# Review of Cyber-Security Event on Jefferson Lab's Accelerator Network

Theo McGuckin

(Special Thanks: Anthony Cuffe, Andy Kowalski, Theo Larrieu)

# Outline

INTRODUCTION

THE CYBER-EVENT

ACE IMMEDIATE CHANGES

ACE LONG-TERM PLAN

LESSONS LEARNED

Section I

# INTRODUCTION

# Disclaimer

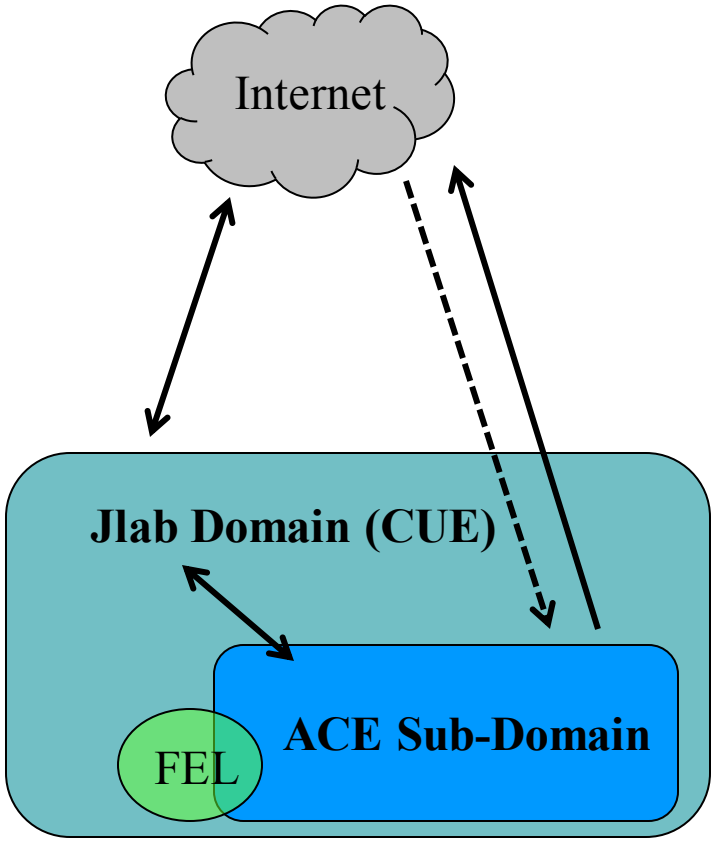
- The investigation of the cyber-event at Jlab is still on-going. As such many aspects of the event cannot be discussed or published in great detail.
- This talk will focus on the impact and resulting changes to the Accelerator Computing Environment (ACE) portion of the network.
- For security reasons many IP-addresses, computer names and subnet references have been obfuscated.

# Definitions

- CUE – Common User Environment – portion of Jlab network outside of accelerator division, supported by Computer Center. Generally covers the jlab.org domain
- ACE – Accelerator Computer Environment – portion of Jlab network inside accelerator division, supported by accelerator sys-admin team (including me). Generally covered under acc.jlab.org sub-domain.
- On-site – anything inside the jlab.org domain.
- Fiefdom – a block of IP-space (possibly covering multiple subnets) that encompasses all systems required for a given subnet to function (example: the file-server(s), webserver(s), database server(s), printers, gateways and workstations used by operations would be in the "OPS-fiefdom"). Fiefdoms should be completely independent.

# JLab Network Overview (pre-event)

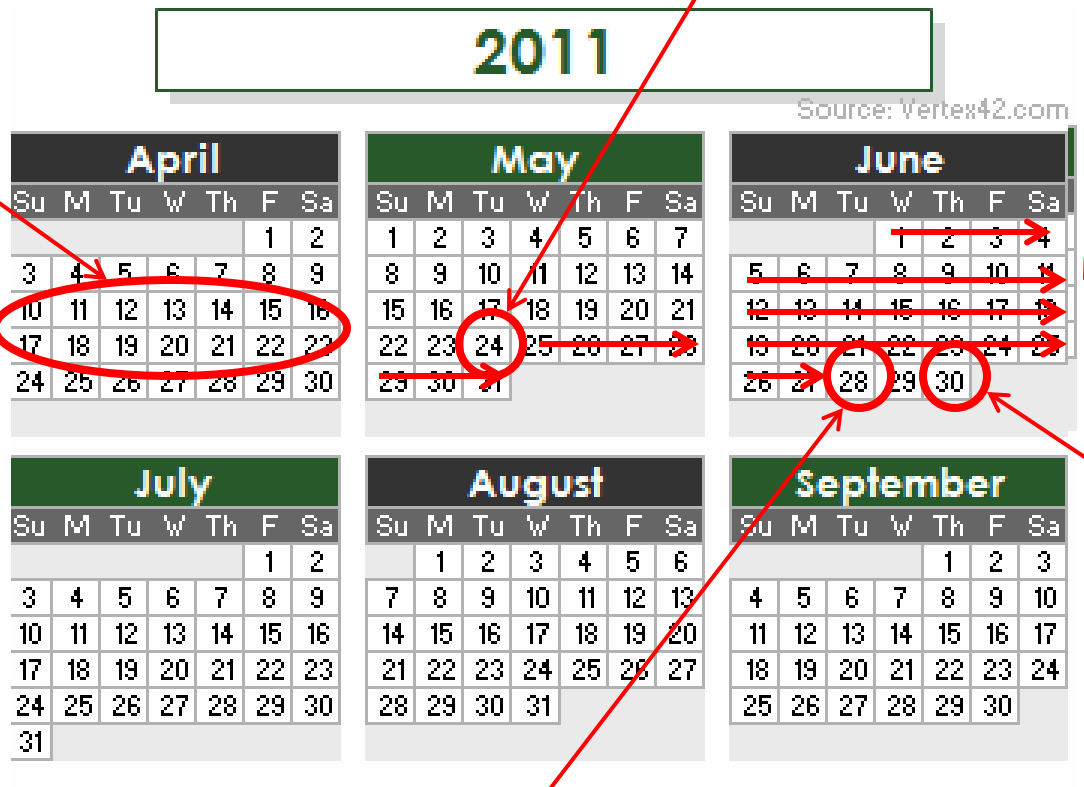
- The overall JLab network is maintained by the Common User Environment (CUE) group.
- JLab's accelerator network is maintained by the Accelerator Computing Environment (ACE) team.
- While most access into ACE network segment from internet was blocked (or had to go through Jlab domain first), outbound traffic from ACE to internet was completely open.
- Free-Electron Laser (FEL) – special case



