Tom Barton
UChicago IT Services

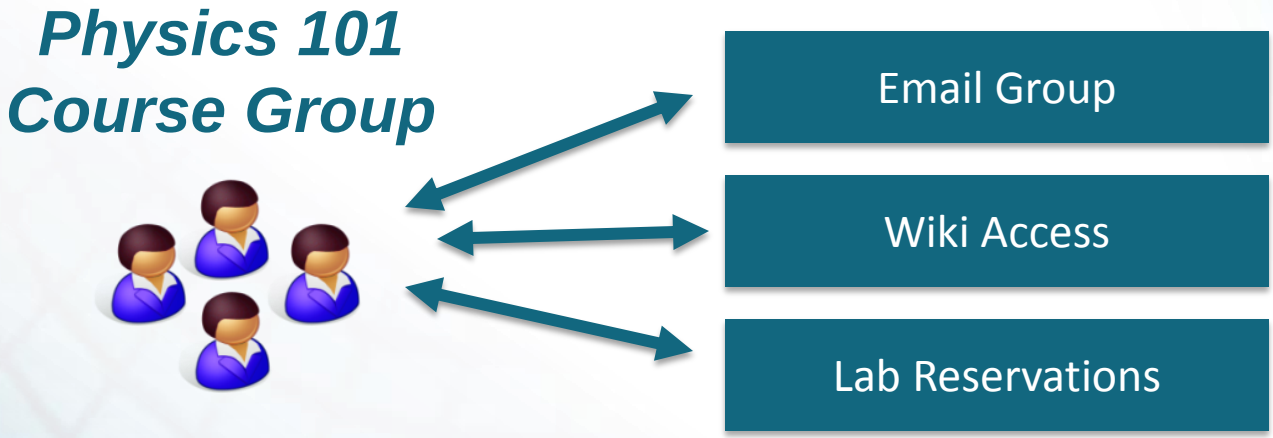
Access Management in the Network @UChicago

Main messages

- An access management service is a Good Thing!
  - Grouper is a great way to support that service
- Identity and Access Management (IAM) has become a critical infrastructure service for supporting research
- Examples of how we use it in UChicago's network

Why have an access management strategy?

- Lower cost and time to deliver a new service.
- Simplify and make consistent by using the same group or role in many places.



Additional benefits of access management

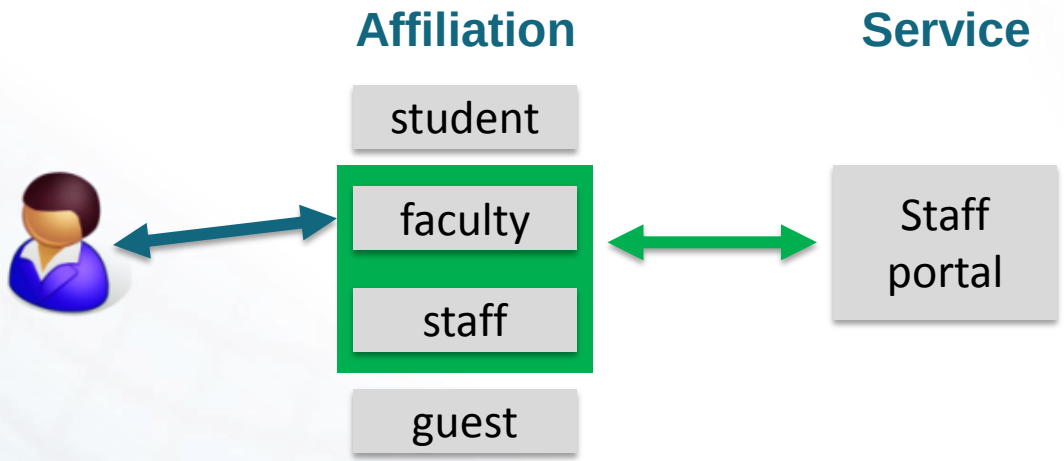
- Delegation to empower the right people to manage access. Take central IT out of the loop.

- Operational transparency. See who can access what, with a report rather than a fire drill.

Access management stages: authorization > authentication

1. Start out using a single user attribute, ***affiliation***, in LDAP or Active Directory.

- This allows simple access policies to be implemented in services.



