alkira

Solution Brief

On Demand Network Services Marketplace

Industry's only solution with single-click provisioning of the entire global multi-cloud network and network services. Connect users and sites to public clouds and connect public clouds together, while cutting provisioning time from months to minutes.

Cloud adoption continues to accelerate. Organizations are increasingly transitioning business critical applications from on-premise data centers to the public cloud and SaaS environments.

In response to this rapid adoption of the cloud, compute and storage have evolved beyond virtualization and automation to as-a-service offerings. Cloud architects and engineers are now focused on choosing the service attributes they want to consume, such as compute instances and storage volumes, rather than worry about implementation details. Complexity has been eliminated and cloud computing has become a business enabler for compute and storage.

Key Challenges

In contrast, the network and network services have not made a similar transition, nor do they operate in true concert with the cloud. One of the most popular network services examples is the Firewall. As applications increasingly move from on-premise data centers to the public cloud and SaaS environments, Firewalls play a pivotal role in enforcing organizational security policy to and across clouds. Deploying cloud Firewalls comes with the following key challenges:

- Complicated routing domains to accommodate the traffic steering symmetry needed for stateful, global deployment of cloud Firewalls, especially when Firewall inspection is required only for selected application traffic
- Inconsistent security policies resulting from a lack of a standardized Firewall deployment and operating model across a multi-cloud environment
- Overprovisioning and high TCO of cloud Firewalls to accommodate peak capacity demand, resulting in high total cost or ownership (TCO)

The network and network services are under ever-increasing pressure to provide an agile, high performing and cost-effective solution to cloud business needs.

Easily choose and insert Alkira or third-party network services into your multi-cloud network, while optimizing and securing access to resources and applications.

Securing the Cloud Network with Alkira Cloud Services Exchange

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 Cloud Services

Alkira Cloud Services Exchange™ is the industry's first as-a-service unified multi-cloud network with integrated network services marketplace, visibility and governance. It removes obstacles to successful cloud and multi-cloud adoption.

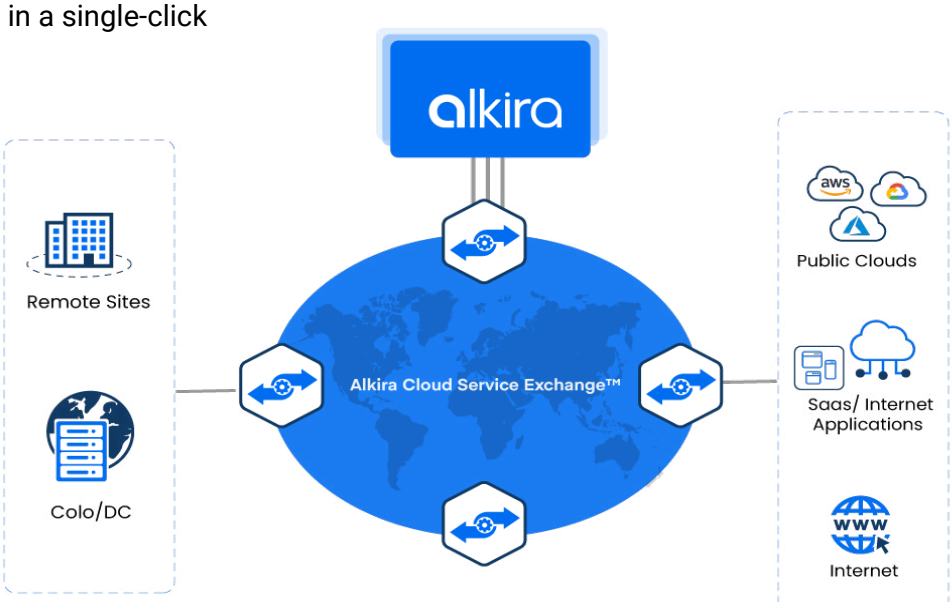
Leveraging a globally distributed virtual infrastructure of Alkira Cloud Exchange Points™ (virtual multi-cloud points of presence with full routing stack and network services capabilities), organizations can extend or migrate their security policy enforcement capabilities into the cloud with Palo Alto VM-Series Firewalls. Palo Alto VM-Series Firewalls can secure both communication from remote sites into the public clouds and the SaaS/Internet, as well as the communication between multiple public cloud instances in the same public cloud or across multiple public clouds, in four easy steps:

