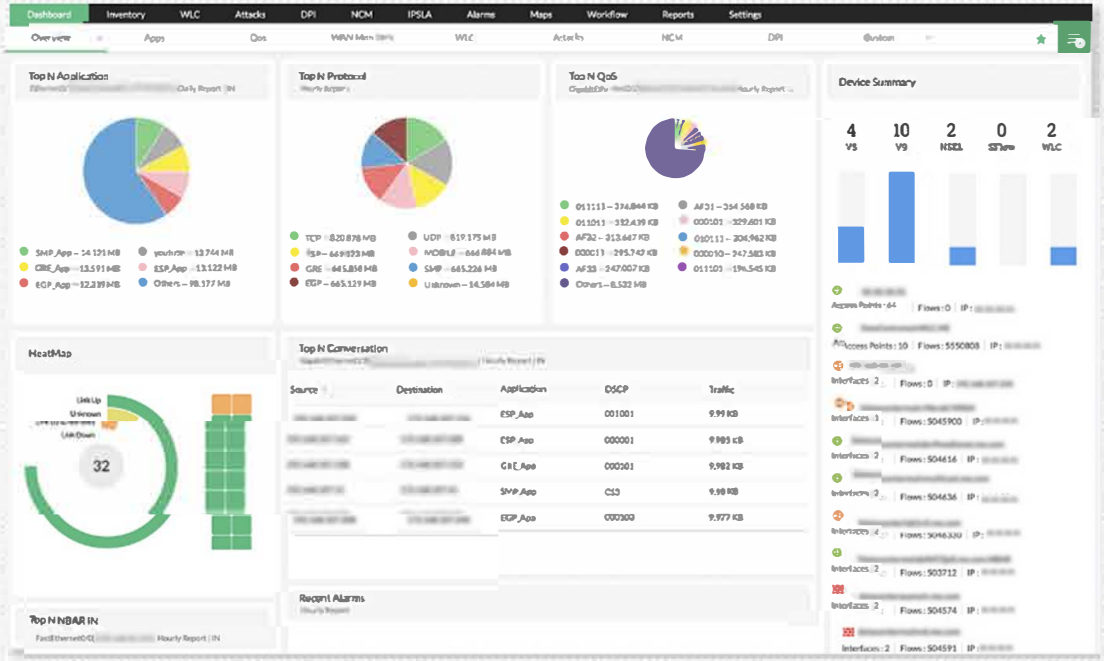
ManageEngine

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

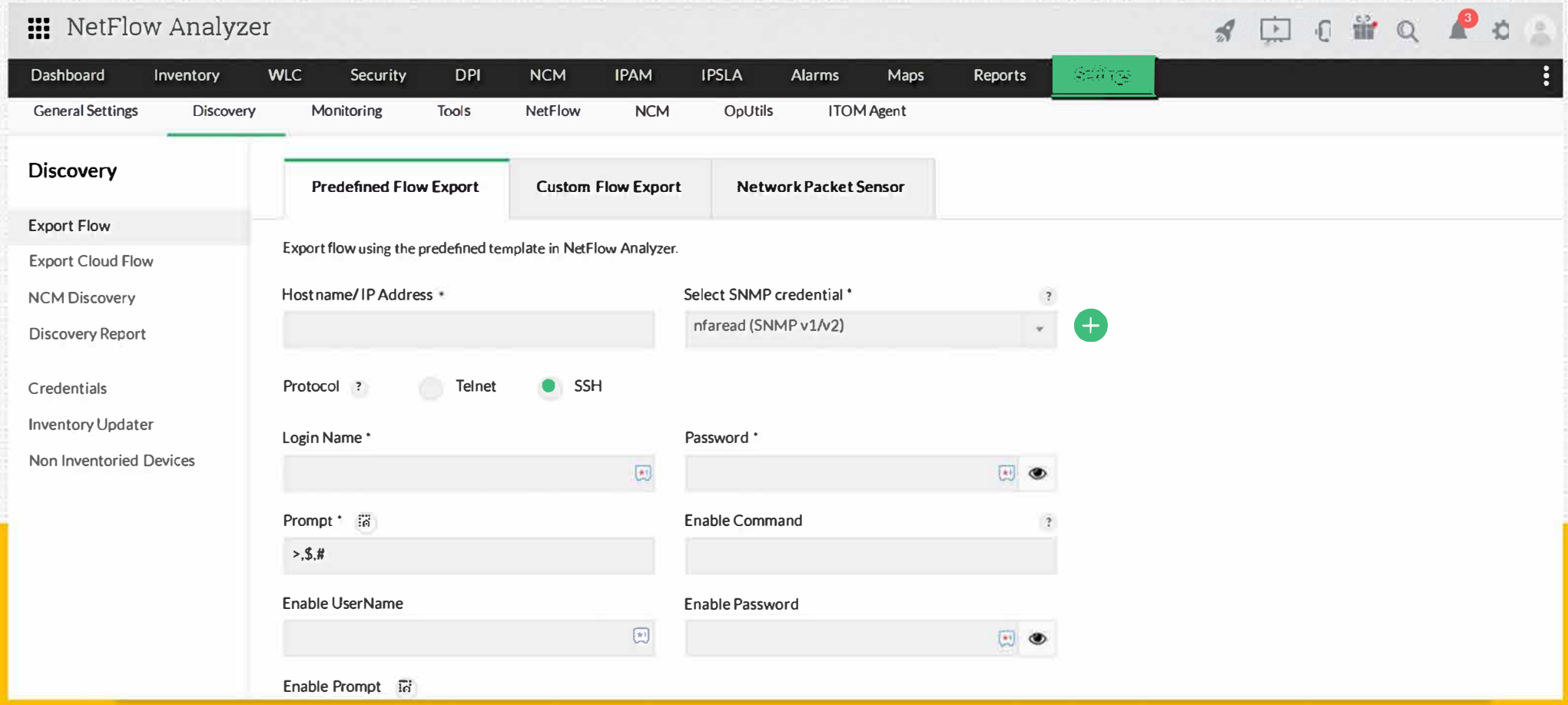
Seguridad

¡Comience a monitorear NetFlow!

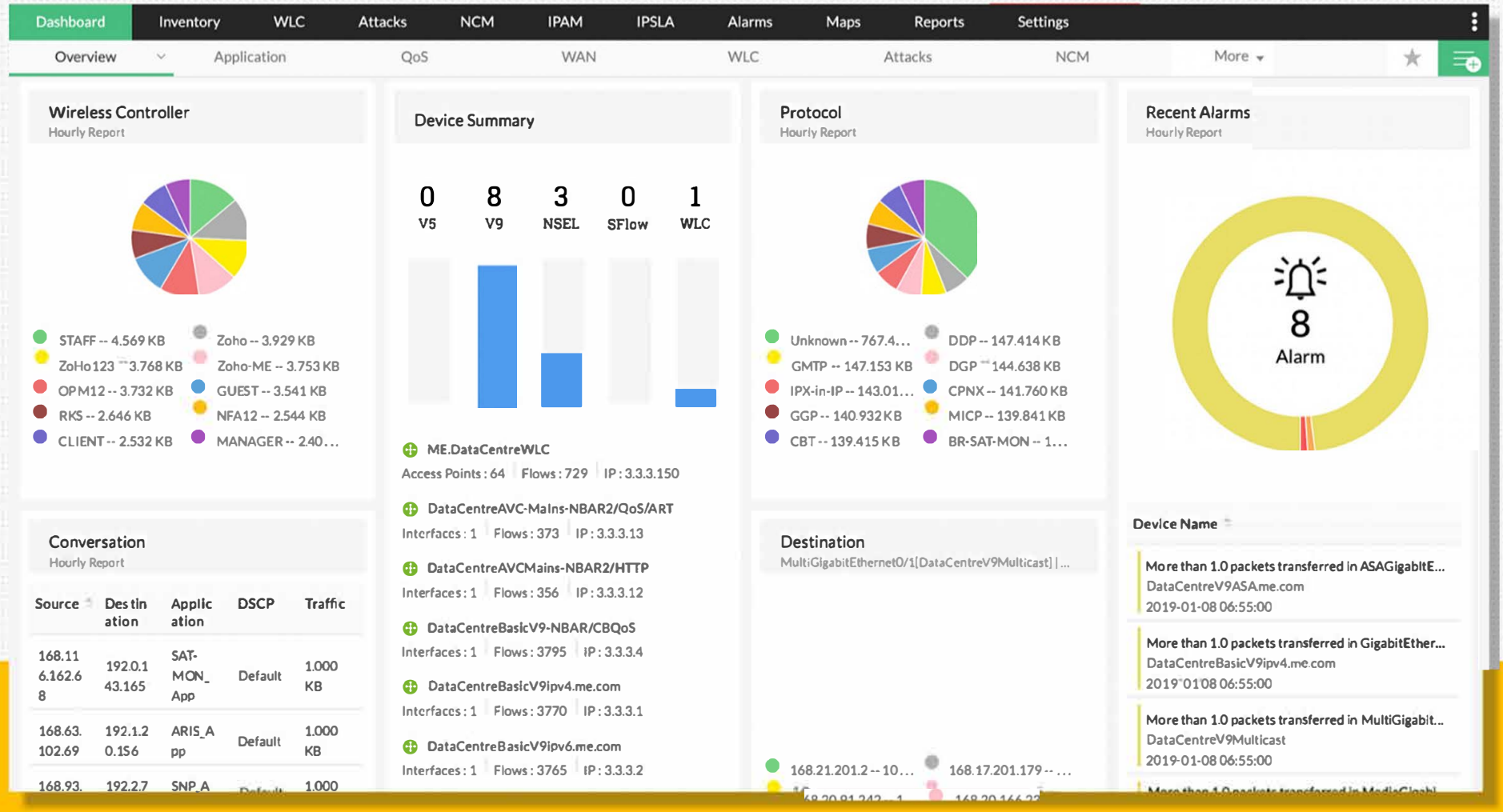
Exportación de flujo

Agregue las credenciales → Ejecute los comandos → Exporte el flujo

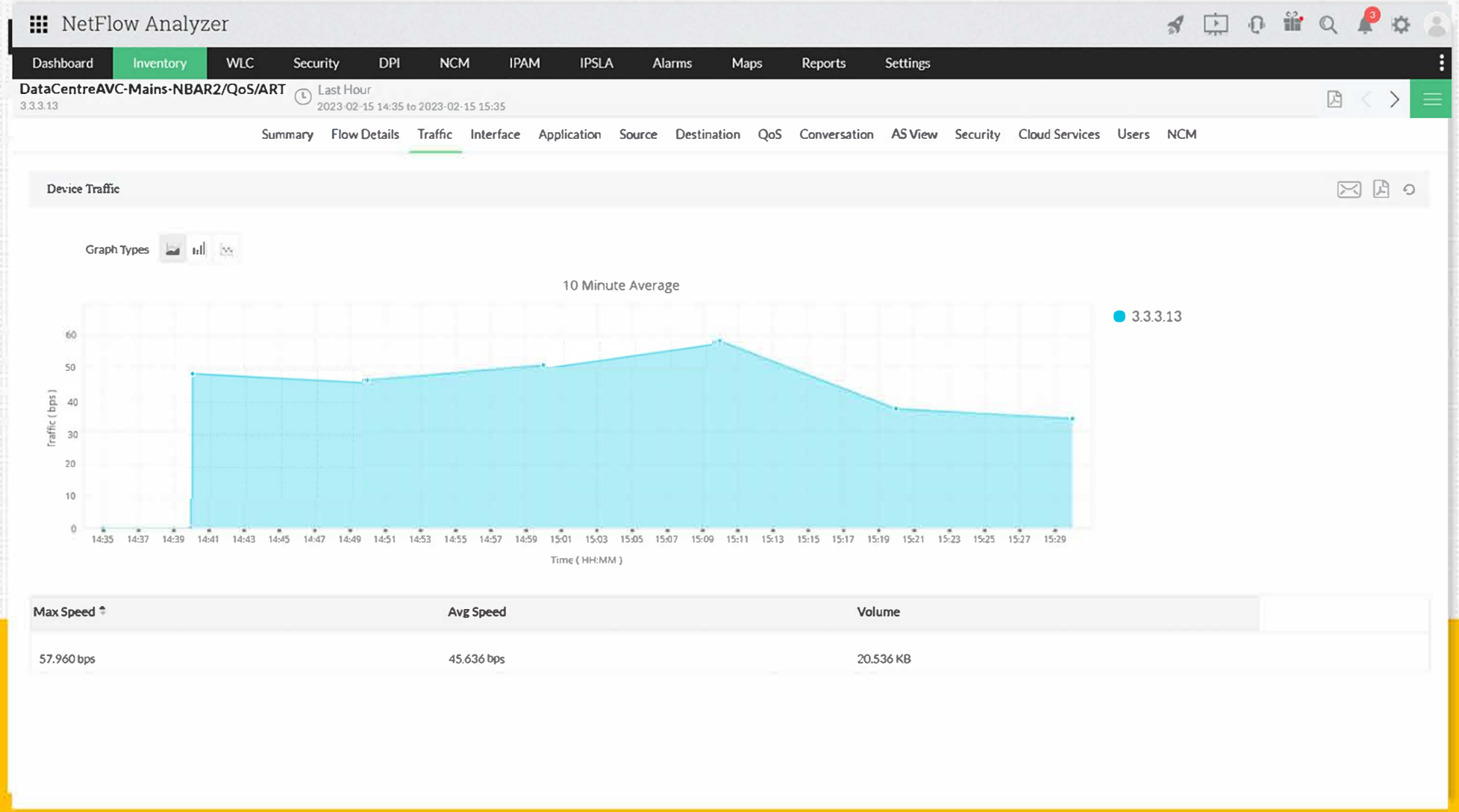
i. Predefinido
ii. Personalizado
iii. Sensor de paquetes de red



