Hewlett Packard
Enterprise

HPE Security ArcSight ESM: Firewall Monitoring

Software Version: 1.1

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

When used to enforce a security policy that is clearly and properly defined, firewalls can help to prevent most network attacks. However, while many firewalls can provide adequate access control, threats exist and hackers continually come up with sophisticated attacks designed to find a way around the common access-control policies enforced by perimeter firewalls.

The Firewall Monitoring use case helps you observe your firewall devices to monitor configuration and to obtain a situational awareness of the traffic coming from and going to your protected network. Using the ESM monitoring and investigation tools, you can examine network traffic going through your firewall, and identify and respond to threats, such as hackers attempting to gain access to back-end information databases or install Trojan horse software, before damage is done.

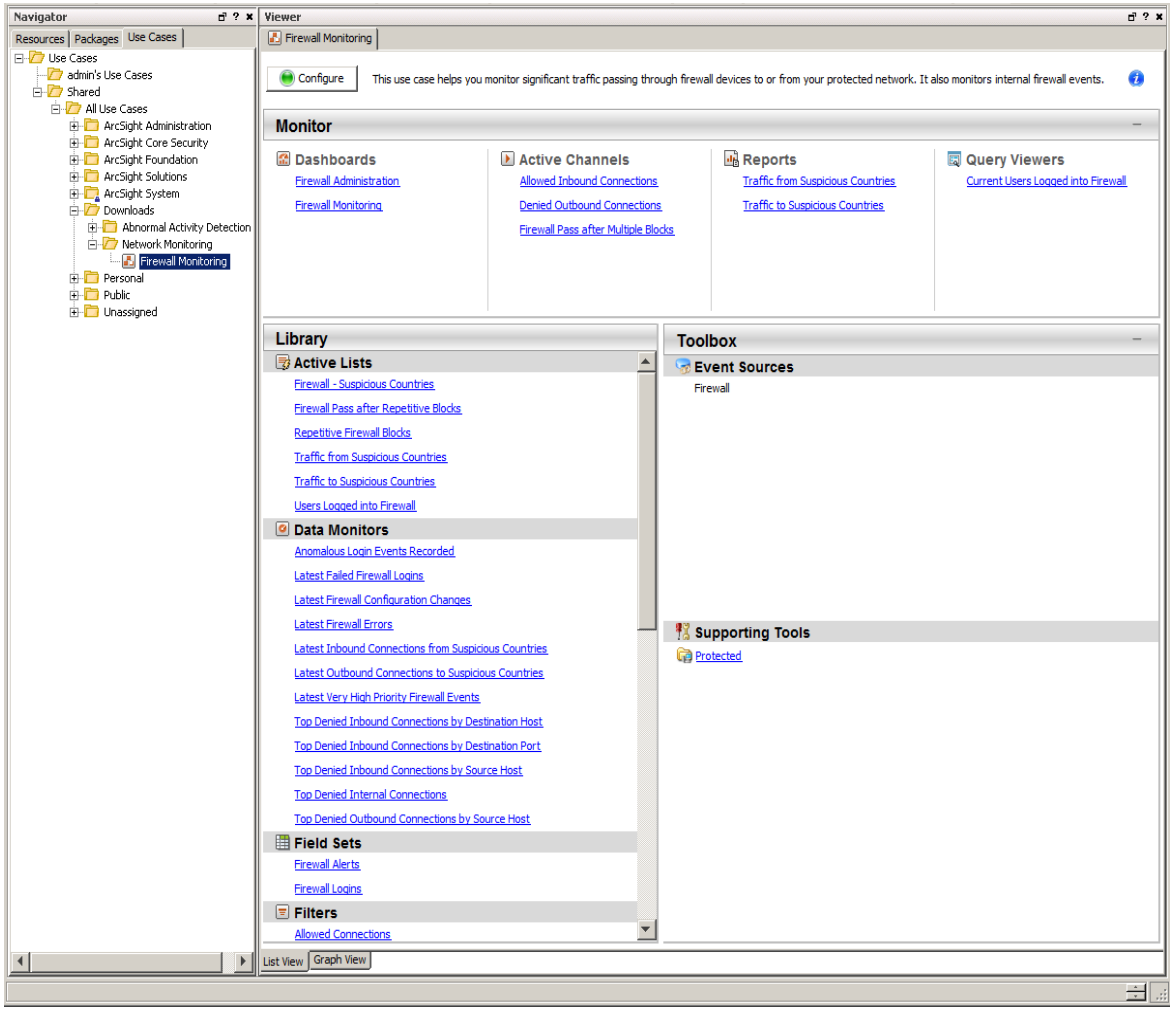
Use the resources in this use case for incident investigation, as well as routine monitoring, to see what type of firewall activity is being detected.

- Two **dashboards** are provided to help you monitor inbound and outbound traffic blocked by a firewall, traffic to and from suspicious countries, as well as real time device configuration updates and login activity.
- Three **active channels** are provided so that you can investigate allowed inbound and denied outbound connections through your firewall, and successful connections after multiple firewall blocks.
- Two **reports** provide historical information about traffic to and from suspicious countries.

You can access the Firewall Monitoring use case from the **Use Cases** tab of the ArcSight Console Navigator panel. The Monitor section of the use case lists the dashboards, active channels, and reports 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, active channels, and reports and includes rules, some of which generate correlation events when triggered.

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

The Firewall Monitoring use case is shown below.



This document describes how to install, configure, and use the Firewall 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 ArcSight ESM help system from the ArcSight Console **Help** menu. Find PDFs of all ArcSight documentation on Protect 724.