Section II

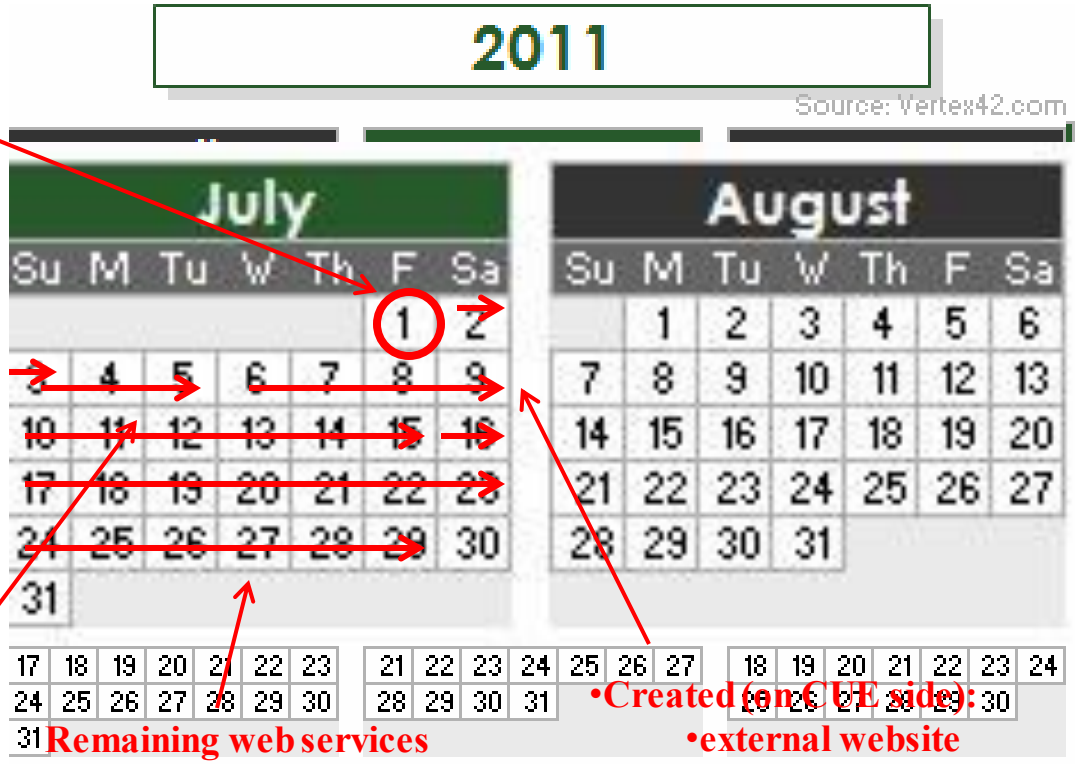
# THE CYBER-EVENT

# Timeline of Attack



# Timeline of Attack (Cont.)

All internet access blocked (except email)




Plans for one and a half years of security upgrades accelerated to ~one week

Launch recovery activities

Remaining web services restored

- Created (on CUE side):
  - external website
  - new Windows domain
- Changed all passwords
- "Smart cards" reissued
- General internet access restored

