

# **Standard Content Guide**

---

Network Monitoring

ArcSight ESM 6.5c

October 11, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

## Contact Information

---

<b>Phone</b>	A list of phone numbers is available on the HP ArcSight Technical Support page: <a href="http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI">http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI</a> .
<b>Support Web Site</b>	<a href="http://support.openview.hp.com">http://support.openview.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.arcsight.com">https://protect724.arcsight.com</a>

---

## Revision History

---

Date	Product Version	Description
10/11/2013	Network Monitoring content for ArcSight ESM 6.5c	Final revision for release.

---

# Contents

---

<b>Chapter 1: Network Monitoring Overview .....</b>	<b>5</b>
What is Standard Content? .....	5
Standard Content Packages .....	7
Network Monitoring Content .....	7
Supported Devices .....	8
Calculating Bytes In and Bytes Out .....	8
<b>Chapter 2: Installation and Configuration .....</b>	<b>11</b>
Installing the Network Monitoring Package .....	11
Configuring Network Monitoring Content .....	12
Configuring the SmartConnector to Aggregate Events .....	12
Modeling the Network .....	13
Categorizing Assets .....	14
Enabling Rules .....	15
Configuring Filters .....	15
Ensuring Filters Capture Relevant Data .....	17
Configuring Notification Destinations .....	18
Configuring Notifications and Cases .....	18
Scheduling Reports .....	18
Configuring Trends .....	18
<b>Chapter 3: Network Monitoring Content .....</b>	<b>21</b>
Bandwidth Usage .....	22
Devices .....	22
Resources .....	22
Device Activity .....	29
Devices .....	29
Resources .....	29
Hosts and Protocols .....	37
Devices .....	37
Configuring the Hosts and Protocols Resource Group .....	37
Resources .....	37
SANS Top 5 Reports .....	43
Devices .....	43

Resources ..... 43

Traffic Overview ..... 47

    Devices ..... 47

    Resources ..... 47

**Index..... 59**

# Chapter 1

## Network Monitoring Overview

---

This chapter discusses the following topics.

["What is Standard Content?" on page 5](#)

["Standard Content Packages" on page 7](#)

["Network Monitoring Content" on page 7](#)

### What is Standard Content?

Standard content is a series of coordinated resources (filters, rules, dashboards, reports, and so on) that address common security and management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out-of-the box with minimal configuration. The content provides a full spectrum of security, network, and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the system.

Standard content is installed using a series of packages, some of which are installed automatically with the ArcSight Manager to provide essential system health and status operations. The remaining packages are presented as install-time options organized by category.

Standard content consists of the following:

- **ArcSight Core Security** content is installed automatically with the ArcSight Manager and consists of key resources for monitoring Microsoft Windows, firewall, IPS and IDS, NetFlow, and other essential security information.
- **ArcSight Administration** content contains several packages that provide statistics about the health and performance of ArcSight products.
  - ◆ ArcSight Administration is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
  - ◆ ArcSight Admin DB CORR is installed automatically with the ArcSight Manager for ArcSight ESM with CORR- (Correlation Optimized Retention and Retrieval) Engine and provides information on the health of the CORR-Engine.
  - ◆ ArcSight Content Management is an optional package that shows information about content package synchronization with the ESM Content Management feature. The information includes a history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered. You can install this package during ArcSight ESM installation or from the ArcSight Console any time after installation.

- ◆ ArcSight Search Filters is installed automatically with the ArcSight Manager for use in the ArcSight Command Center. You cannot edit or use these filters in the ArcSight Console. For information about the search filters, refer to the ArcSight Command Center User's Guide.

**Note**

The ArcSight Admin DB CORR and ArcSight Search Filters content packages are installed automatically when you perform a new ArcSight ESM installation. However, when you upgrade your ArcSight ESM system, these content packages are not installed automatically. You can install these packages from the ArcSight Console any time after upgrade by right-clicking the package on the Packages tab in the Navigator and selecting Install Package.

Refer to the ArcSight ESM Upgrade Guide for information about upgrading ArcSight ESM.

---

- **ArcSight System** content is installed automatically with the ArcSight Manager and consists of resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality.
- **ArcSight Foundation** content (such as Cisco Monitoring, Configuration Monitoring, Intrusion Monitoring, IPv6, NetFlow Monitoring, Network Monitoring, and Workflow) provide a coordinated system of resources with real-time monitoring capabilities for a specific area of focus, as well as after-the-fact analysis in the form of reports and trends. You can extend these foundations with additional resources specific to your needs or you can use them as a template for building your own resources and tasks. You can install a Foundation during ArcSight ESM installation or from the ArcSight Console any time after installation.
- **Shared Libraries** - ArcSight Administration and several of the ArcSight Foundations rely on a series of common resources that provide core functionality for common security scenarios. Dependencies between these resources and the packages they support are managed by the Package resource.
  - ◆ Anti Virus content is a set of filters, reports, and report queries used by ArcSight Foundations, such as Configuration Monitoring and Intrusion Monitoring.
  - ◆ Conditional Variable Filters content is a library of filters used by variables in standard content report queries, filters, and rule definitions. The Conditional Variable Filters are used by ArcSight Administration and certain ArcSight Foundations, such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow.
  - ◆ Global Variables content is a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.
  - ◆ Monitoring Support Data content is a set of active lists that store mapping information for HTTP return status code classes, Cisco firewall syslog message types, and encoded logon types.
  - ◆ Network filters content is a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

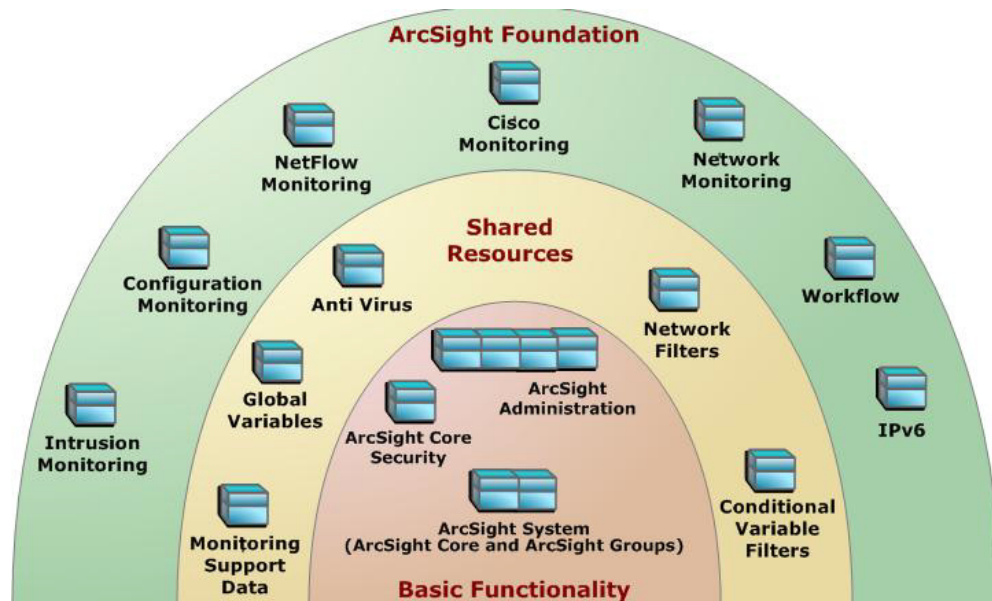
**Caution**

The resources in the ArcSight Core Security, ArcSight Administration, ArcSight DB CORR, Conditional Variable Filters, Global Variables, and Network Filters content packages are not locked even though they manage core functionality; HP recommends that you do not delete or modify these resources unless you are an advanced user who understands fully the resources and their dependencies.

---

## Standard Content Packages

Standard content comes in packages (.arb files) that are either installed automatically or presented as an install-time option. The following graphic outlines the packages.



**Figure 1-1** The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support multiple packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

Depending on the options you install, you will see the ArcSight Core Security, ArcSight Administration, and ArcSight System resources and some or all of the other package content.



**Caution**

When creating your own packages, you can explicitly include or exclude system resources in the package. Exercise caution if you delete packages that might have system resources; for example, zones. Make sure the system resources either belong to a locked group or are themselves locked. For more information about packages, refer to the ArcSight Console User's Guide.

## Network Monitoring Content

The Network Monitoring content monitors the status of network throughput and network infrastructure. This content provides statistics about traffic patterns and bandwidth usage that helps you identify anomalies and areas of the network that need attention. The Network Monitoring content can help you:

- Keep the network up and running
- Ensure maximum availability of mission-critical server applications and vital network resources
- Validate the existence and availability of any network object
- Observe and detect any object in error state
- Monitor common and custom TCP/IP ports

- Evaluate network productivity and utilization of network resources
- Assess impact of changes to the network
- Track network anomaly and security vulnerabilities

## Supported Devices

The Network Monitoring content is built around feeds from the ArcSight SmartConnector that collects events from Qosient Argus, which is a real-time flow monitor. It monitors all network transactions seen in a data network traffic stream. For more information about Qosient Argus, see <http://www.qosient.com/argus/>.

The Argus device detects a transaction from point A to point B and stores the information in the following Argus-specific fields:

Argus event field	Description
lasttime	record last time
srcaddr	source IP address
dstaddr	destination IP address
sport	source port number
dport	destination port number
bytes	total transaction bytes
srcbytes	source-to-destination transaction bytes
dstbytes	destination-to-source transaction bytes

The ArcSight Argus SmartConnector maps this information to the correct fields in the ArcSight event schema, for example:

Argus event field	ArcSight event field
srcaddr	Attacker Address
dstaddr	Target Address
srcbytes	Bytes in
dstbytes	Bytes out

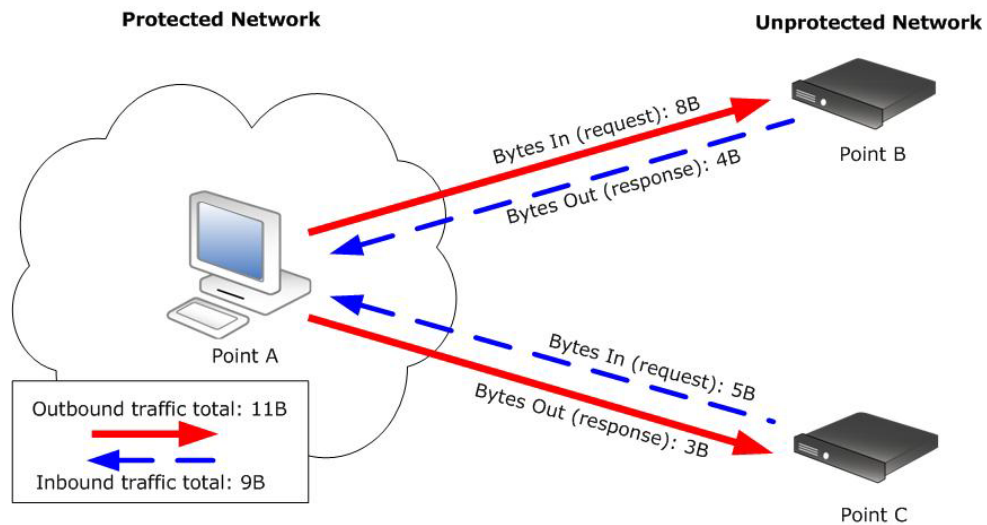
## Calculating Bytes In and Bytes Out

One of the goals of the Network Monitoring content is to analyze how much traffic volume is coming into and going out of the network. Calculating this bandwidth usage involves keeping track of bytes in and bytes out of the network, from what sources, and at what rates.

Argus counts any request as "bytes in" and any response as "bytes out" regardless of where the requestor is located in relation to your protected network. For example, in the illustration below, Point A initiates the request to Point B, and Point C initiates the request to Point A. Both are considered by Argus to be "bytes in."



But as a network administrator, you are also interested in traffic volume outbound *from* and inbound *to* your protected network, illustrated by the blue and red arrows in the example below.



**Figure 1-2** ArcSight variables ensure that Argus byte counts for “bytes in” and “bytes out” correspond with the network notion of inbound traffic and outbound traffic.

To make sure that the byte counts for Argus “bytes in” and “bytes out” correspond with your network’s notion of outbound traffic and inbound traffic, ArcSight has constructed a system of variables and filters that translate Argus “bytes in” and “bytes out” to traffic inbound to and outbound from your network.