Chapter 2: Installation

To install the Firewall Monitoring use case, perform the following tasks in the following sequence:

1. Download the Firewall Monitoring 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 *Firewall_Monitoring_1.1.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 Firewall Monitoring use case package. See "Importing and Installing a Package" on the next page for details.
6. Assign user permissions to the Firewall 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.

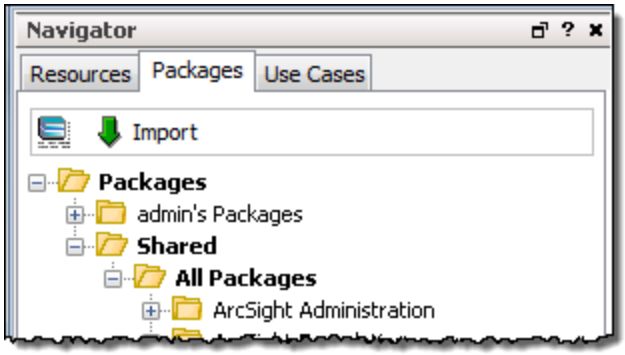
- If the ArcSight Console does not have the Downloads Groups package in `/All Packages/Downloads/Downloads Groups`, import and install the package first. Then repeat the steps to import and install the **Firewall Monitoring** use case package.

  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 Firewall 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 Firewall 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/Firewall Monitoring`.
3. Right-click the `Firewall 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 Firewall Monitoring use case requires the following configuration for your environment:

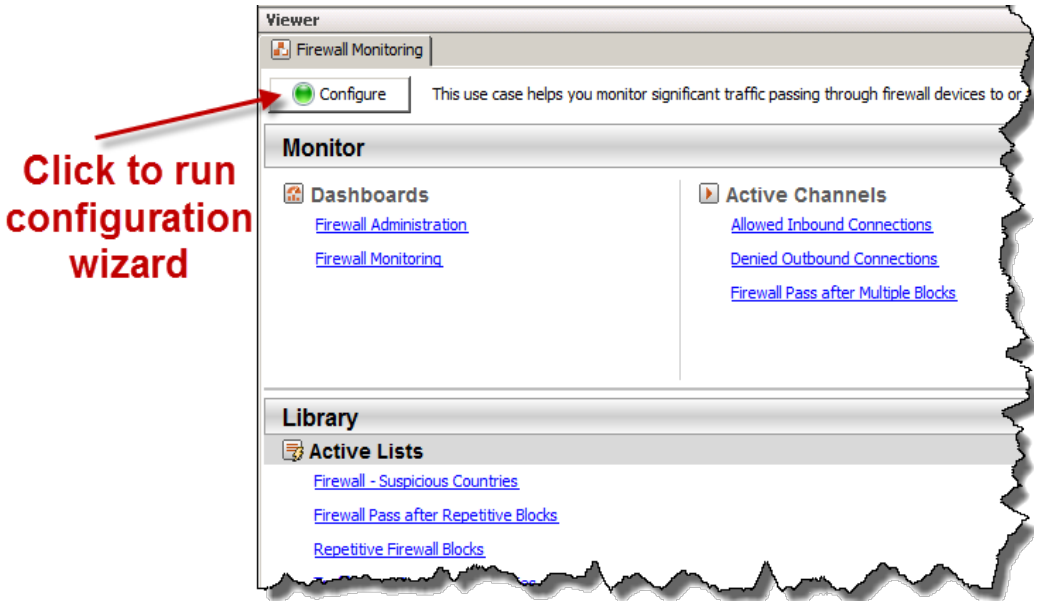
- Install the appropriate ArcSight SmartConnectors to receive relevant events. For example, to receive relevant events from Juniper firewall devices, install the SmartConnector for Juniper Firewall ScreenOS Syslog.
- Manually categorize all internal assets (assets inside the company network), or the 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**.
- Edit the **Firewall - Suspicious Countries** active list, which is pre-populated with certain countries identified by the U.S. Department of State Directorate of Defense Trade Controls (DDTC) on this web page: `http://www.pmddtc.state.gov/embargoed_countries/`
  This active list is used by the **Traffic to Suspicious Countries** and the **Traffic from Suspicious Countries** rules, as well as both the **Latest Inbound Connections from Suspicious Countries** and the **Latest Outbound Connections to Suspicious Countries** data monitors.

A configuration wizard is provided to guide you through some of the configuration.

Note: You must categorize assets internal to the network and edit the **Firewall - Suspicious Countries** active list manually; the procedures are not part of the configuration wizard. For information about categorizing assets, see the *ArcSight Console User's Guide*. To edit the active list, see page 11.

To run the Firewall Monitoring configuration wizard:

1. In the Navigator panel, click the **Use Cases** tab.
2. Browse for the **Firewall Monitoring** use case located in `/All Use Cases/Downloads/Network Monitoring`.
3. Open the Firewall Monitoring use case: either double-click the use case or right-click the use case and select **Open Use Case**. The Firewall Monitoring use case lists all the resources used for monitoring firewalls.
4. Click the **Configure** button to open the configuration wizard.



5. Click **Next** to follow the configuration steps until configuration is complete.

To edit the Firewall - Suspicious Countries active list:

1. In the **Firewall Monitoring** use case, click the link for the **Firewall - Suspicious Countries** active list. The Firewall - Suspicious Countries Details tab opens in the Viewer panel.
2. To add a country:
   a. Click the **Add Entry** button ( ) to open the Active List Entry Editor in the Inspect/Edit panel.
   b. Enter the two-letter code for the country you want to add 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).

