

REMOTE ACCESS TO THE APS

APS-IT
November 30, 2012

Presenting:

D. Cyl
T. Lutes
B. Robinson
M. Westbrook

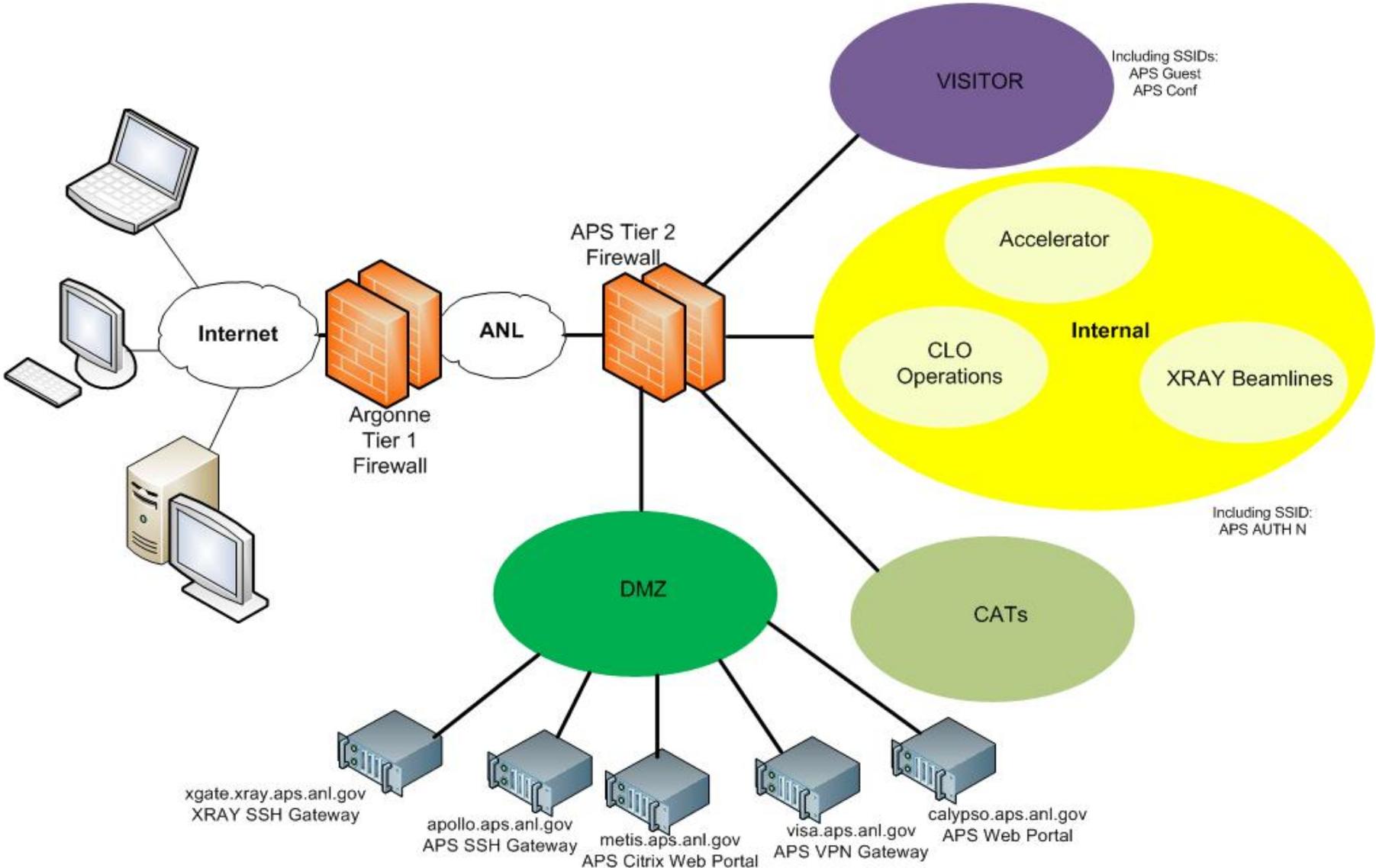
Outline

- Remote Access Options and Fundamentals
 - **APS Web Portal**
 - **Zimbra Web Client**
 - **APS VPN**
 - **WebVPN Portal**
 - **Cisco AnyConnect VPN Client**
 - **OpenConnect VPN Client (Linux)**
 - **Crypto Cards**
 - **APS SSH**
 - **APS Citrix Web Portal**
- **Demonstrations**

Why Remote Access?

- Work from home
- Access internal resources while on travel
- Keep an experiment or project moving forward
- Perform system administration
- MAC and Linux CrashPlan PROe Backups
- Offer remote assistance to users
- Access beamline data for visualization and analysis
- Monitor and control beamline
- Control data acquisition
- View network cameras not open to Internet
- Monitor, troubleshoot and ‘tweak’ the accelerator
- All of above from iPhone/iPad/iPod or Android
- Endless possibilities

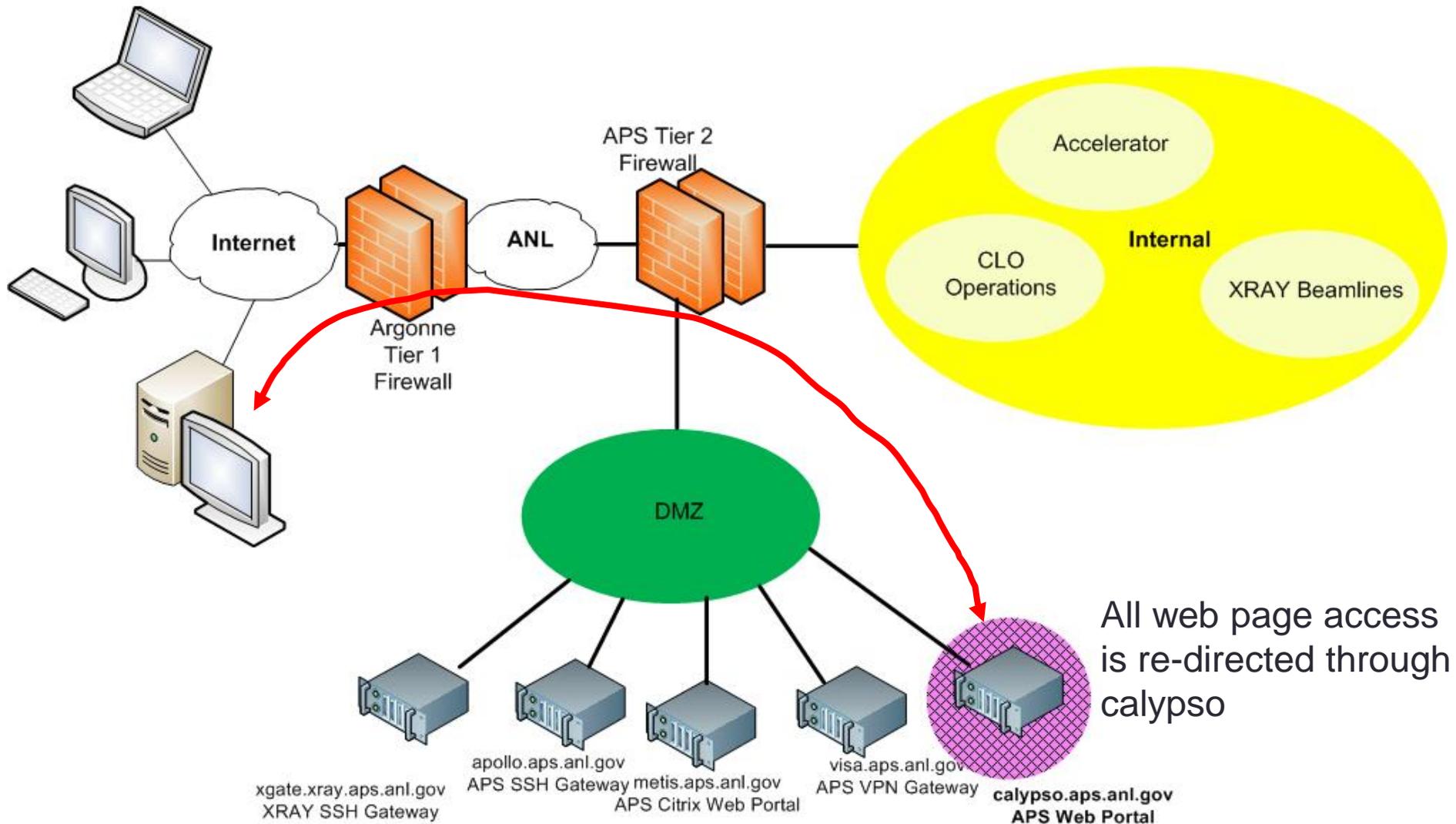
APS Tier 2 Firewall Network Zones



APS Web Portal



APS Web Portal



APS Web Portal Access

- In web browser go to APS Web Portal:
 - <https://calypso.aps.anl.gov>
- Login with APS (Unix) account and password
- User's must request APS Portal access
 - Submit a support request at: <http://www.aps.anl.gov/hd>
- First-time configuration:
 - "User Information", click on the pencil-icon (Settings)
 - Set TZ CST[Central Standard Time] (America/Chicago)
- Access to MCR Logbook
- **APS-IT is currently evaluating web portal technologies and planning an upgrade**

APS Web Portal

APS Portal System (Login) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

APS Portal System (Login)

anl.gov https://calypso.aps.anl.gov/http/

Most Visited Getting Started Latest Headlines IT Absence Calendar

Argonne NATIONAL LABORATORY

Advanced Photon Source

A U.S. Department of Energy, Office of Basic Energy Sciences national synchrotron x-ray research facility

This server uses your APS Unix/LDAP password for Authentication

User Name:

APS Unix/LDAP Password:

Log In

Security Notice

This web site is part of a Federal computer system used to accomplish Federal functions. The Department of Energy monitors this web site for security purposes to ensure it remains available to all

Privacy Notice

We collect no personal information about you when you visit a DOE Web site unless otherwise stated and unless you choose to provide this

APS Portal System - Mozilla Firefox

File Edit View History Bookmarks Tools Help

APS Portal System

anl.gov https://calypso.aps.anl.gov/http://telesto.aps.anl.gov/portal/dt

Most Visited Getting Started Latest Headlines My calendar

Argonne NATIONAL LABORATORY

Advanced Photon Source

A U.S. Department of Energy, Office of Science, Office of Basic Energy Sciences national synchrotron x-ray research facility

[Home](#) | [Logout](#)

User Information

Welcome!

default

Last Update: November 28, 2012 11:58 AM

479 minutes left

120 minutes max idle time

Notes

Nov 28, 2012 11:51:23 AM

Admin

The APS Portal is intended for easy access to simple APS web pages. To access ICMS and ANL applications, use other remote access mechanisms.