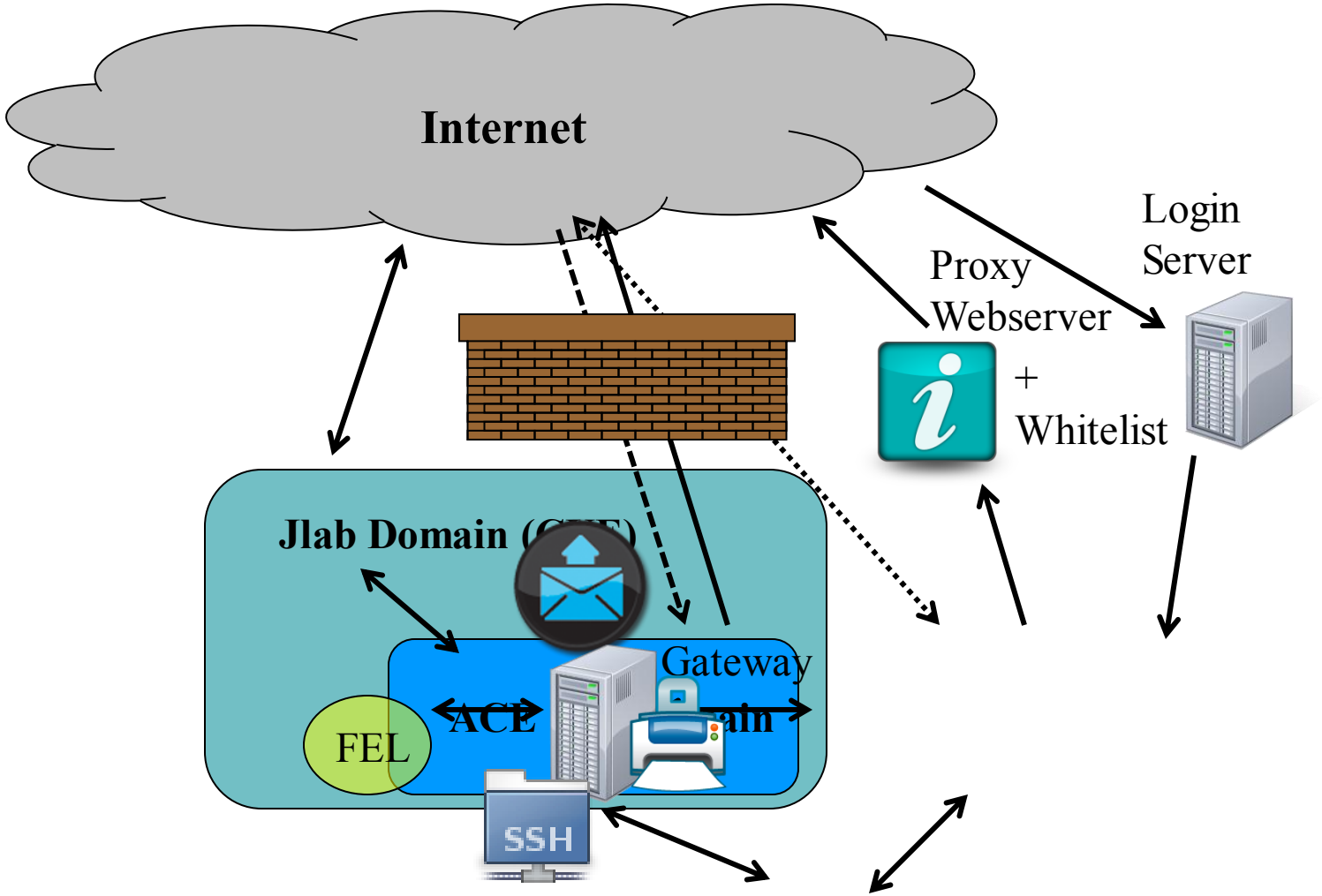
# Initial Impact on ACE

- July 1st: All internet access from ACE blocked. Only limited access between ACE and the rest of lab network allowed.
- July 6th: General internet access restored from ACE to non-ACE systems
  - Off-site access available via two-step (ssh to non-ACE machine, connect to outside via web-browser, for example.)
  - Initial plan was to **not** restore any direct off-site access for ACE machines, but this quickly proved untenable
    - ACE systems could not be patched
    - Developers could not access off-site resources (collaboration was hindered)
    - Too much existing infrastructure was based around off-site access availability

