Tech Note--Audit Support for Symantec Endpoint Protection Manager

Symantec CloudSOC Tech Note

Copyright statement

Table of Contents

Introduction

This Tech Note describes how you configure Symantec Endpoint Protection Manager (SEPM) to log network traffic, and to deliver the traffic logs in either CSV or syslog format for use in the CloudSOC Audit application. It also shows samples of the different log formats.

The procedures in this Tech Note were developed with SEPM version 12.1; other versions may function and appear differently.

Sample log formats

SEPM provides logs in CSV format through manual export and through syslog export. The following sections show samples of SEPM logs in both formats.

Syslog format

```
7/20/2016 5:50:50 PM [22] From:IE11Win7 (127.0.0.1) Fac:5 Sev:3 Msg
>>> Jul 19 14:46:53 IE11Win7 SymantecServer: IE11Win7,Local:
10.0.2.15,Local: 50247,Local: 08002785C5CD,Remote:
23.5.251.27,Remote: g2.symcb.com,Remote: 80,Remote:
525400123502,TCP,Outbound,Begin: 2016-07-19 14:43:17,End: 2016-07-19
14:43:17,Occurrences: 1,Application: C:/Program Files/Internet
Explorer/iexplore.exe,Rule: log_web_traffic,Location: Default,User:
IEUser,Domain: IE11WIN7,Action: Allowed
```

CSV format

```
Time Stamp,Event Type,Event Time,Severity,Host Name,Current IP
Address,Historical IP Address,Remote Host IP,Remote Host Name,Network
Protocol,Local Port,Remote Port,Traffic Direction,Application
Name,Begin Time,End Time,Repetition,ACTION,Rule Name,Alert,Send Snmp
Trap,Local Host Mac,Remote Host Mac,Hardware Key,Location Name,User
Name,Domain Name,Site Name,Server Name,Group Name,Computer Name
```

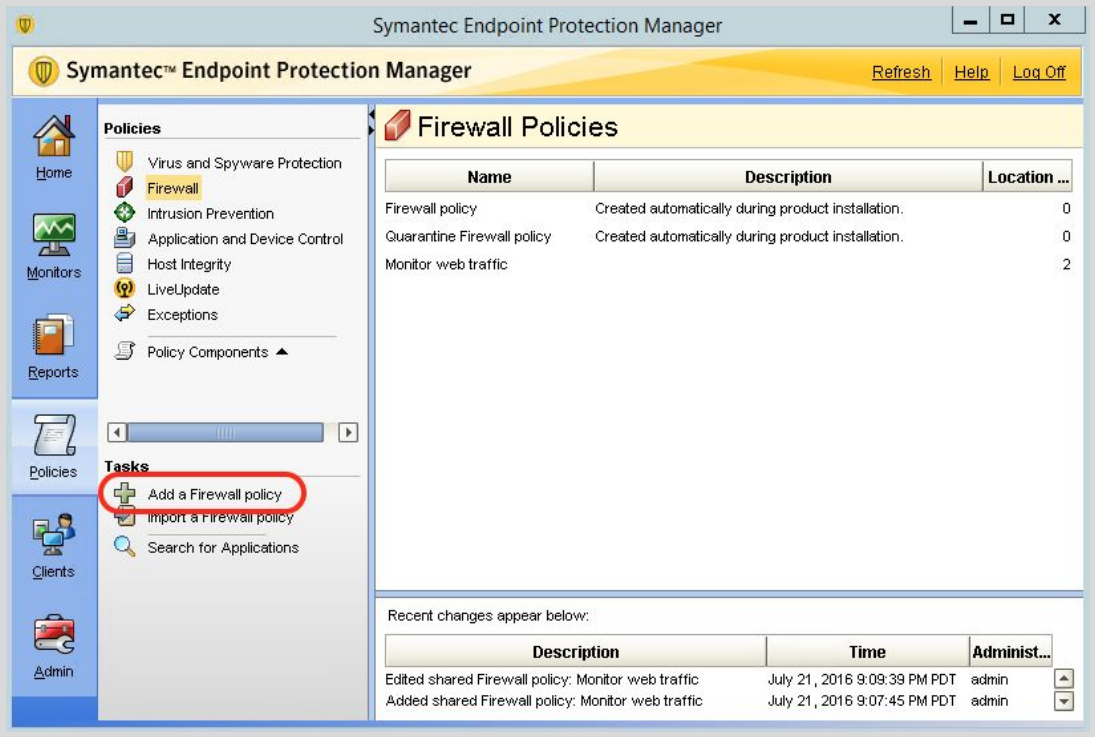
```
07/19/2016 14:46:53,TCP initiated,07/19/2016
14:42:27,Major,IE11Win7,10.0.2.15,10.0.2.15,65.52.108.163,urs.microso
ft.com,TCP,50282,443,Outbound,C:/Program Files/Internet
Explorer/iexplore.exe,07/19/2016 14:43:23,07/19/2016 14:43:23,1,Not
blocked,log_web_traffic,0,0,08002785C5CD,525400123502,909AC2C493CE639
153C2E9A24E4620DD,Default,IEUser,Default,My Site,IE11Win7,My
Company\Default Group,IE11Win7
```

