alkira

SOLUTION WHITEPAPER

WAN Migration

Establish a global, secure, high-speed network connecting users, sites, cloud workloads and applications

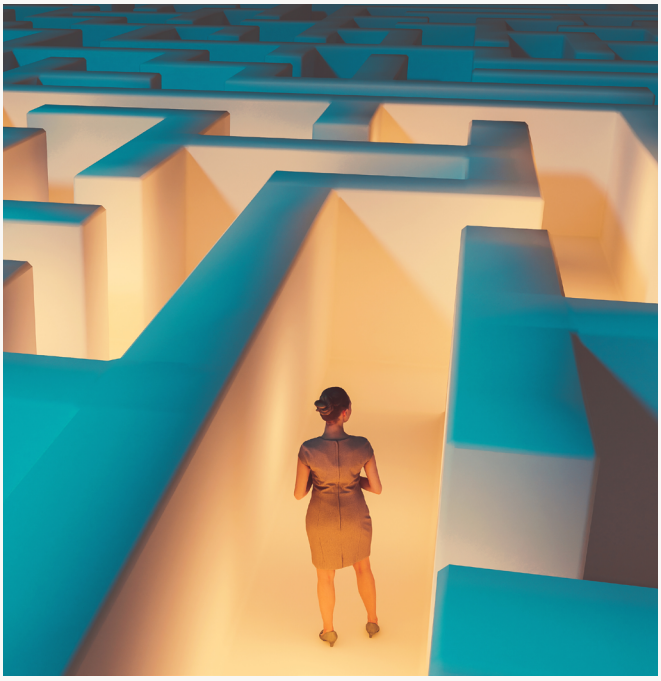
Table of Contents:

WAN Migration to Alkira Cloud Backbone

Wide Area Networks (WAN) are fundamental to any enterprise's global connectivity needs. The benefits of a specific WAN solution do not only depend on the vendor, functionality and the features being used, but they also heavily rely on the architecture and its relevance in the context of the deployment requirements.

As a result, historically, with every changing business requirement, the WAN had to go through a transformation based on the nature of the change. Currently, we are in the midst of one of the most significant WAN transformations fueled by the motions of applications migration from on-premises data centers to one or multiple public cloud and SaaS environments, explosion in remote connectivity demand, and the need for on-demand elastic global connectivity. All these are forcing enterprises to evolve their traditional WAN architectures from the centralized monolithic on-premises model to a software-defined distributed model fully compatible with the cloud attributes of agility, scale and high availability.

Traditional WAN Architecture Challenges



Current WAN architectures have many challenges since they were not designed for the stringent demands of the cloud era. These architectures are better suited for the applications hosted in the corporate data centers and are ideal for traffic flows from branches to data centers in a hub-and-spoke topology.

In terms of WAN design options, enterprises have three different models to choose from:

- MPLS
- SD-WAN
- Internet based VPNs

None of these traditional WAN design options were built with ground-up cloud needs in mind and as a result they struggle to gracefully meet the wide area network requirements of the cloud era.
Let's look more closely at each one of the design options.

Private WAN with MPLS

Arguably, MPLS is the most common way of building wide area networks. It offers enterprise-grade connectivity with privacy, reliability, and quality of service guarantees. At the same time, it's better suited for branch-to-branch and branch-to-data center traffic patterns. This turns into a significant challenge for direct cloud access (DCA) and direct Internet access (DIA) from the branch locations in order to accommodate efficient network connectivity accessing applications hosted in the public cloud environments and offered as SaaS. Enterprises are forced to back-haul application traffic from branches to data centers and colocations for Internet and cloud egress, which adds network latency and affects overall application performance and user experience.

Secondly, the cloud is all about agility. Compute, storage and application teams can move at the speed of business leveraging readily available cloud computing resources. These resources are globally available on-demand, scaled based on need and consumed as a service. When it comes to networking, lengthy MPLS circuit delivery times result in the network being the long pole in the tent for connecting remote offices to the cloud. It is not uncommon for MPLS delivery time to be measured in weeks and even months based on service provider's private infrastructure readiness. This snail pace is orthogonal to the promise of cloud agility turning the network into a bottleneck for delivery of cloud applications and services.

