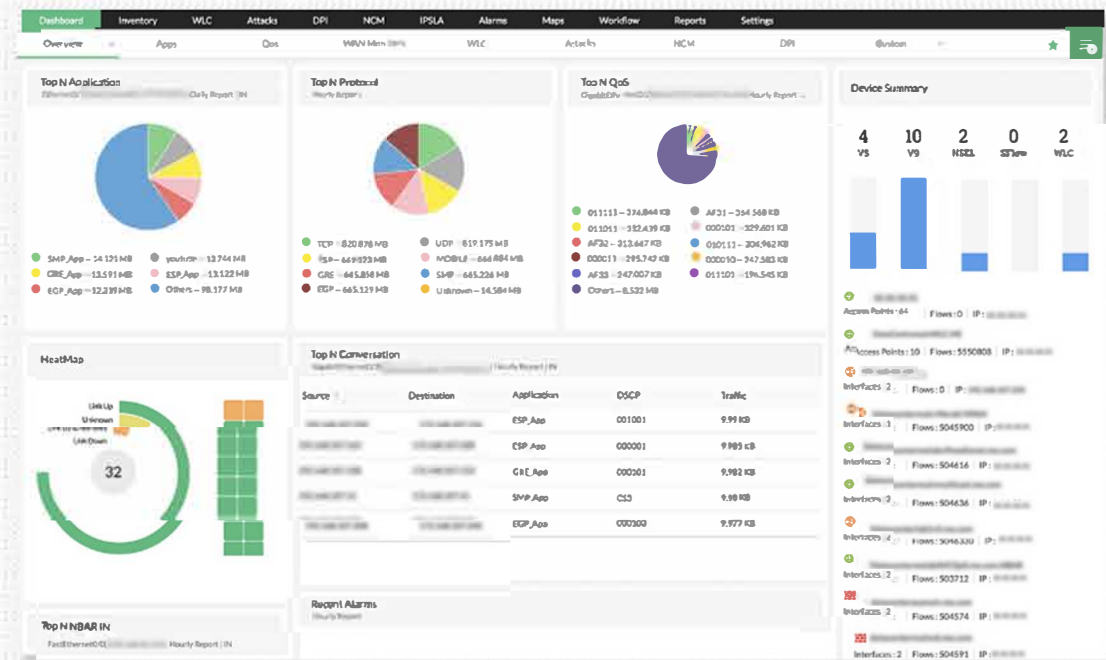


ManageEngine NetFlow Analyzer

Una solución completa de monitoreo del ancho de banda y análisis del tráfico de red para administradores de red.





El qué y por qué del monitoreo del ancho de banda

Monitoreo del ancho de banda: Qué y por qué

- Conocer el rendimiento de su red.
- Evaluar el uso del ancho de banda de cada elemento.
- Identificar los acaparadores de ancho de banda y tensiones en la red.
- Predecir la capacidad del ancho de banda para el futuro.

“

Si no puede medirlo, no podrá gestionarlo

- Peter Drucker

”



Por qué elegir NetFlow Analyzer



Análisis de tráfico basado en flujo.



Compatible con el monitoreo del tráfico de redes distribuidas.



Adaptable a su red y personalizable.



Add-ons y soporte multi-proveedor.



Interfaz de usuario simple y fácil de usar.

Velocidad y uso del ancho de banda

Medianet y multicast

Agrupación de tráfico

Monitoreo de SLA IP

Monitoreo de Cisco AVC

Monitoreo de NBAR

Monitoreo del tráfico de WLC

Seguridad



**iComience a
monitorear
NetFlow!**

Exportación de flujo

Agregue las credenciales



Ejecute los comandos



Exporte el flujo



- i. Predefinido
- ii. Personalizado
- iii. Sensor de paquetes de red

NetFlow Analyzer

Dashboard

Inventory

WLC

Security

DPI

NCM

IPAM

IPSLA

Alarms

Maps

Reports

Settings

General Settings

Discovery

Monitoring

Tools

NetFlow

NCM

OpUtils

ITOM Agent

Discovery

Export Flow

Export Cloud Flow

NCM Discovery

Discovery Report

Credentials

Inventory Updater

Non Inventoried Devices

Predefined Flow Export

Custom Flow Export

Network Packet Sensor

Export flow using the predefined template in NetFlow Analyzer.

Host name/ IP Address *

Select SNMP credential *

nfaread (SNMP v1/v2)

+

Protocol ?

