Broverview

Bro Workshop 2011
NCSA, Urbana-Champaign, IL

Outline

Outline

Philosophy and Architecture

A *framework* for network traffic analysis.

Outline

Philosophy and Architecture

A *framework* for network traffic analysis.

History

From research to operations.

Outline

Philosophy and Architecture

A *framework* for network traffic analysis.

History

From research to operations.

Architecture

Components, logs, scripts, cluster.

What is Bro?

What is Bro?

Packet Capture

What is Bro?

Packet Capture

Traffic Inspection

What is Bro?

Packet Capture

Traffic Inspection

Attack Detection

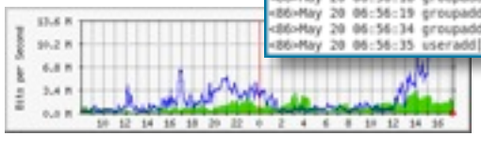
What is Bro?

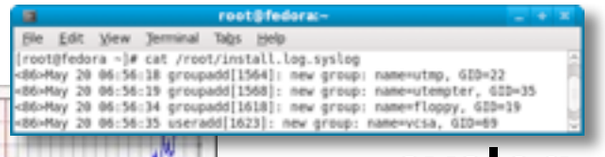
Packet Capture

Traffic Inspection

Attack Detection

NetFlow





syslog

Log Recording

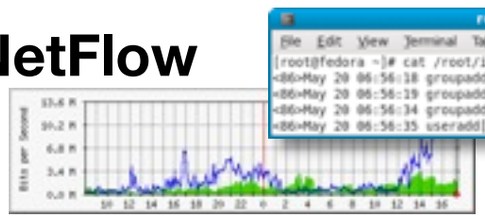
What is Bro?

Packet Capture

Traffic Inspection

Attack Detection

NetFlow



syslog

Log Recording

Flexibility
Abstraction
Data Structures

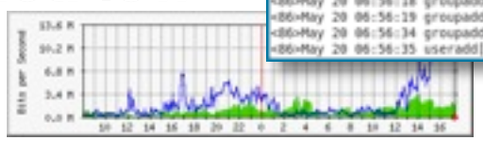
What is Bro?

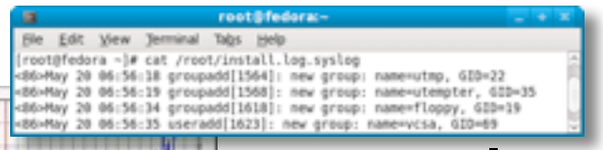
Packet Capture

Traffic Inspection

Attack Detection

NetFlow





syslog

Log Recording

Flexibility
Abstraction
Data Structures

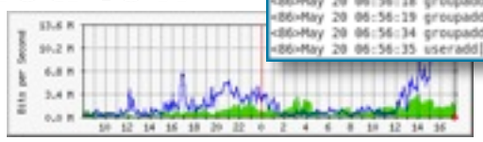
What is Bro?

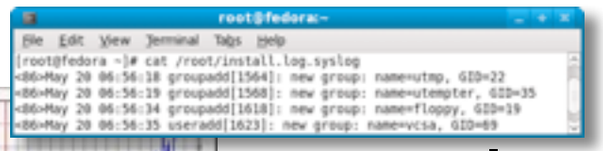
Packet Capture

Traffic Inspection

Attack Detection

NetFlow





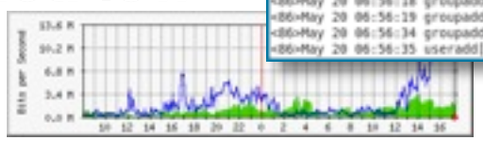
syslog

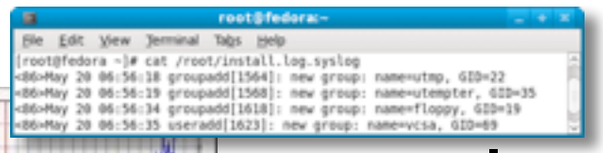
Log Recording

Flexibility
Abstraction
Data Structures

What is Bro?

NetFlow





syslog

Packet Capture

Traffic Inspection

Attack Detection

Log Recording

Flexibility
Abstraction
Data Structures

"Domain-specific Python"

NCSA

What is Bro?

Packet Capture

Traffic Inspection

Attack Detection

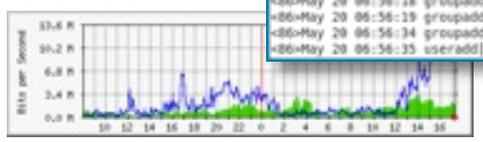
Log Recording

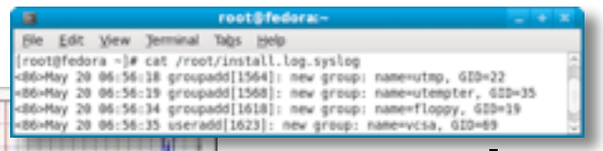
Flexibility
Abstraction
Data Structures

Sum is more than the pieces

"Domain-specific Python"

NetFlow





syslog

Philosophy

Philosophy

Fundamentally different from other IDS.

Reset your idea of an IDS before starting to use Bro.

Philosophy

Fundamentally different from other IDS.

Reset your idea of an IDS before starting to use Bro.

Real-time network analysis *framework.*

Primarily an IDS, but many use it for general traffic analysis.

Philosophy

Fundamentally different from other IDS.

Reset your idea of an IDS before starting to use Bro.

Real-time network analysis *framework.*

Primarily an IDS, but many use it for general traffic analysis.

Policy-neutral at the core.

Can accommodate a range of detection approaches.

Philosophy

Fundamentally different from other IDS.

Reset your idea of an IDS before starting to use Bro.

Real-time network analysis *framework.*

Primarily an IDS, but many use it for general traffic analysis.

Policy-neutral at the core.

Can accommodate a range of detection approaches.

Highly stateful.

Tracks extensive application-layer network state.

Philosophy

Fundamentally different from other IDS.

Reset your idea of an IDS before starting to use Bro.

Real-time network analysis *framework.*

Primarily an IDS, but many use it for general traffic analysis.

Policy-neutral at the core.

Can accommodate a range of detection approaches.

Highly stateful.

Tracks extensive application-layer network state.

Supports forensics.

Extensively logs what it sees.

Target Audience

Target Audience

Large-scale environments.

Effective also with liberal security policies.

Target Audience

Large-scale environments.

Effective also with liberal security policies.

Network-savvy users.

Requires understanding of your network.

Target Audience

Large-scale environments.

Effective also with liberal security policies.

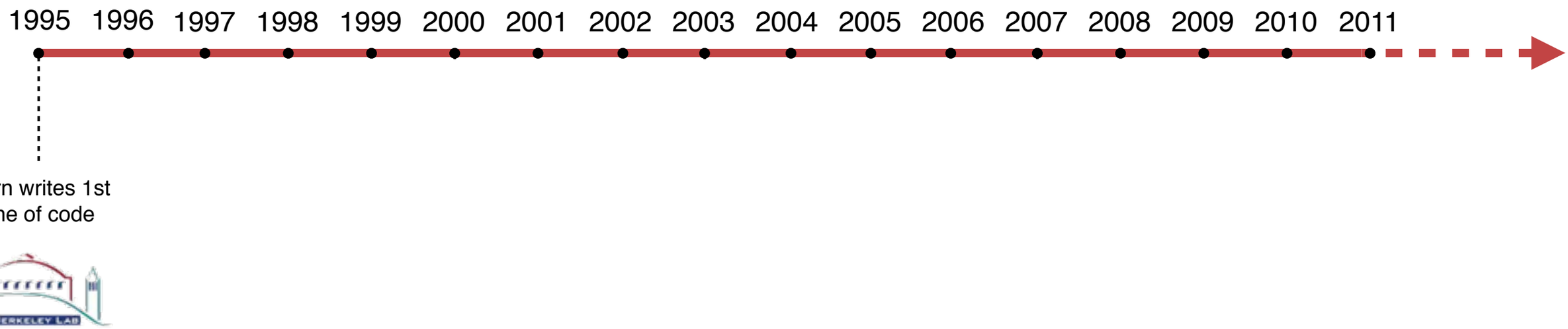
Network-savvy users.

Requires understanding of your network.

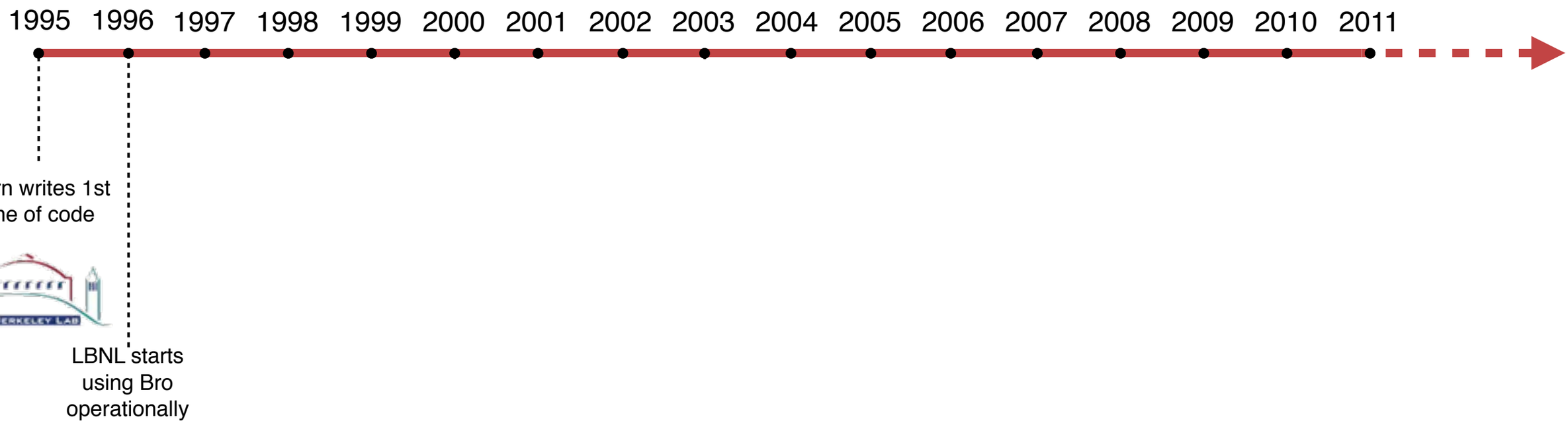
Unixy mindset.

Command-line based, fully customizable.

Bro History


1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
Vern writes 1st line of code

Bro History


1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
Vern writes 1st line of code
LBNL starts using Bro operationally

Bro History

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011

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

Bro Waters

Bro 2.0

Bro History

Academic Publications

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011

Vern writes 1st line of code

LBNL starts using Bro operationally

USENIX Paper

v0.2
1st CHANGES entry

v0.4
HTTP analysis
Scan detector
IP fragments
Linux support

Stepping Stone Detector

v0.6
RegExps
Login analysis

v0.7a48
Consistent CHANGES

v0.7a90
Profiling
State Mgmt

Anonymizer
Active Mapping
Context Signat.

v0.7a175/0.8aX
Signatures
SMTP
IPv6 support
User manual

TRW
State Mgmt.
Indepen. State

0.8a37
Communication
Persistence
Namespaces
Log Rotation

Host Context
Time Machine
Enterprise Traffic

v0.8aX/0.9aX
SSL/SMB
STABLE releases
BroLite

v1.0
BinPAC
IRC/RPC analyzers
64-bit support
Sane version numbers

BinPAC
DPD
2nd Path

v1.1/v1.2
when Stmt
Resource tuning
Broccoli
DPD

Bro Cluster
Shunt

v1.3
Ctor expressions
GeoIP
Conn Compressor

Autotuning

v1.4
DHCP/BitTorrent
HTTP entities
NetFlow
Bro Lite Deprecated

Parallel Prototype

v1.5
BroControl

Bro 2.0

Bro Waters

Research Heritage

Research Heritage

Much of Bro is coming out of research projects.