Bookmarks

Enter URL Below:

[APS home page](#)

[ANL home page](#)

[APS Logbook](#)

[Home](#) | [Help](#) | [Log Out](#)

MCR Logbook

MCR Operations Group - Mozilla Firefox

File Edit View History Bookmarks Tools Help

APS Portal System MCR Operations Group

anl.gov https://calypso.aps.anl.gov/http://www.aps.anl.gov/Accelerator_Sys

Most Visited Getting Started Latest Headlines My calendar

Search Ops pages Search

**APS Accelerator Systems Division
Operations & Analysis Group**

Listing of Statistics for Run3-2012
(Created Wed Nov 28 12:05:39 CST 2012)

Percentage of Scheduled Time **98.66 %**
Mean Time Between Faults (MTBF) **83.56 Hours**

Info Ops Specific Links Ops Most Used Tools Qualification APS P
Schedules & Logbooks Statistics & Reports Local Operational Aids Call In Lists
Links

APS Storage Ring Status 12:21:00

Storage Ring Current : 102.1 mA **TopUp in Progress**
Operating Mode : **Delivered Beam** Global Feedback : **ON** Local Steering : **OFF**
Message from Operations: Beamlines Operating : **55**

Operator in Charge : Sutton, Grodecki
Floor Coordinator : MCR (2-0101)
Fill Pattern : 0+24x1~-1.1%Coupling/Cogging
Problem Info :
Dump/Trip Reason :
Next Fill In fo : Top-Up is ongoing

MCR Operations Group - Mozilla Firefox

File Edit View History Bookmarks Tools Help

APS Portal System MCR Operations Group

anl.gov https://calypso.aps.anl.gov/http://www.aps.anl.gov/Accelerator_Sys

Most Visited Getting Started Latest Headlines My calendar

Percentage of Scheduled Time **98.66 %**
Mean Time Between Faults (MTBF) **83.56 Hours**

Info Ops Specific Links Ops Most Used Tools Qualification APS Procedures
Schedules & Logbooks Statistics & Reports Local Operational Aids Call In Lists APS Homepage &
Links

APS Storage Ring Status 12:21:00

Storage Ring Current : 102.1 mA **TopUp in Progress**
Operating Mode : **Delivered Beam** Global Feedback : **ON** Local Steering : **OFF**
Message from Operations: Beamlines Operating : **55**

Operator in Charge : Sutton, Grodecki
Floor Coordinator : MCR (2-0101)
Fill Pattern : 0+24x1~-1.1%Coupling/Cogging
Problem Info :
Dump/Trip Reason :
Next Fill In fo : Top-Up is ongoing

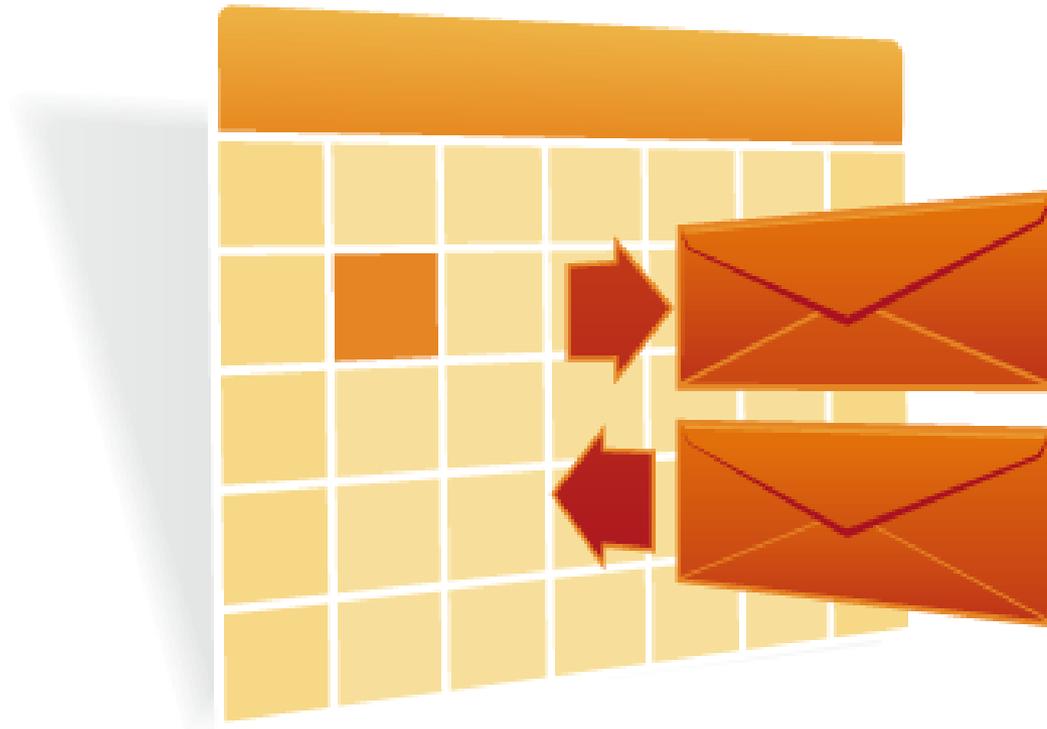
Current in mA

Time of Day (in hours)

■ - Beam Available for User Operations ■ - Beam Not Available

flood@aps.anl.gov (Randy Flood)

Email and Calendar



APS Zimbra Email & Calendar

- Use Zimbra Web Client for access to email and calendar from anywhere (Recommended)
- Open Web browser, go to:
 - <https://zimbra.anl.gov>
- No need to use:
 - VPN
 - SSH
 - WebVPN
 - APS Citrix Web Portal
 - APS Web Portal

Argonne
NATIONAL LABORATORY

Collaboration Suite

Username:

Password:

Remember me on this computer

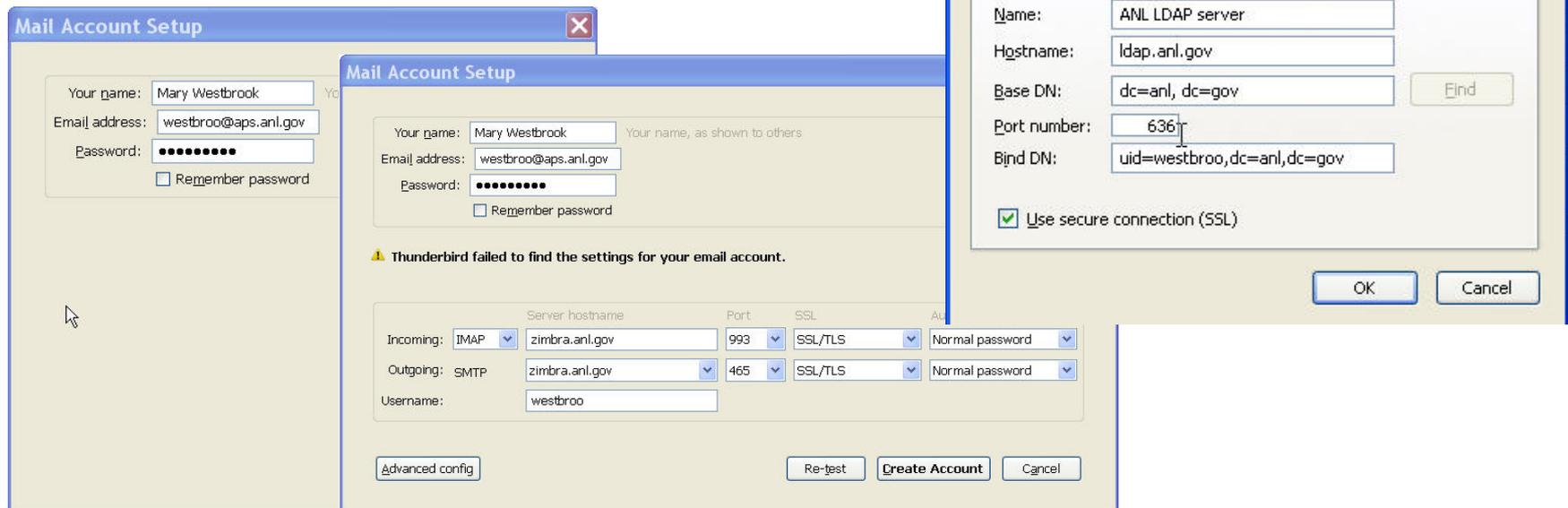
Which version would you like to use? [What's This?](#)

[Zimbra](#) :: the leader in open source messaging and collaboration :: [Blog](#) - [Wiki](#) - [Forums](#)

