a copy icon), 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, and Scan Status (Scanned). The 'IP Availability' chart is a donut chart that is almost entirely orange, with '254' in the center. The 'DNS Status' chart is a donut chart that is almost entirely red, with '254' in the center. A legend below the charts indicates: Used (red), Available (green), Transient (orange), and Not Scanned (blue) for IP Availability; and Success (green), Rev. Lookup Failed (blue), Fwd. Lookup Failed (yellow), and Fwd. Lookup IP Mismatch (red) for DNS Status.

Property	Value
Subnet Address	172.20.2.0
Subnet Name	[Copy Icon]
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

Mieux gérer les adresses IP et les ports de commutation.

# Intégration de ServiceDesk Plus

The screenshot shows a web-based configuration interface for ServiceDesk Plus. The top navigation bar includes 'General Settings', 'Discovery', 'Monitoring', 'Tools', 'NetFlow', 'NCM', and 'OpUtils'. The left sidebar lists various settings categories, with 'General Settings' selected. The main content area is titled 'ServiceDesk Plus - Configuration' and includes a 'Download' button. The configuration is divided into several sections: 'Integrate NetFlow Analyzer with ServiceDesk Plus' with a descriptive paragraph; 'Product Type' with radio buttons for 'ServiceDesk Plus' (selected) and 'ServiceDesk Plus-MSP'; 'Server IP/DNS Name' with a dropdown menu set to 'http' and a text input field; 'Technician Key' with a text input field and a help icon; 'Ticket Settings' with radio buttons for 'Create new ticket' (selected) and 'Re-open closed ticket'; and a checkbox for the license agreement. At the bottom, there are 'Back', 'Reset', and 'Save' buttons.

General Settings | Discovery | Monitoring | Tools | NetFlow | NCM | OpUtils

## 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
- SSH Settings

### 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**

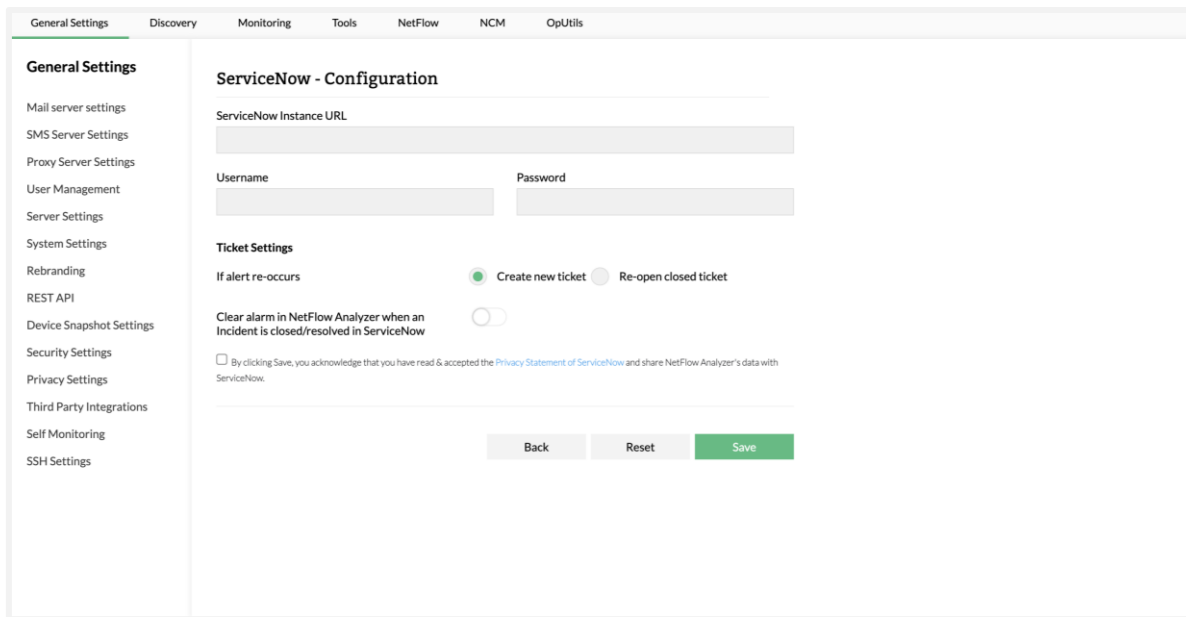
If alert re-occurs  Create new ticket  Re-open closed ticket

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

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

Automatisez la création de tickets d'alarme, la synchronisation des actifs et la planification de la maintenance.

