



# Using Bro to Secure Your Science DMZ

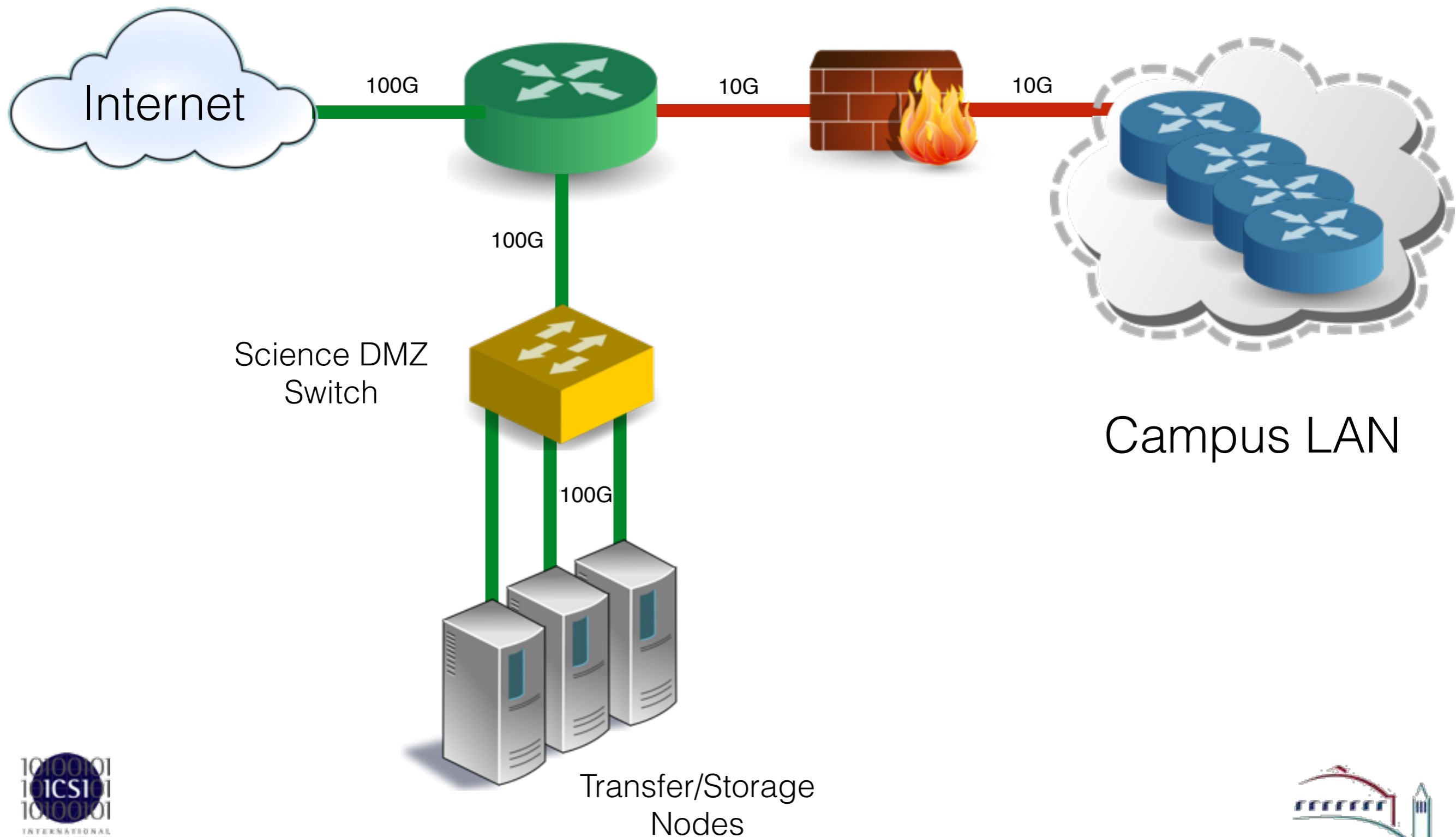
Robin Sommer

International Computer Science Institute, &  
Lawrence Berkeley National Laboratory

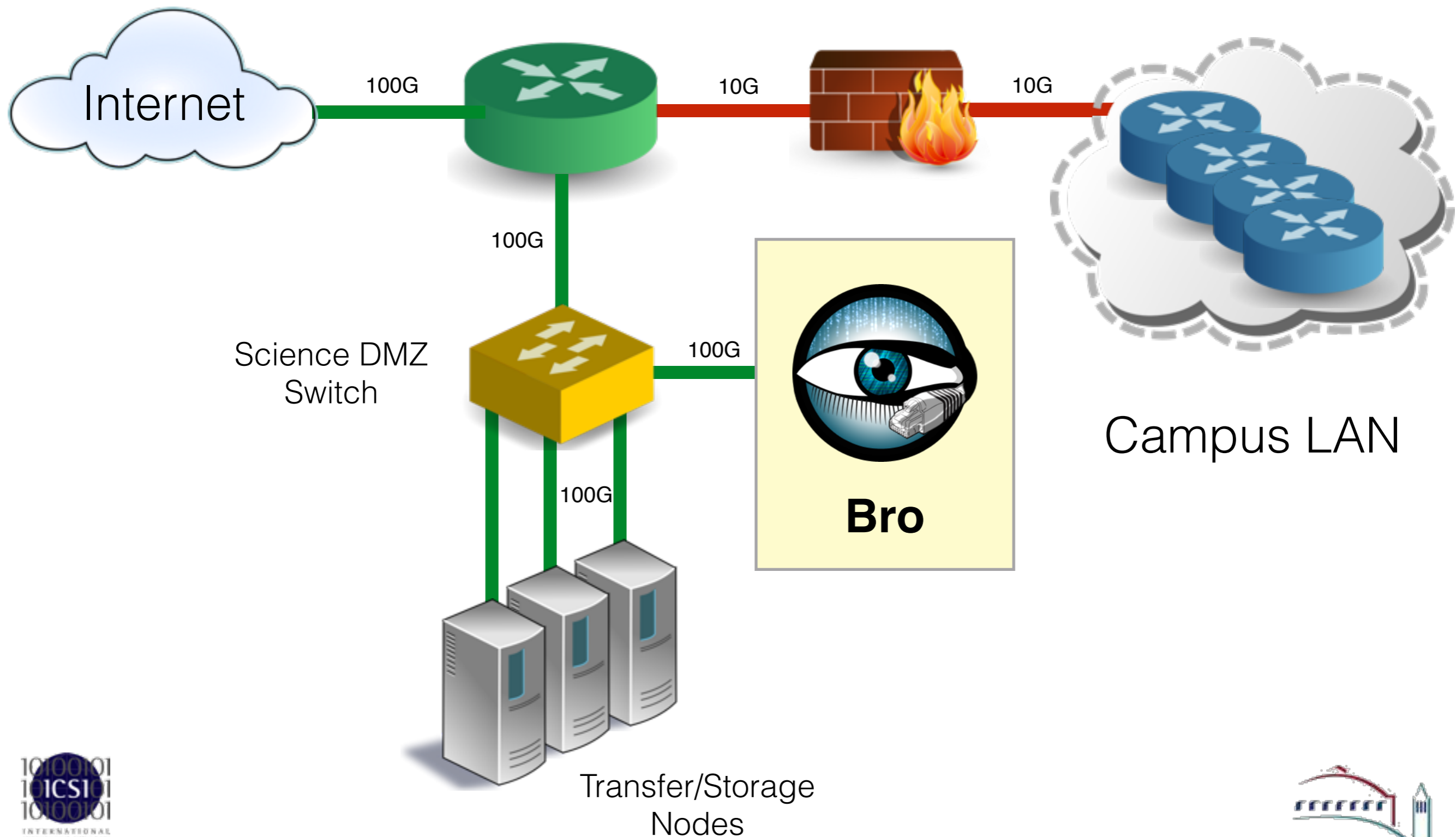
`robin@icsi.berkeley.edu`  
`http://www.icir.org/robin`



# Securing Your Science DMZ Network



# Securing Your Science DMZ Network



# The Bro Platform

---

# The Bro Platform

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

# 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

Detection

Performance

Control

Customization

# Science DMZ Monitoring with Bro

---

Visibility

- Log files
- Host-level visibility

Detection

Performance

Control

Customization

# Connections Logs

---

# Connections Logs

conn.log

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

# HTTP

http.log

ts	1393099291.589208
uid	CKFUW73bIADw0r9p1
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

<b>ts</b>	<b>1443449046.841848</b>
<b>uid</b>	<b>CEA0512D7k0BD9Dda2</b>
<b>id.orig_h</b>	<b>1.2.3.4</b>
<b>id.orig_p</b>	<b>59208</b>
<b>id.resp_h</b>	<b>131.243.231.10</b>
<b>id.resp_p</b>	<b>2811</b>
<b>version</b>	<b>TLSv12</b>
<b>cipher</b>	<b>TLS_RSA_WITH_AES_256_GCM_SHA384</b>
<b>server_name</b>	<b>-</b>
<b>subject</b>	<b>CN=lrc-xfer.lbl.gov,OU=Services,O=Open Science Grid,DC=DigiCert-Grid,DC=com</b>
<b>issuer</b>	<b>CN=DigiCert Grid CA-1,O=DigiCert Grid,DC=DigiCert-Grid,DC=com</b>
<b>client_subject</b>	<b>CN=Foo Bar,O=LBL HPCS,O=Globus,C=US</b>
<b>client_issuer</b>	<b>CN=GO HPCS ONLINE,OU=HPCS LBL,DC=LBL,DC=gov</b>
<b>cert_hash</b>	<b>197cab7c6c92a0b9ac5f37cfb0699268</b>
<b>validation_status</b>	<b>ok</b>