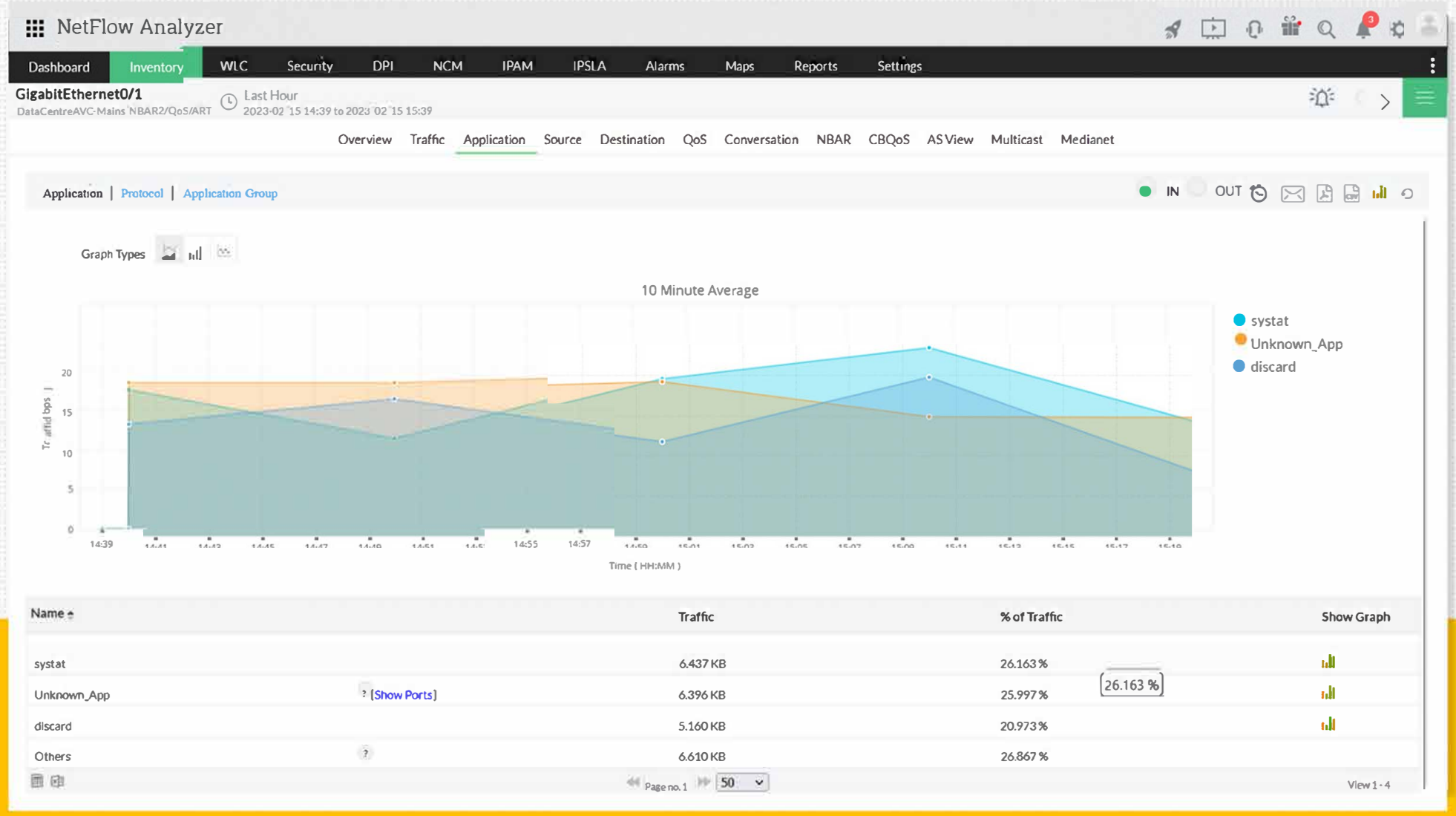
Vista de NOC y dashboard



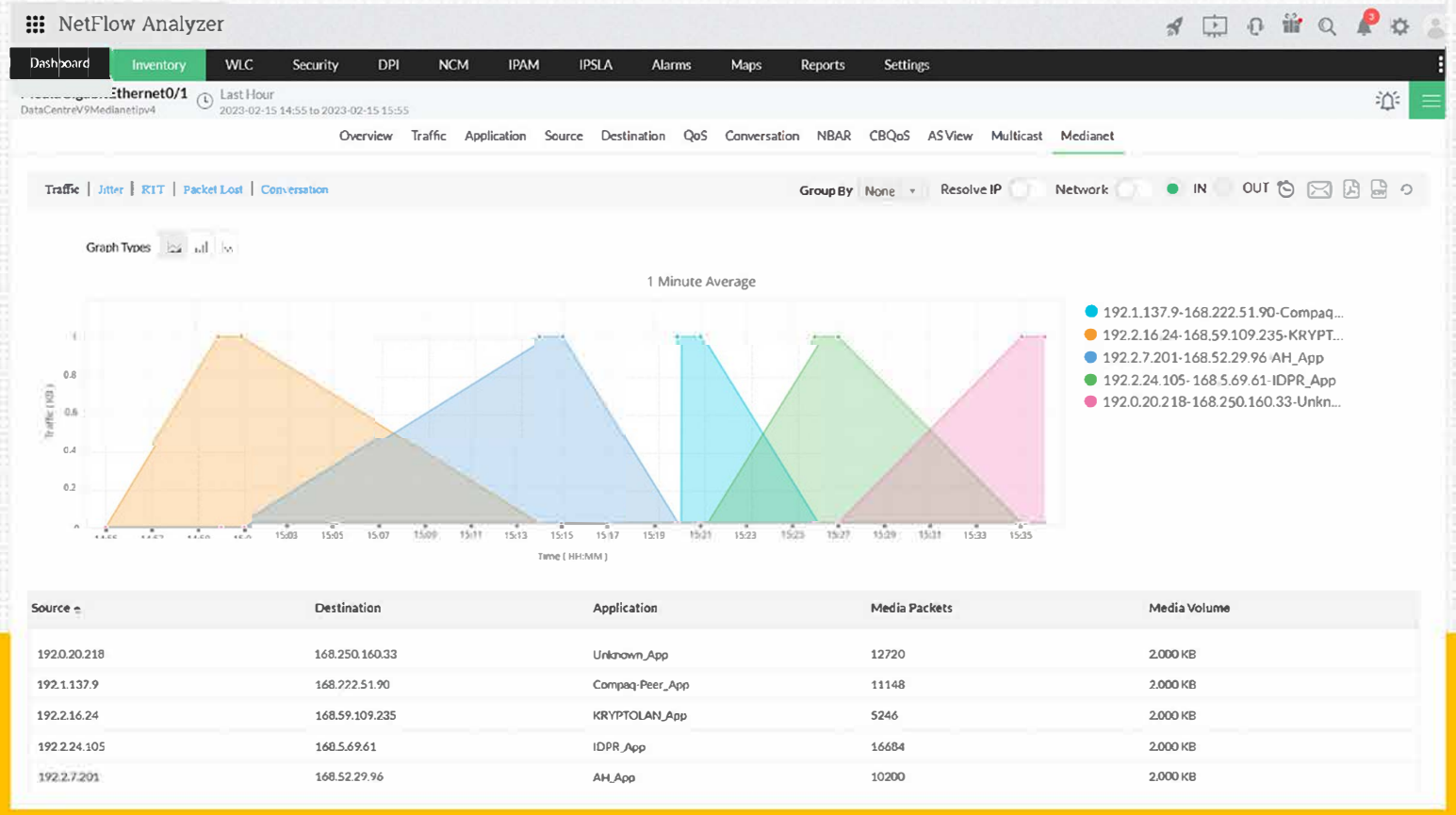
Tráfico de dispositivos e interfaces



Tráfico de aplicaciones

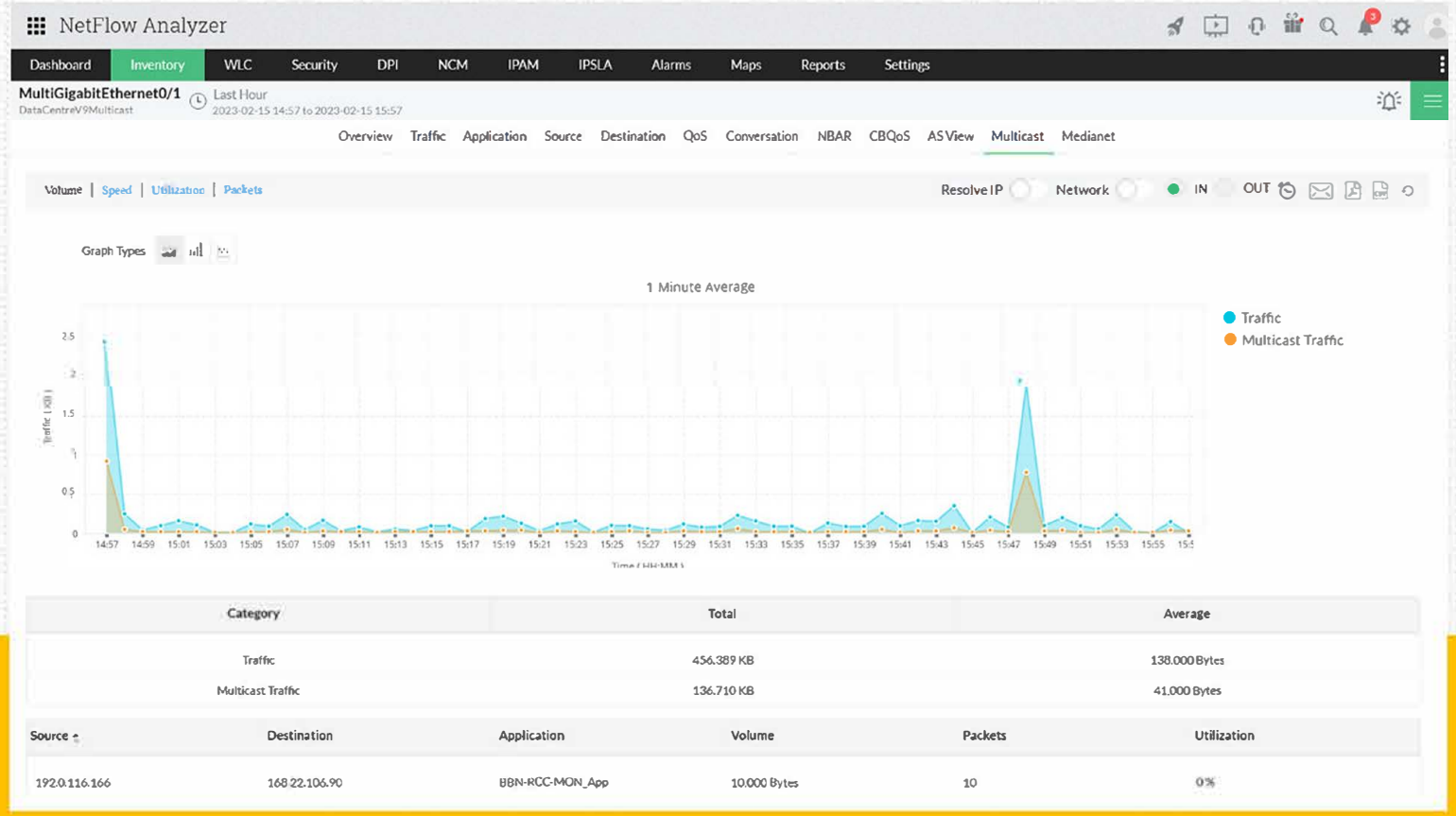


Monitoreo del tráfico de medianet



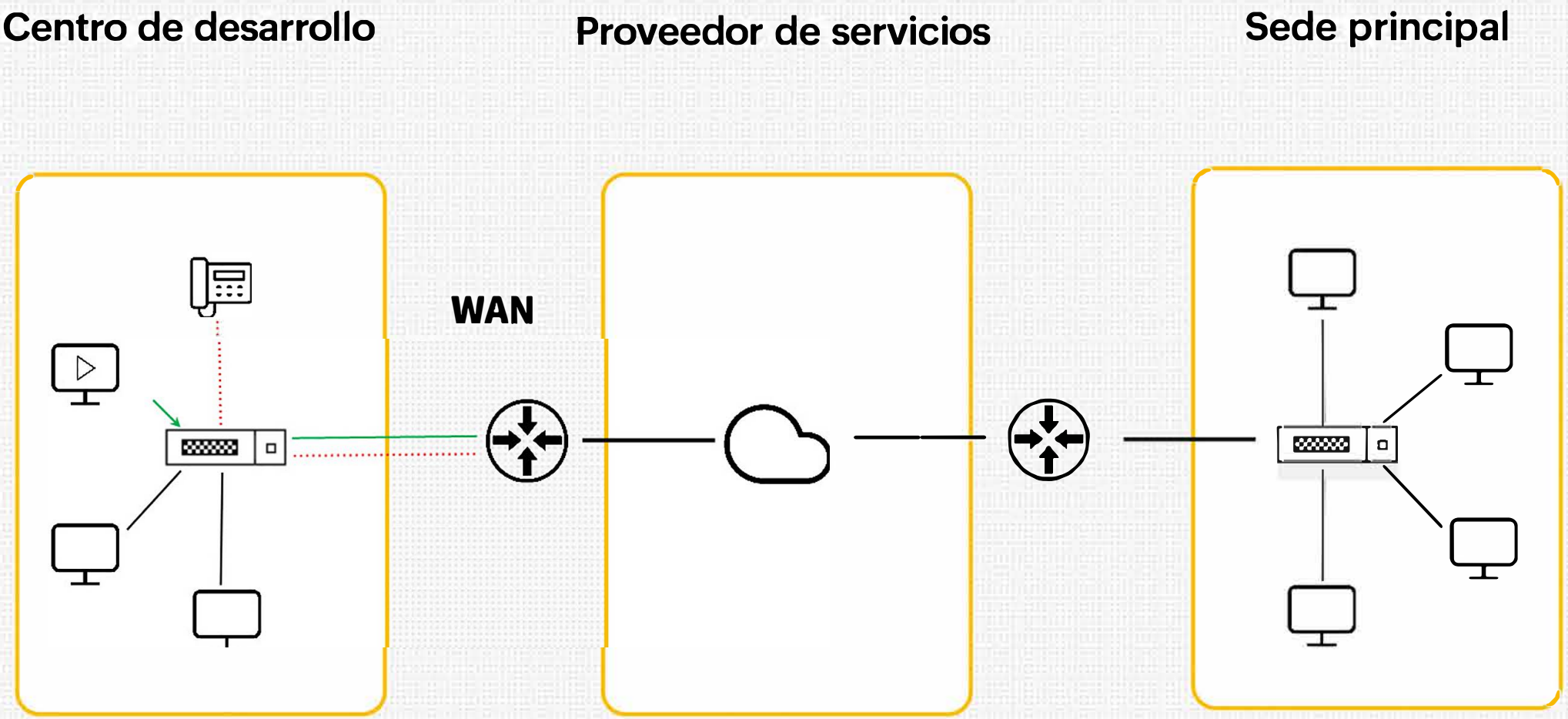
- Monitoree tráfico multimedia como el tráfico de voz y video para mejorar la QoE.
- Mida las estadísticas de rendimiento como fluctuación, pérdida de paquetes y RTT.

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.

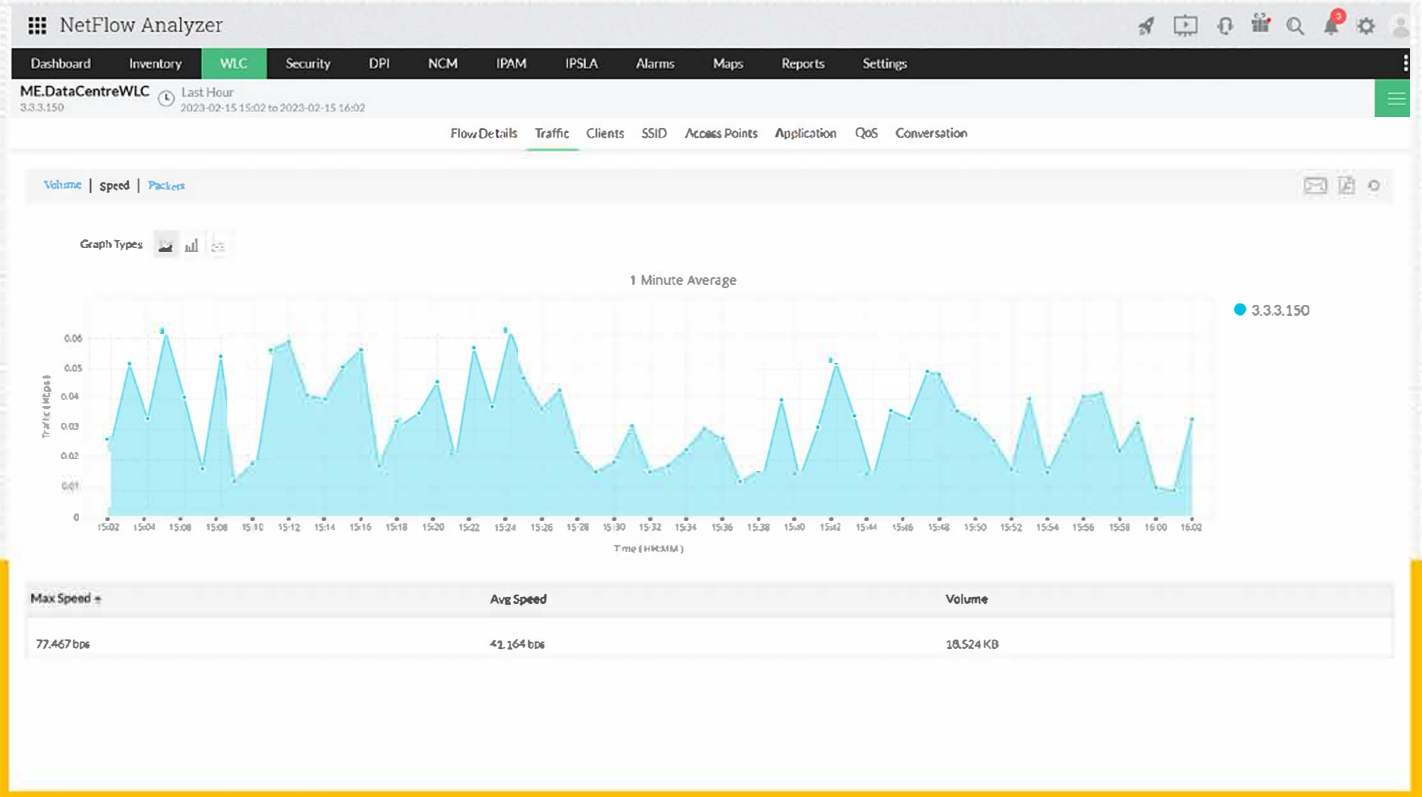
Monitoreo de IPSLA



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.

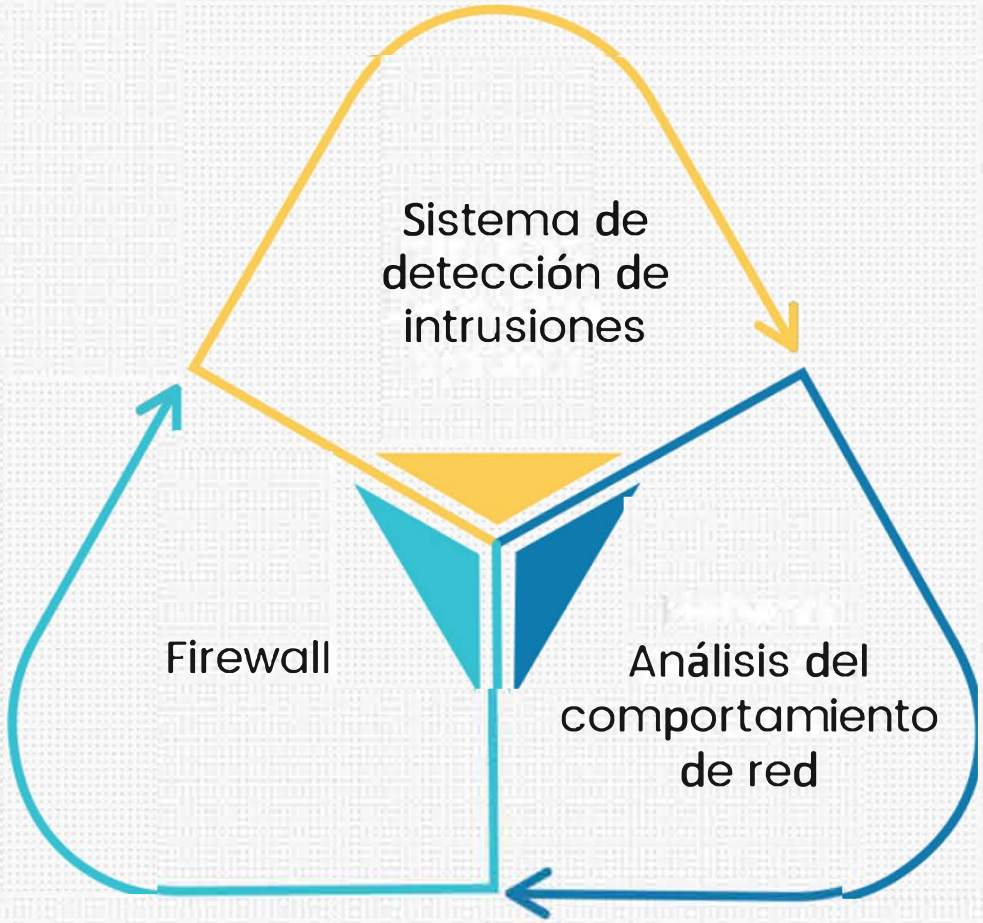
Monitoreo del tráfico inalámbrico



- 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?

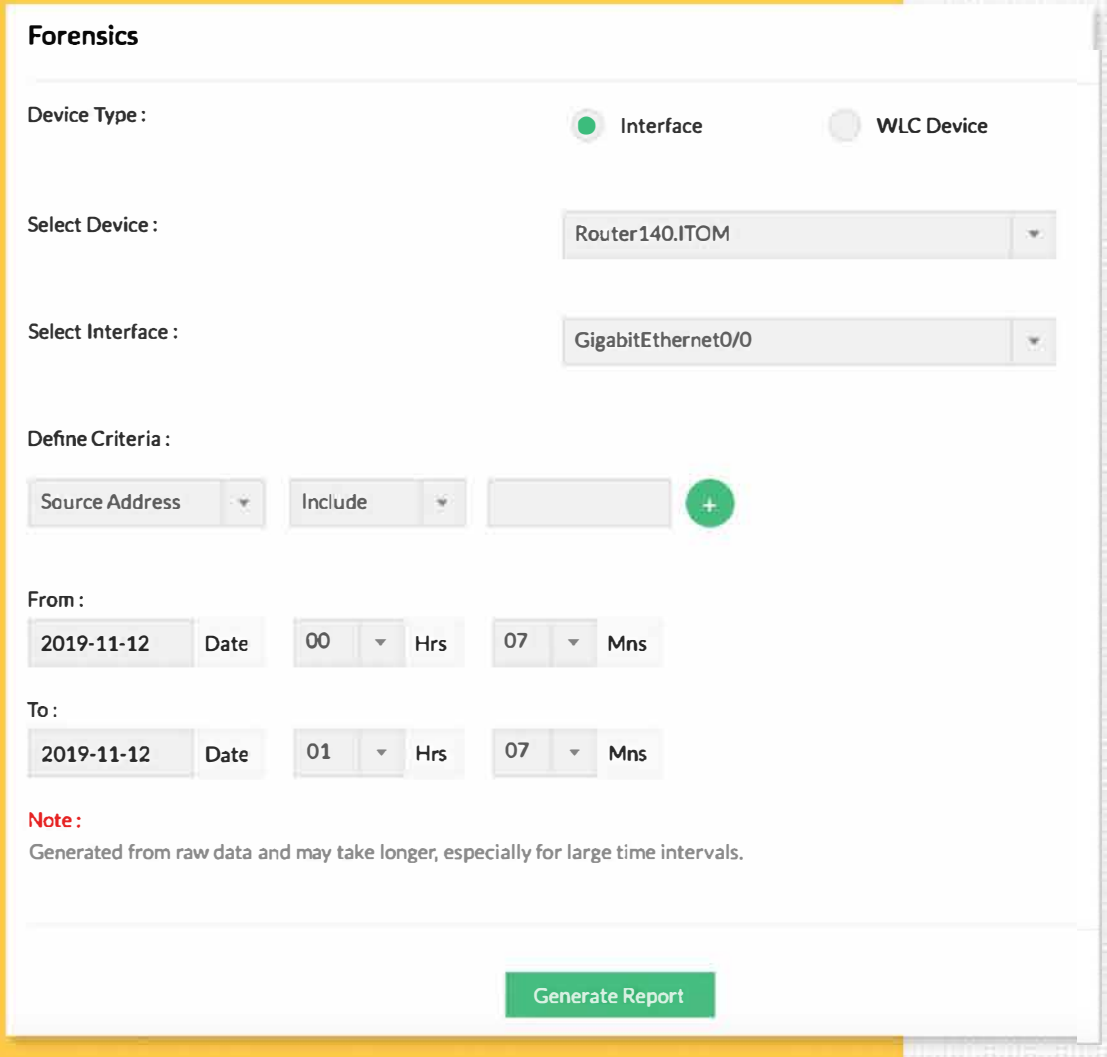
Análisis forense de red

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



- 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?

Importancia tecnológica del módulo de seguridad

- Interfaz de usuario intuitiva y sencilla
- Administración y ajuste efectivos
- Consulta y análisis de eventos exhaustivos
- Evaluación general rápida de amenazas
- Investigación forense detallada

- Monitoreo de eventos de seguridad de red en tiempo real
- Monitoreo de amenazas internas y externas eficiente
- Evaluación continua de la postura de seguridad de la red
- Recopilación e informes exhaustivos de los detalles de incidentes

- Procesamiento de flujo de eventos de alta velocidad y baja latencia
- Distribución eficaz de la carga de trabajo y procesamiento asíncrono
- Marco enriquecido con API para crear aplicaciones de alto rendimiento
- Motor de reglas rápidas y perfiles de criterios flexibles
- Modelado de recursos sensibles al contexto, correlación de eventos complejos, algoritmos de extracción avanzados...