1. Register for Alkira service

2. Point-and-click the entire global on demand multi-cloud network

3. Define Alkira intent-based policies for traffic redirection to Palo Alto VM-Series Firewalls

4. Provision everything in a single-click



Point-and-click Global On demand Multi-Cloud Network

Steps to enable global on demand cloud and multi-cloud network with Palo Alto VM-Series Firewall

Step 1:

Registering for Alkira Service

Registering for Alkira service is the first step to enable global on demand cloud and multi-cloud network with Palo Alto VM-Series Firewall security.

a. Navigate to https://www.alkira.com and register your company

b. Click on the link in the registration confirmation email and create an administrative account

c. Log into Alkira service to start designing your network

Step 2:

Point-and-click Palo Alto VM-Series Firewalls into the Global On demand Multi-Cloud Network

With Alkira CSX, your multi-cloud network and Palo Alto VM-Series Firewall security are offered as-a-service, on demand, when you need it. You do not need to procure any additional Firewall equipment or perform tedious network and routing configuration tasks. Your entire global multi-cloud network with Palo Alto Firewalls is modeled through the intuitive Alkira Cloud Services Exchange Portal in a point-and-click fashion.

a. Select the Alkira Cloud Exchange Point (CXP) where you want to provision the Palo Alto VM-Series Firewall. In a geographically distributed deployment, Palo Alto VM-Series Firewall instances should be provisioned in multiple Alkira Cloud Exchange Points to enforce security policy closest to the source.

b. Select either Pay-As-You-Go (PAYG) or Bring-Your-Own-License (BYOL) licensing option for the Palo Alto VM-Series Firewall deployment. In case of BYOL, please also provide the Firewall license key. Organizations can leverage a mix of both licensing models.

c. Choose whether you want to use Palo Alto Panorama with your Palo Alto VM-Series Firewall deployment. If yes, provide the details of your Palo Alto Panorama deployment, such as server IP address, the device group the Firewall belongs to, and the Firewall instance authentication key.

For centralized and consistent management of all global Palo Alto Firewalls deployed in the Alkira Cloud Services Exchange, it is recommended to use Palo Alto Panorama.

You must enable Palo Alto Panorama if you want to use the Firewall auto scaling feature of the Alkira Cloud Services Exchange.

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

Note: The Alkira service does not deploy the Palo Alto Panorama server, however it does provide all the necessary connectivity from the Palo Alto VM-Series Firewall to the Palo Alto Panorama server deployed by the organization.

d. Provide Firewall specific details, such as the model of Palo Alto VM-series Firewall, the desired Palo Alto PAN-OS software version, and the username and password for the Firewall administrative account.

e. All defined network segments are automatically extended to all provisioned Palo Alto Firewalls across the entire Alkira Cloud Services Exchange. This allows Palo Alto Firewalls to inspect application traffic in any of the segments. Palo Alto Firewalls can also provide secure cross-segment communication, if desired.

