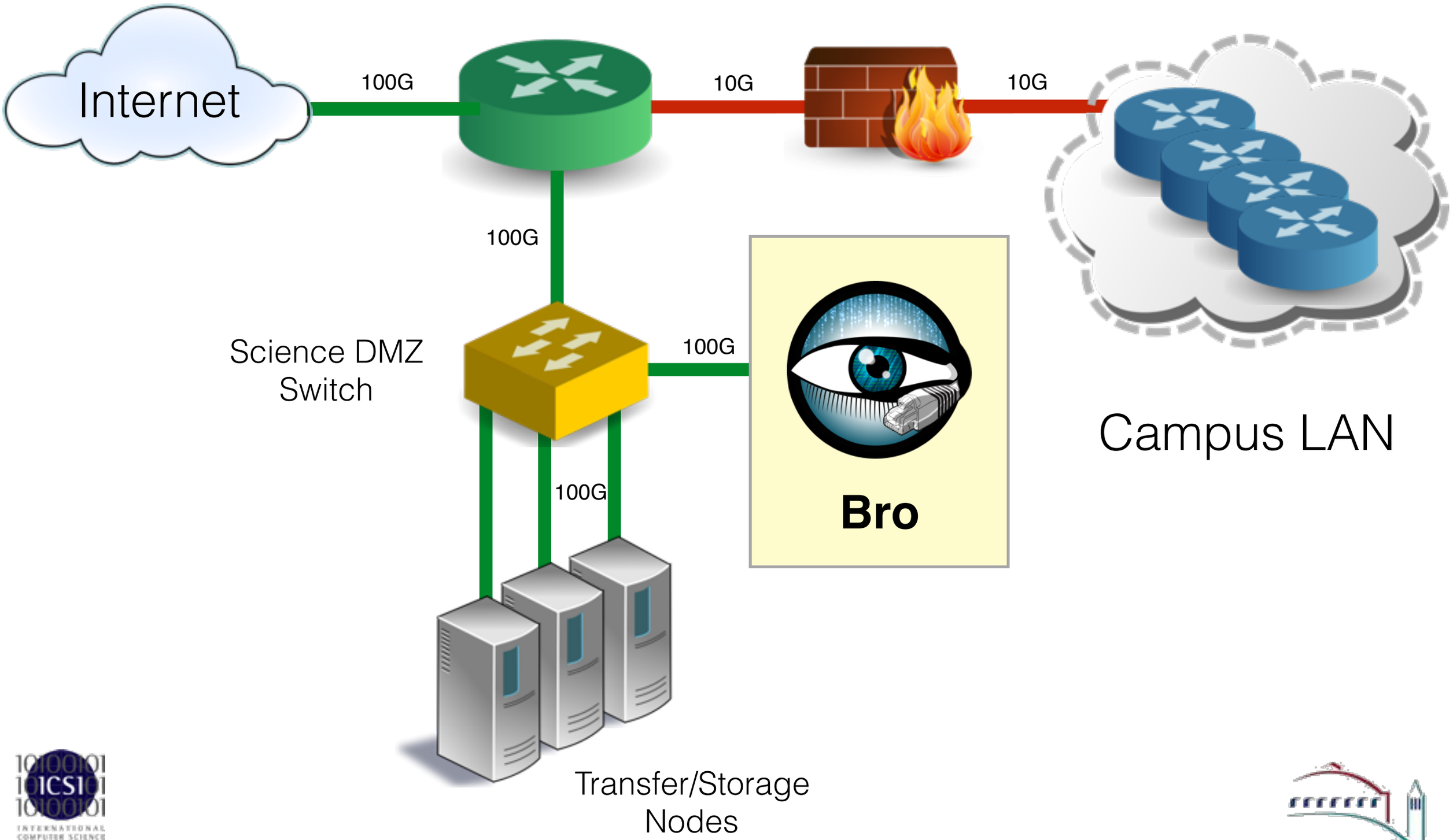
Using Bro to Secure Your Science DMZ

Robin Sommer

International Computer Science Institute, &
Lawrence Berkeley National Laboratory

robin@icsi.berkeley.edu
http://www.icir.org/robin

Securing Your Science DMZ Network



Protecting open-science networks for 20 years now.

Open Source BSD License

Analysis

Intrusion Detection | Vulnerabilit. Mgmt | File Analysis | Traffic Measure-ment | Traffic Control | Compliance Monitoring

Platform

Programming Language | Standard Library

Packet Processing

Tap

Network

Science DMZ Monitoring with Bro

Visibility

- Log files
- Host-level visibility

Detection

Performance

Control

Customization

Connections Logs

conn.log

ts	**1393099191.817686**	Timestamp
uid	**Cy3S2U2sbarorQgmw6a**	Unique ID
id.orig_h	**177.22.211.144**	Originator IP
id.orig_p	**48053**	Originator Port
id.resp_h	**115.25.19.26**	Responder IP
id.resp_p	**2811**	Responder Port
proto	**tcp**	IP Protocol
service	**gridftp,ssl**	App-layer Protocol
duration	**8.405155**	Duration
orig_bytes	**13490**	Bytes by Originator
resp_bytes	**16127**	Bytes by Responder
conn_state	**SF**	TCP state
local_orig	**F**	Local Originator?
history	**ShAdDaFf**	State History
tunnel_parents	**(empty)**	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

