ESnet
ENERGY SCIENCES NETWORK

Securing DOE’s Energy Sciences Network

Fatema Bannat Wala
ESnet Security Team

Wed, July 19 2023

U.S. DEPARTMENT OF ENERGY
Office of Science

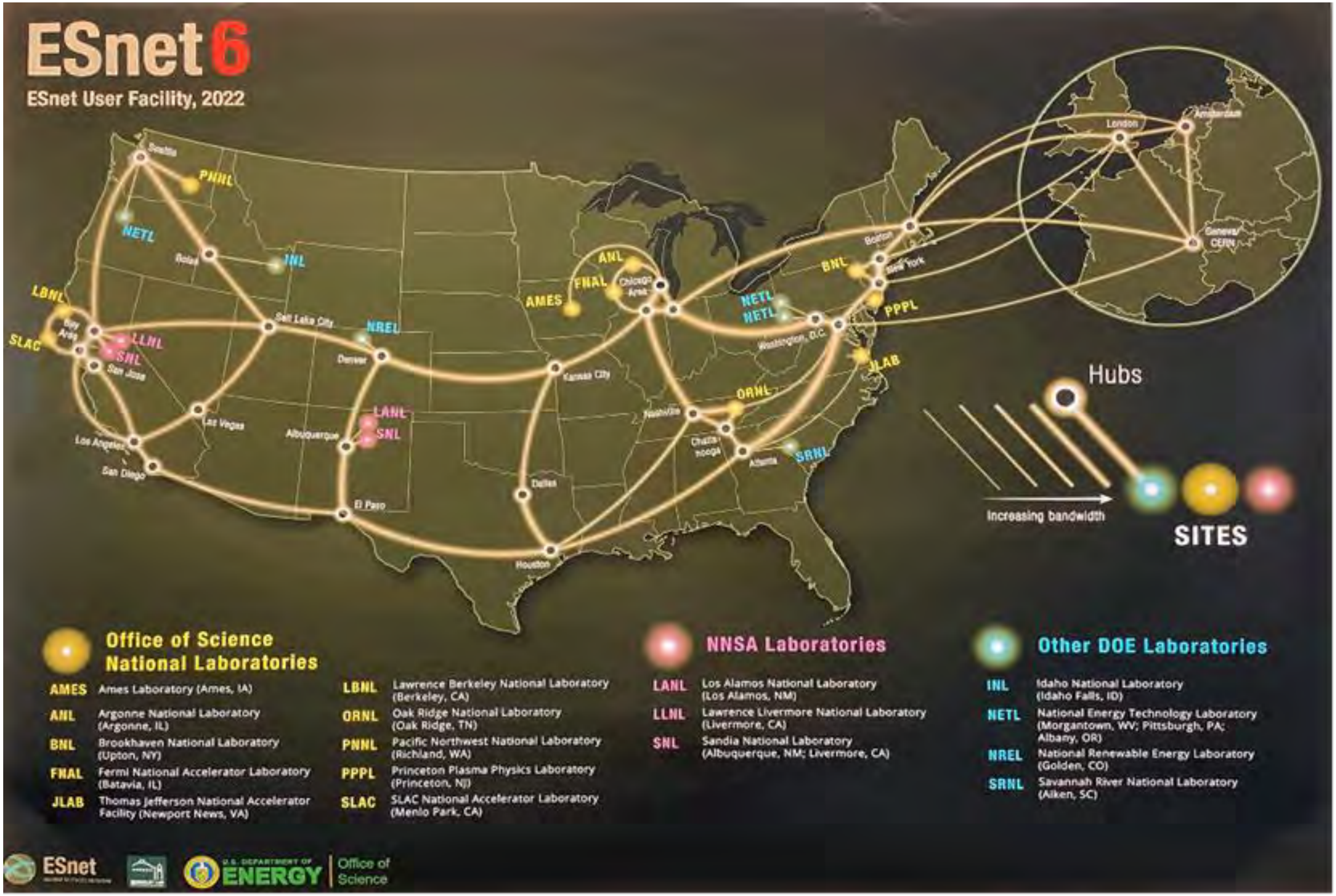
BERKELEY LAB

What is ESnet?

- ESnet is a high-performance, unclassified network built to support scientific research.

- Funded by the U.S. Department of Energy's Office of Science (SC) and managed by Lawrence Berkeley National Laboratory, ESnet provides services to more than 50 DOE research sites, including the entire National Laboratory system, its supercomputing facilities, and its major scientific instruments.