Section III

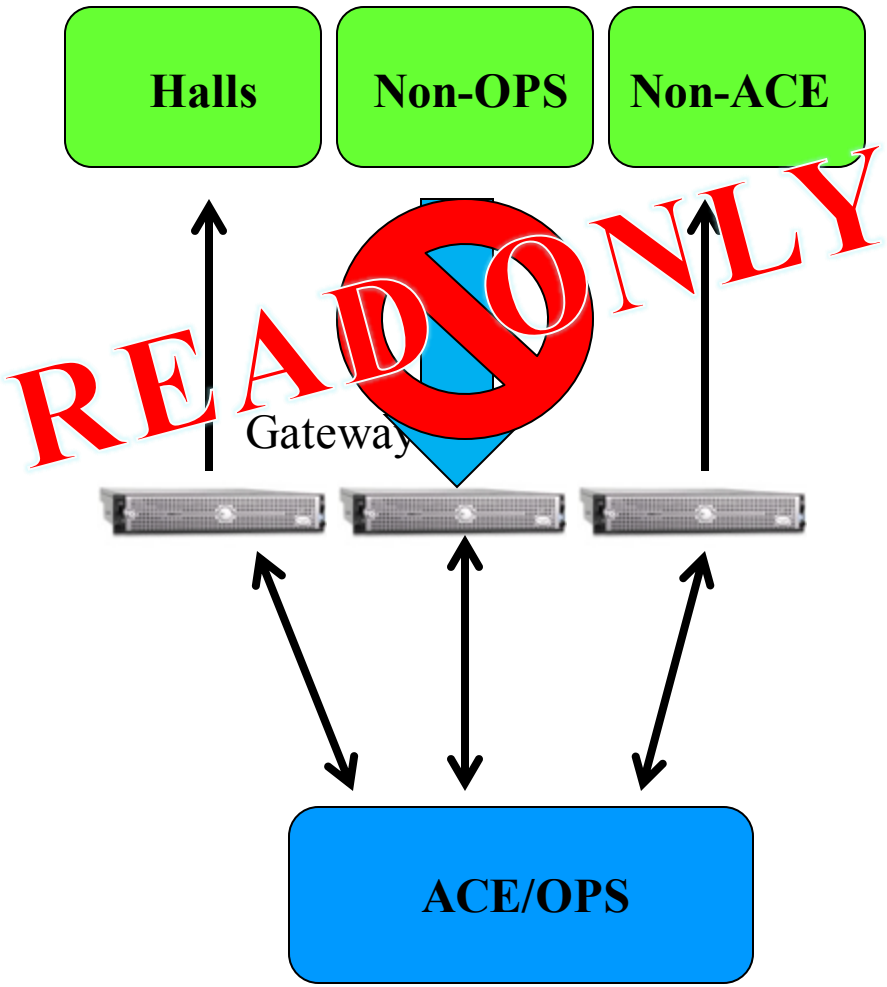
# ACE IMMEDIATE CHANGES

# ACE Network Separation & Access



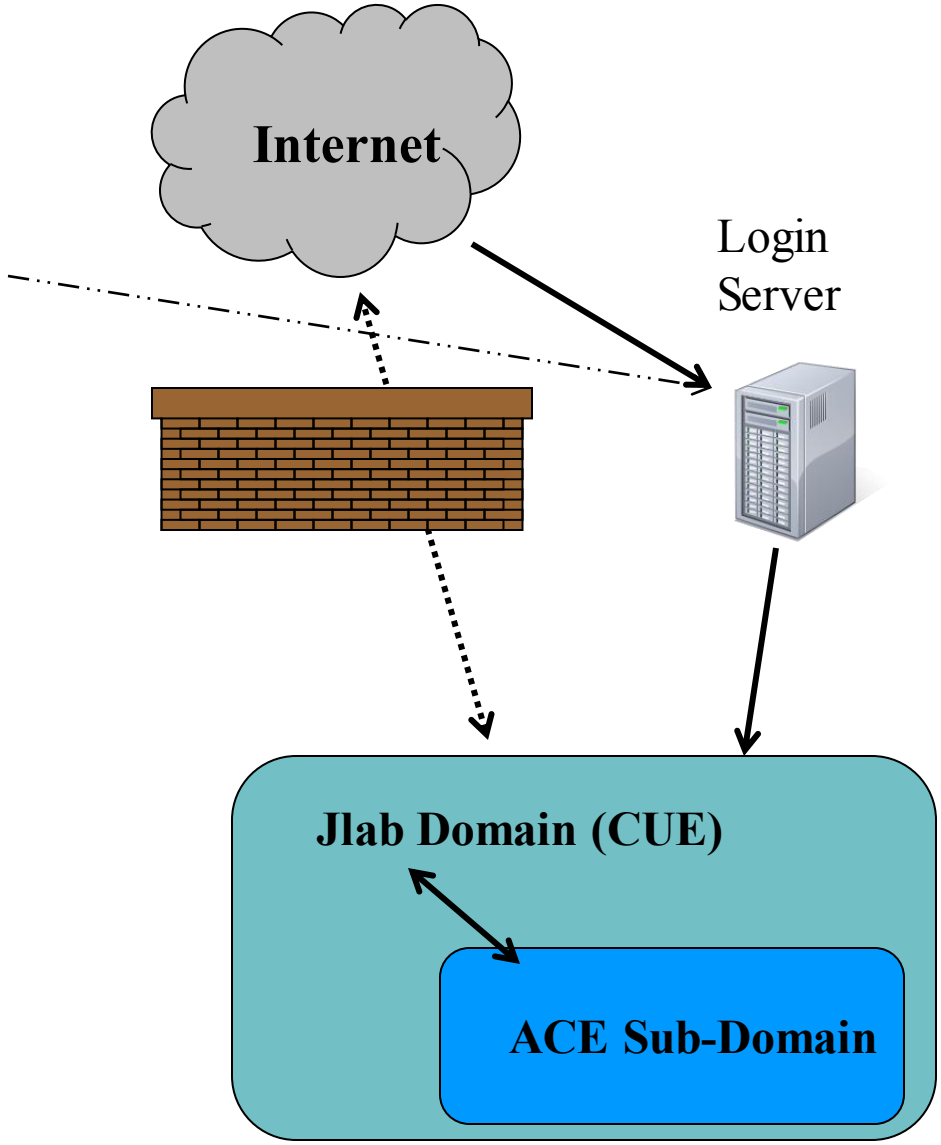
# Channel Access Gateways

- All channel access signals blocked across network by default
- Dedicated gateway systems provided for experimental halls, and other non-ACE systems
  - Gateways are read-only
  - Gateways are isolated so problems with one will not hinder another



