Bringing Bro to the Enterprise

Comprehensive Visibility & Response for Every Corner of Your Network

Robin Sommer

International Computer Science Institute, &
Broala, LLC

robin@icsi.berkeley.edu
robin@broala.com

http://www.icir.org/robin

Outline

Bro Overview

A production-quality open-source network monitor.

A Bit of Bro History

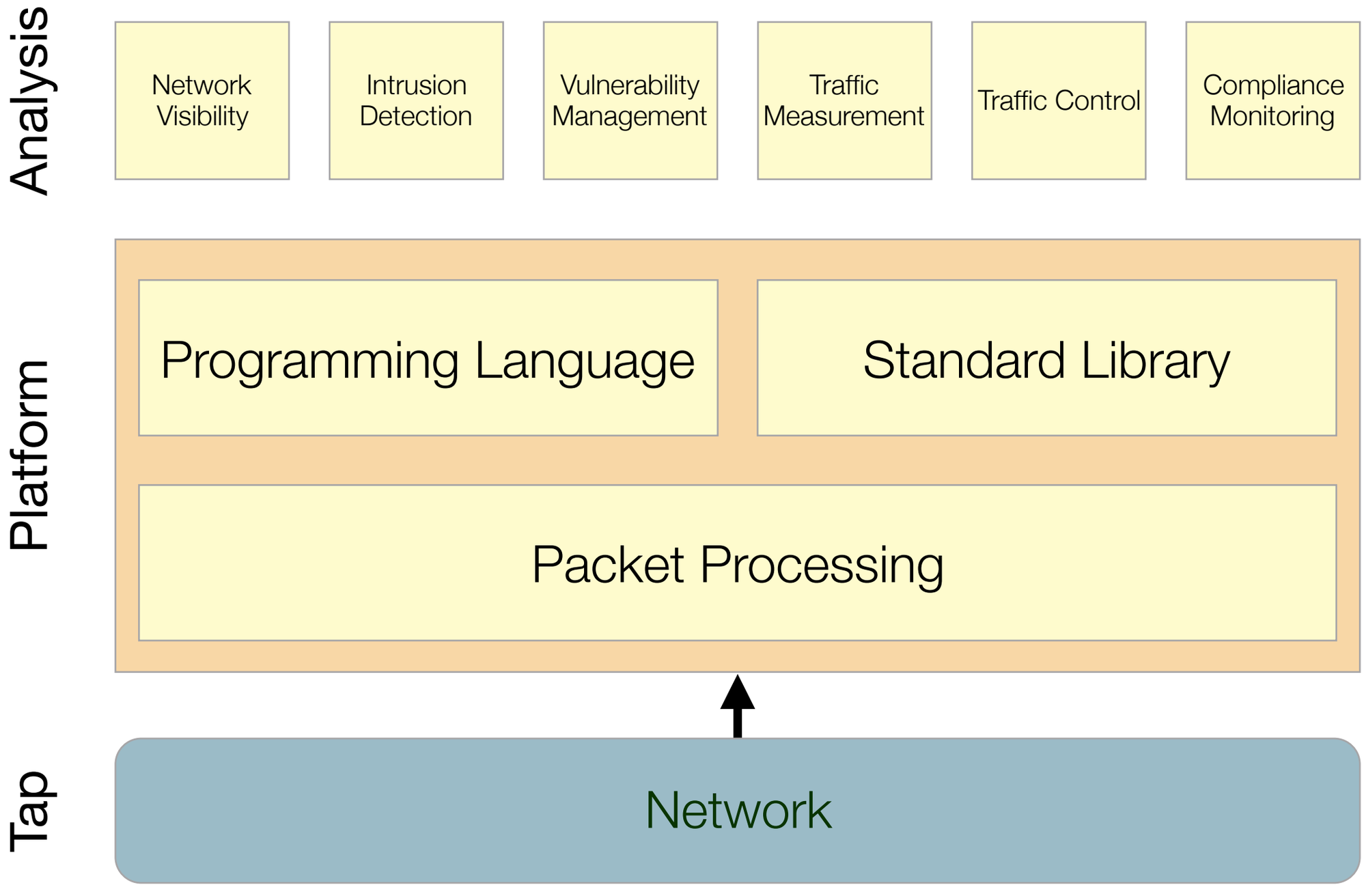
From academic research to enterprise deployment.

Enterprise Solutions

Roadmap for deep visibility and control.

The Bro Platform

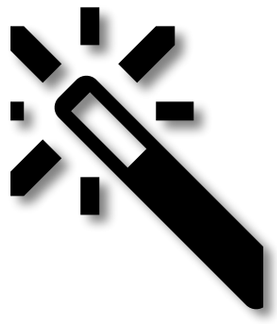
Open Source
BSD License



“What Can It Do?”

Log Files

Alerts



Custom Logic

“Network ground truth”

Bro's Log Files

Rich, structured, real-time activity streams.

Connections Logs

conn.log

ts	1393099415.790834	Timestamp
uid	CSoqsg12YRTsWjYbZc	Unique ID
id.orig_h	2004:b9e5:6596:9876:[…]	Originator IP
id.orig_p	59258	Originator Port
id.resp_h	2b02:178:2fde:bff:[…]	Responder IP
id.resp_p	80	Responder Port
proto	tcp	IP Protocol
service	http	App-layer Protocol
duration	2.105488	Duration
orig_bytes	416	Bytes by Originator
resp_bytes	858	Bytes by Responder
conn_state	SF	TCP state
local_orig	F	Local Originator?
missed_bytes	0	Gaps
history	ShADafF	State History
tunnel_parents	Cneap78AnVWoA1yml	Outer Tunnels

HTTP

http.log

ts	1393099291.589208
uid	CKFUW73bIADw0r9pl
id.orig_h	2a07:f2c0:90:402:41e:c13:6cb:99c
id.orig_p	54352
id.resp_h	2406:fe60:f47::aaeb:98c
id.resp_p	80
method	POST
host	com-services.pandonetworks.com
uri	/soapservices/services/SessionStart
referrer	-
user_agent	Mozilla/4.0 (Windows; U) Pando/2.6.0.8
status_code	200
username	anonymous
password	-
orig_mime_types	application/xml
resp_mime_types	application/xml

SSL

ssl.log

ts	1392805957.927087
uid	CEA05l2D7k0BD9Dda2
id.orig_h	2a07:f2c0:90:402:41e:c13:6cb:99c
id.orig_p	40475
id.resp_h	2406:fe60:f47::aaeb:98c
id.resp_p	443
version	TLSv10
cipher	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
server_name	www.netflix.com
subject	CN=www.netflix.com,OU=Operations, O=Netflix, Inc.,L=Los Gatos, ST=CALIFORNIA,C=US
issuer_subject	CN=VeriSign Class 3 Secure Server CA, OU=VeriSign Trust Network,O=VeriSign, C=US
not_valid_before	1389859200.000000
not_valid_after	1452931199.000000
client_subject	-
client_issuer_subject	-
cert_hash	197cab7c6c92a0b9ac5f37cfb0699268
validation_status	ok

Software

software.log

ts	1392796839.675867
host	10.209.100.2
host_p	-
software_type	HTTP::BROWSER
name	DropboxDesktopClient
version.major	2
version.minor	4
version.minor2	11
version.minor3	-
version.addl	Windows
unparsed_version	DropboxDesktopClient/2.4.11 (Windows; 8; i32; en_US; Trooper 5694-2047-1832-6291-8315)

Files

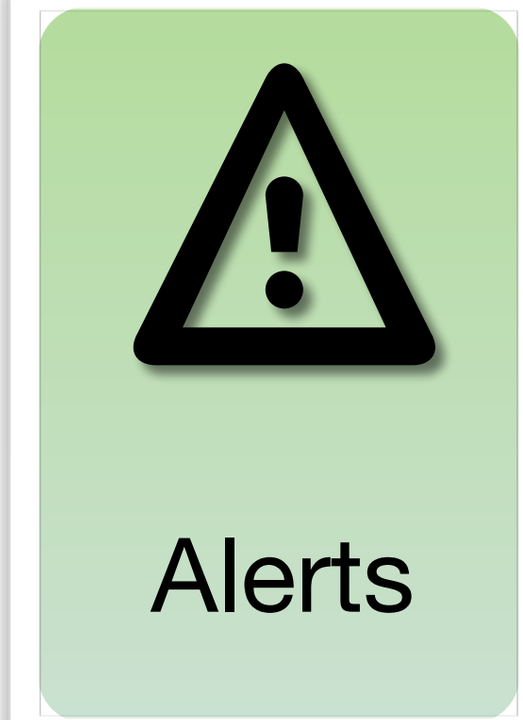
files.log

ts	1392797643.447056
fuid	FnungQ3TI19GahPJP2
tx_hosts	191.168.187.33
rx_hosts	10.1.29.110
conn_uids	CbDgik2fjeKL5qzn55
source	SMTP
analyzers	SHA1,MD5
mime_type	application/x-dosexec
filename	Letter.exe
duration	5.320822
local_orig	T
seen_bytes	39508
md5	93f7f5e7a2096927e06e[…]1085bfcfb
sha1	daed94a5662a920041be[…]a433e501646ef6a03

“What Can It Do?”