The ArcSight `IncomingBytes` and `OutgoingBytes` variables take the Argus byte count of activity on the way out of the protected network and counts it as outbound traffic, and activity coming into the protected network as inbound traffic. In the A-to-B case, it considers the byte count for Argus “bytes in” to be outbound traffic and considers the byte count for Argus “bytes out” to be inbound traffic. The A-to-C case matches: bytes in are counted as inbound traffic, and bytes out are counted as outbound traffic.

In the example, if you add the total bytes out from the network’s perspective (after the values have been normalized by the ArcSight variables), you add the byte counts for the two red arrows, in this case,  $8 + 3$ , or 11. And the byte total for the inbound traffic is the sum of the two blue arrows:  $4 + 5$ , or 9.



## Chapter 2

# Installation and Configuration

---

This chapter discusses the following topics:

[“Installing the Network Monitoring Package” on page 11](#)

[“Configuring Network Monitoring Content” on page 12](#)

## Installing the Network Monitoring Package

The Network Monitoring Foundation is one of the standard content packages that are presented as install-time options. If you selected all the standard content packages to be *installed* at installation time, the packages and their resources will be installed in the ArcSight Database and available in the Navigator panel resource tree. The package icon in the Navigator panel package view will appear blue.

If you opted to exclude a Foundation package during ESM installation, the package is *imported* into the Packages tab in the Navigator panel automatically, but is not available in the resource view. The package icon in the package view appears grey.

If you do not want the package to be available in any form, you can *delete* the package.

### To install a package that is imported, but not installed:

- 1 On the Navigator panel Packages tab, navigate to the package you want to install.
- 2 Right-click the package and select **Install Package**.
- 3 In the Install Package dialog, click **OK**.
- 4 When the installation is complete, review the summary report and click **OK**.

The package resources are fully installed to the ArcSight Database, the resources are fully enabled and operational, and available in the Navigator panel resource tree.

### To uninstall a package that is installed:

- 1 On the Navigator Panel Packages tab, navigate to the package you want to uninstall.
- 2 Right-click the package and select **Uninstall Package**.
- 3 In the Uninstall Package dialog, click **OK**.

The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog. If a message displays indicating that there is a conflict, select an option in the Resolution Options area and click **OK**.

- 4 When uninstall is complete, review the summary and click **OK**.

The package is removed from the ArcSight Database and the Navigator panel resource tree, but remains available in the Navigator panel Packages tab, and can be re-installed at another time.

**To delete a package and remove it from the ArcSight Console and the ArcSight Database:**

- 1** On the Navigator Panel Packages tab, navigate to the package you want to delete.
- 2** Right-click the package and select **Delete Package**.
- 3** When prompted for confirmation, click **Delete**.

The package is removed from the Navigator panel Packages tab.

## Configuring Network Monitoring Content

The list below shows the general tasks you need to complete to configure Network Monitoring content with values specific to your environment.

- ["Configuring the SmartConnector to Aggregate Events" on page 12](#)
- ["Modeling the Network" on page 13](#)
- ["Categorizing Assets" on page 14](#)
- ["Enabling Rules" on page 15](#)
- ["Configuring Filters" on page 15](#)
- ["Ensuring Filters Capture Relevant Data" on page 17](#)
- ["Configuring Notification Destinations" on page 18](#)
- ["Configuring Notifications and Cases" on page 18](#)
- ["Scheduling Reports" on page 18](#)
- ["Configuring Trends" on page 18](#)

## Configuring the SmartConnector to Aggregate Events

The Network Monitoring content is built around feeds from the ArcSight SmartConnector that collects events from Qosient Argus, which is a real-time flow monitor. It monitors all network transactions seen in a data network traffic stream.

To reduce the number of raw events that are sent from your network monitoring device to ArcSight, you can aggregate groups of events with the same characteristics using the `group by` option on the SmartConnector. You can perform this configuration from the ArcSight Console in the Connectors portion of the navigator panel.

For example, the attacker port (Argus `srcPort`) is often less interesting than the target port (`destPort`). If there are many events with the same target port and different attacker ports, you can aggregate the events, which combines the values that are the same, and nulls out the values that are different.

In the example below, the attacker ports are different, but the target ports, attacker IPs, and target IPs are the same for each event. In this case, the value in the attacker port column is null, and the values in the *Bytes in* column are summed.

Attacker port	Target port	Attacker IP	Target IP	Bytes in
3331	80	1.1.1.1	2.2.2.2	2
3332	80	1.1.1.1	2.2.2.2	3
3333	80	1.1.1.1	2.2.2.2	15
3334	80	1.1.1.1	2.2.2.2	9
<b>NULL</b>	<b>80</b>	<b>1.1.1.1</b>	<b>2.2.2.2</b>	<b>29</b>

This reduces the number of individual events that the system has to process, which improves performance and efficiency.



The Argus administrator can perform this aggregation on the Argus device itself using a RAGATOR script and a configuration file that specifies the fields you want to aggregate, those you want to nullify, and those you want to sum.

## Modeling the Network

A network model keeps track of the network nodes participating in the event traffic. Modeling your network and categorizing critical assets using the standard asset categories is what activates some of the standard content and makes it effective.

There are several ways to model your network. For information about populating the network model, refer to the ArcSight Console User's Guide. To learn more about the architecture of the ESM network modeling tools, refer to the ESM 101 guide.

## Categorizing Assets

After you have populated your network model with assets, apply the standard asset categories listed in the following table to activate standard content that uses these categories so that you can apply criticality and business context to events.

Asset Category	Description
/Site Asset Categories/ Address Spaces/Protected	<p>Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category.</p> <p>Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as <i>Protected</i>.</p> <p><b>Note:</b> Assets with a private IP address (such as 192.168.0.0) are considered <i>Protected</i> by the system, even if they are not categorized as such.</p>
/System Asset Categories/ Criticality/High	<p>Categorize all assets that are considered <i>critical</i> to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with this asset category.</p> <p>The asset categories most essential to basic event processing are those used by the Priority Formula to calculate the criticality of an event. Asset criticality is one of the four factors used by the Priority Formula to generate an overall event priority rating.</p>
/System Asset Categories/ Criticality/Very High	See /System Asset Categories/Criticality/High

If you have created your own asset categories that are relevant to the top traffic dashboards, you can add those asset categories to the corresponding filter in All Filters/ArcSight Foundation/Network Monitoring/Application Filters).

You can assign asset categories to assets, zones, asset groups, or zone groups. If assigned to a group, all resources under that group inherit the categories.

You can assign asset categories individually using the Asset editor or in a batch using the Network Modeling wizard. For information about how to assign asset categories using the ArcSight Console tools, refer to the ArcSight Console User's Guide.

For more information about the Priority Formula and how it leverages these asset categories to help assign priorities to events, refer to the ArcSight Console User's Guide or the ESM 101 guide.

## Enabling Rules

Rules trigger only if they are deployed in the `Real-Time Rules` group and are enabled. All of the Network Monitoring rules are deployed by default in the `Real-Time Rules` group and are also enabled.

### To disable a rule:

- 1 In the Navigator panel, go to **Rules** and navigate to the Real-time Rules group.
- 2 Navigate to the rule you want to disable.
- 3 Right-click the rule and select **Disable Rule**.

## Configuring Filters



If you use only Argus, you do not need to perform this procedure.

The events that trigger the Network Monitoring content are controlled by the filters in the Connector Filters group (`/All Filters/ArcSight Foundation/Network Monitoring/Connector Filters`).

If you use a real-time flow monitoring device other than Argus, that device must also report Attacker, Target, Ports, Bytes in and Bytes out. You can then configure the SmartConnector filters to operate on events from that device.

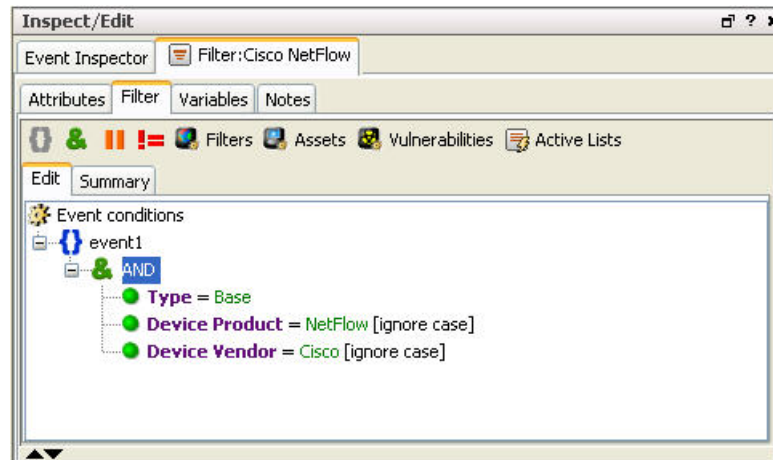


If you have multiple network reporting devices, verify that any overlapping address spaces are defined through their own ArcSight network.

This procedure creates a new filter based on the *Qosient Argus* filter for each reporting device relevant to your network environment.

- 1 Copy the *Qosient Argus* filter: click and drag the filter into the same group; when prompted "Do you want to make a copy of this resource?" select **Yes**.
- 2 Modify the copy to reflect your network monitoring device and vendor.
  - a Open the copy in the Inspect/Edit panel. On the Attributes tab, rename the copy to indicate the name of your network reporting device; for example, `Cisco NetFlow`.
  - b On the Filter tab in the Event conditions window, double-click the condition `Device Product = Argus [ignore case]`. Delete `Argus` and type in the name of your device as your device reports it to the ArcSight SmartConnector; for example, `NetFlow`. Click **OK**.
  - c In the Event conditions window, double-click the condition `Device Vendor = Qosient [ignore case]`. Delete `Qosient` and type in the name of your

device as your device reports it to the ArcSight SmartConnector; for example, Cisco. Click **OK** in the condition. An example is shown below.




- d** Repeat [Step a](#) through [Step c](#) for each of your network monitoring devices.
- e** Click **OK** to apply changes and close the filter editor.

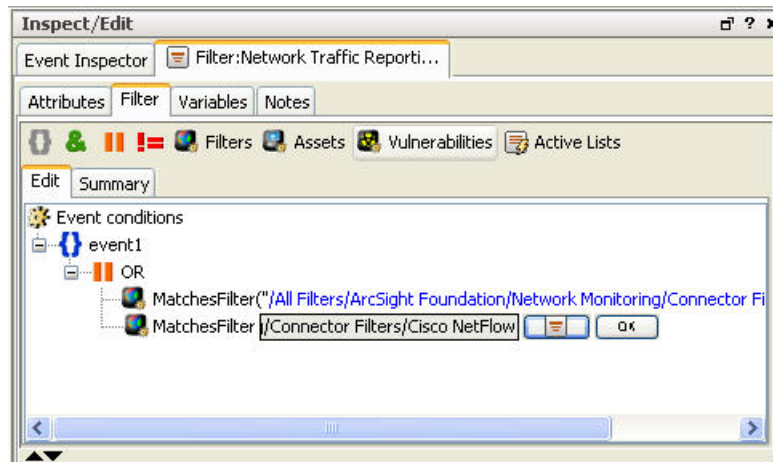


Depending on how you want to organize your content, you can also express all your network reporting devices in a single filter. When adding vendors and products to the expression, add an **OR** clause to the `event1` base.

- 3** Modify the Network Traffic Reporting Devices filter to point to the filter(s) you created in [Step 2](#).
  - a** Open the Network Traffic Reporting Devices filter in the Inspect/Edit panel.
  - b** On the **Filter** tab in the Event conditions window, select `event1` and click the **OR** operator (**||**).
  - c** Select the first condition, `MatchesFilter("/All Filters/ArcSight Foundation/Network Monitoring/Connector Filters/Qosient Argus")`, and select **Copy** from the Edit menu.
  - d** Select the **OR** operator and select **Paste** from the Edit menu.
  - e** Double-click the second condition, `MatchesFilter("/All Filters/ArcSight Foundation/Network Monitoring/Connector`



Filters/Qosient Argus"). Click the filter button (  ) and navigate to the filter you created in step 2. Click **OK**. An example is shown below.



