Integrating Slack and Palo Alto Networks firewalls

For access to live Palo Alto Networks lab boxes, go to:
https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

Overview

Sun Management is a Palo Alto Networks Partner, Palo Alto Networks Certified Services Partner, and Palo Alto Networks Authorized Training Center. Our Engineers have designed and installed over $100M in Palo Alto Firewall Security since 2009. As a Palo Alto Networks Authorized Training Center we have trained over 2000 students on effective utilization of the Palo Alto Networks Firewall. As such, we aim to provide continuous access to on-going training for our existing clients, potential clients and any other individual interested in further develop of their engineering skills with Palo Alto Networks Firewalls.

As organizations move from email to Slack there are opportunities to leverage Slack to receive high-priority notifications from your Palo Alto Networks firewalls (or Panorama). In this walk through I'll show you how easy it is to set that up in Slack and on your Palo Alto Networks firewall and to tailor the alerts to what is important to and urgent for your organization.

The Scenario

You want to team members to get notification in Slack for certain alerts from your firewall. The alerts forwarded to Slack are defined in a filter (or multiple filters) on the firewall, tailored to the requirements of your organization. Examples include threat log entries with severity critical; wildfire submissions with verdict malicious; or configuration or system log entries of particular interest.

Using Slack with targeted notification from Palo Alto Networks firewalls provides a way to reduce alert fatigue while keeping your team informed about relevant critical alerts.

Prep work in Slack

In Slack you need an app, then in the app you are going to add a webhook. This gives you a webhook URL in a format like:

https://hooks.slack.com/services/T01HCxxxxxxxxxxxxx/B01H6xxxxxxxx/Aj8j3J0Vxxxxxxxxxxxxxxxx

You need that webhook URL for the channel or channels you want to post in, and the app is tied to the channel.

See the link in the resources section for instructions about configuring Slack.

On the Palo Alto Networks firewall

High level steps on the firewall for notification for Wildfire malicious events:
1. Setup the HTTP server profile
2. Configure a log forwarding profile
3. Add the log forwarding profile to security policies
4. Commit your changes

paloalto NETWORKS® E L I T E AUTHORIZED TRAINING CENTER

sun mgt Rising Technologies

paloalto NETWORKS CPSP

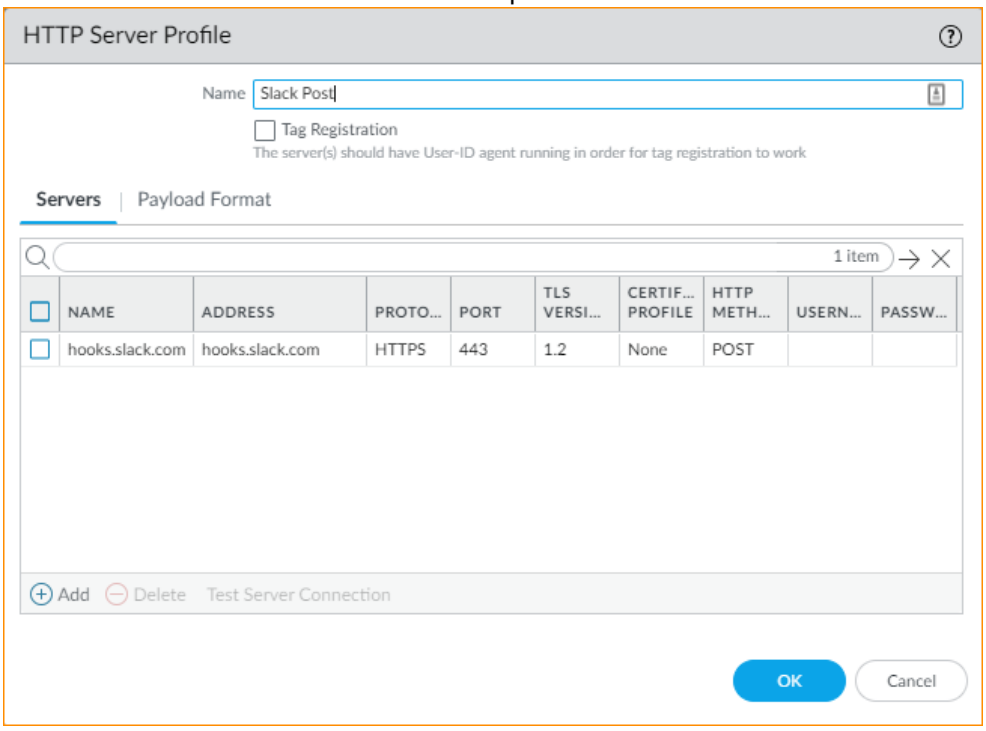
5. Revise formatting and query as needed until it is what you want

