alkira

White Paper

On Demand Next-Generation Cloud Firewalls

Industry's only solution with single-click provisioning of auto-scalable and globally available next generation cloud firewalls protecting communication between remote-users, on-premises sites, public clouds and Internet with consistent security policy enforcement

Cloud adoption continues to accelerate. Organizations are increasingly transitioning business critical applications from on-premises data centers to the public cloud and SaaS environments.

In response to this rapid adoption of the cloud, compute and storage have evolved beyond virtualization and automation to as-a-service offerings. Cloud architects and engineers are now focused on choosing the service attributes they want to consume, such as compute instances and storage volumes, rather than worry about implementation details. Complexity has been eliminated and cloud computing has become a business enabler for compute and storage.

Key Challenges

In contrast, the network and network services have not made a similar transition, nor do they operate in true concert with the cloud. One of the most popular network services examples is the firewall. As applications increasingly move from on-premises data centers to the public cloud and SaaS environments, firewalls play a pivotal role in enforcing organizational security policy to and across clouds.

Deploying cloud firewalls comes with the following key challenges:

- Complicated routing domains to accommodate the traffic steering symmetry needed for stateful, global deployment of cloud firewalls, especially when firewall inspection is required only for selected application traffic
- Inconsistent security policies resulting from a lack of a standardized firewall deployment and operating model across a multi-cloud environment
- Overprovisioning and high TCO of cloud firewalls to accommodate peak capacity demand, resulting in high total cost or owner-ship (TCO)

The network and network services are under ever-increasing pressure to provide an agile, high performing and cost-effective solution to cloud business needs.

Alkira Cloud Network as-a-Service is the industry's only solution with single-click provisioning of the global multi-cloud network and network services. Cut provisioning time from months to minutes.

Networking for the Cloud with Alkira Cloud Network as-a-Service

It is time for the network to evolve. It is time for the network to be reinvented for cloud. Read a white paper by Atif Khan, Alkira Founder and CTO.

The Alkira Cloud Services Exchange® (Alkira CSX) serves as a foundation for Alkira Cloud Network as-a-Service. It consists of a highly available and resilient cloud backbone of globally interconnected Alkira Cloud Exchange Points (Alkira CXPs), virtual multi-cloud points of presence with a full routing stack and network services capabilities, and an Alkira CSX Portal.

Users, sites, data centers, regional SD-WAN fabrics, colocations, public clouds, network and security services, and SaaS/Internet exit points connect to the global network through the geographically closest Alkira Cloud Exchange Point .

Integrated stateful security services coupled with end-to-end segmentation capabilities offered by the Alkira CSX, allow enterprises to consistently secure on-premise, hybrid and multi-cloud environments. The Alkira Cloud Services Exchange Portal offers a modern graphical interface for all design, provisioning, and day-2 operational needs.

