alkira

WHITEPAPER

How to Deploy IoT Infrastructure Using Alkira

A Technical Look

Table of Contents:

Glossary of Terms

CXP Cloud Exchange Point: is a fully virtualized point of presence delivering an entire network stack with rich network services

Connector: is a termination point connecting on-prem and cloud networks

CSP Cloud Service Provider: provides a wide range of cloud computing services

MCN Multi-cloud Networking: utilizing multiple CSPs to build, deploy, and manage applications and workloads

Introduction

The adoption of IoT (Internet of Things) technology has been steadily increasing across various industries, including manufacturing, healthcare, transportation, agriculture, and smart cities. Estimates suggest over 30 billion connected IoT devices in 2020, projected to surpass 75 billion by 2025. IoT networking comes with some inherent challenges.

Complexity of Ecosystem

IoT deployments typically involve a diverse ecosystem of devices, sensors, gateways, networks, and cloud platforms. Creating a standard, repeatable infrastructure is paramount.

Scalability

IoT deployments must scale seamlessly to accommodate a growing number of devices and increasing data volume. Customers are moving their infrastructure away from legacy data centers and into the Cloud. In most cases, multiple cloud providers are used for redundancy and scalability.

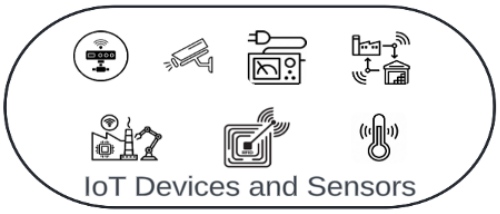
Security Concerns

Security is a significant concern in IoT deployments due to the large number of connected devices and potential vulnerabilities. Segmentation of the IoT network from corporate traffic is critical to deploying a secure IoT infrastructure.

Regulatory Compliance

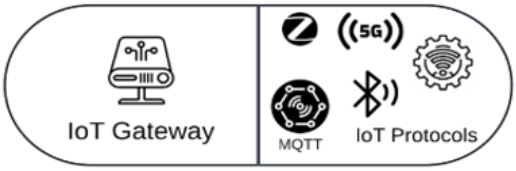
IoT deployments must comply with various regulatory requirements and industry standards related to data privacy, security, and environmental regulations. These regulations include ensuring compliance with GDPR, HIPAA, and FCC regulations.

The IoT Architecture



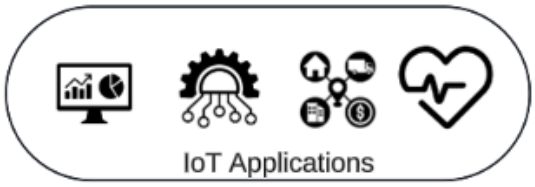
Device and Sensor Layer:

The device and sensor layer is the lowest layer of the IoT architecture and consists of physical devices and sensors that collect data from the environment. These devices can include sensors, actuators, RFID tags, cameras, and other hardware components. They collect various data types, such as temperature, humidity, motion, location, environmental conditions, and supply chain data.



Connectivity, Data Processing, and Edge Compute Layer:

This layer facilitates communication between IoT devices and the rest of the IoT infrastructure. Multiple protocols are supported for IoT communications. The IoT Gateway acts as an integrator for these various protocols. Additionally, the IoT Gateway, in most cases, acts as the edge computing layer for processing and analyzing data collected by IoT devices. Allowing the IoT Gateway to perform the processing tasks locally will significantly reduce latency and bandwidth usage.



