Bro Clusters
• Someone here is analyzing 7Gbps of mixed traffic with Bro.
  • With everything turned on!
• Bro is single threaded.
• Difficult to adapt multithreading into code base as it is.
• Conceptually Bro is very parallelizable but we aren’t taking the bruteforce approach to adding multithreading.
  • This is a topic for a different time.
• Initially implemented as Bro scripts and all nodes needed to be started manually.

• BroControl was originally called “Bro Cluster Shell” and contained all of the Bro script support for clusters but automated the tedium.

• 2.0 introduces the cluster framework which is more abstraction of all previous work and ideas.
Cluster Layout

- Set of Bro processes acting as a single entity.
- Split Bro functionality across node types.
  - Manager
  - Proxies
  - Workers
Manager

• Receives logs

• Handles notices
Proxy

- Synchronizes limited state information across workers.
- For example: active local IP addresses
- Does not examine packets.
Worker

- Sniffs traffic
- Performs protocol analysis
- Generally, most of the heavy lifting
Frontend

• Not a Bro process!
Bidirectional Flow Load Balancing

- Turn a large “pipe” into many bundles of sessions.
- Most common balancing is 4- or 5-tuple
  - 4-tuple - SRC_IP+SRC_PORT+DST_IP+DST_PORT
  - 5-tuple - SRC_IP+SRC_PORT+DST_IP+DST_PORT+PROTO
- Network based balancing.
- Host base balancing.
• Cluster layout specification.
• Easy management and control of large numbers of processes on large numbers of physical hosts.
BroControl in “standalone” mode

node.cfg

[bro]
type=standalone
host=localhost
interface=en1
BroControl in “cluster” mode

**node.cfg**

[manager]
type=manager
host=192.168.1.72

[proxy-1]
type=proxy
host=192.168.1.72

[worker-1]
type=worker
host=192.168.1.72
interface=eth0

[worker-2]
type=worker
host=192.168.1.72
interface=eth1
$ sudo /bro/bin/broctl
Password:

Welcome to BroControl 0.41-128

Type "help" for help.

[BroControl] >
[BroControl] > check
manager is ok.
proxy-1 is ok.
worker-1 is ok.
worker-2 is ok.
[BroControl] > install
removing old policies in /usr/local/bro/spool/policy/site ... done.
removing old policies in /usr/local/bro/spool/policy/auto ... done.
creating policy directories ... done.
installing site policies ... done.
generating cluster-layout.bro ... done.
generating local-networks.bro ... done.
generating broctl-config.bro ... done.
updating nodes ... done.
[BroControl] > start
starting manager ...
starting proxy-1 ...
starting worker-1 ...
starting worker-2 ...
BroControl Version 0.41-128

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capstats &lt;nodes&gt; [secs]</td>
<td>report interface statistics (needs capstats)</td>
</tr>
<tr>
<td>check &lt;nodes&gt;</td>
<td>check configuration before installing it</td>
</tr>
<tr>
<td>cleanup [--all] &lt;nodes&gt;</td>
<td>delete working dirs on nodes (flushes state)</td>
</tr>
<tr>
<td>config</td>
<td>print broctl configuration</td>
</tr>
<tr>
<td>cron</td>
<td>perform jobs intended to run from cron</td>
</tr>
<tr>
<td>cron enable</td>
<td>disable</td>
</tr>
<tr>
<td>df</td>
<td>print nodes' current disk usage</td>
</tr>
<tr>
<td>diag &lt;nodes&gt;</td>
<td>output diagnostics for nodes</td>
</tr>
<tr>
<td>exec &lt;shell cmd&gt;</td>
<td>execute shell command on all nodes</td>
</tr>
<tr>
<td>exit</td>
<td>exit shell</td>
</tr>
<tr>
<td>install</td>
<td>update broctl installation/configuration</td>
</tr>
<tr>
<td>netstats</td>
<td>print nodes' current packet counters</td>
</tr>
<tr>
<td>nodes</td>
<td>print node configuration</td>
</tr>
<tr>
<td>print &lt;id&gt; &lt;nodes&gt;</td>
<td>print current values of script variable at nodes</td>
</tr>
<tr>
<td>peerstatus &lt;nodes&gt;</td>
<td>print current status of nodes' remote connections</td>
</tr>
<tr>
<td>process &lt;trace&gt; [Bro options]</td>
<td>runs Bro offline on trace file</td>
</tr>
<tr>
<td>quit</td>
<td>exit shell</td>
</tr>
<tr>
<td>restart [--clean] &lt;nodes&gt;</td>
<td>stop and then restart processing</td>
</tr>
<tr>
<td>scripts [-p]-c &lt;nodes&gt;</td>
<td>Lists the Bro scripts the nodes will be loading</td>
</tr>
<tr>
<td>start &lt;nodes&gt;</td>
<td>start processing</td>
</tr>
<tr>
<td>status &lt;nodes&gt;</td>
<td>summarize node status</td>
</tr>
<tr>
<td>stop &lt;nodes&gt;</td>
<td>stop processing</td>
</tr>
<tr>
<td>update &lt;nodes&gt;</td>
<td>update configuration of nodes on the fly</td>
</tr>
<tr>
<td>top &lt;nodes&gt;</td>
<td>show Bro processes ala top</td>
</tr>
</tbody>
</table>

Commands provided by plugins:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ps.bro [&lt;nodes&gt;]</td>
<td>Shows Bro processes currently running on nodes' systems.</td>
</tr>
</tbody>
</table>