Log Files

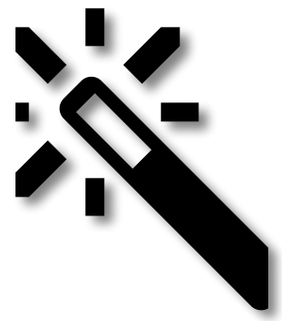
“Network Ground Truth”



Alerts

“Watch this!”

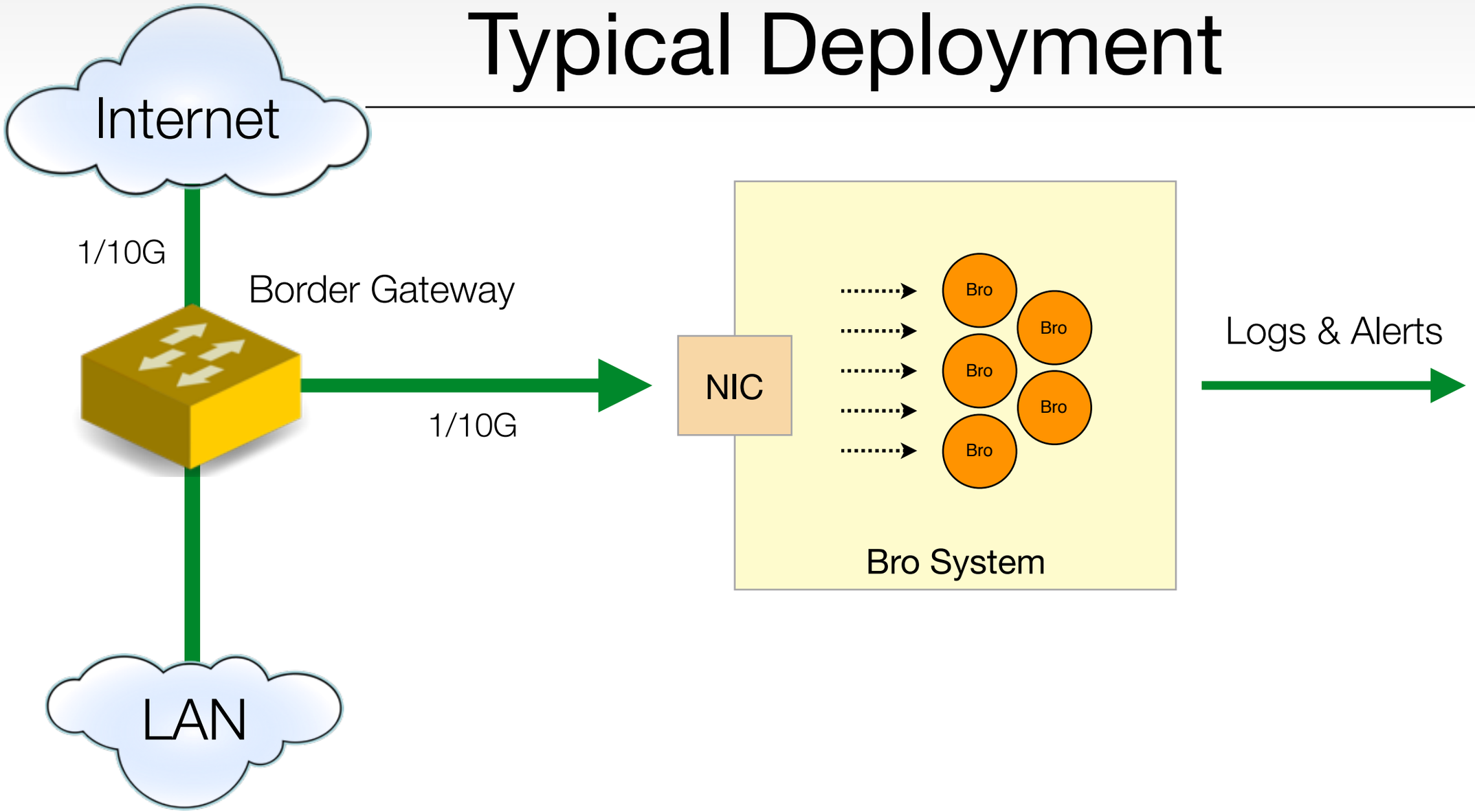
Record & trigger actions



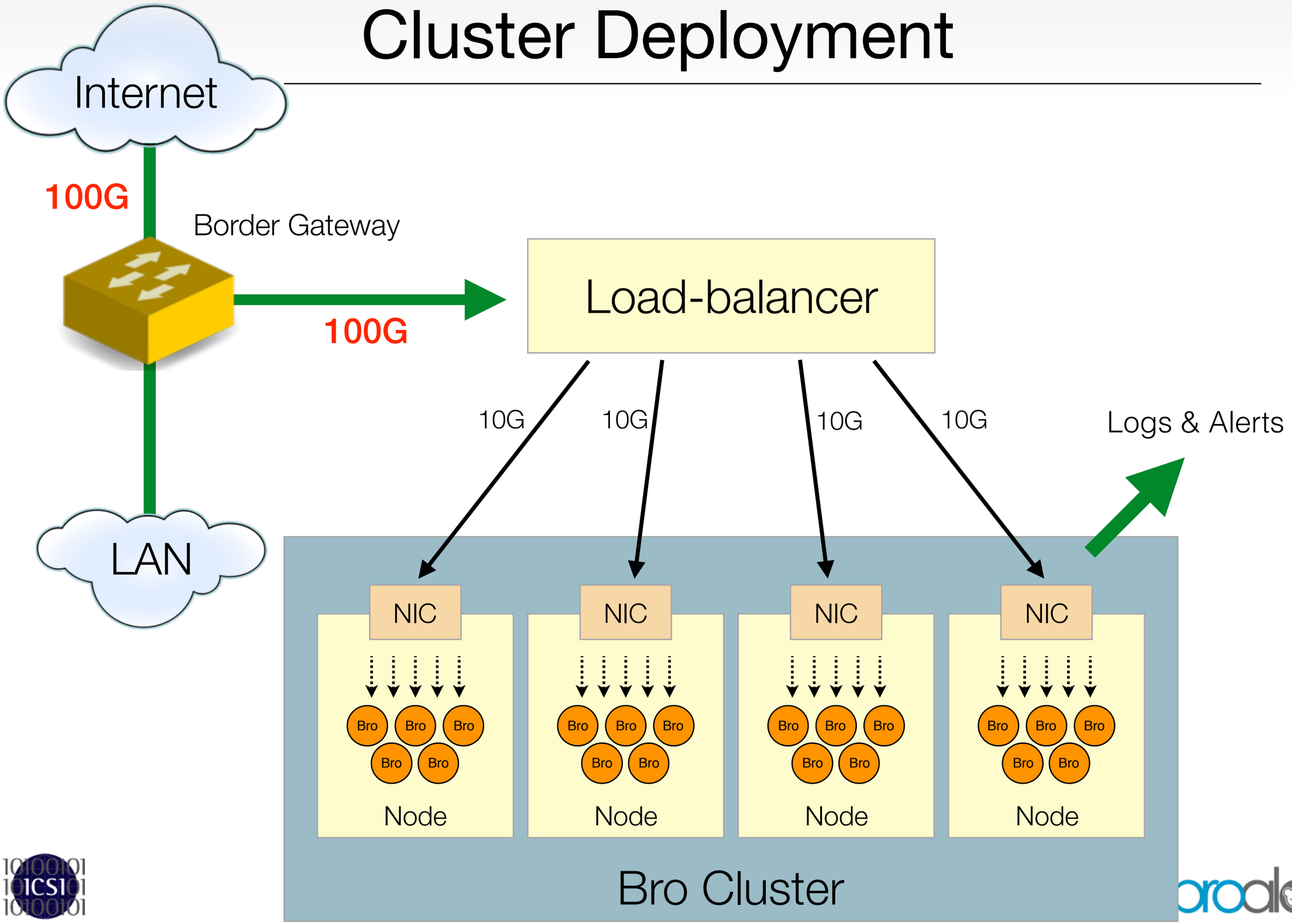
Custom Logic

*“Don’t ask what Bro can do. Ask what **you want** it to do.”*

Typical Deployment



Cluster Deployment



“Who’s Using It?”

