Transforming Security in the Travel & Hospitality Sector

aws partner network

Executive Summary

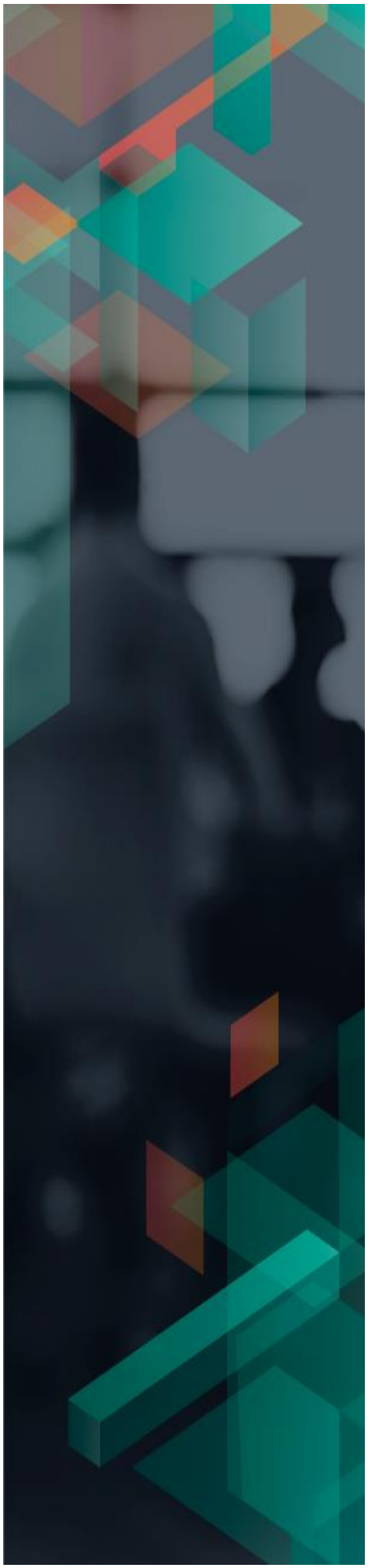
Our featured customer, a key player in the Travel & Hospitality sector, leads the industry with a commitment to exceptional customer experiences. Their substantial presence extends across diverse services and regions, ensuring top-tier quality for travelers.Customer embarked on a transformative journey to enhance its AWS infrastructure's security and resilience. The migration of DNS resolution to private hosted zones in Route 53 reduced exposure to the public internet, while AWS Security Hub integration ensured continuous security assessment and alignment with industry best practices. Migrating VPCs to Transit Gateway architecture improved scalability and reduced security risks, complemented by AWS Direct Connect and Gateway Load Balancer for secure network foundations. Palo Alto Firewalls added advanced threat protection, while a custom Riverbed AWS Lambda script facilitated the integration of VPC Flow Logs with CloudWatch for automated data processing, enhancing network management. SD-WAN overlay encryption secured data in transit. These strategic measures collectively fortified customer's security posture and positioned it to address future security challenges effectively.

Customer Challenges

The customer was trying to establish robust and secure communication channels between multiple Virtual Private Clouds (VPCs) using Transit Gateway, connect AWS VPCs with on-premises networks while shifting public connections to more secure private connections. The migration of public DNS to new private resolvers and the transition of Route53 entries demanded meticulous planning and precise execution to maintain data security and privacy. Furthermore, customer required advanced security measures and scalability, which led to the deployment of Palo Alto Firewall in 3rd AZ, integrating with a new Gateway Load Balancer.

