SolarWinds Orion NetFlow Traffic Analyzer

Evaluation Guide

ORION NETFLOW TRAFFIC ANALYZER

Orion NetFlow Traffic Analyzer Evaluation Guide, Version 3.0, 08.28.2008

Acerca de SolarWinds

SolarWinds, Inc desarrolla y comercializa una variedad de herramientas de descubrimiento, supervisión y gestión de redes para adaptarse a los distintos requisitos de los profesionales actuales en el ámbito de la consultoría y la gestión de redes. Los productos SolarWinds siguen marcando la referencia de calidad y rendimiento y han situado la empresa como líder del sector de la tecnología de descubrimiento y gestión de redes. La base de clientes de SolarWinds incluye a más del 45 por ciento de las empresas Fortune 500 y clientes de más de 90 países. Nuestra red global de distribuidores de socios empresariales supera los 100 distribuidores y proveedores.

Contacto con SolarWinds

Puede ponerse en contacto con SolarWinds de diversas formas, entre las cuales:

Equipo	Información de contacto
Ventas	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Asistencia técnica	www.solarwinds.com/support
Foros de usuarios	www.thwack.com

Convenciones

La documentación utiliza convenciones constantes para ayudarle a identificar elementos en la totalidad de la biblioteca impresa y en línea.

Convención	Especificación
Negrita	Elementos de ventanas, entre los cuales botones y campos
Cursiva	Títulos de libros y CD, nombres variables, términos nuevos
`Fuente fija`	Nombres de archivos y directorios, ejemplos de comandos y códigos, texto escrito por el usuario
Corchetes, como en [*valor*]	Parámetros de comandos opcionales
Llaves, como en {*valor*}	Parámetros de comandos requeridos
Disyunción lógica, como en *valor1*|*valor2*	Parámetros de comandos exclusivos, donde sólo se puede especificar una de las opciones

SolarWinds Orion NetFlow Traffic Analyzer Biblioteca de documentación

Los documentos siguientes se incluyen en la biblioteca de documentación de SolarWinds Orion NetFlow Traffic Analyzer:

Documento	Finalidad
Admisnistrator Guide (Guía del administrador)	Proporciona información detallada de instalación, configuración y conceptual.
Ayuda de página	Proporciona ayuda para cada ventana en la interfaz de usuario de Orion NetFlow Traffic Analyzer.
Evaluation guide (Guía de evaluación	Proporciona una introducción a las funciones de Orion Network Performance Monitor, así como instrucciones para la instalación y la configuración inicial.
Guía rápida de inicio	Proporciona escenarios de instalación, configuración y acontecimientos comunes para los cuales Orion NetFlow Traffic Analyzer proporciona una solución simple y eficaz.
Notas de versión	Proporciona información de última hora, problemas conocidos y actualizaciones. Encontrará las últimas Notas de versión en www.solarwinds.com.

Índice

Capítulo 1

Introducción a Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) proporciona una solución de supervisión de fácil uso y adaptable para profesionales de TI encargados de gestionar redes de cualquier tamaño con NetFlor, sFlow o J-Flow habilitado.

Por qué instalar Orion NetFlow Traffic Analyzer

Del mismo modo que crecen las empresas y sus redes, el ancho de banda debe crecer exponencialmente. Todas las modernas industrias conectadas invierten una cantidad significativa de tiempo y dinero para garantizar que dispondrán de suficiente ancho de banda para las aplicaciones y actividades que son importantes para el negocio. Cuando el ancho de banda supera la capacidad actualmente disponible o cuando la demanda parece crecer más allá de las capacidades de su red, entender el uso del ancho de banda ya no es un interés novedoso, sino que se convierte en algo importante decidir si es necesario invertir en más ancho de banda o si unas pautas más estrictas para su uso son suficientes para recuperar el ancho de banda perdido.

Con la llegada de los medios de comunicación audiovisual por Internet, las tecnologías de voz sobre IP (VoIP), los juegos en línea y otras aplicaciones que requieren un uso intensivo del ancho de banda, usted, como ingeniero de red, debe responder a más que a la sencilla pregunta de si la red está operativa o no. Debe responder a por qué la red no está rindiendo todo lo que debería.

Si necesita saber cómo y por quién está siendo utilizado su ancho de banda, Orion NetFlow Traffic Analyzer proporciona una respuesta integrada sencilla. Puede realizar un seguimiento y supervisar con rapidez el uso del ancho de banda de un tipo de tráfico o una aplicación en particular. Por ejemplo, si observa un uso excesivo del ancho banda en una interfaz particular, puede utilizar Orion NetFlow Traffic Analyzer para ver que la reunión de la empresa, que consiste en vídeos por Internet, está consumiento el 80 % del ancho de banda mediante un conmutador en particular. A diferencia de muchos otros productos de análisis de NetFlow, los datos de NetFlow y de red proporcionados por la solución Orion NetFlow Traffic Analyzer no son datos puramente extrapolados, pero están basados en información real recopilada sobre la red por el producto Orion Network Performance Monitor que se encuentra en el centro del Orion NetFlow Traffic Analyzer.

El innovador Orion NetFlow Traffic Analyzer ofrece grandes capacidades de análisis por gráficos y supervisión, combinadas con estadísticas basadas en información detallada, que incluyen:

- Distribución del ancho de banda por tipos de tráfico
- Patrones de uso a través del tiempo
- Identificación y seguimiento del tráfico externo
- Integración rigurosa con estadísticas de rendimiento de la interfaz detalladas

Estas capacidades de supervisión, junto a la personalizable Orion Network Performance Monitor Web Console y a los motores de sondeo, convierten Orion NetFlow Traffic Analyzer en la mejor opción para supervisar su red con NetFlow habilitado.

Por qué utilizar Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer le ofrece la capacidad de supervisar rápida y fácilmente los recursos de red y los patrones de uso con un nivel de detalles personalizable. Las valiosas funciones que se muestran a continuación representan las capacidades principales de Orion NetFlow Traffic Analyzer.

Disponibilidad y rendimiento mejorados

Con Orion NetFlow Traffic Analyzer, puede detectar, diagnosticar y resolver con más rapidez las desaceleraciones e interrupciones de la red.

Planificación de las capacidades analíticas

Orion NetFlow Traffic Analyzer resalta las tendencias en el tráfico de red, permitiéndole anticiparse con inteligencia a los cambios en el ancho de banda para áreas que están experimentando cuellos de botella.

Asignación de recursos de red optimizada

La información proporcionada por Orion NetFlow Traffic Analyzer le permite identificar áreas de su red que están experimentando conexiones limitadas o demasiado sobrecargadas. De este modo puede redirigir el tráfico existente a otras áreas de su red que tienen ancho de banda disponible.

Alineación de recursos de TI con las necesidades de la empresa

Como Orion NetFlow Traffic Analyzer está diseñado con la infraestructura probada Orion Network Performance Monitor, le permite evaluar tanto las necesidades de la red de la empresa en una vista general de alto nivel como los detalles funcionales de interfaces y nodos específicos.

Mayor seguridad de red

Orion NetFlow Traffic Analyzer le proporciona la capacidad de examinar con rapidez y precisión el tráfico de red y, a continuación, localizar y descubrir patrones extraños, comportamientos no deseados y usos anómalos que pueden indicar posibles infecciones de virus, programas bot o software espía.

Una aplicación de supervisión del rendimiento de red y NetFlow todo en uno

Ya puede dejar de pasar de un programa a otro para conseguir una imagen completa del uso, rendimiento y necesidades de su red. Todo lo que necesita para supervisar su red con NetFlow habilitado se encuentra en Orion Network Performance Monitor y Orion NetFlow Traffic Analyzer.

Funciones de la versión 3.0 de Orion NTA

Orion NTA versión 3.0 proporciona las siguientes funciones para mejorar su capacidad de supervisión de los dispositivos con NetFlow habilitado de su red.

Búsqueda por intervalo de dirección IP

Esta versión de Orion NTA proporciona la capacidad de buscar terminales dentro de un intervalo de dirección IP especificado (p. ej.: `10.10.199.1-10.10.199.50`).

Ya está disponible el soporte de flujo adicional

Orion NTA versión 3 admite actualmente los formatos NetFlow v9, sFlow v5 y J-flow para recopilar datos de tráfico de red.

Vistas del tráfico personalizadas

Con el Traffic View Builder incluido en esta versión de Orion NTA, puede filtrar los datos de NetFlow recopilados para crear y acceder a vistas personalizadas. Por ejemplo, puede crear una vista que muestre el tráfico de un dominio específico generado durante las horas de oficina estándar (de 8.00 a 17.00) desde una dirección IP seleccionada.

10 fuentes principales de NetFlow por recurso de uso porcentual

Un nuevo recurso de la vista NetFlow Summary (Resumen de NetFlow) enumera las fuentes de NetFlow supervisadas por uso porcentual.

Vistas de rendimiento de la calidad del servicio (QoS)

Orion NTA versión 3 le permite ver con facilidad su tráfico de red general segmentado por métodos de clase de servicio como, por ejemplo, Tipo de servicio o DSCP. También puede cuantificar y visualizar la cantidad de ancho de banda consumido por cada uno de sus niveles de QoS indicados, incluidos los datos de voz y vídeo.

Agrupación de aplicaciones de puertos

Esta versión de Orion NTA le proporciona la capacidad de asignar una aplicación que utiliza varios puertos de red a un grupo para calcular el rendimiento de la aplicación.

5 recursos principales de toda la red

Ya están disponibles los nuevos 5 recursos principales de tráfico en toda la red que enumeran grupos de direcciones IP, aplicaciones, conversaciones, países, terminales, tipos de servicio, transmisores, receptores y protocolos.

Integración completa de los recursos de NetFlow en las vistas de Orion

Los recursos de NetFlow pueden agregarse fácilmente a las vistas de Orion de manera automática.

Función de búsqueda de DNS inmediata

Realice búsquedas de DNS manuales sin esperar una actualización de DNS programada.

Cómo funciona Orion NetFlow Traffic Analyzer

Los dispositivos con NetFlow habilitado proporcionan abundante información de tráfico relacionado con la IP. Orion NetFlow Traffic Analyzer recopila estos datos de NetFlow, los correlaciona en un formato utilizable y los presenta, con datos de rendimiento de red detallados recopilados por SolarWinds Orion Network Performance Monitor, ya que lee con facilidad gráficos e informes sobre el uso del ancho de banda de su red, dentro de su red y desde su red. Estos informes le ayudan a supervisar el ancho de banda, realizar un seguimiento de las conversaciones entre terminales internas y externas, analizar el tráfico y planificar las necesidades de capacidad del ancho de banda.

Capítulo 2

Instalación de Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) presenta un procedimiento de instalación guiado por un asistente. Para un producto de calidad empresarial, los requisitos son simbólicos.

Nota: los datos de NetFlow son ampliables y pueden consumir grandes cantidades de memoria de la base de datos en un período de tiempo relativamente corto. Esto es cierto incluso para las redes más pequeñas. Como resultado, SolarWinds recomienda encarecidamente mantener la base de datos de SQL Server y la instalación de su Orion NPM/NTA en servidores físicos diferentes.

Requisitos

El servidor que utilice para alojar su solución de NetFlow deberá admitir Orion NPM y Orion NTA ya que Orion NTA está diseñado a partir de Orion NPM y lo amplía. Los siguientes apartados proporcionan los requisitos mínimos de configuración.

Requisitos de software

Los siguientes requisitos de software asumen que su evaluación de Orion NTA está instalada en un servidor que ejecuta la versión 9.0 de Orion NPM. Si desea evaluar la versión 3.0 de Orion NTA en una instalación de la versión 8.5.1 de Orion NPM, póngase en contacto con SolarWinds en sales@solarwinds.com.

Nota: SQL Express y MSDE limitan el tamaño de la base de datos a 4 GB y 2 GB respectivamente. Por esta razón, SolarWinds no admite su uso con Orion NTA en entornos de producción.

Software	Requisitos
Sistema operativo	Windows Server 2003 (32 bits o 64 bits) con R2, con IIS instalado. SolarWinds recomienda que los administradores de Orion NPM dispongan de privilegios de administrador local para garantizar la completa funcionalidad de las herramientas locales de Orion NPM. Los usuarios limitados a la consola web no requieren privilegios de administrador. **Nota:** SolarWinds no admite las instalaciones de Orion NTA en Windows XP en entornos de producción. Si está instalando Orion NTA en Windows XP, debe confirmar que se han habilitado la memoria compartida, las canalizaciones con nombre y TCP/IP en las bases de datos remotas.

