



U.S. DEPARTMENT  
of ENERGY



BERKELEY LAB



# Performant Perimeter Security for HL-LHC



Eli Dart  
Network Engineer, Science Engagement  
[dart@es.net](mailto:dart@es.net)

LHCONE 55  
Karlsruhe, Germany  
8 October 2025

# Background

- Discussion at LHCONe 54
  - Some WLCG sites getting pressure from site security
    - Move everything behind a firewall
    - Likely to cause performance problems
    - Likely to cost additional money (especially in 400G HL-LHC era)
  - Value in putting together a common narrative for WLCG
    - Something that many sites can adopt
    - Something that many sites can use in discussion with site security
    - Something that works well in the HL-LHC era
- I'm going to test a narrative with you now
  - Listen with the ears of your site security
  - Discuss after
    - What is good about the presentation?
    - What about the presentation needs work or fixing?
    - Am I even thinking about this correctly?

# Begin

# The LHC Experiments: Background

- The Large Hadron Collider is the world's premier particle physics facility
  - Recent Higgs Boson Nobel Prize
  - Vibrant ongoing research program at the leading edge of physics
  - Four major experiments, each with a global collaboration
    - ATLAS, CMS, ALICE, LHCb
    - Thousands of scientists
    - Thousands more students
    - Hundreds of computing and data analysis sites
- The LHC experiments have a global networking, computing, data, and software enterprise
  - Integration with the LHC experiments' environment makes us part of this world-leading scientific environment
  - Through our involvement, our institution and scientists contribute to advancing humanity's understanding of Nature and the Universe

# LHC Experiments: A Global Technical Enterprise

- Very large scale in all dimensions
  - 1.5 exabytes of storage
  - 1.4 million compute cores
  - Global high speed (up to multi-400Gbps) network
  - 1000s of people
  - Extensive software environment
- The LHC experiments have their own internal organizations
  - System and network administration
  - Many software teams
  - Security
  - Science teams
- Each participating institution contributes in support of the whole to advance science
  - Networking, computing, software, data
  - Scientists, students, knowledge

# LHC Networking and Computing

- LHC networking uses two networks: LHCOPN and LHCONE
- LHCOPN is dedicated to traffic between CERN and Tier1 sites
- LHC Open Network Environment (LHCONE) is for analysis
  - Global overlay network with its own routing table
  - Subset of the Internet - only science institutions are present
  - Used by LHC experiments and by collaborating experiments which use the same computing infrastructure (e.g. Belle-II experiment)
- LHC computing: World-wide LHC Computing Grid (WLCG)
  - 1.4 million computing cores and 1.5 exabytes of storage
  - Distributed across the globe
  - Integrated via LHCONE into a single data analysis environment
  - Distributed model gets us more resources
    - Our researchers have access to far more computing and data via WLCG than they would if they were only able to use local resources

# WLCG Systems Profile

- WLCG is composed of servers and storage
  - Linux servers for compute
  - Linux servers or dedicated systems for storage
- No personal or enterprise systems in WLCG
  - No windows workstations
  - No gaming consoles, smart TVs, etc (no student housing)
  - No Citrix boxes, Exchange servers, VPN appliances, etc.
- This distinction is important for security
  - WLCG server systems have small attack surface
  - Most security vulnerabilities are elsewhere
    - Vulnerable user-facing applications
    - Vulnerable enterprise systems
    - Vulnerable firewalls
    - None of these exist in WLCG

# LHC and WLCG: Traffic Profile

- WLCG systems exchange traffic based on job profile
  - Physics data analysis needs determine input data
  - Data is distributed globally
  - Central data catalog knows location of all copies
  - Compute goes to data if possible, else data goes to compute
    - Job migration to data occurs routinely
    - Data access: file copy or remote I/O - both are used routinely
- Traffic is machine to machine
  - No interactive user login to WLCG compute nodes
  - Job execution and data exchange governed by modern auth
    - OAuth, tokens
    - PKI has been retired
  - Cybersecurity profile: simple
    - HTTPS
    - XRootD
- Very large data rates and volumes
  - 100Gbps today
  - 400Gbps in 2029
  - Nx400Gbps in 2030 and beyond

# Connecting WLCG Systems to LHC Networks

- Specific combination of attributes
  - High speed
  - Narrow traffic profile
  - Simple from cybersecurity perspective
    - File transfer, remote I/O
    - No complex applications, no broad attack surfaces
- Easy to secure with performant technologies
  - Stateless firewall (router ACL)
- Difficult to operate well using complex security controls
  - Deep packet inspection does not perform
    - 400Gbps in a few years
  - Enterprise firewall capabilities are wasted
    - Complex firewalls have no specific protocol analyzers for LHC traffic
    - Running 400G through HTTPS analyzers requires needless expense

# Stateless vs. Stateful Firewalls for WLCG

- Comparison of capabilities
- Relevant traffic filtering for WLCG traffic
  - Source and destination address
  - Source and destination port
  - Traffic is data transfer or auth - opaque to packet inspection
- Layer3/Layer4 filters easy with stateless firewall
  - Router ACLs do this at line rate
  - Enterprise firewall config will implement the same thing, but slower and at higher cost
- Key point: WLCG traffic is a good fit for stateless firewalls, poor fit for complex enterprise firewalls

# Strategic Support for WLCG and LHC

- Need a durable policy framework for LHC support
  - Important international collaboration
  - Important global scientific and technical enterprise
  - High speed networking allows our institution to participate fully in this important community
- Performance is key to successful integration with LHC
  - High speed
  - Advanced services
- Performant security is important
  - WLCG computing can be safely operated with stateless firewalls
  - Spending the additional money on enterprise features adds no value, and impedes performance
- How do we work together to ensure WLCG systems here are able to integrate well with the global collaboration?

# End

# Critique and Questions

- How would your security officer receive this?
- This implies the Science DMZ model
  - Should the discussion include the Science DMZ specifically?
  - Is it better to leave it out?
- Would it be useful to enumerate the problems with enterprise firewalls?
  - Some CIOs might view that as combative/hostile
  - It is however true - firewalls, VPN boxes, etc. are full of security holes (yes, this is ironic even though it's true)
- Very interested in your feedback
- Next step is to start working on a document



U.S. DEPARTMENT  
of ENERGY



BERKELEY LAB



# Discussion



Eli Dart

dart@es.net

<https://my.es.net/>

<https://www.es.net/>

<https://fasterdata.es.net/>

# Copy this slide for bullets

- Bullets
  - More bullets
    - Even more bullets
      - C'mon, too many bullets

# Copy this slide for bullets

- Bullets
  - More bullets
    - Even more bullets
      - C'mon, too many bullets