**Infrastructure**

Infrastructure security ensures the availability of information from the CIA’s triad for the ACME Defense contractors to improve security and performance. All systems in the business will have a common security policy and system security configurations or precautions will be taken. The ideal practice will be to rename the administrator account and implement a strong passphrase rather than a password, have the most up-to-date antivirus software, remove unnecessary accounts, protocols, services, and sharing, and only use authorized modems. The business will have a firewall installed between each system and the internet. The business will make use of virtual desktop infrastructure. For security logs and audits, the business will have a centralized log archive on a server and in the cloud to track successful logins and failures, as well as the processes executed. The logs will be continuously audited by an automated system and trigger notifications for unusual activities. The business security network design incorporates increased physical security to secure the wiring closet, which helps the business in preventing unauthorized access. Physical access to IDS, firewalls, and routers is typically restricted. The business employs switches, which completely prevent collisions between domains and also aid in analyzing packet headers and implementing access control lists. Switches are also administered using the Simple Network Management Protocol (SNMP) and Secure Shell (SSH) to limit exposure to any intruders, especially for managed switches. The business uses a secure environment like a virtual local area network (VLAN) in one uplink port that carries multiple virtual local area networks across the line, also known as a trunk, that helps increase network segregation, throughput, and security against unauthorized network connections. The business employs a wireless access point, which serves as a point of entry for a wireless device to a wired network and utilizes an AES cryptography algorithm and regulations to prohibit unauthorized wireless access points like modems, cable modems, routers, and DSLs with periodic auditing. The business uses a network-based intrusion detection system (IDS) that includes signature and anomaly-based detection methodologies. A firewall is also used by the business to impose security regulations across networks to build a trusted network, and the IDS is put right after the firewall to monitor traffic. The business uses VoIP (Voice over Internet Protocol), which enables the business to conduct voice communications via the internet rather than using an outdated analogue phone line. Tunneling is used by the business to protect communication on the public internet by converting it to garbage values and interacting exclusively with IPsec-enabled routers. Tunneling also enables considerable levels of security and secrecy via encryption and encapsulation. Because we have a limited number of addresses, the business will use a complete class C address and will pass through a static (1:1) network address translation (NAT). NAT also aids in the generation of a valid external IP address.