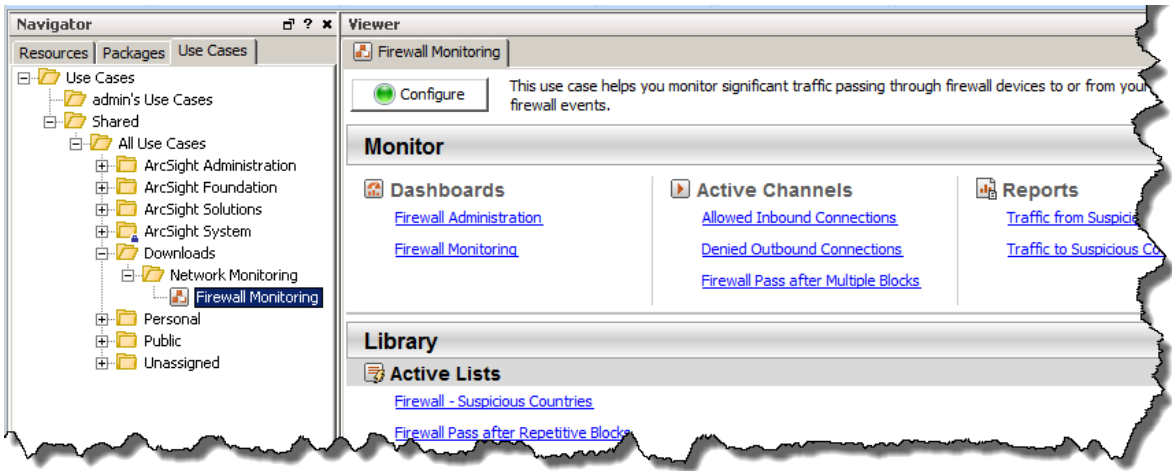
      Alternatively, you can import a csv file with a list of two-letter country codes into the active list; see the *ArcSight Console User's Guide*.
3. To delete an entry:
   a. In the **Firewall - Suspicious Countries** active list, double-click the entry you want to delete. The Active List Entry Editor opens in the Inspect/Edit panel.
   b. At the bottom of the Active List Entry Editor, click the **Delete** button.
   c. When prompted, confirm the deletion.

You are now ready to monitor your firewall devices. See "Using the Firewall Monitoring Use Case" on page 12.

Chapter 4: Using the Firewall Monitoring Use Case

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

To open the Firewall 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 Firewall Monitoring use case provides resources to help you monitor and investigate firewall traffic, and run reports:

- Use the dashboards to monitor blocked traffic, traffic to and from suspicious countries, as well as firewall device configuration updates and login activity. See "Monitoring Firewall Activity in Dashboards" on the next page.
- Use the active channels to investigate allowed inbound and denied outbound connections through your firewall, as well as source IP addresses that had successful connections after multiple firewall blocks. See "Investigating Inbound and Outbound Connections in Active Channels" on page 19.
- Run reports that show traffic to and from suspicious countries. See "Running Reports" on page 22.

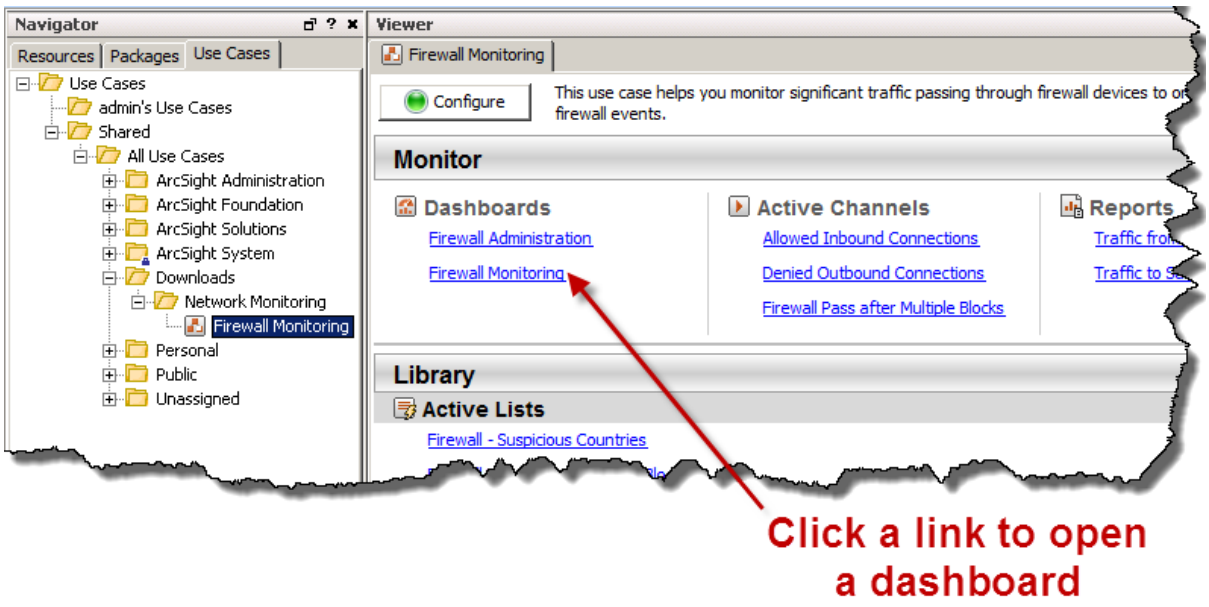
The Library section of the Firewall Monitoring use case lists all supporting resources that help compile information in the dashboards, active channels, and reports and includes rules, some of which generate correlation events when triggered. The rules are described in "Firewall Monitoring Rules" on page 24.

Monitoring Firewall Activity in Dashboards

The Firewall Monitoring use case provides two dashboards to help you monitor traffic blocked by your firewall and traffic to and from suspicious countries, as well as monitor firewall device configuration updates and login activity.

