Argonne NATIONAL LABORATORY

… for a brighter future

U.S. Department of Energy

UChicago ▶ Argonne LLC

A U.S. Department of Energy laboratory managed by UChicago Argonne, LLC

Network Security and Impact on Science

APS/Users Monthly Operations Meeting

September 26, 2007

Kenneth Sidorowicz

AES-IT

Introduction:

- Joint Meeting of the Partner User Council (PUC) Executive Board and APSUO Steering Committee on August 22, 2007

- Description of IT committees at Argonne
- The network architecture at the APS
- Network performance testing
- Remote access policy for Argonne
- The need for cyber security
- Future plans

Lab IT Committees

- 3.2.2.1 The Information Technology Policy Board (ITPB)

  From the Argonne Cyber Security Program Plan

  - Consists of the chief information officer and representative division directors from each of the associate Laboratory directorates and reports to the Laboratory director.
  - Formulates cyber security policy.
  - Recommends policy to the Laboratory director.
  - Maintains an updated CSPP for the Laboratory.
  - Delegates technical details of policy development and implementation to the Cyber Security Technical Working Group.

- Members — Division
  - Bill Ruzicka — AES
  - Tom Wolsko — DIS
  - Donald Schmitt — OPS
  - Ray Bair — MCS
  - Charlie Catlett — CIO/CIS

Lab IT Committees continued

- Information Technology - Architecture Review Group (IT-ARG)
  From the October 3, 2005 Charter Overview

  The Information Technology Architecture and Review Group (ITARG) is responsible for providing guidance, review and recommendations for information technology (IT) changes, handling policy exception requests, and providing technical review of proposed IT policies at the Laboratory. The ITARG is composed of a group of Information Technology experts representing a cross-section of the Laboratory.

IT-ARG Charter

- **Reporting**

  •The ITARG reports to the Information Technology Policy Board (ITPB). It provides an advisory function to the Cyber Security Program Manager (CSPM), Chief Information Officer (CIO) and Information Technology Policy Board (ITPB).

- **Membership**

  Voting Membership of the ITARG shall consist of at least 6 members, including:

  • At least one representative from each of the ANL Associate Lab Directorates (ALD).

  •At least one representative from the Cyber Security Program Manager's office.

  •At least one current member of the Core Networking Group

  •At least two Cyber Security Program Representatives.

In addition, it is a goal that the technical expertise related to both Cyber Security and information technology of the members be as strong as possible.

The ITARG nominated members must be approved by the ITPB. It is expected that membership will change over time in order to involve many different representatives from across the Laboratory. Members will participate for an average of approximately two years.

IT-ARG Charter

– Responsibility

The ITARG has the following responsibilities:

- To provide an internal peer-review process to validate and comment on:
  - Threat, risk, and vulnerability assessments.
  - System class assessments.
  - Any other assessments performed by Laboratory divisions under the direction of the CSPM.

  These assessments will be advisory to the CSPM.
- To approve or disapprove requested exceptions to Cyber Security policies as defined in the ANL Cyber Security policy and requirements documents and to register these decisions with the CSPM.
- To review the technical implementation of Cyber Security requirements (e.g. firewall rules, password analysis programs, etc) and provide commentary upon such to the CSPM and CIO.
- To act as an advisory board for Information Technology architectural and functional issues at both the Laboratory and the Divisional level, as requested.
- To act as an advisory board for proposed Information Technology and Cyber Security policies at the request of the CIO and IT Policy Board.

IT-ARG Committee

MEMBERS	DIVISION	ALD	
Vito Berardi	ES	Al Sattelberger (Interim)	ALD
Paul Domagala	CIS	Bo Arnold	OPS
Rodney East	CNM	Al Sattelberger	ALD
Mathew Kwiatkowski*	CIS	Bo Arnold	CSPO
David Leibfritz	APS	Murray Gibson	ALD/CSPR
Gene Rackow*	CIS	Bo Arnold	CSPO
Tracy Rager*	DIS	Al Sattelberger (Interim)	ALD/CSPR
Dorathea Seymour*	DIS	Al Sattelberger (Interim)	ALD/CSPR
Kenneth Sidorowicz	APS	Murray Gibson	ALD/CSPR
Michael Skwarek	CIS	Bo Arnold	CSPM
Craig Stacey	MCS	Rick Stevens	ALD/CSPR
Scott Pinkerton	CIS	Bo Arnold	Networking