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

NetFlow NCM OpUtils Audit

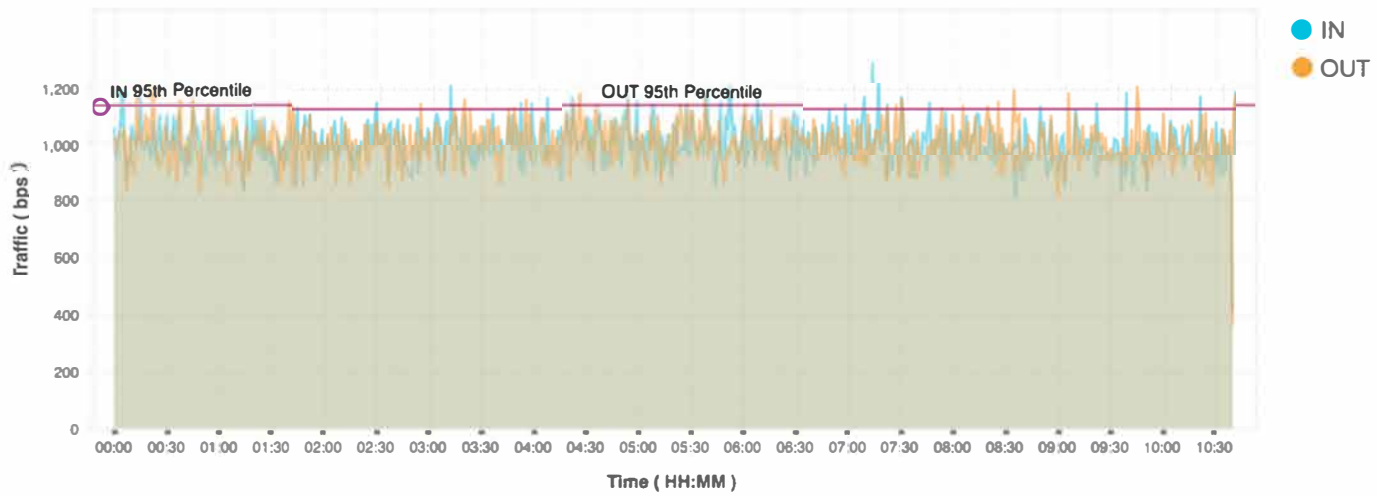
NetFlow Reports

- 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

Informe de previsión

NetFlow NCM OpUtils Audit

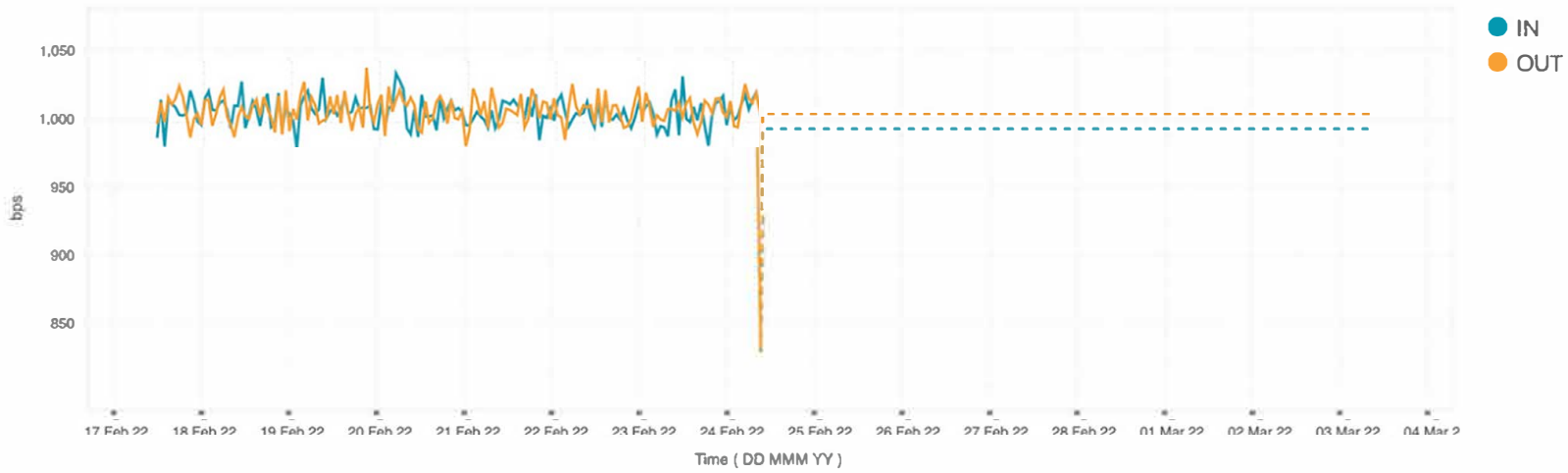
NetFlow Reports

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

Forecast

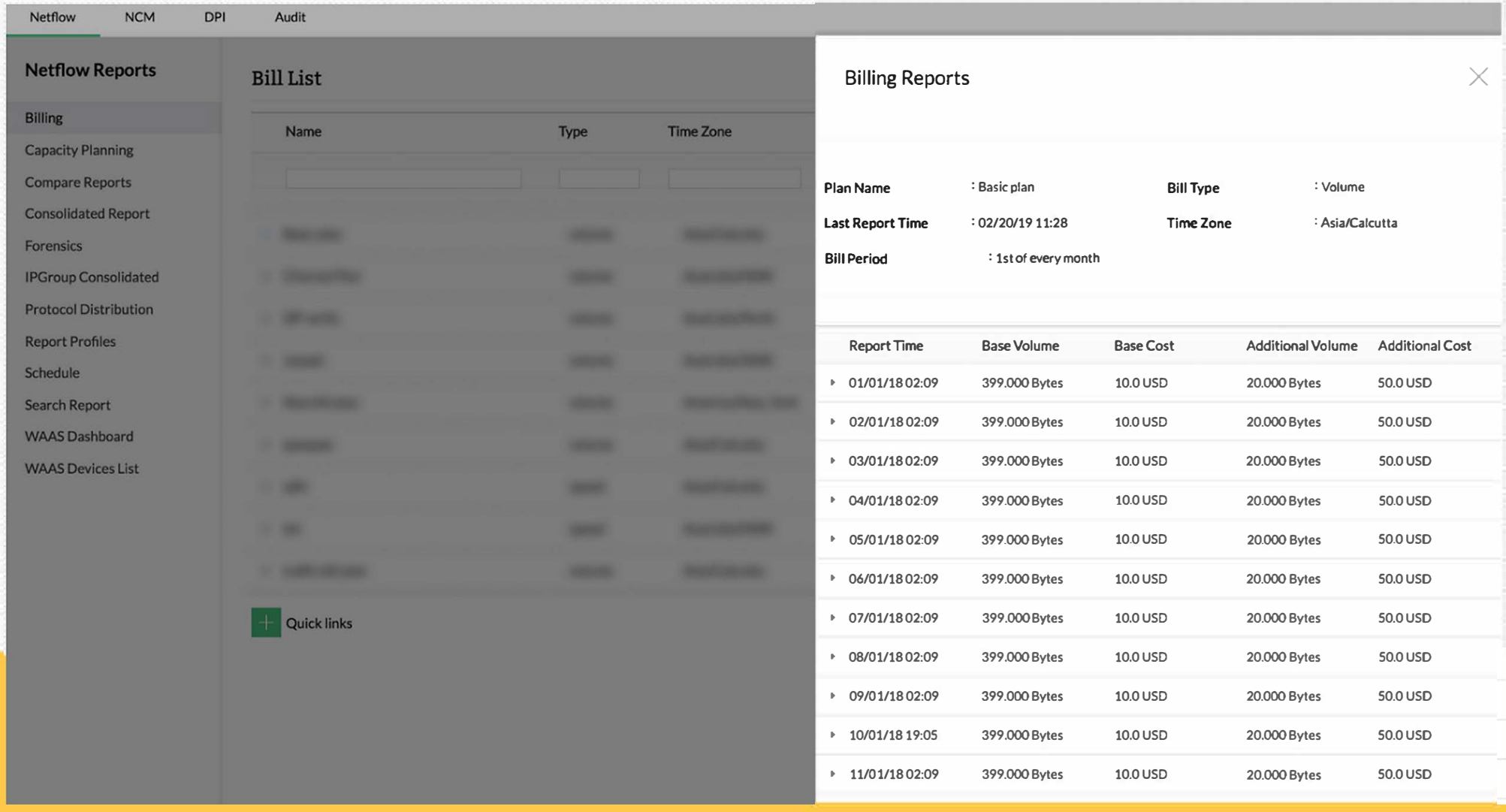
DataCentreV9Medianetipv4 / MediaGigabitEthernet0/1 /

Volume | Speed | Utilization | Show History | 7 Days



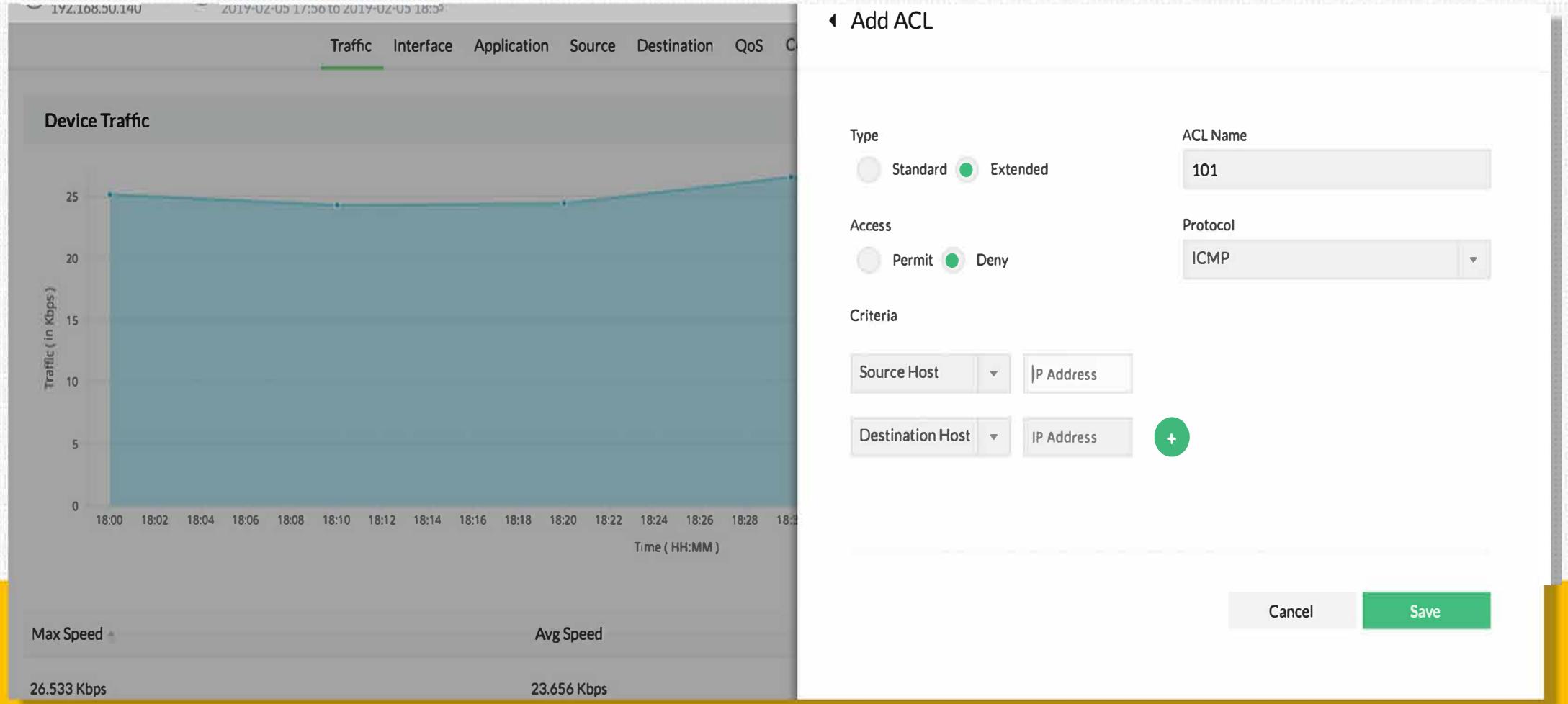
Time	IN	OUT
Feb-17-22 21:30	1.014 Kbps	1.002 Kbps
Feb-17-22 22:30	1.000 Kbps	1.006 Kbps
Feb-17-22 23:30	997.696 bps	997.684 bps