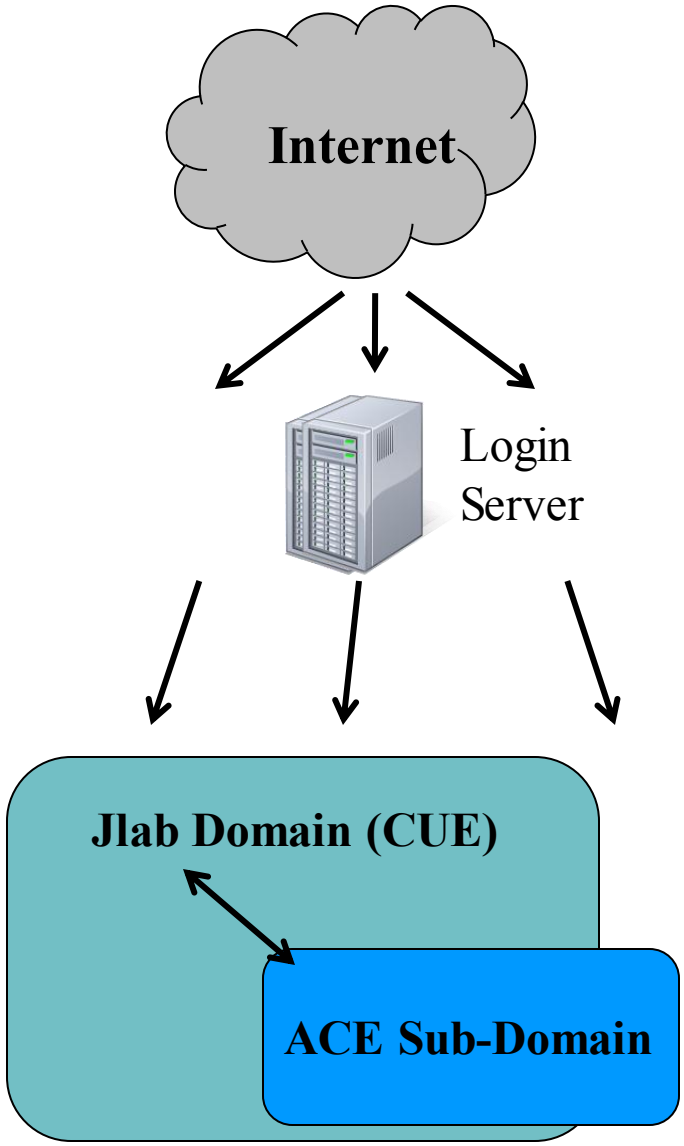
# Off-site Network Access

- Off-site access to Jlab network available via dedicated login servers
- Two-factor authentication required



# ACE Login Server and VPN

- Previously, a single login server was used to access on-site systems
- Now, separate ACE login server (which was already in the works) + VPN allows access to on-site ACE systems
- Again, two-factor authentication required