Installations across the Country

Universities
Research Labs
Supercomputing Centers
Government Organizations
Fortune 20 Enterprises

Community

50/90/150/180 attendees at BroCon ’12/’13/’14/‘15
110 organizations at BroCon ‘15
4,500 Twitter followers
1,000 mailing list subscribers
100 users average on IRC channel
10,000 direct downloads / version
from 150 countries

Fully integrated into Security Onion

Popular security-oriented Linux distribution

A Bit of Bro History

From Academic Research To Enterprise Deployment

Bro History

Academic Publications

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016

- 1998: USENIX Paper
- 2000: Backdoors, Stepping Stones
- 2003: Anonymizer, Active Mapping, Context Signat.
- 2004: TRW, State Mgmt., Independ. State
- 2005: Host Context, Time Machine, Enterprise Traffic
- 2006: BinPAC, DPD, 2nd Path
- 2007: Bro Cluster, Shunt
- 2008: Autotuning
- 2009: Parallel Prototype
- 2012: Input Framework
- 2013: SSL Trust, Relationships
- 2014: Summary Stats, HILTI, DPI Concurrency, PLC Modeling
- 2015: NetControl, VAST, Tor Traffic

- Vern writes 1st line of code
- LBNL starts using Bro operationally
- v0.2 1st CHANGES entry
- v0.4 HTTP analysis, Scan detector, IP fragments, Linux support
- v0.6 RegExps, Login analysis
- v0.7a48 Consistent CHANGES
- v0.7a90 Profiling, State Mgmt
- v0.7a175/0.8aX Signatures, SMTP, IPv6 support, User manual
- 0.8a37 Communication, Persistence, Namespaces, Log Rotation
- v0.8aX/0.9aX SSL/SMB, STABLE releases, BroLite
- v1.0 BinPAC, IRC/RPC analyzers, 64-bit support, Sane version numbers
- v1.1/v1.2 *when* Stmt, Resource tuning, Broccoli, DPD
- v1.3 Ctor expressions, GeoIP, Conn Compressor
- v1.4 DHCP/BitTorrent, HTTP entities, NetFlow, Bro Lite Deprecated
- v1.5 BroControl
- v2.0 User Experience
- v2.1 IPv6, Input Framew.
- v2.2 File Analysis, Summary Stats
- v2.3 Performance, SNMP, Radius, SSL++
- v2.4 Broker, Plugins, DTLS/KRB

Bro SDCI — NSF

Bro Center — NSF — broala

A Tale of Two Users

Science & Higher Education

Happy to experiment.

Used to open-source software.

Driven by skilled individuals.

Limited funding.

Bro Center of Expertise

Enterprises & Government

Used to purchasing solutions.

Require reliable point of contact.

Avoid dependence on individuals.

More flexible budgets.

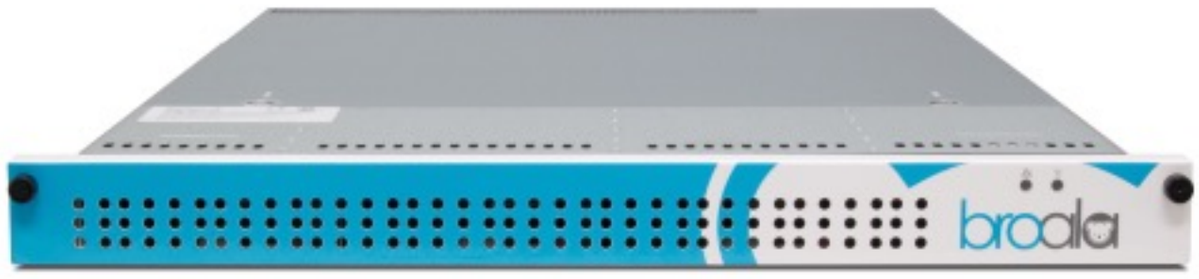
broala

broala

Enterprise-grade Bro solutions, from the creators of Bro.

Commercial Bro support plans.

Plug & play Bro appliances.



BroBox One

Visibility, made elegantly simple.

Bro logs and file extraction.

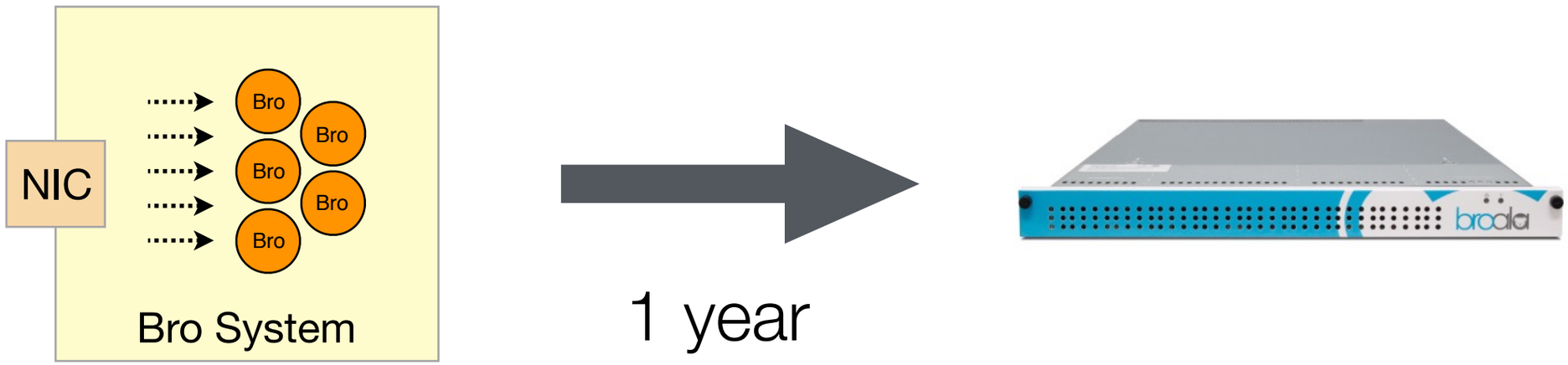
Export to Kafka, Splunk, Syslog, SFTP.

Aggressively tuned for performance.

Zero maintenance, ready for the future.

Advantage: Integration

With BroBox One we are controlling the full stack.

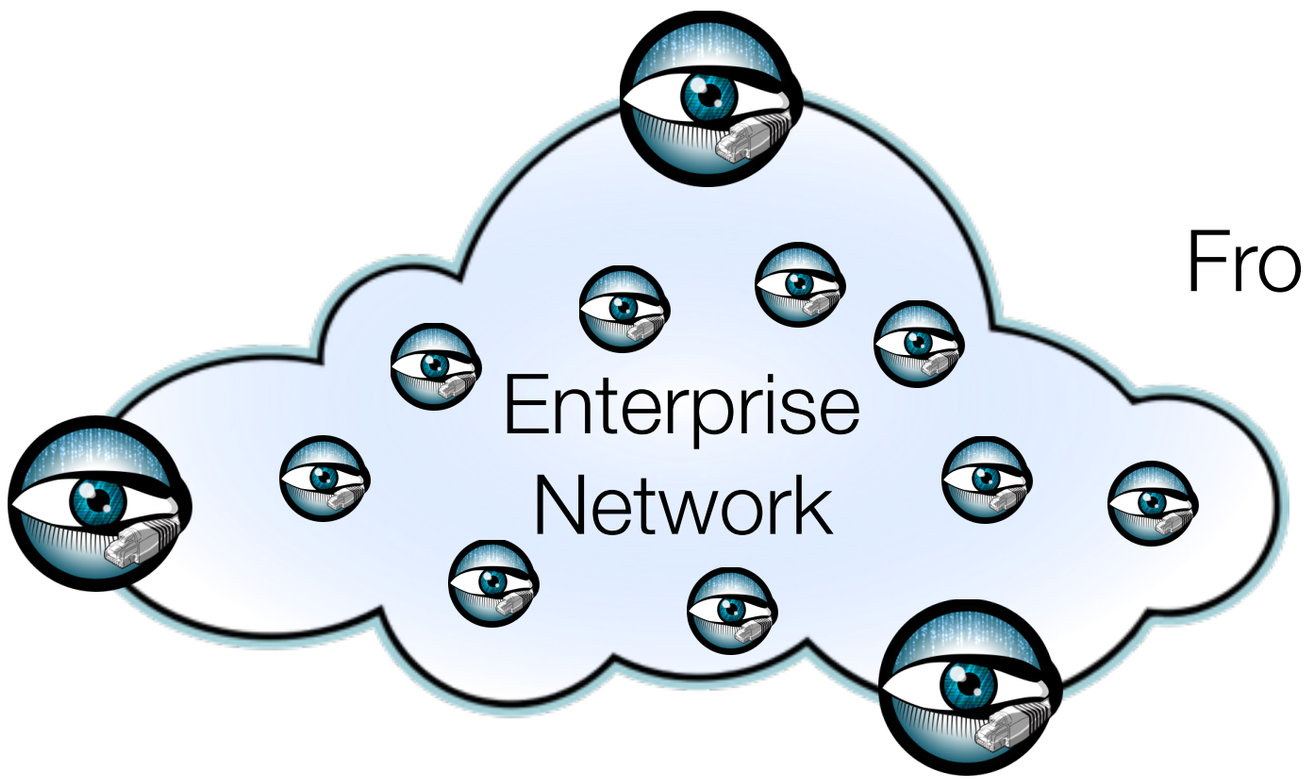


We can take integration much further,
while maintaining the open-source spirit.

