alkira

White Paper

Network Segmentation and Shared Application Services

Network Segmentation and Shared Application Services

Adapting networks to accommodate the hybrid mix of on-premises, cloud, and multi-cloud delivered applications can often mean being constrained to the lowest common denominator in terms of network security and virtualization capabilities. Individual building blocks of the enterprise network fail to form a cohesive whole leading to compromises in adherence to industry best practices.

Businesses seeking to adopt a more flexible IT infrastructure are tasking their application teams to embrace the speed and agility offered by cloud. However, they are slowed down as network teams search for ways to deliver secure network isolation across disparate cloud providers, enterprise networks and regional backbones.

Key Challenges

As enterprises look to build their future network there is an increased focus on incorporating cloud as a first-class citizen, capable of supporting the full suite of core application services, and with a broad range of accessibility options from on-premises sites and remote users. However, building cloud-first networks while maintaining the rich segmentation capabilities and extranet services required to support modern enterprise security demands presents various challenges:

- **Lack of Capabilities:**
  Cloud providers' network constructs lack native support for comprehensive segmentation capabilities. Where such capabilities do exist, they are oftentimes complex to configure and difficult to operate.

- **Limited Scale:**
  Cloud-native routing constructs within the cloud providers' networks have varied and constrained IP prefix limits. This can be exacerbated when attempting to deploy multiple network segments which further increases IP prefix counts.

- **Inconsistency:**
  Inconsistent methods of delivering an end-to-end segmentation across the on-premises networks, remote users, and multi-region/multi-cloud environments. This is also true for delivering segmentation capabilities for B2B and extranet environments, especially if such environments span multiple public clouds.

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.

Simple to Deploy, Enterprise-Grade Network Segmentation

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 CTO.

The Alkira Cloud Services Exchange® (Alkira CSX), industry's first cloud network as-a-service (CNaaS) solution, empowers network teams with secure and globally available Alkira Cloud Backbone interconnecting users, sites, and clouds. Leveraging the intuitive Alkira CSX Portal, administrators can quickly and easily carve out network segments to securely isolate tranches of their IT infra-structure spanning diverse sets of environments. Once centrally defined, network segments are instantly available across the entire global network without the need for hop-by-hop definition or complex routing protocol configuration. Each of the isolated segments can be mapped to the array of Alkira connectors enabling a common segmentation methodology for remote access, on-premises, and cloud connections, even where the underlying infrastructure does not natively offer segmentation capabilities or where such capabilities are offered in a limited fashion. For even greater isolation each segment can be further micro-segmented into discrete groups, enabling policy-based traffic control and service redirection within a segment.

Understanding Alkira Segmententation

Within the Alkira solution, a segment represents a unique routing and policy space, with each segment capable of supporting overlapping IP addressing and independent route policy. A segment is akin to a network-wide VRF or MPLS VPN, providing an identical standard of secure network isolation without the associated complex deployment and operational burden. Simply configure the segment name and it is instantly available across all the Alkira Cloud Exchange Points (Alkira CXPs) in the Alkira Cloud Backbone.

