Hewlett Packard
Enterprise

HPE Security ArcSight ESM: Anomalous Traffic Detection

Software Version: 1.0

Security Use Case Guide

June 17, 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Chapter 1: Overview

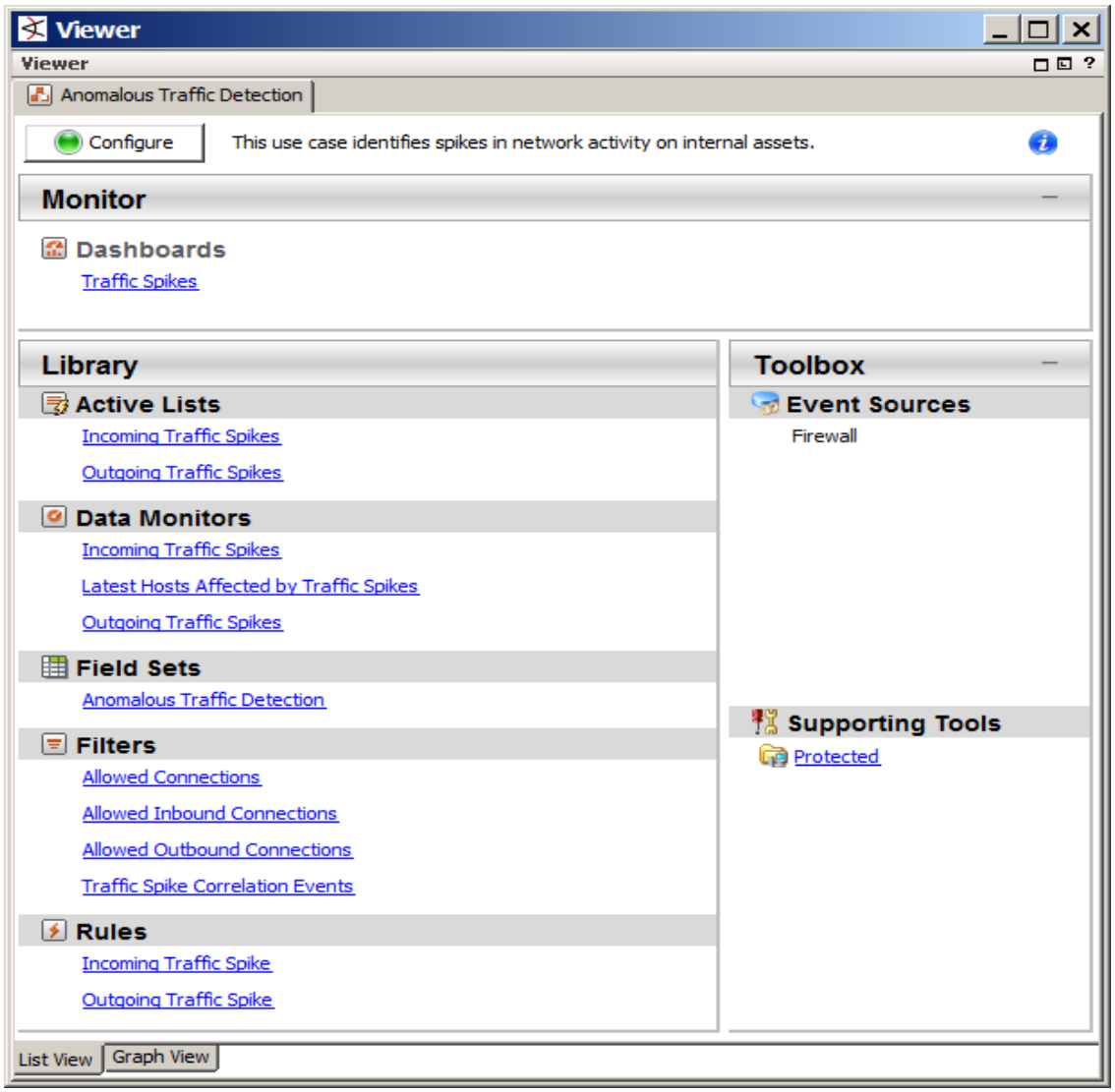
The Anomalous Traffic Detection use case helps you identify alarming or sudden spikes in network traffic so that you can detect malicious activity. Sudden spikes in traffic can be caused by scheduled backups or virus scanner updates inside your LAN, or mail server issues. However, these spikes might also be caused by something more alarming, such as malware outbreaks or hacking attempts. Using the ESM monitoring and investigation tools, you can observe these peaks in network activity, and identify and respond to threats before any damage is done.

