|  |
| --- |
|  |
| Daydreams Travel Agency Configure a Virtual Network and Peering |
|  |

|  |
| --- |
| Thong Thao  Student ID: 474587265 |

**Contents**

[Section A – Design a Virtual Network 2](#_Toc161921009)

[Part 1 – Prepare to Design and Configure the Virtual Network 2](#_Toc161921010)

[Part 2 – Design and Configure the Virtual Network 5](#_Toc161921011)

[Reference 7](#_Toc161921012)

# Section A – Design a Virtual Network

## Part 1 – Prepare to Design and Configure the Virtual Network

For designing Daydream Travel Agency's virtual network on AWS, research is crucial to identify industry standards, procedures, and best practices. Key resources include official AWS documentation, architecture guides, and partner networks for implementation assistance.

Additionally, understanding relevant regulations is essential. The Australian Travel Industry Code of Conduct offers voluntary ethical guidelines, while the Australian Consumer Law and Privacy Act establish baseline requirements for consumer protection and data handling.

**Cloud Vendor Research**

* AWS Official Resource: Detailed information on all AWS services, best practices, tutorials, and solution guides.
* AWS Partner Network: Provide expertise, assistance with implementation, and potentially managed services for ongoing support.

**The Industry Standards, Procedures, and Guidelines**

* AWS Well-architected Framework: A set of pillars (security, reliability, performance efficiency, cost optimisation, operational excellence) for evaluating and designing cloud architectures.
* Cloud Security Alliance (CSA): Promotes security standards and best practices for cloud computing.

**The Legislative Requirements**

* Australian Travel Accreditation Scheme (ATAS): Voluntary code promoting ethical standards. Daydreams may choose to adopt it to demonstrate commitment.

1.1 List all of the networking requirements for Daydreams Travel Agency based on the business needs in the case study. List the cloud resources needed to meet these requirements.

|  |  |  |
| --- | --- | --- |
| Business Needs | Cloud Resource | Comments |
| Increased Storage | Amazon S3 | S3 standard single bucket in the local AWS region |
| Monitoring and Auditing | CloudWatch and CloudTrail | CloudWatch for metrics, alarms, and logs; CloudTrail for auditing API calls and actions |
| Scalability for increased number of employees | Amazon VPC | VPC allows the segmentation and scalability of network resources. |
| Internet Access (Public subnet) Allows publicly facing services like the web to be reached by customers. | Internet Gateway | Enables internet connectivity to the VPC.s |
| Allow internal resources to reach external services. | NAT Gateway | Provides internet access to private subnet instances while protecting their direct exposure. |
| Segmentation of network traffic | Subnets | Subnets allow for the segmentation of network traffic for improved security and management. |
| Compliance with data privacy regulations | Security Group | Security Groups (SGs) can be set up to allow incoming and outgoing traffic for the virtual networks at the instance level |
| Secure remote access for sales representatives | VPN | VPN enables secure access to company resources for remote workers. |

1.2 Identify business and industry requirements. To do this, you will need to conduct research to investigate travel industry standards and guidelines, and state and Commonwealth legislation and frameworks. Also look at tourism industry associations e.g. Tourism Australia, Business Queensland, Australian Federation of Travel agents, etc.

The key business and industry requirements relevant to Daydreams Travel Agency. We'll focus on travel industry standards, relevant legislation, and guidelines from Australian tourism associations.

**Travel Industry Standards and Guidelines**

* Australian Travel Industry Code of Conduct (ATIC): A voluntary code outlining ethical practices and consumer protection standards for travel agents and tour operators.
* Australian Consumer Law (ACL): Protects consumer rights, including fair trading, product safety, and guarantees on goods and services.
* Payment Card Industry Data Security Standard (PCI DSS): Essential for any business handling credit card information. Maintains strict security to protect cardholder data.
* General Data Protection Regulation (GDPR) – If Handling EU Traveler Data: Enforces data privacy and protection for individuals within the European Union. https://gdpr-info.eu/

**State and Commonwealth Legislation**

* Privacy Act 1988 (Cth): Governs the handling of personal information by businesses and government agencies.
* Corporations Act 2001 (Cth): Regulates companies, financial services, and markets in Australia.
* Relevant State Fair Trading Acts: Consumer protection laws, which can vary slightly between states. Daydreams will need to comply with Queensland legislation.

**Tourism Industry Associations**

* Tourism Australia: Provides resources, research, and marketing support for the tourism industry.
* Business Queensland: Offers information, guides, and support for businesses in Queensland.
* Australian Federation of Travel Agents (AFTA): Represents travel agents in Australia and provides industry resources and support.

