the GORILLA GUIDE® to...

Cloud Area Networking

The Network. Reinvented for Cloud.®

TEREN BRYSON

alkira

POWERED BY ActualTech MEDIA

THE GORILLA GUIDE TO...®

Cloud Area Networking

By Teren Bryson

ACTUALTECH MEDIA

6650 Rivers Ave Ste 105 #22489
North Charleston, SC 29406-4829
www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

EDITORIAL DIRECTOR
Keith Ward

DIRECTOR OF CONTENT DELIVERY
Wendy Hernandez

CREATIVE DIRECTOR
Olivia Thomson

SENIOR DIRECTOR OF CONTENT
Katie Mohr

PARTNER AND VP OF CONTENT
James Green

WITH SPECIAL CONTRIBUTIONS FROM ALKIRA
David Klebanov
Richard Darnielle

ABOUT THE AUTHOR

Teren Bryson has spent over 25 years in the network engineering space as a practitioner, consultant, and IT leader with responsibility for large and critical systems infrastructures. He is currently the Director of Engineering and Operations for the Bluetooth SIG, Inc. where he leads the IT and Software Development teams and has leadership responsibility for a large multi-cloud deployment.

ENTERING THE JUNGLE

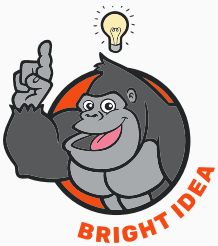
CALLOUTS USED IN THIS BOOK

SCHOOL HOUSE

The Gorilla is the professorial sort that enjoys helping people learn. In this callout, you'll gain insight into topics that may be outside the main subject but are still important.

FOOD FOR THOUGHT

This is a special place where you can learn a bit more about ancillary topics presented in the book.



BRIGHT IDEA

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

Discusses items of strategic interest to business leaders.

ICONS USED IN THIS BOOK

DEFINITION

Defines a word, phrase, or concept.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

PAY ATTENTION

We want to make sure you see this!

GPS

We'll help you navigate your knowledge to the right place.

WATCH OUT!

Make sure you read this so you don't make a critical error!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

Welcome to The Gorilla Guide® To… Cloud Area Networking, Express Edition. In this book we're going to discuss modern cloud networking paradigms and how the Alkira Cloud Area Networking platform solves the challenges associated with the inherent weaknesses in do-it-yourself (DIY) software and hardware approaches. We'll discuss how the Alkira solution revolutionizes networking by applying the cloud principles of ubiquity, elasticity and as-a-service consumption on the cloud network infrastructure. Moving to the cloud doesn't mean giving up security or reliability, either. To the contrary, you should expect, when done correctly, to increase reliability, security, and overall robustness of your cloud environment.

This book is meant for the IT architects and engineers looking to solve complex cloud and multi-cloud networking and network security challenges, while still being accessible to, and providing a good overview for, IT leaders charged with responsibility for the entire cloud lifecycle from instantiation to operation. Budget-minded executives will also benefit from this book as we delve into cost savings and operational efficiencies.

With that in mind, we'll dive right in to the first chapter with a discussion of the current state of networking, and why the time has come to reinvent the network for the cloud era with Alkira Cloud Area Networking.

CHAPTER 1

Why the Time Has Come for Cloud Area Networking

The cloud has become the dominant force in modern computing infrastructure. The public clouds are the targets of a mass move of data processing, storage, and network infrastructure from on-premises legacy data centers and colocation facilities with bare metal infrastructure.

Multi-cloud infrastructures are quickly becoming the dominant force in cloud networking. No longer are most networks homed in on a single public cloud provider. In many cases, multiple cloud providers are used to host different applications and infrastructure, introducing new and unique challenges to network governance.

While most of the IT world from storage to compute has changed to take advantage of new technology developments both on-premises and in the cloud, on-premises networking has remained firmly and somewhat stubbornly locked in the past. Cloud networking itself is advanced and complex to manage, especially when operating in a multi-cloud environment.

Given these new realities, it's clear that on-premises traditional networking is simply not up to the task of interoperating efficiently with the newer cloud networking paradigm.

Cloud Networking Challenges

Networks have always been complex, with specialized knowledge and experience required to keep the proverbial trains on the tracks, but it has taken an exponential leap forward in complexity over the last few years. Networks were more rigid in the days of bare metal servers, physical infrastructure, and fixed perimeters, all of which made them—in some respects—simple as well.

Then came along virtual machines and virtual networking. Now we have our physical network attaching to virtual devices—essentially software applications hosted on bare metal servers—acting as endpoints and transits in our networks.