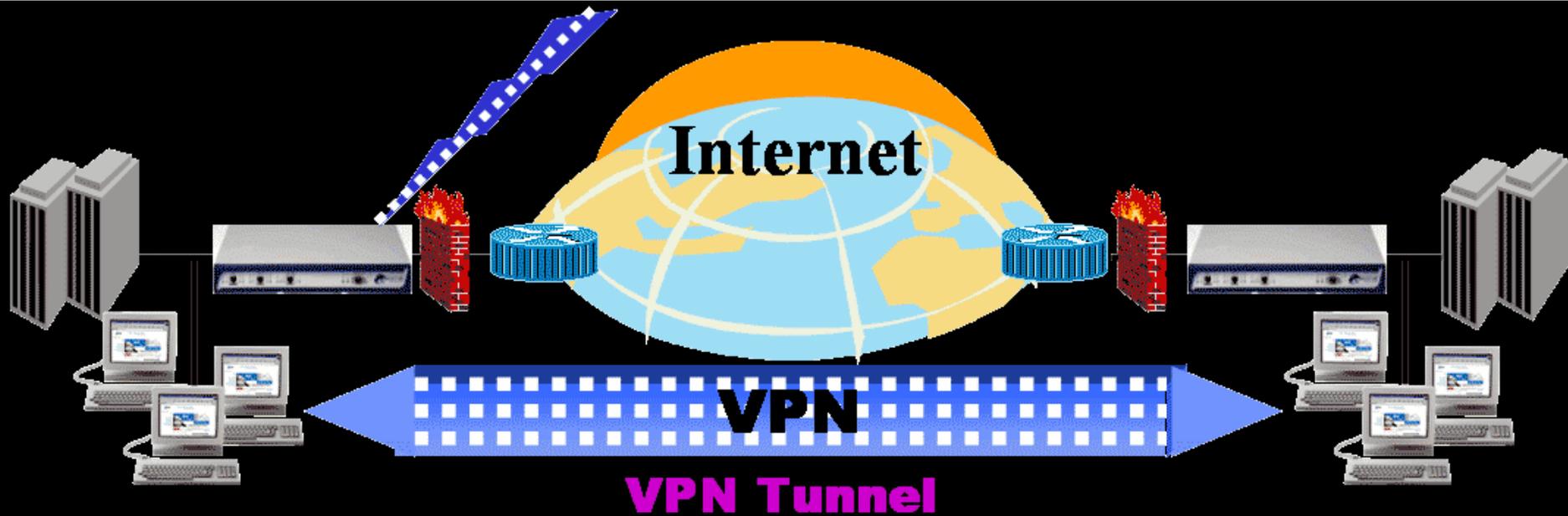
Copyright © 2005-2012 Zimbra, Inc. 'Zimbra' and the Zimbra logos are trademarks of Zimbra, Inc.

APS Zimbra Email

- Can use a mail client, like Mozilla Thunderbird, to access your Zimbra mail remotely
- Use same settings for internal access:
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/Email/Thunderbird/TB_zimbra.pdf
- Be sure to configure ANL LDAP Server



Virtual Private Network

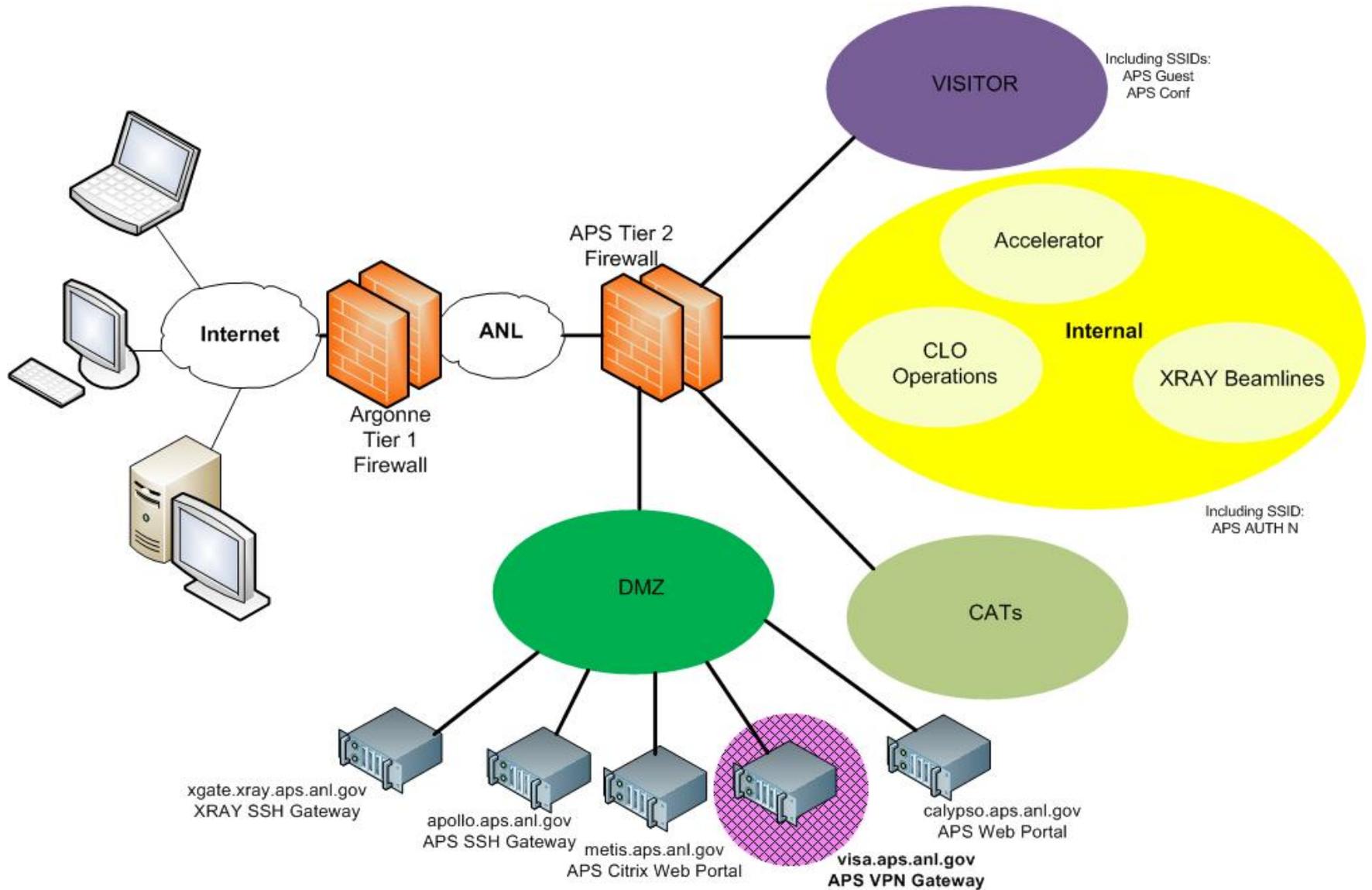


Remote Access

Virtual Private Network

- VPN extends the APS network to remote locations
 - Requires internet connection (cable modem, DSL, wireless)
 - Provides client an internal APS IP address
- VPN provides secure access to internal resources from home or on travel
 - Requires authentication
 - Uses SSL encryption for security
- VPN options at the APS:
 - WebVPN
 - Cisco Anyconnect Secure Mobility Client
 - MAC OS and Windows (32-bit and 64-bit supported)
 - iPhone/iPad/iPod (select models)
 - Android (select Samsung models)
 - OpenConnect client for Linux

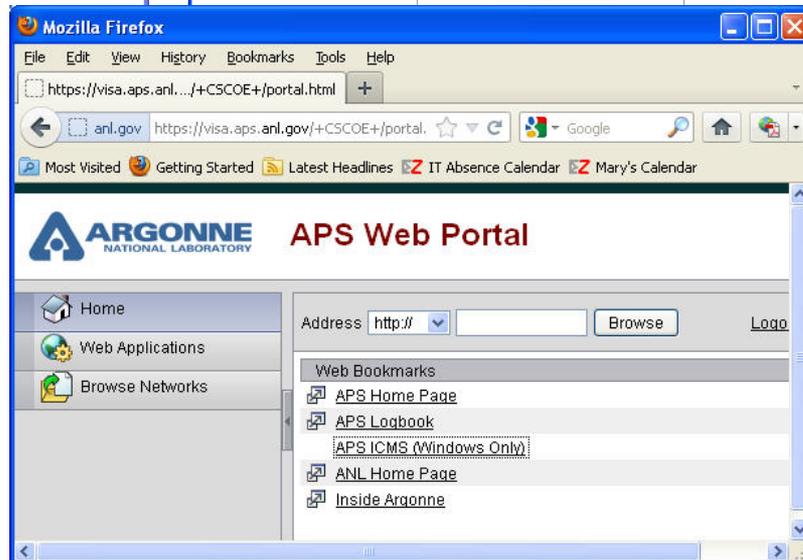
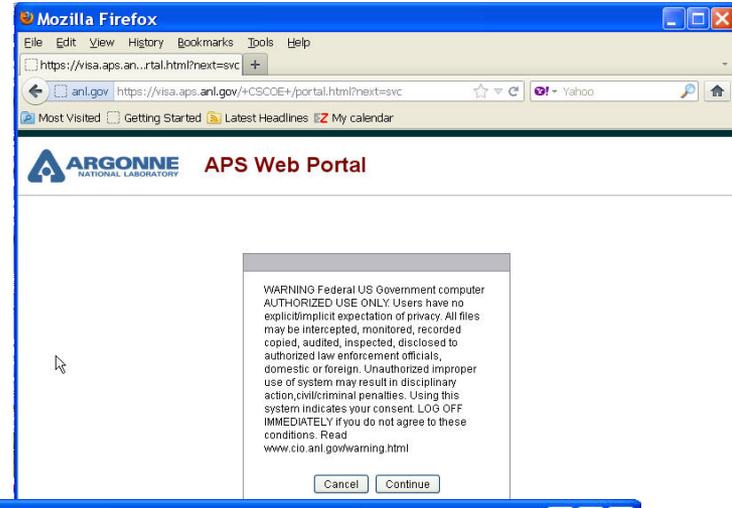
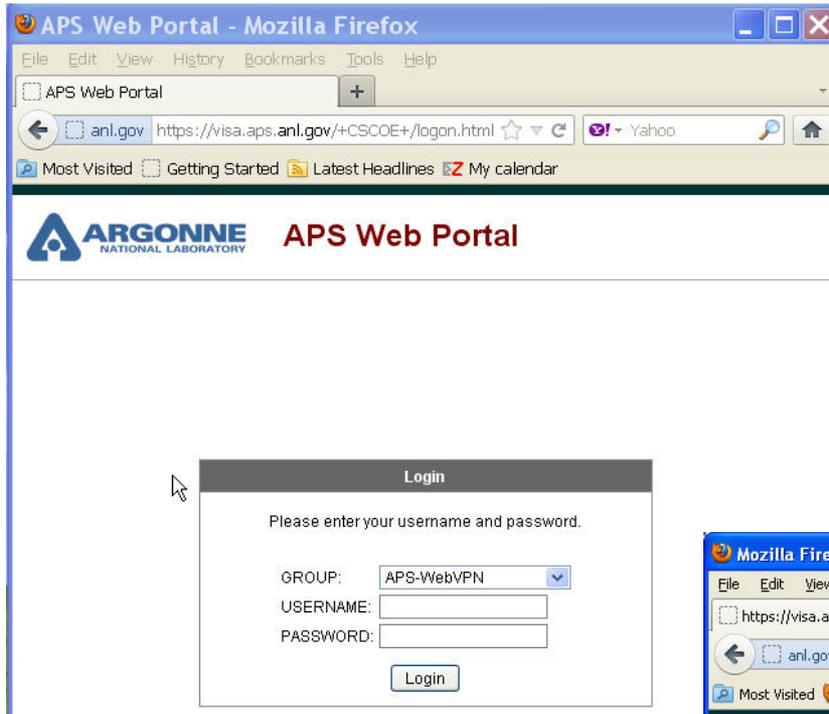
APS VPN Access