Bridging gap between academia and operations.

Research Heritage

Much of Bro is coming out of research projects.

Bridging gap between academia and operations.

However, that meant limited engineering resources.

We were lacking resources for development, documentation, polishing.

Research Heritage

Much of Bro is coming out of research projects.

Bridging gap between academia and operations.

However, that meant limited engineering resources.

We were lacking resources for development, documentation, polishing.

NSF now funding Bro *development* at ICSI and NCSA.

Full-time engineers working 3 years on capabilities & user experience.

Office of Cyberinfrastructure

Research Heritage

Much of Bro is coming out of research projects.

Bridging gap between academia and operations.

However, that meant limited engineering resources.

We were lacking resources for development, documentation, polishing.

NSF now funding Bro *development* at ICSI and NCSA.

Full-time engineers working 3 years on capabilities & user experience.

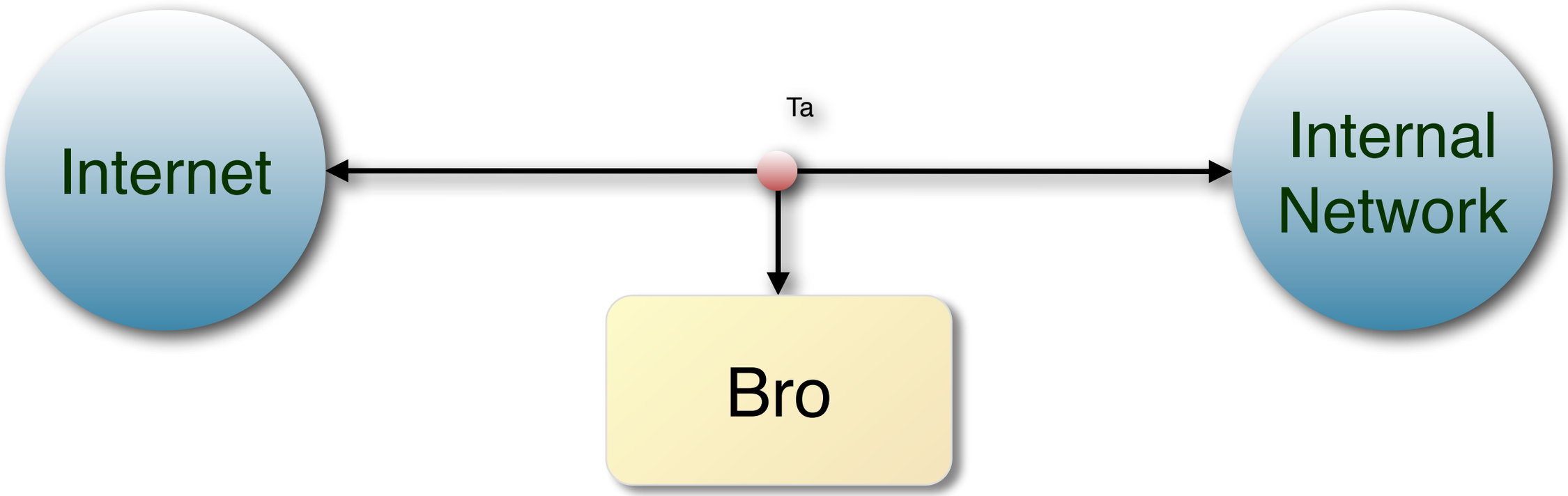
Objective is a sustainable development model.

Aiming to create a larger user and development community.

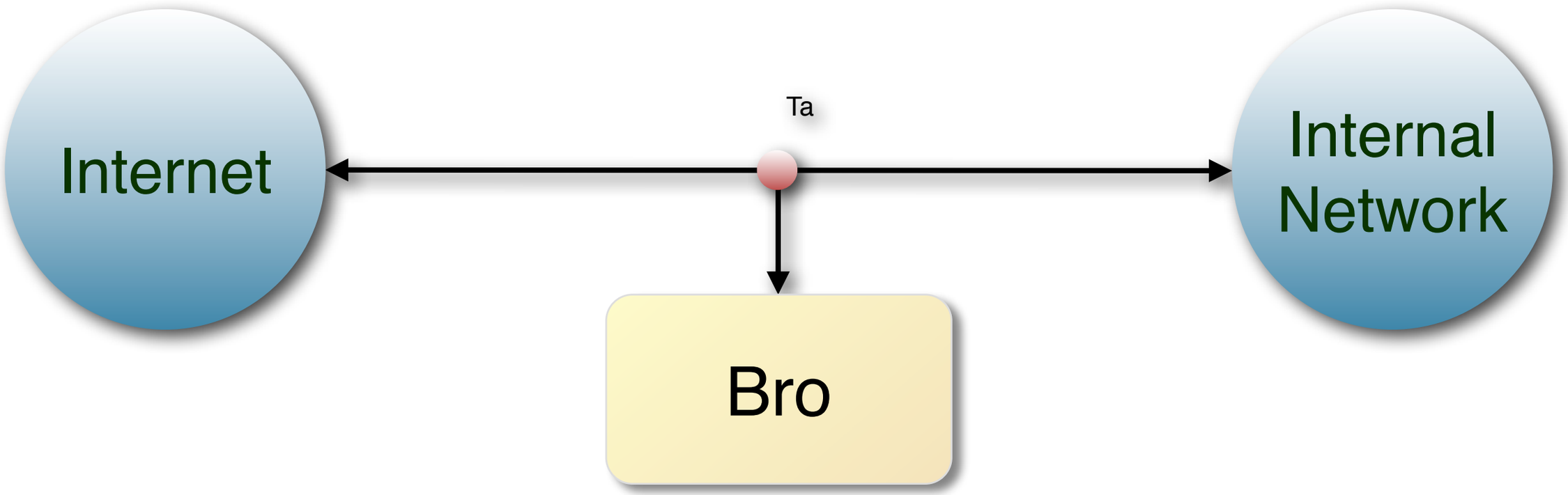
Office of Cyberinfrastructure

Deployment

Deployment



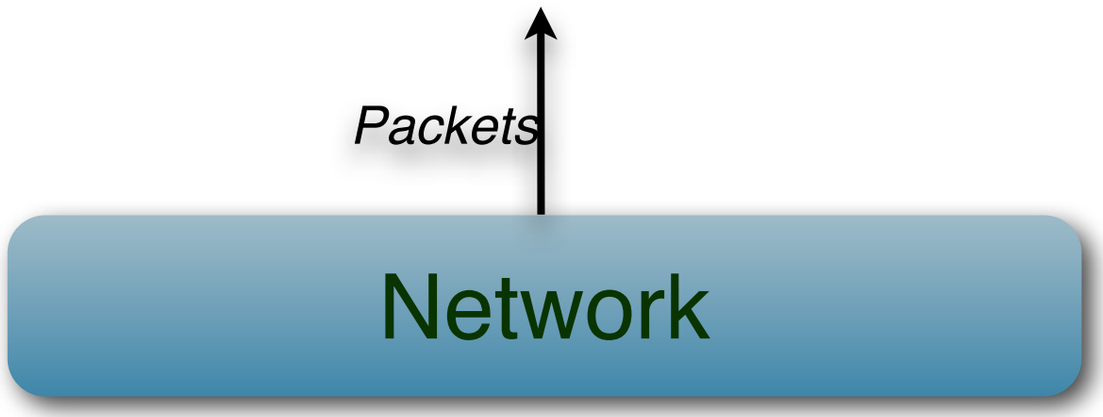
Deployment



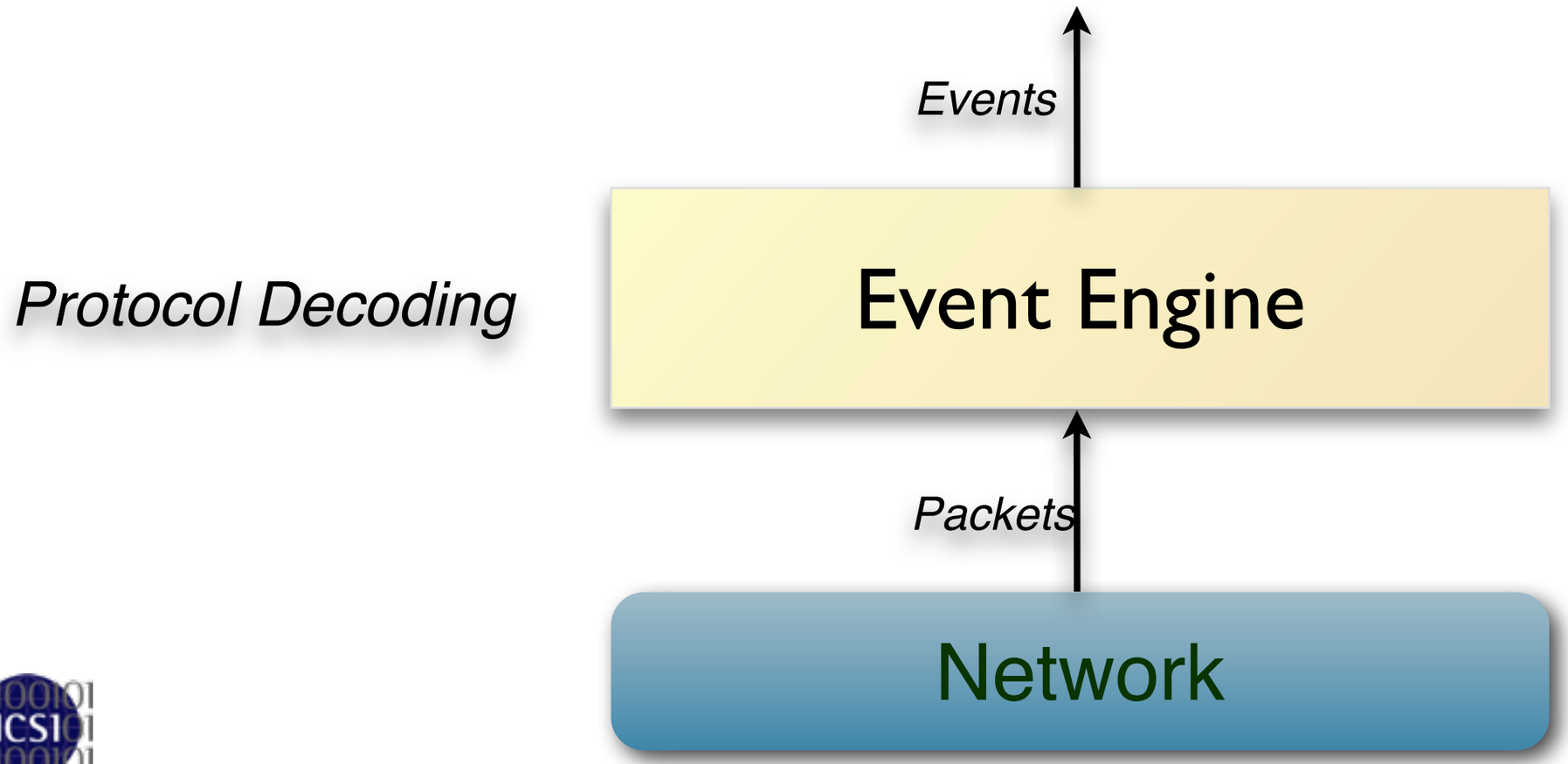
Runs on commodity platforms.

- Standard PCs & NICs.
- Supports FreeBSD/Linux/OS X.