This is also when we started seeing overlay networking—a network on top of a network—to gain flexibility in bridging the needs of our virtual infrastructure with our physical underlay network. That created two networks to manage: the underlay connections of the physical gear, and the overlay network where the logical traffic flow between services occurred.

The cloud arrived next, and it fundamentally altered the compact we network engineers had with our networks. The rules in the cloud included new constructs and principles, doing away with large swaths of the traditional features and principles we had grown accustomed to in our on-premises deployments. It wasn't until enterprises became serious about the cloud that this presented a challenge, as operators looked for network and security features which simply did not exist, or were severely limited, in the cloud-native world.

Integrating cloud networking into existing infrastructure, along with the requisite skills to architect and maintain the solution, was challenging enough when there was just a single public cloud. But almost overnight, it seemed, there were multiple clouds with competing features and functionality, and a desire by the business to utilize more than one. This presented new challenges.

A Multi-Cloud Future

While not every enterprise is fully cloud-centric yet, and not all of those that are have assets in multiple clouds, the future is clear: Multi-cloud will be the dominant paradigm of cloud deployment modalities as we move into the future. Routing between those clouds will continue to be a key architectural challenge in modern network design.

A Multi-Cloud Morass

Each public cloud provider, while ostensibly providing similar offerings, implemented their networking stacks very differently. Everything from the terminology and functionality to billing and visibility was different between each cloud.

This introduced an entirely new set of problems. Now we had to connect between our on-premises data centers, any collocated data centers, and *multiple* public clouds. The era of multi-cloud had officially been born, and all aspects of networking from load balancing and security, to routing and switching, was going to have to change.

For some time, however, it didn't. We struggled with multi-cloud connectivity, cobbling together all sorts of solutions with the proverbial bailing wire of our trade, peering and routing, and called it good enough. There are many challenges to getting it right, and many pitfalls along the journey. It soon became apparent that "good enough" was anything but. Network engineers were becoming stretched thin trying to develop and maintain knowledge of multiple clouds and the vagaries of the networking stack as implemented on each. Outages were becoming more commonplace than ever before. And the business was suffering as a result.

So, what options are we left with, and how well do each solve the growing problem? Let's take a look at each solution, and how it stacks up.

On-premises

On-premises environments operate in a much different manner than their cloud counterparts, leaving organizations moving some or all of their infrastructure to the cloud with several untenable choices.

Leaving on-premises equipment in place for cloud networking, using colocation facilities and onramp services is highly inefficient, slow, complex, and costly. Investing more money into this paradigm doesn't scale well and trades nimbleness for a "we've always done it this way" mindset.

Going Cloud-Native

Building your network using the native capabilities of the varying cloud providers is another challenge, largely due to the vast differences between the capabilities and deployment modalities of each cloud.

While cloud-native is the goal of many organizations, and a laudable one at that, it brings with it a set of challenges very different than the on-premises datacenters of the past. Cloud-native does not mean we're dependent on the native tools of a particular cloud. We are free to choose from among the best tools the marketplace has to offer when it comes to our network infrastructure, as an example.

Additionally, while it may seem that relying strictly on the capabilities of the public clouds is a solid choice, those capabilities do not approach, in many cases, the levels of reliability and robustness needed to be considered enterprise grade. Cloud service outages can and do happen, and

when that happens you can be dead in the water if you rely on that component for your network traffic.

Building using the cloud-native capabilities of each cloud is also an operational nightmare, as each provider has their own methods of providing what turns out to be very disparate architectures.

The DIY Approach

Some organizations have gone down the path of creating virtualized DIY networks in and across cloud providers, largely using centralized controllers to orchestrate VNFs. This is an improvement over relying solely on the cloud-native capabilities of each provider, but still requires a solid understanding of the underlying infrastructure, as well as the varying complexities of each VNF or other type of virtualized appliance. Now there are two complexities, and while the result is much more robust and predictable in uptime and overall reliability, the management of it is more complex than relying on the cloud providers alone.

Network as a Service

The last choice in network infrastructure deployment modalities in the cloud is a Network-as-a-Service model. This provides the ultimate abstraction of the underlying cloud infrastructure, presented as a service for on-demand consumption.

This matches with the cloud mentality of consuming vs. building. Instead of focusing on building your own virtualized infrastructure on top of the cloud provider's networks, you rely on someone else to build the infrastructure and manage the underlays across clouds. This allows you to consume network services on an as-needed basis, with no need to build and maintain your own VNFs or other solutions, obviating the need for additional hardware purchases, or software downloads. This is the foundation for cloud area networking.