Enterprise Solutions

Roadmap for deep visibility and control

Monitoring Enterprise Environments

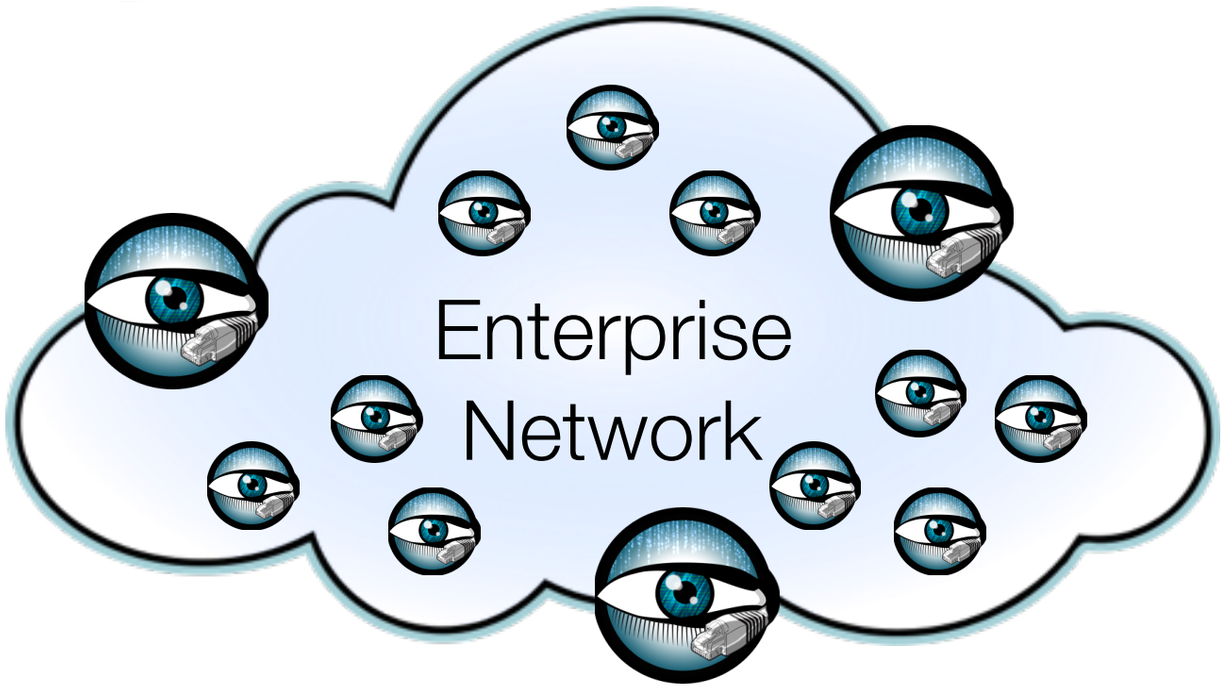


From perimeter to internal.

From standalone to coordinated.

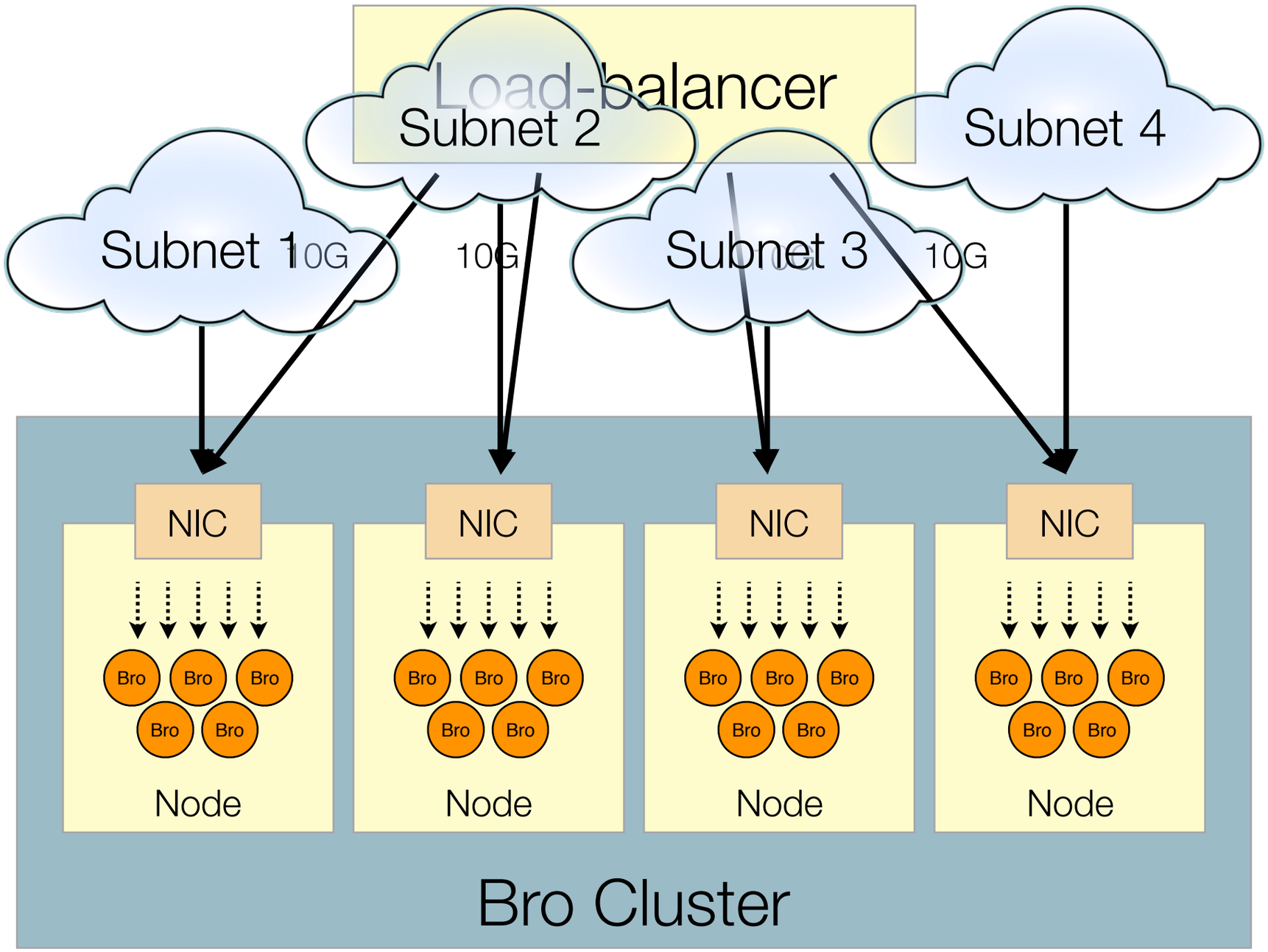
From passive to active.

Bro's open-source roadmap is full of functionality to support all of this.



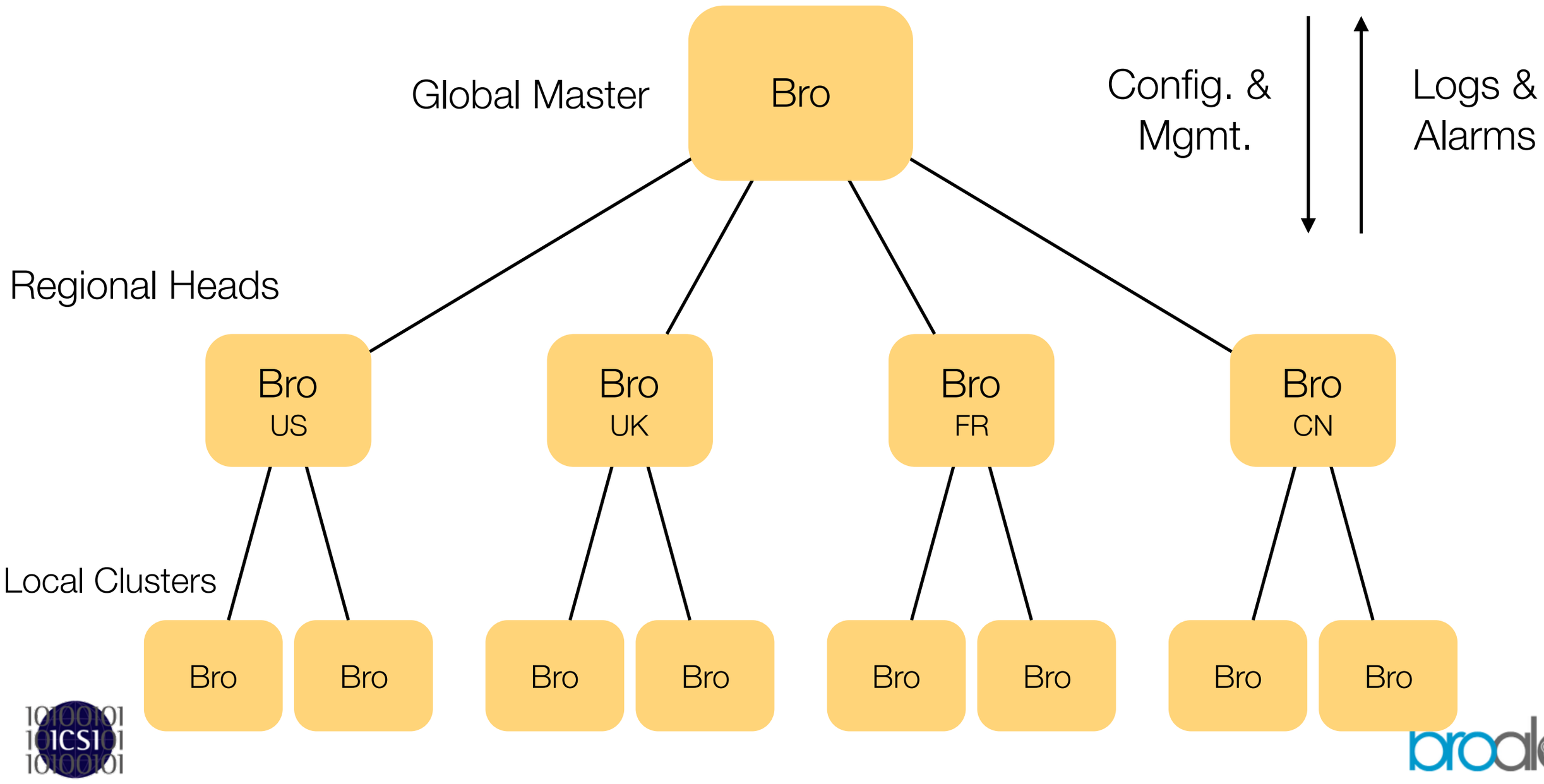
Monitoring Internal Traffic

LBNL's Pragmatic Approach: The "Internal Cluster"