Use these dashboards to help identify suspicious inbound and outbound connections, and their corresponding hosts. You can see which assets and which ports are being targeted inside your network, as well as identify internal assets blocked from accessing hosts outside your firewall.

To open a dashboard, click the link for the dashboard in the Firewall Monitoring use case.

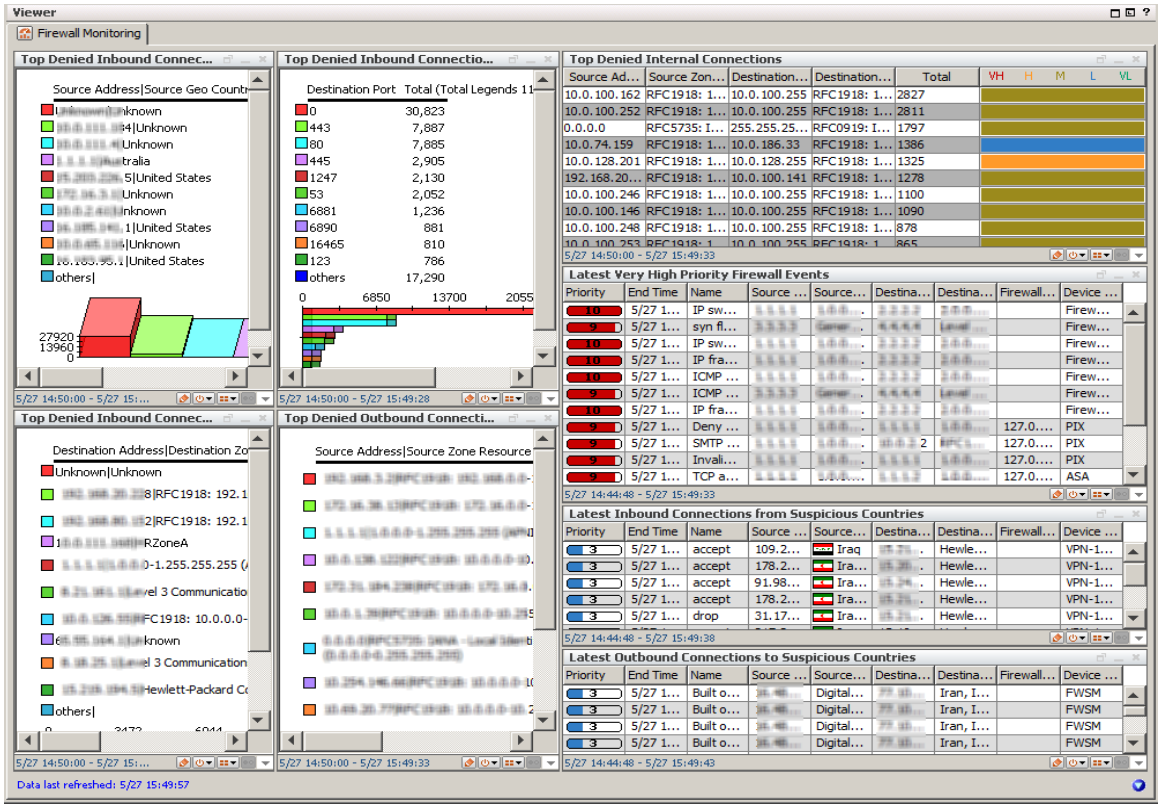


The dashboard opens in the Viewer panel of the ArcSight Console.

The following section describes the **Firewall Monitoring** dashboard and the **Firewall Administration** dashboard.

Firewall Monitoring Dashboard

An example dashboard is shown below.



The **Firewall Monitoring** dashboard provides the following data monitors.

- **Top Denied Inbound Connections by Source Host** displays the top ten inbound connections blocked by a firewall within the last hour of activity, by source IP address and country name. Monitor the source of inbound connections to see if some one from the outside is trying to gain unauthorized access to your protected network through your firewall device.

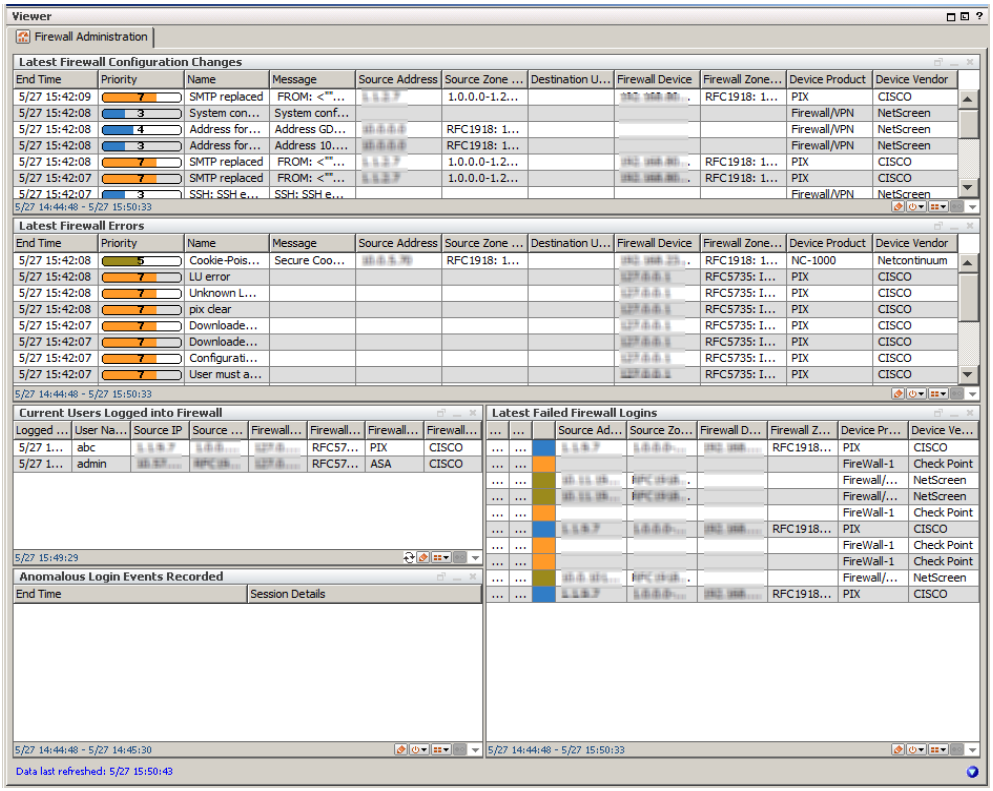
  Note: Make sure to set up locations in your network model for internal IP addresses; otherwise, the country name shows Unknown.