- f** Repeat [Step 3](#) for each network monitoring filter you want to add. If you do not have Argus, you can remove the Qosient Argus filter from the **OR** statement (select it and press the **Delete** key).
- g** Click **OK** to apply changes and close the filter editor.

## Ensuring Filters Capture Relevant Data

Standard content relies on specific event field values to identify events of interest. Although this method applies to most of the events and devices, be sure to test key filters to verify that they actually capture the required events.

### To ensure that a filter captures the relevant events:

- 1** Generate or identify the required events and verify that they are being processed by viewing them in an active channel or query viewer.
- 2** Navigate to the appropriate filter, right-click the filter and choose **Create Channel with Filter**. If you see the events of interest in the newly created channel, the filter is functioning properly.

If you do not see the events of interest:

- a** Verify that the configuration of the active channel is suitable for the events in question. For example, ensure that the event time is within the start and end time of the channel.
- b** Modify the filter condition to capture the events of interest. After applying the change, repeat [Step 2](#) to verify that the modified filter captures the required events.

## Configuring Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, notifications are disabled in the standard content rules, so the admin user needs to configure the destinations *and* enable the notification in the rules. For details about enabling the notifications in rules, see ["Configuring Notifications and Cases" on page 18](#).

Network Monitoring rules reference the CERT Team notification group. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center. Refer to the ArcSight Console User's Guide for information on how to configure notification destinations.

## Configuring Notifications and Cases

Content depends on rules to send notifications and open cases when conditions are met. Notifications and cases are how users can track and resolve the security issues that the content is designed to find.

By default, the notifications and create case actions are disabled in the standard content rules that send notifications about security-related events to the CERT Team notification group.

To enable rules to send notifications and open cases, first configure notification destinations as described in [Configuring Notification Destinations](#) above, then enable the notification and case actions in the rules.

For more information about working with rule actions in the Rules Editor, refer to the ArcSight Console User's Guide.

## Scheduling Reports

You can run reports on demand, automatically on a regular schedule, or both. By default, reports are not scheduled to run automatically.

Evaluate the reports that come with Network Monitoring, and schedule the reports that are of interest to your organization and business objectives. For instructions about how to schedule reports, refer to the ArcSight Console User's Guide.

## Configuring Trends

Trends are a type of resource that can gather data over longer periods of time, which can be leveraged for reports. Trends streamline data gathering to the specific pieces of data you want to track over a long range, and breaks the data gathering up into periodic updates. For long-range queries, such as end-of-month summaries, trends greatly reduce the burden on system resources. Trends can also provide a snapshot of which devices report on the network over a series of days.

Network Monitoring content includes several trends, which are disabled by default. These disabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m. when network traffic is usually less busy than during peak daytime business hours. These schedules can be customized to suit your needs using the Trend scheduler in the ArcSight Console.

To enable a trend, go to the Navigator panel, right-click the trend you want to enable and select **Enable Trend**.



To enable a disabled trend, you must first **change the default start date** in the Trend editor.

If the start date is not changed, the trend takes the default start date (derived from when the trend was first installed), and backfills the data from that time. For example, if you enable the trend six months after the first install, these trends try to get all the data for the last six months, which might cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

---

For more information about trends, refer to the the ArcSight Console User's Guide.



## Chapter 3

# Network Monitoring Content

---



In this section, the Network Monitoring resources are grouped together based on the functionality they provide. The Network Monitoring resource groups are listed in the table below.

Resource Group	Purpose
<a href="#">"Bandwidth Usage" on page 22</a>	The Bandwidth Usage resources provide information about bandwidth utilization.
<a href="#">"Device Activity" on page 29</a>	The Device Activity resources provide information about firewall, network, and VPN connection activity.
<a href="#">"Hosts and Protocols" on page 37</a>	The Hosts and Protocols resources provide information about the network traffic to the mail and web server by host and application protocol.
<a href="#">"SANS Top 5 Reports" on page 43</a>	The SANS Top 5 Reports resources provide information about suspicious or unauthorized network traffic patterns.
<a href="#">"Traffic Overview" on page 47</a>	The Traffic Overview resources provide an overview of network traffic.

## Bandwidth Usage

The Bandwidth Usage resources provide information about bandwidth utilization.

### Devices

The following device types can supply events that apply to the Bandwidth Usage resource group:

- Qosient Argus and network devices such as routers, firewalls, and VPNs

### Resources

The following table lists all the resources in this resource group and any dependant resources.

**Table 3-1** Resources that Support the Bandwidth Usage Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Argus Events	This active channel shows all the events from Argus SmartConnectors within the past eight hours.	Active Channel	ArcSight Foundation/Network Monitoring/
Inbound Bandwidth	This dashboard shows an overview of the inbound bandwidth and contains three data monitors: Inbound Bandwidth - Last 10 Minutes, Inbound Bandwidth - Last Hour, and Inbound Bandwidth - Last Minute.	Dashboard	ArcSight Foundation/Network Monitoring/Bandwidth Usage/
Current Bandwidth	This dashboard shows an overview of the current bandwidth usage and contains two data monitors: Inbound Bandwidth - Last Minute and Outbound Bandwidth - Last Minute.	Dashboard	ArcSight Foundation/Network Monitoring/Bandwidth Usage/
Outbound Bandwidth	This dashboard shows an overview of the outbound bandwidth and contains three data monitors: Outbound Bandwidth - Last 10 Minutes, Outbound Bandwidth - Last Hour, and Outbound Bandwidth - Last Minute.	Dashboard	ArcSight Foundation/Network Monitoring/Bandwidth Usage/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage by top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find hosts with the highest bandwidth.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/ Cross-Device/

Resource	Description	Type	URI
Bandwidth Utilization - Last Hour	This report shows the bandwidth utilization for the last hour. A chart has two sets of values. The first set shows the number of bytes per second for the inbound traffic and the second set shows the number of bytes per second for the outbound traffic.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/
Bandwidth Usage by Protocol	This report displays the applications that are consuming the most bandwidth. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/ Cross-Device/
Bandwidth Usage by Hour	This report shows a summary of bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/ Cross-Device/
Bandwidth Utilization - Business Hours	This report shows the average bandwidth utilization during business hours. The first chart shows the average bytes per second for incoming traffic and the second chart shows the average bytes per second for outgoing traffic.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/
Bandwidth Utilization - Last 24 Hours	This report displays the bandwidth utilization for the last 24 hours. The first chart shows the number of bytes per second for inbound traffic and the second chart shows the number of bytes per second for outbound traffic.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/
<b>Library Resources</b>			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Outbound Bandwidth - Last Minute	This data monitor shows the outbound bandwidth (bytes/sec) for the last minute. The bandwidth values are updated every five seconds.	Data Monitor	ArcSight Foundation/Network Monitoring/Bandwidth Usage/Current Bandwidth/
Outbound Bandwidth - Last Hour	This data monitor shows the average outbound bandwidth (bytes/sec) for the last hour. The values are updated every five minutes.	Data Monitor	ArcSight Foundation/Network Monitoring/Bandwidth Usage/Outbound Bandwidth/

Resource	Description	Type	URI
Inbound Bandwidth - Last Minute	This data monitor shows the inbound bandwidth (bytes/sec) for the last minute. The bandwidth values are updated every five seconds.	Data Monitor	ArcSight Foundation/Network Monitoring/Bandwidth Usage/Inbound Bandwidth
Inbound Bandwidth - Last 10 Minutes	This data monitor shows the average inbound bandwidth (bytes/sec) for the last ten minutes. The values are updated every 30 seconds.	Data Monitor	ArcSight Foundation/Network Monitoring/Bandwidth Usage/Inbound Bandwidth/
Outbound Bandwidth - Last 10 Minutes	This data monitor shows the average outbound bandwidth (bytes/sec) for the last ten minutes. The values are updated every 30 seconds.	Data Monitor	ArcSight Foundation/Network Monitoring/Bandwidth Usage/Outbound Bandwidth/
Inbound Bandwidth - Last Hour	This data monitor shows the average inbound bandwidth (bytes/sec) for the last hour. The values are updated every five minutes.	Data Monitor	ArcSight Foundation/Network Monitoring/Bandwidth Usage/Inbound Bandwidth/
Argus	This field set shows a summary of the attacker and target hosts. This is the default field set for the Argus Events active channel.	Field Set	ArcSight Foundation/Network Monitoring/
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	Filter	ArcSight Foundation/Common/Device Class Filters
VPN Events	This filter identifies events in which the category device group is VPN.	Filter	ArcSight Foundation/Common/Device Class Filters
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Application Protocol is NULL	This filter identifies if the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Common/Conditio nal Variable Filters/Protocol
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
All Events	This filter matches all events.	Filter	ArcSight System/Core
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters



Resource	Description	Type	URI
Inbound and Outbound Traffic	This filter detects Argus inbound events (external to internal) and Argus outbound events (internal to external). This filter is used by all the bandwidth-related moving average data monitors.	Filter	ArcSight Foundation/Network Monitoring/Network Traffic Filters/
Qosient Argus	This filter identifies events originating from Argus connectors.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
Outbound Traffic	This filter detects Argus events originating inside the company network and targeting the outside network.	Filter	ArcSight Foundation/Network Monitoring/Network Traffic Filters/
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Foundation/Common/Device Class Filters
Bandwidth to or from External Systems	This filter detects events in which the source or destination of the event is internal to the network (but one of them is external), and at least one of Bytes In or Bytes Out values is present.	Filter	ArcSight Foundation/Network Monitoring/Network Traffic Filters/
Inbound Traffic	This filter identifies Argus events originating from the outside network, targeting inside the company network.	Filter	ArcSight Foundation/Network Monitoring/Network Traffic Filters/
Network Traffic Reporting Devices	This filter identifies your network traffic reporting devices. The default network traffic reporting device is QoSient Argus.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Firewall/
Bandwidth Usage per Hour	This report shows a summary of the bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the previous day (by default). Use this report to find high bandwidth usage hours during the day.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Firewall/

Resource	Description	Type	URI
Bandwidth Usage by Protocol	This report shows a summary of network bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Network/
Bandwidth Usage by Protocol	This report shows a summary of VPN bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/VPN/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage reported by network devices by the top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find the highest bandwidth hosts.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Network/
Bandwidth Usage per Hour	This report shows a summary of VPN bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the past 24 hours. Use this report to find high bandwidth usage hours during the day.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/VPN/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage reported by firewalls by the top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find the highest bandwidth hosts.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Firewall/
Top Bandwidth Hosts	This report shows a summary of the VPN bandwidth usage by the top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find the highest bandwidth hosts.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/VPN/
Bandwidth Usage per Hour	This report shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Network/

Resource	Description	Type	URI
Top Bandwidth Hosts	This query identifies the count of TotalBytes (Bytes In + Bytes Out) for each host, and sorts them so that the hosts with the highest totals are reported first. The query identifies events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/
Bandwidth Utilization - By Minute	This query returns the average number of bytes in and bytes out per second for the inbound and outbound traffic and groups the values by minute.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/
Overall Traffic	This query identifies the overall number of incoming bytes and outgoing bytes. The incoming bytes are the sum of the number of bytes in requests in the inbound events (external network to internal network) and the number of bytes in responses in the outbound events (internal network to external network). The outgoing bytes are the sum of the number of bytes in requests in the outbound events (internal network to external network) and the number of bytes in responses in the inbound events (external network to internal network). This query is used by the Overall Traffic trend.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Event Queries/
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/
Average Bandwidth Utilization - Business Hours	This query identifies the average number of bytes in and bytes out per second in the Overall Traffic Trend Table, and groups the values by hour during business hours (by default: 8:00 a.m. to 5:00 p.m.).	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Trend Queries/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/

Resource	Description	Type	URI
Bandwidth Utilization - By Hour	This query returns the average number of bytes in and bytes out per second for inbound and outbound traffic, and groups the values by hour.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Two Charts Portrait	This template is designed to show two charts. The orientation is portrait.	Report Template	ArcSight System/2 Charts/Without Table
Overall Traffic	This trend stores the total number of incoming bytes and outgoing bytes per hour. The trend runs every day using the Overall Traffic query.	Trend	ArcSight Foundation/Network Monitoring/

## Device Activity

The Device Activity resources provide information about firewall, network, and VPN connection activity.