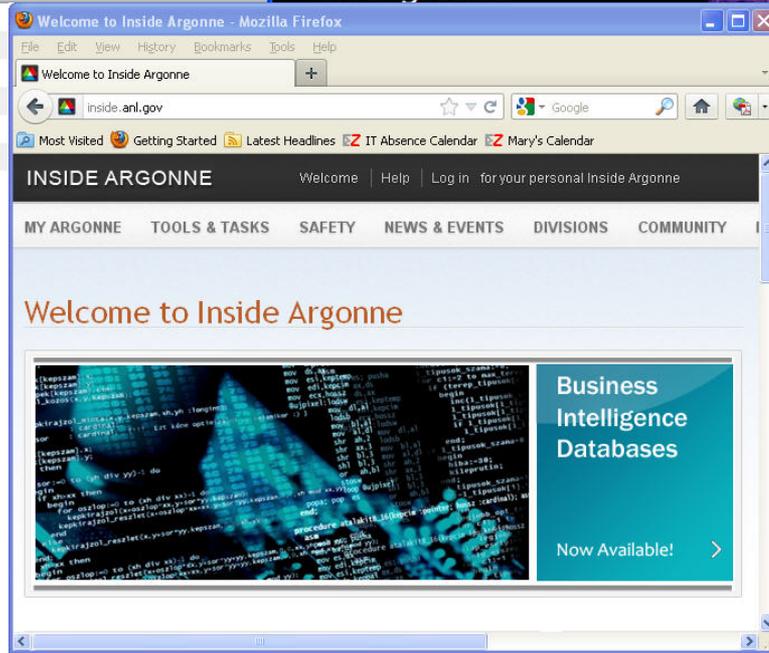
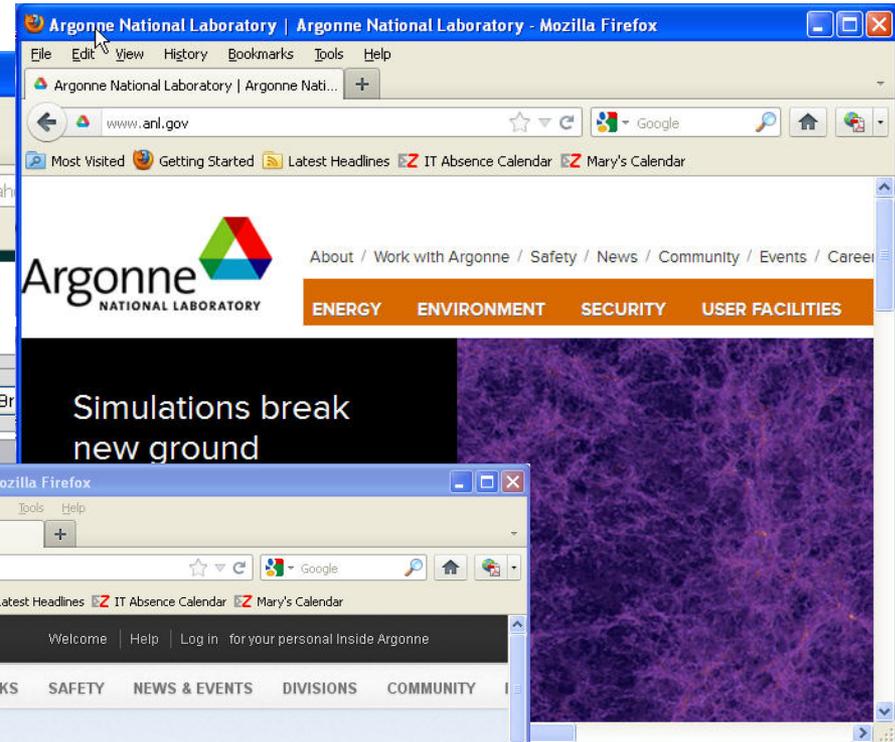
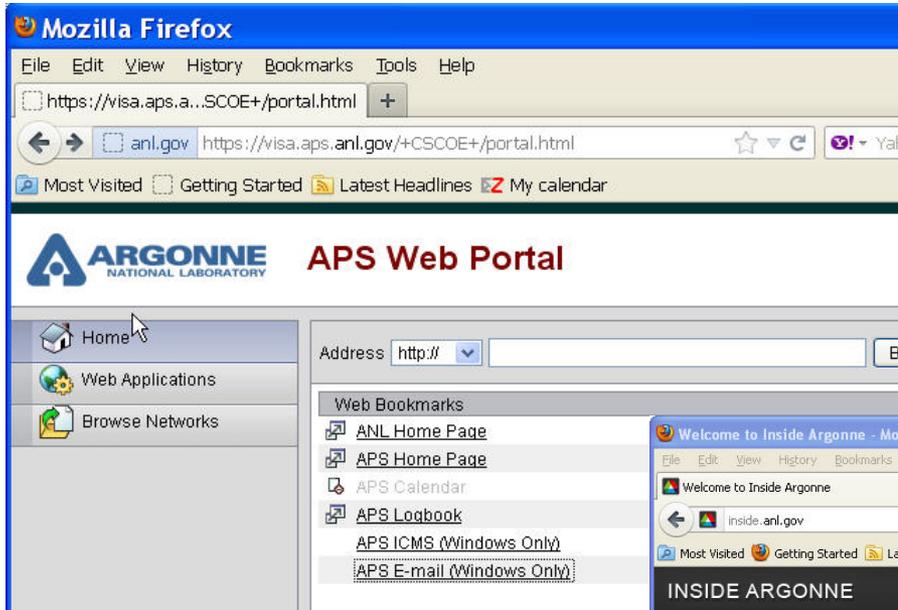
APS WebVPN

- APS offers “clientless” VPN access using WebVPN
- From anywhere, users can open a browser and connect to:
 - <https://visa.aps.anl.gov>
 - Select grout: APS –WebVPN
 - Login using your **APS credentials**
 - Does not require CryptoCard token authentication
- Have access to:
 - ANL home page and Intranet (Inside Argonne)
 - Administrative Apps: AMOS, KRONOS, PARIS, XINK, Argonne’s File Transfer Utility
 - APS home page and Intranet
 - ICMS, web browse (APS-IT Services and Support Request System), and others
 - MCR Logbook
- Supported platforms:
 - Windows
 - Mac OS
 - Linux
- Users must request WebVPN access
 - Submit a support request at: <http://www.aps.anl.gov/hd>

APS WebVPN



ANL Web Site and Inside Argonne



APS Web Sites

- APS Home page
- APS Intranet
- Beam Time Access System (GUP)
 - https://beam.aps.anl.gov/pls/apsweb/gup0005.start_page
- User Facilities Remote Training
 - http://www.aps.anl.gov/Safety_and_Training/Training/employees.html

[ml](http://www.aps.anl.gov/Safety_and_Training/Training/employees.html)

The screenshot shows the 'Type of Beam Time Request - Main Menu' page. It features the Argonne National Laboratory logo and a navigation menu. The main content area displays a welcome message: 'Welcome to the APS Beam Time Access System. Please select an action.' Below this, there are two primary buttons: 'Create a New Proposal' and 'Existing Proposals'. Under 'Create a New Proposal', there are sub-buttons for 'General Users' and 'Partner Users'. Under 'Existing Proposals', there is a 'Find Proposal:' section with a text input field for 'Proposal #' and a 'Submit Query' button. The URL in the browser address bar is https://beam.aps.anl.gov/pls/apsweb/req0002.validate_user.