Monitoring web traffic through SEPM

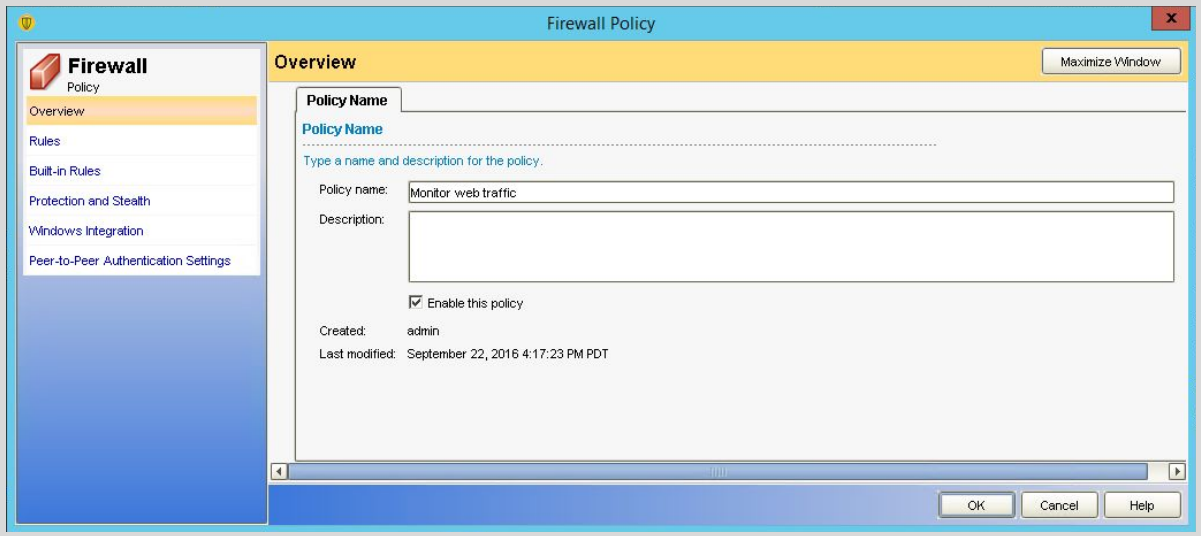
To record network logs, you configure a custom firewall policy to capture web traffic going to ports 80 and 443. Once you activate this policy, SEPM collects network logs from each client and store them in its database.