Goals

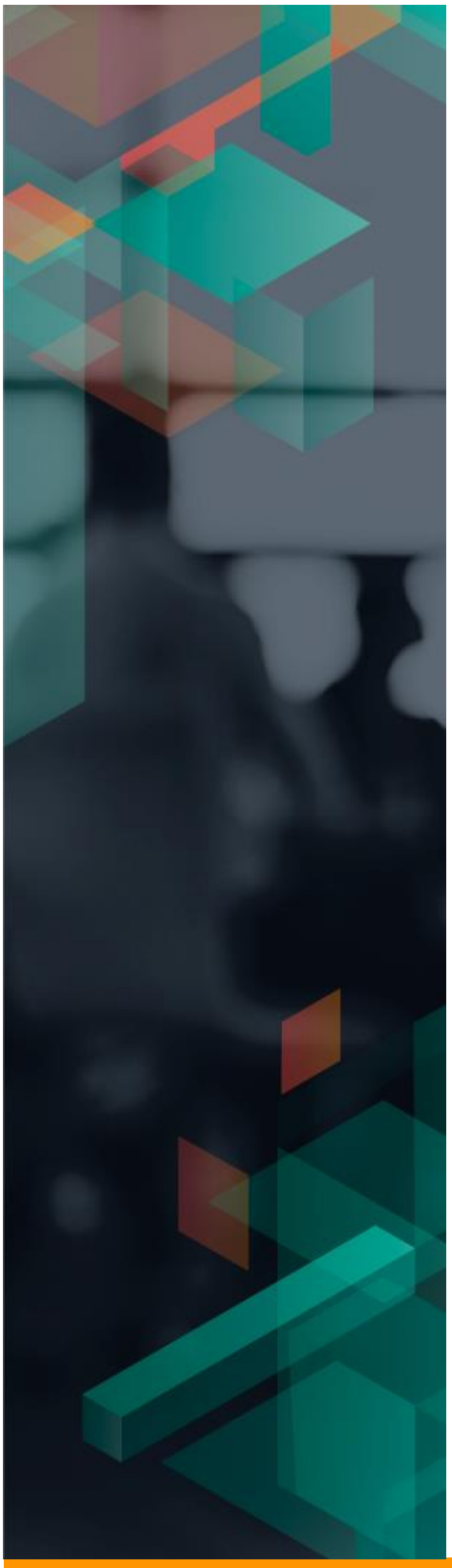
The project's core objectives were to streamline network routing for increased efficiency, establish secure and optimized communication pathways between diverse VPCs, TGW's and on-premise networks, enhance system resiliency through the implementation of a 3-Availability Zone model in which a new Palo Alto Firewall was placed behind a Gateway Load Balancer, transition Route 53 public connections to more secure private routes, improve overall network performance, and meet customer-specified availability requirements to ensure the robustness and resilience of critical applications.



Partner Solution

To address the customer's challenges and achieve the project goals, a comprehensive solution was deployed:

