alkira

WHITEPAPER

Modernizing Business Partner Connectivity

Secure, Agile, and Simplified with Alkira

Table of Contents:

Executive Summary	03
The Evolving Landscape of Business Partner Connectivity	03
Why Customers Need Robust Business Partner Connectivity	03
The Imperative of Secure Partner Connectivity	04
Current Methods of Business Partner Connectivity: A Critical Analysis	05
Alkira's Modern Solution: Secure and Agile Partner Connectivity	10
Use Cases and Customer Success Stories	11
Conclusion: Embracing the Future of Partner Connectivity	13

Introduction

In today's interconnected business world, robust and secure business partner connectivity is paramount. Traditional siloed and hardware based methods struggle to meet the demands of cloud-centric and distributed environments, leading to complexity, security vulnerabilities, and agility limitations. Alkira's Network Infrastructure-as-a-Service Platform offers a modern solution, simplifying connectivity, enhancing security, and improving agility. This whitepaper explores the challenges of traditional partner connectivity, demonstrates how Alkira addresses these issues, and highlights the benefits of a modernized approach.

The Evolving Landscape of Business Partner Connectivity

Business partner ecosystems are expanding rapidly, fueled by digital transformation and cloud adoption. This shift towards distributed operations demands secure and seamless connectivity. Alkira's cloud-native solution meets these evolving needs by supporting a comprehensive range of connectivity options, from traditional IPSec VPNs, MPLS, SD-WAN, and L2 Private Circuits to diverse cloud connectivity options.

Why Customers Need Robust Business Partner Connectivity

Expanding Ecosystems: Collaboration with suppliers, distributors, and partners is crucial for business success. Seamless data exchange and application access drive efficiency and innovation.

Digital Transformation: Digital supply chains and B2B SaaS applications require high availability and secure connections for real-time data exchange.

Business Agility: Rapid onboarding of new partners and quick adaptation to changing business requirements are essential for maintaining a competitive edge.

The Imperative of Secure Partner Connectivity

In today's interconnected business landscape, secure partner connectivity is no longer a luxury, but a necessity. The risks are substantial, ranging from costly data breaches and regulatory penalties to severe reputation damage. To mitigate these threats, a comprehensive security strategy encompassing several critical elements is essential:

1. **Data Protection: Fortifying Sensitive Information**

   Encryption, DLP, and IDPS: A robust security posture relies on a layered defense. Together, these technologies ensure data confidentiality, integrity, and availability.

2. **Zero Trust Network Access (ZTNA): Limiting Exposure**

   ZTNA ensures partners are granted access only to the specific resources required for their tasks. This principle of least privilege minimizes the potential for unauthorized access and lateral movement, significantly reducing the attack surface.

3. **Logging and Auditing: Maintaining Visibility and Accountability**

   Comprehensive logging captures detailed system and user activity, providing crucial insights for incident response and forensic analysis. Regular auditing of these logs verifies adherence to security policies and regulatory requirements, enabling organizations to detect anomalies, investigate incidents, and demonstrate compliance.

4. **Compliance and Regulatory Adherence: Meeting Legal Obligations**

   Adhering to industry-specific regulations, such as GDPR and HIPAA, is mandatory. Secure partner connectivity solutions must facilitate compliance to avoid substantial penalties and legal repercussions.

5. **Mitigating the Evolving Threat Landscape**

   Sophisticated cyberattacks targeting partner networks pose significant risks. A strong security framework is required to defend against these ever-evolving threats.

6. **Enhanced Security through Segmentation and Micro-Segmentation:**

   Isolating partner and customer networks through segmentation and micro-segmentation limits the impact of security breaches and failures to specific segments, preventing widespread compromise.

Current Methods of Business Partner Connectivity: A Critical Analysis

Traditional hardware-based deployments, operating in silos, suffer from limited scalability, increased complexity, and security vulnerabilities stemming from a lack of standardization and visibility. Addressing high availability and various failure scenarios further compounds these challenges. The speed at which these partner connectivity requirements are coming in and requiring immediate solution leaves no time for planning or strategizing on a well thought out design, resulting in reactive constant one off deployments.