Create firewall policy

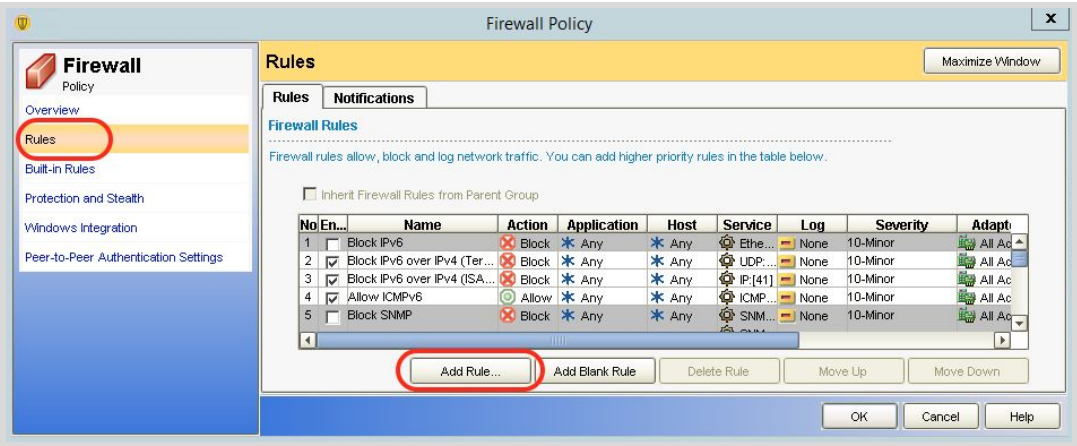
1. If you have not already done so, login to Symantec Endpoint Protection Manager.
2. On the SEPM console click **Policies**, and in the Policies area click **Firewall**. Then click **Add a Firewall Policy** as shown below.



3. On the Overview page, fill in a name for the policy as shown below, then click **OK**.



4. At the left edge of the Firewall Policy window, click **Rules**, then click **Add Rule** as shown below.



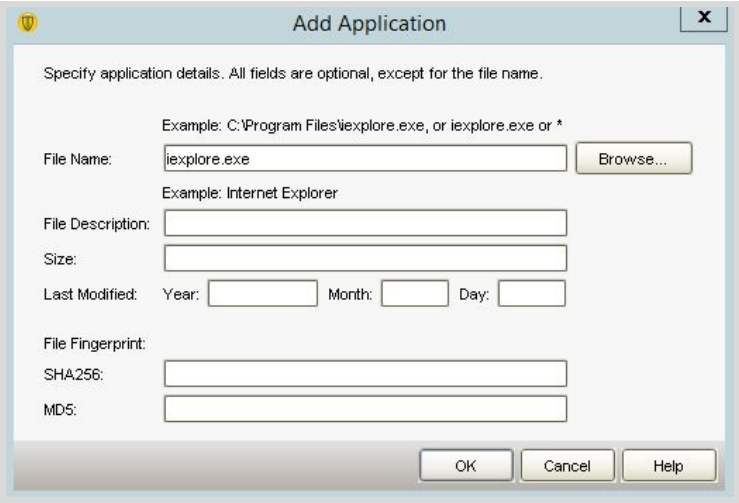
5. On the Add Firewall Rule Wizard, enter a name for the rule and click **Next** as shown below.

6. Mark **Allow Connections** as shown below and click **Next**.

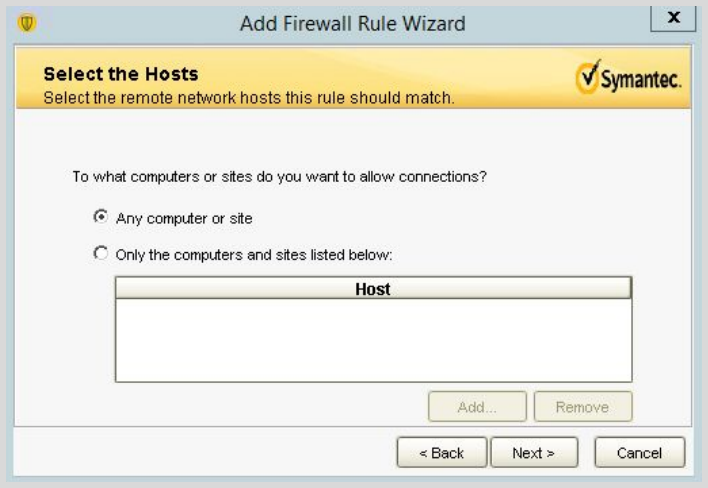
7. On the Select the Rule Applications page, choose the applications that the rule matches. We recommend you choose **All Applications**.

