VM-Series Virtual Firewalls and Prosimo Full Stack Cloud Transit Platform

An Integrated Cloud Networking and Security Architecture for Multicloud to Avert Security Incidents

Benefits of the Integration

- **Effortless management** via a single interface for efficiently deploying and managing cloud networking and security infrastructure.
- **Comprehensive security layers** using NGFWs and WAFs, providing traffic inspection, encryption, and multilayer threat defense.
- The joint solution enables **rapid network and security infrastructure scaling** to meet performance demands.
- The integration promotes a centralized security architecture that aligns with the **cost management framework** via resource optimization.
- **Detailed monitoring and analytics** for swift identification and resolution of network and application performance issues.

Navigating Cloud Networking and Security Challenges

Organizations often rely on next-generation firewalls (NGFWs) for their multifaceted threat detection and prevention, but implementing networking and security solutions within cloud service provider (CSP) environments presents unique challenges. Specialized skill sets required for CSP environments are scarce, making deployment and management difficult. Navigating complex CSP-specific configurations such as security virtual private clouds (VPCs), virtual networks (VNETs), and subnets within can lead to inconsistencies across cloud deployments. Additionally, east-west and internet-bound traffic introduce complexity, requiring the management of access control lists (ACLs), traffic isolation, and route tables for inspection. Also, achieving defense in depth involves deploying various security tools and enacting Zero Trust policies across multiple layers, while scalability and performance impact pose further challenges, as security infrastructure must handle increasing traffic without compromising performance.

The Solution

Cloud security solutions mitigate risks, streamline operations, and optimize resource utilization. A comprehensive solution integrates best-of-breed cloud networking and security technologies for unified protection. The solution features native integration between technologies for easy firewall orchestration via a unified interface. It also includes onboarding of brownfield firewalls, ensuring flexibility and continuity. Lifecycle management and coordination with cloud-native elements are additional benefits. The solution contains a robust policy engine that maintains traffic within Zero Trust access and segmentation guardrails, while firewalls protect against threats, allowing for overall deep flow visibility.

Prosimo Full Stack Platform

Prosimo Full Stack Cloud Transit is a networking platform that empowers organizations to use the cloud as their enterprise backbone network, seamlessly connecting hybrid multicloud environments. Operating within the customer's cloud subscription, Prosimo uses microservices-based edge gateways and cloud-native networking services such as Transit Gateway (TGW) and Virtual WAN (VWAN) peering to create secure connections across hybrid clouds.

Prosimo's policy engine allows for fine-grained access control and Zero Trust security policies, enabling identity-centric access to corporate applications. Its adaptive service insertion model redirects traffic to NGFWs and WAFs for inspection, handling application-layer traffic using FQDNs, URLs, and API endpoints. This extends to PaaS and other applications with dynamic IP addresses. Prosimo's observability stack provides detailed insights into traffic flows and policy enforcement, helping network teams effectively understand and address traffic issues.

Palo Alto Networks VM-Series Virtual Firewalls

The Palo Alto Networks VM-Series Next-Generation Firewalls consistently protect public and private clouds, virtualized data centers, and branch environments by delivering inline network security and threat prevention. Public cloud platforms and software-defined network solutions lack the threat prevention capabilities needed to keep your environment safe. VM-Series virtual firewalls augment your security posture with the industry-leading threat prevention capabilities of the Palo Alto Networks Next-Generation Firewall in a VM form factor, making it automatable, scalable, and easily deployed.

Palo Alto Networks and Prosimo

The joint solution from Prosimo and Palo Alto Networks represents a fusion of best-of-breed cloud networking and security solutions. Prosimo orchestrates cloud-native services to connect VPCs/VNETs across regions and clouds while autoscaling and intelligent path routing provide robust, redundant infrastructure. Its Zero Trust policy engine allows organizations to manage traffic directionality as well as by segmentation, and it offers application protection with inline WAF, reverse proxy, and NAT.

Palo Alto Networks VM-Series NGFWs secure this by inspecting traffic between segments, offering Advanced URL Filtering and internet egress control, and preventing malware and advanced threats. Together, they deliver deep visibility and insights across multiple networking layers for comprehensive security and performance.

The joint solution unlocks an array of use cases that help streamline cloud adoption and facilitate the implementation of security policies governing network and application endpoints in the cloud.