Cloud Area Networking

Cloud Area Networking is cloud infrastructure offered as a service on top of the underlying cloud providers' infrastructure. Cloud providers have spent billions on their architecture, all of which can be leveraged to provide global, elastic, and highly available network and security services, all backed by enterprise grade SLAs.

Cloud Area Networking (**Figure 1**) offers end-to-end connectivity between users, sites, edge computing environments, Software-as-a-Service (SaaS) applications, and various clouds. This connectivity is high-speed, low-latency, and fully encrypted, offering faster delivery and transit times than DIA or MPLS circuits. The days of pulling dedicated circuits just for transit are gone. Cloud Area Networking offers flexibility in speeds and connection options, providing for a true consumption, "use as you go" model. All while abstracting the complexities of the underlying cloud providers' infrastructure.

Cloud Area Networking offers integrated network and security services, as opposed to instantiating VNFs from a cloud provider's marketplace where organizations struggle with provisioning, connecting, monitoring, scaling, and load balancing.

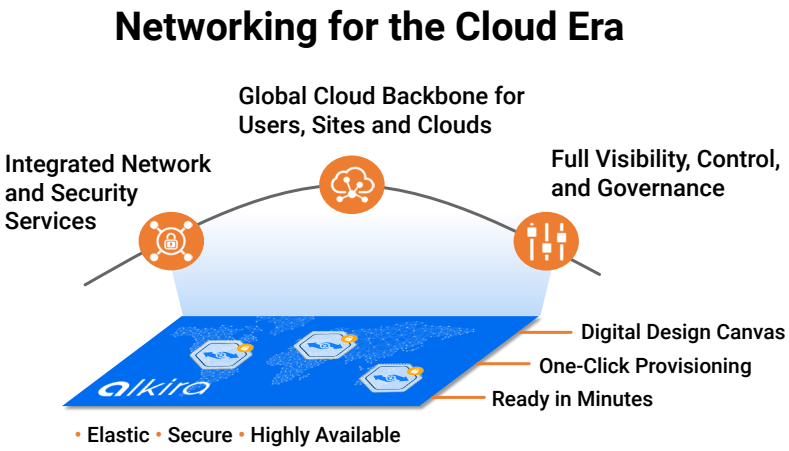


Figure 1: Cloud Area Networking architecture

Examples of integrated services include DNS, DHCP, IPAM, NAT, IDS/IPS, ADC, WAN optimization, SIP gateways, next generation firewalls, WAFs, as well as the integration of cloud-native services. The cloud network as-a-service is a fully featured, consumption-based model for delivering network and security services in a seamless, easy to instantiate and operate manner.

Visibility, control, and governance are critical pieces of any network. Maintaining those as organizations transition to the cloud can be challenging. Luckily, with the Cloud Area Network, those controls and levels of visibility allow for a strict governance model that easily matches on-premises traditional infrastructure and, in many cases, far surpassing it. You shouldn't lose features or functionality when transitioning to the cloud, and the Cloud Area Network makes certain that you don't.

Often, network infrastructure is difficult to design correctly, and a successful architecture begins with a detailed and annotated set of drawings. The cloud makes this process even more complicated, simply due to the underlying architecture and the amplified differences between cloud providers.

The Cloud Area Network allows you to create network topologies using a visual interface while still maintaining fidelity to the highly performant and architecturally sound design principles of modern network infrastructures. Abstracting the underlying complexity allows for graphical point-and-click design of cloud infrastructure, without having a deep level of expertise in multiple cloud providers' offerings. This democratizes the process of creation, while simultaneously guaranteeing good design principles.

One-click provisioning of cloud infrastructure allows for a fully functional system to be up and running in minutes or hours, rather than weeks or months. All without costly hardware to purchase and deploy, or manual VNF deployments at the edge or in the cloud. The ability to fully stand up new sites quickly, while connecting cloud workloads and inserting stateful security services, drastically shortens the

time-to-value cycle of deploying technology. This allows organizations to operate their IT infrastructure with a level of nimbleness not seen in traditional on-premises or public cloud deployments.

Traditional network designs have served us well over the years, changing incrementally with each new generation of technologies. The cloud represents a paradigm shift of unprecedented proportions, however, and as such requires a new way of thinking about our IT systems.

Taking the Next Step

The move to the Cloud Area Network is inevitable as it's the only practicable way to consume network infrastructure across multiple cloud providers, as is the common modality these days. Preventing the further rise of shadow IT while providing a competitive advantage in network and security deployment methodologies is driving organizations to the Cloud Area Network as the logical next step in the continued evolution of our architectures.

Next, we'll talk about how the Alkira Cloud Area Network platform delivers a dramatically simplified experience of deploying a cloud networking solution for the most critical enterprise needs.