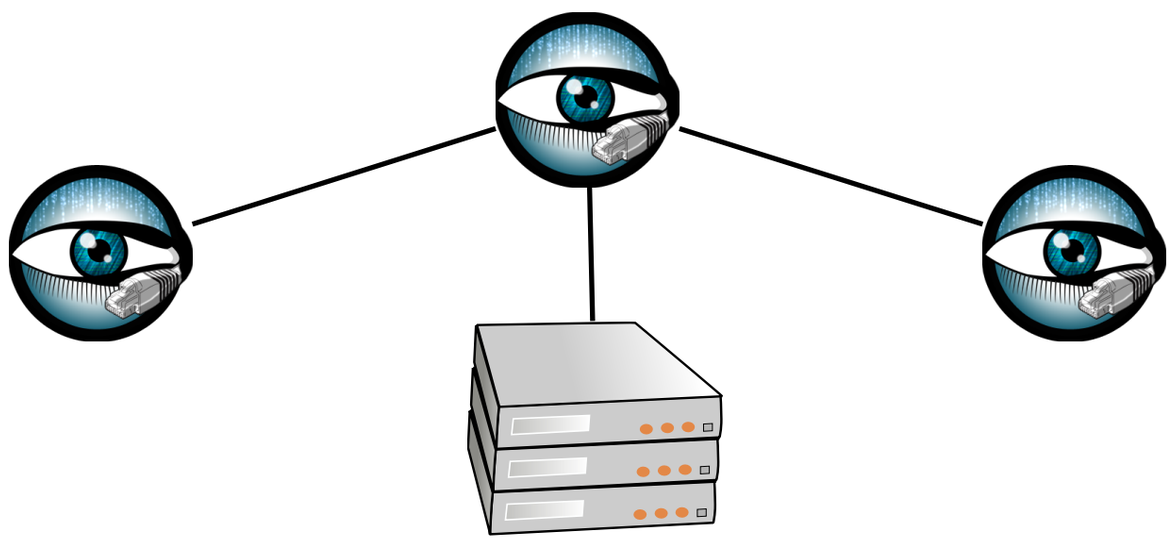
Vision: Deep Cluster

Example: Geographically distributed organization.



Foundation: Broker

Bro's new unified communication library.

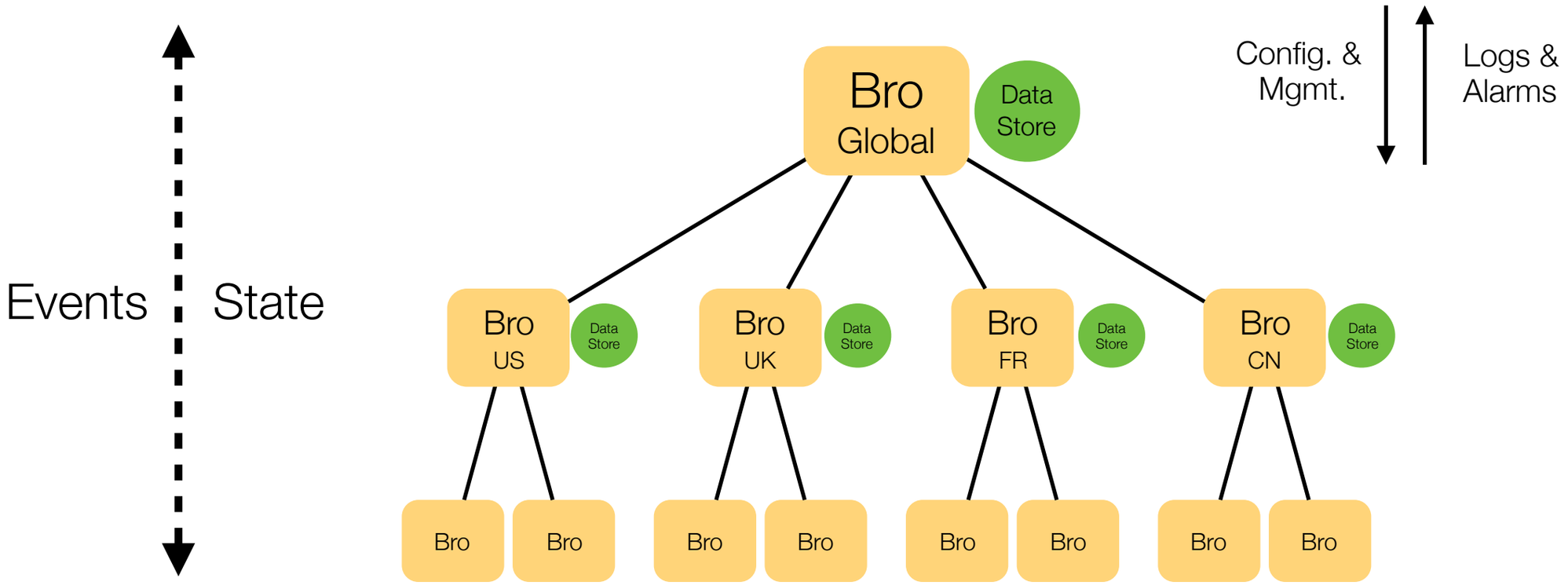


Log forwarding.
Event exchange.
Global key/value stores.

Public/subscribe.
APIs for Bro, C++, C, Python.
BSD license.

`http://github.com/bro/broker`

Global Coordination with Broker

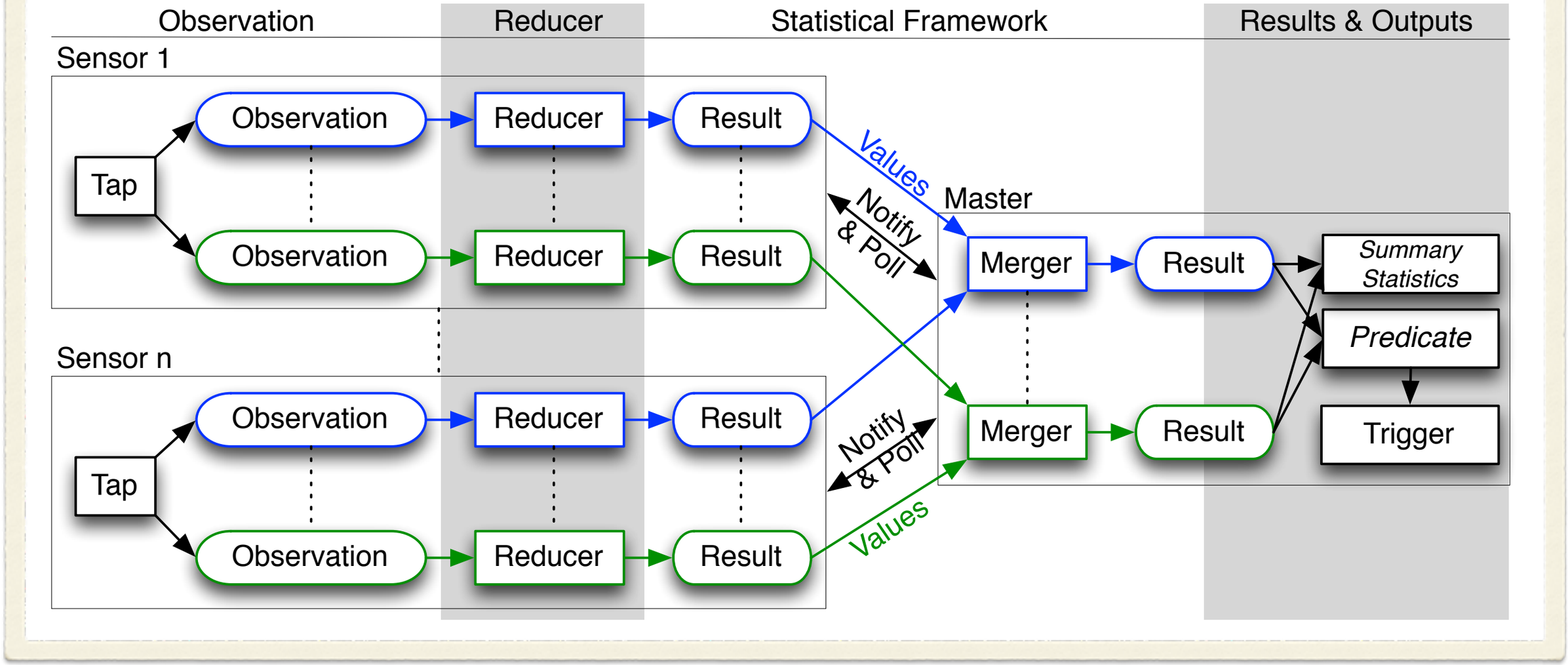


Global state through persistent data stores.

Global correlation through message passing.

