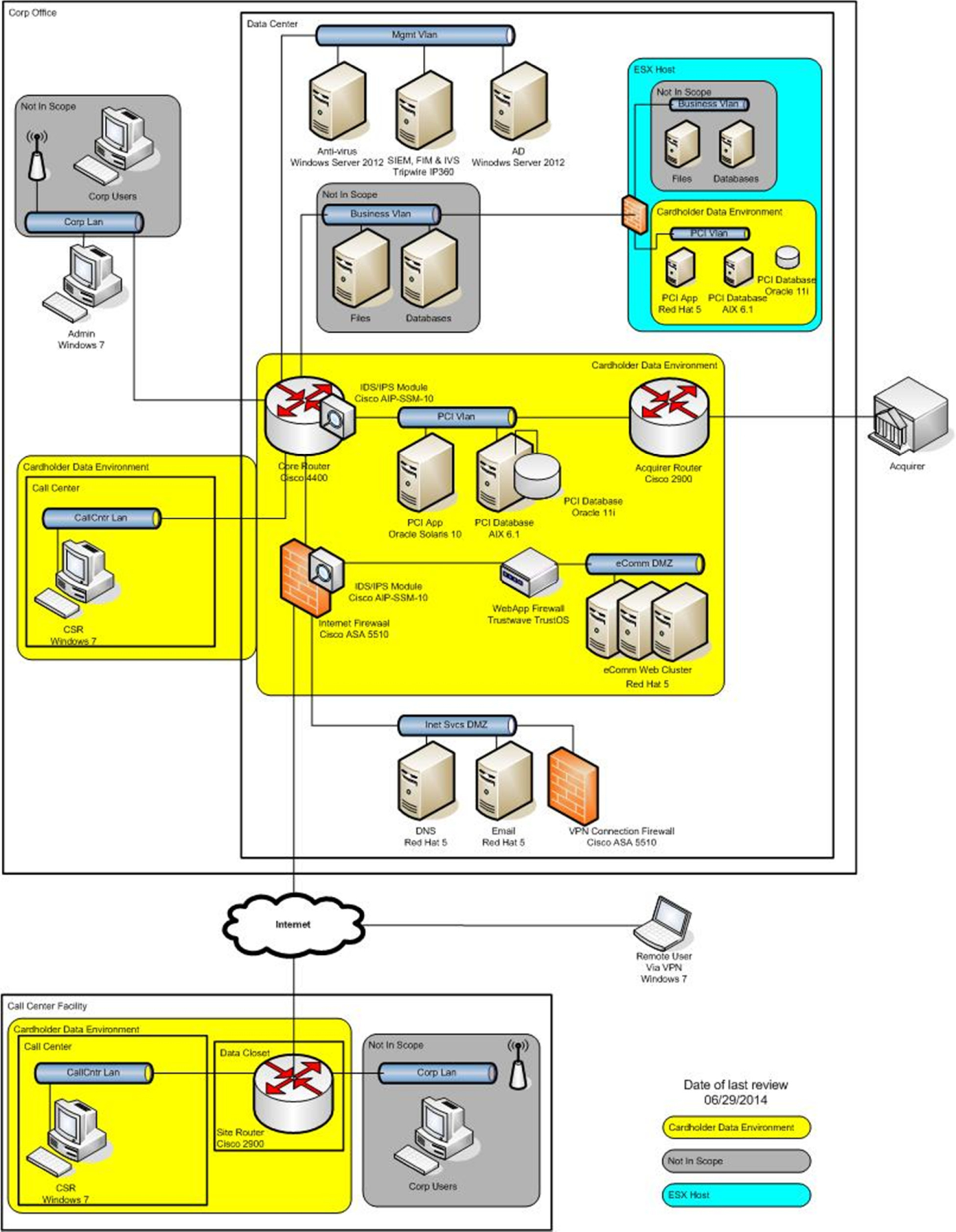
**Network Diagram**

The Network Diagram is intended to accurately portray the cardholder data environment and its associated systems and components, and clearly indicate in-scope and out-of-scope network segments.

**The high-level diagram must include the following:**

* + All in-scope network segments
  + All systems and components which store, process, or transmit cardholder data, including but not limited to:
    - Firewalls
    - Web application servers
    - Databases and database servers
    - PoS terminals
    - Payment applications
    - Workstations
  + All systems and components which connect to systems which process, store or transmit cardholder data, including, but not limited to:
    - Admin workstations
    - Other workstations
    - Connected third parties
  + All systems and components which support the security of the CDE, including, but not limited to:
    - Anti-virus servers
    - Logging servers
    - IDS/IPS systems
    - FIM servers
    - System administrator workstations
    - Hardware security modules
    - Vulnerability scanner
    - Two-factor authentication solution
    - Access control mechanisms
    - Key management systems
  + Devices which provide connectivity and segmentation including, but not limited to:
    - Firewalls
    - Web application firewalls
    - Routers
    - Load balancers
    - Layer-three switches
    - VPN concentrators
  + All locations sampled in the report, including, but not limited to:
    - Retail locations
    - Datacenters
    - Corporate locations
    - Hosting providers
    - Connected 3rd parties
  + Any wireless networks or devices, whether in scope or not. If the wireless components are not in scope they should be labeled as such.
  + Other systems and components as applicable
  + Non-PCI segments (clearly labeled as such)
  + All connections into and out of the network, including demarcation points between the cardholder data environment (CDE) and other networks/zones
  + Direct connections to any other entity, including card brands
  + A key or legend as needed
  + Date of last review
* **Additional details:**
  + Diagram must clearly correspond to the connectivity diagram (see p. 4)
  + All systems included in the diagram must be clearly labeled, to include make/model and function (e.g. Win2008 e-comm web server, Cisco ASA 5510 border firewall)
  + Do not include IP addresses or hostnames. Only functional descriptions should be used.
  + All diagrams must be legible on 8.5 x 11 paper. If they cannot be easily read on the page then they should be split into multiple diagrams.
  + Where multiple devices perform the same function, e.g., clustered devices and server farms, these can be represented by a single object
  + Virtual servers and virtual networks should be grouped inside a container which is shaded to indicate the virtual environment