ESnet6



ESnet6

ESnet User Facility, 2022

Office of Science National Laboratories

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)

NNSA Laboratories

LANL	Los Alamos National Laboratory (Los Alamos, NM)
LLNL	Lawrence Livermore National Laboratory (Livermore, CA)
SNL	Sandia National Laboratory (Albuquerque, NM; Livermore, CA)

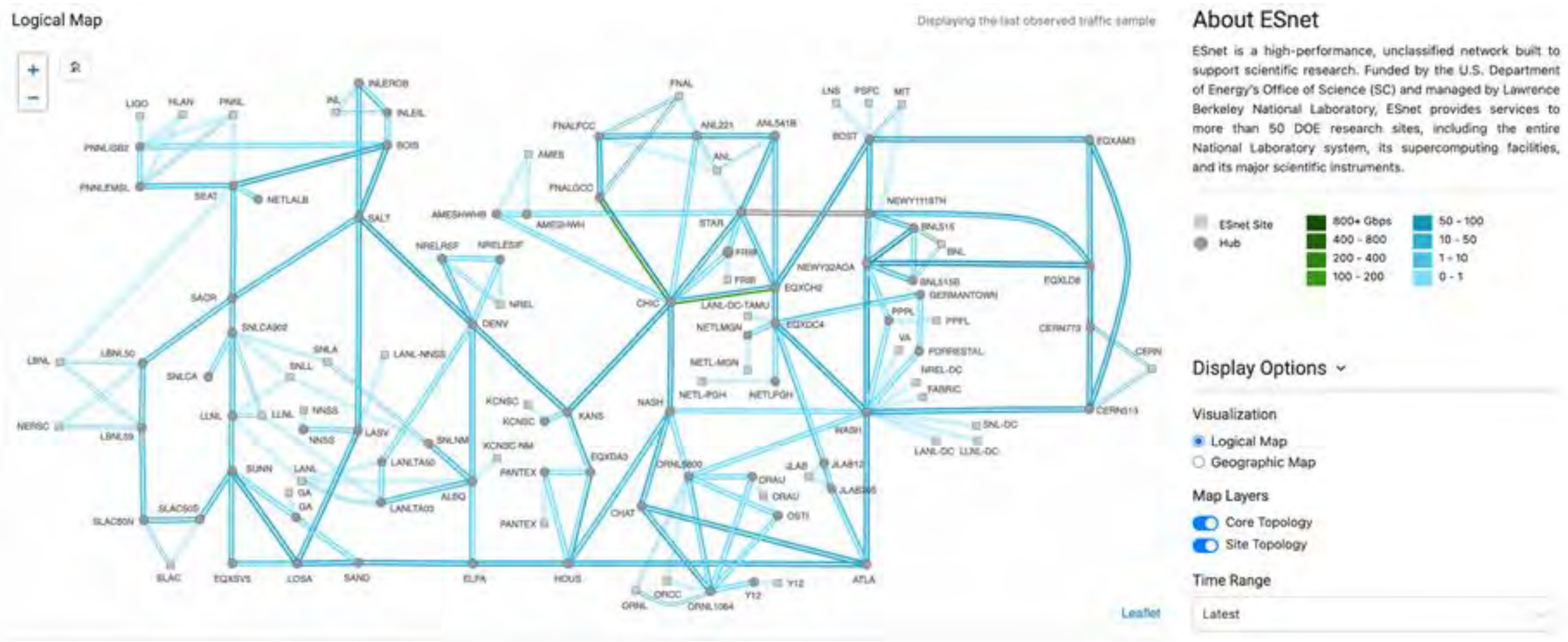
Other DOE Laboratories

INL	Idaho National Laboratory (Idaho Falls, ID)
NETL	National Energy Technology Laboratory (Morgantown, WV; Pittsburgh, PA; Albany, OR)
NREL	National Renewable Energy Laboratory (Golden, CO)
SRNL	Savannah River National Laboratory (Aiken, SC)

ESnet U.S. DEPARTMENT OF ENERGY | Office of Science

ESnet

Logical Map of ESnet



Logical Map

Displaying the last observed traffic sample

About ESnet

ESnet is a high-performance, unclassified network built to support scientific research. Funded by the U.S. Department of Energy's Office of Science (SC) and managed by Lawrence Berkeley National Laboratory, ESnet provides services to more than 50 DOE research sites, including the entire National Laboratory system, its supercomputing facilities, and its major scientific instruments.

▢ ESnet Site	■ 800+ Gbps	■ 50 - 100
● Hub	■ 400 - 800	■ 10 - 50
	■ 200 - 400	■ 1 - 10
	■ 100 - 200	■ 0 - 1