### Devices

The following device types can supply events that apply to the Device Activity resource group:

- Network devices such as routers, firewalls, and VPNs

### Resources

The following table lists all the resources in the Device Activity resource group and any dependant resources.

**Table 3-2** Resources that Support the Device Activity Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Firewall Connection Overview	This dashboard shows an overview of all the connection events originating from firewalls.	Dashboard	ArcSight Foundation/Network Monitoring/Device Activity/
VPN Connection Statistics	This dashboard displays data monitors related to VPN servers, including connection status counts and authentication errors.	Dashboard	ArcSight Foundation/Network Monitoring/Device Activity/
Network Status Overview	This dashboard displays data monitors related to network device errors, network interfaces, and critical network events.	Dashboard	ArcSight Foundation/Network Monitoring/Device Activity/
Connections Denied by Address	This report shows denied VPN connection data. A chart summarizes the top VPN device addresses with denied connections. A table shows details of the denied connections.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Connections Denied by Hour	This report shows denied VPN connection data. A chart summarizes the number of denied connections for each hour. A table shows details of the denied connections by hour.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Device Interface Down Notifications	This report displays the network devices that report a down link.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
Top VPN Event Sources	This report shows event information reported by VPN devices, excluding modification events.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/

Resource	Description	Type	URI
Top VPN Event Destinations	This report shows event information reported by VPN devices, excluding modification events.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Device Interface Status Messages	This report shows the network devices reporting link status changes.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
Top VPN Access by User	This report displays information about VPN access, authorization or authentication events.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
VPN Connection Failures	This report displays information about VPN access where authorization or authentication failed.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Authentication Errors	This report shows errors generated by a VPN connection attempt. The address is the IP address of the VPN connection source. Use this report to see which users are having difficulties using or setting up their VPN clients.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Top VPN Events	This report displays event information reported by VPN devices, excluding modification events.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Device Events	This report shows information about events on network devices.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
Connections Accepted by Address	This report shows successful VPN connection data. A chart summarizes the top VPN device addresses with successful connections. A table shows details of the successful connections.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Device Errors	This report shows information about system errors on network devices. These events might be an indication of hardware failures, resource exhaustion, configuration issues, or attacks.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
VPN Connection Attempts	This report displays information about events in which VPN access, authorization, or authentication did not result in failure.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/

Resource	Description	Type	URI
Device Critical Events	This report shows information about critical events on network devices. These critical events might be an indication of hardware failures, resource exhaustion, configuration issues, or attacks.	Report	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
<b>Library Resources</b>			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Last 10 Critical Network Events	This data monitor displays the last ten events reported by network devices with an agent severity of High or Very High.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Network Status Overview/
Devices with High Error Rates	This data monitor tracks network device error rates over the last hour. The devices listed when this data monitor is displayed in a dashboard or in the resulting correlation events, have reported at least three errors within a five minute period.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Network Status Overview/
Top VPN Servers with Denied Connections	This data monitor tracks the number of failed VPN connection events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/VPN Connection Statistics/
Top VPN Servers with Authentication Errors	This data monitor tracks the number of VPN authentication error events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/VPN Connection Statistics/
Top 10 Hosts With Denied Outbound Connections	This data monitor shows the top ten hosts with denied outbound connections.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Firewall Connection Overview/
Last 10 Interface Status Messages	This data monitor displays the last ten events reported by network devices related to network interfaces, ports, or links.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Network Status Overview/
Top 10 Hosts With Denied Inbound Connections	This data monitor shows the top ten hosts with denied inbound connections.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Firewall Connection Overview/
Top VPN Users with Authentication Errors	This data monitor tracks the number of VPN authentication error events for each VPN user (including the VPN server), every five minutes for an hour.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/VPN Connection Statistics/

Resource	Description	Type	URI
Top 10 Accepted Ports (Outbound)	This data monitor shows the top ten ports with accepted outbound connections.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Firewall Connection Overview/
Top 10 Accepted Ports (Inbound)	This data monitor shows the top ten ports with accepted inbound connections.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Firewall Connection Overview/
Last 10 Interface Down Messages	This data monitor displays the last ten events reported by network devices related to down network interfaces, ports, or links.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Network Status Overview/
Top 10 Denied Ports (Outbound)	This data monitor shows the top ten ports with denied outbound connections.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Firewall Connection Overview/
Top 10 Denied Ports (Inbound)	This data monitor shows the top ten ports with denied inbound connections.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/Firewall Connection Overview/
Top VPN Servers with Successful Connections	This data monitor tracks the number of successful VPN connection events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/VPN Connection Statistics/
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	Field Set	ArcSight System/Event Field Sets/Active Channels
Denied Outbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Failure. The filter identifies outbound events.	Filter	/All Filters/ArcSight Core Security/Firewall Monitoring
Target User ID is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Target User ID is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Failed VPN Connection Events	This filter identifies unsuccessful VPN events in which the behavior is /Access/Start.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/VPN/



Resource	Description	Type	URI
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Denied Inbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Failure. The filter identifies inbound events.	Filter	/All Filters/ArcSight Core Security/Firewall Monitoring
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
All Events	This filter matches all events.	Filter	ArcSight System/Core
Critical Network Events	This filter identifies critical events related to network devices.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/Network/
Accepted Inbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Success. The filter identifies inbound events.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/Firewall/
Accepted Outbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Success. The filter looks for outbound events.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/Firewall/
Network Device Interface Status Events	This filter identifies events related to device interfaces, ports, or links. VPN events are excluded.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/Network/
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Successful VPN Connection Events	This filter identifies successful VPN events in which the behavior is /Access/Start.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/VPN/
Target User Name is NULL	This filter identifies events where the Target User Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User

Resource	Description	Type	URI
Network Error Events	This filter identifies events related to network device errors.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/Network/
VPN Authentication Errors	This filter identifies VPN authentication error events in which an authentication error event is defined as having the category behavior of /Authentication/Verify and the category significance of /Informational/Error.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/VPN/
Network Device Interface Down Messages	This filter identifies device interface events stating that an interface, port, or link is down. VPN events are excluded.	Filter	ArcSight Foundation/Network Monitoring/Device Activity/Network/
Connections Accepted by Address	This query returns the device zone, address, host name, and a count of VPN devices with successful connections.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/Connections Accepted by Address/
Top VPN Event Sources	This query returns VPN events, excluding modification events.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Device Interface Down Notifications	This query returns device information from network device events for network interfaces that are not VPN interfaces, where a link has been reported to be down and the inbound or outbound interface is defined.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
Device Errors	This query returns base error events in which the device group is Network Equipment or Operating System, and the object starts with Network.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
VPN Connection Attempts	This query returns events where the VPN access, authorization or authentication event did not result in failure.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Top VPN Event Destinations	This query returns VPN events, excluding modification events.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Top Connections Denied by Address	This query returns the device zone, address, and a count to show the top VPN devices with denied connections.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/Connections Denied by Address/

Resource	Description	Type	URI
Authentication Errors	This query returns VPN authentication events in which there has been an error. The query returns the user information, the host information, the error, the time (within an hour), and the number of times the error occurred within the hour.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Device Events	This query returns base events in which the device group is Network Equipment or Operating System, and the object starts with Network.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
VPN Connection Failures	This query returns VPN events in which there is a VPN access, authorization, or authentication failure.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Device Critical Events	This query returns critical base events where the device group is Network Equipment or Operating System, and the object starts with Network.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
Top VPN Events	This query returns all events reported by VPN devices, excluding modification events.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Top VPN Accesses by User	This query returns events for VPN access, authorization, or authentication.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/
Top Connections Accepted by Address	This query returns the device zone, address, and a count to show the top VPN devices with successful connections.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/Connections Accepted by Address/
Connections Denied by Address	This query returns the device zone, address, host name, and a count of VPN devices with denied connections.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/Connections Denied by Address/
Device Interface Status Messages	This query returns device information from network device events where the network interfaces are not VPN interfaces, where a link has been reported to be up or down and the inbound or outbound interface is defined.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/Network/
Connections Denied by Hour	This query returns the device zone, address, host name, and a count of VPN devices with denied connections.	Query	ArcSight Foundation/Network Monitoring/Details/Device Activity/VPN/

Resource	Description	Type	URI
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

## Hosts and Protocols

The Hosts and Protocols resources provide information about the network traffic to the mail and web server by host and application protocol.

### Devices

The following device types can supply events that apply to the Hosts and Protocols resource group:

- Qosient Argus and network devices such as routers, firewalls, and VPNs

### Configuring the Hosts and Protocols Resource Group

The Hosts and Protocols resource group requires the following configuration for your environment.

- To activate content that references email and web servers, categorize your email servers with the [Email](#) asset category, and your web servers with the [Web Server](#) asset category.

### Resources

The following table lists all the resources in the Hosts and Protocols resource group and any dependant resources.

**Table 3-3** Resources that Support the Hosts and Protocols Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Top Traffic to Mail Server	This dashboard shows an overview of the traffic targeting internal hosts categorized as mail servers. This dashboard contains four data monitors: Top Traffic from External to Mail Server (Request), Top Traffic from External to Mail Server (Response), Top Traffic from Internal to Mail Server (Request), and Top Traffic from Internal to Mail Server (Response).	Dashboard	ArcSight Foundation/Network Monitoring/General/
Traffic Moving Average	This dashboard shows a moving average of the ICMP, SYN, and UDP traffic. The dashboard contains three data monitors: Traffic Moving Average (ICMP), Traffic Moving Average (SYN), and Traffic Moving Average (UDP).	Dashboard	ArcSight Foundation/Network Monitoring/General/

Resource	Description	Type	URI
Top Traffic to Web Server	This dashboard shows an overview of the traffic targeting internal hosts categorized as web servers. This dashboard contains several data monitors: Top Traffic from External to Web Server (Request), Top Traffic from External to Web Server (Response), Top Traffic from Internal to Web Server (Request), and Top Traffic from Internal to Web Server (Response).	Dashboard	ArcSight Foundation/Network Monitoring/General/
Attacker Details by Protocol	This report shows the top attackers for a specific application protocol. A chart shows the top five attackers. A table shows details of the top attackers.	Report	ArcSight Foundation/Network Monitoring/Details/By Protocol/
Detailed Traffic by Protocol	This report shows the traffic for a specific application protocol. Charts show the top five attackers and the top five targets. A table shows the top attacker-target pairs.	Report	ArcSight Foundation/Network Monitoring/Details/By Protocol/
Protocol Details by Host	This report shows the application protocol repartition for a specific host. A chart shows the top five protocols with the total number of bytes (BytesIN + BytesOUT). A table shows details for the top protocols (BytesIN, BytesOUT, and Total Number of Bytes).	Report	ArcSight Foundation/Network Monitoring/Details/By Host/
Detailed Traffic by Host	This report shows a chart of the total bytes (in and out) by host, a chart of the total bytes by protocol, and a detailed table showing the bytes in, bytes out, and total bytes for each protocol by host.	Report	ArcSight Foundation/Network Monitoring/Details/By Host/
Target Details by Host	This report shows the top targets for a specific host. A chart shows the top five targets. A table shows the details of the top targets.	Report	ArcSight Foundation/Network Monitoring/Details/By Host/
Target Details by Protocol	This report shows the top targets for a specific application protocol. A chart shows the top five targets. A table shows details of the top targets.	Report	ArcSight Foundation/Network Monitoring/Details/By Protocol/
<b>Library Resources</b>			
Email	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type

Resource	Description	Type	URI
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Web Server	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Top Traffic from Internal to Mail Server (Request)	This data monitor shows the ten internal source hosts with the highest amount of traffic targeting internal hosts categorized as mail servers.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Top Traffic to Mail Server/
Traffic Moving Average (TCP)	This data monitor shows a moving average of the incoming UDP traffic per minute for the last hour using 12 five-minute buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Traffic Moving Average/
Top Traffic from Internal to Web Server (Request)	This data monitor shows the ten internal source hosts with the highest amount of traffic targeting internal hosts categorized as web servers.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Top Traffic to Web Server/
Top Traffic from Internal to Web Server (Response)	This data monitor shows the ten internal source hosts with the highest amount of traffic targeting internal hosts categorized as web servers.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Top Traffic to Web Server/
Top Traffic from External to Web Server (Request)	This data monitor shows the ten external source hosts with the highest amount of traffic targeting internal hosts categorized as web servers.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Top Traffic to Web Server/
Traffic Moving Average (SYN)	This data monitor shows a moving average of the incoming SYN traffic (TCP connection requests) per minute for the last hour using 12 five-minute buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Traffic Moving Average/
Top Traffic from External to Mail Server (Response)	This data monitor shows the ten external source hosts with the highest amount of traffic targeting internal hosts categorized as mail servers.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Top Traffic to Mail Server/
Top Traffic from Internal to Mail Server (Response)	This data monitor shows the ten internal source hosts with the highest amount of traffic targeting internal hosts categorized as mail servers.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Top Traffic to Mail Server/
Top Traffic from External to Mail Server (Request)	This data monitor shows the ten external source hosts with the highest amount of traffic targeting internal hosts categorized as mail servers.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Top Traffic to Mail Server/