- **Top Denied Inbound Connections by Destination Host** displays the top ten inbound connections blocked by a firewall within the last hour of activity, by destination address and zone name. Track such activity to see if some one is targeting a specific host in your network to access information or make unauthorized changes.
- **Top Denied Inbound Connections by Destination Port** displays the top ten inbound connections blocked by a firewall within the last hour of activity, by destination port number. Monitor the ports that are being targeted; an attacker might be trying to find an open ftp, telnet, or ssh port to access sensitive information.

- **Top Denied Internal Connections** displays the top ten connections between hosts within the protected network that are blocked by the firewall, within the last hour of activity. Monitor this activity to see if some one inside the firewall is attempting to access a sensitive asset that is protected by an internal firewall or within a protected internal subnet (for example, a system that has restricted or internal data); there might be an exploit in progress and you should investigate promptly.
- **Top Denied Outbound Connections by Source Host** displays the top ten outbound connections blocked by a firewall within the last hour of activity, by source address and zone name. Monitor blocked outbound traffic for any unusual patterns; some one might be attempting to transmit sensitive data outside your network or someone on the internal network might be continuously trying to establish an outbound connection that violates the firewall policy.
- **Latest Very High Priority Firewall Events** displays the last 15 very high ESM priority firewall events (level 9 or 10), as well as events with IP addresses that have a successful firewall connection after multiple blocks. Investigate events with a very high ESM priority immediately as this might indicate a grave concern; an exploit might be in progress. For details about the priority rating and how it is calculated, see the *ArcSight Console User's Guide*.
- **Latest Inbound Connections from Suspicious Countries** displays the last ten inbound firewall events whose source IP address is located in a suspicious country. Observe this traffic to determine if this traffic is authorized. Some one from a country on your suspicious list might be attempting to get to your data.
- **Latest Outbound Connections to Suspicious Countries** displays the last ten outbound firewall events originating in the protected network, whose destination IP address is located in a suspicious country. Monitor all traffic that 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.

Firewall Administration Dashboard

An example **Firewall Administration** dashboard is shown below.



The **Firewall Administration** dashboard provides the following data monitors and query viewer:

- The **Latest Firewall Configuration Changes** data monitor displays the last 15 configuration changes made to your firewall devices. You can see the time the configuration change was made, the type of configuration change, the source IP address and zone name, the user name logged into the firewall device, and the IP address, zone name, product type, and vendor of the firewall device. You can use this data monitor as a basic intrusion detection system. Monitor all configuration changes to make sure they are valid and are being carried out by authorized personnel.

  The data monitor also shows the ESM priority of the configuration change event. Investigate configuration change events with a priority of 7 or higher as this might indicate a potential problem. For details about the priority rating and how it is calculated, see the *ArcSight Console User's Guide*.

- The **Latest Firewall Errors** data monitor displays the last 15 firewall configuration errors. You can see the time the error recorded, the error type, the source IP address and zone name, and the IP address, zone name, product type, and vendor of the firewall device with the error event.

  Investigate any errors to make sure that your firewall devices are secure and functioning without problems. Also, track any mis-configuration. Attackers often look for vulnerable default settings and

exploit firewall weakness so that they can access your networks, intercept information in transmission, and redirect traffic. When a firewall device is not configured correctly, some one can access sensitive data, change important information, or even use a compromised system to pose as another trusted system on the network.

This data monitor also shows the ESM priority of the firewall error. Investigate events with a priority of 7 or higher as this might indicate a potential problem. For details about the priority rating and how it is calculated, see the *ArcSight Console User's Guide*.

- The **Latest Failed Firewall Logins** data monitor displays the last ten unsuccessful login attempts to a firewall device since the ArcSight Manager started. The data monitor is refreshed every 30 seconds. You can use this information to see from which machine access to the firewall device is being attempted so that you know where a potential attack is originating.
- The **Current Users Logged into Firewall** query viewer displays current login activity to your firewall devices. You can see details about each user logged into a firewall device, such as the user name, the IP address and zone from which the user logged in, and the time at which the user logged in. You can also see information about the firewall device, such as the firewall IP address, zone, product type, and vendor. Monitor the users currently logged into your firewall device to make sure they are authorized and valid. If ESM does not receive the proper logout event from the firewall device after 24 hours, it removes the entry from the query viewer and adds the session information to the **Anomalous Login Events Recorded** data monitor, as this is unexpected and potentially malicious behavior.

  Query viewers enable you to get quick, high-level summaries of security-related activity. You can use a query viewer to investigate situations as they are developing.
- The **Anomalous Login Events Recorded** data monitor displays the last ten firewall login sessions that are still active after 24 hours (ESM did not receive the proper logout event 24 hours after it received the login event). Monitor this activity as it presents a potential security risk; an unauthorized user that gains access to an active session can carry out malicious activity.

