Palo Alto Networks

Use the IBM® Security QRadar® SIEM DSM for Palo Alto PA Series to collect events from Palo Alto PA Series devices.

The following table identifies the specifications for the Palo Alto PA Series DSM:

Table 1. DSM specifications for Palo Alto PA Series

Specification	Value
Manufacturer	Palo Alto Networks
DSM name	Palo Alto PA Series
RPM file name	`DSM-PaloAltoPaSeries-`*`build_number`*`.noarch.rpm`
Supported versions	PanOS v3.0 and later
Event format	Syslog LEEF
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	Yes
More information	Palo Alto Networks website (http://www.paloaltonetworks.com)

To integrate Palo Alto PA Series with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the Palo Alto PA Series DSM RPM.
2. Configure your Palo Alto PA Series device to enable communication with QRadar. You must create a syslog destination and forwarding policy on the Palo Alto PA Series device.
3. If QRadar does not automatically detect Palo Alto PA Series as a log source, create a Palo Alto PA Series log source on the QRadar Console. Use the following Palo Alto values to configure the log source parameters:

Log Source Identifier	The IP address or host name of the Palo Alto PA Series device
Log Source Type	Palo Alto PA Series
Protocol Configuration	Syslog

Creating a syslog destination on your Palo Alto device

Before you can send Palo Alto events to IBM Security QRadar, create a syslog destination on the Palo Alto PA Series device.

Procedure

1. Log in to the Palo Alto Networks interface.
2. Click the **Device** tab.

3. Select **Server Profiles** > **Syslog**.
4. Click **Add**.
5. Create a syslog destination:
   a. On the **Syslog Server Profile** dialog box, click **Add**.
   b. Specify the name, server IP address, port, and facility of the QRadar system that you want to use as a syslog server:
   c. Click **OK**.
6. Configure LEEF events:
   a. Click the **Custom Log Format** tab.
   b. Copy the following text and paste it in the **Custom Format** column for the Config log type.

      ```
      LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$result|cat=$type|
      usrName=$admin|src=$host|devTime=$cef-formatted-receive_time|client=$client|
      sequence=$seqno|serial=$serial|msg=$cmd
      ```

   c. Copy the following text and paste it in the **Custom Format** column for the System log type.

      ```
      LEEF:1.0|Palo  Alto Networks|PAN-OS Syslog Integration|4.0|$eventid|cat=$type
      |subtype=$subtype|devTime=$cef-formatted-receive_time|sev=$severity|msg=$opaque
      |Filename=$object
      ```

   d. Copy the following text and paste it in the **Custom Format** column for the Threat log type.

      ```
      LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$threatid|cat=$type|
      subtype=$subtype|src=$src|dst=$dst|srcPort=$sport|dstPort=$dport|protol=$proto|
      usrName=$srcuser|SerialNumber=$serial|NATSourceIP=$natsrc|NATDestIP=$natdst|
      RuleName=$rule|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
      VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=
      $inbound_if|EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=
      $sessionid|RepeatCount=$repeatcnt|NATSourcePort=$natsport|NATDestPort=$natdport|
      Flags=$flags|URLCategory=$category|Severity=$number-of-severity|Direction=
      $direction|Miscellaneous=$misc|ContentType=$contenttype
      ```

   e. Copy the following text and paste it in the **Custom Format** column for the Traffic log type.

      ```
      LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$action|cat=$type|
      src=$src|dst=$dst|srcPort=$sport|dstPort=$dport|protol=$proto|usrName=$srcuser|
      SerialNumber=$serial|Type=$type|Subtype=$subtype|NATSrcIP=$natsrc|NATDstIP=$natdst|
      RuleName=$rule|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
      VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
      EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
      RepeatCount=$repeatcnt|NATSourcePort=$natsport|NATDestPort=$natdport|Flags=$flags|
      Bytes=$bytes|Packets=$packets|ElapsedTime=$elapsed|URLCategory=$category|BytesIn=
      $bytes_received|BytesOut=$bytes_sent
      ```

7. Click **OK**.
8. Specify the severity of events that are contained in the syslog messages:
   a. Select **Log Setting** > **System** and click **Edit**.
   b. Select the check box for each event severity level that you want contained in the syslog message.
   c. Type the name of the syslog destination.
   d. Click **OK**.
9. Click the **Device** tab, click **Commit**.

What to do next

To allow communication between your Palo Alto Networks device and QRadar, create a forwarding policy. See "Creating a forwarding policy on your Palo Alto device."

Creating a forwarding policy on your Palo Alto device

If your QRadar Console or Event Collector is in a different security zone than your Palo Alto PA Series device, create a forwarding policy rule.

Procedure

1. Log in to the Palo Alto Networks interface.
2. On the dashboard, click the **Policies** tab.
3. Select **Policies** > **Policy Based Forwarding**.
4. Click **New**.
5. Configure the parameters. For descriptions of the policy-based forwarding values, see your *Palo Alto Networks Administrator's Guide*.