CHAPTER 2

Alkira Reinvents Networking

While most of the IT world from storage to compute has changed to take advantage of new technology developments both on-premises and in the cloud, networking has remained firmly and somewhat stubbornly locked in the past, as we've discussed.

Cloud networking itself is advanced, of course. But it's complex to manage, especially when operating in a multi-cloud environment, the most common modality these days. And on-premises traditional networking is simply not up to the task of interoperating efficiently with the newer cloud networking paradigm.

Alkira's unique solution to this problem uniformly connects on-premises and cloud networks, bringing both into the modern age. Alkira Cloud Area Networking® simplifies the complicated by simultaneously taming cloud networking complexity and adding value with point-and-click deployment models, as well as supporting a DevOps approach with Infrastructure as Code and a rich set of APIs. Alkira was founded on the idea that enterprise networks should be as simple as Software-as-a-Service (SaaS). Consume only what you need without costly hardware purchases or complicated software configurations, and let Alkira handle the underlying complexities of multi-cloud routing at scale.

Alkira Cloud Area Networking

Alkira Cloud Area Networking is the industry's first cloud network as-a-service solution with integrated security, services, visibility, and governance (see **Figure 2**). It's built upon a highly available and resilient network of globally distributed Alkira Cloud Exchange Points, or CXPs, providing any-to-any high-bandwidth low-latency connectivity between remote users, on-premises sites, and cloud workloads. As a global, on-demand multi-cloud network, it was created from the ground up to provide customers with the power of the cloud in an easy-to-consume package—while still providing visibility and governance at levels enterprise network practitioners have come to demand.

The Alkira Cloud Area Networking design offers you flexibility in the deployment of your network. Alkira CXPs are strategically distributed multi-cloud points of presence across the globe—spanning all major cloud providers to offer backbone connectivity across a diverse multi-cloud infrastructure. They're virtual network infrastructure constructs—not just a single virtual network function (VNF).

CXPs utilize cloud-native architecture, abstracting the underlay networks and services already present in the cloud, while offering advanced enterprise-grade networking, security, and operational capabilities. That smooths the complexities of each unique cloud in

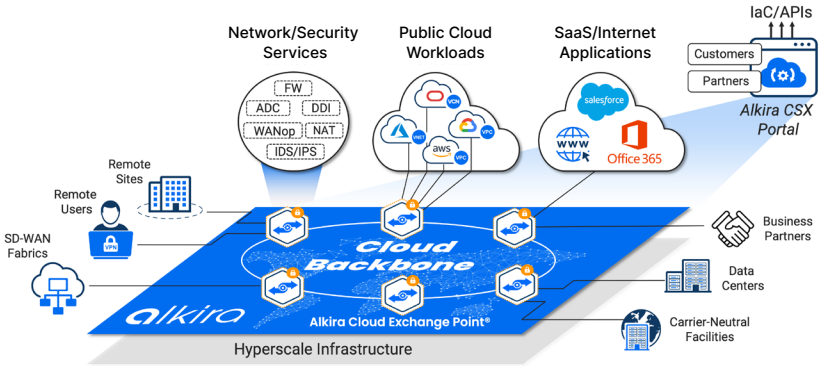


Figure 2: Alkira Cloud Area Networking platform

favor of an intuitive, easy-to-consume design canvas. CXPs allow for the software-defined management, control, and data plane modalities, but customers don't have to deep dive into each cloud provider's particular nomenclature and paradigm. They are the key elements in delivering global network and cloud connectivity, intent-based policies, end-to-end segmentation, and auto-scalable network services insertion.

Delivered as a Service for Easy Consumption

Alkira Cloud Area Networking is delivered as a service-based offering similar to SaaS. Like most SaaS offerings, it all begins with logging in to an online portal using the credentials you receive during the onboarding process. This takes you into an intuitive design canvas where you can begin building your network across Alkira regions, which span the globe at strategic geographic locations. The Alkira solution is remarkably easy to consume and easy to instantiate. It requires no complex commands or deployment buildouts, and there's no agents to install nor expensive hardware to purchase or license. It also requires no knowledge of deep cloud architecture, which means you can deploy much more quickly and greatly shorten your time-to-value realization. Instead of days, weeks, or even months, you can be up and running in minutes or hours.

Software-as-a-Service Is Easy to Consume

Software as a Service (SaaS) is easy to consume because the provider of the software maintains the infrastructure (compute, storage, networking) needed to deliver the software. As contrasted with Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) products, both of which require more effort for the IT practitioner, SaaS is consumed as needed with no maintenance work required for it to operate.

