alkira

White Paper

Alkira Elastic Zero Trust Network Access

Industry's only solution with single-click provisioning of secure, auto-scalable and globally available zero-trust network access optimally connecting remote users to data center, cloud and multi-cloud applications in minutes

Working remotely has become a new normal for most organizations around the world turning each remote user into a "branch of one". The highly distributed nature of the modern application landscape spanning on-premise data centers, single or multiple public clouds, SaaS offerings and edge computing environments demands a secure, elastic and globally available remote access solution.

Over the years enterprises have seen an increase in users re-motely accessing corporate resources from outside of the enterprise physical security perimeter. Recent pandemic has fueled this phenomenon even further, whereby most of the enterprises have made it mandatory for their employees to work remotely. This has forced enterprise IT to either adjust their existing remote access solutions or look for a new secure, scalable and future-proof remote access solution, which addresses the needs of the cloud era.

To this end, Alkira has launched a remote access solution, part of its zero trust network architecture (ZTNA), which allows enterprises to securely connect remote users into the closest Alkira service point of presence (Alkira Cloud Exchange Point®) for accessing enterprise on-premise and cloud applications through the secure, global, low latency high bandwidth Alkira cloud backbone. The solution is horizontally scalable and delivered as-a-service with zero upfront costs in software, hardware and licenses.

Key Challenges

The rapid explosion in connectivity demand puts a significant strain on traditional do-it-yourself enterprise remote access VPN solutions that in many cases were designed for only limited or occasional use.

- Data center dependency results in limited global availability and increased cloud applications latency
- The lack of auto-scale forces wasteful infrastructure and licensing over-provisioning to accommodate peak usage or a restrictive under-provisioning to keep costs under control
- Traditional "trust, but verify" approach to security provides inadequate response to the ever-growing world of security threats

An innovative solution is needed to address the challenges around providing a global, elastic, zero trust network access.

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.

Solution Details

Architecture

Alkira reinvents networking for the cloud era by providing global network infrastructure as-a-service. With Alkira, enterprises can establish secure network connectivity between remote users, branches, on-premises data centers, multiple public clouds, regions of the same public cloud, Internet and SaaS applications through the cloud backbone of the Alkira Cloud Exchange Points (CXPs). Alkira CXPs are virtual globally distributed points of presence leveraging the public cloud infrastructure. They offer enterprise-grade network and network services capabilities with integrated management, control and data plane functions. Customers can easily select from the Alkira portal the Alkira CXPs they wish to leverage for their global network based on the desired locations.

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.

Alkira CXPs also offer the ability to enable remote access, allowing users to securely connect to the closest Alkira CXP to access applications in the cloud, on-premises data centers or the Internet. For applications hosted in remote regions, users can leverage Alkira's high bandwidth low latency cloud backbone for optimized access. Alkira's remote access VPN solution allows customers to create VPN termination points across all Alkira CXPs.