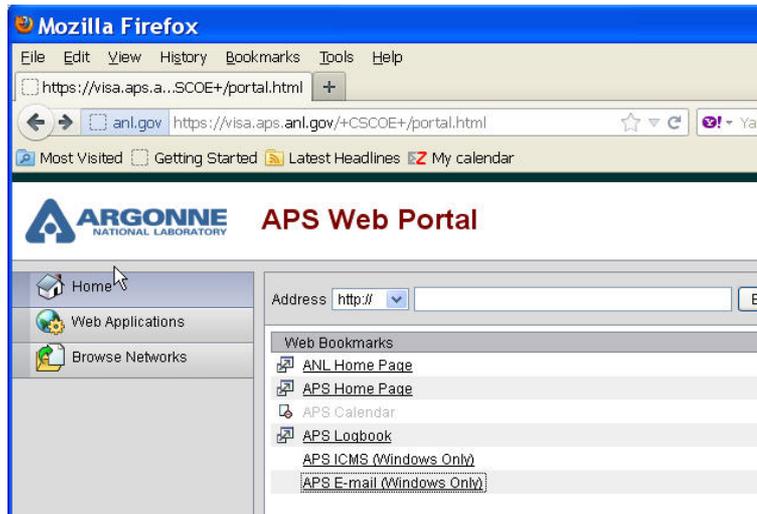
The screenshot shows the 'User Facility Courses for Argonne Employees' page. It features the Argonne National Laboratory logo and a navigation menu. The main content area displays a welcome message: 'Welcome to the APS Beam Time Access System. Please select an action.' Below this, there are two primary buttons: 'Create a New Proposal' and 'Existing Proposals'. Under 'Create a New Proposal', there are sub-buttons for 'General Users' and 'Partner Users'. Under 'Existing Proposals', there is a 'Find Proposal:' section with a text input field for 'Proposal #' and a 'Submit Query' button. The URL in the browser address bar is http://www.aps.anl.gov/Safety_and_Training/Training/employees.html.

Course	Name
APS 101	Advanced Photon Source User Orientation (2 year retraining)
ESH 100	Argonne National Laboratory User Facility Orientation (one time)
ESH 223	Cybersecurity Annual Education and Awareness (1 year retrain)
ESH 377	Electrical Safety Awareness Training (3 year retraining)
ESH 738	OERT General Employee Radiation Training (2 year retraining)

Course	Name
CNM 101	Center for Nanoscale Materials User Orientation (2 year retrain)
ESH 100	Argonne National Laboratory User Facility Orientation (one time)

MCR Logbook

Accessible from APS WebVPN



MCR Operations Group - Mozilla Firefox

File Edit View History Bookmarks Tools Help

MCR Operations Group

anl.gov https://visa.aps.anl.gov/+CSCO+00756767633A2F2F6A6A6A2E6E63F Yahoo

Most Visited Getting Started Latest Headlines My calendar

Search Ops pages Search

**APS Accelerator Systems Division
Operations & Analysis Group**

Listing of Statistics for Run3-2012
(Created Wed Nov 21 12:05:33 CST 2012)

Percentage of Scheduled Time **98.42 %**
Mean Time Between Faults (MTBF) **81.12 Hours**

Info Ops Specific Links Ops Most Used Tools Qualification APS Procedures

Schedules & Logbooks Statistics & Reports Local Operational Aids Call In Lists APS Homepage & Links

APS Storage Ring Status 12:57:00

Storage Ring Current : **101.9 mA** **TopUp in Progress**

Operating Mode : **Delivered Beam** Global Feedback : **ON** Local Steering : **OFF**

Message from Operations: Beamlines Operating : **58**

Operator in Charge : LaBuda, Weyer
Floor Coordinator : Patti Pederghana (2-0101)
Fill Pattern : 0+24x1
Problem Info :
Dump/Trip Reason : 11/21/12 10:02, SR Kicker PS.
Next Fill Info : Top-up ongoing.

Current in mA

Cisco AnyConnect Secure Mobility VPN Client



Cisco AnyConnect Secure Mobility VPN Client

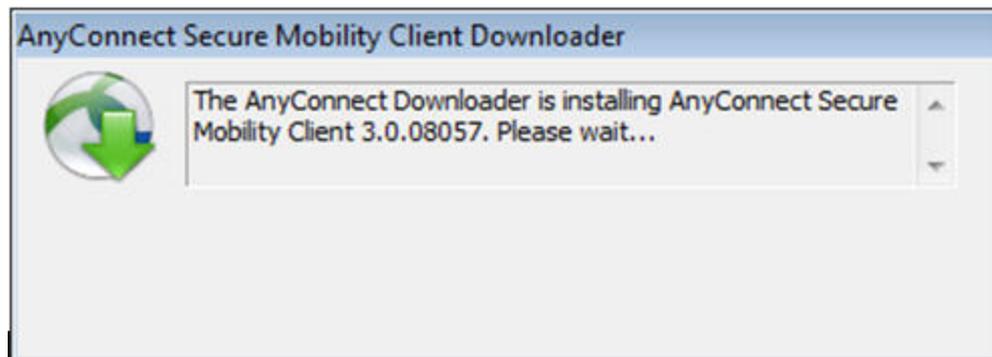
- Cisco provides a VPN client compatible with Cisco VPN Servers
 - Cisco AnyConnect Secure Mobility VPN Client
- VPN client downloads for all Cisco-supported platforms:
 - 32-bit and 64-bit support
 - Windows
 - MAC OS
 - Linux (not used at APS)
 - iPhone/iPad/iPod (select models)
 - Android (select Samsung)
- Downloads only available from APS networks:
 - APS Staff (all non-CAT users)
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/RemoteAccess/VPN/
 - CATs
 - <http://cat.aps.anl.gov/vpn.html>
- Install Cisco AnyConnect VPN Client

Cisco IPsec VPN Client Support Discontinued

- Cisco is phasing out support for the Cisco IPSec VPN client
- See Cisco Notice “End-of-Life Cisco IPsec VPN Client”:
 - http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5743/ps5699/ps2308/end_of_life_c51-680819.html
- All users are directed to switch to the Cisco AnyConnect client **NOW**
- APS support for Cisco IPsec client will terminate on 1/7/2013
- All IPsec VPN users have been contacted since 8/2012

Cisco AnyConnect Secure Mobility VPN Client Advantages

- **AnyConnect client as compared with original Cisco IPsec client**
 - More reliable and faster than older Cisco IPsec VPN client
 - Uses SSL: Easier to get through remote firewalls
 - No need for a “shared secret”
 - Outdated AnyConnect Client are updated automatically
 - Following an upgrade of the VPN Servers
 - Be sure to allow the upgrade to finish without interruption
 - If not, Cisco AnyConnect client may need to be reinstalled



CAT Users

VPN Authentication

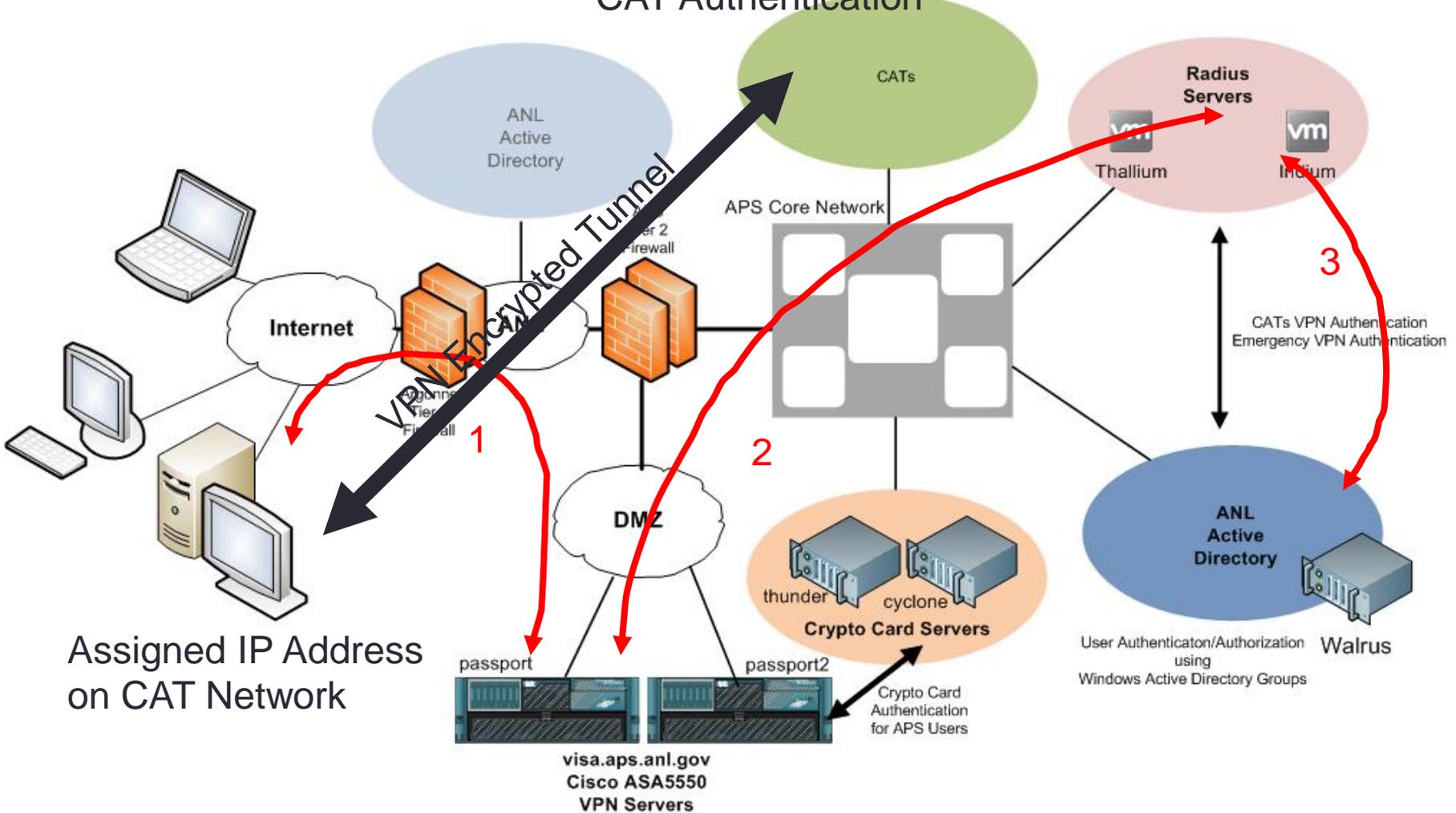
- Cisco AnyConnect client settings to use for remote access to CAT network:

- Connect : visa.aps.anl.gov
- Group: Select-appropriate-CAT-group
 - CARS: carscat-vpn
 - DND: dndcat-vpn
 - HP: hpcat-vpn
 - IMCA: imccat-vpn
 - LS: lscat-vpn
 - MR: mrcat-vpn
 - NE: necat-vpn
 - SBC: sbccat-vpn
 - SER: sercat-vpn
- Username: ANLusername
- Password: ANLpassword



- CAT users are assigned IP address on their CAT network
- CAT remote access is limited to CAT network
- CAT remote access users have no access to APS or XRAY beamlines
- CAT users need to request VPN access
- VPN access is monitored per account and removed for no activity
- (1 year, Lab Policy)

APS Virtual Private Network Remote Access CAT Authentication



Assigned IP Address
on CAT Network

APS Staff

VPN Authentication

- For APS staff, APS VPN access is protected by CryptoCard authentication
- CryptoCard authentication is used for “edge” (VPN client) authentication only
 - After that use your normal credentials to access other internal APS machines and resources
- APS users must request VPN access
- VPN access is monitored per account and removed for no activity (1 year, Lab Policy)

CryptoCard™ Technology



Why CryptoCard™ Technology for APS?

- Compromise occurred at the APS on June 3, 2009
 - Compromise achieved with a stolen password
 - 5 beamline systems were compromised before “break-in” was detected
- Outcome
 - APS Cyber Security Program Representative (CSPR) filed a report to DOE Cyber Security
 - Argonne Cyber Security Office advised APS to use 2-factor authentication technology to prevent this type of incident in the future
 - In their words, “...to protect the *Crown Jewels* of Argonne...”
 - Argonne Cyber Security Office contributed 50% of the cost of implementing the CryptoCard token technology
- Same technology used in HPC field, Argonne’s Blue Gene supercomputer (ACLF)
- No compromises since CryptoCard implementation
 - 😊 Lab Cyber and DOE

CryptoCard™ Authentication

Used at DOE Facilities

- APS-IT administrators have used CryptoCard tokens since 2009
- Currently, over 430 CryptoCard token users at the APS
- CryptoCard authentication is also used at other DOE Facilities:
 - Los Alamos
 - Sandia
 - Berkeley
 - Brookhaven
 - Fermi Lab
 - Lawrence Livermore
 - Others
- For more information about this technology, see:
 - <http://www.cryptocard.com/>

CryptoCard™ Tokens

- APS staff and other users use CryptoCard™ tokens for authentication
 - VPN
 - SSH
- CryptoCard token authentication uses “2-factor Authentication”
 - User PIN (something user knows)
 - CryptoCard keycode (something unique that identifies user)
- Account is created for each user on the CryptoCard server
- A token is programmed for each user
- An initial PIN is assigned to each token
 - PIN is changed by user on first-time-use
- In addition, user account needs to be granted permissions for remote access:
 - VPN
 - SSH

CryptoCard™ Token PIN

- Rules for PIN
 - 4 characters (4 numbers, 4 letters: uppercase or lowercase letters, or combination)
 - No special characters allowed in PIN
 - There is a sanity check on the PIN number which will not allow for any sequence greater than 2
 - e.g. 2376 is valid, but 2346 will fail
 - e.g. abc5 will fail, but abd5 will be valid
- If an incorrect PIN is used when authenticating, the user is immediately prompted for the password again
- Following a cyber security “best practice”, no feedback is provided regarding the nature of the failure

CryptoCard™ Token Keycode

- CryptoCard uses a “connectionless” model for authentication
- Token and CryptoCard Server are synchronized upon token initialization
 - i.e. Server and token generate the same keycode for same user at specific time
- When user attempts VPN connection with keycode:
 - User presses token button to generate an 8 character keycode
 - User enters keycode as part of password provided in the VPN client
 - Keycode is then presented to CryptoCard Server
 - User’s keycode will be compared with the Server’s keycode
 - Authentication is granted on a match

CryptoCard™ Token Keycode

- Press token button generates an 8 character keycode
 - Valid for 1 minute
- Press button again within the first minute
 - Keycode will remain valid (active on the display) for an additional minute
 - After the minute the key will shut off and a subsequent button press will generate a new keycode
 - After the minute the key will shut off and a subsequent button press will generate a new keycode
- If user mis-reads or mis-types the keycode when authenticating, the user is immediately prompted for the password again
- Following a cyber security “best practice”, no feedback is provided regarding the nature of the failure

CryptoCard™ Token

Potential Token Issues

- CryptoCard tokens may need replacement
 - Batteries can fail over time
 - Display grows dim, hard to read
 - In the event of loss
- CryptoCard tokens may need to be re-programmed
 - Can fall “out-of-sync”
- CryptoCard token PIN may need to be re-initialized
 - For example, user forgets PIN
- CryptoCard token becomes “disabled” after 7 unsuccessful login attempts
 - Token will need to re-enable the device
- CryptoCard token becomes “locked” after 15 unacknowledged keycodes
 - A unacknowledged keycode is one in which the user did not attempt to login and keycode was left to time-out
 - Crypto card token display shows “LOCKED”
 - Crypto card token will need to be re-initialized and a new PIN assigned

CryptoCard™ Token Help

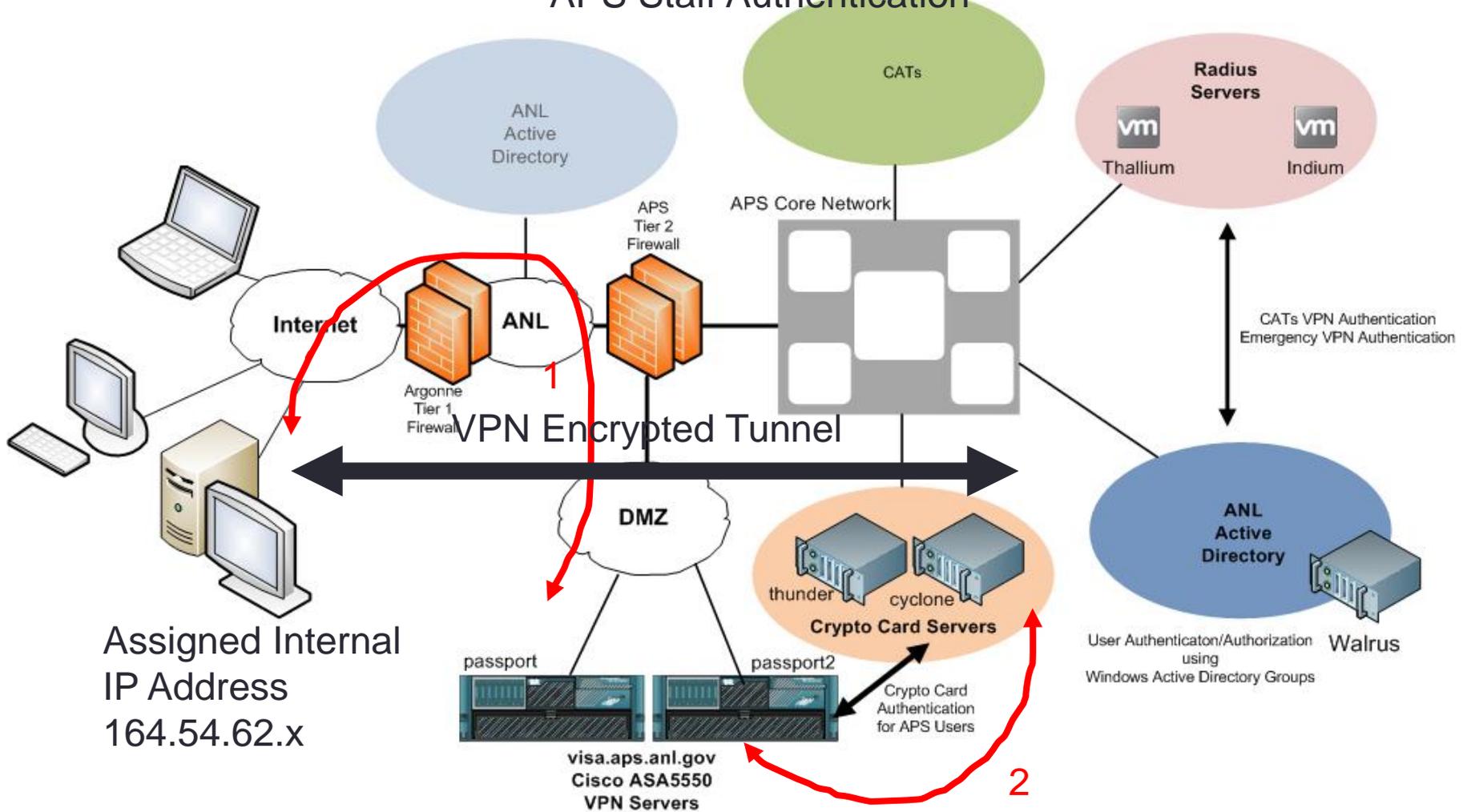
- Contact APS-IT regarding any CryptoCard token issues
 - Submit a support request at: <http://www.aps.anl.gov/hd>
 - Call APS-IT Emergency Line 2-9700
 - Primary APS-IT CryptoCard contacts: Dave Cyl, Joe Hermans and Mary Westbrook
 - After hours:
 - Beamline users call Floor Coordinator on-duty, 2-0101
 - All other users contact the MCR 2-9424
- I'm on travel, but forgot my crypto card at home, or lost it, but I need to access my data at the APS, what can I do?
 - Contact APS-IT, we can provide SSH/VPN permissions without CryptoCard token use temporarily until you return
- APS-IT can perform troubleshooting remotely:
 - Reset PIN
 - Re-enable token remotely
 - Provide emergency/temporary SSH/VPN permissions without token
- For all other problems, APS-IT will need access to the CryptoCard token
- Please return CryptoCard token to APS-IT
 - Upon leaving APS
 - No longer needed for remote access
 - Tokens cost \$65 each
 - Tokens can be recycled to new users
 - Tokens are disabled when user leaves APS

