WAF Implementation for ULURN

About Customer: ULURN

Ulurn is an educational portal with a vision to provide aspiring financial professional students with comprehensive study guides and training materials, both online and offline, to ensure they shine brightly in their chosen career path. Ulurn team has some of the best-certified faculties with a sound understanding of the subjects they offer, who are constantly coming up with tested and continuously upgraded study materials. We are constantly striving to make education accessible for all!

Ulurn provide easily accessible study materials to students pursuing financial professional courses for easy understanding and comprehension. To ensure that the students opting for online courses can prepare for the tough exams in their chosen career thoroughly they deliver their study materials directly at their doorstep. Ulurn also run mock tests for various exams so that students gain confidence in their ability to clear the exams with ease. They are confident that the study guides they offer for a comprehensive preparation for the examinations will help students secure a place on top of the success pyramid.

Customer Challenge

Ulurn was facing challenges to protect their content (video tutorials) from illegitimate users, and identify the specific problem statements which are described below -

1. Initially there was no authentication/authorization mechanism in Ulurn to identify legitimate user – so unauthorized users were able to download videos just by directly hitting to the URL. Because of this lots of unnecessary traffic slow down the server.

2. Ulurn also facing activities like - from few clients/IPs send a large number of SYN packets, but never send the final ACK packets to complete the handshakes. The server is left waiting for a response to the half-open TCP connections and eventually runs out of capacity to accept new TCP connections.

3. Ulurn also detect their video contents had been accessed from some backlisted countries. Though the users were authorized but the purpose of accessing video tutorials had some malicious purpose like piracy and so. This causing Ulurn reputation harm in severe manner which they were never wanted.

Solution Approach

1. To protect the video content from unauthorized access a token is generated from WAF (integrated with CloudFront) and appended with the signed URL of video content, so only legitimate users can access the link. Anybody other than authorized users if trying to access the link the WAF Query-String rule will block the access due to absence of the specific token defined in Query-String Rule.

2. Enable the firewall to detect and filter the SYN packets. While modern operating systems are better equipped to manage resources, which makes it more difficult to overflow connection tables, servers are still vulnerable to SYN flood attacks.

   There are a number of techniques have been adopted to mitigate SYN flood attacks, which mainly rely on the target network's ability to handle large-scale volumetric DDoS attacks, with traffic volumes measured in tens of Gigabits (and even hundreds of Gigabits) per second.

   Micro blocks—administrators can allocate a micro-record (as few as 16 bytes) in the server memory for each incoming SYN request instead of a complete connection object.

