RSA NetWitness Platform

Event Source Log Configuration Guide

Cisco Firepower and Sourcefire Defense Center

Last Modified: Tuesday, August 13, 2019

Event Source Product Information:

Vendor: Cisco
Event Source: Defense Center, AMP (Advanced Malware Protection), NGFW (Next-Generation Firewall), Firepower
Versions: 4.x, 5.x, 6.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: snort
Collection Method: Syslog
Event Source Class.Subclass: Security.IDS

To configure Sourcefire Defense Center, you must:

Configure Sourcefire/Firepower

I. Configure Syslog Output on Sourcefire

II. Configure Sourcefire to Send Intrusion and AMP Events

III. Configure Audit Logging

IV. (Optional) Configure Health Monitoring Alerts

Configure Syslog Output on Sourcefire

Perform the following procedure on the Sourcefire event source.

To set up Syslog Output via Sourcefire Defense Center:

1. Configure the Sourcefire Sensor and Sourcefire Defense Center per the vendor's instructions.
2. Connect to the Defense Center web management console and log in.
3. Depending on your version of Sourcefire Snort, do one of the following:
   - For versions 4.6, 4.8, or 4.9, click **Policy & Response** > **Responses** > **Alerts**.
   - For version 5.0 and higher, click **Policies** > **Action** > **Alerts**.
4. Click the **Create Alert** icon and set the following parameters in the Create Alert area:
   a. Select **Syslog** from the drop down box.

      Note: In version 5.0 and higher, select **Create Syslog Alert** from the drop down box.

   b. In the **Name** field, enter a name for the Alert (for example, Sourcefire48).

   c. In the **Host** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

   d. In the **Port** field, type **514**.

   e. In the **Facility** drop down list, select USER.

   f. In the **Severity** drop down list, select the level of alerts you want to send to RSA NetWitness Platform.

   g. In the **Tag** field, enter a tag name (for example, Sourcefire48).

h. Check the **Active** check box.

> **Note:** In version 5.0 and higher, please skip 4h. There is no **Active**box to be checked.

i. Click **Save** to apply the changes.

> **Note:** If you choose to configure Health Monitoring alerts, use the name of the alert you created in this step.

5. Depending on your version of Source Fire Snort, do one of the following:
   - For versions 4.6, 4.8, or 4.9, click **Policy & Response** > **Responses** > **Impact Flag Alerts** in the top menu bar.
   - For version 5.0 and higher, click the **Impact Flag Alerts** tab adjacent to **Alerts** tab.

   The system displays the Syslog entry that you created above.
6. In the **Impact Flag** area, do the following:
   a. Check the **Syslog Notification** box for the alerts that you want to send (the box on the blue bar selects all).
   b. Click **Save** to apply the changes.
7. Depending on your version of Source Fire Snort, do one of the following:
   - For versions 4.6, 4.8, or 4.9, click **Policy & Response** > **Responses** > **RNA Event Alerts** in the top menu bar.
   - For version 5.0 and higher, click the **Discovery Event Alerts** tab adjacent to the **Impact Flag Alerts** tab.

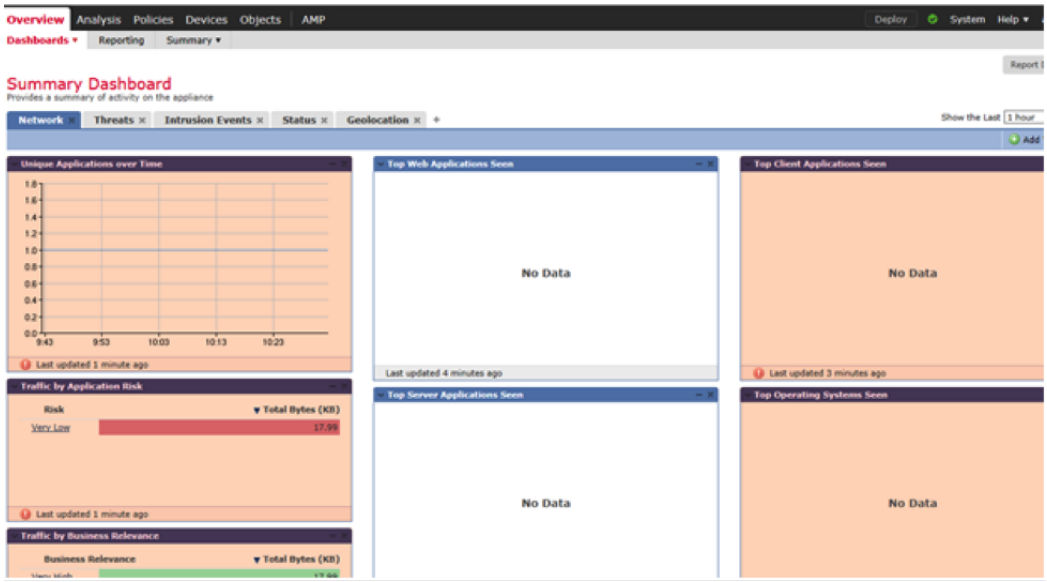
   The system displays the Syslog entry that you created above.
8. In the **Event** area, do the following:
   a. Check the **Syslog Notification** box for the alerts that you want to send (the box on the blue bar selects all).
   b. Click **Save** to apply the changes.