Step by step on the firewall for Wildfire malicious event notification:

1. Setup the HTTP server profile. Go to Device > Server Profiles > HTTP and click Add.
   a. Use the dialog to create a new profile named Slack Post
   b. Click Add at bottom to add a new server, using the info below:

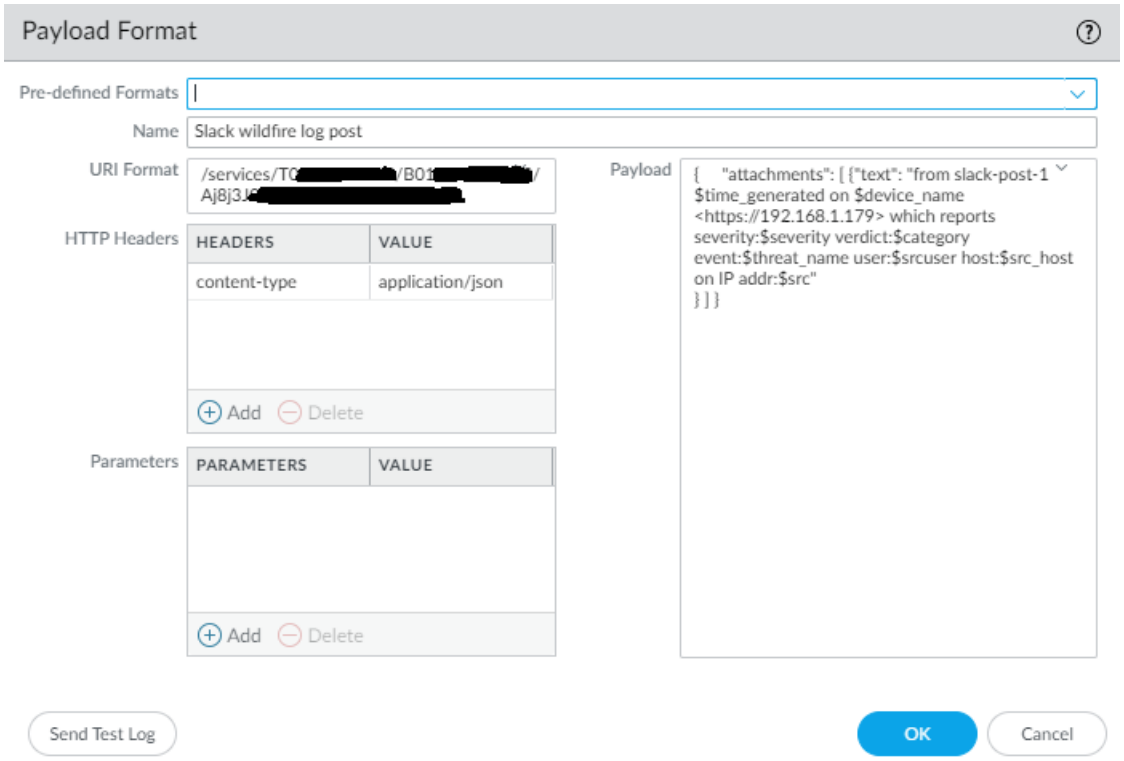
   Name: hooks.slack.com
   Address: hooks.slack.com
   Protocol: HTTPS
   Port 443
   TLS 1.2
   Certificate profile: none
   HTTP method: POST

   Here is what it looks like once that profile is created and the server is added:



   c. Next, go to the Payload Format tab

paloalto NETWORKS ELITE AUTHORIZED TRAINING CENTER
sun mgt Rising Technologies
paloalto NETWORKS CPSP



For Wildfire log, click on Wildfire and use these settings

Name: Slack Wildfire log post

URI Format: /services/the rest of your webhook URL from Slack

HTTP Headers:

Headers: content-type

Value: application/json

No Parameters

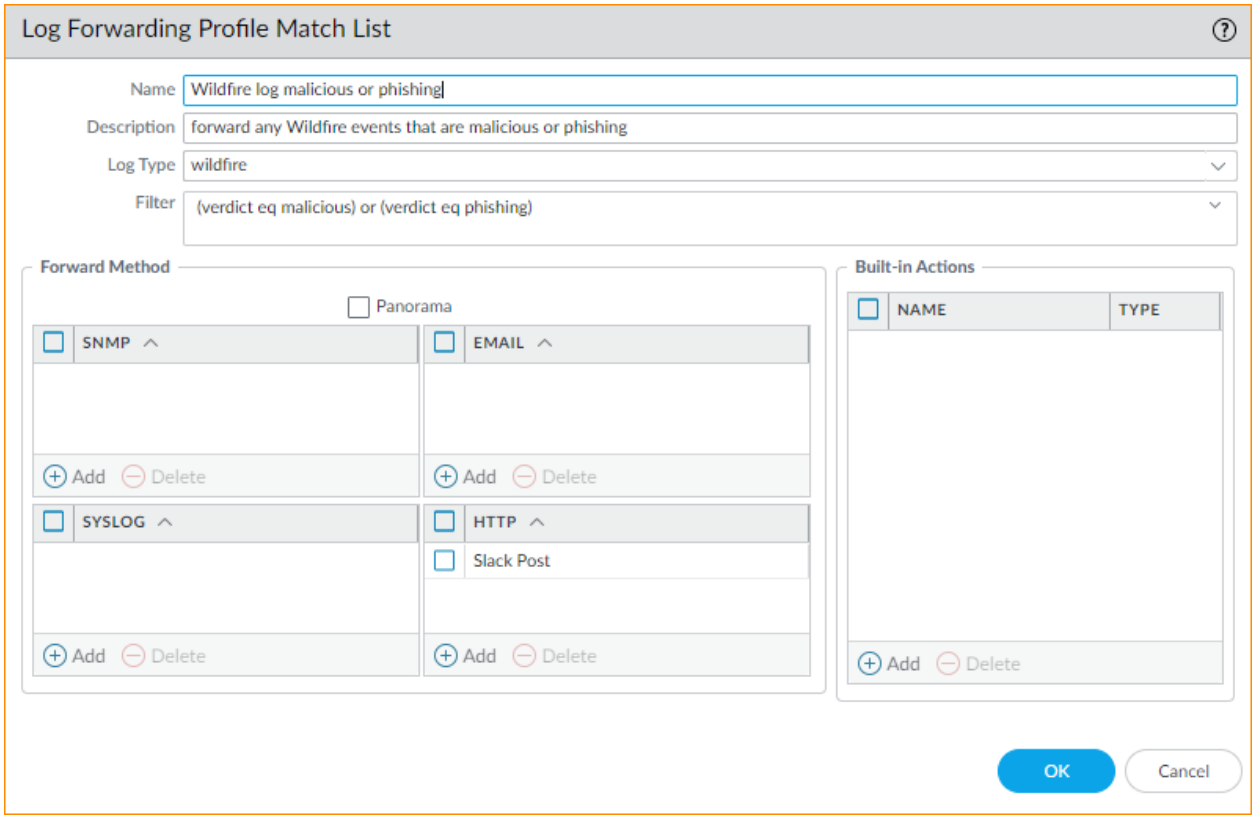
For Payload, start with what is shown below, and modify as needed after testing, depending on your environment. Use the management IP address for your firewall in place of 192.168.1.179 shown below.

{ "attachments": [{"text": "$time_generated on $device_name <https://192.168.1.179> which reports severity:$severity verdict:$category event:$threat_name user:$srcuser host:$src_host on IP addr:$src" }] }

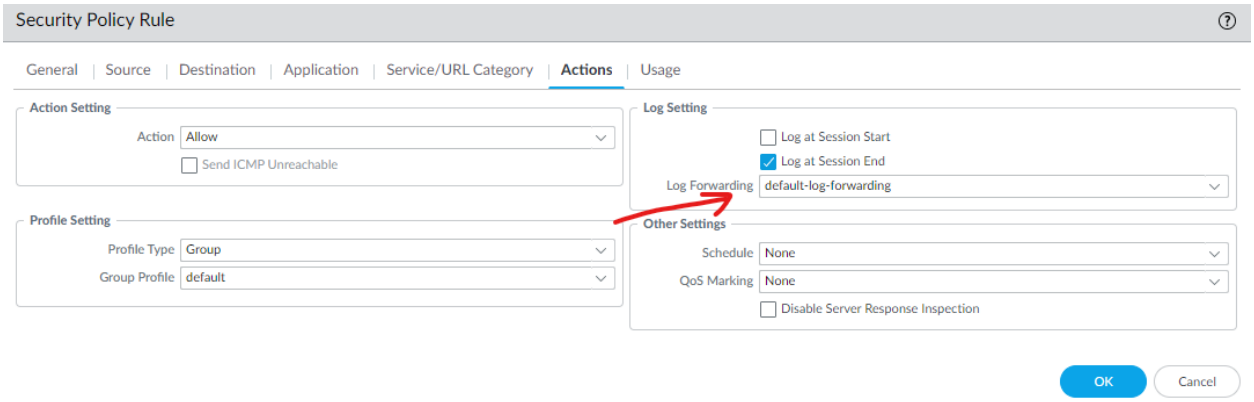
Press OK twice to save changes and exit config dialog.