Telnet

SSH

Login Name *

Password *

Prompt *

>,\$,#

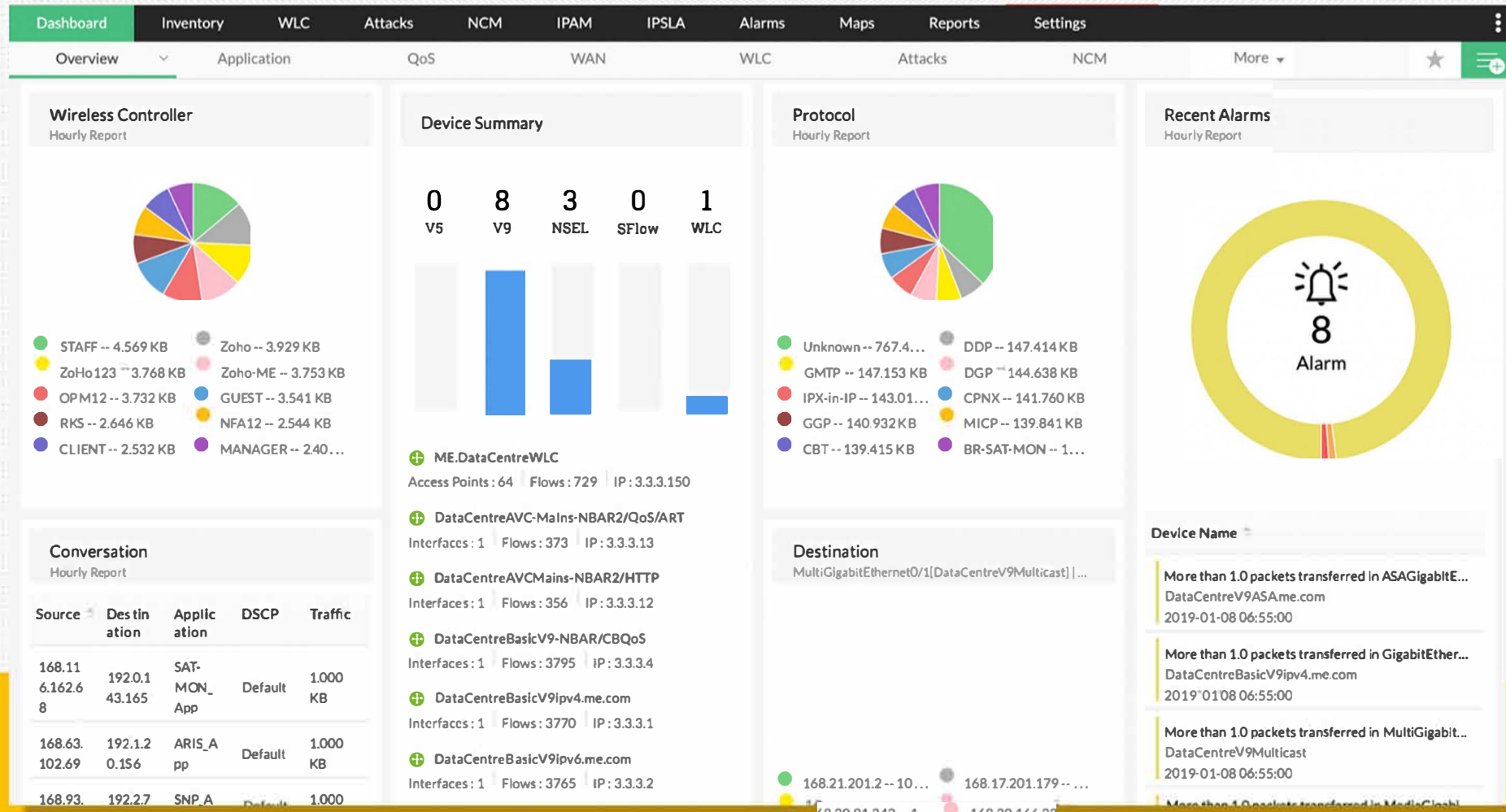
Enable Command

Enable UserName

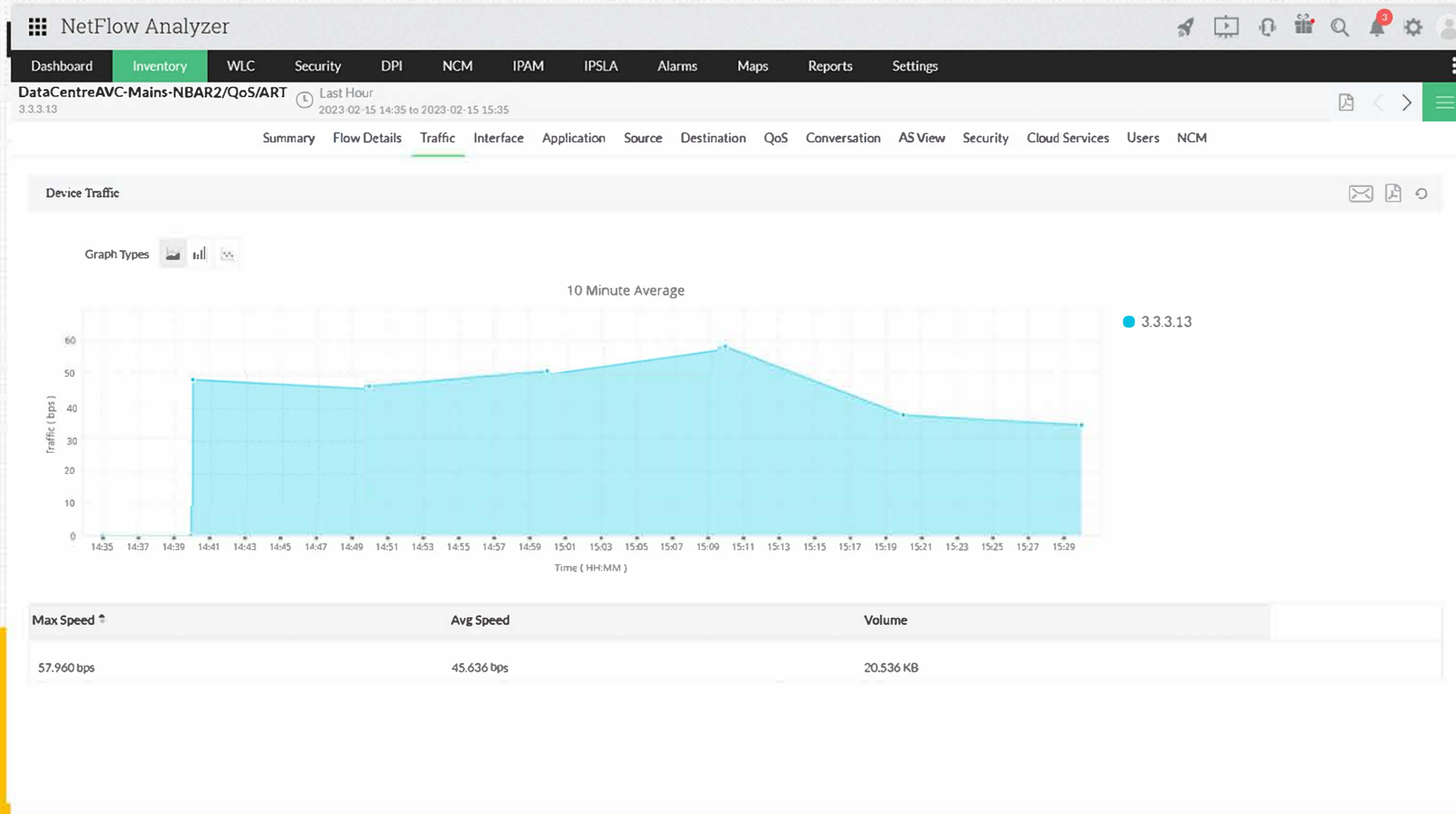
Enable Password

Enable Prompt

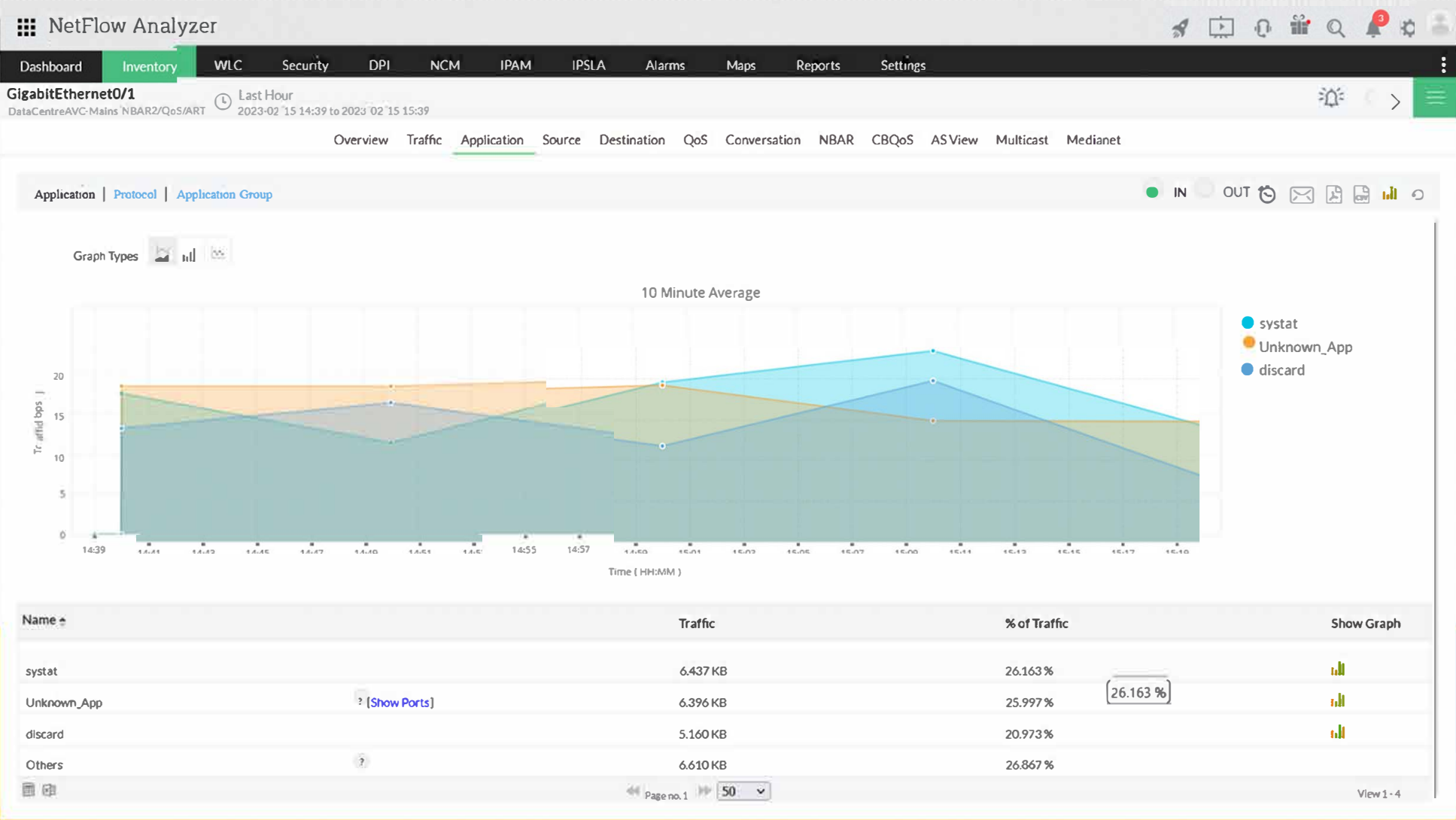
Vista de NOC y dashboard



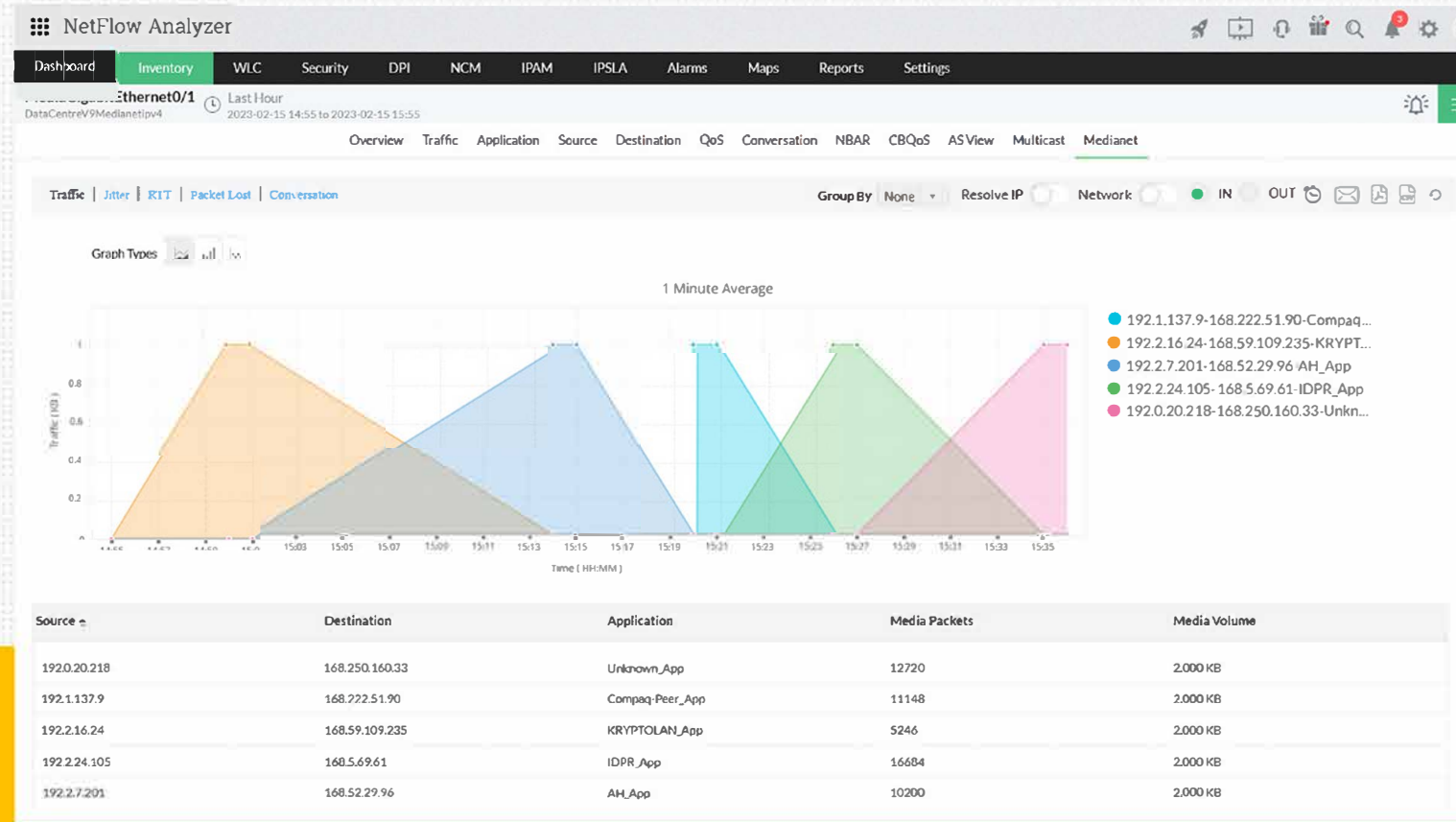
Tráfico de dispositivos e interfaces



Tráfico de aplicaciones

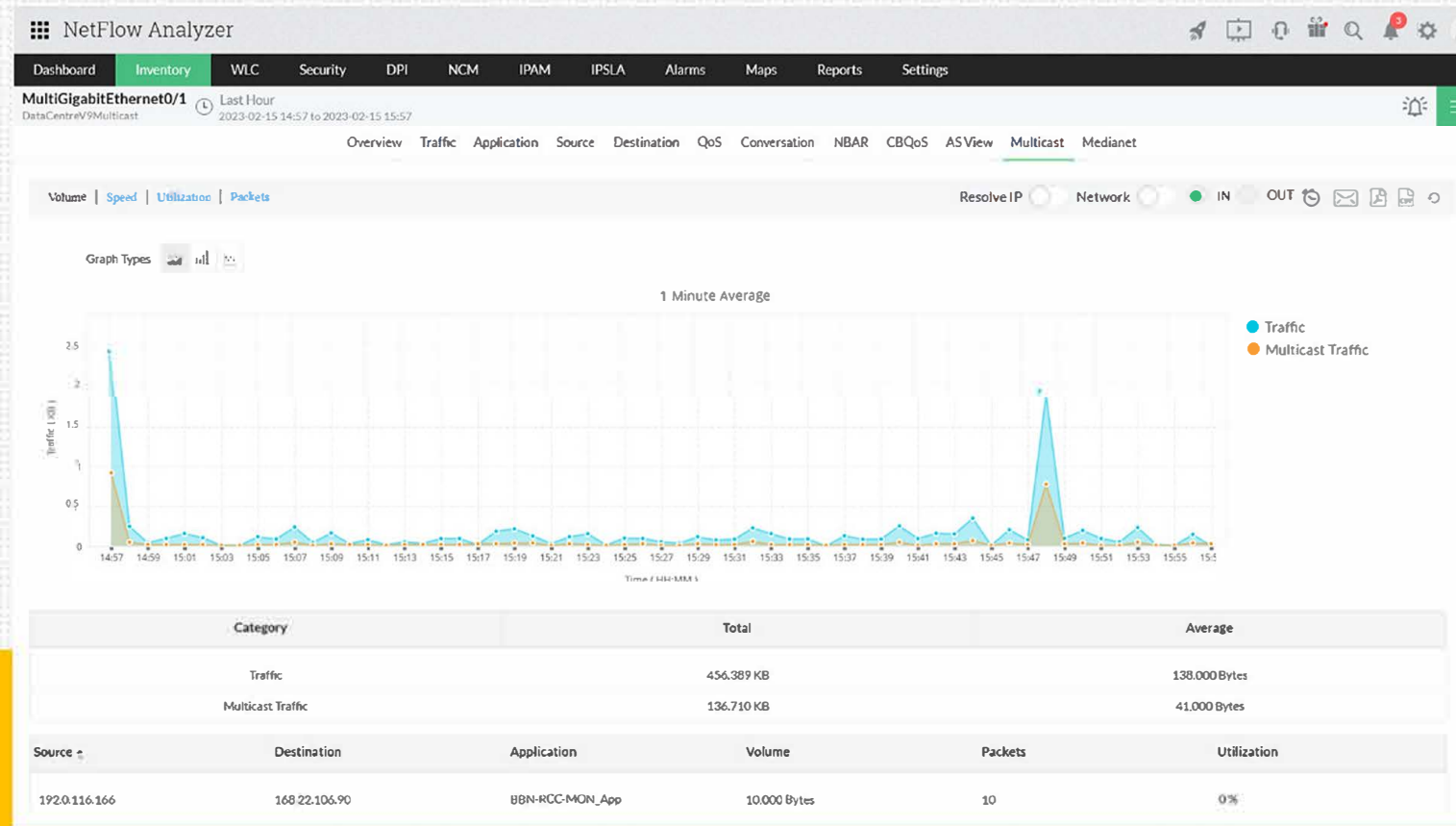


Monitoreo del tráfico de medianet



- Monitoree tráfico multimedia como el tráfico de voz y video para mejorar la QoE.
- Mida las estadísticas de rendimiento como fluctuación, pérdida de paquetes y RTT.