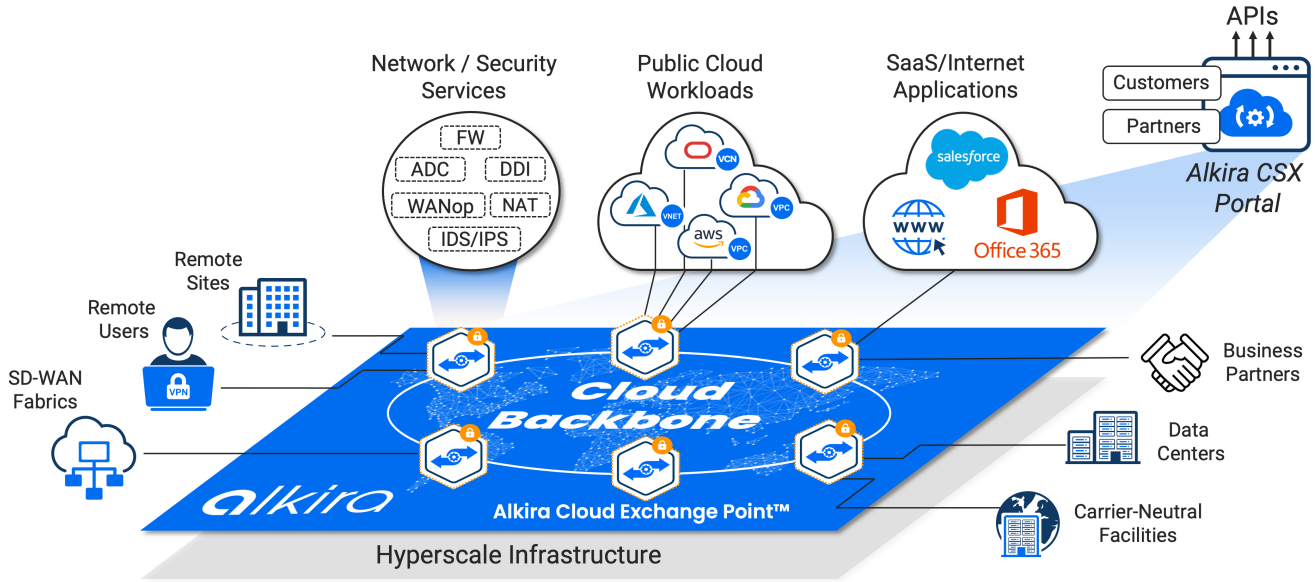


Figure 1: Alkira Cloud Services Exchange

Securing the Network Cloud with Next-Generation Cloud Firewalls

Alkira network services marketplace allows enterprises to choose a next-generation firewall of their choice in a global network. Alkira solution takes care of provisioning and scaling the firewalls in a highly available topology in a geographically distributed Alkira Cloud Exchange Points, as well as symmetrically steering the traffic to the firewalls based on the Alkira intent-based policies. Once provisioned and operational, firewall administrators can continue enforcing firewall zone-based security policies across the entire network.

Zone-Based Policies

All resources connected to Alkira Cloud Exchange Points are assigned to a specific Alkira group. This grouping allows enforcing identical policy across the entire network regardless of the type and location of the resource. Examples of such groups are remote user groups, groups of on-premise sites, segments of SD-WAN fabric extended into Alkira, Internet exit points and so on. Alkira groups are mapped to the firewall zones. Each zone has a a high speed virtual connection to the Alkira Cloud Exchange Point infrastructure where the firewall is provisioned. Traffic is routed toward the firewall over the appropriate virtual connection, which abstracts the firewall from the underlying infrastructure. This allows security engineers to focus on creating and administering firewall security policy, rather than get involved in the details of firewall deployment, scaling and routing.

