**1. AAA Server Configuration**

* Configured TACACS+ servers on Lebanese (R4) and Egyptian (R2, R3) routers to centralize authentication for network devices.
* For each router, AAA new-model was enabled, and TACACS+ server IP addresses and keys were configured.
* Authentication login and authorization exec methods were set to use TACACS+ with fallback to local user databases.
* Console and VTY lines were configured to use AAA authentication.
* Local user accounts were created as fallback in case the TACACS+ server is unreachable.

**2. VPN Setup Between Lebanese and Egyptian Branches**

* Established a site-to-site IPsec VPN tunnel between Lebanese router (R4) and Egyptian router (R1).
* Used ISAKMP policies with AES encryption, pre-shared keys, and group 5 Diffie-Hellman.
* Created crypto IPsec transform sets and crypto maps matching ACLs defining allowed subnets.
* Applied crypto maps to outgoing serial interfaces.
* Verified the VPN tunnel establishment with show crypto isakmp sa and show crypto ipsec sa.
* Confirmed connectivity by successful pings across the VPN between branch devices.

**3. SYSLOG Server Integration**

* Configured the Lebanese SYSLOG server at IP 192.168.5.11 to collect system logs from all Lebanese branch devices.
* Enabled logging on routers specifying the SYSLOG server IP.
* Enabled service timestamps for log messages.
* Verified that the routers send syslog messages and confirmed their receipt on the server in Packet Tracer.

**4. Brute Force Attack Prevention**

* Configured login blocking on the Lebanese server room router (R4) to prevent brute force attacks.
* Set the router to block login attempts for 5 minutes after 3 failed login attempts within 1 minute.

**5. Access Control Lists (ACLs)**

* Implemented extended ACLs on R4 to prevent Lebanese branch employees from pinging Egyptian IT network addresses (20.0.0.2 and 192.168.1.1).
* Applied ACL outbound on the interface connecting Lebanese and Egyptian branches.
* Confirmed that ICMP traffic from Lebanese LAN to Egyptian IT subnets is blocked while allowing other traffic.

**6. Port Security Configuration on Switches**

* Configured port security on all switches to enhance LAN security.
* For critical devices (AAA server, SYSLOG server, CEO PC, main PC in server rooms), ports were configured with:
  + Violation mode: **shutdown** (port disables on violation).
  + Maximum 1 MAC address.
  + Sticky MAC address learning.
* For all other devices, ports were configured with:
  + Violation mode: **restrict** (violations logged and packets dropped, but port remains up).
  + Maximum 1 MAC address.
  + Sticky MAC address learning.
* Configured ports on each switch based on device roles and locations.
* Verified port security settings per interface.