Monitoreo del tráfico de multicast



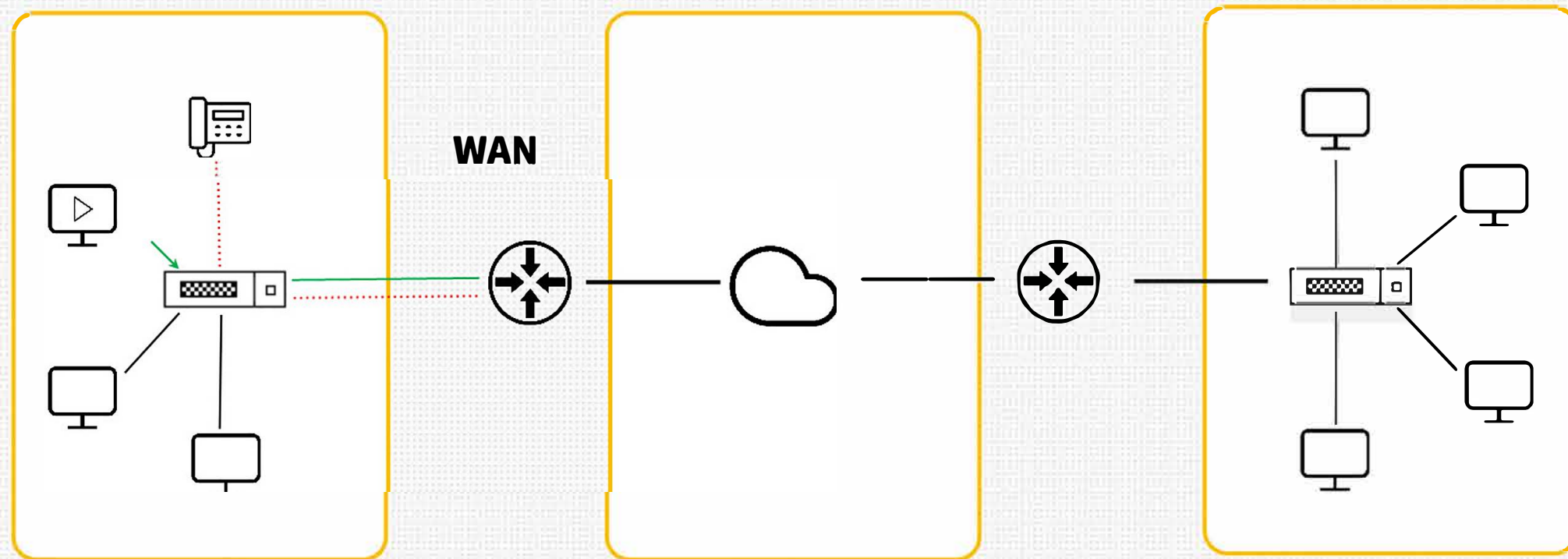
- La multidifusión IP permite a un host enviar paquetes a un grupo específico de hosts.
- Monitoree el uso y velocidad del tráfico de multicast.

Monitoreo de IPSLA

Centro de desarrollo

Proveedor de servicios

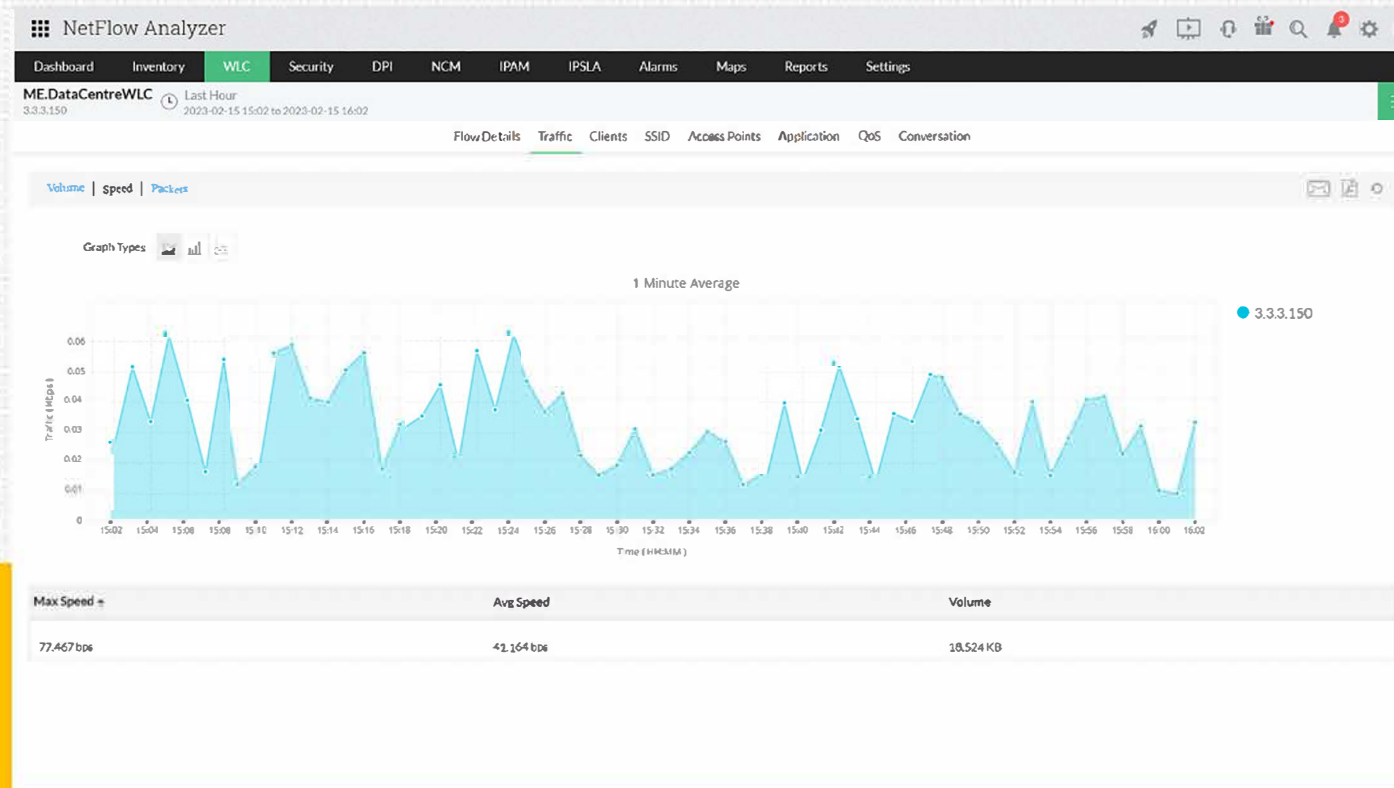
Sede principal



Visibilidad y control de la aplicación

- Obtenga visibilidad de las aplicaciones NBAR2 con Cisco AVC (visibilidad y control de la aplicación).
- El NBAR avanzado se usa para identificar tráfico web. URL, archivos compartidos y aplicaciones con puerto aleatorio.
- Vea informes de monitoreo de aplicaciones NBAR2, recuento de aciertos de URL (informe de host HTTP), jerarquía de clase QoS y tiempo de respuesta de la aplicación (monitoreo de ART).
- Cómo habilitar: Se deben configurar campos adicionales durante la exportación de flujo.

Monitoreo del tráfico inalámbrico

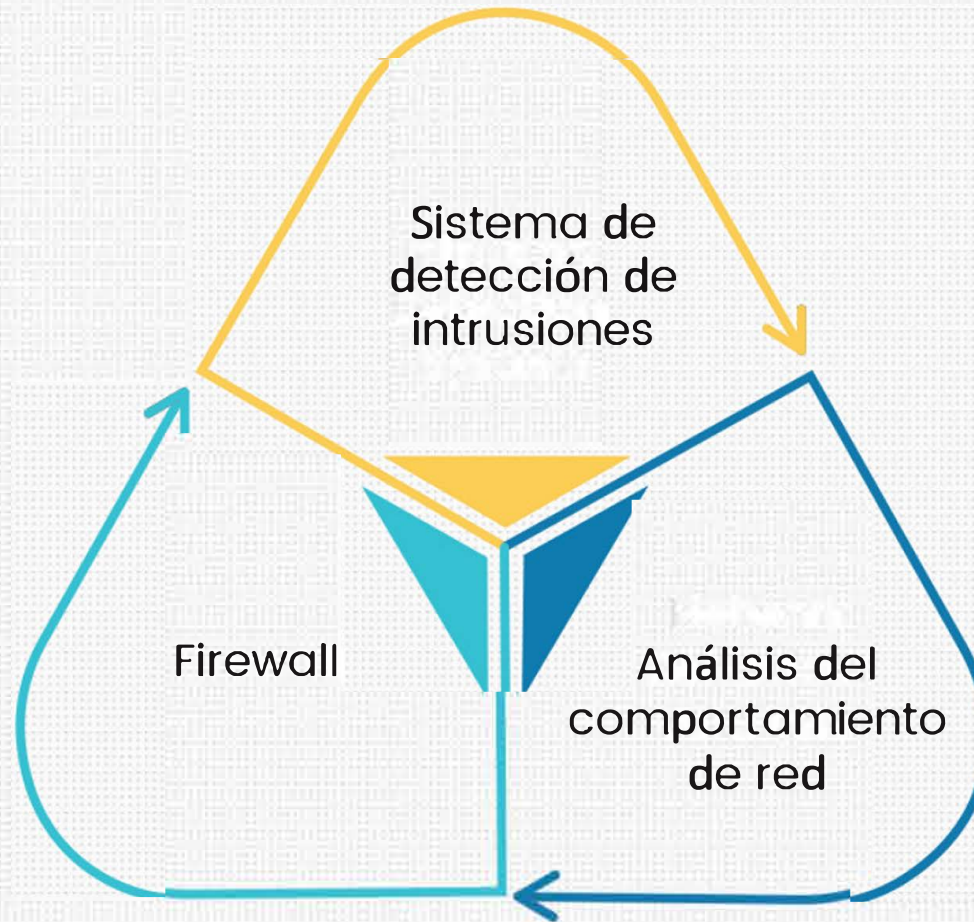


- Monitoree controladores de Cisco WLAN.
- Encuentre quién usa más tráfico por puntos de acceso, SSID, aplicaciones, clientes, etc.
- Agrupe WLAN por SSID.
- Solucione los picos en el ancho de banda identificando el consumo por SSID y encontrando los principales clientes y detalles completos de la conversación para el periodo de tiempo seleccionado.



Seguridad, más allá del NTA básico

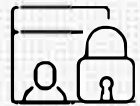
Análisis de comportamiento



¿Cómo ayuda NetFlow Analyzer?