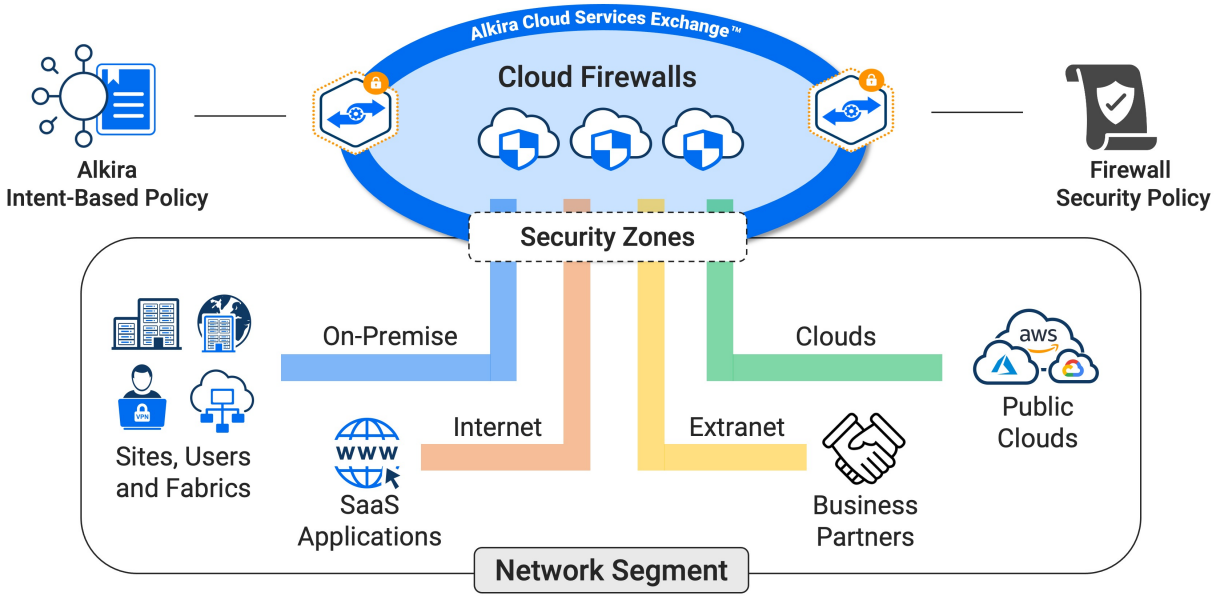


Figure 2: Alkira Cloud Firewall Security

Firewall zone-based policies work in concert with Alkira network segmentation. Grouping of resources is done in the context of a network segment. When multiple groups are defined in a given segment, it effectively sub-divides the segment creating micro-segments. Since each group is assigned to the firewall security zone, firewalls can enforce intra-segment security policy for traffic between multiple micro-segments.

In certain cases, firewalls also need to provide inter-segment security policy enforcement, specifically when application resources need to be shared across segments, for example, in cases of mergers and acquisitions, partner connectivity or IT-as-a-service offerings. The integration of the next-generation firewalls with the Alkira solution allows for this capability by properly routing the traffic of interest.

Routing and Scaling

The ability to insert stateful firewalls for network traffic to and across clouds is imperative for successful cloud adoption. Next-generation firewalls are stateful entities, and as such, they have to observe the entire bi-directional communication in order to be able to enforce their policies. This implies traffic symmetry. Networks are inherently asymmetric, which creates challenges and can break communication, especially in deployments where firewalls are geographically distributed. Alkira Cloud Services Exchange leverages intelligent traffic steering to preserve symmetry across a global Firewall deployment.

There are two specific cases where traffic symmetry plays a role:

1. Symmetric traffic to autoscaled next-generation cloud firewalls hosted inside an individual Alkira Cloud Exchange Point

2. Symmetric traffic across the entire cloud and multi-cloud network consisting of multiple Alkira Cloud Exchange Points and multiple next-generation firewalls

Case 1

Application traffic is symmetrically distributed across a number of next-generation firewalls in a given Alkira Cloud Exchange Point.

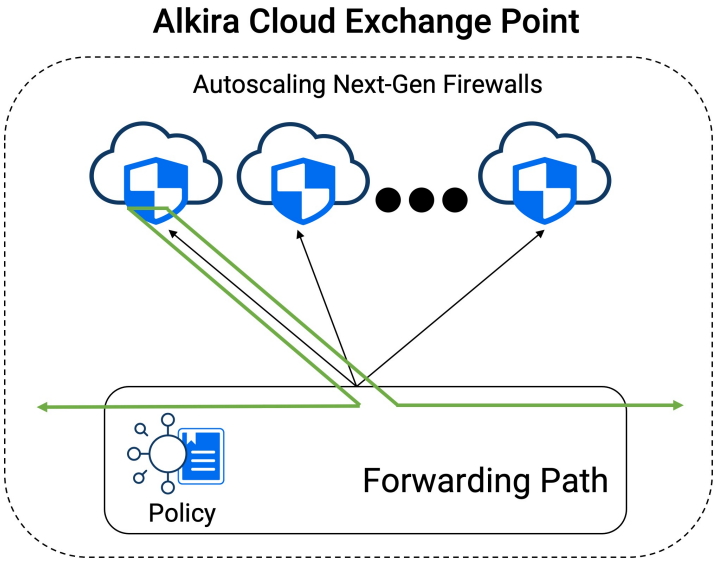


Figure 3: Symmetric application traffic distribution across autoscaling next-generation firewalls

Alkira Cloud Exchange Points preserve traffic symmetry bi-directionally, sending individual session traffic to the same firewall in order to maintain stateful behavior. Different sessions may end up being forwarded to different firewalls for horizontal scale.