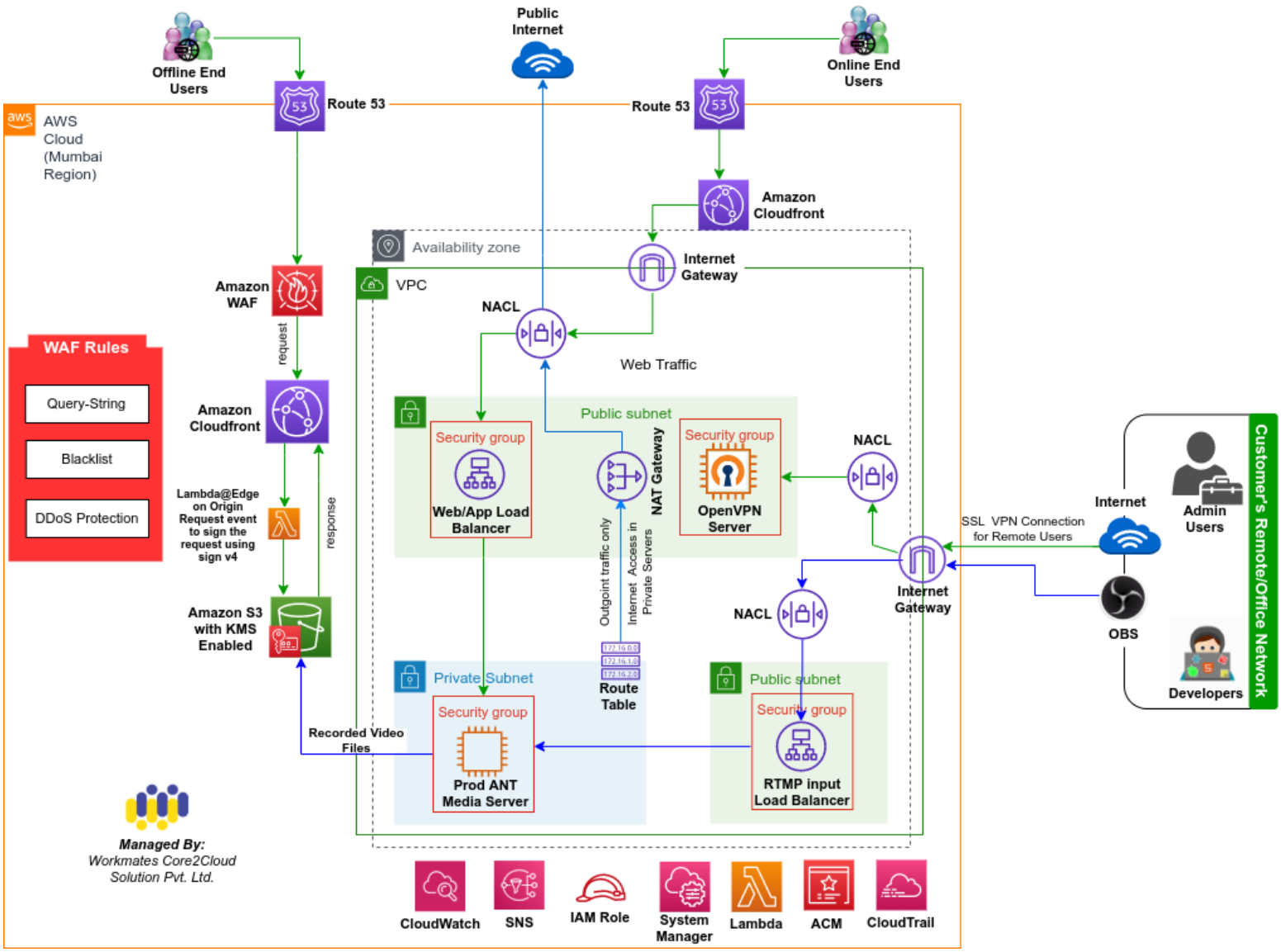
   SYN cookies—using cryptographic hashing, the server sends its SYN-ACK response with a sequence number (seq-no) that is constructed from the client IP address, port number, and possibly other unique identifying information. When the client responds, this hash is included in the ACK packet. The server verifies the ACK, and only then allocates memory for the connection.

   RST cookies—for the first request from a given client, the server intentionally sends an invalid SYN-ACK. This should result in the client generating an RST packet, which tells the server something is wrong. If this is received, the server knows the request is legitimate, logs the client, and accepts subsequent incoming connections from it.

   Stack tweaking—administrators can tweak TCP stacks to mitigate the effect of SYN floods. This can either involve reducing the timeout until a stack frees memory allocated to a connection, or selectively dropping incoming connections.

3. To protect the video content accessing from embargoed countries we noted backlisted IP ranges from OFAC sanctioned countries. We create a WAF Stack for this Black-Listed IP ranges in Web-ACL which works for both IPv4 and IPv6 address type.

Solution Architecture



Key AWS Services Used

CloudFront, S3, WAF, Lambda, ALB, IAM, SNS etc.

Results and Benefits

- After implementing Query-String rules in WAF, Ulurn account now completely eliminate the possibility of unauthorized user access thus saving the unwanted traffic which previously put unnecessary load on the

server causing extra penny to lose for nothing.

- Benefits are multifold when the DDOS protection from WAF is enabled – which helps Ulurn account to rightfully identify the spoofer and blocking them from IP spoofing thus saving Ulurn account from exploiting. Also, it helps from unnecessary exploitation of TCP connections pool resulting legitimate users can now connect the application in time without any hassle.

- Nowadays piracy is the major challenge in all sector and learning portal like Ulurn was also a victim of this kind of malicious activity. But after implanting WAF rule for the Black-listed IPs it can now block all type of access from OFAC sanctioned countries and help Ulurn account to save their learning tutorial being pirated.

About Workmates

Workmates core2cloud Solution Pvt. Ltd is an AWS Advance consulting partner and Leading Cloud Management Company in Eastern India. Workmates Core2cloud is a cloud managed services company focused on AWS services, the fastest growing AWS Advanced Consulting Partner in India. We focus on Managed services, Cloud Migration and Implementation of various value-added services on the cloud including but not limited to Cyber Security and Analytics. Our skills cut across various workloads like Microsoft, SAP, Media Solutions, E-commerce, Analytics, IOT, Machine Learning, VR, AR etc. Our VR services are transforming many businesses.
Workmates has a yellow theme which is the color of youth. Our Vibrant team of 100% certified resources brings the edge to customers for an End-to-End AWS partner, committed towards quality and supporting their business on a 24X7 basis.