Diagram 1 illustrates a common scenario where a company establishes multiple VPN connections with its business partners (A - D) through hardware firewalls located in multiple data centers. These VPN connections were created manually, resulting in a lengthy process that took weeks for each partner to go live. This was due to the manual tasks involved, such as gathering requirements, coordinating schedules, planning changes, and implementing them within a limited time maintenance window.

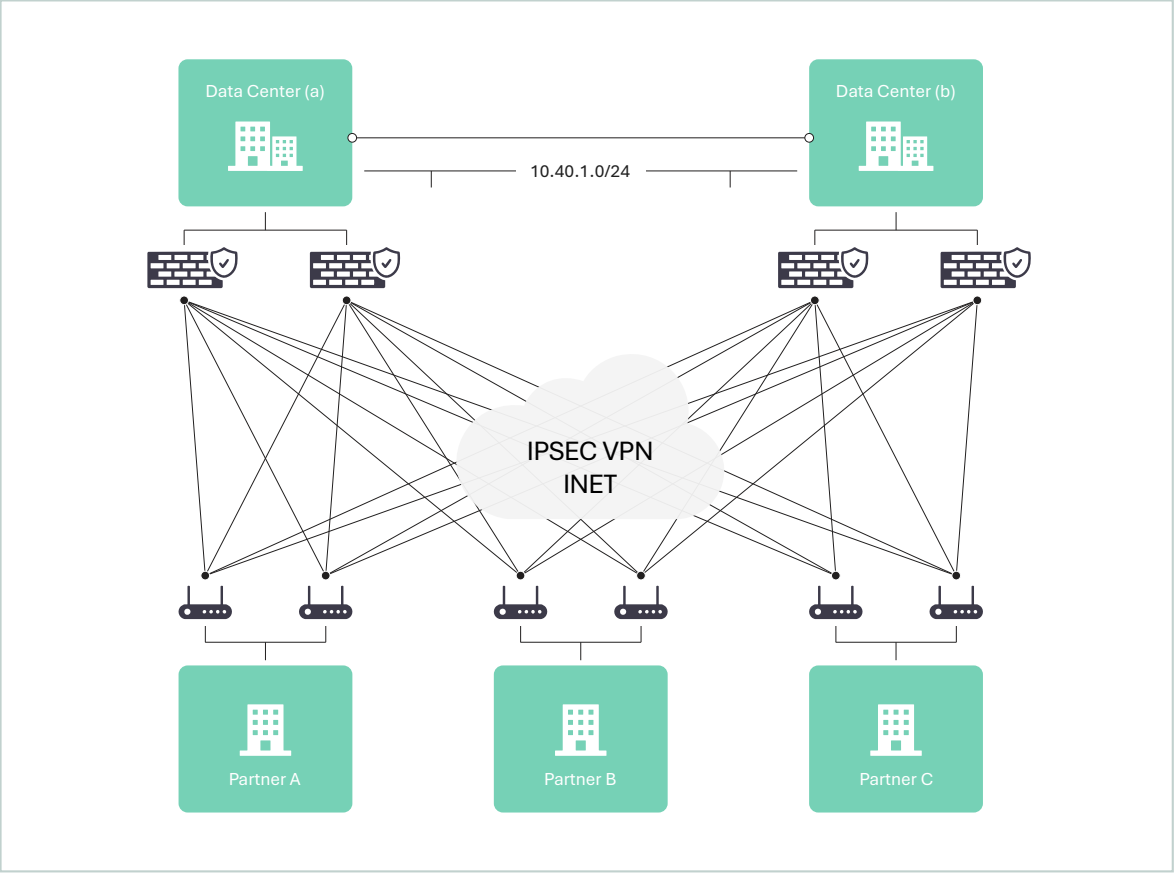


Diagram 1

Diagram 2 depicts the necessity of extending MPLS, leased lines, and colocation cross-connects (Partners G-I) to the customer's data center, a requirement frequently imposed by highly regulated business partners demanding private circuit connectivity.

Given the external nature of partner connections, robust firewall protection is essential for both security inspection and resolving IP address conflicts. While utilizing existing partner VPN firewall clusters (as illustrated in Diagram 1) might seem feasible, practical challenges in traffic steering and isolation often necessitate deploying a dedicated firewall pair, as shown in Diagram 2.