Informe de facturación

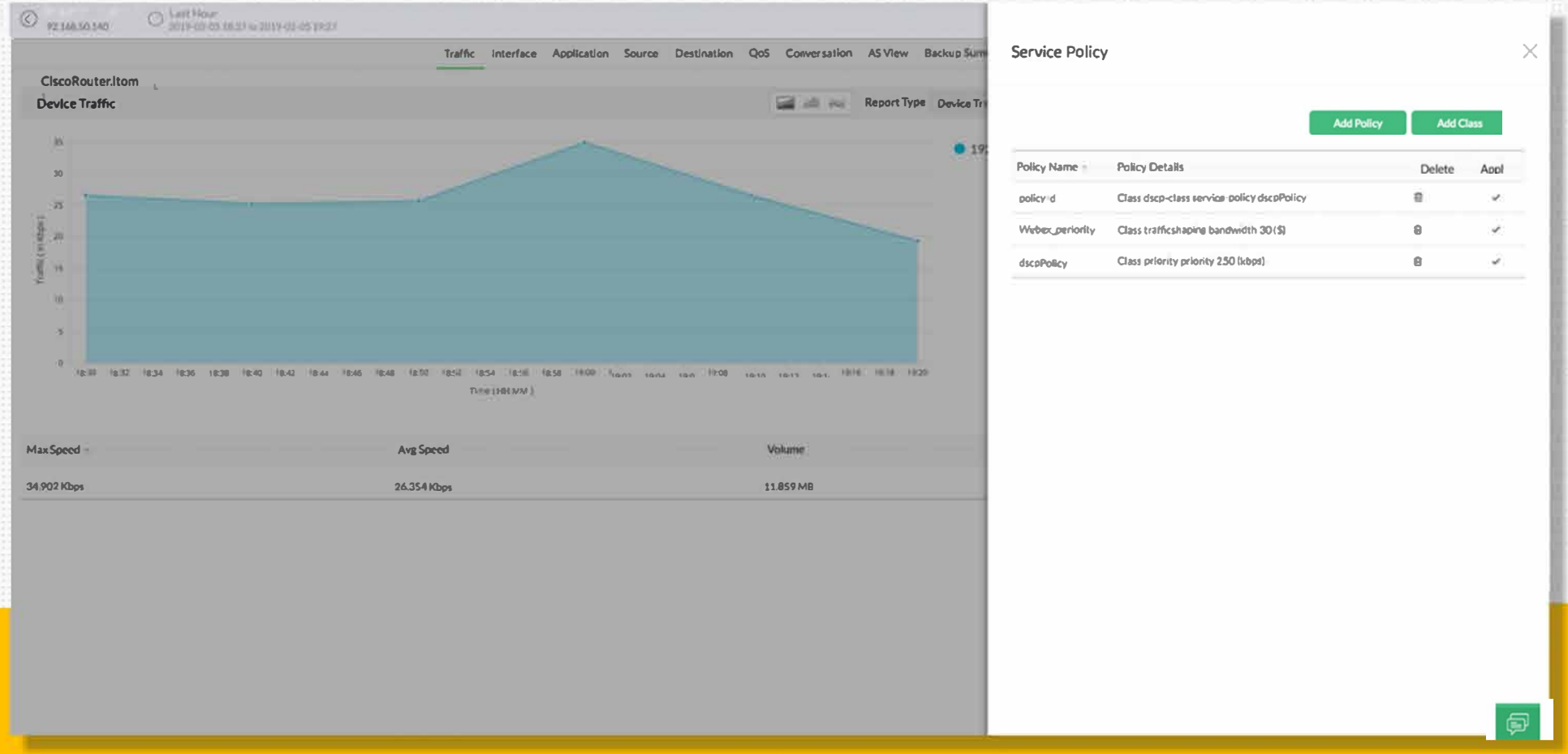


Priorice el modelado de tráfico y datos: Optimización más simple

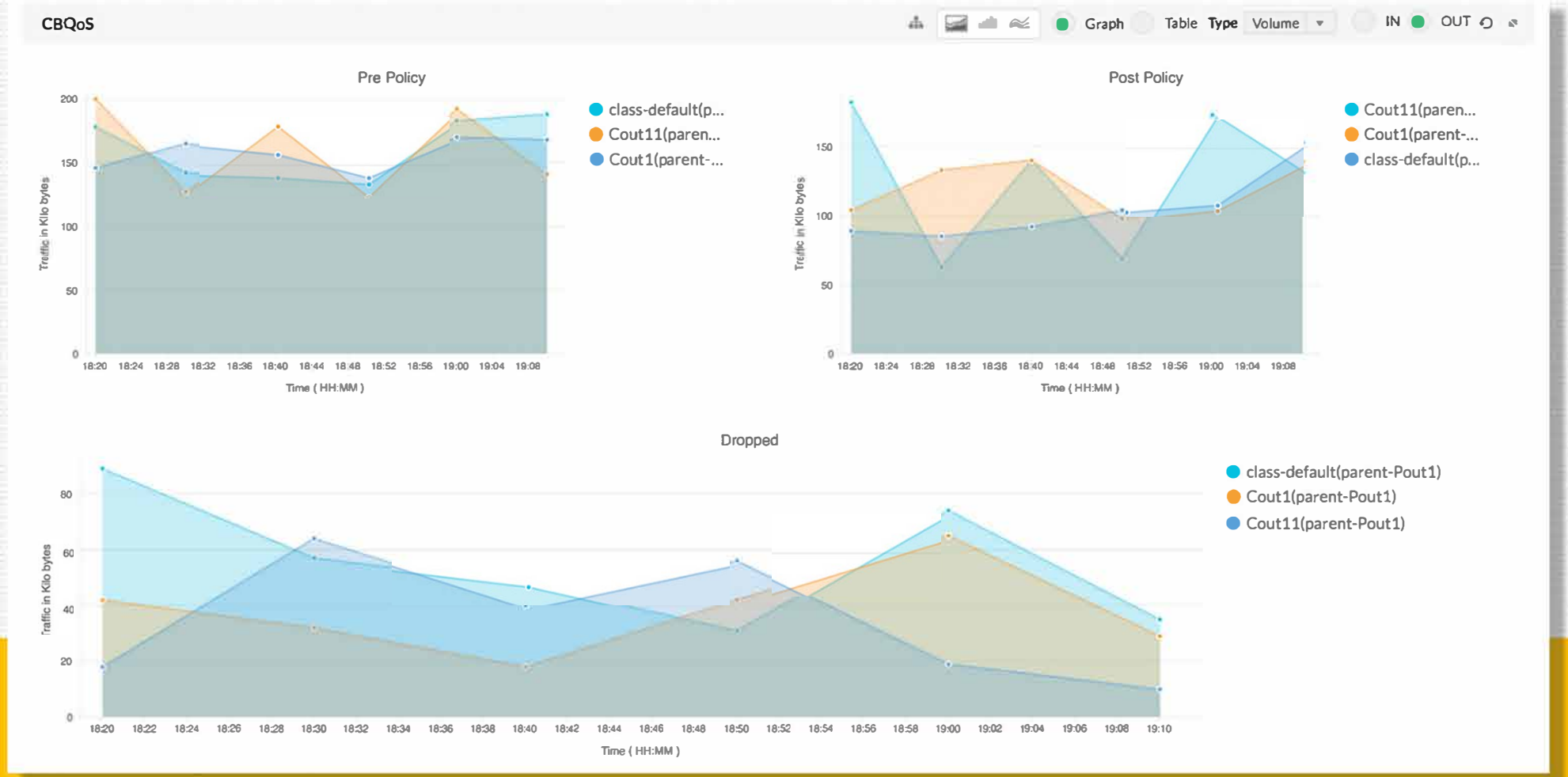
Filtre el exceso de tráfico del router bloqueando o restringiendo IP/redes IP con ACL



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

IP

Aplicación

DSCP

SSID

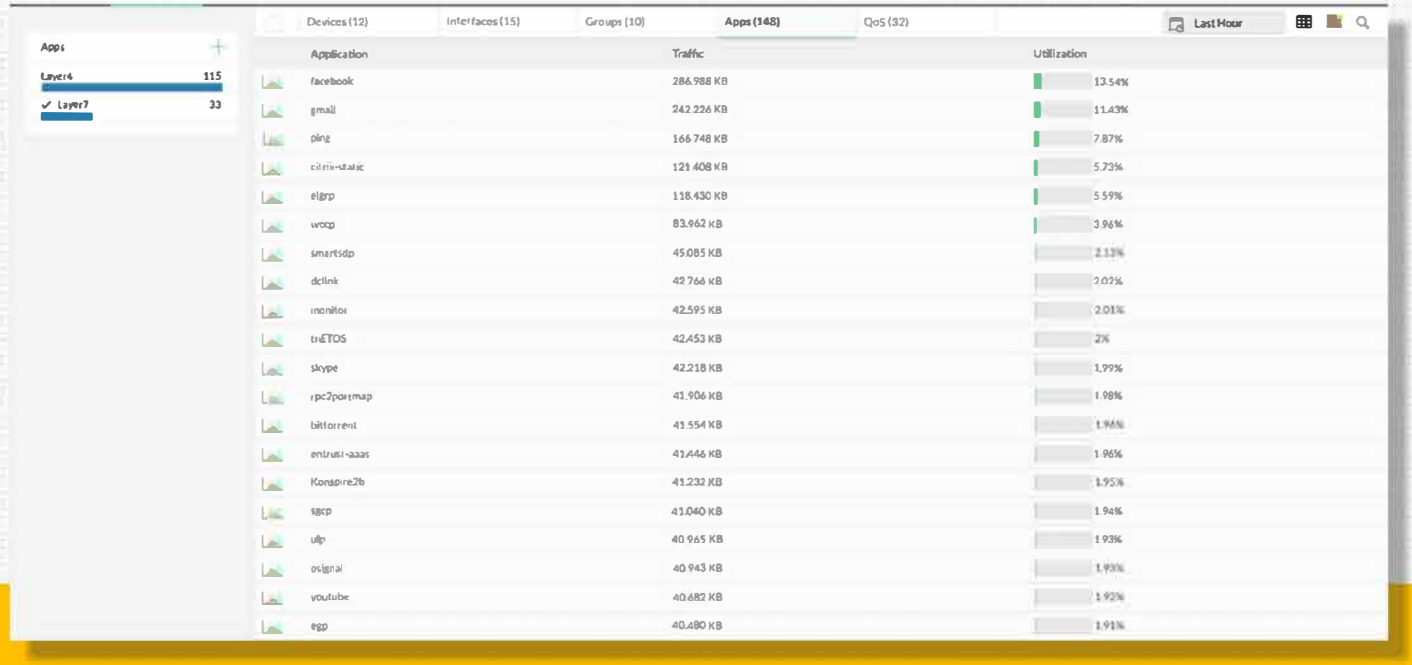
SSID

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

Proporcione acceso a los operadores según los grupos.

Brinde una mejor visibilidad para mejorar la resolución de problemas.

Monitoree aplicaciones personalizadas



- **Asignación de aplicaciones para _App**

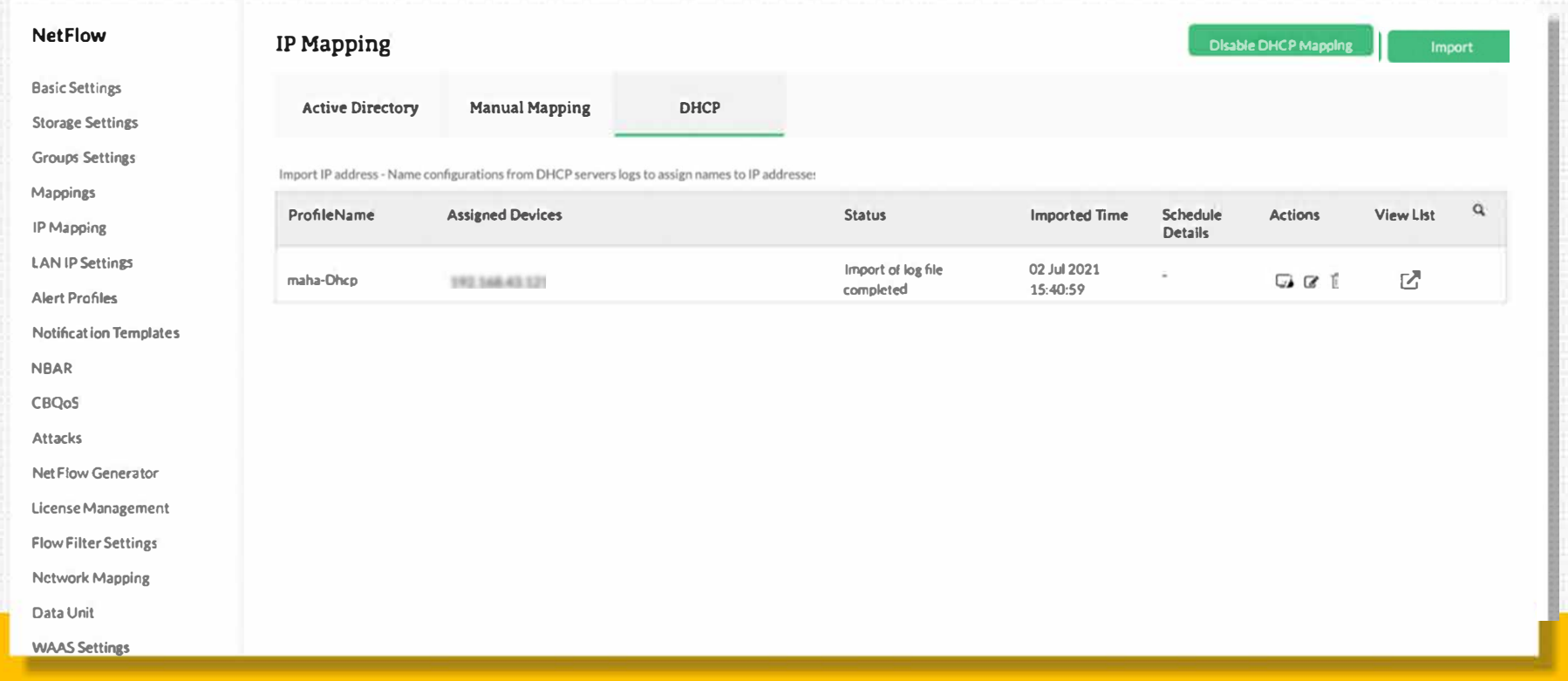
  Interfaz > Aplicación > _App > Mostrar puerto (para usar la función "Mostrar puerto" se deben habilitar los datos sin procesar).