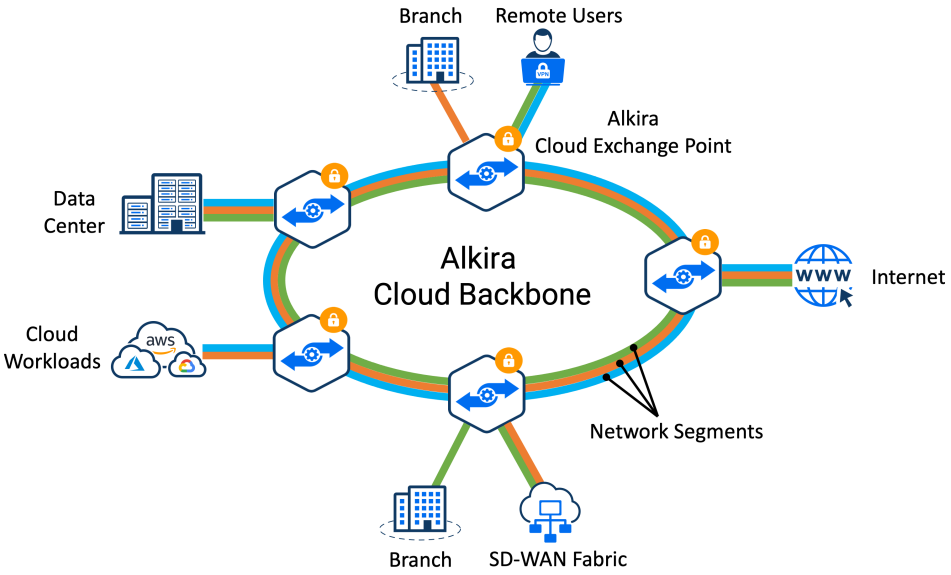

Figure 1: Segmentation Across the Alkira Cloud Backbone

All connector types within the Alkira topology, both cloud and on-premises, can be mapped to any of the available segments to form an isolated virtual network. Certain connector types, for example SD-WAN and AWS Direct Connect, additionally support the extension of segmentation deployed in the broader enterprise into the Alkira Cloud Backbone, and vice versa. While the remote access connectors allow for the mapping of users to varying segments based on the user identity supplied at login.

Combining segmentation capabilities with Alkira's unique approach to cloud and multi-cloud connectivity further enables administrators to seamlessly extend segments to, through and between the cloud providers. Alkira network segmentation does not require deployment of any virtual appliances into the customer's cloud environment. It relies on the capabilities of the Alkira Cloud Exchange Points to enforce segmentation on the attached connectors.

Understanding Alkira Micro-Segmententation

Alkira's approach to micro-segmentation centers around the concept of groups which enable the further subdivision of segments into discrete policy domains. Groups pool together a collection of connectors requiring common policy handling. Using Alkira's intent-based policy administrators can now implement granular control of intra-segment traffic based on 6-tuple and/or application-based traffic identification and enforcement.

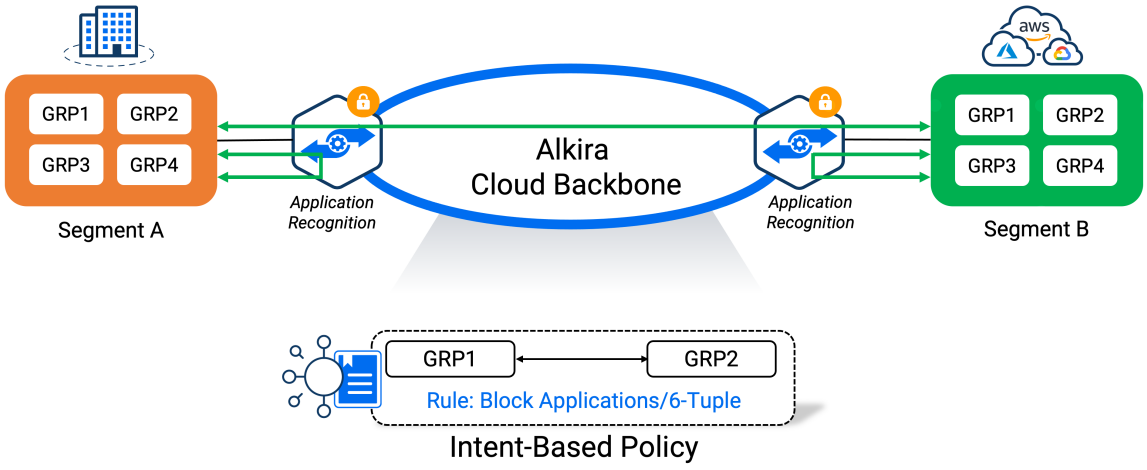

Figure 2: Micro-Segmentation with Alkira Groups

Intra-segment policy can optionally be supplemented with a range of third-party security services available through the Alkira Network Services Marketplace. Groups can be mapped to an auto-scaling set of the next-generation cloud firewalls hosted within the Alkira Cloud Exchange Points, allowing administrators to deploy consistent security policy across the environment. Alkira's solution makes sure to symmetrically route the traffic across the firewalls in single-region, multi-region, and multi-cloud scenarios.