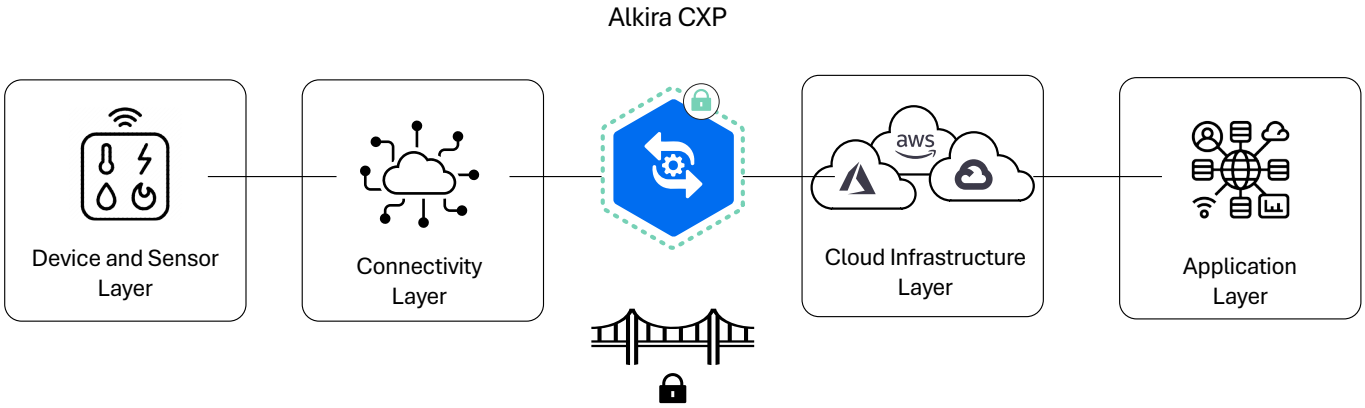
Cloud Infrastructure Layer:

The cloud infrastructure layer provides scalable and elastic computing resources for storing, processing, and analyzing large volumes of IoT data. Each cloud service provider offers data storage, computing, analytics, and machine learning services.

Application Layer:

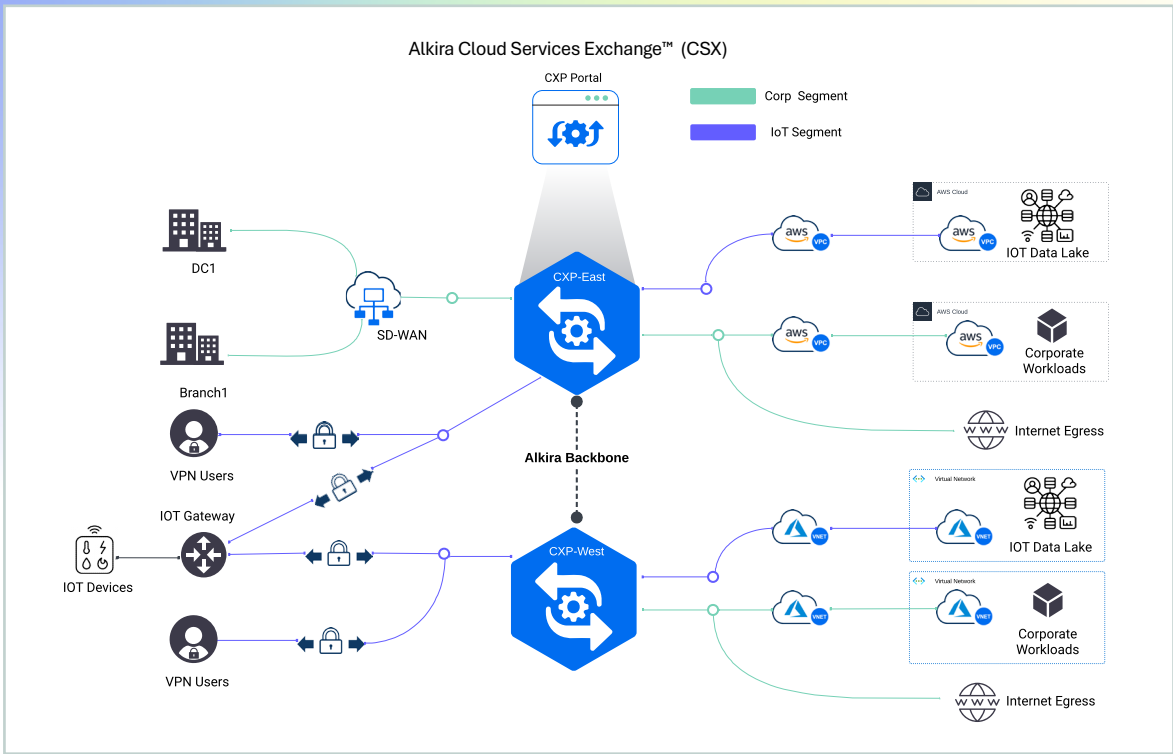
The application layer consists of IoT applications and services that utilize processed data to deliver value to end-users. These applications typically include dashboards for predictive maintenance systems, asset tracking, and healthcare monitoring. Users access this data through alerting, actionable information, and Alops.

Where does Alkira fit into the IOT architecture?



