Business Technologies
Secure Mobility

LeRoy Dennison
Apple Consulting Manager - Apple, Mobility & Consulting Services Teams
PC Mall Services

PCMall SARCOM

Secure Mobility Problem/Solution

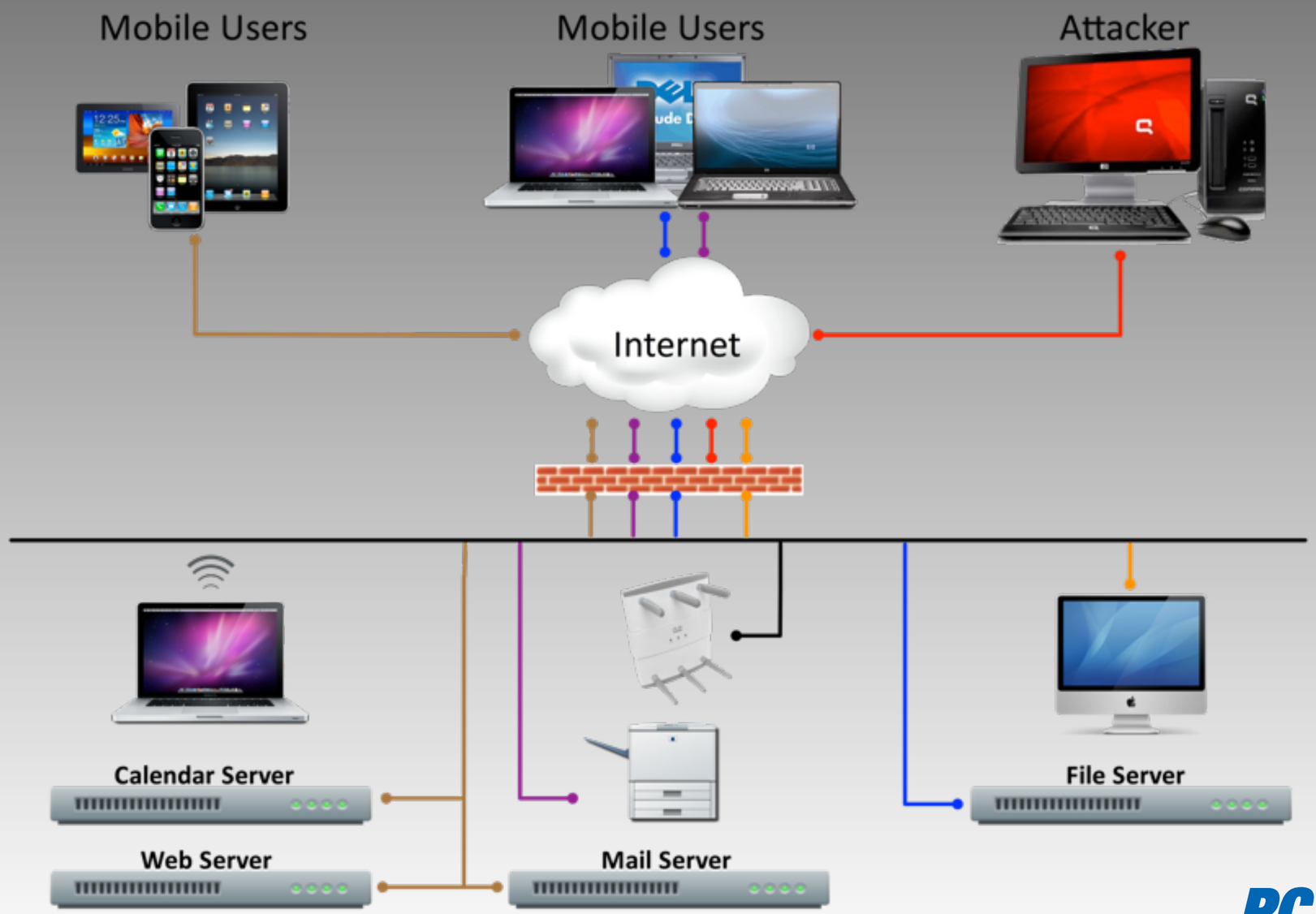
PCMall SARCOM

Secure Mobility Problem Characteristics

- Mobile users
  - Smart phones
  - Tablet devices
  - Netbooks/Ultrabooks/Laptops
- End of XP
- Consumers (end users) are driving IT
  - Consumers KNOW how it should work!
- But, IT still needs to secure corporate data

PCMall SARCOM

Problem...