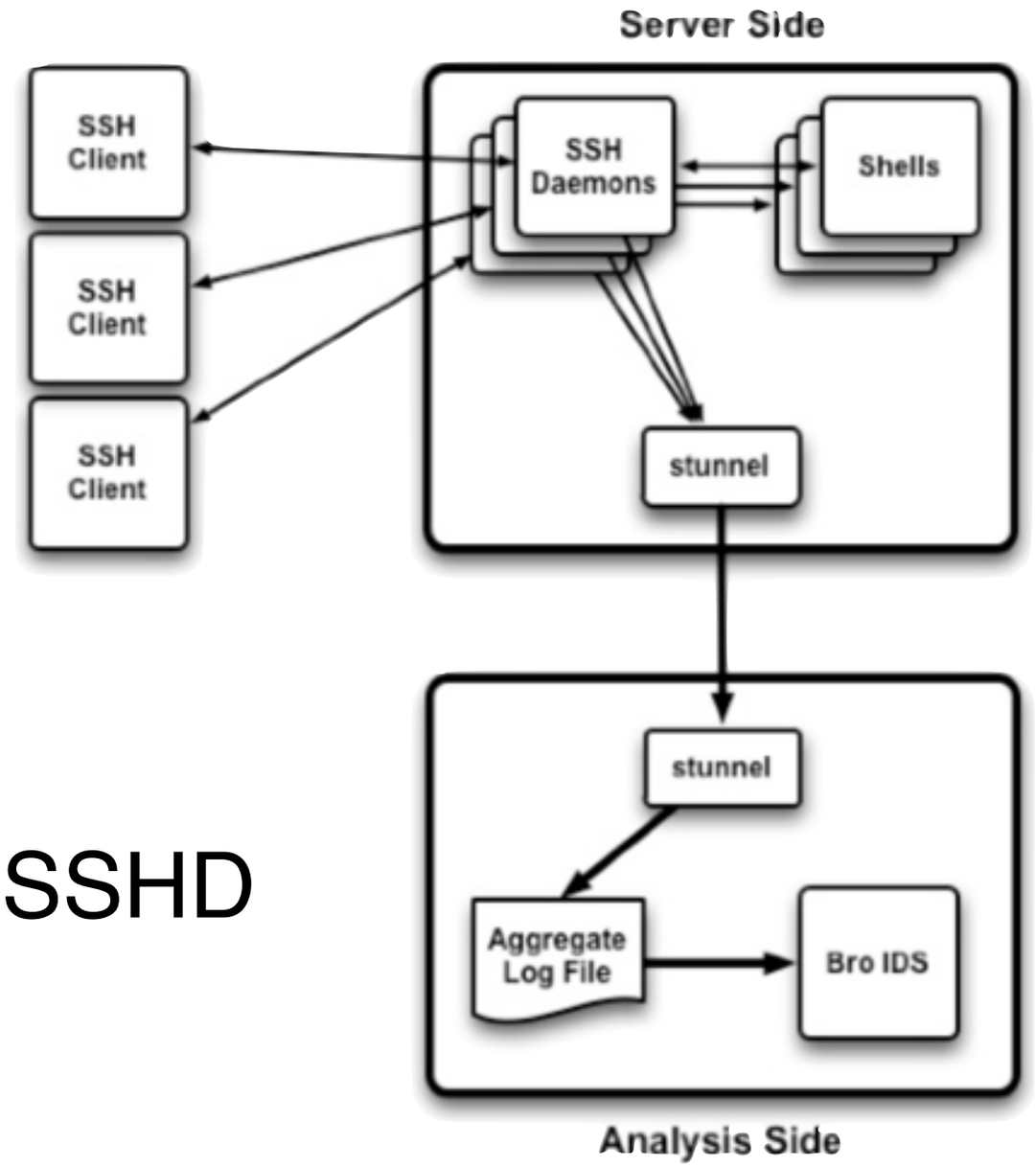
ts	1443449046.841848
uid	CEA05l2D7k0BD9Dda2
id.orig_h	1.2.3.4
id.orig_p	59208
id.resp_h	131.243.231.10
id.resp_p	2811
version	TLSv12
cipher	TLS_RSA_WITH_AES_256_GCM_SHA384
server_name	-
subject	CN=lrc-xfer.lbl.gov,OU=Services,O=Open Science Grid,DC=DigiCert-Grid,DC=com
issuer	CN=DigiCert Grid CA-1,O=DigiCert Grid,DC=DigiCert-Grid,DC=com
client_subject	CN=Foo Bar,O=LBNL HPCS,O=Globus,C=US
client_issuer	CN=GO HPCS ONLINE,OU=HPCS LBNL,DC=LBL,DC=gov
cert_hash	197cab7c6c92a0b9ac5f37cfb0699268
validation_status	ok

Bro Analyzers

AYIYA	Ident	Rlogin
BitTorrent	Kerberos	Rsh
DCE_RPC	Login	SIP
DHCP	Modbus	SMTP
DNP3	MySQL	SNMP
DNS	NCP	SOCKS
DTLS	NFS	SSH
FTP	NTP	SSL
Finger	NetBIOS	Syslog
GTPv1	PE	Telnet
Gnutella	POP3	Teredo
HTTP	Portmapper	X509
ICMP	Radius	ZIP
IRC	RDP	

Host-level Visibility

Leverage control over end hosts.