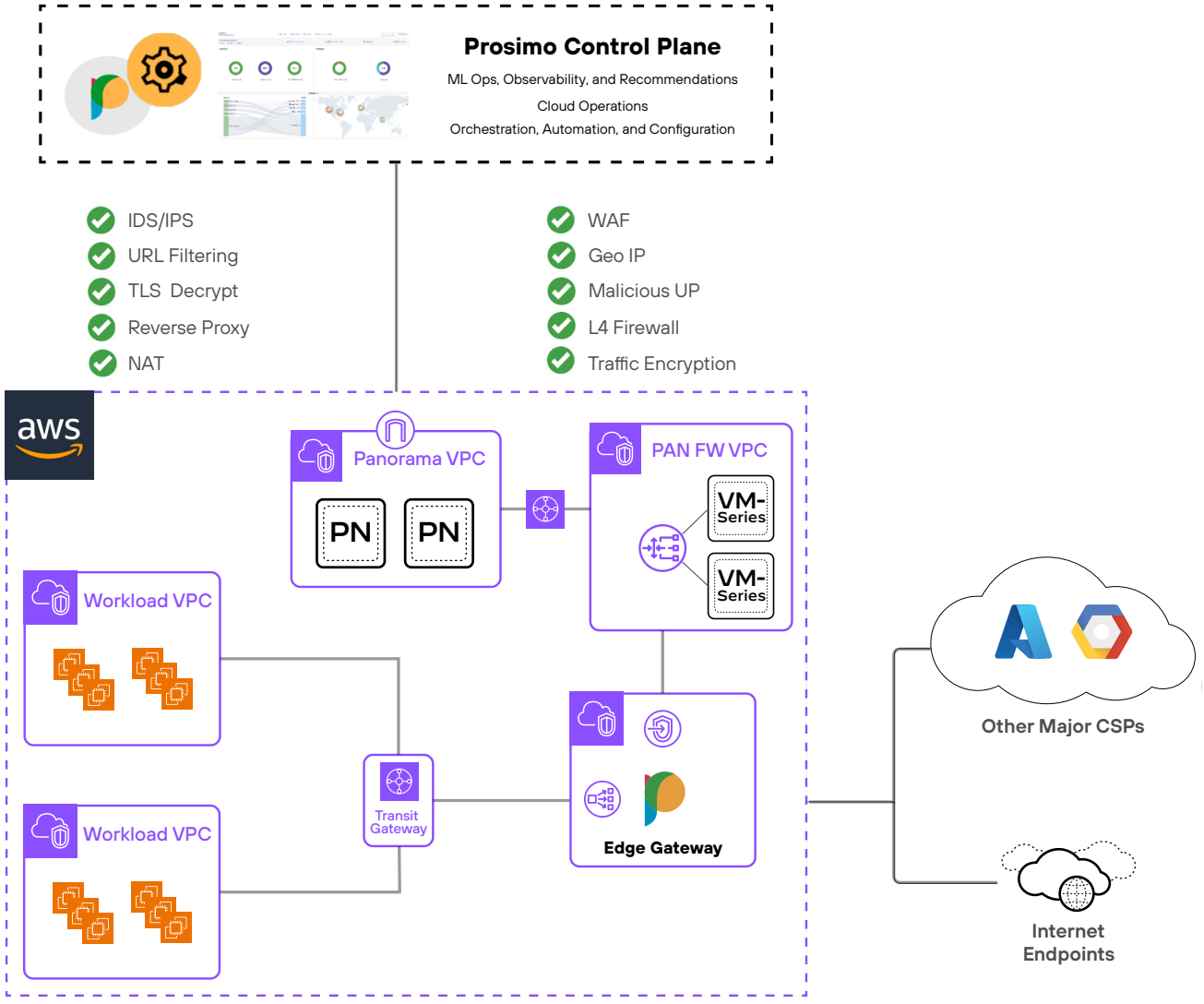

Figure 1: Architectural overview of the joint solution

Use Case 1: Secure Multicloud Networking

Challenge

Organizations in today's cloud-centric environment manage multiple cloud environments with unique challenges. They require secure networking solutions for seamless communication and protection of endpoints across layers. High-performance encryption is essential to safeguard sensitive information due to the increasing data transmitted over these networks.

Solution

The joint solution provided by Prosimo and Palo Alto Networks addresses these needs by offering a comprehensive approach to secure multicloud networking. Prosimo's traffic encryption and scalable east-west segmentation capabilities ensure the confidentiality and integrity of data transmitted between networks and application endpoints within and across regions and clouds. Moreover, traffic inspection capabilities from Prosimo's inline WAF and Palo Alto Networks VM-Series effectively mitigate a wide range of cyberthreats and enforce granular access controls, enhancing their overall security posture in the cloud.

Use Case 2: Centralized Internet Egress Control

Challenge

The rise of cloud applications boosts connectivity but also brings new security challenges. Organizations must route internet-bound traffic through appropriate services to prevent unauthorized access and cyberthreats. To combat data exfiltration and botnet infiltration, they need centralized control over internet ingress and egress to enforce security policies and safeguard network endpoints.

Solution

A joint solution from Prosimo and Palo Alto Networks effectively implements internet egress control by combining multiple security capabilities. Prosimo's WAF, geo IP restriction, and reverse proxy work together to protect web applications, restrict access based on location, and manage traffic flow. Palo Alto Networks VM-Series, URL Filtering, and malicious IP detection enhance security by identifying and blocking threats, filtering unwanted content, and preventing access to known malicious IP addresses. Together, the joint solution can proactively detect and respond to cyberthreats, minimizing the risk of data breaches and network compromises.

About Prosimo

Prosimo streamlines multi-cloud infrastructure by integrating networking, performance, security, observability, and cost management. Leveraging data insights and machine learning, Prosimo minimizes complexity and risk, enabling faster innovation. Fortune 100 companies use Prosimo to launch revenue-generating apps and enhance operational efficiency. For more information, visit www.prosimo.io.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS | prosimo

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_pb_prosimo_052224