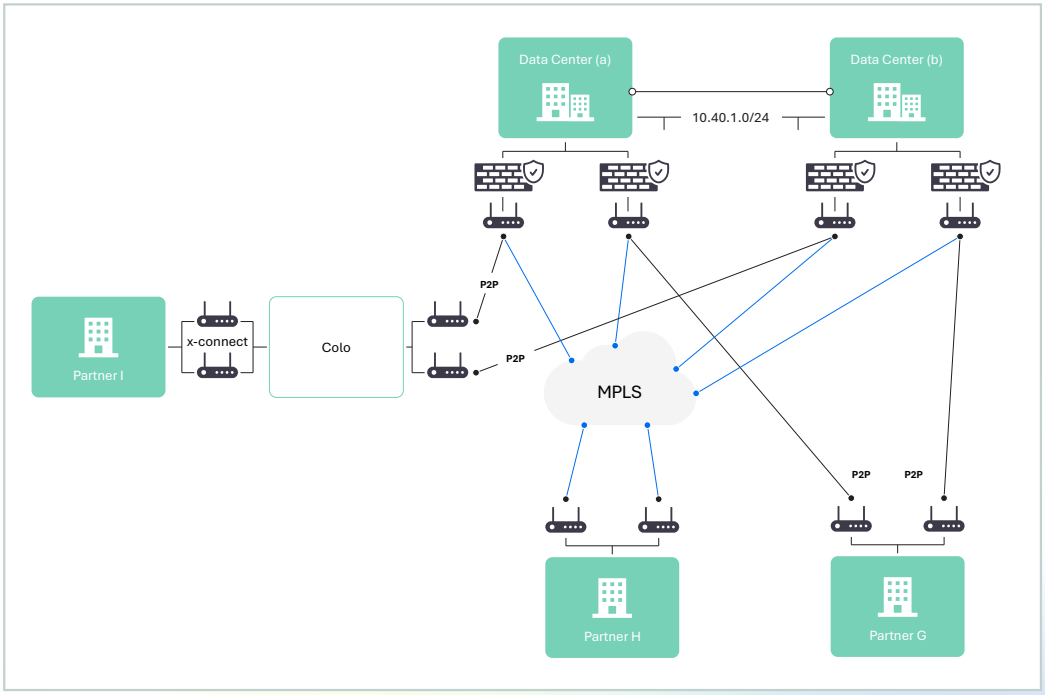


Diagram 2

Diagram 3 presents a business partner (Partner J) connectivity model where customers manage last-mile circuits and customer premises equipment (CPE) at partner sites. Enterprises frequently deploy SD-WAN solutions to simplify this model, which introduces an additional connectivity type into the production data center, requiring dedicated management and ongoing support.