Scientific User Facilities	2
Physical Sciences	1
Applied Science and Technology	2
Operations and Business Management	4
Computing and Life Sciences	1

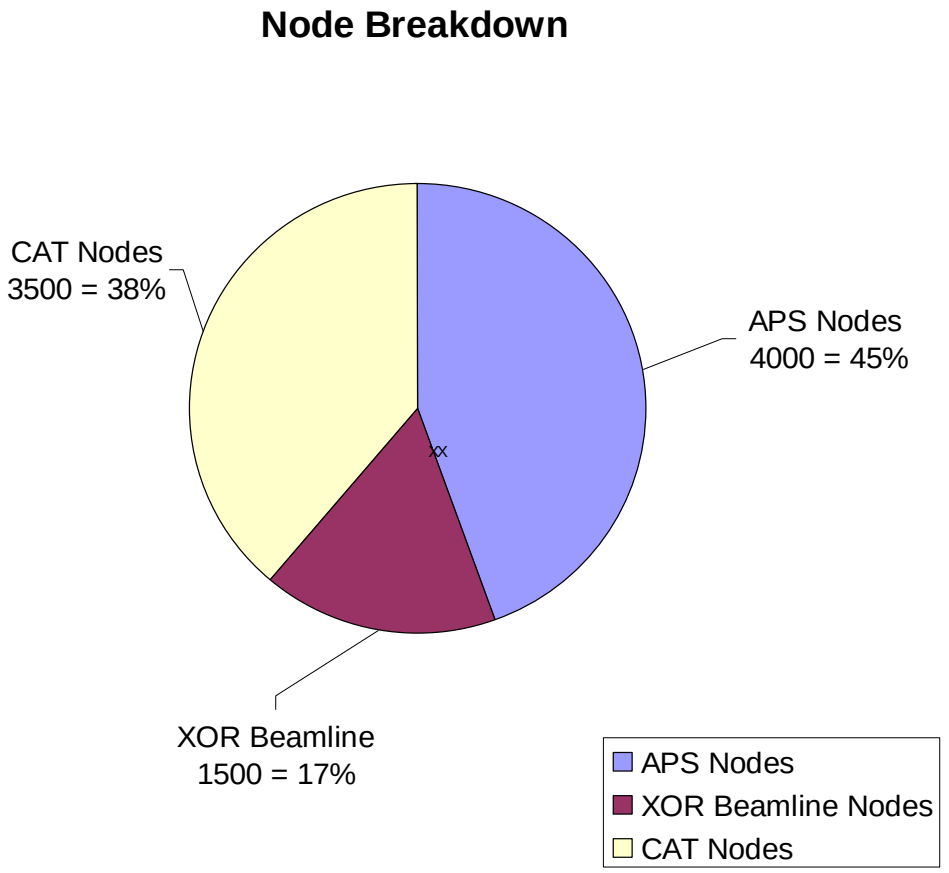
* = rotating membership

