Hewlett Packard
Enterprise

HPE Security ArcSight ESM: Suspicious Outbound Traffic

Software Version: 1.0

Security Use Case Guide

April 3, 2017

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.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Chapter 1: Overview

Watching activity within the network and looking for suspicious traffic leaving your perimeter is essential so that you can spot attacker activity on systems more quickly and prevent an eventual security breach from occurring. For example, systems that are compromised often *call home* to command-and-control servers; it is important to see this type of traffic before any real damage is done.

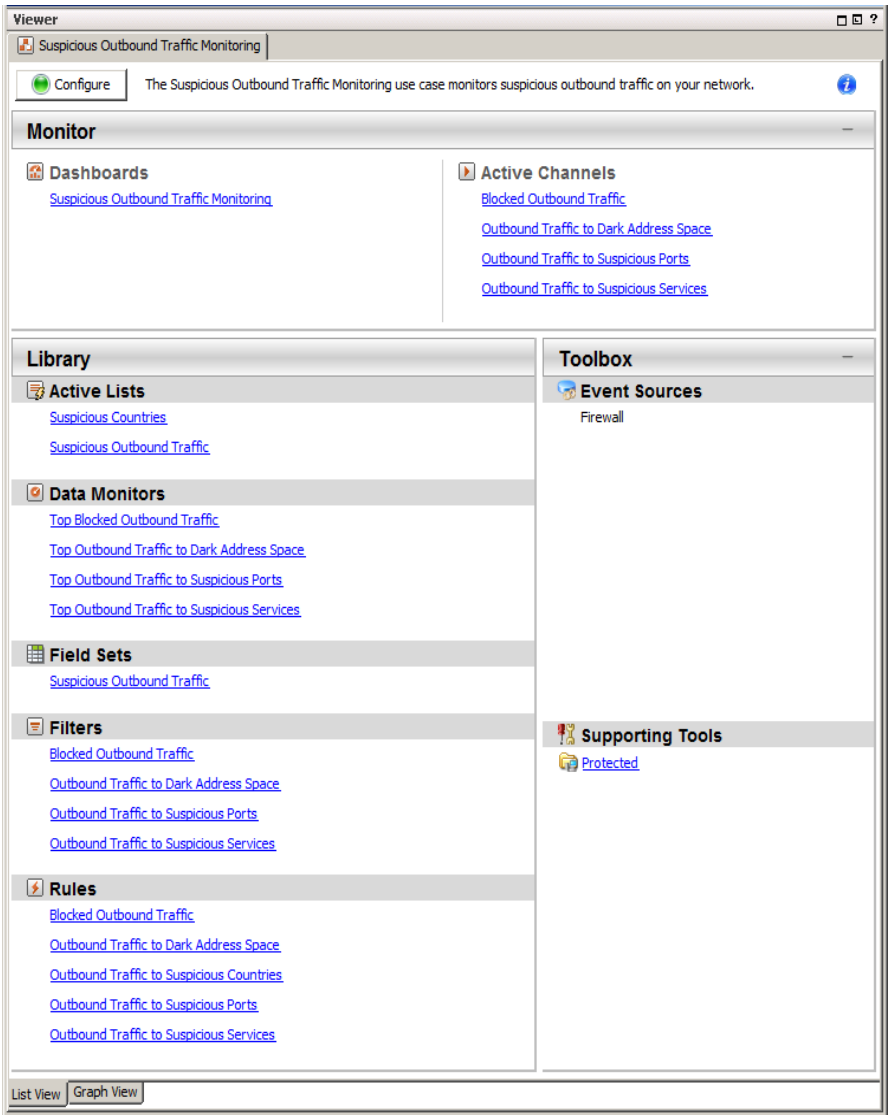
Use the resources in this use case for incident investigation as well as routine monitoring to track unusual outbound traffic patterns. Suspicious outbound traffic might indicate that internal servers are compromised by external attackers, that some one is attempting to access restricted sites with illegal material, or sending proprietary data outside the company.