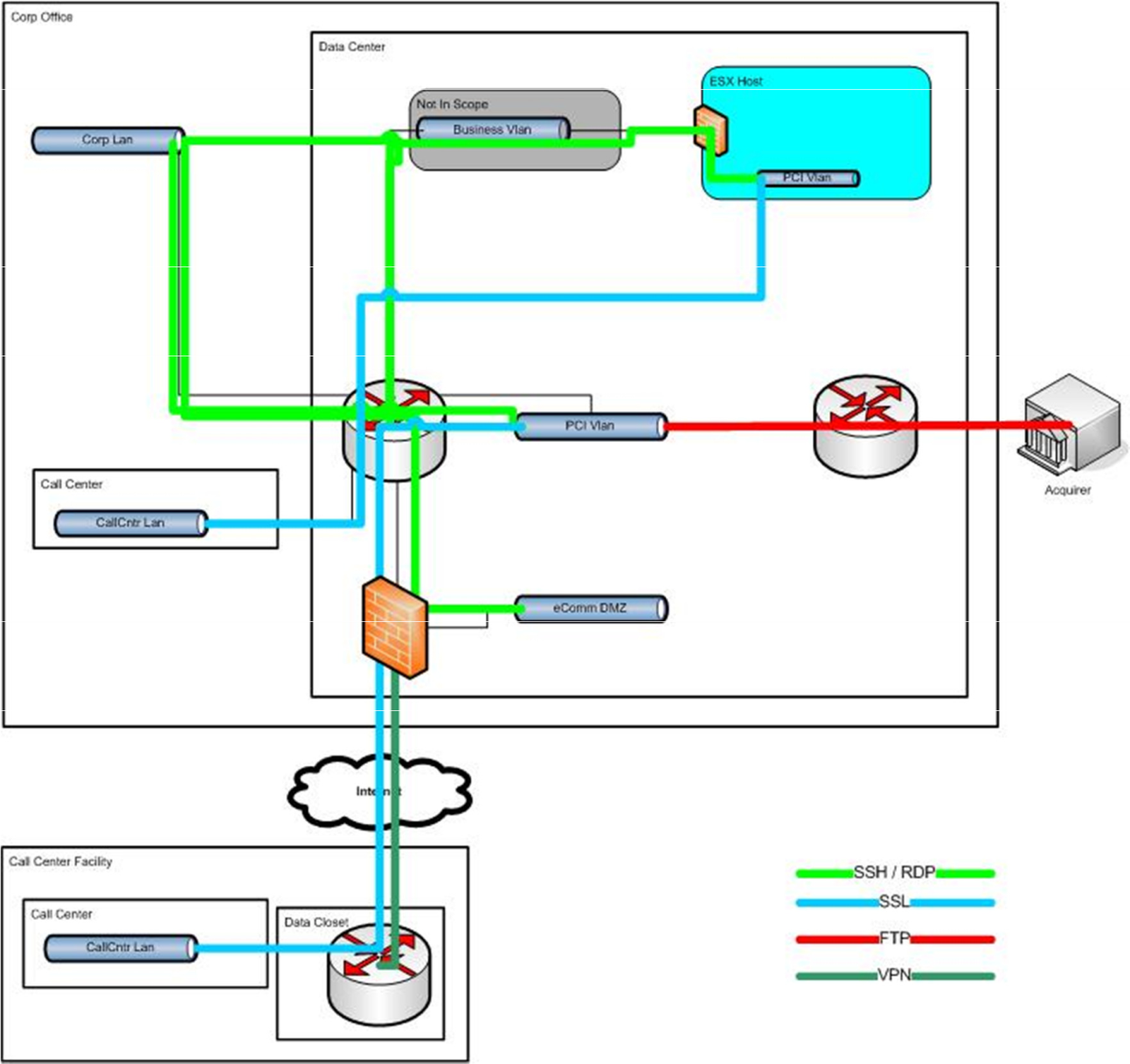


Sample Network Diagram

**Connectivity Diagram**

The connectivity diagram is intended to portray communications between the cardholder data environment and other networks.

* **The connectivity diagram must include the following:** 
  + All external connections to third parties, including payment processors, service providers, card brands, etc.
  + All internal environment, networks, or systems which are connected to the CDE
  + All boundaries of the CDE
  + Any segmentation points used to reduce the scope of the assessment
  + All wireless networks
  + All physical locations (some locations, such as retail stores, can be depicted with single representation provided they are configured identically)
  + Other connection points applicable to the assessment as needed
  + All locations included in the CDE
  + A key or legend as needed
  + Date of last review
* **Additional details:**
  + All segments must be labeled in a consistent manner which corresponds to the labeling on the high-level diagram
  + All segments must indicate if they are in scope or out of scope
  + All systems and components must be labeled in a consistent manner which corresponds to the labeling on the high-level diagram
  + Diagram must clearly correspond to the high-level diagram (see p. 1)
  + For each communication point show the applicable device interfaces, network technologies, protocols, and security controls applicable



Sample Connectivity Diagram