Display Options ˅

Visualization

● Logical Map
○ Geographic Map

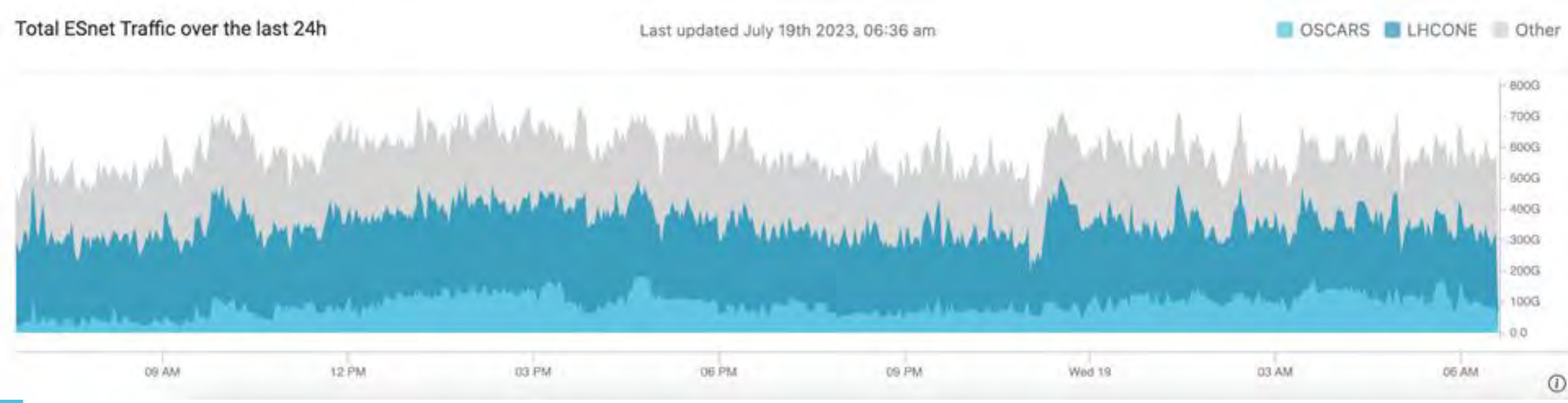
Map Layers

Core Topology: on
Site Topology: on

Time Range

Latest

How much Data/traffic?



Total ESnet Traffic over the last 24h

Last updated July 19th 2023, 06:36 am

Securing ESnet - Locations

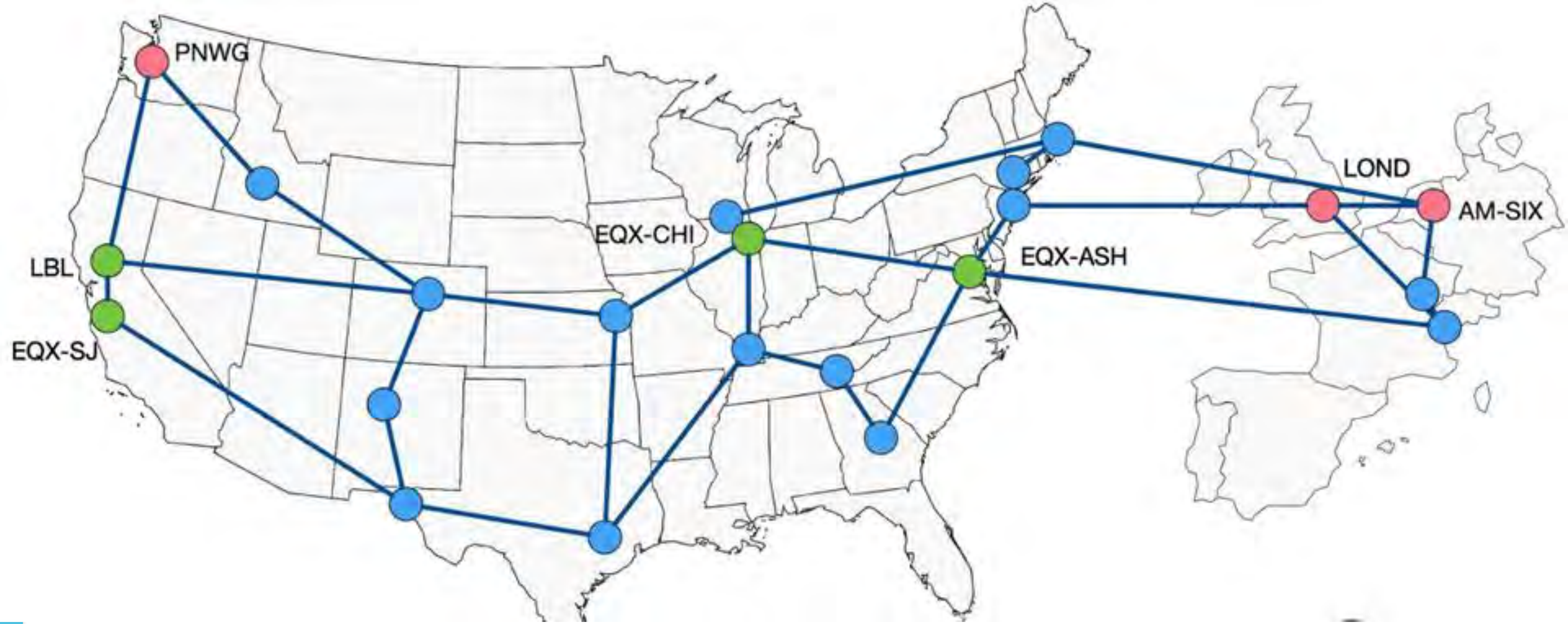
Three primary networks to focus on -

- **WAN Network** - Our Backbone with high speed upto ~400Gbps network traffic monitoring
- **LAN Network** - Our Data Centers with upto ~10Gbps network traffic links
- **Management Network** - Our isolated management network with upto ~10Gbps network traffic links

What does Securing the network mean?