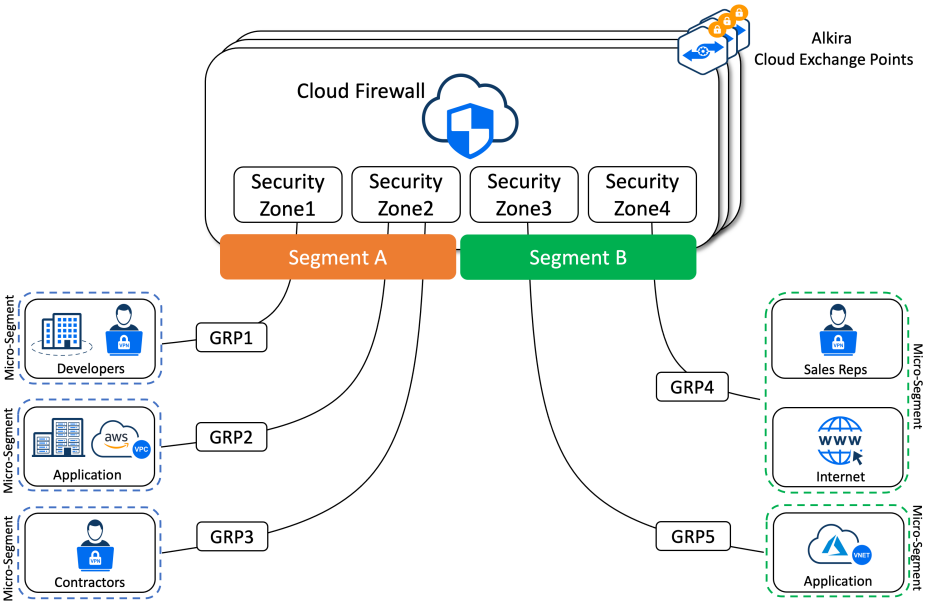

Figure 3: Firewall Service Insertion with Micro-Segmentation

Applying Alkira's Secure Segmentation and Micro-Segmentation

Network segmentation is an essential component in modern enterprise security architectures to constrain both incidental and malicious lateral movement within the network across a range of use cases, as well as limit the security attack surface. Alkira's segmentation solutions enable organizations to incorporate their current best practice approaches across both on-premises and cloud without the cost and complexity of legacy approaches.

Compliance with information security standards is complex in on-premises environments, this complexity only increases as organizations build environments that extend into one or multiple cloud providers. The complexity further increases as additional firewalls and other security services are deployed to the various cloud and colocation environments supporting the organization's cloud footprint. Alkira segmentation provides a simple, consistent, and easily auditable solution that assists organizations to meet their compliance obligations regardless of where applications and data are hosted. In addition, the Alkira Network Services Marketplace allows for the consolidation of security infrastructure with intelligent insertion for any flows traversing the Alkira Cloud Backbone.

Administrative isolation of environments can be crucial in a range of settings. Some of the more prominent examples are:

- Preventing bleed-through from development to production environments
- Separating customer environments from each other, as well as the corporate IT in a SaaS or service provider business
- Maintaining line-of-business independence in a conglomerate of companies whether operating in a shared services model or independently

Alkira segmentation provides a flexible choice of segmentation approaches depending on the degree of isolation required. Both segmentation and microsegmentation can be utilized independently or in combination to achieve the desired outcomes.