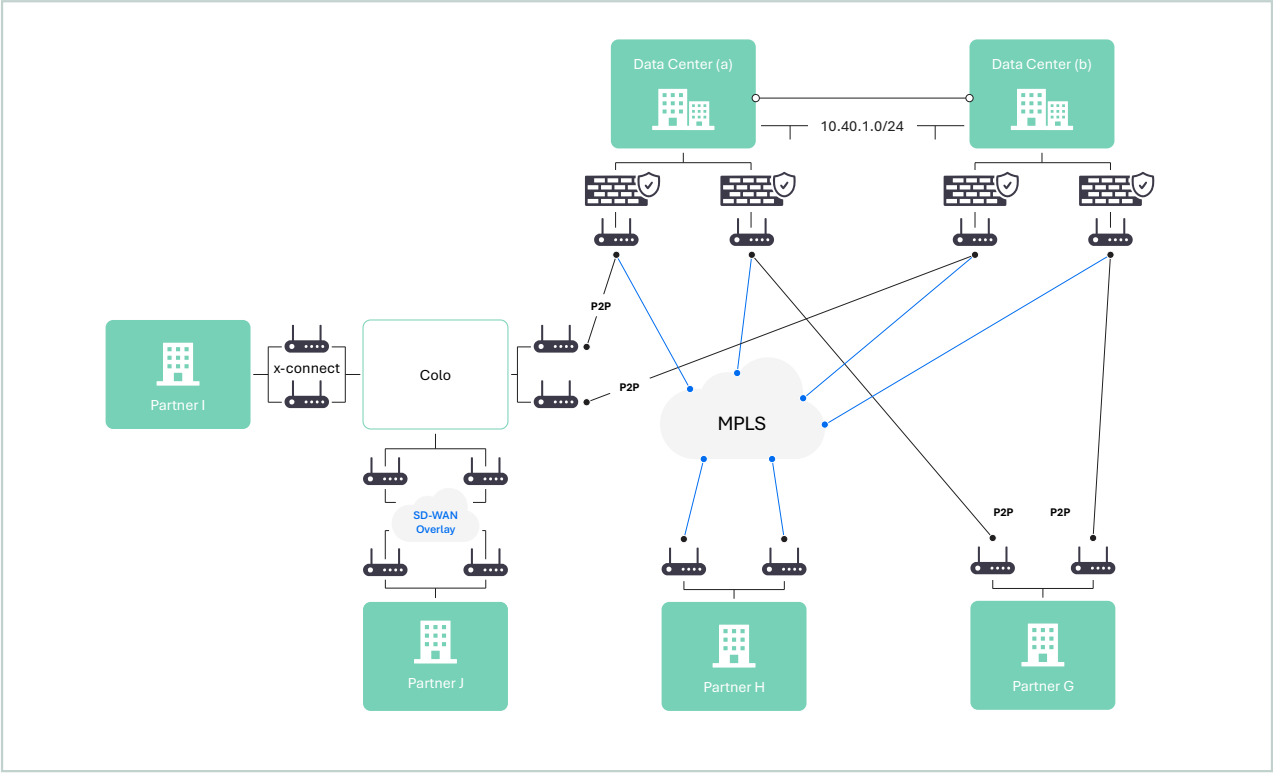


Diagram 3

Diagram 4 illustrates a growing enterprise challenge: cloud-native business partner connectivity. As partners migrate to cloud environments, the diverse connectivity models of cloud service providers (CSPs)—including AWS Private Endpoints, Azure Private Links, and GCP Private Service Connect—create significant standardization and support hurdles. While these cloud-native constructs offer benefits like localized traffic within CSP networks, they introduce complexities in visibility, scalability, management, and troubleshooting. Notably, they lack native support for granular routing controls, advanced security inspection, and IP overlap resolution. This paradigm shift also exposes a critical skills gap: cloud teams, despite their assistance, often lack the necessary network and security expertise for these scenarios, while traditional network and security teams struggle with cloud proficiency to effectively manage and troubleshoot these cloud-native connections.