- Visibility of our important choke points - You can't defend what you can't see!
- Traffic monitoring of those choke points
- Log collection and aggregation
- Alerting and reporting

Tackling Visibility of network - WAN Zeek on WAN (ZoW)

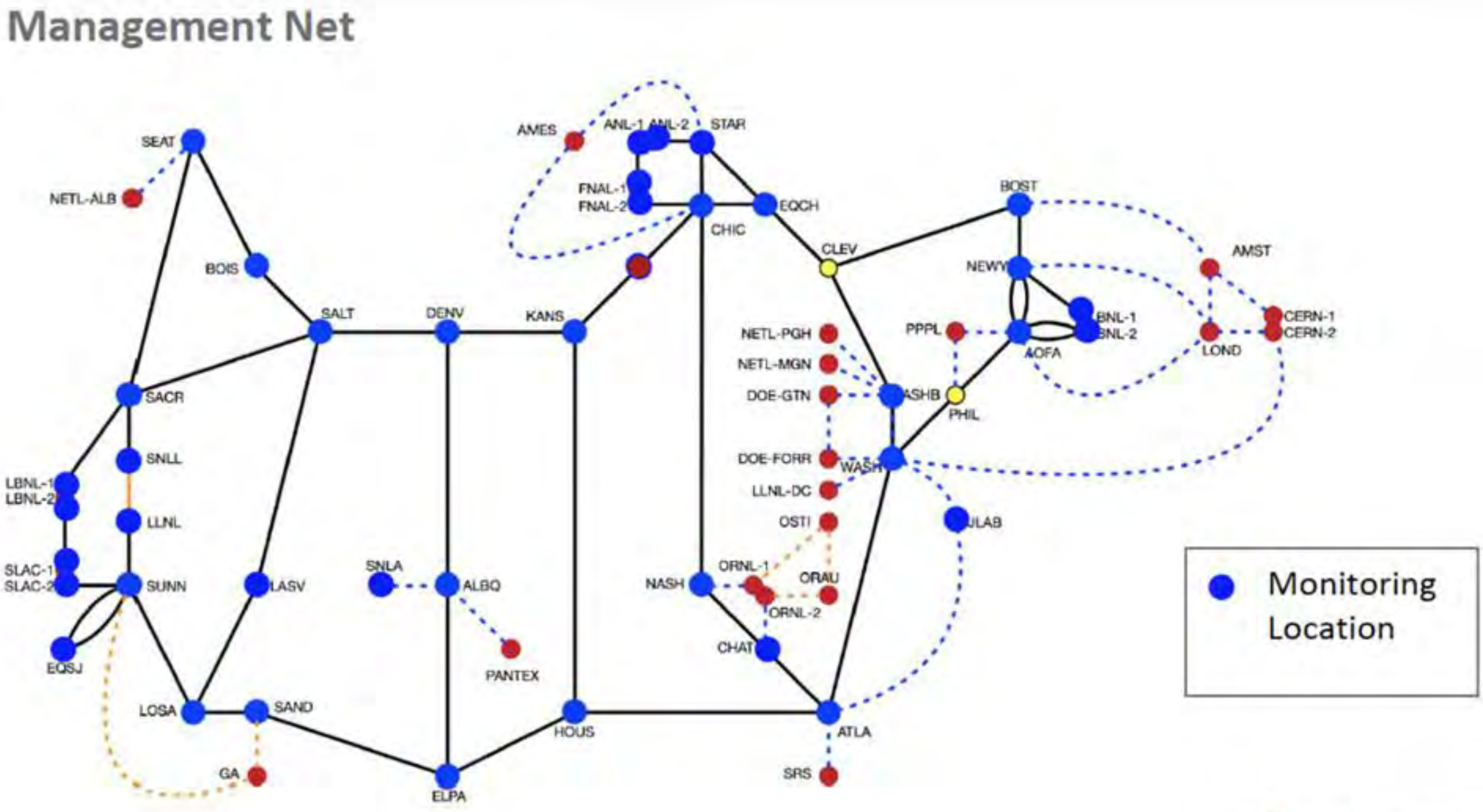


- WAN links b/w 1 - 400Gbps
- High value locations - commodity internet peerings