Configure Sourcefire to Send Intrusion and AMP Events

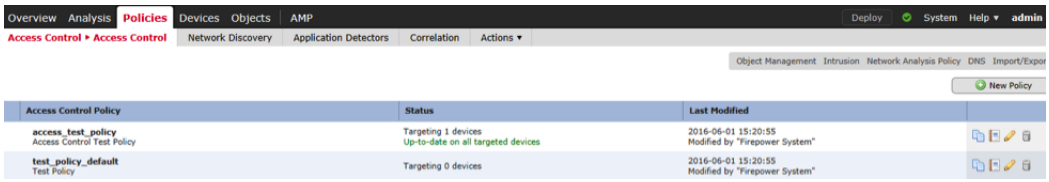
Perform the following procedure to configure Sourcefire to send connection, intrusion and AMP events:

To set up Syslog Output via Sourcefire Defense Center:

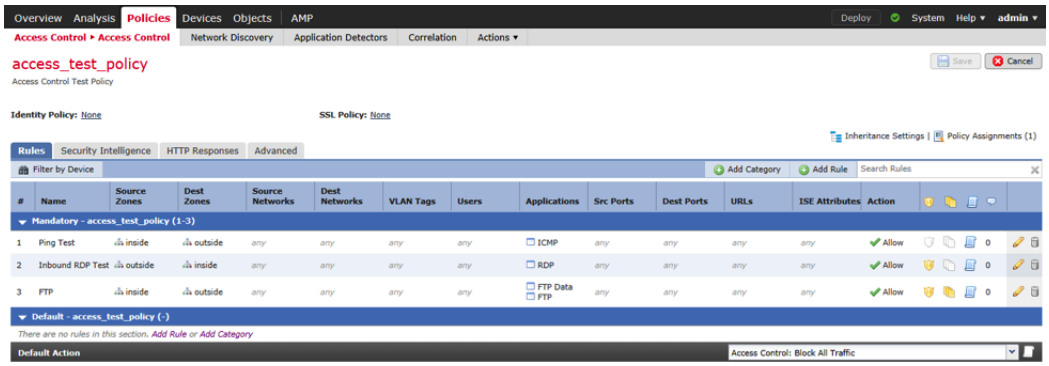
1. Connect to the Cisco Firepower Management console and log in.



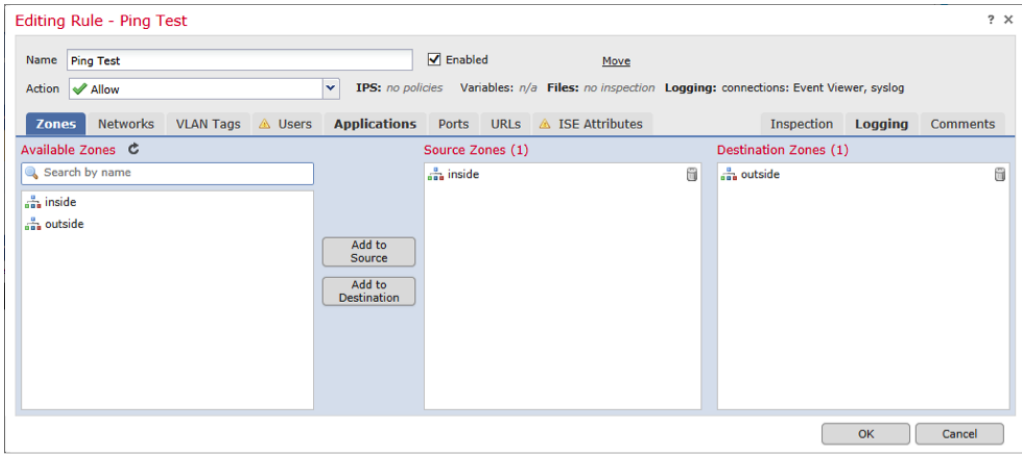
2. Click on **Policies > Access Control >Access Control**.