Alkira acts as a secure bridge between the connectivity and cloud infrastructure layers. Alkira provides a segmented, secure, highly available, and scalable infrastructure on demand for your IoT environment. Next, we will investigate how Alkira can solve many inherent issues troubling IoT initiatives.

Alkira IoT Reference Architecture



The above architecture depicts an existing Alkira manufacturing customer. That deployed a large IoT environment using Alkira infrastructure-as-a-service. We will discuss the different attributes in further detail.

Alkira Reference Architecture IoT Attributes

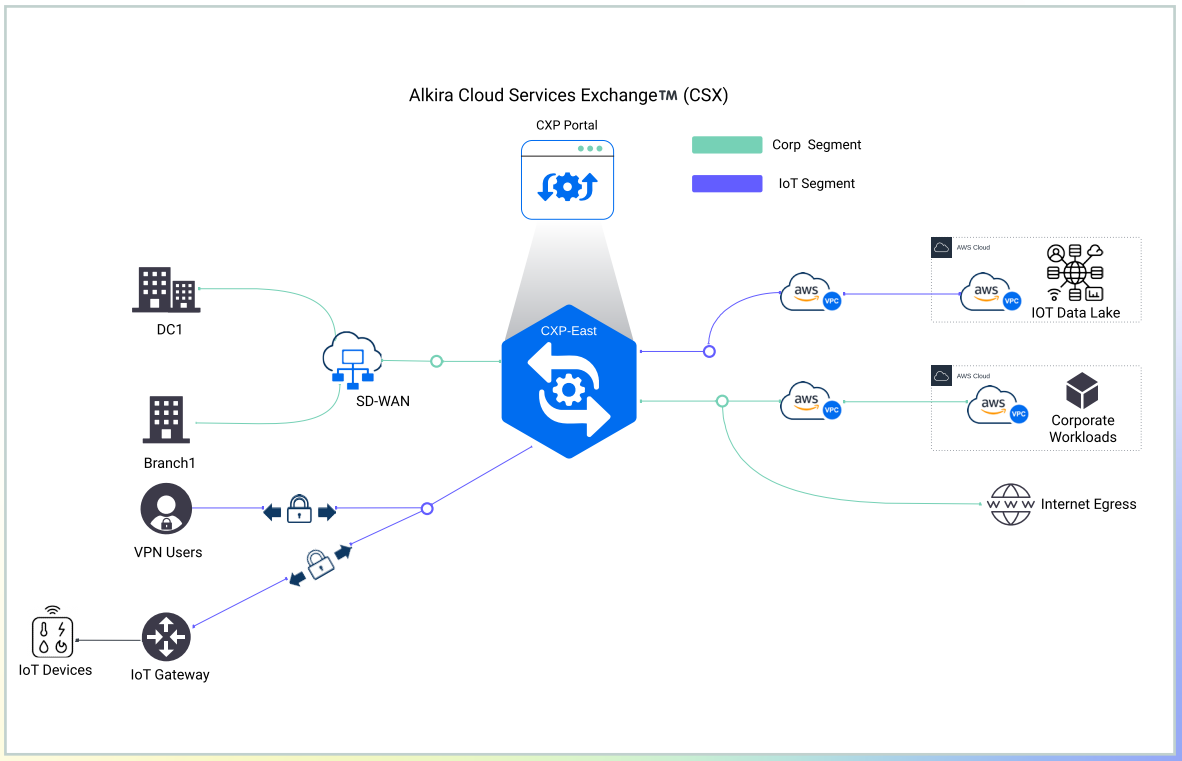
Next, I would like to discuss some foundational features built into the Alkira platform and how they align with standard IoT architecture requirements. Each feature discussed aligns with the typical challenges our customers face deploying IoT.

Segmentation

Many of us remember the Target data breach in 2013, which allowed hackers to steal the credit card and personal information of over 40 million customers. However, many people forget how hackers gained access to Target's network in the first place. The attackers reportedly gained access to Target's system by stealing credentials from an HVAC and refrigeration company, Fazio Mechanical Services, based in Sharpsburg, Pennsylvania. The hackers would then "crawl" across the network by accessing the HVAC IoT devices, eventually allowing them access to POS systems where they installed malware. What did the IT world learn from this? IoT devices need to be segmented off from the corporate infrastructure and, in most cases, from other IoT networks based on their functionality. In traditional on-premises environments, customers can use security tools and network VRFs to ensure these networks are segmented.

