Version 1.0.0

Network Diagram

November 9, 2022

Issued by:

Algorithmic Alchemist

Team Lead

Sierra Harris

Team Members

Bryant Lam

Abhay Solanki

Faisal Al Muharrami

David Chan

Github: https://github.com/abhay772/AA_Senior_Project/

Version History

Version #	Date	Reason for Change
Version 1.0.0	11/9/2022	Original Document

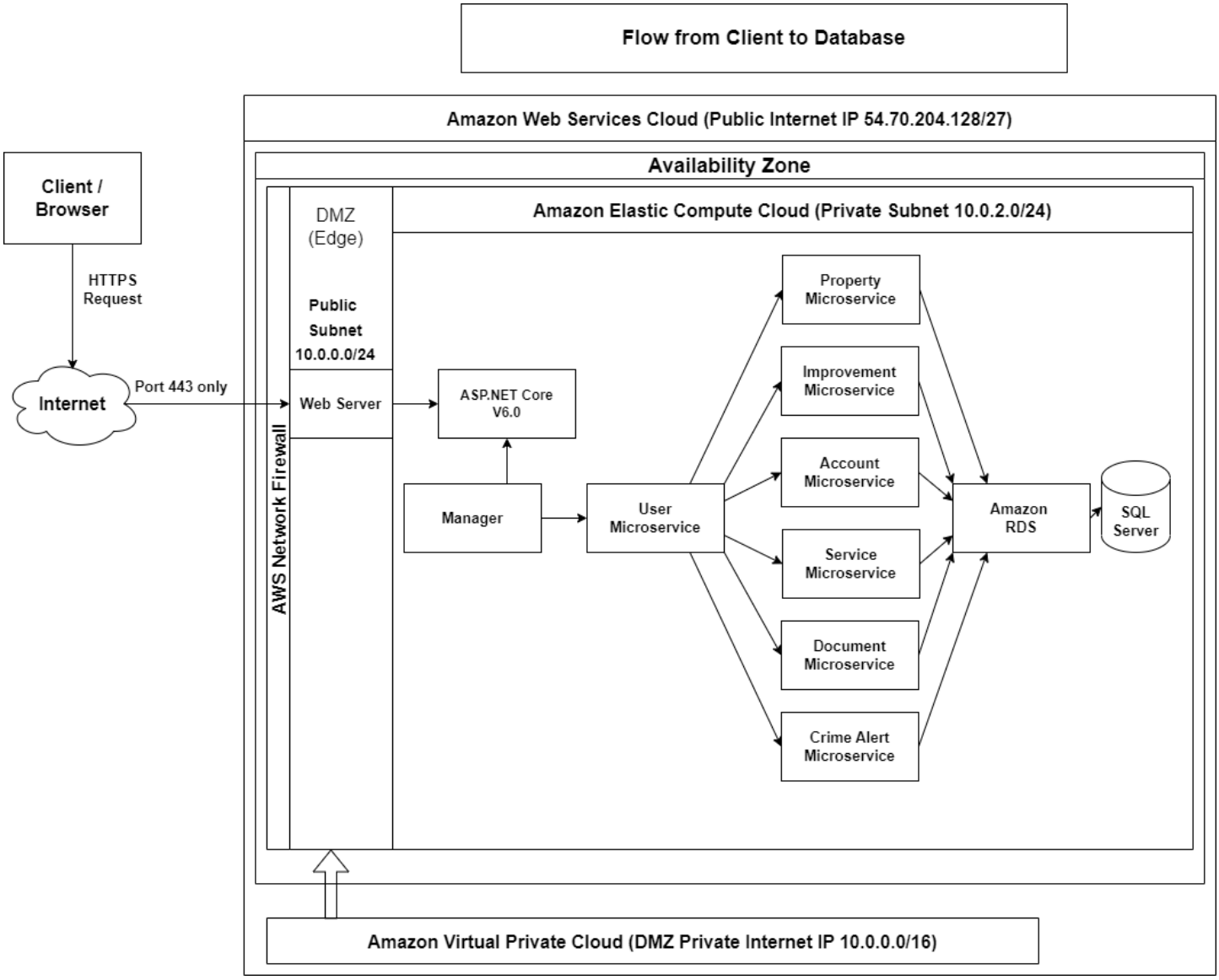
Table of Contents

Overview

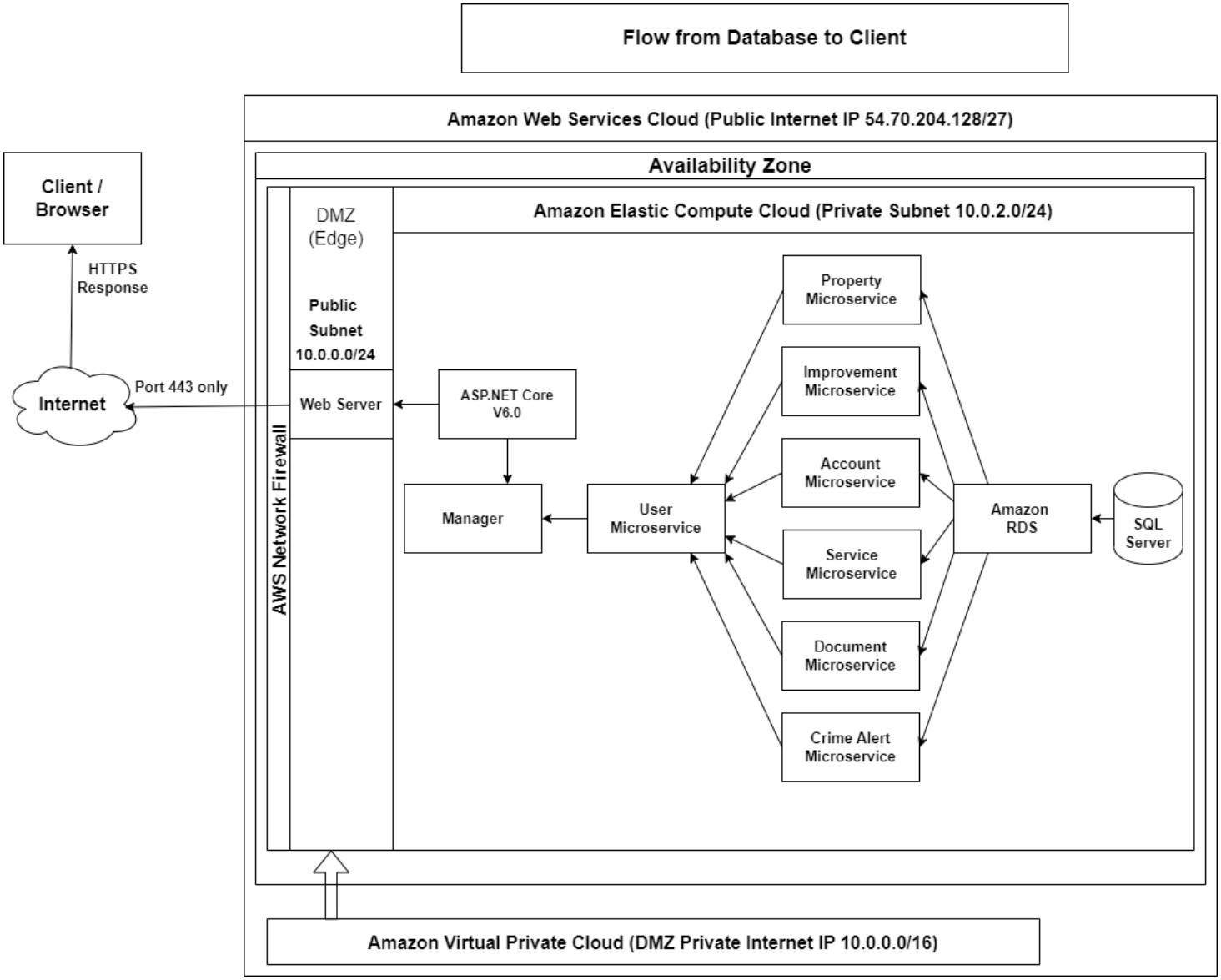
Our application will be using Amazon Web Services (AWS) to host our application to the internet. Since we will be using a microservice architecture for our application we will be separating each microservice to different ports. We will also be using HTTPS and SSL to be more secure.

The datastore will be using Microsoft SQL Server which is supported by Amazon Relational Database Services (Amazon RDS). The application will run within a single instance of EC2 that is within a VPC. The client will interact with the web server within the DMZ which then sends the request to be handled by ASP.NET Core V6.0. Then it will be sent to the manager which will handle the flow to the Datastore made with SQL Server.

Diagrams


Flow from Client to Database
Amazon Web Services Cloud (Public Internet IP 54.70.204.128/27)
Availability Zone
Client / Browser
HTTPS Request
Internet
Port 443 only
AWS Network Firewall
DMZ (Edge)
Public Subnet 10.0.0.0/24
Web Server
Amazon Elastic Compute Cloud (Private Subnet 10.0.2.0/24)
ASP.NET Core V6.0
Manager
User Microservice
Property Microservice
Improvement Microservice
Account Microservice
Service Microservice
Document Microservice
Crime Alert Microservice
Amazon RDS
SQL Server
Amazon Virtual Private Cloud (DMZ Private Internet IP 10.0.0.0/16)