APS Staff VPN CryptoCard™ Token Authentication

- Cisco AnyConnect client settings to use when authenticating with CryptoCard token:
 - Connect : visa.aps.anl.gov
 - Group: VPN-Secure
 - Username: ANLusername
 - Password: PIN + CryptoCard-keycode



APS Virtual Private Network Remote Access APS Staff Authentication



Assigned Internal
IP Address
164.54.62.x

Secure Your Home PC

- APS-IT recommends VPN from LAB-owned computers
- If using a personal computer:
 - VPN is NOT recommended
 - APS Citrix Web Portal is recommended
- Be sure to secure your personal computer
- Under no circumstances, should user VPN in as admin
- APS-IT can setup Linksys routers securely for user

ESH223A - Mozilla Firefox

Zimbra: Search results

www.eshtesting.anl.gov/courses/session/StartCourse.php

Remote and Home Computing

Could your home computer be a back door? Absolutely!

Argonne incidents are often the result of infected home computers. Many employees use their home computers for work related to the Laboratory or to connect remotely to Argonne's systems using technology like VPN (Virtual Private Network). You can use the strategies listed below to protect your home computer as well as Argonne's computing systems.

To protect the Laboratory while computing remotely:

- **Install virus protection and spam filters.**
- **Maintain your home computer monthly.** Visit this website to obtain a guideline for your home security: <http://tom-cat.com/security.html>
- **Install a home firewall.** Use either:
 - Antivirus software for personal use is available from your internet service provider for little to no cost. There are also Argonne Cyber Security vetted [free alternatives for antivirus software](#).
 - **A hardware firewall such as a Linksys router** behind your cable modem or DSL service.

Implement home wireless networks with caution! Verify your home wireless access point is in a secure configuration. Malicious users exploit open wireless access points to give an extra layer of anonymity by making it look like their attack came from your home!

Visit the Cyber Security [web page](#) to obtain a copy of the Cyber Security for Your Home Machine guide.

Back 22 of 28 Next

VPN Client Recommendations

- Linux
 - OpenConnect Client (built-in RHEL)
- MAC OS
 - Cisco AnyConnect Secure Mobility Client
- Windows
 - Cisco AnyConnect Secure Mobility Client
- Android OS
 - Cisco AnyConnect Secure Mobility Client
- iPhone OS
 - Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect Secure Mobility Client iPhone and Android

- iPhone/iPad/iPod
 - Cisco AnyConnect Secure Mobility client available for select Apple iPhone/iPad/iPod devices
 - Client download from “App Store”
 - Client install:
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/RemoteAccess/VPN/CiscoAnyConnectiPhoneiPad2.5.5130.pdf
- Android
 - Cisco Anyconnect Secure Mobility client available for select Samsung Android models only
 - Client download from “Android Market”
 - Client install:
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/RemoteAccess/VPN/AnyConnectAndroid.pdf
- Error message and failure to install
 - Results when attempting install on an unsupported device

Cisco AnyConnect Secure Mobility Client iPhone and Android

- Cisco AnyConnect Secure Mobility client connection settings for APS staff:
 - Connect : visa.aps.anl.gov
 - Group: VPN-Secure
 - Username: ANLusername
 - Password: PIN + CryptoCard-keycode
- Cisco AnyConnect Secure Mobility client connection settings for CATs:
 - Connect : visa.aps.anl.gov
 - Group: VPN-Secure (or CAT group)
 - Username: ANLusername
 - Password: ANLpassword

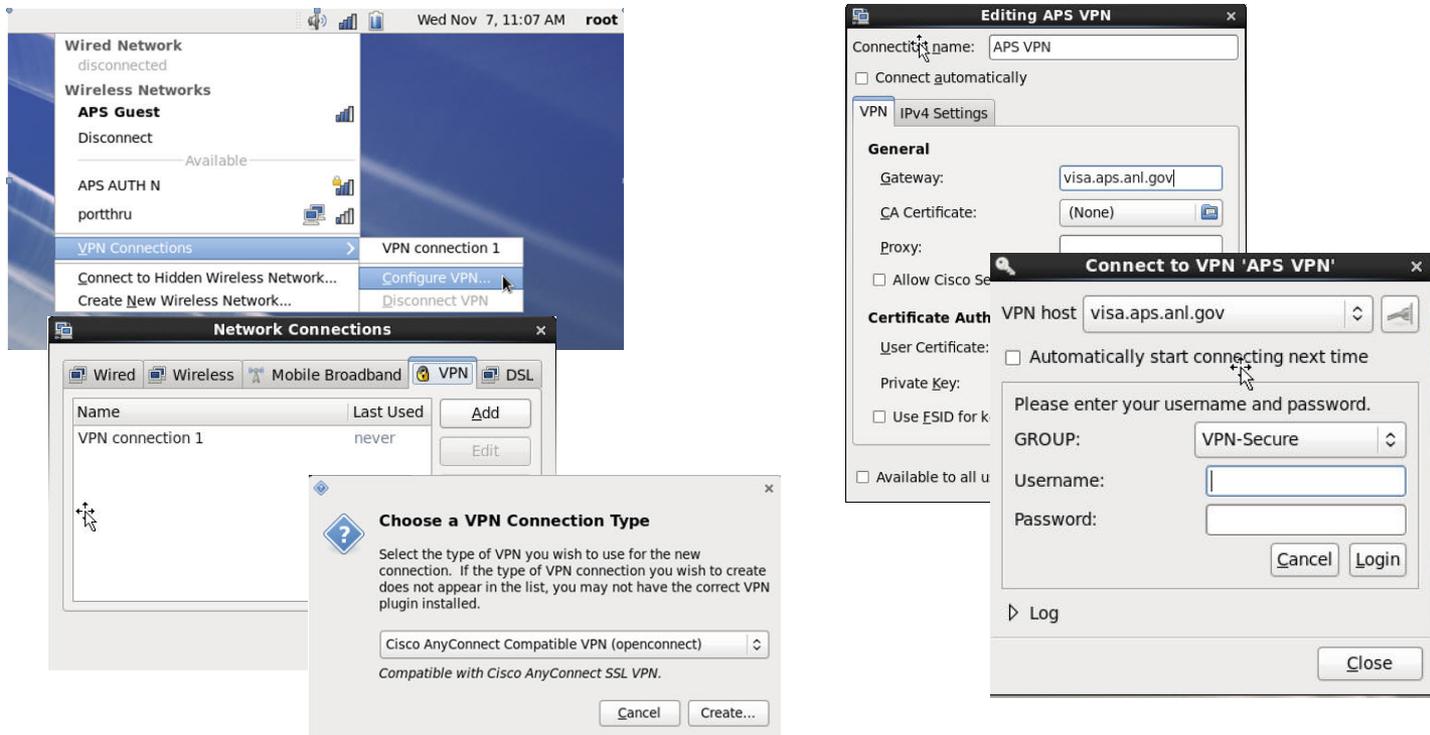
APS VPN Considerations

- When using VPN client to connect to the APS network,
 - All internet traffic is routed through APS network, including your non-APS traffic
 - All traffic is subject to DOE Cyber Security Policies
 - SSL encryption impacts network speeds
- Disconnect VPN connection when you are done accessing APS internal resources
 - Launch Cisco AnyConnect client and select “Disconnect”
 - Your connection will be faster without the extra routing and encryption overhead
- When using VPN client:
 - Assigned an internal APS IP address
 - VPN does not allow split tunneling for security reasons
 - All network traffic is through VPN tunnel
 - Lose access to network resources (printers) on local network
 - Will not affect your access to a locally connected printer (USB)
- With Windows 7, can have multiple users logged into system, with only 1 active and switch between active user
 - Cannot VPN in, if more than 1 user is logged into your system (Cisco)



OpenConnect Client (Linux)

- OpenConnect VPN client is built-in RHEL
- Others can download OpenConnect from:
 - <http://www.infradead.org/openconnect/>



