



Bro Clusters

Bro Workshop 2011
NCSA, Urbana-Champaign, IL



Bro Workshop 2011

-
- Someone here is analyzing 7Gbps of mixed traffic with Bro.
 - With everything turned on!

Cluster Purpose

- 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 brute force approach to adding multithreading.
 - This is a topic for a different time.

Cluster Background

- 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 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

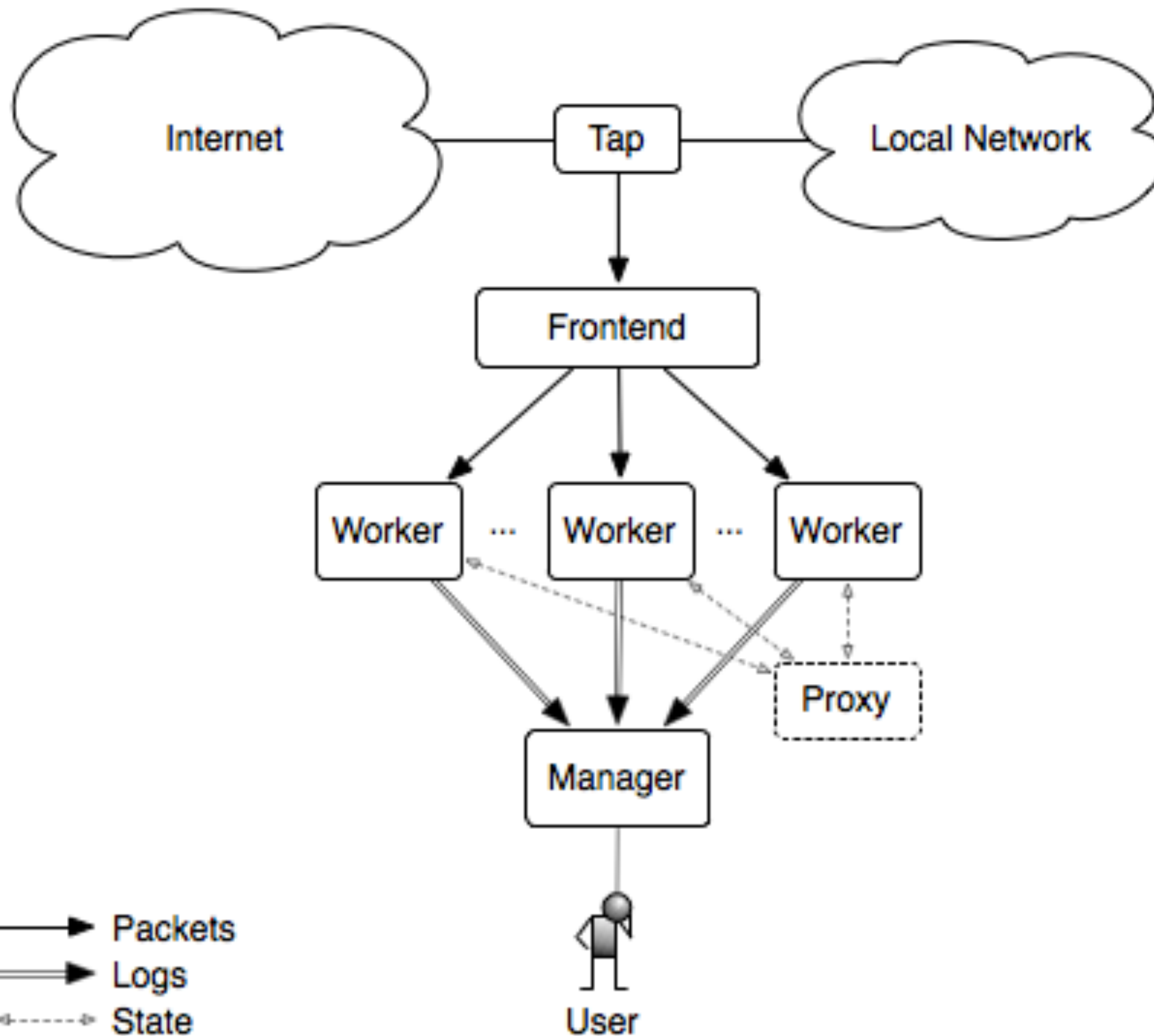
- Sniffs traffic
- Performs protocol analysis
- Generally, most of the heavy lifting

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.



BroControl

- 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=enl
```

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] > ?

BroControl Version 0.41-128

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

Commands provided by plugins:

ps.bro [<nodes>] - Shows Bro processes currently running on nodes' systems.