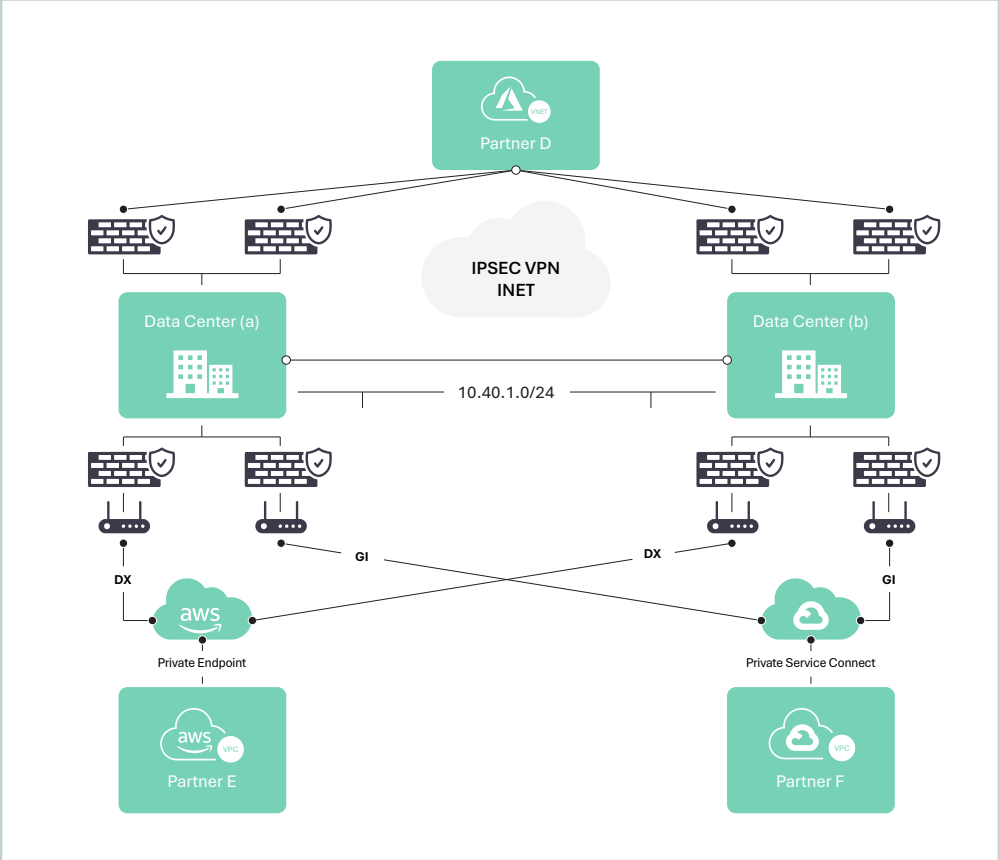


Diagram 4

We know ‘complexity is the enemy of agility.’ When we look at all the connectivity types in Diagram 5, and step into the shoes of an Enterprise Architect, we have to ask: With this complex partner network, and remembering it’s only part of the bigger picture, can we find a more efficient and sustainable way forward?

Consider the operational burden of managing this diverse setup, enforcing consistent security policies, driving standardization across disparate technologies, achieving comprehensive visibility, scaling globally, and providing robust operational support. Moreover, the inherent lack of these capabilities inevitably amplifies security risks, demanding a fundamental reassessment of the current strategy.

