ROI Perth branch office network - Project brief

ROI management had decided that they wanted to open a new branch office in Perth and have asked a third-party organisation called ***XYZ Networking Services*** to produce an enterprise network topology considering the technical requirements, physical and financial constraints and expansion projections.

You are working as a network engineer at XYZ Networking Services and have been assigned to investigate the ROI project.

Internetwork design specifications

The following information have been provided to you by ROI management:

- Budget allocated for the project: AUD 100, 000
- The branch office should be able to:
    - accommodate at least half of the equipment and staff compared to the ROI head office, having potential for further expansion in future.
    - facilitate communication between the branch and the head office.
    - facilitate data and voice communications within the branch itself and the head office.

Security considerations

ROI's head office network is established and maintained according to the following network security specifications. Therefore, ROI management had requested for these security specifications to be considered when designing the internetwork for the branch office.

- network device access should be limited only to network administrators.
- remote access of the network devices should be controlled with appropriate security measures such as the use of security protocols, encryption and strong passwords.

- Network traffic should be restricted between production (multimedia-production) environment and non-production (accounts, sales, human resources) environments.

- The following protocols should be prohibited for use: FTP, telnet and SSHv1

- Where technically feasible, all communication devices and systems should be enabled with encryption solutions.
    - Minimum acceptable hash algorithm: SHA 256
    - Minimum acceptable encryption algorithms:
        - Symmetric: AES, 3DES
        - Asymmetric: RSA, DSA
    - Acceptable minimum crypto key length:
        - Symmetric: 128 bits
        - Asymmetric: 1024 bits

Enterprise procedures for implementing network security

Every router or switch must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device’s support organization.
3. The following services or features must be disabled:
    a. IP directed broadcasts
    b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    c. TCP small services and UDP small services
    d. All source routing and switching
    e. All web services running on router

   f. Telnet, FTP, and HTTP services
   g. Auto-configuration

4. Each router must have the following statement presented for all forms of login whether remote or local:

   "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

5. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

6. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

7. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.