d. Open the HTTP Server profile, then on the second tab, go into the Slack Wildfire Log post and use the Send Test Log button to see if it can submit to Slack. You should see it in your Slack channel.
e. If you do not see in your Slack channel check the traffic log to see if you have denied traffic from the firewall management interface (by default, or from specified interface if using service routes). Hint: view the traffic log using the filter “(app eq slack-base) and (addr.src in <your firewall mgmt. port IP Address>)” to see those submissions.
f. Once the test post shows in Slack, proceed with next step.

2. Configure a Log forwarding profile. Go to Objects > Log Forwarding, create new or edit an existing profile.
    a. In the profile, click Add at bottom and use these settings:
    Name: Wildfire log malicious or phishing <or whatever is descriptive for your setup>
    Description: forward any wildfire events that are malicious or phishing
    Log type: wildfire
    Filter: (verdict eq malicious) or (verdict eq phishing) <or whatever is appropriate for your organization>
    Forward method: Slack Post
    Click OK twice to save changes



3. Add the log forward profile to Security Policies if this is a new Log Forwarding profile
    a. Under Policies > Security open each security policy
    b. On the Actions tab, select the log forwarding profile you just created
    c. If required by your organizational policies add an audit comment on the General tab
    d. Click OK to save changes



4. Commit your changes
5. Test and revise as needed to generate notifications for the events you want to see in Slack, and to provide useful information in the body of the notification.

The example above is for notification from the Wildfire log. If you want to get notified for Threat log events you would use the same process with different payload formatting. If you want to get notified for configuration or system events (e.g., HA failover, Commit) you would change step 2 above. Instead of going to Objects > Log Forwarding, you would go to Device > Log settings and configure a filter for the interesting events to be sent to the Server Profile created in step 1. For configuration and system log forwarding you do not have to do step 3 (attach forwarding profile to a security policy). You still would commit (step 4) and test/revise (step 5).

Next Steps

If you want to implement this in your environment and would be more comfortable having someone with experience help you in the process, contact your Sun Management account rep to schedule one of our certified Palo Alto Networks engineers to assist with setting up notification from the firewalls into Slack.

If you want to test this on your own and do not have access to a lab environment to do so, contact your Sun Management account rep to get pricing on a lab bundle. The PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

Sun Management

Sun Management is a Value Added Reseller (VAR) focusing on Network and Internetwork Security Requirements. We work primarily in the Mid Atlantic area: Maryland (MD), Virginia (VA), District of Columbia (DC), West Virginia (WV), Delaware (DE) and Pennsylvania (PA). Our credentials include Palo Alto Networks Services Provider, Palo Alto Networks Certified Training Partner, and Palo Alto Networks Certified Managed Security Service Provider (MSSP) using CORTEX XSOAR in a multi-tenant environment.

We address requirements concerning Network Detection and Response (NDR); internal and external TLS and SSL requirements for complete data visibility; End Point Detection and Response (EDR); Gramm Leach Bliley Act, HIPPA, Sarbanes Oaxley and PCI DSS; penetration testing and firewall optimization; and Data Protection by tracking all Data Flows within the network, across applications, between users/servers and in the cloud. Contact us at (888) 773-9422 to setup a POC or if you just want more

paloalto NETWORKS® E L I T E AUTHORIZED TRAINING CENTER

sun mgt Rising Technologies

paloalto NETWORKS CPSP

Resource Links

https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack
https://live.paloaltonetworks.com/t5/log-forwarding-articles/pan-os-8-0-http-log-integration-with-slack/ta-p/172093
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/monitoring/forward-logs-to-an-https-destination.html
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFfCAK

paloalto NETWORKS® E L I T E AUTHORIZED TRAINING CENTER
sun mgt Rising Technologies
paloalto NETWORKS CPSP