**Cyber Connexion Cohort 7**

**An AWS Simulated Hybrid Cloud Architecture with Site-to-Site VPN**

**Capstone Project Report**

Samprit Ghosh

Mojdeh Akhavan

Sangeeth Das Kallullathil

June 2023

**Table of Contents**

Introduction …..………………………………………………… 1

Zero Trust Architecture: Trust is a Vulnerability ……………… 2

Design of the Hybrid Cloud Architecture ……………………… 3

Security Features within the Zero Trust Maturity Model ……… 4

Vulnerability Management ……………………………..……… 6

Concluding Remarks ……………………………..…………...… 9

Supplementary Information …………………………………… 11

**1. Introduction**

This report outlines an imaginary business scenario: a software solution provider seeking to migrate to the cloud environment, specifically Amazon Web Services (AWS). The company requires both a production environment and a non-production (or development) environment. In the production environment, a website is needed for selling licenses/subscriptions, and a database is required for storing sensitive data, including customers’ personally identifiable information (PII) such as credit card information, address, phone number, birthday, and gender. The customers of this business access the website and provide login credentials. The non-production environment is intended for testing and development, requiring different operating systems. The business has also requested secure connectivity between their on-premises systems and the cloud environment, which includes a VPN connection.

When constructing a cybersecurity plan for a business, it is imperative to begin with the meticulous identification of the assets that necessitate protection. These assets encompass a wide range of valuable elements, including but not limited to highly sensitive data such as customer information and financial records, as well as critical systems like servers and networks. Moreover, given their ongoing software development endeavors, an equally crucial asset deserving protection is the repository of codes and systems within their development cloud environment. Safeguarding these intellectual properties (IP) not only fortifies their innovative endeavors but also ensures the smooth operation of their overall business operations.

In light of the digital transformation, cloud adoption, and remote/hybrid working, the conventional approach of granting trust to anyone or any system within the internal network is no longer secure enough for network and data protection. As a result, many companies are now turning to the **zero-trust architecture** (ZTA) as a reliable security plan, which has gained recognition as one of the industry's best practices. In the following sections, we will introduce the zero-trust architecture and then delve into the cloud infrastructure that we deployed. We will discuss the security measures we implemented to establish a secure hybrid cloud solution within the framework of a ZTA, addressing the specific business needs of this customer.

**2. Zero Trust Architecture: Trust is a Vulnerability**

Zero Trust is a comprehensive security framework that encompasses a range of ideas and concepts. It places emphasis on continuous verification and reassessment of trust for all subjects accessing network resources, regardless of their location or prior trust level. This proactive stance helps mitigate risks and provides a more robust security framework for the organization.

Within the context of ZTA, there are two critical components to consider: understanding and managing the attack surface and safeguarding the protect surface. Understanding the attack surface enables us to comprehend the potential entry points that attackers could exploit. By identifying these vulnerabilities, we can enhance our readiness and fortify our systems against potential threats using protective perimeter security tools like firewalls and intrusion protection systems. Conversely, the protect surface prioritizes the implementation of robust security measures to ensure the safety of the organization's *data, applications, assets,* and *services* (DAAS). This includes significantly reducing the attack surface and establishing a micro-perimeter with concise, comprehensible, and restricted policy statements.

As a core working principle, ZTA follows three fundamental concepts. Firstly, "*Never trust, always verify*" emphasizes the continuous verification of trust for every access request, regardless of the user's location or network connection. Secondly, "*Effective Context Collection and Analysis*" relies on analyzing various data points such as user behavior, device health, location, and time to detect any suspicious or anomalous activities that could indicate potential threats. Finally, "*Minimize Attack Impact*" aims to reduce the impact of attacks by implementing least-privilege principles, micro-segmentation, encryption of data in transit and at rest, and robust authentication mechanisms.

Considering our current compliance to the traditional security model, we acknowledge that the immediate adoption of ZTA is not feasible. We understand that transitioning towards zero trust is a gradual process that may take several years to fully implement. Therefore, our strategy involves introducing elements of zero trust into our infrastructure with a long-term objective in mind.

In the following section, we will present the design we have developed, carefully considering the business requirements and incorporating the necessary security measures. Our infrastructure is built upon a simulated hybrid-cloud environment hosted on AWS, with a strong emphasis on incorporating **Infrastructure as Code** (IaC) principles. Furthermore, we have implemented vulnerability management by utilizing both Tenable scanners and agents.