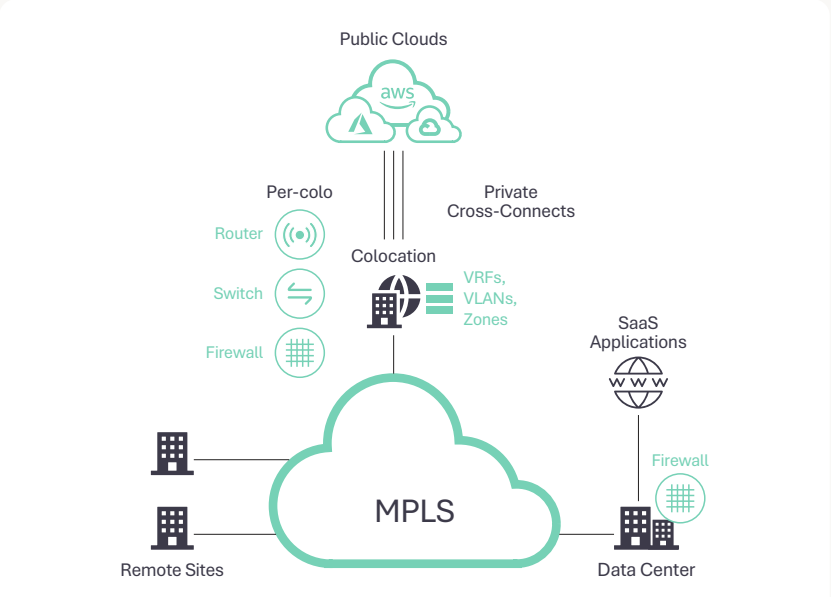


Figure 1: Private WAN with MPLS

Lastly, the reliance on MPLS to extend wide area networks to the cloud proves to be a costly and skills-demanding proposition. One of the more popular methods for extending an MPLS network into the cloud is the use of colocations. Leveraging this option, enterprises establish a footprint of physical colocation facilities in the global regions as close as possible to where the cloud workloads reside. MPLS network is extended to these facilities. Routers, switches, firewalls and other oftentimes physical appliances are procured, installed and configured at the colocation facilities. Ultimately, private cloud cross-connects are established to extend the MPLS wide area network through the colocations into the cloud.

Stacks of hardware, colocation MPLS circuits and private cloud cross-connects result in significant upfront costs for cloud adoption. Configuration of such an environment requires teams of engineers with extensive networking, security and cloud expertise. Multi-region and multi-cloud expansion typically obsoletes this deployment model.

Hybrid WAN with MPLS and Internet (SD-WAN)

SD-WAN allows enterprises to have a hybrid WAN connectivity model, since it can simultaneously leverage both MPLS and Internet circuits as a transport. It provides protection against blackout and brownout conditions by failing over the traffic based on individual physical circuit availability and performance. The use of Internet transport does offer SD-WAN a degree of agility connecting branches and data centers together, which is an improvement over MPLS-only WAN.

Even though SD-WAN provides advantages over MPLS, it still falls short of delivering optimal solution to help enterprises rapidly embrace the cloud. SD-WAN requires a virtual appliance to be provisioned inside the cloud infrastructure. This helps establish connectivity to the cloud, but does not address the various networking and security needs between the cloud workloads themselves in regard to high availability, throughput and security services insertion, which are the main reasons slowing down cloud adoption. Consequently, enterprises are forced to acquire cloud networking expertise for each of the cloud providers in order to figure out the optimal way to securely connect the cloud workloads to the SD-WAN appliances in the cloud.