SSH

SSH

SSH

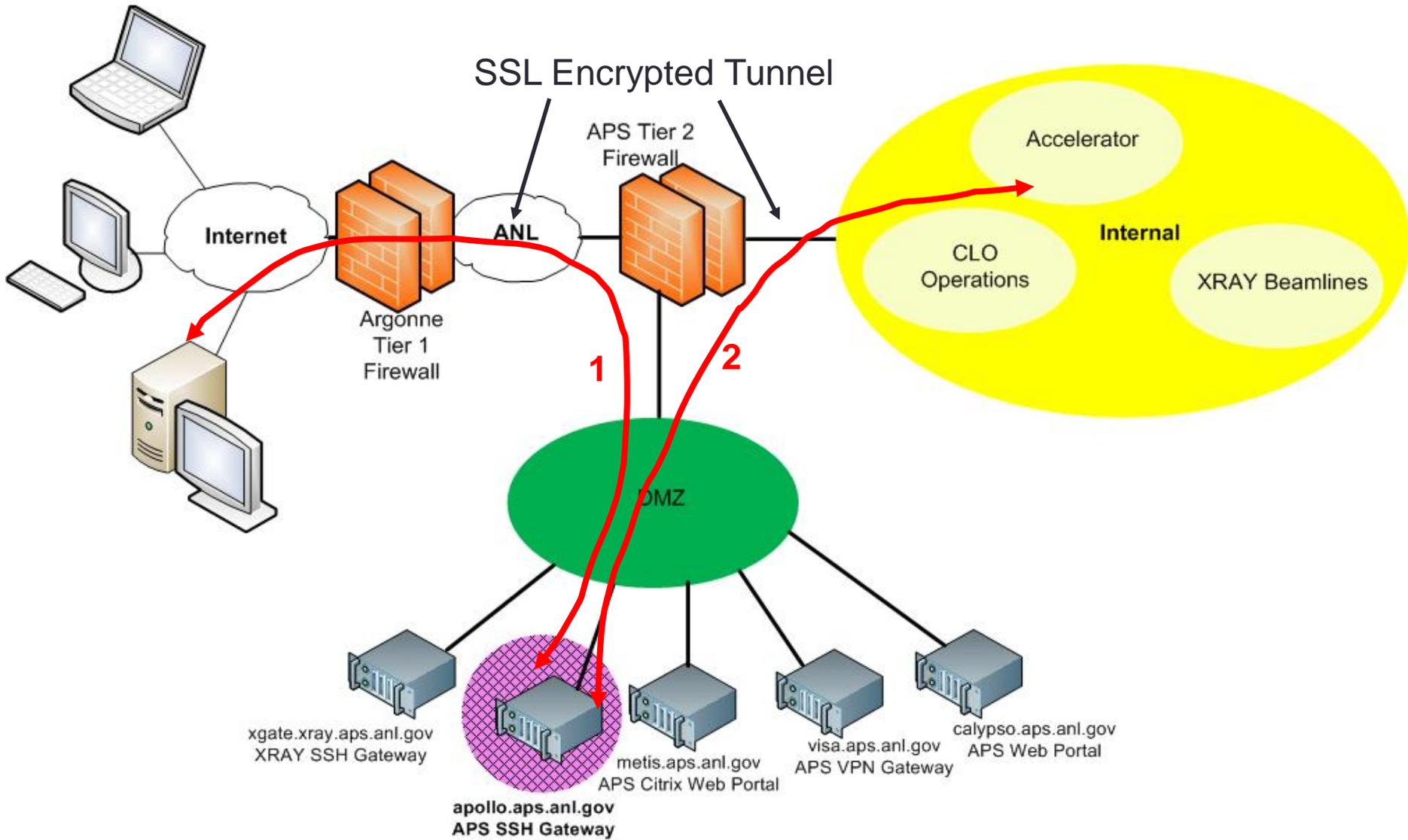
SSH

SSH Access to the APS

APS Staff

- Users must request permissions to SSH into APS network
- CryptoCard token is programmed for user
- User connects using SSH to APS SSH Gateway
- From SSH Gateway, user can connect to internal resources
- APS users use command “ssh apollo” or using FQDN “ssh apollo.aps.anl.gov”
 - Login with username: “APS username”
 - Password: PIN+CryptoCard-keycode
- From apollo, user can SSH into other internal Lab systems
- Apollo use is monitored per account and removed for no activity
- Apollo is a Linux system

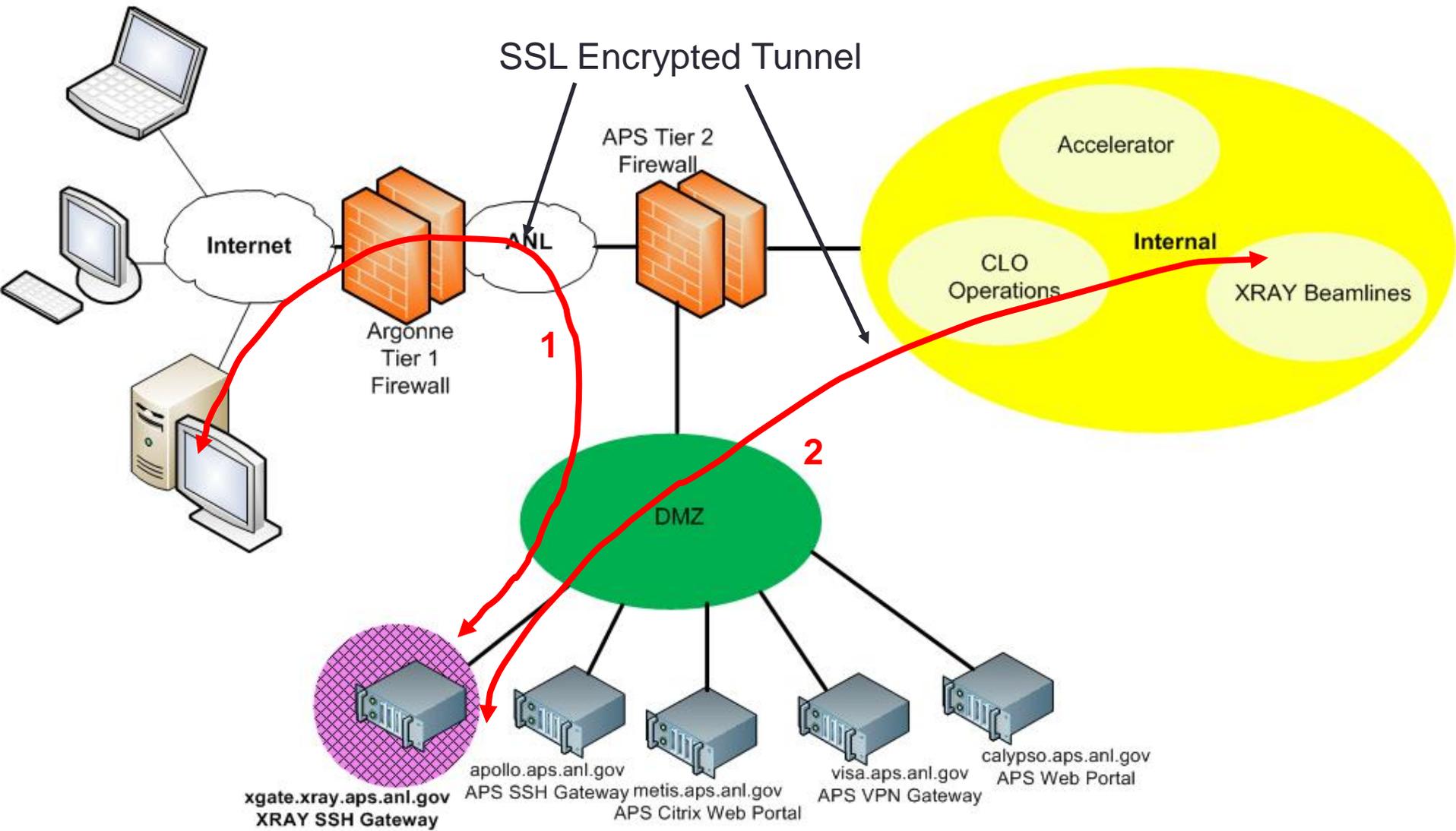
APS SSH Access



SSH Access to the APS Beamline Users

- Users must request permissions to SSH into APS beamline network
- CryptoCard token is programmed for user
- User connects using SSH to XRAY SSH Gateway
- From XRAY SSH Gateway, user can connect to internal beamline resources
- Beamline users use command “ssh xgate” or using FQDN “ssh xgate.xray.aps.anl.gov”
 - Login with username: “XRAY Unix username”
 - Password: PIN+CryptoCard-keycode

XRAY SSH Access



Supported SSH Clients

- Linux
 - Built-in OpenSSH
- MAC OS
 - Built-in SSH binary (ssh command)
- Windows
 - Putty
 - Tectia SSH Client
 - Exceed xterm

SSH Access to APS

CAT Users

- CAT users check with your local IT staff for appropriate SSH server to connect to and credentials required

Tunnel X11 through SSH Windows

- Users can tunnel X11 (NX) through Putty
- See:
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/RemoteAccess/NXPuttyWindows.pdf

Tunnel NX and VNC through SSH Linux

- Users can tunnel NX and VNC through SSH
 - ssh to apollo
 - NX with ssh tunnel through apollo
 - VNC with ssh tunnel through apollo
- See:
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/RemoteAccess/aps_1262111_NX.pdf

Where to Obtain Remote Access Help?

- APS-IT is a team of over 20 IT professionals ready and willing to help
- Submit a support request at:
 - <http://www.aps.anl.gov/hd>
- Call APS-IT Emergency Line: 2-9700 during business hours
- After hours assistance:
 - Beamline users contact Floor Coordinator on-duty
 - All other users contact MCR 2-9424
- Contact APS-IT Staff directly:
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/staff/
- APS-IT Services web documentation:
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/

Thanks

- Thanks for your kind attention!
- APS-IT encourages you to explore remote access alternatives
- Please share your remote access experiences!
- Questions?

- **Today's slides will be published at:**
- **APS VPN and SSH**
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/RemoteAccess/RemoteAccessVPN_SSH.pdf
- **APS Citrix Web Portal**
 - http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/RemoteAccess/RemoteAccessCitrixWebPortal.pdf