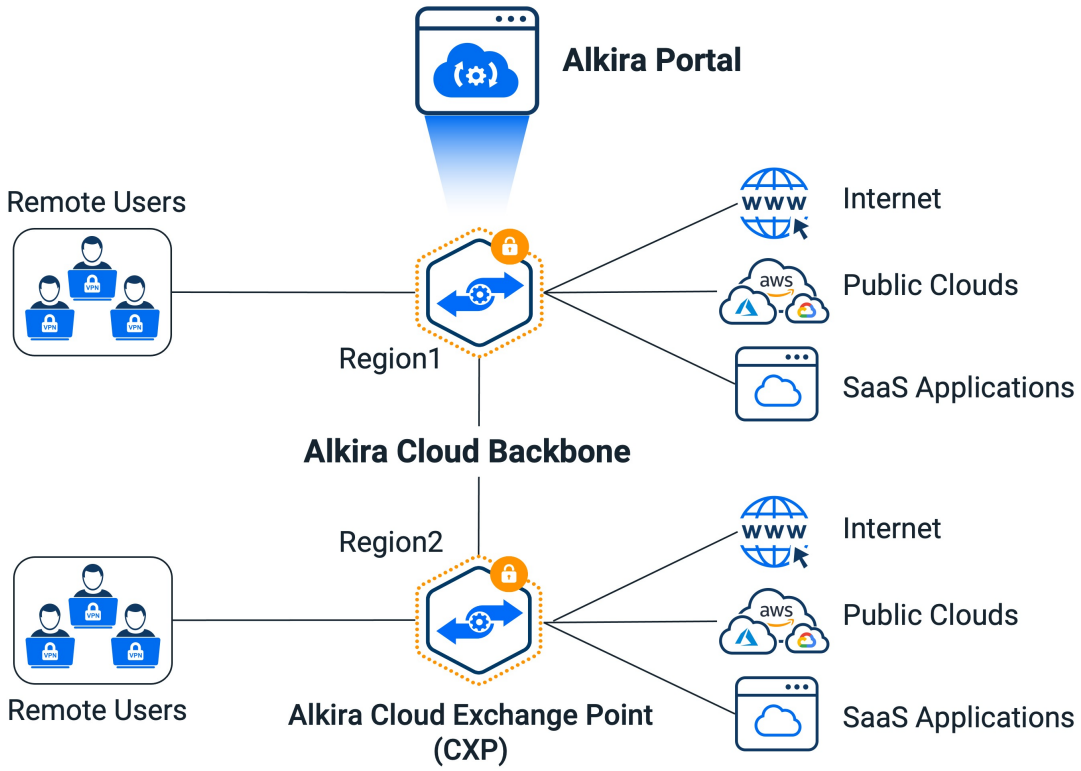

Figure 1: Remote Users Connect to the Closest Alkira CXP

Security and Performance

Historically, enterprises have hosted the remote access VPN solutions in a DMZ environment inside their on-premises data centers, where they were completely secured by the firewall security zones, and at times by multiple firewall layers for even further protection. This castle-and-moat security architecture made sense in a centralized environment where most of the applications still resided in the on-premises data centers along with the network services elements, like remote access VPN concentrators. However, over time, enterprise applications have transitioned out of the on-premises data centers and have become geographically distributed in different types of public and private clouds, as well as consumed as SaaS.

In this new world where applications are decentralized, enterprises can no longer be tied to a centralized model for network connectivity, security and remote access. Backhauling remote users' VPN connections into the on-premises data centers in order to access public cloud applications and enforce security policy adds unnecessary network latency, which negatively impacts application performance. Network functions, like remote access VPN, need to be designed and architected in a decentralized manner and the zero trust security model needs to be tightly integrated to provide both the optimal application experience and a strong security posture enforcement.

This distributed model is achieved using geo-DNS functionality, which automatically picks the Alkira CXP closest to the user location based on the user's IP address. User authentication is done through the enterprise directory infrastructure, which is linked to the Alkira remote access VPN at the time of service provisioning. Centralized user repository maintained by the enterprises avoids the need for separate credentials for remote access and at the same time allows for multi-factor authentication (MFA) if desired.

Once authenticated, remote users are assigned to a user group, which then maps to an Alkira segment. Different user groups can map to different segments without a requirement to have separate Alkira CXP remote access connectors for each segment. This approach is unique to the Alkira solution. Traditional remote access VPN solutions don't natively support segmentation, administrators are required to spin up separate VPN concentrators for each segment and treat them as separate networks, which is no longer the case with Alkira solution.