Simplified Cloud and Multi-Cloud Deployment

Single and multi-cloud deployments are made dramatically easier with Alkira Cloud Area Networking, eliminating the cloud networking complexity with point-and-click deployment using Alkira's design canvas to instantiate robust networks. Alkira's networking within a single cloud or between multiple clouds is easier and significantly more advanced than using cloud-native capabilities, most of which are restricted and more complex because of their different design paradigms, terminologies, and deployment methodologies. And, as you would expect from SaaS, the design canvas provides a modern and consistent dashboard from which to instantiate and monitor your networks. Does your organization lack cloud expertise? It's no longer an issue.

The Alkira design canvas allows you to visually create your network in a manner that's simple and intuitive, yet comprehensive. You begin by defining the global regions within which your network needs to operate, which yields a visual representation of those areas on the screen. There are Alkira CXPs across the major cloud providers' networks, with more being added constantly. This approach ensures that wherever you have business, inside or outside the cloud, there's a presence of Alkira's global cloud network infrastructure that will match your needs. Aligning Alkira's points of presence with cloud provider's regions helps to ensure the most efficient, low-latency routing across the Alkira cloud backbone.

Extend your network functionality to whatever scale and scope you need by adding connectors to the Alkira CXPs. These can tap into a multitude of methods ranging from cloud connectivity and direct Internet Access (DIA), to SD-WAN fabrics and VPN tunnels. Instantiate a connector to Amazon Web Services (AWS) and within seconds you have a working cloud connection to your AWS workloads. Do the same for Google Cloud Platform (GCP), Microsoft Azure, or Oracle Cloud (OCI)

and you now have an instant any-to-any multi-cloud network. You can do all of this without having to deep dive into the technical differences between cloud routing methodologies or fret about the complexity of connecting multiple clouds. This is where the true power of the Alkira's solution becomes apparent.

It doesn't stop there, however, as there are other connection options readily available within the Alkira design canvas. You can just as easily create connections to elements, like on-premises data centers or remote facilities, either by directly connecting via IPSec tunnels, or by extending existing SD-WAN deployments into and across the Alkira CSX. Those elements then become available to communicate to one another, the various public clouds or SaaS and Internet applications. And these connections can be sized to the appropriate scale for your existing needs, growing in the future as business dictates. Even if you're using physical colocation facilities, those can be easily connected into the multi-cloud network using high-speed private cloud cross-connects available from cloud services providers.

All communication between elements connected to different Alkira CXPs occurs over the Alkira cloud backbone leveraging cloud providers' hyperscale infrastructure, with segmentation, dynamic routing, and high availability all baked into the solution.

Routing between connectors can be defined in terms of segments. A finance segment, for instance, may span multiple clouds and data centers, but by default is not allowed to talk to a human resources segment in the same location. Intra-segment traffic, known as micro-segmentation, can be selectively allowed or disallowed based on the intent-based policies you define.

Links across the cloud backbone are strongly encrypted, adding another layer of security on top of an already secure deployment model.

In addition to defining regions and connections, Alkira also allows for a granular approach to billing visibility. Billing tags round out the

offering by allowing you to create an appropriate system for back-charging departments based on cloud and on-premises deployment, network traffic usage, consumed network services and so on. Each month's itemized bill offers full transparency into the incurred Alkira service changes.

There are no costly hardware purchases for initial setup or continuing operations. The result is an overall reduction in the total cost of ownership (TCO), allowing for a quicker time-to-value realization, without worrying about constraints on supply or manufacturing slowdowns causing delivery windows to slip. Instead of over-provisioning up-front in anticipation of future growth, you can build your network as your business needs dictate, at the speed of business.

Modern Cloud Networking Done Right

Modern clouds have advanced our data centers and systems far into the future, and now the Alkira Cloud Area Networking solution does the same thing for networking, bringing it into the 21st century. No longer are we constrained by the old models of networking, predicated on outdated architectures that are no longer relevant in a cloud environment. With Alkira, we have stepped firmly into the future and have rewritten how a modern network should look and behave. Cloud Area Networking truly is modern networking done right.

Next, we'll talk about the need for security in a cloud and multi-cloud environment, and how Alkira Cloud Area Networking offers the ability to enforce consistent security policies across the infrastructure.

CHAPTER 3

Alkira Secures Your Multi-Cloud World

We've established the need for more advanced networking in the cloud, and that the Alkira Clouda Area Networking solution provides multi-cloud networking consistency, but we haven't yet talked about security in the multi-cloud enterprise architecture. Without security, the best network infrastructures are vulnerable to all manner of threats from malicious sources.

Moving services to the cloud advances the sophistication of modern cloud networks significantly. But doing so while still leaving firewalls on-premises is counterproductive. It makes more sense to move firewalls into the cloud closer to where the applications and services reside.