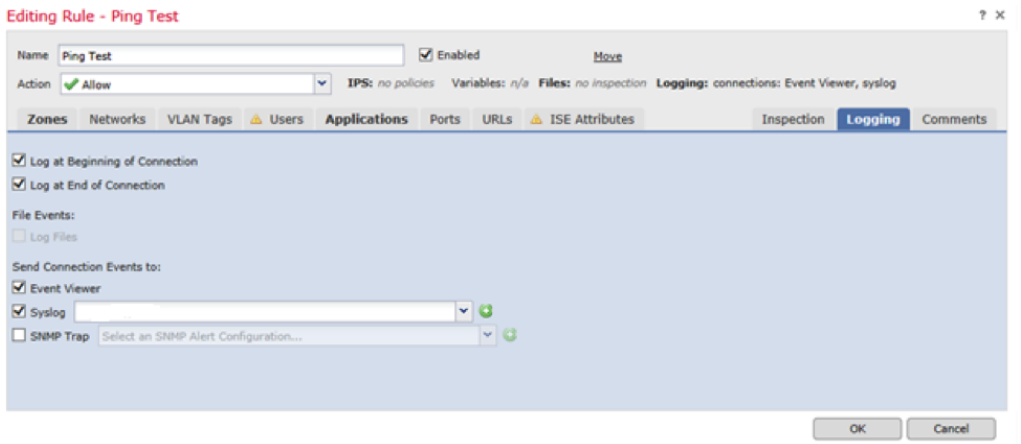
3. Click on the policy for which you want to send alerts.



4. Edit the rule for which logging needs to be activated.



5. Click on the **Logging** tab.



6. In the **Send Connection Events to** section, check the **Syslog** box, and add the host information that you added in Step 4 of the Configure Syslog Output on Sourcefire procedure.

Note: To assign Intrusion and File policy, use the **Inspection** tab (located to the left of the **Logging** tab in the menu bar).

Configure Audit Logging

To pick up Admin Policy changes from the Sourcefire logs, perform the following steps.

To Configure Audit Logging:

1. Connect to the Defense Center web management console and log in.
2. In the top menu bar, click **System** > **Local** > **System Policy**.
3. Create a new policy, or edit an existing one.
4. Set the audit log settings as follows:

Field	Action
Send Audit Log to Syslog	Set to **enabled**.
Host	Enter the IP address of your RSA NetWitness Platform Log Decoder or RSA NetWitness Platform Remote Log Collector.
Facility	Select AUTH or choose a value that fits the needs of your organization.
Severity	Select INFO or choose a value that fits the needs of your organization.

5. Save the policy and exit.

Configure Health Monitoring Alerts

RSA NetWitness Platform can process Defense Center health alerts. If you want to configure Health Monitoring Alerts, perform the following steps.

To Configure Health Monitoring Alerts:

1. Connect to the Defense Center web management console and log in.
2. In the top menu bar, click **Policy & Response** > **Responses** > **Alerts**.

   Note: For version 5.0 and up, hover over the **Health** tab in the top menu bar to show its options.

3. Click **Health Monitor Alerts**.
4. In the Health Alert Name field, enter the name for your health alert.
5. Select severity and modules based on kind of messages that you want to send to RSA NetWitness Platform

Note: Select all severities and modules to get the maximum set of messages.

6. From the **Alert** list select the alert you created in step 4 from the **To set up Syslog Output via Sourcefire Defense Center** procedure.
7. Click **Save** to apply the changes.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **snort**.

Configure Syslog Collection

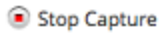
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:

- If you see 

, click the icon to start capturing Syslog.
- If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.