You can also choose to match only specific applications, then click **Add** to build a list of applications as shown below, then click **Next**.

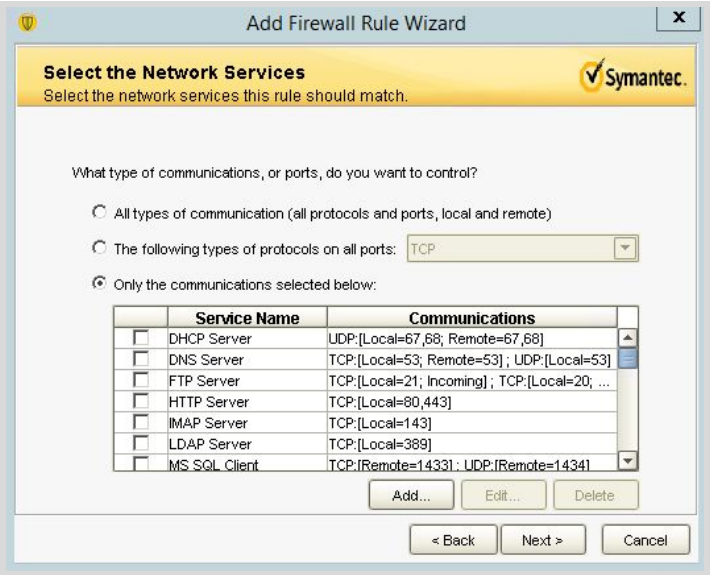
If you build an application list for the rule, typically you would list browsers and other web applications as shown in the example below.



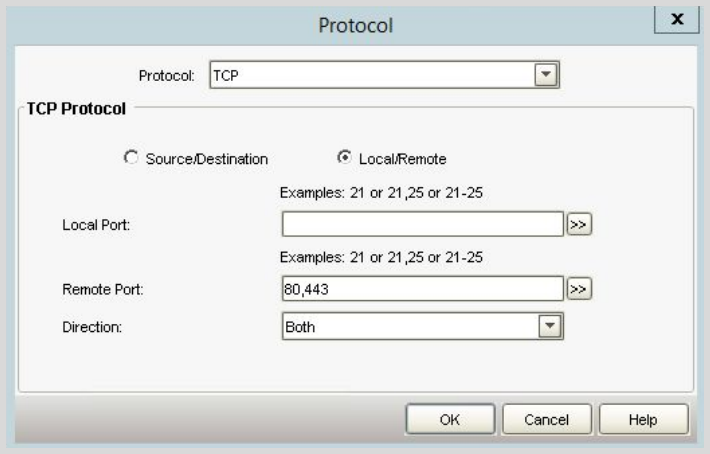
8. For Hosts, click **Any computer or site** as shown below, then click **Next**.



9. On the Select Network Services page, click **Add** to add protocols and ports.



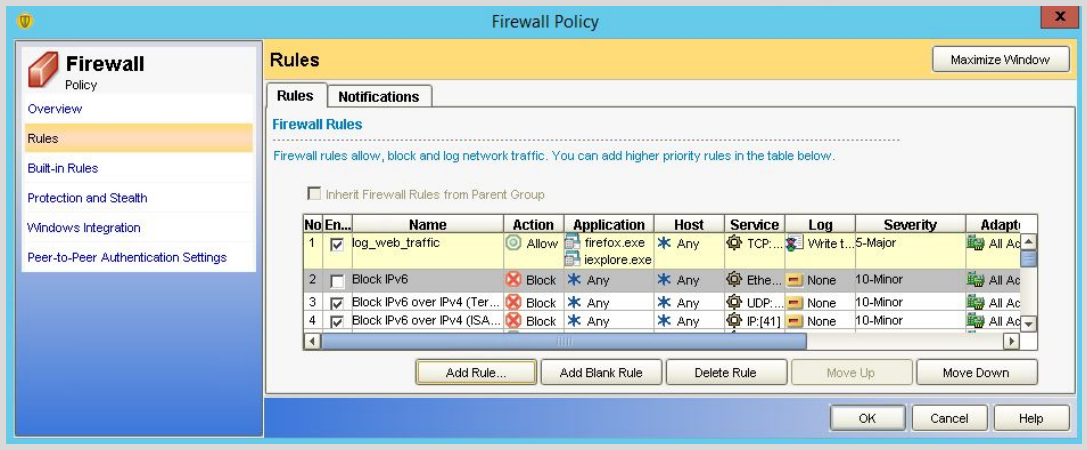
10. Enter remote ports 80 and 443 to capture traffic going to http and https as shown below. If browser traffic goes through a web proxy, then also add the proxy ports in addition to the standard ports 80 and 443.