# 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	

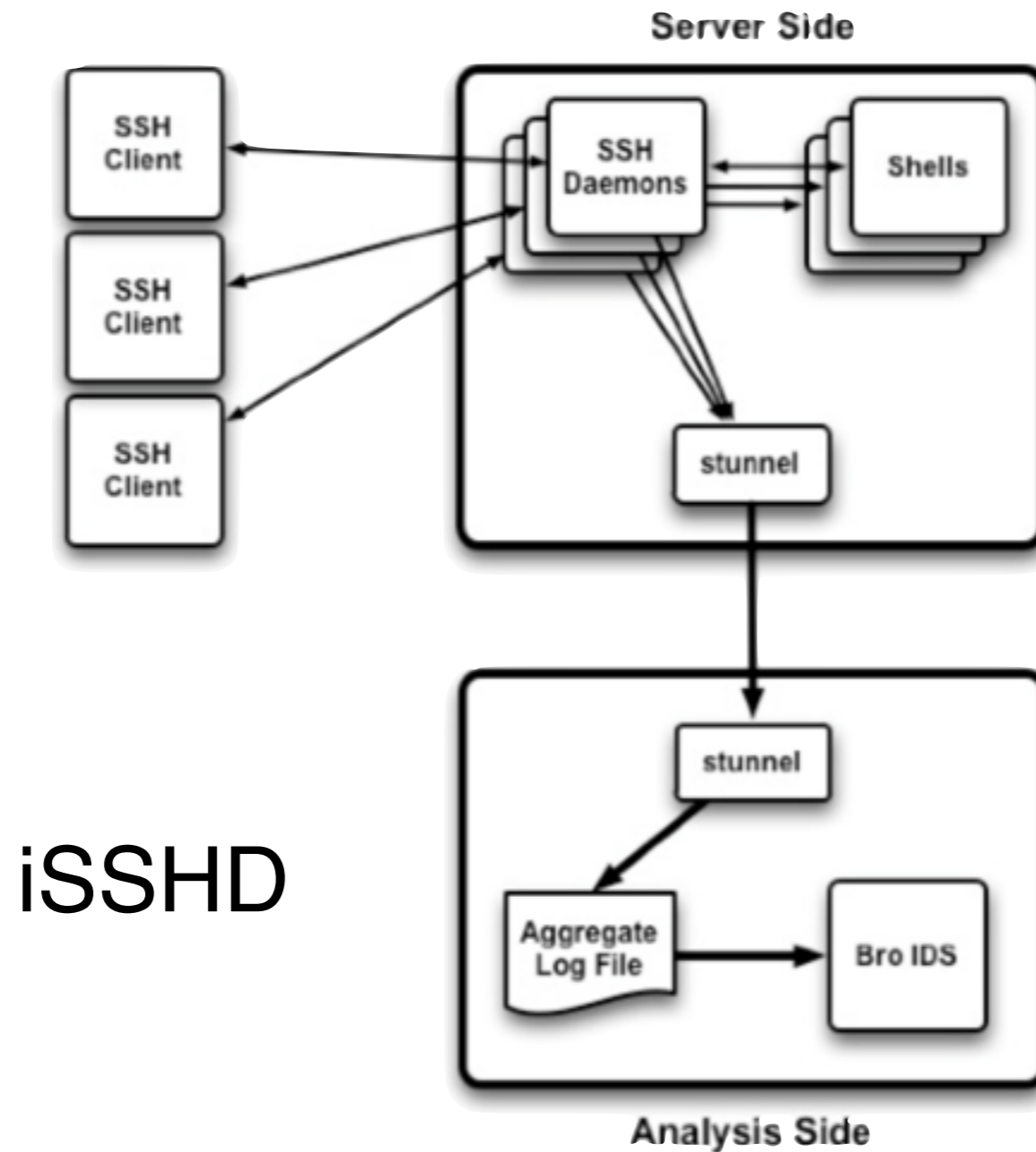
# Host-level Visibility

---

Leverage control over end hosts.

# Host-level Visibility

Leverage control over end hosts.



Source: NERSC



# Science DMZ Monitoring with Bro

---

Visibility

- Log files
- Host-level visibility

Detection

Performance

Control

Customization

# Science DMZ Monitoring with Bro

---

## Visibility

- Log files
- Host-level visibility

## Detection

- Suspicious activity
- Intelligence feeds

## Performance

## Control

## Customization

# Watching for Suspicious Logins

---

# Watching for Suspicious Logins

---

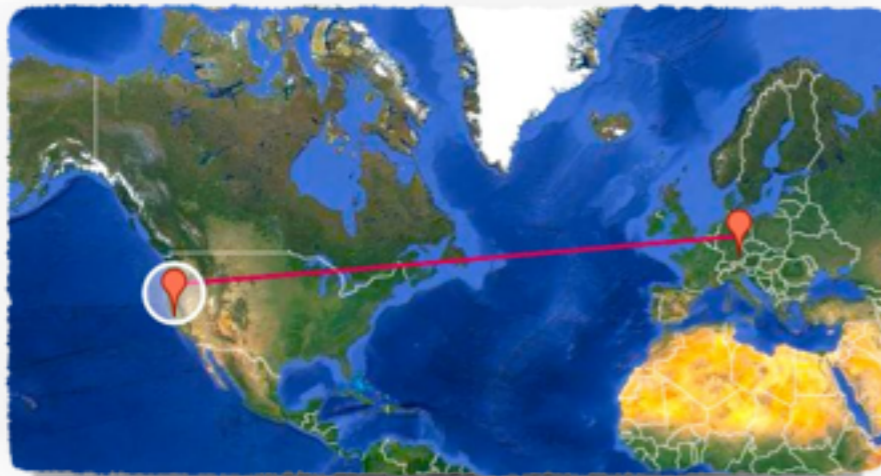


**SSH: :Watched\_Country\_Login**

Successful login from an unexpected country.

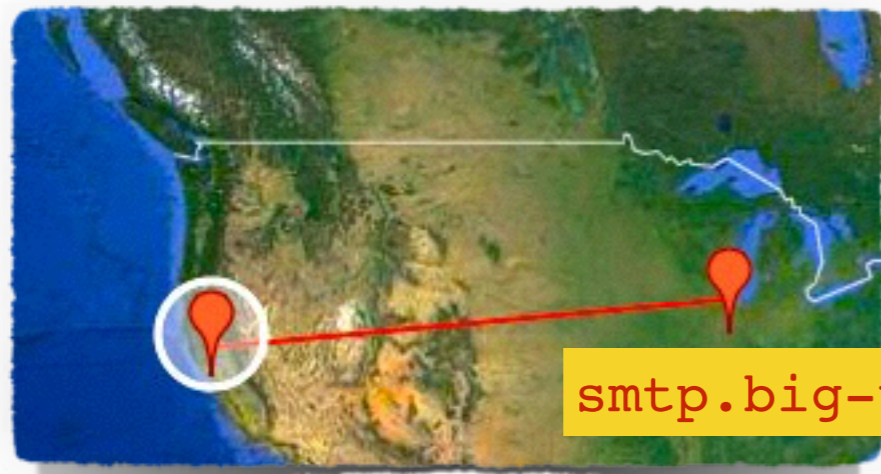
# Watching for Suspicious Logins

---



## **SSH::Watched\_Country\_Login**

Successful login from an unexpected country.



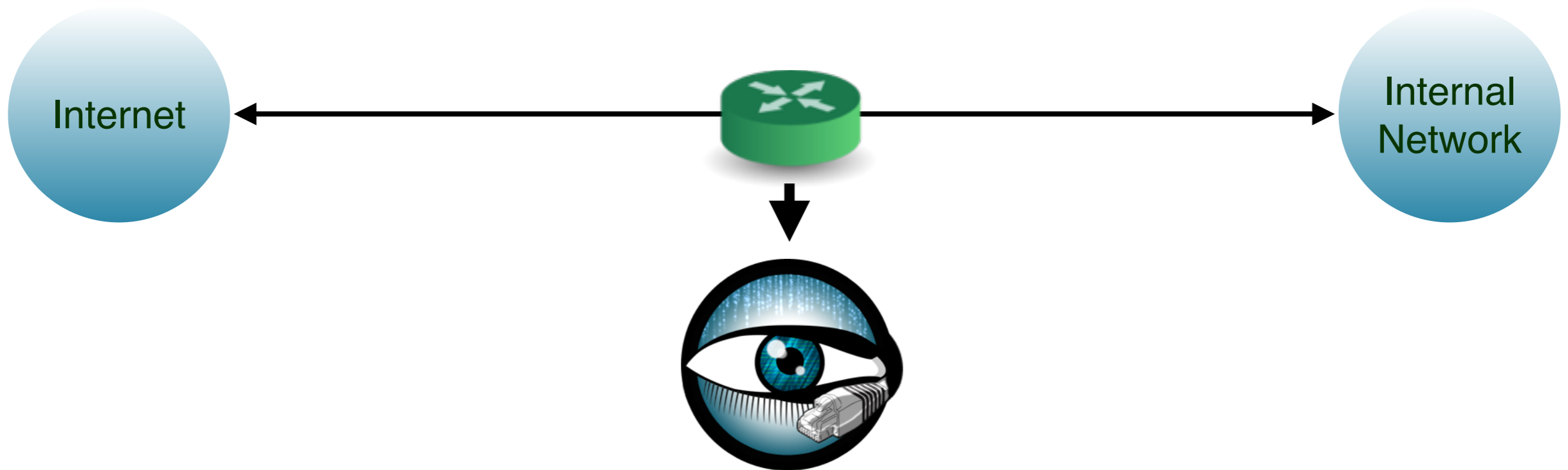
## **SSH::Interesting\_Hostname\_Login**

Successful login from an unusual host name.

