

# SolarWinds

## NetFlow Traffic Analyzer Evaluation Guide

Copyright © 1995-2013 SolarWinds Worldwide, LLC. All rights reserved worldwide.

No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, the SolarWinds & Design, ipMonitor, LANsurveyor, Orion, and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies. Microsoft®, Windows®, and SQL Server® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Revised: 4/26/2013

## About SolarWinds

SolarWinds, Inc. develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

## Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

| Team              | Contact Information                                                             |
|-------------------|---------------------------------------------------------------------------------|
| Sales             | sales@solarwinds.com<br>www.solarwinds.com<br>1.866.530.8100<br>+353.21.5002900 |
| Technical Support | www.solarwinds.com/support                                                      |
| User Forums       | thwack.solarwinds.com                                                           |

## Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

| Convention                       | Specifying                                                                  |
|----------------------------------|-----------------------------------------------------------------------------|
| <b>Bold</b>                      | Window items, including buttons and fields.                                 |
| <i>Italics</i>                   | Book and CD titles, variable names, new terms                               |
| Fixed font                       | File and directory names, commands and code examples, text typed by you     |
| Straight brackets, as in [value] | Optional command parameters                                                 |
| Curly braces, as in {value}      | Required command parameters                                                 |
| Logical OR, as in value1 value2  | Exclusive command parameters where only one of the options can be specified |

**NetFlow Traffic Analyzer Documentation Library**

The following documents are included in the NetFlow Traffic Analyzer documentation library:

| Document            | Purpose                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator Guide | Provides detailed setup, configuration, and conceptual information.                                                                                                  |
| Evaluation Guide    | Provides an introduction to NetFlow Traffic Analyzer features and instructions for installation and initial configuration.                                           |
| Page Help           | Provides help for every window in the NetFlow Traffic Analyzer user interface                                                                                        |
| Release Notes       | Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at <a href="http://www.solarwinds.com">www.solarwinds.com</a> . |

The following documents supplement the NetFlow Traffic Analyzer documentation library with information about Network Performance Monitor:

| Document                                              | Purpose                                                                                                                                                              |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Orion Network Performance Monitor Administrator Guide | Provides detailed setup, configuration, and conceptual information for Network Performance Monitor.                                                                  |
| Orion Network Performance Monitor Evaluation Guide    | Provides an introduction to Network Performance Monitor features and instructions for installation and initial configuration.                                        |
| Page Help                                             | Provides help for every window in the Network Performance Monitor user interface                                                                                     |
| Release Notes                                         | Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at <a href="http://www.solarwinds.com">www.solarwinds.com</a> . |

**Contents**

|                                                             |            |
|-------------------------------------------------------------|------------|
| <i>About SolarWinds .....</i>                               | <i>iii</i> |
| <i>Contacting SolarWinds .....</i>                          | <i>iii</i> |
| <i>Conventions .....</i>                                    | <i>iii</i> |
| <i>NetFlow Traffic Analyzer Documentation Library .....</i> | <i>iv</i>  |

**Chapter 1**

|                                                       |          |
|-------------------------------------------------------|----------|
| <b>Introduction to NetFlow Traffic Analyzer .....</b> | <b>1</b> |
| <i>Why Install NetFlow Traffic Analyzer .....</i>     | <i>1</i> |
| <i>How NetFlow Traffic Analyzer Works .....</i>       | <i>2</i> |
| <i>Why Use NetFlow Traffic Analyzer .....</i>         | <i>3</i> |

**Chapter 2**

|                                                                        |           |
|------------------------------------------------------------------------|-----------|
| <b>Installing NetFlow Traffic Analyzer .....</b>                       | <b>5</b>  |
| <i>SQL Server and SQL Server Express with NTA .....</i>                | <i>5</i>  |
| <i>Requirements .....</i>                                              | <i>5</i>  |
| <i>Software Requirements .....</i>                                     | <i>6</i>  |
| <i>Hardware Requirements .....</i>                                     | <i>7</i>  |
| <i>Virtual Machine Requirements .....</i>                              | <i>8</i>  |
| <i>NetFlow, IPFIX, J-Flow, NetStream, and sFlow Requirements .....</i> | <i>8</i>  |
| <i>Installing NetFlow Traffic Analyzer .....</i>                       | <i>9</i>  |
| <i>Enabling Flow Analysis .....</i>                                    | <i>13</i> |
| <i>Preparing to Collect Flow Data .....</i>                            | <i>13</i> |
| <i>Adding Devices and Interfaces to the Orion Database .....</i>       | <i>13</i> |
| <i>Setting NetFlow Collector Services .....</i>                        | <i>14</i> |
| <i>Automatically Adding Flow- and CBQoS-enabled Devices .....</i>      | <i>15</i> |
| <i>Adding NetFlow Sources to NetFlow Traffic Analyzer .....</i>        | <i>15</i> |

**Chapter 3**

|                                                   |           |
|---------------------------------------------------|-----------|
| <b>NetFlow Traffic Analyzer Quick Tour .....</b>  | <b>19</b> |
| <i>Starting NetFlow Traffic Analyzer .....</i>    | <i>20</i> |
| <i>Using Search and Filtering Tools .....</i>     | <i>20</i> |
| <i>The NetFlow Traffic Analyzer Summary .....</i> | <i>20</i> |
| <i>NetFlow Sources .....</i>                      | <i>20</i> |

- Top 10 NetFlow Sources by % Utilization* ..... 21
- Top 5 Applications* ..... 22
- Top 5 Conversations*..... 23
- Top 5 Endpoints*..... 24
- Last 25 Traffic Analysis Events* ..... 25
- NetFlow Traffic Analyzer Views* ..... 25
  - NetFlow Application View* ..... 25
  - NetFlow Conversations View*..... 27
  - NetFlow Endpoint View*..... 28
  - NetFlow Interface Details View*..... 30
  - NetFlow Node Details View* ..... 33

Chapter 4

- Using NetFlow Traffic Analyzer** ..... 37
- Adding Endpoint Centric Resources to Orion Nodes*..... 37
- Adding Top Talker Statistics to Orion Alerts* ..... 40
  - Top Talker Advanced Alerts* ..... 41
- Using the Search by Endpoint or Application/Port Tool*..... 43
  - Searching for Endpoints* ..... 43
  - Searching for Application/Port* ..... 44
- Using the Flow Navigator* ..... 45
  - Viewing Traffic for a Designated IP Address*..... 45
- Locating and Isolating an Infected Computer* ..... 48
- Locating and Blocking Unwanted Use* ..... 49
- Recognizing and Thwarting Denial of Service Attacks* ..... 50
- Investigating NTA Further* ..... 50

---

## Chapter 1

# Introduction to NetFlow Traffic Analyzer

NetFlow Traffic Analyzer (NTA) provides a simple-to-use, scalable network monitoring solution for IT professionals managing any size NetFlow-, sFlow-, J-Flow-, NetStream-, or Class-based quality of service- (CBQoS)-enabled network.

## ***Why Install NetFlow Traffic Analyzer***

As companies and their networks grow, bandwidth needs grow exponentially. All modern connected industries invest significant amounts of time and money to ensure that enough bandwidth is available for business-critical activities and applications. When bandwidth needs exceed currently available capacity or when demand seems to expand beyond the abilities of your network, understanding bandwidth use is no longer a novel interest, but it becomes critical to deciding whether it is necessary to invest in more bandwidth or if stricter usage guidelines are sufficient to regain lost bandwidth.

With the advent of streaming media, voice over IP (VoIP) technologies, online gaming, and other bandwidth-intensive applications, you, as a network engineer, must answer more than the simple question of whether the network is up or down. You must answer why the network is not performing up to expectations.

If you need to know how and by whom your bandwidth is being used, NetFlow Traffic Analyzer provides a simple, integrated answer. You can quickly trace and monitor the bandwidth usage of a particular application or type of traffic. For example, if you see excessive bandwidth use on a particular interface, you can use NetFlow Traffic Analyzer to see that the company meeting, consisting of streaming video, is consuming 80% of the available bandwidth through a particular switch. Unlike many other NetFlow analysis products, the network and NetFlow data provided by the NetFlow Traffic Analyzer solution are not purely extrapolated data, but they are based on real information collected about the network by the Network Performance Monitor product that is at the heart of NetFlow Traffic Analyzer.

Out of the box, NetFlow Traffic Analyzer offers broad monitoring and charting capabilities, coupled with detail-driven statistics, including the following:

- Bandwidth distribution across traffic types
- Usage patterns over time
- External traffic identification and tracking
- Tight integration with detailed interface performance statistics

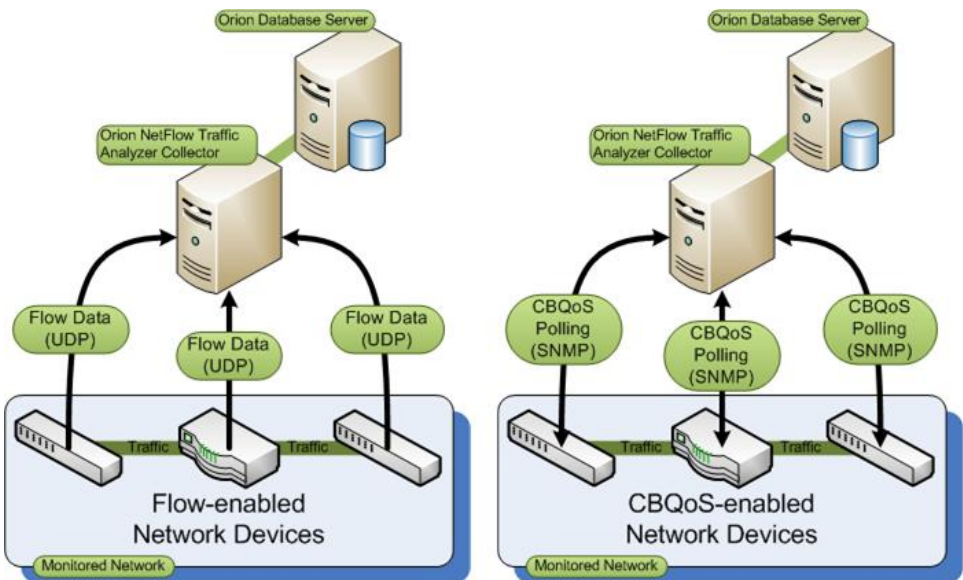
These monitoring capabilities, along with the customizable Network Performance Monitor Web Console and reporting engines, make NetFlow Traffic Analyzer your best option for monitoring your Flow-enabled network.

## How NetFlow Traffic Analyzer Works

Flow- and CBQoS-enabled devices can provide a wealth of IP-related traffic information. NTA collects this traffic data, correlates it into a useable format, and then presents it, with detailed network performance data collected by SolarWinds Network Performance Monitor, as easily read graphs and reports on bandwidth use on your network. These reports help you monitor and shape bandwidth usage, track conversations between internal and external endpoints, analyze traffic patterns, and plan bandwidth capacity needs.

The following diagram provides an overview of a simple NTA installation. The diagram shows, generally, how Flow analysis and CBQoS polling functions polling occur simultaneously in NTA. Flow-enabled devices send Flow data to the NTA collector on port 2055, and the NTA collector polls CBQoS-enabled devices for traffic-shaping policies and results on port 161.

**Note:** The diagram shows CBQoS and Flow monitoring separately to emphasize the difference in collection methods. Network endpoints do not appear in the diagram. Also, a typical NTA installation would not require all CBQoS- and Flow-capable devices be configured to interact directly with the NTA collector. For more information about effectively deploying NetFlow on your network, see [NetFlow Basics and Deployment Strategies](#).



## ***Why Use NetFlow Traffic Analyzer***

NetFlow Traffic Analyzer gives you the ability to quickly and easily monitor network resources and usage patterns at a customizable level of detail. The following valuable features represent core NetFlow Traffic Analyzer capabilities:

### **Enhanced Monitoring and Analytical Planning Capabilities**

NTA highlights trends in network traffic, enabling you to intelligently monitor and anticipate changes in bandwidth to areas that are experiencing bottlenecks.

### **Orion Alerts Integration**

NTA automatically adds top talker information to Orion interface utilization alerts. You can navigate directly to NTA interface details from messages in the Orion Events resource.

For more information, see [Adding Top Talker Statistics to Orion Alerts](#).