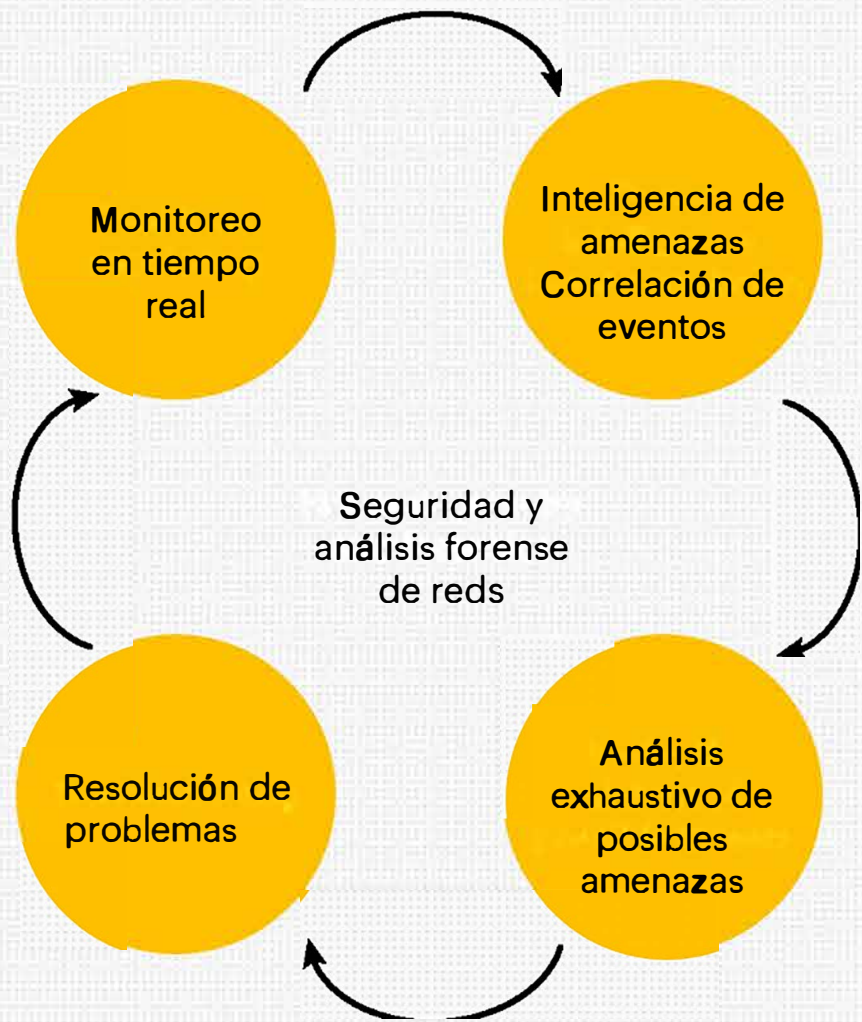


Análisis forense de red



Módulo de seguridad

Análisis forense de red



Mejor visibilidad



Fácil identificación de problemas en la infraestructura de la red, rendimiento general y uso del ancho de banda.



Mejor respuesta para la resolución de problemas.

Análisis forense de red

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.

Generate Report



Obtenga estadísticas de tráfico más detalladas usando datos sin procesar.



Profundice para identificar qué usuarios, aplicaciones y protocolos están consumiendo más ancho de banda en un momento determinado.



Solucione problemas de forma precisa definiendo varios criterios para filtrar el tráfico requerido.

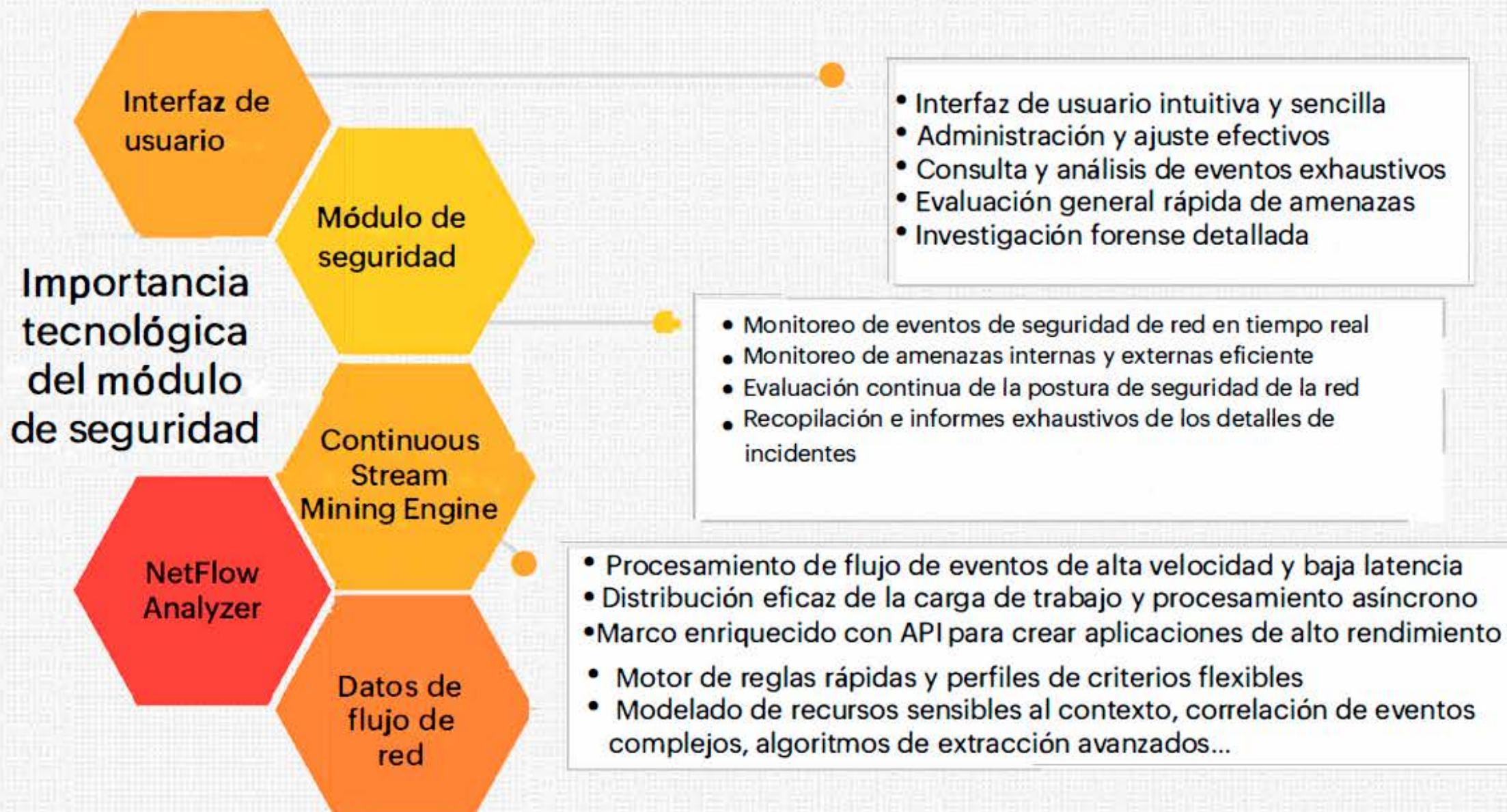
Análisis de seguridad

DDOS

Escaneos/ sondeos

Botnets

¿Qué es el módulo de seguridad?



Detecte los ataques con el módulo de análisis de seguridad basado en el flujo

» Identifique el tráfico basura/malicioso mediante un algoritmo de minería avanzado.

» El módulo de seguridad clasifica el tráfico como flujos sospechosos, origen y destino malicioso, DDoS y escaneos/sondeos.

	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



Informes

Informes

Informe de búsqueda

Busque detalles de tráfico específicos por la aplicación asociada, el protocolo, el host o la IP.

Informe de comparación

Compare el uso de ancho de banda en diferentes intervalos de tiempo.

Informe consolidado

Supervise los principales conversadores y conversaciones con un informe completo.

Informe de inventario

Visualize the combined traffic usage of all interfaces.

Informes

Informe de percentil

Genere informes de tráfico en los valores del percentil 90 y 95 para interfaces, grupos de IP

Informe de geolocalización

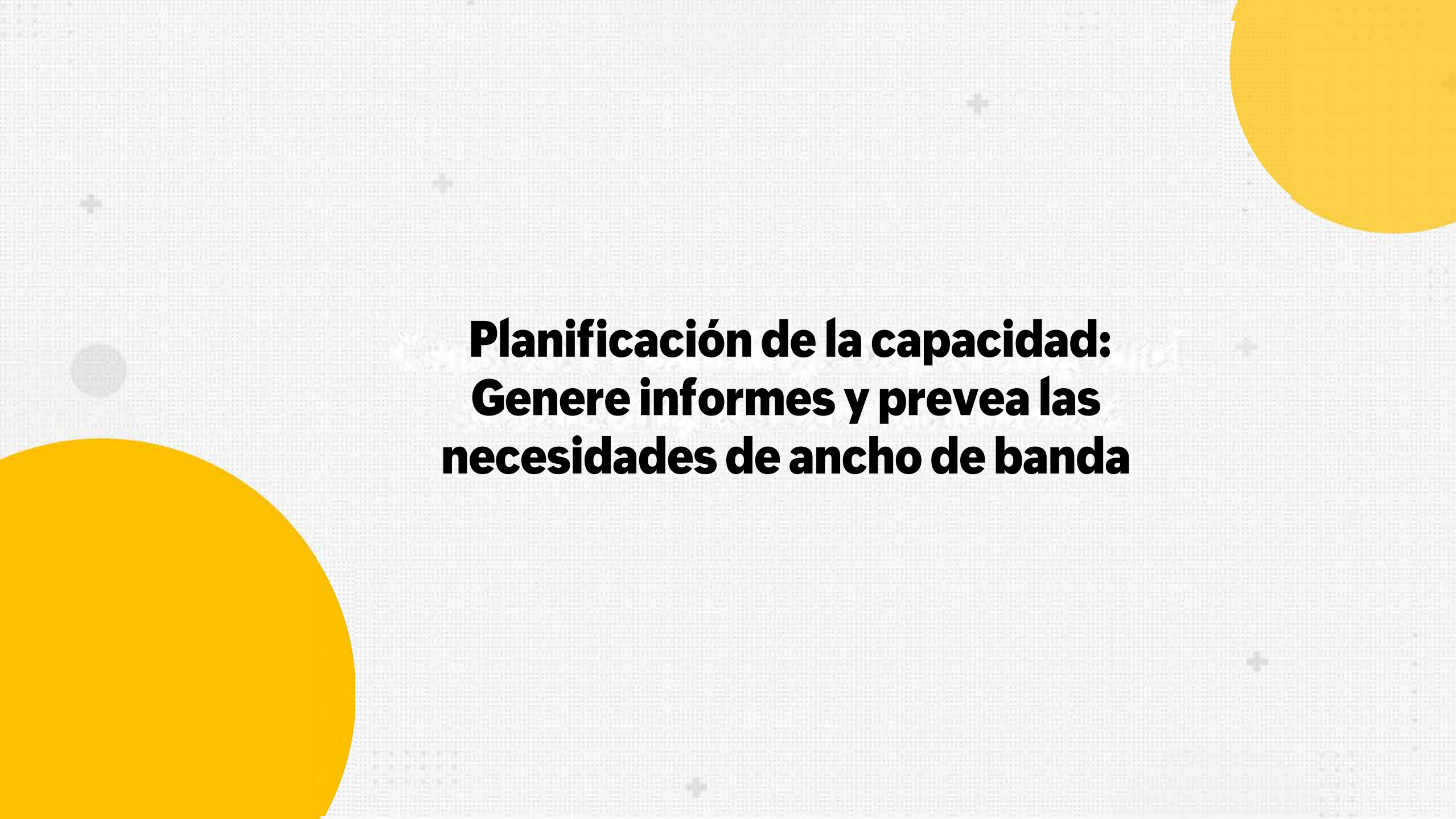
Identifique la información basada en la región del tráfico de origen y destino

