# New Fermilab VPN System

Dave Coder

Network Services

September 29, 2009

# New Fermilab VPN System

- The Fermilab Virtual Private Networking (VPN) system is used to create a secure connection between a remote (off-site) computer and the Fermilab network.
- When the VPN session is established, your computer has access to network resources as if it were locally connected.
- Users log in to the VPN with their Services Account credentials.

# New Fermilab VPN System

- Services Account
  - A Services account enables you to access a number of important applications at Fermilab with a single username/password. It is based on a centralized authentication database and LDAP, and is separate from a KCA account.
  - Applications now available via the Services account are: Fermilab Service Desk, Fermilab Time and Labor Reporting (FTL), Meeting Maker, and Fermilab Exchange Email.
  - Over time, more and more applications will come under the Services account umbrella, such as the new VPN system.
  - If you do not have a Services account, contact the Service Desk to get set up.

# New Fermilab VPN System

- Authorized Users
  - Anyone with a Services account can access the new VPN system, whether Employees, Contractors, or Visitors.
  - Persons that do not have a Services account cannot use the new VPN system.
  - There are no separate usernames or passwords to remember for the VPN. Password resets for the Services account should be directed to the Service Desk.
  - There is no longer a VPN account request form; if you have a Services account you have VPN access.

# New Fermilab VPN System

## System Features

- Provide off-site user's computers a 131.225.0.0 IP address to function as if they were local to the Fermilab site.
  - Some network resources, applications and web sites are only available to computers with a Fermilab IP address.
- Communication between off-site computers and the VPN appliance is encrypted over the public Internet.
- System is for off-site remote users.
  - Connecting to the VPN from on-site computers will result in limited or no connectivity while the session is active.

# New Fermilab VPN System

- When to use the VPN (some examples):
  - When you need to mount a network drive
  - When accessing Fermi Time and Labor/Effort
  - When accessing MISCOMP
- When not to use the VPN (some examples):
  - When using Email or MeetingMaker via Web interface
  - Using Certificate version of DocDB
  - When using the Service Desk console
- Why not to use the VPN:
  - The VPN will slow you down
  - Session and Idle time outs
  - Web proxy

# New Fermilab VPN System

## System Features

- VPN uses “split tunnel” routing by default to direct traffic intended for Fermilab to Fermilab, routing all other traffic to the client’s ISP.
- VPN “full tunnel” routing option is being researched for access to off-site applications that need to originate from Fermilab.
  - Full tunnel access will be subject to Fermilab network security controls.
  - Full tunnel access to off-site resources will be slower than direct access from client computers directly routing through their ISP.

# New Fermilab VPN System

## User Features

- Remote access is available to everyone with a SERVICES account
  - User authentication uses SERVICES credentials
  - Device authentication is no longer needed
  - Separate VPN account request is no longer needed
  - Separate VPN username and password is no longer needed
- VPN system provides network access only
  - Host or application access may require additional logins or Kerberos authentication
  - VPN client software does not provide security for the client computer such as anti-virus, anti-spam, anti-spyware, or PC firewall.

# New Fermilab VPN System

## Old System

- Server is a single Cisco VPN 3060 appliance.
- Client system software is the Cisco VPN Client.

## New System

- Servers are a pair of Cisco ASA 5540 load-sharing appliances.
- Client system software is the Cisco AnyConnect VPN Client.

## New Client Features

- Windows Vista and Linux 64-bit operating systems.
- IPv6 (under research for future deployment at Fermilab).

# New Fermilab VPN System

Cisco AnyConnect Client Application Features

- Software is available for:
  - Windows: XP, Vista, 7; 32 and 64-bit
  - Linux: 2.4 or 2.6 kernel, 32 and 64-bit (in 32-bit mode)
  - Mac: i386 and PowerPC, Mac OS X 10.4 or later
- Support is through the Service Desk
- Centralized software distribution is being researched
- Only the Cisco AnyConnect VPN client is supported by the Service Desk

# New Fermilab VPN System

## New System Timeline

- Pilot Users and Early Adopters
  - Limited deployment starting October 1, 2009
- General Deployment
  - General deployment starting November 1, 2009

## Old System Timeline

- Old VPN system available into calendar year 2010
  - Lifetime of old system depends on our operational experience with the new system