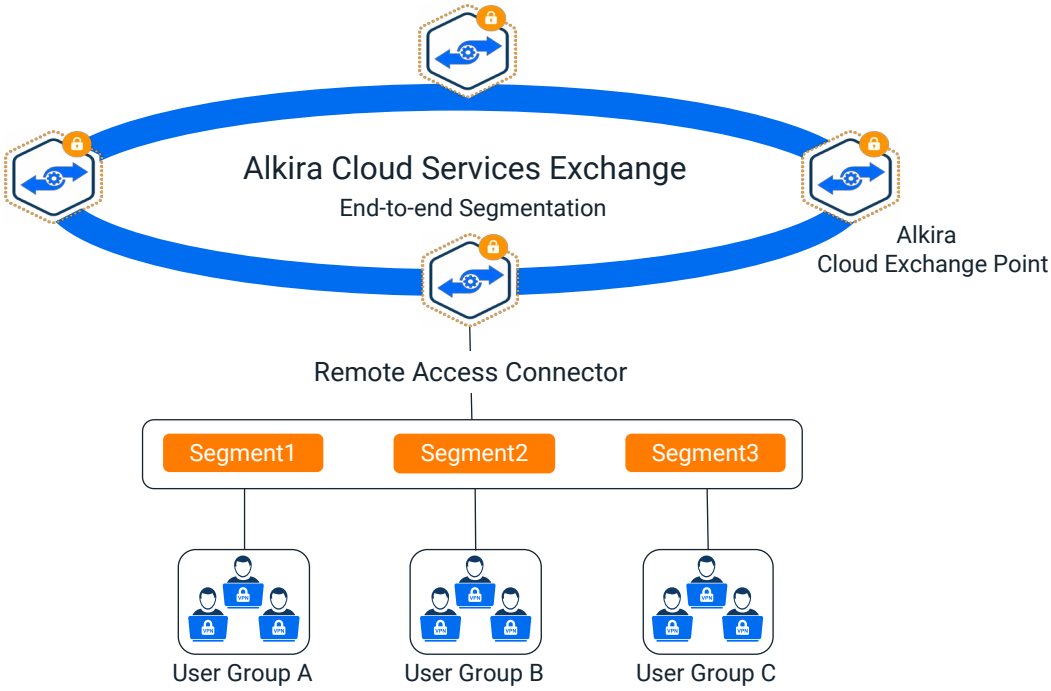

Figure 2: Alkira CXP Remote Access Connector and Segments

Remote users' access to applications is granted based on the security policies. A user is restricted access to only authorized applications by enforcing security policies defined in the Alkira portal. User traffic can also be redirected to globally deployed firewalls leveraging Alkira intent-based policies before accessing cloud or on-premises applications. More specifically, remote user groups are mapped to the Alkira groups, which are part of the Alkira segments, effectively creating a micro-segmented environment. This mapping is automatically done by leveraging attributes assigned during the user authentication process. Alkira groups are mapped to the firewall security zones. One or multiple Alkira groups can map to a single firewall security zone, but a given Alkira group can be mapped to only one firewall security zone. Based on the mapping and the desired communication patterns, firewalls will be enforcing intra-zone or inter-zone security policy.