Challenges of WAN

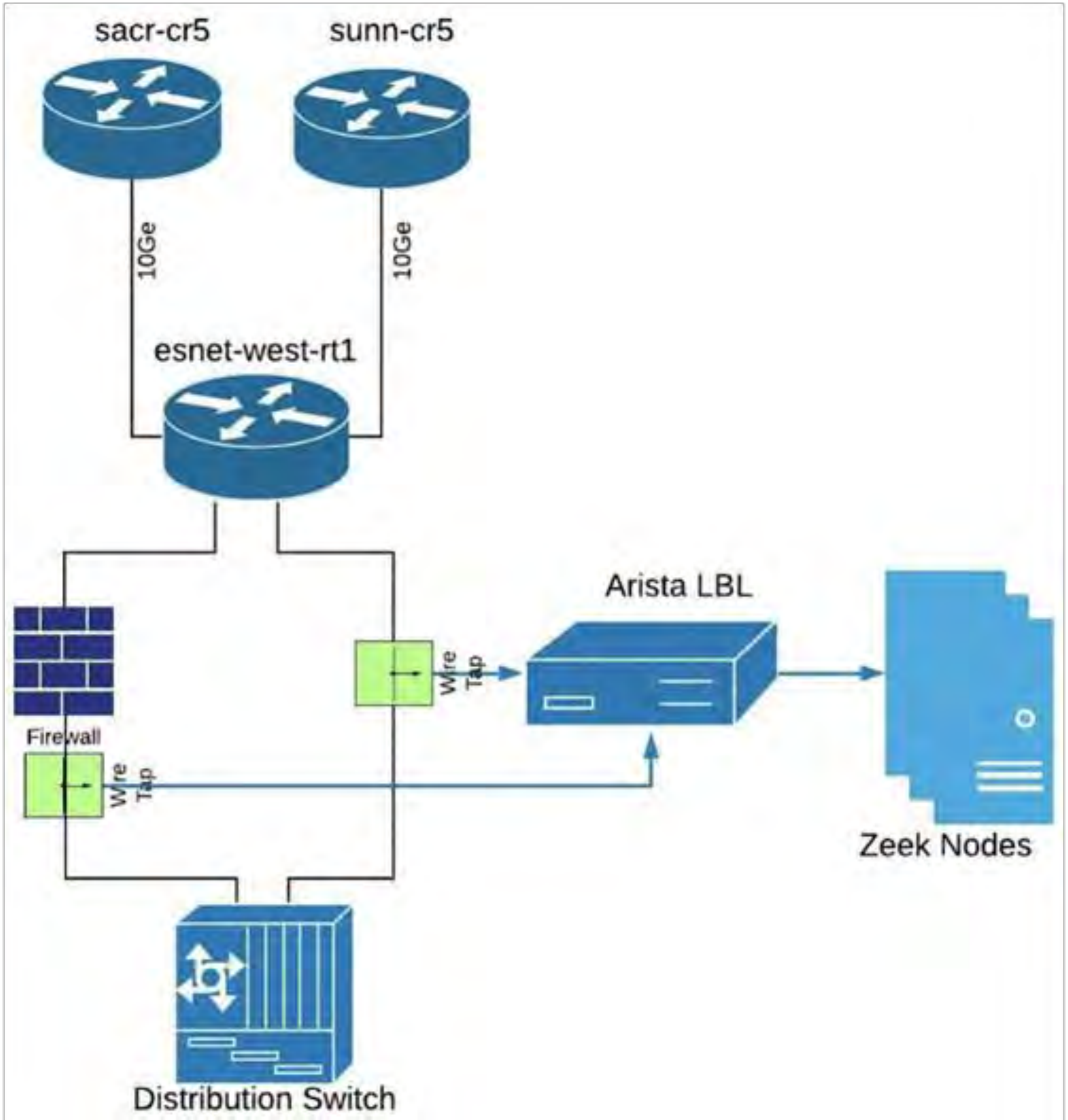
- WAN links between 1-400Gbps
- Power and space constraints
- Unhappy Zeek on WAN
  - Data Encapsulation - Zeek Does not like variable length headers
  - Asymmetric flows - Huge problem for any NSM

Tackling Visibility of network - Mgmt
Zeek on Mgmt n/w - ZoMbis (IPv6 only)



