Case Study

Cloud access control for automotive supplier

In cooperation with

aws PARTNER Premier Tier Services

Executive summary

A global automotive components supplier, has asked T-Systems to create a scalable and global network architecture on AWS as a foundation for their planned SAP on AWS migration across their worldwide business.

A key priority has been the compliance with the company's strict networking security standards across a multi-region landscape involving EMEA, US and even AWS regions in APAC.

About the customer

The client is an independent automotive component maker. As well as automotive wire harnesses, their core product for which they command a large share in the global market, they develop and manufacture meters, electronic components and a host of other products for automotive use.

Since their first overseas production site was established in Thailand, their global development and manufacturing network has continued to grow, along with their relationship of mutual trust with car manufacturers around the world.

They are committed to being environment-friendly in every aspect of their business. They have developed and produced a long line of eco-friendly and energy saving products, starting with the world‘s first solar thermal powered air conditioning system, to the world‘s first wood biomass energy air conditioning system.

The company is dedicated to caring for the environment, making a contribution to society and inspiring trust in all their stakeholders.

The challenge

The automotive supplier decided to move their SAP landscapes from on-premises to AWS cloud. They wanted the same security and network operation team to manage the network security in AWS cloud. Their current supplier is Palo Alto. Their firewalls and security management tools are used extensively in the client's office, factories and remote sites.

The customer needs to continue with their current network security framework in AWS cloud in their offices, factories and remote sites. The security standards must also apply to the SAP landscape which includes the following:

- VPN service using Palo Alto Prisma which will support thousands of SAP users accessing the SAP systems in AWS
- The implementation of Palo Alto firewalls EC2 appliance from the AWS marketplace must be a highly available configuration
- All traffic between VPCs must be controlled and inspected by Palo Alto firewall
- All traffic between on-premises and virtual private clouds (VPC) must be controlled and inspected by Palo Alto firewall
- The Internet breakout of the SAP and related systems in AWS cloud are controlled and inspected by Palo Alto firewall
- The monitoring and backup service of the Palo Alto EC2 appliances and all the network services in AWS are managed by T-Systems whilst the operation and maintenance of the Palo Alto firewall are managed by the customer‘s network team.

It is the first implementation of this design in AWS for the customer and they were looking for guidance and assistance.

T Systems

Let's power
higher performance

The solution

To ensure high availability, the SAP landscape and network services are deployed across two availability zones. A multi-account structure was used to separate the SAP workload, SAP-related workload and the network account which provided the site to site VPN service and security service with the Palo Alto firewall appliances. The customer selected their EMEA region as the first migration region and the AWS region eu-west-1 (Ireland) was selected based on location and cost.

Below is the list of the AWS services deployed in the network account to support the customer's requirement

- AWS Internet Gateway
- AWS Transit Gateway
- AWS Site to Site VPN
- AWS Gateway Load Balancer (appliance mode)
- AWS Marketplace (Palo Alto firewall appliances)
- AWS Backup
- AWS Cloudwatch

Results and benefits

Due to demanding timeline of the migration, the Site to Site VPN between the customer's sites and AWS was set up initially without high availability (HA). Only one Palo Alto firewall (FW) in a single availability zone (AZ).

A migration plan was developed to upgrade the VPN to HA with the deployment of two Palo Alto FW across two AZ with Gateway Load Balancer in appliance mode. The implementation took several iterations to complete and the customer was able to integrate Palo Alto FW into their existing network and security process and tools. Failover testing was carried out and the customer was satisfied with the outcome.

The AWS network service implementation was re-engineered into Terraform source code stored in the T-Systems repository and deployed with CI/CD pipeline. When the customer completed the EMEA migration and started their SAP migration for the next region, North and Central America, the network service was deployed in the new network account for North and Central America region (us-east-1) with the Terraform code and CI/CD pipeline. This approach reduced the deployment time from days to hours, also the deployment effort and cost were reduced for the customer.

There was an undesirable characteristic using the Gateway Load Balancer: SAP users (including RFC users) were timed out of their session after inactivity, this characteristic did not occur previously in the on-premises SAP systems. After investigation and research, it was discovered that the Gateway Load Balancer has a fixed TCP session timeout of 350 seconds (less than 6 minutes), whereas the default TCP timeout on many systems (Windows and Linux) are 7200 seconds (120 minutes). To overcome this limitation, TCP session timeout parameters in the Windows and Linux Operation Systems were reduced to 60 seconds. Additionally, TCP keep alive parameters in SAP profile and UC4 agent were reduced. So TCP packets are continuously sent between client and server in shorter intervals to avoid the TCP session timeout of the Gateway Load Balancer (350 seconds).

About the partner

With a footprint in more than 20 countries, T-Systems is one of the world's leading vendor-independent providers of digital services headquartered in Europe. The Deutsche Telekom subsidiary offers one-stop shopping: from secure operation of legacy systems and classical ICT services, transition services to cloud solutions as well as new business models and innovation projects in the Internet of Things (IoT). T-Systems is also an accredited AWS Managed Service Provider (MSP) and Premier Consulting Partner with more than 500 experts on AWS with a growing list of competencies that include cloud migration, SAP system integration and consultancy support with the AWS Well-Architected Framework.

Moreover, T-Systems is an official AWS Direct Connect delivery partner, which means it is in the position to handle hosted-connections.

Contact

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
Tel: 00800 33 090300
E-Mail: info@t-systems.com
Internet: www.t-systems.com

Published by

T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main, Germany

T Systems

Let's power
higher performance

Last update: 07/2022 | Designed by: Creative Factory, TSIN