It's tricky to move firewalls to the cloud, however. You'll face tough challenges related to such issues as instantiation, traffic steering, availability, capacity planning, and ensuring symmetrical flows. Alkira's security solutions for cloud firewalls make the journey to cloud security simple and effective by addressing these challenges.

Moving Security to the Cloud Is Challenging

Given all the challenges of securing cloud networks, you might be inclined to throw in the proverbial towel. And while moving security services to the cloud is challenging under the best of circumstances, trying to do so in a *do-it-yourself* fashion is even more difficult. Moving to

the cloud should be about getting your security services to a place where they can be ubiquitous and provide the most value for your business. It shouldn't be about the journey itself.

Cloud Security Challenges

Many challenges exist in moving security to the cloud, the first of which is instantiation. Where do you instantiate your security devices, like the next-generation firewalls? It used to be easy—just secure the perimeter of the data centers or overall network, secure the endpoints, and be done with it. In a multi-cloud world, however, strategic placement of security services is critical to ensure symmetry, high availability, and on demand scale.

Traffic steering is a key consideration in placement of the next-generation firewalls in the cloud. Place them correctly and interesting traffic will flow in optimally to and through the firewalls, as required by policy guidelines and architecture. Place them incorrectly and you risk missing interesting traffic or having asymmetrical traffic flows that break stateful security enforcement. Ensuring symmetrical flows is a key piece of having stateful security devices in the cloud, especially in a multi-cloud environment where you're securing traffic flows between and across different regions and providers.

Capacity planning is another challenge that must be addressed. The fact is runaway cloud spending can sneak up on you if you don't plan ahead and address real-time capacity of services. One way to mitigate this problem is auto-scaling up and down in capacity and device count. Moreover, you must be able to tune your capacity, in near-real time, in order to meet SLAs and maintain reasonable cost containment.

Finally, availability of services is key to a successful security deployment in the cloud. As with the other factors mentioned previously, it's a challenge to get it right. Availability is more than just spinning up virtual appliances in the cloud, baking in redundancy, and hoping for the best if some of these virtual appliances go down. Availability

encompasses the total framework of how you deliver services in the cloud, as well as how you guarantee uptime and resiliency. Availability is of paramount strategic importance when designing and deploying your cloud strategy.

Integrated Cloud Security Services

An alternative to "dumping" security services into a cloud-native environment is intelligently onboarding next-generation firewalls into the Alkira Cloud Area Networking platform. The result is security services that are integrated into the network fabric, scale as the needs arise, and get provisioned from a centrally managed and cloud-agnostic portal. This approach makes a tremendous amount of sense and allows for a level of flexibility not found in cloud-native deployment modalities.

Cloud Security Services Provisioning

Deploying security services from the Alkira Network Services marketplace is a point-and-click affair. The provisioning complexity is abstracted as well by bootstrapping the parameters required to instantiate the next-generation firewalls in the globally distributed Alkira Cloud Exchange Points (CXPs). None of this requires any cloud architecture or cloud-specific knowledge, which is a serious boon when deploying into multi-region or multi-cloud networks. What's more, you're not subjected to cloud-native limitations regarding traffic steering capabilities or scale, and you maintain the ability to enforce the uniform zone-based firewall security policy for on-premises, cloud, and multi-cloud environments.

Alkira Policy Framework

The Alkira policy framework allows you to focus on intent-based policies rather than the complexities associated with more imperative approaches. With intent-based policies, you define the interesting

application traffic and determine whether it will be allowed, denied, or steered toward the firewalls for stateful inspection. This is based on either 6-tuple matching or application recognition.

With Alkira you can also group individual connectors together to simplify intent-based policy enforcement, then enforce policy on those groups. Any new connector—Amazon Virtual Private Cloud (VPC), Azure Virtual Network (VNet), remote site, and so forth—automatically inherits the intent-based policy of the group without any additional configuration. This further simplifies the uniform deployment of security devices and services. That, in turn, maximizes your security posture by abstracting away potential pitfalls that may be lurking in more complex deployment methodologies.

Stateful Multi-Cloud Security and Segmentation

If your traffic is in the open, all the security in the world doesn't matter. Traffic between the Alkira CXPs across the Alkira Cloud Backbone is protected using strong encryption. This means that you can rest assured that your important traffic is secured from prying eyes.

Segmentation allows you to isolate resources and prevent unwanted communication between them. It also implies segregation of the routing domains. Segmentation is particularly valuable in reducing the security attack surface and preventing attackers from unrestricted lateral moves in case of a security breach. In certain cases, cross-segment communication can be selectively allowed by leaking routes between the segments.