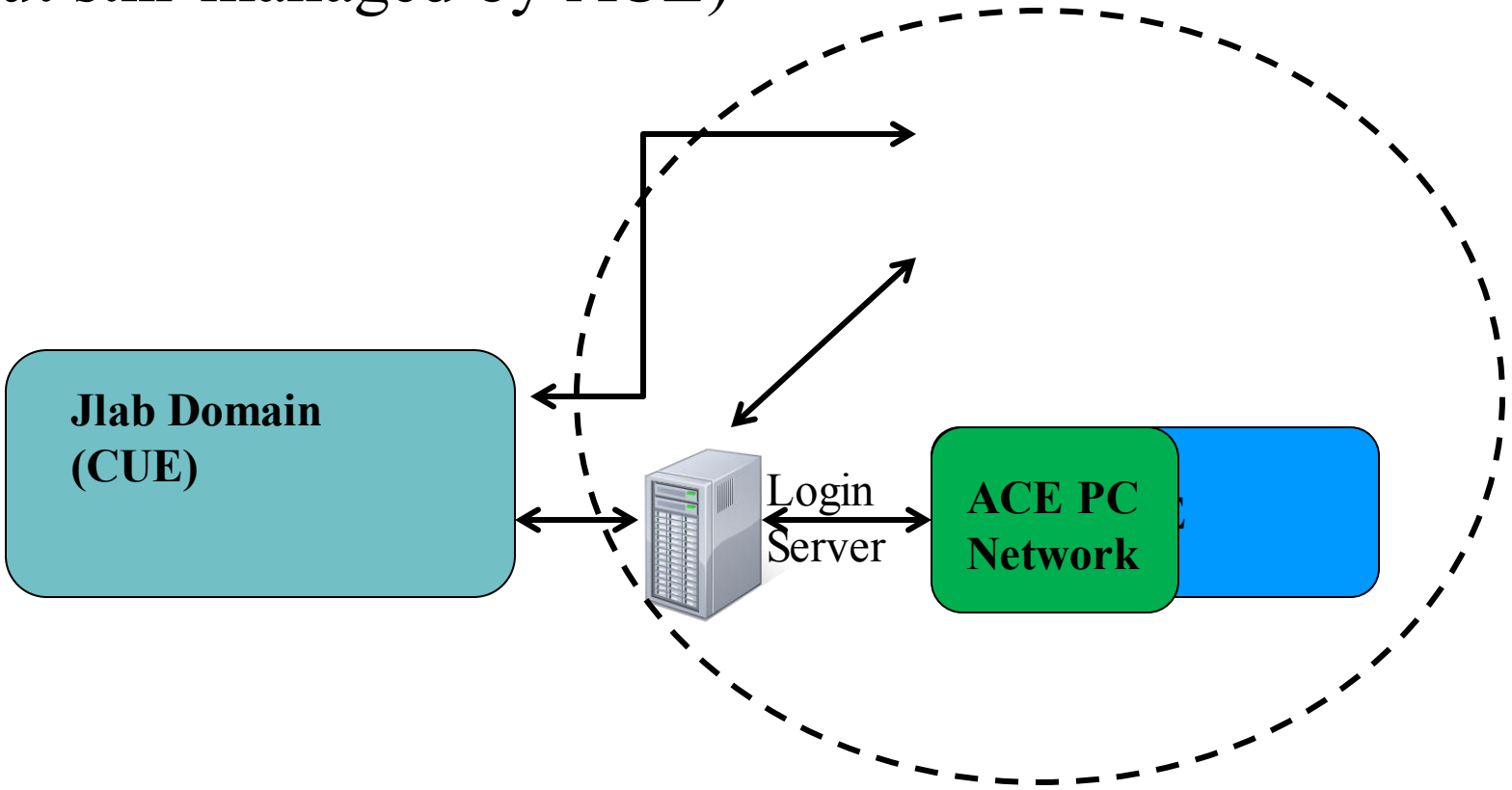
# Two-factor Authentication

- Required for all off-site access to ACE systems (via login server)
- Smart card (USB) requirement added for all admin user functions on Windows machines
- Crypto card implementation required


+ **Password**

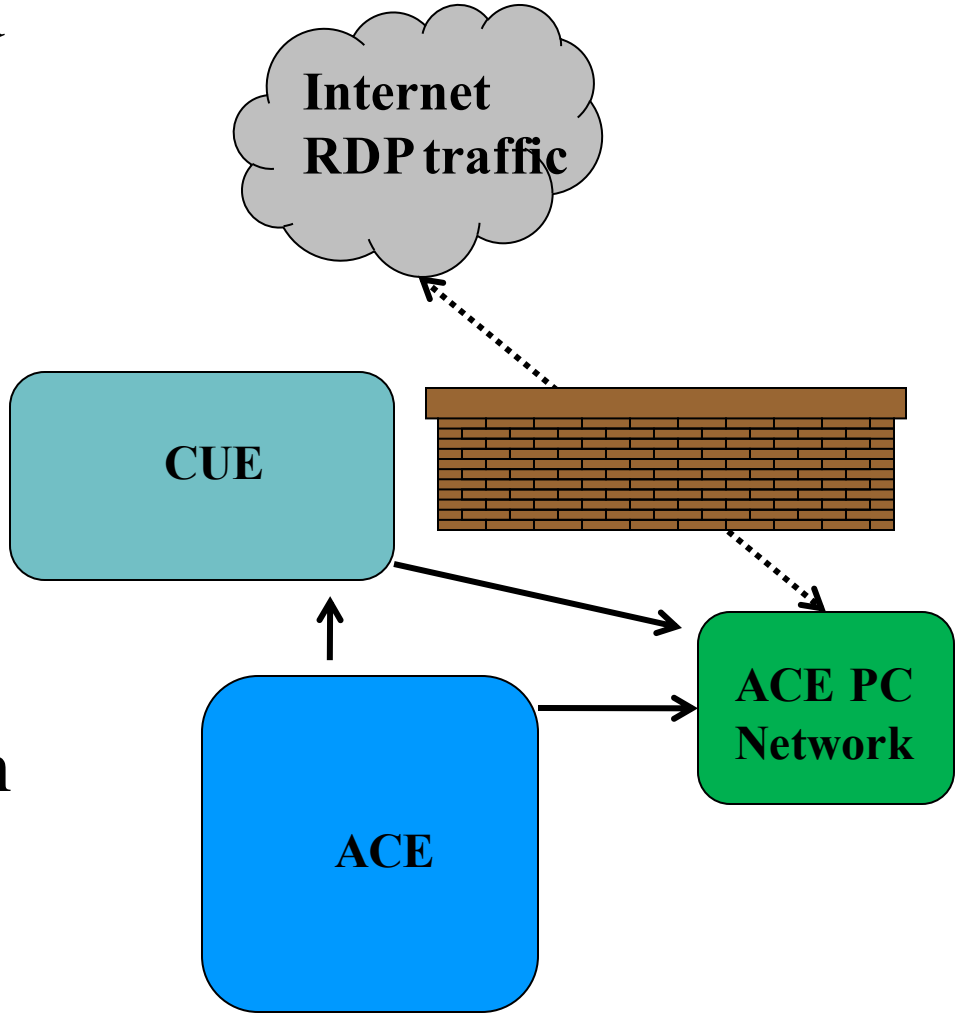
# Dedicated Windows-network

All Windows desktop machines moved to a dedicated fiefdom located outside of ACE network (but still managed by ACE)



# Remote Desktop Protocol

- RDP traffic allowed out from ACE (specifically to new ACE PC network)
- RDP traffic into ACE PC Network from CUE allowed.
- No direct RDP traffic allowed from off-site.