### **Customizable Rate-based Charts**

Stacked area charts and line charts offer options to include splines showing data trends, and chart data unit options include Rate (Kbps), Percent of interface speed, Percent of total traffic, and Data transferred per interval.

### **Advanced Port and Application Mapping**

Application mappings may be defined based on source and destination IP addresses, in addition to ports and protocols.

### **Flow Monitoring Support for Cisco Adaptive Security Appliances (ASA)**

NTA can report network traffic data provided by NetFlow-enabled Cisco ASA devices.

### **Filtered Views Including Both Ingress and Egress traffic**

NTA provides the ability to select the direction of traffic over any viewed interface. On any monitored interface, you can view traffic data for ingress traffic, egress traffic, or both.

### **Support for IPFIX-enabled Devices**

Internet Protocol Flow Information Export (IPFIX) is a developing standard for formatting and transmitting IP-based network traffic information. As more devices features IPFIX capability, NTA will immediately be able to provide IPFIX Flow monitoring.

## **Cisco CBQoS Monitoring**

NTA provides resources giving you the ability to easily view, chart, and report on the effects of the class-based quality of service policies you have enabled on your CBQoS-capable Cisco devices.

This release enhances CBQoS monitoring with support for nested policies and more granular control over polling specific devices.

## **Improved availability and performance**

With NTA, you can more quickly detect, diagnose, and resolve network slowdowns and outages.

This release improves CBQoS polling efficiency, load times for reports, and summary views.

## **Optimized Network Resource Allocation**

Information provided by NTA enables you to identify and reassign areas with excess bandwidth capabilities to areas with limited or stressed connections.

## **Alignment of IT Resources with Enterprise Business Needs**

Because NTA is built on the proven NPM infrastructure, you can assess both the needs of the enterprise network in a high-level overview and the functional details of specific interfaces and nodes.

## **Increased Network Security**

NTA gives you the ability to quickly and precisely pinpoint network traffic and expose curious patterns, unwanted behaviors, and anomalous usage that may indicate possible virus, bot, or spyware infection.

## **Support for Multiple Flow Ports**

The number and types of available Flow-enabled devices has increased, so the number of ports over which Flow data is transmitted has also increased. NTA now supports the designation of multiple ports on which Flow data may be received.

## **An All-in-One NetFlow, sFlow, J-Flow, NetStream, and IPFIX monitoring solution**

Now you can stop switching between network monitoring packages to acquire a complete picture of the usage, performance, and needs of your network, regardless of the type of Flow records provided by your various network devices.

This release adds support for sampled NetFlow; NTA now takes into account the sample rate set on your devices to display the traffic statistics that match Orion interface utilization charts.

---

## Chapter 2

# Installing NetFlow Traffic Analyzer

NTA features a wizard-driven installation procedure. For an enterprise-class product, the requirements are nominal.

**Note:** NetFlow data is extensive and can consume large amounts of database memory in a relatively short period of time. This is true even for smaller networks. As a result, SolarWinds requires that your SQL Server database and your NPM/NTA installation are maintained on separate physical servers.

## ***SQL Server and SQL Server Express with NTA***

Due to the fact that NetFlow data is extensive and can consume large amounts of database memory in a relatively short period of time, SolarWinds does not recommend using SQL Server Express database instances for NTA. Instead, SolarWinds recommends the use of a production version of SQL Server.

Evaluations of NTA are a limited exception. For evaluation purposes, NPM and NTA can support the use of SQL Server Express 2005 database instances. SQL Express allows you to evaluate NTA with a real database, and it is available, free of charge, from Microsoft. However, SolarWinds does not recommend its use with NTA in any production environment for the following reasons:

- SQL Express is unable to manage databases larger than 4GB.
- SQL Express is limited to a single processor.
- SQL Express is unable to utilize more than 1MB RAM.

**Note:** For production environments, NPM and NTA installations should use a SQL Server database instance installed on a separate server.

## ***Requirements***

The server you use to host your NetFlow solution must support both NPM and NTA as NTA is built on and extends NPM. In general, requirements for the current NTA version follow the requirements of an NPM version 10.4.2 installation, as provided in the NPM Requirements in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

**Note:** By default, NTA listens for Flow data on port 2055 (UDP). Ensure that port 2055 is open for UDP communication on any NTA collector.

# Software Requirements

The following tables list software requirements for the current NTA version.

**Notes:**

- Due to the high speed and large memory requirements of Flow monitoring transactions, NTA and SQL Server must be installed on separate physical servers.
- SQL Express and MSDE restrict the size of any database to 4GB and 2GB, respectively. For this reason, SolarWinds does not support the use of either SQL Express or MSDE with NTA in production environments.

| Software            | Requirements                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NPM                 | Version 10.4.2 or higher                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Operating System    | Windows Server 2012 (32-bit or 64-bit, with IIS in 32-bit mode)<br>Windows Server 2008, 2008 SP2, 2008 R2 and R2 SP1 (32-bit or 64-bit, with IIS in 32-bit mode).<br>Windows Server 2003 SP2 and 2003 R2 SP2 (32-bit or 64-bit, with IIS in 32-bit mode)<br>IIS must be installed. SolarWinds recommends that NPM administrators have local administrator privileges to ensure full functionality of local NPM tools. Accounts limited to use of the web console do not require administrator privileges.<br><b>Note:</b> SolarWinds does not support installation of NPM on Windows XP, Windows Vista, and Windows 7, Windows 8 in production environments. |
| Web Server          | Microsoft IIS, version 6.0 and later, in 32-bit mode. DNS specifications require that hostnames be composed of alphanumeric characters (A–Z, 0–9), the minus sign (–), and periods (.). Underscore characters ( ) are not allowed. For more information, see RFC 952.<br><b>Note:</b> SolarWinds neither recommends nor supports the installation of NTA on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.                                                                                                                                                                                               |
| .NET Framework      | .NET 3.5 SP1 and .NET 4.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SNMP Trap Services  | Windows operating system management and monitoring tools component                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Web Console Browser | Microsoft Internet Explorer version 7 or later<br>Firefox 17 or later<br>Chrome 24 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| SQL Server Software   | Requirements                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating System      | Windows Server 2012 (32- or 64-bit)<br>Windows Server 2008 (32- or 64-bit)<br>Windows Server 2003 R2, SP1 and higher (32- or 64-bit)                                                                                                                                                                                                                                                     |
| SQL Server            | SQL 2012<br>SQL Server 2008 without SP, 2008 SP1, 2008 SP2, 2008 SP3<br>SQL Server 2008 R2 without SP, 2008 R2 SP1, 2008 R2 SP2<br>SQL Server 2005 SP1, 2005 SP2, 2005 SP3, 2005 SP4<br><b>Note:</b> Though SQL Express may be used for limited evaluations purposes to monitor one or two interfaces for a very limited time SolarWinds recommends against its use for larger networks. |
| SQL Server Collations | English with collation setting SQL_Latin1_General_CP1_CI_AS<br>English with collation setting SQL_Latin1_General_CP1_CS_AS<br>German with collation setting German_PhoneBook_CI_AS<br>Japanese with collation setting Japanese_CI_AS<br>Simplified Chinese with collation setting Chinese_PRC_CI_AS                                                                                      |

## Hardware Requirements

The following table lists minimum hardware requirements for monitoring a typical network with the current version of NTA.

**Note:** NTA requires that TCP port 17777 is opened both to send and to receive traffic between NPM and any other Orion modules.

**Warning:** The only RAID configurations that should be used with NTA are 0, 1, 0+1, or 1+0. Due to the high speed and large memory requirements of NetFlow data transactions, SANs or other RAID configurations should not be used, as they may result in data losses and significantly decreased performance.

| Hardware                                                                                                                                                                                                       | Requirements                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU                                                                                                                                                                                                            | 3GHz or faster, dual processors with dual cores                                                                                                                                                                                                   |
| RAM                                                                                                                                                                                                            | 3GB or more                                                                                                                                                                                                                                       |
| Hard Drive Space                                                                                                                                                                                               | <b>NTA server:</b> 5GB or more, RAID 0, 1, 01, or 10. Other RAID or SAN configurations are not recommended.<br><b>SQL Server:</b> 5GB or more, RAID 0, 1, 01, or 10 on at least 6 spindles. Other RAID or SAN configurations are not recommended. |
| NetFlow devices                                                                                                                                                                                                | Cisco devices using NetFlow version 5 or 9<br><b>Note:</b> NTA only recognizes NetFlow version 9 templates that include all fields included in the NetFlow version 5 template.                                                                    |
| IPFIX devices                                                                                                                                                                                                  | Network devices using IPFIX                                                                                                                                                                                                                       |
| J-Flow devices                                                                                                                                                                                                 | Network devices using J-Flow                                                                                                                                                                                                                      |
| sFlow devices                                                                                                                                                                                                  | Network devices using sFlow version 5                                                                                                                                                                                                             |
| NetStream device                                                                                                                                                                                               | Network devices using NetStream                                                                                                                                                                                                                   |
| <b>Note:</b> For more information about supported Flows, see <a href="#">NetFlow, IPFIX, J-Flow, sFlow, and NetStream Requirements</a> in the <i>SolarWinds NetFlow Traffic Analyzer Administrator Guide</i> . |                                                                                                                                                                                                                                                   |

## Virtual Machine Requirements

NTA may be installed on VMware Virtual Machines and Microsoft Virtual Servers if the following requirements are met by each virtual server.

| Virtual Machine Configuration | Requirements                                                                                                                                                                                                                                                                                                     |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU Speed                     | 3.0 GHz                                                                                                                                                                                                                                                                                                          |
| Allocated Hard Drive Space    | <b>NTA server:</b> 5GB or more, RAID 0, 1, 01, or 10. Other RAID or SAN configurations are not recommended.<br><b>SQL Server:</b> 5GB or more, RAID 0, 1, 01, or 10 on at least 6 spindles. Other RAID or SAN configurations are not recommended.                                                                |
| Memory                        | 2GB or more                                                                                                                                                                                                                                                                                                      |
| Network Interface             | Each installation of NPM should have its own, dedicated NIC<br><b>Note:</b> Since NPM uses SNMP to monitor your network, if you are unable to dedicate a network interface card to your NPM installation, you may experience gaps in monitoring data due to the low priority generally assigned to SNMP traffic. |

For more information about NPM requirements, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

## NetFlow, IPFIX, J-Flow, NetStream, and sFlow Requirements

Any NetFlow, IPFIX, J-Flow, NetStream, or sFlow packets that do not include the following field types and field values may be ignored by NTA:

| Field Type    | Field Type Number | Description                  |
|---------------|-------------------|------------------------------|
| IN_BYTES      | 1                 | Ingress bytes counter        |
| IN_PKTS       | 2                 | Ingress packets counter      |
| PROTOCOL      | 4                 | Layer 4 protocol             |
| L4_SRC_PORT   | 7                 | Source TCP/UDP port          |
| IPV4_SRC_ADDR | 8                 | Source IP address            |
| INPUT_SNMP    | 10                | SNMP ingress interface index |
| L4_DST_PORT   | 11                | Destination TCP/UDP port     |
| IPV4_DST_ADDR | 12                | Destination IP address       |
| OUTPUT_SNMP   | 14                | SNMP egress interface index  |

**Notes:**

- Only one interface index is absolutely required, but both interface indexes (`INPUT_SNMP` and `OUTPUT_SNMP`) should be provided to view accurate statistics for both ingress and egress flows.
- The `SRC_TOS` field type (field type number 5) is required to view Type of Service data for traffic over a Flow source, but the template used by Cisco Adaptive Security Appliances (ASA) does not provide this field.
- If SolarWinds states that NTA supports Flow monitoring for a device, at least one of the templates the device exports satisfies these requirements.
- Including BGP/AS data in NetFlow packets is optional.

***Installing NetFlow Traffic Analyzer***

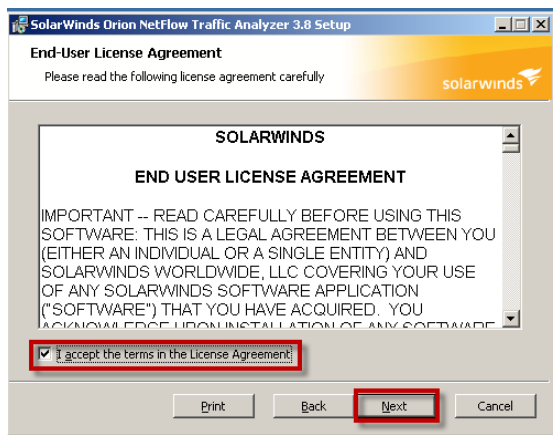
Complete the following procedure to install NTA. You must provide your NetFlow traffic port and confirm that it is enabled and sending NetFlow traffic data in order to complete your installation.