Access management stages: authorization > authentication

2. Enrich & centralize access management with groups determined from systems of record
   - Courses, financial accounts, departments
   - Define service-specific access policies in the centralized access management system

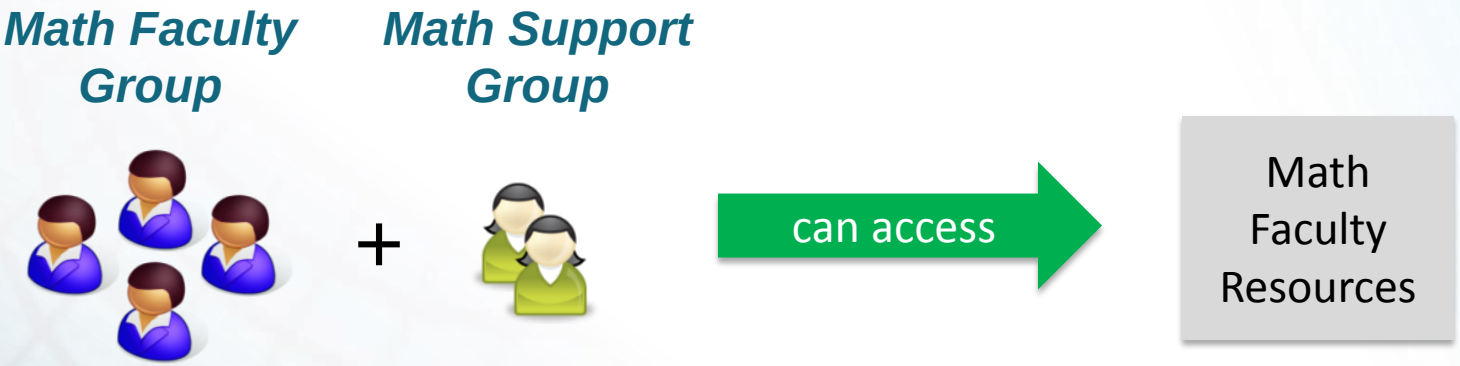
Math Faculty Group

can access

Math Faculty Resources

Access management stages: authorization > authentication

3. Get central IT out of the loop
   - Distributed management
   - Exceptions
   - Departmental applications



Access management stages: authorization > authentication

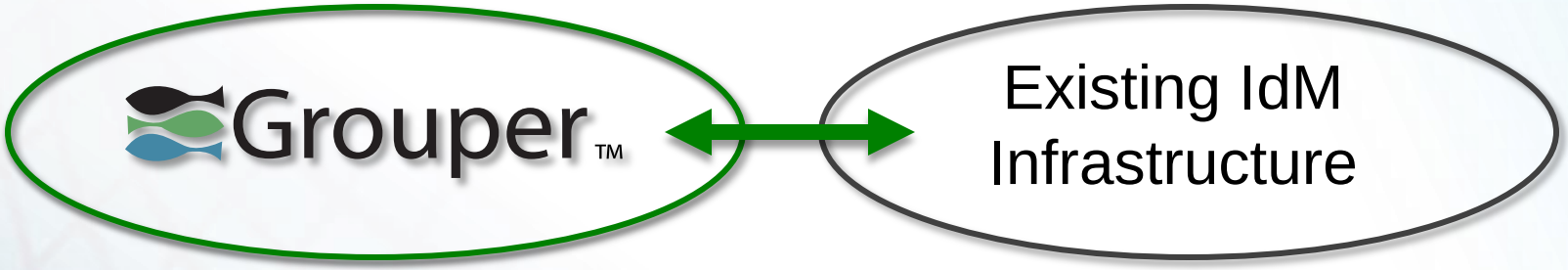
4. Deeper integration of access management
   - Direct integration with applications using web services
     - SOAP/REST/ESB
   - Roles & privileges to support applications more deeply