APS Network Infrastructure

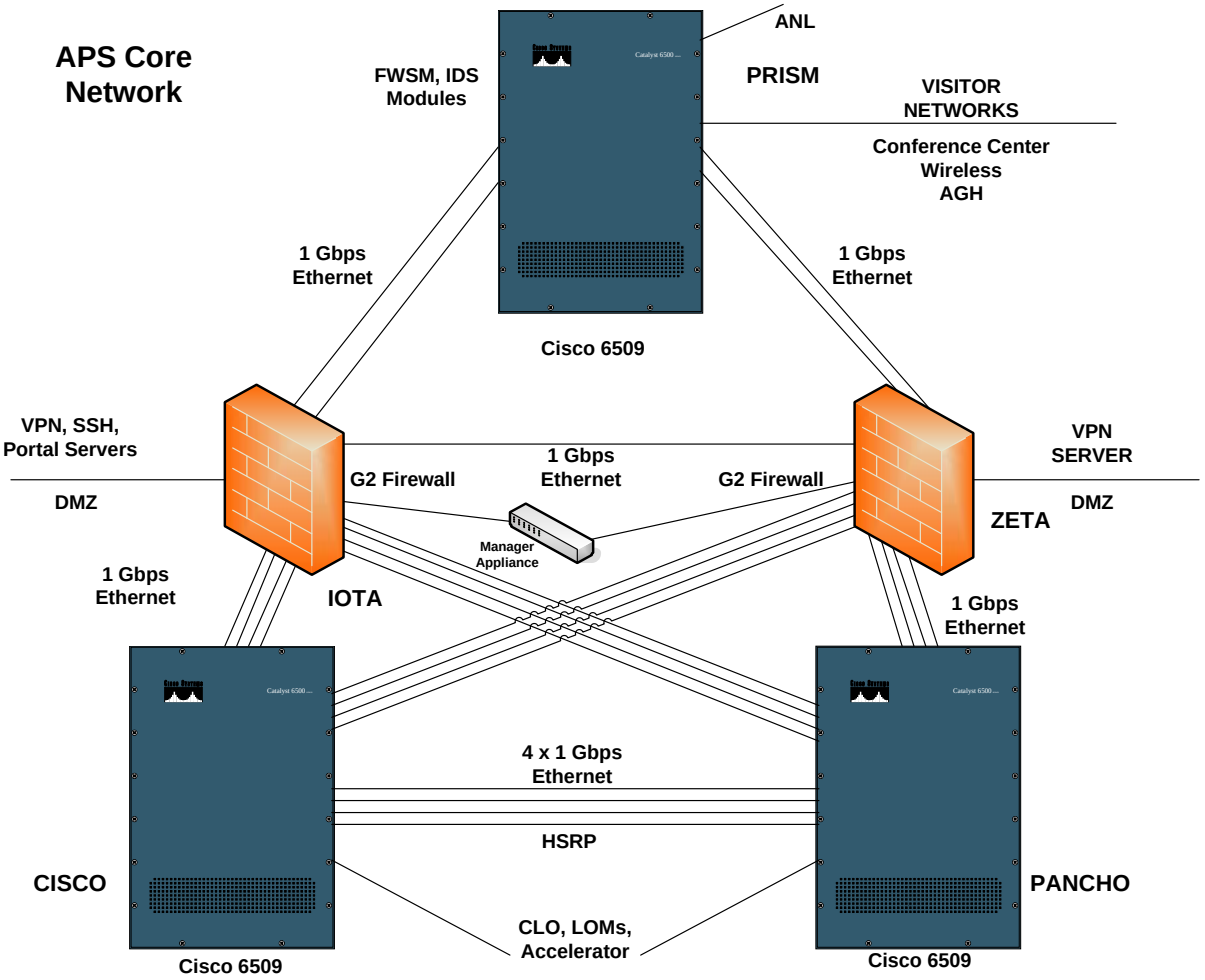
- APS - 4000 nodes
  - 40 switches/routers
  - 30 subnets
- XOR Beamlines - 1500 nodes
  - 20 switches/routers
  - 55 subnets
- CAT - 3500 nodes