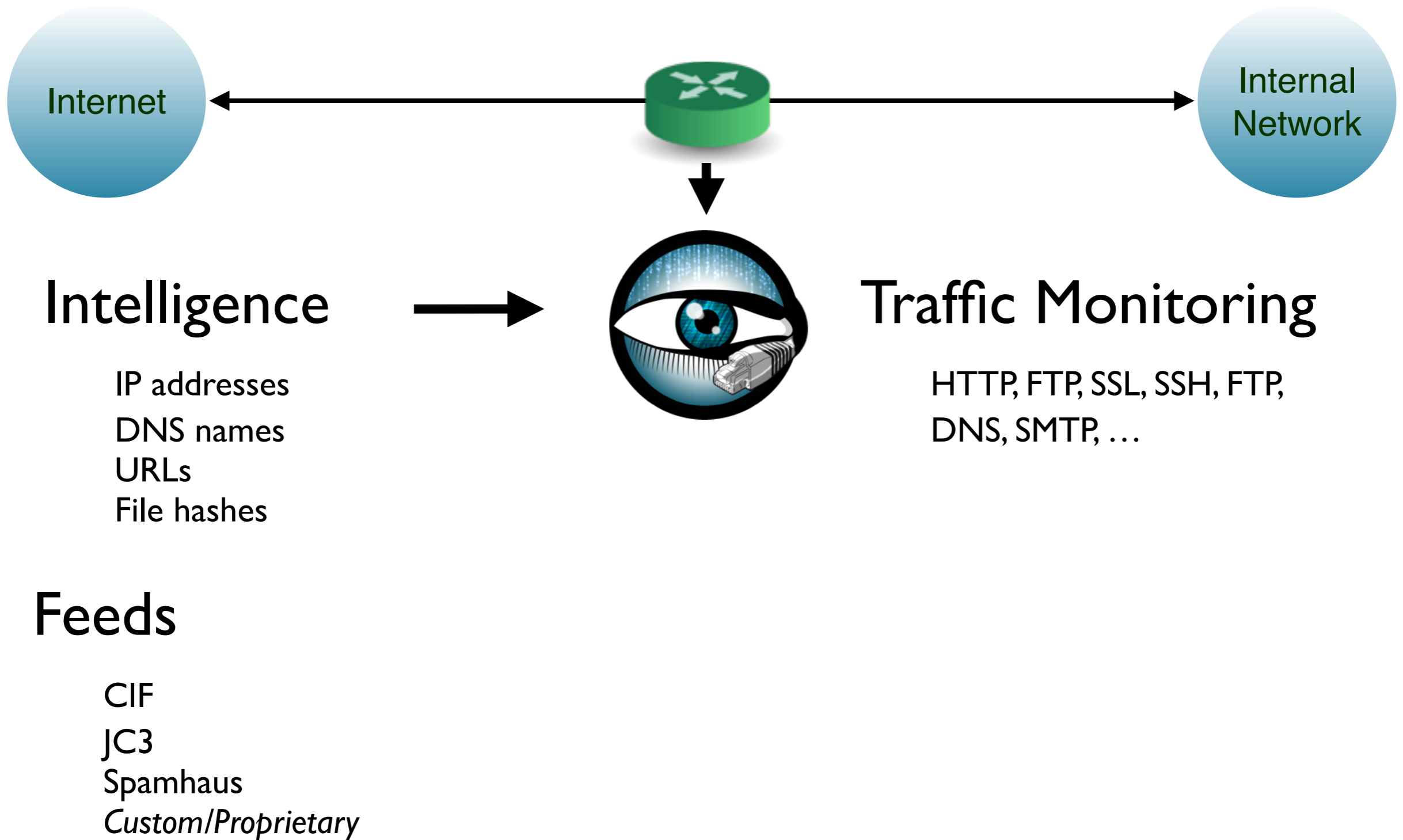
`smtp.big-university.edu`

# Intelligence Integration

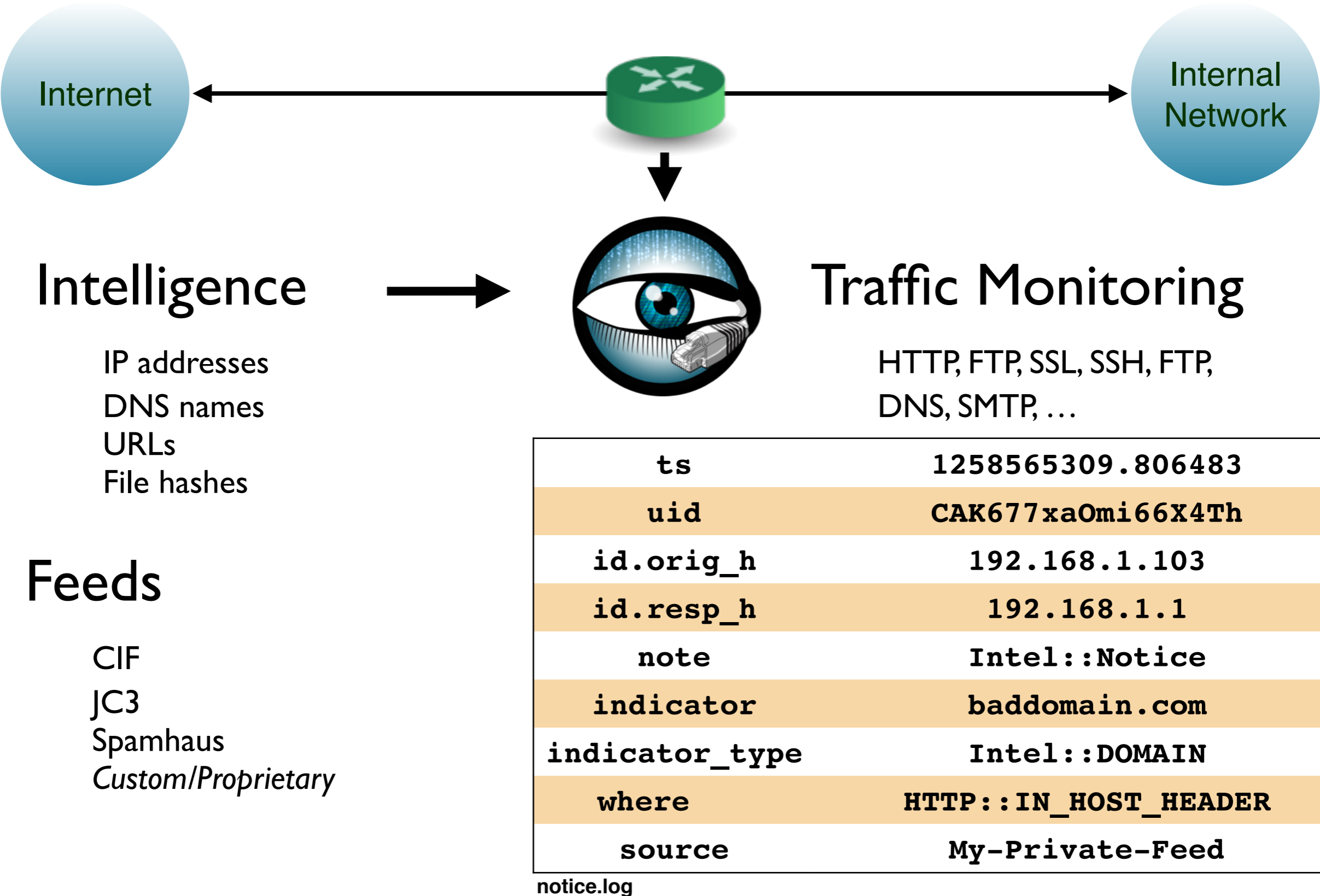
---



# Intelligence Integration



# Intelligence Integration



# Science DMZ Monitoring with Bro

---

## Visibility

- Log files
- Host-level visibility

## Detection

- Suspicious activity