Connectivity from SD-WAN enabled branches into the cloud is achieved over the Internet using direct Internet access (DIA) for SaaS applications and direct cloud access (DCA) for applications hosted in the public cloud environments. These methods do not offer enterprise-grade security, quality of service, and reliability. Furthermore, long-haul last-mile Internet circuits cause poor application performance for inter-region traffic.

Internet-Based VPNs

Another alternative to MPLS is the IPSec based tunnels over the Internet. The tunnels can be established site-to-site, site-to-cloud and cloud-to-cloud, as well as between the regions of the same cloud. Similar to SD-WAN, Internet based VPNs offer a degree of agility compared to MPLS. At the same time they are challenged by complex manageability, limited scalability, and lower reliability.

As the network grows over time by adding more sites and cloud workloads, manageability of large scale IPSec VPNs becomes a significant administrative burden and high skill demand. It becomes extremely difficult to manage, monitor and troubleshoot problems. Large scale deployments also stretch router resources, increase router CPU demand and subsequently negatively affect the network performance. Lastly, depending on the specifics of the deployment, IPSec VPNs may lack the ability to detect intermediate transport failures resulting in traffic blackholing.

Alkira Solution Overview

Alkira is reinventing networking for the cloud era. Alkira Cloud Network as-a-Service is the industry's first cloud network infrastructure as-a-service allowing enterprises to instantly connect users, sites, cloud workloads and SaaS applications over high-speed, low latency, global cloud backbone. It fully integrates network and security services and comes with a complete set of operational capabilities for end-to-end visibility, advanced controls and governance.

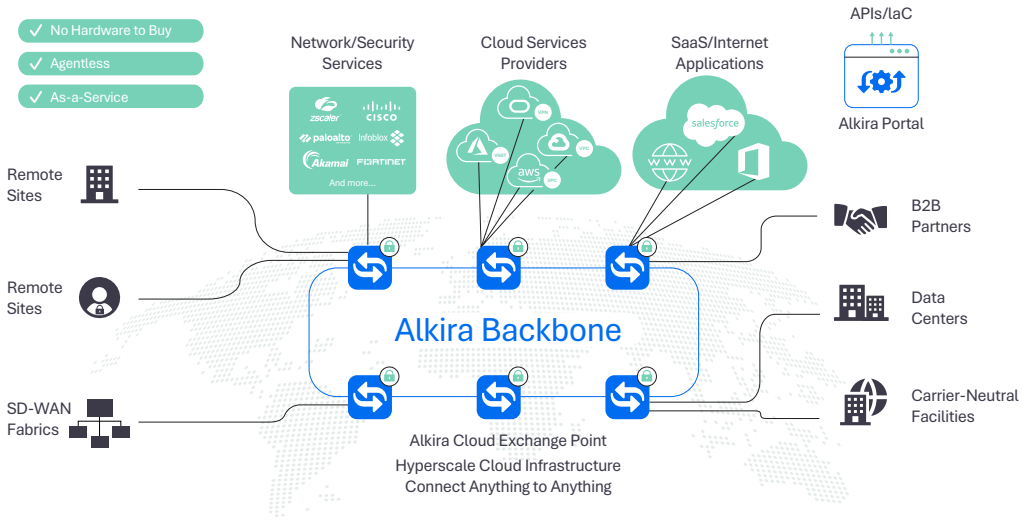


Figure 2: Alkira Network Cloud

The solution is built on a highly available and resilient network of globally interconnected Alkira Cloud Exchange Points (CXPs) – multi-cloud virtual points of presence. Users, branches, data centers, SD-WAN fabrics, cloud workloads (VPCs and vNets) and Internet exit points all connect to the closest CXP, improving overall application performance by constraining the last-mile path utilizing less efficient Internet transport.

In addition to connectivity and network services, the solution offers a portal with a simple graphical user interface for provisioning, management, operations and troubleshooting needs. Provisioning is done through an intuitive single click drag-and-drop operation, eliminating the need for purchasing costly hardware equipment, making complex software configurations and learning the details of cloud architecture. Further, visibility and governance offer deep insights in regard to the network infrastructure and can help identify problems before they occur across the entire network. Devops teams can leverage the extensive set of REST APIs exposed by the portal or make use of infrastructure-as-a-code approach through a Terraform provider.