Architecture



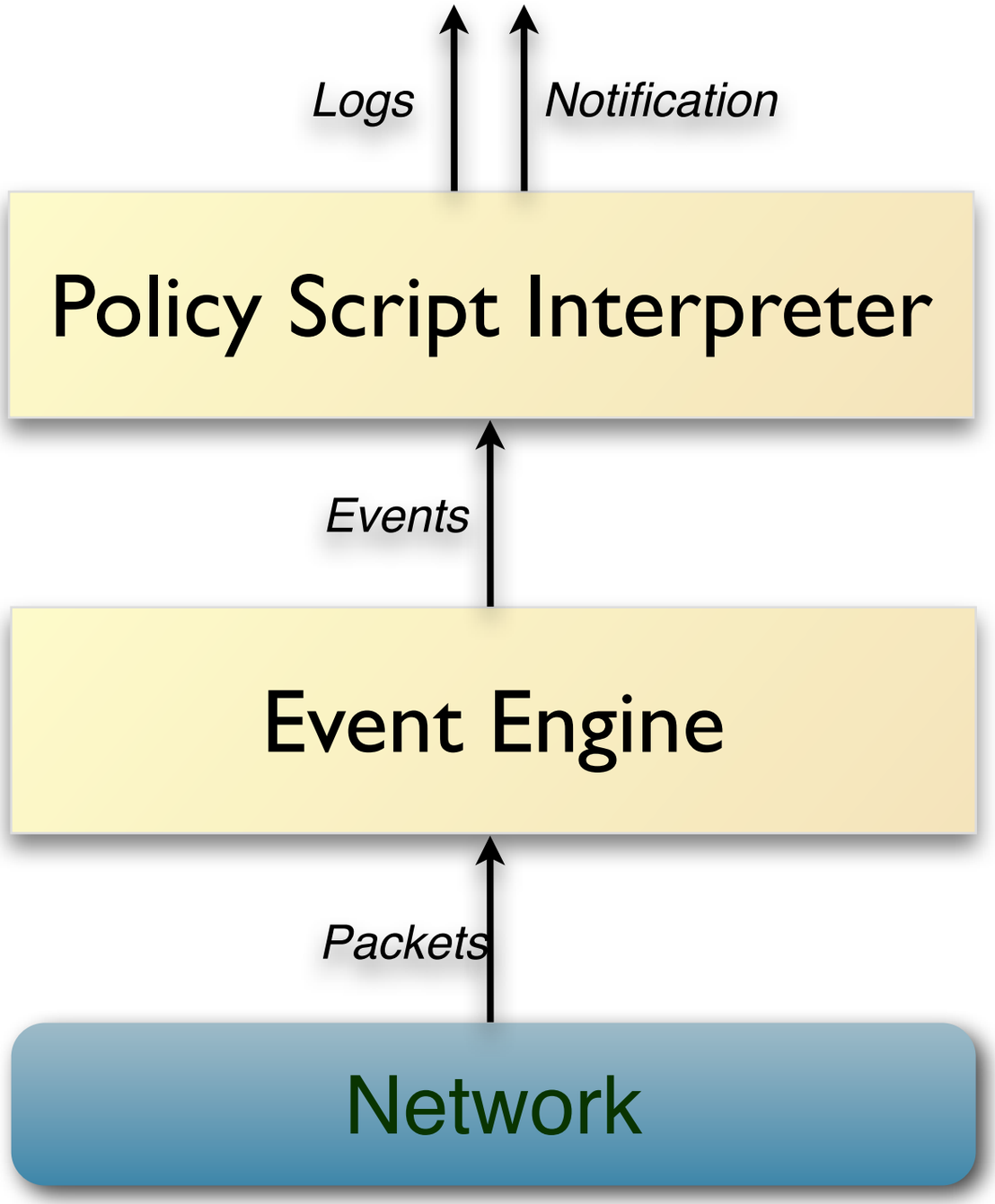
Architecture



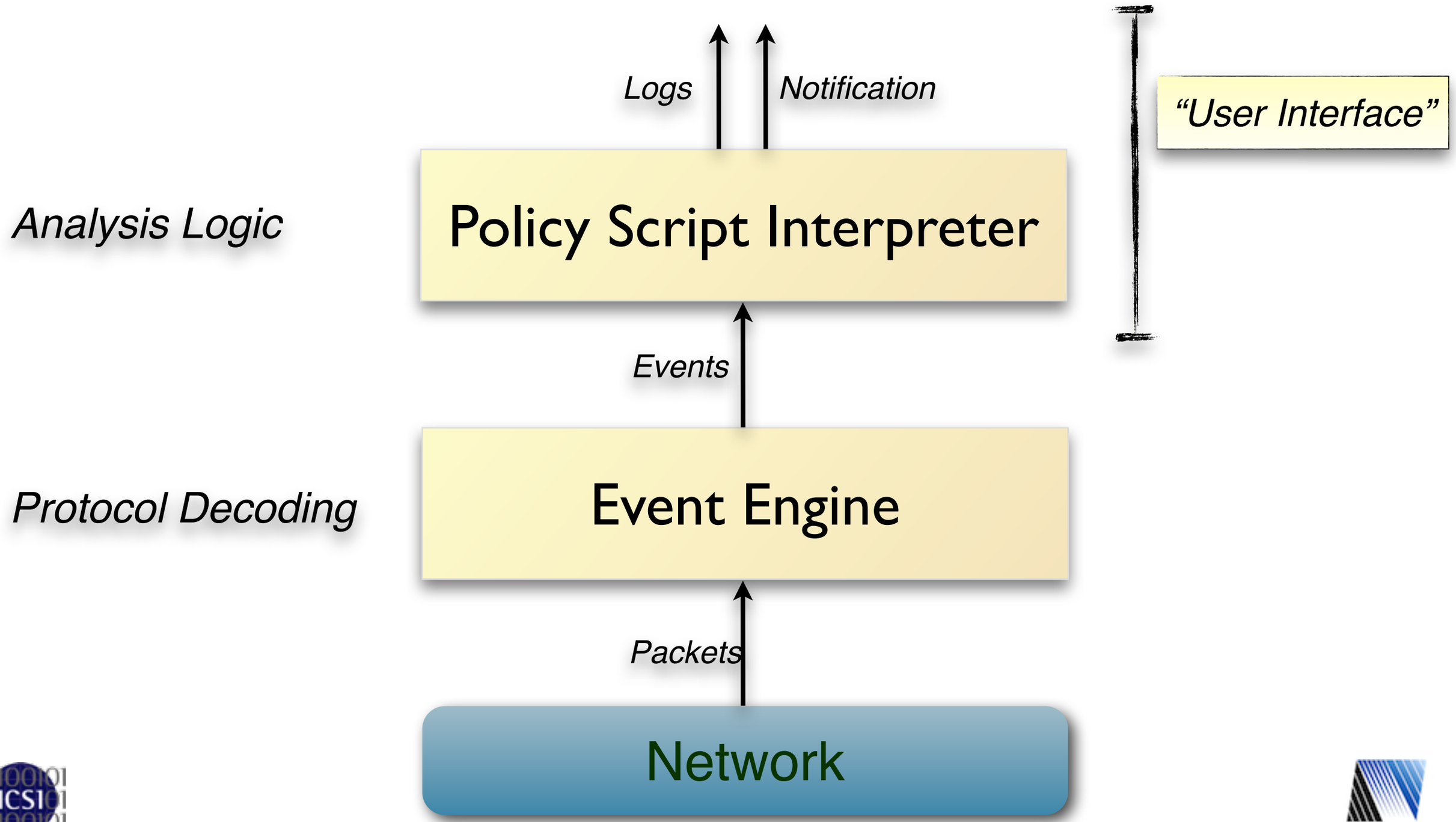
Architecture

Analysis Logic

Protocol Decoding



Architecture



Script Example: Matching URLs

Task: Report all Web requests for files called "`passwd`".

Script Example: Matching URLs

Task: Report all Web requests for files called "`passwd`".

```
event http_request(c: connection,           # Connection.
                   method: string,          # HTTP method.
                   original_URI: string,    # Requested URL.
                   unescaped_URI: string,   # Decoded URL.
                   version: string)         # HTTP version.
{
    if ( method == "GET" && unescaped_URI == /.*passwd/ )
        NOTICE(...); # Alarm.
}
```

Script Example: Scan Detector

Task: Count failed connection attempts per source address.

Script Example: Scan Detector

Task: Count failed connection attempts per source address.

```
global attempts: table[addr] of count &default=0;

event connection_rejected(c: connection)
{
        local source = c$id$orig_h;      # Get source address.
        local n = ++attempts[source];    # Increase counter.
        if ( n == SOME_THRESHOLD )       # Check for threshold.
            NOTICE(...);                 # Alarm.
}
```

Distributed Scripts

Distributed Scripts

Bro comes with >10,000 lines of script code.

Prewritten functionality that's just loaded.

Distributed Scripts

Bro comes with >10,000 lines of script code.

Prewritten functionality that's just loaded.

Scripts generate alarms and logs.

Amendable to extensive customization and extension.

Example Logs

Example Logs

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

Example Logs

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

#fields ts	*id.orig_h*	*id.orig_p*	*id.resp_h*	*id.resp_p*	*proto*	*service*	*duration*	*obytes*	*rbytes* [...]
1144876741.1198	192.150.186.169	53115	82.94.237.218	80	tcp	http	16.14929	435	66363
1144876612.6063	192.150.186.169	53090	198.189.255.82	80	tcp	http	4.437460	8661	63663
1144876596.5597	192.150.186.169	53051	193.203.227.129	80	tcp	http	0.372440	461	753
1144876606.7789	192.150.186.169	53082	198.189.255.73	80	tcp	http	0.597711	337	5146
1144876741.4693	**192.150.186.169**	**53116**	**82.94.237.218**	**80**	**tcp**	**http**	**16.02667**	**3027**	**11761**
1144876745.6102	**192.150.186.169**	**53117**	**66.102.7.99**	**80**	**tcp**	**http**	**1.004346**	**422**	**1637**
1144876605.6847	192.150.186.169	53075	207.151.118.143	80	tcp	http	0.029663	347	1011

Example Logs

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

#fields ts	*id.orig_h*	*id.orig_p*	*id.resp_h*	*id.resp_p*	*proto*	*service*	*duration*	*obytes*	*rbytes* [...]
1144876741.1198	192.150.186.169	53115	82.94.237.218	80	tcp	http	16.14929	435	66363
1144876612.6063	192.150.186.169	53090	198.189.255.82	80	tcp	http	4.437460	8661	63663
1144876596.5597	192.150.186.169	53051	193.203.227.129	80	tcp	http	0.372440	461	753
1144876606.7789	192.150.186.169	53082	198.189.255.73	80	tcp	http	0.597711	337	5146
1144876741.4693	**192.150.186.169**	**53116**	**82.94.237.218**	**80**	**tcp**	**http**	**16.02667**	**3027**	**11761**
1144876745.6102	**192.150.186.169**	**53117**	**66.102.7.99**	**80**	**tcp**	**http**	**1.004346**	**422**	**1637**
1144876605.6847	192.150.186.169	53075	207.151.118.143	80	tcp	http	0.029663	347	1011

```
> cat http.log
```