- A **dashboard** is provided to help you monitor in real time the greatest number of events with blocked outbound traffic, and traffic to the dark address space, suspicious services, or suspicious ports. Traffic to the dark address space is especially important as these subnets are currently unused with no active servers or services; nobody should be trying to access them.
- Several **active channels** are provided so that you can investigate all events received within the last ten minutes with unusual outbound traffic patterns. Use these active channels to see details about events of interest, such as traffic to an IP address in the dark address space, to services that are not permitted in your network, and blocked ports that are not commonly used.

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

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

The Suspicious Outbound Traffic Monitoring use case is shown below.



This document describes how to install, configure, and use the Suspicious Outbound Traffic Monitoring use case and is designed for security professionals who have a basic understanding of ArcSight ESM and are familiar with the ArcSight Console. For detailed information about using ArcSight ESM, 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 Suspicious Outbound Traffic Monitoring use case, perform the following tasks in the following sequence:

1. Download the Suspicious Outbound Traffic Monitoring use case zip file into the ArcSight Console system where you plan to install the use case, then extract the zip file.
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 Suspicious Outbound Traffic Monitoring use case package. See "Importing and Installing a Package" on the next page for details.
6. Assign user permissions to the Suspicious Outbound Traffic Monitoring 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.

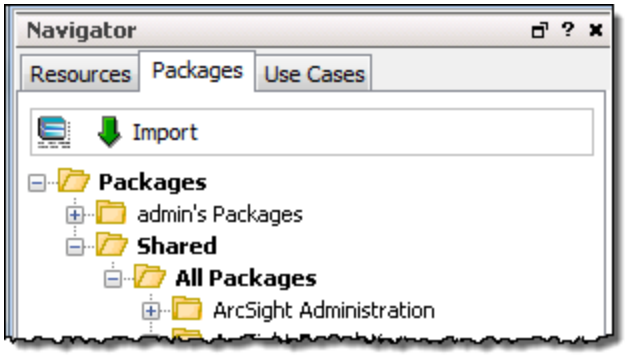
- If the ArcSight Console does not have the Downloads Groups package in `/All Packages/Downloads/Downloads Groups`, import and install the package first. Then repeat the steps to import and install the **Suspicious Outbound Traffic Monitoring** use case package.

  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 **Suspicious Outbound Traffic Monitoring** 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 Suspicious Outbound Traffic Monitoring 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/Suspicious Outbound Traffic Monitoring`.
3. Right-click the `Suspicious Outbound Traffic Monitoring` 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 Suspicious Outbound Traffic Monitoring 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**.
- Add the two-letter code for each country with which you do not do business or communicate, to the **Suspicious Countries** active list. The **Suspicious Countries** active list is used by the Outbound Traffic to Suspicious Countries rule.

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

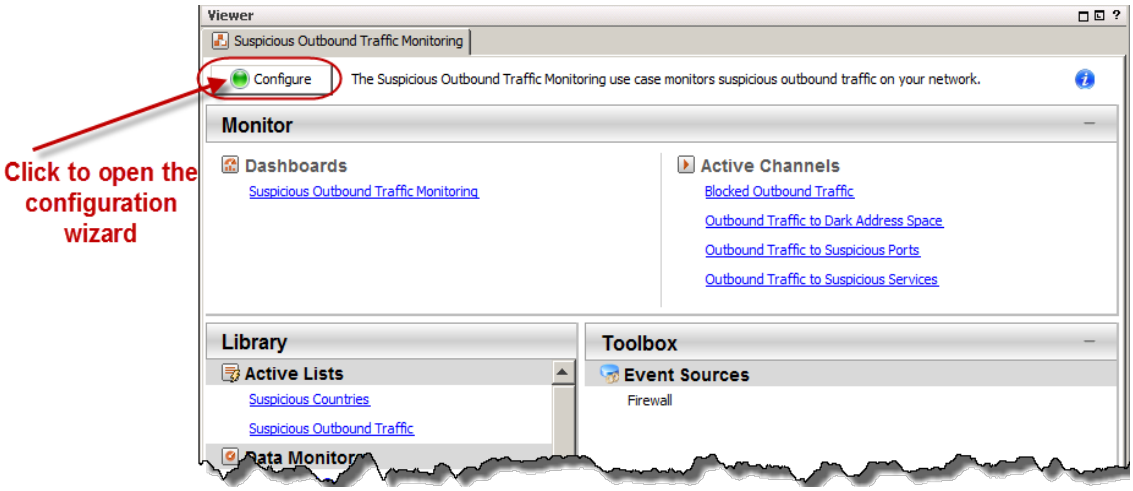
Note: You must add countries to the **Suspicious Countries** active list manually; the procedure is not part of the configuration wizard. See page 10.