ESnet

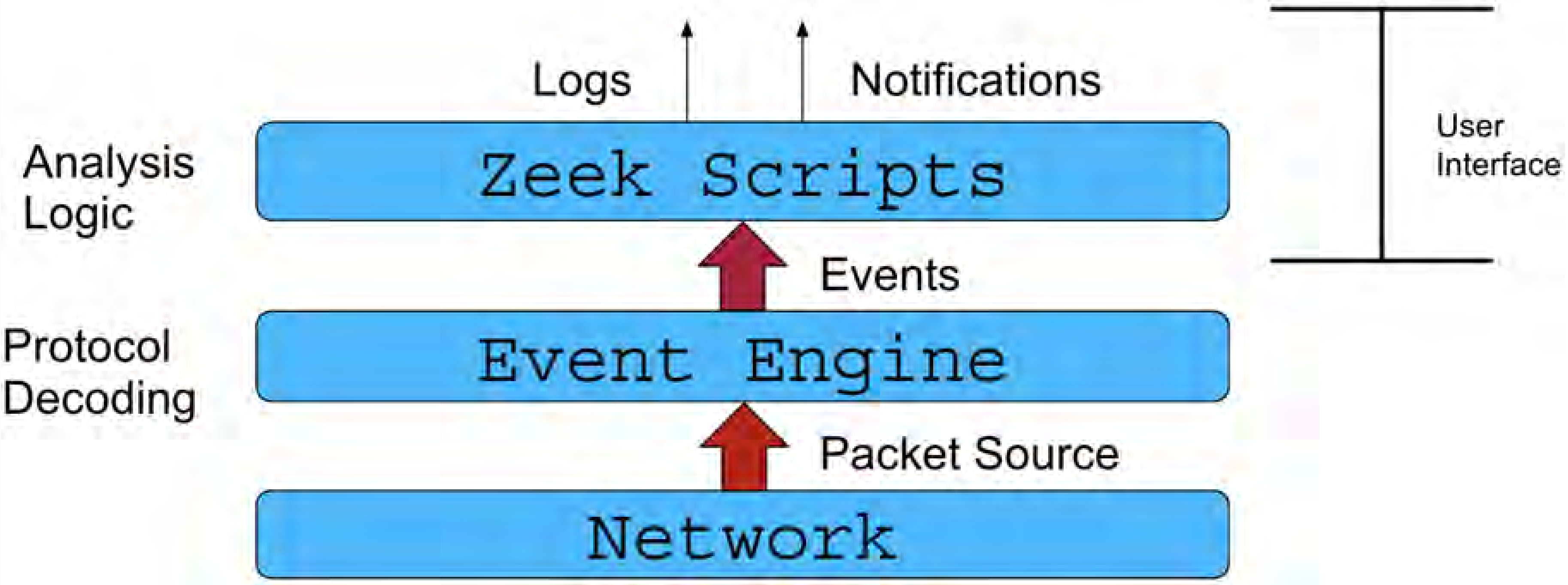
Tackling Visibility of network - LAN
Zeek on LAN (ZoL)



Brief introduction to Zeek!

- ~26 years old, long history in academia
- Domain Specific Network Monitoring Language
- Policy Neutral
- Leave your IDS ideas behind
- Developed by Vern Paxson @LBL

Zeek Architecture



Analyzers

- Protocol Analyzers
  - ➢ Most popular - SMTP / HTTP / SSL / DNS / DHCP
  - ➢ Authentication - SSH / KERBEROS / RADIUS
  - ➢ MS protocols - RPC / NTLM / SMB / RDP
  - ➢ Interesting ones - SOCKS / TUNNEL / IRC / FTP

- File Analyzers
  - ➢ EXTRACT / HASH / PE / X509

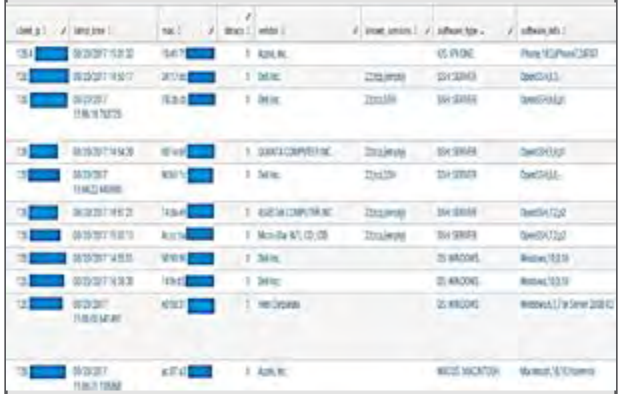
- Spicy!
  - ➢ C++ parser generator that makes it easy to create robust parsers for network protocols, file formats, and more..

What Zeek Does?

Sniffs traffic

Creates traffic logs

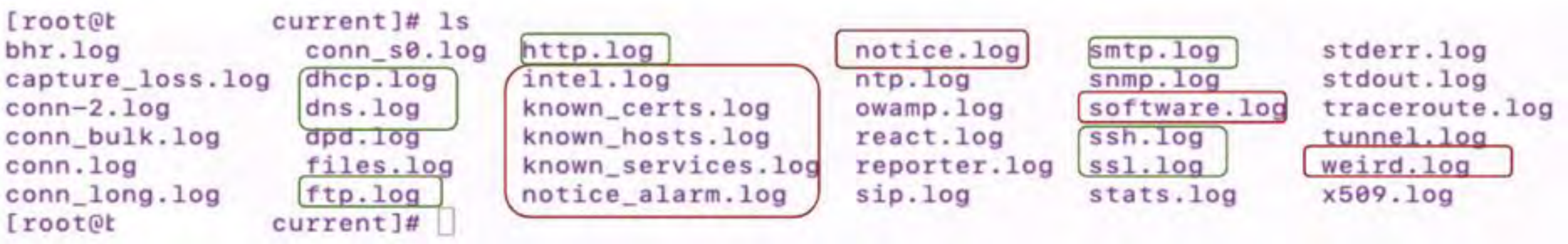
Zeek Logs aggregated at SIEM



client_ip	latest_time	mac	dhcp	vendor	known_services	software_type	software_info
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Apple, Inc.		IOS IPHONE	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Dell Inc.	[illegible]	SSH SERVER	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Dell Inc.	[illegible]	SSH SERVER	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	QUANTA COMPUTER INC.	[illegible]	SSH SERVER	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Dell Inc.	[illegible]	SSH SERVER	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	ASUSTek COMPUTER INC.	[illegible]	SSH SERVER	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Micro-Star INT'L CO., LTD	[illegible]	SSH SERVER	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Dell Inc.		OS WINDOWS	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Dell Inc.		OS WINDOWS	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Intel Corporate		OS WINDOWS	[illegible]
[illegible] [redacted]	[illegible]	[illegible] [redacted]	1	Apple, Inc.		MACOS MACINTOSH	[illegible]