Example Logs

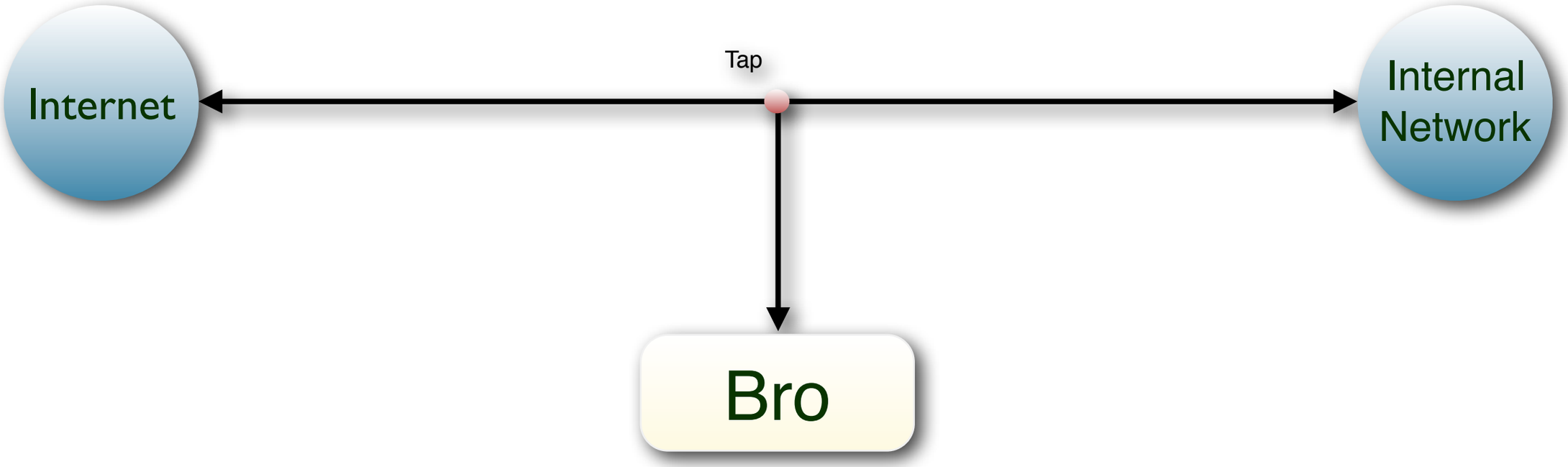
```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

#fields ts	*id.orig_h*	*id.orig_p*	*id.resp_h*	*id.resp_p*	*proto*	*service*	*duration*	*obytes*	*rbytes* [...]
1144876741.1198	192.150.186.169	53115	82.94.237.218	80	tcp	http	16.14929	435	66363
1144876612.6063	192.150.186.169	53090	198.189.255.82	80	tcp	http	4.437460	8661	63663
1144876596.5597	192.150.186.169	53051	193.203.227.129	80	tcp	http	0.372440	461	753
1144876606.7789	192.150.186.169	53082	198.189.255.73	80	tcp	http	0.597711	337	5146
1144876741.4693	**192.150.186.169**	**53116**	**82.94.237.218**	**80**	**tcp**	**http**	**16.02667**	**3027**	**11761**