But, as the IoT applications and infrastructure move to the cloud, using "cloud-native" tools can make standardization difficult. Alkira provides customers with the tools to achieve these segmentation requirements quickly and provides standardization so that the IoT infrastructure can scale. There are two key features native to the Alkira cloud service exchange that help customers achieve these goals.

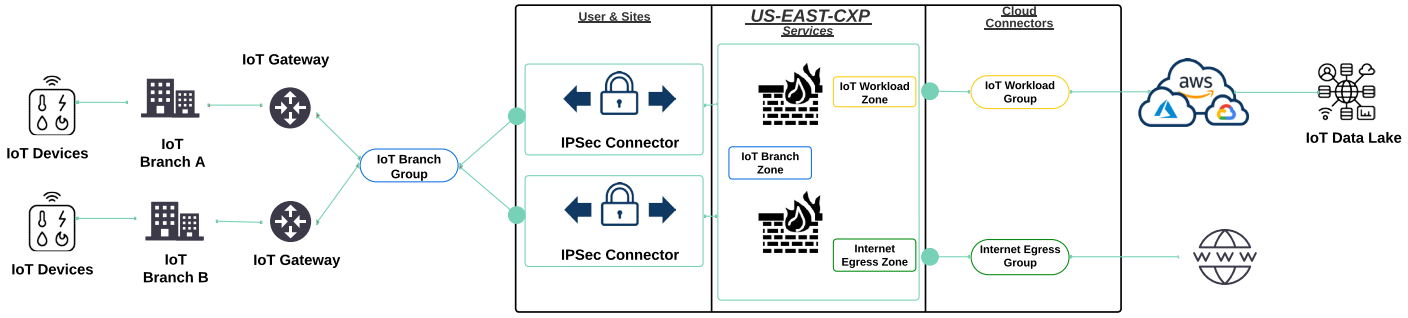
Segments



Alkira natively allows you to create segments. Each segment will have its own routing table that will be isolated from the others. As shown in the reference architecture, you can have the corporate network in one segment and the IoT network in another. These segmented networks will not be allowed to communicate by default.

Groups

Now, I would like to discuss the concepts of Groups within the Alkira platform. A Group is a "tag" that can be assigned to a connector. When you build a policy, whether it is a traffic policy, NAT policy, or routing policy inside Alkira, you can refer to these Groups to set configuration standards and have consistent policies across all of the connections terminated on an Alkira CXP. This is important to eliminate any "snowflake" configuration, which could lead to an IoT device or the network configuration having a non-compliant policy being applied to them.



In the diagram above, you can see how groups can be used to tag connectors so that these groups can be referenced in the policies you create. The "IoT Branch" group can be applied to any new branch that is migrated onto Alkira, and ensure that the correct policies are always assigned to these new branches based on your security and networking requirements.

Multi-cloud Connectivity

Multi-Cloud Networking, or MCN for short, is a philosophy that spans multiple use cases, including IoT. Some of the key reasons why customers deploy their IoT platform using the MCN approach are:

Vendor-agnostic approach: Taking a vendor-agnostic approach to the cloud eliminates the risks of price increases, service quality decreases, and technology focus shifts at a particular CSP.

Cost Optimization: A multi-cloud strategy allows customers to select the most cost-effective services across all CSPs. Building an IoT platform is highly advantageous because workloads can be spread across multiple CSPs, reducing overall costs.

High Availability: Uptime is paramount when deploying an IoT platform for mission-critical data such as healthcare, supply chain, environmental regulation, and access technologies. The ability to "failover" or provide disaster recovery to another CSP is critical.

Scalability and Flexibility: In an IoT environment, processing and analyzing large amounts of data is essential to a well-performing application. The ability to use "best-in-breed technologies" from different CSPs will optimize the application's performance.

Alkira's IaaS was built with an understanding of how vital an MCN strategy is. Using the Alkira platform, you can deploy your workloads in multiple cloud environments in minutes. Alkira's CXPs can be deployed in Azure, AWS, and Google Cloud across all available regions. Once these CXPs are deployed, you can onboard VPC and VNets and connect these multi-cloud workloads over the Alkira high-speed low-latency network. Next, I would like to go through an example customer and show how Alkira is crucial to creating a scalable, secure, resilient IoT platform.

