TechTarget Custom Media
White Paper

Delivering Scalable and Simple Network Security in AWS

The migration to the public cloud using fully cloud native infrastructure continues to accelerate. A clear benefit of this move is the ability to utilize and deploy resources holistically, at speed and with agility. There's more to this development than just moving workloads, however: those workloads must be secured.

A key strategy for securing cloud workloads is cloud network security—the discipline of inserting security controls into cloud networks to gain comprehensive visibility into traffic and prevent threats from propagating throughout the environment. While cloud network security has become an essential part of overall cloud security posture, network operations teams have historically struggled to insert security controls without complicating cloud networks and negatively impacting application performance.

Meeting the challenge of providing adaptive, scalable, and automated network security and performance begins with solving two allied problems. First, it is essential to have a cloud network that can support the throughput, dynamism, and resilience necessary for cloud native infrastructure. The other half of the equation is to have a cloud native virtual firewall that is automated and flexible. However, to really deliver an optimal environment, it is necessary for both network security tools and cloud networks to work together seamlessly.

This empowers DevOps, SecOps, and network security teams to each focus on their unique tasks. Absent an integrated solution, complexity and manual intervention increase to unacceptable levels. When there is no automation or process, security often "breaks" or is left out of the equation for simplicity's sake.

To help organizations move forward to a truly secure cloud environment, this paper explores the benefits of the recently introduced AWS® Gateway Load Balancer (GWLB) from Amazon Web Services and its integration with Palo Alto Networks VM-Series Virtual Next-Generation Firewalls. This joint offering ensures the cloud network can deliver the agility and reliability organizations need, coupled with flexible, always-on security. The following details how the service goes beyond the limitations of legacy security approaches and simplifies numerous aspects of cloud network security operations.

The Limitations of Common Legacy Approaches

As organizations move to cloud native infrastructure, the problem of consistent security with scale, visibility, and agility becomes apparent. Additionally, there are many other challenges that stem from bringing legacy security approaches to the leading cloud service platforms. These limitations include:

- **Lack of automation:** As workload mobility increases, it can become overwhelming when network traffic must be secured with many manual processes. DevOps teams want to help the business by accelerating cloud agility, and SecOps teams must ensure the business is safe by securing the cloud. If security tools and workflows require constant manual intervention with every change in the cloud, the business must make tradeoffs between agility and security in the cloud, creating friction between SecOps and DevOps teams. As such, the dynamic nature of the cloud requires automating as many operational tasks as possible.
- **Inability to deploy consistent security:** Without automation and integration of the network firewall and the cloud service, it is difficult to ensure all security policies are put in place every time. In a dynamic environment, SecOps can be stuck playing whack-a-mole as inconsistent security implementations frequently and unexpectedly show up. Worse, inconsistent security coupled with poor network visibility will almost ensure the existence of vulnerabilities.
- **Lack of support for shared responsibility models:** These models assign obligations for who does what for securing cloud applications and workloads. Cloud service providers are responsible for the security of the underlying infrastructure of the cloud environment while users are responsible for the workloads, assets, and data placed in the cloud. Most legacy security deployments were not designed with this in mind, which adds to the IT and security staff workload. A solution built to align with shared responsibility models, and proven to support them, solves numerous problems before they have a chance to occur.

Simple and Scalable Network Security: AWS and Palo Alto Networks Provide a Better Way

The launch of AWS GWLB, integrated with the VM-Series NGFW, offers the solution to providing scalable and secure infrastructure. AWS GWLB is designed to balance network traffic for AWS environments. This managed service supports the deployment of a stack of VM-Series firewalls that are both scalable and fault-tolerant. Simplifying firewall insertion enables next-generation threat prevention at scale in an AWS environment. The integration of these two solutions eliminates the security-performance tradeoff while solving the other limitations of legacy approaches. It provides a central point of management to drive consistency, using GWLB to scale and load balance across a fleet of VM-Series firewalls.