After adding the ports, click **OK** on the Protocol dialog box, then click **Next**.

11. On the Select a Log Action page, mark **Yes** to create a log entry when the rule is matched, as shown below. Then click **Finish**.

SEPM creates the rule similar to that shown below.



12. On the Rules page, click **OK**.

    SEPM prompts you to assign the policy as shown below.

13. Click **Yes**, then assign the policy to either your entire company, or to specific groups or locations as shown below.

14. Click **Assign**, and then then click **Yes** when SEPM asks you to confirm as shown below.

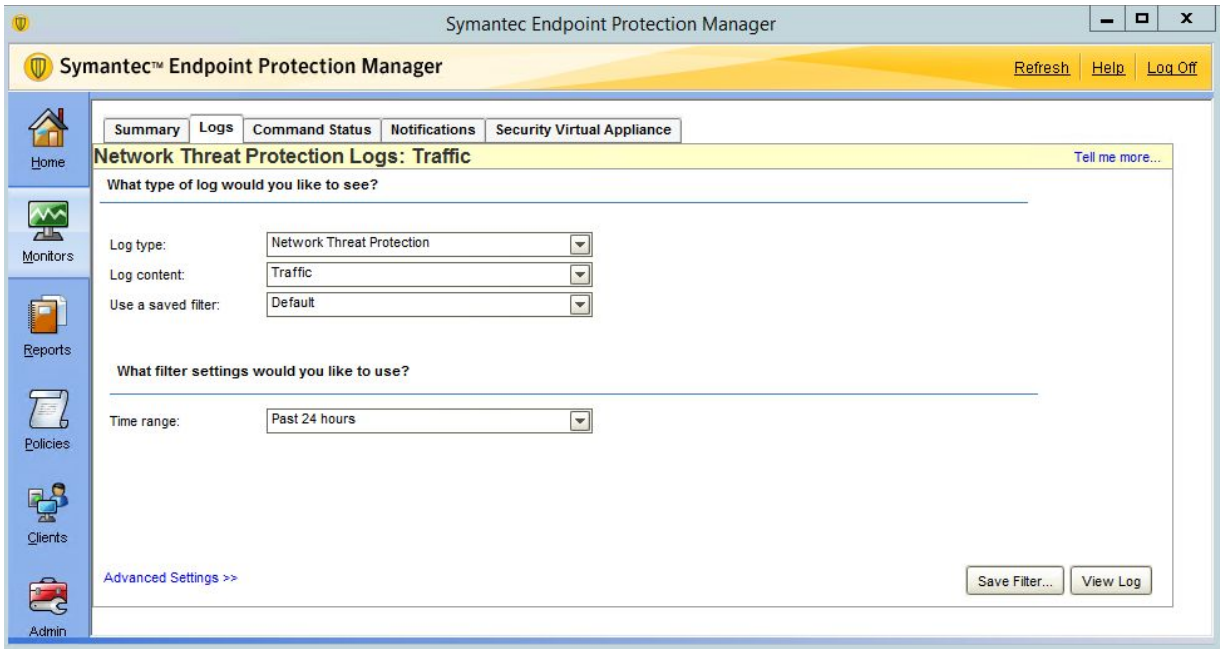
Exporting logs from SEPM

After creating the custom firewall policy SEPM starts capturing the web traffic logs. You can export these logs using one of the methods described in the following sections.