Case 2

Alkira Cloud Services Exchange leverages ability to intelligently and symmetrically send the traffic of interest to globally distributed next-generation firewalls in a way that prevents unnecessary firewall over-provisioning. This traffic symmetry is globally enforced for multiple Alkira Cloud Exchange Points hosting the firewalls.

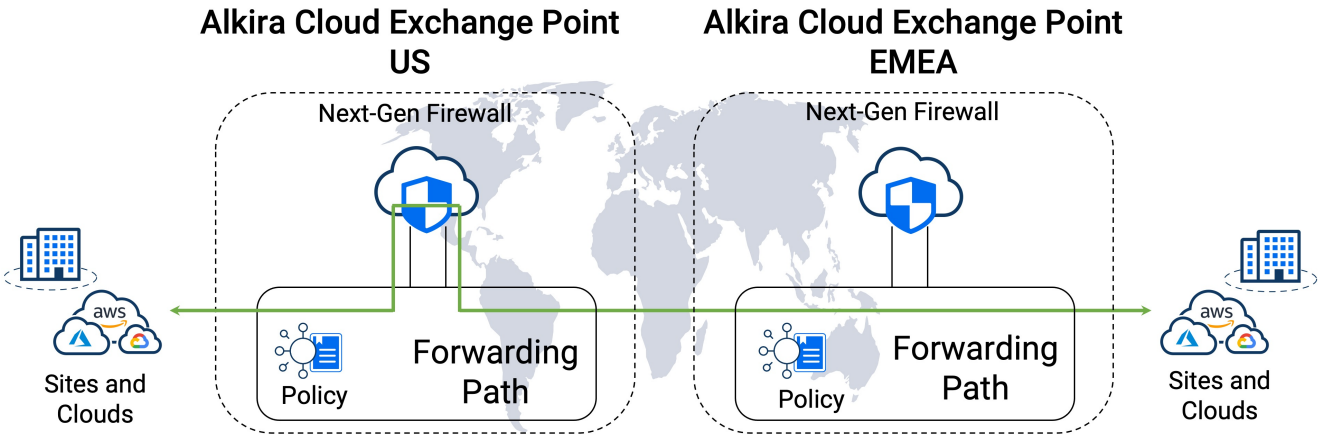


Figure 4: Symmetric application traffic distribution across multiple Alkira Cloud Exchange Points

In this example case, the communication between the sites and cloud instances in the US and the sites and cloud instances in EMEA occurs across two respective Alkira Cloud Exchange Points, each hosting a next-generation firewall selected from the Alkira Network Services Marketplace. The Alkira solution ensures that this traffic is symmetrically routed through the firewall in US CXP, while the firewall in EMEA CXP is bypassed for this particular communication. This approach effectively doubles the globally available firewall capacity, while maintaining global security policy enforcement.

As firewalls autoscale to accommodate needed real-time capacity demand and the communication occurs across multiple Alkira Cloud Exchange Points, both case 1 and case 2 described above can occur at the same time.

The Alkira solution takes care of instantiating next-generation firewalls and the associated symmetric traffic steering. Organizations are responsible for configuring the firewall security policy.

SaaS/Internet Firewall Security

SaaS applications are becoming increasingly popular. Access to SaaS applications is most often done through the Internet and as such, Internet exit points need to be carefully engineered to balance between security, performance and budgetary spend. Traditional methods of Internet access through the data center carry the advantage of fewer number of firewalls (albeit with higher capacity) and subsequently fewer number of administrative touch-points; however, they fail to provide adequate application performance due to high data center backhaul latency and a possible data center bandwidth starvation. In recent years the method of direct Internet access (DIA) at remote sites has become increasingly popular. This method offers much improved application performance when compared with data center-based access, however it proliferates the number of required Firewalls (for each remote site) and the subsequent number of administrative touch-points.