Solving the scalability problem in this way enables both DevOps and SecOps to focus on what they do best. This is important because they sometimes have conflicting goals. With the GWLB and VM-Series solution, the DevOps team can focus on building or enhancing applications, and the SecOps team can focus on network security policy without impeding the DevOps team's agility and productivity. SecOps will continue to be concerned about development, but the integration will help ensure more consistent compliance with the company's security policies.

Another important component of the solution is solving the security-performance tradeoff that occurs when network security and cloud services are managed separately. Without this resolution, the ability to leverage cloud benefits is severely restricted. For the SecOps team, this offering also supports distributed security inspection. The work AWS and Palo Alto Networks have done to integrate their respective products makes a great deal of difference in achieving both performance and security.

One very important benefit of using the combination of GWLB and VM-Series virtual firewalls is that traffic can be decrypted on the fly by the firewall, allowing all traffic to be evaluated. These benefits and many others simplify the deployment and daily operations of the joint solution, relieving IT and SecOps teams from several low-value, repetitive, and manual tasks. With a single solution, it is possible to ensure consistent security policy implementation across all workloads. As a result, security posture is improved, which helps when it is necessary to demonstrate regulatory compliance.

This consistency is supported using a single console to manage all firewalls across cloud networks. Furthermore, the joint solution is designed with the shared responsibility model in mind, which simplifies what the customer must do to ensure its security obligations are met. Many of the manual and time-intensive elements of the process are in place thanks to the work AWS and Palo Alto Networks have already done.

Business Benefits of the Joint AWS-Palo Alto Networks Solution

The real value of a technology solution is defined by how it supports business success: technology must be an enabler. The combination of GWLB and VM-Series firewalls delivers several compelling benefits to organizations that implement it.

The first benefit is critical to a modern digital business: improved speed and agility for delivering new digital business processes. Enabling DevOps to focus on delivering applications more quickly without requiring the team to focus on security means projects can be completed faster. These new or enhanced apps are the drivers of better digital processes, and the more rapidly they are delivered, the sooner they can be used to create competitive advantage and deliver better return on investment.

Ensuring performance is not impacted when workloads scale up is a major benefit as many cloud workloads can have frequent or unexpected peaks and need to scale up quickly. This flexibility helps ensure all performance metrics remain within normal operating parameters.

Another important benefit of the joint offering is ensuring consistent and effective security is automatically put in place. The corporate penalties for data breaches or falling out of compliance can be substantial. With a solution capable of reducing the risk profile across the cloud, there is less potential for a damaging public data breach. From a compliance perspective, the ability to show consistent and pervasive deployment of security policies makes it easier to pass audits.

Improved efficiency is an important goal for a modern enterprise. This solution supports efficiency in several ways. First, cost-effective deployment and management reduces demands on staff resources. Using one solution across AWS—including AWS Outposts™—for network security reduces the demands on IT and SecOps staff. Complexity is reduced, and that leads to more efficient daily operations, with changes and updates being less resource-intensive. This comprehensive solution also makes numerous point products redundant and therefore no longer necessary, eliminating the cost of adding and managing them.

Key Takeaways

The promise of the cloud must not be undermined by any aspect of IT infrastructure. Application performance problems are unacceptable. Ensuring network and virtual firewalls do not become bottlenecks is an important factor in delivering effective cloud infrastructure. The integration of VM-Series virtual firewalls with load-balancing technology solves the problem. To be effective, the virtual firewall and AWS cloud services must be seamlessly integrated. Full integration ensures protection of workloads without the need for constant manual intervention.

The recent delivery of AWS GWLB, leveraging seamless integration with Palo Alto Networks VM-Series firewalls, provides a consistent and effective security layer with the agility cloud demands. This automated solution lets IT Ops and SecOps work better together and allows each team to focus on more pressing tasks. For more information, please visit Palo Alto Networks online for a virtual Ultimate Test Drive.

paloalto NETWORKS

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

This content was commissioned by Palo Alto Networks and produced by TechTarget Inc.