Solution Brief

Next generation security and threat defense for the multi-cloud networks

Overview

In the world driven by the digital transformation and increased cloud adoption, network and security play an imperative role in any modern enterprise infrastructure. The need to respond to an ever-increasing demand for network agility and to combat sophisticated security attacks forces enterprises to reevaluate the traditional on-premises network and security architectures, which are not optimized for the distributed nature of the cloud applications.

Enterprises are planning to transition their trusted next-generation firewall security services from the on-premises data centers and colocation facilities, and into the public cloud environments they are servicing. Public cloud environments offer ubiquitous global presence and virtually unlimited compute capacity; however, they severely lack the capabilities and controls required to successfully deploy the cloud firewalls of choice. The do-it-yourself (DIY) approach to cloud firewall deployment forces enterprise IT teams to invest a significant amount of time and effort in learning the intricacies of the cloud infrastructure and workaround it's limitations, which is further exacerbated in the multi-cloud environment.

In this solution brief we are proud to introduce a joint solution between Cisco and Alkira, which greatly simplifies provisioning, monitoring, troubleshooting of the cloud networking and security environments, while at the same time offering advanced routing and thread detection capabilities to address the most critical enterprise needs in the cloud era.

Benefits

Integrated Network and Security Architecture

Intelligent integration of the firewall security services into the global cloud network.

Unified Security Posture

Uniformly enforce firewall security policy across on-premises, cloud, and multi-cloud environments.

Auto-scaling Capacity

Automatically scale up and down firewalling capacity based on real-time demand.

Application Visibility

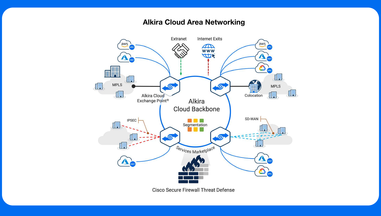
Symmetrically steer application traffic and eliminate IP address obfuscation.

Simplified Operations

Intuitive graphical user interface for all network provisioning, monitoring, and troubleshooting tasks.

Solution

The joint solution from Cisco and Alkira allows organizations to seamlessly extend their security services to the cloud with Cisco Secure Firewall Threat Defense (formerly FTD), providing granularity, control, and simplicity; unmatched by the native cloud deployments. Cisco firewalls are integrated into the Alkira Network Services Marketplace, which is part of Alkira Cloud Area Networking.



This integration allows organizations to enforce uniform firewall security policies for the application traffic between on-premises, cloud, multi-cloud, and Internet environments. The joint customers can continue to manage and operate the firewall security policy through the Cisco Secure Firewall Management Center (FMC) while Alkira Cloud Area Networking takes care of the entire lifecycle management of the firewalls by automating the provisioning. With automated provisioning, firewalls can be symmetrically inserted into any application traffic of interest in accordance with Alkira intent-based policy while auto-scaling up and down the firewalling capacity based on the real-time demand.

Solution Details

The joint solution provisions Cisco Secure Firewall Threat Defense (formerly FTD) firewalls in the Alkira Cloud Exchange Points (Alkira CXPs). Alkira CXPs are virtual multi-cloud points of presence with full routing and network services capabilities. Alkira CXPs are distributed across the globe leveraging the hyperscale public cloud infrastructure.

Cisco Secure Firewall Threat Defense hosted within the Alkira Cloud Exchange Points can be used to secure a variety of use cases:

Multi-Cloud Security

Enforce firewall security policy for application traffic to and between public cloud workloads in a single and multi-cloud environments.

Branch Security

Cloud-based firewall security policy enforcement for application traffic between on-premises locations, such as remote sites, campuses, and data centers.

Secure Internet Egress

Enforce egress firewall security policy for application traffic between on-premises and cloud environments communicating with Internet-based applications.

Cloud DMZ

Enforce ingress firewall security policy for application traffic between remote users and Internet facing applications deployed in the on-premises data centers or cloud environments.

Shared Application Services

Enforce firewall security policy for cross-segment application traffic in cases of business partner integration, mergers, acquisitions, and divestitures.