Alkira Cloud Backbone Benefits

Global Connectivity in Minutes

Building a global network for wide area and cloud networking needs is not easy. It requires significant upfront planning, working with service providers on private circuit delivery, possibly upgrading hardware routers, learning new software solutions and understanding cloud architectures. These tasks can take months depending upon the size of the network. With Alkira, enterprises can now build a high-speed global network securely connecting users, sites, cloud workloads and SaaS applications leveraging point-and-click interface in minutes. This provides the elasticity and agility that the network architects are asking for to support business needs in the cloud era.

As-A-Service Consumption

Alkira Cloud Network as-a-Service is offered as-a-service. Enterprises can sign-up for Alkira service and get access to the portal to start designing, provisioning and managing the entire global wide area and cloud network. This results in significant TCO savings due to zero CAPEX investment in new or upgraded network hardware and lower OPEX investment due to consumption-based pricing and streamlined operations. As enterprises grow by adding additional locations and expanding the cloud footprint, elasticity of Alkira infrastructure coupled with as-a-service consumption-based pricing prevents wasteful over-provisioning and upfront costs.

On-Demand Network Services Marketplace

Just as workloads are moving from on-premises data centers to the cloud, so are the associated network and security services. From an enterprise standpoint, cloud-based network services need to continue offering the same level of features and functionality as they used to in the on-premises data centers. Alkira offers a network services marketplace to allow enterprises to easily deploy Alkira, third-party and cloud-native network and security services onto the Alkira infrastructure. Beyond deployment, Alkira's solution takes care of the entire lifecycle of the network service, including health, availability and performance. Network services can auto-scale based on a real time capacity demand, e.g. next-generation firewalls or remote access VPN. Alkira also supports both pay-as-you-go (PAYG) and bring-your-own-license (BYOL) network services licensing models for the utmost flexibility.

Visibility and Governance

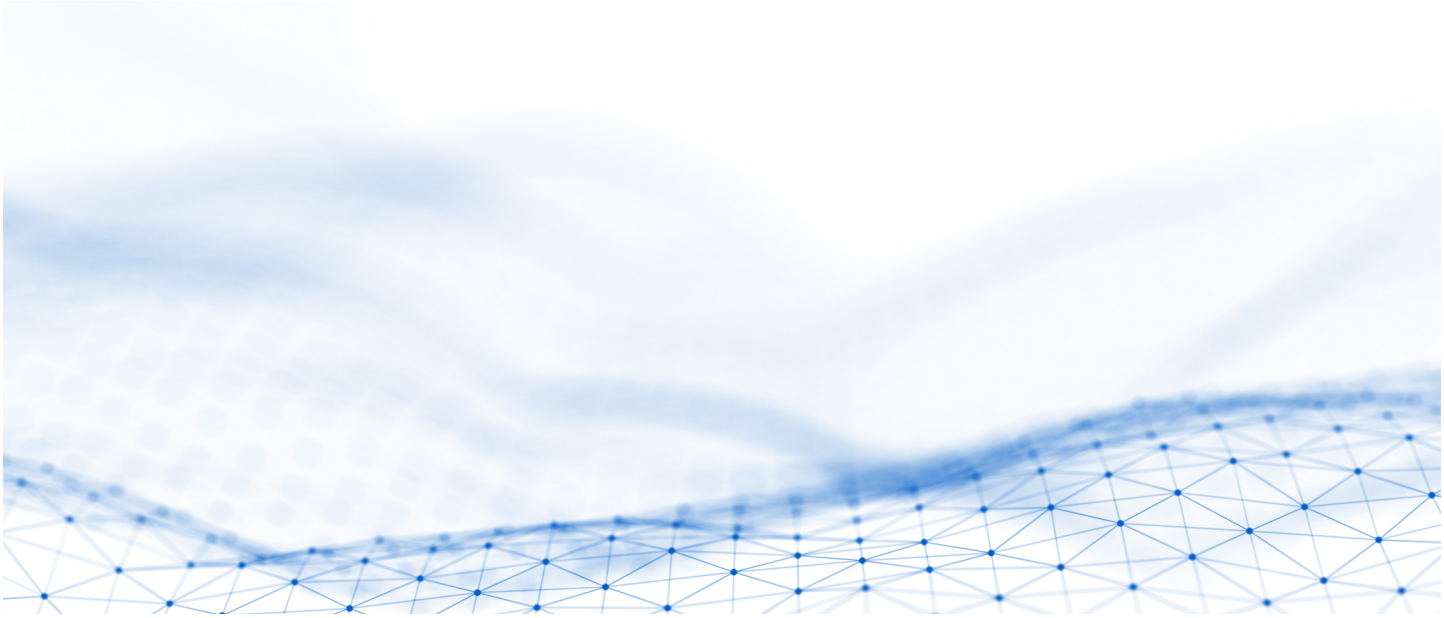
Alkira portal provides an intuitive graphical interface with end-to-end visibility and governance that eliminates operational blind spots for wide area and cloud networks. Enterprises can gain comprehensive insights into their global network infrastructure health and inventory, network traffic patterns and routing, application flow level details, network services performance and auto-scaling, and many more. For governance, the portal offers a single pane of glass with a standardized way of configuring and managing end-to-end policies for on-premises and cloud environments.