Extranets servicing business partners, vendors or suppliers have traditionally been built alongside an organization's on-premises DMZ infrastructure. However, as applications move to cloud these existing extranet solutions are not optimally positioned to service the hybrid network footprint. While cloud providers do offer native solutions to peer between accounts in cases where both extranet parties exist in the same provider, these features do not offer viable solutions for multi-cloud or hybrid cloud infrastructure. Alkira enables enterprises to shift to a cloud-hosted extranet with strong segmentation and policy controls for addressing on-premises, hybrid, and multi-cloud scenarios. Alkira's Shared Application Services solutions facilitate 'pin-hole' access to corporate extranet endpoints while maintaining strict isolation desirable in extranet use-cases. These solutions can also incorporate the use of the next-generation firewalls for even further security controls.

Mergers and acquisitions are a challenging process for IT teams as they balance the need to integrate the systems and data of the new company while managing potential security concerns, IP address overlaps, and variations in cloud presence. Alkira segmentation and Shared Application Services empowers IT teams to simultaneously isolate and integrate the acquired entity while managing conflicts and addressing security gaps.

Inter-Segment Transit with Alkira Shared Application Services

The strict isolation offered by Alkira segmentation ensures a high-level of security for environments sharing the common Alkira Cloud Backbone. However, there are cases that require limited communication between isolated segments, such as extranet, shared services and M&A scenarios. This is where Alkira Shared Application Services offers enterprises a robust solution that maintains strict isolation of domains while permitting constrained, policy-controlled access between segments.

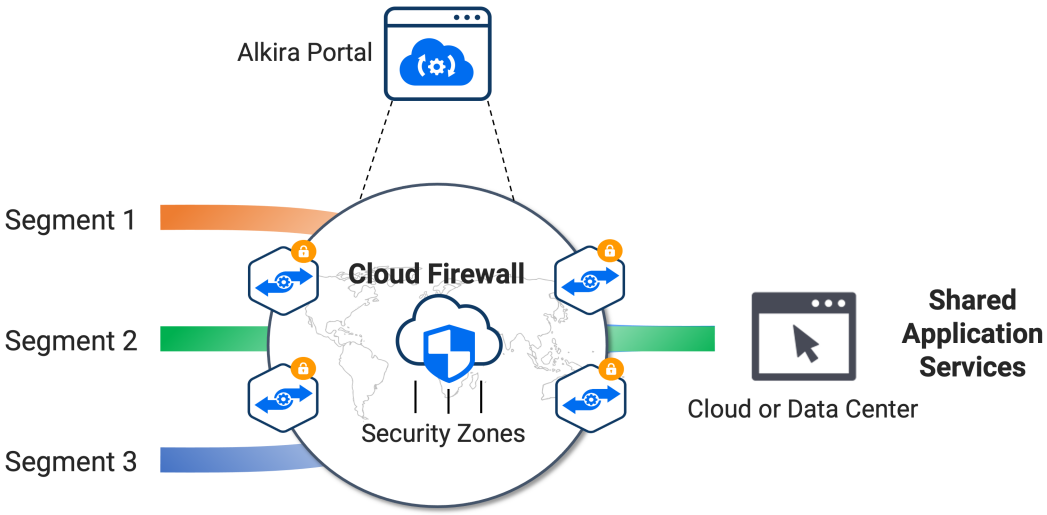

Figure 4: Alkira Shared Application Services

Traditional route leaking requires arcane configuration, complex operations and layering of multiple solutions to achieve the desired policy control. Alkira eliminates these barriers with an easy-to-use interface that allows administrators to quickly and securely define limited cross-segment communication including end-to-end policy, NAT to address IP overlap, and intelligent insertion of network services. Alkira Shared Application Services policies are applied globally to the entire Alkira solution, meaning both the sources and destinations shared between segments can be attached to multiple Alkira Cloud Exchange Points in the global network, via cloud or on-premises connectors, without the need for hop-by-hop configuration.

Administrators can choose to limit how flows are initiated between the segments, selecting either unidirectional or bidirectional communication. This added flexibility can help eliminate accidental inter-segment transit when origination of flows should only be permitted from one of the segments involved in the application sharing configuration.