Provisioning the firewalls in the Alkira CXPs involves following the intuitive process in the Alkira portal where the administrator:

1. Provides the IP address of the Cisco Secure Firewall Management Center (FMC)
2. Chooses from the pay-as-you-go (PAYG) or bring-your-own-license (BYOL) licensing models
3. Selects auto-scaling high and low water marks
4. Assigns the proper security zones to be created on the firewalls for the zone-based security policy

Once provisioned, the joint solution seamlessly orchestrates connectivity between the Cisco firewalls and the FMC management, so firewall policy can be deployed.

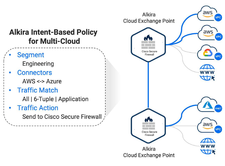
The joint solution monitors the performance of the Cisco firewalls deployed in the Alkira Cloud Exchange Points and auto-scales the firewall capacity up or down by adding or removing firewall instances based on the real-time capacity demand. This automated behavior removes the need to over provision the firewall capacity for peak usage or under provision firewall capacity to conserve resources and control cost.

Alkira Cloud Exchange Points (Alkira CXPs) converge connectivity and security. All remote locations connect to their closest Alkira Cloud Exchange Point, leveraging a variety of Alkira on-premises connectors, such as IPSec VPN, SD-WAN, or private cloud cross-connect (like AWS Direct Connect or Azure ExpressRoute). All cloud workloads connect to their closest Alkira Cloud Exchange Point leveraging Alkira cloud connectors that rely on cloud-native mechanisms available in each individual public cloud. On-premises and cloud connectors are assigned to network segments that, by default, restrict communication between connectors residing in different segments, unless allowed by the Alkira policy. The segments are end-to-end and automatically span the entire network. These segments are also extended to the Cisco firewalls for intra-segment or inter-segment firewall security policy enforcement.

Furthermore, connectors can be grouped together creating micro-segments. Alkira intent-based policies can be used to permit, deny, or steer application traffic to the firewalls within multiple connector groups, or across multiple connector groups. This allows fine-grained control of the firewall security policy enforcement.

Administrators can choose to steer all traffic between connectors or connector groups to the Cisco firewalls. Alternatively, administrators can use 6-tuple matching or application recognition to selectively steer only the specific traffic types. During redirection, Alkira's routing fabric automatically tracks session state to ensure symmetric connection steering through the firewall instances while maintaining original source and destination IP addressing without the need for network address translation (NAT). Where multiple Cisco Secure Firewall Threat Defense instances are provisioned, the Alkira routing fabric natively manages load balancing across these instances in an active-active fashion. Symmetric traffic steering applies to both the cases of multiple Cisco firewalls in a single Alkira Cloud Exchange Point (e.g. auto-scaling), as well as the global Cisco firewall deployment across multiple Alkira Cloud Exchange Points. In the latter case, Alkira's routing intelligence offers overall higher firewalling capacity removing the need to unnecessarily subject application traffic to the firewall policy enforcement numerous times.

Configuration of the Alkira intent-based policy is made easy with Alkira's visual policy manager integrated into the Alkira Cloud Area Networking Portal, which provides a straightforward approach to policy scoping and inspection while simplifying auditing for assurance and compliance purposes.



Cisco Secure Firewall Threat Defense security policies provisioned within the Alkira solution are managed from either on-premises or cloud-based Cisco Secure Firewall Management Center. Joint customers continue to benefit from integrated policy management, threat intelligence, and application visibility and control offered by the Cisco firewalls as it works coherently with the Alkira Cloud Area Networking solution to build simplified and comprehensive network-wide security controls.

Alkira Cloud Area Networking brings Cisco Secure Firewall Threat Defense to the Alkira Network Services Marketplace. This addition allows enterprises to dramatically simplify and expedite their cloud and multi-cloud networking journey, while securing it with Cisco's rich firewall feature set. The entire integrated solution is consumed as a service, eliminating hardware proliferation, complex software configuration, and the need to learn cloud architectures.

About Cisco

Cisco Systems (www.cisco.com) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your enterprise, transforming your infrastructure, and empowering your teams for a global and inclusive future.

About Alkira

Alkira Cloud Area Networking (www.alkira.com) is the fastest way to unify clouds, sites, and users. With Alkira Cloud Area Networking, you can deliver secure, end-to-end networking in hours instead of months. One cloud or many. Enjoy an elastic network that scales up and down based on business demand. The only enterprise-grade network built 100% in the cloud. Agentless. And delivered as-a-service. With Alkira, your network team will move faster. Manage less. And save more.