  10 switches/routers

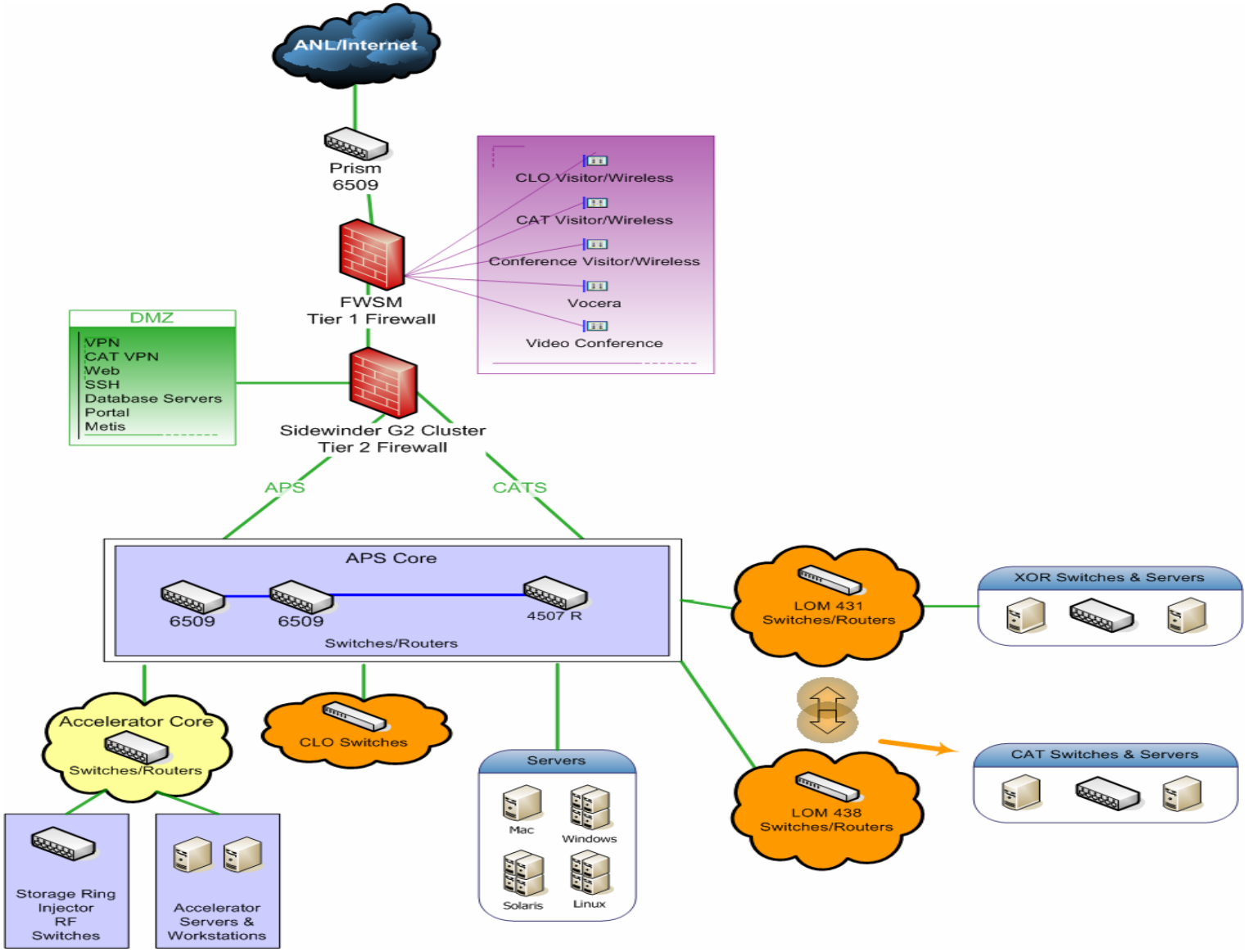
  35 subnets



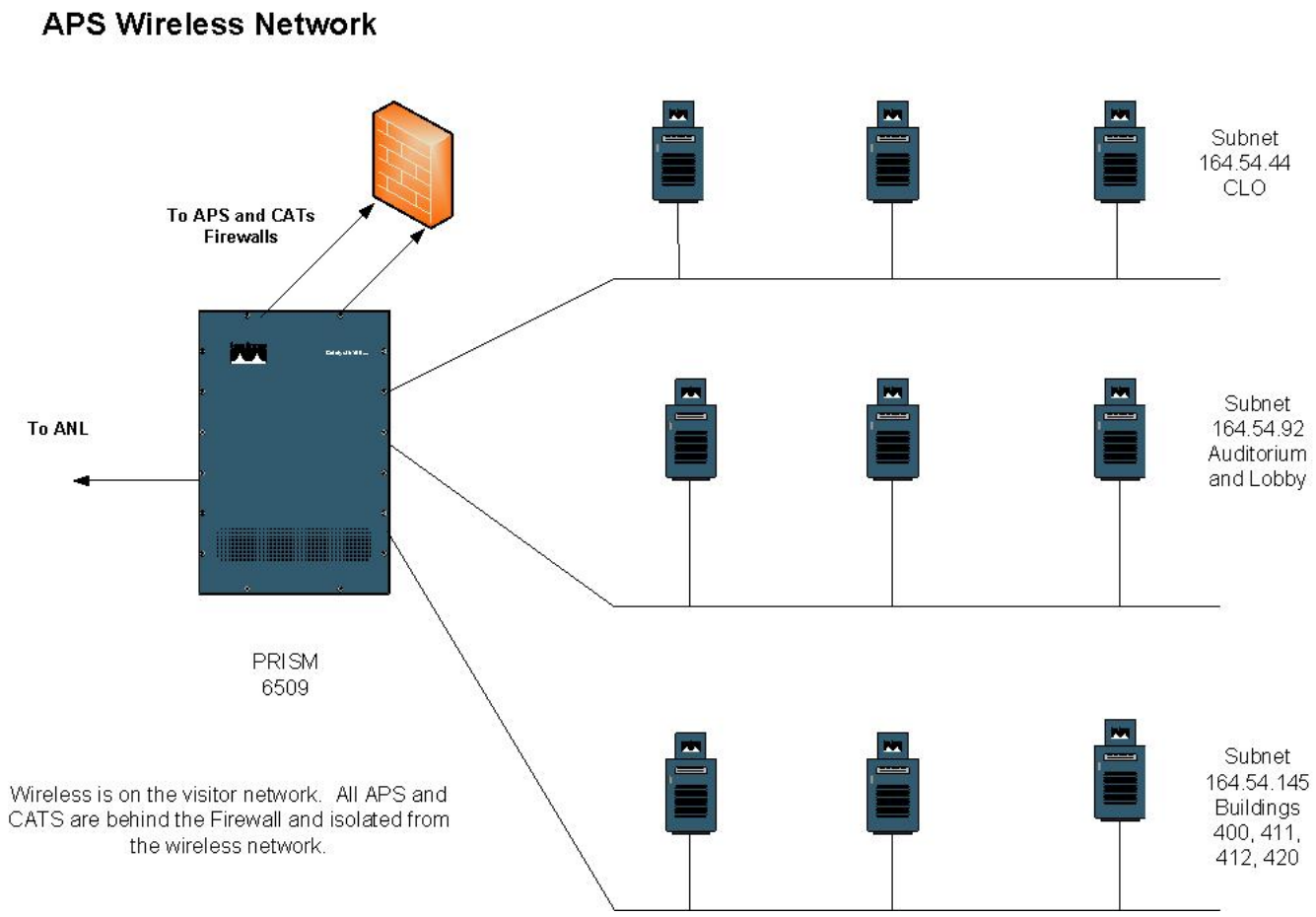
APS Core Network



APS Network


ANL/Internet
Prism
6509
FWSM
Tier 1 Firewall
CLO Visitor/Wireless
CAT Visitor/Wireless
Conference Visitor/Wireless
Vocera
Video Conference
DMZ
VPN
CAT VPN
Web
SSH
Database Servers
Portal
Metis
Sidewinder G2 Cluster
Tier 2 Firewall
APS
CATS
APS Core
6509
6509
4507 R
Switches/Routers
LOM 431
Switches/Routers
XOR Switches & Servers
Accelerator Core
Switches/Routers
CLO Switches
Servers
Mac
Windows
Solaris
Linux
LOM 438
Switches/Routers
CAT Switches & Servers
Storage Ring
Injector
RF
Switches
Accelerator
Servers &
Workstations

Wireless at the APS



Argonne Remote Access Policy

APPENDIX G CSD-R4.1

REQUIREMENTS AND RECOMMENDATIONS ON REMOTE ACCESS TO AND EXTENSION OF ARGONNE NATIONAL LABORATORY NETWORKS

1 PURPOSE OF THIS DOCUMENT

This document describes the requirements and recommendations for:

Systems and applications that enable remote access to the Laboratory.

Systems and applications that extend the Laboratory network.