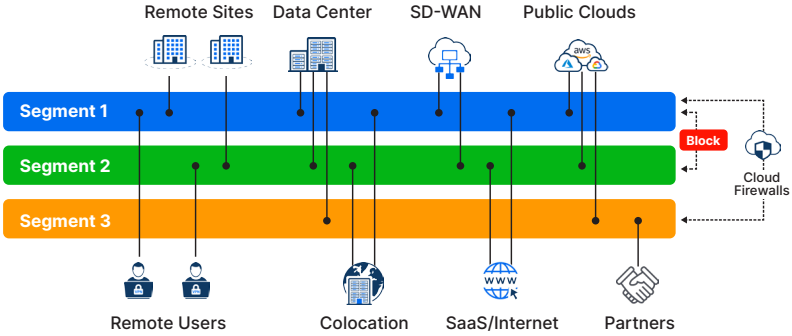


Figure 3: The Alkira Network Segmentation Architecture

Segmentation and micro-segmentation are hot topics currently, and with Alkira you have access to these modalities. Segments can be centrally provisioned and automatically span an entire network. By default, segments are isolated from one another, helping to compartmentalize resources and reduce attack surfaces (see **Figure 3**). Alkira's intent-based policy, mentioned earlier, is enforced on a per-segment basis.

Micro-segmentation with Alkira takes the form of grouping connectors within segments, thereby creating micro-segments. Application traffic within and across micro-segments can be allowed or dropped within the Alkira network fabric or steered to the firewall devices for stateful inspection. This framework offers an immense amount of flexibility in how you steer and isolate traffic across your network, and all with the ease of a point-and-click interface—it doesn't require any expansive depth of knowledge in the cloud provider's inner workings.

Service insertion and traffic symmetry are two important concepts that Alkira addresses and solves for, as well. All traffic is sent symmetrically to the firewalls, even in cases where the firewalls are auto-scaling up and down based on traffic capacity demands. In cases where there are numerous firewalls spread across multiple Alkira CXPs, traffic is symmetrically steered across multiple Alkira points of presence. This ensures that application traffic destined for a firewall isn't inspected redundantly at each CXP it traverses. This is a key concept because it effectively increases overall firewalling capacity (see **Figure 4**).

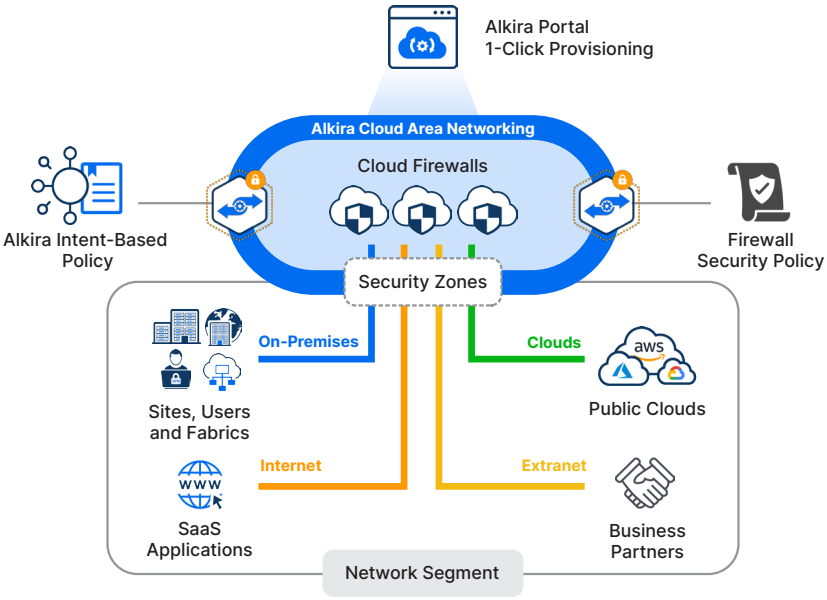


Figure 4: Alkira Cloud Firewall Architecture

Groups in Alkira map to firewall security zones, which allow firewalls deployed in CXPs to enforce zone-based security policy across on-premises, cloud, and multi-cloud environments. Firewalls deployed in traditional data center or colocation environments can be managed by the same management system as the firewalls deployed within the Alkira CXPs for end-to-end security policy consistency. It helps ensure a simplified firewall management experience and allows your team to focus on policy rather than deployment complexities.

Zero-Touch Auto-Scaling

One of the benefits of Alkira's security services instantiation model is that auto-scaling becomes trivial. Auto-scaling firewalls helps save money and resources by adding and subtracting the number of firewalls based on traffic patterns and load. Try this using cloud-native tools and you'll find it to be very difficult, but with Alkira it is, once again, a point-and-click affair.

