Installation

Installation Requirements

The VM has the following resource requirements:
2 virtual CPU cores
4GB of RAM
20GB of storage space
Note that these requirements may have to be increased depending on configuration but we expect this to be adequate for most sites. It is also entirely possible to deploy the individual components of the appliance on bare metal or another VM of your choice.

The VM is required to run Ubuntu 16 LTS. Note that Ubuntu 18 is not currently supported. CentOS 7 is tentatively supported.

Networking Requirements

The SDAIA security appliance is designed to be deployed on a campus network perimeter or DMZ. While the target user base are open science networks that employ the Science DMZ model, the appliance can be deployed in any number of suitable locations. It's primary purpose is to be "visible" to outside attackers and collect intelligence on their activities, whether they be automated or targeted. To that end we recommend that the appliance have large number of allocated but unused IPs routed to it. This allows the appliance's "honeypot" capabilities to react and gather data from illegitimate activity. Alternatively, the appliance's honeypot can be assign IPs individually up to 32 (which hits a Linux kernel limit)–although typically this kind of network setup only uses 2 or 3 interfaces for the honeypot.

Firewall Requirements

TCP ports needed:

1. 5670 for the gateway process
2. 22 for the SSH honeypot
3. 1100 for the sshd management process

Installation Steps

1. Check out SDAIA repo from git.
    a. `git clone https://git.ncsa.illinois.edu/awithers/sdaia`

    b. Verify gateway binary (public key):
        i. `cd sdaia; gpg --verify gateway.s/gateway.sig gateway.s/gateway`

2. Run ansible playbook.
    a. cd sdaia; ./install.sh
    b. note that install.sh just runs the ansible playbook locally.
3. Check installation:
    a. The following commands will check that zyre gateway, CIF, Bro IDS and honeypot (if installed) are running:
        i. systemctl status zyre-gateway
        ii. `systemctl status csirtg-cef-zmq`

        iii. `ps ax | grep bro`

        iv. `docker ps`

4. Add key to NCSA's key repo.
    a. A public key is generated in /usr/local/gateway/client.key. This key needs to be shared in order for your deployment to join the network. You can add the key to https://github.com/ncsa/sdaiakeys with a pull request. Please email alexw1@illinois.edu or jazoff@illinois.edu for further instructions.