It is a companion document to CSD-R2, "Network-Based Access to Hosts" and CSD-G14, "ANL Firewall Architecture." CSD-R2 describes the security measures that must be in place in the network to protect against unauthorized entry, whereas this document describes how entry is to be authorized.

2 EXECUTIVE SUMMARY

This requirements document is designed to provide the Laboratory with protection from unauthorized and insecure access to Laboratory network resources. The policy states that all network-based remote access to Laboratory computer systems that are not intended for public use shall use a secure, encrypted access method to prevent unauthorized access to Laboratory resources.

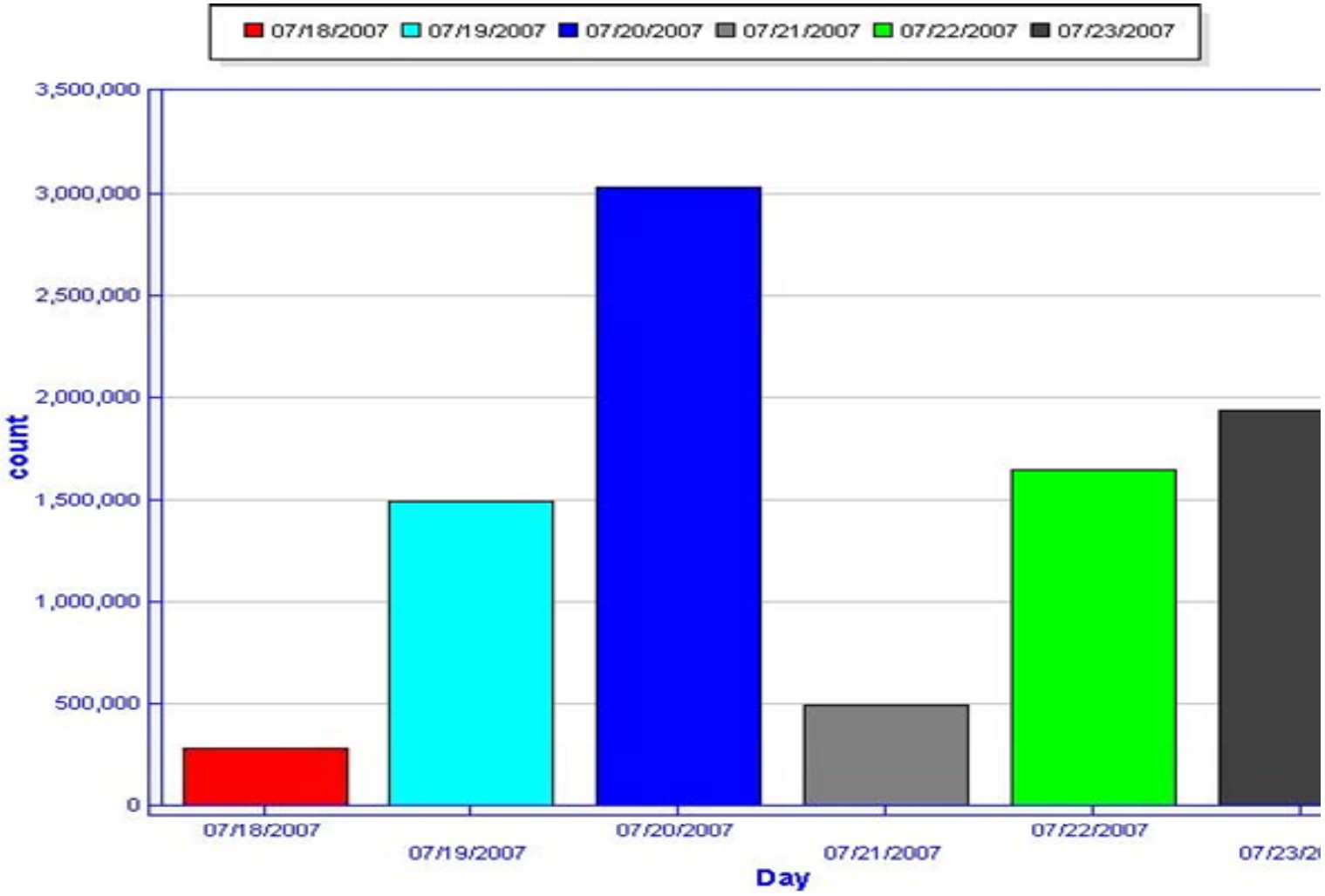
To provide this protection, the Laboratory requires that methods of accessing the Laboratory network be documented, approved, and verified. The methods of access include modems, ISDN devices, virtual private networks (VPNs), secure web services (such as https), wireless devices, methods using secure shell protocols, methods using Kerberos authentication, and network-based video conferencing. Any technology that extends the boundaries of the Laboratory network is bound by this policy.