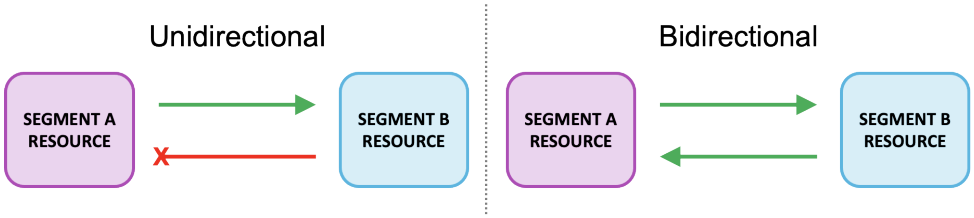

Figure 5: Shared Resource Flow Origination

Resolving Overlapping Prefixes

It is not always possible to ensure unique IP addressing amongst segments when implementing Shared Application Services, particularly in extranet and M&A scenarios. In the event that address overlap does exist, Alkira NAT capabilities can be implemented alongside Shared Application Services to maintain IP uniqueness. Alkira offers both bidirectional (1:1) NAT or unidirectional PAT when communicating across segments. When implementing bidirectional (1:1) NAT for a group of hosts the Alkira policy engine allows for the definition of a subnet-based translation reducing the administrative burden in managing a large volume of NAT translations.

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

Securing Inter-Segment Transit

Enabling communication with potentially untrusted entities requires strict policy control to ensure the security of enterprise systems. Alkira's policy engine provides granular control to restrict inter-segment communication based on 6-tuple or application matching with intelligent insertion of third-party security services. Administrators can choose to permit, deny, or redirect traffic to security appliances hosted within the Alkira Cloud Exchange Points. Integrating third-party services, instantiated from the Alkira Network Services Marketplace, allows organizations to continue utilizing their existing security policy and management tools.

Empowering IT Teams With Rich Visibility Into Network Operations

The Alkira CSX Portal provides IT teams with the ability to centrally monitor global network operations. View application flows in real time, check the health of on-premises and cloud connectors, and visualize network policy, including segmentation and inter-segment Shared Application Services.

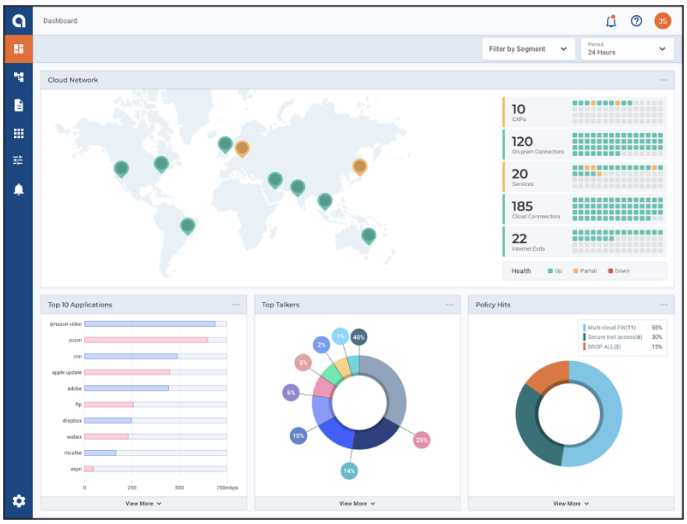

Figure 6: Alkira CSX Portal Monitoring Dashboard

The Alkira CSX portal offers a single view of the global routed network with detailed insights into per-segment routing tables. With Alkira's route visualization there is no need to interrogate devices hop-by-hop, or piece together topology data from disparate sources.

Figure 7: Per-Segment Route Visualization

Benefits of Alkira Segmentation and Shared Application Services

Alkira is changing the game by offering enterprises simple, ubiquitous, and consistent network segmentation capabilities based on business requirements, unshackling enterprise IT teams from the constraints and complexity of the traditional architectures.