Bro's Summary Statistics

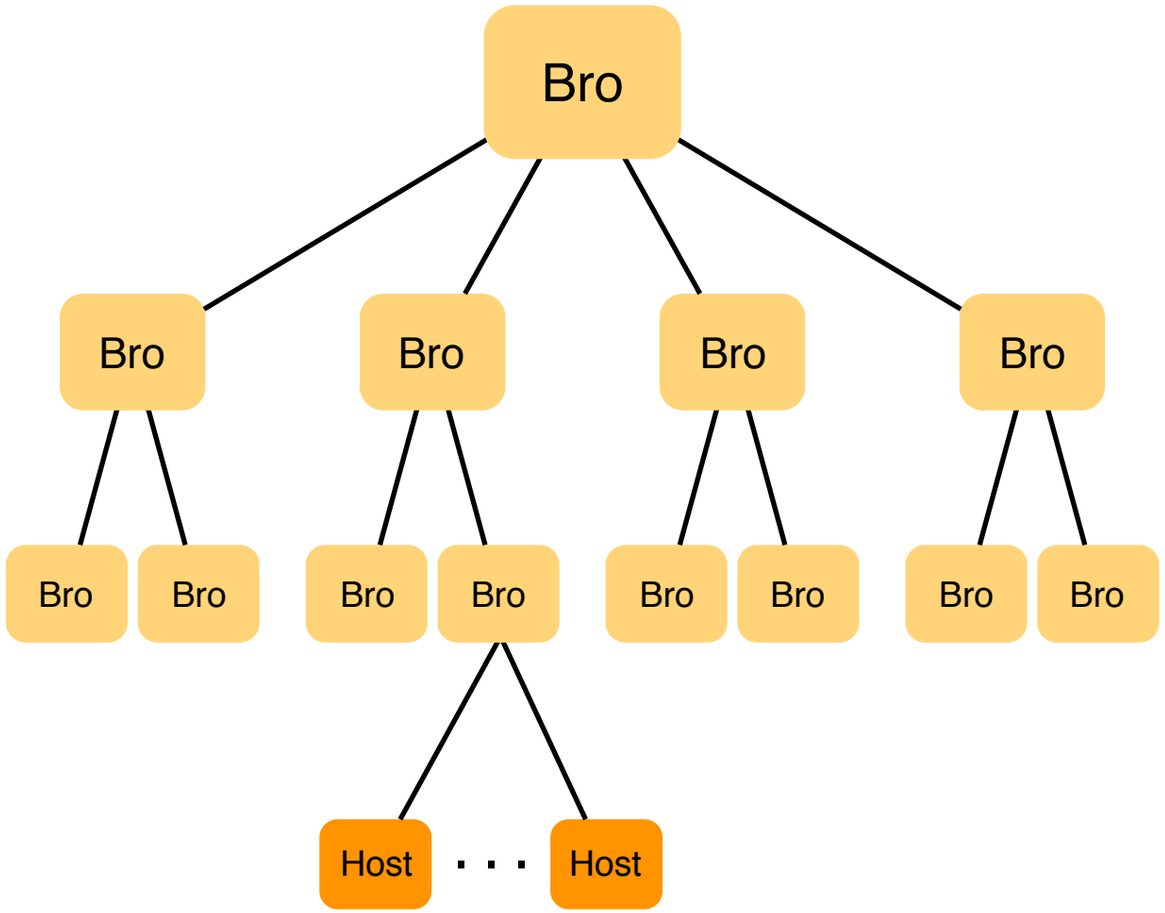
"Bro's version of MapReduce."



Comes with Bro for the classic cluster. Deep Cluster support in planing.

Integrating Host Monitoring

Leverage control over end hosts.



osquery

Source: Facebook

processes

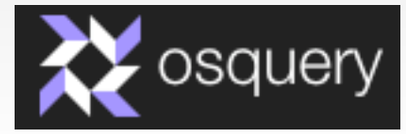
All running processes on the host system.

Column	Type	Description
pid	INTEGER	Process (or thread) ID
name	TEXT	The process path or shorthand argv[0]
path	TEXT	Path to executed binary
cmdline	TEXT	Complete argv
cwd	TEXT	Process current working directory
root	TEXT	Process virtual root directory
uid	BIGINT	Unsigned user ID
gid	BIGINT	Unsgiend groud ID
euid	BIGINT	Unsigned effective user ID
egid	BIGINT	Unsigned effective group ID
parent	INTEGER	Process parent's PID

```
select * from processes where pid = 1
```

https://osquery.io

Broker Plugin for osquery




```
event bro_init()
    {
    […]
    local ev = [$ev=processes,
                $query="SELECT pid, path, cmdline, uid, gid FROM processes"];

    osquery::subscribe(ev);
    }
```

```
event processes(host: string,
                pid: int, path: string, cmdline: string, uid: int, gid: int)
    {
    Log::write(LOG, […]);
    }
```

processes.log

```
#fields t           host        pid    path           uid    gid    argv
1453849601.880629   127.0.0.1   40136  /usr/bin/git   10000  10000  git diff --no-ext-diff --quiet --exit-code
1453849643.924678   127.0.0.1   40397  /usr/bin/git   10000  10000  git push
1453849643.924678   127.0.0.1   40404  /usr/bin/ssh   10000  10000  ssh git@github.com git-receive-pack '/bro-osquery'
```

https://github.com/bro/bro-osquery

From Passive to Active

Bro is not an inline solution.

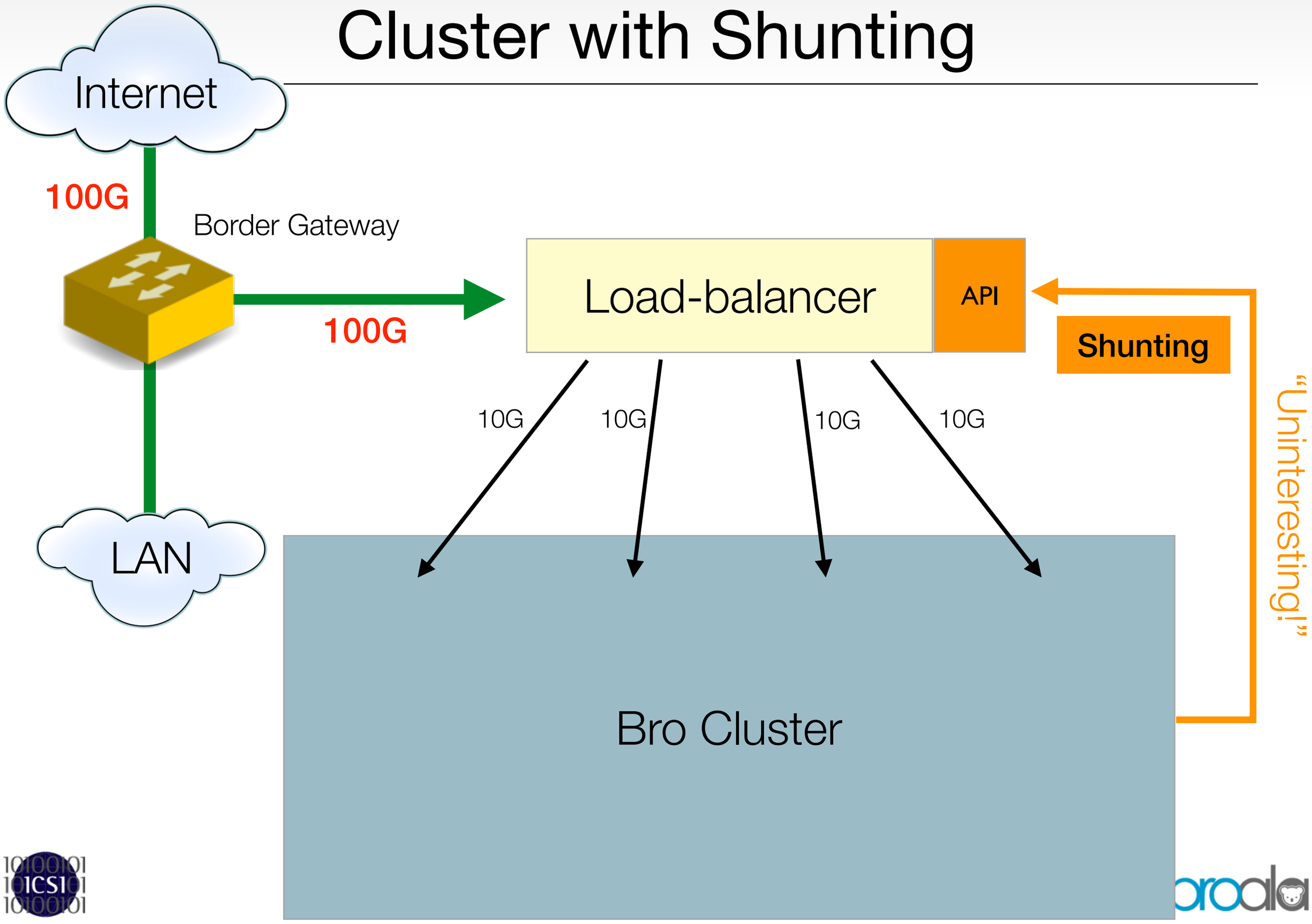
But it can still talk to your network.

