

# ***APS Firewall Upgrade***

*Ken Sidorowicz*

*July 15, 2004*

## ***Argonne National Laboratory***



Office of Science  
U.S. Department of Energy

*A U.S. Department of Energy  
Office of Science Laboratory  
Operated by The University of Chicago*



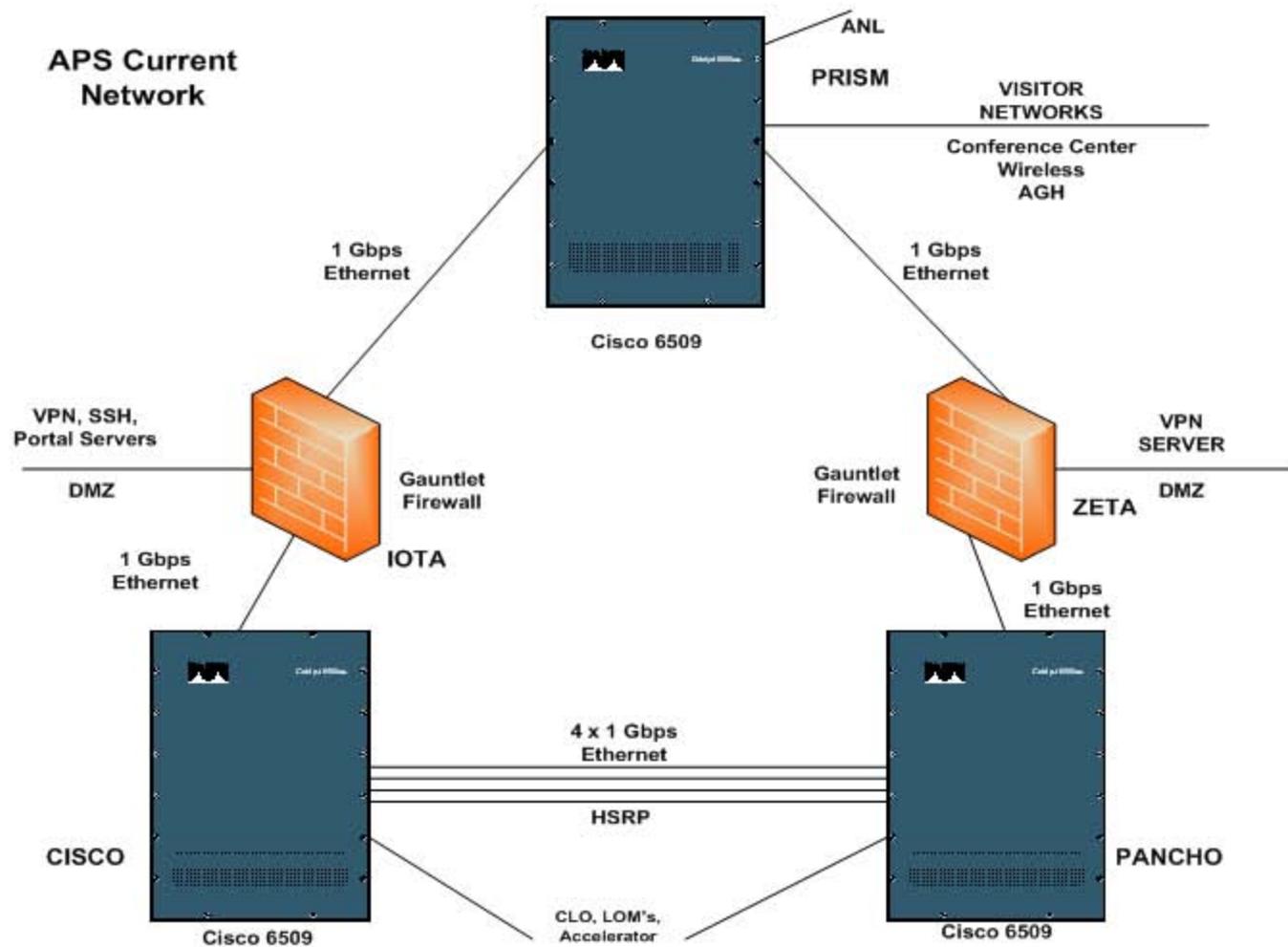
# ***Current Network***

---

- **ACL-Based Firewall Installed on Prism July 1998**
- **Gauntlet Firewall Installed August 2000**
- **Gauntlet Firewall Performance - 200 Mbps throughput**
- **Cyber Patrol, Spam Assassin, McAfee Anti-Virus**
- **Solaris 2.8 Hardened**
- **Number of Gigabit Ethernet Interfaces is 3**
- **Stateful Inspection and Proxy Rules**



# APS Current Network



# ***New Network Configuration***

---

- **Secure Computing G2 Model 4150 Firewalls**
- **Active/Active High Availability Configuration with Cluster Management via Enterprise Management Appliance**
- **Sidewinder G2 Performance - 1.8 Gbps throughput X 2**
- **Smart Filter Provides Web Content Filtering and Web Caching**
- **Cloudmark Anti-Spam and McAfee Anti-Virus**
- **Protects Against Web and Email Viruses and Spyware**



## ***New Network Configuration (continued)***

---

- **Integrated IDS with Real-Time Alerts and Automatic Strikeback Response for DOS Attacks, Drops the Attack Source IP into a Virtual “Black Hole”**
- **Existing Gauntlet Rules are Imported into Sidewinder G2’s**
- **Stateful Inspections and Proxy Rules**
- **Maximum Number of Gigabit Ethernet Interfaces is 20**
- **Unix-Based Secure Operating System**
- **New Firewall Service Module (PIX in a Blade) Installed in Prism**
- **Cisco IDS Module Installed in Prism**



# APS Upgraded Network