Alkira's auto-scaling is based on real-time capacity demands, using minimum and maximum watermarks as the framework. That's opposed to a more traditional provisioning-for-peak model that requires you to deploy for the worst-case scenario. In the latter model, resources are significantly wasted when traffic volume is low. Alkira helps contain costs because the capacity and number of deployed devices more closely match real-time traffic demands. Bi-directional traffic symmetry exists across these auto-scaled deployments, with flow load-balancing across the firewalls.

Auto-scaling allows for more granular control of costs in a cloud environment. Network services, like firewalls, are only auto-scaled when needed, and are decommissioned, in real time, when not being utilized. Without this feature, costs can be high as you are paying for services sitting idle.

Security Services Operation

Good stewardship of your network includes lifecycle management of on-premises infrastructure—and devices in the cloud are no different. You still must work with licensing, but now you have a pay-as-you-go licensing model in addition to the more traditional bring-your-own-license. Alkira fully supports both options. Instantiation, recovery on failure, monitoring of performance and load, and auto-scaling are all additional lifecycle management components with which you must deal.

Alkira offers full visibility into which traffic is sent to the firewalls, in which security zone that traffic sits, and how much traffic exists in the network. Additionally, the work of your security team is simplified because security policy management happens through a unified vendor UI. That means security team members can continue to manage the firewalls as they always have, whether they be on-premises, hybrid cloud, or spread across multiple public clouds.

Advanced Cloud Security Use Cases

Alkira's solution with integrated best-of-breed next-generation firewalls caters to a variety of security use cases. Some of the use cases we touched upon in this brief include firewall service insertion for on-premises, cloud, and multi-cloud applications, end-to-end segmentation and micro-segmentation, and consistent zone-based security policies. However, at times, more advanced use cases are required.

Cloud DMZ

Deploying a cloud DMZ provides a great example of the advantages of deploying security services with Alkira. As IT teams struggle with providing adequate ingress access to Internet-facing applications located across different data centers and cloud providers, location of the firewalls becomes key. If this isn't done correctly, you can inadvertently introduce sub-optimal routing or even security weaknesses into the system. With Alkira, ingress Internet traffic can be steered toward the firewalls deployed in Alkira CXPs. This results in a global, secure, highly available, and auto-scaling deployment which is implemented using an as-a-service model.

Shared Application Services

Shared application services provide another use case. Cross-segment communication can be allowed, while traffic is still steered toward the firewall for policy enforcement. Examples of cross-segment traffic include allowing access to shared application services from different segments, integration of mergers and acquisitions where each company is a different segment, and connectivity to partners where, again, each partner is a different segment.

Simplified Yet Powerful

In this Gorilla Guide, we've discussed the challenges associated with the cloud and multi-cloud environments, how Alkira solves these challenges using its Cloud Area Networking platform, and how security is a key factor that's an integral part of the Alkira solution.

You've seen just how complex multi-cloud environments can be, and how crucial it is to utilize a solution that offers a modern and robust approach to solving cloud networking and network security challenges. With Alkira Cloud Area Networking, enterprises can have a dramatically simplified yet powerful solution to unifying cloud and multi-cloud architectures.

To get more details about how Alkira reinvents networking and network security for the cloud era: https://www.alkira.com

Read a whitepaper on how to deploy the next-generation firewalls in the Alkira cloud network as-a-service: https://www.alkira.com/on-demand-next-generation-firewalls/

Take a self-guided tour of the solution: https://www.alkira.com/virtual-tour

Request your personalized demo: https://www.alkira.com/demo

ABOUT ALKIRA

Alkira was founded in 2018 by Amir and Atif Khan, the visionary computer networking team that created the multi-billion-dollar SD-WAN market with the founding of Viptela. After Viptela was acquired by Cisco in 2017, it was time to look for another significant customer problem to solve.

Storage and compute had evolved to be cloud-friendly and cloud-like, but the network had not, and so the idea of Cloud Area Networking was born.

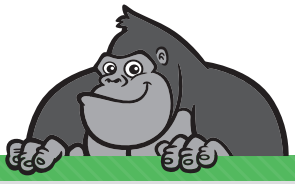
Alkira has reinvented networking for the cloud era by delivering Cloud Area Networking, the first global unified network infrastructure with on-demand hybrid and multi-cloud connectivity, integrated network and security services, end-to-end visibility, controls and governance, all delivered as-a-service.

ABOUT ACTUALTECH MEDIA

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit https://www.gorilla.guide/custom-solutions/