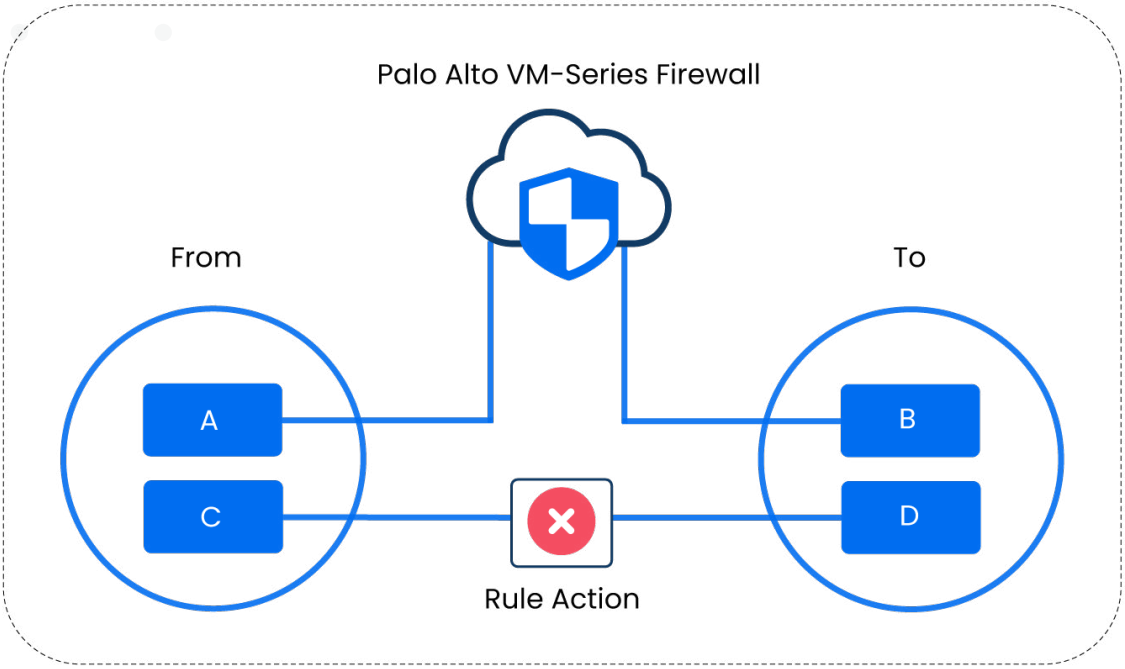
f. Optionally, enable Firewall autoscaling. Firewall autoscaling, as the name suggests, allows horizontal scaling in and out of Palo Alto VM-Series Firewall instances deployed in the Alkira Cloud Exchange Point based on required real-time capacity. You can set the minimum and maximum number of Palo Alto VM-Series Firewall instances deployed with autoscaling to make sure there is sufficient minimum of Firewall capacity always available for the typical use and a sufficient maximum Firewall capacity for the burst use. During the off-peak hours, when Firewall load subsides, Alkira solution will automatically scale in the Firewall capacity by bringing down the unneeded Firewall nodes, potentially all the way down to the minimum specified number.

Step 3:

Define Alkira Intent-based Policies for Palo Alto VM-Series Firewall Redirection

Organizations create Alkira intent-based policies and rules in order to forward the application traffic of interest to the globally provisioned Palo Alto VM-Series Firewalls. Rules identify the traffic of interest to be subjected to Firewall inspection. Traffic of interest can be identified based on 6-tuple matching (including DSCP) or based on an application recognition engine. Intent-based policies identify the communicating source/destination parties and the particular network segment they belong to (different segments can have different policies). Communicating parties can be different cloud instances, remote sites communicating to the cloud, remote sites communicating to the Internet and so on. A single Alkira intent-based policy can have multiple rules.

The Alkira Cloud Services Exchange can also enforce basic allow/drop security rules for the traffic of interest without the use of the fully featured stateful Firewall.



Rule 1: Send traffic from A to B to the Firewall for inspection

Rule 2: Drop traffic from C to D (no Firewall inspection)

Step 4:

Single-Click Provisioning

Provisioning the entire global on demand multi-cloud network and network services is done in a single click! Alkira Cloud Services Exchange will automatically instantiate all the necessary elements required to establish global on demand multi-cloud network connectivity and network services, based on the created point-and-click design. Alkira service billing will start incurring charges after all cloud infrastructure elements had been provisioned.