The Grouper Story

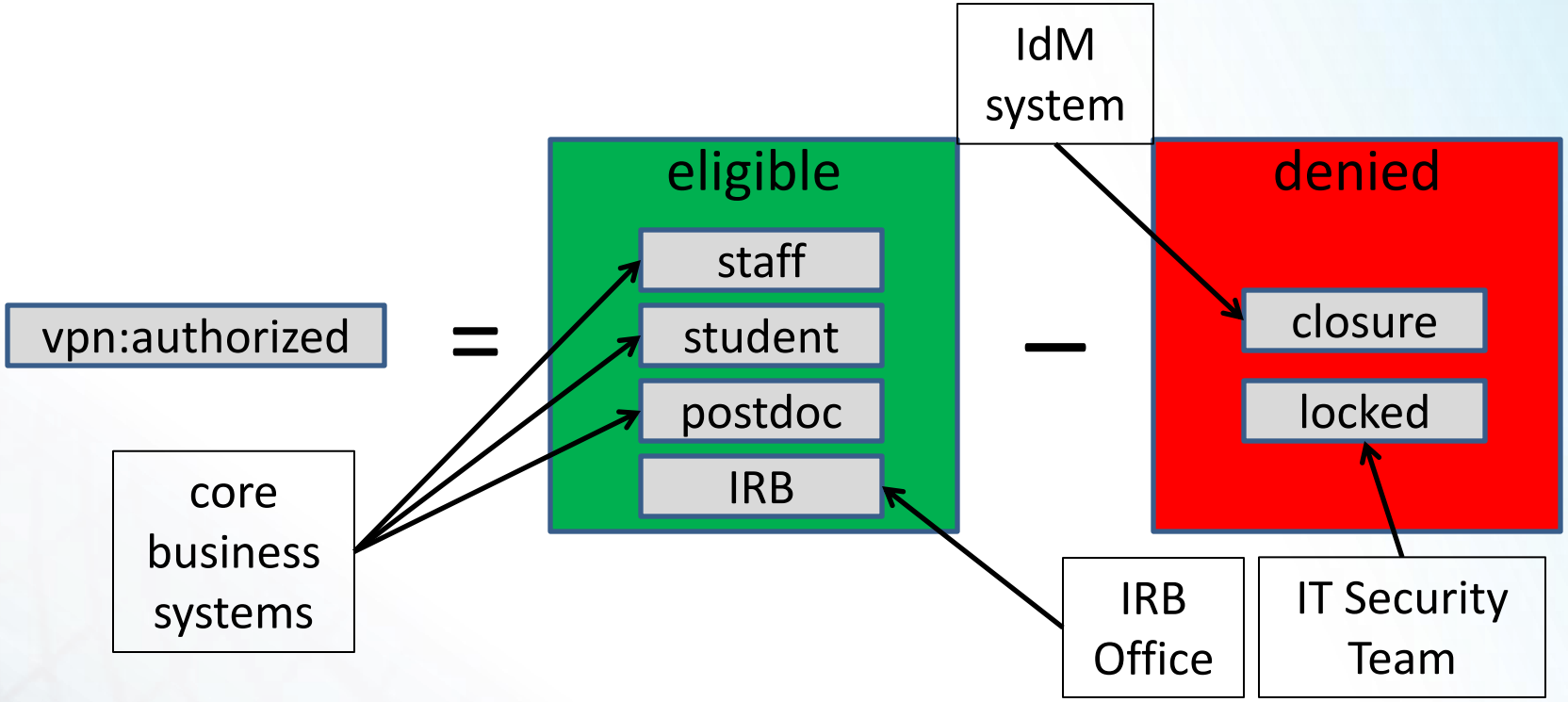
- Open source, community-driven project of the Internet2 Middleware Initiative
  - Initial release v0.5 in December 2004

The Grouper Story

- Key aims
  - Delegation and distributed management
  - Integration with most any existing Identity Management infrastructure