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

- **Asignación de aplicaciones para aplicaciones personalizadas**

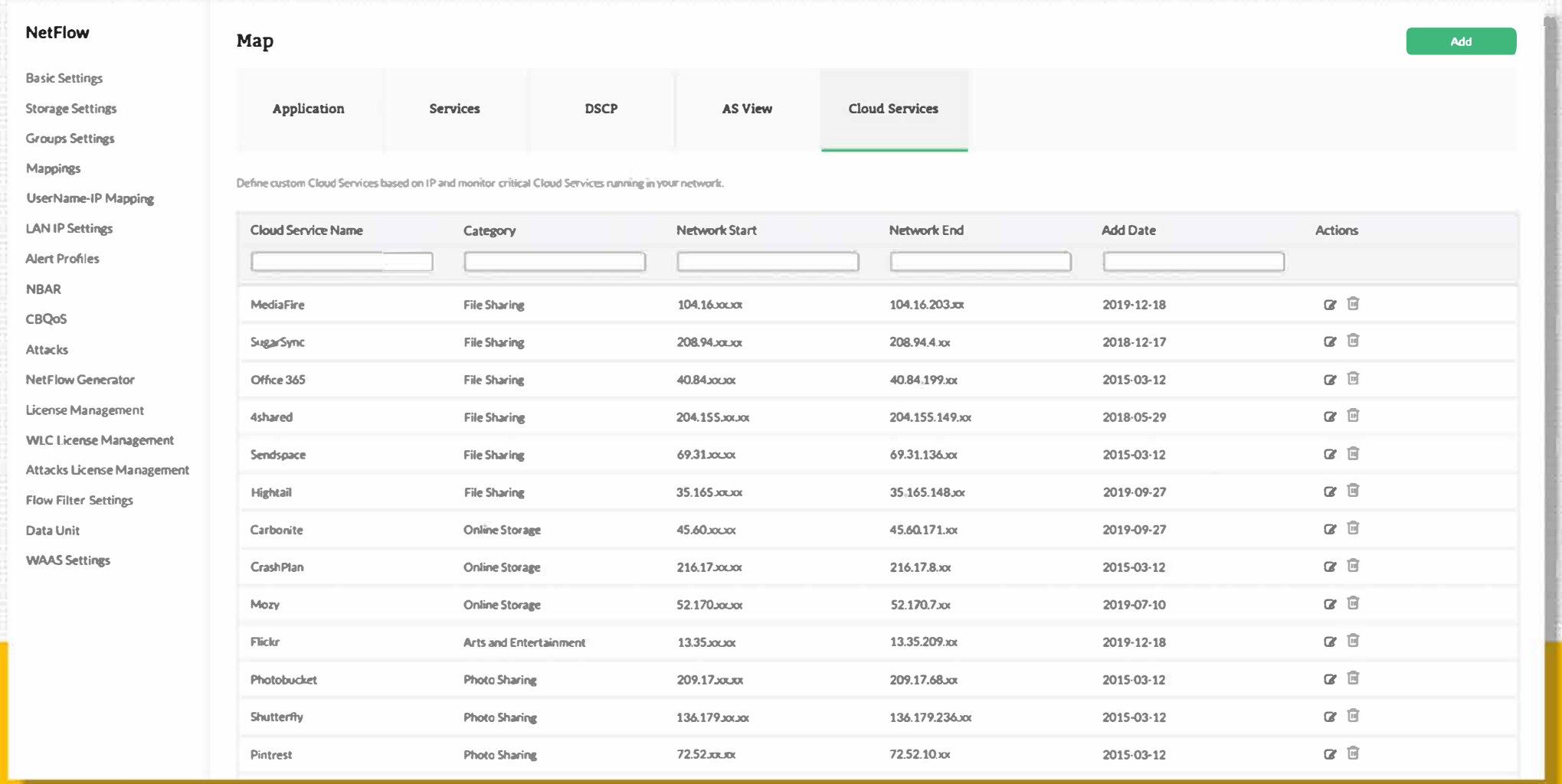
  Ajustes > NetFlow > Asignación > Lista de aplicaciones > Añadir

Nombre de usuario - Asignación de IP



- Asignación de AD
- Manual
- Asignación
- DHCP

Servicios en la nube



Gestión proactiva

Configure alertas

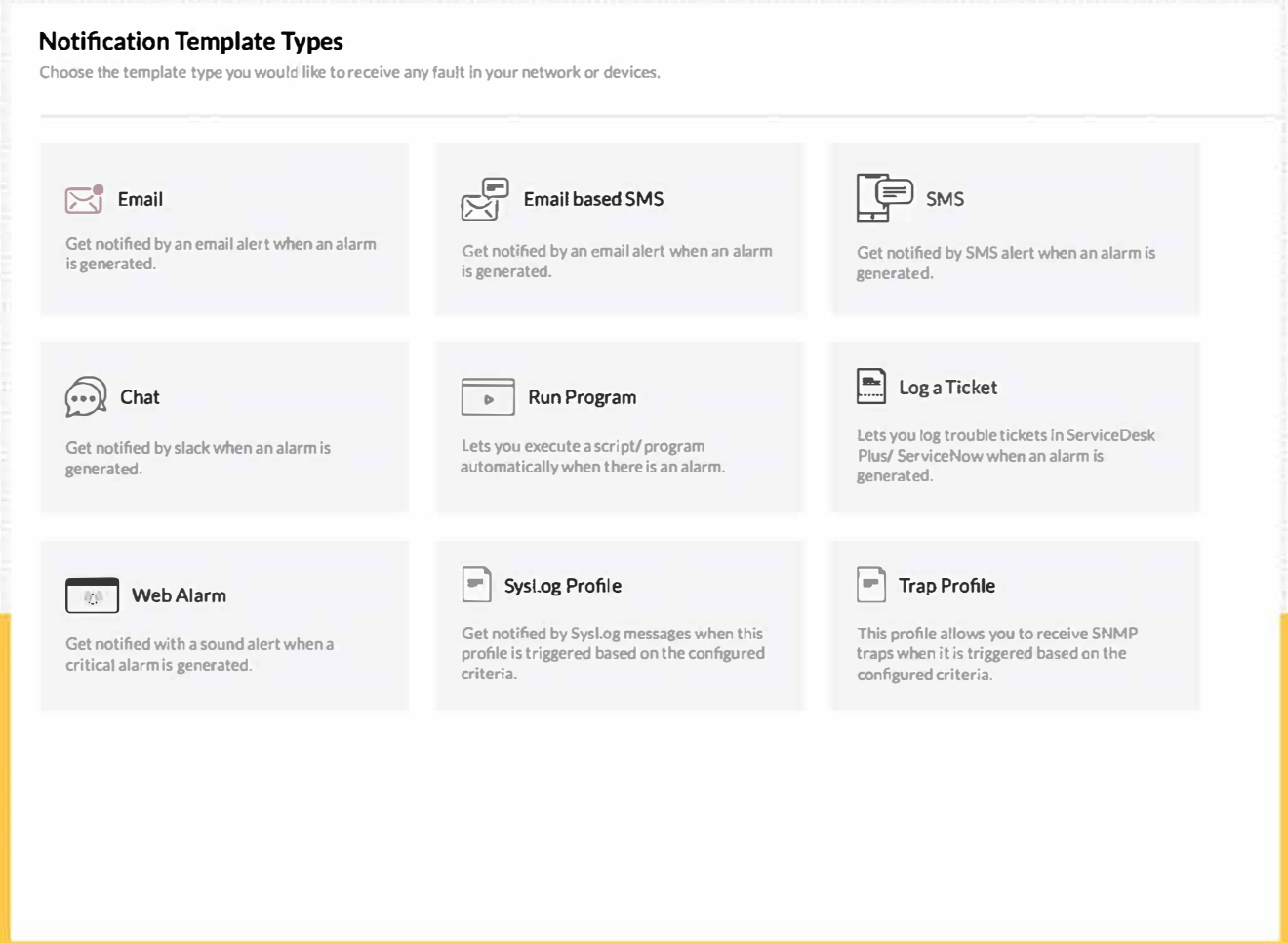
Alertas en tiempo real

Alertas agregadas

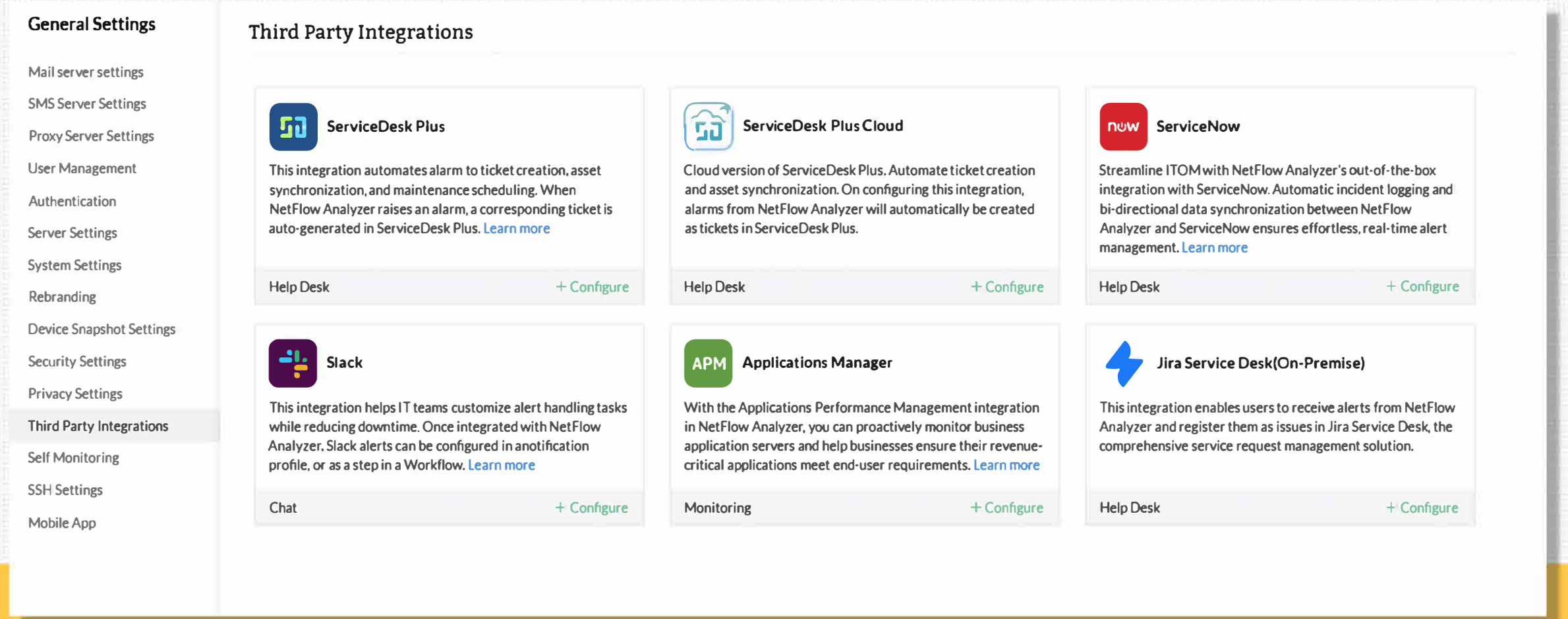
- Alertas preconfiguradas (enlace inactivo / sin flujo)
- Alertas basadas en umbrales

- **Reciba notificaciones por correo electrónico, SMS, tickets, SMS basado en correo electrónico, chat, ejecución de programa, perfil de syslog, perfil de trap, alarma web**

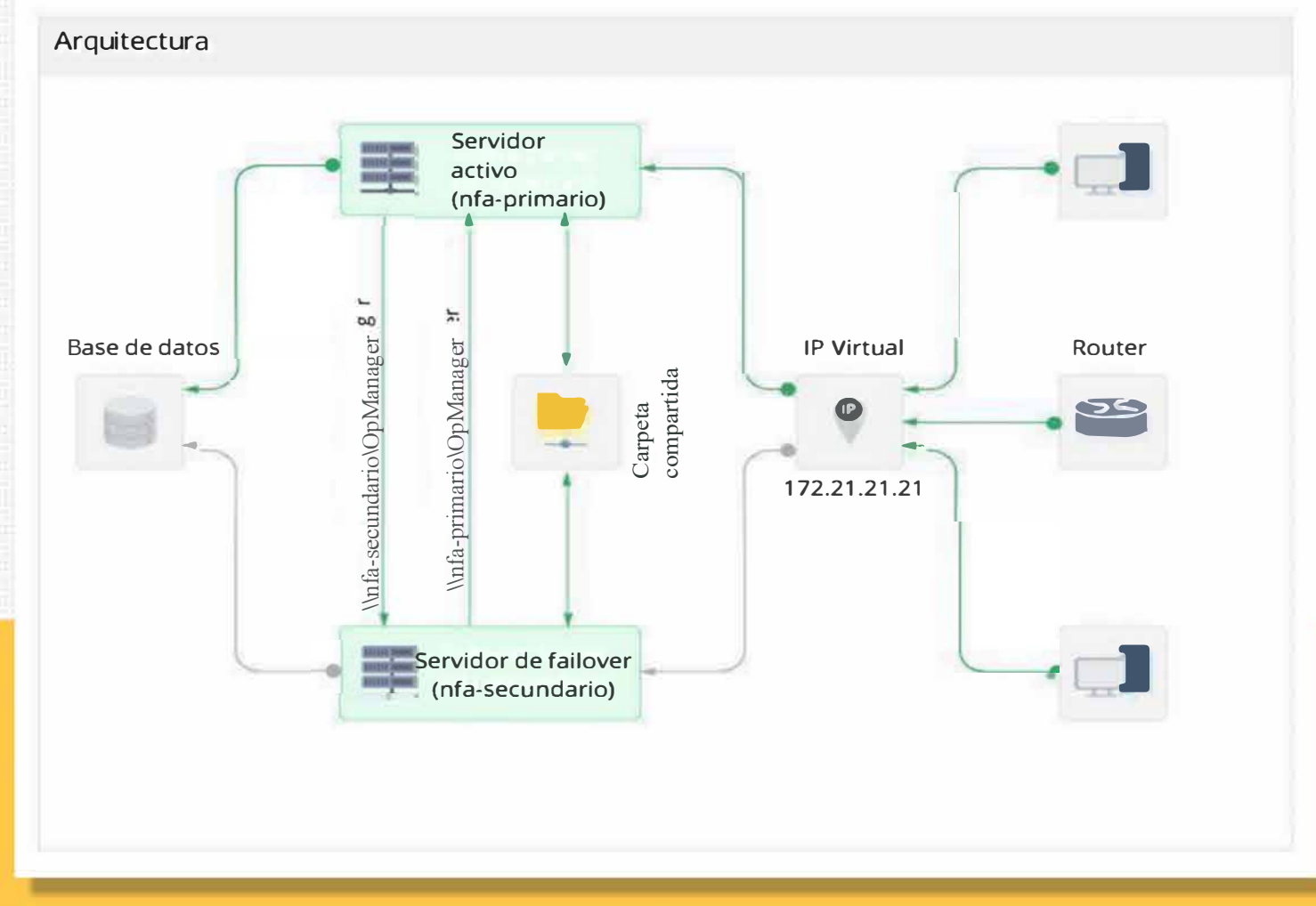
Cree y gestione plantillas de notificación para recibir alertas por correo electrónico / SMS, alarmas web, registrar tickets o traps SNMP / syslogs