Software	Requisitos
Servidor web	Microsoft IIS versión 6.0 y superior. Las especificaciones de DNS requieren que los nombres de anfitrión estén formados por caracteres alfanuméricos (A–Z, 0–9), el signo de restar (–) y puntos (.). No se permiten caracteres de guión bajo (_). Para obtener más información, consulte *RFC 952*. **Nota:** SolarWinds no recomienda ni admite la instalación de Orion NTA en el mismo servidor ni el uso del mismo servidor de base de datos que un servidor de Blackberry Research in Motion (RIM).
.NET Framework	Versión 3.5 o superior
SNMP Trap Services	Componente de herramientas de supervisión y administración del sistema operativo de Windows
SQL Server	SQL Server 2000 SP4, Standard o Enterprise SQL Server 2005 Standard o Enterprise La base de datos debe admitir la autenticación SQL o de modo mixto. **Nota:** SQL Server Express no puede gestionar bases de datos superiores a 4 GB. Está limitado a un único procesador y no utiliza más de 1 GB de memoria RAM. Aunque puede utilizarse para supervisar una o dos interfaces con fines evaluativos, SolarWinds no recomienda su uso para redes de tamaño superior que necesiten bases de datos mayores.
Web Console Browser	Microsoft Internet Explorer versión 6 o superior con secuencia de comandos Mozilla Firefox 2.0 o superior

Requisitos de hardware

Los siguientes requisitos de hardware asumen que su evaluación de Orion NTA está instalada en un servidor que ejecuta la versión 9.0 de Orion NPM. Si desea evaluar la versión 3.0 de Orion NTA en otra versión de Orion NPM, póngase en contacto con SolarWinds en sales@solarwinds.com.

Nota: Orion NTA necesita que el puerto TCP 17777 esté abierto tanto para enviar como para recibir tráfico entre Orion NPM y cualquier módulo Orion, incluido Orion NTA.

Advertencia: las únicas configuraciones de RAID que deben utilizarse en una instalación de Orion NTA son 0, 1, 0+1, ó 1+0. Debido a las necesidades de alta velocidad y gran memoria de las transacciones de datos de NetFlow, SolarWinds recomienda que no se utilice otras configuraciones de RAID o SAN ya que pueden provocar pérdidas de datos y una reducción significativa del rendimiento.

Hardware	Requisitos
CPU	3 GHz o más rápido
RAM	2 GB o más
Espacio en la unidad de disco duro asignado	5 GB o más. Se recomienda el uso de las configuraciones de RAID 0, 1, 0+1 ó 1+0. No se recomienda el uso de otras configuraciones de RAID o SAN.
Dispositivos de NetFlow	Dispositivos Cisco con la versión 5 ó 9 de NetFlow **Nota:** Orion NTA sólo reconoce las plantillas de la versión 9 de NetFlow que incluye todos los campos utilizados por la versión 5 de NetFlow.
J-Flow	Dispositivos de red con J-Flow
Dispositivos sFlow	Dispositivos sFlow con la versión 5 de sFlow

Requisitos de Virtual Machine (Máquina virtual)

Las instalaciones de Orion NTA en máquinas virtuales de VMware y servidores virtuales de Microsoft están totalmente admitidas si se cumplen los siguientes requisitos de configuración mínimos en cada máquina virtual.

Configuración de máquina virtual	Requisitos
Velocidad de CPU	3,0 GHz
Espacio en la unidad de disco duro asignado	5 GB **Nota:** se recomienda RAID 1+0; debido a los elevados requisitos I/O no se recomienda RAID 5.
Memoria	2 GB
Interfaz de red	Cada instalación de Orion NPM debería tener su propia tarjeta de interfaz dedicada. **Nota:** dado que Orion NPM utiliza SNMP para supervisar la red, si no puede dedicar una tarjeta de interfaz de res a la instalación de Orion NPM, puede experimentar vacíos en los datos de supervisión debido a la baja prioridad asignada generalmente al tráfico SNMP.

Para obtener más información acerca de los requisitos de Orion NPM, consulte “Requisitos” en la *SolarWinds Orion Network Performance Monitor Administrator Guide*.

SQL Server y SQL Server Express con Orion NTA

Debido al hecho de que los datos de NetFlow son ampliables y pueden consumir grandes cantidades de memoria de la base de datos en un período de tiempo relativamente corto, SolarWinds no recomienda el uso de archivos de base de datos SQL Server Express para Orion NTA. En su lugar, SolarWinds recomienda el uso de una versión de producción de SQL Server.

Las evaluaciones de Orion NTA son una excepción limitada. Con fines evaluativos, Orion NPM y Orion NTA pueden admitir el uso de archivos de base de datos SQL Server Express 2005. SQL Express le permite evaluar Orion NTA con una base de datos real y se encuentra disponible, de forma gratuita, en Microsoft. Sin embargo, SolarWinds no recomienda su uso con Orion NTA en ningún entorno de producción por las siguientes razones:

- SQL Express no puede gestionar bases de datos superiores a 4 GB.
- SQL Express está limitado a un único procesador.
- SQL Express no puede utilizar más de 1 MB de memoria RAM.

Nota: para entornos de producción, las instalaciones de Orion NPM y Orion NTA deberían utilizar un archivo de base de datos SQL Server instalado en un servidor diferente.

Instalación de Orion NetFlow Traffic Analyzer

Realice el procedimiento siguiente para instalar Orion NetFlow Traffic Analyzer. Debe proporcionar su puerto de tráfico NetFlow y confirmar que está habilitado y enviando datos de tráfico NetFlow para completar la instalación.

Nota: el siguiente procedimiento asume que ya ha instalado la versión 9.0 de Orion Network Performance Monitor en el servidor en el que desea instalar Orion NetFlow Traffic Analyzer. Si desea evaluar la versión 9.0 de Orion Network Performance Monitor, póngase en contacto con SolarWinds en la dirección de correo electrónico sales@solarwinds.com.

Para instalar Orion NetFlow Traffic Analyzer:

1. Inicie sesión en el servidor de Orion Network Performance Monitor que desea utilizar para el análisis del tráfico de NetFlow.
2. ***Si instala NetFlow Traffic Analyzer en un servidor terminal,*** realice los siguientes pasos antes de continuar la instalación para asegurarse de que NetFlow Traffic Analyzer está instalado correctamente:

a. Haga clic en **Start** (Inicio) **> Control Panel** (Panel de control) **> Add or Remove Programs** (Agregar o quitar programas).

b. Haga clic en **Add New Programs** (Agregar programas nuevos).

c. En la ventana Instalar programa desde disquete o CD-ROM, haga clic en **CD or Floppy** y, a continuación, haga clic en **Next** (Siguiente).

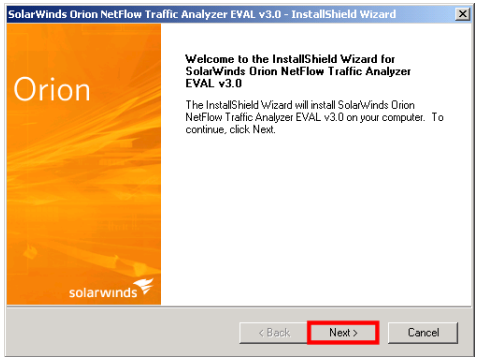
3. ***Si ha descargado el producto del sitio web de SolarWinds,*** realice los pasos siguientes:

   a. Navegue hasta la ubicación de su archivo `.zip` descargado y extraiga el paquete de evaluación a una ubicación adecuada.

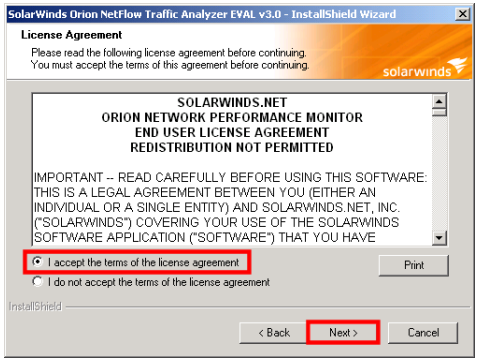
   b. Ejecute el archivo ejecutable de evaluación de SolarWinds Orion NTA.

4. ***Si ha recibido medios físicos,*** navegue hasta el archivo ejecutable de evaluación de SolarWinds Orion NTA y ejecútelo.

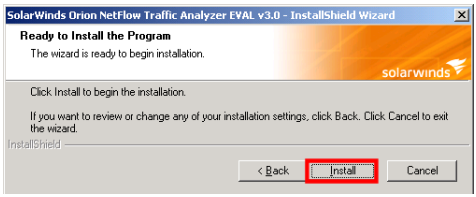
5. Revise el texto de bienvenida y haga clic en **Next** (Siguiente).



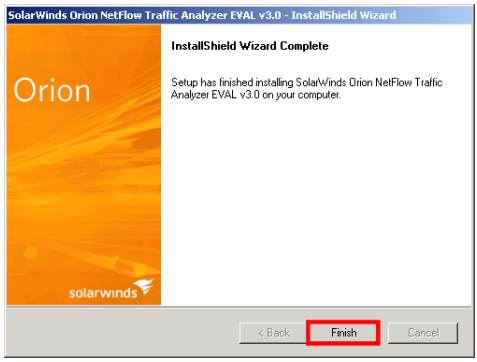
6. Seleccione **I accept the terms of the license agreement** (Acepto las condiciones del acuerdo de licencia) y haga clic en **Next** (Siguiente).



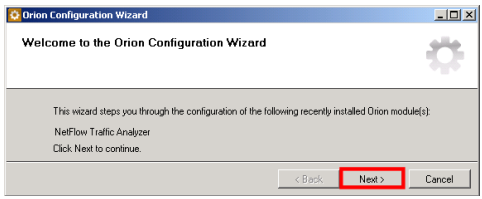
7. En la ventana Ready to Install the Program (Preparado para instalar el programa), haga clic en **Install** (Instalar).



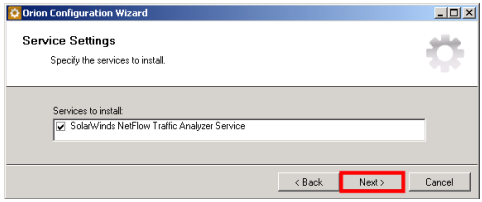
8. Cuando el InstallShield Wizard finalice, haga clic en **Finish** (Finalizar) para salir del asistente.



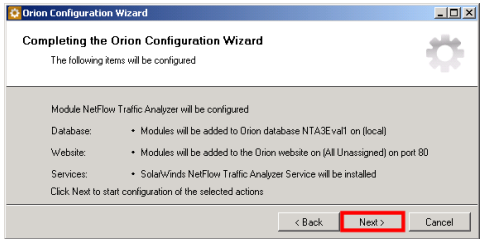
9. ***Si se le indica que reinicie su servidor,*** seleccione una de las siguientes opciones, de la forma necesaria:
   - ***Si está instalando Orion NTA en un servidor terminal,*** haga clic en **No**.
   - ***Si no está instalando Orion NTA en un servidor terminal,*** haga clic en **Yes** (Sí).
10. ***Si el Configuration Wizard (Asistente de configuración) no se inicia automáticamente,*** haga clic en **Start** (Inicio) **> All Programs** (Todos los programas) **> SolarWinds Orion > Configuration Wizard** (Asistente de configuración).
11. Revise el texto de bienvenida y haga clic en **Next** (Siguiente).



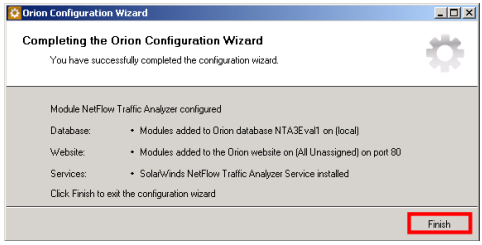
12. Asegúrese de que está marcado **SolarWinds NetFlow Traffic Analyzer Service** en la ventana Service Settings (Configuraciones del servicio) y, a continuación, haga clic en **Next** (Siguiente).



13. Revise el resumen de la configuración y haga clic en **Next** (Siguiente).



14. Una vez completado el Configuration Wizard (Asistente de configuración) haga clic en **Finish** (Finalizar).



Habilitación del análisis del tráfico de NetFlow

Para empezar a analizar los datos de NetFlow disponibles producidos por dispositivos de su red, debe agregar una interfaz con NetFlow habilitado a su base de datos de Orion o supervisar una interfaz agregada anteriormente que sea capaz de generar datos de NetFlow. Para poder supervisar los dispositivos con NetFlow habilitado en Orion NTA, estos deben haberse agregado a la base de datos de Orion con anterioridad.