The Anomalous Traffic Detection use case provides a dashboard for routine monitoring to see what type of abnormal activity is taking place. You can monitor sudden spikes in incoming and outgoing traffic permitted through a firewall, and investigate further to remediate potential threats.

You can access the Anomalous Traffic Detection use case from the **Use Cases** tab of the ArcSight Console Navigator panel. The Monitor section of the use case lists the dashboard used to monitor traffic. The Library section of the use case lists all supporting resources that help compile information in the dashboard and includes rules that generate correlation events when triggered.

The use case also provides a configuration wizard that guides you through some of the required configuration.

The Anomalous Traffic Detection use case is shown below.



This document describes how to install, configure, and use the Anomalous Traffic Detection use case and is designed for security professionals who have a basic understanding of ArcSightESM and are familiar with the ArcSight Console. For detailed information about using ArcSightESM, see the ArcSightESM help system from the ArcSight Console**Help** menu. Find PDFs of all ArcSight documentation on Protect 724.

Chapter 2: Installation

To install the Anomalous Traffic Detection use case, perform the following tasks in the following sequence:

1. Download the Anomalous Traffic Detection use case zip file into the ArcSight Console system where you plan to install the use case, then extract the zip file.

   The zip file includes the *Anomalous_Traffic_Detection_1.0.arb* package, the accompanying Readme file, and the *Downloads_Groups_1.0.arb* package.
2. Log into the ArcSight Console as administrator.

   Note: During the package installation process, do not use the same administrator account to start another Console or Command Center session simultaneously. This login is locked until the package installation is completed.
3. Verify if you have a previous version of the use case package you want to install. If so, uninstall and delete this previous version:
   a. On the **Packages** tab of the Navigator panel, right-click the package and select **Uninstall Package**. The package icon is gray when it is uninstalled.
   b. Right-click the package and select **Delete Package**.
4. On the Packages tab, verify if **Downloads Groups** is already installed. If you see packages in `/All Packages/Downloads/Downloads Groups`, then ignore this step.

   If the Downloads Groups package is not present, import and install the *Downloads_Groups_1.0.arb* package. See "Importing and Installing a Package" on the next page for details.
5. Import and install the Anomalous Traffic Detection use case package. See "Importing and Installing a Package" on the next page for details.
6. Assign user permissions to the Anomalous Traffic Detection resources. See "Assigning User Permissions" on page 8 for details.

Importing and Installing a Package

Follow the steps below to import and install the package(s). This assumes you have downloaded the zip file and extracted the contents into the ArcSight Console system.

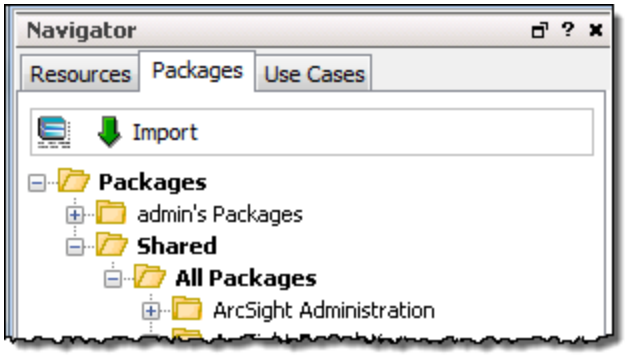
- If the ArcSight Console does not have the Downloads Groups package in `/All Packages/Downloads/Downloads Groups`, import and install the package first. Then repeat the steps to import and install the Anomalous Traffic Detection use case package.

  Note: The Downloads Groups package contains the groups used by the resources in the security use case; you must import and install this package first.

- If the Downloads Groups package is already installed, follow the steps to import and install the Anomalous Traffic Detection use case package only.

To import and install a package:

1. Log into the ArcSight Console as administrator. In the Navigator panel, click the **Packages** tab.



2. Click **Import**.
3. In the Open dialog, browse and select the package file (`*.arb`) you want to import, then click **Open**.
   The Importing Packages dialog shows how the package import is being verified for any resource conflicts.
4. In the Packages for Installation dialog, make sure that the check box is selected next to the name of the package you want to install and click **Next**.
   The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the summary report.
5. In the Installing Packages dialog, click **OK**. In the Importing Packages dialog, click **OK**.
6. On the **Packages** tab of the Navigator panel, expand the package group in `/All Packages/Downloads/` to verify that the package group is populated and that installation is successful.