Based on the extent of the network design, for example the number of geographic locations, remote sites, public cloud instances and network services, the provisioning cycle may take as little as ten minutes. Alkira Cloud Services Exchange Portal provides a progress bar to keep you updated on the provisioning cycle. Your global multi-cloud network is ready for use immediately after the provisioning cycle completes.

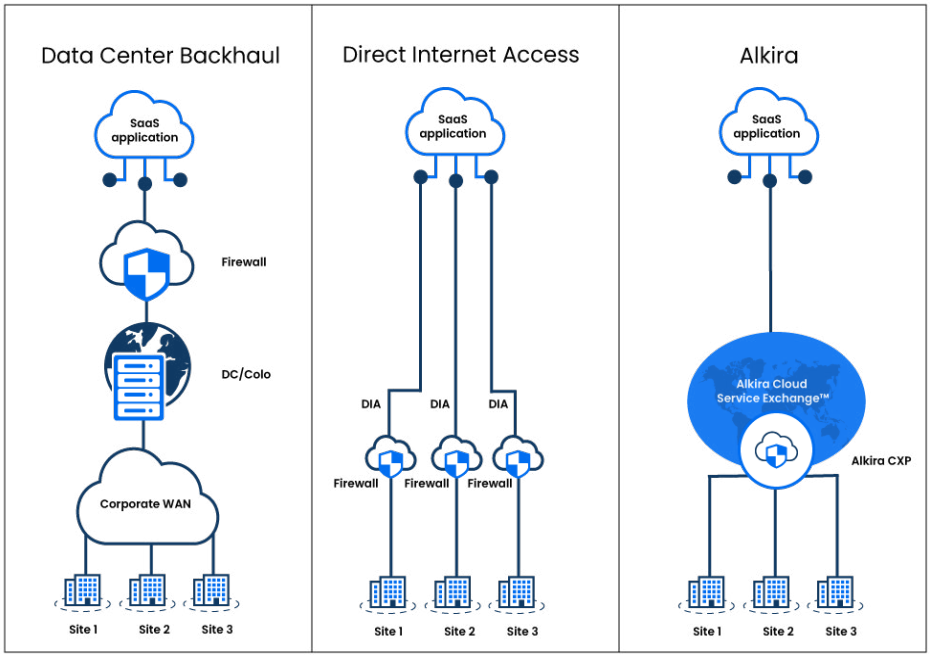
Securing Network for cloud

Cloud Firewall Security for SaaS/Internet Access

SaaS applications are becoming increasingly popular. Access to SaaS applications is most often done through the Internet and as such, Internet exit points need to be carefully engineered to balance between security, performance and budgetary spend. Traditional methods of Internet access through the data center carry the advantage of fewer number of Firewalls (albeit with higher capacity) and subsequently fewer number of administrative touchpoints; however, they fail to provide adequate application performance due to high data center backhaul latency and a possible data center bandwidth starvation. In recent years the method of direct Internet access (DIA) at remote sites has become increasingly popular. This method offers much improved application performance when compared with data center-based access, however it proliferates the number of required Firewalls (for each remote site) and the subsequent number of administrative touchpoints.

Alkira Cloud Services Exchange offers high-speed, low-latency transport from all sites to the SaaS/Internet applications. Geographically distributed Alkira Cloud Exchange Points with provisioned Palo Alto VM-series Firewalls offer the needed balance between optimal (regional) connectivity to SaaS/Internet applications coupled with stateful Firewall security and fewer number of administrative touchpoints when compared to direct Internet access at each remote site.

The Alkira solution takes care of instantiating Palo Alto VM-series Firewalls and the associated symmetric traffic steering. Organizations are still responsible for configuring Palo Alto VM-Series Firewall security policy.