Nota: la adición de sus interfaces y dispositivos de NetFlow a la base de datos de Orion y la adición de sus interfaces y dispositivos de NetFlow a Orion NTA como fuentes de NetFlow son procedimientos independientes, detallados en apartados independientes, como se muestra a continuación.

Agregar dispositivos e interfaces a la base de datos de Orion

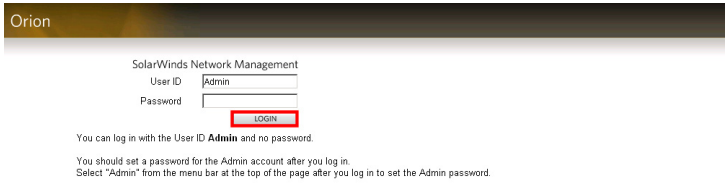
El siguiente procedimiento agrega un dispositivo y sus interfaces a la base de datos de Orion mediante la función Web Node Management de Orion Web Console. Si su dispositivo de NetFlow ya está configurado para enviar datos de NetFlow, Orion NTA empezará a recibir datos de NetFlow en cuanto su dispositivo se agregue a la base de datos de Orion.

Nota: para obtener más información acerca de la designación de las fuentes de NetFlow en Orion NTA, consulte “Agregar fuentes de NetFlow a NetFlow Traffic Analyzer” en la página 18.

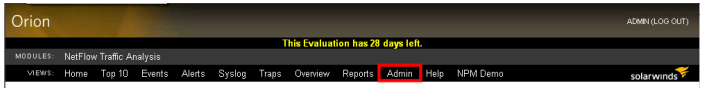
Para agregar dispositivos e interfaces con NetFlow habilitado a la base de datos de Orion:

1. Inicie sesión en el servidor de Orion NPM que aloja su instalación de Orion NTA.
2. Haga clic en **Start** (Inicio) **> SolarWinds Orion > Orion Web Console**.
3. Inicie sesión en Orion Web Console como administrador.

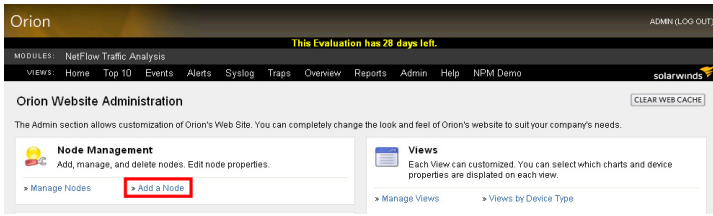
   Nota: si todavía no ha configurado otra contraseña de administrador, puede iniciar sesión con `Admin` como **User ID** (ID de usuario) y sin contraseña.



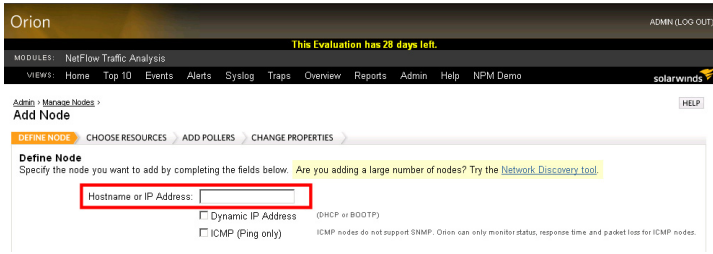
4. Haga clic en **Admin** en la barra de herramientas Views (Vistas).



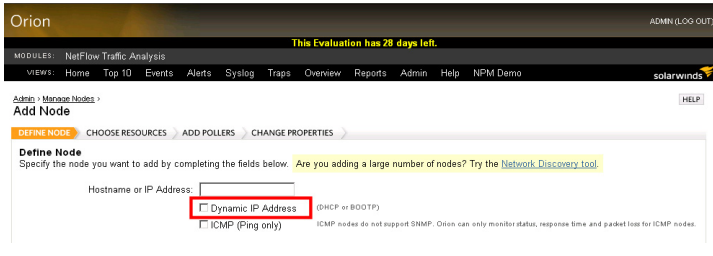
5. Haga clic en **Add a Node** (Agregar nodo) en la agrupación Node management (Gestión de nodos).



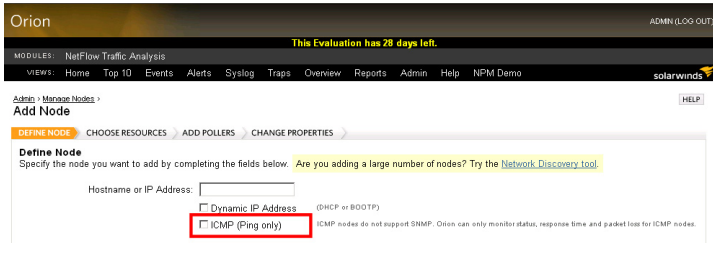
6. Proporcione el nombre de anfitrión o la dirección IP del dispositivo con NetFlow habilitado que desee agregar en el campo **Hostname or IP Address** (Nombre de anfitrión o dirección IP).



7. ***Si la dirección IP del dispositivo que agrega está asignada dinámicamente (DHCP o BOOTP),*** marque **Dynamic IP Address** (Dirección IP dinámica).

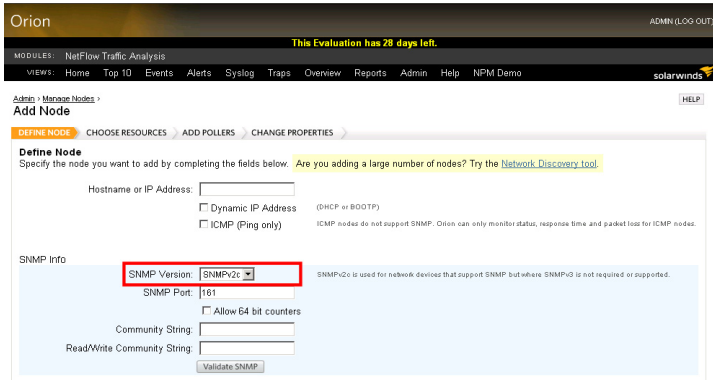


8. Asegúrese de que **ICMP (Ping only)** (ICMP sólo Ping) no está marcado.



9. Seleccione la **SNMP Version** (Versión SNMP) del nodo agregado.

   Nota: Orion NPM utiliza **SNMPv2c** por defecto. Si su nuevo dispositivo admite o requiere las funciones de seguridad ampliada de SNMPv3, seleccione **SNMPv3**.



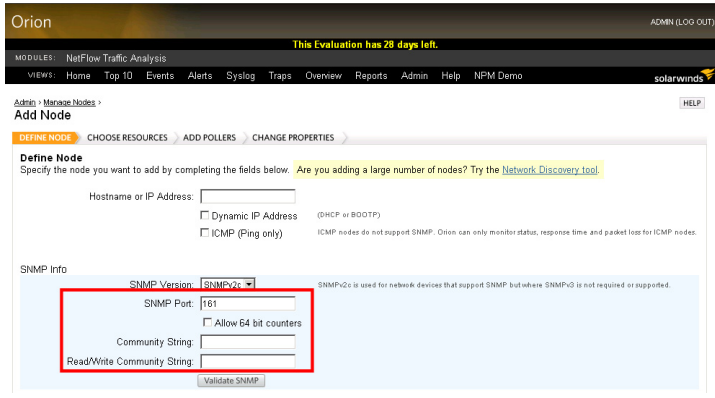
10. ***Si ha seleccionado*** **SNMPv2c**, realice los pasos siguientes:

    a. ***Si el puerto SNMP del nodo agregado no es la opción predeterminada de Orion NPM de 161,*** proporcione el número de puerto actual en el campo **SNMP Port** (Puerto SNMP).

    b. ***Si el nodo agregado es compatible con contadores de 64 bits y desea utilizarlos,*** marque **Allow 64 bit counters** (Permitir contadores de 64 bits).

    c. Proporcione cadenas de comunidad válidas para el nodo agregado.

       Nota: la **Read/Write Community String** (Cadena de comunidad de lectura/escritura) es opcional, pero Orion NPM sí requiere la **Community String** (Cadena de comunidad) `public`, como mínimo.



11. ***Si ha seleccionado* SNMPv3,** realice los pasos siguientes:

    a. ***Si el puerto SNMP del nodo agregado no es la opción predeterminada de Orion NPM de 161,*** proporcione el número de puerto actual en el campo **SNMP Port** (Puerto SNMP).

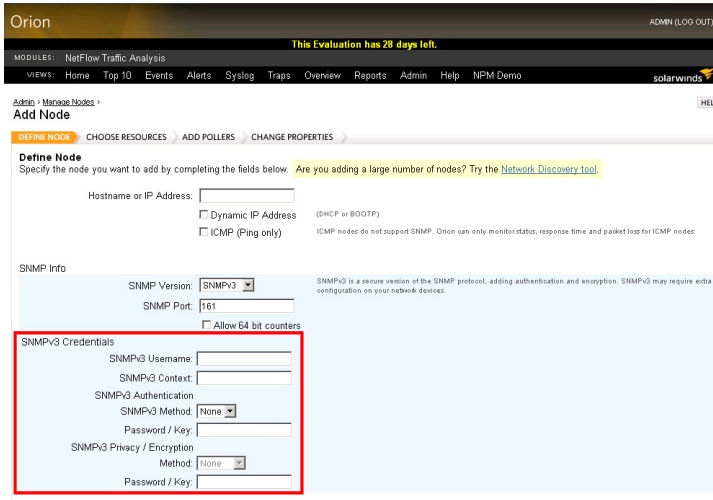
    b. ***Si el nodo agregado es compatible con contadores de 64 bits y desea utilizarlos,*** marque **Allow 64 bit counters** (Permitir contadores de 64 bits).

       Nota: Orion NPM es totalmente compatible con el uso de contadores de 64 bits, aunque estos contadores de alta capacidad pueden presentar comportamientos erráticos en función de la implementación del fabricante. Si advierte resultados peculiares al utilizar esos contadores, utilice la vista Node Details (Información de nodos) para inhabilitar el uso de contadores de 64 bits para el dispositivo y póngase en contacto con el fabricante de hardware.

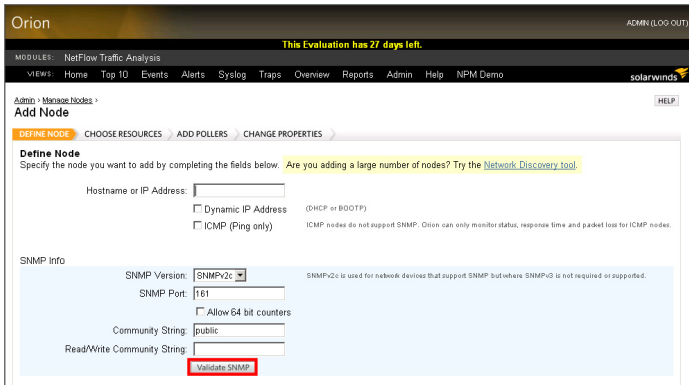
    c. Proporcione la siguiente configuración de **SNMP Credentials** (Credenciales SNMP), **Authentication** (Autenticación) y **Privacy/Encryption** (Privacidad/Cifrado):

       - **SNMPv3 Username** (Nombre de usuario SNMPv3)
       - **SNMPv3 Context** (Contexto SNMPv3)
       - **SNMPv3 Authentication Method** (Método de autenticación SNMPv3)
       - **SNMPv3 Authentication Password/Key** (Clave/Contraseña de autenticación SNMPv3)
       - **SNMPv3 Privacy/Encryption Method** (Método de Privacidad/Cifrado SNMPv3)
       - **SNMPv3 Privacy/Encryption Password/Key** (Clave/Contraseña de Privacidad/Cifrado SNMPv3)

    Nota: para los fines de esta evaluación, no se requieren las **Read/Write SNMPv3 Credentials** (Credenciales SNMPv3 de lectura/escritura).



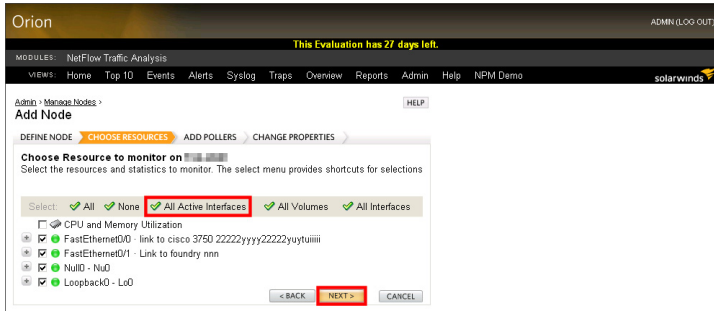
12. Haga clic en **Validate SNMP** (Validar SNMP) después de introducir todas las credenciales SNMP requeridas.



