New network access infrastructure for research and collaborations

Michal Kouril and Michael Wagner

Case Study

- Suppose you have a (web-) site or application that collects data from multiple (external) sites.
- It is hosted inside CCHMC
  - Inside access is direct
  - Employees are also allowed to use VPN to access the internal servers
  - External access is provided through "extranet.cchmc.org"

Case Study

- You typically face one or more of the following (technical) issues:
  - All external users need "extranet" accounts from IS
  - External accounts have relatively long request cycle
  - Account expirations without notification
  - Few disincentives for external collaborators NOT to share usernames and passwords
  - No readily available access audit trails on the network level
    - (needs to be implemented on the application level)
  - No centralized, audited access approval/removal process
  - Hard to find out who has access to what and why
  - If an external user has access to multiple applications, removal from one may well result in removal from all….
  - Timeouts in Extranet…
  - Mandatory extranet menu page, multiple steps
  - Links in emails (internal vs. external)

Expectations

- Increase in number of applications and complexity
- Number of external users increasing
  - UC especially
- Using CCHMC credentials to access other sites
  - NIH, UC, …
- Increased enforcement of regulations
- More complicated access approval workflows

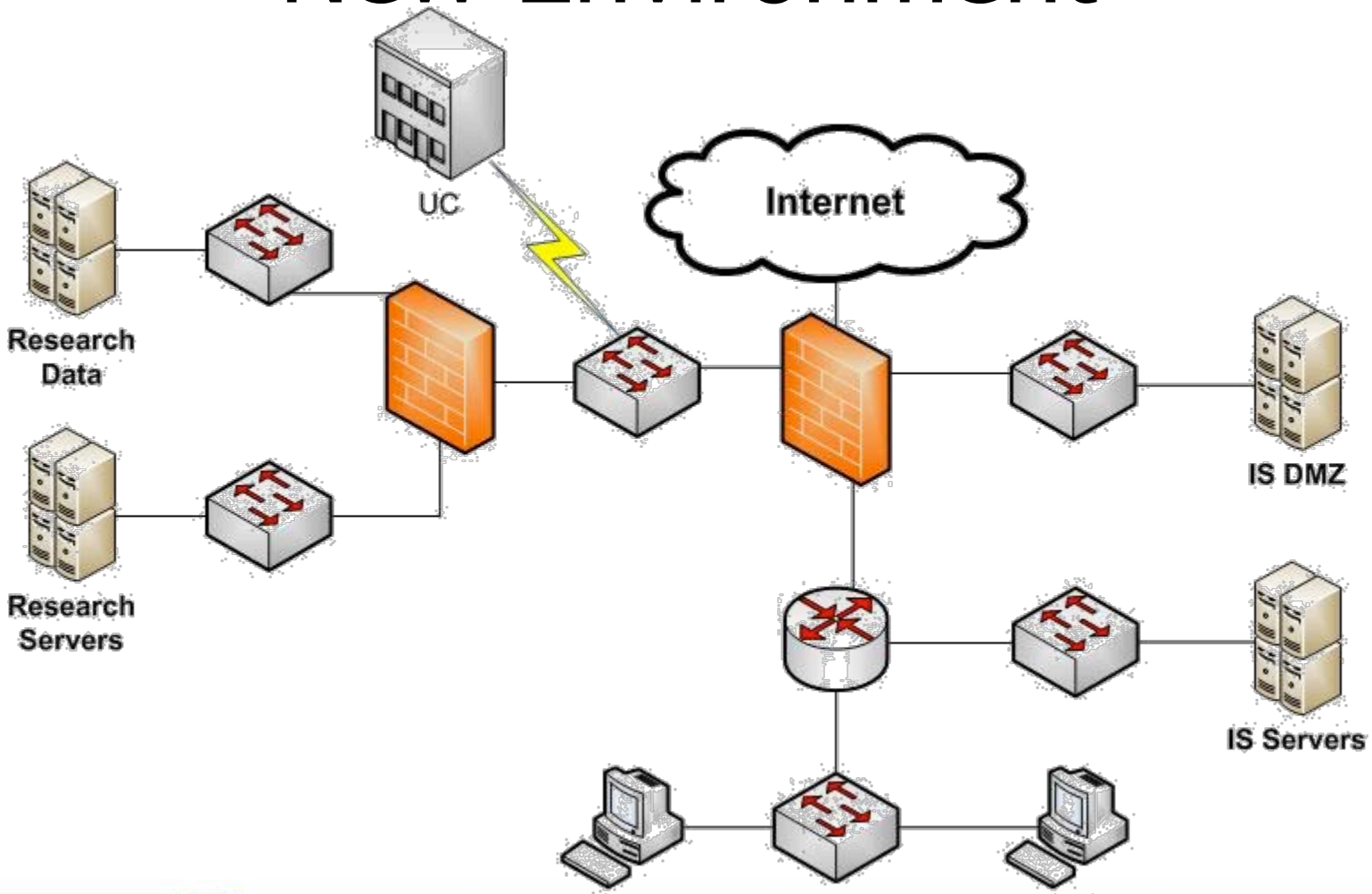
New network access infrastructure

- Ability to handle 1000s of users
- Single access point regardless where you are: same access mechanisms from inside CHMC and outside
- Ability to add/change/remove applications easily
- Ability to identify access levels across the board
- Give the responsible parties (application owners, PI, ORCRA, etc.) one place and ability to validate access lists on demand