PCMall SARCOM

Solution Characteristics

- Secure the infrastructure
- Split DNS
- Certificates
- VPN
- Web-based file-sharing
- No directory binding

Services

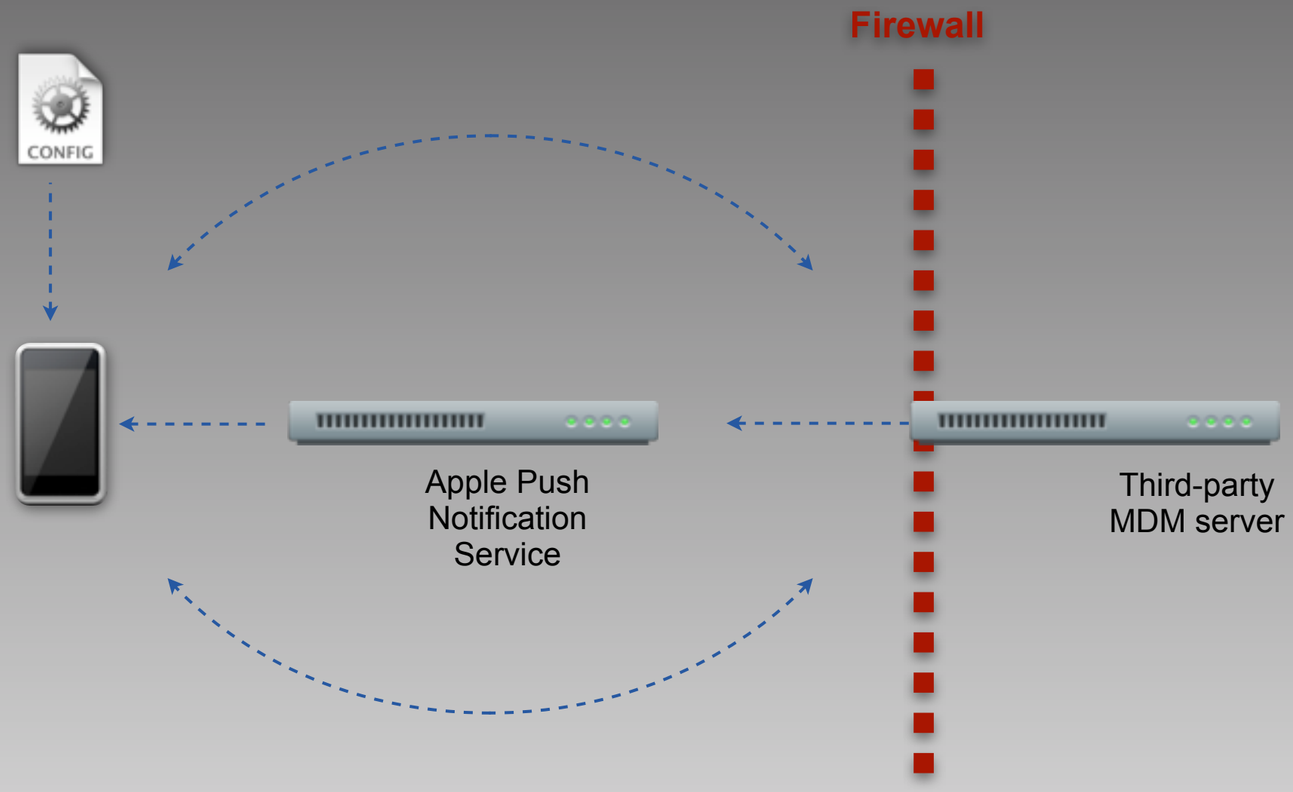
PCMall SARCOM

http://support.apple.com/kb/HT5012

How Certificates Work - BASIC

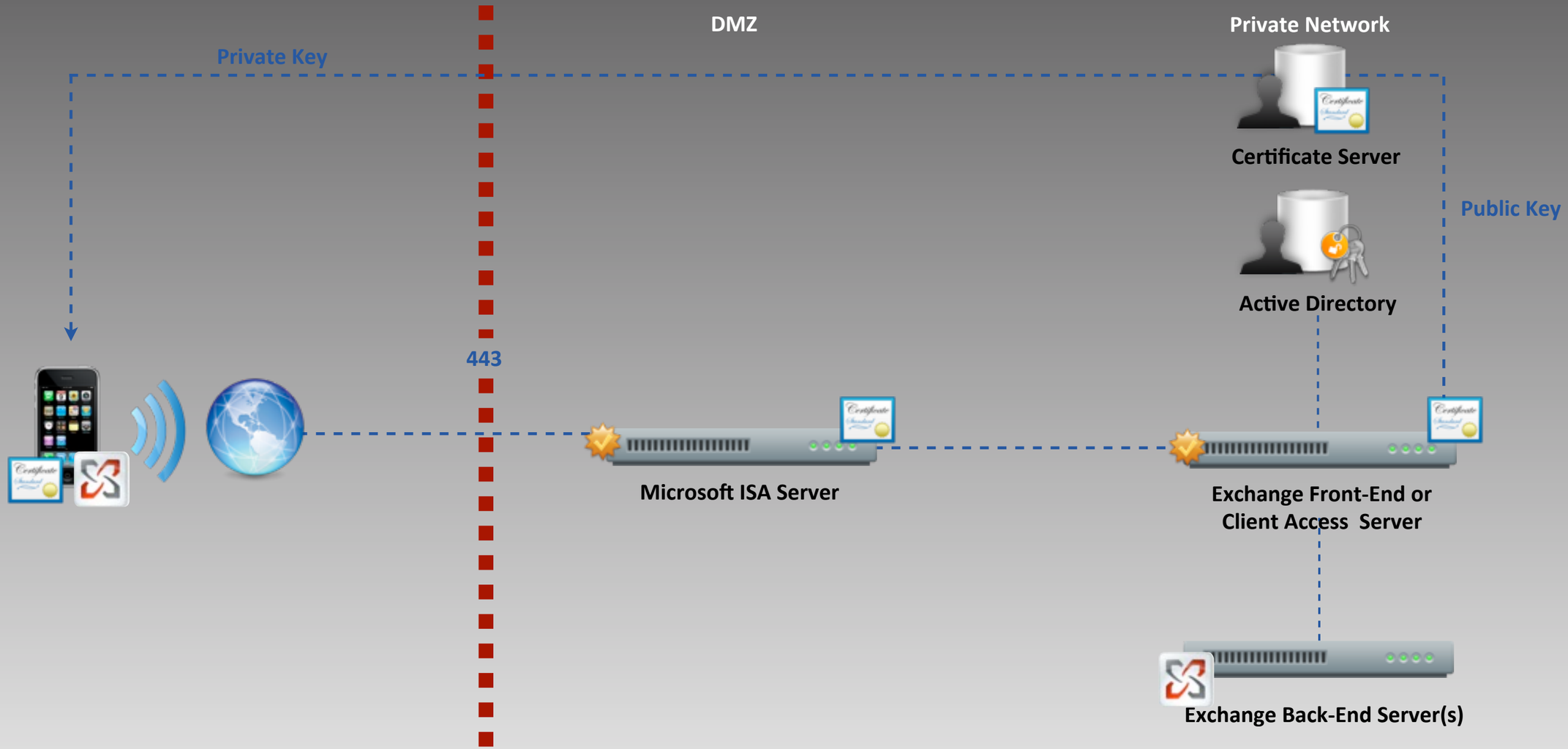
PCMall SARCOM

1. A Configuration Profile containing MDM server information is sent to the device.
   User is presented with information on what will be managed or queried by the server.
2. User installs profile to opt-in to device being managed.
3. Device enrollment takes place as the profile is installed. The server validates device and allows access.
4. Server sends push notification prompting device to check in for tasks or queries.
5. Device connects directly to server over HTTPS. Server sends down commands or requests information.