Diagrams


Flow from Database to Client
Amazon Web Services Cloud (Public Internet IP 54.70.204.128/27)
Availability Zone
Client / Browser
HTTPS Response
Internet
Port 443 only
DMZ (Edge)
Public Subnet 10.0.0.0/24
Web Server
AWS Network Firewall
Amazon Elastic Compute Cloud (Private Subnet 10.0.2.0/24)
ASP.NET Core V6.0
Manager
User Microservice
Property Microservice
Improvement Microservice
Account Microservice
Service Microservice
Document Microservice
Crime Alert Microservice
Amazon RDS
SQL Server
Amazon Virtual Private Cloud (DMZ Private Internet IP 10.0.0.0/16)

Network

Amazon Web Services:

We chose to use Amazon Web Service (AWS) mainly due to it being the most used industry standard for cloud computing and free to use if using the “Free Tier” which includes 750 hours of windows t2.micro instances and 5 GB storage each month for 1 year. AWS also have Amazon Elastic Compute Cloud (Amazon EC2) which is

Amazon AWS also contains datastore services that can assist in microservices like Amazon ElastiCache service which puts a cache between application servers and a database to reduce load on databases.

The AWS IP we will be using is 54.70.204.128/27 which is the IP address range of Amazon’s Oregon us-west-2 servers because it is cheaper and closer to avoid any delays from traveling between servers.

Microservices:

The application will keep each microservice separate by restricting each microservice to different unique ports on the same machine. We will be restricted by cost so everything must be run on a single instance of Amazon EC2. The expected traffic and usage will be low so there will be no need for the ability to handle large loads. It will also have a single point of failure because if the server crashes then the entire application crashes also. The advantages are that it will be lightweight, convenient, and easy for troubleshooting since everything will be in a single instance of EC2.

Ports:

The ports incoming into the DMZ’s firewalls will be restricted to port 443 for inbound and outbound due to the fact that 443 is the assigned port for HTTPS. This will ensure that the application will not receive any requests that are not encrypted to assist in defending against man in the middle attacks. We will also restrict ports using the Amazon Security Groups and change the default port range for inbound and outbound to increase security.

Microservices will be isolated by separating the services by restricting them to unique ports.

- User Microservice will be any port for inbound and outbound so that it would be able to communicate with all the other microservices.
- Property Microservice will be port 8001 for inbound and any port for outbound.
- Improvement Microservice will be port 8002 for inbound and any port for outbound.

- Account Microservice will be port 8003 for inbound and any port for outbound.
- Service Microservice will be port 8004 for inbound and any port for outbound.
- Document microservice will be port 8005 for inbound and any port for outbound.
- Crime Alert Microservice will be port 8006 for inbound and any port for outbound.
- Amazon RDS and SQL Server will allow any port for inbound and will be restricted to port 443 for outbound so that it will have all data leaving the datastore be encrypted.

Load Balancers:

Our application most likely will not be expected to reach anywhere near 10,000 users so it would not make sense to include one due to financial restrictions. In the future if the application is able to reach close to 8,000 ,which is 80 percent of 10,000 users, then we would add a load balancer into the DMZ and move the web server inside the EC2. The load balancer will be connected to a web farm containing multiple duplicate servers running duplicate applications. The load balancer balancing system we would use is the “least connections” system so it would send all the new requests to the server that currently has the least amount of users connected. The load balancer would also send head request every 60 second

ASP.NET Core v6.0:

Microsoft’s ASP.NET Core v6.0 will be used to handle the HTTPS request between the webserver and the manager. It will be used to set HTTPS protocols and commands to set a browser to server bilateral communication and cooperation for the web application.

Microsoft SQL Server:

We chose Microsoft SQL Server because it is free and easily allows us to integrate data into applications using a wide set of cognitive services and tools aimed at data management and analysis. It also has data encryption features built in to assist in securing data. It is a relational database that uses multiple interconnected tables to store and organize data correctly.

Security

VPC:

The application will use a Virtual Private Container to have a private space within the public cloud owned by AWS. Only certain parts of the application will need to have access to the internet so by creating a private network it allows us to limit and control what parts have internet access. By limiting access we can defend those chokepoints with firewalls to increase security.

To set up the VPC we will create an amazon web service account, create an elastic IP address, and confirm the number of VPC which will be only 1. Next we will set up the Availability Zone along with the VPC CIDR with the default 10.0.0.0/16.

Public subnet configuration will be setting the public subnet CIDR at 10.0.0.0/24. The private subnet configuration will be setting the private subnet CIDER at 10.0.2.0/24. Then we will set the NAT configuration with the Elastic IP Address Allocation ID.

HTTPS:

We will be using HTTPS which will encrypt the data sent to prevent a man in the middle attack. The port restrictions on our firewall will only allow port: 443. We will be getting a TLS 1.2 certificate using AWS.