Alkira Cloud Backbone – The New WAN

Migrating to a newer WAN architecture is never easy. Enterprise business-critical applications rely on the availability and security of the underlying network infrastructure. The new WAN architecture needs to overcome the challenges around business agility, elastic scalability and cloud adoption to give your business a competitive advantage and future-proof the solution. These changes do not typically occur over-night and ultimately, the new architecture transition needs to be thoroughly and systematically planned out with a detailed stepwise execution to minimize business disruption.

The typical traditional enterprise WAN consists of remote sites connected to the data centers over MPLS, SD-WAN or IPSec based VPN solutions. Remote users' VPN connections are terminated at the VPN concentrator appliances placed in the data centers. Cloud connectivity transits or d) service providers' offered cloud service. SD-WAN offers a cloud onramp option of extending the fabric into the public cloud providers' network using a cloud transit architecture. For SaaS applications, Internet exit points are oftentimes delivered centrally through the data centers, while SD-WAN deployments allow for direct Internet access (DIA) straight from the remote sites.

Security controls and inspection points protect application environments. For data center hosted applications, security controls, like the next-generation firewalls, are placed in the data center infrastructure. For cloud applications, the firewalls are placed in either data centers, colocation facilities or the cloud transits based on how cloud connectivity is delivered. For SaaS applications leveraging direct Internet access, the firewalls are placed at the remote sites as either a standalone physical or