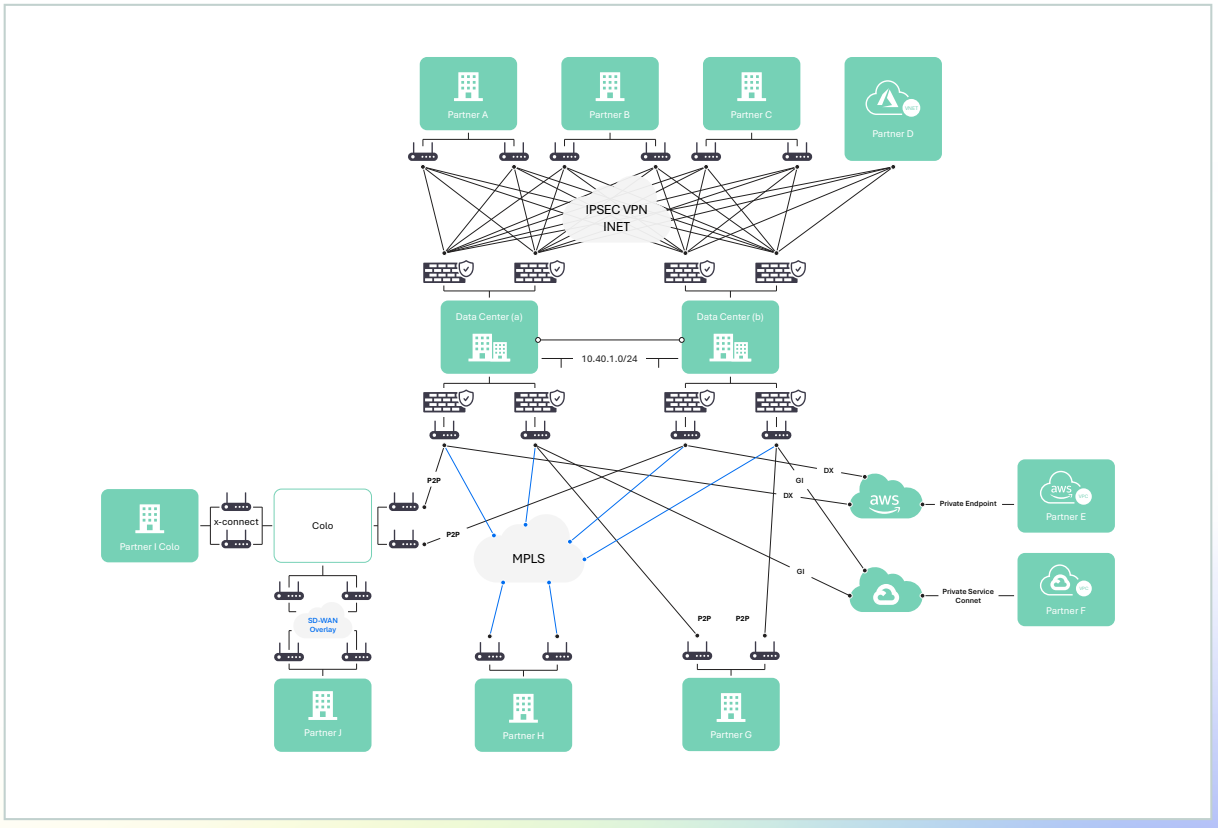


Diagram 5

Alkira's Modern Solution: Secure and Agile Partner Connectivity

Addressing the previously outlined connectivity challenges requires a fundamentally different approach. Alkira's Network Infrastructure-as-a-Service (NIaaS) platform offers a comprehensive solution for enterprises seeking agile, secure, and scalable business partner interconnectivity. Leveraging Alkira's NIaaS, organizations can rapidly deploy global networks through a click-and-deploy interface, eliminating hardware and software dependencies, as well as the need for physical colocation presence. This as-a-service model supports diverse business partner connectivity types, including VPN, MPLS, leased lines, SD-WAN, colocation cross-connects, and cloud-native integrations, providing a unified platform for diverse networking needs and more.

Diagram 6 illustrates Alkira's architectural components, centered around the Cloud Services Exchange (CSX) portal. The CSX portal provides a user-friendly interface, API integration, and Infrastructure as Code (IaC) support via Terraform. From this portal, users deploy Cloud Exchange Points (CXPs) globally. CXPs are regional constructs, spanning multiple data centers, designed for scalability, resilience, and redundancy. Upon deployment of multiple CXPs, a full-mesh, low-latency private backbone is automatically established between them. CXPs scale horizontally and vertically to meet evolving business demands, eliminating the need for complex capacity planning.

Each CXP offers advanced routing, segmentation, micro-segmentation, service insertion, and stateful security policy enforcement. This solution also integrates network services from leading vendors, including Infoblox, Fortinet, Palo Alto Networks, Cisco, and Check Point, and enables seamless connectivity to AWS, Azure, GCP, and OCI at the spoke VPC/VNET level, extending connectivity beyond the cloud perimeter into the cloud itself. Furthermore, for on-premises connectivity, administrators can extend private P2P, MPLS, IPSec over the public internet and SD-WAN for remote sites; and Zero Trust Network Access (ZTNA) for remote or mobile users. Centralized internet ingress and egress connectivity for visibility and security inspection is also provided.

Users deploy CXPs in regions proximate to their business partners and data centers. Diagram 6 depicts two segments: CORP, for corporate resources, and Extranet, for business partners. Data centers (a) and (b), located in us-east and us-west respectively, connect to corresponding CXPs. Connectivity between data centers and CXPs can be established using any supported transport method. All partner connectivity types from Diagram 5 can be terminated on Alkira's virtual CXPs, freeing customer data centers from direct partner connections.

Customers looking to go away with managing partner connections can alternatively expose their Business partner applications publicly with Alkira. Alkira will assure secure and selective access to the application by opening inbound access to that particular app from CXP while keeping the origin server privately connected with a private IP address. Alkira refers to this feature as Internet Facing Applications (IFA).

(Refer to Diagram 6) Here is how it works: the customer's application (app1) connected to the Extranet segment in the us-east CXP remains private, while Alkira generates a public FQDN (app1.alkira.com) and securely exposes the application through its internet inbound connector. Two static public IPs are created per app with the option of BYOIP. Customers can then integrate this FQDN with their preferred cloud proxy and do a CNAME mapping if desired and provide the ability to steer the incoming traffic via NGFW before accessing the origin server. In addition to the business partner connectivity, Alkira also provides connectivity to private SaaS peering.