iSSHD

Source: NERSC

Science DMZ Monitoring with Bro

Visibility

- Log files
- Host-level visibility

Detection

- Suspicious activity
- Intelligence feeds

Performance

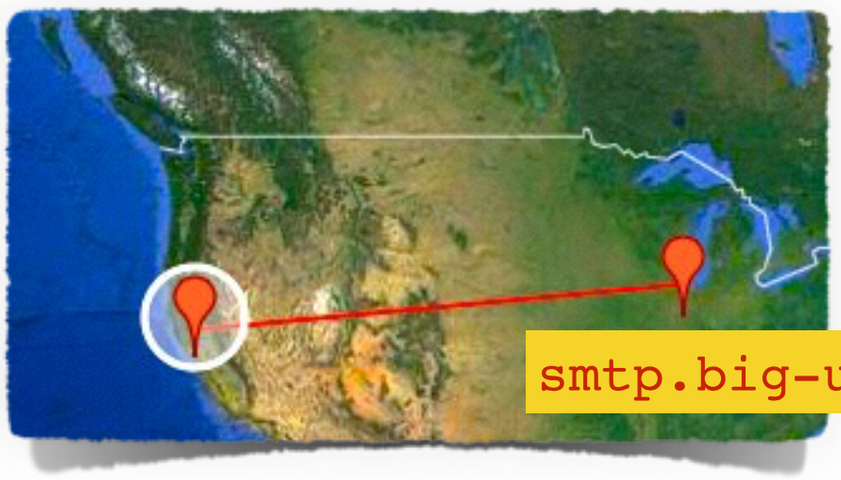
Control

Customization

Watching for Suspicious Logins

`SSH::Watched_Country_Login`

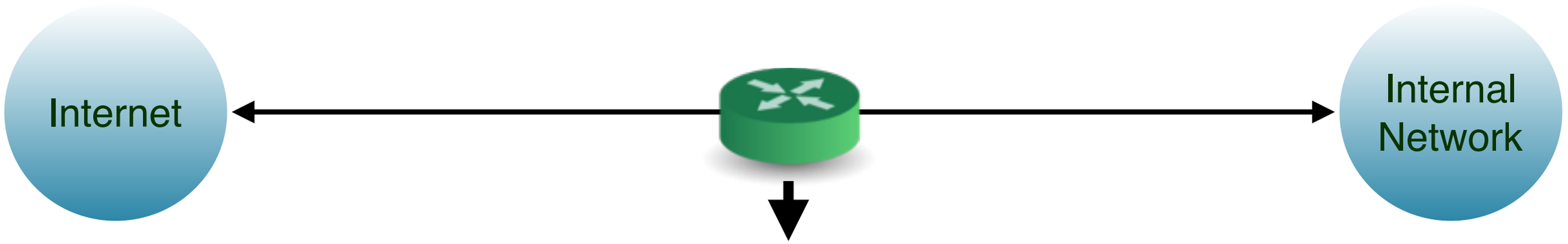
Successful login from an unexpected country.



`SSH::Interesting_Hostname_Login`

Successful login from an unusual host name.

Intelligence Integration



Intelligence

IP addresses
DNS names
URLs
File hashes

Feeds

CIF
JC3
Spamhaus
Custom/Proprietary

Traffic Monitoring

HTTP, FTP, SSL, SSH, FTP,
DNS, SMTP, …

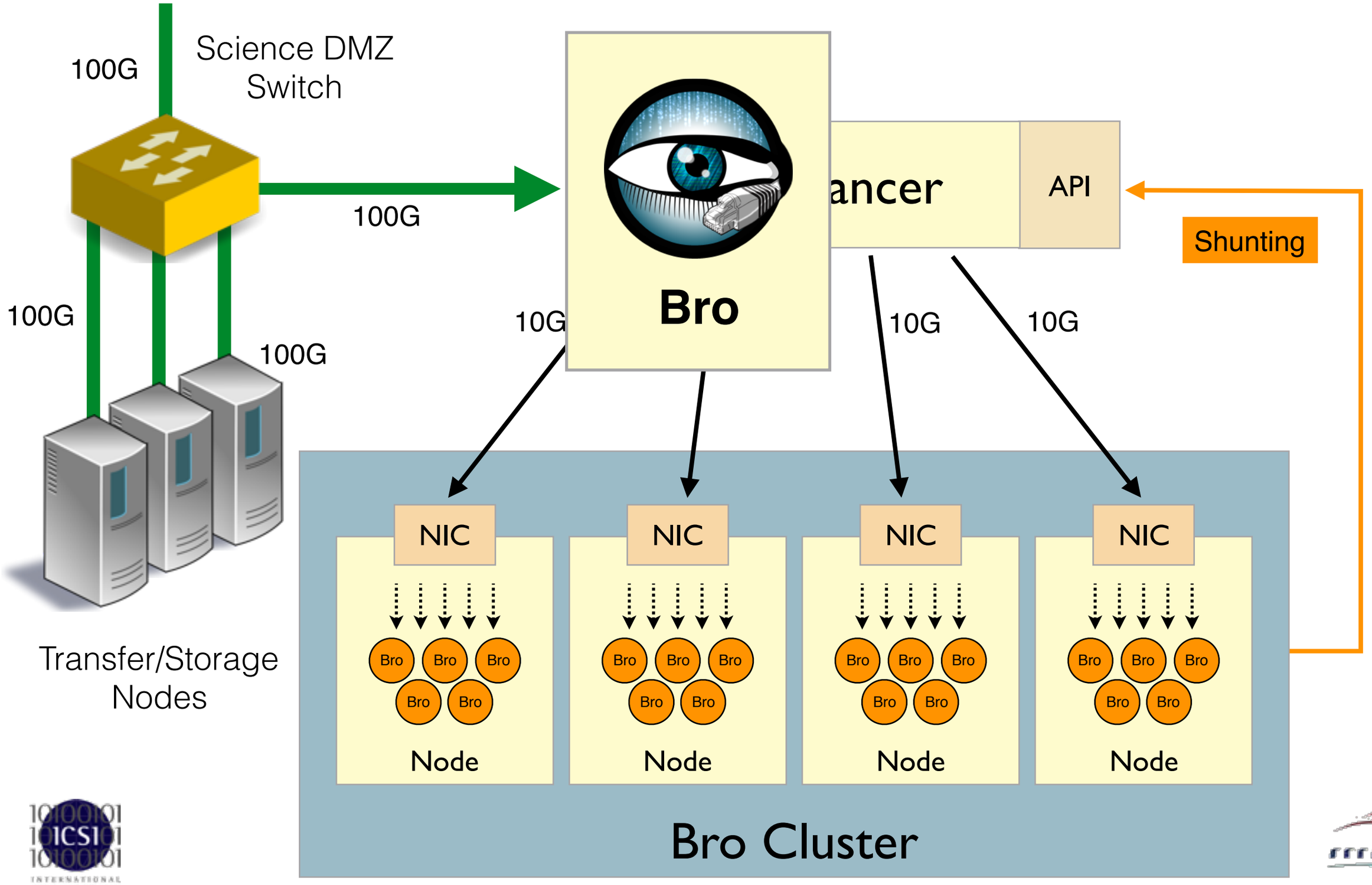
ts	**1258565309.806483**
uid	**CAK677xaOmi66X4Th**
id.orig_h	**192.168.1.103**
id.resp_h	**192.168.1.1**
note	**Intel::Notice**
indicator	**baddomain.com**
indicator_type	**Intel::DOMAIN**
where	**HTTP::IN_HOST_HEADER**
source	**My-Private-Feed**

