Integrating Check Point SMS with SolarWinds LEM

Robert Greenwell
Security Engineer
February 1, 2019

Overview:

You can integrate your R80.10 Check Point Security Management Server (SMS) with the SolarWinds Log and Event Manager (LEM) appliance to allow Check Point logs to be stored in the LEM database and shown as normalized alerts in the LEM Console.

Environment:

Check Point SMS with SolarWinds LEM

Configure your Check Point SMS:

Two procedures need to be completed on your SMS. These steps will help you create an OPSEC application that will allow communication between your SMS and the LEM Manager.

Creating the OPSEC application for communication with the LEM Manager

1) Open SmartConsole.
2) In the right hand object bar, click New -> Host…
3) Enter the name and ip address of the LEM Manager. Click OK.
4) Click New -> More -> Server -> OPSEC Application -> Application…
5) Enter a name for the SolarWinds OPSEC application using lower-case characters. For example, enter solarwinds.
6) Next to Host, click the dropdown and select the host object you just created.
7) Under Client Entities, check LEA and SAM. Click OK.
8) Click Publish. From the lefthand dropdown menu, select Install Database.
9) Open the new OPSEC application solarwinds object.
10) Under Secure Internal Communication, click Communication to set the one-time password that will be used to establish trust between your SMS and the LEM Manager.
    a. Enter and confirm a one-time password in the fields provided. Important: Remember this password. It will be used in a later step.
    b. Click Initialize.
    c. If the initialization is successful, the Trust state value changes to *Initialized but trust not established.*
    d. Click Close.

11) Click OK.
12) In the Object Explorer window, double click the application you just created to edit it.
13) Under Secure Internal Communication, copy the value in the DN field. This value will be used to configure the LEM Manager to communicate with your SMS.

Locating the DN for your SMS

1) SSH to your SMS.
2) In Clish, run the command: cpca_client lscert -kind SIC
3) Note the value next to Subject that begins with CN=cp_mgmt.
   For example: CN=cp_mgmt,O=example-mgmt..pdaeyz
4) Exit

Note: If you cannot complete this entire procedure at one time, save the password, OPSEC application DN, and SMS DN noted above in a text document for future reference.

Pulling the Check Point security Certificate:

Note: This procedure uses the opsec_pull_cert command, which can be found with your SMS when logged in as Expert mode.

1) SSH to your SMS.
2) From Clish, enter the command: expert
3) Enter the password for expert mode. If necessary, create an expert password with the command: set expert-password
4) Enter the following command at the command line: /opt/CPrt-R80/log_indexer/opsec_pull_cert –h host -n name -p password [-o output file]
   where:
   - folder is the folder identified in Step 1.
   - host is the hostname of the firewall or management station you used to create the OPSEC application above.
   - name is the name you provided to the SolarWinds OPSEC application in Step 4 above.
   - password is the password you provided in Step 7 above.
   - If you are performing this function on the Check Point SMS, you can use:
     - localhost
     - output file (optional) is the folder and file name for the certificate generated by the executable. By default, the executable exports the file to opsec.p12.

Configure the LEM Manager:

This section contains a procedure that you will complete in your LEM Console to configure the connector needed by your LEM Manager to process the log data it collects from your Check Point SMS.

To configure the Check Point connector for your LEM Manager:

1) Open your LEM Console and log into your LEM Manager.
2) In the Manage > Appliances view, click the Manager gear icon and select Connectors.

3) In the Tool Configuration window, enter Check Point in the search box under Refine Results.
4) Select the OPSEC™ / Check Point™ NG LEA Client connector, and then click Connectors gear icon > New.
5) Configure the connector with the following values.
   - **Alias:** Enter a custom Connector Alias or accept the default.
   - **OPSEC Server:** Enter the IP address of your Check Point SMS.
   - **Auth Port:** Enter the LEA port for your Check Point SMS. The default port is18184, and is provided.
   - **Server DN:** Enter your Check Point SMS DN, which you noted in Step 3 above.
     Note: You must use the DN for your Check Point SMS here, and the value must use only lower case letters. The default value will not work and your LEM Manager will not accept capital letters.
   - **NG SSL CA:** Click Browse (...) and open the certificate you saved above. The default file name is opsec.p12.
   - **Client DN:** Enter your OPSEC application's DN, which you noted in Step 10 above.
     Note: You must use the DN for your LEM OPSEC application here, which is case sensitive. The default value will not work.
   - Leave the remaining values at their default unless your LEM implementation warrants otherwise.
6) Click Save.
7) Next to the connector you just configured, click Connector gear icon > Start. When the connector starts properly, the Status icon turns green.

You will now begin to see alerts from your Check Point firewall in your LEM Console. You can use the default Firewall filter as long as the Connector Alias defined in Step 5 contains the word firewall.

Create a Rule in Check Point Policy:

1) In Smart Console, click on Security Policies and then click Policy under Access Control.
2) Create a new rule.
3) Set Source as LEM node.
4) Set Destination as Check Point SMS
5) Add the following services:
   - FW1_lea
   - FW1_pull_cert
   - FW1_sam
6) Click Install Policy to install the policy.

References:
SolarWinds LEM Admin Guide
SolarWinds knowledgebase