1144876745.6102	**192.150.186.169**	**53117**	**66.102.7.99**	**80**	**tcp**	**http**	**1.004346**	**422**	**1637**
1144876605.6847	192.150.186.169	53075	207.151.118.143	80	tcp	http	0.029663	347	1011

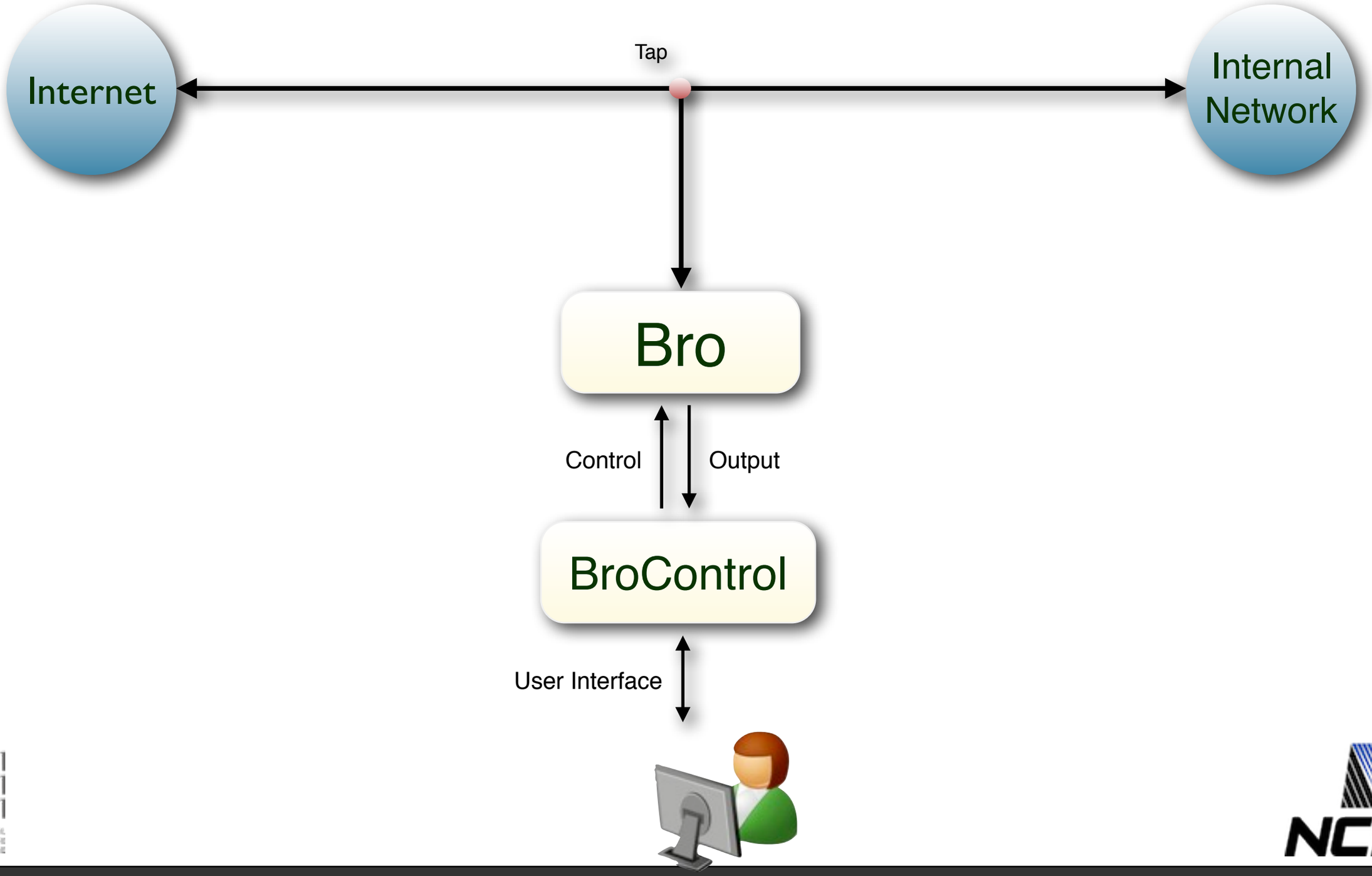
```
> cat http.log
```

#fields ts	*id.orig_h*	*id.orig_p [...]*	*host*	*uri*	*status_code*	*user_agent [...]*
1144876741.6335	192.150.186.169	53116	docs.python.org	/lib/lib.css	200	Mozilla/5.0
1144876742.1687	192.150.186.169	53116	docs.python.org	/icons/previous.png	304	Mozilla/5.0
1144876741.2838	192.150.186.169	53115	docs.python.org	/lib/lib.html	200	Mozilla/5.0