notice.log

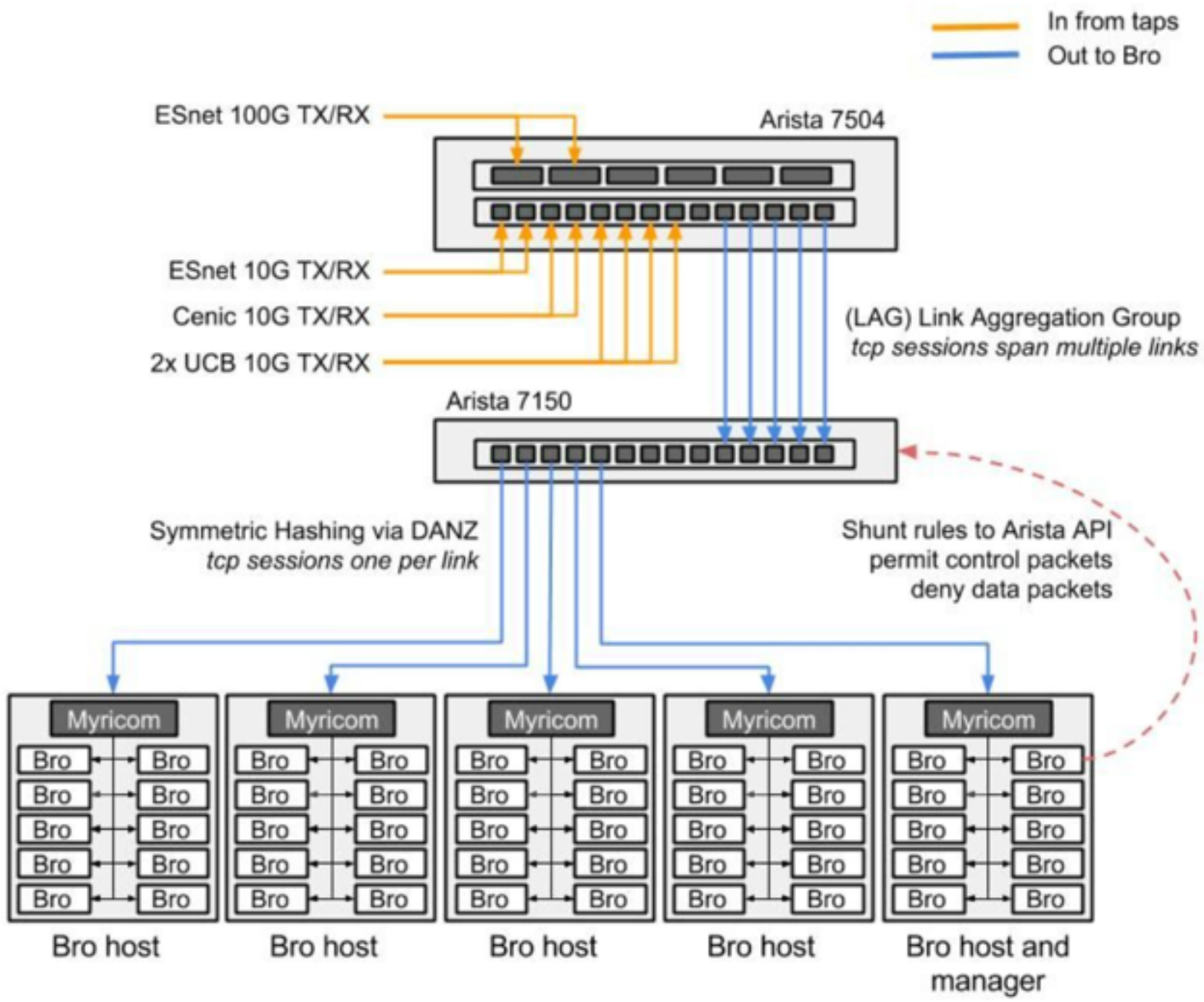
Science DMZ Monitoring with Bro

Visibility	■ Log files ■ Host-level visibility
Detection	■ Suspicious activity ■ Intelligence feeds
Performance	■ Bro Cluster ■ Shunting
Control	
Customization	