- Intelligence feeds

## Performance

## Control

## Customization

# Science DMZ Monitoring with Bro

---

## Visibility

- Log files
- Host-level visibility

## Detection

- Suspicious activity
- Intelligence feeds

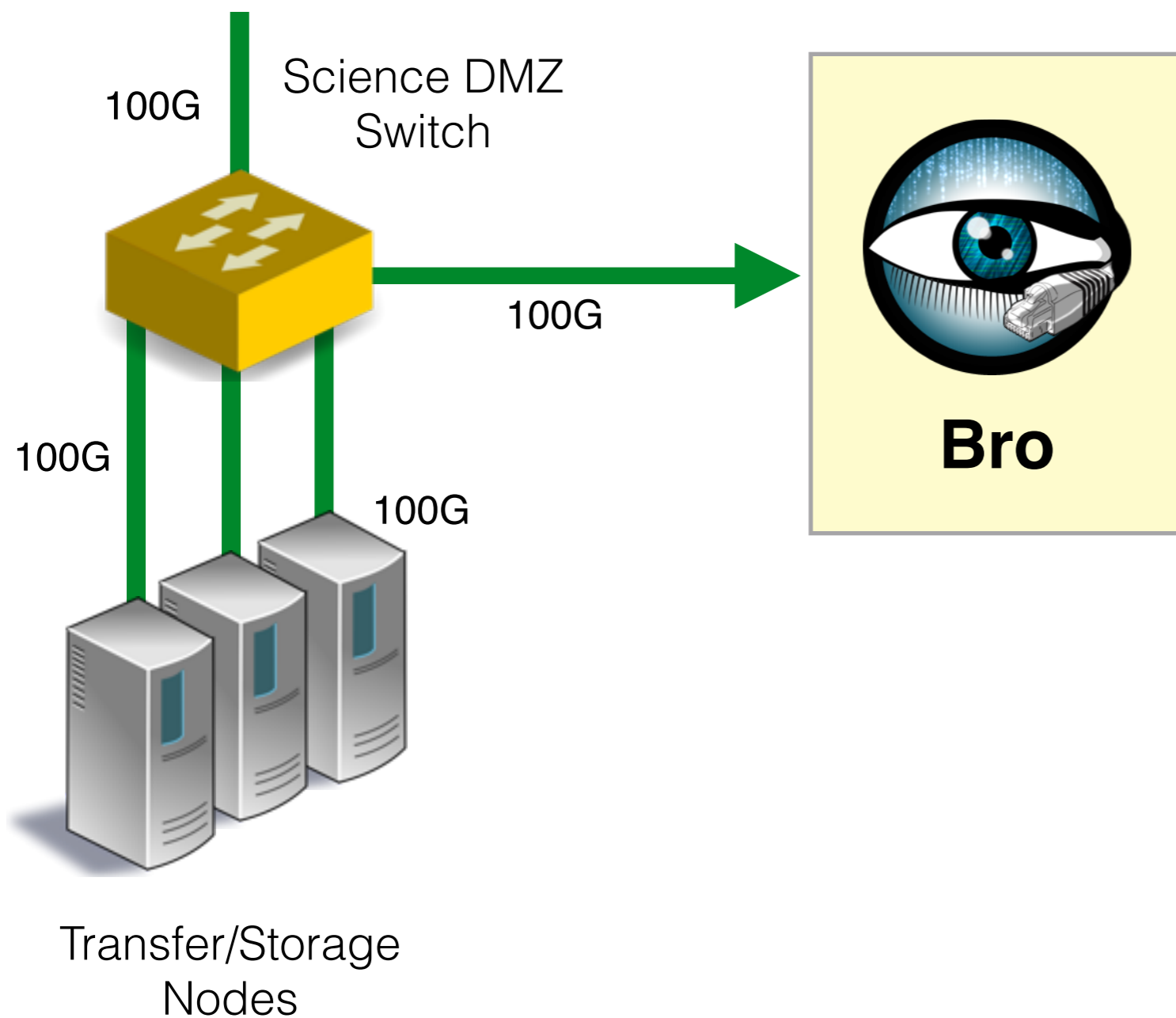
## Performance

- Bro Cluster
- Shunting

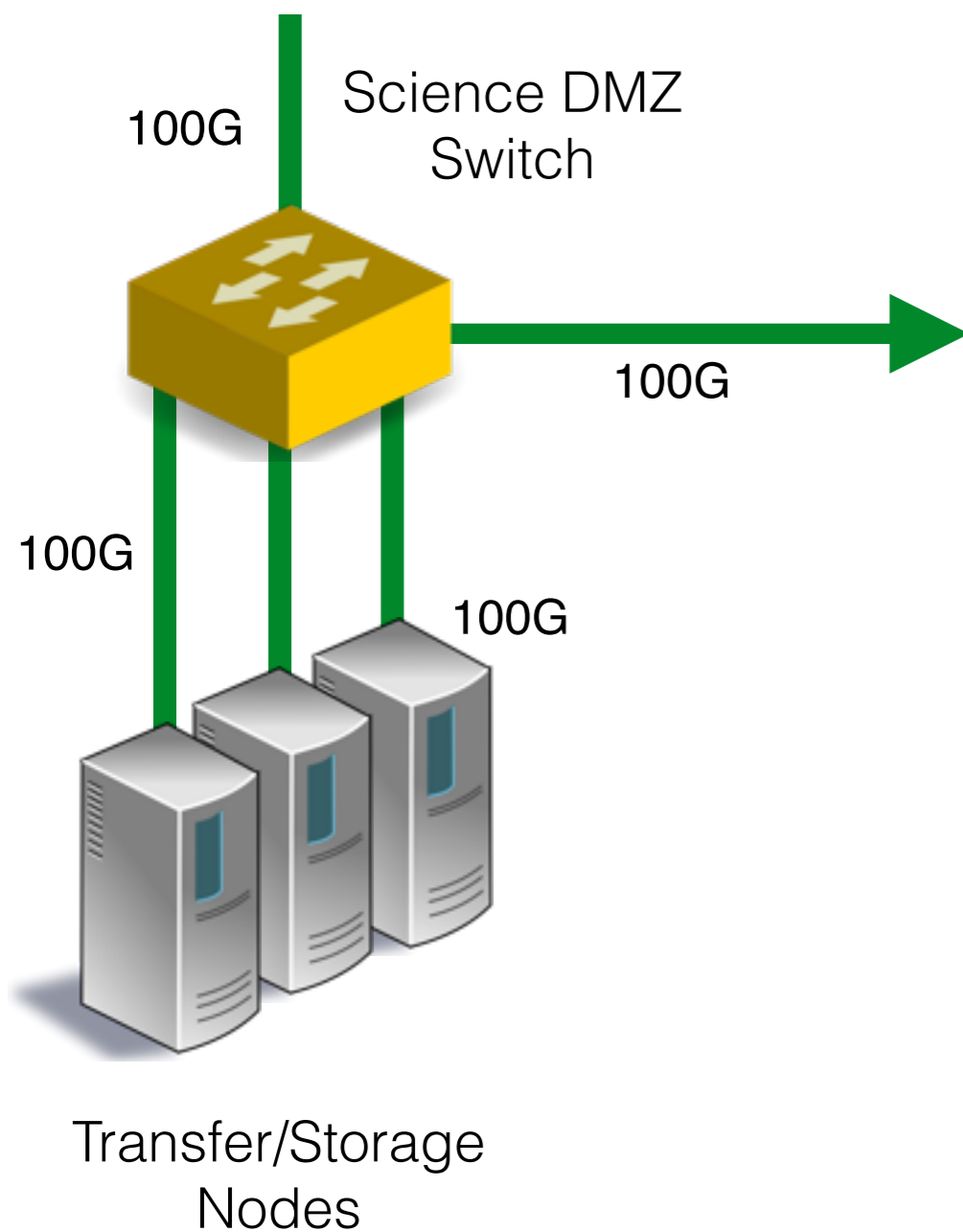