# Sudo

- Removal of sudoer privileges for admin account
  - Account primarily used for file synchronization across fiefdoms
  - Previously used for logging in to file servers
  - Previously had full, non-password sudo priviledges
- All sudo commands now require password authentication
  - Time-out after five minutes
  - Previously NO sudo commands required password authentication

# User-Audit and Policy

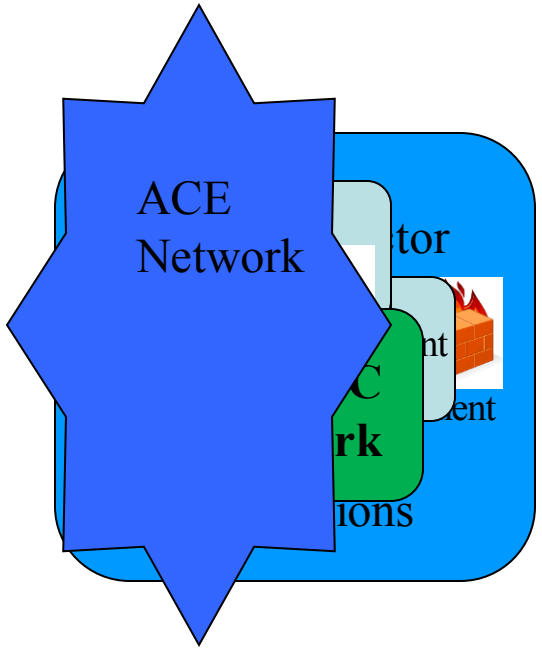
- Previously completed user-account audit and policy definition allowed for strong control over user-accounts
- Very easy to update all passwords in short time.

Section IV

# ACE LONG-TERM PLAN

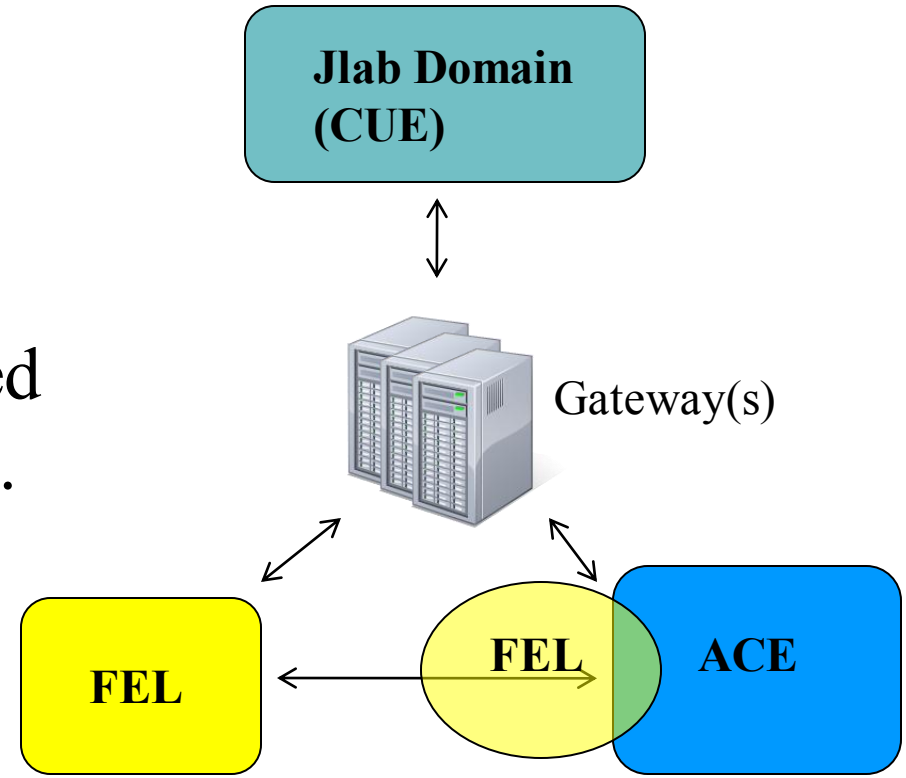
# New Network Separation

- New enclave for Windows PCs (DONE)
- Firewall and ACL rule implementation between fiefdoms



# FEL Complete Segmentation

- Due to the sensitive nature of some of its work, and separate operating schedule, FEL fiefdom will need to be fully segmented.
- This will require additional configuration and hardware changes.



# Switch from NIS to NIS+Kerberos

- NIS shortcomings
  - Open access to users and password hashes
  - Auditing, password aging, password cracking – all afterthoughts or external utilities
  - Password maintenance across fiefdoms non-trivial
- Kerberos advantages
  - User policies available
  - Scheduled and On-demand password expiration
  - Password strength testing
  - Simplified password changing

# NIS+Kerberos (Cont.)

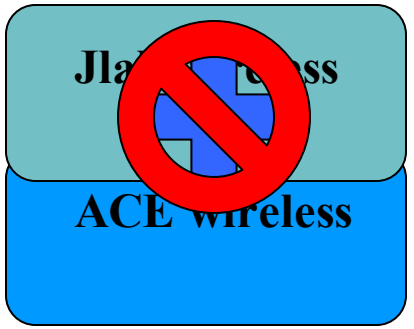
- Kerberos would handle authentication
  - User password authentication
  - Server and workstation authentication
- NIS would handle authorization
  - Groups, netgroups, uids, etc. still live in NIS

# NIS -> Local Files (or LDAP?)

- Replace NIS with Local Files
  - Removes “ypcat”-dump capability
  - Permissions on local files add an extra layer of security
- LDAP may also be a possible replacement for NIS

# Wireless

- Currently the wireless networks for ACE and CUE are tightly bound.
- New policies may need to be put in place to strongly restrict what can go on ACE wireless network.
- Only dedicated devices on ACE wireless?



