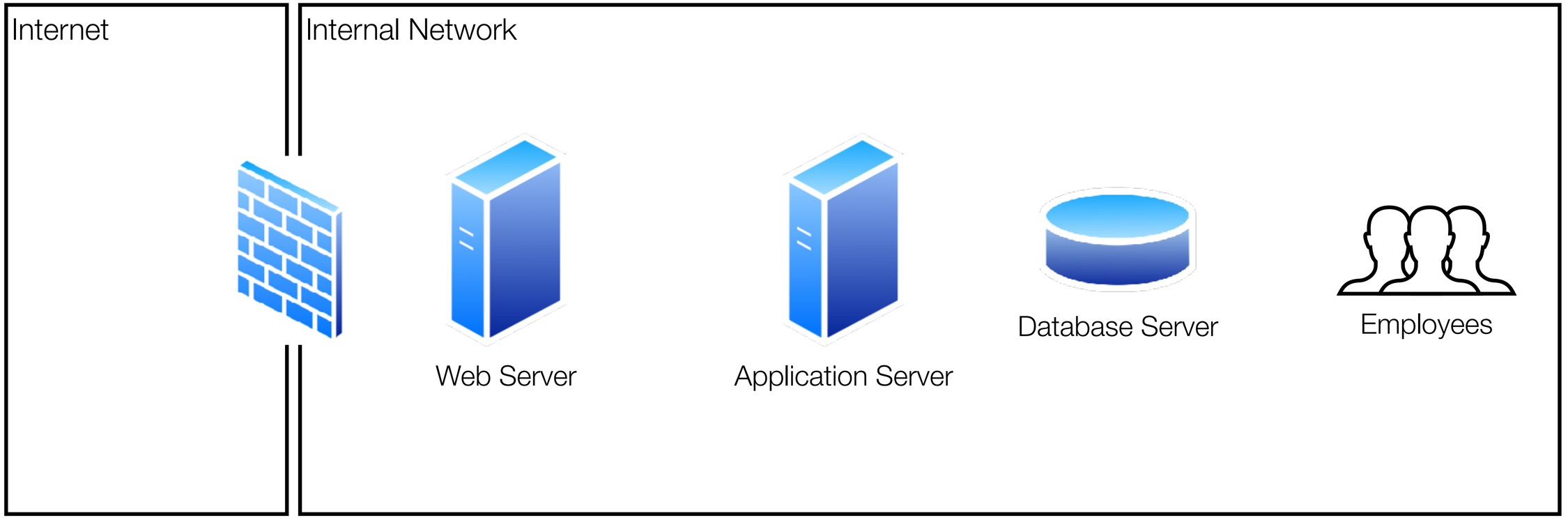
Operating System Security

Review

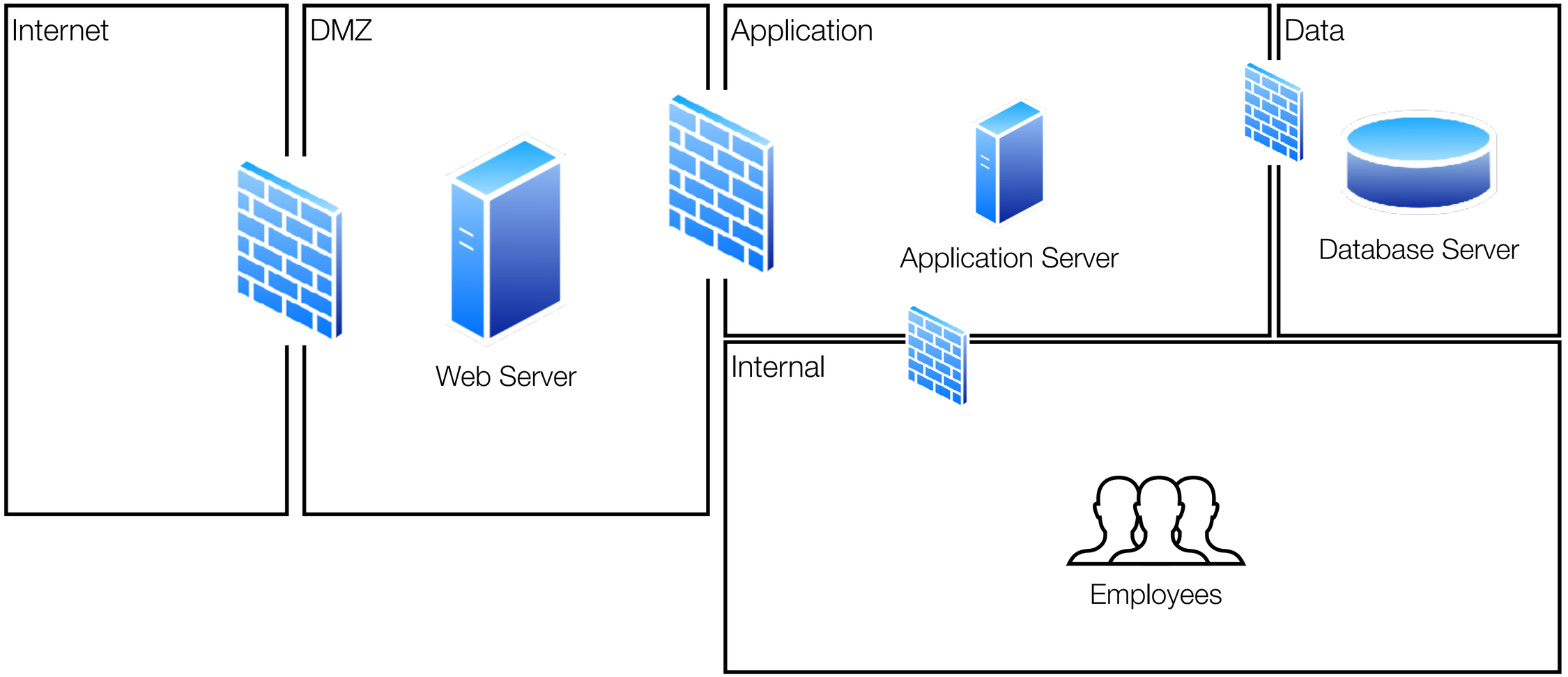
- What does the concept "defense in depth" mean?
- What is a DMZ in the context of firewalls?
- What is an IDS and what is the difference between an IDS and IPS?
- What is Wireshark and what can you do with it?
- Why should we use SFTP/SCP instead of FTP?
- What is the difference between a packet filter firewall and a stateful firewall?
  - Which one is easier to implement? Which one might provide additional security benefits?

Network Zoning Exercise

Given the following network, how can it be improved?



Network Zoning Exercise



Operating System Security - Fundamentals

- Remove unnecessary software
- Keep software and OS updated
- Remove unneeded services
- Apply principle of least privilege - permissions and accounts
- Change default accounts and default configuration for software
- Log and audit
- Periodic scanning

Software

- Software should be installed from trusted sources
  - Debian and other Linux OS make this easy using apt
- Software should be checked for upgrades and upgraded
  - Again, Debian and other Linux OS make this easy with apt
- Software should be removed if it is not being used
  - Every piece of additional software can prevent a vulnerability
  - Again, ... apt!
- Let's give it a try ...

Services

- It is good to do an occasional scan of what services are running on an operating system
- In Linux, this is fairly easy with systemd
- Let's take a look ...

Exercise - 5 Minutes

- How can you install MariaDB on your VM using apt? What is the full command and the package name?
- When you install MariaDB, is there a service associated with it? How do you know?
- What does the status show?
- When checking the status of SSH, what does the log information show at the bottom?

Exercise - 5 Minutes

- Uninstall MariaDB
- What does "apt autoremove" do?
  - You will see this when you uninstall MariaDB

Apply Principle of Least Privilege

- We should modify our OS so that only permissions that are absolutely needed are available for users
- Let's create a user and apply this concept with services

File Permission Exercise - 10 Minutes

- Using the test account you created, create a directory that has "devs" as the group owner
- Create 2 files in the directory, a and b:
  - One file has the word "hello" in it
  - The other file has the word "world" in it
- Change the permissions of "a" so that the group can read the file, change "b" so the group cannot read the file
- Change the directory so that the group "devs" can read, write, and execute the directory
  - Switch to the other user. What files can you read? What files can you change? Can you add a file? Can you run ls -l on the directory?
  - Change permissions for group to just "r". Can you add a file? Can you run ls -l on the directory?
- Be ready to describe the differences of permissions on regular files vs directories