Resource	Description	Type	URI
Traffic Moving Average (ICMP)	This data monitor shows a moving average of the incoming ICMP traffic per minute for the last hour using 12 five-minute buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Traffic Moving Average/
Top Traffic from External to Web Server (Response)	This data monitor shows the ten external source hosts with the highest amount of traffic targeting internal hosts categorized as web servers.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Top Traffic to Web Server/
Traffic Moving Average (UDP)	This data monitor shows a moving average of the incoming UDP traffic per minute for the last hour using 12 five-minute buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Traffic Moving Average/
SYN Traffic	This filter identifies SYN (TCP transaction request) traffic.	Filter	ArcSight Foundation/Network Monitoring/Moving Average Filters/
Internal to Internal Traffic	This filter identifies Argus events internal to the company network.	Filter	ArcSight Foundation/Network Monitoring/Network Traffic Filters/
Application Protocol is NULL	This filter identifies if the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Common/Conditio nal Variable Filters/Protocol
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
External to Web Server	This filter identifies Argus events originating from the outside network, targeting internal hosts categorized as web servers.	Filter	ArcSight Foundation/Network Monitoring/Application Filters/Web Server/
UDP Traffic	This filter identifies UDP traffic.	Filter	ArcSight Foundation/Network Monitoring/Moving Average Filters/
TCP Traffic	This filter identifies TCP traffic.	Filter	ArcSight Foundation/Network Monitoring/Moving Average Filters/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Internal to Web Server	This filter identifies Argus events originating from inside the company network, targeting internal hosts categorized as web servers.	Filter	ArcSight Foundation/Network Monitoring/Application Filters/Web Server/



Resource	Description	Type	URI
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
External to Mail Server	This filter identifies Argus events originating from the outside network, targeting internal hosts categorized as mail servers.	Filter	ArcSight Foundation/Network Monitoring/Application Filters/Mail Server/
Internal to Mail Server	This filter identifies Argus events originating from inside the company network, targeting internal hosts categorized as mail servers.	Filter	ArcSight Foundation/Network Monitoring/Application Filters/Mail Server/
Qosient Argus	This filter identifies events originating from Argus connectors.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
Internal to Internal Events	This filter retrieves events internal to the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Network Traffic Reporting Devices	This filter identifies your network traffic reporting devices. The default network traffic reporting device is QoSient Argus.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
Inbound Traffic	This filter identifies Argus events originating from the outside network, targeting inside the company network.	Filter	ArcSight Foundation/Network Monitoring/Network Traffic Filters/
ICMP Traffic	This filter identifies ICMP traffic.	Filter	ArcSight Foundation/Network Monitoring/Moving Average Filters/
Top Attacker-Target Pairs by Protocol	This query returns the attacker-target pairs with the highest number of total bytes (Bytes In + Bytes Out) for a specific application protocol and groups them by attacker address, attacker zone, target address and target zone.	Query	ArcSight Foundation/Network Monitoring/Details/By Protocol/
Attacker Details by Protocol	This query returns the number of Bytes In, Bytes Out, and Total Bytes (Bytes In + Bytes Out) for a specific application protocol and groups them by attacker address and attacker zone.	Query	ArcSight Foundation/Network Monitoring/Details/By Protocol/

Resource	Description	Type	URI
Top Attackers by Protocol	This query returns the attacker/zone with the highest number of total bytes (Bytes In + Bytes Out) for a specific application protocol.	Query	ArcSight Foundation/Network Monitoring/Details/By Protocol/
Target Details by Protocol	This query returns the number of bytes in, bytes out, and total bytes (Bytes In + Bytes Out) for a specific application protocol and groups them by target address and target zone.	Query	ArcSight Foundation/Network Monitoring/Details/By Protocol/
Protocol Details by Host	This query returns the number of bytes in, bytes out, and total bytes (Bytes In + Bytes Out) for a specific attacker address/zone and groups the values by protocol, target address, and target zone.	Query	ArcSight Foundation/Network Monitoring/Details/By Host/
Top Protocols by Host	This query returns the protocols with the highest number of total bytes (Bytes In + Bytes Out) for a specific attacker address/zone.	Query	ArcSight Foundation/Network Monitoring/Details/By Host/
Top Targets by Protocol	This query returns the target/zone with the highest number of total bytes (Bytes In + Bytes Out) for a specific application protocol.	Query	ArcSight Foundation/Network Monitoring/Details/By Protocol/
Target Details by Host	This query returns the number of bytes in, bytes out, and total bytes (Bytes In + Bytes Out) for a specific attacker address/zone, and groups the values by target address and target zone.	Query	ArcSight Foundation/Network Monitoring/Details/By Host/
Top Targets by Host	This query returns the target address/zone with the highest number of total bytes (Bytes In + Bytes Out) for a specific attacker address/zone.	Query	ArcSight Foundation/Network Monitoring/Details/By Host/
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Two Charts One Table Portrait	This template is designed to show two charts and a table. The orientation is portrait.	Report Template	ArcSight System/2 Charts/With Table

## SANS Top 5 Reports

The SANS Top 5 Reports resources provide information about suspicious or unauthorized network traffic patterns.

### Devices

The following device types can supply events that apply to the SANS Top 5 Reports resource group:

- Network devices such as routers, firewalls, and VPNs

### Resources

The following table lists all the resources in the SANS Top 5 Reports resource group and any dependant resources.

**Table 3-4** Resources that Support the SANS Top 5 Reports Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Protocol Distribution Report	This report shows the top busiest protocols.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Traffic by Transport Protocol	This report shows the traffic repartition by transport protocol by minute for the last hour.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Traffic Moving Average Report	This report shows the moving average of ICMP, UDP, and TCP Traffic for the last hour.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top 10 Talkers	This report shows the top ten talkers.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top List of Accessed Web Sites	This report shows the top accessed web sites.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/

Resource	Description	Type	URI
Top Target IPs	This report shows the top target IP addresses.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top Source Ports	This report shows the busiest source ports.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top 10 Types of Traffic	This report shows the top ten types of traffic.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top List of Highest Bandwidth-Consuming Conversations	This report shows the highest bandwidth-consuming conversations.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
<b>Library Resources</b>			
TCP Traffic	This filter identifies TCP Traffic.	Filter	ArcSight Foundation/Network Monitoring/Report Parameter Filters/
Application Protocol is NULL	This filter identifies if the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Qosient Argus	This filter identifies events originating from Argus connectors.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
UDP Traffic	This filter identifies UDP Traffic.	Filter	ArcSight Foundation/Network Monitoring/Report Parameter Filters/
ICMP Traffic	This filter is used to identify ICMP Traffic.	Filter	ArcSight Foundation/Network Monitoring/Report Parameter Filters/
Network Traffic Reporting Devices	This filter identifies your network traffic reporting devices. The default network traffic reporting device is QoSient Argus.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/

Resource	Description	Type	URI
Top Targets	This query retrieves the target ports with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top Target IPs/
Top Source Ports	This query retrieves the attacker ports with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top Source Ports/
Traffic by Transport Protocol	This query retrieves the number of total bytes (Bytes In + Bytes Out) by transport protocol within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Traffic by Transport Protocol/
Top Protocols	This query retrieves the protocol with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top 10 Types of Traffic
Top Attacker-Target Pairs	This query retrieves the attacker-target pairs with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top List of Highest Bandwidth- Consuming Conversations/
Top Accessed Web Sites	This query retrieves the target address or zone of the websites with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top List of Accessed Web Sites/
Top Attackers	This query retrieves the attacker or zone with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top 10 Talkers/

Resource	Description	Type	URI
Traffic Spike Rule Fired Events	This query retrieves correlation events generated by moving average data monitors looking for TCP, UDP, and ICMP spikes within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Traffic Moving Average Report/
Simple Chart Portrait	This template is designed to show one chart. The orientation is portrait.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Three Tables Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/3 Tables
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

## Traffic Overview

The Traffic Overview resources provide an overview of network traffic.

### Devices

The following device types can supply events that apply to the Traffic Overview resource group:

- Qosient Argus and network devices such as routers, firewalls, and VPNs

### Resources

The following table lists all the resources in the Traffic Overview resource group and any dependant resources.

**Table 3-5** Resources that Support the Traffic Overview Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Top Inbound Traffic by Host	This dashboard shows an overview of the inbound traffic (external network to internal network) by source host. This dashboard contains the Top Inbound Traffic by Host (Request) and Top Inbound Traffic by Host (Response) data monitors.	Dashboard	ArcSight Foundation/Network Monitoring/Inbound Traffic/
Top Outbound Traffic by Application Protocol	This dashboard shows an overview of the outbound traffic (internal network to external network) by application protocol. This dashboard contains the Top Outbound Traffic by Application Protocol (Request) and Top Outbound Traffic by Application Protocol (Response) data monitors.	Dashboard	ArcSight Foundation/Network Monitoring/Outbound Traffic/
Outbound Traffic Moving Average	This dashboard shows a moving average of the outbound traffic (internal network to external network) for the last hour. This dashboard contains the Outbound Traffic Moving Average (Request) and Outbound Traffic Moving Average (Response) data monitors.	Dashboard	ArcSight Foundation/Network Monitoring/Outbound Traffic/
Inbound Traffic Moving Average	This dashboard shows a moving average of the inbound traffic (external network to internal network) for the last hour. This dashboard contains the Inbound Traffic Moving Average (Request) and Inbound Traffic Moving Average (Response) data monitors.	Dashboard	ArcSight Foundation/Network Monitoring/Inbound Traffic/

Resource	Description	Type	URI
Top Inbound Traffic by Application Protocol	This dashboard shows an overview of the inbound traffic (external network to internal network) by application protocol. This dashboard contains the Top Inbound Traffic by Application Protocol (Request) and Top Inbound Traffic by Application Protocol (Response) data monitors.	Dashboard	ArcSight Foundation/Network Monitoring/Inbound Traffic/
Top Outbound Traffic by Host	This dashboard shows an overview of the outbound traffic (internal network to external network) by source host. This dashboard contains the Top Outbound Traffic by Host (Request) and Top Outbound Traffic by Host (Response) data monitors.	Dashboard	ArcSight Foundation/Network Monitoring/Outbound Traffic/
Traffic Statistics	This report displays the bytes in and out by hour, and bytes in and out by device. A table shows the hour, firewall zone and address, the transport protocol, and the bytes in and out.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/
Outbound Traffic by Protocol - Weekly Summary	This report shows an operational summary of the outbound traffic usage for the last week. You can specify the application protocol on which you want to focus.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/Summaries/
Daily Traffic Summary	This report shows a daily traffic summary.	Report	ArcSight Foundation/Network Monitoring/Executive Summaries/
Inbound Traffic - Top Protocols	This report shows an operational summary of the inbound traffic usage by protocol.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/
Quarterly Traffic Summary	This report shows an executive summary of the traffic for the last quarter, grouped by week.	Report	ArcSight Foundation/Network Monitoring/Executive Summaries/
Weekly Traffic Summary	This report shows an executive summary of the traffic for the last week, grouped by day.	Report	ArcSight Foundation/Network Monitoring/Executive Summaries/
Outbound Traffic - Weekly Summary	This report shows an operational summary of the outbound traffic usage for the last week.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/Summaries/