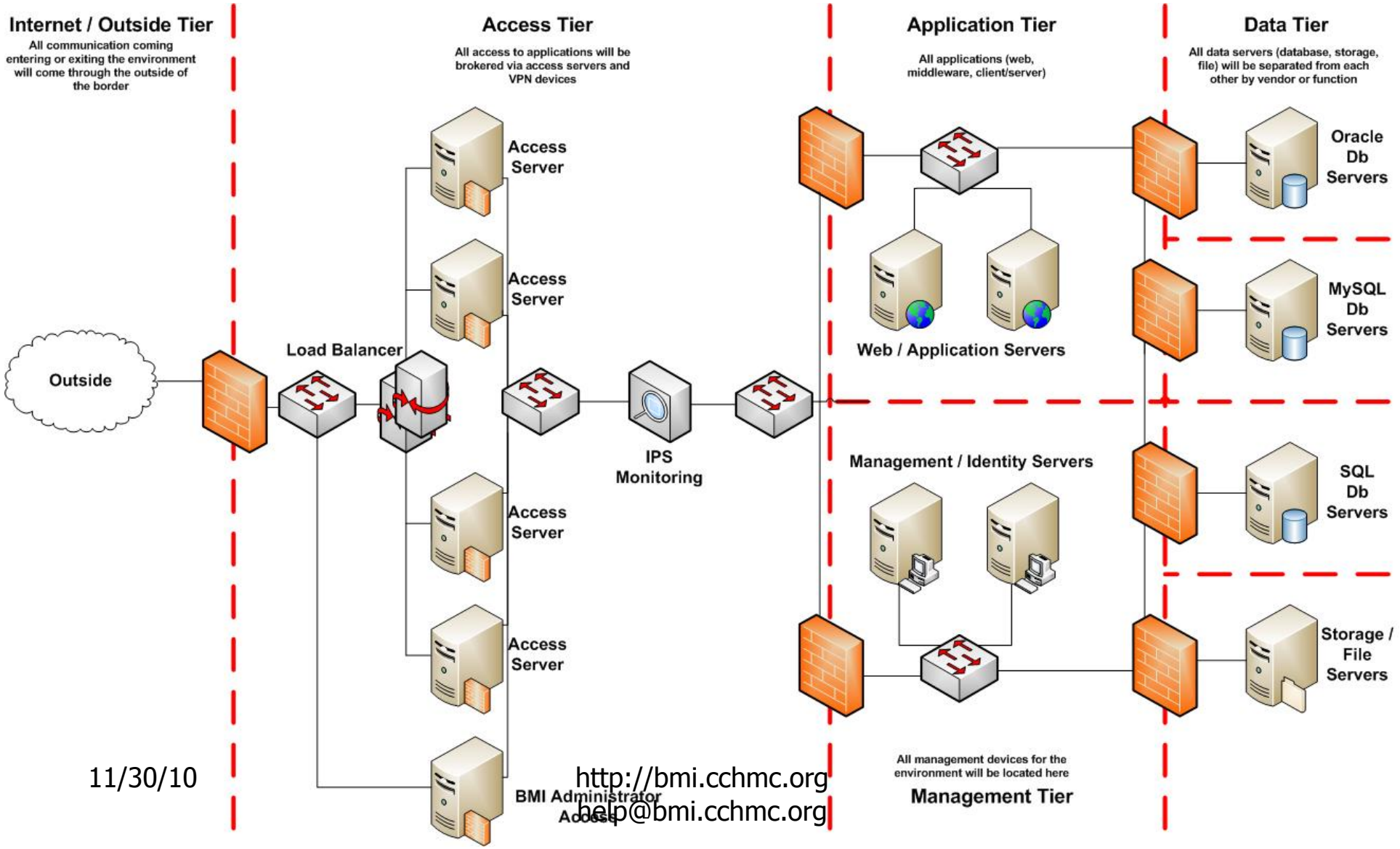
New network access infrastructure

- Increase security
- Create layered network infrastructure to divide production, staging and test/dev environment
- … and further separate research servers from the inside network and CCHMC mission critical servers

New Environment



New Environment



New network access infrastructure

- Provides platform for implementation of policies (current or upcoming)
- Provides platform for implementation of auditing capabilities
- Provides platform for implementation of a central place holding audit information for access granting

New network access infrastructure

- IS and BMI have built the network infrastructure and continuing to develop the identity management system
- Initially federation with UC and NIH and potentially other organizations: UC and NIH users will use their UC/NIH usernames and passwords on our systems. This will decrease the likelihood of their sharing of passwords etc.

New Environment

- IAM Environment
  - Self service for user administration:
    - Depending on regulatory requirements, PIs and application owners will have increased rights and responsibilities to administer access to their applications
    - Private roles for higher security application / requests
      - Limited to only application owners by proxy for requests
    - Public roles for user self service requests
      - Allows for both stringent approval and automatic approval
  - Shorter time to get users access
    - Go from days to <60 minutes based on approvals / availability

New Environment

- Accountability / ownership of access
  - With application owners / approvers, users can/will be responsible for security of their own applications and reviews
  - Regular reviews of access to ensure access is still required
- Strong authentication
  - All access is restricted at gateways until authenticated and authorized to access applications
- Fine grained authorizations
  - All users are authorized on an application by application basis rather than by location

New Environment

- Single Sign-on
  - Single point of authentication / identity providers allows simplification of sign-on process
  - Federation allows for management of personal credentials with partners and simplified access to hosted applications

How do sites/applications get into this new environment?

- Process will involve working with identity management team
- Initial documentation steps
- Transition time will depend on complexity of application, regulatory requirements

- (show the draft of the questionnaire)

It does not stop here…

- If your application requires closed data environment (no downloads)…
  - capability to lock it down completely and provide all tools within the environment
- If your application is not web based…
  - VDI capability (virtual desktop infrastructure)

Limited Demo

- https://access.research.cchmc.org