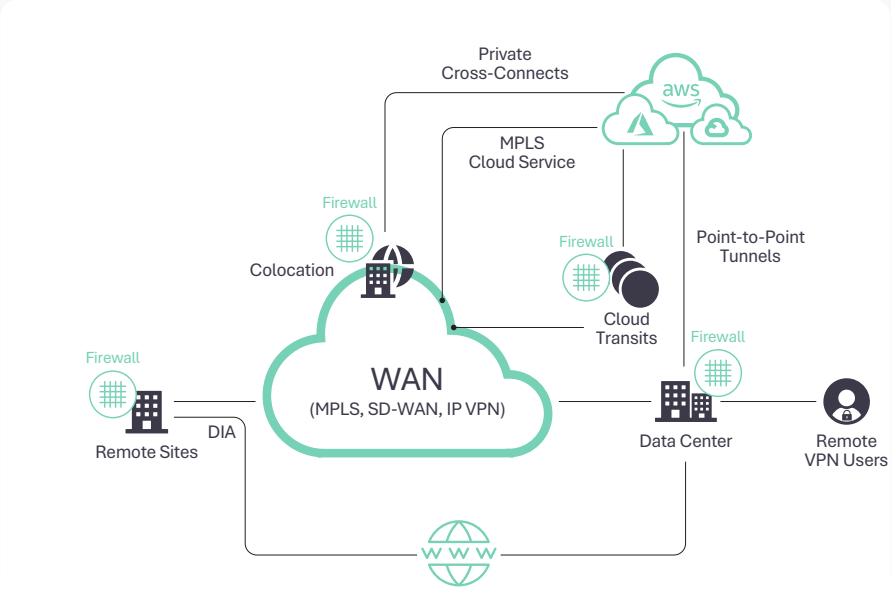


Figure 3: Typical Enterprise WAN Complexity

The centralized nature of traditional networking and security infrastructure comes at a stark contrast with the distributed nature of cloud era enterprise application deployment. Alkira Cloud Network as-a-Service bridges the gap and brings networking and security into the cloud era.

While the specifics of migration from traditional WAN technologies to Alkira Cloud Network as-a-Service vary between different deployments, in general, it typically entails a three-step process.

Step 1 : Connect regional hubs, data centers and colocation facilities to Alkira CXPs

Step 2 : Migrate cloud workloads to Alkra CXPs

Step 3 : Migrate remote sites and remote users to Alkira CXPs

Once migration is complete, the legacy WAN can be decommissioned.

Step 1: Connect regional hubs, data centers and colocation facilities to Alkira CXPs

In this initial step, enterprises establish regionalized connections from their existing hubs, data centers and colocation facilities into the Alkira Cloud Backbone through the geographically distributed Alkira Cloud Exchange Points.

These connections serve as on-ramps for the duration of the migration process connecting the two environments together. The regionalization of these connections reduces traffic back-haul and a subsequent latency between migrated and non-migrated resources.

Hubs, data centers and colocation facilities establish IPSec VPN tunnels to the nearest Alkira CXP using the Internet as transport. Multiple routers with multiple tunnels and dynamic routing are typically used to make sure the connection is highly resilient. Alkira CXPs are built on top of highly available public cloud infrastructure backed by an Alkira service level guarantee. It's worth noting that this approach also minimizes the last-mile Internet path, which can vary in its performance. Instead, inter-region and inter-cloud communication occurs over the Alkira Cloud Backbone, which relies on superior high speed low latency cloud service providers' infrastructure.

In case of colocation facilities, enterprises can also leverage AWS Direct Connect and Microsoft Azure ExpressRoute for dedicated high-speed cloud connectivity. In this case Direct Connect and ExpressRoute are terminated on Alkira CXPs, which then in turn connect the colocations to the cloud workloads across the Alkira Cloud Backbone.