## Control

## Customization

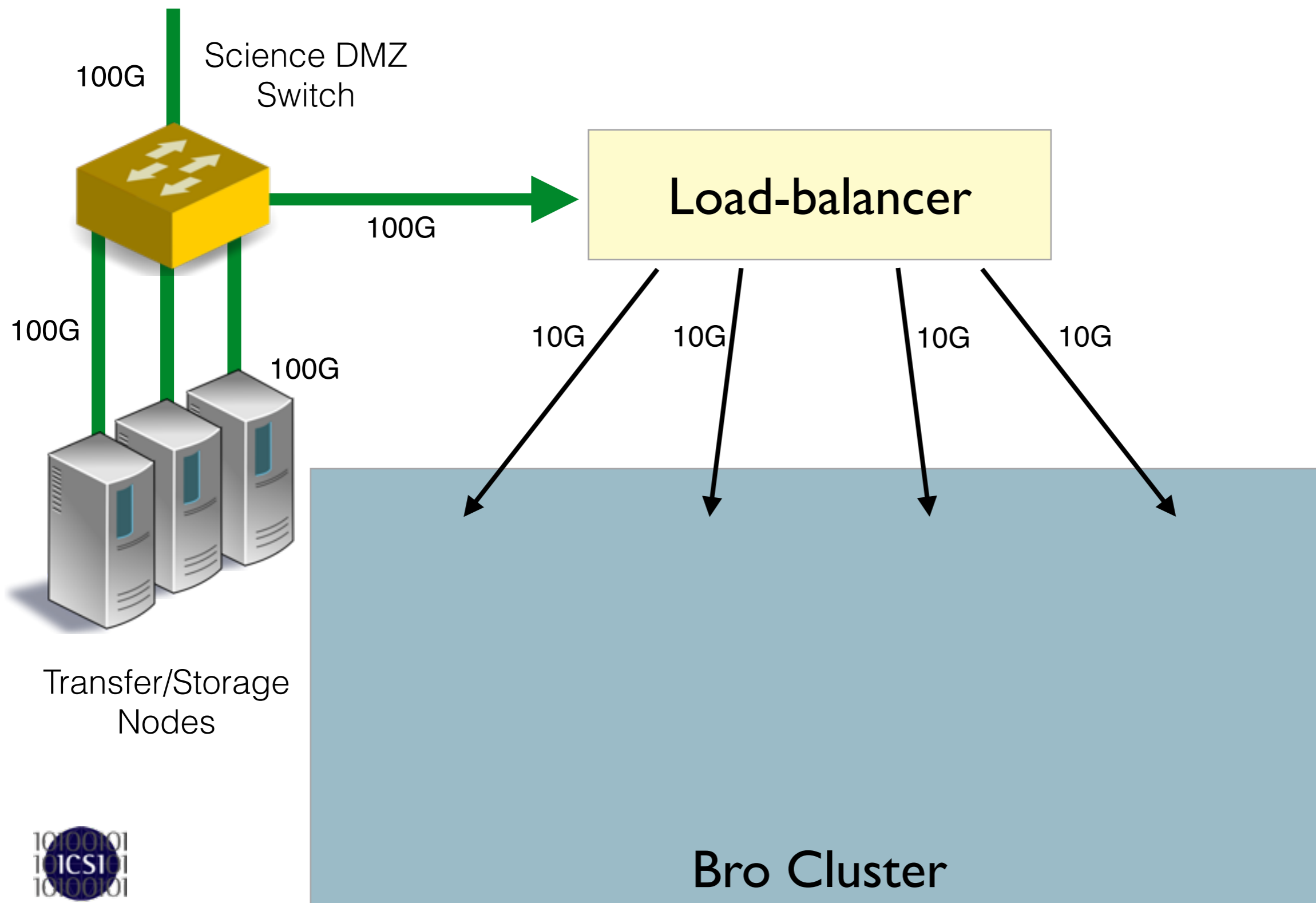
# Scaling Bro to 100G



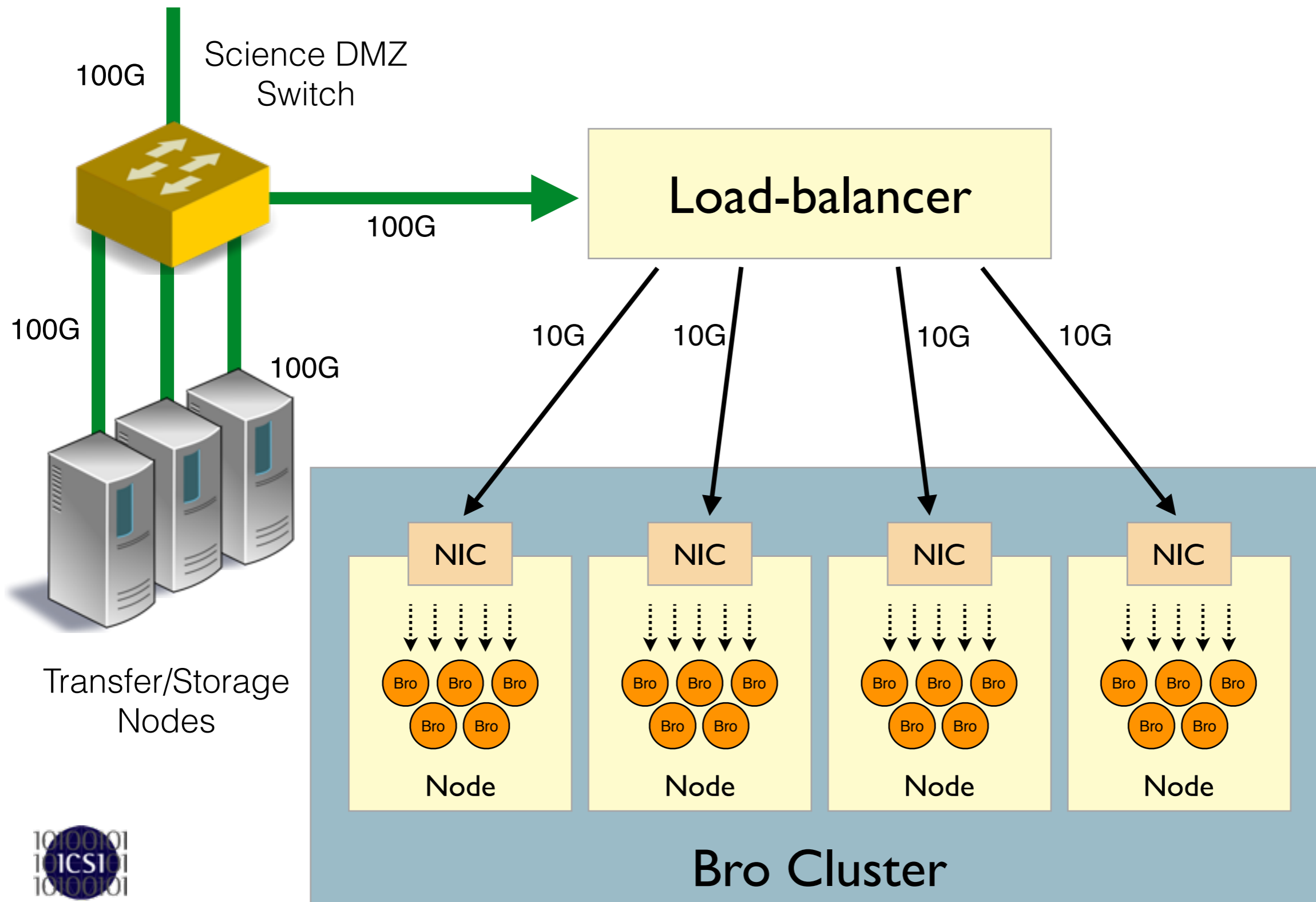
# Scaling Bro to 100G



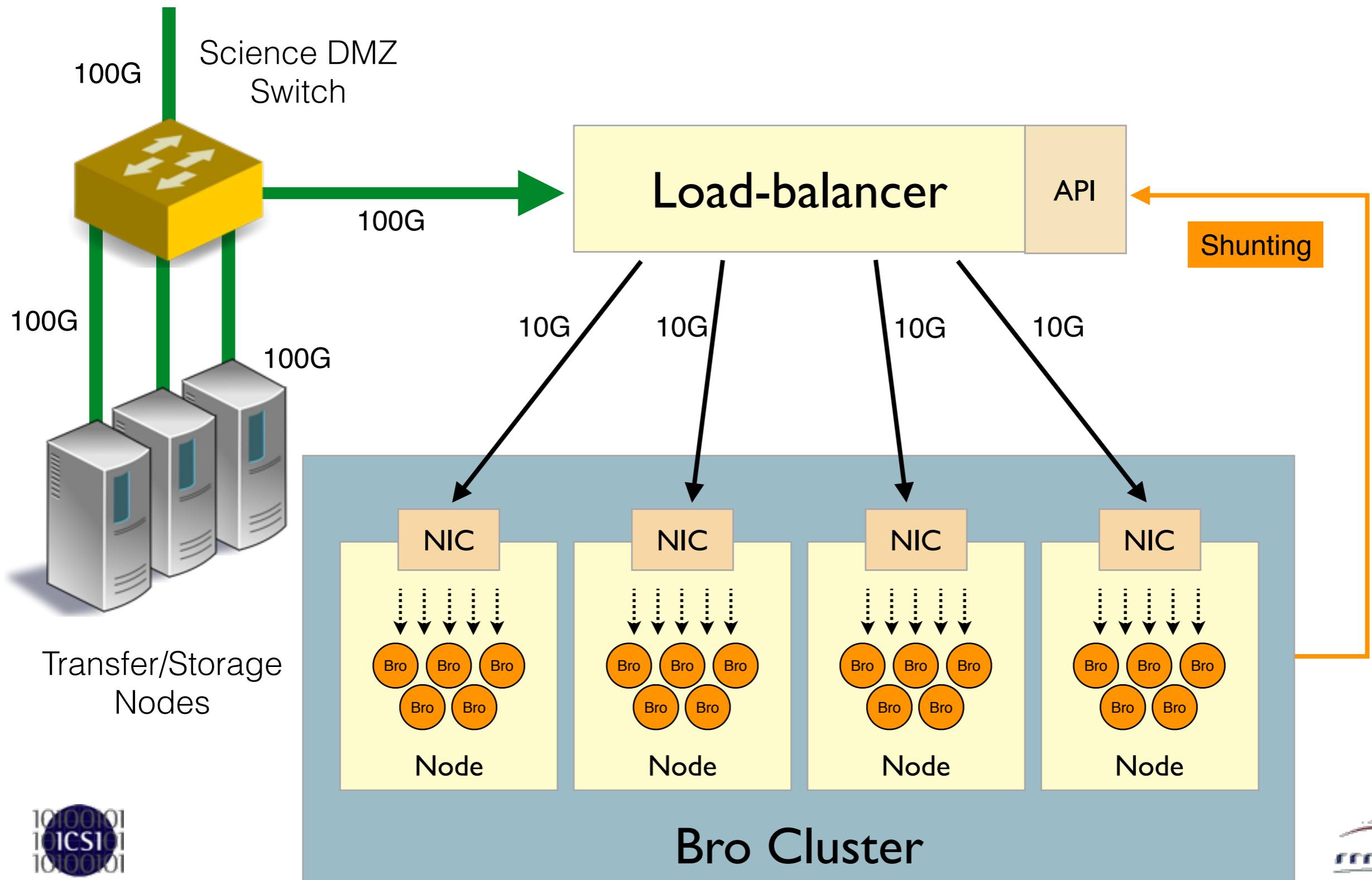
# Scaling Bro to 100G



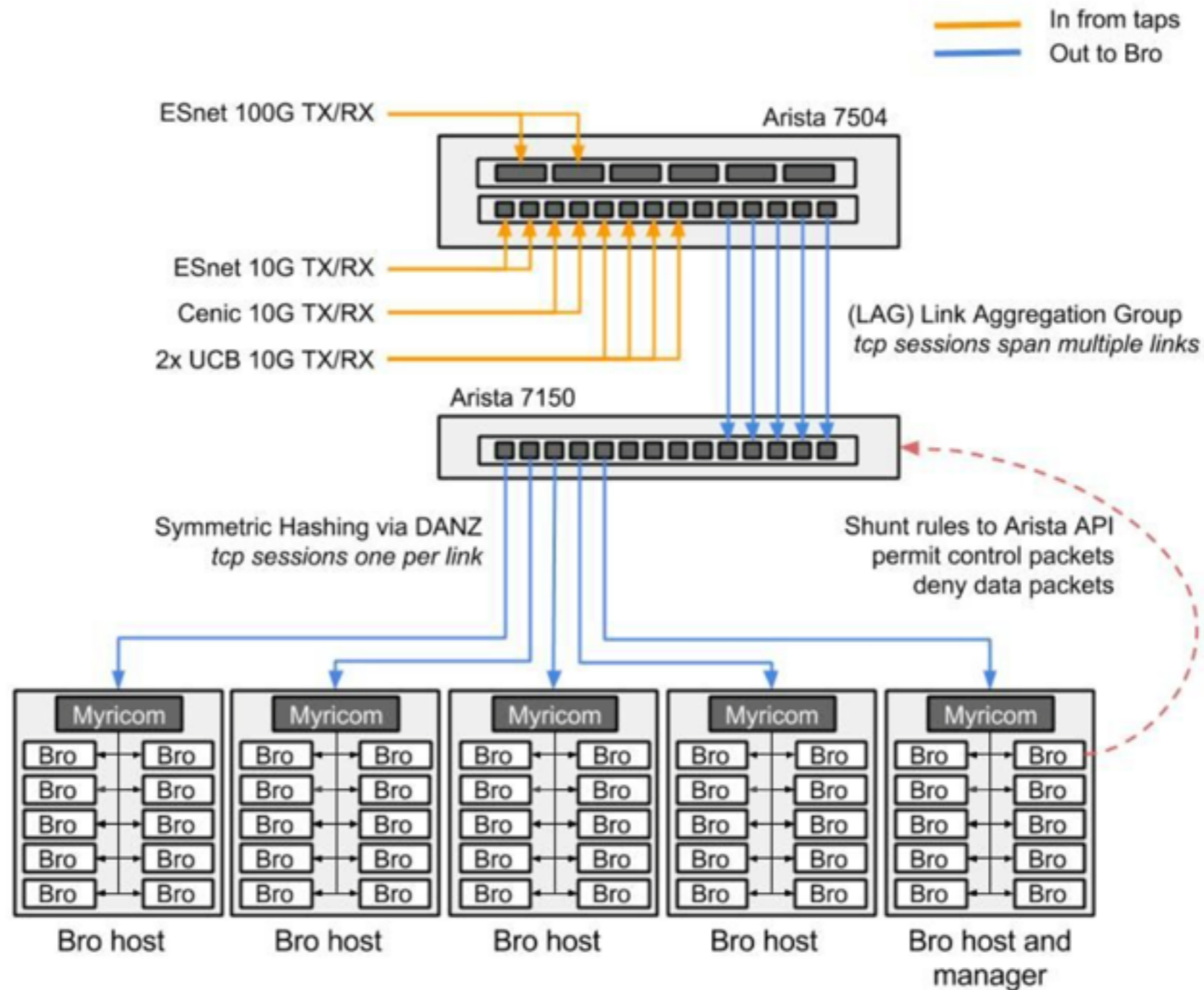
# Scaling Bro to 100G



# Scaling Bro to 100G



# 100G Bro at LBNL

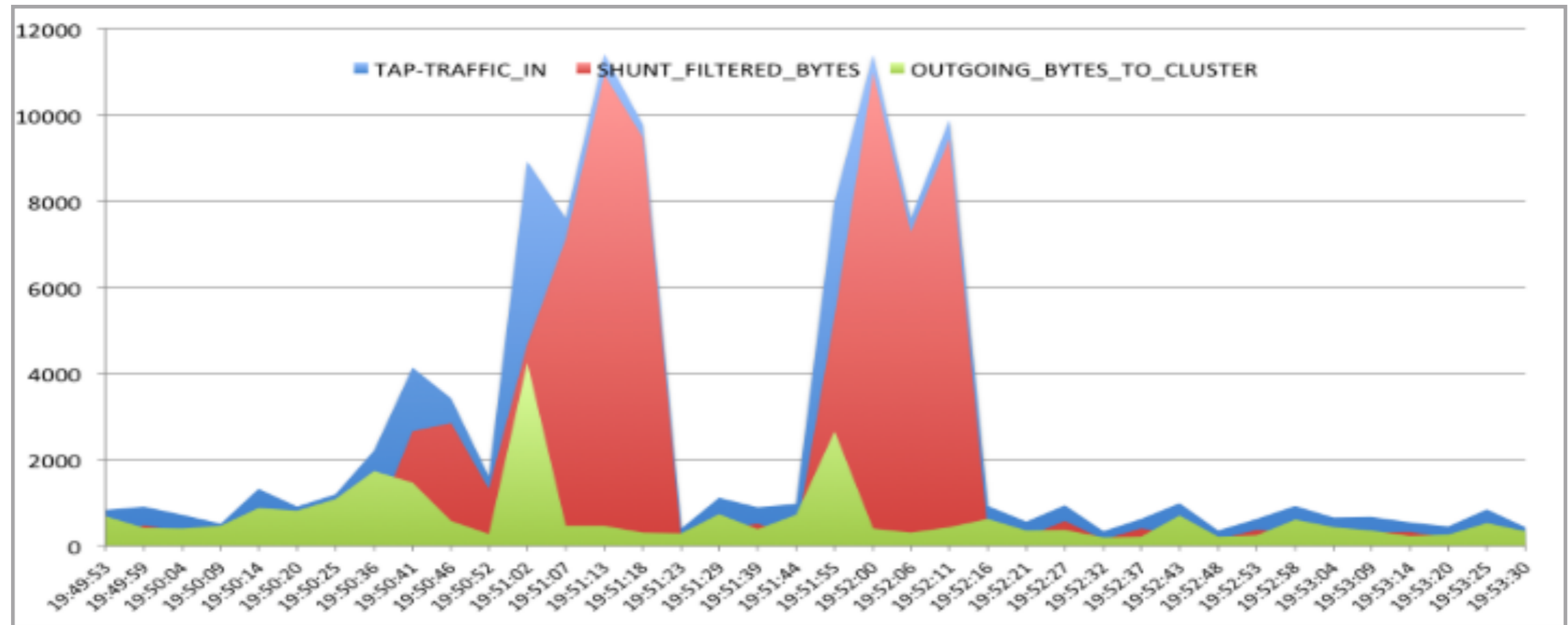