Alkira Cloud Services Exchange offers high-speed, low-latency transport from all sites to the SaaS/Internet applications. Geographically distributed Alkira Cloud Exchange Points with provisioned next-gen firewalls offer the needed balance between optimal (regional) connectivity to SaaS/Internet applications coupled with stateful firewall security and fewer number of administrative touch-points when compared to direct Internet access at each remote site.

The Alkira solution takes care of instantiating the firewalls and the associated symmetric traffic steering. Organizations are still responsible for configuring the firewall security policy.

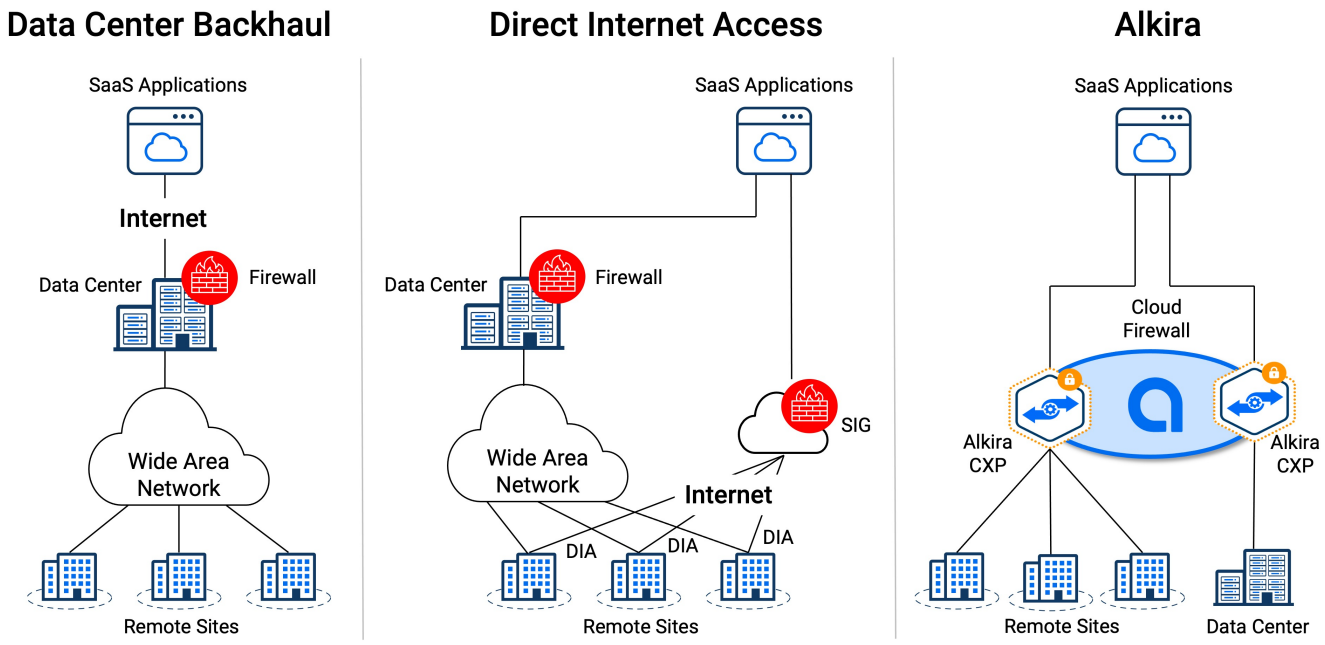


Figure 5: Compare Secure Internet/SaaS Access

Steps To Enable Global On Demand Multi-Cloud Network With Next-Generation Cloud Firewalls

Step 1:

Registering for Alkira Service

Registering for Alkira service is the first step to enable global on demand cloud and multi-cloud network with next generation firewall security.

a. Navigate to https://www.alkira.com and register your company

b. Click on the link in the registration confirmation email and create an administrative account

c. Log into Alkira portal to start designing your network

Experience the power of Alkira solution today and watch your multi-cloud network come to life in minutes.