- Create secure isolation alleviating complexity with Alkira's simple, automated, and easy to audit segmentation capabilities
- Extend segmentation into cloud and on-premises networks without reliance on the underlying infrastructure support
- Extend segmentation across a single region, multi-region, and multi-cloud environments in minutes not months
- Create cloud-based extranet services that can instantly extend and adapt to new business partners and regions
- Implement advanced and secure architectures with no requirement for extensive training
- Incorporate existing best-of-breed network security vendors into enterprise cloud network infrastructure allowing the re-use of existing policy and tooling and avoiding resource duplication and overprovisioning
- Single platform for deployment of secure segmentation and full end-to-end operations and management, enhancing security and visibility into cloud network infrastructure

How to get started

Getting started is easy. It requires no training and takes minutes to set up and provision through a simple 3 step point-and-click operation from the Alkira CSX portal.

Step 1
Register for the Alkira Service

Registering for Alkira service is the first step to enabling global on demand cloud and multi-cloud connectivity.

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 CSX portal to start building your network

Step 2
Define Segments and Groups (microsegmentation)

Creating Alkira segments is a simple process; just specify the desired segment name and BGP ASN to be used when peering the segment to networks outside the Alkira CSX. The segment will automatically be propagated to all Alkira CXP regions without the need for any routing protocol configuration.

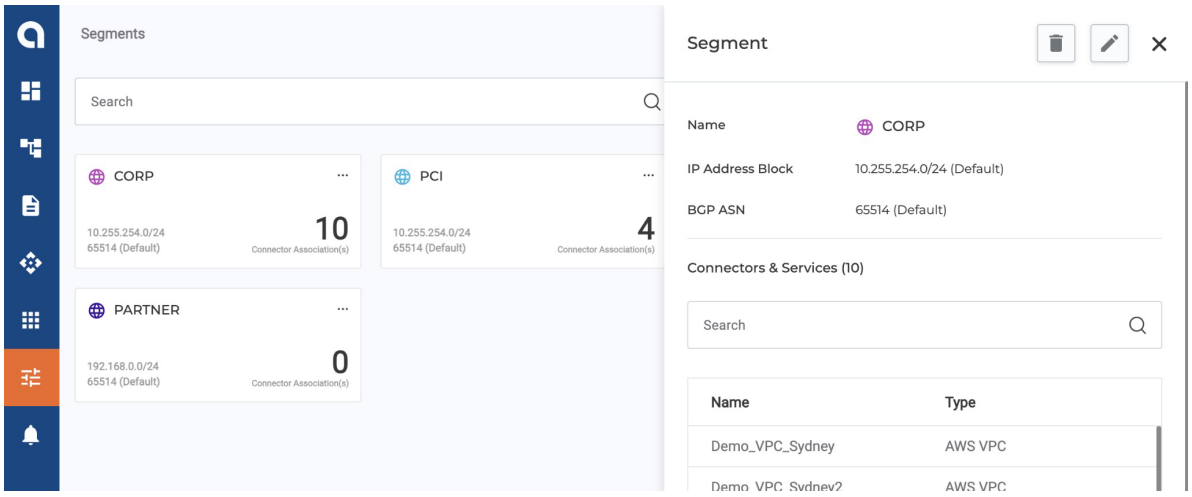

Figure 8: Define New End-to-End Segment

Defining Alkira groups for microsegmentation is just as straightforward. Just define the group name and it is immediately available to be used in Alkira policy.