Mobile Device Management

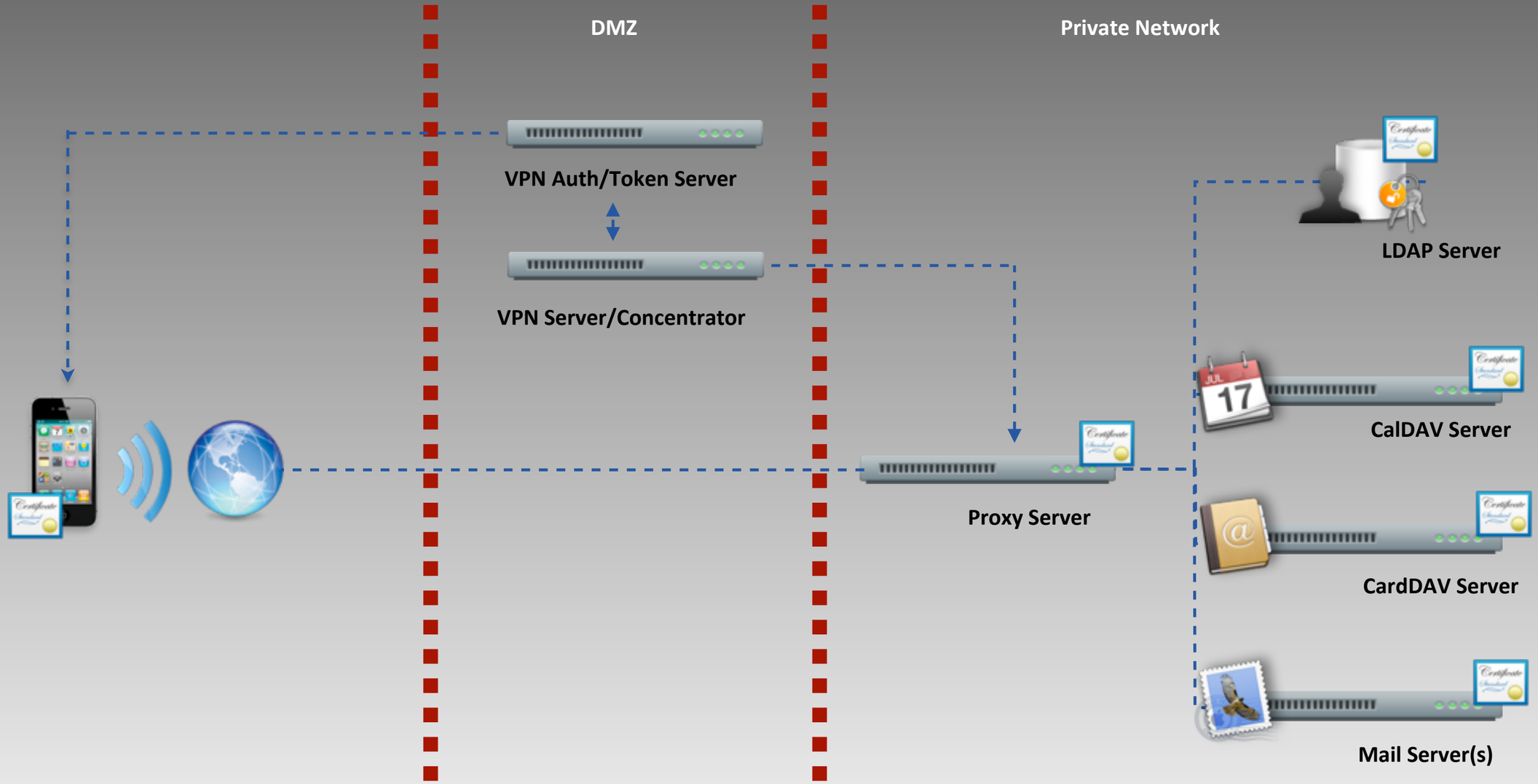
PCMall SARCOM



Microsoft Exchange ActiveSync

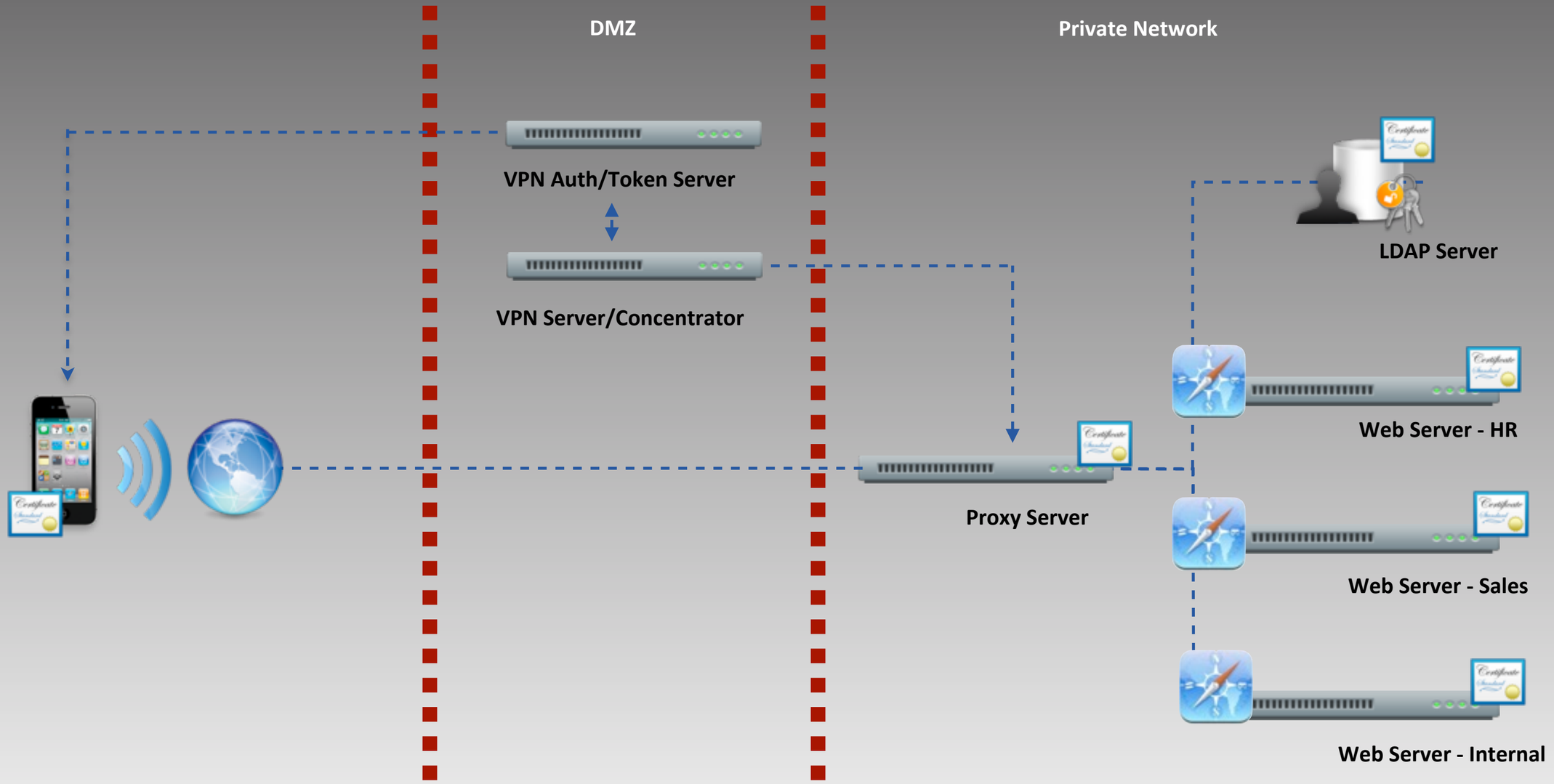
PCMall SARCOM

Deployment example