Assigning User Permissions

By default, users in the `Administrators` and `Default User Groups/Analyzer Administrators` user groups can view and edit the resources. Users in the `Default User Groups` (and any custom user group under this group) can only view Anomalous Traffic Detection resources. Depending on how you set up user access controls within your organization, you might need to adjust those controls to make sure the resources are accessible to the right users.

Note: By default, the `Default User Groups/Analyzer Administrators` user group does not have edit permissions for archived reports in the Downloads group.

The following procedure assumes that you have logged into the ArcSight Console as administrator, and that you have set up the required user groups with the right users.

To assign user permissions:

1. In the Navigator panel, open the **Resources** tab.
2. For each of the resource types provided in the use case, navigate to `Downloads/Abnormal Activity Detection`.
3. Right-click the `Abnormal Activity Detection` group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
4. Select the user groups for which you want to grant permissions and click **OK**.

Chapter 3: Configuration

Before configuring the use case, make sure that you have populated your ESM network model. A network model keeps track of the network nodes participating in the event traffic. For information about populating the network model, refer to the *ArcSight Console User's Guide*.

The Abnormal Activity Detection use case requires the following configuration for your environment:

- Install the appropriate ArcSight SmartConnectors to receive relevant events. For example, to receive relevant events from Juniper firewall devices, install the SmartConnector for Juniper Firewall ScreenOS Syslog.
- Manually categorize all internal assets (assets inside the company network), or the zones to which the assets belong, with the **Protected** asset category (located in `/All Asset Categories/Site Asset Categories/Address Spaces/Protected`). 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 **Protected**.

A configuration wizard is provided to guide you through some of the required configuration. Follow the procedure below.

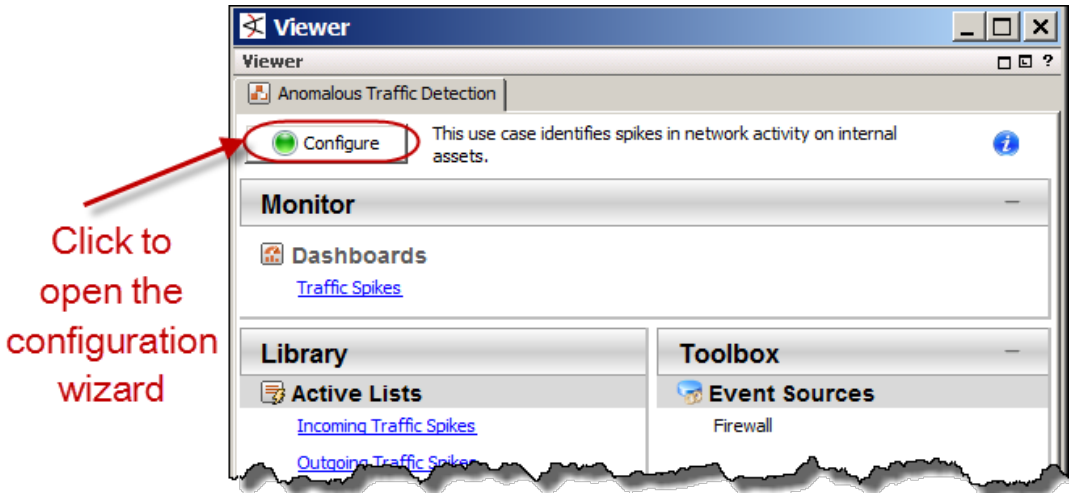
Note: You must categorize assets internal to the network manually; the procedure is not part of the configuration wizard. For information about categorizing assets, see the *ArcSight Console User's Guide*.

To configure the Abnormal Activity Detection use case:

1. In the Navigator panel, click the **Use Cases** tab.
2. Browse for the **Abnormal Activity Detection** use case located in `/All Use Cases/Downloads/Abnormal Activity Detection`.
3. Open the Abnormal Activity Detection use case: either double-click the use case or right-click the use case and select **Open Use Case**.

   The Abnormal Activity Detection use case lists all the resources you need to monitor and detect anomalous traffic.