Resource	Description	Type	URI
Outbound Traffic - Daily Summary	This report shows an operational summary of the outbound traffic usage for the last day.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/Summaries/
Inbound Traffic - Daily Summary	This report shows an operational summary of the inbound traffic usage for the last day.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Summaries/
Traffic Snapshot	This report shows the top ten protocols, top ten attackers, and top ten targets.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/
Inbound Traffic - Weekly Summary	This report shows an operational summary of the inbound traffic usage for the last week.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Summaries/
Inbound Traffic - Top Source Hosts	This report shows an operational summary of the inbound traffic usage by source hosts.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/
Outbound Traffic - Top Source Hosts	This report shows an operational summary of the outbound traffic usage by source hosts.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/
Outbound Traffic - Top Protocols	This report shows an operational summary of the outbound traffic usage by protocol.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/
Inbound Traffic by Protocol - Weekly Summary	This report shows an operational summary of the inbound traffic usage for the last week. You can specify the application protocol on which you want to focus.	Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Summaries/
Monthly Traffic Summary	This report shows an executive summary of the traffic for the last month.	Report	ArcSight Foundation/Network Monitoring/Executive Summaries/
<b>Library - Correlation Resources</b>			
TCP Traffic Spike	This rule monitors the moving average of inbound TCP events (external network to internal network). The rule triggers when the number of TCP packets per minute increases 50% or more.	Rule	ArcSight Foundation/Network Monitoring/

Resource	Description	Type	URI
High Number of Denied Connections for A Source Host	This rule detects firewall deny events. The rule triggers when ten events originating from the same source host occur within two minutes.	Rule	ArcSight Foundation/Network Monitoring/
ICMP Traffic Spike	This rule monitors the moving average of inbound ICMP events (external network to internal network). The rule triggers when the number of ICMP packets per minute increases 50% or more.	Rule	ArcSight Foundation/Network Monitoring/
High Number of Connections	This rule detects firewall accept events for MSSQL, Terminal Services, and TFTP connections (default destination ports: MSSQL=1433, Terminal Services=2289, TFTP=69). The rule triggers when ten events from the same device occur within two minutes.	Rule	ArcSight Foundation/Network Monitoring/
High Number of Denied Inbound Connections	This rule detects inbound firewall deny events. The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Foundation/Network Monitoring/
SYN Traffic Spike	This rule monitors the moving average of inbound SYN events (external network to internal network). The rule triggers when the number of SYN packets per minute increases 50% or more.	Rule	ArcSight Foundation/Network Monitoring/
UDP Traffic Spike	This rule monitors the moving average of inbound UDP events (external network to internal network). The rule triggers when the number of UDP packets per minute increases 50% or more.	Rule	ArcSight Foundation/Network Monitoring/
<b>Library Resources</b>			
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	Active List	ArcSight System/Tuning
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces

Resource	Description	Type	URI
Outbound Traffic Moving Average (Response)	This data monitor shows a moving average of the outbound traffic (internal network to external network). This data monitor focuses on the bytes contained in the responses the internal hosts get from the external hosts. This data monitor shows the average amount of bytes/sec for the last hour using 12 five-minutes buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/Outbound Traffic/Outbound Traffic Moving Average/
Top Outbound Traffic by Application Protocol (Request)	This data monitor shows the ten application protocols with the highest amount of outbound traffic (internal network to external network). This data monitor focuses on the total number of bytes by application protocol contained in the requests the internal hosts are sending to the external hosts.	Data Monitor	ArcSight Foundation/Network Monitoring/Outbound Traffic/Top Outbound Traffic by Application Protocol/
Top Inbound Traffic by Host (Request)	This data monitor shows the ten source hosts with the highest amount of inbound traffic (external network to internal network). This data monitor focuses on the total number of bytes contained in the requests the host is sending to the internal network.	Data Monitor	ArcSight Foundation/Network Monitoring/Inbound Traffic/Top Inbound Traffic by Host/
Top Outbound Traffic by Application Protocol (Response)	This data monitor shows the ten application protocols with the highest amount of outbound traffic (internal network to external network). This data monitor focuses on the total number of bytes by application protocol contained in the responses the internal hosts get from the external hosts.	Data Monitor	ArcSight Foundation/Network Monitoring/Outbound Traffic/Top Outbound Traffic by Application Protocol/
Top Outbound Traffic by Host (Request)	This data monitor shows the ten source hosts with the highest amount of outbound traffic (internal network to external network). This data monitor focuses on the total number of bytes contained in the requests the internal host is sending to the external network.	Data Monitor	ArcSight Foundation/Network Monitoring/Outbound Traffic/Top Outbound Traffic by Host/

Resource	Description	Type	URI
Top Inbound Traffic by Application Protocol (Request)	This data monitor shows the ten application protocols with the highest amount of inbound traffic (external network to internal network). This data monitor focuses on the total number of bytes by application protocol contained in the requests the external hosts are sending to the internal hosts.	Data Monitor	ArcSight Foundation/Network Monitoring/Inbound Traffic/Top Inbound Traffic by Application Protocol/
Top Inbound Traffic by Host (Response)	This data monitor shows the ten source hosts with the highest amount of inbound traffic (external network to internal network). This data monitor focuses on the total number of bytes contained in the responses the host gets from the external network.	Data Monitor	ArcSight Foundation/Network Monitoring/Inbound Traffic/Top Inbound Traffic by Host/
Top Inbound Traffic by Application Protocol (Response)	This data monitor shows the ten application protocols with the highest amount of inbound traffic (external network to internal network). This data monitor focuses on the total number of bytes by application protocol contained in the responses the external hosts get from the internal hosts.	Data Monitor	ArcSight Foundation/Network Monitoring/Inbound Traffic/Top Inbound Traffic by Application Protocol/
Inbound Traffic Moving Average (Response)	This data monitor shows a moving average of the inbound traffic (external network to internal network). This data monitor focuses on the bytes contained in the responses the external hosts get from the internal hosts. This data monitor shows the average amount of bytes/sec for the last hour using 12 five-minutes buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/Inbound Traffic/Inbound Traffic Moving Average/
Top Outbound Traffic by Host (Response)	This data monitor shows the ten source hosts with the highest amount of outbound traffic (internal network to external network). This data monitor focuses on the total number of bytes contained in the responses the internal host gets from the external network.	Data Monitor	ArcSight Foundation/Network Monitoring/Outbound Traffic/Top Outbound Traffic by Host/

Resource	Description	Type	URI
Inbound Traffic Moving Average (Request)	This data monitor shows a moving average of the inbound traffic (external network to internal network). This data monitor focuses on the bytes contained in the requests the external hosts are sending to the internal hosts. This data monitor shows the average amount of bytes/sec for the last hour using 12 five-minutes buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/Inbound Traffic/Inbound Traffic Moving Average/
Outbound Traffic Moving Average (Request)	This data monitor shows a moving average of the outbound traffic (internal network to external network). This data monitor focuses on the bytes contained in the requests the internal hosts are sending to the external hosts. This data monitor shows the average amount of bytes/sec for the last hour using 12 five-minutes buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/Outbound Traffic/Outbound Traffic Moving Average/
Target Port is NULL	This filter is used by variables to check if the event target has a port number associated with it.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Application Protocol is NULL	This filter identifies if the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Qosient Argus	This filter identifies events originating from Argus connectors.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
Outbound Traffic	This filter detects Argus events originating inside the company network and targeting the outside network.	Filter	ArcSight Foundation/Network Monitoring/Network Traffic Filters/
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters

Resource	Description	Type	URI
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Inbound Traffic	This filter identifies Argus events originating from the outside network, targeting inside the company network.	Filter	ArcSight Foundation/Network Monitoring/Network Traffic Filters/
Network Traffic Reporting Devices	This filter identifies your network traffic reporting devices. The default network traffic reporting device is QoSient Argus.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
Inbound http Traffic - Weekly Summary	This report shows an operational summary of the inbound http traffic usage for the last week. This is a focused report that depends on the Inbound Traffic by Protocol - Weekly Summary report.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Summaries/Focused Reports/
Outbound http Traffic - Weekly Summary	This report shows an operational summary of the outbound http traffic usage for the last week. This is a focused report that depends on the Outbound Traffic by Protocol - Weekly Summary report.	Focused Report	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/Summaries/Focused Reports/
Top Protocols	This query returns the protocol with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Traffic Snapshot/
Outbound Traffic by Source Host	This query returns outbound events (internal network to external network) and groups them by attacker address and attacker zone. The query selects the attacker address, the attacker zone name, and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/
Outbound Traffic by Transport Protocol	This query returns outbound events (internal network to external network) and groups them by transport protocol. The query selects the transport protocol and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/

Resource	Description	Type	URI
Inbound Traffic - Hourly	This query retrieves the information stored in the Inbound Traffic by Application Protocol trend table. The query returns the sums of Bytes In and Bytes Out and groups them by hour.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Trend Queries/
Outbound Traffic by Application Protocol - Daily	This query retrieves the information stored in the Outbound Traffic by Application Protocol trend table. The query returns the sums of Bytes In and Bytes Out and groups them by day. You can choose a specific application protocol to create a focused report, such as the Outbound http Traffic - Weekly Summary report.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/Trend Queries/
Inbound Traffic by Transport Protocol	This query retrieves inbound events (external network to internal network) and groups them by transport protocol. The query returns the transport protocol and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/
Inbound Traffic by Application Protocol	This query returns inbound events (external network to internal network) and groups them by application protocol. The query selects the application protocol and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/
Outbound Traffic - Daily	This query retrieves the information stored in the Outbound Traffic by Application Protocol trend table. The query returns the sums of Bytes In and Bytes Out grouped by day.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/Trend Queries/
Inbound Traffic by Application Protocol - Daily	This query retrieves the information stored in the Inbound Traffic by Application Protocol Trend Table. The query returns the sums of Bytes In and Bytes Out and groups them by day. You can choose a specific application protocol to create a focused report, such as the Inbound http Traffic - Weekly Summary report.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Trend Queries/
Overall Traffic - By Day	This query retrieves the number of incoming bytes, outgoing bytes, and total bytes (Incoming Bytes + Outgoing Bytes) in the Overall Traffic trend table and groups the values by day.	Query	ArcSight Foundation/Network Monitoring/Executive Summaries/Trend Queries/

Resource	Description	Type	URI
Top Attackers	This query returns the attacker address or zone with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Traffic Snapshot/
Outbound Traffic	This query retrieves outbound events (internal network to external network) and returns the sums of Bytes In and Bytes Out grouped by target port, application protocol, and hour. This query is used by the Outbound Traffic by Application Protocol trend.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/Event Queries/
Top Targets	This query returns the target address or zone with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Traffic Snapshot/
Inbound Traffic	This query retrieves inbound events (external network to internal network) and returns the sums of Bytes In and Bytes Out grouped by target port, application protocol, and hour. This query is used by the Inbound Traffic by Application Protocol Trend.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Event Queries/
Overall Traffic - By Month	This query retrieves the number of incoming bytes, outgoing bytes, and total bytes (Incoming Bytes + Outgoing Bytes) in the Overall Traffic trend table and groups the values by month.	Query	ArcSight Foundation/Network Monitoring/Executive Summaries/Trend Queries/
Inbound Traffic - Daily	This query retrieves the information stored in the Inbound Traffic by Application Protocol trend table. The query returns the sums of Bytes In and Bytes Out and groups them by day.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/Trend Queries/
Inbound Traffic by Source Host	This query returns inbound events (external network to internal network) and groups them by attacker address and attacker zone. The query selects the attacker address, the attacker zone, and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Inbound Traffic/
Firewall Bandwidth Usage by Hour (chart)	This query returns firewall events.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Traffic Statistics/



Resource	Description	Type	URI
Bandwidth Usage by Firewall Address	This query returns firewall events.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Traffic Statistics/
Firewall Bandwidth Usage per Hour	This query returns firewall events.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Traffic Statistics/
Overall Traffic	This query identifies the overall number of incoming bytes and outgoing bytes. The incoming bytes are the sum of the number of bytes in requests in the inbound events (external network to internal network) and the number of bytes in responses in the outbound events (internal network to external network). The outgoing bytes are the sum of the number of bytes in requests in the outbound events (internal network to external network) and the number of bytes in responses in the inbound events (external network to internal network). This query is used by the Overall Traffic trend.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Bandwidth Utilization/Event Queries/
Outbound Traffic - Hourly	This query retrieves the information stored in the Outbound Traffic by Application Protocol trend table and returns the sums of Bytes In and Bytes Out and groups them by hour.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/Trend Queries/
Overall Traffic - By Hour	This query returns the number of incoming bytes, outgoing bytes, and total bytes (Incoming Bytes + Outgoing Bytes) in the Overall Traffic trend table and groups the values by hour.	Query	ArcSight Foundation/Network Monitoring/Executive Summaries/Trend Queries/
Outbound Traffic by Application Protocol	This query retrieves outbound events (internal network to external network) and groups them by application protocol. The query returns the application protocol and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Foundation/Network Monitoring/Operational Summaries/Outbound Traffic/
Three Charts Landscape	This template is designed to show three charts and a description field. The orientation is landscape.	Report Template	ArcSight System/3 Charts/Without Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table

