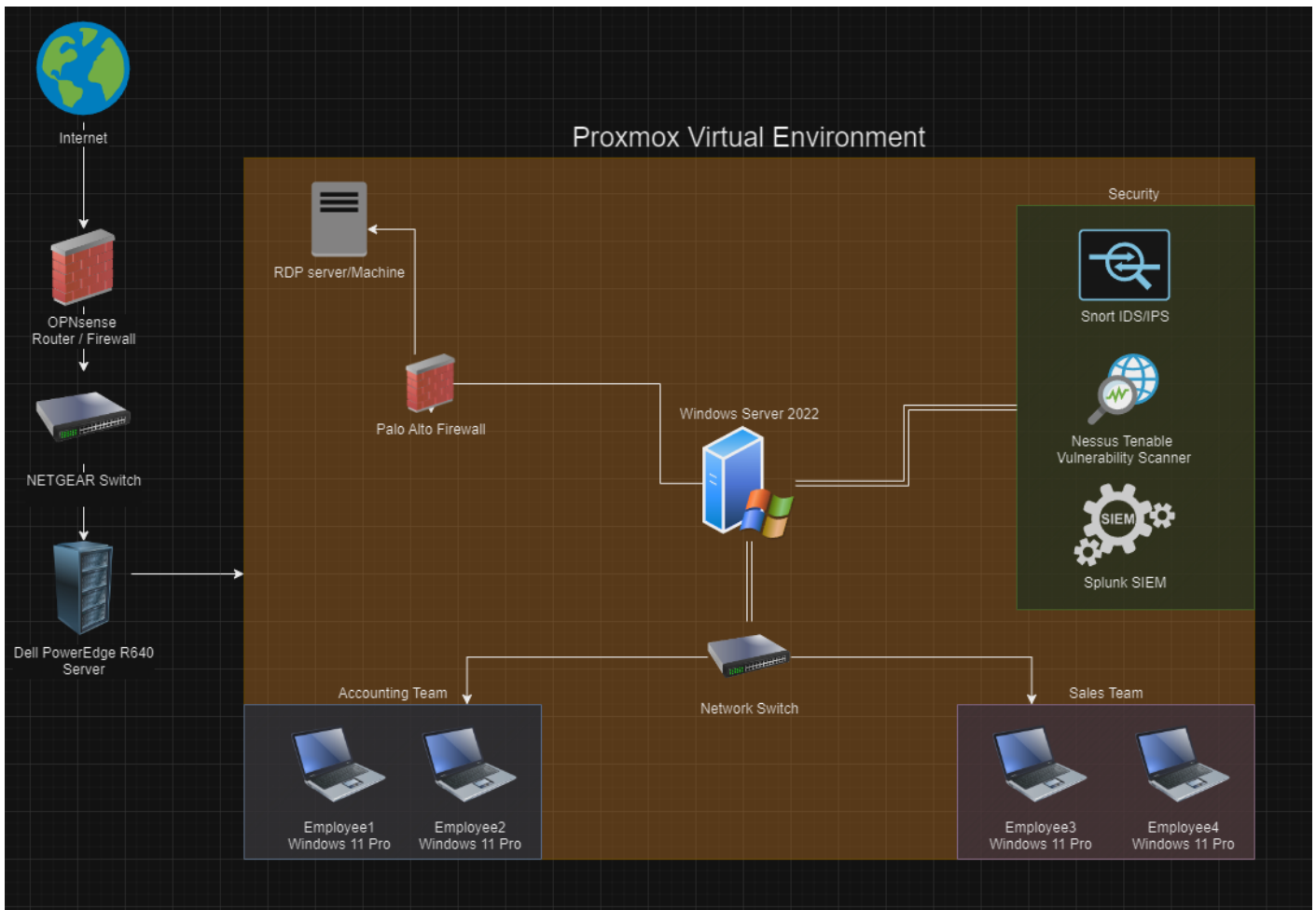


Topology



Palo Alto Firewall: Serves as a firewall between the authentication server and the remaining network. Setting this up will give me some experience with commonly used security devices in enterprises today.

Windows Server: Hosts various services like Active Directory for user management, file storage, and possibly application services. This server will be essential for managing the network's resources and users.

Email Server: Manages all email communications within the enterprise. It can be a dedicated server or a hosted service. It's responsible for receiving, sending, and storing emails for all users within the network.

Splunk SIEM: A dedicated server or appliance running Splunk for Security Information and Event Management (SIEM). It aggregates and analyzes log data from across the network, including the firewall, servers, and endpoints to detect, alert, and respond to potential security incidents.

Nessus Tenable: A vulnerability scanning tool that regularly scans the network for vulnerabilities. It can be hosted on a dedicated server or run as a service. Nessus helps in identifying and remediating security vulnerabilities in the network's devices and software.

Windows 11 Pro Laptops: Represents the employee endpoints connected to the network. These devices are used for daily operations and access the network's resources securely, often through the firewall's protective mechanisms.

Revision #2

Created 2024-03-23 02:14:35 UTC by Austin

Updated 2024-03-23 19:14:02 UTC by Austin