Informe programado

Obtenga informes de uso del ancho de banda automáticamente cada día, semana o mes

Informe de LAN-WAN

Supervise el tráfico entre sus IP de LAN, y LAN y WAN



**Planificación de la capacidad:
Genere informes y prevea las
necesidades de ancho de banda**

Informes de planificación de la capacidad y previsión del rendimiento



Planificación de la capacidad

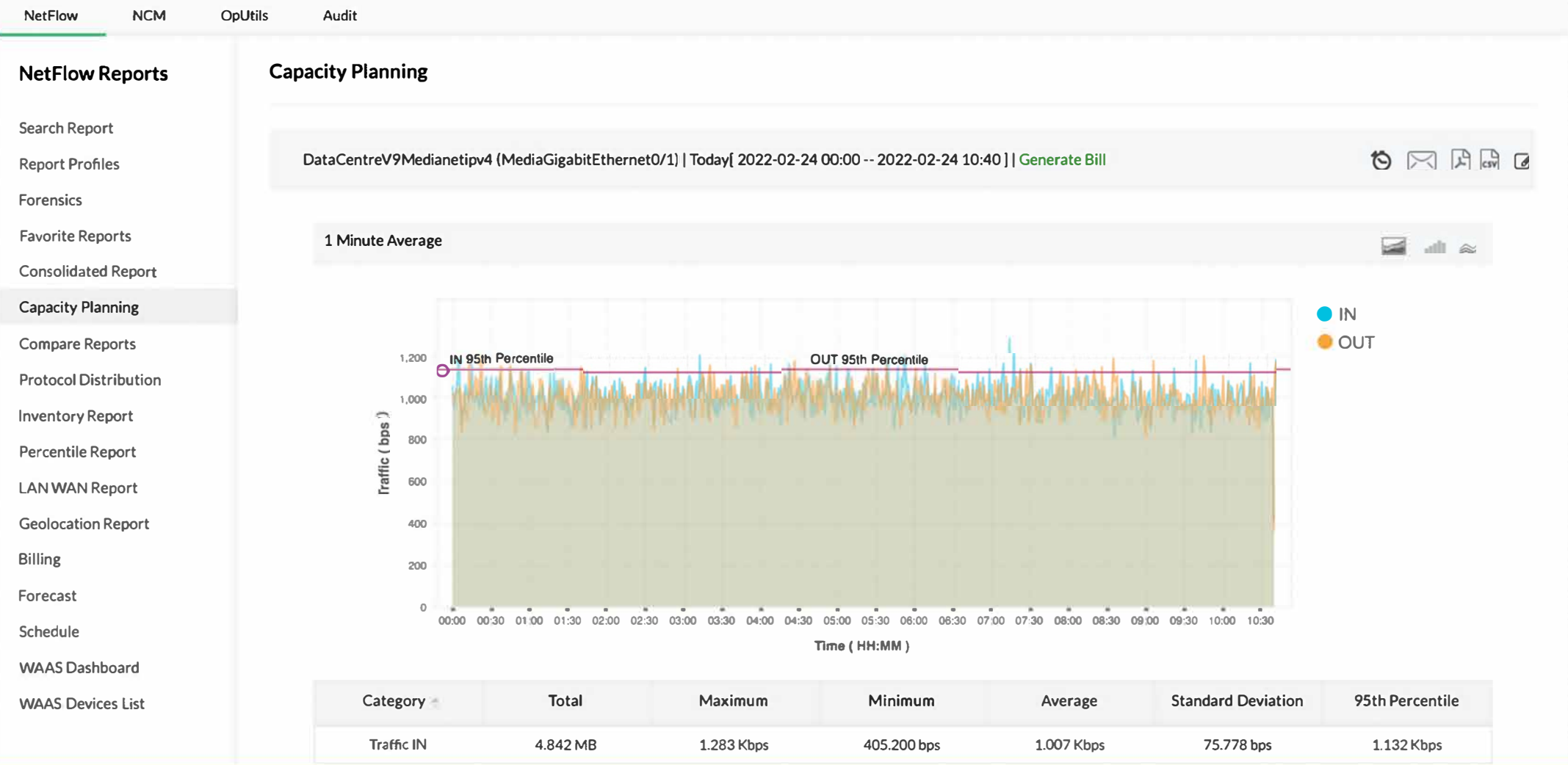
Tendencias de uso de dispositivos y aplicaciones y tendencias de crecimiento para planificar medidas proactivas.



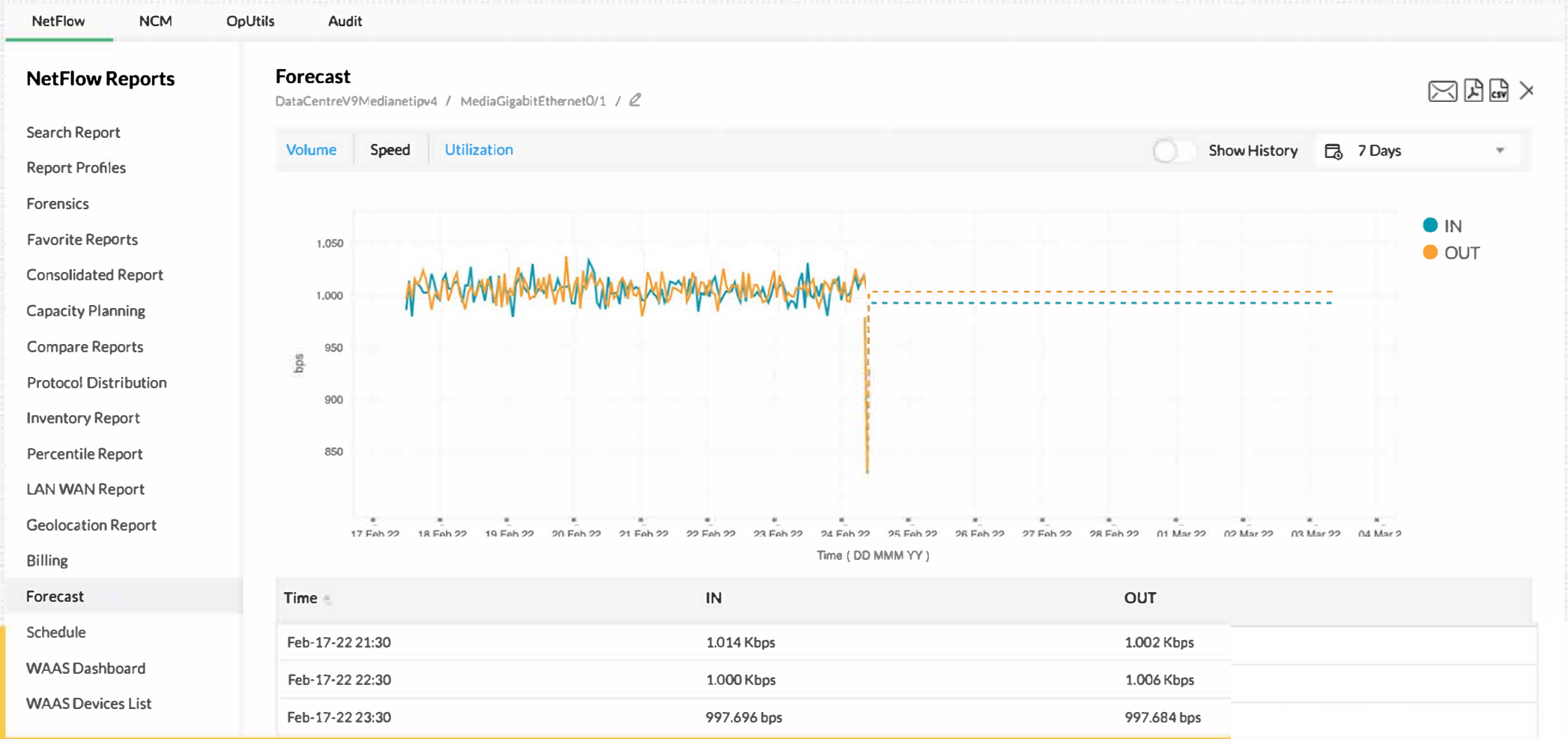
Informes de previsión

Análisis predictivo basado en el crecimiento histórico y las tendencias de uso.

Informes de tendencia de la capacidad



Informe de previsión

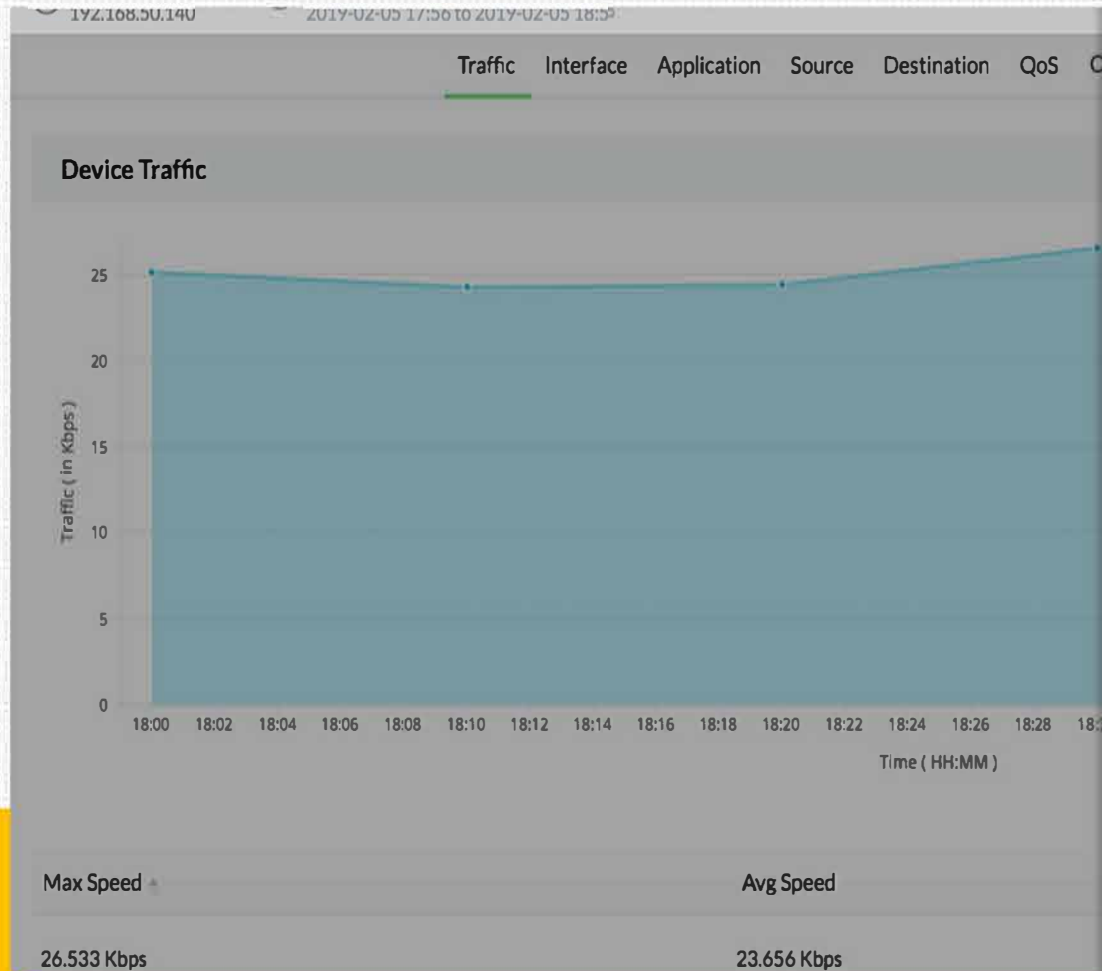


+



**■ Priorice el modelado de
tráfico y datos:
Optimización más simple**

Filtre el exceso de tráfico del router bloqueando o restringiendo IP/redes IP con ACL