13. Tras asegurarse de que sus credenciales SNMP son válidas, haga clic en **Next** (Siguiente).

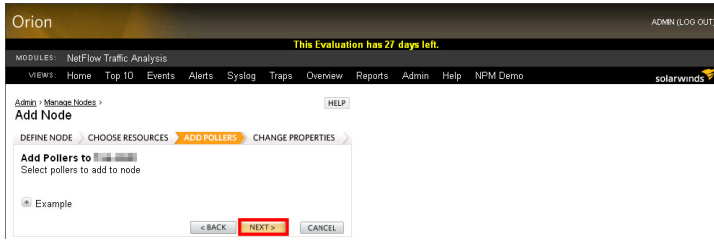
14. Marque las interfaces que desee que Orion NTA supervise y haga clic en **Next** (Siguiente).

Nota: si no sabe qué interfaces tienen NetFlow habilitado, haga clic en **All Interfaces** (Todas las interfaces) para seleccionar todas las interfaces.

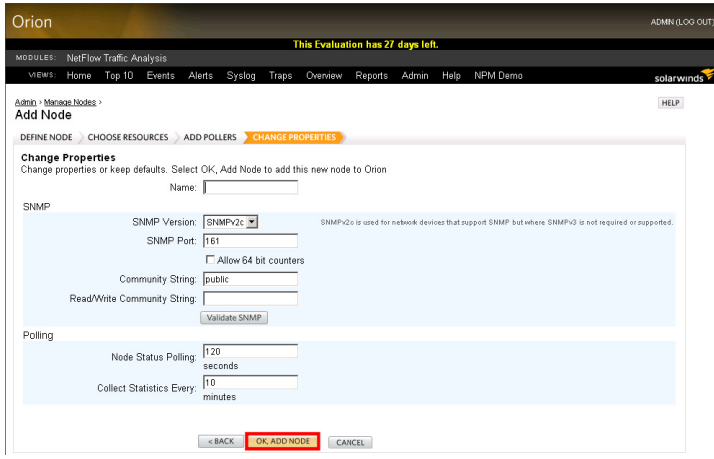


15. Para los fines de esta evaluación, haga clic en **Next** (Siguiente) en la vista Add Pollers (Agregar sondeadores).

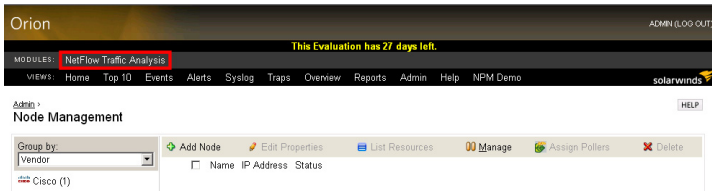
Nota: para obtener más información sobre el uso o definición de los sondeadores, consulte la *SolarWinds Orion Network Performance Monitor Administrator Guide*.



16. Haga clic en **OK, Add node** (Aceptar, Agregar nodo) en la vista Change Properties (Cambiar propiedades).



17. Haga clic en **NetFlow Traffic Analysis** (Análisis del tráfico de NetFlow) en la barra de herramientas Modules (Módulos).



La siguiente sección proporciona los pasos requeridos para empezar a recibir datos de NetFlow desde los dispositivos con NetFlow habilitado de su red.

Agregar fuentes de NetFlow a NetFlow Traffic Analyzer

Una vez agregados su dispositivo con NetFlow habilitado y sus interfaces a Orion NPM, debe establecer el dispositivo como una fuente de NetFlow. El siguiente procedimiento proporciona los pasos requeridos para agregar fuentes de NetFlow a Orion NTA.

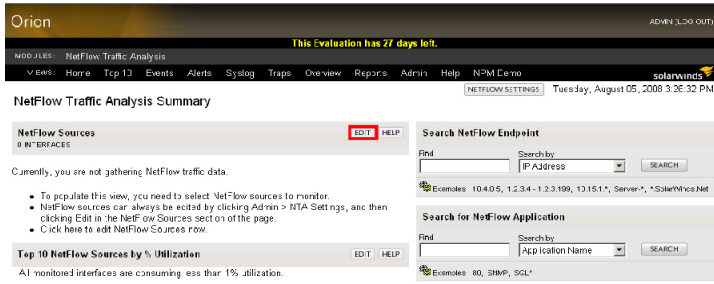
Nota: Orion NTA sólo reconoce las plantillas de la versión 9 de NetFlow que incluye todos los campos utilizados por la versión 5 de NetFlow.

Para agregar interfaces y dispositivos de NetFlow a NetFlow Traffic Analyzer:

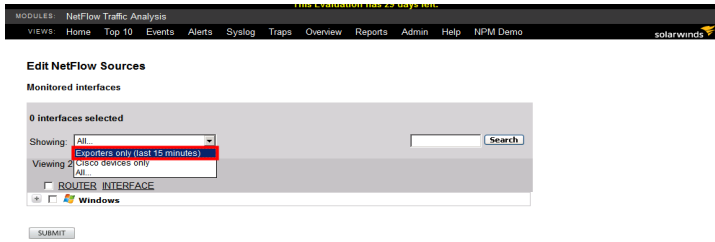
1. Inicie sesión en el servidor de Orion NPM que aloja Orion NetFlow Traffic Analyzer.
2. Haga clic en **Start** (Inicio) **> All Programs** (Todos los programas) **> SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Inicie sesión en Orion Web Console como administrador.

   Nota: si todavía no ha configurado otra contraseña de administrador, puede iniciar sesión con `Admin` como **User ID** (ID de usuario) y sin contraseña.

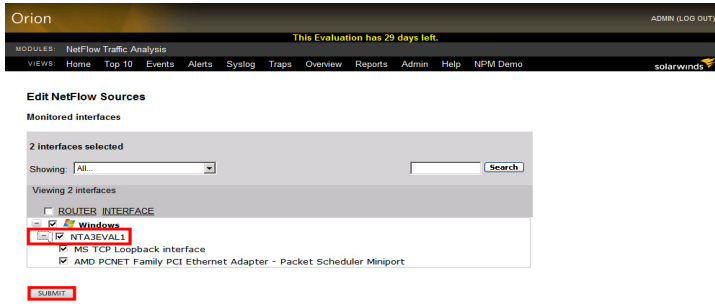
4. Haga clic en **Edit** (Editar) en el encabezamiento del recurso NetFlow Sources (Fuentes de NetFlow).



5. Seleccione **Exporters Only (last 15 minutes)** [Sólo exportadores (últimos 15 minutos)] en el menú Showing (Visualización).



6. Amplíe la lista de dispositivos para ver todos los nodos supervisados, marque los nodos superiores de las interfaces que desee que Orion NTA supervise y, a continuación, haga clic en **Submit** (Enviar).



Como resultado, Orion NTA recibirá los datos de tráfico significativos y los mostrará en la Orion Web Console transcurridos unos minutos.

Capítulo 3

Orion NetFlow Traffic Analyzer Visita rápida

Las funciones y la flexibilidad que Orion NetFlow Traffic Analyzer ofrece proporcionan una percepción detallada de la cantidad y la calidad del tráfico de su red. Los apartados de este capítulo se complementan, de forma secuencial, para mostrarle las funciones clave de Orion NetFlow Traffic Analyzer. Este capítulo es especialmente útil si se lee y sigue de principio a fin. El empieza con una vista general de los recursos disponibles de manera inmediata en la vista NetFlow Traffic Analysis Summary (Resumen del análisis del tráfico de NetFlow) y continúa con resúmenes de las vistas de Orion NTA más utilizadas.

Nota: puede encontrar casos de uso exhaustivos, incluidos los acontecimientos que incorporan otras herramientas de SolarWinds, en el capítulo final de esta Evaluation Guide. Para obtener más información, consulte “Uso de Orion NetFlow Traffic Analyzer” en la página 41.

Iniciar Orion NetFlow Traffic Analyzer

Para iniciar Orion NetFlow Traffic Analyzer, haga clic en **Start** (Inicio) **> All Programs** (Todos los programas) **> SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**. Para obtener más información acerca de la instalación y configuración de Orion NTA, consulte “Instalación de Orion NetFlow Traffic Analyzer” en la página 5.

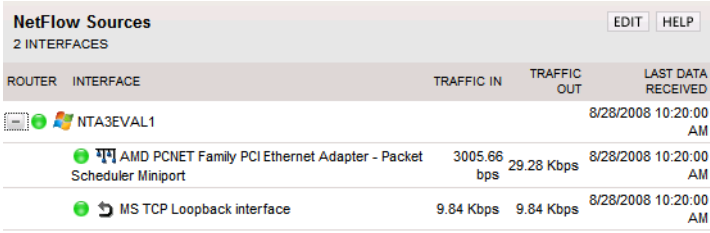
El resumen del análisis del tráfico de NetFlow

Al ejecutar Orion NetFlow Traffic Analyzer, el NetFlow Traffic Analysis Summary (Resumen del análisis del tráfico de NetFlow) es la primera vista que se muestra. Esta vista proporciona una percepción de las condiciones del tráfico de datos de toda su red. Los siguientes recursos están incluidos en la vista NetFlow Traffic Analysis Summary (Resumen del análisis del tráfico de NetFlow) por defecto.

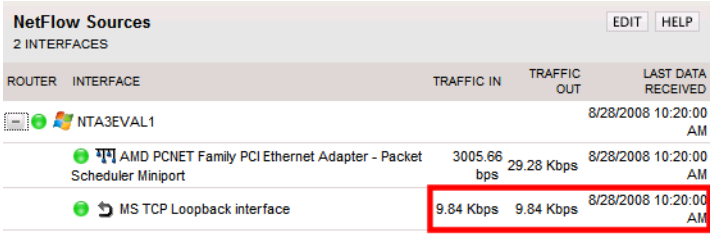
Fuentes de NetFlow

Este recurso, NetFlow Sources (Fuentes de NetFlow), proporciona una lista de todos los dispositivos con NetFlow habilitado de su red que están actualmente configurados para enviar datos de NetFlow al servidor que aloja su instalación de Orion NTA. Para obtener más información acerca de la adición de dispositivos con NetFlow habilitado, consulte “Habilitación del análisis del tráfico de NetFlow” en la página 11.

Haga clic en **+** al lado de cualquier nombre de enrutador para visualizar las interfaces con NetFlow habilitado en el enrutador seleccionado.



Las interfaces también se enumeran con un icono de estado y un sello de hora que indican cuándo Orion NTA recibió por última vez datos de NetFlow desde la interfaz seleccionada. Además, el recurso NetFlow Sources (Fuentes de NetFlow) proporciona valores registrados para el tráfico entrante y saliente de cada interfaz.

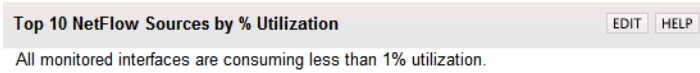


Al hacer clic en el nombre de un enrutador, se abrirá la vista NetFlow Node Details (Información de nodos de NetFlow), y al hacer clic en el nombre de una interfaz se abrirá la vista NetFlow Interface Details (Información de interfaz de NetFlow). Para obtener más información acerca de la vista NetFlow Node Details (Información de nodos de NetFlow), consulte “Vista Información de nodos de NetFlow” en la página 38. Para obtener más información acerca de la vista NetFlow Interface Details (Información de interfaz de NetFlow), consulte “Vista Información de interfaz de NetFlow” en la página 36.

10 principales fuentes de NetFlow por % de uso

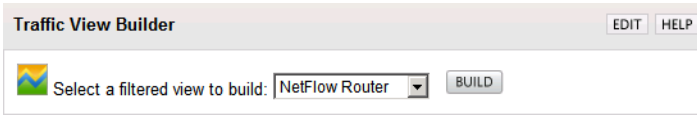
Este recurso, Top 10 NetFlow Sources by % Utilization (10 principales fuentes de NetFlow por % de uso), proporciona una lista de las fuentes de NetFlow de su red que enrutan actualmente suficiente tráfico como para poner a prueba significativamente los recursos de su sistema.

Nota: las fuentes sólo se enumeran si experimentan un exceso de uso del 1 %.