**Note:** The following procedure assumes NPM version 10.4.2 or later is already installed on your designated NTA server. If you would like to evaluate NPM, contact SolarWinds at [sales@solarwinds.com](mailto:sales@solarwinds.com).

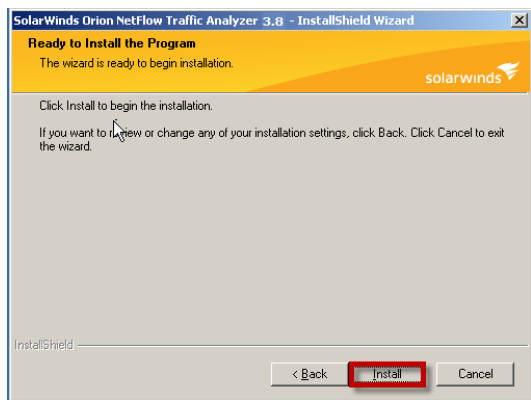
**To install NetFlow Traffic Analyzer:**

1. Log on to the NPM server you want to use for NetFlow traffic analysis.
2. ***If you are installing NTA on a terminal server***, complete the following steps before continuing with your NTA installation:
  - a. Click **Start > Control Panel > Add or Remove Programs**.
  - b. Click **Add New Programs**.
  - c. Click **CD or Floppy**.
  - d. Click **Next** in the Install Program From Floppy Disk or CD-ROM window.
3. ***If you downloaded NetFlow Traffic Analyzer from the SolarWinds website***, launch the SolarWinds NTA installer executable from the directory where it is being stored.
4. ***If you received physical media***, launch the SolarWinds NTA installer executable from you CD drive.
5. Review the Welcome text.
6. Click **Next**.

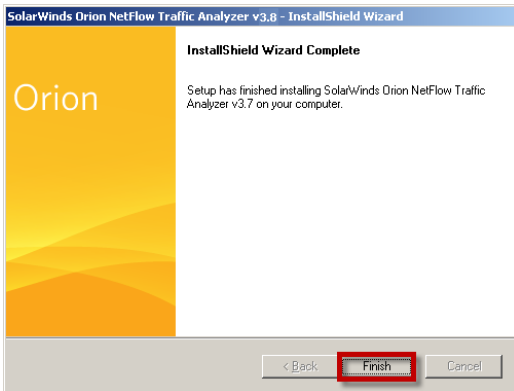
7. Select **I accept the terms of the license agreement**, and then click **Next**.



8. Click **Install** on the Ready to Install the Program window.



9. When the InstallShield Wizard completes, click **Finish** to exit the wizard.



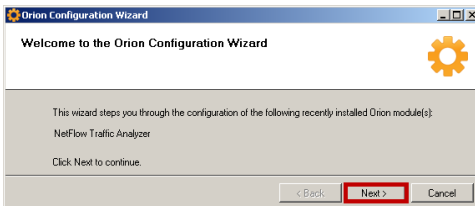
10. Click **Continue Evaluation**.

11. *If you are prompted to reboot your server*, select from the following options, as appropriate:

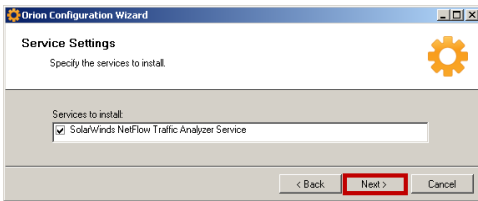
- *If you are installing NTA on a terminal server*, click **No**.
- *If you are NOT installing NTA on a terminal server*, click **Yes**.

12. *If the Configuration Wizard does not start automatically*, start the **Configuration Wizard** in the Orion **Configuration and Auto-Discovery** folder.

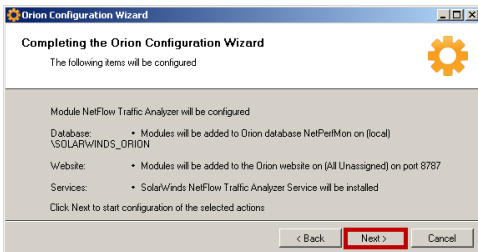
13. Review the Welcome text, and then click **Next**.



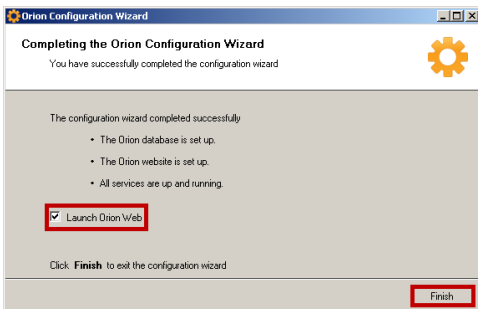
14. Confirm that **SolarWinds NetFlow Traffic Analyzer Service** is checked in the Service Settings window, and then click **Next**.



15. Review the configuration summary, and then click **Next**.



16. After the Configuration Wizard completes, confirm that **Launch Orion Web** is checked, and then click **Finish**.



17. Log in to the Orion Web Console as an administrator.

**Note:** If you have not already configured another Admin password, you can log in with the **User ID** `Admin` and no password.

18. *If you are prompted to add NetFlow resources to the Orion website,* click **Add Resources**.

## Enabling Flow Analysis

To begin analyzing available Flow data produced by devices within your network, you must either add a Flow-enabled interface to your Orion database or monitor a previously added interface that is capable of generating NetFlow data. Adding your NetFlow devices and interfaces to the Orion database and adding your NetFlow devices and interfaces to NTA as NetFlow sources are separate procedures, detailed in separate sections, as follows.

## Preparing to Collect Flow Data

Before you attempt to set up NetFlow Sources in NTA, configure each relevant network device to export Flow data to NTA.

### To prepare for flow collections:

1. Configure your network devices to export data regarding each relevant interface.

Consult vendor documentation on your model. See the *Orion Network Traffic Analyzer Administrator Guide* for examples of Flow configurations for Cisco, Foundry, Extreme, and HP devices.

For information on enabling NetFlow for Cisco Catalyst switches, consult [this SolarWinds technical reference paper](#).

For information on enabling NetFlow on Cisco ASA devices, consult [this SolarWinds Knowledge Base article](#).

2. Verify that each interface for which you want to collect and view data is actively being monitored in NPM.

For this task, for any interface that you need to add into NPM, consult Network Discovery Using Sonar Wizard in the *SolarWinds Orion NPM Administrator Guide*.

3. Use a packet capture tool (for example, WireShark) on the relevant interface and port to verify that the device is in fact exporting data as expected.

## Adding Devices and Interfaces to the Orion Database

You add nodes and their interfaces to the Orion database using the Web Node Management feature of the Orion Web Console. Nodes must be added as SNMP capable. If nodes are not SNMP capable, add them as ICMP, external, or WMI sources. If your NetFlow device is already configured to send NetFlow data, NTA receives NetFlow data as soon as your device is added to the Orion database.

For step-by-step instructions on adding nodes to the Orion database, see the [SolarWinds® Orion® Network Performance Monitor Evaluation Guide](#).

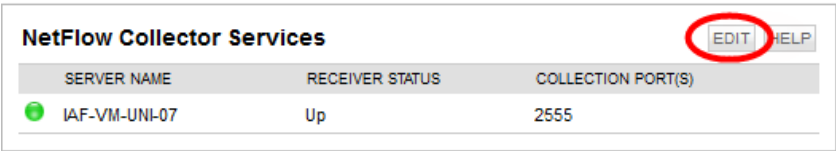
The following sections provide the required steps to start receiving NetFlow data from Flow-enabled devices on your network.

## Setting NetFlow Collector Services

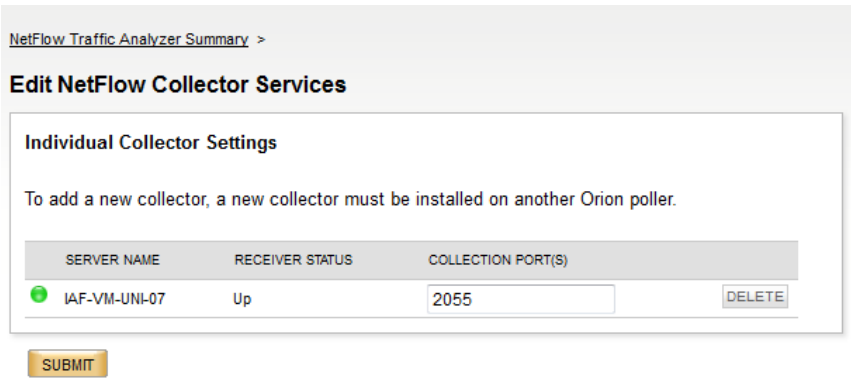
To enable proper collection of NetFlow data, NTA's NetFlow Collector Services must be listening on the correct port. NetFlow data defaults to port 2055.

### To set NetFlow Collector Services to port 2055:

1. Log on to the NPM server that hosts NetFlow Traffic Analyzer.
2. Start the **Orion Web Console** in the Orion program folder.
3. Click **EDIT** in the NetFlow Collector Service panel in the NetFlow Traffic Analyzer Summary window.

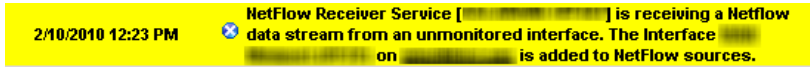


4. Type 2055 in the **COLLECTION PORT(S)** field and then click **SUBMIT**.

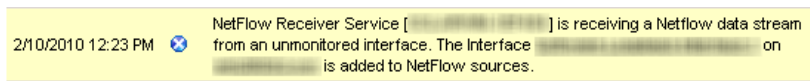


## Automatically Adding Flow- and CBQoS-enabled Devices

NTA can automatically add Flow- and CBQoS-enabled devices as NetFlow sources if they are configured to send Flows to your designated NTA server, as shown in the following message from the Last 25 Traffic Analysis Events resource.



NPM also provides the following message in the Last 25 Events resource when a source is detected and added.



By default on new installs, NTA detects Flow-enabled devices on your network as NetFlow sources and automatically adds them to your network.

For more information about managing new network devices, see [Adding Devices and Interfaces to the Orion Database](#) on page 13. For more information about configuring Flow-enabled devices, see [Device Configuration Examples](#) in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.

## Adding NetFlow Sources to NetFlow Traffic Analyzer

After your Flow-enabled device and its interfaces have been added to NPM, you must designate the device as a NetFlow source. The following procedure provides the steps required to add NetFlow sources to NTA.

**Note:** NTA only recognizes NetFlow version 9 templates that include all fields utilized by NetFlow version 5. For more information about the NetFlow templates NTA recognizes, see [NetFlow, IPIX, J-Flow, SFlow, and NetStream Requirements](#) in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.

### To add NetFlow devices and interfaces to NetFlow Traffic Analyzer:

1. Log on to the NPM server that hosts NetFlow Traffic Analyzer.
2. Start the **Orion Web Console** in the Orion program folder.

