Case Study

Network architecture for Telco provider

In cooperation with

aws PARTNER Premier Tier Services

Executive summary

The telco unit asked T-Systems to help design and implement a highly scalable network architecture, following their strict security and compliance requirements. Key feature is the ability to monitor and control potential risks at any time to the core network. This resulting solution serves as foundation for a broader migration project, spanning over 500 applications.

About the customer

The unit is responsible for the design, development and operation of all its owned and transferred IT systems supporting business processes at the telco. It creates user-friendly web portals with intelligent self-service functions as a basis for an integrated, cross-channel customer experience in compliance with corporate identity and design guidelines. The unit is in the middle of a large-scale transformation program, adopting cloud migration as well as integrating agile frameworks such as Scaled Agile Framework (SAFe).

The challenge

The customer as an organization is undergoing substantial changes in the way it carries out DevOps. It is in the process of embracing a more agile approach to collaboration and is commencing its AWS cloud journey. It is important to note that a large number of applications in their current ecosystem–over 500 applications–rely on conventional interfaces that are available only within its legacy network on site, in its own datacenters. Moving this large-scale, legacy suite of networked applications from an on-premises solution to the cloud requires diligent and meticulous planning by network and security experts to ensure that the new network architecture is safe, stable and still be able to communicate with the „old fashioned“ application backends.

The solution

The network architecture deployed in eu-central-1 and eu-west-1 consists of multiple building blocks.

- **VPC/ Cloud Shepherd**

  Initially there are multiple types of virtual private clouds (VPC), which are connected to the central Transit Gateway(s). Those VPCs are provided in multiple stages for both production and non-production environments. In order to protect production data, connection is prohibited between production to non-production VPCs. For demonstration and testing purposes we provide some VPCs which are not connected to any other network component and can be viewed as standalone, default AWS VPCs. „Green VPCs“ can be used for applications, which do not require any connection to the on-premises corporate network. The majority of applications use so-called „Blue VPCs“, which are provided in two ways:

  - Larger projects are able to use dedicated VPCs, where the associated „System Team“ is responsible for managing the VPC.
  - „Shared VPCs“ are used the most. Those VPCs are controlled by the AWS team and the subnets of that VPCs are shared via AWS Resource Manager with the customer accounts.

  The customer has a central SSO portal to connect and control the cloud: Cloud Shepherd. Here central cloud management functionality is available, such as

  - ordering an AWS account of a certain type (VPC type, prod/non-prod),
  - deleting an AWS account and
  - cloud access management

- **Controlled Egress Traffic (FPA – Forward Proxy Area)**

  Today, almost every application must connect to multiple interfaces, either located in the on-premises network or on the Internet. To control the egress traffic to the Internet we provide egress VPCs, which offer proxy functionality for either an explicit proxy configuration of the application, or in a transparent way, where the proxies are part of the routing path. We are using GitOps to provide transparency of the running whitelist and also to interact with the application teams. The egress VPC is connected via AWS Transit Gateway to the customer VPCs.

- **Controlled Internet Exposure (RPA – Reverse Proxy Area)**

  Per default, applications running on AWS do not need to be exposed to the Internet. However, if that is defined as a requirement, additional security controls apply. To expose applications to the Internet securely we offer a secure ingress solution called Reverse Proxy Area (RPA). This solution consists of controlled public subnets, which can only be used to provision load balancers into. This control is realized via a SCP using resource tags. Additionally, we are using the AWS Firewall Manager to provide an additional layer of security by enforcing a centrally managed AWS WAF WebACL to each application load balancer. This enforcement is critical for the organization and the AWS team is also providing support with a comprehensive WAF documentation and consultancy. Logging data is centrally gathered and monitored.

- **Direct Connect**

  To allow efficient migration and connection to on-premises systems we are using AWS Direct Connect with 2x10G connections to the data centers of the customer. Within the on-premises network there is an additional firewall, the so called „Cloud Firewall“, in place. The corresponding policies can be controlled via Tufin Secure Change. Changes can be requested by DevOps and the AWS team.

  Direct Connect is being used for two regions, eu-central-1 and eu-west-1, which both have a Direct Connect Gateway association to the regional Transit Gateways.

- **IP Management**

  One of the basic requirements every network team faces is how to control the use of IP addresses. For that we recently have migrated to AWS IPAM, which we integrated into our automations. This eliminated the old spreadsheet-based IP management and also the Serverless Transit Network Orchestrator.