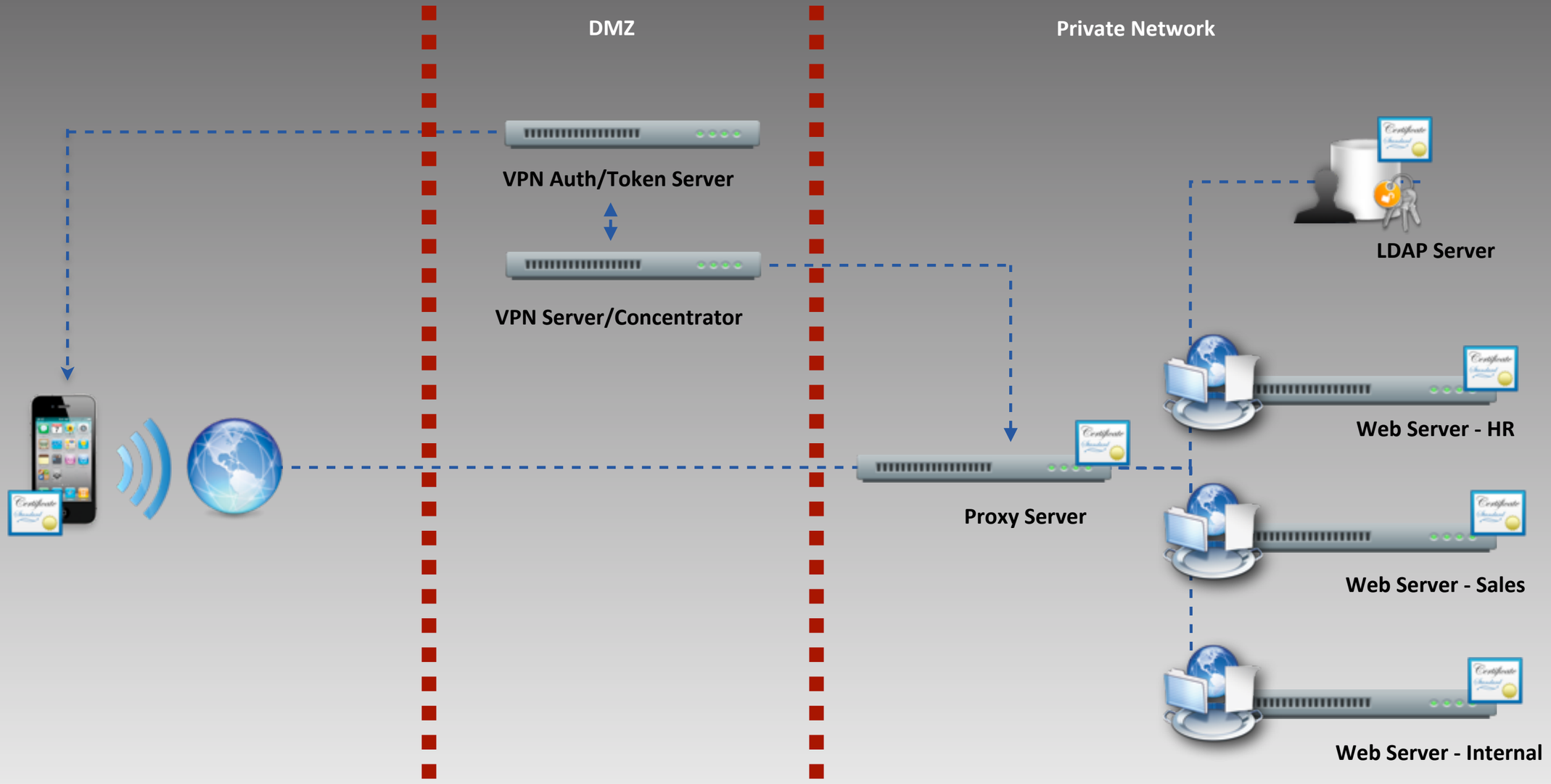
Open-Standards Collaboration

PCMall SARCOM



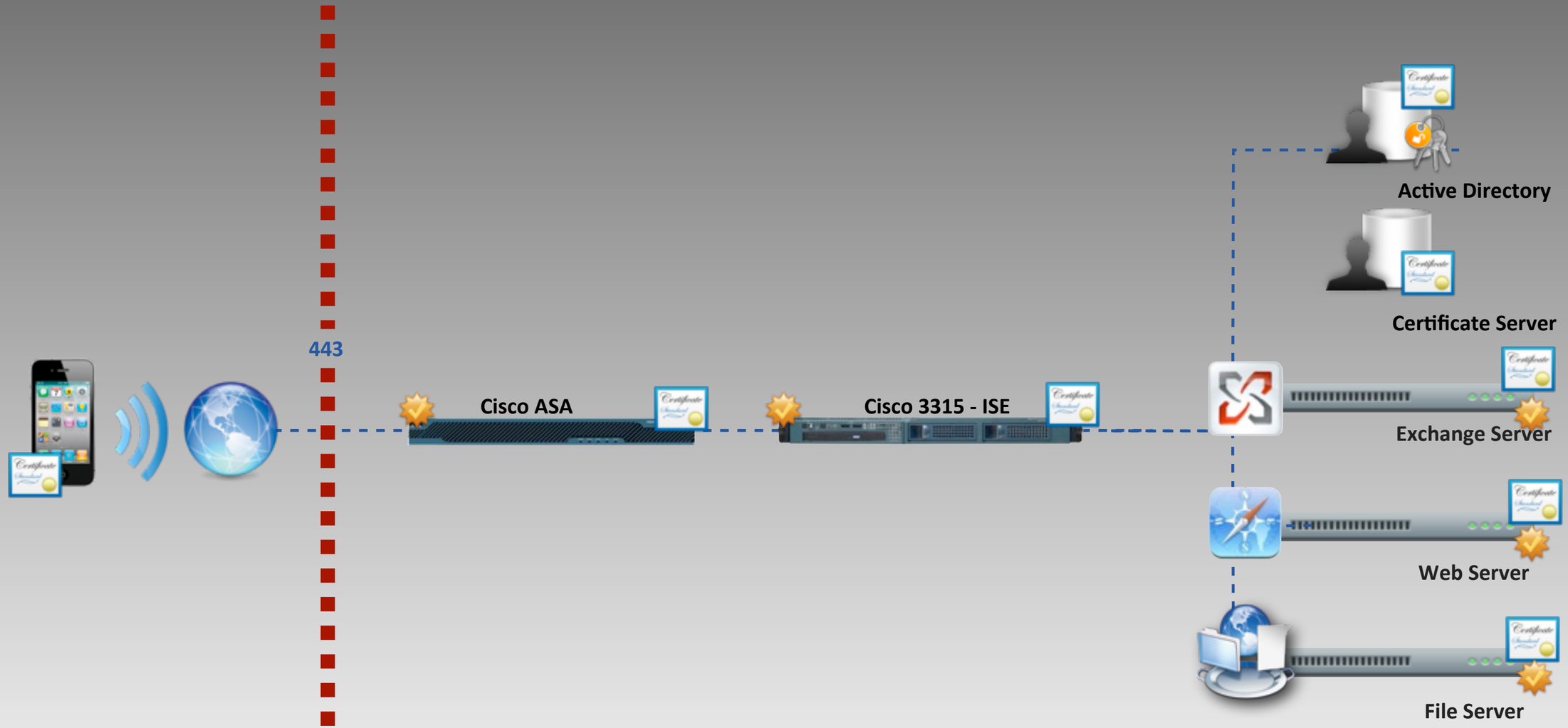
Web Server

PCMall SARCOM



File Server

PCMall SARCOM



How it Works

PCMall SARCOM

Configure

Enroll

Query

Manage

Mobile Device Management

PCMall SARCOM

MDM Tiers

- Tier 0 - Manual, on the device itself
- Tier 1 - iPCU or Apple Configurator, tethered
- Tier 2 - Profiles distributed via email or HTTP
- Tier 3 - Profile Manager (Mountain Lion Server), over-the-air updates
- Tier 4 - 3rd party MDM (needed for any MDM scenarios that are not all iOS)

Q & A