3. Log in to the Orion Web Console as an administrator.

4. Click **Manage Sources** in the header of the NetFlow Sources resource.

## NetFlow Sources

887 INTERFACES

[MANAGE SOURCES](#)
[EDIT](#)
[HELP](#)

| ROUTER                                                                            | INTERFACE          | TRAFFIC IN | TRAFFIC OUT | LAST RECEIVED NETFLOW | LAST RECEIVED CBQOS |
|-----------------------------------------------------------------------------------|--------------------|------------|-------------|-----------------------|---------------------|
|  | Bas-2505           |            |             | 7/25/12 6:55 PM       | never               |
|  | Bas-2621           |            |             | 7/25/12 6:55 PM       | never               |
|  | Bas-ForeES         |            |             | 7/25/12 6:55 PM       | never               |
|  | Bas-HP5400         |            |             | 7/25/12 6:55 PM       | never               |
|  | cur-3725           |            |             | never                 | 7/17/12 3:40 PM     |
|  | ICMP - 10.199.4.13 |            |             | 7/25/12 6:55 PM       | never               |
|  | Tex-2821.tex       |            |             | 7/25/12 6:55 PM       | never               |

5. Select **Exporters Only (last 15 minutes)** from the Showing menu.

NetFlow Traffic Analyzer Summary >

## Manage NetFlow Sources and CBQoS Polling

Interfaces grouped by vendor, router

882 interfaces currently selected, viewing 882 interfaces

Show Exporters only (last 15 minutes)

|                      | NetFlow<br><input type="checkbox"/> | CBQoS<br><input checked="" type="checkbox"/> | Globally enabled<br>(edit_settings) |  |
|----------------------|-------------------------------------|----------------------------------------------|-------------------------------------|--|
| + Cisco              | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/>          |                                     |  |
| + Fore Systems, Inc. | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/>          |                                     |  |
| + HP                 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/>          |                                     |  |
| + Unknown            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/>          |                                     |  |

SUBMIT CANCEL

6. Expand the device list to see all monitored nodes, check the options (NetFlow and/or CBQoS) for the parent nodes of the interfaces you want NTA to monitor, and then click **Submit**.

NetFlow Traffic Analyzer Summary >

### Manage NetFlow Sources and CBQoS Polling

Interfaces grouped by vendor, router

882 interfaces currently selected, viewing 882 interfaces

Show: Exporters only (last 15 minutes) ▾

|              | NetFlow                             | CBQoS                               | Globally enabled<br>( <a href="#">edit settings</a> ) |                                                            |
|--------------|-------------------------------------|-------------------------------------|-------------------------------------------------------|------------------------------------------------------------|
| <b>Cisco</b> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                                                       | <input type="text"/> <input type="button" value="Search"/> |
| Bas-2505     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                       |                                                            |
| Ethernet0    | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                                       |                                                            |
| Serial0      | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                                       |                                                            |
| Serial1      | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                                       |                                                            |
| Loopback0    | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                                       |                                                            |
| if-249       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-250       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-251       | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-252       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-253       | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-254       | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-255       | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-256       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-257       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                       |                                                            |
| if-258       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                       |                                                            |

**Note:** For pure CBQoS devices—those that do not export NetFlow—use **Show** to filter for **Cisco only** or **All Devices** and then check the CBQoS box.

NTA should receive traffic data and display it within a few minutes.



---

## Chapter 3

# NetFlow Traffic Analyzer Quick Tour

NetFlow Traffic Analyzer (NTA) gives highly detailed insight into the quantity and the quality of traffic on your network. This chapter is most useful when read from start to finish. It begins with an overview of the resources immediately available on the NetFlow Traffic Analyzer Summary view, and it continues with summaries of the most often used NTA views. The sections of this chapter build on each other sequentially, to show you NTA's key features.

**Note:** Extensive use cases, including scenarios incorporating other SolarWinds tools, are available in the final chapter of this Evaluation Guide. For more information, see [Using NetFlow Traffic Analyzer](#) on page 37.

Before we start the NTA quick tour, we must explain two terms: **view** and **resource**.

**View** is a web page showing information about your network and the traffic going through individual nodes and interfaces. Views consist of resources. You can customize which resources you want to have on a view.

NTA provides two basic types of views:

- **Summary views** show traffic details on all nodes and interfaces managed by your NTA, such as top applications, conversations, and endpoints. You can access your summary views either in the NETFLOW Views menu bar or by clicking an item in another view. For example, clicking on an application in the Top 5 Applications Summary view displays a summary view covering the use of the selected application in all nodes monitored in NTA. For more information about customizing the menu bar, see the *NetFlow Traffic Analyzer Administrator Guide*.
- **Detail views** show traffic information on individual objects in your network, such as interface details, node details, and application details. You can access your detail views by opening a summary view and clicking on the object whose details you want to see.

**Resource** is a building block of your views, it displays on your views as a box and provides information about different aspects of traffic monitoring, usually in a chart and a table. Some resources are meant to be used on summary views, some are suitable for detail views, and some can be useful on both view types. The information shown pertains to either all devices NTA monitors (if used on a summary view) or to the selected object (if used on a detail view for a node, interface, conversation, application, CBQoS class, or other object).

## Starting NetFlow Traffic Analyzer

To start NetFlow Traffic Analyzer, start the **Orion Web Console** in the Orion program folder. For more information about installing and configuring NTA, see [Installing NetFlow Traffic Analyzer](#) on page 5.

## Using Search and Filtering Tools

NTA views are extremely customizable and display a lot of traffic data organized by different resources. To quickly navigate in your views, NTA provides you with the following tools:

- **Flow Navigator** allows you to define and apply a filter to NTA-collected data, so that the displayed page shows only the information you need. You can also bookmark a filtered view or add it on your Views menu bar. For more information, see [Using the Flow Navigator](#) on page 45.
- **Search field** in the top right corner of the view allows you to search for endpoints or application/ports. For more information, see [Using the Search by Endpoint or Application/Port Tool](#) on page 43.

## The NetFlow Traffic Analyzer Summary

When you launch NetFlow Traffic Analyzer, the NetFlow Traffic Analyzer Summary is the first view displayed. This view provides insight into data traffic conditions over your entire network. The following resources are included in the NetFlow Traffic Analyzer Summary View by default.

## NetFlow Sources

This resource provides a list of all Flow- and CBQoS-enabled devices on your network that are currently configured to send NetFlow data to the server hosting your NTA installation. For more information about adding Flow-enabled devices, see [Enabling Flow Analysis](#) on page 13.

Click + next to any router name to display Flow- and CBQoS-enabled interfaces on the selected router.

| NetFlow Sources                                                                              |                                  |             |             |                       |                     | MANAGE SOURCES | EDIT | HELP |
|----------------------------------------------------------------------------------------------|----------------------------------|-------------|-------------|-----------------------|---------------------|----------------|------|------|
| 8 INTERFACES                                                                                 |                                  |             |             |                       |                     |                |      |      |
| ROUTER                                                                                       | INTERFACE                        | TRAFFIC IN  | TRAFFIC OUT | LAST RECEIVED NETFLOW | LAST RECEIVED CBQOS |                |      |      |
|  Cisco    | FlowSource                       |             |             | 2/11/10 3:29 PM       | 2/11/10 3:29 PM     |                |      |      |
|  Mikrotik | FastEthernet0/0 - Public Network |             |             |                       |                     |                |      |      |
| Interface to <MCI> NOC # <FILL IN> Acct. # <utw00                                            |                                  | 1165.33 bps | 29.42 Kbps  | 2/11/10 3:29 PM       | 2/11/10 3:29 PM     |                |      |      |

Interfaces are also listed with both a status icon and a timestamp indicating when NTA last received NetFlow data from the selected interface. Additionally, the NetFlow Sources resource provides reported values (as polled by NPM) for both incoming and outgoing traffic on each interface.

**Note:** Since NetFlow Sources display values as polled by NPM, these numbers may differ from those displayed in NTA charts.

| NetFlow Sources                                                                              |                                                   |             |             |                       |                     | MANAGE SOURCES | EDIT | HELP |
|----------------------------------------------------------------------------------------------|---------------------------------------------------|-------------|-------------|-----------------------|---------------------|----------------|------|------|
| 8 INTERFACES                                                                                 |                                                   |             |             |                       |                     |                |      |      |
| ROUTER                                                                                       | INTERFACE                                         | TRAFFIC IN  | TRAFFIC OUT | LAST RECEIVED NETFLOW | LAST RECEIVED CBQOS |                |      |      |
|  FlowSource |                                                   |             |             | 2/11/10 3:29 PM       | 2/11/10 3:29 PM     |                |      |      |
|             | FastEthernet0/0 · Public Network                  |             |             |                       |                     |                |      |      |
|                                                                                              | Interface to <MCI> NOC # <FILL IN> Acct. # <utw00 | 1165.33 bps | 29.42 Kbps  | 2/11/10 3:29 PM       | 2/11/10 3:29 PM     |                |      |      |

Clicking a router name opens the NetFlow Node Details view, and clicking an interface name opens the NetFlow Interface Details view. For more information about the NetFlow Node Details view, see [NetFlow Node Details View](#) on page 33. For more information about the NetFlow Interface Details view, see [NetFlow Interface Details View](#) on page 30.

## Top 10 NetFlow Sources by % Utilization

This resource provides a list of the NetFlow sources on your network that are currently routing enough traffic to significantly tax their system resources.

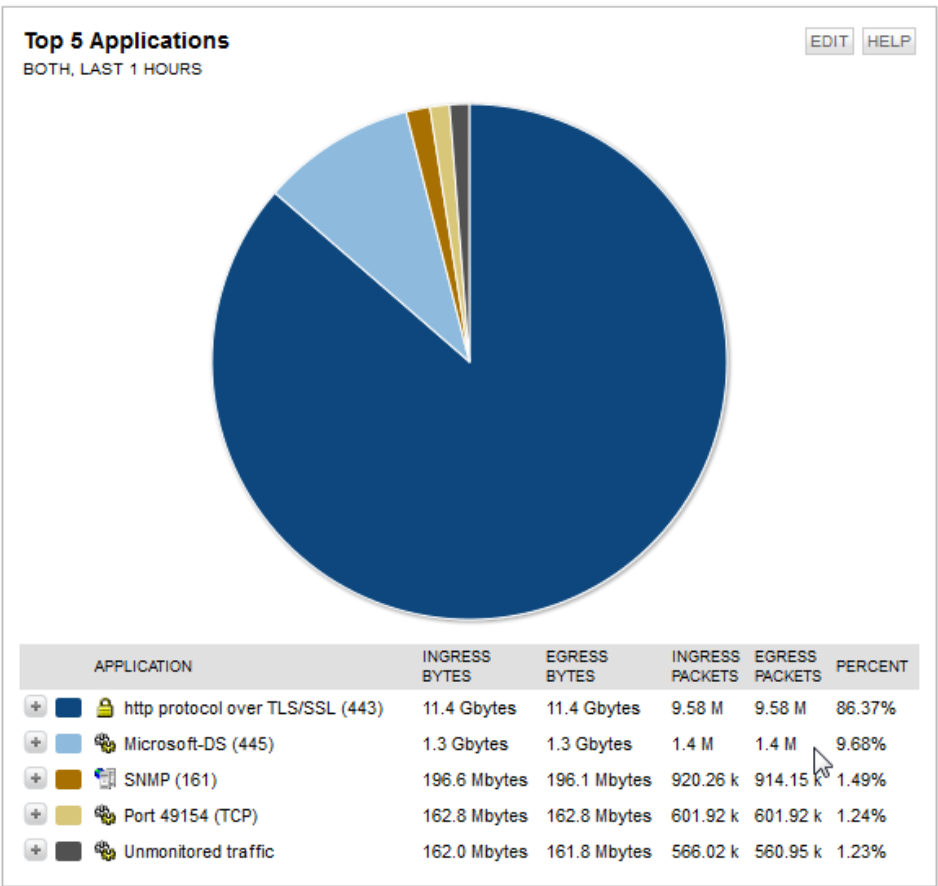
**Note:** Sources are only listed if they experience utilization in excess of 1%. Clicking on displayed interface opens NetFlow Interface Details.

| Top 10 NetFlow Sources by % Utilization                          | EDIT | HELP |
|------------------------------------------------------------------|------|------|
| All monitored interfaces are consuming less than 1% utilization. |      |      |

## Top 5 Applications

The Top 5 Applications resource provides a quick view of the applications and ports that are most in use by the devices on your network.