Scaling Bro to 100G

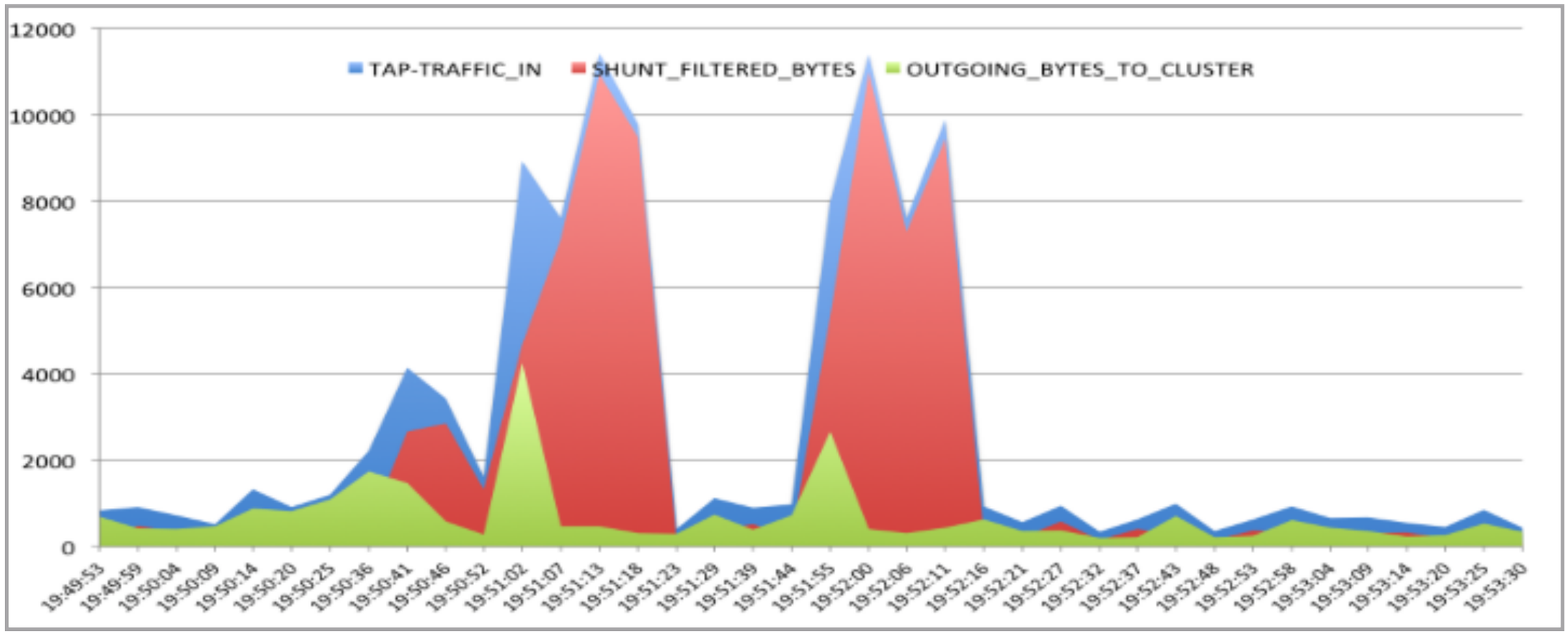


100G Bro at LBNL



http://go.lbl.gov/100g

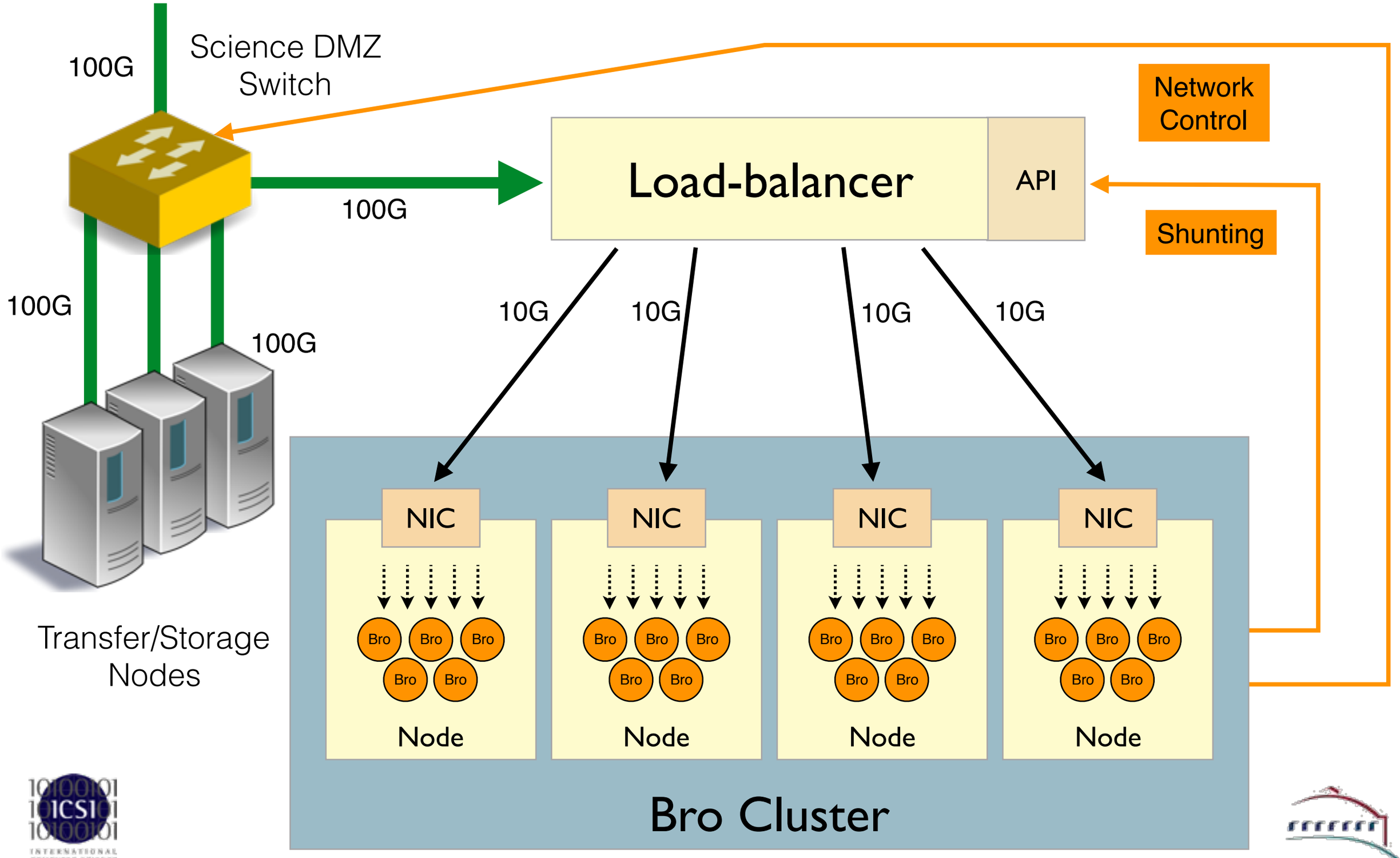
Shunting at LBNL



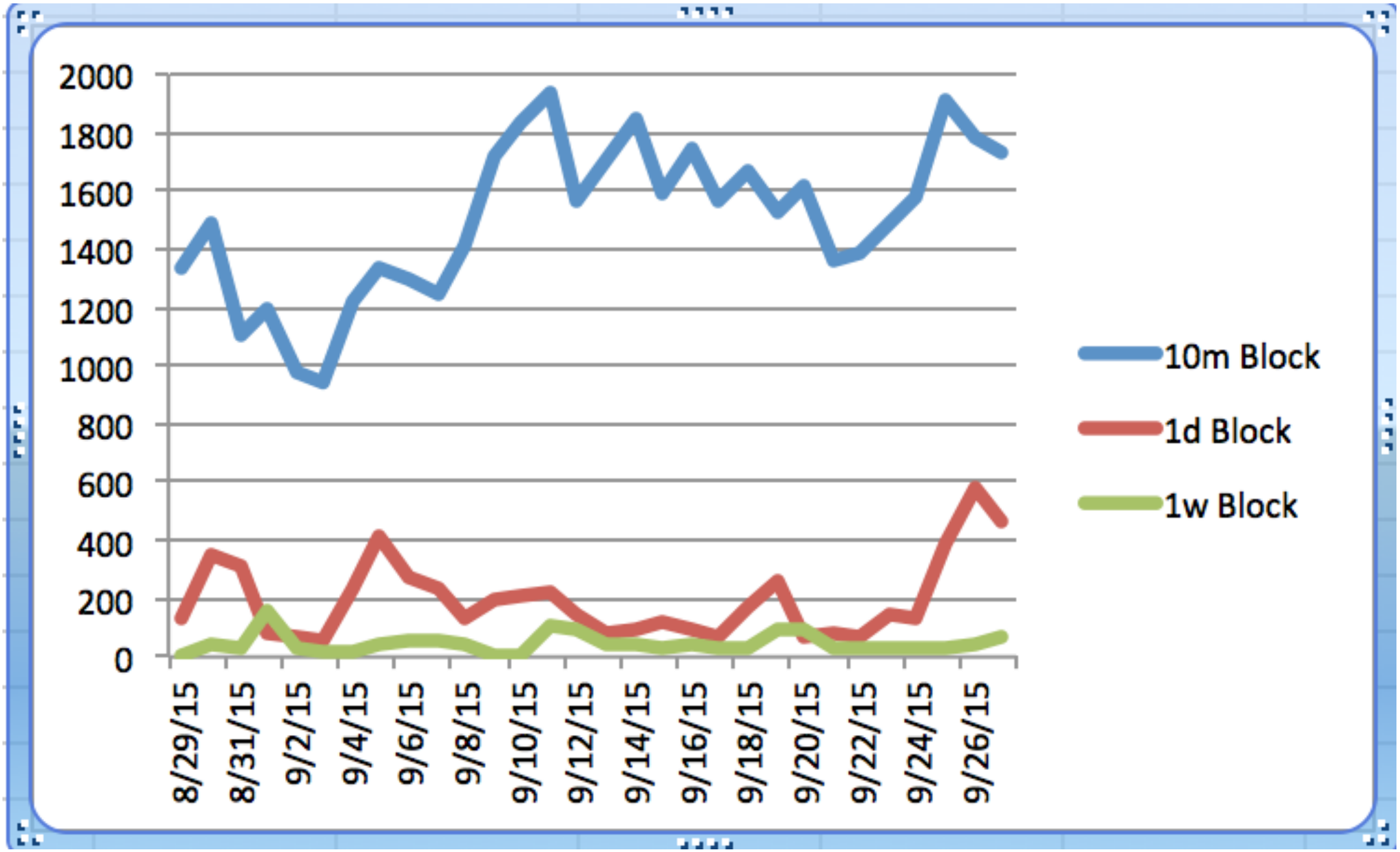
Science DMZ Monitoring with Bro

Visibility	■ Log files ■ Host-level visibility