Cloud Firewall Security for SaaS/Internet Access

Cloud Firewall Security To and Across Public Clouds

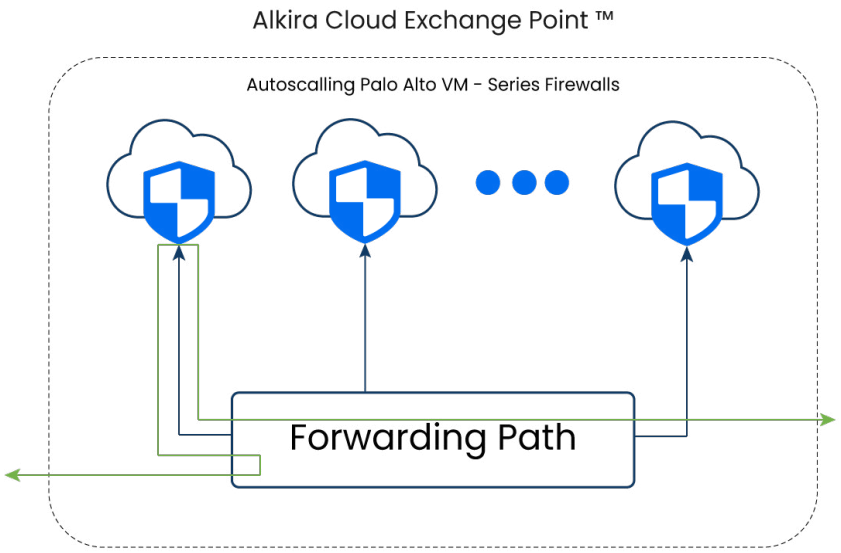
The ability to insert stateful firewalls for network traffic to and across clouds is imperative for successful cloud adoption. Firewalls, like Palo Alto Firewalls, are stateful entities, and as such, they have to observe the entire bi-directional communication in order to be able to enforce their policies. This implies traffic symmetry. Networks are inherently asymmetric, which creates challenges and can break communication, especially in deployments where Firewalls are geographically distributed. Alkira Cloud Services Exchange leverages intelligent traffic steering to preserve symmetry across a global Firewall deployment.

There are two specific cases where traffic symmetry plays a role:

1. Symmetric traffic to autoscaled Palo Alto VM-Series Firewalls inside an individual Alkira Cloud Exchange Point
2. Symmetric traffic across the entire cloud and multi-cloud network consisting of multiple Alkira Cloud Exchange Points and multiple Palo Alto VM-Series Firewalls

Case 1

Application traffic is symmetrically distributed across a number of Palo Alto VM-Series Firewalls in a given Alkira Cloud Exchange Point.

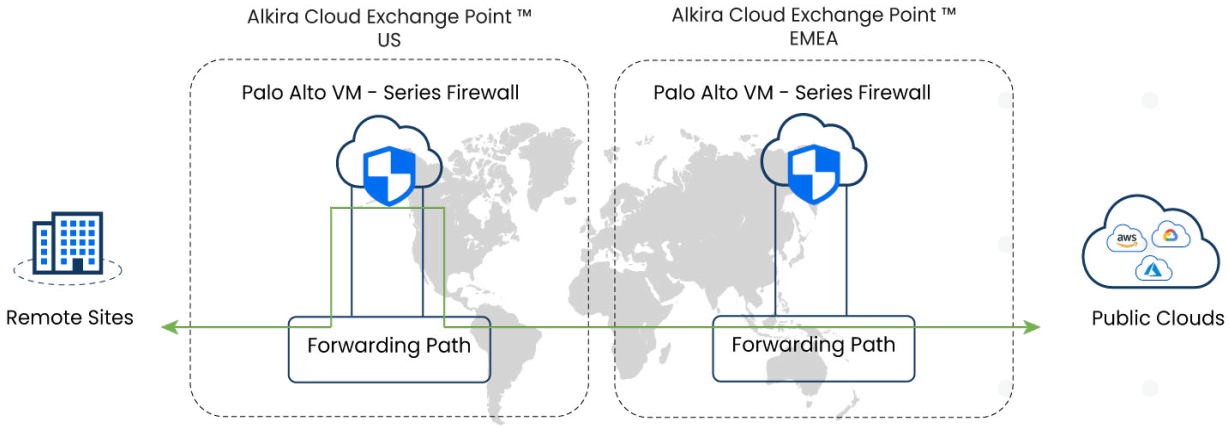


Symmetric application traffic distribution across autoscaling Palo Alto VM-Series Firewalls