Examples

Shunting

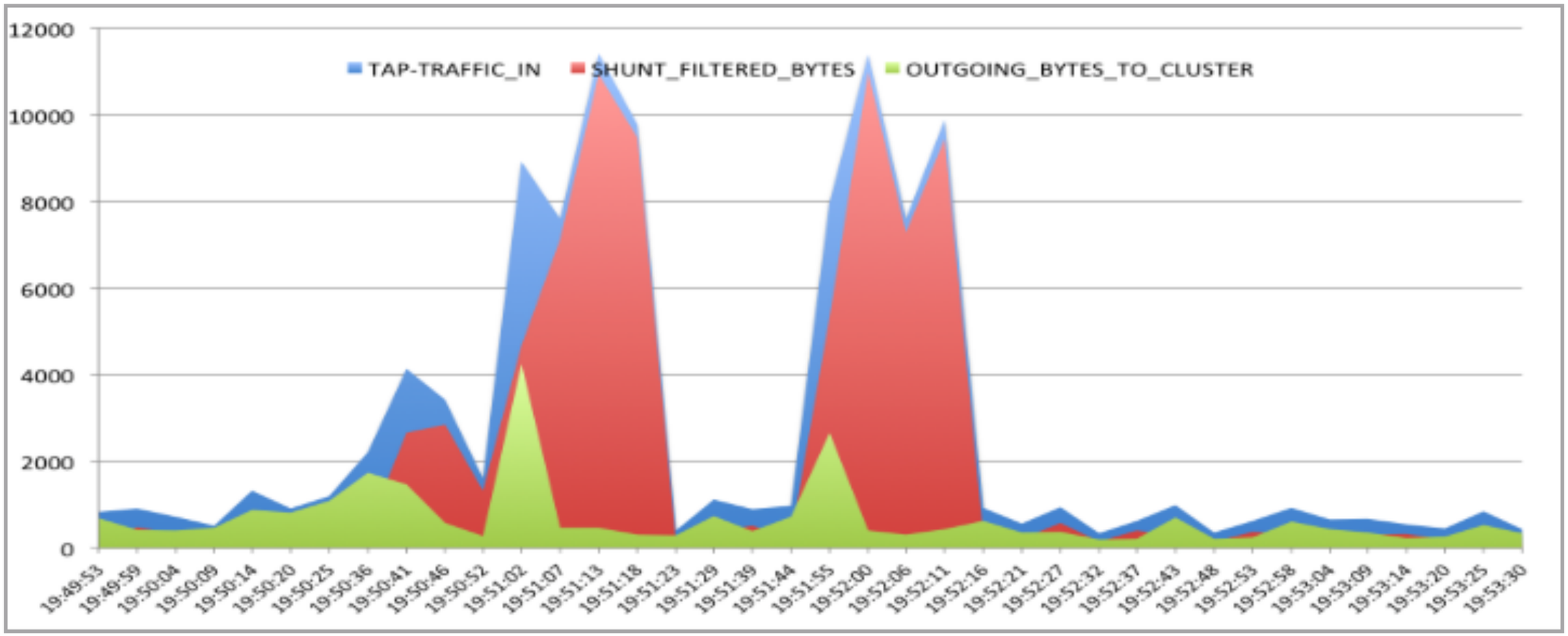
Dynamic Firewall

Cluster with Shunting



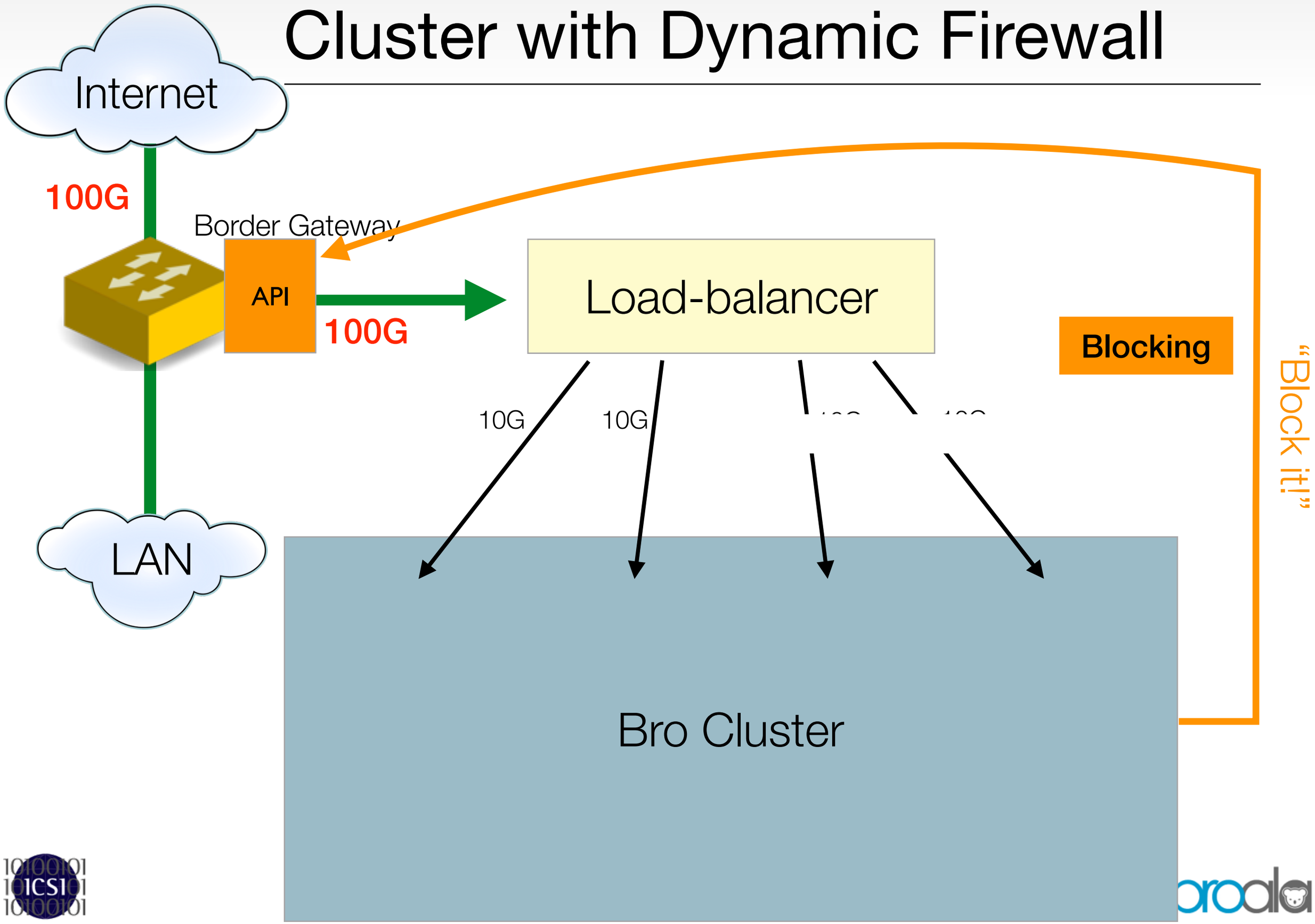
Shunting at Berkeley Lab

Very effective with heavy-tailed network loads.



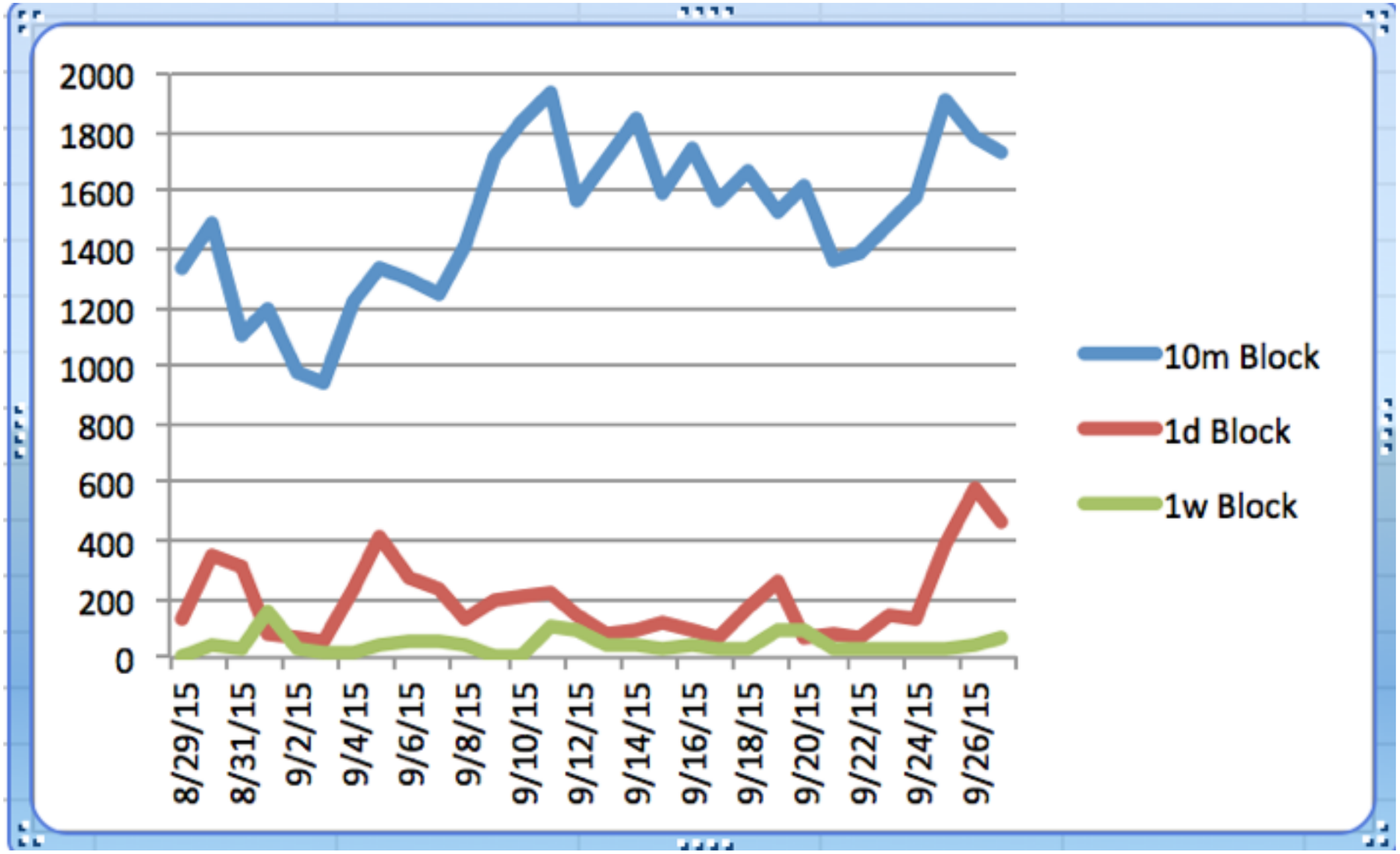
Source: Lawrence Berkeley National Laboratory