Let’s talk about Zeek Logs

Logs



```
[root@t          current]# ls
bhr.log           conn_s0.log  http.log            notice.log    smtp.log      stderr.log
capture_loss.log  dhcp.log     intel.log           ntp.log       snmp.log      stdout.log
conn-2.log        dns.log      known_certs.log     owamp.log     software.log  traceroute.log
conn_bulk.log     dpd.log      known_hosts.log     react.log     ssh.log       tunnel.log
conn.log          files.log    known_services.log  reporter.log  ssl.log       weird.log
conn_long.log     ftp.log      notice_alarm.log    sip.log       stats.log     x509.log
[root@t          current]# 
```

- All the logs are written in ASCII log files (tsv format)
- Zeek generates the log files for the protocols it sees in your network traffic (more than 50 protocols currently parsed)
- Apart from conventional protocol log files, interesting logs pertaining to noticeable/statistical activity (weird.log, notice.log etc.)

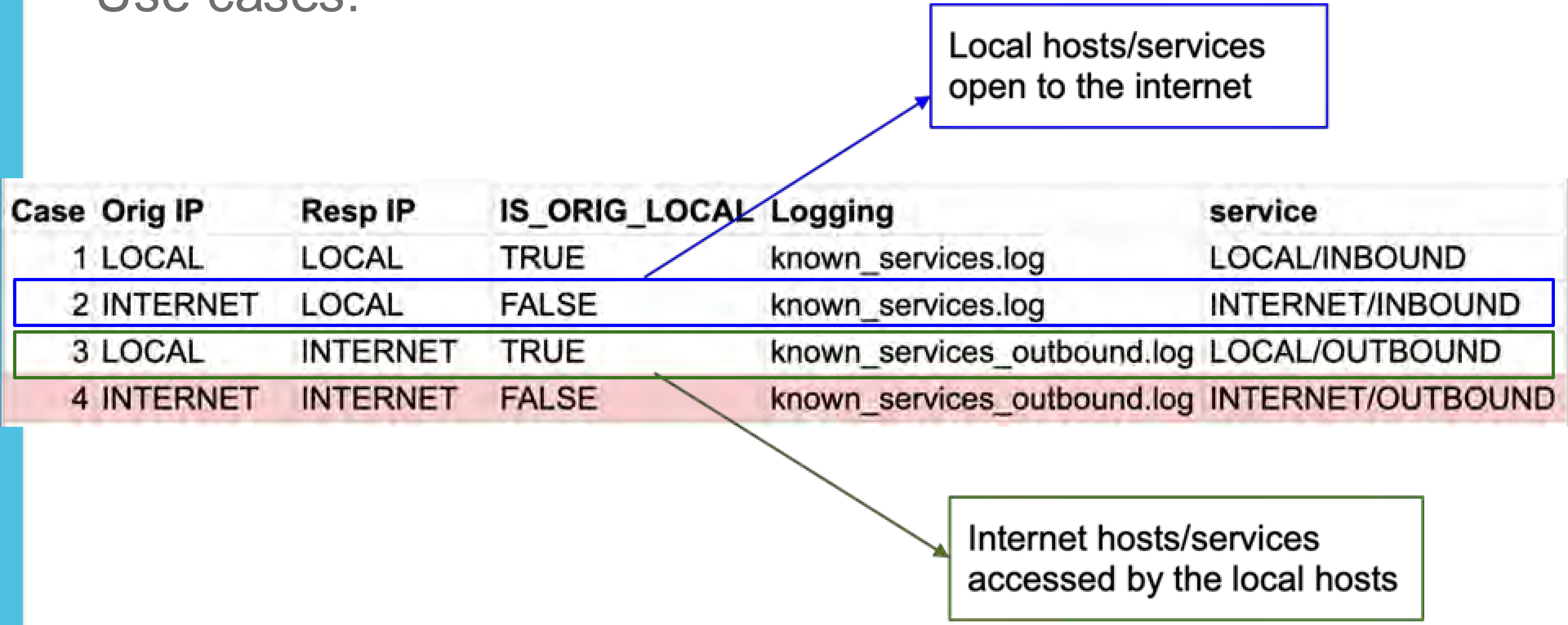
Example usage of Zeek @ESnet

Zeek + ZTA

- Egress traffic filtering - Restrict the outbound access to the internet based on what is needed and what is not
- Solution - Use Zeek to detect known outbound services!