ABC Company Sample Multi-Cloud IoT Deployment

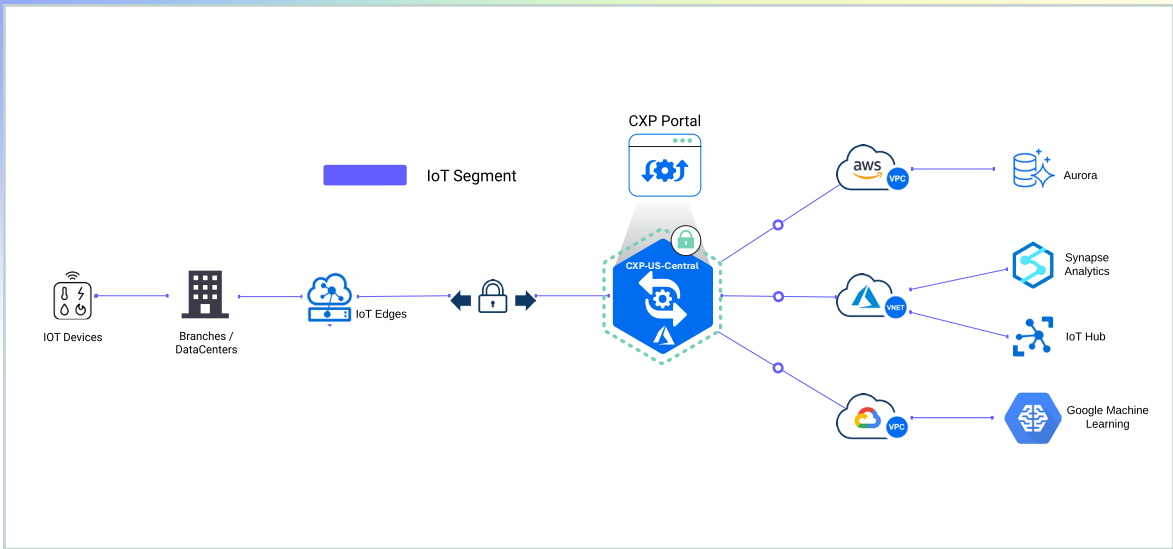
Let's walk through a "real-world" scenario for a customer looking to deploy a multi-cloud IoT platform. The ABC Company has already vetted each CSP, done its cost analysis, and decided to deploy the services below for its new IoT platform deployment.

ABC company will deploy services across all three clouds in three geographically diverse regions. We already discussed the advantages of a multi-cloud approach. However, even with these advantages, there are still challenges, and the network infrastructure needs to be able to handle the requirements set forth by the platform architects.

Some challenges that network, security, and cloud engineers will face include:

- Operational Complexity
- Skilled engineers in each of the CSPs
- Inconsistent Routing and Security Policies
- Network Latency and Reliability
- Traffic visibility from on-premises to cloud and across CSPs

Let's see how Alkira addresses these challenges.



Here is a high-level design of an IoT network infrastructure that ABC company can deploy with Alkira. A CXP can be deployed in any required CSP region. Inside the CXP, a firewall service can be installed. Connectivity from on-prem data centers and branches is terminated via IPSec tunnels; however, SD-WAN is also supported.

Operational Complexity and Engineering Skills

The onboarding of the VPCs and VNets is a straightforward process done through the Alkira UI, and no work is required on the CSP except for VPC and VNet creation. This is important because each CSP has its idiosyncrasies and complexities, which can be

detrimental to standardization. Abstracting these complexities allows the network and security team to meet the application teams' demands.

Inconsistent Routing and Security Policies

Traffic across the entire Alkira infrastructure can be forwarded to firewalls for inspection simply by creating a policy in the Alkira CXP portal. These policies will then be standardized, portable, and can be worked into CI/CD pipelines.

Network Latency and Reliability

Alkira's low latency, high throughput, and highly available backbone are built on a robust hyper-scaled infrastructure. This allows our customers to scale up as their cloud environments and IoT device footprints grow. The Alkira cloud service exchange is redundant and provides customers with a high SLA commensurate with supporting high-business-impact applications such as IoT.

Traffic visibility from on-premises to cloud and across CSPs

Visibility into each traffic flow is presented in the Alkira portal for troubleshooting and analysis. Other tools like utilization reporting, cloud insights, and IPFIX/Netflow integration allow engineers to respond quickly to network problems.

Summary

Alkira's platform provides robust solutions for the inherent challenges of IoT deployments, ensuring scalable, secure, and efficient multi-cloud IoT infrastructure. This white paper emphasized Alkira's role in enhancing IoT deployments through segmentation, policy consistency, and multi-cloud connectivity.

Author

Mike Benoit

Solution Architect