To run the Suspicious Outbound Traffic Monitoring configuration wizard:

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

   The Suspicious Outbound Traffic Monitoring use case lists all the resources you need to monitor suspicious outbound traffic.

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



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

To add countries to the Suspicious Countries active list:

1. In the **Suspicious Outbound Traffic Monitoring** use case, click the link for the **Suspicious Countries** active list.
2. Click the button to open the Active List Entry Editor.
3. Enter the two-letter code for the country you want to add to the list and click **Add**. The country name is optional. The International Organization for Standardization supplies a list of the two-letter codes for all countries (ISO 3166).

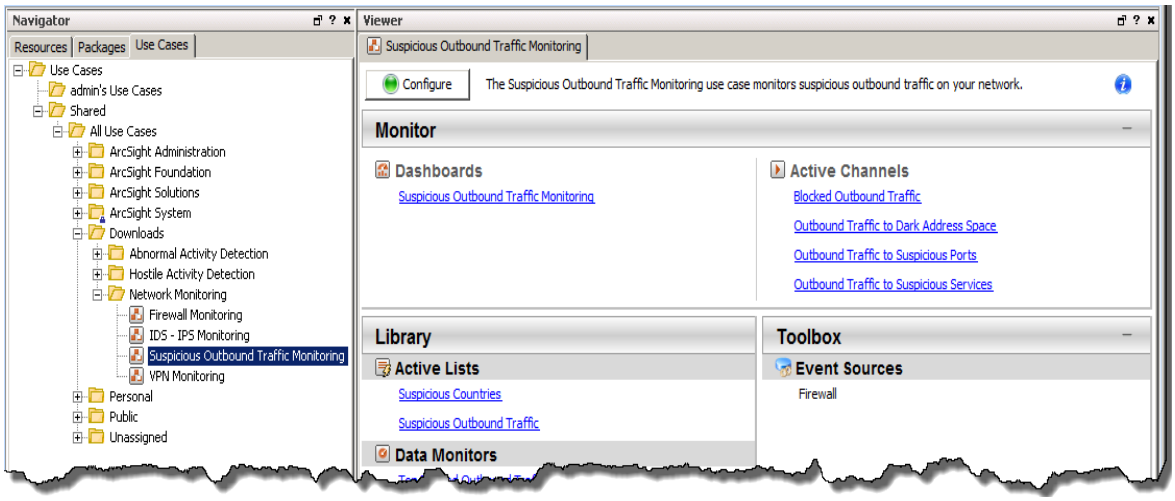
   Alternatively, you can import a csv file that contains the two-letter country codes into the active list. See the *ArcSight Console User's Guide* for information about importing csv files.

After you configure the Suspicious Outbound Traffic Monitoring use case, you are ready to monitor suspicious activity. See "Using the Suspicious Outbound Traffic Use Case" on page 11.

Chapter 4: Using the Suspicious Outbound Traffic Use Case

The Suspicious Outbound Traffic Monitoring use case is located on the **Use Cases** tab in the Navigator panel under `/All Use Cases/Downloads/Suspicious Outbound Traffic Monitoring`.

To open the Suspicious Outbound Traffic Monitoring 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 Suspicious Outbound Traffic Monitoring use case provides resources to help you monitor and investigate abnormal traffic leaving your network:

- Use the dashboards to monitor the top ten events with suspicious traffic. See "Monitoring Suspicious Outbound Traffic in a Dashboard" on the next page.
- Use the active channels to investigate events with suspicious traffic. See "Investigating Suspicious Outbound Traffic in Active Channels" on page 14.