Right-click on an item in a data monitor and select **Investigate > Create Channel** to open an active channel and investigate events further. See "Investigating Further from a Data Monitor" below.

Investigating Further from a Data Monitor

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 destination port in the **Top Denied Inbound Connections by Destination Port** data monitor of the Firewall Monitoring dashboard and select **Investigate > Create Channel [Destination Port = *portnumber]*** to open an active channel and see more details, such as the source and destination IP address. 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 on denied inbound connections to a sensitive asset on your network, such as a DNS server or a domain controller. For detailed information about using inline filters, see the *ArcSight Console User's Guide*.

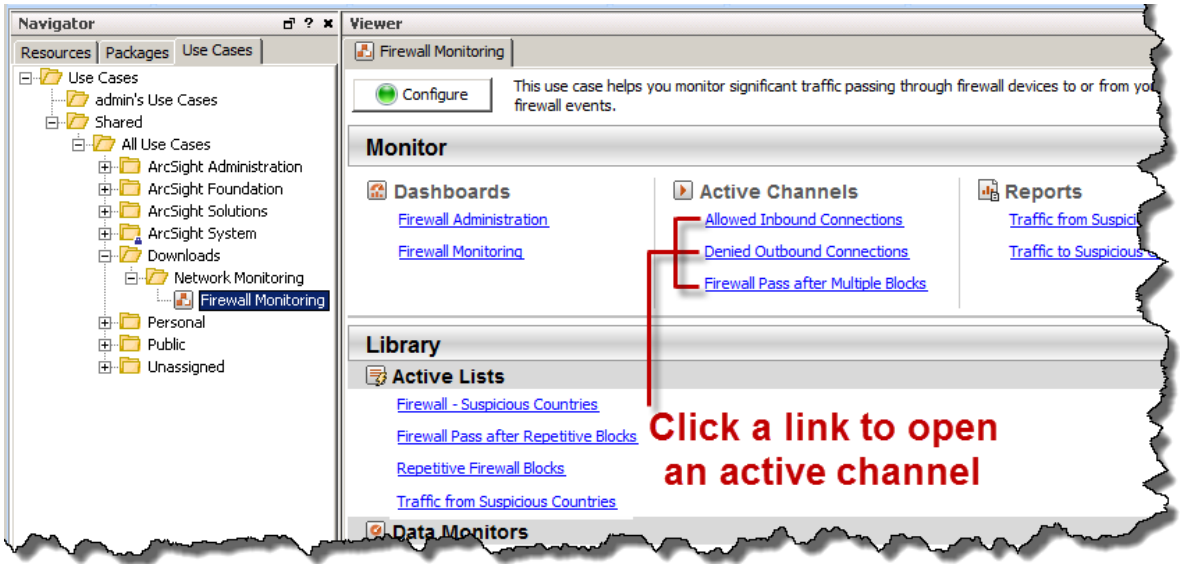
- Double-click on an event in the active channel to open the event inspector and see details about the event. For some events, the Details tab of the Event Inspector provides external links to Reference pages and Vulnerability pages, which describe an issue or a vulnerability in more detail.

Investigating Inbound and Outbound Connections in Active Channels

The Firewall Monitoring active channels show all events received within the last ten minutes with authorized connections coming into your network through a firewall device, with outbound connections denied by a firewall device, and with successful connections after multiple firewall blocks.

Understanding authorized and non-authorized activity on your firewall-protected network is essential to the health of the network, enabling you to keep unwanted traffic out, and important and confidential data in.

To open an active channel, click the link for the active channel in the Firewall Monitoring use case.



The active channel opens in the Viewer panel of the ArcSight Console 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 Firewall Monitoring use case provides these active channels:

- The **Allowed Inbound Connections** active channel displays all events received within the last ten minutes with authorized traffic coming into your network through the firewall. Examining these events helps to make sure that only authorized traffic is entering your network and prevents potential malicious attacks from exploiting weaknesses in the network and stealing your confidential data.

  For example, if you see that a lot of authorized traffic from a specific IP address to a confidential server on your network, you might want to investigate further to check that the inbound communication is coming from an authorized person and not someone who is trying to access confidential information from your secure server.