1144876742.3337	192.150.186.169	53116	docs.python.org	/icons/up.png	304	Mozilla/5.0
1144876742.3337	192.150.186.169	53116	docs.python.org	/icons/next.png	304	Mozilla/5.0
1144876742.3337	192.150.186.169	53116	docs.python.org	/icons/contents.png	304	Mozilla/5.0
1144876742.3337	192.150.186.169	53116	docs.python.org	/icons/modules.png	304	Mozilla/5.0
1144876742.3338	192.150.186.169	53116	docs.python.org	/icons/index.png	304	Mozilla/5.0
1144876745.6144	192.150.186.169	53117	www.google.com	/	200	Mozilla/5.0

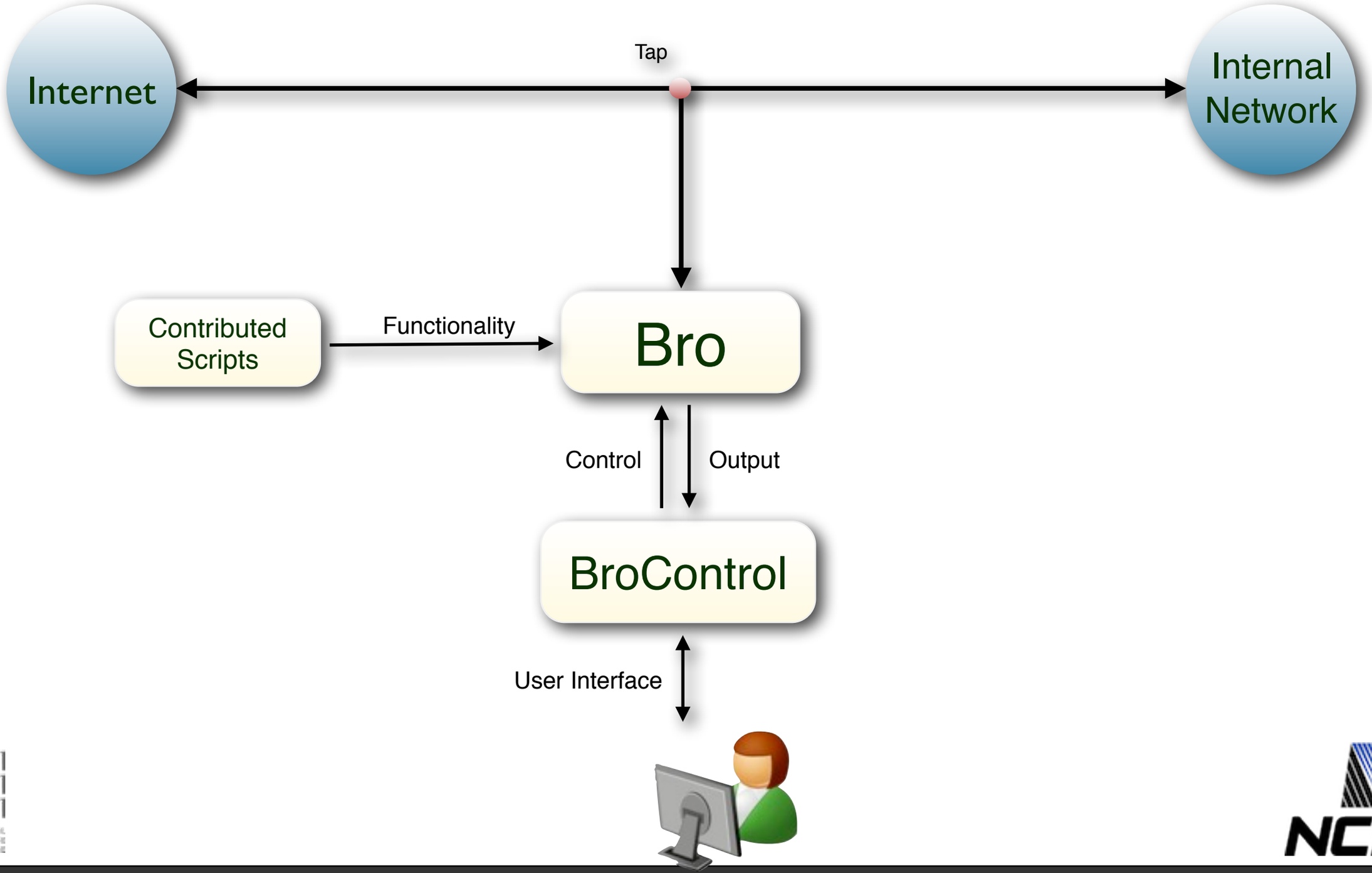
Bro Ecosystem



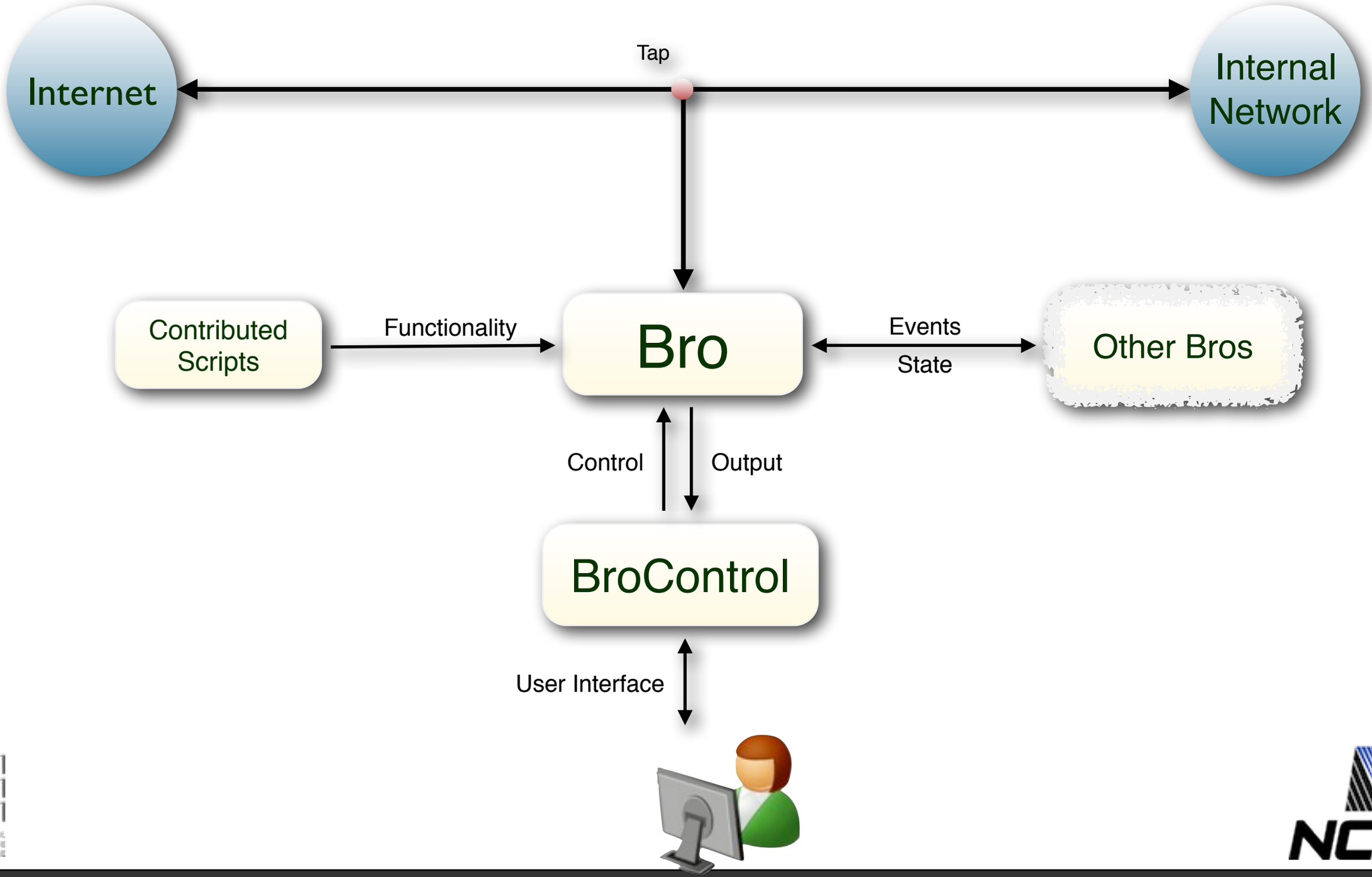