# Intégration de Service Now



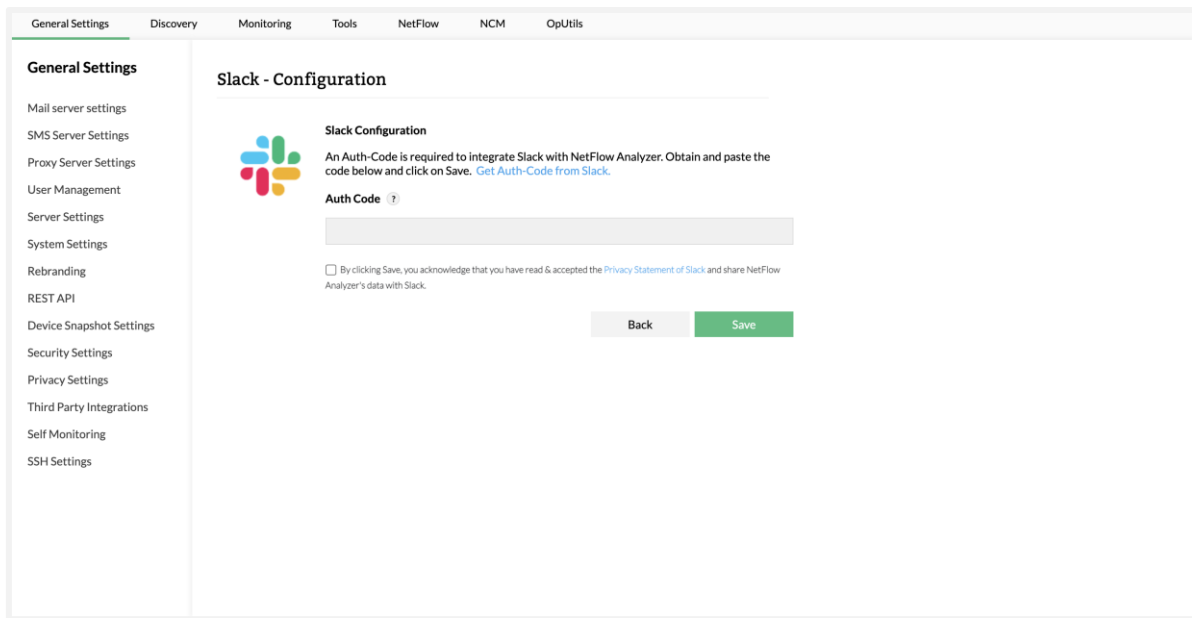
The screenshot shows a web interface for configuring ServiceNow integration. The top navigation bar includes 'General Settings' (highlighted), 'Discovery', 'Monitoring', 'Tools', 'NetFlow', 'NCM', and 'OpUtils'. The left sidebar lists various settings categories: 'General Settings', 'Mail server settings', '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:** Two radio buttons: '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'.

Assurez une gestion des alertes sans effort et en temps réel grâce à l'enregistrement automatique des incidents et à la synchronisation bidirectionnelle des données qu'offre cette intégration.

# Intégration de Slack



The screenshot shows a web interface for configuring Slack integration. At the top, there is a navigation bar with tabs: General Settings (selected), Discovery, Monitoring, Tools, NetFlow, NCM, and OpUtils. On the left side, there is a sidebar menu under 'General Settings' with various options: 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, a section header 'Slack Configuration', and a paragraph explaining that an Auth-Code is required for integration with NetFlow Analyzer. Below this is a text input field for the 'Auth Code'. A checkbox is present 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.' At the bottom right of the configuration area, there are two buttons: 'Back' and 'Save'.

Personnalisez les tâches de traitement des alertes tout en réduisant les temps d'arrêt grâce aux alertes Slack qui peuvent être configurées dans un profil de notification ou comme étape d'un flux de travail.



**Autres points forts**

# Exportation de flux en un clic

Ajouter des informations d'identification



Exécuter les commandes



Exportation de flux



i. Prédéfini  
ii. Personnalisé  
iii. Générateur de NetFlow

**Discovery**

Export Flow

NCM Discovery

Discovery Report

Credentials

Inventory Updater

Non Inventoried Devices

**Predefined Flow Export** Custom Flow Export NetFlow Generator

Flow export's status:

Commands are executed. Flows are received.