Add ACL

Type

☐ Standard ☒ Extended

ACL Name

101

Access

☐ Permit ☒ Deny

Protocol

ICMP

Criteria

Source Host



IP Address

Destination Host



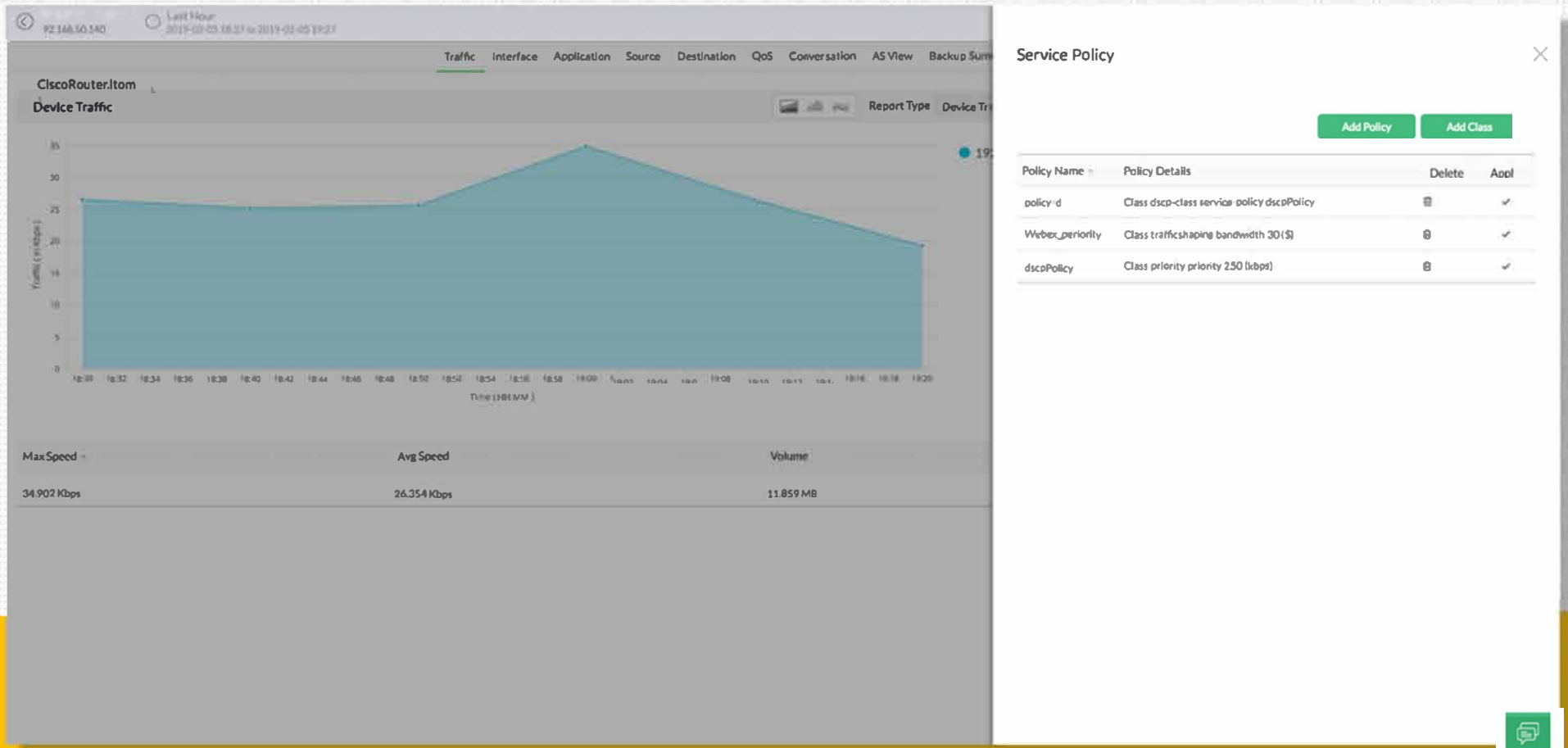
IP Address



Cancel

Save

Gestione sus políticas de servicio y limite el acceso a las aplicaciones en función de la prioridad con políticas de servicio



Valide las políticas de QoS con CBQoS





**Monitoreo del
tráfico acumulado:
Mejore la gestión
del ancho de banda**

Categorice el uso del tráfico

Departamento

Sucursales

Subred de la red

Aplicaciones relacionadas

VLAN

Ordene el uso del tráfico por grupos

Interfaz

Monitoree el uso de ancho de banda combinado para obtener una mejor imagen del consumo de tráfico.

IP

Aplicación

Proporcione acceso a los operadores según los grupos.

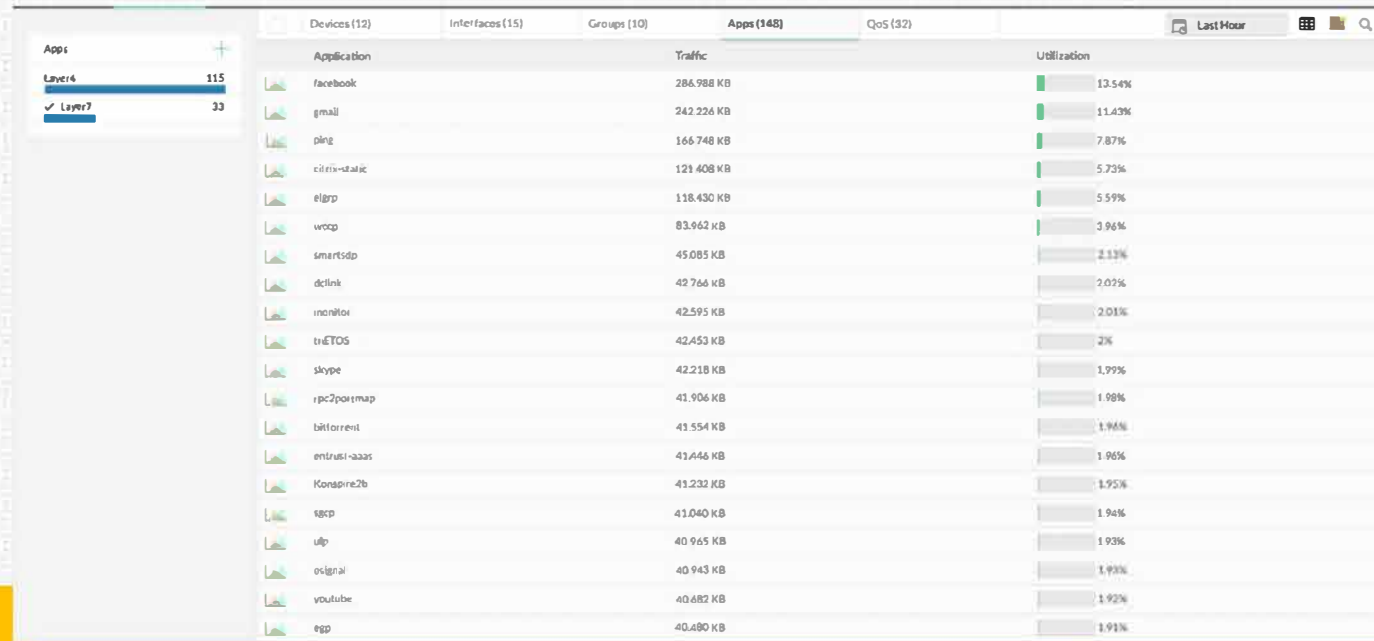
DSCP

SSID

Brinde una mejor visibilidad para mejorar la resolución de problemas.

SSID

Monitoree aplicaciones personalizadas



» Asignación de aplicaciones para _App

Interfaz > Aplicación > _App > Mostrar puerto (para usar la función "Mostrar puerto" se deben habilitar los datos sin procesar).

Asignar aplicación y definir dirección IP/ red IP/ rango IP.

» Asignación de aplicaciones para aplicaciones personalizadas

Ajustes > NetFlow > Asignación > Lista de aplicaciones > Añadir

Nombre de usuario - Asignación de IP

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:

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

➤➤ Asignación de AD

}> Manual

}> Asignación

}> DHCP

Servicios en la nube

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

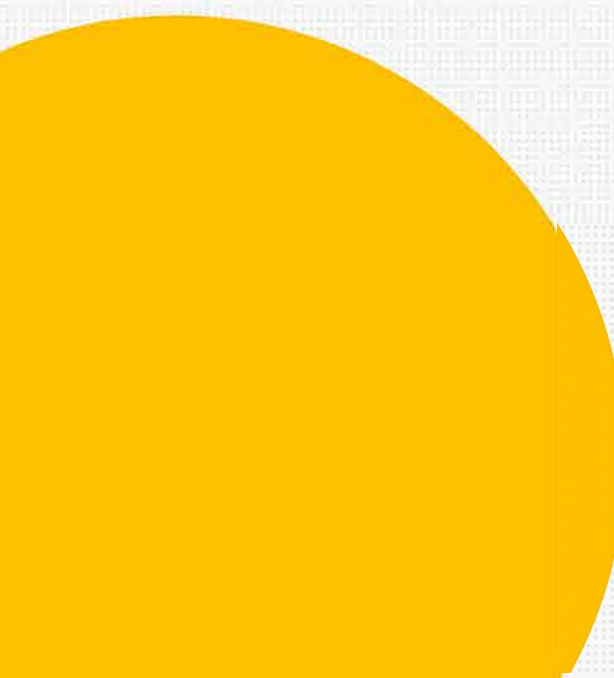
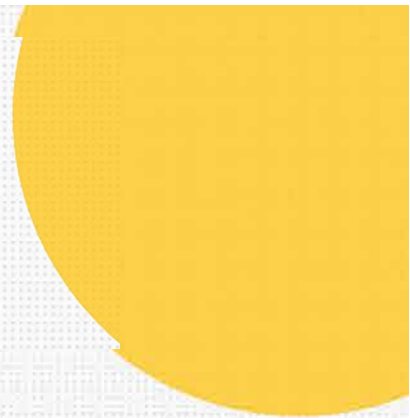
DSCP

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
MediaFire	File Sharing	104.16.x0x0x	104.16.203.x0x	2019-12-18	 
SugarSync	File Sharing	208.94.x0x0x	208.94.4.x0x	2018-12-17	 
Office 365	File Sharing	40.84.x0x0x	40.84.199.x0x	2015-03-12	 
4shared	File Sharing	204.155.x0x0x	204.155.149.x0x	2018-05-29	 
Sendspace	File Sharing	69.31.x0x0x	69.31.136.x0x	2015-03-12	 
Hightail	File Sharing	35.165.x0x0x	35.165.148.x0x	2019-09-27	 
Carbonite	Online Storage	45.60.x0x0x	45.60.171.x0x	2019-09-27	 
CrashPlan	Online Storage	216.17.x0x0x	216.17.8.x0x	2015-03-12	 
Mozy	Online Storage	52.170.x0x0x	52.170.7.x0x	2019-07-10	 
Flickr	Arts and Entertainment	13.35.x0x0x	13.35.209.x0x	2019-12-18	 
Photobucket	Photo Sharing	209.17.x0x0x	209.17.68.x0x	2015-03-12	 
Shutterfly	Photo Sharing	136.179.x0x0x	136.179.236.x0x	2015-03-12	 
Pinterest	Photo Sharing	72.52.x0x0x	72.52.10.x0x	2015-03-12	 



Gestión proactiva

Configure alertas

Alertas en tiempo real

Alertas agregadas

- Alertas preconfiguradas (enlace inactivo / sin flujo)
 - Alertas basadas en umbrales
-
- Reciba notificaciones por correo electrónico, SMS, tickets, SMS basado en correo electrónico, chat, ejecución de programa, perfil de syslog, perfil de trap, alarma web

Cree y gestione plantillas de notificación para recibir alertas por correo electrónico / SMS, alarmas web, registrar tickets o traps SNMP / 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.