- **DNS**

  Another basic building block is DNS, where every customer is able to use Route53 freely. We are using Route53 Inbound Resolver to allow access to our private zones for the on-premises networks and Route53 Outbound Resolver rules to define, which internally controlled DNS zones should be resolved by the on-premises DNS network.

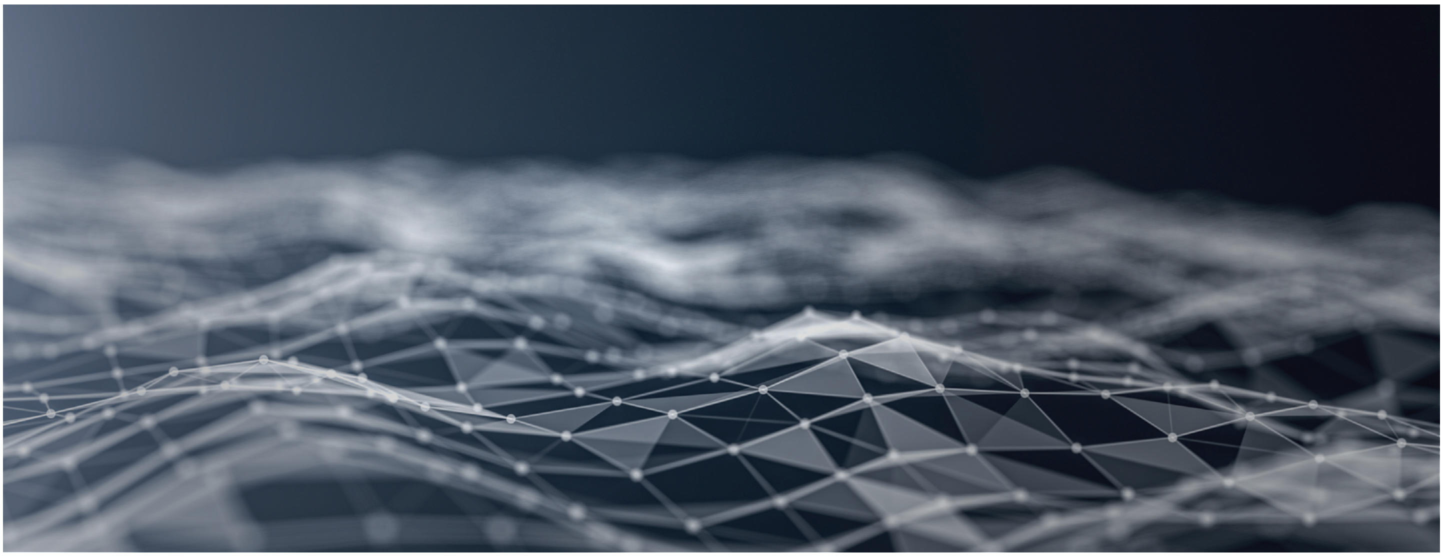
  For the private zones, which only work from within the VPC they are associated with, we have service catalog products in place, which allow cross-account zone association to every relevant VPC. These associations are automatically updated for every new zone or VPC, which has been created.

  We are also using Route53 query logs for monitoring.

  Some domains are controlled centrally and are used for zone delegations or very specific records.

- **Service Catalog**

  As it is our aim to enable our customers to perform operations independently, we use AWS Service Catalog for certain products. They are able to provision internet exposure (RPA – Reverse Proxy Area), Private Hosted Zones with automation to associate to VPCs, store certain DNS records in central domains or to order dedicated subnets or Private Link endpoints to partners.



Results and benefits

With the architecture described here, we jointly built a highly redundant and scalable networking solution. The users are able to work independently on their application-specific needs without relying on a central team of networking experts.

The collaboration between the customer and T-Systems resulted in a quick ramp-up of a secure and scalable AWS landing zone, approvals and guardrails for AWS usage in Telecom, transparent and open communication, which can be attributed to the nature of the work engagement between the two internal parties, robust consultancy work. It also witnessed the migration of services that left the customer with a highly reliable support platform.

The SVP and managing director of the customer expressed his appreciation for the work done when he said: „We appreciate the continuous collaboration with T-Systems in our Cloud Center of Excellence. The colleagues are experts on AWS; with their support we could significantly accelerate our AWS journey. We are looking forward to future collaboration on achieving our cloudification targets and becoming the leading digital telco.“

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