Capirca howto

> *Capirca is a tool designed to utilize common definitions of networks, services and high-level policy files to facilitate the development and manipulation of network access control lists (ACLs) for various platforms. It was developed by Google for internal use, and is now open source.*

https://github.com/google/capirca

Installation

There's several ways to install and run capirca, via docker or using python venv for example.

This example shows installation using python venv:

1. Install python and python-venv
2. Create a new venv: venv capirca
3. Activate venv: cd capirca ; source bin/activate
4. Clone capirca github repo: git clone https://github.com/google/capirca.git
5. cd capirca
6. pip install -r requirements.txt
7. cd ..
8. mkdir mypolicies
9. cd mypolicies
10. Create directories and files:

```
.
 def
    NETWORK.net
    SERVICES.svc
 policies
     includes
        untrusted-networks-blocking.inc
     pol
         arista_test1.pol
```

Example files:

$ cat def/NETWORK.net

```
#
# Sample naming defintions for network objects
#
RFC1918 = 10.0.0.0/8      # non-public
          172.16.0.0/12   # non-public
          192.168.0.0/16  # non-public
```

$ cat policies/pol/arista_test1.pol

```
header {
  comment:: "Server network ingress ACL to be applied to gateway vlan interface"
  target:: arista servernet-in
}

term accept-dhcp {
  comment:: "Optional - allow forwarding of DHCP requests."
  destination-port:: DHCP
  protocol:: udp
  action:: accept
}

term accept-to-dns {
  comment:: "Allow name resolution"
  destination-address:: OFFICE_NETS
  source-port:: DNS
  protocol:: udp
  action:: accept
}

term accept-tcp-replies {
  comment:: "Allow tcp replies to internal hosts."
  destination-address:: OFFICE_NETS
  protocol:: tcp
  option:: tcp-established
  action:: accept
}

term deny-to-internal {
  comment:: "Deny access to rfc1918/internal."
  destination-address:: INTERNAL
  action:: deny
}

term deny-to-bogons {
  comment:: "Deny access to bogons"
  destination-address:: BOGON
  action:: deny
  expiration:: 2019-10-01
}

term default-permit {
  comment:: "Allow what's left (internet)"
  action:: accept
}
```

Run "aclgen" from mypolicies directory and a new file called arista_test1.pol will appear in the directory. This file can be included in a Jinja2 template for example.

Todo

Match netflow data with policy definitions to see what policies actually get hits from traffic.