Integraciones de terceros

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](#)



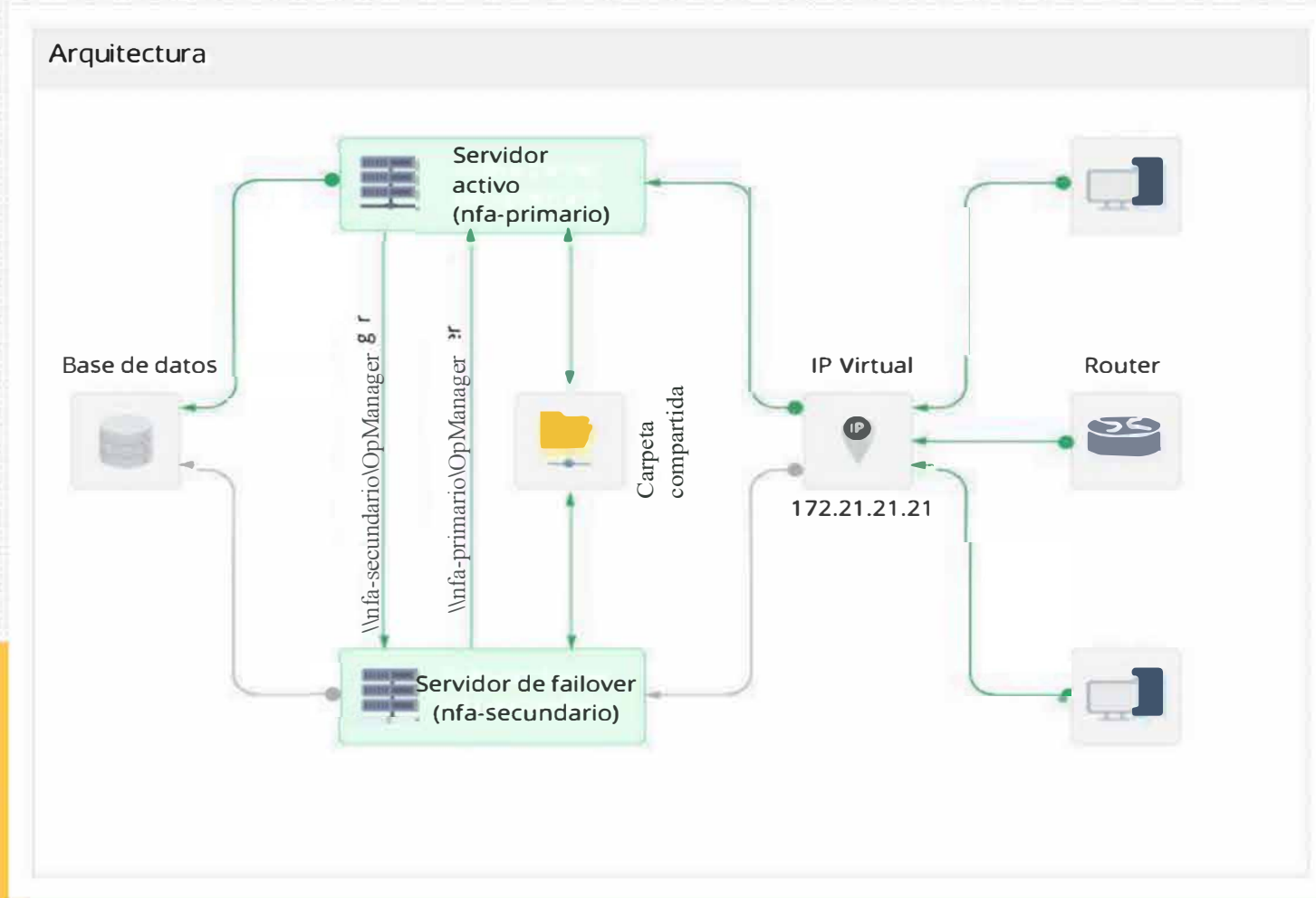
Jira Service Desk(On-Premise)

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](#)

Asegúrese de que su red siempre esté monitoreada con el failover de NetFlow Analyzer



The background features a light gray grid pattern. There are two large yellow circles: one in the top right corner and another in the bottom left corner. Several small gray stars are scattered across the grid.

Nuevas actualizaciones e integraciones

Integración con Applications Manager

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.

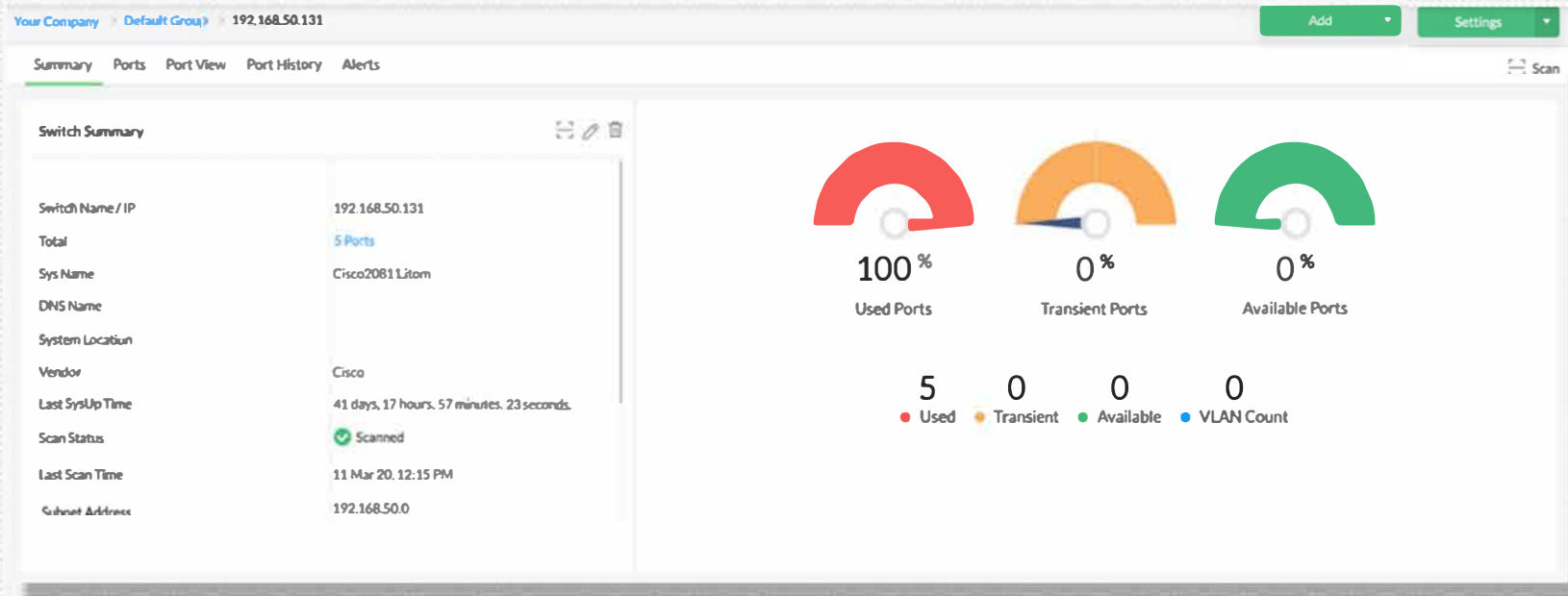
Sync now

Back

Save

- Sincronice los detalles de la aplicación (puerto, protocolo, IP)
- Categorice la aplicaciones críticas por separado
- Monitoree el tráfico de las aplicaciones por origen, destino, byte y más.

Integración con OpUtils



- Visibilidad de los puertos de red
- Capacidad de inspeccionar direcciones IP
- Widgets intuitivos

Monitoreo del tráfico en la nube - Monitoree y gestione los recursos de AWS y las nubes privadas virtuales en su red

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		
eni-0312cb732a499ce96	In-Use	ap-south-1	fl-0538cf969cf18a995		
eni-0d73e9d1ea840a7c3	Available	ap-south-1	fl-0ef7b6d63cfd2a34		
eni-057a0b8dac09489c5	In-Use	ap-south-1	fl-05c1dcd8a8c487c44		
eni-0869450aac8286554	Available	ap-south-1	fl-0c13110e120ef26fc		

Integración de webhooks con NetFlow Analyzer

NetFlow Analyzer

All Collectors are Up

DashboardInventoryWLCSecurityIPAMIPSLAAlarmsMapsReportsSettings

General SettingsDiscoveryMonitoringToolsNetFlowITOM Agent

NetFlow

Basic SettingsStorage SettingsGroups SettingsMappingsIP MappingLAN IP SettingsAlert ProfilesNotification TemplatesNBARCBQoSSecurity AnalyticsLicense ManagementFlow FiltersHighPerf Addon SettingsData UnitWAAS Settings

Notification Templates > Invoke a Webhook

Webhooks are user-defined callbacks via HTTP. Use webhooks to push alarms to the specified URL when an event is triggered in the product.

Template Name

Hook URL

POST

Enter the URL

Data Type

raw

form-urlencodedform-data

Payload TypeJSON

Content-Typeapplication/json

Body Content

```
{  "NFASource Type": "${NetFlowField(sourceType)},  "NFAAlert Profile Name": "${NetFlowField(alertName)}  }
```

Request Headers

Header NameHeader Value

Header Name	Header Value	Delete
No records to view.		

