

HELPED A BUSINESS CONGLOMERATE WITH AWS RE-ARCHITECTING AND IMPROVING SECURITY POSTURES WITH MANAGED IT SECURITY SERVICES



SUCCESS STORY

INDUSTRY:
Information and Finance

OFFERING:
Managed IT Security
Service

CUSTOMER OVERVIEW

Headquartered in Durham, North Carolina, USA, the client is a conglomeration of independent portfolios comprising more than 115 businesses with more than 8,000 of the brightest minds and determined entrepreneurs, generating over \$2 billion in revenue around the world. The client's portfolios operate in 15 different sectors, including health care, technology, insurance and financial services.

CONTEXT

The client was looking to engage with the Progressive for AWS re-architecting, which included validation of existing deployment, and introduction of UTM and WAF for their 278 public facing websites and management of all the web domain through GUI based cPanel controller hosted behind the Unified Threat Management (UTM). The client wanted to make their infrastructure more fault tolerant and separate out the databases and the websites. There was no filtering and the server was in a default VPC with the management ports open to the public. The client wanted to improve its security postures with Perimeter security and Distributed denial of service (DDoS) protection on their websites and were seeking consulting and best practices recommendation.

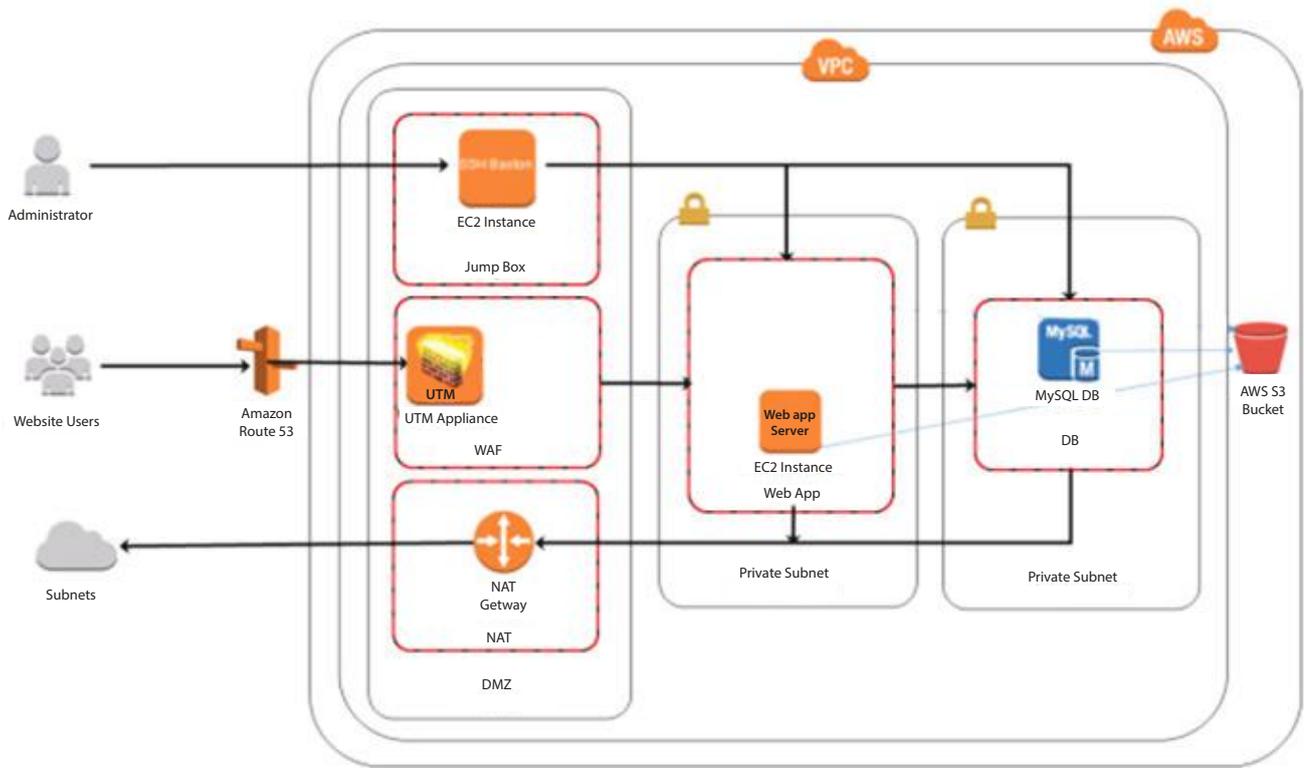
KEY BUSINESS CHALLENGES

- Migration of all 278 databases to Amazon Relational Database Service (Amazon RDS) and then re-configuration of the website pointers to the new database locations
- Using UTM+WAF security solution to achieve complete security from layer 3-layer 7 of OSI framework.
- Managing cPanel-UTM from internet
- Using DNAT (Network Address Translation) and forwarding different URL based on ports and same private IP.
- Separate tracking of Traffic and attacks for all the websites.

SOLUTION

- Progressive introduced an RDS and enabled strict Security Group rules so that only relevant traffic coming from the web subnet is able to access the DB tier.
- Introduced a Sophos UTM + WAF bundle for the client to take care of the security.
- Also introduced a bastion host so that the management ports for the servers are not exposed to the internet.
- Introduced web application and Sophos UTM V9.0 hosted server in same subnet.
- Configured Sophos so that the traffic flow and security is tracked for all the 278 websites.

SOLUTION ARCHITECTURE



ABOUT PROGRESSIVE INFOTECH

Trusted IT partner since 1998, Progressive Infotech provides a comprehensive suite of transformation and support services. The offerings span across cloud, digital and support operations, delivered through a matured and scalable service delivery model. In every client engagement, Progressive ensures clients realize higher ROI, stretch the intrinsic value of existing IT investments and are better prepared for emergent market changes.

Gartner lists Progressive Infotech as a notable vendor in Magic Quadrant for Public Cloud Infrastructure Managed Service Providers, Worldwide 2018- Asia/Pacific Context.

Experience the outcomes at www.progressive.in
For more information contact us at info@progressive.in