Manually export logs in CSV

1. From the SEPM console, click **Monitors** > **Logs**.

2. For Log Content choose **Traffic** as shown below.

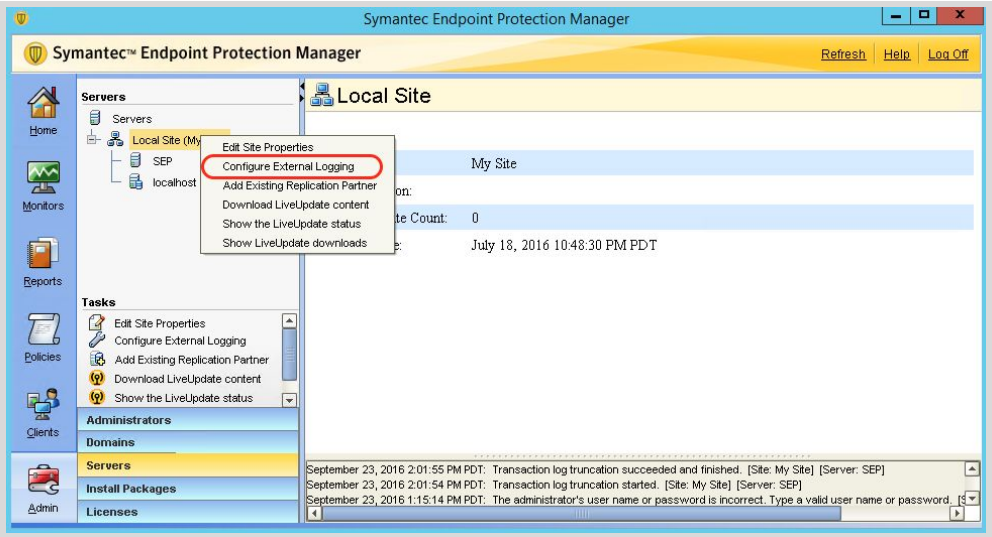


Export logs through Syslog

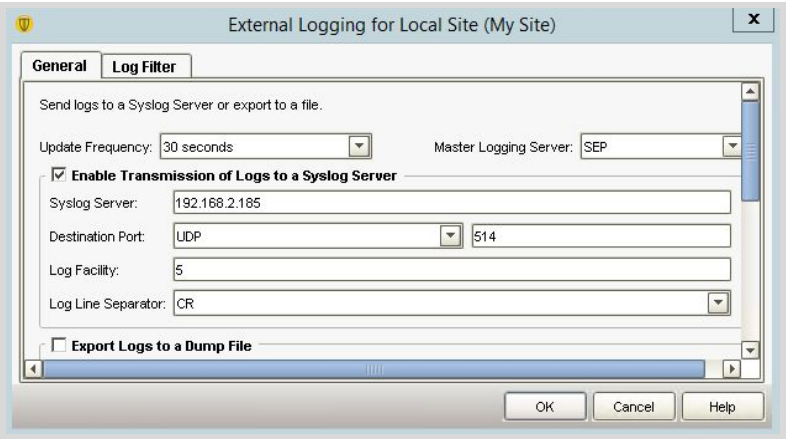
Use the syslog option to export logs continuously. SEPM periodically pushes the logs to a syslog server that you can configure as a CloudSOC Audit datasource. You can also use this method to make SEPM push logs to the syslog server on a SpanVA instance.

To configure SEPM to push logs with syslog:

1. In SEPM, click **Admin** and **Servers**. Then right-click on **Local Site** and choose **Configure External Logging** as shown below.



2. On the External Logging dialog box, enter the syslog server IP address as shown below, then click OK. In the case of a SpanVA syslog server, enter the SpanVA IP address.



Creating a SpanVA data source in CloudSOC

If you are using a SpanVA instance at your location to collect logs for use in CloudSOC Audit, create a SpanVA datasource for the SEPM logs as described in the following sections. See the CloudSOC Tech Note *Installing and Configuring SpanVA* For more information.