4. Click the **Configure** button to open the configuration wizard.



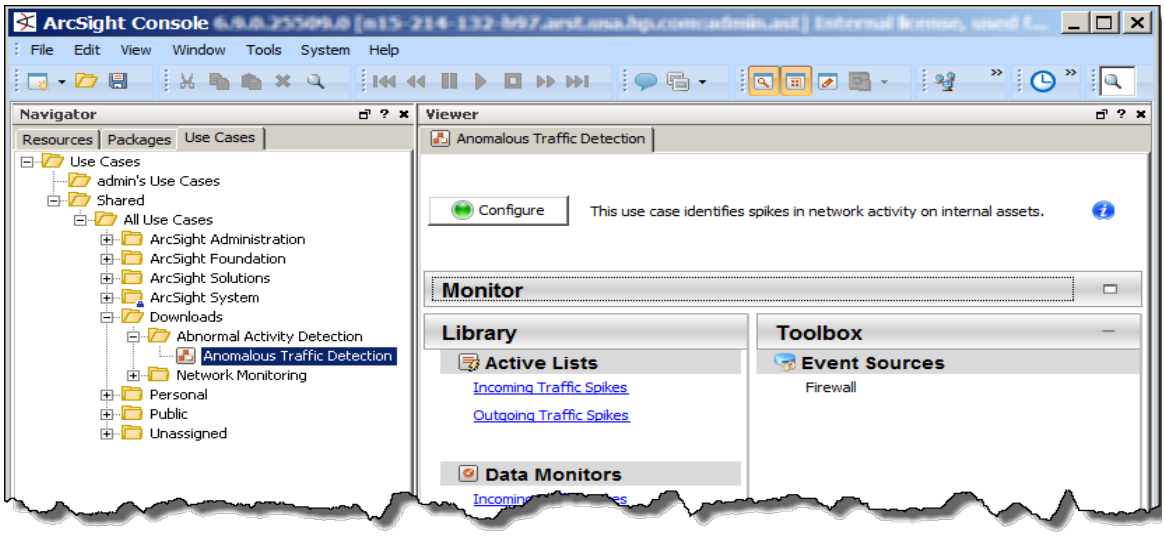
5. Click **Next** to follow the configuration steps.

After you configure the Abnormal Activity Detection use case, you are ready to detect abnormal network activity. See "Using the Anomalous Traffic Detection Use Case" on page 11.

Chapter 4: Using the Anomalous Traffic Detection Use Case

The Abnormal Activity Detection use case is located on the **Use Cases** tab in the Navigator panel under `/All Use Cases/Downloads/Abnormal Activity Detection`.

To open the Abnormal Activity Detection use case in the Viewer panel, either double-click the use case or right-click the use case and select **Open Use Case**.



The Monitor section of the Abnormal Activity Detection use case provides a dashboard that helps you detect traffic anomalies. A traffic anomaly is a pattern that indicates abnormal network activity. See "Detecting Anomalous Traffic in a Dashboard" on the next page.

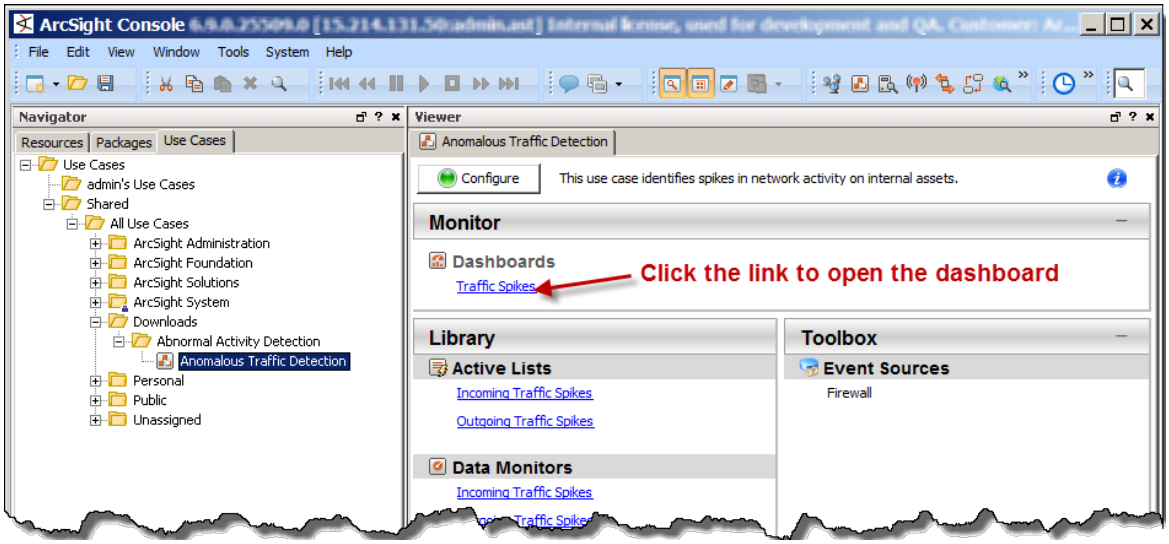
The Library section of the Abnormal Activity Detection use case lists all supporting resources that help compile information in the dashboard and includes rules that generate correlation events when triggered. The rules are described in "The Anomalous Activity Detection Rules" on page 15.

