Palo Alto Monitoring

Enable Rule Hit Count Columns:

- https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-firewalls/device-monitoring-on-panorama/monitor-policy-rule-usage
- https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/rule-usage-query

1. Requirements: >= PA 8.1
    a. Step by step walkthrough for updating: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/upgrade-to-pan-os-81/upgrade-the-firewall-to-pan-os-81/upgrade-a-firewall-to-pan-os-81.html
    b. Device -> Software -> Check Now
    c. Download newer version
    d. Activate downloaded software
    e. If the above doesn't work:
        i. https://github.com/PaloAltoNetworks/iron-skillet/wiki/PAN-OS-8.0-and-8.1
        ii. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CloaCAC
2. Enable rule: Device -> Setup -> Management -> General Settings -> Gear Icon
    a. Check the box for Policy Rule Hit Count
3. Enable column: Policies -> Drop Down Arrow on a Column -> Columns
    a. Check the boxes for:
        i. Rule Usage Hit Count
        ii. Rule Usage First Hit
        iii. Rule Usage Last Hit

Workaround 1 for Rule Hit Count if PA can't be >=8.1:

- Export logs as CSV: Monitor -> Logs -> Traffic
    - Go to the right side of the search bar, click the excel button, click download
    - If it's not exporting enough logs, see https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClaPCAS

#rulehitcounter.py

```
import csv
import collections as c
m = []
r = csv.reader(open('log.csv','r'))
next(r) #skip headers
for z in r:
    m.append(z[11])
print(c.Counter(m))
```

README

- This script can be run on Windows or Linux
- It can be run with either Python 2 or Python 3

- Either run this in the same directory as you downloaded the log.csv file to or edit the file path in the script
- If you want to use this to filter/count a different PA csv log file, change the z[11] part of the script to be z[whatever].

DON'T FORGET TO COMMIT

Workaround 2 for Rule Hit Count if PA can't be >=8.1:

- https://live.paloaltonetworks.com/t5/General-Topics/Show-hit-count-in-CLI/td-p/68530?lightbox-message-images-68606=1332iEA0668657F5F4B4E
- sitweak.wordpress.com/2012/07/27/workaround-policy-hit-counter-on-paloalto-firewalls/

Show Active Sessions:

- https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/monitor/monitor-logs.html#73873
- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CluBCAS

Monitor -> Session Browser

1. For filtering the results on this page, see the first link above.
2. Remember that RDP / SSH may have spun up multiple sessions...*thoroughly* kill.
3. For CLI, see the second link above.

CLI Error Messages:

```
tail follow yes mp-log ms.log
tail follow yes mp-log paninstaller_content.log
```

Other Helpful Resources:

- Monitor -> Logs
- Monitor -> App Scope
- https://securelink.net/en-be/insights/4-palo-alto-networks-tools-you-have-to-discover/
- https://github.com/cpainchaud/pan-configurator

DON'T FORGET TO COMMIT