Wireless devices have unique security issues. The ANL policies for wireless networks are described in CSD-R7.

Network Performance - Iperf Testing at the APS

- 938 Mbps between LOM's and APS edge router Prism
- 920 Mbps between LOM's and Argonne's edge router
- Iperf measures TCP and UDP bandwidth performance
- Iperf is available at http//dast.nlanr.net/Projects/Iperf
- IT web page is being created to display Iperf data

External Attacks



Firewall Anti-Spam Summary

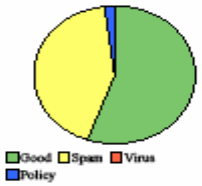
CipherTrust

Executive Summary

(Cumulative counts for 07/01/2007 00:00:00 to 08/20/2007 08:53:18)

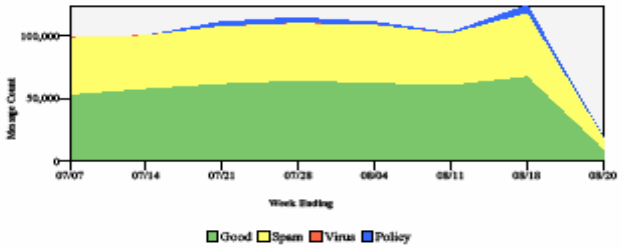
INBOUND

Message Classification



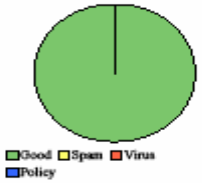
	Good	Spam	Virus	Policy	Total
Count	429294	329679	962	20363	780298
%	55.0	42.3	0.1	2.6	100.0

Message Trend



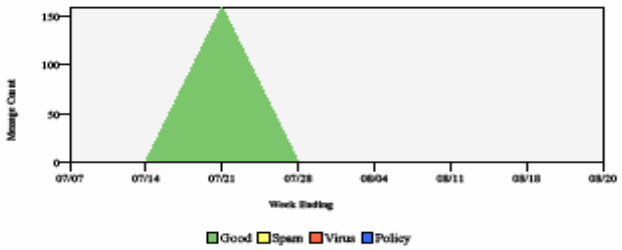
OUTBOUND

Message Classification



	Good	Spam	Virus	Policy	Total
Count	159	0	0	0	159
%	100.0	0.0	0.0	0.0	100.0

Message Trend



IM: hestia.aps.anl.gov Executive Summary / Page 1 Created: 08/20/2007

Future Plans

- Upgrade the backbone network and Argonne uplink to redundant 10 GigE. Vendors are promising new modules will be available during calendar year 2007.
- Upgrade Tier 1 and Tier 2 firewalls to 10 GigE. Vendors are promising new firewalls will be available at the end of calendar year 2007.
- 802.1x authentication for wireless access to internal network.
- Distributed iperf servers to measure network performance.
- SSL VPN – Clientless or automatically downloaded client. Web-based “Anywhere” access. Support for Windows Vista, Mac OS X, Linux.

Conclusion:

- IT committees at Argonne determine cyber security policy
- The network architecture at the APS is designed to maximize network performance and provide a highly-available environment to minimize network downtime
- Network performance testing with iperf will provide real-time network statistics via the web
- Remote access policy for Argonne covers the APS.
- The need for cyber security is essential to prevent network hackers from disrupting accelerator and/or beamline operations
- Future plans to improve network performance from beamlines to Argonne and the Internet. Next generation VPN server for remote access.