Step 2:

Point-and-Click Next-Generation Firewalls Into The Global On Demand Multi-Cloud Network

With Alkira Cloud Network as-a-Service, your multi-cloud network and the next- gen firewall security are offered as-a-service, on demand, when you need it. You do not need to procure any additional firewall equipment or perform tedious network and routing configuration tasks. Your entire global multi-cloud network with next-generation firewalls is modeled through the intuitive Alkira portal in a point-and-click fashion.

a. Select the Alkira Cloud Exchange Point (CXP) where you want to provision the next-generation firewall. In a geographically distributed deployment, next-generation firewall instances should be provisioned in multiple Alkira Cloud Exchange Points to enforce security policy closest to the source.

b. Select either Pay-As-You-Go (PAYG) or Bring-Your-Own-License (BYOL) licensing option for the firewall deployment. In case of BYOL, please also provide the firewall license key. Organizations can leverage a mix of both licensing models.

c. Choose whether you want to use centralized firewall management tool with your firewall deployment. If yes, provide all the necessary details.

For centralized and consistent management of all global next-generation firewalls deployed in the Alkira Cloud Services Exchange, it is recommended to use the centralized firewall management tool.

You must enable centralized firewall management tool if you want to leverage the firewall auto scaling feature of the Alkira Cloud Services Exchange.

Note: The Alkira solution does not deploy the centralized firewall management tool. The deployment of the tool is enterprise responsibility.

d. Provide firewall specific details, such as the model, the desired software version, and the username and password for the firewall administrative account.

e. All defined network segments are automatically extended to all provisioned firewalls across the entire Alkira Cloud Services Exchange. This allows the firewalls to inspect application traffic in any of the segments. Firewalls can also provide secure cross-segment communication, if desired.

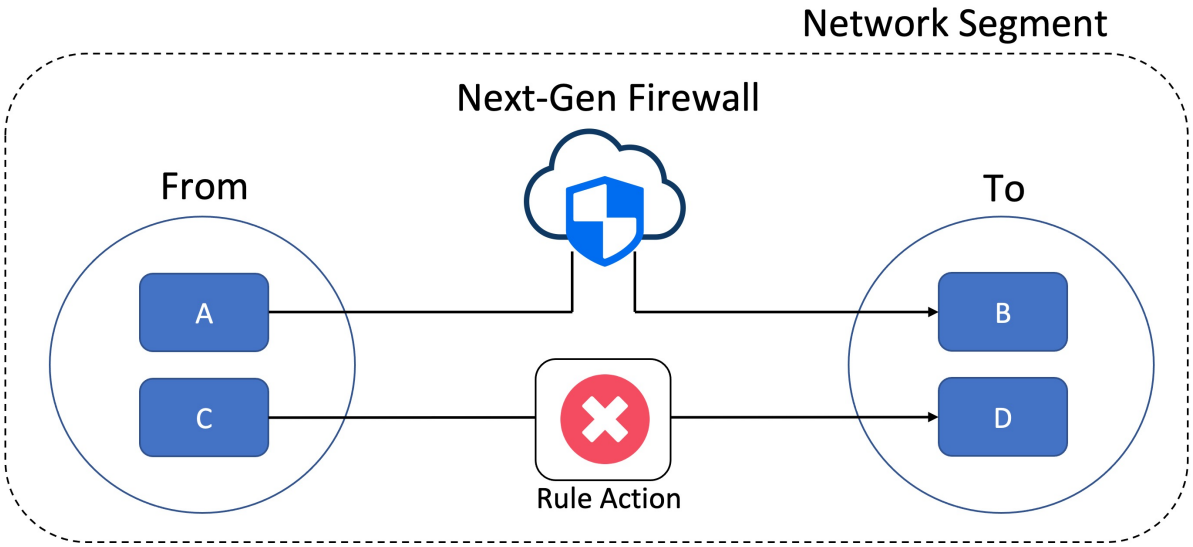
f. Optionally, enable firewall autoscaling. Firewall autoscaling, as the name suggests, allows horizontal scaling in and out of the next-generation firewall instances deployed in the Alkira Cloud Exchange Point based on required real-time capacity demand. You can set the minimum and maximum number of the firewall instances deployed with autoscaling to make sure there is sufficient minimum of firewall capacity always available for the typical use and a sufficient maximum firewall capacity for the burst use. During the off-peak hours, when firewall load subsides, Alkira solution will automatically scale in the firewall capacity by bringing down the unneeded firewall nodes, potentially all the way down to the minimum specified number.