Integraciones de terceros

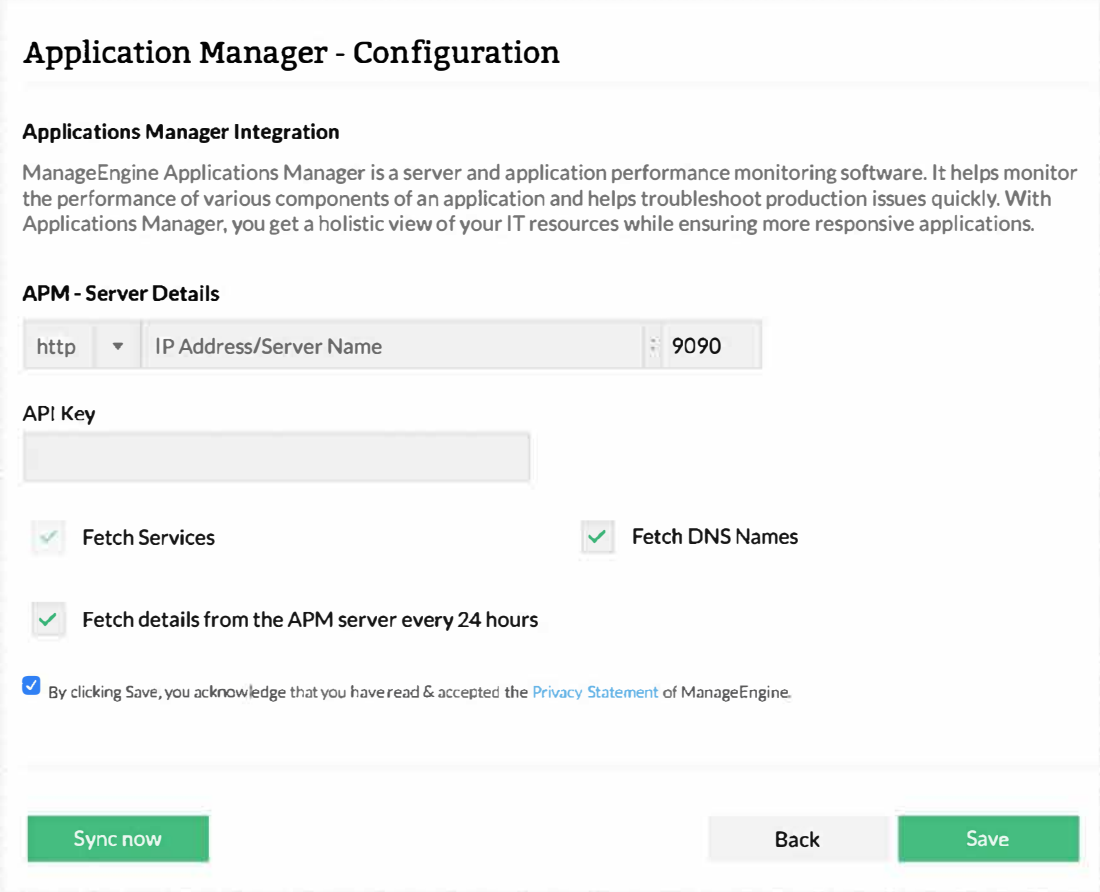


Asegúrese de que su red siempre esté monitoreada con el failover de NetFlow Analyzer



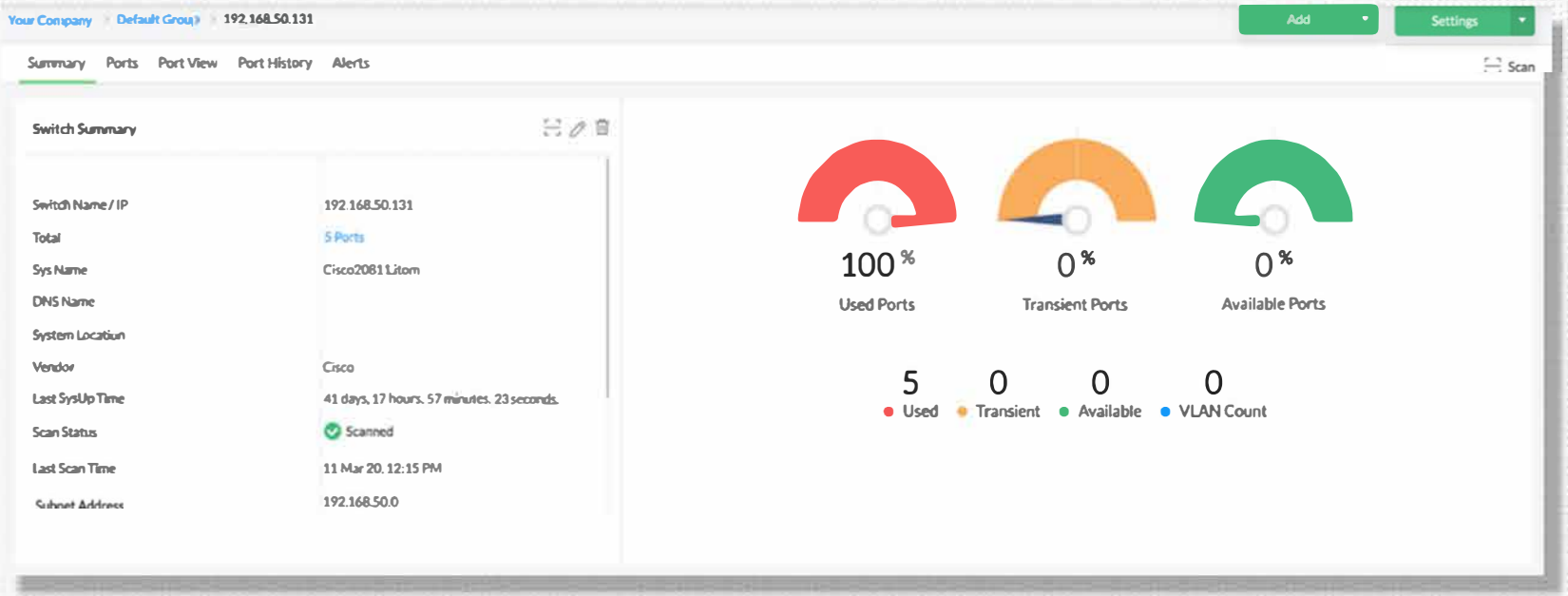
Nuevas actualizaciones e integraciones

Integración con Applications Manager



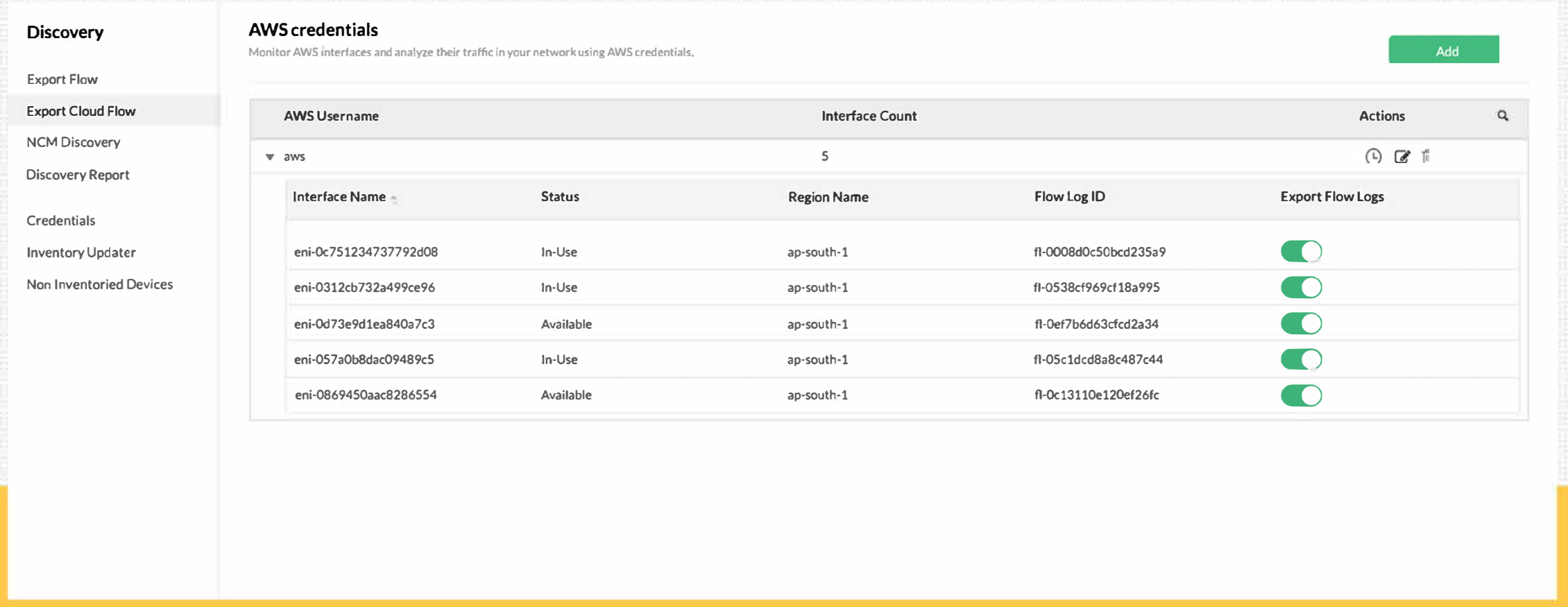
- Sincronice los detalles de la aplicación (puerto, protocolo, IP)
- Categorice la aplicaciones críticas por separado
- Monitoree el tráfico de las aplicaciones por origen, destino, byte y más.