Execution Output:

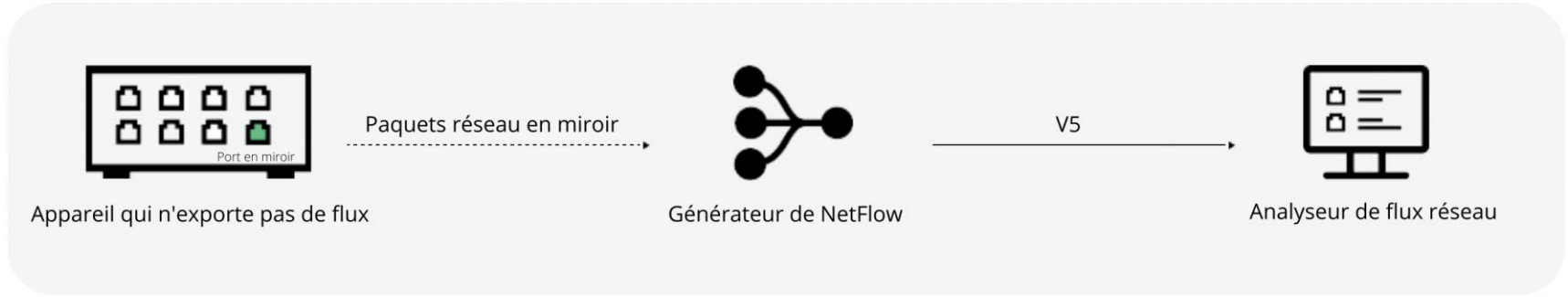
```
Config1
Enter configuration commands, one per line. End with CNTL/Z.
CiscoRouter(config)#
CiscoRouter(config)#
NExceeded maximum export destinations
CiscoRouter(config)#
ip flow-export source GigabitEthernet0/2
ip flow-export source GigabitEthernet0/2
CiscoRouter(config)#
ip flow-export version 5
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 findas permit
snmp-server findas permit
CiscoRouter(config)#
interface backplane GigabitEthernet0/3
interface backplane GigabitEthernet0/3
^
```

**Note:** In case of any errors in the output of command execution, contact netflowanalyzer-support@manageengine.com

Back Close

Exportez des flux en utilisant des modèles prédéfinis ou une configuration personnalisée directement depuis l'interface utilisateur.

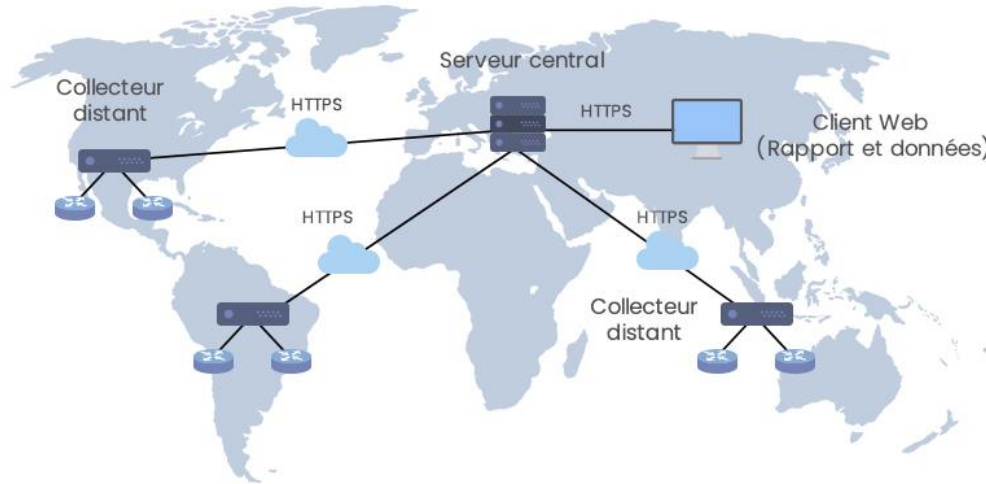
# Générateur de NetFlow



Avec NetFlow Generator, capturez et convertissez les paquets réseau en paquets NetFlow pour surveiller les périphériques qui ne prennent pas en charge le flux.

# Édition Entreprise pour la supervision distribuée

Bureaux internationaux. Supervision locale.