Step 3:

Define Alkira Intent-based Policies For The Next-Generation Cloud Firewall Redirection

Organizations create Alkira intent-based policies and rules in order to forward the application traffic to the globally provisioned next-generation firewalls. Rules identify the traffic of interest to be subjected to Firewall inspection. Traffic of interest can be identied based on 6-tuple matching (including DSCP) or based on a deep packet inspection capabilities in the Alkira Cloud Exchange Points. Alkira intent-based policies identify the communicating source/destination parties and the particular network segment they belong to (different segments can have different policies). Communicating parties can be different cloud instances, remote sites communicating to the cloud, remote sites communicating to the Internet and so on. A single Alkira intent-based policy can have multiple rules.

The Alkira Cloud Services Exchange can also enforce basic allow/drop security rules for the traffic of interest without the use of the fully featured stateful Firewall.



Rule1: Send traffic from A to B to the Firewall for inspection
Rule2: Drop traffic from C to D (no Firewall inspection)

Figure 6: Cloud Firewall Traffic Redirection

Step 4:

Single-Click Provisioning

Provisioning the entire global on demand multi-cloud network and network services is done in a single click! Alkira Cloud Services Exchange will automatically instantiate all the necessary elements required to establish global on demand multi-cloud network connectivity and network services, based on the created point-and-click design. Alkira service billing will start incurring charges after all cloud infrastructure elements had been provisioned.

Based on the extent of the network design, for example the number of geographic locations, remote sites, public cloud instances and network services, the provisioning cycle may take as little as ten minutes. Alkira Cloud Services Exchange Portal provides a progress bar to keep you updated on the provisioning cycle. Your global multi-cloud network is ready for use immediately after the provisioning cycle completes.

Customer Benefits

Alkira Cloud Network as-a-Service allows organizations to turn networking and security from a business inhibitor to a business enabler, while providing the following main benefits.

- Faster time to cloud reduces deployment time from months to minutes in full alignment with business SLAs
- High bandwidth, low latency network between remote users, on-premises sites, public clouds (AWS, Microsoft Azure and GCP) and SaaS/Internet applications, and between multiple public clouds or multiple regions of the same public cloud
- Eliminate cloud-specific limitations by building a multi-region, multi-cloud overlay network, leveraging cloud-native and advance routing and security constructs
- Global security policy enforcement by leveraging firewalls of choice and global symmetric traffic steering
- Elasticity to accommodate on demand capacity, e.g. periodic high-volume data transfers, seasonal retail customer uptake, etc.
- End-to-end segmentation between remote users, on-premises sites, public cloud instances, cloud network services and SaaS/Internet exit points for compliance and sensitive or secure applications
- Pay as you go/subscription consumption cost model to ensure customers are charged for only the network and network services resources they actually consume
- High availability and resiliency backed up by high uptime service guarantee
- Full visibility to eliminate operational blind spots and improve day-2 operations

Summary

Alkira Cloud Network as-a-Service, powered by Alkira Cloud Services Exchange®, is industry's first solution offering global unified network infrastructure as-a- service. With Alkira, enterprises can have a consistent and significantly simplified experience deploying a global cloud network for end-to-end and any-to-any network connectivity across users, sites, and clouds with integrated network and security services, full day-2 operational visibility, advanced controls, and governance. The entire network is drawn on an intuitive design canvas, deployed in a single click and is ready in minutes!

The Network. Reinvented for Cloud.®

alkira

2001 Gateway Place,
Suite 610W, San Jose,
CA 95110

+1 855-925-5472

www.alkira.com