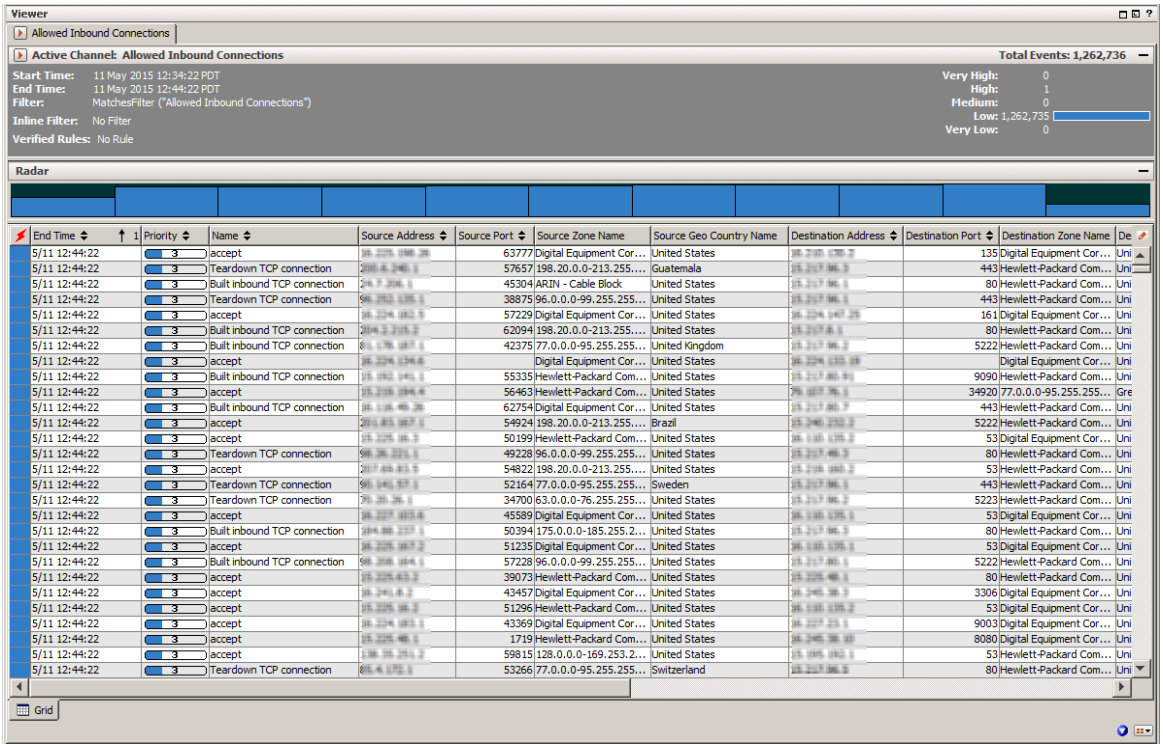
- The **Denied Outbound Connections** active channel displays all events received within the last ten minutes with unauthorized traffic trying to leave your network through the firewall (traffic from protected network assets trying to access assets external to the protected perimeter of the firewall).

  Certain activity, such as using social media, viewing online videos, and gaming can be a drain on employee productivity, on network bandwidth, and might expose you to viruses. Examining denied outbound traffic can help you prevent and mitigate internal threats to security and productivity.

- The **Firewall Pass after Multiple Blocks** active channel displays events received within the last ten minutes with successful inbound or outbound communication after being blocked by the firewall four times. Examine this activity, as it might indicate that an attacker found an open port during a port scan or that a brute force attack might be taking place.

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 **Allowed Inbound Connections** active channel is shown below.



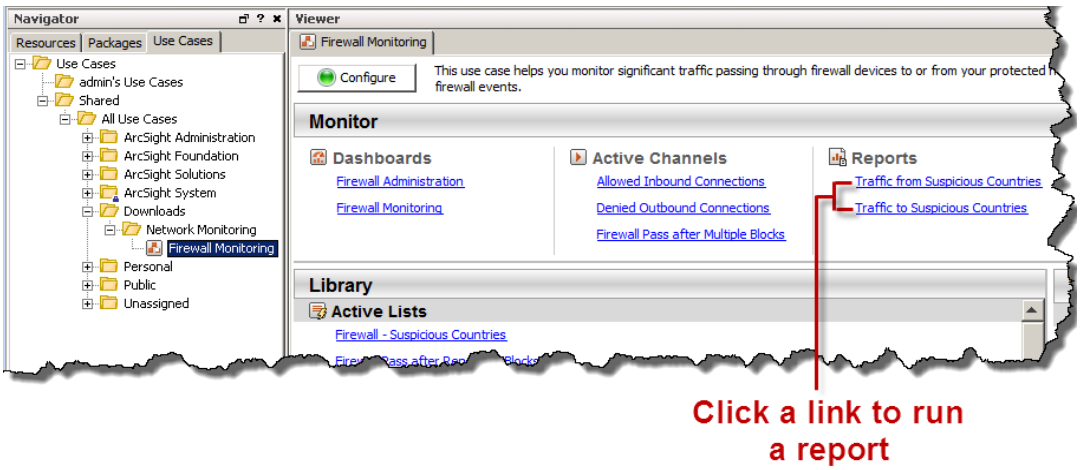
Running Reports

The Firewall Monitoring use case provides two reports that you can run to see events with firewall connections (successful or unsuccessful) to and from suspicious countries. You can provide these reports to the stakeholders in your company, when needed.

By default, the reports use data from the previous 24 hours. You can change the start and end time of the report for shorter- or longer-term analysis when you run the report.

To run a report:

1. Click the link for the report in the Firewall Monitoring use case.



2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The use case provides the following reports:

- The **Traffic from Suspicious Countries** report shows events with successful and unsuccessful inbound firewall connections from suspicious countries, within the last 24 hours. The report shows the time each event was first received, the time each event was last received, the source and destination IP address of each communication, the country from which the communication originated, the destination port and zone name, and the number of events calculated from the time the events were first received (if an event was last received outside the 24 hour time frame, it is not included in the event count).
- The **Traffic to Suspicious Countries** report shows events with successful and unsuccessful outbound connections through a firewall to suspicious countries, within the last 24 hours. The report shows the time each event was first received, the time each event was last received, the source and

destination IP address of each communication, the country to which the communication was being sent, the destination port and zone name, and the number of events calculated from the time the events were first received (if an event was last received outside the 24 hour time frame, it is not included in the event count).

Note: For both the **Traffic to Suspicious Countries** and **Traffic from Suspicious Countries** reports, if an event was last received outside the specified time frame (24 hours by default), the event does not appear in the reports.

Run these reports so that you can identify any traffic patterns from countries that are on your suspicious list. Look out for traffic from specific countries known to be hotbeds for malicious activity.

Note: The **Firewall - Suspicious Countries** active list contains the suspicious countries used in the reports. Make sure you configure this active list according to your business needs. See "Configuration" on page 9.

An example report is shown below.