**3. Design of the Hybrid Cloud Architecture**

The infrastructure diagram depicted in Figure S1 displays the architecture constructed for this specific scenario. It includes three separate Virtual Private Clouds (VPCs).

The Production (Prod) VPC is a three-tier architecture within two availability zones, including a presentation (or Web) tier, a logic (or App) tier and a data tier. The presentation tier encompasses the essential components that facilitate direct user interactions, such as the e-Commerce website utilized by the business. The logic tier includes the vital codebase responsible for translating user actions into application functionality. On the other hand, the data tier serves as the storage medium that securely retains the pertinent data associated with the application. To ensure high availability, all compute and storage resources in this VPC are deployed across two availability zones. Additionally, **autoscaling groups** are utilized for the Web and App tiers to dynamically add or remove instances based on health checks or scaling policies, thereby maintaining availability, and improving cost management.

The Development (Non-Prod) VPC serves as a dedicated environment where the business can carry out comprehensive software testing, experimenting with various operating systems, and conducting critical debugging and troubleshooting operations. Finally, a "simulated" on-premises VPC has been implemented to act as a virtual representation of the business's physical office space. This VPC hosts a VPN gateway that enables the establishment of **site-to-site VPN** connections between the on-premises infrastructure and the cloud environment, ensuring seamless and secure communication between the two.

We have used **Terraform** for deploying most parts of the cloud infrastructure on AWS. Terraform provides infrastructure as code (IaC) capabilities, enabling the management and provisioning of AWS resources using declarative code. This allows for efficient and consistent deployments, eliminating manual and error-prone processes. Additionally, Terraform offers a wide range of AWS provider resources, enabling the creation and management of various AWS services and configurations. Its modular and reusable code structure promotes scalability and ease of maintenance.

**4. Security Features within the Zero Trust Maturity Model**

In this section, we will elaborate on the safeguards implemented in the simulated hybrid-cloud environment. Our approach is based on the CISA's Zero Trust Maturity Model (ZTMM), which aligns with the seven fundamental tenets of ZTA outlined in NIST SP 800-207. This model encompasses five core pillars: *Identity, Devices, Networks, Applications,* and *Data*. Additionally, it incorporates three overarching capabilities: Visibility and Analysis, Automation and Orchestration, and Governance. We will delve into the safeguards implemented within each of these areas to ensure the confidentiality, integrity, and availability (the CIA triad) for systems, applications and data.

*4.1. Identity*

The identity pillar serves as a crucial component within the Zero Trust Maturity Model, focusing on the verification and management of the identities of all users and entities accessing the network.

To effectively implement this, we leverage robust identity and access management (**IAM**) tools on AWS. These tools enable us to manage access controls for users, groups, and roles, ensuring that only authorized individuals and devices are granted access to specific resources, adhering to the principle of least privilege. In order to safeguard the root AWS account, we activate multi-factor authentication (**MFA**), providing an additional layer of security to verify user identities. Furthermore, we create administrator users for daily admin tasks, while also ensuring that non-root users are protected with MFA.

To facilitate programmatic access to AWS from Terraform, we generate unique and short-term access keys on AWS for authorized users. This eliminates the need to share passwords or access keys with other users, enhancing security. Additionally, we utilize **AWS CloudTrail** to monitor user activities and validate the effectiveness of our protection measures. This enables us to maintain compliance auditability, track resource changes, and facilitate troubleshooting.

*4.2. Devices*

The devices pillar is an integral aspect of the Zero Trust Maturity Model (ZTMM), focusing on securing and managing the devices that access the network. In the context of cloud environments, these devices encompass various resources, including compute resources like EC2 instances, storage resources such as EBS volumes, platform assets like databases and web servers, and network resources like VPCs, VPNs, and gateways.

To enhance the security of our cloud resources, we have implemented multiple layers of security in a **defense-in-depth** approach. A key aspect of our security strategy is the establishment of logically isolated private subnets for all sensitive cloud devices, including EC2 and database instances. By ensuring these subnets have no public internet access, we achieve micro-segmentation and maintain granular and controlled access to resources.

To facilitate secure SSH access to EC2 instances in private subnets, we employ bastion hosts deployed in the public subnets of the production VPC. By utilizing these bastion hosts, we establish a secure mechanism for managing and accessing the private EC2 instances through unique RSA-4096 key pairs, adding an additional layer of protection against unauthorized access.