User Agent

Time out

Sensor de paquetes de red

Sensor de paquetes de red (NPS)

General SettingsDiscoveryMonitoringToolsNetFlowNCMOpUtilsITOM Agent

ITOM Agent

Network Packet Sensor

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

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

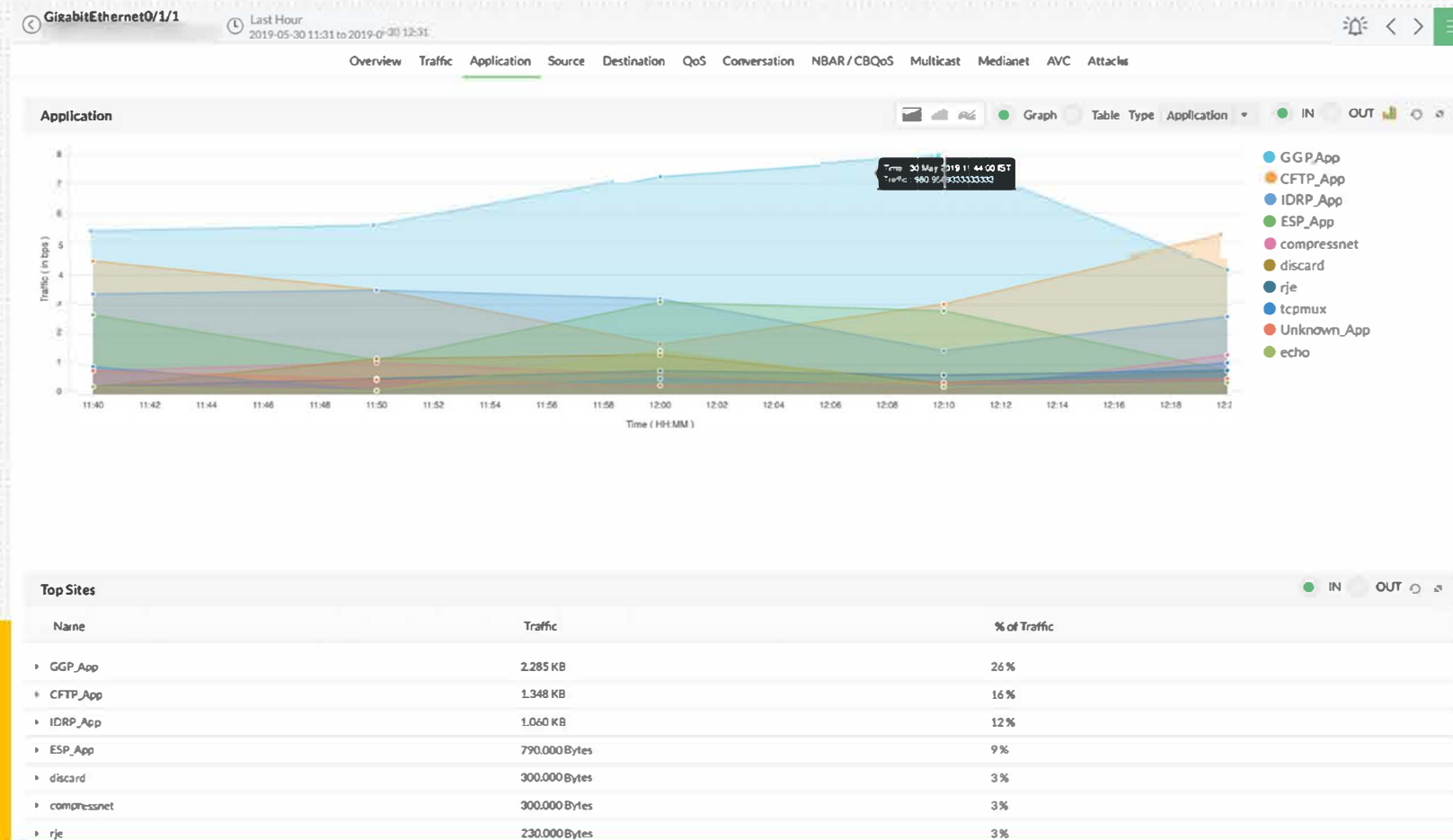
```
graph TD; subgraph Sensor1 [Network Packet Sensor 1]; direction TB; DPI1[DPI Engine 1]; NF1[NetFlow Generator 1]; end; subgraph Sensor2 [Network Packet Sensor 2]; direction TB; DPI2[DPI Engine 2]; NF2[NetFlow Generator 2]; end; subgraph Sensor3 [Network Packet Sensor 3]; direction TB; DPI3[DPI Engine 3]; NF3[NetFlow Generator 3]; end; subgraph Sensor4 [Network Packet Sensor 4]; direction TB; DPI4[DPI Engine 4]; NF4[NetFlow Generator 4]; end; Sensor1 --> NF_Analyzer[NetFlow Analyzer]; Sensor2 --> NF_Analyzer; Sensor3 --> NF_Analyzer; Sensor4 --> NF_Analyzer;
```

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](#)

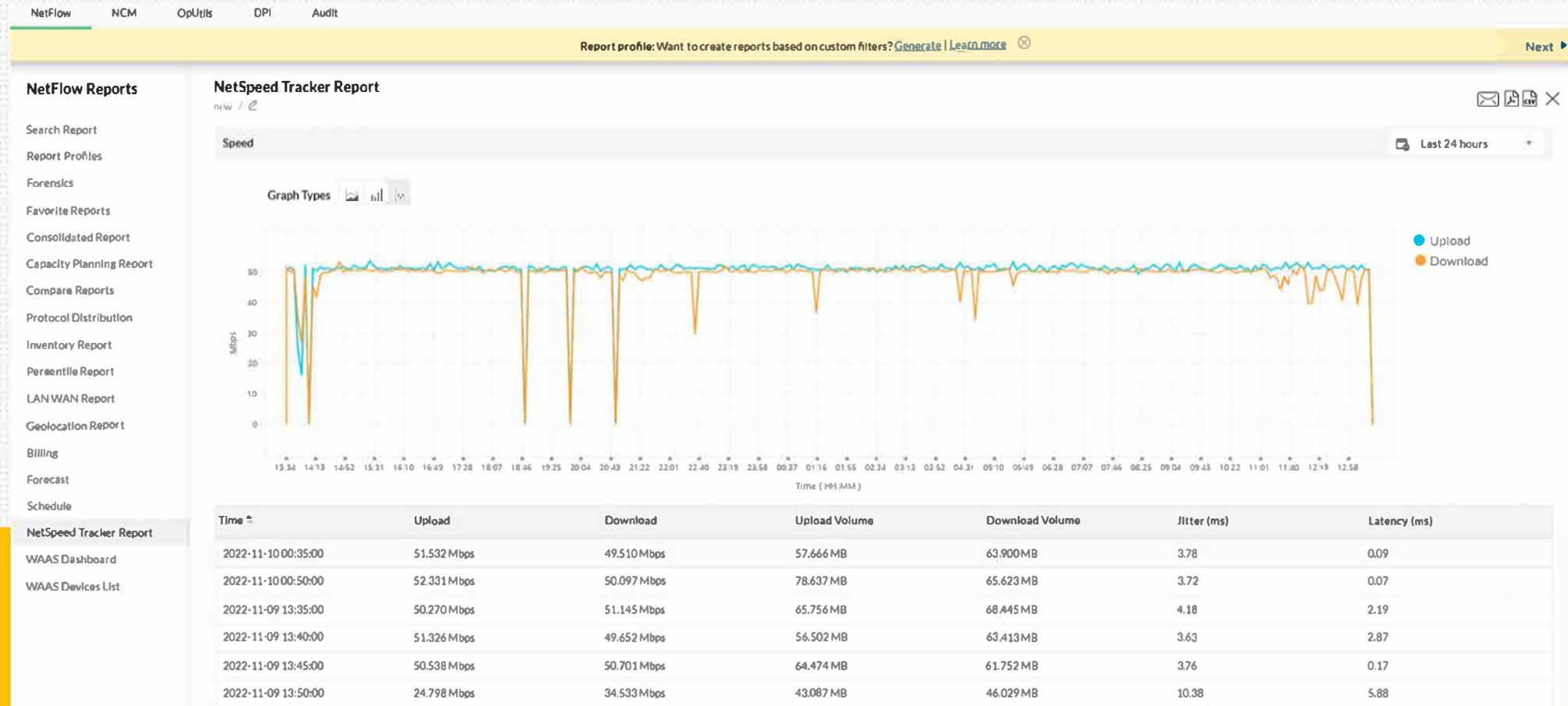
Download Network Packet Sensor

WindowsLinux

Generador de NetFlow



Controlador de la velocidad de red





[youtube.com/
@ManageEngineLATAM](https://www.youtube.com/@ManageEngineLATAM)



[forums.manageengine.com/netflo
wanalyzer](https://forums.manageengine.com/netflow-wanalyzer)



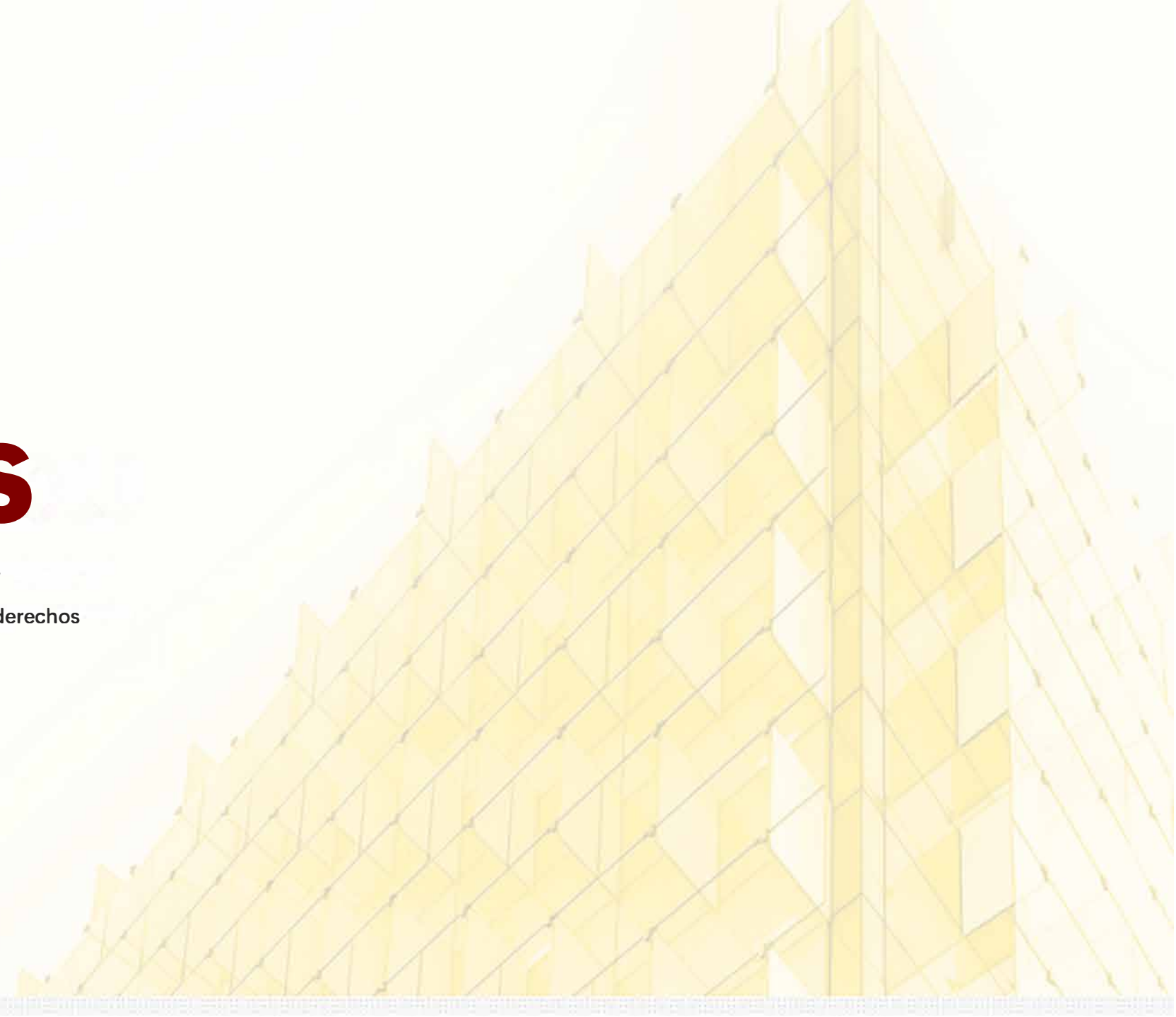
[https://www.manageengine.com/
latam/netflow/documentacion-
de-ayuda.html](https://www.manageengine.com/latam/netflow/documentacion-de-ayuda.html)



tech-latam@manageengine.com



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



GRACIAS

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

© 2023, Zoho Corp., ManageEngine - Todos los derechos reservados.