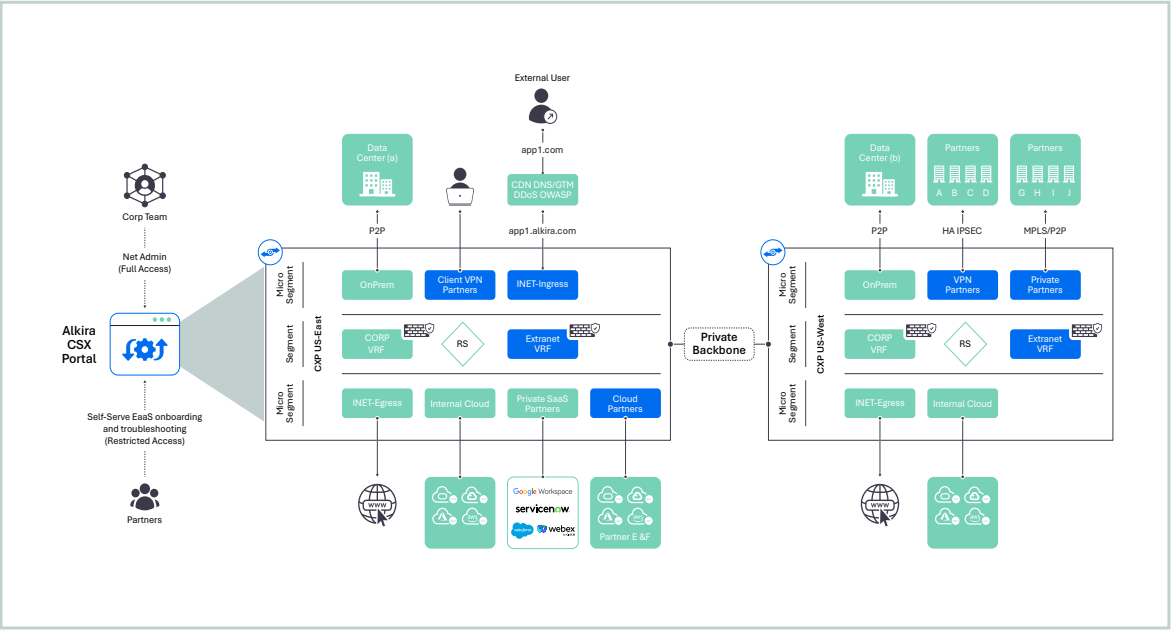


Diagram 6

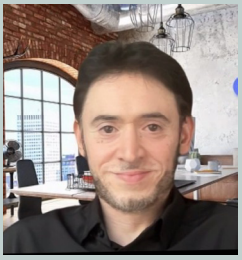
Key Features and Benefits:

- **Eliminate Hardware and Software Dependencies:**
  Leverage a solution free from underlying hardware or software prerequisites.
- **Unified Multi-Cloud and On-Premise Connectivity:**
  Seamlessly connect across multiple cloud environments and existing infrastructure.
- **Simplified Network Architecture:**
  Eliminate the complexities associated with traditional VPN and MPLS deployments.
- **Scalable On-Demand Connectivity:**
  Deploy Alkira's Network Infrastructure as a Service (NIaaS) to support anywhere from a single business partner to thousands, accommodating diverse connectivity types without upfront capacity planning.
- **Rapid, Automated Provisioning:**
  Significantly accelerate deployment times through streamlined and automated provisioning processes.
- **Purpose-Built Sizing:**
  Design your network infrastructure based on current needs, not maximum hypothetical capacity.
- **Flexible, Usage-Based Pricing:**
  Benefit from a pay-as-you-go model that aligns costs with actual consumption.
- **Non-Disruptive Elasticity:**
  Dynamically scale network resources up or down at any time without impacting existing critical partner traffic.
- **Robust Secure Segmentation:**
  Implement granular security through comprehensive segmentation and micro-segmentation capabilities.
- **Centralized Network Oversight:**
  Gain unified visibility and control over your entire network infrastructure.
- **Integrated Zero Trust Security:**
  Enforce a Zero Trust Network Access (ZTNA) framework inherently within the solution.
- **Embedded Security Services:**
  Utilize a suite of integrated security services for comprehensive protection.
- **Seamless Existing Tool Integration:**
  Integrate effortlessly with your current operational tools and workflows

Conclusion: Embracing the Future of Partner Connectivity

Alkira simplifies and secures business partner connectivity, offering enhanced security, agility, and cost efficiency. Embrace Alkira for a modernized approach.

Ready to transform your network? Explore Alkira at www.alkira.com. Request a demo, download our solution brief, or contact sales to learn more.



Author

Syed Ali

VP, Pre-Sales
Solutions Engineering