Firewalls:

Our firewall will be only allowing port: 443 through to make sure all requests will be encrypted through HTTPS. It will only allow requests from California since that is our only supported area of service. The firewall we will be using is AWS Network Firewall and we will be managing it along with Security groups to configure a common baseline of security rules and if we add new resources it will automatically add protection to the new resource added to the account. AWS Network Firewall does add a cost that is $0.395/hr to keep up and $0.065/GB for data which we are willing to pay.

DMZ:

The demilitarized zone (DMZ) will be using a web server subnet behind a firewall to add further security to the network. It will be the outward facing public access point used to filter out malicious users. This will allow the application to have a secure access point while keeping the rest of the application in a completely private inaccessible network. Usually there would be a load balancer included inside the DMZ but our application does not currently have one due to funding and needs.

Our system will be using Amazon Virtual Private Container (VPC) to set up a private internet space to act as the DMZ Edge. The firewall that will be used is AWS Network Firewall which will be used to define rules and policies like to filter inbound and outbound traffic.

Glossary

Microservice	It is separating services into smaller individual parts so that it could be easily expanded and work faster.
Firewall	It is used to block unwanted inbound and outbound traffic of a system to prevent malicious users.
Load Balancer	A tool used to distribute traffic loads to multiple different points to avoid traffic congestion.
CIDR	It stands for classless inter-domain routing for allocating IP addresses for IP routing.
NAT	It stands for network address translation for mapping an IP address space.
Port	It is a number assigned to uniquely identify a connection endpoint and to direct data to a specific service.
IP	It is Internet Protocol which is a unique address to send data over the internet.
Subnet	It is a network inside a network where traffic can be routed to separate locations inside a single network.

References

Free Cloud Computing Services - AWS Free Tier. (n.d.). Amazon Web Services, Inc. Retrieved October 17, 2022, from https://aws.amazon.com/free/?all-free-tier.sort-by=item.additionalFields.SortRank

AWS Whitepaper. (n.d.). Implementing Microservices on AWS. Amazon.com. Retrieved October 17, 2022, from https://docs.aws.amazon.com/pdfs/whitepapers/latest/microservices-on-aws/microservices-on-aws.pdf#simple-microservices-architecture-on-aws

Fernandez, T., & Ackerson, D. (2022, July 14). 5 Options for Deploying Microservices. Semaphore. https://semaphoreci.com/blog/deploy-microservices

ASP.NET - Introduction. (n.d.). Retrieved October 25, 2022, from https://www.tutorialspoint.com/asp.net/asp.net_introduction.htm

Wikipedia contributors. (2022, August 28). DMZ (computing). Wikipedia. https://en.wikipedia.org/wiki/DMZ_(computing)

Bellasio, S. (2019, July 11). Amazon VPC: 5 Reasons to Use and Learn it Cloud Academy. https://cloudacademy.com/blog/how-and-why-to-use-vpc-for-your-amazon-aws-infrastructure/

What is Microsoft SQL Server and what is it for? (n.d.). Intelequia. Retrieved October 25, 2022, from https://intelequia.com/en/blog/post/2948/what-is-microsoft-sql-server-and-what-is-it-for

Create an Amazon VPC with a DMZ architecture using CloudFormation—ArcGIS Enterprise in the cloud | Documentation for ArcGIS Enterprise. (n.d.). https://enterprise.arcgis.com/en/server/latest/cloud/amazon/cf-vpc-dmz.htm

Managed Network Firewall – AWS Network Firewall – Amazon Web Services. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/network-firewall/

AWS Regions, websites, IP address ranges, and endpoints - Amazon QuickSight. (n.d.). https://docs.aws.amazon.com/quicksight/latest/user/regions.html

create-nat-gateway — AWS CLI 1.27.5 Command Reference. (n.d.). https://docs.aws.amazon.com/cli/latest/reference/ec2/create-nat-gateway.html

Wikipedia contributors. (2022, November 9). List of TCP and UDP port numbers. Wikipedia. https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Control traffic to resources using security groups - Amazon Virtual Private Cloud. (n.d.). https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

NGINX, Inc. (2022, January 3). What Is Load Balancing? How Load Balancers Work. NGINX. https://www.nginx.com/resources/glossary/load-balancing/

Wikipedia contributors. (2022a, November 9). Classless Inter-Domain Routing. Wikipedia. https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

Wikipedia contributors. (2022c, November 9). Network address translation. Wikipedia. https://en.wikipedia.org/wiki/Network_address_translation

Wikipedia contributors. (2022a, September 8). Port (computer networking). Wikipedia. https://en.wikipedia.org/wiki/Port_(computer_networking)

What is a subnet? | How subnetting works. (n.d.). Cloudflare. Retrieved November 9, 2022, from https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/