Flow Shunting

Flow shunting with Arista switches requires two components; the react module and a dumbno server instance. This is a decent explanation of what needs to happen: http://mailman.icsi.berkeley.edu/pipermail/zeek/2017-July/012353.html

The dumbno server needs to run on a server that can access the Arista API.

Adding the react module to Bro

Clone Justin Azoff's bro react repo and add it to the Bro site directory.

https://github.com/JustinAzoff/bro-react

In /usr/local/bro/share/bro/site/local.bro, load the react framework and the bulk connection script.

local.bro

```
@load conn-bulk.bro
@load react
```

Configuring and running Dumbno server

Download dumbno from the dumbno repo.

https://github.com/ncsa/dumbno

Edit the configuration file to talk to the API on the Arista switch. We are applying a single incoming ACL named "bulk_1" on a port-channel that includes all taps. The egress ports section is used in the "stats" function of dumbno to gather traffic statistics.

dumbno.cfg

```
[switch]
scheme = https
ip = <ip of arista device>
user = admin
password = <password>

[ports]
Port-Channel1 = bulk_1

[egress_ports]
Port-Channel10 = tool1
```

Set up the ACLs on the switch (only needs to be done once)

```
PYTHONHTTPSVERIFY=0 python dumbno.py dumbno.cfg setup
```

Start dumbno

```
PYTHONHTTPSVERIFY=0 python dumbno.py dumbno.cfg
```

Dumbno provides a log file at /var/log/dumbno.log which can be used to monitor ACL changes.

Start dumbno stats monitor

```
PYTHONHTTPSVERIFY=0 python dumbno.py dumbno.cfg stats
```

A log file is generated at /var/log/dumbno.stats which gives information about ingress, egress and amount of traffic filtered by the dumbno ACL.

Python had some trouble verifying the certificate we used, even though it was signed by a trusted CA. PYTHONHTTPSVERIFY=0 disables the certificate verification.

Redefining variables in Bro

From base/protocols/ftp/gridftp.bro, the number of bytes transferred before guessing a connection is a GridFTP data channel is originally set to 1 GB.

```
const size_threshold = 1073741824 &redef;
```

This can be changed to 2 MB in local.bro, along with the size_threshold for identifying bulk flows.

```
redef GridFTP::size_threshold = 1048576; # 2 MB
redef Bulk::size_threshold = 134217728 ; # 128 MB
```