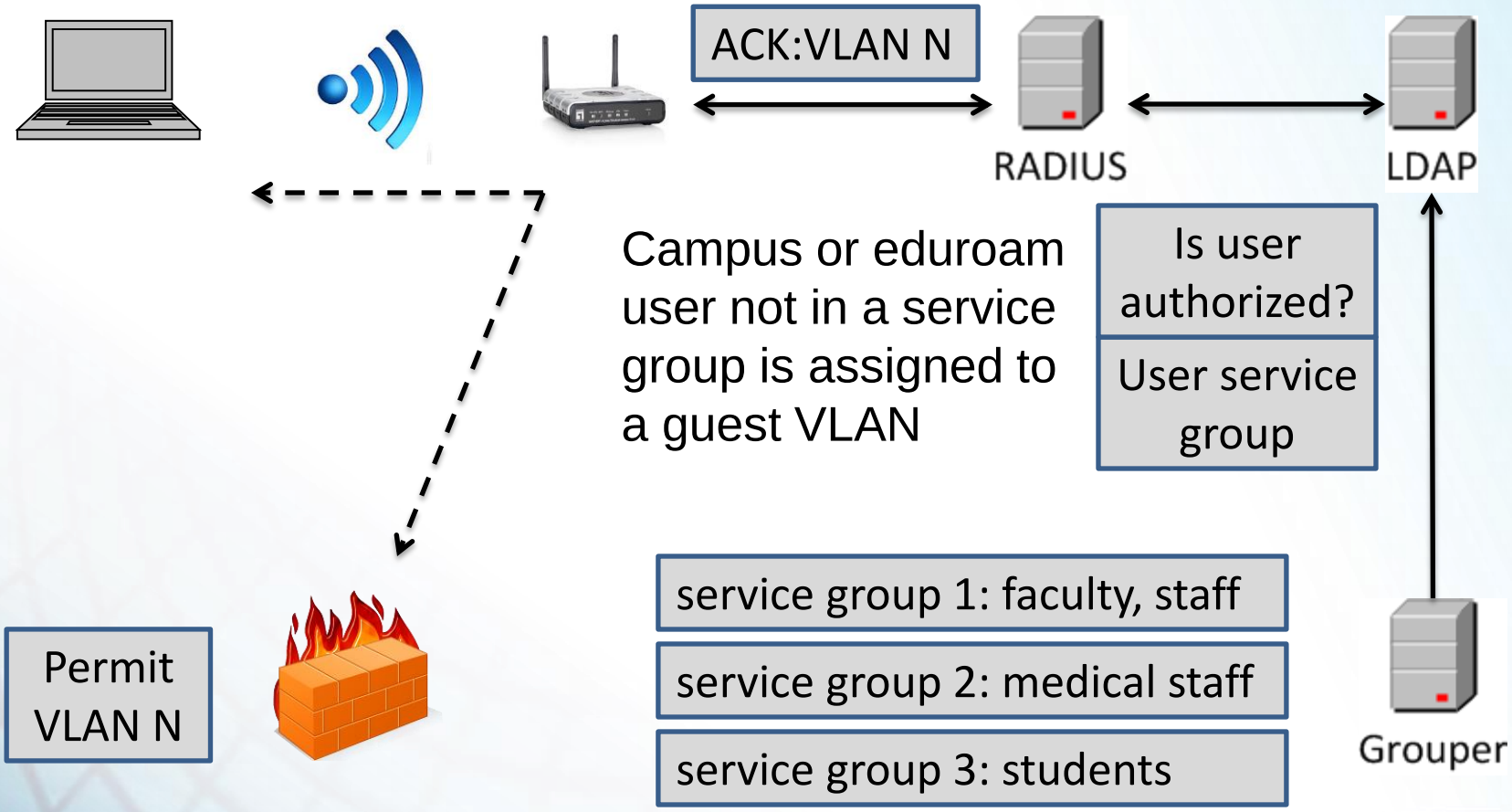
Access management for UChicago VPN



Different groups, different authorities

VPN only uses “vpn:authorized”

802.1X: map user groups to VLANs



IAM aaS for Research Computing Center

- HPC IAM requirements
  - Campus users use campus credentials
  - Federated access, even for gridFTP
  - Accounts for other collaborators
  - Unix group management
  - No central IT involvement in day to day operations

- Central IAM service
  - Delegated admin of collaborator accounts
  - Delegated group management good for OS level and more
  - Integration with CILogon
  - Support for federation at the command line via SAML ECP

Future network-IAM integrations?

- Role-based dynamic firewall rules for user access to service endpoints?
- Role-based policy enforced by SDN?