Detecting Anomalous Traffic in a Dashboard

The Abnormal Activity Detection use case provides a dashboard to help you detect abnormal network traffic in real time, so that you can investigate network events that might be malicious.

Use the dashboard to help identify unusual traffic activities, such as a flood of UDP packets or a new service appearing on the network. Traffic anomalies can be used to identify unknown attacks and DoS floods, as well as a potential intrusion or new attacks for which signatures have yet to be developed.

To open the dashboard, click the link for the dashboard in the Abnormal Activity Detection use case.



The dashboard opens in the Viewer panel of the ArcSight Console and displays three data monitors, two of which are moving average data monitors. A moving average data monitor displays the moving average of events by selected data fields. The display provides a running count of events within a specified time frame and generates an event when the moving average changes significantly.

The data monitors are described below.

- **Latest Hosts Affected by Traffic Spikes** shows the last 15 hosts that were either destinations for incoming traffic spikes or sources for outbound traffic spikes. Information about each traffic spike is displayed, such as the time the traffic spike ended, the ESM priority level, the type of traffic spike detected (such as, Incoming Traffic Spike or Outbound Traffic Spike), the source IP address and zone name for outbound traffic spikes, the destination IP address and zone name for incoming traffic spikes, and the customer name (such as the MSSP customer or company business unit).

  Investigate traffic spikes with an ESM priority rating of 7 or higher as this might indicate a potential problem. For details about the ESM priority rating and how it is calculated, see the *ArcSight Console User's Guide*.
- **Incoming Traffic Spikes** tracks the moving average volume of inbound traffic permitted through a

firewall device (the number of connections allowed by a firewall from the outside to an internal asset). If the moving average of connections to an internal host from the outside increases by 150 percent or more, an alert is raised (a correlation event triggers).

Look closely at any sudden peak in incoming traffic. If your volume of inbound traffic suddenly spikes upward, someone might be starting a DOS or DDoS attack. Most DDoS attacks begin with a sharp spike in traffic; it is important to be able to tell the difference between a sudden surge of legitimate visitors and the start of a DDoS attack.

If you see a sudden spike of activity to a particular host or to multiple IP addresses on your network, investigate to make sure an attack is not under way. For example, attackers use automated port scanning tools to perform reconnaissance on your network; attempting to connect to every port on a single machine or to multiple IP addresses on a network to determine which services are allowed and responding.