Resource	Description	Type	URI
Three Tables Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/3 Tables
Two Charts Portrait	This template is designed to show two charts. The orientation is portrait.	Report Template	ArcSight System/2 Charts/Without Table
Two Charts One Table Landscape	This template is designed to show two charts and a table. The orientation is landscape.	Report Template	ArcSight System/2 Charts/With Table
Two Charts Landscape	This template is designed to show two charts and a description field. The orientation is portrait.	Report Template	ArcSight System/2 Charts/Without Table
Outbound Traffic by Application Protocol	This trend runs every hour using the Outbound Traffic query. The trend table stores the total number of bytes contained in the requests and responses and group them by application protocol, target port, and hour.	Trend	ArcSight Foundation/Network Monitoring/
Inbound Traffic by Application Protocol	This trend runs every hour using the Inbound Traffic query. The trend table stores the total number of bytes contained in the requests and responses and group them by application protocol, target port, and hour.	Trend	ArcSight Foundation/Network Monitoring/
Overall Traffic	This trend stores the total number of incoming bytes and outgoing bytes per hour. The trend runs every day using the Overall Traffic query.	Trend	ArcSight Foundation/Network Monitoring/

# Index

---

## A

- Accepted Inbound Connections filter 33
- Accepted Outbound Connections filter 33
- active channels
  - Argus Events 22
- active lists
  - Event-based Rule Exclusions 50
  - general configuration 18
- All Events filter 24, 33
- Application Protocol is NULL filter 24, 40, 44, 53
- ArcSight Administration overview 5
- ArcSight Core Security overview 5
- ArcSight Express field set 32
- ArcSight Foundations overview 6
- ArcSight System overview 6
- Argus Events active channel 22
- Argus field set 24
- asset categories
  - Email 38
  - Protected 23, 31, 39, 50
  - Web Server 39
- Attacker Details by Protocol query 41
- Attacker Details by Protocol report 38
- Authentication Errors query 35
- Authentication Errors report 30
- Average Bandwidth Utilization - Business Hours query 27

## B

- Bandwidth to or from External Systems filter 25
- Bandwidth Usage by Firewall Address query 57
- Bandwidth Usage by Hour report 23
- Bandwidth Usage by Protocol focused report 25, 26
- Bandwidth Usage by Protocol query 27
- Bandwidth Usage by Protocol report 23
- Bandwidth Usage per Hour focused report 25, 26
- Bandwidth Usage per Hour query 27
- Bandwidth Usage resource group 22
- Bandwidth Utilization - Business Hours report 23
- Bandwidth Utilization - By Hour query 28
- Bandwidth Utilization - By Minute query 27
- Bandwidth Utilization - Last 24 Hours report 23
- Bandwidth Utilization - Last Hour report 23

## C

- Chart and Table Landscape report template 28, 46
- Chart and Table Portrait report template 28, 36, 42, 46
- configuration
  - active lists 18
- Connections Accepted by Address query 34

- Connections Accepted by Address report 30
- Connections Denied by Address query 35
- Connections Denied by Address report 29
- Connections Denied by Hour query 35
- Connections Denied by Hour report 29
- content packages 7
- Critical Network Events filter 33
- Current Bandwidth dashboard 22

## D

- Daily Traffic Summary report 48
- dashboards
  - Current Bandwidth 22
  - Firewall Connection Overview 29
  - Inbound Bandwidth 22
  - Inbound Traffic Moving Average 47
  - Network Status Overview 29
  - Outbound Bandwidth 22
  - Outbound Traffic Moving Average 47
  - Top Inbound Traffic by Application Protocol 48
  - Top Inbound Traffic by Host 47
  - Top Outbound Traffic by Application Protocol 48
  - Top Outbound Traffic by Host 48
  - Top Traffic to Mail Server 37
  - Top Traffic to Web Server 38
  - Traffic Moving Average 37
  - VPN Connection Statistics 29
- data monitors
  - Devices with High Error Rates 31
  - Inbound Bandwidth - Last 10 Minutes 24
  - Inbound Bandwidth - Last Hour 24
  - Inbound Bandwidth - Last Minute 24
  - Inbound Traffic Moving Average (Request) 53
  - Inbound Traffic Moving Average (Response) 52
  - Last 10 Critical Network Events 31
  - Last 10 Interface Down Messages 32
  - Last 10 Interface Status Messages 31
  - Outbound Bandwidth - Last 10 Minutes 24
  - Outbound Bandwidth - Last Hour 23
  - Outbound Bandwidth - Last Minute 23
  - Outbound Traffic Moving Average (Request) 53
  - Outbound Traffic Moving Average (Response) 51
  - Top 10 Accepted Ports (Inbound) 32
  - Top 10 Accepted Ports (Outbound) 32
  - Top 10 Denied Ports (Inbound) 32
  - Top 10 Denied Ports (Outbound) 32
  - Top 10 Hosts With Denied Inbound Connections 31
  - Top 10 Hosts With Denied Outbound Connections 31
  - Top Inbound Traffic by Application Protocol (Request) 52

- Top Inbound Traffic by Application Protocol (Response) 52
- Top Inbound Traffic by Host (Request) 51
- Top Inbound Traffic by Host (Response) 52
- Top Outbound Traffic by Application Protocol (Request) 51
- Top Outbound Traffic by Application Protocol (Response) 51
- Top Outbound Traffic by Host (Request) 51
- Top Outbound Traffic by Host (Response) 52
- Top Traffic from External to Mail Server (Request) 39
- Top Traffic from External to Mail Server (Response) 39
- Top Traffic from External to Web Server (Request) 39
- Top Traffic from External to Web Server (Response) 40
- Top Traffic from Internal to Mail Server (Request) 39
- Top Traffic from Internal to Mail Server (Response) 39
- Top Traffic from Internal to Web Server (Request) 39
- Top Traffic from Internal to Web Server (Response) 39
- Top VPN Servers with Authentication Errors 31
- Top VPN Servers with Denied Connections 31
- Top VPN Servers with Successful Connections 32
- Top VPN Users with Authentication Errors 31
- Traffic Moving Average (ICMP) 40
- Traffic Moving Average (SYN) 39
- Traffic Moving Average (TCP) 39
- Traffic Moving Average (UDP) 40
- Denied Inbound Connections filter 33
- Denied Outbound Connections filter 32
- Detailed Traffic by Host report 38
- Detailed Traffic by Protocol report 38
- Device Activity resource group 29
- Device Critical Events query 35
- Device Critical Events report 31
- Device Errors query 34
- Device Errors report 30
- Device Events query 35
- Device Events report 30
- Device Interface Down Notifications query 34
- Device Interface Down Notifications report 29
- Device Interface Status Messages query 35
- Device Interface Status Messages report 30
- Devices with High Error Rates data monitor 31

## E

- Email asset category 38
- Event-based Rule Exclusions active list 50
- External Source filter 24, 32, 40, 53
- External Target filter 25, 33, 53
- External to Mail Server filter 41
- External to Web Server filter 40

## F

- Failed VPN Connection Events filter 32
- field sets
  - ArcSight Express 32

- Argus 24
- filters

- Accepted Inbound Connections 33
- Accepted Outbound Connections 33
- All Events 24, 33
- Application Protocol is NULL 24, 40, 44, 53
- Bandwidth to or from External Systems 25
- Critical Network Events 33
- Denied Inbound Connections 33
- Denied Outbound Connections 32
- External Source 24, 32, 40, 53
- External Target 25, 33, 53
- External to Mail Server 41
- External to Web Server 40
- Failed VPN Connection Events 32
- Firewall Events 25
- ICMP Traffic 41, 44
- Inbound and Outbound Traffic 25
- Inbound Events 25, 33, 41, 53
- Inbound Traffic 25, 41, 54
- Internal Source 24, 33, 40, 54
- Internal Target 24, 33, 41, 54
- Internal to Internal Events 41
- Internal to Internal Traffic 40
- Internal to Mail Server 41
- Internal to Web Server 40
- Network Device Interface Down Messages 34
- Network Device Interface Status Events 33
- Network Error Events 34
- Network Events 24
- Network Traffic Reporting Devices 25, 41, 44, 54
- Outbound Events 24, 33, 53
- Outbound Traffic 25, 53
- Qosient Argus 25, 41, 44, 53
- Successful VPN Connection Events 33
- SYN Traffic 40
- Target Port is NULL 53
- Target User ID is NULL 32
- Target User Name is NULL 33
- TCP Traffic 40, 44
- UDP Traffic 40, 44
- VPN Authentication Errors 34
- VPN Events 24
- Firewall Bandwidth Usage by Hour (chart) query 56
- Firewall Bandwidth Usage per Hour query 57
- Firewall Connection Overview dashboard 29
- Firewall Events filter 25
- focused reports
  - Bandwidth Usage by Protocol 25, 26
  - Bandwidth Usage per Hour 25, 26
  - Inbound http Traffic - Weekly Summary 54
  - Outbound http Traffic - Weekly Summary 54
  - Top Bandwidth Hosts 26

## H

- High Number of Connections rule 50
- High Number of Denied Connections for A Source Host rule 50
- High Number of Denied Inbound Connections rule 50
- Hosts and Protocols resource group 37

## I

- ICMP Traffic filter 41, 44

ICMP Traffic Spike rule 50  
 Inbound and Outbound Traffic filter 25  
 Inbound Bandwidth - Last 10 Minutes data monitor 24  
 Inbound Bandwidth - Last Hour data monitor 24  
 Inbound Bandwidth - Last Minute data monitor 24  
 Inbound Bandwidth dashboard 22  
 Inbound Events filter 25, 33, 41, 53  
 Inbound http Traffic - Weekly Summary focused report 54  
 Inbound Traffic - Daily query 56  
 Inbound Traffic - Daily Summary report 49  
 Inbound Traffic - Hourly query 55  
 Inbound Traffic - Top Protocols report 48  
 Inbound Traffic - Top Source Hosts report 49  
 Inbound Traffic - Weekly Summary report 49  
 Inbound Traffic by Application Protocol - Daily query 55  
 Inbound Traffic by Application Protocol query 55  
 Inbound Traffic by Application Protocol trend 58  
 Inbound Traffic by Protocol - Weekly Summary report 49  
 Inbound Traffic by Source Host query 56  
 Inbound Traffic by Transport Protocol query 55  
 Inbound Traffic filter 25, 41, 54  
 Inbound Traffic Moving Average (Request) data monitor 53  
 Inbound Traffic Moving Average (Response) data monitor 52  
 Inbound Traffic Moving Average dashboard 47  
 Inbound Traffic query 56  
 Internal Source filter 24, 33, 40, 54  
 Internal Target filter 24, 33, 41, 54  
 Internal to Internal Events filter 41  
 Internal to Internal Traffic filter 40  
 Internal to Mail Server filter 41  
 Internal to Web Server filter 40

## L

Last 10 Critical Network Events data monitor 31  
 Last 10 Interface Down Messages data monitor 32  
 Last 10 Interface Status Messages data monitor 31

## M

Monthly Traffic Summary report 49

## N

Network Device Interface Down Messages filter 34  
 Network Device Interface Status Events filter 33  
 Network Error Events filter 34  
 Network Events filter 24  
 Network Monitoring Foundation  
   Supported Devices 8  
 Network Status Overview dashboard 29  
 Network Traffic Reporting Devices filter 25, 41, 44, 54

## O

Outbound Bandwidth - Last 10 Minutes data monitor 24  
 Outbound Bandwidth - Last Hour data monitor 23  
 Outbound Bandwidth - Last Minute data monitor 23  
 Outbound Bandwidth dashboard 22  
 Outbound Events filter 24, 33, 53  
 Outbound http Traffic - Weekly Summary focused report 54