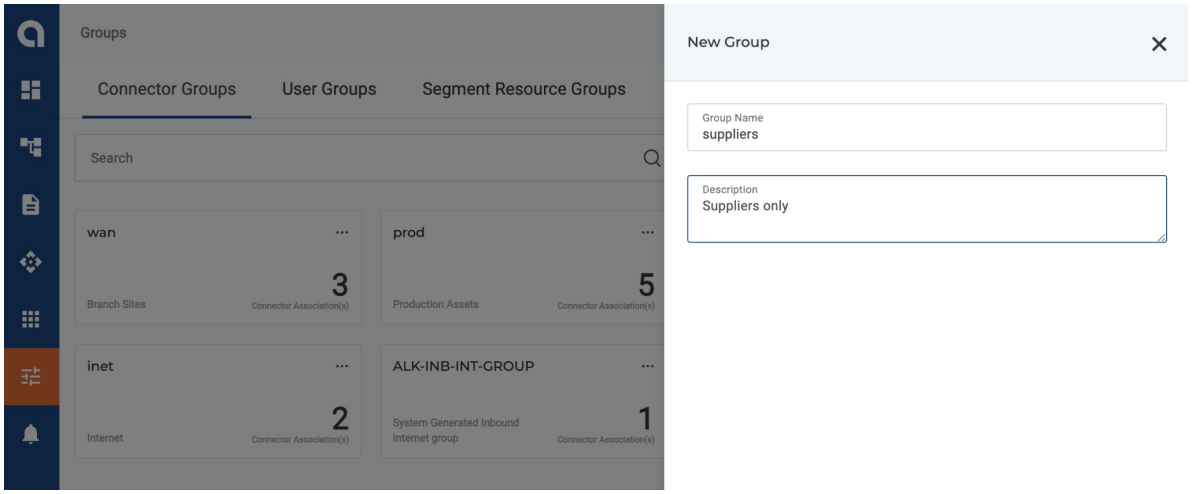

Figure 9: Define New Group for Microsegmentation

Once defined both segments and groups can easily be applied to any connector as it is added to the Alkira fabric.

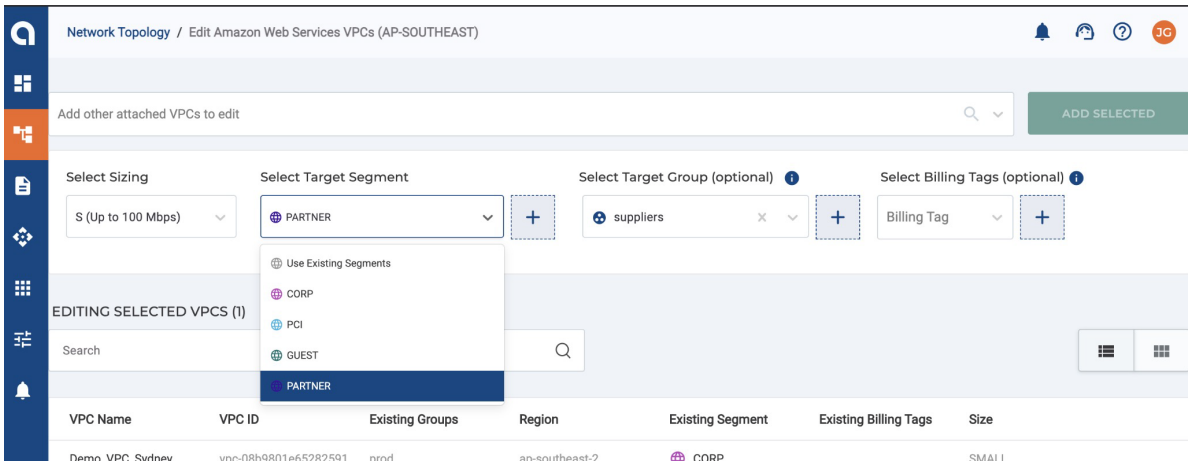

Figure 10: Assign Connectors to Segments and Groups

Step 3

Single-Click Provisioning

Provisioning the entire global multi-cloud network is done in a single click. Alkira Cloud Services Exchange will automatically instantiate all the necessary elements required to establish global segmented network connectivity with network services, based on the point-and-click design.

To sign-up for Alkira service, please navigate to https://www.alkira.com/create-account to get started or reach out to contact@alkira.com for any assistance.

Summary

Alkira is reinventing networks for the cloud era with Alkira Cloud Services Exchange®, the industry's first cloud networking as-a-service (CNaaS) solution. 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