Known services detection - Zeek

Use-cases:



Case	Orig IP	Resp IP	IS_ORIG_LOCAL	Logging	service
1	LOCAL	LOCAL	TRUE	known_services.log	LOCAL/INBOUND
2	INTERNET	LOCAL	FALSE	known_services.log	INTERNET/INBOUND
3	LOCAL	INTERNET	TRUE	known_services_outbound.log	LOCAL/OUTBOUND
4	INTERNET	INTERNET	FALSE	known_services_outbound.log	INTERNET/OUTBOUND

Local hosts/services open to the internet

Internet hosts/services accessed by the local hosts

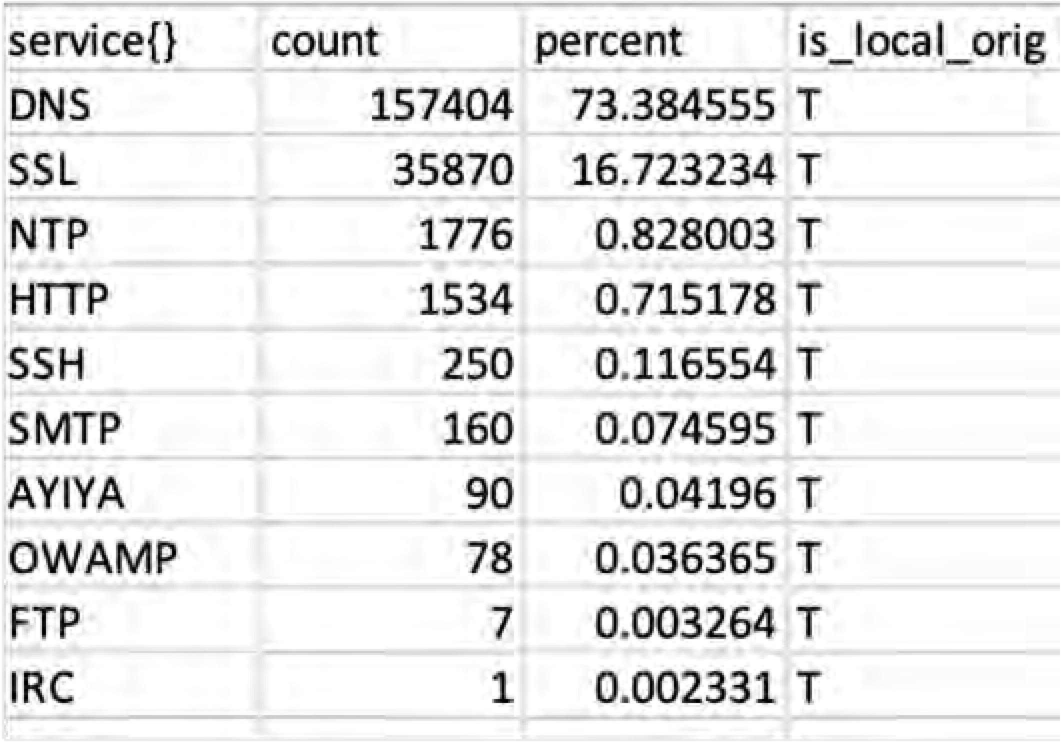
*case no. 1 should never happen, for North-South.

*case no. 4 should never happen..

Egress traffic result

Statistical summary (past 7 days of traffic)

- Only ~12-15 services detected outbound (*known_services_outbound.log*)
- Investigated those services, resulted in interesting findings!



service{}	count	percent	is_local_orig
DNS	157404	73.384555	T
SSL	35870	16.723234	T
NTP	1776	0.828003	T
HTTP	1534	0.715178	T
SSH	250	0.116554	T
SMTP	160	0.074595	T
AYIYA	90	0.04196	T
OWAMP	78	0.036365	T
FTP	7	0.003264	T
IRC	1	0.002331	T

Egress/outbound services detection scripts

Available via zkg install:

```
# zkg install Zeek-Known-Services-With-OrigFlag
# zkg install zeek-outbound-known-services-with-origflag
```

OR

Scripts:

https://github.com/esnet-security/Zeek-Known-Services-With-OrigFlag

https://github.com/esnet-security/zeek-outbound-known-services-with-origflag

References

ESnet Network graph:
https://my.es.net/

ZW’22 - Zeek - Zero Trust and Verify:
https://www.youtube.com/watch?v=07w4632mPRI

ZW’22 - Zeek Known services classification - ZTA edition:
https://youtu.be/BFS0aU7khTw

ZoW: -
https://indico.cern.ch/event/762505/contributions/3375196/attachments/1829810/2996233/Zeek_on_the_WAN.pdf

ZoMbis:
https://lightbytes.es.net/2021/03/02/defending-esnet-with-zombis/

Questions?

Thank You for attending!