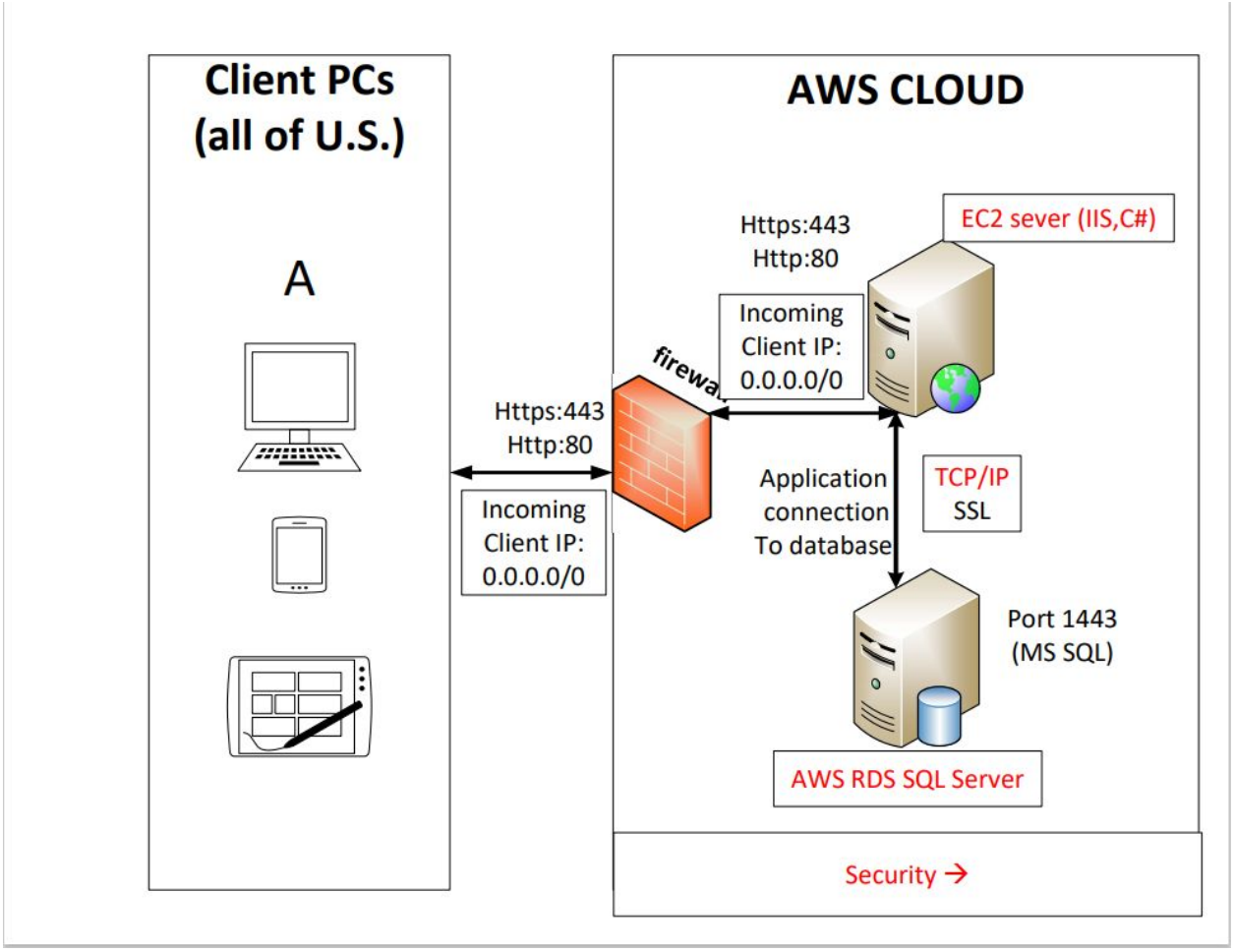
Network flow diagram.



Technologies represented in the network diagram:

AWS Cloud services used.

- EC2 server
- RDS server
-

Protocol that are used (based on our business requirements):

- SSL/ TLS - an encrypted protocol used over a connection. Used to encrypt all traffic, in the form of a SSL certificate.
- HTTP/ HTTPs : HTTP:hypertext transfer protocol This protocol is used by sites.
- TCP/IP: the standard which allows computers to communicate, it established a connection between the two.

Security measures to be decided. (such as security groups)

Understanding the flow of the network diagram:

The defined scope of audience for this web application is clients within the United States, this is where requests will be generated from. The start of traffic flow is when client ‘A’ sends a URL request, in our case a HTTP request, to the application server. Now the request is captured (or handled) by the firewall that evaluates (or filters) requests that meet firewall rules. These rules will be applied on both incoming traffic (inbound) and outbound traffic. In our case the firewall will allow HTTP and HTTPs access from clients (typically any IP address depicted by: 0.0.0.0/0).[CIT-001][CIT-007]
If the request is granted access then trafic will continue to the EC2 Web Server, which is listening on ports 80 (HTTP) and 443 (HTTPS). [CIT-005]
Now this request will be processed by the web application server, which is hosting IIS, to return a ‘Static’ web content or runs the C# program to generate the ‘dynamic’ content per users request. [CIT-005]
This EC2 server will have a connection to the database server, which it has to communicate to. In our case this connection will be with amazon's RDS server. This connection to the database will be made by the application on a TCP/IP connection with SSL encryption of data traffic. [CIT-004] [CIT-008][CIT-010]
When the web server (EC2 server) finishes processing the request, the web content generated is returned to the firewall that forwards the traffic to the client as a http/ https request AKA client A’s browser.

All references:

Security group rules reference
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/security-group-rules-reference.html#sg-rules-local-access [CIT-001]

Walk through of the network diagram
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/security-group-rules-reference.html#sg-rules-web-server [CIT-002]

AWS Managed Microsoft AD
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html [CIT-003]

Reviewing my protocols:
What is SSL, TLS? And how this encryption protocol works
https://www.csoonline.com/article/3246212/what-is-ssl-tls-and-how-this-encryption-protocol-works.html [CIT-004]

Cloud customer Architecture for web application hosting, Version 2.0
https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-Web-Application-Hosting.pdf [CIT-005]

MySQl on Amazon RDS
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_MySQL.html
[CIT-006]

Secure Your Network with Amazon VPC Security Learning Objective
https://trailhead.salesforce.com/en/content/learn/modules/aws-networking/secure-your-network-with-amazon-vpc-security [CIT-007]

SQL Server network configuration
https://www.sqlshack.com/sql-server-network-configuration/ [CIT-008]

Configure the Windows Firewall to Allow SQL Server Access
https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver15 [CIT-009]

Security group rules reference
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/security-group-rules-reference.html#sg-rules-web-server [CIT-010]