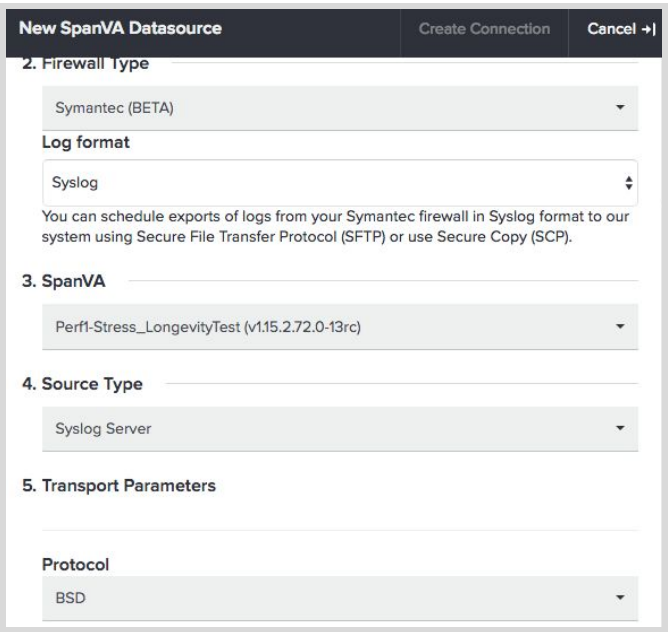
Syslog and CSV source types

Use either Syslog or CSV source types if SEPM is writing logs to a server.

1. In CloudSOC, choose **Audit** > **Device Logs**.
2. On the Device Logs page, click **New Data Sources** > **SpanVA Datasource**.
3. On the New SpanVA Datasource panel, use the following settings:

Field	**Setting**
Datasource Name	Enter a descriptive name.
Firewall Type	Choose **Symantec Endpoint Protection Manager**.
Log format	Choose **Syslog** or **CSV logs**.
SpanVA	Choose the SpanVA instance from the menu of those available. Make sure that the version listed for the SpanVA instance is 1.15.2.72 or later.
Source Type	Choose **Syslog Server** or **SCP/SFTP/FTP/HTTPS Server**.
Protocol (Syslog source type only)	choose either **BSD** or **IETF**.

The following figure shows a typical SpanVA data source configuration.



SQL Database source type

Use the DB source type when SEPM writes logs into an SQL server database.

Note the following details and limitations relating to SpanVA MS SQL support for Symantec Endpoint Protection Manager:

- Turn off Windows Firewall on the Windows machine where the SQL database resides. Otherwise SpanVA cannot access the database.
- You must open the TCP port (default 1433) on the Windows machine where the SQL database resides.
- Do not end the SQL query with a semicolon (;) when creating the Datasource Definition.
- Each time SpanVA pulls data from your SQL server, CloudSOC advances an internal marker to the day and time of the latest record obtained from the server. SpanVA only pulls data from after the marker was set, and does not go back and re-pull any data predating the marker. Note the following implications of this system:
    - You must be careful when creating Custom Headers. If you create an invalid Custom Header and use it to pull data from the server, the Audit app is unable to parse that data, and so ignores it. After you fix the custom header, Audit correctly parses new data pulled from the database, but SpanVA does not go back and re-pull the data previously obtained.
    - If for whatever reason your SQL server contains records relating to some future date (for example, because of a date/time misconfiguration on a device), CloudSOC advances the date/time marker to that future date, and does not pull any records dated prior to that date/time.

  If you encounter either of these situations, easiest thing to do is to delete the datasource. If for some reason you encounter such a situation on a datasource that has important historical data, contact CloudSOC technical support to have the SpanVA date/time marker reset so you can re-pull the data.

To use the DB source type:

1. In CloudSOC, choose **Audit** > **Device Logs**.
2. On the Device Logs page, click **New Data Sources** > **SpanVA Datasource**.