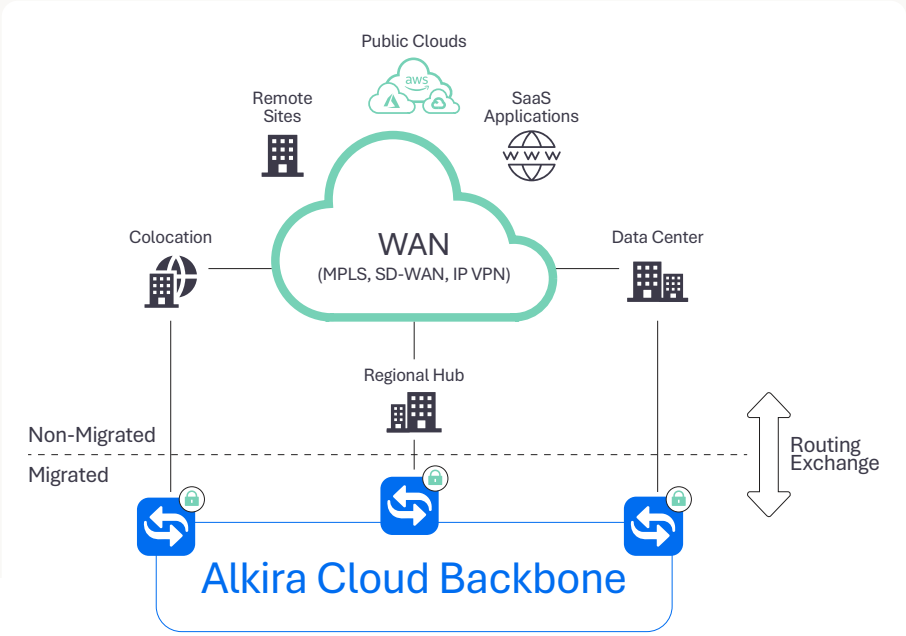


Figure 4: On-Ramps Between Traditional WAN and Alkira Cloud Backbone

Any new site or cloud workload can be connected directly to the Alkira infrastructure leveraging the benefits of Alkira Cloud Backbone for the wide area network connectivity between on-premises sites, between on-premises sites and cloud workloads and between various cloud workloads in a single or multiple public clouds.

Step 2: Migrate cloud workloads to Alkra CXPs

In the second step enterprises migrate cloud workloads to be connected to the Alkira CXPs. The process of connecting cloud workloads into the Alkira CXPs is completely automated through the Alkira portal. These connections are called the cloud connectors. For each cloud connector, the administrator needs to decide on the desired network capacity, the network segment and the optional billing tag to perform departmental chargeback for the expenses incurred as part of the cloud workload's connectivity. Once connected, the workloads can immediately communicate with other workloads connected to the Alkira CXPs as long as they belong to the same network segment. This holds true even if the other workloads reside in a different cloud region or an entirely different cloud. In case the workloads are connected to different Alkira CXPs, such communication occurs over the Alkira Cloud Backbone.

Note: Alkira solution supports inter-segment routing allowing workloads residing in different network segments to securely communicate with each other, if such communication has been permitted by the policy.

Alkira CXPs establish a dynamic routing relationship with hubs, data centers and colocation facilities to make sure all cloud prefixes are automatically advertised into the non-migrated legacy environment, so network connectivity can be maintained during the migration process. If the same prefix is advertised through multiple connections, Alkira traffic policies can set route attributes advertised into the legacy non-migrated environment to influence the traffic flow.

Step 3: Migrate remote sites and remote users to Alkira CXPs

The final third step entails connecting remote sites and remote users to the Alkira CXPs. These connections are called the on-premises connectors. Much like for cloud connectors, for each on-premises connector, the administrator needs to decide on the desired network capacity, the network segment and the optional billing tag. Once connected, the remote sites and remote users belonging to the same network segment can immediately communicate with each other across the Alkira Cloud Backbone.

Note: Alkira solution supports inter-segment routing allowing remote sites and remote users residing in different network segments to securely communicate with each other, if such communication has been permitted by the policy.

Alkira supports several types of on-premises connectors. Standards based IPSec is the simplest method of connecting each individual remote site into the closest Alkira CXP. In case of MPLS WAN, enterprises do need to procure Internet circuits for each remote site in order to establish IPSec connectivity. If procuring Internet circuits for each remote site is not desired, it is possible to maintain MPLS WAN in a limited fashion, while establishing IPSec connectivity to Alkira CXPs only across Internet circuits provisioned at regional hubs, data centers or colocation facilities. This is not a recommended option, however it may become necessary with certain design and business considerations.

BGP dynamic routing protocol is used across the IPSec tunnels to ensure bidirectional reachability exchange. Alkira portal generates all the necessary router configurations for both IPSec and BGP, which need to be applied by the administrator on a remote router.

Note: It is also possible to use static routing as an alternative to BGP.