*4.3. Networks*

The network pillar of ZTMM focuses on the security and management of the network infrastructure. Within this pillar, we leverage **advanced network segmentation** techniques to create isolated security zones, implementing strict access controls and network policies that govern traffic flow and minimize lateral movement. Network access control lists control both the incoming and outgoing traffic at the subnet level. Additionally, security groups are used to control access at the instance level, as well as the application load balancers that control the traffic between different subnets within the production VPC. Application load balancers provide a single point of contact for clients and simplify and improve the security of applications by ensuring that the latest SSL and TLS ciphers and protocols are used at all times.

To enable connectivity for instances in private subnets, we utilize NAT gateways. These gateways allow the instances to connect to the internet and other AWS services, while preventing incoming connections from the internet. This further strengthens the security posture of our infrastructure by minimizing the exposure of internal resources to potential threats.

*4.4. Applications*

Another vital element of the ZTMM is securing and managing the applications that reside within the network. To ensure the security and integrity of applications, we implement strong authentication and authorization mechanisms, ensuring that only authorized users have access to the applications and their respective functionalities within both production and non-production VPCs. Security measures are enforced to prevent communication between the production and non-production environments. Updating and patching is another measure to address any security vulnerabilities or bugs that may arise. By adopting a comprehensive approach to securing our applications, we bolster their resilience, protect intellectual properties of software developers, and maintain a secure environment for users and systems.

*4.5. Data*

The last pillar concentrates on securing and managing the organization's data assets. To ensure the confidentiality, integrity, and availability of the data, we implement robust measures and best practices. We employ **encryption** techniques, both **at rest** (using unique AWS KMS[[1]](#footnote-1) keys for EBS volumes connected to instances and the database) and in transit (using VPN connection), to protect the data from unauthorized access or interception.

Within the production VPC, the data tier is strategically located in a private subnet, along with a read-only replica in another availability zone. The read replica provides high availability, data durability and fault tolerance. The App tier is the only component allowed to access the data tier, and it does so by using specific credentials. We utilize AWS Secrets Manager to securely store and retrieve this username and password.

By adhering to data security measures, we safeguard the organization's valuable information, maintain compliance, and instill trust in stakeholders regarding the handling of their data.

**5. Vulnerability Management**

Vulnerability management is integral to computer and network security, especially in a zero-trust framework. A good vulnerability management tool identifies security vulnerabilities and evaluates the risks involved. The evaluations then lead to remediation or acceptance of risks by an organization. Vulnerability management is a continuous process, the easiest way to describe it is through the following diagram of a vulnerability management life cycle. We first prepare and get an accurate account of assets; we then perform necessary scans and identify the vulnerabilities. The next step is to analyze them and prioritize on which vulnerabilities should be addressed first. We write a detailed report and remediate or accept the vulnerabilities based on the report. (The statistics below on the right are from a study conducted by IBM.[[2]](#footnote-2) )

A diagram of a life cycle

Description automatically generated with medium confidence A screenshot of a cell phone

Description automatically generated with low confidence

For our project, doing comprehensive scans of the entire architecture is beyond the scope, however, we implemented some basic scans using sophisticated vulnerability management tools. This was achieved through [tenable.io](https://cloud.tenable.com/). We used both, Nessus Agent and Nessus Scanner.

**Nessus Agents** have the benefit that they do not have to manage credentials, since the Agent runs on the target device. It can collect the local vulnerability data at high frequency. The downside is that we are only looking at the vulnerabilities from the inside out view of the device.

**Nessus Scanners** have the benefit that they will scan the whole network and find anything that is on the network, the Scanner will see all the vulnerabilities from the outside in view, plus if we provide credentials, they will be able to login to the device and see the vulnerabilities from inside out view as well. The downside is that now we must manage credentials, permission and failed login issues. Another downside is that we will not be able to have such a high frequency scanning schedule as it will be impacting the network.

That’s why Tenable recommends a combination of agents and scanners to ensure full visibility into the entire network.

Tenable also has an interactive and graphical vulnerability management dashboard that provides at-a-glance view of the key performance indicators relevant to a particular objective.