Integración con OpUtils

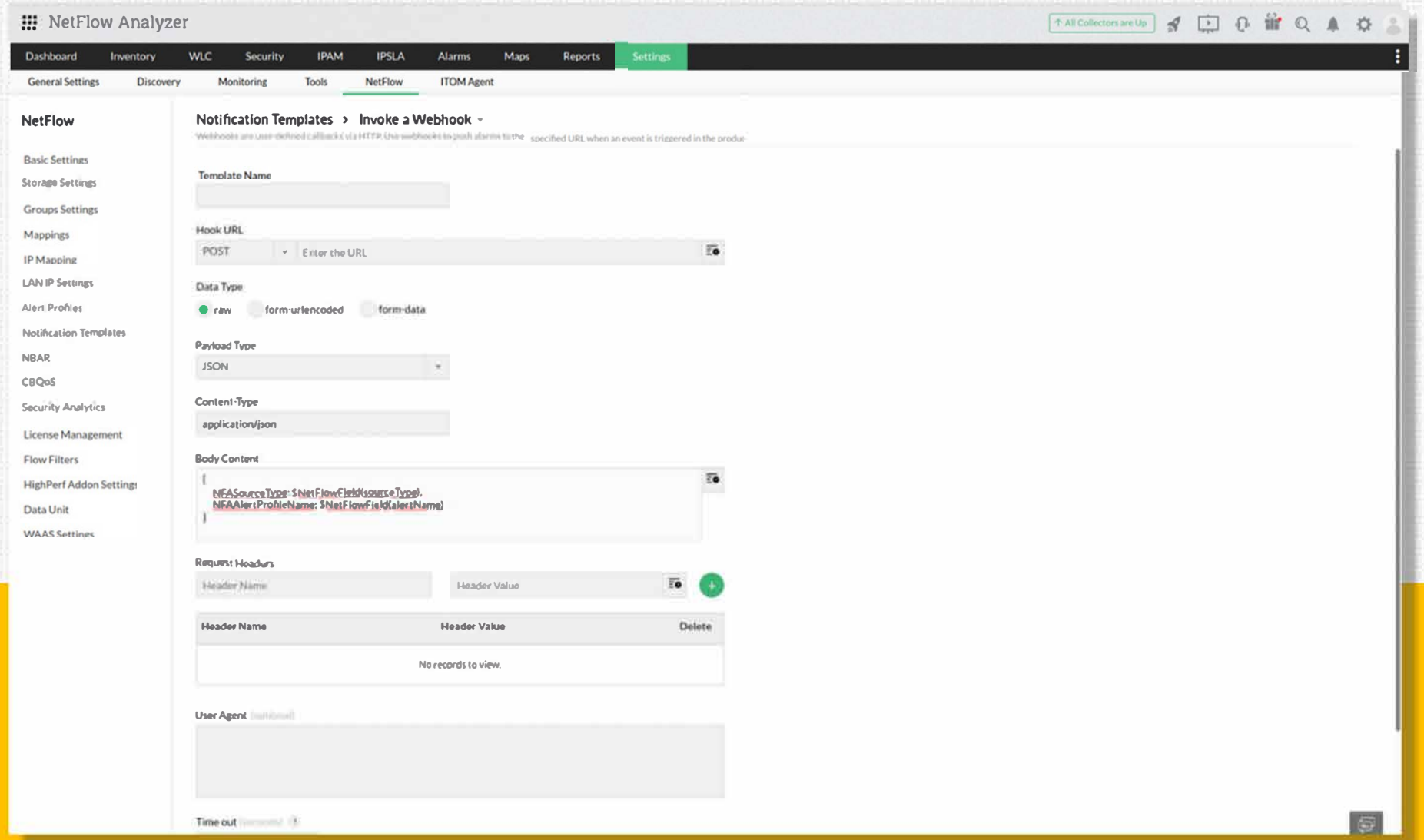


- Visibilidad de los puertos de red
- Capacidad de inspeccionar direcciones IP
- Widgets intuitivos

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

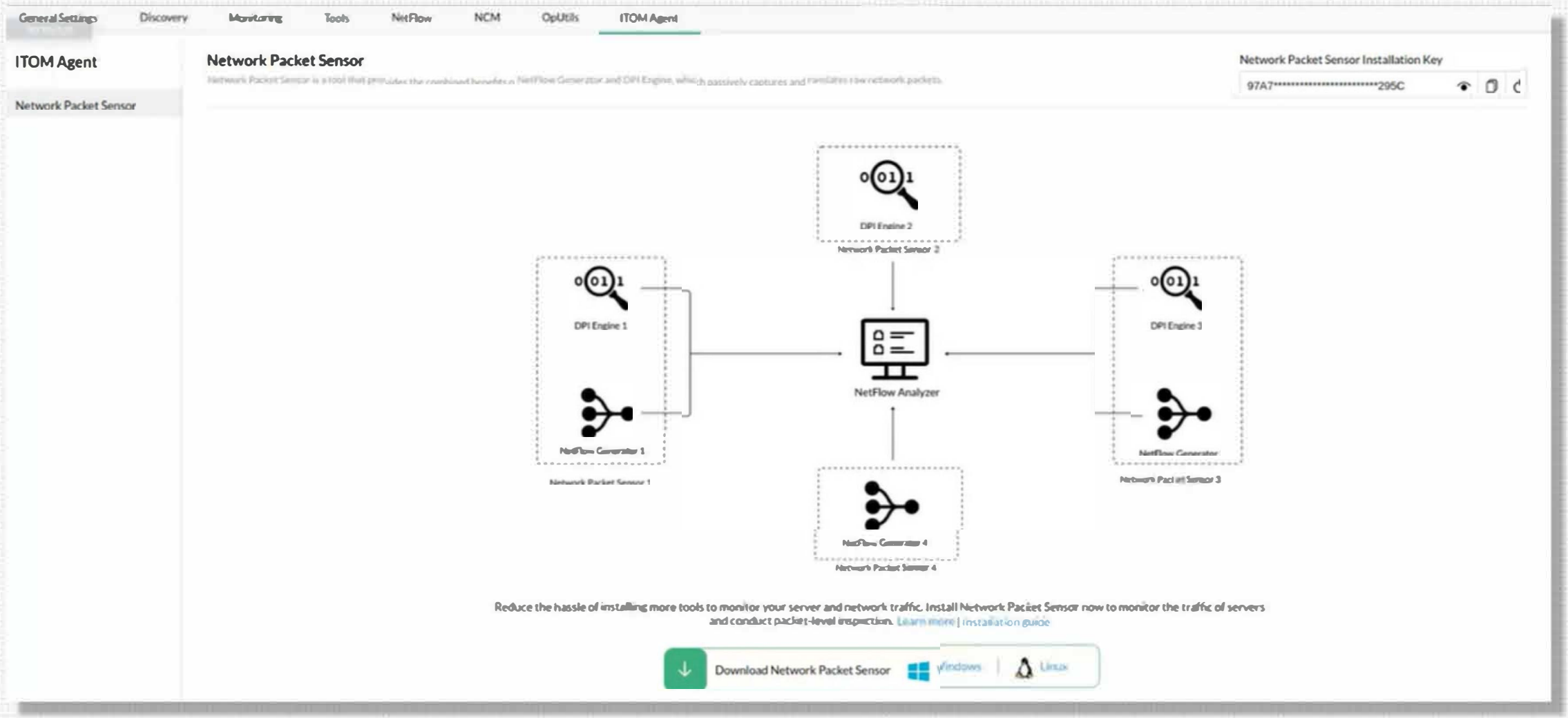


Integración de webhooks con NetFlow Analyzer

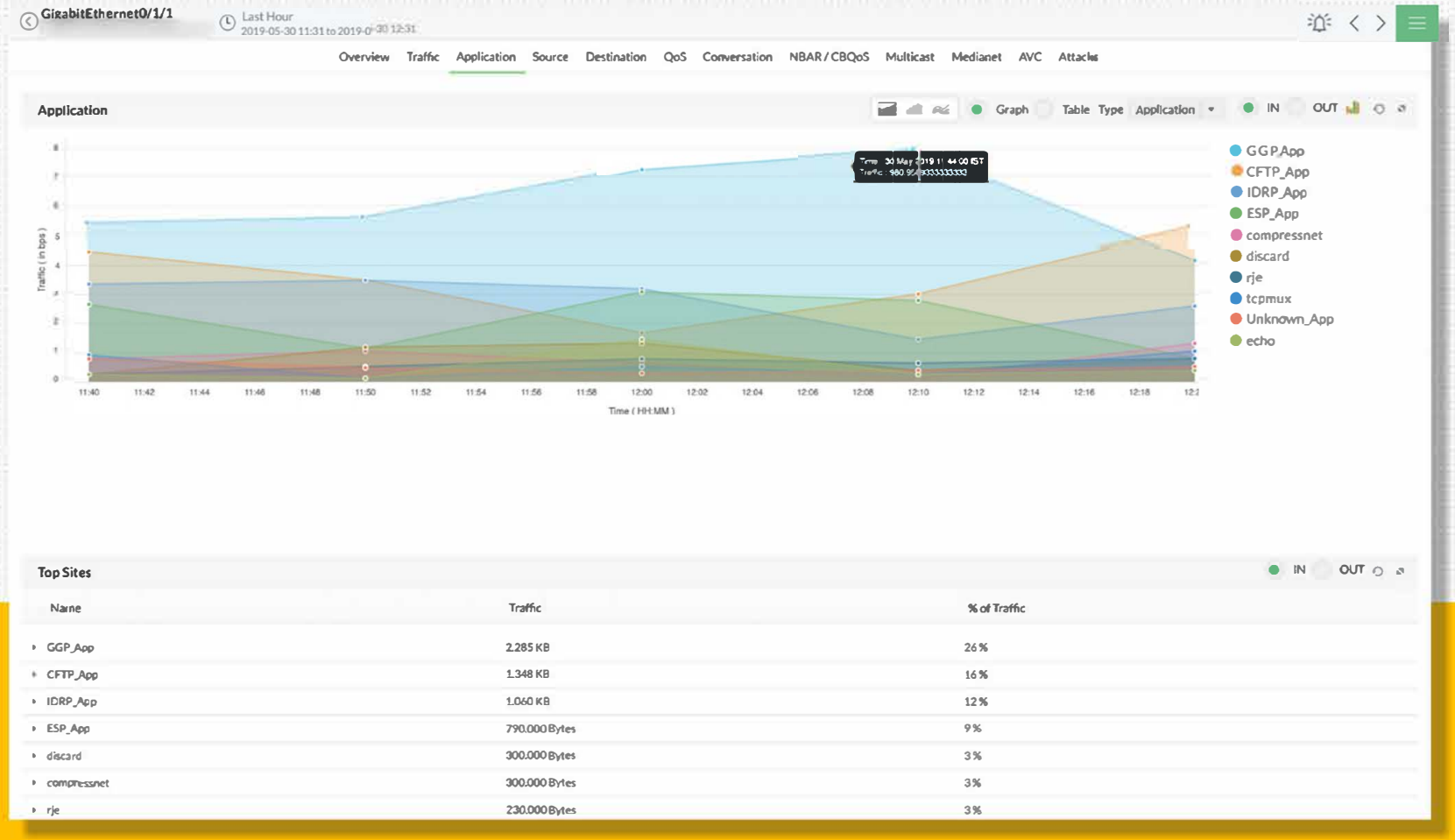


Sensor de paquetes de red

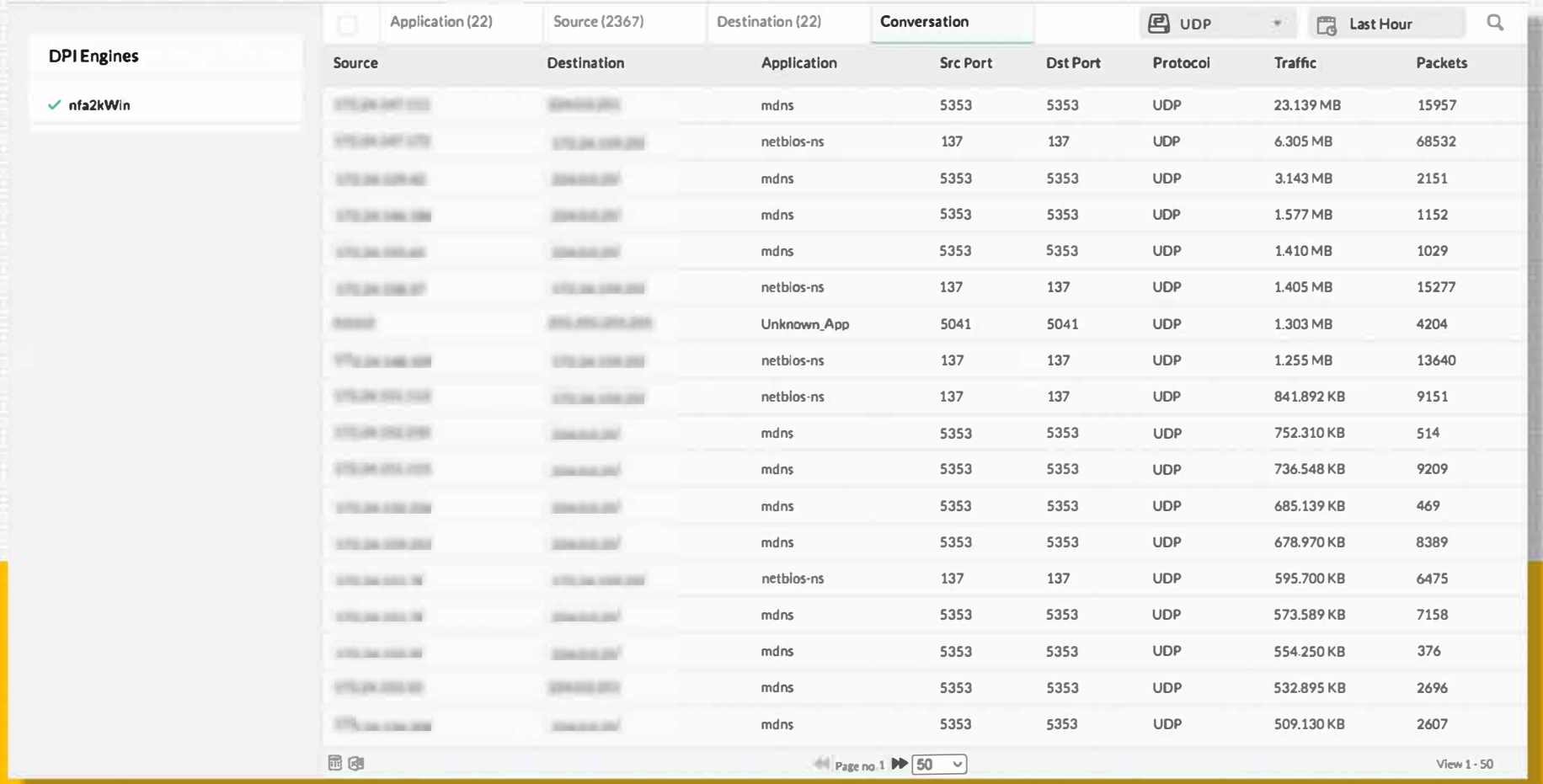
Sensor de paquetes de red (NPS)



Generador de NetFlow



Inspección profunda de paquetes



Controlador de la velocidad de red

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/
@ManageEngineLATAM

ManageEngine
PitStop

forums.manageengine.com/netflowanalyzer

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/