DEPLOYMENT SECTION

1) Configure Active/Passive relationship between **ASAv1** and **ASAv2**
   a. must be named “inside”, “outside”, and “mgmt”.
   b. Follow the IP addressing as per the diagram
   c. Ensure Fail and state interfaces are names as LAN and state
   d. Use .1 (first IP of octet) to assign addresses to the FWs
2) Configure Active/Active relationship between **ASA12** and **ASA13**
   a. must be named “inside”, “outside”, and “mgmt”.
   b. context HR and context ACC is to be created and assign Ips as per the diagram
   c. Follow the IP addressing as per the diagram
   d. Ensure Fail and state interfaces are names as LAN/ST
   e. Use .1 (first IP of octet) to assign addresses to the FWs
3) Configure Clustering relationship between **ASA20** and **ASA21**
   a. must be named “inside”, “outside”, and “mgmt”.
   b. Cluster group name should be Cisco
   c. Follow the IP addressing as per the diagram
   d. Key should be C1sC0123!
   e. Inside network should be part of VLAN 100 & outside network should be part of VLAN 200
   f. Use .1 (first IP of octet) to assign addresses to the FWs
4) Configure AnyConnect VPN on London Site with requirements as below
   a. HR department should have a dedicated profile named as **HR-Profile** and pool 172.16.10.0/24
   b. ACC department should have a dedicated profile named as **SALES-Profile** and pool 172.16.20.0/24
   c. Ensure you enable split tunneling
   d. IPSec IKEV2 tunnel with an idle timeout of 2 Days.
   e. Create local users on ASA DB for HR it should be hr/cisco123
   f. Create local users on ASA DB for ACC it should be acc/cisco123
5) Configure Clientless SSL VPN for Dubai Remote-Site on ASAv-W
   a. Tech department should have a dedicated profile named as **Tech-profile**
   b. Username should be tech and password cisco123
   c. Use a web-acl and add it the group policy so that user tech can access tech-server only.
6) Configure Site-2-Site **IKEv1 VPN** between **DC23** and **Gisborne** edges.
   a. Ensure your VPN profile name is DC23-GS
   b. Pre-shared key should be Cisco123
   c. Ensure your **DC23 FTD** should be added as **FTD-DC23**
   d. Ensure your **GISBORNE FTD** should be added as **FTD-GISBORNE**
7) Configure **Flex VPN** between **Napier** & **Nelson** branch
   a. Tunnel network to be used is **192.168.100.0/24**
   b. Pre-shared key to be used is **Cisco123**
   c. Tunnel should be native ipsec
   d. Ensure you exchange internal routes using EIGRP and **AS** to be used is **100**
8) Configure **Site-2-Site VPN** between **DC400** & **DC500** branch
   a. Pre-shared key to be used is **Cisco123**
   b. Make sure CRM server can talk to server 50 and back and forth
9) Configure **Dot1x** and **Mab** for **Customer service-PC** & **IT-PC**
   a. DHCP pool for **IT-PC** should be **10.10.10.0/24 VLAN 10**
   b. DHCP pool for **Customer service** should be **10.20.20.0/24 VLAN 20**
   c. Push DACL to IT-PC so that it can telnet **CRMSERVER**
   d. Push DACL to Customer service so that it can browse the **CRMSERVER**
   e. Ensure Customer service user is authenticated using ISE Local DB and username should be **cspc/Cisco123**

10) Configure **NTP server** on your **NTP router**
    a. NTP should use authentication
        i. Key should be **100**
        ii. Password **cisco123**
    b. Configure NTP client config on **R17 & R18**
11) Configure **SYSLOG** on **R9**
    a. Ensure logs are sent to log server located in management PC
12) Configure **WSA redirection** on **Call center router**
    a. **CC-team lead** should be able to access **Call center Dashboard**
    b. **IT-admin** should be able to access **Call center manager**
13) Optimization/Troubleshooting
    a. You have been asked to **optimize zone-based FW for DC100**, so that only ICMP traffic from outside to inside should be inspected.
    b. Users on **win machine** are not able to connect to **DC200 server on port 8080**, troubleshoot and fix the issue.