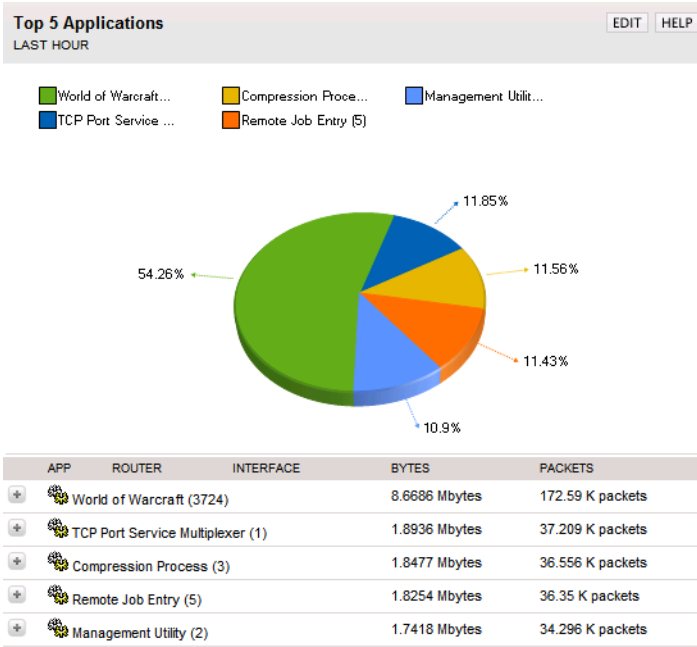
Traffic View Builder

La aplicación Traffic View Builder le permite crear sus propias vistas personalizadas de Orion NTA. Como Orion NTA es un módulo web-based, puede crear marcadores de navegador para cualquier vista de Orion NTA con fin de comprobar con facilidad el estado de puntos problemáticos potenciales en una fecha posterior. Para obtener más información acerca de Traffic View Builder, consulte “Uso de Traffic View Builder” en la página 41.



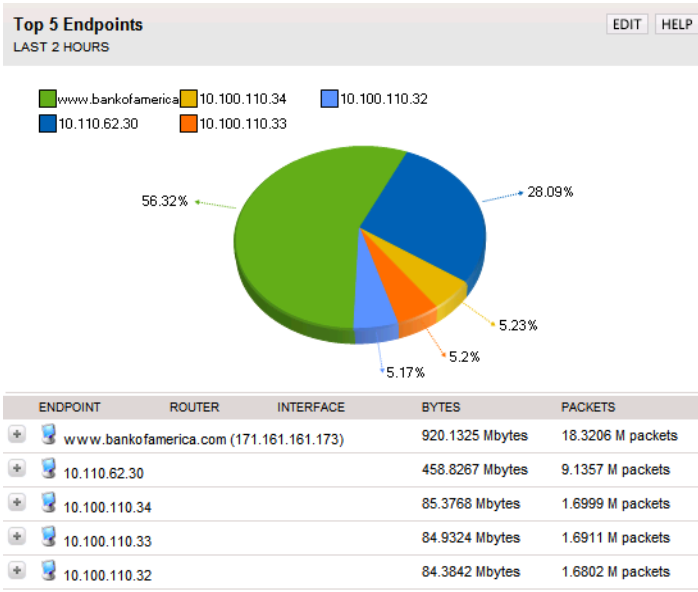
5 aplicaciones principales

El recurso de las Top 5 Applications (5 aplicaciones principales) proporciona una vista rápida de las aplicaciones y puertos más utilizados por los dispositivos de su red. Puede hacer clic en **+** para ampliar cada aplicación y ver el tráfico de enrutamiento de los dispositivos de la red de cada aplicación.



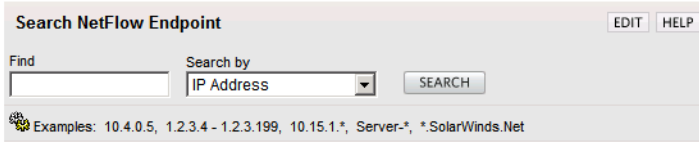
5 terminales principales

El recurso de las Top 5 Endpoints (5 terminales principales) ofrece una vista rápida de los terminales que son fuentes o destinos de la mayoría del tráfico de red. Puede hacer clic en **+** para ampliar cada terminal y ver el tráfico de enrutamiento de los dispositivos de red para cada terminal.



Buscar terminales de NetFlow

Mediante este recurso Search NetFlow Endpoint (Buscar terminales de NetFlow), puede localizar con rapidez cualquier terminal en comunicación con cualquier dispositivo de su red.

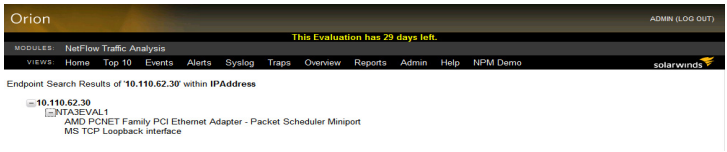


Simplemente busque terminales mediante cualquiera de los criterios de la tabla siguiente:

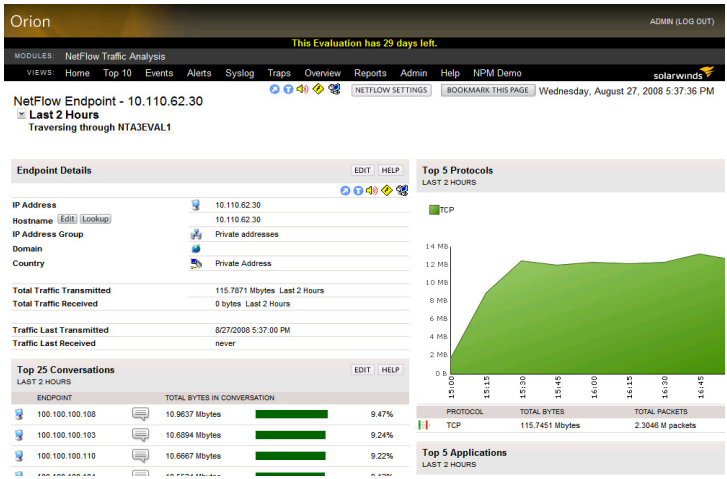
Criterios de búsqueda de terminales de NetFlow

Criterios de búsqueda de terminales de NetFlow		
País	Dominio	Nombre de anfitrión
Dirección IP	Nombre del grupo de direcciones IP	

Proporcione un término de búsqueda adecuado y, a continuación, haga clic en **Search** (Búsqueda). Los resultados de su búsqueda proporcionan una lista ampliable de los dispositivos de su red que enrutan tráfico a o desde el terminal buscado.

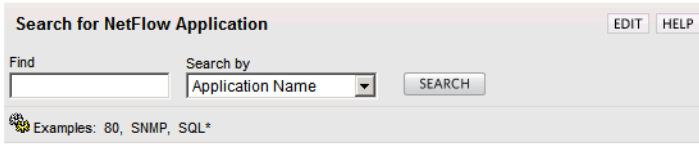


Al hacer clic en el nombre de cualquiera de los dispositivos de su red se abrirá NetFlow Endpoint View (Vista Terminal de NetFlow) con todo el tráfico de terminal del dispositivo seleccionado. Para obtener más información acerca de NetFlow Endpoint View, consulte “Vista Terminal de NetFlow” en la página 34.

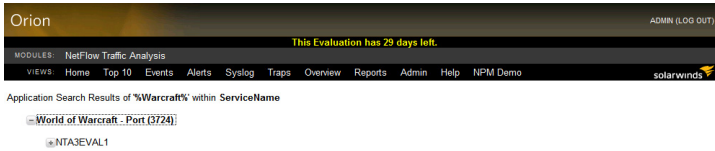


Buscar aplicación de NetFlow

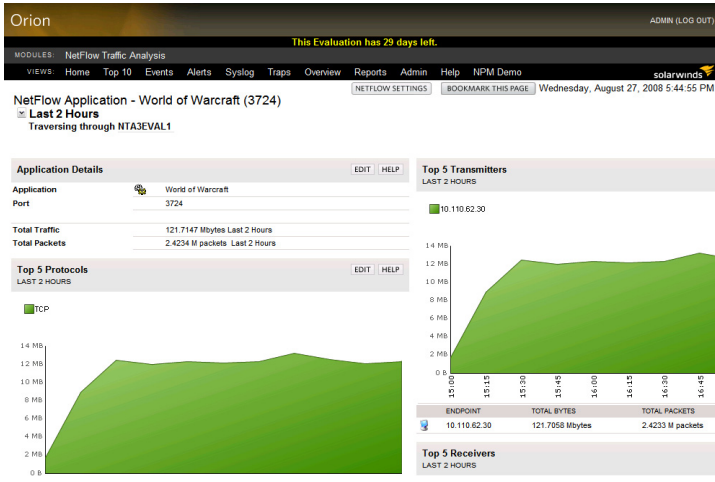
Con el recurso Search for NetFlow Application (Buscar aplicación de NetFlow) podrá ver con rapidez qué dispositivos de su red utilizan una aplicación o puerto específicos en cualquier momento. Simplemente escoja buscar por Application Name or Port (Nombre de aplicación o puerto), proporcione un número de puerto o nombre de aplicación adecuado y, a continuación, haga clic en **Search** (Búsqueda).



Los resultados de su búsqueda proporcionan una lista ampliable de los dispositivos de su red que enrutan tráfico para la aplicación seleccionada o sobre el puerto seleccionado.

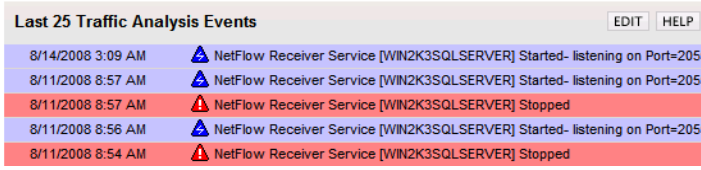


Al hacer clic en el nombre de un dispositivo de su red se abrirá la vista NetFlow Application (Aplicación de NetFlow) para todo el tráfico del dispositivo seleccionado que está dirigido a la aplicación buscada o enrutado mediante el puerto buscado. Para obtener más información acerca de la vista NetFlow Application, consulte “Vista aplicaciones de NetFlow” en la página 30.



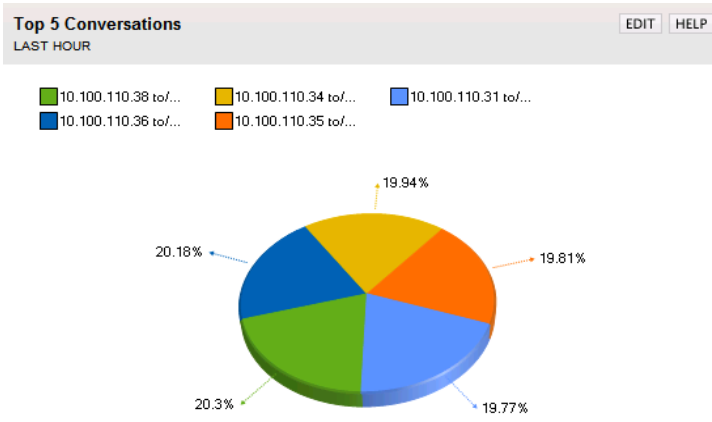
Últimos 25 acontecimientos de análisis del tráfico

El recurso Last 25 Traffic Analysis Events (Últimos 25 acontecimientos de análisis del tráfico) enumera los últimos 25 acontecimientos específicos de NetFlow que se han producido en su red supervisada. Normalmente, este recurso enumera las fechas y horas en las que NetFlow Receiver Service (Servicio receptor NetFlow) se detiene y se inicia.