Grande évolutivité et console centralisée pour la surveillance

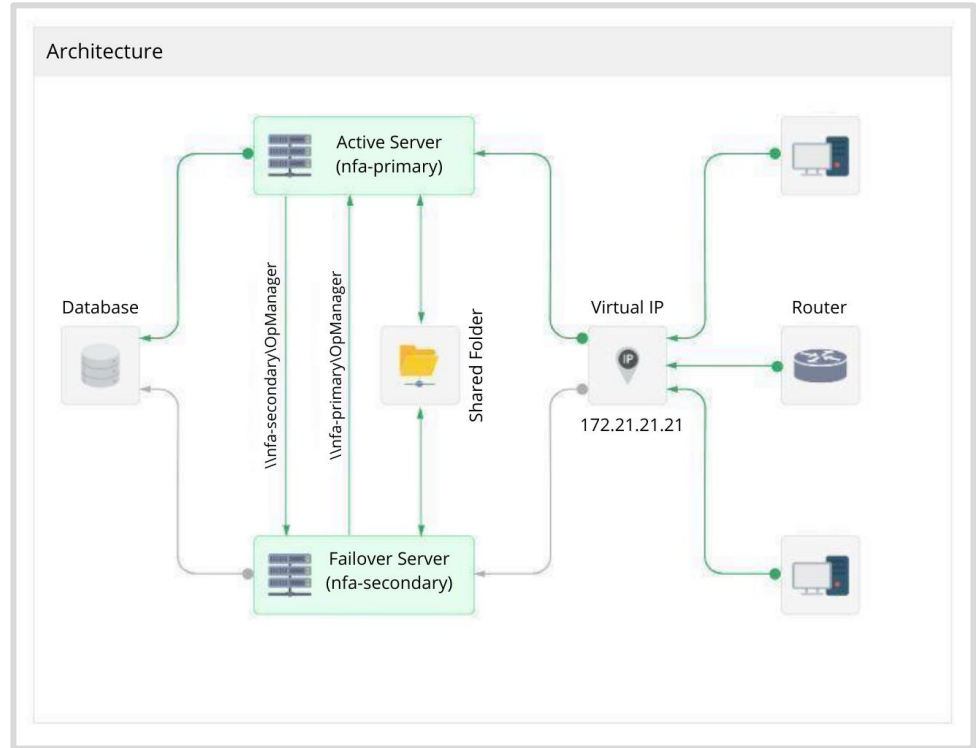
# Supervision distribuée

The screenshot shows a web-based configuration interface. On the left is a vertical navigation menu under the heading 'Configuration'. The menu items are: 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, and Distributed Monitoring (which is highlighted). The main content area is titled 'Distributed Monitoring'. It features a toggle switch for 'Enable Distributed Mode' which is currently turned off. Below this are two input fields: 'https port for Central Server' with the value '443' and 'Internal Collector name' with the value 'Collector1'. A red asterisk warning states '\* Requires Server Restart'. A small note below reads: '\* Note: On clicking the enable button, the product converts from Essential Edition to Distributed Edition and the process becomes Irreversible.' At the bottom of the main area is a large green button labeled 'Enable'.

Passez à l'édition Enterprise en un seul clic.

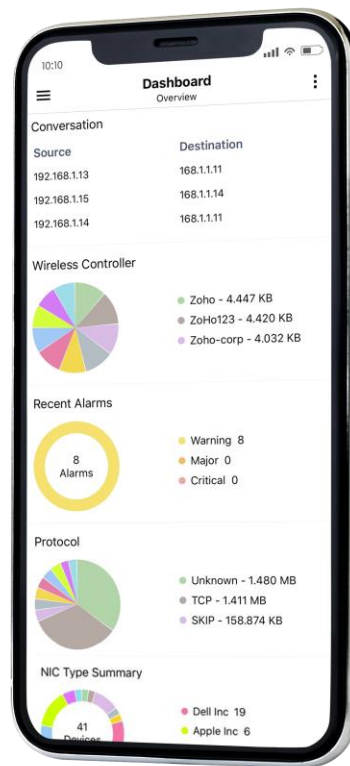
# Basculement

Assurez-vous que votre réseau est toujours surveillé grâce à la fonction de basculement de NetFlow Analyzer. Le basculement prend en charge un serveur secondaire de secours pour une haute disponibilité.



# Application Mobile

Surveillez vos périphériques réseau en déplacement avec les applications NetFlow Analyzer iOS et Android.



# Vous avez besoin d'aide?



[helpdesk@pgsoftware.support](mailto:helpdesk@pgsoftware.support)

Merci

<https://www.pgsoftware.fr/itom/netflow-analyzer>