Bro Ecosystem



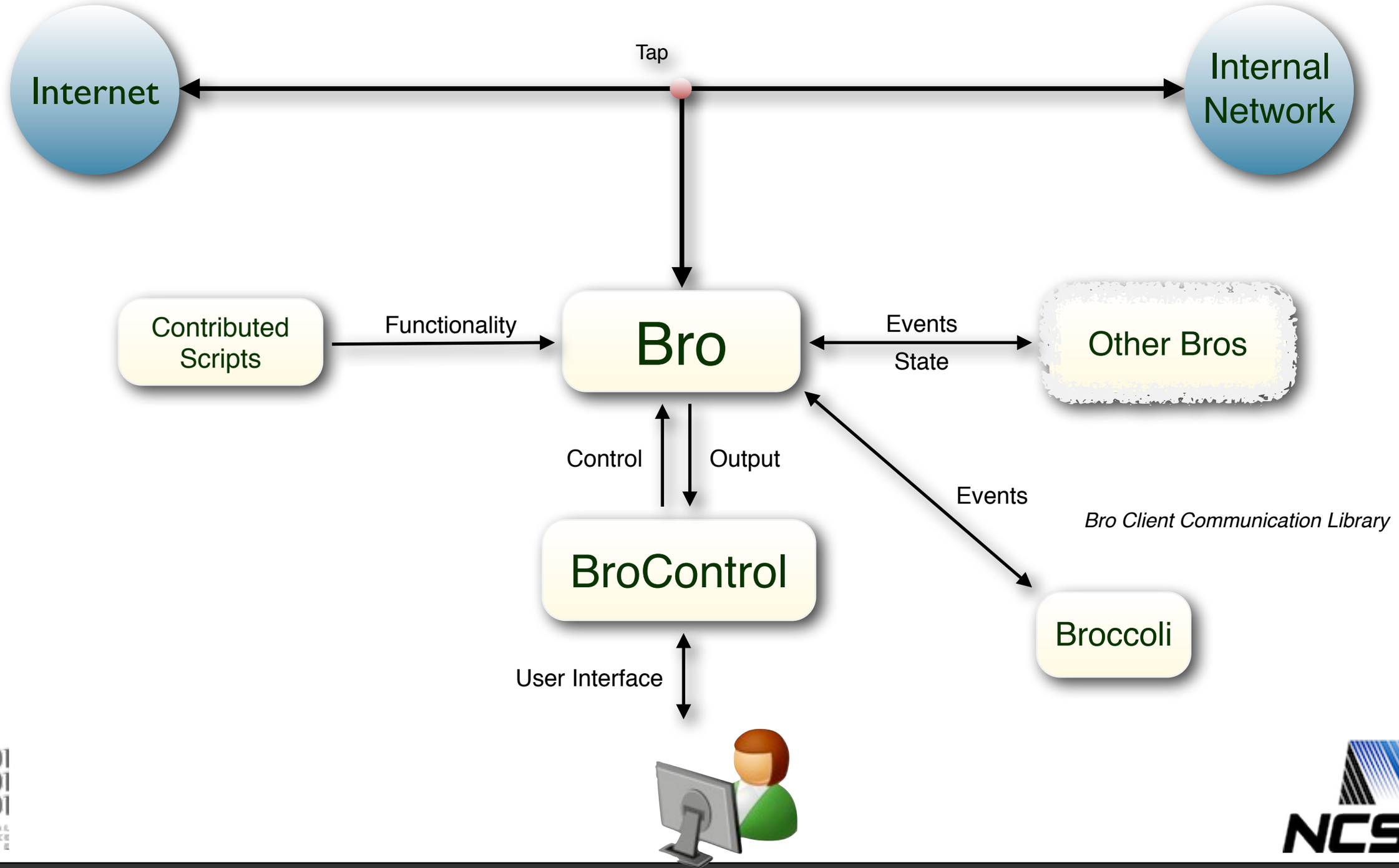
Bro Ecosystem



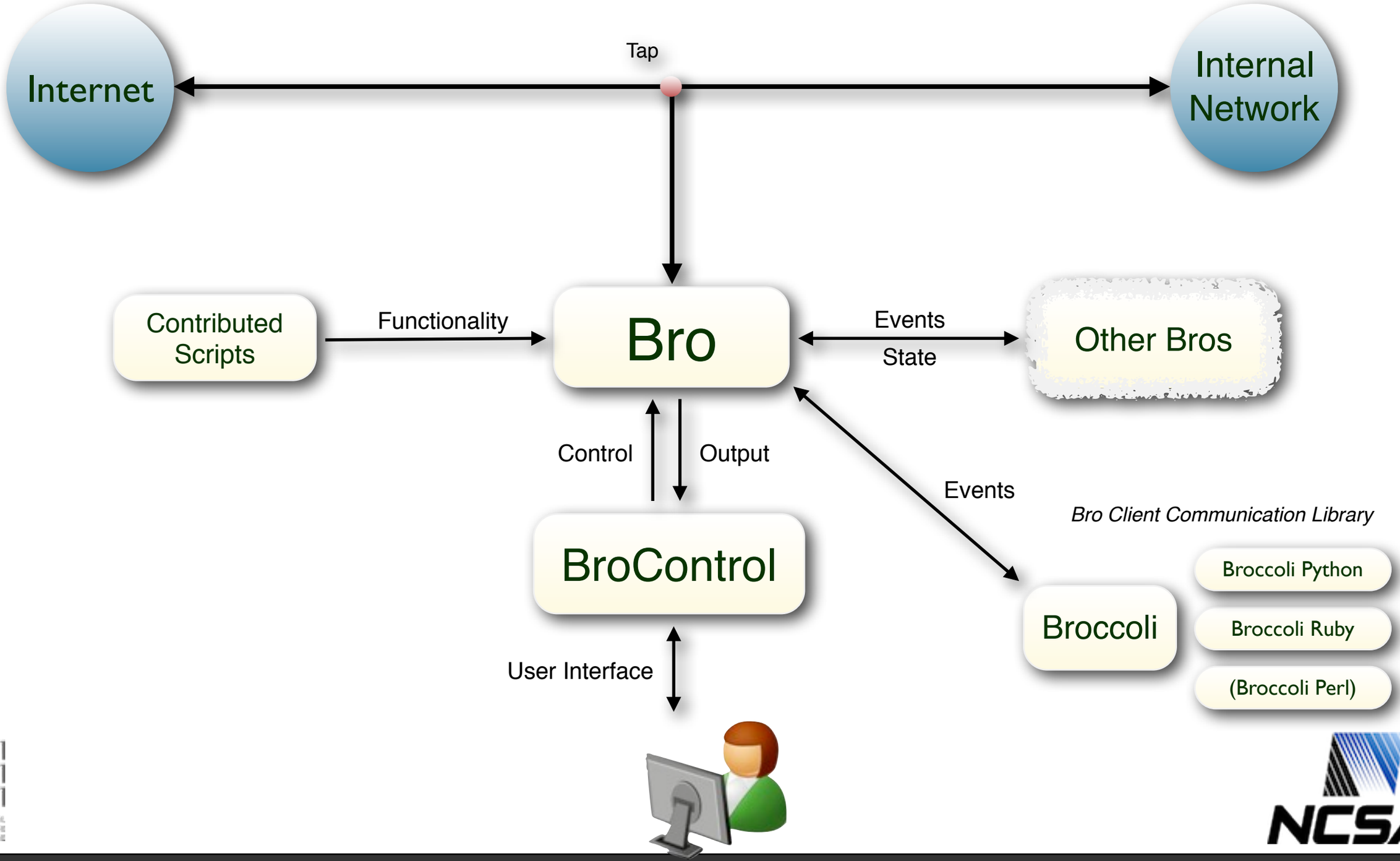
Bro Ecosystem



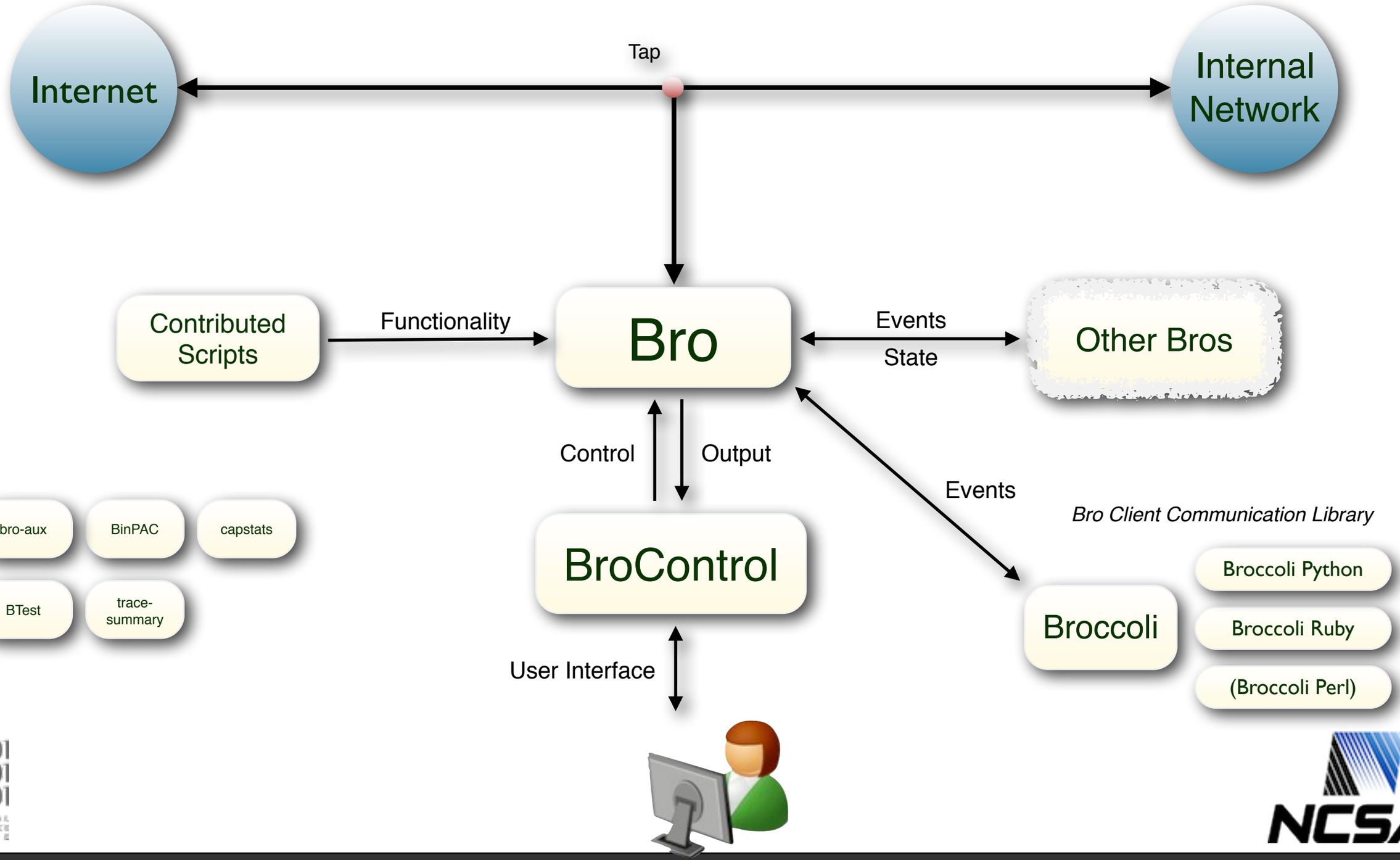
Bro Ecosystem



Bro Ecosystem



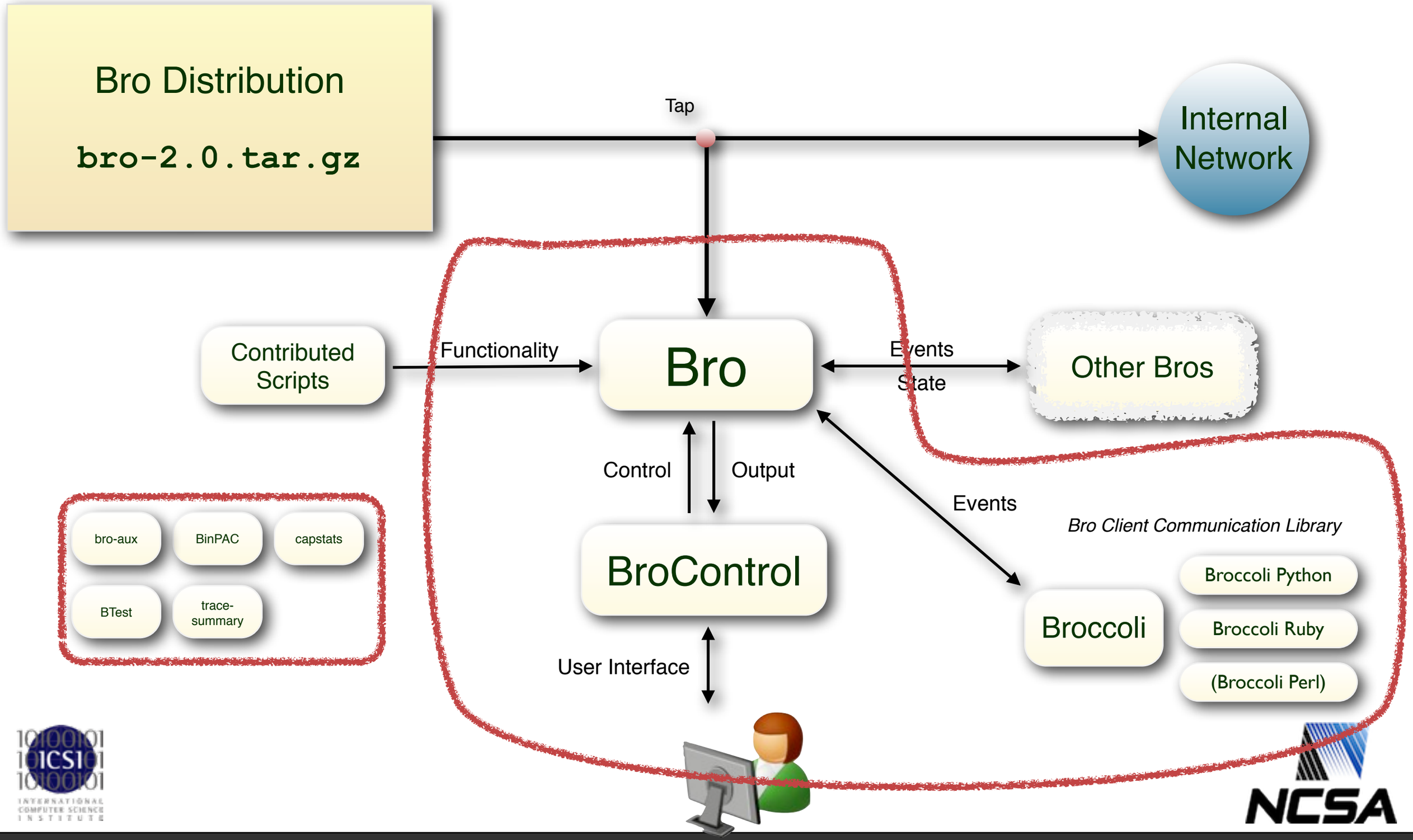
Bro Ecosystem



Bro Ecosystem

Bro Distribution

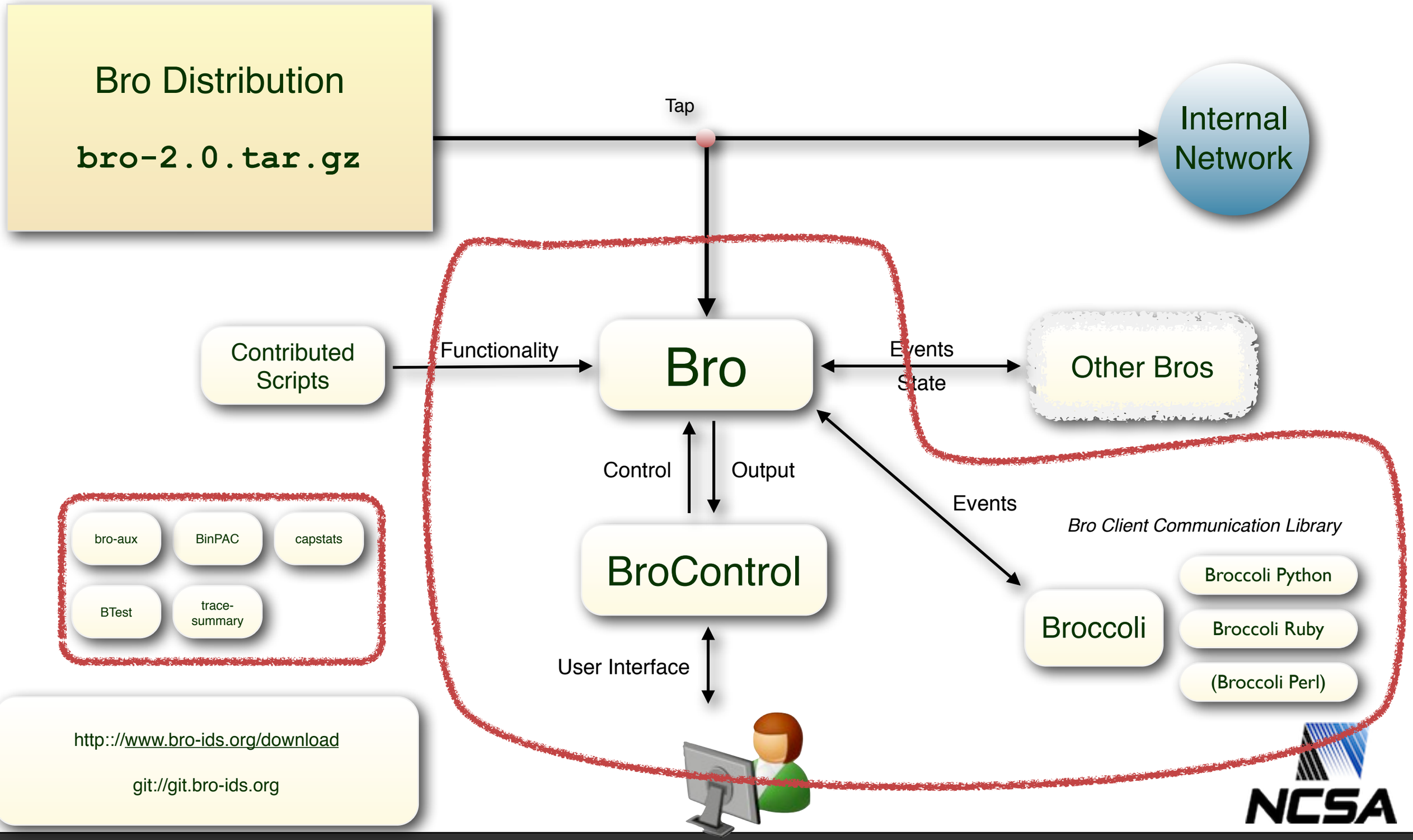
`bro-2.0.tar.gz`



Bro Ecosystem

Bro Distribution

`bro-2.0.tar.gz`

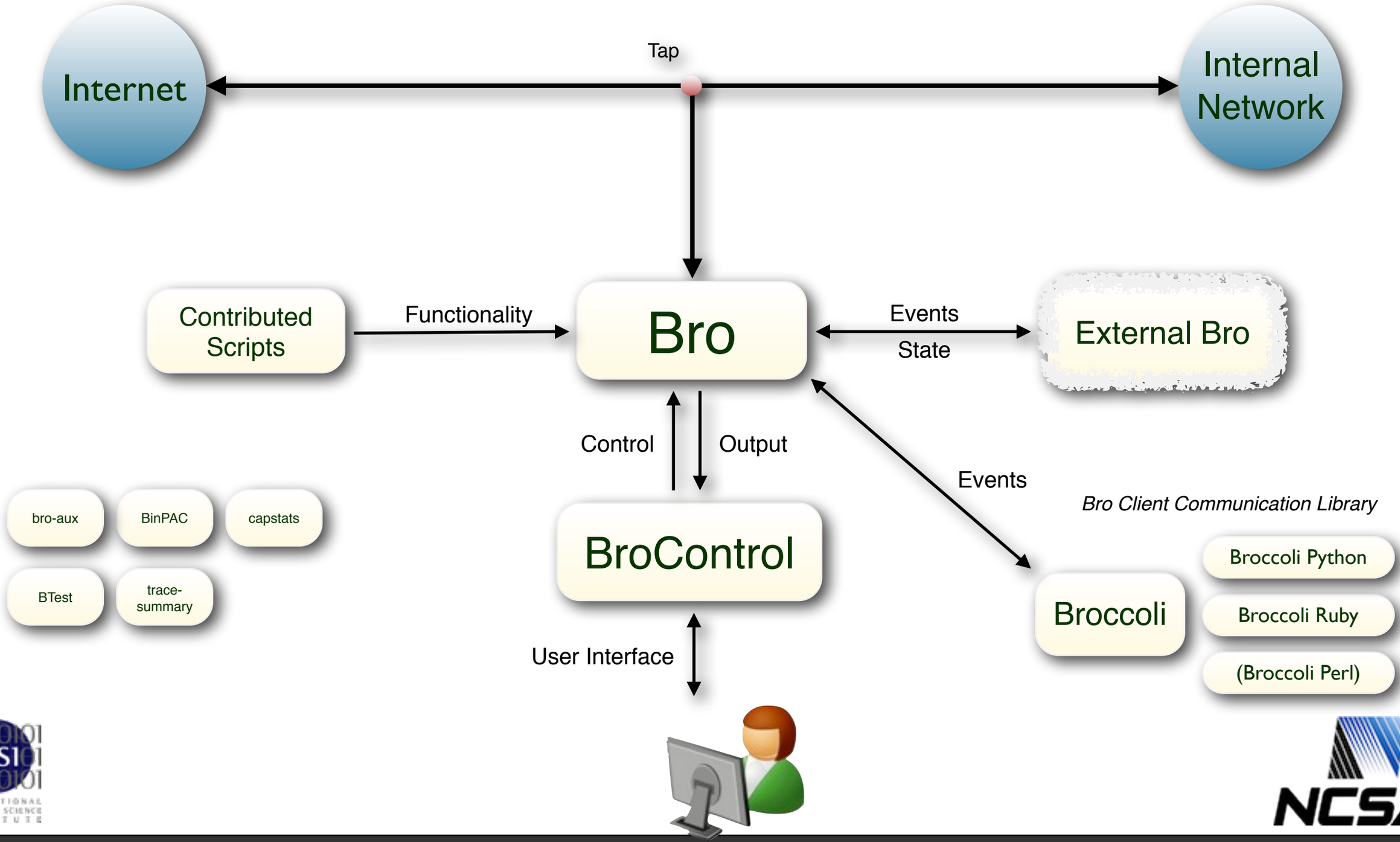


http:://www.bro-ids.org/download

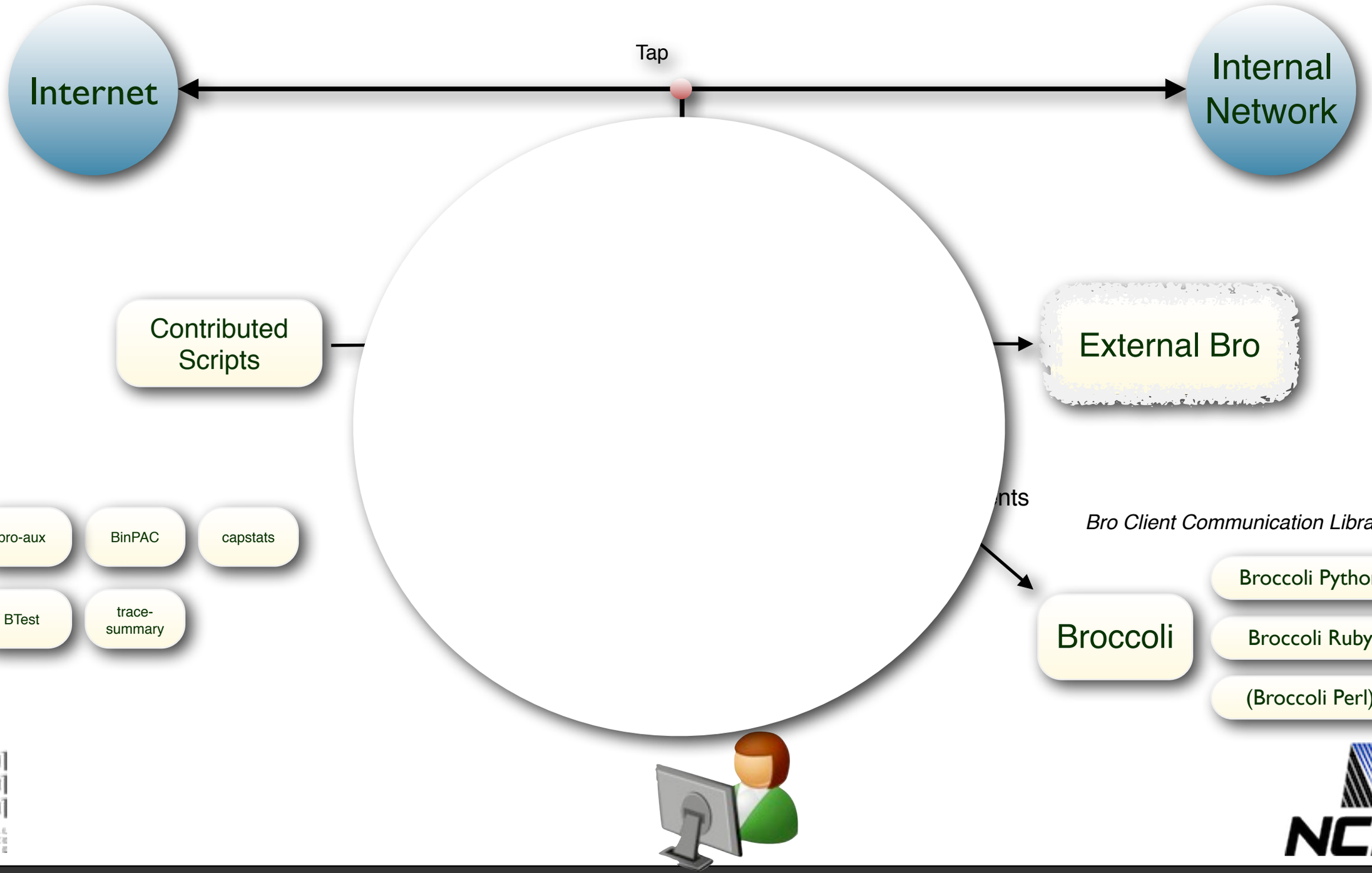
git://git.bro-ids.org

NCSA

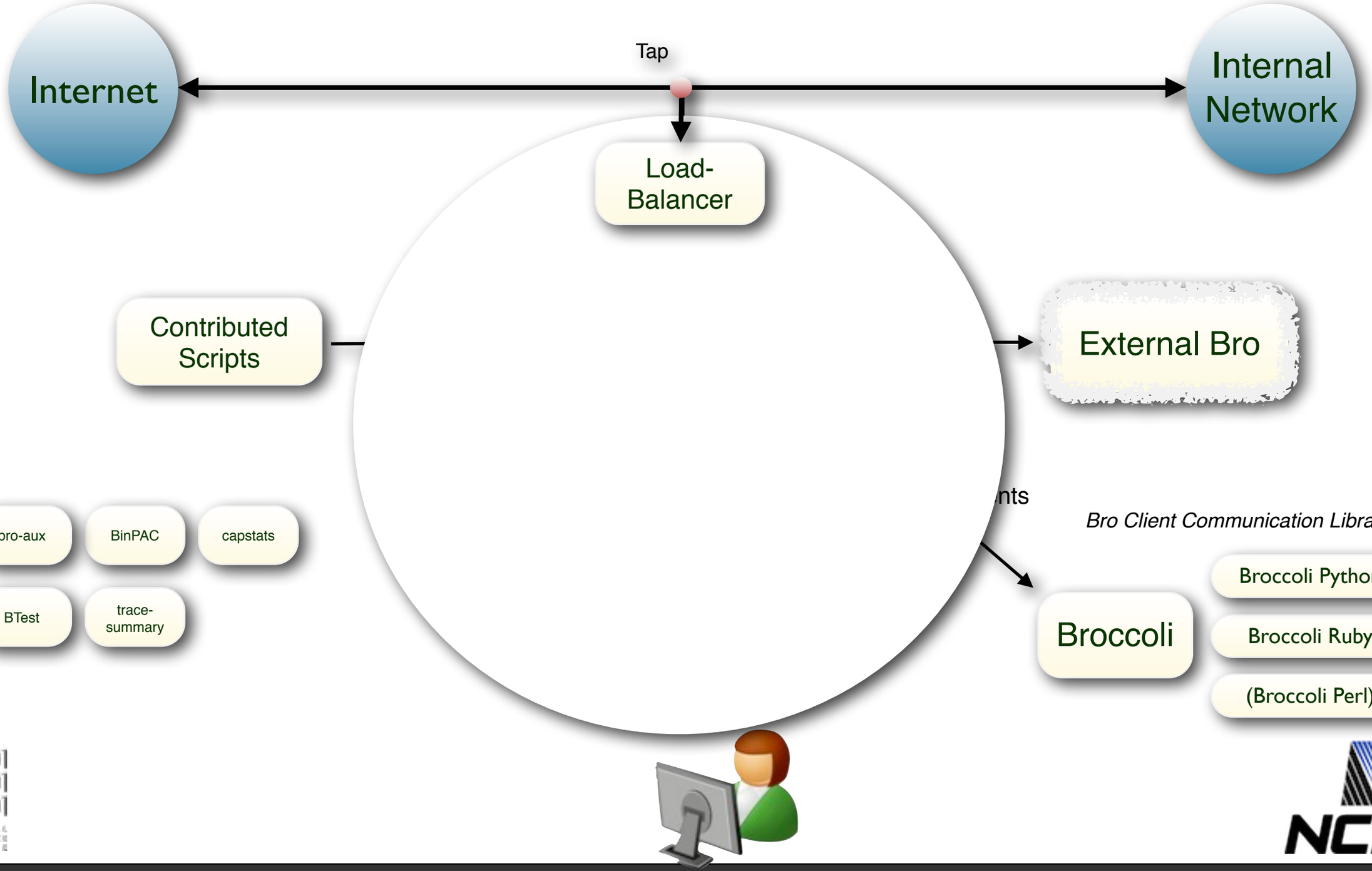
Bro *Cluster* Ecosystem