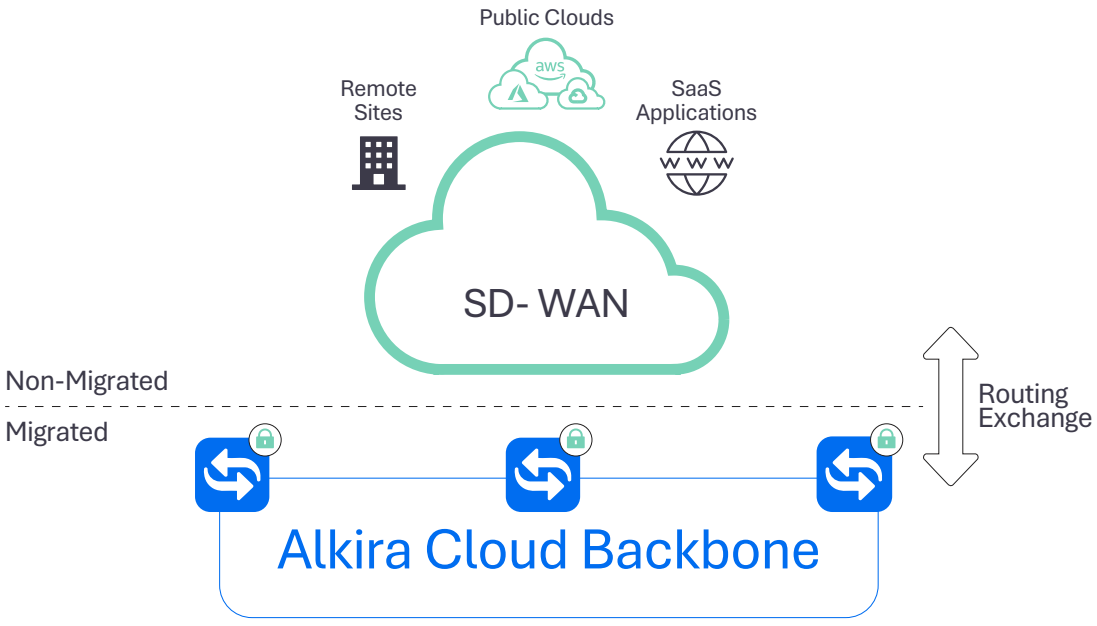


Figure 5: SD-WAN Integration into Alkira Cloud Backbone

For enterprises leveraging SD-WAN, Alkira supports an SD-WAN connector by on-boarding SD-WAN virtual routers into the Alkira CXP and performing full lifecycle management. SD-WAN fabric can connect to multiple Alkira CXPs at different geographic locations in order to minimize the use of last-mile underlay transport (either Internet, MPLS or both) and rely on Alkira Cloud Backbone long-haul connectivity for better performance and reliability.

Network segments defined in the SD-WAN fabric are extended into the Alkira infrastructure for end-to-end segmentation.

Cloud Firewall Security

Users, sites and cloud workloads migrated from traditional WAN to the Alkira Cloud Backbone can also be secured by the next-generation firewalls fully integrated into the solution. Alkira intent-based policies are used to symmetrically steer the traffic of interest to the firewalls. This applies to all types of traffic within the migrated environment, as well as the traffic between migrated and non-migrated environments using any of the integration methods mentioned above.

If additional firewall capacity is required, Alkira solution can automatically scale up the firewall deployment to meet the real time demand. Once the demand subsides, Alkira's solution will scale down the firewalls to prevent over-provisioning and a subsequent over-spend.

Conclusion

With Alkira Cloud Backbone enterprises can establish a global, secure, high-speed network connecting users, sites, cloud workloads and SaaS applications with integrated security, full operational visibility, advanced controls and governance. It is an ultimate network connectivity solution enterprises need to bring the wide area network into the cloud era in minutes.

Summary

Alkira® Network Cloud, powered by Alkira Cloud Services Exchange®, is industry's first solution offering global unified network infrastructure as-aservice. 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!