<http://go.lbl.gov/100g>

# Shunting at LBNL

---

# Shunting at LBNL



# Science DMZ Monitoring with Bro

---

## Visibility

- Log files
- Host-level visibility

## Detection

- Suspicious activity
- Intelligence feeds

## Performance

- Bro Cluster
- Shunting

## Control

## Customization

# Science DMZ Monitoring with Bro

---

## Visibility

- Log files
- Host-level visibility

## Detection

- Suspicious activity
- Intelligence feeds

## Performance

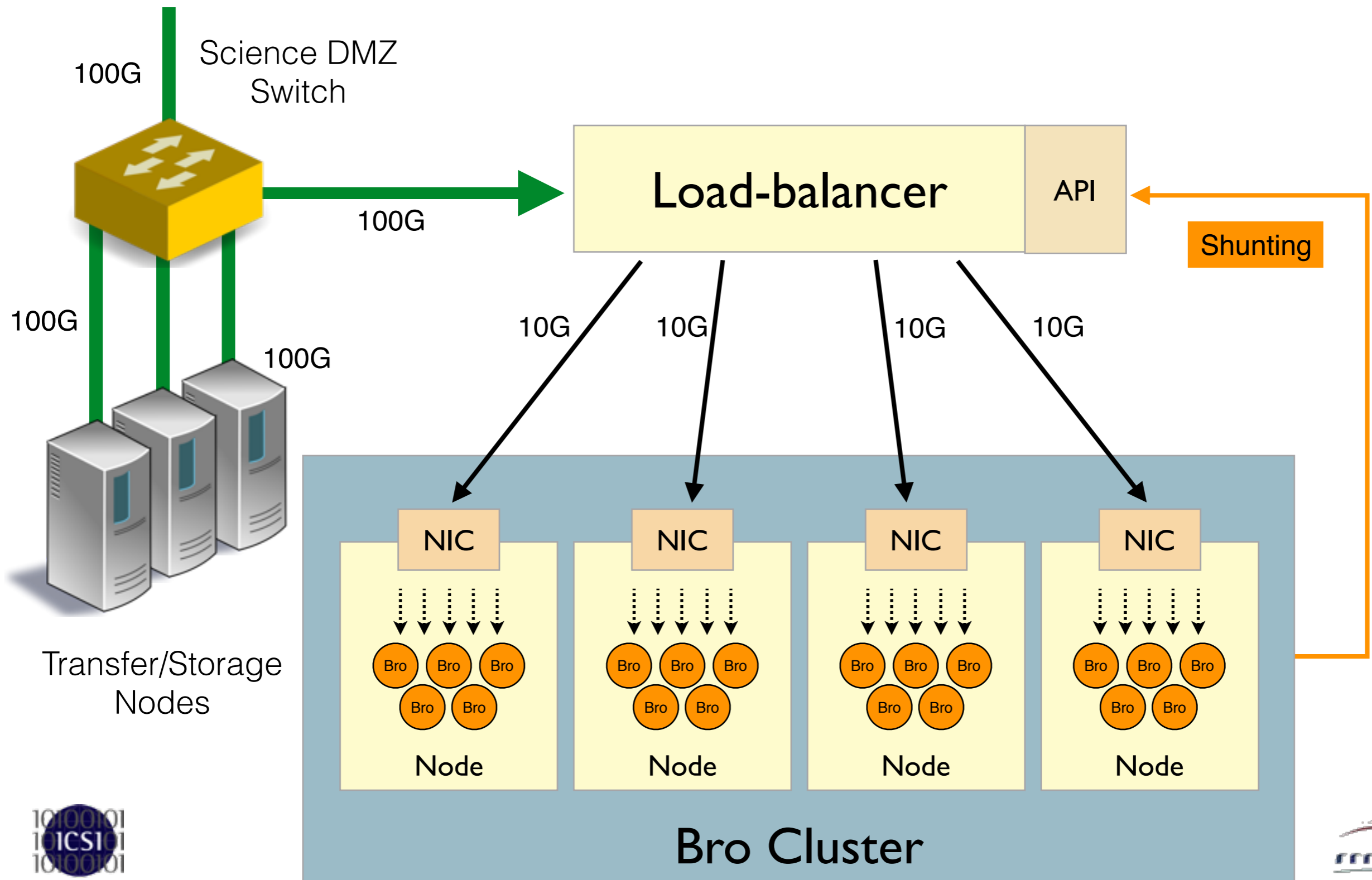
- Bro Cluster
- Shunting

## Control

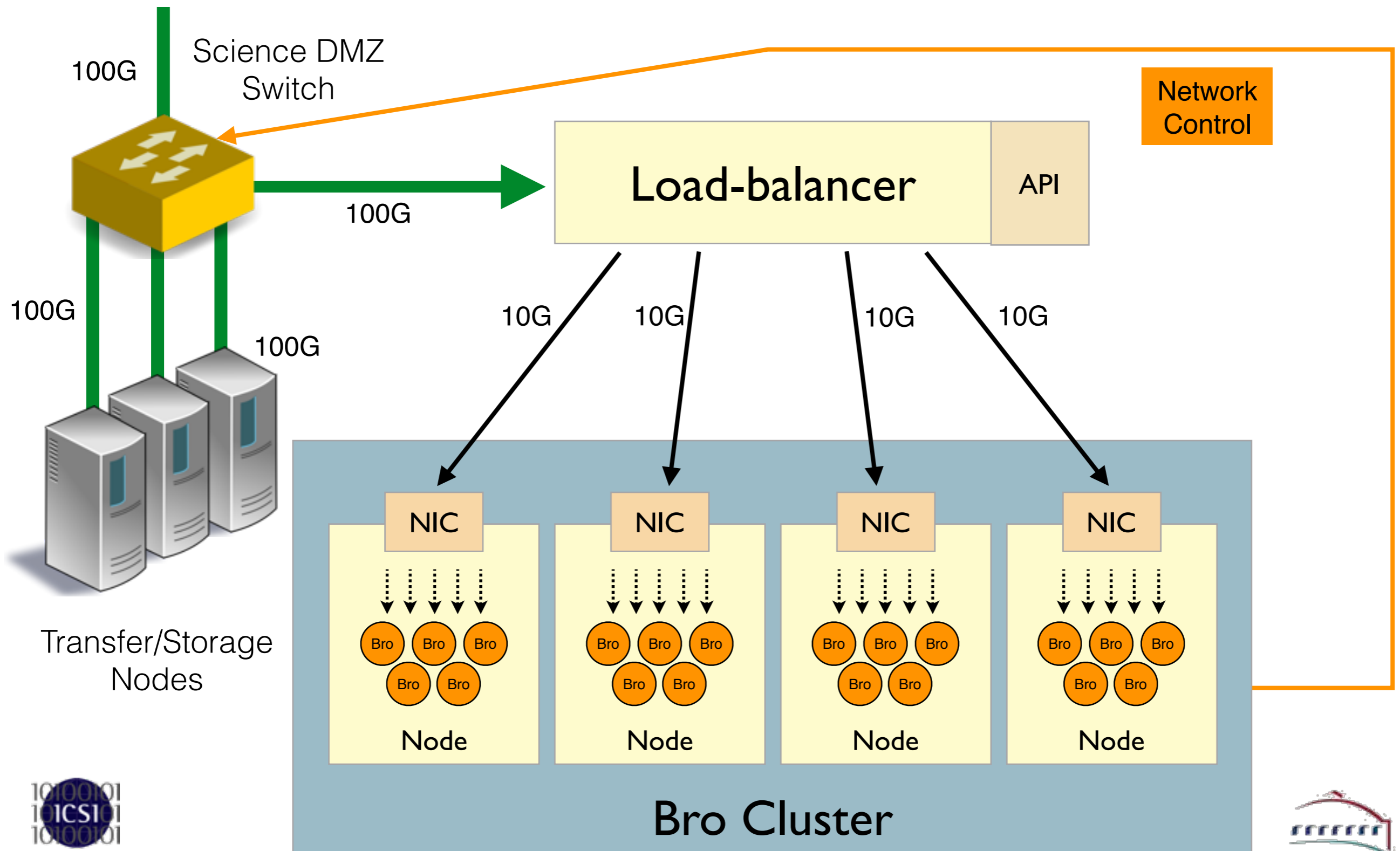
- Black- and whitelisting
- Traffic engineering

