Building a Highly Available and Secure Network on AWS for One of the Largest Electricity Distribution Utility in India

From Vision to Reality:

Crafting a Secure and Highly Available AWS Network

Summary

The customer had been operating their 100+ applications within a monolithic network architecture, leading to challenges in scalability, manageability, and operational agility. To address these issues, the customer began transitioning to a more modular and cloud optimized architecture using several AWS services – enabling improved performance, isolation, security, and observability across their workloads.

Challenge

Initially, the customer's billing, SAP, meter systems were within a monolithic architecture. All ingress and egress traffic were funnelled through a single firewall, creating a significant performance bottleneck and a single point of failure. This kind of architecture lacked segmentation, making it difficult to isolate workloads and enforce granular security policies.

Additionally, customer relied on AWS Direct Connect to transfer large volumes of backup data from the cloud to on-premise storage. This setup led to severe bandwidth congestion, impacting the performance of production workloads. As a result, the organization experienced frequent SLA breaches, reduced operational efficiency, and limited scalability.

Proposed Solution

To address the above challenges, StarOne IT designed and implemented a scalable, secure and segmented multi-account AWS architecture. AWS Transit Gateway was deployed to replace legacy point-to-point VPNs and VPC peering, enabling centralized connectivity across all VPCs. The architecture introduced three distinct segments for ingress traffic: WebApp for customer-facing applications, IoT and MDAS for smart meter systems, and Dev, Management for internal and test environments.

A dedicated egress firewall was deployed to manage all egress traffic, including internet-bound connections and VPNs to vendor networks. Secure connectivity to multiple vendor environments was established using Site-to-Site VPNs integrated with the egress firewall. To enhance backup transfer efficiency, the existing 500 Mbps AWS Direct Connect was upgraded to a 1 Gbps connection, significantly improving throughput to on-premise storage.

To overcome Direct Connect VIF prefix limitations, StarOne IT collaborated with the customer's network team to summarize route prefixes. AWS Network Manager was used for centralized monitoring, while custom AWS Lambda functions were developed to track changes in networking components such as Transit Gateway and VPNs.

Additionally, StarOne IT configured cross-region Disaster Recovery using AWS Disaster Recovery Service for critical applications and cross-region automated backups for RDS Databases, which provided enhanced business continuity, minimized data loss risk, and ensured rapid recovery in the event of regional outages or failures.

CloudWatch alarms were set up to monitor key metrics like Direct Connect connection state and VPN tunnel status. Additional Lambda scripts monitored BGP neighbour status and automated route propagation and static route updates in Transit Gateway. EventBridge, in combination with AWS Network Manager and Lambda, was used to monitor changes in security groups, Transit Gateway, and VPN configurations, ensuring continuous compliance and operational visibility.

StarOne IT also implemented micro-segmentation using ColorTokens and configured third-party application and security monitoring tools such as Dynatrace, SIEM, and SOAR. Internal firewall was also configured to monitor

east-west traffic between VPCs. This enhanced visibility across the network, strengthened threat detection and response capabilities, and ensured proactive monitoring of application and infrastructure health.

Results & Benefits

The network re-architecture and segmentation enabled the customer to achieve an impressive application availability rate of 99.5% and led to a significant reduction in network bandwidth-related issues.

Key Outcomes

- **Improved Network Performance and Reliability**
  The new architecture reduced latency and eliminated single points of failure, ensuring consistent performance for critical applications.

- **Enhanced Security and Compliance**
  Segmented network design and integration with third-party firewalls improved security posture and enabled better compliance with regulatory standards.

- **Operational Efficiency and Scalability**

  Centralized monitoring, automation using AWS Lambda, and use of AWS Network Manager simplified network operations and reduced manual intervention.

- **High Availability and Disaster Recovery Readiness**

  Automated failover mechanisms and backup connectivity ensured business continuity and minimized downtime.

About StarOne IT Solutions

StarOne IT is an Advanced AWS Partner with significant credentials such as AWS Storage Services Competency, Migration Capability Review (MCR), and Well-Architected Review, focused on relevance, innovation and value engineering. StarOne IT works with customers to drive digital transformation and explore ways in which organizations can stay nimble and relevant by leveraging AWS Technologies. Our Advanced tier partnership status with AWS accelerates our ability to design, architect, build, migrate and manage customer IT workloads.