5 conversaciones principales

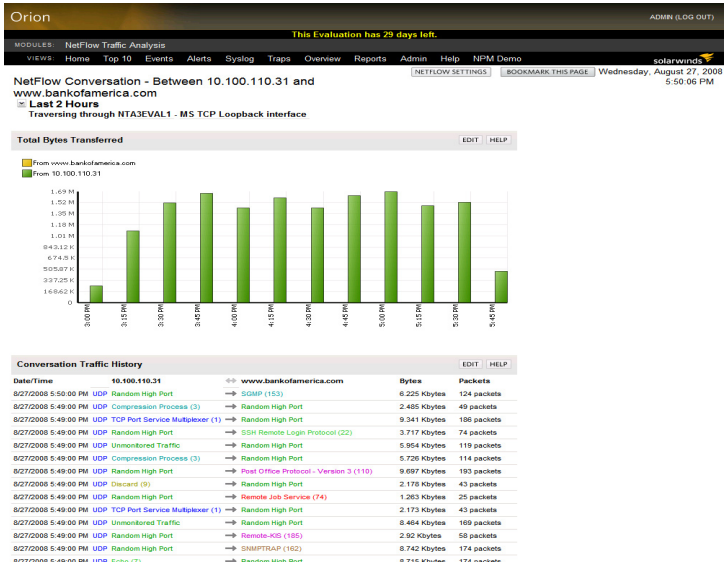
Este recurso,Top 5 Conversations (Top 5 Conversations), proporciona una vista rápida, con un gráfico y una tabla, de las conversaciones que utilizan el mayor ancho de banda de su red. Cada color del gráfico corresponde a una única conversación continuada entre dos terminales específicos. La tabla que sigue al gráfico enumera los terminales relacionados con cada conversación, con el ancho de banda consumido por cada conversación en términos de bytes y paquetes. Ha clic en **+** para ampliar la descripción de la conversación y ver todos los dispositivos de su red que han llevado a cabo la conversación seleccionada. El primer nivel de ampliación muestra los nodos de red mediante los que se ha enrutado el tráfico de la conversación. El nivel de ampliación siguiente muestra las interfaces que pasan tráfico para la conversación seleccionada.



CONVERSATION ROUTER INTERFACE	BYTES	PACKETS
Between 10.100.110.38 and www.bankofamerica.com (171.161.161.173)	8.3817 Mbytes	166.891 K packets
Between 10.100.110.36 and www.bankofamerica.com (171.161.161.173)	8.3306 Mbytes	165.879 K packets
Between 10.100.110.34 and www.bankofamerica.com (171.161.161.173)	8.2335 Mbytes	163.935 K packets
Between 10.100.110.35 and www.bankofamerica.com (171.161.161.173)	8.1783 Mbytes	162.829 K packets
Between 10.100.110.31 and www.bankofamerica.com (171.161.161.173)	8.1605 Mbytes	162.464 K packets
NTA3EVAL1	8.1605 Mbytes	162.464 K packets
NTA3EVAL1 - MS TCP Loopback interface	2.9147 Mbytes	58.042 K packets
NTA3EVAL1 - AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport	2.6416 Mbytes	52.593 K packets

Tanto en el nivel de nodo como en el de interfaz, los usos compartidos respectivos del ancho de banda total consumido por la conversación seleccionada se enumeran en bytes y paquetes. Para cada nodo, el tráfico de la conversación en el nodo equivale a la suma del tráfico de la conversación en todas las interfaces de ese nodo.

Al hacer clic en el nombre de cualquier dispositivo de red se abrirá la vista NetFlow Conversation (Conversación NetFlow) que muestra todo el tráfico entre los dos terminales que conversan mediante el dispositivo de red seleccionado. Para obtener más información, consulte “Vista de conversación NetFlow” en la página 33.



Orion NetFlow Traffic Analyzer Vistas

Los siguientes apartados proporcionan información detallada sobre los tipos de información disponibles por defecto en las vistas de Orion NTA seleccionadas.

Notas:

- Las vistas que aparecen a continuación son una muestra de las vistas de Orion NTA más utilizadas. Están enlazadas directamente desde recursos predeterminados de la vista NetFlow Traffic Analysis Summary (Resumen del análisis del tráfico de NetFlow). Los recursos adicionales enlazan a vistas adicionales. Para obtener más información, consulte “Ver datos de NetFlow Traffic Analyzer en la Orion Web Console” en la *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.
- Algunos recursos pueden no estar presentes en la configuración por defecto de una vista seleccionada. Para ver todos los recursos disponibles, debe editar la vista desde la vista Admin de la Orion NPM Web Console. Para obtener más información, consulte “Ver datos de NetFlow Traffic Analyzer en la Orion Web Console” en la *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Vista aplicaciones de NetFlow

Los siguientes apartados ofrecen breves descripciones de los recursos de la vista NetFlow Application (Aplicaciones de NetFlow) por defecto. Puede obtener más información acerca de cada recurso, incluida la información de configuración, haciendo clic en **Help** (Ayuda) en la barra de título del recurso.

Información sobre la aplicación

El recurso Application Details (Información sobre la aplicación) proporciona una tabla que contiene la siguiente información acerca de la aplicación y el puerto que está visualizando actualmente:

- Nombre de la aplicación
- Puerto utilizado por la aplicación
- Cantidad total de datos de tráfico en el período de tiempo seleccionado
- Número total de paquetes enviados en el período de tiempo seleccionado

5 protocolos principales

El recurso Top 5 Protocols (5 protocolos principales) proporciona una vista rápida de los protocolos de tráfico que la aplicación seleccionada utiliza con más frecuencia. La tabla que sigue al gráfico proporciona el tipo de protocolo, la cantidad de datos, el número total de paquetes y el porcentaje de todo el tráfico que cada protocolo enumerado ha estado utilizando.

5 tipos principales de servicio

El recurso Top 5 Types of Service (5 tipos principales de servicio) proporciona una vista rápida, en forma de gráfico, de los servicios más activos empleados por la aplicación seleccionada. La tabla que sigue al gráfico proporciona la siguiente información para cada tipo de servicio:

- El tipo de servicio
- La cantidad de tráfico gestionado por el servicio
- El número de paquetes gestionados por el servicio
- El porcentaje de todo el tráfico proporcionado a la aplicación seleccionada que está gestionado por el tipo seleccionado de servicio

Total de bytes transferidos

El recurso Total Bytes Transferred (Total de bytes transferidos) muestra un gráfico que detalla el número total de bytes transferidos por la aplicación seleccionada durante un período de tiempo especificado. Dispone de una amplia variedad de gráficos personalizados para imprimir o exportar para la gestión de registros. Al hacer clic en el gráfico se abrirá la página Customize Chart

(Personalizar gráficos) para el gráfico seleccionado. Para obtener más información acerca de la personalización de gráficos, consulte “Personalizar gráficos en NetFlow Traffic Analyzer” en la *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Visitantes únicos

El recurso Unique Visitors (Visitantes únicos) proporciona un gráfico que detalla el número de direcciones IP únicas que han utilizado la aplicación seleccionada durante un período de tiempo especificado. Dispone de una amplia variedad de gráficos personalizados para imprimir o exportar para la gestión de registros. Al hacer clic en el gráfico se abrirá la página Customize Chart (Personalizar gráficos) para el gráfico seleccionado. Para obtener más información acerca de la personalización de gráficos, consulte “Personalizar gráficos en NetFlow Traffic Analyzer” en la *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Total de paquetes transferidos

El recurso Total Packets Transferred (Total de paquetes transferidos) muestra un gráfico que detalla el número total de paquetes transferidos por la aplicación seleccionada durante un período de tiempo especificado. Dispone de una amplia variedad de gráficos personalizados para imprimir o exportar para la gestión de registros. Al hacer clic en el gráfico se abrirá la página Customize Chart (Personalizar gráficos) para el gráfico seleccionado. Para obtener más información acerca de la personalización de gráficos, consulte “Personalizar gráficos en NetFlow Traffic Analyzer” en la *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

5 transmisores principales

El recurso Top 5 Transmitters (5 transmisores principales) proporciona una vista rápida, en forma de gráfico, de los terminales con más actividad de transmisión que utilizan la aplicación seleccionada. La tabla que sigue al gráfico proporciona la siguiente información para cada terminal:

- El nombre o dirección IP del terminal
- La cantidad de tráfico transmitido por el terminal
- El porcentaje de todo el tráfico transmitido atribuible al terminal

Puede hacer clic en cada uno de los terminales de la lista para abrir la vista NetFlow Endpoint que presenta estadísticas similares para cada terminal con transmisión. Para obtener más información, consulte “Vista Terminal de NetFlow” en la página 34.

5 receptores principales

El recurso Top 5 Receivers (5 receptores principales) proporciona una vista, en forma de gráfico, de los terminales con más actividad de recepción que utilizan la aplicación seleccionada. La tabla que sigue al gráfico proporciona la siguiente información para cada terminal:

- El nombre o dirección IP del terminal
- La cantidad de tráfico recibido por el terminal
- El porcentaje de todo el tráfico recibido atribuible al terminal

Puede hacer clic en cada uno de los terminales de la lista para abrir la vista NetFlow Endpoint que presenta estadísticas similares para cada terminal con transmisión. Para obtener más información, consulte “Vista Terminal de NetFlow” en la página 34.

5 fuentes de tráfico principales por país

El recurso Top 5 Traffic Sources by Country (5 fuentes de tráfico por país) proporciona una vista rápida, en forma de gráfico, de los países donde se origina el tráfico de la aplicación seleccionada, ordenados por el porcentaje de tráfico total de la aplicación. La tabla que sigue al gráfico proporciona la siguiente información para cada país:

- El nombre del país
- La cantidad de tráfico originado en el país
- El porcentaje de todo el tráfico atribuible al país

5 destinos de tráfico principales por país

El recurso Top 5 Traffic Destinations by Country (5 destinos de tráfico por país) proporciona una vista rápida, en forma de gráfico, de los países que sirven de destino para el tráfico de la aplicación seleccionada, ordenados por el porcentaje de tráfico total de la aplicación. La tabla que sigue al gráfico proporciona la siguiente información para cada país:

- El nombre del país

- La cantidad del tráfico de la aplicación enrutado a terminales del país
- El porcentaje de todo el tráfico de la aplicación atribuible a terminales del país

5 conversaciones principales

El recurso Top 5 Conversations (5 conversaciones principales) proporciona una lista de las conversaciones con el ancho de banda más pesado enrutadas a través del dispositivo seleccionado, mediante la aplicación seleccionada. Las conversaciones se enumeran con la cantidad de datos transferidos en la conversación, en bytes y paquetes, y el porcentaje del tráfico total de la aplicación generado por la conversación. Al hacer clic en una conversación se abrirá la vista NetFlow Conversation (Conversación NetFlow) para la conversación seleccionada. Para obtener más información, consulte “Vista de conversación NetFlow” en la página 33.

Vista de conversación NetFlow

Los siguientes apartados ofrecen breves descripciones de los recursos de NetFlow Conversation View (Vista de conversación NetFlow) por defecto. Puede obtener más información acerca de cada recurso, incluida la información de configuración, haciendo clic en **Help** (Ayuda) en la barra de título del recurso.

Total de bytes transferidos

El recurso Total Bytes Transferred (Total de bytes transferidos) muestra un gráfico que detalla el número total de bytes transferidos, durante un período de tiempo especificado, entre los dos nodos, direcciones IP o dominios indicados en el título de la vista.

Historial de tráfico de conversaciones

El recurso Conversation Traffic History (Historial de tráfico de conversaciones) proporciona una tabla que muestra la siguiente información para cada intercambio de conversación enumerado:

- El sello de fecha/hora del intercambio
- El protocolo utilizado para el intercambio
- La aplicación y el puerto utilizados para el intercambio
- La dirección del flujo de tráfico

- La cantidad de tráfico comunicado en bytes
- El número equivalente de paquetes comunicados

Vista Terminal de NetFlow

Los siguientes apartados ofrecen breves descripciones de los recursos de la vista NetFlow Endpoint (Vista Terminal de NetFlow) por defecto. Puede obtener más información acerca de cada recurso, incluida la información de configuración, haciendo clic en **Help** (Ayuda) en la barra de título del recurso.

Información del terminal

El recurso Endpoint Details (Información del terminal) proporciona la siguiente información acerca de un terminal seleccionado:

- Dirección IP
- Nombre de anfitrión
- Grupo de direcciones IP
- Dominio
- País
- Tráfico total transmitido y recibido
- Sellos de hora-fecha de los últimos datos transmitidos y recibidos

5 conversaciones principales

Este recurso Top 5 Conversations (5 conversaciones principales) proporciona una lista de los terminales con los que el terminal actualmente visualizado ha transferido la mayoría de los datos. Para cada conversación, este recurso informa de la cantidad de datos transferidos en la conversación y el porcentaje que la conversación enumerada representa del total de datos transferidos por el terminal visualizado. Al hacer clic en un terminal, se abre la vista NetFlow Endpoint para el terminal seleccionado. Todos los demás enlaces para un terminal enumerado abren la vista NetFlow Conversation para la conversación entre los terminales visualizados y seleccionados. Para obtener más información, consulte “Vista de conversación NetFlow” en la página 33.

Total de paquetes transferidos

El recurso Total Packets Transferred (Total de paquetes transferidos) muestra un gráfico que detalla el número total de bytes transmitidos desde el terminal visualizado y recibidos por el terminal visualizado, durante un período de tiempo especificado.