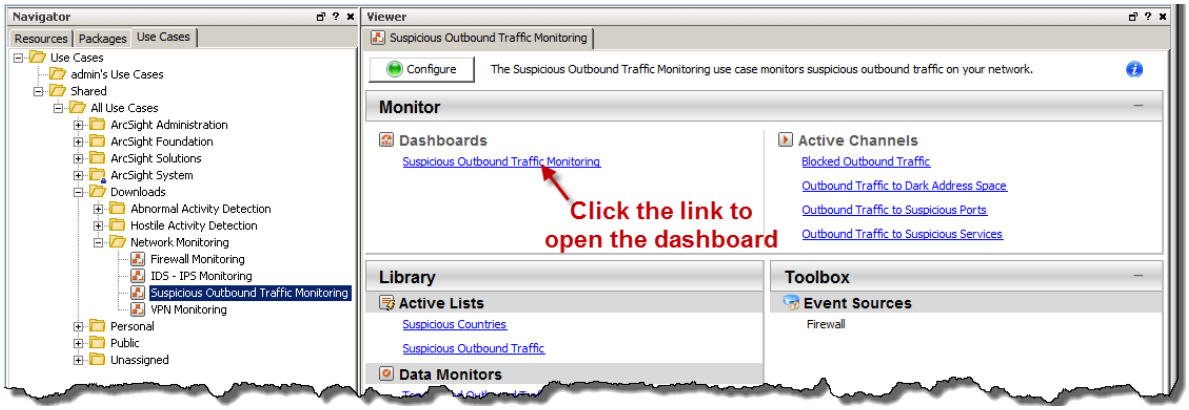
The Library section of the Suspicious Outbound Traffic Monitoring use case lists all supporting resources that help compile information in the dashboard and active channels, and includes rules that generate correlation events when triggered. The rules are described in "Suspicious Outbound Traffic Monitoring Rules" on page 17.

Monitoring Suspicious Outbound Traffic in a Dashboard

The Suspicious Outbound Traffic Monitoring use case provides a dashboard to help you monitor in real time all events with blocked outbound traffic, traffic to suspicious services, traffic to the dark address space, and traffic to suspicious ports.

Use the dashboard to help identify unusual traffic patterns leaving the network.

To open the dashboard, click the link for the **Suspicious Outbound Traffic Monitoring** dashboard in the Suspicious Outbound Traffic Monitoring use case.



The dashboard opens in the Viewer panel of the ArcSight Console and displays several data monitors:

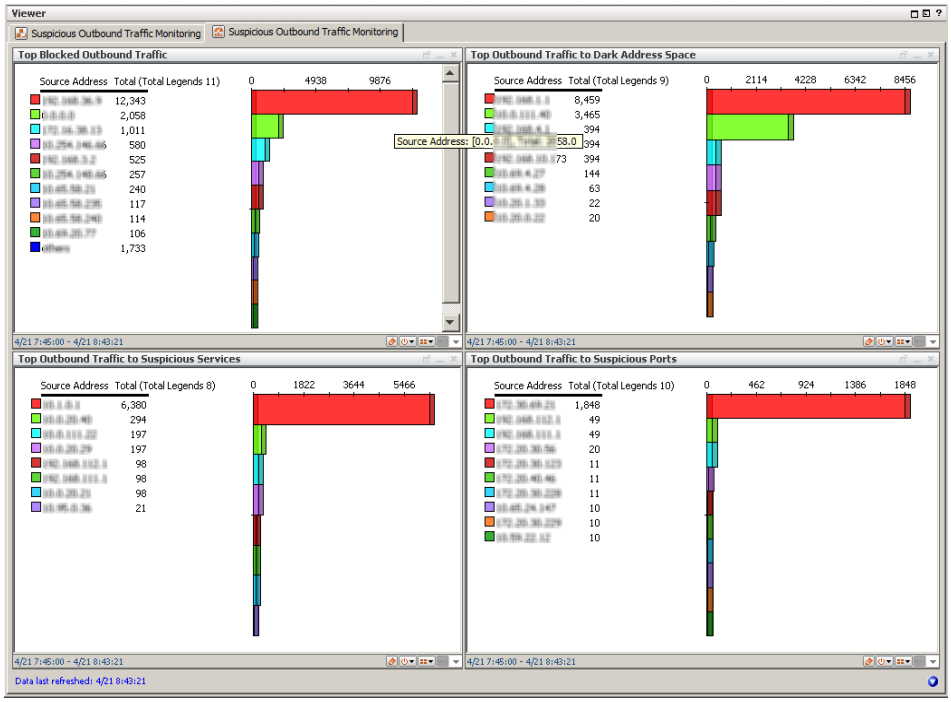
- **Top Blocked Outbound Traffic** displays the top ten sources (by IP address) with the greatest number of blocked outbound traffic events. For example, outbound traffic can be blocked by a firewall when a host in your network is trying to access a restricted service or when traffic is leaving your network to a country with which your company does not do business. Investigate any host with a high number of blocked outbound traffic events. This might indicate that data exfiltration is being attempted or that malware is sending data to a location that an attacker controls. Data exfiltration might be unintentional, but monitoring such traffic can prevent serious security breaches from happening.
- **Top Outbound Traffic to Dark Address Space** displays the top ten sources (by IP address) with the greatest number of events with outbound traffic to the dark address space; the area of the Internet's routable address space that is currently unused, with no active servers or services. An excessive number of events to the dark address space from a particular source might indicate malware is sending data to a location that an attacker controls or that attempts are being made to access restricted sites with illegal material. Investigate this type of abnormal traffic immediately.
- **Top Outbound Traffic to Suspicious Ports** displays the top ten sources (by IP address) with the greatest number of outbound traffic events to destination ports greater than 1024. Attackers often

take advantage of obscure ports to circumvent less complex web filtering procedures. If an application is using an unusual port, it might indicate that command-and-control traffic is masquerading as normal application behavior.

- **Top Outbound Traffic to Suspicious Services** displays the top ten sources (by IP address) with the greatest number of outbound traffic events to ftp, ssh, telnet, and rdp services. There are few legitimate reasons to connect to these services outside the corporate network. Observe this traffic to determine if this traffic is authorized.

  Note: ftp, ssh, telnet, and rdp are the default suspicious services; to change the default services, edit the **Destination Port** condition in the **Outbound Traffic to Suspicious Services** filter.

An example **Suspicious Outbound Traffic Monitoring** 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 a source IP address in the **Top Outbound Traffic to Suspicious Ports** data monitor and select **Investigate > Create Channel [Source Address = *IP address]*** to open an active channel and see more details about the event, such as the destination IP address and the geographical country name. 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

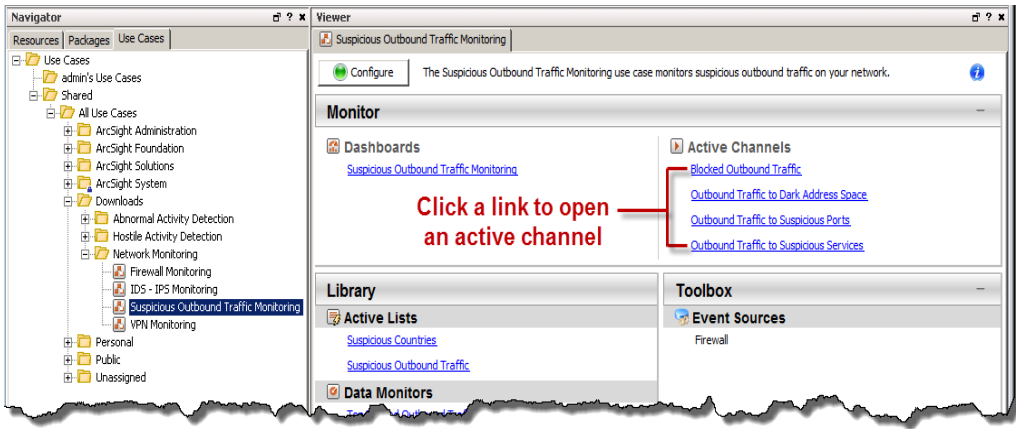
event. The Details tab of the Event Inspector provides external links to reference pages and vulnerability information that discuss a vulnerability in more detail.