Detection	■ Suspicious activity ■ Intelligence feeds
Performance	■ Bro Cluster ■ Shunting
Control	■ Black- and whitelisting ■ Traffic engineering
Customization	

Network Control

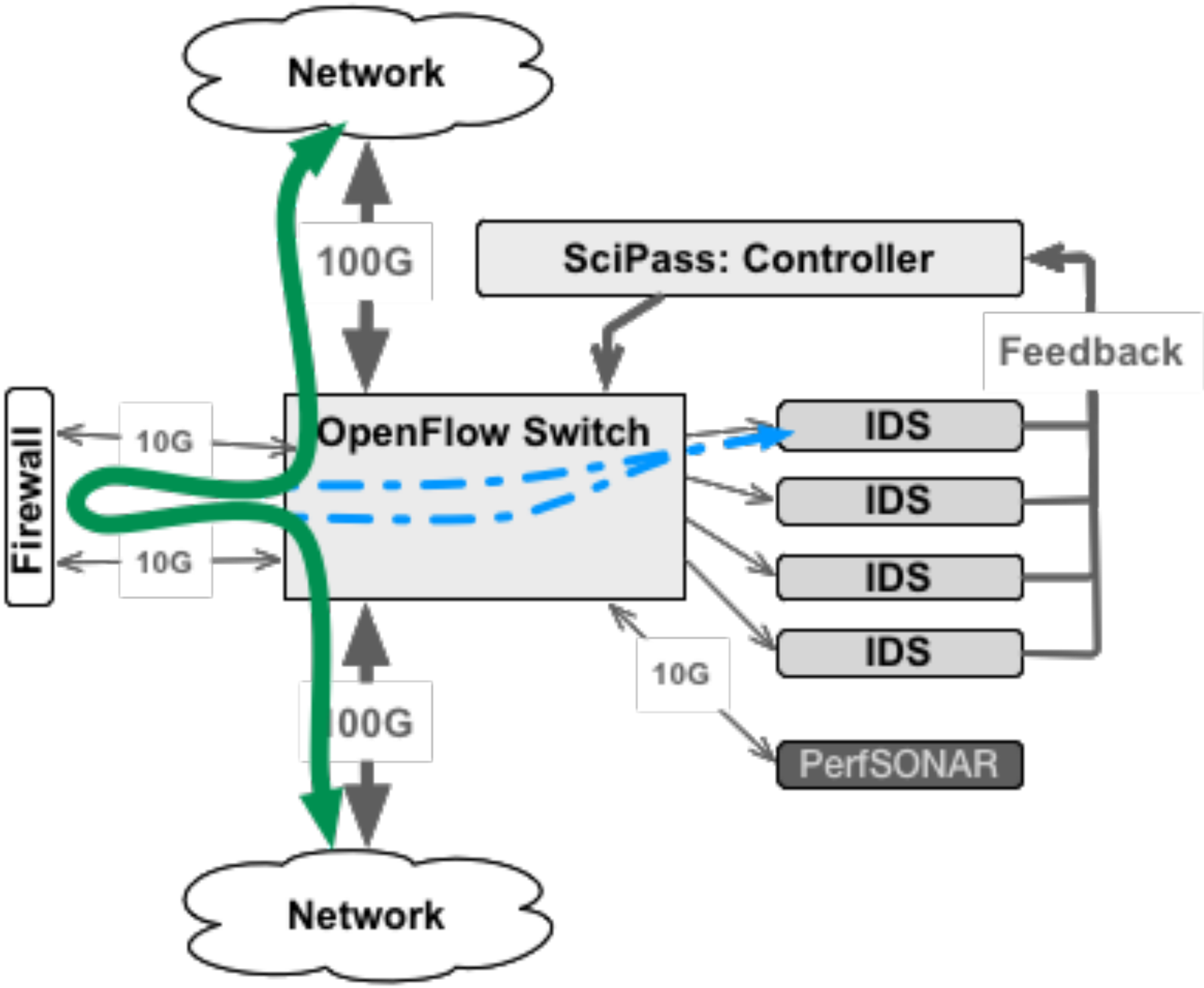


Blacklisting: "Catch & Release" Dropping



Source: Indiana Unversity

Whitelisting: IU's SciPass



Source: Indiana University

Upcoming: Bro's NetControl Framework

drop_connection (*connection*, *timeout*)

drop_address (*host*, *timeout*)

shunt_flow (*flow*, *timeout*)

redirect (flow, port, timeout)

Backends

OpenFlow, iptables, acld; Arista planned.