Total de bytes transferidos

El recurso Total Bytes Transferred (Total de bytes transferidos) muestra un gráfico que detalla el número total de bytes transmitidos desde el terminal visualizado y recibidos por el terminal visualizado, durante un período de tiempo especificado.

5 protocolos principales

El recurso Top 5 Protocols (5 protocolos principales) proporciona una vista rápida de los protocolos de tráfico que el terminal seleccionado utiliza con más frecuencia. La tabla que sigue al gráfico proporciona el tipo de protocolo, la cantidad de datos, el número total de paquetes y el porcentaje de todo el tráfico que cada protocolo enumerado ha estado utilizando.

5 aplicaciones principales

El recurso Top 5 Applications (5 aplicaciones principales) proporciona una vista rápida de las aplicaciones más utilizadas por el terminal seleccionado. La tabla que sigue al gráfico proporciona el nombre de la aplicación, la cantidad de datos que fluye, el número total equivalente de paquetes y el porcentaje de todo el tráfico atribuible al uso de la aplicación enumerada por el terminal seleccionado. Al hacer clic en una aplicación, se abre la vista NetFlow Application. Para obtener más información, consulte “Vista aplicaciones de NetFlow” en la página 30.

5 fuentes de tráfico principales por país

El recurso Top 5 Traffic Sources by Country (5 fuentes de tráfico principales por país) proporciona una vista rápida, en forma de gráfico, de los países donde se origina el tráfico para el terminal seleccionado, ordenados por el porcentaje de tráfico total para el terminal seleccionado. La tabla que sigue al gráfico proporciona el nombre del país donde se origina el tráfico para el terminal visualizado, la cantidad de tráfico enrutado al terminal desde el país enumerado y el porcentaje de todo el tráfico enrutado al terminal visualizado atribuible al país enumerado.

5 destinos de tráfico principales por país

El recurso Top 5 Traffic Destinations by Country (5 destinos de tráfico principales por país) proporciona un gráfico y una tabla de los países que alojan destinos de tráfico desde el terminal seleccionado, ordenados por el porcentaje de tráfico total desde el terminal seleccionado. La tabla que sigue al gráfico proporciona el nombre del país al que se enruta el tráfico, la cantidad de tráfico enrutado a servidores del país enumerado y el porcentaje de todo el tráfico enrutado desde el terminal visualizado enrutado a servidores del país enumerado.

Visitantes únicos

El recurso Unique Visitors (Visitantes únicos) proporciona un gráfico de direcciones IP únicas que se han comunicado con el terminal visualizado durante un período de tiempo especificado.

5 tipos principales de servicio

El recurso Top 5 Types of Service (5 tipos principales de servicio) proporciona una vista rápida de los servicios más activos empleados por el terminal seleccionado. La tabla que sigue al gráfico proporciona la siguiente información para cada tipo de servicio:

- El tipo de servicio
- La cantidad de tráfico, en bytes y paquetes, gestionada por el servicio
- El porcentaje de todo el tráfico proporcionado al terminal seleccionado que está gestionado por el tipo de servicio seleccionado

Para obtener más información acerca de la supervisión del tipo de servicio de Orion NTA**,** consulte “Configuración de tipos de servicio de NetFlow” en la *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Vista Información de interfaz de NetFlow

Los siguientes apartados ofrecen breves descripciones de los recursos de la vista NetFlow Interface Details (Información de interfaz de NetFlow) por defecto. Puede obtener más información acerca de cada recurso, incluida la información de configuración, haciendo clic en **Help** (Ayuda) en la barra de título del recurso.

5 protocolos principales

El recurso Top 5 Protocols (5 protocolos principales) proporciona una vista rápida de los protocolos de tráfico que la interfaz visualizada observa con más frecuencia. La tabla que sigue al gráfico proporciona el tipo de protocolo, la cantidad de datos, el número total de paquetes y el porcentaje de todo el tráfico de la interfaz visualizada que utiliza cada protocolo enumerado.

5 terminales principales

El recurso Top 5 Endpoints (5 terminales principales) proporciona una vista de gráfico y una vista de tabla de los terminales que producen más tráfico sobre la interfaz seleccionada. La tabla que sigue al gráfico proporciona el nombre o dirección IP de cada terminal enumerado, la cantidad de tráfico desde cada terminal enumerado, tanto en bytes como en paquetes, y el porcentaje de todo el tráfico sobre la interfaz visualizada que es atribuible a cada terminal enumerado. Al hacer clic en un terminal, se abre la vista NetFlow Endpoint para el terminal seleccionado. Para obtener más información, consulte “Vista Terminal de NetFlow” en la página 34.

5 aplicaciones principales

El recurso Top 5 Applications (5 aplicaciones principales) proporciona una vista rápida de las aplicaciones más utilizadas por la interfaz visualizada. La tabla que sigue al gráfico proporciona el nombre de la aplicación, la cantidad de datos que fluye, el número total equivalente de paquetes y el porcentaje de todo el tráfico atribuible al uso de la aplicación enumerada por la interfaz visualizada. Al hacer clic en una aplicación, se abre la vista NetFlow Application. Para obtener más información, consulte “Vista aplicaciones de NetFlow” en la página 30.

5 dominios principales

Este recurso, Top 5 Domains (5 dominios principales), proporciona una vista rápida de los dominios que están produciendo más tráfico en la interfaz seleccionada. La tabla que sigue al gráfico proporciona el nombre de dominio, la cantidad del tráfico en bytes, el número total de paquetes comunicados y el porcentaje de todo el tráfico de la interfaz seleccionada atribuible a cada dominio.

5 tipos principales de servicio

El recurso Top 5 Types of Service (5 tipos principales de servicio) proporciona una vista rápida de los servicios más activos empleados por la interfaz visualizada. La tabla que sigue al gráfico proporciona la siguiente información para cada tipo de servicio:

- El tipo de servicio
- La cantidad de tráfico, en bytes y paquetes, gestionada por el servicio en la interfaz visualizada
- El porcentaje de todo el tráfico proporcionado en la interfaz visualizada que está gestionado por el tipo de servicio seleccionado

Para obtener más información acerca de la supervisión del tipo de servicio de Orion NTA**,** consulte “Configuración de tipos de servicio de NetFlow” en la *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

5 conversaciones principales

Este recurso, Top 5 Conversations (5 conversaciones principales), proporciona una lista de las conversaciones que crean el mayor tráfico sobre la interfaz visualizada. Para cada conversación, este recurso informa de la cantidad de datos transferidos en la conversación y el porcentaje que la conversación enumerada representa del total de datos transferidos sobre la interfaz visualizada. Al hacer clic en una conversación se abrirá la vista NetFlow Conversation para la conversación seleccionada. Para obtener más información, consulte “Vista de conversación NetFlow” en la página 33.

Vista Información de nodos de NetFlow

Los siguientes apartados ofrecen breves descripciones de los recursos de la vista NetFlow Node Details (Información de nodos de NetFlow) por defecto. Puede obtener más información acerca de cada recurso, incluida la información de configuración, haciendo clic en **Help** (Ayuda) en la barra de título del recurso.

5 protocolos principales

El recurso Top 5 Protocols (5 protocolos principales) proporciona una vista rápida de los protocolos de tráfico que el nodo visualizado utiliza con más frecuencia. La tabla que sigue al gráfico proporciona el tipo de protocolo, la cantidad de datos, el número total de paquetes y el porcentaje de todo el tráfico del nodo visualizado que utiliza cada protocolo enumerado.

5 aplicaciones principales

El recurso Top 5 Applications (5 aplicaciones principales) proporciona una vista rápida de las aplicaciones más utilizadas por el nodo visualizado. La tabla que sigue al gráfico proporciona el nombre de la aplicación, la cantidad de datos que fluye, el número total equivalente de paquetes y el porcentaje de todo el tráfico atribuible al uso de la aplicación enumerada por el nodo visualizado. Al hacer clic en una aplicación, se abre la vista NetFlow Application. Para obtener más información, consulte “Vista aplicaciones de NetFlow” en la página 30.

5 conversaciones principales

Este recurso, Top 5 Conversations (5 conversaciones principales), proporciona una lista de las conversaciones que están creando más tráfico sobre el nodo visualizado. Para cada conversación, este recurso informa de la cantidad de datos transferidos en la conversación y el porcentaje que la conversación enumerada representa del total de datos transferidos sobre el nodo visualizado. Al hacer clic en una conversación se abrirá la vista NetFlow Conversation para la conversación seleccionada. Para obtener más información, consulte “Vista de conversación NetFlow” en la página 33.

5 terminales principales

El recurso Top 5 Endpoints (5 terminales principales) proporciona una vista de gráfico y una vista de tabla de los terminales que producen más tráfico sobre el nodo visualizado. La tabla que sigue al gráfico proporciona el nombre o dirección IP de cada terminal enumerado, la cantidad de tráfico desde cada terminal enumerado, tanto en bytes como en paquetes, y el porcentaje de todo el tráfico sobre el nodo visualizado que es atribuible a cada terminal enumerado. Al hacer clic en un terminal, se abre la vista NetFlow Endpoint para el terminal seleccionado. Para obtener más información, consulte “Vista Terminal de NetFlow” en la página 34.

5 dominios principales

Este recurso, Top 5 Domains (5 dominios principales), proporciona una vista rápida de los dominios que están produciendo más tráfico en el nodo visualizado. La tabla que sigue al gráfico proporciona el nombre de dominio, la cantidad del tráfico en bytes, el número total de paquetes comunicados y el porcentaje de todo el tráfico del nodo visualizado atribuible a cada dominio.

Interfaces de nodos

Este recurso, Node Interfaces (Interfaces de nodos), proporciona una lista de todas las interfaces supervisadas en el nodo visualizado. Se informa del tráfico entrante y saliente de cada interfaz. Al hacer clic en una interfaz, se abre la vista NetFlow Interface Details (Información de interfaz de NetFlow) para la interfaz seleccionada. Para obtener más información, consulte “Vista Información de interfaz de NetFlow” en la página 36.

Capítulo 4

Uso de Orion NetFlow Traffic Analyzer

Mientras que Orion Network Performance Monitor puede informarle del uso del ancho de banda en una interfaz dada, Orion NetFlow Traffic Analyzer lleva esta capacidad más lejos, proporcionándole más información acerca del usuario real de ese ancho de banda y de las aplicaciones que están utilizando. Las situaciones que se presentan en este capítulo ilustran el valor de Orion NetFlow Traffic Analyzer y cómo pueden ofrecerle de manera inmediata un rendimiento de su inversión.

Uso de Traffic View Builder

Mediante el recurso Traffic View Builder puede generar con rapidez sus propias vistas personalizadas para cualquier dispositivo con NetFlow habilitado. Traffic View Builder le permite crear sus propias versiones de cualquiera de las vistas de la tabla siguiente.

Tipos de vista de Traffic View Builder		
Aplicación	País	Dominio
Terminal	Interfaz	Grupo de direcciones IP
Protocolo	Enrutador	Tipo de servicio

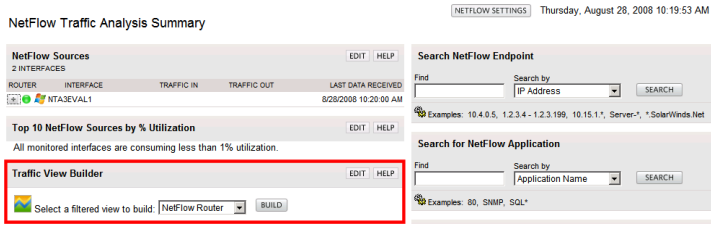
Los siguientes apartados presentan situaciones que muestran cómo el recurso Orion NTA Traffic View Builder le permite crear sus propias vistas.

Ver tráfico para una dirección de IP indicada

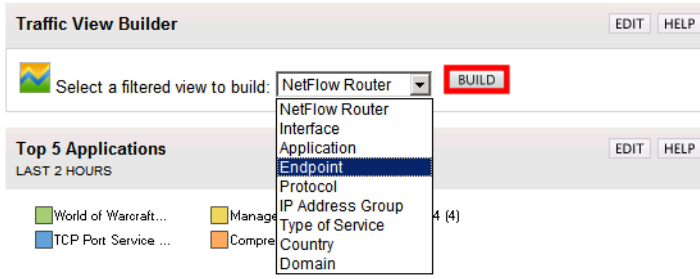
El siguiente procedimiento crea una vista Orion NTA personalizada que muestra el tráfico de red entrante y saliente de una dirección IP indicada.