## Customization

# Network Control

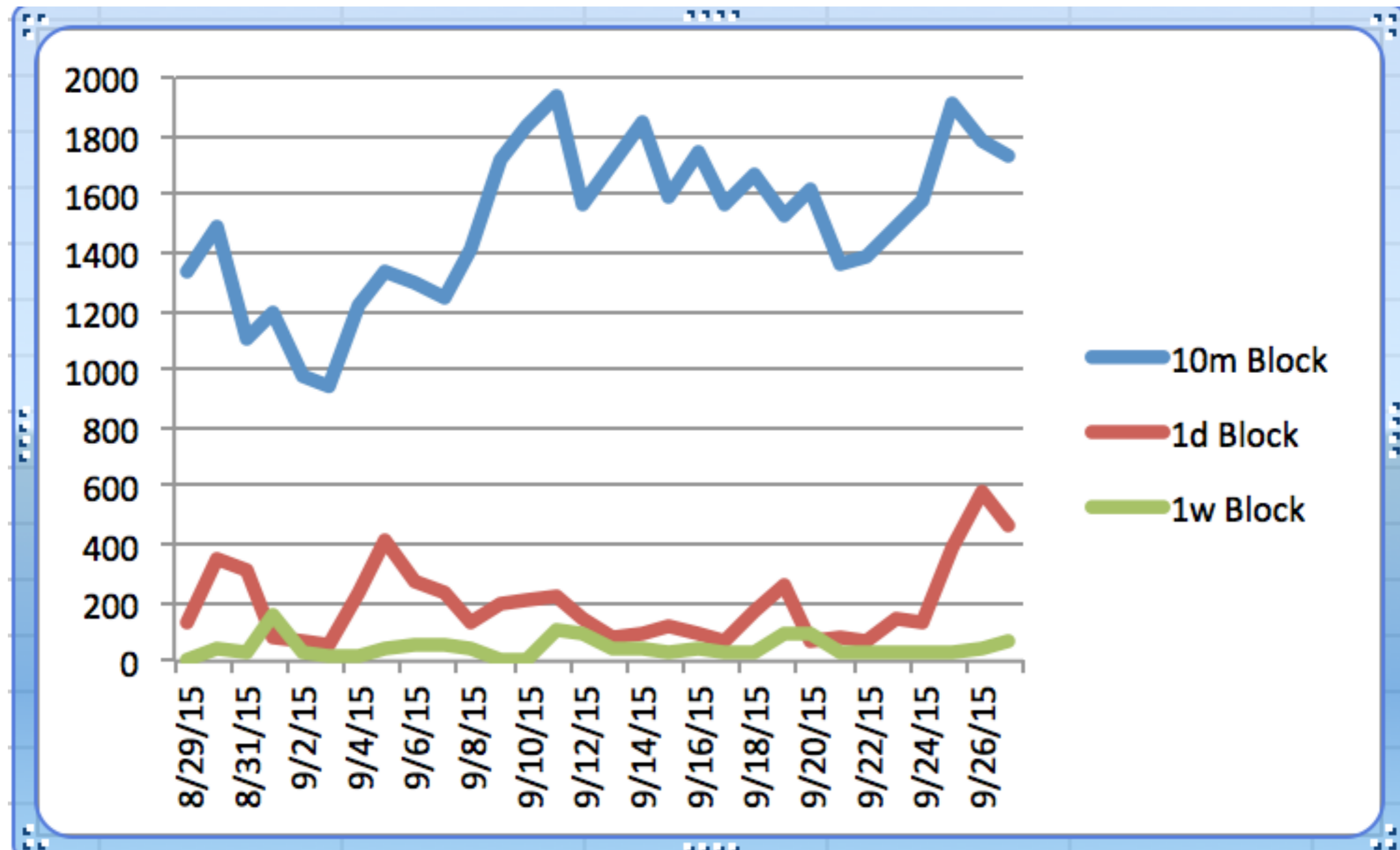


# Network Control



# Blacklisting: “Catch & Release” Dropping

# Blacklisting: “Catch & Release” Dropping

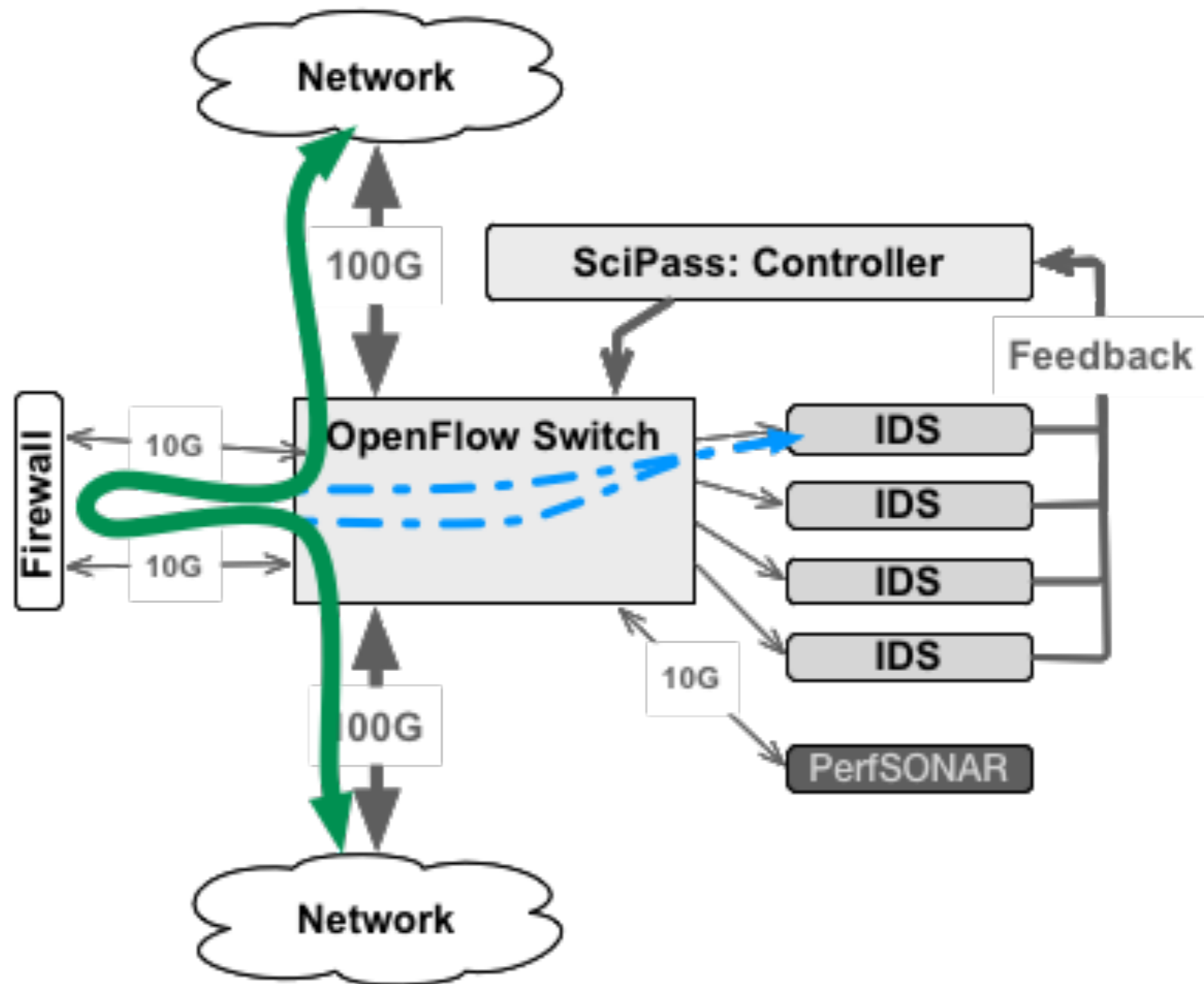


Source: Indiana University

# Whitelisting: IU's SciPass

---

# Whitelisting: IU's SciPass



Source: Indiana University

# Upcoming: Bro's NetControl Framework

---

# 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

# 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.**

# 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.

# 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

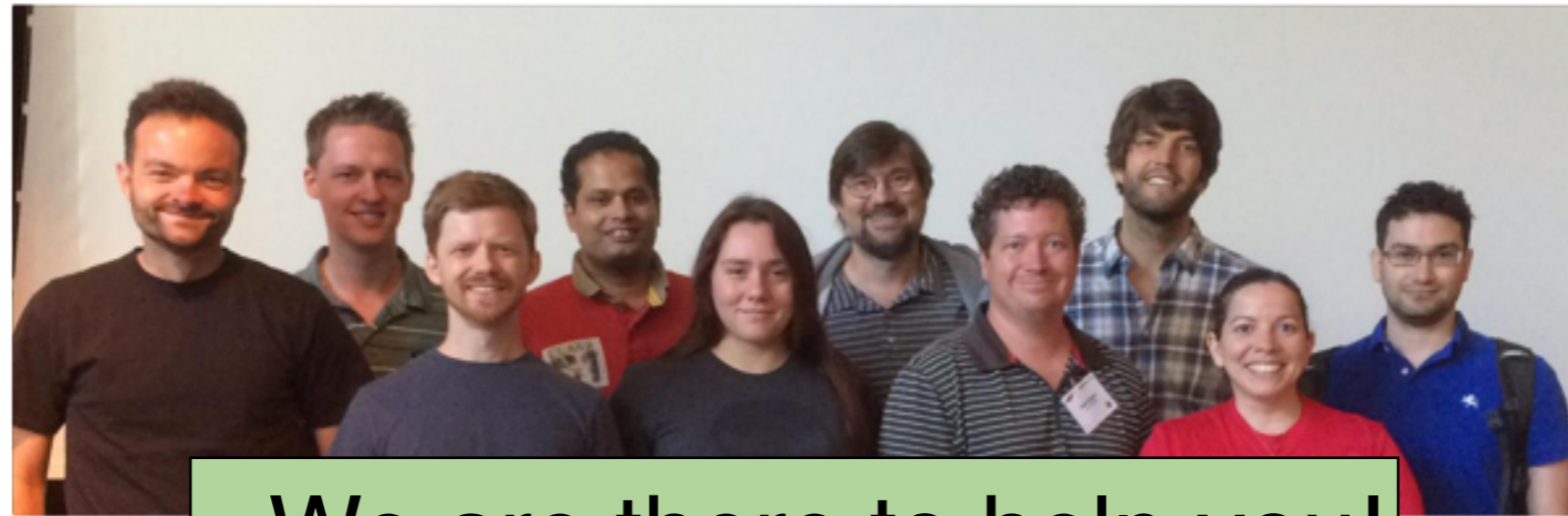
- Write your own scripts!

# The NSF Bro Center of Expertise

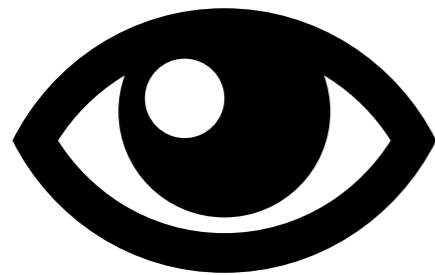
---

# The NSF Bro Center of Expertise

---



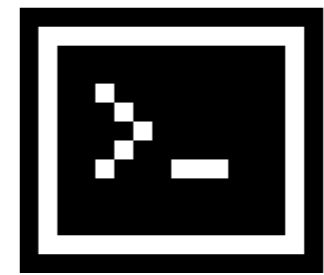
We are there to help you!



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](http://www.bro.org)  
[info@bro.org](mailto:info@bro.org)  
[@Bro\\_IDS](#)

## **Commercial Support**

[www.broala.com](http://www.broala.com)  
[info@broala.com](mailto:info@broala.com)  
[@Broala\\_](#)

---