05-26-2015-15:57:12 to 05-27-2015-15:57:12

Traffic from Suspicious Countries

Event First Received	Event Last Received	Event Name	Source Address	Source Country	Destination Address	Destination Port	Destination Zone Name	Event Count
May 27 2015 14:45:07	May 27 2015 15:56:12	Built inbound TCP connection	[redacted]	Iraq	[redacted]	80	Hewlett-Packard Company	1338
May 27 2015 14:45:09	May 27 2015 15:56:12	Teardown TCP connection	[redacted]	Iraq	[redacted]	80	Hewlett-Packard Company	1335
May 27 2015 14:45:08	May 27 2015 15:56:16	Built inbound TCP connection	[redacted]	Iraq	[redacted]	80	Hewlett-Packard Company	1045
May 27 2015 14:45:58	May 27 2015 15:51:39	Teardown TCP connection	[redacted]	Iraq	[redacted]	80	Hewlett-Packard Company	849
May 27 2015 14:45:02	May 27 2015 15:56:17	Built inbound TCP connection	[redacted]	Iran, Islamic Republic of	[redacted]	80	Hewlett-Packard Company	782
May 27 2015 14:45:06	May 27 2015 15:56:09	accept	[redacted]	Iran, Islamic Republic of	[redacted]	53	Hewlett-Packard Company	586
May 27 2015 14:45:05	May 27 2015 15:56:24	Teardown TCP connection	[redacted]	Iran, Islamic Republic of	[redacted]	80	Hewlett-Packard Company	535
May 27 2015 14:44:58	May 27 2015 15:56:20	accept	[redacted]	Iran, Islamic Republic of	[redacted]	80	Hewlett-Packard Company	445
May 27 2015 14:45:02	May 27 2015 15:55:51	Built inbound TCP connection	[redacted]	Iran, Islamic Republic of	[redacted]	80	Hewlett-Packard Company	445
May 27 2015 14:45:11	May 27 2015 15:56:21	accept	[redacted]	Iran, Islamic Republic of	[redacted]	80	Hewlett-Packard Company	442
May 27 2015 14:45:01	May 27 2015 15:56:25	Built inbound TCP connection	[redacted]	Iran, Islamic Republic of	[redacted]	5222	Hewlett-Packard Company	442
May 27 2015 14:46:46	May 27 2015 15:51:39	Built inbound TCP connection	[redacted]	Libyan Arab Jamahiriya	[redacted]	80	Hewlett-Packard Company	400
May 27 2015 14:44:50	May 27 2015 15:55:53	Teardown TCP connection	[redacted]	Iran, Islamic Republic of	[redacted]	80	Hewlett-Packard Company	399
May 27 2015 14:45:46	May 27 2015 15:56:13	Built inbound TCP connection	[redacted]	Iran, Islamic Republic of	[redacted]	443	Hewlett-Packard Company	396

Page 1 of 16

Firewall Monitoring Rules

The Firewall 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/Firewall Monitoring`) and are enabled by default. The rules trigger when events match one or more set of conditions, at which point certain rules generate correlation events, which are 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 **Firewall Pass After Repetitive Blocks** rule triggers when a source in the **Repetitive Firewall Blocks** active list (populated by the **Repetitive Inbound Firewall Blocks** and **Repetitive Outbound Firewall Blocks** rules) finally makes a successful connection attempt through a firewall device. The rule adds the source to the `/All Active Lists/ArcSight System/Threat Tracking/Suspicious List` so that it can be tracked down by other ESM content. The rule also adds the source to the **Firewall Pass after Repetitive Blocks** active list. (The entry expires from this active list after 12 hours if there is no more activity from the source.)

  The correlation event that this rule creates is shown in the **Latest Very High Priority Firewall Events** data monitor. Investigate this activity as it might indicate that an attacker found an open port during a port scan or that a brute force attack might be taking place.
- The **Repetitive Inbound Firewall Blocks** rule triggers when four inbound firewall blocks occur within one minute. The rule adds the host to the **Repetitive Firewall Blocks** active list. (The entry expires from the active list after 12 hours if there are no more blocked events.) This activity might indicate a port scan (reconnaissance), network scan, or other malicious activity.
- The **Repetitive Outbound Firewall Blocks** rule triggers when four outbound firewall blocks occur within one minute. The rule adds the hosts to the **Repetitive Firewall Blocks** active list. (The entry expires from the active list after 12 hours if there are no more blocked events.) This activity might indicate that a host in your network is repeatedly trying to access a restricted service or server outside your network. Perhaps data exfiltration is being attempted or 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.
- The **Traffic from Suspicious Countries** rule triggers when an event is identified with an inbound connection from a suspicious country (successful or unsuccessful). This is a lightweight rule that does not generate a correlation event but adds the event information to the **Traffic from Suspicious Countries** active list, which is then used in the **Traffic from Suspicious Countries** report. Inbound traffic from countries with which you do not conduct business might indicate malicious activity.
- The **Traffic to Suspicious Countries** rule triggers when an event is identified with an outbound

connection to a suspicious country (successful or unsuccessful). This is a lightweight rule that does not generate a correlation event but adds the event information to the **Traffic to Suspicious Countries** active list, which is then used in the **Traffic to Suspicious Countries** report. Outbound connections to countries with which you do not conduct business might indicate that sensitive data is being siphoned to another country.

- The **Successful Firewall User Logins** rule triggers when a user successfully logs into a firewall device. The rule is a lightweight rule, which does not generate a correlation event but adds the event information to the **Users Logged into Firewall** active list.
- The **Successful Firewall User Logouts** rule triggers when a user successfully logs out of a firewall device. The rule is a lightweight rule, which does not generate a correlation event but removes the event information from the **Users Logged into Firewall** 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: Firewall Monitoring 1.1)

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!