Outbound Traffic - Daily query 55  
 Outbound Traffic - Daily Summary report 49  
 Outbound Traffic - Hourly query 57  
 Outbound Traffic - Top Protocols report 49  
 Outbound Traffic - Top Source Hosts report 49  
 Outbound Traffic - Weekly Summary report 48  
 Outbound Traffic by Application Protocol - Daily query 55  
 Outbound Traffic by Application Protocol query 57  
 Outbound Traffic by Application Protocol trend 58  
 Outbound Traffic by Protocol - Weekly Summary report 48  
 Outbound Traffic by Source Host query 54  
 Outbound Traffic by Transport Protocol query 54  
 Outbound Traffic filter 25, 53  
 Outbound Traffic Moving Average (Request) data monitor 53  
 Outbound Traffic Moving Average (Response) data monitor 51  
 Outbound Traffic Moving Average dashboard 47  
 Outbound Traffic query 56  
 Overall Traffic - By Day query 55  
 Overall Traffic - By Hour query 57  
 Overall Traffic - By Month query 56  
 Overall Traffic query 27, 57  
 Overall Traffic trend 28, 58

## P

packages  
   deleting 12  
   installing 11  
   uninstalling 11  
 Protected asset category 23, 31, 39, 50  
 Protocol Details by Host query 42  
 Protocol Details by Host report 38  
 Protocol Distribution Report report 43

## Q

Qosient Argus filter 25, 41, 44, 53  
 Quarterly Traffic Summary report 48  
 queries  
   Attacker Details by Protocol 41  
   Authentication Errors 35  
   Average Bandwidth Utilization - Business Hours 27  
   Bandwidth Usage by Firewall Address 57  
   Bandwidth Usage by Protocol 27  
   Bandwidth Usage per Hour 27  
   Bandwidth Utilization - By Hour 28  
   Bandwidth Utilization - By Minute 27  
   Connections Accepted by Address 34  
   Connections Denied by Address 35  
   Connections Denied by Hour 35  
   Device Critical Events 35  
   Device Errors 34  
   Device Events 35  
   Device Interface Down Notifications 34  
   Device Interface Status Messages 35  
   Firewall Bandwidth Usage by Hour (chart) 56  
   Firewall Bandwidth Usage per Hour 57  
   Inbound Traffic 56  
   Inbound Traffic - Daily 56  
   Inbound Traffic - Hourly 55  
   Inbound Traffic by Application Protocol 55  
   Inbound Traffic by Application Protocol - Daily 55

- Inbound Traffic by Source Host 56
- Inbound Traffic by Transport Protocol 55
- Outbound Traffic 56
- Outbound Traffic - Daily 55
- Outbound Traffic - Hourly 57
- Outbound Traffic by Application Protocol 57
- Outbound Traffic by Application Protocol - Daily 55
- Outbound Traffic by Source Host 54
- Outbound Traffic by Transport Protocol 54
- Overall Traffic 27, 57
- Overall Traffic - By Day 55
- Overall Traffic - By Hour 57
- Overall Traffic - By Month 56
- Protocol Details by Host 42
- Target Details by Host 42
- Target Details by Protocol 42
- Top Accessed Web Sites 45
- Top Attackers 45, 56
- Top Attackers by Protocol 42
- Top Attacker-Target Pairs 45
- Top Attacker-Target Pairs by Protocol 41
- Top Bandwidth Hosts 27
- Top Connections Accepted by Address 35
- Top Connections Denied by Address 34
- Top Protocols 45, 54
- Top Protocols by Host 42
- Top Source Ports 45
- Top Targets 45, 56
- Top Targets by Host 42
- Top Targets by Protocol 42
- Top VPN Accesses by User 35
- Top VPN Event Destinations 34
- Top VPN Event Sources 34
- Top VPN Events 35
- Traffic by Transport Protocol 45
- Traffic Spike Rule Fired Events 46
- VPN Connection Attempts 34
- VPN Connection Failures 35

## R

### report templates

- Chart and Table Landscape 28, 46
- Chart and Table Portrait 28, 36, 42, 46
- Simple Chart Landscape 28, 46, 57
- Simple Chart Portrait 46
- Simple Table Landscape 36
- Simple Table Portrait 36
- Three Charts Landscape 57
- Three Tables Portrait 46, 58
- Two Charts Landscape 58
- Two Charts One Table Landscape 38
- Two Charts One Table Portrait 42
- Two Charts Portrait 28, 58

### reports

- Attacker Details by Protocol 38
- Authentication Errors 30
- Bandwidth Usage by Hour 23
- Bandwidth Usage by Protocol 23
- Bandwidth Utilization - Business Hours 23
- Bandwidth Utilization - Last 24 Hours 23
- Bandwidth Utilization - Last Hour 23
- Connections Accepted by Address 30
- Connections Denied by Address 29
- Connections Denied by Hour 29

- Daily Traffic Summary 48
- Detailed Traffic by Host 38
- Detailed Traffic by Protocol 38
- Device Critical Events 31
- Device Errors 30
- Device Events 30
- Device Interface Down Notifications 29
- Device Interface Status Messages 30
- Inbound Traffic - Daily Summary 49
- Inbound Traffic - Top Protocols 48
- Inbound Traffic - Top Source Hosts 49
- Inbound Traffic - Weekly Summary 49
- Inbound Traffic by Protocol - Weekly Summary 49
- Monthly Traffic Summary 49
- Outbound Traffic - Daily Summary 49
- Outbound Traffic - Top Protocols 49
- Outbound Traffic - Top Source Hosts 49
- Outbound Traffic - Weekly Summary 48
- Outbound Traffic by Protocol - Weekly Summary 48
- Protocol Details by Host 38
- Protocol Distribution Report 43
- Quarterly Traffic Summary 48
- Target Details by Host 38
- Target Details by Protocol 38
- Top 10 Talkers 43
- Top 10 Types of Traffic 44
- Top Bandwidth Hosts 22
- Top List of Accessed Web Sites 43
- Top List of Highest Bandwidth-Consuming Conversations 44
- Top Source Ports 44
- Top Target IPs 44
- Top VPN Access by User 30
- Top VPN Event Destinations 30
- Top VPN Event Sources 29
- Top VPN Events 30
- Traffic by Transport Protocol 43
- Traffic Moving Average Report 43
- Traffic Snapshot 49
- Traffic Statistics 48
- VPN Connection Attempts 30
- VPN Connection Failures 30
- Weekly Traffic Summary 48

### resource group

- Bandwidth Usage 22
- Device Activity 29
- Hosts and Protocols 37
- SANS Top 5 Reports 43
- Traffic Overview 47

### rules

- High Number of Connections 50
- High Number of Denied Connections for A Source Host 50
- High Number of Denied Inbound Connections 50
- ICMP Traffic Spike 50
- SYN Traffic Spike 50
- TCP Traffic Spike 49
- UDP Traffic Spike 50

## S

- SANS Top 5 Reports resource group 43
- shared libraries 6
- Simple Chart Landscape report template 28, 46, 57
- Simple Chart Portrait report template 46

Simple Table Landscape report template 36  
 Simple Table Portrait report template 36  
 Successful VPN Connection Events filter 33  
 SYN Traffic filter 40  
 SYN Traffic Spike rule 50

## T

Target Details by Host query 42  
 Target Details by Host report 38  
 Target Details by Protocol query 42  
 Target Details by Protocol report 38  
 Target Port is NULL filter 53  
 Target User ID is NULL filter 32  
 Target User Name is NULL filter 33  
 TCP Traffic filter 40, 44  
 TCP Traffic Spike rule 49  
 Three Charts Landscape report template 57  
 Three Tables Portrait report template 46, 58  
 Top 10 Accepted Ports (Inbound) data monitor 32  
 Top 10 Accepted Ports (Outbound) data monitor 32  
 Top 10 Denied Ports (Inbound) data monitor 32  
 Top 10 Denied Ports (Outbound) data monitor 32  
 Top 10 Hosts With Denied Inbound Connections data monitor 31  
 Top 10 Hosts With Denied Outbound Connections data monitor 31  
 Top 10 Talkers report 43  
 Top 10 Types of Traffic report 44  
 Top Accessed Web Sites query 45  
 Top Attackers by Protocol query 42  
 Top Attackers query 45, 56  
 Top Attacker-Target Pairs by Protocol query 41  
 Top Attacker-Target Pairs query 45  
 Top Bandwidth Hosts focused report 26  
 Top Bandwidth Hosts query 27  
 Top Bandwidth Hosts report 22  
 Top Connections Accepted by Address query 35  
 Top Connections Denied by Address query 34  
 Top Inbound Traffic by Application Protocol (Request) data monitor 52  
 Top Inbound Traffic by Application Protocol (Response) data monitor 52  
 Top Inbound Traffic by Application Protocol dashboard 48  
 Top Inbound Traffic by Host (Request) data monitor 51  
 Top Inbound Traffic by Host (Response) data monitor 52  
 Top Inbound Traffic by Host dashboard 47  
 Top List of Accessed Web Sites report 43  
 Top List of Highest Bandwidth-Consuming Conversations report 44  
 Top Outbound Traffic by Application Protocol (Request) data monitor 51  
 Top Outbound Traffic by Application Protocol (Response) data monitor 51  
 Top Outbound Traffic by Application Protocol dashboard 47  
 Top Outbound Traffic by Host (Request) data monitor 51  
 Top Outbound Traffic by Host (Response) data monitor 52  
 Top Outbound Traffic by Host dashboard 48  
 Top Protocols by Host query 42  
 Top Protocols query 45, 54  
 Top Source Ports query 45

Top Source Ports report 44  
 Top Target IPs report 44  
 Top Targets by Host query 42  
 Top Targets by Protocol query 42  
 Top Targets query 45, 56  
 Top Traffic from External to Mail Server (Request) data monitor 39  
 Top Traffic from External to Mail Server (Response) data monitor 39  
 Top Traffic from External to Web Server (Request) data monitor 39  
 Top Traffic from External to Web Server (Response) data monitor 40  
 Top Traffic from Internal to Mail Server (Request) data monitor 39  
 Top Traffic from Internal to Mail Server (Response) data monitor 39  
 Top Traffic from Internal to Web Server (Request) data monitor 39  
 Top Traffic from Internal to Web Server (Response) data monitor 39  
 Top Traffic to Mail Server dashboard 37  
 Top Traffic to Web Server dashboard 38  
 Top VPN Access by User report 30  
 Top VPN Accesses by User query 35  
 Top VPN Event Destinations query 34  
 Top VPN Event Destinations report 30  
 Top VPN Event Sources query 34  
 Top VPN Event Sources report 29  
 Top VPN Events query 35  
 Top VPN Events report 30  
 Top VPN Servers with Authentication Errors data monitor 31  
 Top VPN Servers with Denied Connections data monitor 31  
 Top VPN Servers with Successful Connections data monitor 32  
 Top VPN Users with Authentication Errors data monitor 31  
 Traffic by Transport Protocol query 45  
 Traffic by Transport Protocol report 43  
 Traffic Moving Average (ICMP) data monitor 40  
 Traffic Moving Average (SYN) data monitor 39  
 Traffic Moving Average (TCP) data monitor 39  
 Traffic Moving Average (UDP) data monitor 40  
 Traffic Moving Average dashboard 37  
 Traffic Moving Average Report report 43  
 Traffic Overview resource group 47  
 Traffic Snapshot report 49  
 Traffic Spike Rule Fired Events query 46  
 Traffic Statistics report 48  
 trends  
     Inbound Traffic by Application Protocol 58  
     Outbound Traffic by Application Protocol 58  
     Overall Traffic 28, 58  
 Two Charts Landscape report template 58  
 Two Charts One Table Landscape report template 58  
 Two Charts One Table Portrait report template 42  
 Two Charts Portrait report template 28, 58

## U

UDP Traffic filter 40, 44  
 UDP Traffic Spike rule 50

## **V**

VPN Authentication Errors filter 34  
VPN Connection Attempts query 34  
VPN Connection Attempts report 30  
VPN Connection Failures query 35  
VPN Connection Failures report 30  
VPN Connection Statistics dashboard 29

VPN Events filter 24

## **W**

Web Server asset category 39  
Weekly Traffic Summary report 48