# Network monitoring tools for ACE

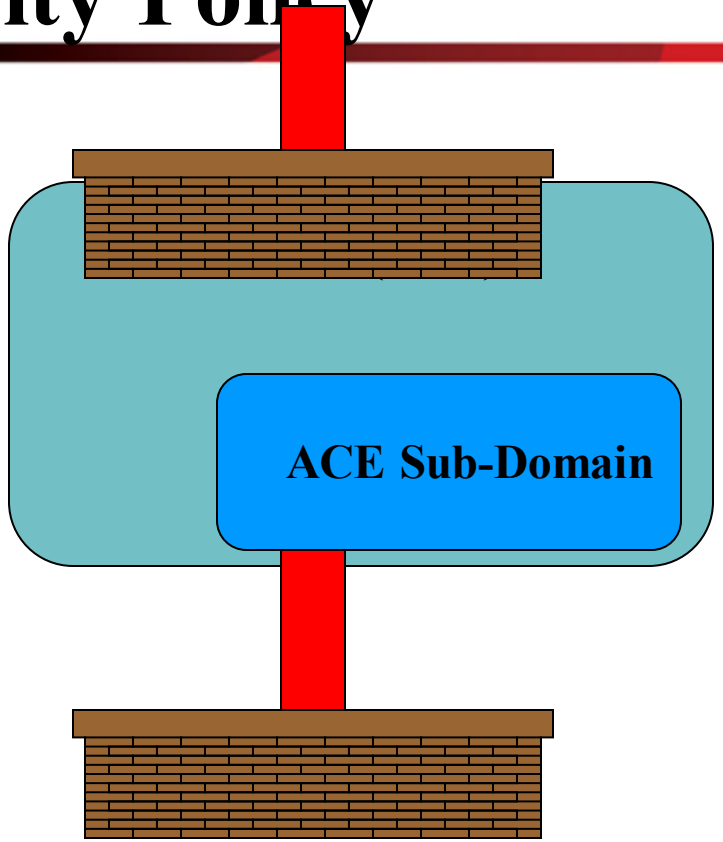
- Expand existing tools
  - Cacti
  - smokeping
- Add additional network monitoring
  - Splunk/Global syslog
  - Nagios
  - Swatch (not the watch company)

Section V

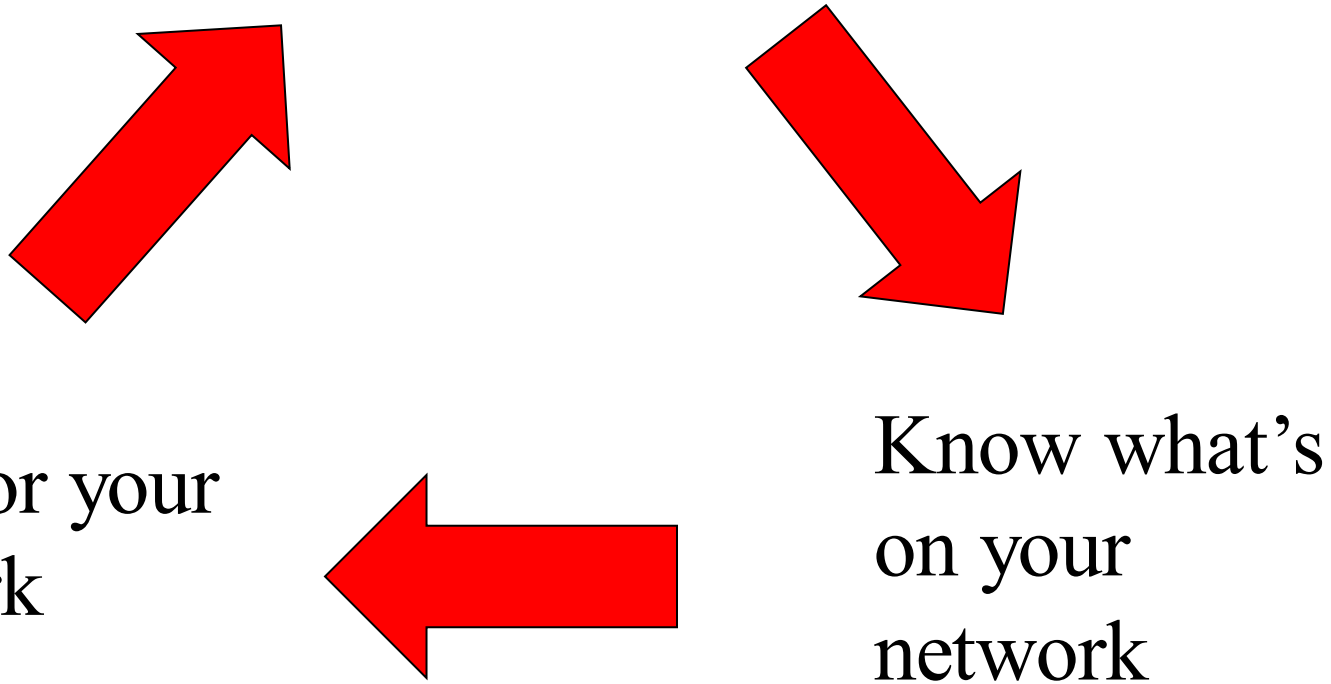
# LESSONS LEARNED

# Own Your Security Policy

- Layered nature of Jlab's network (ACE subnet within CUE) lead to an attitude that CUE would handle all security
- Problem arises if CUE becomes compromised
  - Layered defense required
  - Active ACE security required



# Know Your Security



fin