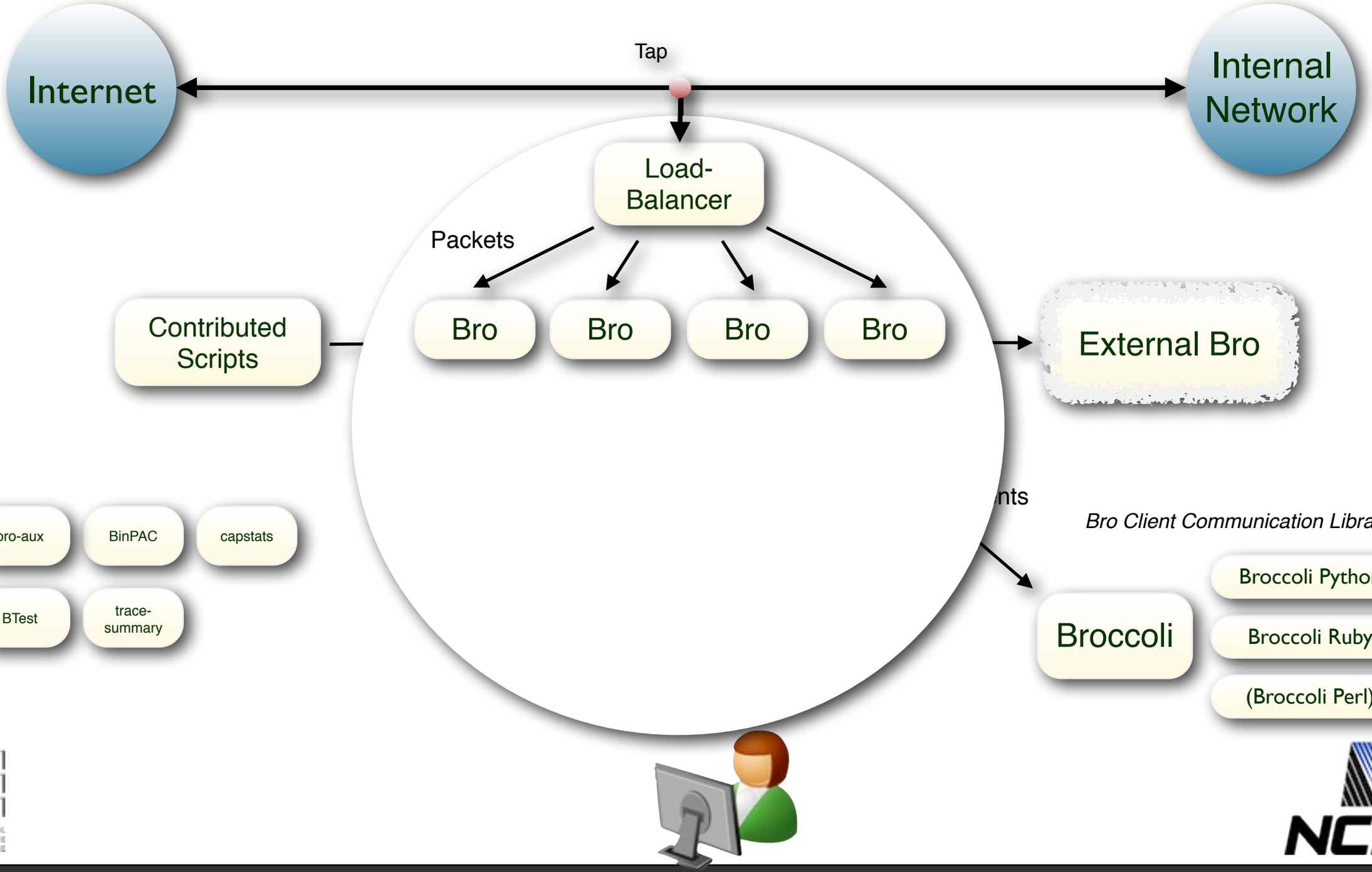
Bro *Cluster* Ecosystem



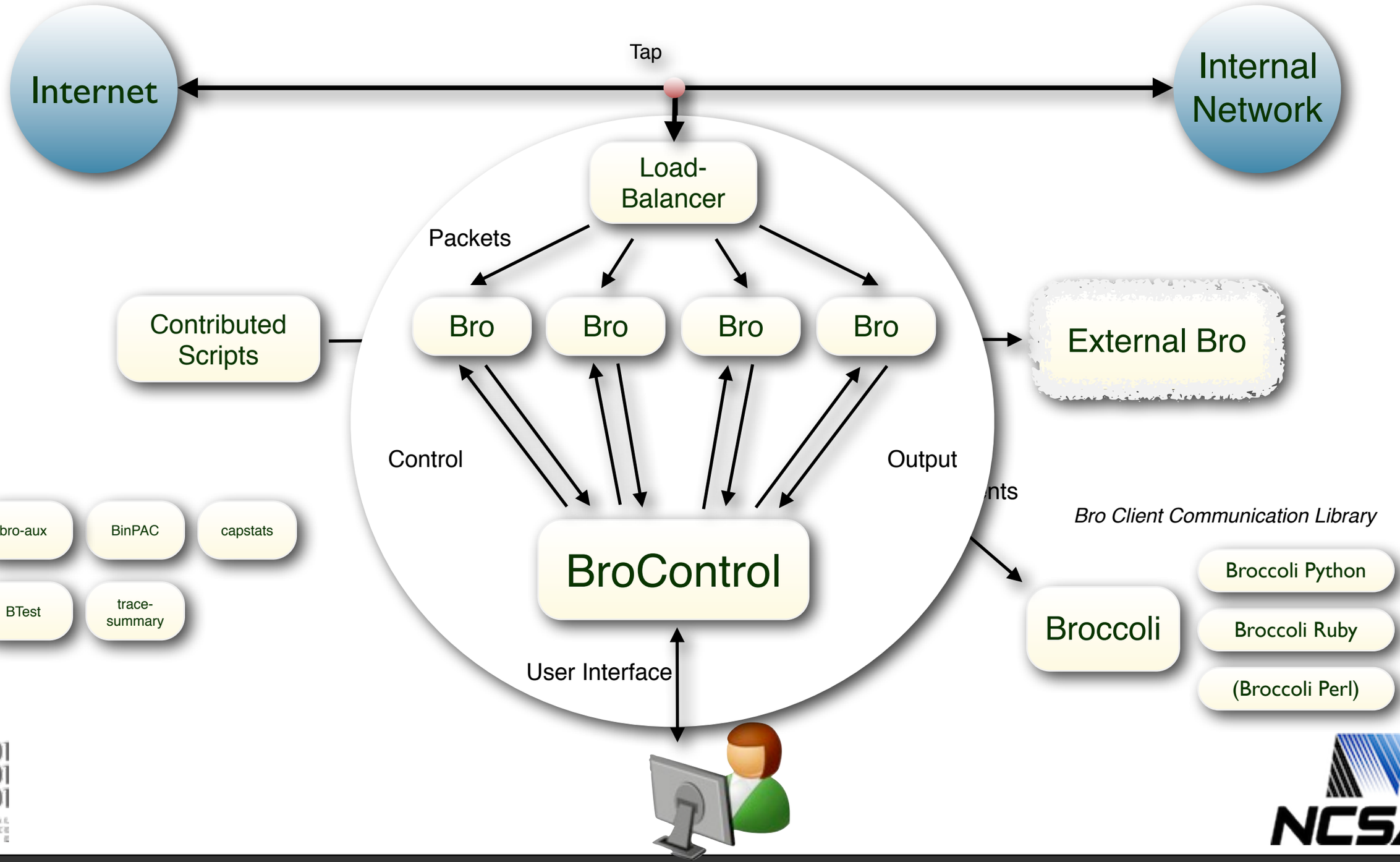
Bro *Cluster* Ecosystem



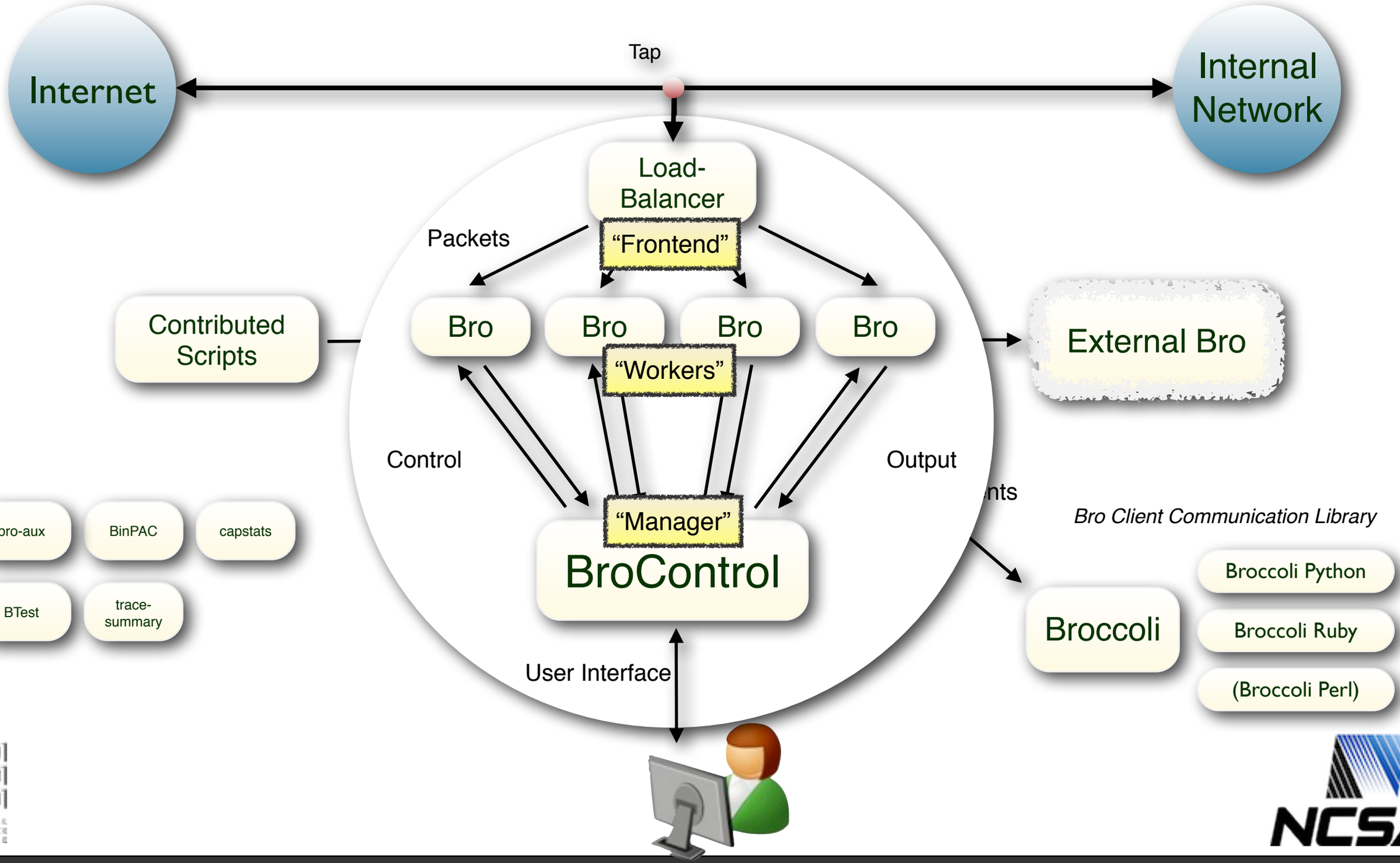
Bro *Cluster* Ecosystem



Bro *Cluster* Ecosystem



Bro *Cluster* Ecosystem

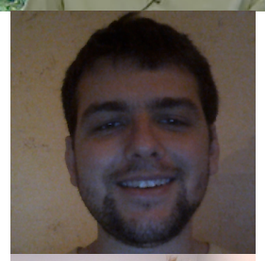


"The Bro Team"

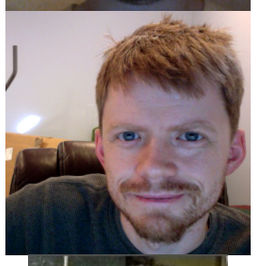
Vern Paxson

Jim Barlow

Gilbert Clark



Seth Hall

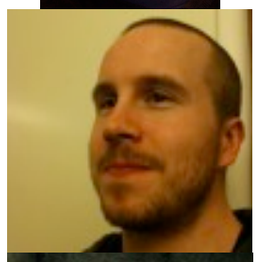


Christian Kreibich

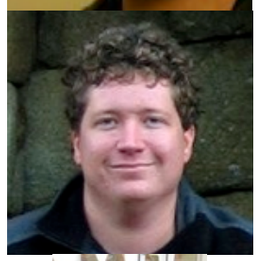
Hui Lin

Gregor Maier

Jonathan Siwek



Adam Slagell



Robin Sommer

Daniel Thayer

Matthias Vallentin