Investigating Suspicious Outbound Traffic in Active Channels

The Suspicious Outbound Traffic Monitoring active channels show all events received within the last ten minutes with suspicious outbound traffic: blocked outbound traffic, traffic to suspicious services, traffic to the dark address space, and traffic to suspicious ports.

Understanding suspicious outbound activity on your network is essential to the security of your environment and can help you prevent malicious activity and mitigate significant security risks.

To open an active channel, click the link for the active channel in the Suspicious Outbound Traffic Monitoring use case.



The active channel opens in the Viewer panel and displays events received within the last ten minutes.

Note: The events displayed in an active channel do not refresh automatically at ten-minute intervals. To refresh the view, click the **Stop** and **Replay** channel controls in the toolbar.

Depending on your environment, ESM load, and specific investigation needs, you can configure an active channel to use continuous, automatic channel refresh: Right-click the link for the active channel in the use case and select **Edit Active Channel**. From the Time Parameters drop-down on the Attributes tab of the Inspect/Edit panel, select **Continuously evaluate**.

Note: In a high EPS environment, you might see performance issues if you scroll down to try and view all the events in the active channel.

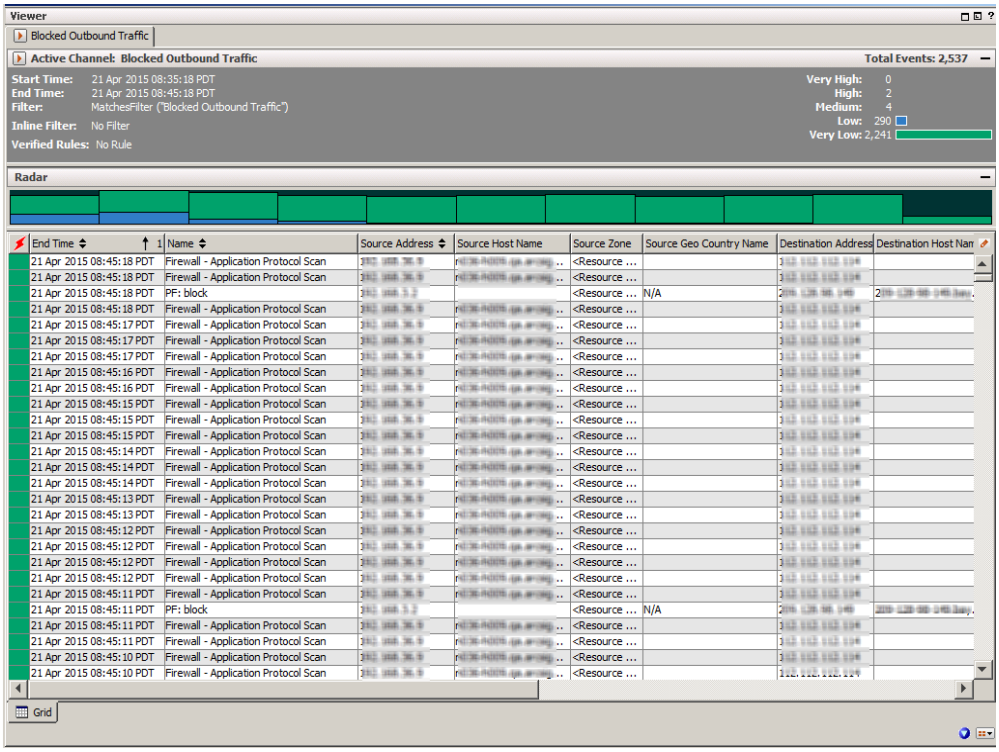
The Suspicious Outbound Traffic Monitoring use case provides these active channels:

- The **Blocked Outbound Traffic** active channel displays all events with unusual traffic patterns or traffic that did not meet the corporate firewall policy that were blocked from leaving the network. For each event, you can see the source IP address, hostname, and geographical country name, the destination IP address, hostname, port, and geographical country name, and the application protocol. The product and vendor of the device sending the event is also shown. Investigate an excessive number of events with blocked outbound traffic going to the same destination from multiple hosts, as this might indicate that the hosts in your network are infected by malware.
- The **Outbound Traffic to Dark Address Space** active channel displays all events with traffic going to the dark address space (the area of the Internet's routable address space that is currently unused, with no active servers or services). For each event, you can see the source IP address, hostname, and geographical country name, the destination IP address, hostname, port, and geographical country name, and the application protocol. The product and vendor of the device sending the event is also shown. Investigate this type of abnormal traffic immediately. An excessive number of events to the dark address space from a particular source might indicate that malware is sending data to a location that an attacker controls or that attempts are being made to access restricted sites with illegal material.
- The **Outbound Traffic to Suspicious Ports** active channel displays all events with outbound traffic to ports greater than 1024. For each event, you can see the source IP address, hostname, and geographical country name, the destination IP address, hostname, port, and geographical country name, and the application protocol. The product and vendor of the device sending the event is also shown. Examine these events to determine if suspicious activity might be taking place, such as some one sending proprietary data outside the company or downloading malware.
- The **Outbound Traffic to Suspicious Services** active channel displays all events with outbound traffic to ftp, ssh, telnet, and rdp services. For each event, you can see the source IP address, hostname, and geographical country name, the destination IP address, hostname, port, and geographical country name, and the application protocol. The product and vendor of the device sending the event is also shown. Examine these events to see abnormal patterns, such as excessive internet activity that does not seem consistent with traffic generated by any legitimate processes that you have running.

  Note: ftp, ssh, telnet, and rdp are the default suspicious services; to change the default services, edit the **Destination Port** condition in the **Outbound Traffic to Suspicious Services** filter.

Use these active channels as a base line for your investigation. Right-click an item (such as IP address) and select **Show Event Details** to see detailed information about the event. You can also create an inline filter to display events from a specific item. See the *ArcSight Console User's Guide*'s topic on using active channels for information about menu options and inline filters.

An example active channel is shown below.


Viewer
Blocked Outbound Traffic
Active Channel: Blocked Outbound Traffic
Total Events: 2,537
Start Time: 21 Apr 2015 08:35:18 PDT
End Time: 21 Apr 2015 08:45:18 PDT
Filter: MatchesFilter ("Blocked Outbound Traffic")
Inline Filter: No Filter
Verified Rules: No Rule
Very High: 0
High: 2
Medium: 4
Low: 290
Very Low: 2,241
Radar
End Time
Name
Source Address
Source Host Name
Source Zone
Source Geo Country Name
Destination Address
Destination Host Nam
Grid

Suspicious Outbound Traffic Monitoring Rules

The Suspicious Outbound Traffic Monitoring 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/Network Monitoring/Suspicious Outbound Traffic Monitoring`) 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 **Blocked Outbound Traffic** rule triggers when blocked outbound traffic is detected. This activity might indicate that internal servers or workstations are compromised by external attackers.
- The **Outbound Traffic to Suspicious Countries** rule triggers when outbound traffic is detected to the suspicious countries defined in the **Suspicious Countries** active list.

  Note: The **Suspicious Countries** active list is empty by default. Add the two-letter code to this active list for each country with which you do not do business or communicate. See "Configuration" on page 9.

- The **Outbound Traffic to Suspicious Ports** rule triggers when outbound traffic to destination ports greater than 1024 is detected.
- The **Outbound Traffic to Suspicious Services** rule triggers when outbound traffic to ftp, ssh, telnet, and rdp services is detected. These are the default suspicious services; to change the default services, edit the **Destination Port** condition in the rule.
- The **Outbound Traffic to Dark Address Space** rule triggers when outbound traffic to the dark address space is detected.

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: Suspicious Outbound Traffic Monitoring 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!