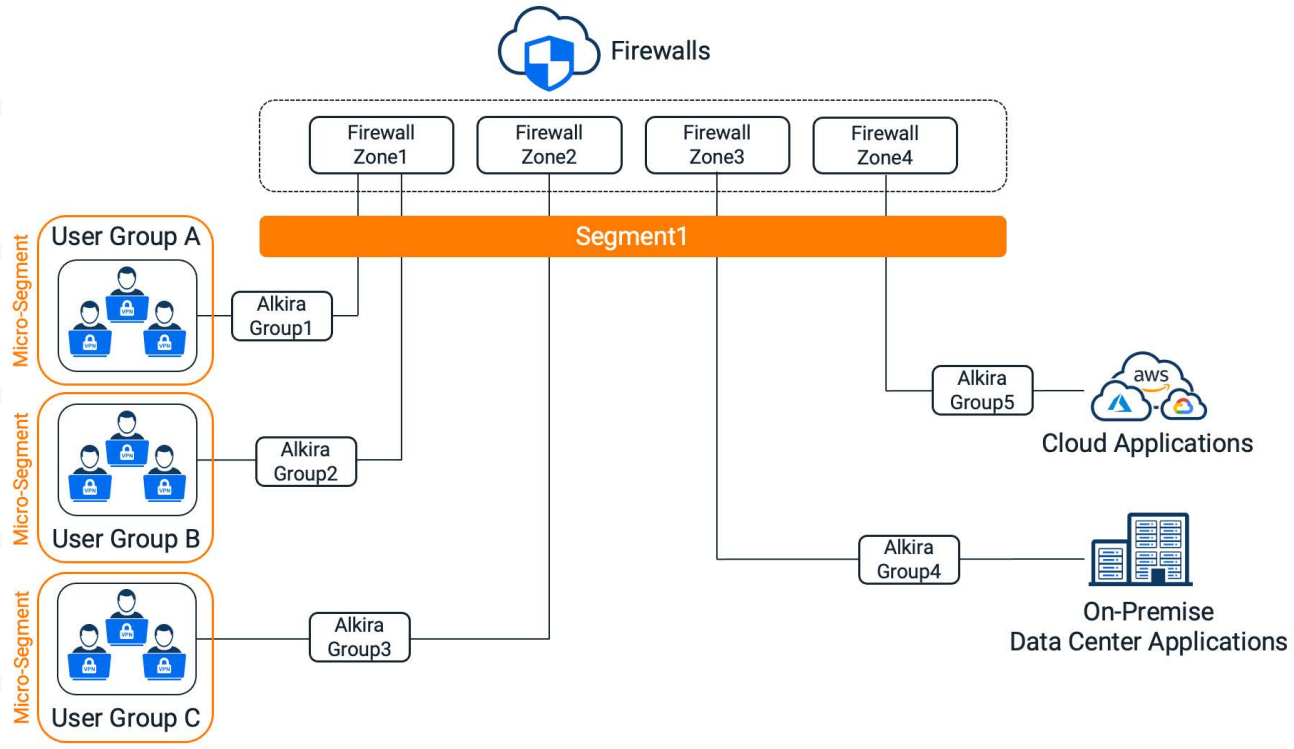

Figure 3: Micro-segmentation and Firewall Security Zone Mapping

For traffic destined to Internet and public SaaS applications, Alkira remote access VPN solution supports an approach where Internet access and security controls are applied at the Alkira CXP where remote users are connected. These security controls can be strictly enforced by the Alkira policies, firewalls or the combination of two. One good example of this behavior is the ability to block non-business critical traffic, such as peer-to-peer sharing, leveraging a combination of Alkira security policies and Alkira deep packet inspection for application recognition, while forwarding other types of traffic to the firewall for stateful security policy enforcement.

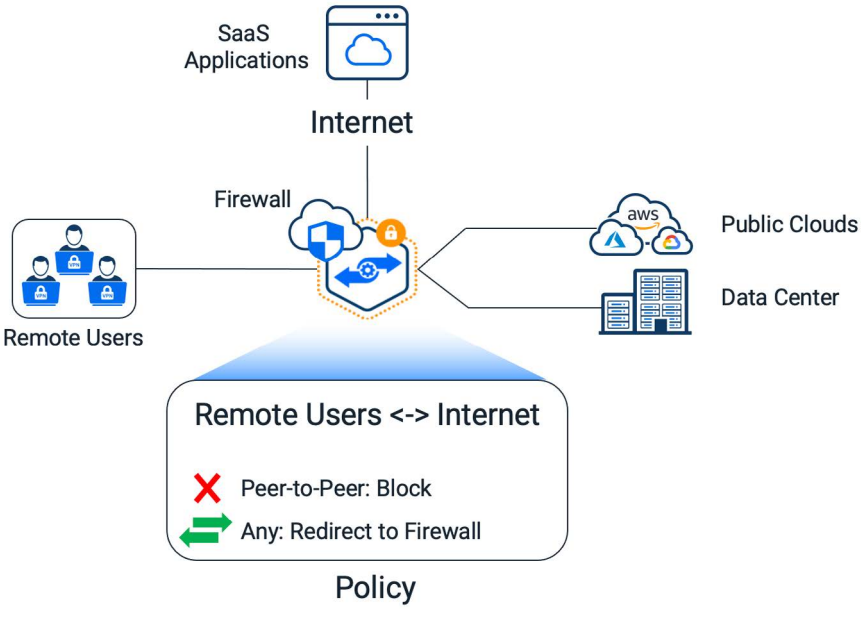

Figure 4: Internet Traffic Security

Centralized remote user authentication, segmentation and micro-segmentation, and a firewall security policy enforcement are all part of Alkira elastic zero trust network access (ZTNA) architecture that allows fine-grained controls, ensures strong security posture and significantly reduces security attack surface. Ultimately, Alkira elastic zero trust network access controls the enforcement of enterprise security policy for user-to-application traffic.