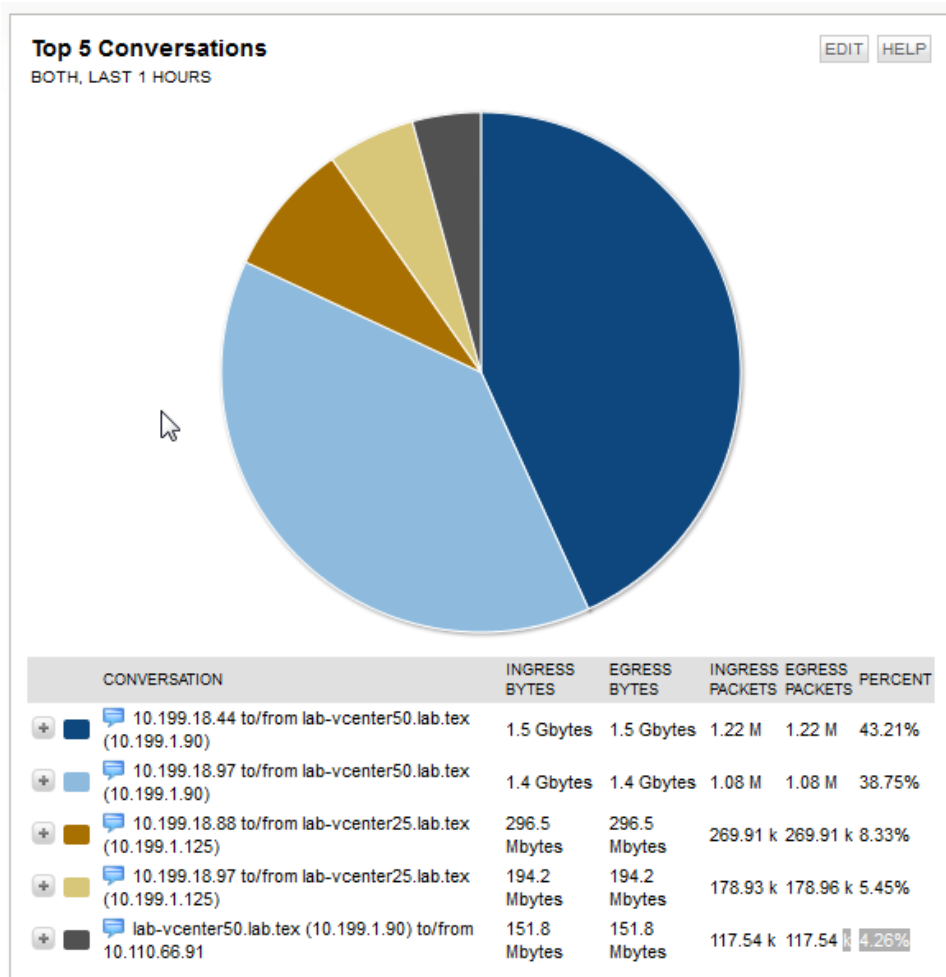
By clicking +, you can expand each application to see the network devices routing traffic for each application.



## Top 5 Conversations

This resource provides view of the conversations using the most bandwidth on your network. Each color in the chart corresponds to a single continuing conversation between two specific endpoints. The table below the chart lists the endpoints involved in each conversation, with the bandwidth consumed by each conversation, in both bytes and packets.

Click + to expand the conversation description to see all devices on your network through which the selected conversation is conducted. The first level of expansion shows the network nodes through which conversation traffic is routed. The next level of expansion shows the interfaces that are passing traffic for the selected conversation.

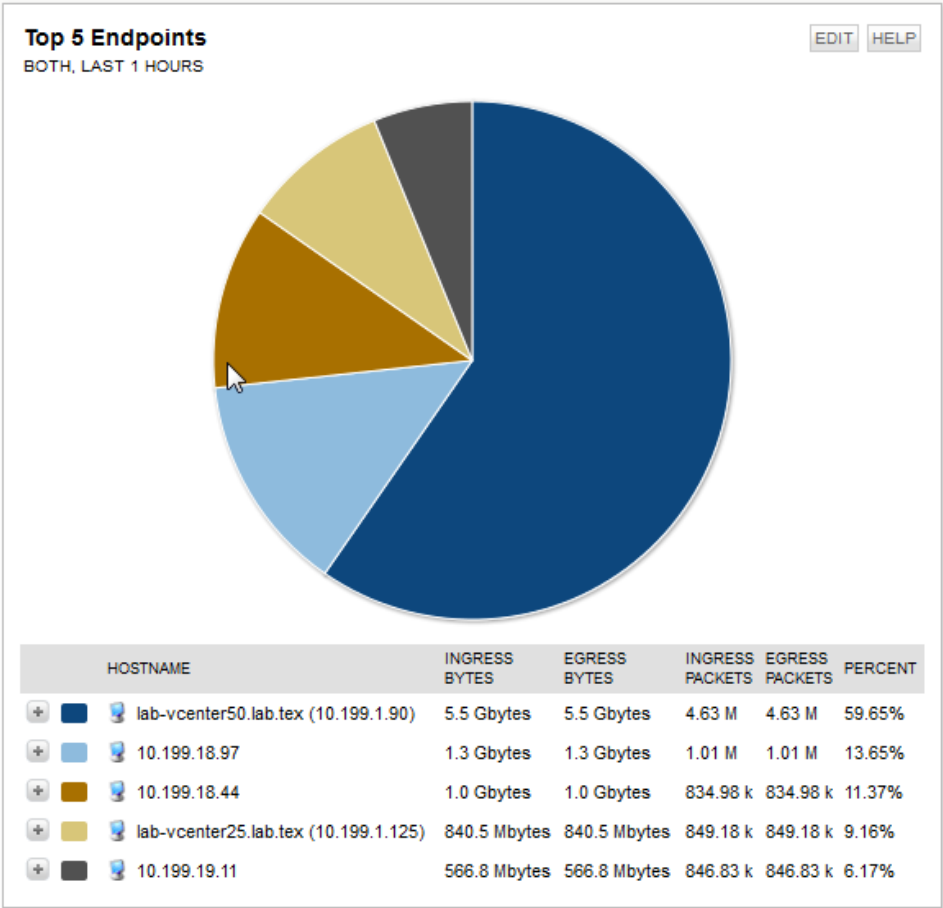


At both the node and interface levels, respective shares of the total bandwidth consumed by the selected conversation are listed in both bytes and packets. For any node, the conversation traffic on the node is equal to the sum of the conversation traffic on all the interfaces on that node.

For more information, see [NetFlow Conversations View](#) on page 27.

## Top 5 Endpoints

The Top 5 Endpoints resource gives an at-a-glance view of the endpoints that are the sources or targets of the most network traffic. By clicking + to expand each endpoint, you can see the network devices routing traffic for each endpoint.



## Last 25 Traffic Analysis Events

This resource lists the last 25 NetFlow-specific events that have occurred to devices on your monitored network. Typically, this resource lists the dates and times when the NetFlow Receiver Service stops and starts, but it is also used to communicate updates for database upgrades and to provide notification of newly discovered Flow sources.

| Last 25 Traffic Analysis Events |                                                                                                                                                              | EDIT | HELP |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|
| 8/14/2008 3:09 AM               |  NetFlow Receiver Service [WIN2K3SQLSERVER] Started- listening on Port=2055 |      |      |
| 8/11/2008 8:57 AM               |  NetFlow Receiver Service [WIN2K3SQLSERVER] Started- listening on Port=2055 |      |      |
| 8/11/2008 8:57 AM               |  NetFlow Receiver Service [WIN2K3SQLSERVER] Stopped                         |      |      |
| 8/11/2008 8:56 AM               |  NetFlow Receiver Service [WIN2K3SQLSERVER] Started- listening on Port=2055 |      |      |
| 8/11/2008 8:54 AM               |  NetFlow Receiver Service [WIN2K3SQLSERVER] Stopped                         |      |      |

## NetFlow Traffic Analyzer Views

The following sections detail the types of information that are available by default on selected NTA views.

### Notes:

- The following are a few of the NTA views that are used in most typical installations. These listed views are linked directly from default resources on the NetFlow Traffic Analyzer Summary view. Additional resources available on the NetFlow Traffic Analyzer Summary view and on subsequent NTA views link to additional views. For more information about NTA views and resources, see [Viewing NetFlow Traffic Analyzer Data in the Orion Web Console](#) in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.
- Some resources may not be present in the default configuration of a selected view. To see all available resources, you must edit the view with the Customize Page options. For more information, see [Viewing NetFlow Traffic Analyzer Data in the Orion Web Console](#) in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.

## NetFlow Application View

The following sections offer brief descriptions of the resources on the NetFlow Application view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

## **Application Details**

The Application Details resource provides a table that contains the relevant application name, port used by the application, total amount of traffic data within the selected period of time, and the total number of packets sent within the selected period of time.

## **Top 5 Protocols**

The Top 5 Protocols resource provides a view of the traffic protocols the selected application uses most. The table below the chart provides the protocol type, the amount of data, the total number of packets, and the percentage of all traffic that has been using each listed protocol.

## **Top 5 Types of Service**

The Top 5 Types of Service resource provides a view of the most active services employed by the selected application. The table below the chart provides the type of service, the amount of traffic handled by the service, the number of packets handled by the service, and the percentage of all serviced traffic to the selected application that is handled by the selected type of service

## **Total Bytes Transferred**

The Total Bytes Transferred resource displays a chart that details the total number of bytes that are transferred by the selected application over a specified period of time.

## **Unique Visitors**

The Unique Visitors resource provides a chart that details the number of unique IP addresses that have used the selected application over a specified period of time.

## **Total Packets Transferred**

The Total Packets Transferred resource displays a chart that details the total number of packets transferred by the selected application over a specified period of time.

## **Top 5 Transmitters**

The Top 5 Transmitters resource provides a view of the most active transmitting endpoints using the selected application. The table below the chart provides the name or IP address of the endpoint, the amount of traffic that is transmitted by the endpoint, and the percentage of all transmitted traffic that is traceable to the endpoint.

You can click each listed endpoint to open the NetFlow Endpoint view that presents similar statistics for each transmitting endpoint. For more information, see [NetFlow Endpoint View](#) on page 28.

### **Top 5 Receivers**

The Top 5 Receivers resource provides a view of the most active receiving endpoints using the selected application. The table below the chart provides the name or IP address of the endpoint, the amount of traffic that is received by the endpoint, and the percentage of all received traffic that is traceable to the endpoint.

You can click each listed endpoint to open the NetFlow Endpoint view that presents similar statistics for each receiving endpoint. For more information, see [NetFlow Endpoint View](#) on page 28.

### **Top 5 Traffic Sources by Country**

The Top 5 Traffic Sources by Country resource provides a view of the countries where traffic on the selected application originates, ranked by percentage of total application traffic. The table below the chart provides the name of the country, the amount of traffic that is sourced in the country, and the percentage of all traffic that is traceable to the country.

### **Top 5 Traffic Destinations by Country**

The Top 5 Traffic Destinations by Country resource provides a view of the countries that serve as destinations of traffic on the selected application, ranked by percentage of total application traffic. The table below the chart provides the name of the country, the amount of application traffic that is routed to endpoints in the country, and the percentage of all application traffic traceable to endpoints in the country.

### **Top 5 Conversations**

The Top 5 Conversations resource provides a list of the most bandwidth-heavy conversations routed through the selected device, using the selected application. Conversations are listed with the amount of data transferred in the conversation, in both bytes and packets, and the percentage of total application traffic generated by the conversation. Clicking a conversation opens the NetFlow Conversation view for the selected conversation. For more information, see [NetFlow Conversations View](#) below.

## **NetFlow Conversations View**

The following sections offer brief descriptions of the resources on the NetFlow Conversation view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

### **Total Bytes Transferred**

The Total Bytes Transferred resource displays a chart detailing the total number of bytes transferred, over a specified period of time, between the two nodes, IP addresses, or domains indicated in the view title.

### **Conversation Traffic History**

The Conversation Traffic History resource provides a table displaying the date/time stamp of the exchange, the protocol used for the exchange, the application and port used for the exchange, the direction of the traffic flow, the amount of traffic communicated in bytes, and the equivalent number of packets communicated.

## **NetFlow Endpoint View**

The following sections offer brief descriptions of the resources on the NetFlow Endpoint view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

### **Endpoint Details**

The Endpoint Details resource provides the following information about a selected endpoint:

- IP address
- Hostname
- IP address group
- Domain
- Country
- Total traffic transmitted
- Total traffic received

### **Top 25 Conversation Endpoints**

This resource provides a list of the endpoints with which the currently viewed endpoint has transferred the most data. For each conversation, this resource reports the amount of data transferred in the conversation and the percentage the listed conversation represents of the total data transferred by the viewed endpoint. Clicking an endpoint opens the NetFlow Endpoint view for the selected endpoint. All other links for a listed endpoint open the NetFlow Conversation view for the conversation between the viewed and selected endpoints. For more information, see [NetFlow Conversations View](#) on page 27.