Alkira Cloud Exchange Points preserve traffic symmetry bi-directionally, sending individual session traffic to the same Palo Alto VM-Series Firewall in order to maintain stateful behavior. Different sessions may end up being forwarded to different Palo Alto VM-Series Firewalls for horizontal scale.

Case 2

Alkira Cloud Services Exchange leverages ability to intelligently and symmetrically send the traffic of interest to globally distributed Palo Alto VM-Series Firewalls in a way that prevents unnecessary Firewall overprovisioning. This traffic symmetry is globally enforced for multiple Alkira Cloud Exchange Points hosting Palo Alto VM-Series Firewalls.



Symmetric application traffic distribution across multiple Alkira Cloud Exchange Points

In this example case, the communication between the site in the US and a public cloud resource in EMEA occurs across two respective Alkira Cloud Exchange Points, each hosting a Palo Alto VM-Series Firewall from the Alkira Network Services Marketplace. The Alkira solution ensures that this traffic is symmetrically routed through the Palo Alto VM-Series Firewall in US CXP, while Palo Alto VM-Series Firewall in EMEA CXP is bypassed for this particular communication. This approach reduces the globally required Firewall capacity by 50%, while maintaining global security policy enforcement. The same scenario applies for communication between various public cloud instances connected to different Alkira Cloud Exchange Points.

As Firewalls autoscale to accommodate needed real-time capacity and communication occurs across multiple Alkira Cloud Exchange Points, both case 1 and case 2 described above can occur at the same time.
The Alkira solution takes care of instantiating Palo Alto VM-series Firewalls and the associated symmetric traffic steering. Organizations are responsible for configuring Palo Alto VM-Series Firewall security policy.

Customer Benefits

The Alkira solution allows organizations to turn networking for the cloud from a business inhibitor to a business enabler, while providing the following main benefits.

- Faster time to cloud reduces deployment time from months to minutes in full alignment with business SLAs
- High bandwidth, low latency network from remote sites to public clouds (AWS, Microsoft Azure and GCP) and SaaS/Internet applications, and between multiple public clouds or multiple regions of the same public cloud
- Eliminate cloud-specific limitations by building a multi-region, multi-cloud overlay network, leveraging cloud-native and advance routing and security constructs
- Global security policy enforcement by leveraging firewalls of choice and global symmetric traffic steering
- Elasticity to accommodate on demand capacity, e.g. periodic high-volume data transfers, seasonal retail customer uptake, etc.
- End-to-end segmentation between remote sites, public cloud instances, cloud network services and SaaS/Internet exit points for compliance and sensitive or secure applications
- On demand/subscription consumption cost model to ensure customers are only charged for the network and network services resources they actually consume
- High availability and resiliency backed up by high uptime service guarantee
- Full visibility to eliminate operational blind spots and improve day-2 operations

Summary

In summary, Alkira Cloud Services Exchange™ offers the industry's first leapfrog solution focusing on removing obstacles to successful cloud and multi-cloud adoption. Leveraging globally distributed network of Alkira Cloud Exchange Points™ (multi-cloud virtual points of presence), organizations can establish global on demand connectivity between remote locations and the public clouds. Organizations can easily insert on demand stateful global network and security services from the Alkira services marketplace, leveraging intent-based policies. End-to-end visibility and governance offer deep network and network services insights eliminating operational blind spots. The Alkira™ industry-leading graphical user interface enables dramatic operational simplification by offering a point-and-click modeling canvas with single-click provisioning of the entire end-to-end multi-cloud service in minutes.

The Network. Reinvented for Cloud.™

alkira

www.alkira.com

SB-101-12123