1. DNS Migration: The migration of DNS resolution from public to private using private hosted zones in Route 53 not only enhanced security but also contributed to network segmentation and access control. This strategic move reduced exposure to the public internet and minimized potential attack vectors, thereby strengthening security.
2. AWS Security Hub Integration: AWS Security Hub played a pivotal role in customer's security strategy. By enabling AWS Security Hub with AWS Foundational Security Best Practices v1.0.0 and CIS AWS Foundations Benchmark v1.2.0, customer achieved continuous security assessment of their infrastructure. This integration allowed customer to align with industry best practices, meet regulatory requirements, and ensure a robust security posture.
3. VPC Peering to Transit Gateway Migration: The core of the solution was the migration of all VPCs to the Transit Gateway architecture. This intricate process involved meticulous planning and execution. VPN connections to CSR routers were removed to reduce potential security risks associated with these access points. Simultaneously, non-CSR VPN connections were reviewed and eliminated, further reducing potential attack vectors. This migration greatly improved the scalability, security, and manageability of the network architecture.
4. Direct Connect and Direct Connect Gateway: AWS Direct Connect was used to establish private links from on-premises networks to AWS. Additionally, a Direct Connect Gateway was combined with Transit Gateway to create a strong network foundation. This setup provided a secure pathway that supported the use of Cisco Viptela SD-WAN routers, enhancing network security.
5. Gateway Load Balancer (GWLB): As part of security enhancements, a new Gateway Load Balancer was utilized in the third Availability Zone (AZ). Alongside this addition, three private VPC endpoints were implemented, as well as a third Palo Alto firewall, and all the necessary networking components, including subnets, attachments to the Transit Gateway (TGW), route tables, and NAT gateways. This comprehensive deployment bolstered security measures and resilience.
6. Palo Alto Firewall Integration: Palo Alto Firewalls were strategically deployed behind a Gateway load balancer to provide advanced security measures. These firewalls played a pivotal role in inspecting and filtering traffic, ensuring robust protection against potential threats. Their deployment in EC2 instances behind a Gateway load balancer ensured scalability, high availability, and the flexibility to integrate additional firewalls in the future as needed.
7. VPC Flow Logs integrated with CloudWatch: The Riverbed AWS Lambda script plays a crucial role. It is deployed as an AWS Lambda function, which acts as a bridge between AWS VPC flow logs and Amazon CloudWatch Logs. The Lambda function is configured to collect and export IPv4 flow data from VPC flow logs in near real-time intervals. By integrating Lambda, organizations can automate the process of data extraction and synchronization, ensuring that the network flow data is efficiently transferred to Amazon CloudWatch Logs. This technical setup allows for streamlined and automated data processing, enabling effective traffic analysis on the NetProfiler platform for enhanced network management and troubleshooting capabilities within AWS VPCs.



8. SD-WAN Overlay Encryption: To secure data in transit between Data Centre and AWS, SDWAN overlay encryption was introduced. This encryption ensured data confidentiality and integrity during transit, mitigating the risk of unauthorized access and data breaches.

Results and Benefits

The deployment of the partner solution yielded several key benefits and results:

A. Enhanced Network Security: The integration of Palo Alto Firewalls, optimized traffic flows, and centralized security controls significantly enhanced network security. Palo Alto Firewalls provided advanced traffic inspection and filtering, ensuring robust protection against potential threats. This enhancement reduced the risk of security incidents and unauthorized access.

B. Streamlined Network Management: The migration to Transit Gateway simplified network connectivity, reducing complexity and operational overhead. Centralized security controls streamlined governance and monitoring, enabling more efficient network management. This simplification contributed to improved network performance and security.

C. Seamless On-Premises Connectivity: AWS Direct Connect provided secure, dedicated connections between on-premises data centers and AWS cloud resources, ensuring uninterrupted data transfers crucial for customer's operations. This improved connectivity enhanced business continuity and data availability.

D. Improved Compliance: AWS Security Hub's continuous security assessment ensured that customer's infrastructure consistently adhered to recognized security standards and AWS guidelines. This improved compliance with industry best practices and regulatory requirements, reducing the risk of non-compliance.

E. Future-Ready Network: The solution positioned customer for future growth and scalability. The deployment of Palo Alto Firewalls and the centralization of security controls allowed for the integration of additional firewalls and security measures as needed. This flexibility supported customer's evolving security requirements.

F. Cost Optimization: By optimizing network design, consolidating security controls, and enhancing operational efficiency, customer achieved cost savings in managing their AWS network infrastructure. These cost optimizations contributed to improved resource allocation and budget efficiency.

About Intuitive.Cloud

Intuitive is a global cloud innovation company that partners with the world's leading enterprises to deliver high-impact, end-to-end solutions and drive extraordinary business outcomes. We are one of the fastest growing (CRN & INC5000 recognized) Cloud & SDx solutions and services companies in the Americas supporting enterprise customers on a global scale. Intuitive Superpowers: Cloud FinOps, Cloud Infrastructure Engineering, Cloud Native+AppSecOps+DevSecOps, DataOps, AI&ML, CyberSecurity & GRC, Digital Workspaces (M365), Hybrid Cloud, SDDC, SD-WAN, SDN

Intuitive.Cloud