### **Total Packets Transferred**

The Total Packets Transferred resource displays a chart displaying the total number of packets both transmitted from the viewed endpoint and received by the viewed endpoint over a specified period of time.

**Total Bytes Transferred**

The Total Bytes Transferred resource displays a chart detailing the total number of bytes both transmitted from the viewed endpoint and received by the viewed endpoint, over a specified period of time.

**Top 5 Protocols**

The Top 5 Protocols resource provides an at-a-glance view of the traffic protocols that the selected endpoint uses most. The table below the chart provides the protocol type, the amount of data, the total number of packets, and the percentage of all traffic that has been using each listed protocol.

**Top 5 Applications**

The Top 5 Applications resource provides a quick view of the applications used most by the selected endpoint. The table below the chart provides the application name, the amount of data that is flowing, the equivalent total number of packets, and the percentage of all traffic that is traceable to use of the listed application by the selected endpoint. Clicking an application opens the NetFlow Application view. For more information, see [NetFlow Application View](#) on page 25.

**Top 5 Traffic Sources by Country**

The Top 5 Traffic Sources by Country resource provides an at-a-glance view, in the form of a chart, of the countries where traffic to the selected endpoint originates, ranked by percentage of total traffic to the selected endpoint. The table below the chart provides the name of the country sourcing traffic to the viewed endpoint, the amount of traffic routed to the endpoint from the listed country, and the percentage of all traffic routed to the viewed endpoint that is traceable to the listed country.

**Top 5 Traffic Destinations by Country**

The Top 5 Traffic Destinations by Country resource provides a chart and table of the countries hosting destinations of traffic from the selected endpoint, ranked by percentage of total traffic from the selected endpoint. The table below the chart provides the name of the country to which traffic is routed, the amount of traffic routed to servers in the listed country, and the percentage of all routed traffic from the viewed endpoint that is routed to servers in the listed country.

**Unique Visitors**

The Unique Visitors resource provides a chart of unique IP addresses that have communicated with the viewed endpoint over a specified period of time.

**Top 5 Traffic Destinations by Domain**

The Top 5 Traffic Destinations by Domain resource provides a chart and table of the domains hosting destinations of traffic from the selected endpoint, ranked by percentage of total traffic from the selected endpoint. The table below the chart

provides the name of the domain to which traffic is routed, the amount of traffic routed to servers in the listed domain, and the percentage of all routed traffic from the viewed endpoint that is routed to servers in the listed domain.

### **Top 5 Traffic Sources by Domain**

The Top 5 Traffic Sources by Domain resource provides a chart and table of the domains hosting sources of traffic from the selected endpoint, ranked by percentage of total traffic from the selected endpoint. The table below the chart provides the name of the domain to which traffic is routed, the amount of traffic routed to servers in the listed domain, and the percentage of all routed traffic from the viewed endpoint that is routed to servers in the listed domain.

### **Top 5 IP Group Conversations**

The Top 5 IP Groups Conversations resource provides a chart and table of the conversations generating traffic from the selected endpoint, ranked by percentage of total traffic. The table below the chart provides the name of the IP Group to which traffic is routed, the amount of traffic routed to servers in the listed IP Group, and the percentage of all routed traffic from the viewed endpoint that is routed to servers in the listed IP Group.

### **Top 5 Types of Service**

The Top 5 Types of Service resource provides a quick view of the services most actively employed by the selected endpoint. The table below the chart provides the type of service, the amount of traffic in bytes and packets that is handled by the service, and the percentage of all serviced traffic to the selected endpoint that is handled by the selected type of service.

For more information about service type monitoring in NTA, see [Configuring NetFlow Types of Service](#) in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.

## **NetFlow Interface Details View**

The following sections offer brief descriptions of the resources on the default NetFlow Interface Details view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

**Note:** For the NetFlow Node Details View, and the NetFlow Interface Detailed View, and for any managed Orion device, you can add endpoint-centric resources that filter information regarding the node in terms of all standard NTA filters, giving you relevant traffic initiation and termination information. For information on adding such resources, see [Adding an Endpoint Centric Resource](#).

### **Top 5 Protocols**

The Top 5 Protocols resource provides a view of the traffic protocols the viewed interface sees most. The table below the chart provides the protocol type, the amount of data, the total number of packets, and the percentage of all traffic over the viewed interface using each listed protocol.

### **Top 5 Applications**

The Top 5 Applications resource provides a quick view of the applications used most by the viewed interface. The table below the chart provides the application name, the amount of data that is flowing, the equivalent total number of packets, and the percentage of all traffic that is traceable to use of the listed application by the viewed interface. Clicking an application opens the NetFlow Application view. For more information, see [NetFlow Application View](#) on page 25.

### **Top 5 Conversations**

This resource provides a list of conversations creating the most traffic over the viewed interface. For each conversation, this resource reports the amount of data transferred in the conversation and the percentage the listed conversation represents of the total data transferred over the viewed interface. Clicking a conversation opens the NetFlow Conversation view for the selected conversation. For more information, see [NetFlow Conversations View](#) on page 27.

### **CBQoS Pre-Policy Class Map**

If you are viewing a CBQoS-enabled interface to which a CBQoS policy is currently applied, this resource displays the classes of traffic traversing the viewed interface. For each class of defined traffic, the table below the chart reports the average and most recently polled interface utilization values as a percentage of total defined interface bandwidth as measured before any traffic-shaping CBQoS policy is applied on the viewed interface.

### **CBQoS Post-Policy Class Map**

If you are viewing a CBQoS-enabled interface to which a CBQoS policy is currently applied, this resource displays the classes of traffic traversing the viewed interface. For each class of defined traffic, the table below the chart reports the average and most recently polled interface utilization values as a percentage of total defined interface bandwidth as measured after any traffic-shaping CBQoS policy is applied on the viewed interface.

### **CBQoS Policy Details**

If you are viewing a CBQoS-enabled interface to which a CBQoS policy is currently applied, this resource displays the applied traffic policies, corresponding defined traffic classes and nested policies on the viewed interface. For each defined traffic class, this resource provides the amount of traffic and corresponding percentage of total defined interface bandwidth over both the last hour and the last 24 hours.

### **CBQoS Drops**

If you are viewing a CBQoS-enabled interface to which a CBQoS policy is currently applied, this resource displays the amount of traffic traversing the viewed interface that is dropped as a result of CBQoS policy application. For each class of defined traffic, the table below the chart reports the average and most recently polled interface utilization values as a percentage of total defined interface bandwidth corresponding to the amount of traffic that is dropped as a result of CBQoS policy application.

### **Top 5 Endpoints**

The Top 5 Endpoints resource provides a view of the endpoints producing the most traffic over the selected interface. The table below the chart provides the name or IP address of each listed endpoint, the amount of traffic from each listed endpoint, in both bytes and packets, and the percentage of all traffic over the viewed interface that is traceable to each listed endpoint. Clicking an endpoint opens the NetFlow Endpoint view for the selected endpoint. For more information, see [NetFlow Endpoint View](#) on page 28.

### **Top 5 Traffic Destinations by Domain**

The Top 5 Traffic Destinations by Domain resource provides a chart and table of the domains hosting destinations of traffic from the selected interface, ranked by percentage of total traffic. The table below the chart provides the name of the domain to which traffic is routed, the amount of traffic routed to servers in the listed domain, and the percentage of all routed traffic from the viewed interface that is routed to servers in the listed domain.

### **Top 5 Traffic Sources by Domain**

The Top 5 Traffic Sources by Domain resource provides a chart and table of the domains hosting sources of traffic from the selected interface, ranked by percentage of total traffic from the selected interface. The table below the chart provides the name of the domain to which traffic is routed, the amount of traffic routed to servers in the listed domain, and the percentage of all routed traffic from the viewed interface that is routed to servers in the listed domain.

## **Top 5 IP Group Conversations**

The Top 5 IP Groups Conversations resource provides a chart and table of the conversations generating traffic from the selected interface, ranked by percentage of total traffic. The table below the chart provides the name of the IP Group to which traffic is routed, the amount of traffic routed to servers in the listed IP Group, and the percentage of all routed traffic from the viewed interface that is routed to servers in the listed IP Group.

## **Top 5 Domains**

This resource provides a view of the domains producing the most traffic on the selected interface. The table below the chart provides the domain name, the amount of traffic in bytes, the total number of packets communicated, and the percentage of all traffic on the selected interface that is traceable to each domain.

**Note:** This resource is only available if persistent DNS resolution is enabled. On evaluation installations, DNS resolution is set to persistent by default. For more information, see [Configuring DNS and NetBIOS Resolution](#) in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.

## **Top 5 Types of Service**

The Top 5 Types of Service resource provides a quick view of the services most actively employed by the viewed interface. The table below the chart provides the type of service, the amount of traffic in bytes and packets that is handled by the service over the viewed interface, and the percentage of all serviced traffic over the viewed interface that is handled by the selected type of service.

For more information about service type monitoring in NTA, see [Configuring NetFlow Types of Service](#) in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.

## **NetFlow Node Details View**

The following sections offer brief descriptions of the resources on the default NetFlow Node Details view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

**Note:** For the NetFlow Node Details View, and the NetFlow Interface Detailed View, and for any managed Orion device, you can add endpoint-centric resources that filter information regarding the node in terms of all standard NTA filters, giving you relevant traffic initiation and termination information. For information on adding such resources, see [Adding an Endpoint Centric Resource](#).

## **Top 5 Protocols**

The Top 5 Protocols resource provides a view of the traffic protocols the viewed node uses most. The table below the chart provides the protocol type, the amount of data, the total number of packets, and the percentage of all traffic on the viewed node using each listed protocol.

## **Top 5 Applications**

The Top 5 Applications resource provides a quick view of the applications used most by the viewed node. The table below the chart provides the application name, the amount of data that is flowing, the equivalent total number of packets, and the percentage of all traffic that is traceable to use of the listed application by the viewed node. Clicking an application opens the NetFlow Application view. For more information, see [NetFlow Application View](#) on page 25.

## **Top 5 Conversations**

This resource provides a list of conversations that are creating the most traffic over the viewed node. For each conversation, this resource reports the amount of data transferred in the conversation and the percentage the listed conversation represents of the total data transferred over the viewed node. Clicking a conversation opens the NetFlow Conversation view for the selected conversation. For more information, see [NetFlow Conversations View](#) on page 27.

## **Top 5 Endpoints**

The Top 5 Endpoints resource provides both a chart and a table view of the endpoints producing the most traffic over the viewed node. The table below the chart provides the name or IP address of each listed endpoint, the amount of traffic from each listed endpoint, in both bytes and packets, and the percentage of all traffic over the viewed node that is traceable to each listed endpoint. Clicking an endpoint opens the NetFlow Endpoint view for the selected endpoint. For more information, see [NetFlow Endpoint View](#) on page 28.

## **Top 5 Domains**

This resource provides an at-a-glance view of the domains that are producing the most traffic on the viewed node. The table below the chart provides the domain name, the amount of traffic in bytes, the total number of packets communicated, and the percentage of all traffic on the viewed node traceable to each domain.

**Note:** This resource is only available if persistent DNS resolution is enabled. By default on evaluation installations, DNS resolution is configured to occur on demand only. For more information, see [Configuring DNS and NetBIOS Resolution](#) in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.

**Node Interfaces**

This resource provides a list of all monitored interfaces on the viewed node. For each interface, both incoming and outgoing traffic are reported. Clicking an interface opens the NetFlow Interface Details view for the selected interface. For more information, see [NetFlow Interface Details View](#) on page 30.



## Chapter 4

# Using NetFlow Traffic Analyzer

While Orion Network Performance Monitor can tell you the bandwidth usage on an interface, NTA takes this ability one step further, by providing information about the actual user of that bandwidth and the applications they are using. The scenarios presented in this chapter illustrate the value of NTA and how it can immediately offer you a significant return on your investment.