1.3 Identify security options for the virtual network based on AWS tools. The table below will provide a basic framework for this task. Provide enough information that this table could be used as a guide for implementation of security tools.

|  |  |  |
| --- | --- | --- |
| Security tool | Applied to … | Comments |
| Amazon IAM (Identity and Access Management) | Users, groups, and roles within the AWS account | Granular permissions are vital. Implement least privilege principles, use MFA, and rotate access keys regularly. |
| AWS Security Groups | EC2 instances (virtual machines) | Act as virtual firewalls for instance. Allow only necessary traffic on specific ports and protocols. |
| AWS Network ACLs (Network Access Control Lists) | Subnets within the VPC | Provide an additional layer of security by controlling traffic at the subnet level (stateless filtering). |
| AWS VPC Flow Logs | VPC network traffic | Capture information about network traffic for monitoring, analysis, and troubleshooting security issues. |
| AWS KMS (Key Management Service) | Encryption keys for data at rest and in transit | Helps safeguard sensitive data using industry-standard encryption. Integrate with other AWS services (e.g., S3, EBS). |
| AWS CloudTrail | API calls and actions within the AWS account | Maintain an audit trail of all activity – invaluable for compliance and investigating security incidents. |
| AWS Config | AWS resource configurations | Monitor and track configuration changes. Helps ensure resources are compliant with security standards and identify potential vulnerabilities. |
| AWS Shield | Protection against DDoS attacks (Standard offered at no extra cost; Advanced provides more protection) | Critical for any publicly facing web services to mitigate disruptions. |

## Part 2 – Design and Configure the Virtual Network

2.1 List and describe the AWS tools, resources, gateways, and services required to build a multi-tier solution for the case study company. Use the table below as a framework. Use the third column to indicate the procedure or command you might use to achieve the implementation. You may add rows and columns as needed. Your completed table must address how you would use SSH and VPN to support the network.

|  |  |  |
| --- | --- | --- |
| Tools/Resources Gateways/Services | Applied to … | How will you implement |
| Amazon S3 (Simple Storage Service) | Will provide storage for all DTA operations in the local geographical area | Create S3 buckets. Set appropriate access policies and encryption options or AWS CLI (Command Line Interface). |
| Amazon VPC (Virtual Private Cloud) | Logically isolates Daydreams' network within AWS | Create a VPC using the AWS Management Console or AWS CLI (Command Line Interface). |
| Subnets | Divide the VPC into public, private | Create subnets within the VPC, associating them with specific Availability Zones (AZs). Configure appropriate CIDR blocks. |
| Internet Gateway | Allows internet connectivity for resources in public subnets | Create an Internet Gateway and attach it to the VPC. |
| Amazon EC2 (Elastic Compute Cloud) | Virtual machines to host web servers, application servers, database servers | Launch EC2 instances of inappropriate subnets based on their function. Choose suitable instance sizes based on workload. |
| AWS Security Groups | Instance-level firewalls to control inbound and outbound traffic | Configure security groups allowing only necessary traffic on specific ports. Apply to EC2 instances. |
| Route Tables | Define the paths that network traffic takes within the VPC | Create and configure route tables to direct traffic between subnets, to the Internet Gateway, and towards VPN connections. |
| Amazon RDS (Relational Database Service) | Managed database service (MySQL, PostgreSQL etc.) | Launch an RDS instance; select database engine, instance size, and storage. Configure security group access. |
| AWS IAM | Control and manage access to AWS resources | Define users, groups, and roles. Attach granular policies granting the least privilege access. |

2.2 Create a logical topology for your virtual network. Show your subnet scheme using the table below as a template. Add rows as needed.

|  |
| --- |
| **TOPOLOGY** |

|  |  |  |
| --- | --- | --- |
| Components requiring IP addresses (including instances and gateways) | IP address | Subnet mask |
| DayDreams-Web | 10.10.10.87 | 255.255.255.192 |
| Public Subnet | 10.10.10.0 | 255.255.255.192 |
| Private Subnet 1 | 10.10.10.64 | 255.255.255.192 |
| Private Subnet 2 | 10.10.10.128 | 255.255.255.192 |
| NAT Gateway | 10.10.10.248 | 255.255.255.192 |

‌

## Reference

ACCC (2018). *Consumer rights & guarantees*. [online] Australian Competition and Consumer Commission. Available at: <https://www.accc.gov.au/consumers/consumer-rights-guarantees>.

Amazon Web Services, Inc. (n.d.). *AWS Partner Network*. [online] Available at: <https://aws.amazon.com/partners/>.

Amazon Web Services, Inc. (n.d.). *AWS Well-Architected - Build secure, efficient, cloud enabled applications*. [online] Available at: <https://aws.amazon.com/architecture/well-architected/>.

Australian Travel Accreditation Scheme (ATAS) Code of Conduct. (2022). Available at: <https://www.atas.com.au/wp-content/uploads/2023/08/atas-code-of-conduct.pdf>.

Cloud Security Alliance. (n.d.). *Home*. [online] Available at: <https://cloudsecurityalliance.org/>.

PCI Security Standards Council (2019). *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. [online] Pcisecuritystandards.org. Available at: <https://www.pcisecuritystandards.org/>.