We have installed Nessus Agents on the Web and App tier EC2 instances of the Prod VPC and have performed a ***Basic Agent Scan*** on these. Whereas we installed a Nessus Scanner on EC2 of the On-prem VPC. Using this scanner, we were able to perform a ***Basic Network Scan*** and a ***Host Discovery Scan*** targeting the EC2 instances on the Non-Prod VPC. [[3]](#footnote-3)

We present a short report of our findings below. Note that, tenable uses the following severity indicators based on the respective CVSSv3 scores:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Severity | Info | Low | Medium | High | Critical |
| Scores | 0 | 0.1 – 3.9 | 4.0 – 6.9 | 7.0 – 8.9 | 9.0 – 10.0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Scans | Info | Low | Medium | High | Critical |
| Basic Agent Scan | 128 | 0 | 0 | 0 | 0 |
| Host Discovery Scan | 24 | 0 | 0 | 0 | 0 |
| Basic Network Scan | 140 | 0 | 5 | 0 | 0 |

*Basic Agent Scan*

Note that all the vulnerabilities revealed through this scan are of info level severity. Some examples: Nessus was able to enumerate the open ports, identify the OS, enumerate IP address assignment method (static/dynamic), enumerate AWS Web Services EC2 instance metadata etc.

*Host Discovery Scan*

Note that all the vulnerabilities revealed through this scan are also of info level severity. There were only two types of vulnerabilities detected namely, Nessus was able to ping the remote hosts and was able to have information about the scan itself, e.g., type of scanner, Nessus engine version, date and duration of the scan etc.

*Basic Network Scan*

This scan reveals two important types of vulnerabilities which are of medium level severity:

1. The remote web server supports Trace and/or Track methods. (These are HTTP methods that are used to debug web server connections)
2. The server’s SSL certificate cannot be trusted.

Note that (1) can be resolved by disabling these HTTP methods, whereas (2) can be resolved by purchasing a proper SSL certificate.

**Concluding Remarks**

In conclusion, this report discussed the implementation of a secure hybrid cloud solution based on the principles of the zero-trust architecture (ZTA) for an imaginary software solution provider migrating to Amazon Web Services (AWS). It presented the design of the hybrid cloud architecture, including separate VPCs for production and development environments, as well as a simulated on-premises VPC for secure connectivity. The use of Infrastructure as Code (IaC) principles, specifically with Terraform, was mentioned for efficient and consistent deployments. Additionally, security features within the zero-trust maturity model were discussed, focusing on identity, devices, networks, applications, and data. Measures such as robust identity and access management, principle of lease privilege and defense in depth, logically isolated private subnets, network segmentation, and encryption of data were implemented to ensure the confidentiality, integrity, and availability of systems, applications, and data.

In order to further enhance the security and efficiency of the hybrid cloud environment, several future improvements can be considered:

Firstly, implementing SSL certificates for HTTPS is essential to protect data in transit. By ensuring that all web traffic is encrypted, sensitive information is safeguarded from potential eavesdropping or interception.

Secondly, replacing the use of a bastion host with AWS Session Manager offers a more secure and streamlined approach to managing and accessing instances. This eliminates the need for direct SSH access to instances and provides enhanced control and auditing capabilities.

Creating web servers in private subnets and utilizing a proxy server in public subnets can enhance security by reducing the attack surface. This approach restricts direct access to web servers and allows for more granular control over incoming traffic.

Consideration can be given to implementing SASE/SSE zero-trust solutions instead of a traditional VPN. This approach combines secure access service edge (SASE) and secure service edge (SSE) principles, providing a comprehensive and efficient security solution for network access and data protection.

