Cisco: Adaptive Security Appliance

Cisco Adaptive Security Appliance (ASA) logs combine firewall, antivirus, intrusion prevention, and virtual private network (VPN) data. The logs provide data for the following devices and solutions: firewall, antivirus, antispam, intrusion detection, intrusion prevention, VPN devices, SSL devices, and content inspection. They provide information about proactive threat defense efforts that stop attacks before they spread through networks, both large and small. Cisco ASA software also integrates with other critical security technologies to deliver comprehensive solutions that meet continuously evolving security needs. This includes multi-site and multi-node clustering, high availability, context awareness, dynamic routing and site-to-site VPN, and unified communications.

Configuration

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Recommended index: netfw
- Source type: cisco:asa, cisco:fws, and cisco:pix
- Input type: var/log/rsyslog/cisco/asa/*.log
- Add-on or app: Splunk Add-on for Cisco ASA
- Sizing estimate: The volume depends on the size of your ASA device. It can be +/- 10MB/day for a branch office to north of 50 GB/day for a main datacenter cluster. The following estimates are predicated on logging configuration of "level 6 (informational)."
  - Edge firewall: Negligible
  - Zone-based firewall: 230 bytes per event
  - VPN Services: 10 kb per session, plus firewall activity
  - Operational: Variable, but typically < 200 MB per day, per Cisco ASA

Using only Cisco's built-in tools, the show ip inspect statistics command will tell you how many connections there have been since last reset. So, one way of estimating event volume is to check that number at the same time on subsequent days and then calculate the number of connections you typically see per day. When multiplied by the general 230 byte number, you will get a reasonable expectation for data size.

Validation

After the daemon is restarted and traffic is sent to rsyslog, you should see this directory created: /var/logs/rsyslog/cisco/asa/
Data application

When your Splunk deployment is ingesting Cisco ASA logs, you can use the data to achieve the following:

- Managing firewall rules
- Complying with General Data Privacy Regulation
- Monitoring for network traffic volume outliers