Para crear una vista para una dirección IP específica:

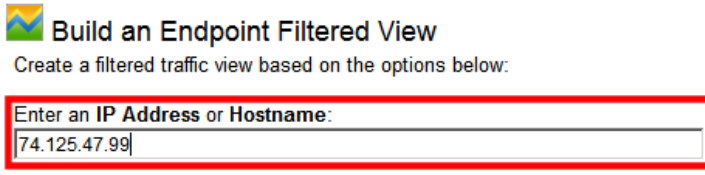
1. Haga clic en **Start** (Inicio) **> All Programs** (Todos los programas) **> SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** y, a continuación, localice el recurso Traffic View Builder.



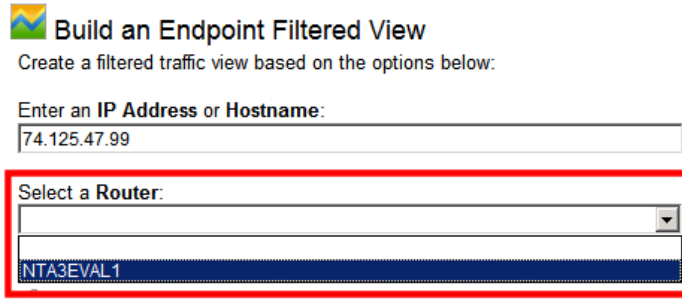
2. Seleccione **Endpoint** (Terminal) y haga clic en **Build** (Crear).



3. Introduzca la **IP address** (Dirección IP) que desea supervisar.



4. Seleccione el enrutador que está enviando tráfico a la dirección IP que ha seleccionado.



5. Seleccione **All Interfaces** (Todas las interfaces) cuando se muestre el menú Select an Interface (Seleccione una interfaz).

   Nota: puede personalizar más su vista para mostrar sólo el tráfico en una interfaz específica del enrutador pero, para los fines de esta evaluación, seleccione **All Interfaces** (Todas las interfaces) para ver todo el tráfico del enrutador seleccionado.

6. Haga clic en **Submit** (Enviar) y se mostrará su vista NetFlow Endpoint personalizada.

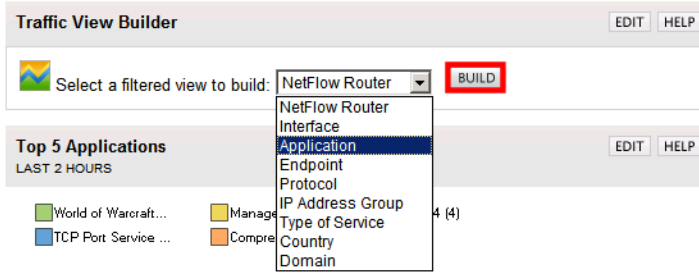
   Nota: para obtener más información acerca de la vista NetFlow Endpoint y sus recursos por defecto, consulte “Vista Terminal de NetFlow” en la página 34.

Ver tráfico de aplicaciones o puertos específicos

El siguiente procedimiento crea una vista Orion NTA personalizada que muestra el tráfico de red a través de puertos especificados o para aplicaciones indicadas.

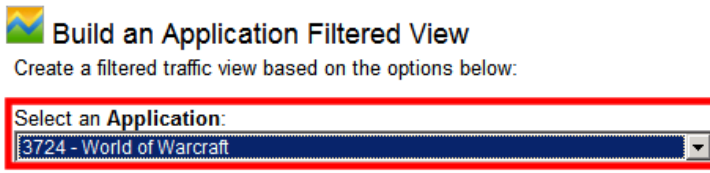
Para crear una vista para aplicaciones o puertos específicos:

1. Haga clic en **Start** (Inicio) **> All Programs** (Todos los programas) **> SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** y, a continuación, localice el recurso Traffic View Builder.
2. Seleccione **Application** (Aplicación) y haga clic en **Build** (Crear).



3. Seleccione la **Application** (Aplicación) o Port (Puerto) que desea supervisar.

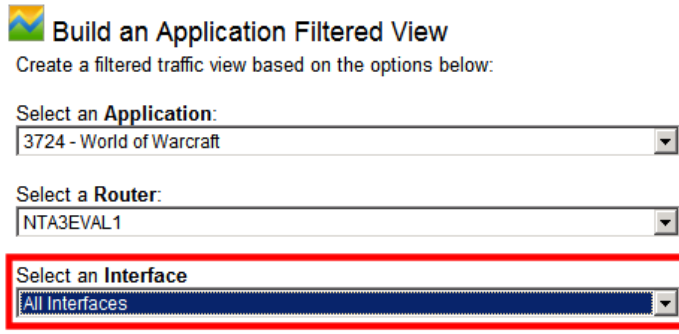
   Nota: las aplicaciones se enumeran por números de puertos asociados. Para determinar las asociaciones del número de puerto de la aplicación, utilice el recurso Search for NetFlow Application (Buscar aplicación de NetFlow)) en la vista NetFlow Traffic Analysis Summary (Resumen del análisis del tráfico de NetFlow). Para obtener más información, consulte “Buscar aplicación de NetFlow” en la página 26.



4. Seleccione el enrutador con NetFlow habilitado que está enrutando el tráfico de su aplicación.

5. Seleccione **All Interfaces** (Todas las interfaces) cuando se muestre el menú Select an Interface (Seleccione una interfaz).

   Nota: puede personalizar más su vista para mostrar sólo el tráfico de la aplicación en una interfaz específica del enrutador pero, para los fines de esta evaluación, seleccione **All Interfaces** (Todas las interfaces) para ver todo el tráfico del enrutador seleccionado.



6. Haga clic en **Submit** (Enviar) y se mostrará su vista NetFlow Application personalizada.

Nota: para obtener más información acerca de la vista NetFlow Application y sus recursos por defecto, consulte “Vista aplicaciones de NetFlow” en la página 30.

Localizar y aislar un ordenador infectado

Puede utilizar su archivo Orion NPM actualmente instalado, agregando Orion NTA, para localizar y responder con rapidez a la amplia variedad de virus autopropagantes que pueden atacar su red. Considere la siguiente situación:

1. Una sucursal local de su red bancaria que gestiona todas las transacciones de tarjeta de crédito se queja de una red extremadamente lenta, que causa frecuentes tiempos de inactividad durante transferencias de datos confidenciales.
2. La Orion Web Console muestra que el enlace a la red de la sucursal está operativo.
3. Los gráficos de porcentaje de uso de Orion NPM de la página inicial del resumen de red muestran que el uso actual es del 98 %, incluso cuando el uso normal de la red de la sucursal es del 15 % al 25 %.
4. Haga clic en **NetFlow Traffic Analysis** (Análisis del tráfico de NetFlow) en la barra de herramientas Modules (Módulos) y, a continuación, haga clic en el nombre del enlace de la red de la sucursal en el recurso NetFlow Sources (Fuentes de NetFlow) para ver el enrutador con NetFlow habilitado de la red de la sucursal.
5. Al echar un vistazo al recurso Top 5 Endpoints (5 terminales principales), observa que un único ordenador en el intervalo de dirección IP `10.10.10.0-10.10.10.255` está generando el 80 % de la carga en el enlace de la sucursal.
6. Sabe que los clientes tienen acceso a los ordenadores en este intervalo de dirección IP para realizar transacciones personales mediante la web.
7. Al ver el recurso Top 5 Applications (5 aplicaciones principales), observa rápidamente que el 100 % de las últimas dos horas de tráfico se ha generado desde un ordenador accesible al público mediante una aplicación de mensajería IBM MQSeries.
8. Al hacer clic en el nombre de la aplicación de mensajería IBM MQSeries en el recurso Top 5 Applications (5 aplicaciones principales), puede determinar que los mensajes de IBM MQSeries se llevan a cabo sobre el puerto 1883.
9. Sabiendo que no posee ningún dispositivo que utilice la mensajería IBM MQSeries en la ubicación accesible por el cliente, ni ningún otro servicio o protocolo que requiera el puerto 1883, puede reconocer que se trata de un virus.
10. Mediante una herramienta de gestión de configuración, como Cirrus Configuration Manager, establece una nueva configuración en su cortafuegos que bloquea el puerto 1883.

Localizar y bloquear el uso no deseado

Con Orion NTA, puede registrar gráficamente con facilidad el uso creciente de cualquiera de sus diferentes enlaces a la red. Orion NPM ya le permite registrar gráficamente el uso pero, agregando Orion NTA, puede localizar archivos específicos de uso no deseado, permitiéndole llevar a cabo de manera inmediata acciones correctivas, como en la situación siguiente:

1. Su enlace a Internet se ha ido ralentizando progresivamente durante los últimos 6 meses, aunque el recuento por unidades corporativas, el uso de las aplicaciones y el ancho de banda dedicado han sido estables.
2. Cuando abre la Orion Web Console, la vista Network Summary Home (Inicio del resumen de red) muestra que su enlace de sitio a Internet está operativo pero, cuando hace clic en su enlace ascendente específico y consulta el uso porcentual actual de cada gráfico de interfaz, observa que el uso actual de su interfaz orientada a la web es del 80 %.
3. Haga clic en su interfaz orientada a la web para abrir la vista Interface Details (Información de interfaz).
4. Al personalizar el gráfico de uso porcentual para mostrar los últimos 6 meses, observa que ha habido un crecimiento continuo de consumo del 15 % al 80 % con el paso del tiempo. Incluso hay picos que superan el 90 %.
5. Haga clic en la pestaña NetFlow Traffic Analysis (Análisis del tráfico de NetFlow) y, a continuación, haga clic en la interfaz orientada a la web para abrir la vista NetFlow Interface Details (Información de interfaz de NetFlow).
6. Al mirar los Top 50 Endpoints (50 terminales principales), observa que un grupo de ordenadores en el intervalo de dirección IP `10.10.12.0-10.10.12.255` está consumiendo la mayor parte del ancho de banda. Dichos ordenadores se encuentran en el intervalo de dirección IP de su departamento de ventas internas.
7. Empieza a desplazarse a cada una de las direcciones IP inválidas y cada dirección de IP que investiga muestra el uso de Kazaa (puerto 1214) y World of Warcraft (puerto 3724) entre las 5 aplicaciones principales.
8. Mediante una herramienta de gestión de configuración, como Cirrus Configuration Manager, establece una nueva configuración en su cortafuegos que bloquea los puertos 1214 y 3724.
9. Al cabo de unos minutos, observa que el tráfico de su interfaz desciende al 25 %.

Reconocer e impedir ataques de denegación de servicio

Orion NTA le permite representar fácilmente el tráfico entrante y saliente. Esta capacidad es más importante que nunca ya que las redes corporativas están expuestas al aumento de los ataques de denegación de servicio maliciosos. Considere la siguiente situación:

1. Un aviso avanzado de Orion NPM le informa que su enrutador orientado a la web está teniendo problemas para crear y mantener una conexión estable a Internet.
2. Abre la Orion Web Console para buscar posibles problemas. Todas las conexiones están actualmente operativas y el uso del ancho de banda parece correcto. Pero entonces advierte el uso de su CPU en el nodo del cortafuegos. Se mantiene estable entre el 99 % y el 100 %.
3. Al hacer clic en el nombre del nodo del cortafuegos se abre la página Node Details (Información de nodos), donde el recurso Current Percent Utilization of Each Interface (Porcentaje actual de utilización de cada interfase) muestra que las interfaces de su cortafuegos están recibiendo unos niveles anormalmente altos de tráfico.
4. Haga clic en **NetFlow Traffic Analysis** (Análisis del tráfico de NetFlow) en la barra de herramientas Modules (Módulos) para echar un vistazo rápido a su recurso personalizado 50 terminales principales.
5. El recurso Top 50 Endpoints (50 terminales principales) muestra que los seis ordenadores principales que intentan acceder a su red están en el extranjero.
6. Se da cuenta de que sus puertos están siendo examinados y de que su cortafuegos está bloqueando de manera interactiva estos ataques.
7. Mediante una herramienta de gestión de configuración, como Cirrus Configuration Manager, establece una nueva configuración en su cortafuegos que bloquea todo el tráfico del intervalo de dirección IP de los ordenadores que intentan acceder a su red.
8. Al cabo de unos minutos, el uso de CPU de su enrutador orientado a la web vuelve a ser normal.

Análisis más profundo de Orion NTA

Mientras que esto concluye el tour guiado de Orion NetFlow Traffic Analyzer, esta *Evaluation Guide* no trata todas las posibilidades de las funciones de supervisión de la red disponibles con Orion NPM. Explore la *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*, disponible en el sitio web de SolarWinds, en http://www.solarwinds.com/support/documentation.aspx, para aprender incluso más sobre el poder y las ventajas de usar Orion NetFlow Traffic Analyzer.