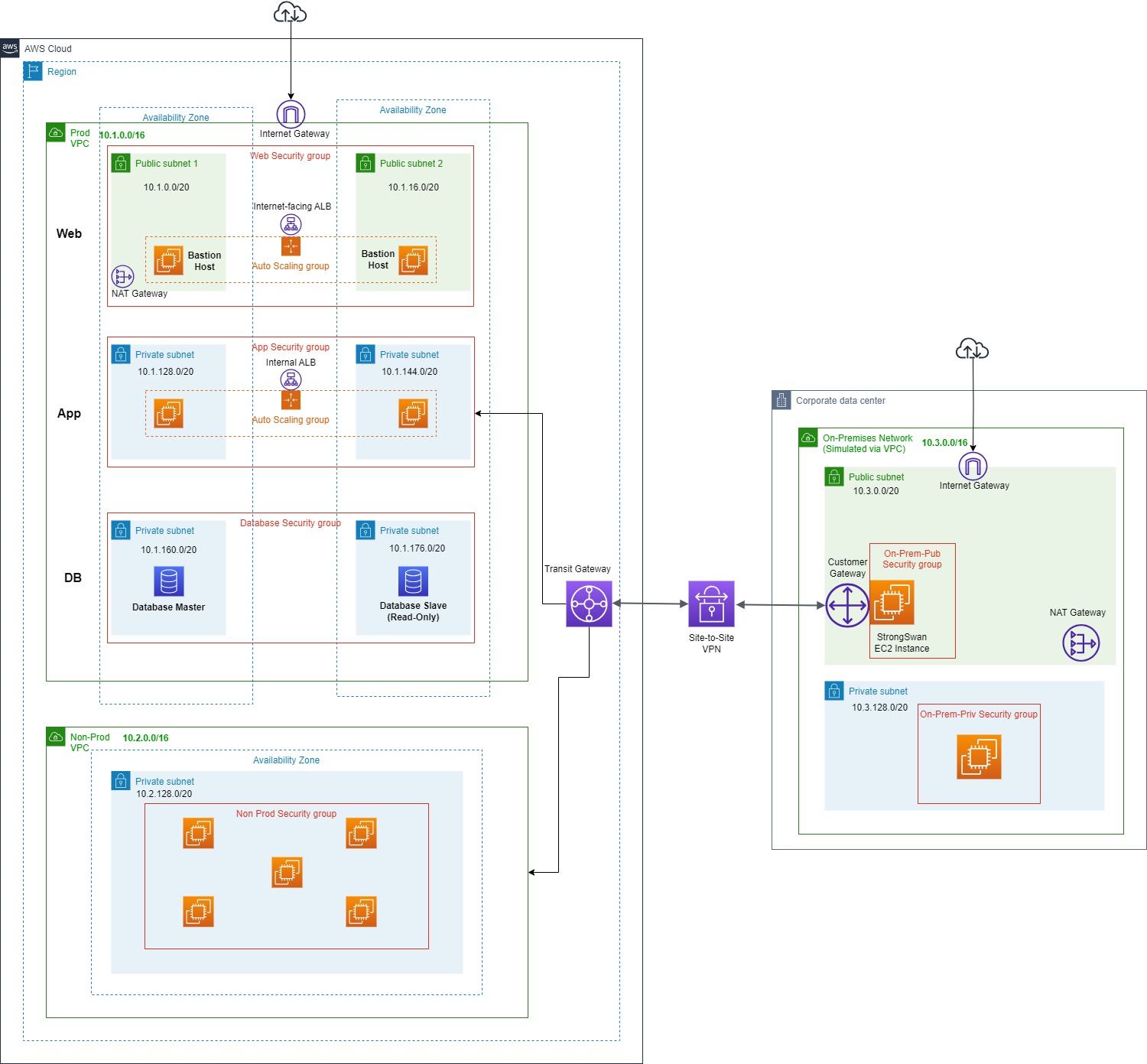
Utilizing a web application firewall (WAF) adds an additional layer of protection to the production environment. A WAF can detect and mitigate various web-based attacks, such as SQL injection and cross-site scripting, safeguarding the web servers and applications from potential vulnerabilities.

Implementing Tenable Credentialed Scans enhances vulnerability management by conducting authenticated scans that provide deeper insights into the security posture of the infrastructure. This approach helps identify and remediate potential vulnerabilities before they can be exploited.

Lastly, establishing a robust incident response plan and implementing notifications for security events can improve the organization's ability to detect, respond to, and recover from security incidents promptly. This proactive approach helps minimize the impact of potential breaches and ensures timely remediation.

By considering these future improvements, the hybrid cloud environment can be fortified with additional layers of security, resilience, and efficiency, aligning with industry best practices and safeguarding the organization's assets and operations.

**Supplementary Information**



**Figure S1.** The simulated hybrid-cloud architecture deployed on AWS, featuring three VPCs.

A picture containing text, screenshot, diagram, plan

Description automatically generated

**Figure S2.** Nessus Scanners, Agents and Targets for the vulnerability management scans.

1. Key Management Service [↑](#footnote-ref-1)
2. *The state of vulnerability management in the cloud and on-premises*, independently conducted by Ponemon Institute LLC, IBM, August 2020 [↑](#footnote-ref-2)
3. See Figure S2 for a graphical view. [↑](#footnote-ref-3)