13. Challenges Faced & Solutions

This project spanned multiple technical domains including networking, security, IAM, and hybrid connectivity.
As a result, several design and conceptual challenges emerged. Each challenge was addressed through deliberate trade-offs, practical experimentation, and clearly documented decisions.

13.1 Challenge: IAM Role and Permission Design

Problem

Designing IAM permissions for EC2 and supporting services required a clear understanding of AWS identity concepts, which initially introduced confusion around:

- The distinction between IAM roles, policies, and instance profiles
- How permissions are assumed by EC2 instances at runtime
- Avoiding overly permissive policies while still enabling required functionality such as SSM and CloudWatch logging

Solution

IAM concepts were explicitly separated and applied correctly:

- **IAM Role**: Defined as the identity assumed by EC2 instances
- **IAM Policy**: Used to specify the exact permissions required
- **Instance Profile**: Used to attach the role to EC2 instances and Auto Scaling Groups

Least-privilege policies were applied, granting only:

- CloudWatch Logs write permissions
- AWS Systems Manager (Session Manager) access

Static access keys were avoided entirely in favor of IAM roles.

Outcome

- Secure and auditable access model
- No credentials stored on EC2 instances
- Clear understanding of how AWS identity and access flows operate in practice

---

13.2 Challenge: Hybrid Routing and CIDR Planning

Problem

Hybrid connectivity introduced complexity in several areas:

- Selecting non-overlapping CIDR ranges
- Understanding how traffic flows between on-premise and AWS environments
- Differentiating the responsibilities of route tables, subnets, and gateways

Solution

CIDR ranges were explicitly planned and documented:

- **On-Premise:** `192.168.10.0/24`
- **AWS VPC:** `10.0.0.0/16`

End-to-end traffic flows were clearly defined and validated:

- On-prem → firewall → VPN tunnel → VGW → VPC router → private subnet

Explicit routing entries were added on both sides:

- AWS route tables forward on-prem CIDR traffic to the VGW
- On-prem routing forwards AWS CIDR traffic into the VPN tunnel

Outcome

- Predictable and debuggable routing behavior
- No CIDR overlap or asymmetric routing issues
- A clear mental model of packet flow across environments

13.3 Challenge: Selecting the Appropriate Hybrid Connectivity Model

Problem

Multiple connectivity options were available for integrating on-premise systems with AWS:

- Public internet exposure
- Site-to-Site VPN
- AWS Direct Connect

Choosing the appropriate model required balancing security, complexity, cost, and scope.

Solution

Each option was evaluated against project constraints:

- **Public exposure** was rejected due to unacceptable security risk
- **Direct Connect** was rejected due to cost and operational overhead inappropriate for a proof-of-concept
- **Site-to-Site VPN** was selected as the optimal balance

A conceptual Site-to-Site IPsec VPN was implemented using:

- OpenSwan / strongSwan on the on-premise side
- AWS Virtual Private Gateway on the cloud side

Outcome

- Secure, encrypted private connectivity
- Industry-standard hybrid architecture
- Realistic and assessment-appropriate design

13.4 Challenge: Security Versus Operational Simplicity

Problem

Balancing strong security controls with operational clarity required deliberate decisions around:

- Whether to introduce custom Network ACLs
- Whether to deploy a bastion host
- How much complexity to introduce at the proof-of-concept stage

Solution

Security controls were simplified without reducing effectiveness:

- **Security Groups** were used as the primary enforcement mechanism:
    - Stateful
    - Easier to reason about
    - Aligned with least-privilege principles
- Default Network ACLs were retained to avoid unnecessary stateless rule complexity
- AWS Systems Manager Session Manager was chosen over a bastion host for administrative access

Outcome

- Reduced attack surface
- Clear and maintainable security boundaries