Science DMZ Monitoring with Bro

Visibility	■ Log files ■ Host-level visibility
Detection	■ Suspicious activity ■ Intelligence feeds
Performance	■ Bro Cluster ■ Shunting
Control	■ Black- and whitelisting ■ Traffic engineering
Customization	■ Write your own scripts!

Scripts are Bro's "Magic Ingredient"

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

Prewritten functionality that's just loaded.

Scripts generate & do everything we have seen.

Amendable to extensive customization and extension.

User community writing 3rd party scripts.

Mozilla just released >20 scripts.

Script Example: Shunting

Task: Shunt all GridFTP data connections.

```
event GridFTP::data_channel_detected(c: connection) {

    NetControl::shunt_flow(
      [$src_h=c$id$orig_h, $src_p=c$id$orig_p,
       $dst_h=c$id$resp_h, $resp_p=c$id$resp_p], 1hr);

}
```

Script Example: Scan Detector

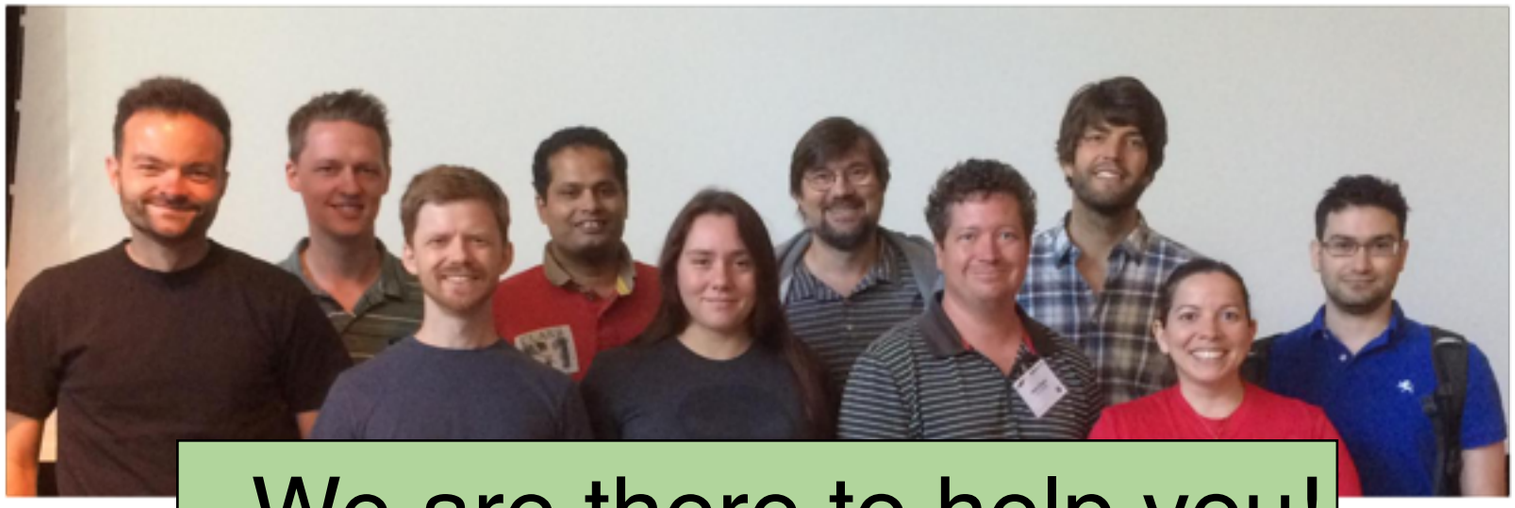
Task: Count failed connection attempts per source address.

```
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.
        NetControl::drop_address(source, 1hr); # Drop host.
}
```

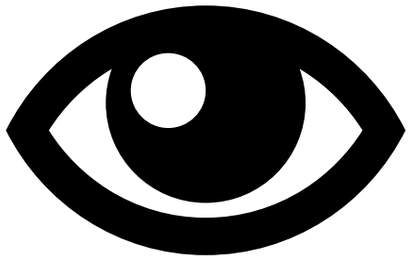
Science DMZ Monitoring with Bro

Visibility	■ Log files ■ Host-level visibility
Detection	■ Suspicious activity ■ Intelligence feeds
Performance	■ Bro Cluster ■ Shunting
Control	■ Black- and whitelisting ■ Traffic engineering
Customization	■ Write your own scripts!

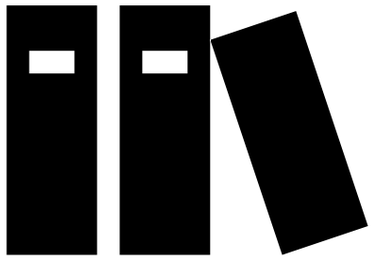
The NSF Bro Center of Expertise



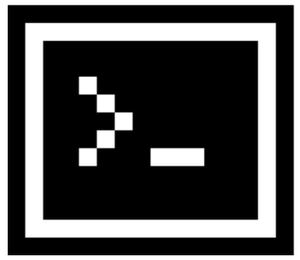
We are there to help you!



Individual Advice



Training Material, Best Practices



Development, Maintenance

http://nsf.bro.org mailto:nsf@bro.org

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 Expertise at the International Computer Science Institute and the National Center for Supercomputing Applications.

The Bro Project is a member of Software Freedom Conservancy.

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 Support
www.broala.com
info@broala.com
@Broala_