3. On the New SpanVA Datasource panel, use the following settings for Datasource Name, Firewall Type, and SpanVA:

Field	**Setting**
Datasource Name	Enter a descriptive name for the new datasource.
Firewall Type	Choose **Symantec Endpoint Protection Manager**.
Log format	Choose **DB**.
Custom Headers	Mark the checkbox and and copy the following headers into the text box: `USN,DOMAIN_ID,SITE_ID,SERVER_ID,GROUP_ID,COMPUTER_ID,TIME_STAMP,EVENT_ID,EVENT_TIME,SEVERITY,AGENT_ID,HARDWARE_KEY,HOST_NAME,LOCAL_HOST_IP,REMOTE_HOST_IP,REMOTE_HOST_NAME,NETWORK_PROTOCOL,LOCAL_PORT,REMOTE_PORT,TRAFFIC_DIRECTION,BEGIN_TIME,END_TIME,REPETITION,APP_NAME,BLOCKED,RULE_ID,RULE_NAME,ALERT,SEND_SNMP_TRAP,LOCAL_HOST_MAC,REMOTE_HOST_MAC,LOCATION_NAME,USER_NAME,DOMAIN_NAME,RESERVED_INT1,RESERVED_INT2,RESERVED_BIGINT1,RESERVED_BIGINT2,RESERVED_CHAR1,RESERVED_CHAR2,RESERVED_VARCHAR1,RESERVED_BINARY,LOG_IDX,LOCAL_HOST_IPV6,REMOTE_HOST_IPV6,NESTED_PROTOCOL_TYPE,NESTED_PROTOCOL_SUB_TYPE,LOCAL_HOST_IP_TEXT,REMOTE_HOST_IP_TEXT`
SpanVA	Choose the SpanVA instance from the menu of those available. Make sure that the version listed for the SpanVA instance is 1.15.2.72 or later.

4. On the New SpanVA Datasource panel, use the following Transport Parameters settings:

Field	**Setting**
Host	Enter the host IP of the SQL Server where the SEPM is exporting logs.
Port	Enter the port number the SQL server has been configured to listen for TCP connections. The default port is 1433.
User Name	Enter the username for the SQL server that has permission to read the database tables. Make sure this user can run the query and has connect and read access to all the tables, views and dbs associated with the query.
Password	Enter the password for the database user.
Maximum History Days	Enter the number of days in the past the SpanVA pulls logs.
Database Type	Choose **Microsoft SQL Server**.
Database Name	Enter the name of the database table you have configured in the SEPM for exporting the logs.
SQL Query	`SELECT USN,DOMAIN_ID,SITE_ID,SERVER_ID,GROUP_ID,COMPUTER_ID,TIME_STAMP,EVENT_ID,EVENT_TIME,SEVERITY,AGENT_ID,HARDWARE_KEY,HOST_NAME,LOCAL_HOST_IP,REMOTE_HOST_IP,REMOTE_HOST_NAME,NETWORK_PROTOCOL,LOCAL_PORT,REMOTE_PORT,TRAFFIC_DIRECTION,BEGIN_TIME,END_TIME,REPETITION,APP_NAME,BLOCKED,RULE_ID,RULE_NAME,ALERT,SEND_SNMP_TRAP,LOCAL_HOST_MAC,REMOTE_HOST_MAC,LOCATION_NAME,USER_NAME,DOMAIN_NAME,RESERVED_INT1,RESERVED_INT2,RESERVED_BIGINT1,RESERVED_BIGINT2,RESERVED_CHAR1,RESERVED_CHAR2,RESERVED_VARCHAR1,RESERVED_BINARY,LOG_IDX,LOCAL_HOST_IPV6,REMOTE_HOST_IPV6,NESTED_PROTOCOL_TYPE,NESTED_PROTOCOL_SUB_TYPE,LOCAL_HOST_IP_TEXT,REMOTE_HOST_IP_TEXT FROM sem5.dbo.V_AGENT_TRAFFIC_LOG`

5. At the top of the New SpanVA Datasource panel, Click **Create Connection** as shown below.

Revision history

Date	Version	Description
11 October 2016	1.0	Initial release
7 November 2016	1.1	Revise SQL query and default port
7 September 2017	1.2	Add SQL details from SpanVA Tech Note
10 January 2019	1.3	Update SQL query and custom headers
28 June 2019	1.4	Removed broken link