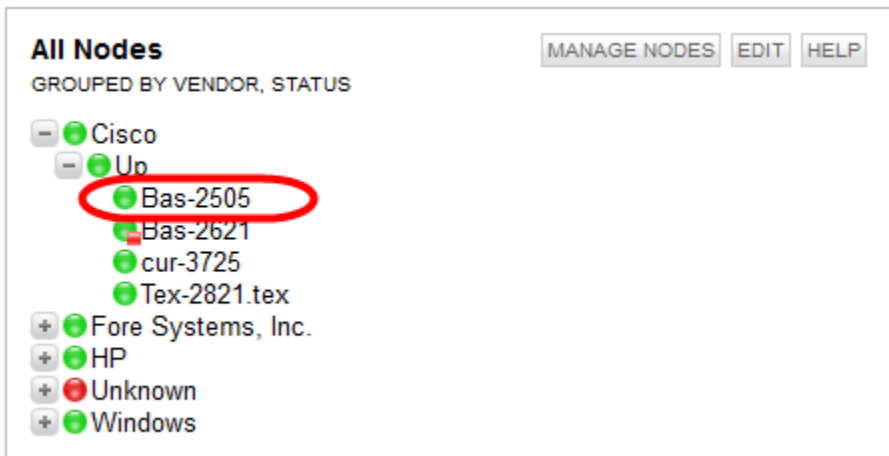
## *Adding Endpoint Centric Resources to Orion Nodes*

Using **Customize Page**, you can add an endpoint-centric resource to the Node Details or Interface Details view on any node in Network Performance Manager.

**Note:** An endpoint centric resource displays information related to a concrete node, which is also an endpoint.

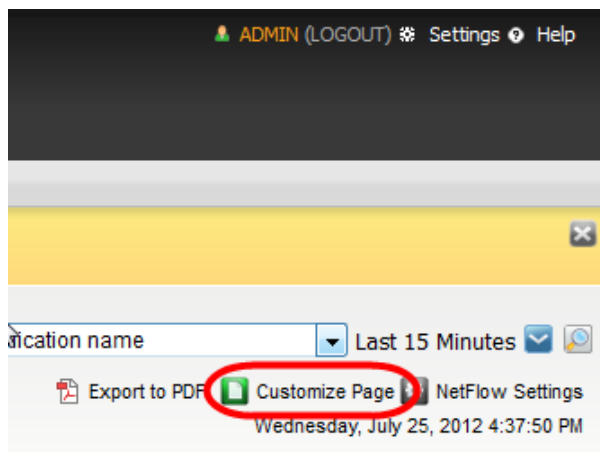
**To add an endpoint-centric resource:**

1. Open the Orion Web Console.
2. Click the relevant node in All Nodes on the HOME page.



If nodes on All Nodes are grouped, drill down as needed into the relevant group.

3. Click **Customize Page** on the Node Details view.



4. Click + over the column in which you want the new resource to be placed.

### Customize Node Details

Name

Type of view: **NodeDetails**

Column 1 Width: **450**

Column 2 Width: **640**

#### Resources in Column 1

- Average Response Time & Packet I
- CPU Load & Memory Utilization
- Node Details
- Event Summary
- Polling Details
- Availability Statistics
- Custom Properties for Nodes
- EnergyWise Node Details
- All Dependencies including \${Capti
- Virtual Machine Details
- Top XX Applications
- Top XX Conversations
- Top XX Conversations (Endpoint C

#### Resources in Column 2

- Multiple Interfaces Chart
- UCS Overview
- Average Response Time & Packet I
- Min/Max Average CPU Load
- Last 10 Errors & Failures
- Current Cisco Buffer Misses
- Current Percent Utilization of Each I
- Disk Volumes
- Active Alerts on This Node
- Device Power Consumption
- NPM Network Topology
- List of VSANs
- Connectivity Unit Status
- Sensor Details

5. Click **NetFlow Endpoint Centric Resources** and check the appropriate resource.

**Add Resources to Node Details Column 1**

- ☒ NetFlow Traffic Analyzer Summary - Summary Reports and Charts for NetFlow Traffic Analyzer
- ☒ Node Lists - All Nodes and Grouped Node Lists
- ☒ NetFlow Top Resources - Traffic Analyzer Resources suitable for all NetFlow views
- ☒ NetFlow Endpoint Centric Resources - Traffic Analyzer Resources analyzing node as communication endpoint
  - ☐ Top XX Applications (Endpoint Centric)
  - ☐ Top XX Conversations (Endpoint Centric)
  - ☐ Top XX Countries (Endpoint Centric)
  - ☐ Top XX Domains (Endpoint Centric)
  - ☒ Top XX Endpoints (Endpoint Centric)
  - ☐ Top XX IP Address Groups (Endpoint Centric)
  - ☐ Top XX IP Groups Conversations (Endpoint Centric)
  - ☐ Top XX Protocols (Endpoint Centric)
  - ☐ Top XX Receivers (Endpoint Centric)
  - ☐ Top XX Transmitters (Endpoint Centric)
  - ☐ Top XX Type of Services (Endpoint Centric)
  - ☐ Total Transferred Bytes (Endpoint Centric)
  - ☐ Total Transferred Packets (Endpoint Centric)
  - ☐ Unique Visitors (Endpoint Centric)

6. Click **Submit**.

7. Use the arrow controls to move the resources listed in the column into the order you want displayed in the Orion Web Console.

### Customize Node Details

Name

Type of view: **NodeDetails**

Column 1 Width: **450**

Column 2 Width: **640**

#### Resources in Column 1

|                                     |   |
|-------------------------------------|---|
| Average Response Time & Packet I    | + |
| CPU Load & Memory Utilization       | × |
| Node Details                        | + |
| Event Summary                       | + |
| Polling Details                     | + |
| Availability Statistics             | + |
| Custom Properties for Nodes         | + |
| EnergyWise Node Details             | + |
| All Dependencies including \$(Capti | + |
| Virtual Machine Details             | + |
| Top XX Applications                 | + |
| Top XX Conversations                | + |
| Top XX Endpoints (Endpoint Centri   | + |
| Top XX Conversations (Endpoint C    | + |

#### Resources in Column 2

|                                       |   |
|---------------------------------------|---|
| Multiple Interfaces Chart             | + |
| UCS Overview                          | × |
| Average Response Time & Packet I      | + |
| Min/Max Average CPU Load              | + |
| Last 10 Errors & Failures             | + |
| Current Cisco Buffer Misses           | + |
| Current Percent Utilization of Each I | + |
| Disk Volumes                          | + |
| Active Alerts on This Node            | + |
| Device Power Consumption              | + |
| NPM Network Topology                  | + |
| List of VSANs                         | + |
| Connectivity Unit Status              | + |
| Sensor Details                        | + |

8. Click **Done**.

## Adding Top Talker Statistics to Orion Alerts

Orion alerting software can alert on polled, syslog, and trap data. Alerts are defined in terms of thresholds related to data in the Orion database. Scans in the form of SQL queries at set intervals detect recorded values that exceed thresholds, triggering an alert if relevant conditions pertain.

When an Orion alert is triggered, the software evaluates suppression criteria. If an alert is not qualified to be suppressed, the software executes a defined action. If no action is defined, the software merely displays the alert on the web console.

Throughout this workflow timers are used to allow the software to do its work at each step and to ensure that the alerting workflow had appropriate redundancy for timely reporting of alerts.

For an excellent overview of alerting in Orion advanced alerts, see [Understanding Orion Advanced Alerts](#). For all specific information on Orion basic and advanced alerts, including detailed instructions for creating and managing them with the Orion Alert Manager, see [Creating and Managing Alerts](#), in the *Orion Network Performance Monitor Administrator's Guide*.

## Top Talker Advanced Alerts

When you install SolarWinds Orion Network Traffic Analyzer, the software automatically creates in the Orion Alert Manager two predefined alerts called “High Receive Percent Utilization with Top Talkers” and “High Transmit Percent Utilization with Top Talkers.”

The primary purpose of these alerts is to help in understanding what specific network traffic contributed most to reaching the set interface bandwidth utilization threshold, triggering the utilization threshold alert.

By default, these advanced alerts, when triggered, do two things: 1) write the bandwidth utilization event to the SolarWinds event log when the current percent utilization on the transmit side of an interface rises above specified value, and then again when the utilization drops back down below a specified value. 2) Initiate a web capture of the most current top talker information and then append and send that information in an email to the configured recipient.

The instructions in this section assume you are familiar with the Orion Alert Manager and already know how to setup an advanced alert.

For steps on creating an advanced alert see the sections on advanced alerts in [Creating and Managing Alerts](#) in the *Orion Network Performance Monitor Administrator's Guide*.

### To use the default NetFlow alert:

1. Start the **Advanced Alert Manager** in the Orion **Alerting, Reporting and Mapping** folder.
2. Navigate to the Manage Alerts resource (**View > Configure Alerts**).
3. Select the relevant top talker alert.
4. Click **Edit**.
  - a. On General, check **Enable this Alert** and select an appropriate **Alert Evaluation Frequency**.
  - b. On Trigger Condition, define the conditions in which the software launches the alert.

The default condition is the interface's transmit utilization percentage exceeding 75. You can adjust this condition or add conditions.

- c. On Reset Condition, define the conditions in which the software resets the alert.

The default condition is the interface's transmit utilization percentage going below 50. You can adjust this condition or add conditions.

- d. On Alert Suppression, define the conditions in which the software suppresses the alert.

The default condition is no suppression.

- e. On Time of Day, define the days and times during which the software actively evaluates the database for trigger conditions.

The default range is 24/7.

- f. On Trigger Actions, create actions to execute when the software triggers the alert.

As discussed, the default action writes to the SolarWinds event log, initiates a web capture of current top talkers transmitting on the over-utilized interface, and then append and send the information in email to an appropriate contact.

**Note:** On the **URL** tab, if you changed the default Orion login from 'Admin' with a blank password, then accordingly you will need to change the URL that the trigger action uses to send out the notification.

For example, if your new credentials were username **NTA User** with password **Bravo**, you would adjust the default URL so that:

```
$(SQL:SELECT REPLACE(REPLACE(Macro, '$$Password$$',
    ''), '$$User$$', 'Admin') FROM NetFlowAlertMacros WHERE
    ID='InWebMailInterfaceDetailsLink'}
```

becomes:

```
$(SQL:SELECT REPLACE(REPLACE(Macro, '$$Password$$',
    'Bravo'), '$$User$$', 'NTA User') FROM NetFlowAlertMacros WHERE
    ID='InWebMailInterfaceDetailsLink'}
```

- g. On Reset Conditions, define actions to execute when the software resets the alert.

As discussed, the default reset action writes to the SolarWinds event log.

5. Click **OK** and then click **Done**.

## Using the Search by Endpoint or Application/Port Tool

Using the Search tool, you can quickly locate any endpoint communicating with any devices or using a specific application on your network.

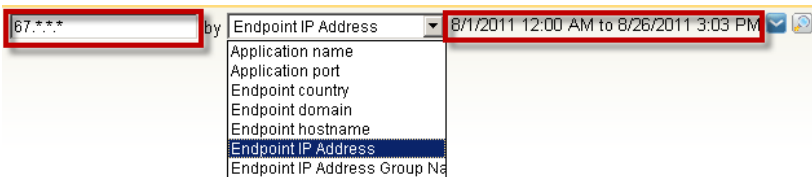
Search results provide an expandable list matching your search criteria. Clicking any result, followed by clicking the name of any of your network devices, opens the appropriate view—NetFlow Endpoint View or NetFlow Application View—for all traffic passing through the selected device.

For more information about the NetFlow Endpoint View, see [NetFlow Endpoint View](#) on page 28. For more information about the NetFlow Application View, see [NetFlow Application View](#) on page 25.

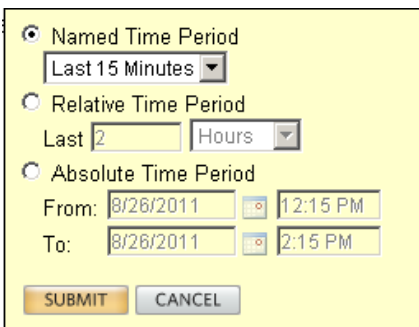
### Searching for Endpoints

To search for an endpoint:

1. Select the appropriate endpoint filter in the list.



2. Select a time period.



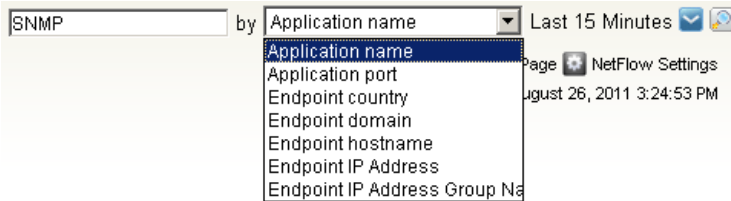
3. Enter the endpoint's IP address and then push **Enter**.