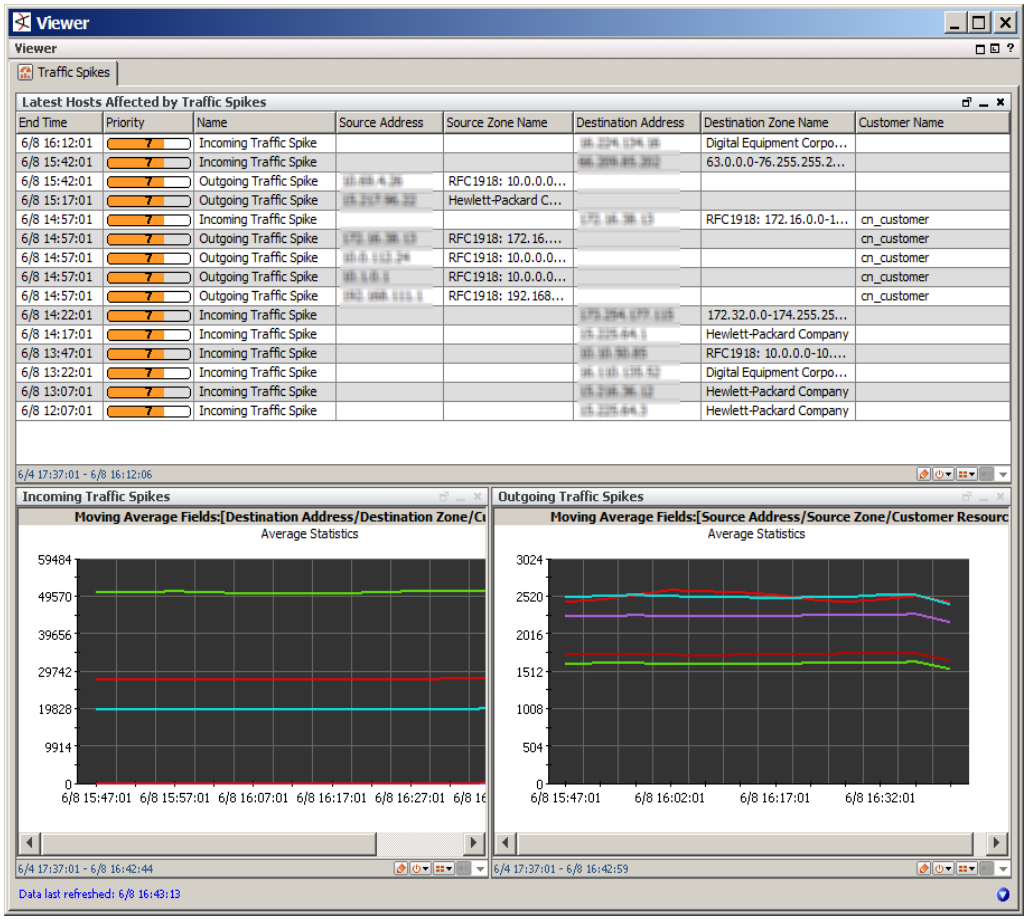
- **Outgoing Traffic Spikes** tracks the moving average volume of outbound traffic permitted through a firewall device (the number of connections allowed by a firewall from an internal asset to the outside world). If the moving average of outbound events allowed by a firewall changes by 150 percent or more, an alert is raised (a correlation event triggers).

  Investigate any sudden peak in outbound traffic as this might indicate that a compromised system on your network is being used as part of a DDoS attack. Modern malware often *calls home* and a sudden increase in outbound traffic might indicate such activity, which requires further research. A sudden spike in outbound traffic can also indicate data exfiltration; someone might be sending large volumes of sensitive data from an internal system to an system outside your network.

Note: If the alerts are too frequent and raise too many false positives, increase the threshold in the data monitor to a higher percentage.

Note: Only devices with significant traffic appear in these data monitors. You can change the **Group Discard Threshold** setting of the data monitors to specify the minimum event counts needed to generate a threshold exceeded event.

An example dashboard is shown below.



Investigating Further

Right-click on an item in a data monitor and select **Investigate > Create Channel** to open an active channel and investigate events further. For example, right-click on an IP address in the **Outgoing Traffic Spikes** data monitor and select **Investigate > Create Channel [Source Address = *IP address]*** to open an active channel and see more details about the event. In the active channel, you can also:

- Create an inline filter to focus on events of interest; for example, you can select an IP address on which to filter and focus your attention. For detailed information about using inline filters, see the *ArcSight Console User's Guide*.
- Double-click on an event in the active channel to open the event inspector and see details about the event. The Details tab of the Event Inspector provides external links to reference pages and vulnerability information (if available) that discuss a vulnerability in more detail.

The Anomalous Activity Detection Rules

The Anomalous Activity Detection use case provides the rules described below. The rules are deployed in the `Real-time Rules` group on the Resources tab of the Navigator panel (`/All Rules/Real-time Rules/Downloads/Abnormal Activity Detection/Anomalous Traffic Detection`) and enabled by default. The rules trigger when events match one or more set of conditions, at which point a correlation event is generated. A correlation event is displayed in an active channel with the flash icon  . Correlation events are fed back into the event life cycle at the ArcSight Manager and are evaluated by both the ArcSight Manager and by the correlation processes. For more information about rule triggering and correlation events, see the *ArcSight Console User's Guide*.

It is very important to investigate and set a proper incident handling procedure to follow up on events generated by these rules.

- The **Incoming Traffic Spike** rule triggers when the moving average of connections to an internal host from the outside increases by 150 percent or more. When triggered, the rule adds the destination address, zone, and customer resource to the **Incoming Traffic Spikes** active list.
- The **Outgoing Traffic Spike** rule triggers when the moving average of outbound events allowed by a firewall changes by 150 percent or more. When triggered, the rule adds the source address, zone, and customer resource to the **Outgoing Traffic Spikes** active list.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Security Use Case Guide (ESM: Anomalous Traffic Detection 1.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!