Palo Alto Networks Next-Generation Firewall with Big Cloud Fabric

Leverage the benefits of the industry-leading Palo Alto Networks® Next-Generation Firewall combined with Big Switch’s Next-Generation DC switching Fabric, Big Cloud Fabric, for rapid and secure application deployment with a scale-out network infrastructure. This integration enables operational velocity for end-to-end security provisioning across the switch fabric with reduced total cost of ownership for enterprise IT as well as service provider cloud environments.

THE CHALLENGE

Modern applications demand a secure and agile data center infrastructure to support dynamic workload placement and business agility. However, traditional networking is inflexible and proprietary, and causes operational bottlenecks due to complex, manual configurations. IT administrators need simplified network operations and holistic telemetry to enable rapid application deployment, change management, and troubleshooting. Such a dynamic infrastructure often runs applications of different trust levels, creating big challenges to secure the environment. While the perimeter of data center is typically secured with firewalls, there is a need to secure the increasing amount of VM-to-VM (east-west) traffic that is generated by modern applications. In other words, both network infrastructure and security provisioning need to be dynamic to enable application agility for enterprise IT. Equally so, in service provider environments, infrastructure automation and dynamic chaining of network functions remain the top priorities in their journey towards implementing their cloud infrastructure.

THE SOLUTION

The Big Cloud Fabric™ (BCF) solution with Palo Alto Networks next-generation firewall enables a simple, yet powerful approach to enforce fabric-wide security for any variety of virtual/bare metal workloads. This can be achieved by configuring policies for redirecting traffic to firewall irrespective of the physical location of the workloads or the location of the physical or virtual Palo Alto Networks next-generation firewall. The interoperability of the two products has been validated for VMware and OpenStack environments. For VMware powered data centers, the solution offers firewall service insertion for both north-south and east-west traffic in the fabric. Customers can benefit from the flexibility and simplicity of firewall service insertion provided by this integration along with physical networking automation and visibility achieved through BCF integration with VMware vCenter. For OpenStack deployments, the joint integration secures OpenStack clouds at a tenant level through automation enabling rapid deployment of clouds that are secure, scalable, and resilient.
**SOLUTION BRIEF**

**THE SOLUTION COMPONENTS**

**Palo Alto Networks Next-Generation Firewall**

Palo Alto Networks next-generation firewalls are architected to safely enable applications and prevent modern threats. They identify all network traffic based on applications, users, content and devices, and let users express business policies in the form of easy-to-understand security rules. There are multiple deployment options including the VM-Series virtualized next-generation firewall that brings secure application enablement and advanced threat prevention for private, public and hybrid cloud environments. The VM-Series has feature parity with Palo Alto Networks physical form factor firewalls, and is managed using the same management, ensuring a consistent set of policies is maintained across heterogeneous environments. Palo Alto Networks Panorama™ is a centralized management that provides the ability to manage a distributed network of virtualized and physical firewalls from a single location. Capabilities include the ability to view all firewall traffic, manage all aspects of device configuration, push global policies, and generate reports on application traffic patterns or security incidents.

**Big Cloud Fabric**

Big Cloud Fabric is the next-generation datacenter switching fabric that leverages software-defined networking (SDN) controller technology and open networking (white-box or brite-box) switches, to make networks intelligent, agile and flexible. Intelligence stems from its software-defined switching fabric acting as “one logical switch” that simplifies operations and provides full visibility & telemetry. Agility is delivered via network automation for rapid deployment of applications and services, one-click troubleshooting for faster resolution, and zero touch upgrades. Flexibility is provided by BCF’s scale-out capabilities to accommodate future growth in east-west traffic. Leveraging its ability to run on open hardware, BCF provides network hardware vendor choice and lowers costs.

**HOW THE SOLUTION WORKS**

**Palo Alto Networks with Big Cloud Fabric for OpenStack**

The BCF P+V (Physical + Virtual) solution for OpenStack with Palo Alto Networks next-generation firewall provides a self-service model for secure, application deployment. The joint solution enables the firewall service to be deployed at the edge of the tenant network for north-south traffic or between the application tiers for east-west traffic. The tenant can define a service insertion policy to redirect traffic to the firewall from the tenant logical router that connects multiple segments within the tenant. The solution simplifies OpenStack networking through L2/L3 automation achieved through the BCF OpenStack plugin. In addition, policies for the firewall can be configured through a plugin that is available on the Horizon dashboard. With Palo Alto Networks next-generation firewall, security policy attributes such as application name, user and network traffic content can be leveraged and configured with Palo Alto Networks Panorama™.

**Palo Alto Networks with Big Cloud Fabric for VMware**

The joint solution for VMware-based workloads offers simplicity, automation, security, and visibility for physical networking via the BCF integration with VMware vCenter and with a simplified mechanism for Palo Alto Networks next-generation firewall service insertion. From a logical view, fabric-wide policies can be configured to redirect traffic to the Palo Alto Networks next-generation firewall for inspection from the logical router that connects one BCF logical network segment to another. Physically, the workload VMs can be residing on different machines across different racks, associated with different VMware port-groups, and the Palo Alto Networks next-generation firewall can be deployed on a different rack. When deployed with NSX, the solution provides visibility and automation for underlay networking with ability to enforce security policies for inter-VM traffic.
SOLUTION BENEFITS

Simplified Security Provisioning.
With a software-defined architecture, BCF acts as “one logical switch” with the ability to configure the entire fabric from a single pane of glass. The solution offers a simplified way of configuring fabric-wide policies for redirecting traffic irrespective of the physical location of the workloads. The Palo Alto Networks Panorama provides ease of security policy configuration and visibility to all traffic going through the next-generation firewall.

Secure Application Enablement and Comprehensive Threat Protection
The Palo Alto Networks next-generation firewall offers complete visibility into all network traffic based on applications, users, content and devices. Business policies and practices are translated into security posture, resulting in safe enablement of applications and comprehensive threat prevention from modern-day threats. The combination of Content-IDTM and WildFireTM technologies provide protection from known and unknown threats. Content-ID limits unauthorized data transfer, detects and blocks a wide range of threats. WildFire identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment, and automatically disseminates updated protections globally in near-real time.

Centralized Visibility and Troubleshooting
Big Cloud Fabric GUI provides fabric analytics for advanced multi-node analytics, troubleshooting, and telemetry. This includes historic time series information related to specific VM workloads. BCF provides the capability to trace the path through the fabric from one VM endpoint to another. This enables data center operators to deploy applications rapidly, simplifies operational workflows and provides immediate root-cause analysis when application performance issues arise.

Agile and Secure Application Deployment
The centralized BCF controller exposes REST APIs and acts a single point of integration for orchestration systems such as VMware vSphere and OpenStack. The solution thus brings operational agility through physical network automation for VMware and OpenStack environments. The dynamic security provisioning and management that can be achieved with automated insertion of the Palo Alto Networks next-generation firewall in the fabric enables agile deployment of secure applications.

About Palo Alto Networks
Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyberthreats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today’s dynamic computing environments: applications, users and content.
Find out more at www.paloaltonetworks.com.