+ 67.195.160.127  
- 67.195.160.141  
DPARISWHITE-DEV  
MS TCP Loopback interface

## Searching for Application/Port

To search for an application/port:

1. Select the appropriate application filter in the list.

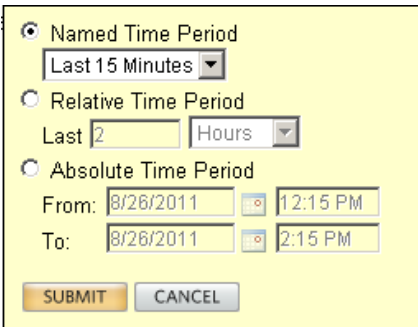


SNMP by Application name Last 15 Minutes

Application name  
Application port  
Endpoint country  
Endpoint domain  
Endpoint hostname  
Endpoint IP Address  
Endpoint IP Address Group Name

Page NetFlow Settings  
August 26, 2011 3:24:53 PM

2. Select a time period.



☒ Named Time Period  
Last 15 Minutes

☐ Relative Time Period  
Last 2 Hours

☐ Absolute Time Period  
From: 8/26/2011 12:15 PM  
To: 8/26/2011 2:15 PM

SUBMIT CANCEL

3. Enter the relevant application information and then push **Enter**.

- SSH Remote Login Protocol  
DPARISWHITE-DEV  
MS TCP Loopback interface

## Using the Flow Navigator

The Flow Navigator application allows you to filter your NTA views and add them directly to the Views toolbar. Also, because NTA is a web-based module, you can create browser bookmarks for any NTA view to easily check the status of potential trouble spots at a later date.

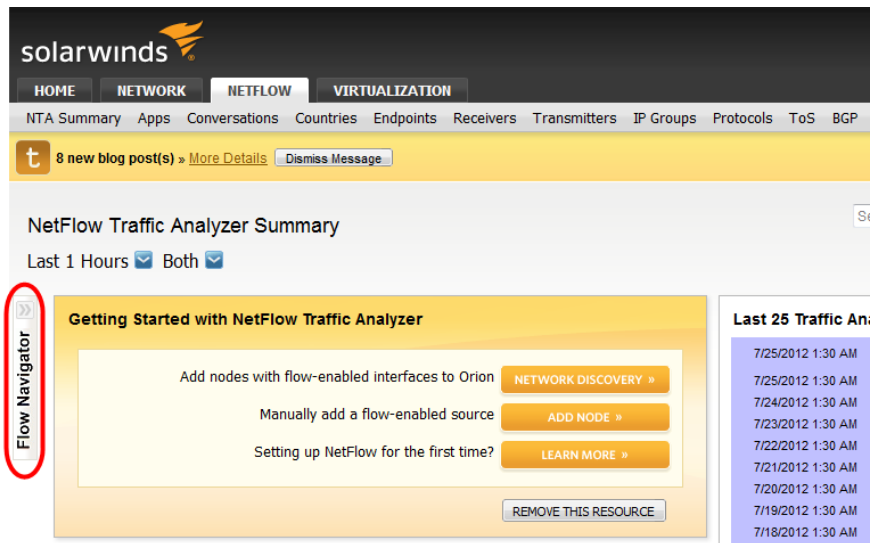
You can create custom traffic views directly from any NetFlow view, using the Flow Navigator. These custom filters allow you to view specific statistics about your entire network and its devices without having to navigate through the web console a single device view at a time. You can configure your custom traffic view to include devices, applications, time periods, and more, all from one configuration pane, as shown in the following procedures.

## Viewing Traffic for a Designated IP Address

The following procedure filters the current NTA view by showing both incoming and outgoing network traffic from a designated IP address.

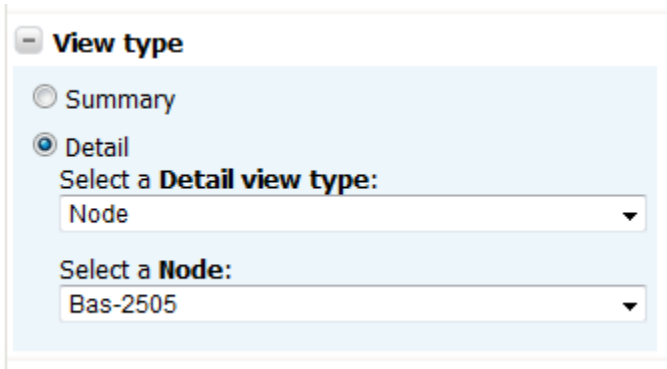
### To filter a NetFlow traffic view with the Flow Navigator:

1. Start the **Orion Web Console** in the Orion program folder.



3. Click **Flow Navigator** on the left edge of the summary view. (The Flow Navigator is available on any default NTA view.)

4. Select a view type.



**View type**

☐ Summary

☒ Detail

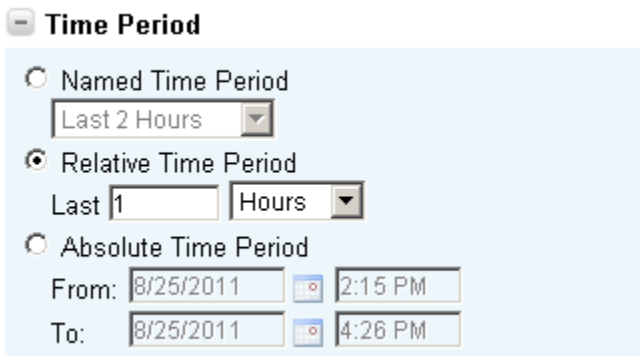
Select a **Detail view type**:

Node

Select a **Node**:

Bas-2505

- a. *If you want a filtered view of your entire network*, click **Summary**.
- b. *If you want a filtered view of traffic passing through a specific node and interface*, click **Detail**.
- Select the **Node** for which you want to monitor network traffic attributed to the selected view type.
  - Select the **Interface** for which you want to monitor network traffic attributed to the selected view type.
  - Select or type in the view-related information.
5. Select the **Time Period** from which you want to view traffic data, using any of the following options:



**Time Period**

☐ Named Time Period

Last 2 Hours

☒ Relative Time Period

Last 1 Hours

☐ Absolute Time Period

From: 8/25/2011 2:15 PM

To: 8/25/2011 4:26 PM

- Select **Named Time Period**, and then select a predefined period from the Named Time Period menu.
- Select **Relative Time Period**, and then provide a number appropriate for the selected time units.

**Note:** The relative time period is measured with respect to the time at which the configured view is loaded.

- Select **Absolute Time Period**, and then provide both the start time and the end time for the period over which you want to view monitoring data.

**Note:** Use the calendars to set your time.

## 6. Select a **Flow Direction**.

### **Flow Direction**

- ☒ Both
- ☐ Ingress
- ☐ Egress

- Select **Both** to include ingress and egress traffic in the calculations NTA makes.

**Note:** For the Node Details view, this selection is automatically converted to Ingress.

- Select **Ingress** to include only ingress traffic in the calculations NTA makes.
- Select **Egress** to include only egress traffic in the calculations NTA makes.

## 7. Select **Endpoints**.

### **Endpoints**

Include ▾

10.110.2.110



Add Filter

**Note:** *If you want a filtered view of a subnet*, type the appropriate range of IP addresses here, either as a range (192.168.1.0-192.168.1.255) or using the CIDR notation (192.168.1.0/24).

8. When you have completed configuration of your filtered application view, click **SUBMIT**.
9. *If you want to save your custom view for future reference*, click **SAVE FILTERED VIEW TO MENU BAR**.

**Note:** You can also use an IP Groups filter for endpoints.

## ***Locating and Isolating an Infected Computer***

You can use your currently installed NPM instance, with the addition of NTA, to quickly pinpoint and respond to the wide variety of self-propagating viruses that can attack your network. Consider the following scenario:

1. A local branch of your bank network that handles all credit card transactions complains of an extremely sluggish network, causing frequent timeouts during sensitive data transfers.
2. The Orion Web Console shows that the link to the branch network is up.
3. NPM Percent Utilization charts on the Network Summary home page show that current utilization is 98%, even though normal branch network utilization is 15-25%.
4. You click **NetFlow** in the Modules toolbar, and then click the name of the branch network link in the NetFlow Sources resource to view the Flow-enabled router on the branch network.
5. Taking a quick look at the Top 5 Endpoints resource, you see that a single computer in the 10.10.10.0-10.10.10.255 IP address range is generating 80% of the load on the branch link.
6. You know that computers in this IP address range are accessible to customers for personal transactions using the web.
7. By viewing the Top 5 Applications resource, you quickly see that 100% of the last two hours of traffic from a publicly accessible computer has been generated by an IBM MQSeries messaging application.
8. By clicking the IBM MQSeries messaging application name in the Top 5 Applications resource, you are able to determine that IBM MQSeries messaging occurs over port 1883.
9. Knowing that you don't have any devices using IBM MQSeries messaging in the customer accessible location, nor any other services or protocols that require port 1883, you recognize that this is a virus exploit.

10. To address the problem discovered (in step 5), using a configuration management tool, such as Orion Network Configuration Manager, you push a new configuration to your firewall that blocks port 1883.

## ***Locating and Blocking Unwanted Use***

With NTA, you can easily chart increasing usage on any of your different network uplinks. NPM already allows you to chart utilization, but, with the addition of NTA, you can locate specific instances of unwanted use, immediately allowing you to take corrective action, as in the following scenario:

1. Your uplink to the internet has been slowing progressively over the last 6 months, even though your corporate head count, application use, and dedicated bandwidth have all been stable.
2. When you open the Orion Web Console, the Network Summary Home view shows that your site link to the internet is up, but, when you click your specific uplink and consult the Current Percent Utilization of each Interface chart, you see that the current utilization of your web-facing interface is 80%.
3. You click your web-facing interface to open the Interface Details view.
4. Customizing the Percent Utilization chart to show the last 6 months, you see that there has been steady growth from 15% to 80% consumption over time. There are even spikes into the high 90s.
5. You click the NetFlow Traffic Analysis tab, and then click the web-facing interface to open the NetFlow Interface Details view.
6. Looking at the top 50 Endpoints, you see that a group of computers in the 10.10.12.0-10.10.12.255 IP address range is consuming most of the bandwidth. These computers reside in your internal sales IP address range.
7. You begin to drill into each of the offending IP addresses, and each IP address you investigate shows Kazaa (port 1214) and World of Warcraft (port 3724) usage in the Top 5 applications.
8. Using a configuration management tool, such as Orion Network Configuration Manager, you push a new configuration to your firewall that blocks ports 1214 and 3724.
9. Within minutes, you see the traffic on your interface drop back to 25%.

## ***Recognizing and Thwarting Denial of Service Attacks***

NTA enables you to easily characterize both outgoing and incoming traffic. This ability becomes ever more important as corporate networks are exposed to increasingly malicious denial of service attacks. Consider the following scenario:

1. An NPM advanced alert tells you that your web-facing router is having trouble creating and maintaining a stable connection to the internet.
2. You open the Orion Web Console to search for possible issues. All connections are currently up, and bandwidth utilization looks good. But then you notice your CPU utilization on the firewall node. It is holding steady between 99% and 100%.
3. Clicking the firewall node name opens its Node Details page where the Current Percent Utilization of Each Interface resource shows that your firewall interfaces are receiving abnormally high levels of traffic.
4. You click **NetFlow** in the Modules toolbar to take a quick look at your customized Top 50 Endpoints resource.
5. The Top 50 Endpoints resource shows that the top six computers attempting to access your network are from overseas.
6. You realize that your ports are being scanned and that your firewall is interactively blocking these attacks.
7. Using a configuration management tool, such as Orion Network Configuration Manager, you push a new configuration to your firewall that blocks all traffic over the IP address range of the computers trying to access your network.
8. In minutes, CPU utilization on your web-facing router returns to normal.

## ***Investigating NTA Further***

While this concludes the guided tour of NetFlow Traffic Analyzer, this *Evaluation Guide* has in no way fully covered the wealth of Flow-enabled network monitoring features available with NTA. Please explore the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*, available on the SolarWinds website, at <http://www.solarwinds.com/support/documentation.aspx>, to learn even more about the power and convenience of NetFlow Traffic Analyzer.