Cluster with Dynamic Firewall



Dynamic Firewall Example

Managing 1000s of blocks with “catch & release”.



Source: Indiana University

Foundation: Bro's NetControl Framework

High-level script API to talk to network equipment.

```
drop_connection (connection, timeout)
```

```
drop_address (host, timeout)
```

```
shunt_flow (flow, timeout)
```

```
redirect (flow, port, timeout)
```

Current Backends

OpenFlow, iptables, acld.

`https://github.com/bro/bro-netcontrol`

BYOBro

All this is there, or coming — all open-source.

Central aggregation & management.
Global state & correlation.
Dynamic firewall and shunting.

Bro Frameworks.
Broker communication library.
osqueryd integration.

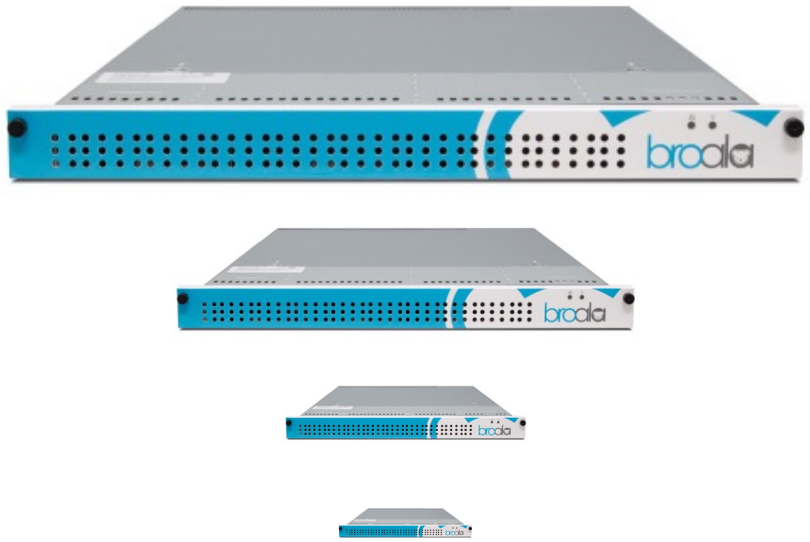
Intelligence integration.
Enterprise context.
Authentication framework.
Dynamic reconfiguration.
Enterprise & domain protocols.
Comprehensive Archival.
Scalability & performance.

Build your own solution.

Opportunity: Integration, Part II.

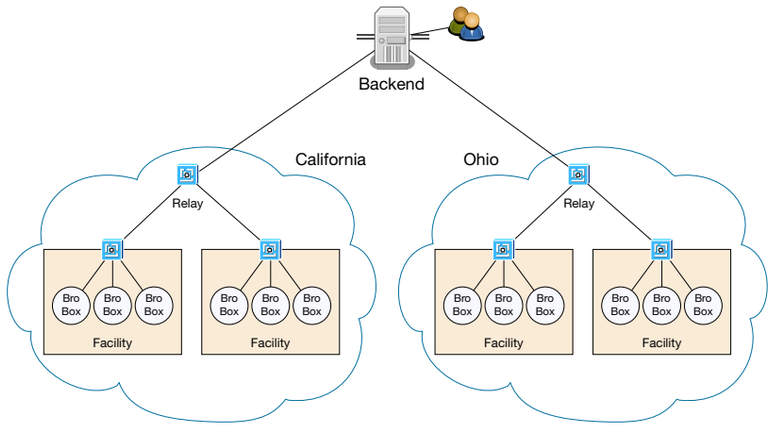
Broala is building a turn-key solution to operate Bro at scale.

Range of BroBox Models



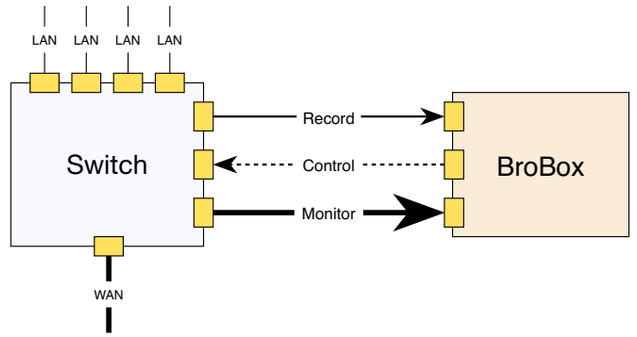
Backbone, data center, offices, factory floor, cloud.

Central Fleet Management



Global aggregation, correlation, & management across 100s of locations.

Active Response



Dynamic firewall.

Help us prioritize!

Join the Bro Community

Broala is just one of many companies leveraging Bro.

Joint goal: A sustainable long-term open-source model.

Software Freedom Conservancy

Fiscal sponsor & neutral 3rd party.

Bro Leadership Team

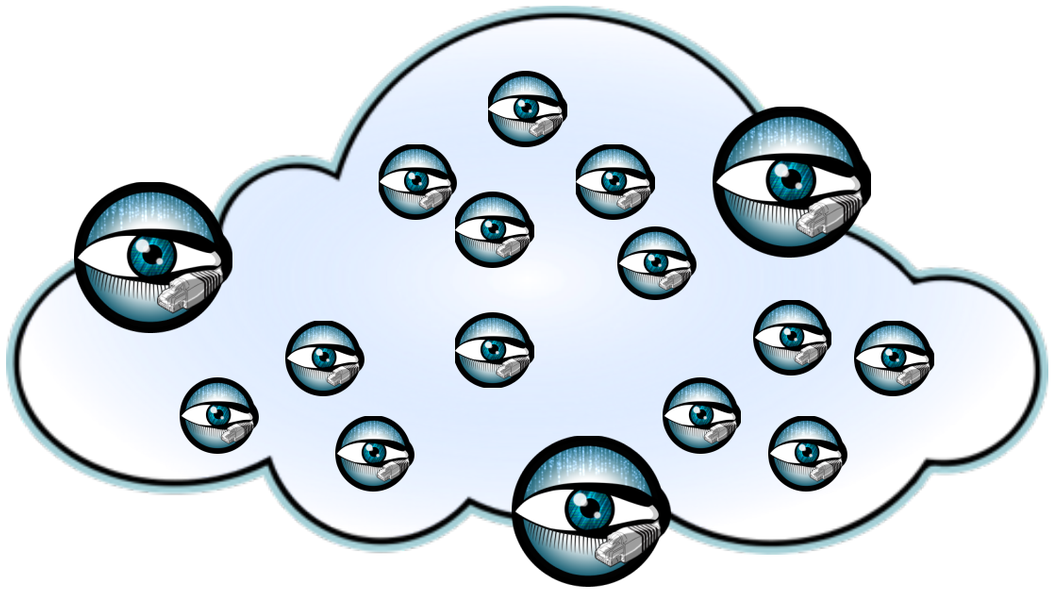
Steering Committee including community members.

Bro Future Fund

Precious metal sponsorships.

Conclusion

The Bro Team is working to bring Bro to the enterprise.



From perimeter to internal.

From standalone to coordinated.

From passive to active.

Build your own solution.

Or come talk to us at Broala.

The U.S. National Science Foundation has enabled much of Bro.

Bro is coming out of two decades of academic research, along with extensive transition to practice efforts. NSF has supported much of that, and is currently funding the Bro Center of

nd

The B

ncy.

Upcoming Bro Events

March 15	Bro4Pros @ Mozilla, San Francisco, CA
April 18	EDUCAUSE Training, Seattle, OR
Sep 13–15	BroCon 2016, Austin, TX

Software Freedom Conservancy, Inc. is a 501(c)(3) not-for-profit organization that helps promote, improve, develop, and defend Free, Libre, and Open Source Software projects.

The Bro Project
www.bro.org
info@bro.org
@Bro_IDS

Commercial Bro Solutions
www.broala.com
info@broala.com
@Broala_