Auto-Scale

As demand for concurrent user capacity varies over time, Alkira remote access VPN solution can auto-scale up and down the service preventing over-provisioning and a subsequent over-spend. At the time of higher capacity demand Alkira remote access VPN solution can accommodate thousands of concurrent VPN connections, while each connection benefits from low latency, high bandwidth access to enterprise on-premises and cloud applications reachable across the Alkira cloud backbone.

The auto-scaling also extends to licensing, eliminating one of IT's main challenges around traditional remote access VPN solutions. In the world where teleworking has become a new norm, global availability, integrated zero trust security, auto-scaling and consumption-based pricing address enterprise's fundamental needs for the remote access VPN solution.

Operations

A solution would not be complete without a comprehensive operational toolset. Alkira portal offers full range of visibility, control and troubleshooting capabilities for the remote access VPN solution allowing enterprises to address any day-2 operational challenges. Administrators can quickly diagnose service outages, see consumed applications and network bandwidth, view real-time and historic user information, get live flow visibility, troubleshoot failed authentication attempts and so on.

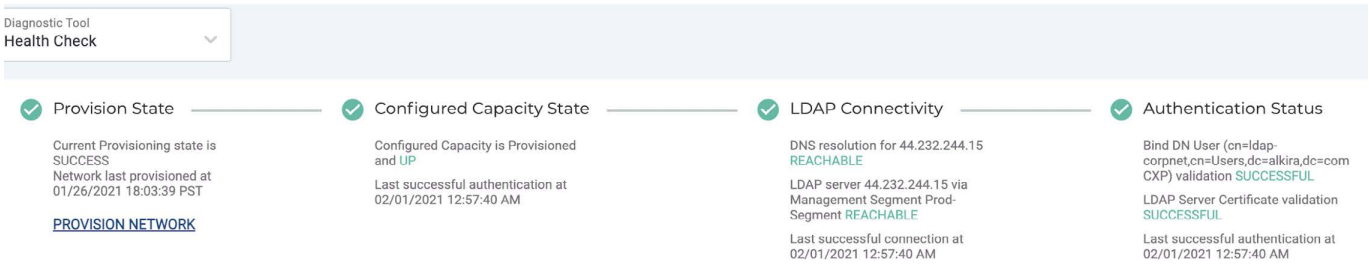

Figure 5: Diagnostic Health Check for the Remote Access VPN Service

For organizations preferring the devops model, Alkira portal exposes a rich set of REST APIs supporting all functions, including the remote access VPN.

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

Alkira Differentiation

In terms of baseline feature and functionality, Alkira's remote access VPN solution provides all the capabilities of a traditional remote access VPN solution, such as split-tunneling, user authentication using LDAP and Active Directory, multi-factor authentication integration. At the same time, Alkira offers superior and agile elastic zero trust network architecture for the remote access VPN solution built for the cloud era ensuring optimized and secure access to all applications whether they are hosted on-premises or in the cloud leveraging network as-a-service approach.

Below is a quick comparison of the main benefits of using Alkira's remote access VPN solution compared to a typical legacy VPN solution.

	alkira	Legacy Remote Access VPN
Solution Offering	Offered as a service	Do it yourself
Deployment Model	Decentralized	Centralized
Scale	Horizontally scalable	Appliance dependent
Segmentation	Multi-segmented	Separate appliance per-segment
Security Architecture	Zero trust network access	Trust, but verify
Operations	Centralized through Alkira portal	Separate tools
Consumption Model	Pay-as-you-go or subscription with no upfront costs	Perpetual with high upfront cost

Figure 6: Alkira Differentiation

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 portal.

STEP 1: Add a remote access connector for a given Alkira Cloud Exchange Point

STEP 2: Pick the authentication method, like LDAP or Active Directory, and provide authentication and certificate details for secure connection

STEP 3: Create user groups, map them to the segment and click provision to deploy remote access VPN service

Alkira is changing the game by offering an elastic zero trust network access solution to the burning enterprise remote access needs with no upfront hardware investments, no software installation and no learning curve.

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

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