Cloud Generation Firewalls

Security, Access, and Reliability for Cloud-connected Networks and Applications

White Paper

Introduction

As the adoption of cloud-hosted applications and infrastructures has grown, there has been an increasing awareness that previously existing firewall capabilities are insufficient to meet the needs of distributed organizations whose networks and mission-critical applications are integrated with the cloud.

This has led to the development of "Cloud Generation" firewalls. These firewalls retain the application awareness, visibility, and granular controls that characterized the earlier "next generation" firewalls. However, they add capabilities that enable robust SD-WAN infrastructures, and they simplify deployment, configuration, and management across hybrid networks that integrate both on-premises and cloud-hosted resources, applications, and workloads.

Barracuda has been at the forefront of development of cloud generation firewalls. The Barracuda CloudGen Firewall delivers extraordinary benefits by combining:

- Highly effective security capabilities
- Features that improve branch-to-branch, branch-to-cloud, and cloud-to-cloud connectivity
- Infrastructure cost savings derived from leveraging multiple low-cost lines in the place of high-cost MPLS connections
- Native public-cloud platform integration

Shortcomings of Traditional Perimeter Firewalls in the Cloud Era

Traditional security strategies and network architectures were never intended for today's cloud-integrated infrastructures and workloads.

Lack of Scalability for Branch-to-Cloud Connectivity

As you add more locations and adopt SaaS applications such as Office365 and SalesForce, backhauling becomes too expensive, complex, and limiting, robbing you of the benefits of the SaaS model. Instead, your remote branch offices need secure, optimized connectivity to cloud applications through direct internet breakouts. Firewall architectures based on custom hardware can provide high performance on large, centralized appliances, but the features and performance cannot scale out to branch office firewalls without significantly compromising functionality, security, and performance.

Lack of Scalability for Public Cloud and Hybrid Environments

Traditional "next-generation" firewalls and traditional data-center firewalls don't easily translate to a public-cloud environment. Some vendors may create stripped-down virtual firewalls to address public cloud use cases, but these editions come with significant performance and feature limitations. Moreover, you cannot easily integrate them into cloud fabrics, and they don't leverage the benefits of cloud automation around deployment, auto-scaling, high-availability, cloud networking topologies, and cloud monitoring. They are not interoperable with the variety of management and monitoring tools available on public cloud platforms. And they are unable to deal with routing and network related limitations within cloud fabrics. This prevents you from fully leveraging the simplicity, elasticity, and performance benefits of the cloud.

High Management Complexity in Cloud and Hybrid Environments

If you're operating distributed firewalls across multiple locations, including in public-cloud infrastructures, you need an easy way to deploy, configure, manage, and monitor your entire firewall deployment through a unified interface. This is even more critical for highly dispersed environments, hybrid environments across on-premises and cloud platforms, and deployments across multiple cloud platforms. The lack of a well-designed, easy-to-use centralized management console can mean that your management overhead expands uncontrollably.

New Requirements for Cloud Generation Firewalls

In the cloud era, the role of the firewall is expanding significantly. Public cloud infrastructure deployments introduce a completely new set of security requirements. In addition, they require firewalls that have the capability to scale networks and applications rapidly while simplifying management and optimizing connectivity.

Act as Secure Connectivity Gateways

In addition to typical security and application regulation functions, the cloud era requires network firewalls to regulate traffic flows across on-premises and cloud-hosted data centers. This includes providing secure and optimized site-to-cloud tunnels, SD-WAN features to economically route traffic across the extended network while maintaining performance, and traffic compression or deduplication to minimize network bandwidth costs.

Fully Integrate with Public-Cloud Platforms

Network firewalls should integrate with the full suite of management, monitoring, and automation capabilities that are built into public cloud infrastructures. This includes technologies like AWS Cloudwatch, AWS Direct Connect, Azure Security Center, Azure OMS, Azure ExpressRoute, and Cloud Interconnect in Google Cloud Platform. Firewalls should be capable of being deployed in high-availability clusters for full redundancy across architectures that may span multiple availability zones. In addition, they should support new consumption and payment models that allow you to maximize your cloud investments.

Centrally Managed "Security at the Source"

Network firewalls should support micro-segmented, application-centric, network architectures for distributed policy enforcement at all cloud network gateways. And administrators must be able to manage a dispersed security posture across multiple data paths from a unified control panel.

Web application firewalls in the cloud should easily scale, migrate, and adapt to each application workload (as opposed to traditional data centers where multiple services are secured behind a single hardware appliance). Web application firewalls must also be easy for cloud developers to deploy and configure, so that they can accelerate development by integrating robust application security during the development process. They must also provide API-based interfaces so they can be integrated into agile DevOps tool chains like Puppet and monitoring tools like Splunk.

Cloud Generation Firewalls Ensure You Are "Cloud Ready"

Unlike the rigid perimeter security devices of the past, Barracuda CloudGen Firewalls are scalable, elastic, extensible solutions that can seamlessly bridge on-premises, internet, private, and public cloud networks. Without compromising on comprehensive protection against advanced threats, they give you fast, secure, and reliable access to business applications across any deployment scenario.

Barracuda CloudGen Firewalls are ideally suited for distributed organizations leveraging SaaS applications and adopting public cloud platforms like Amazon Web Services, Microsoft Azure, and Google Cloud Platform. They are deeply integrated with AWS and Azure, to maintain and amplify all the key benefits of the cloud through auto-scaling, templatized deployments, HA support, data-logging, and more. Barracuda CloudGen Firewalls for GCP are the first network firewalls for Google's public cloud offering.

They are based on cloud-first architectures, and they leverage micro-services to deliver rich features and high performance. They provide secure connectivity, network traffic optimization, and advanced application security for at-scale deployments in a variety of network environments. Powerful centralized management makes it easy and highly cost effective to manage a unified security posture across hybrid and multi-cloud environments.

Barracuda CloudGen WAF is an enterprise-grade application security solution built in and for the cloud. Configured and provisioned within the Azure, AWS, and Google Cloud Platform marketplaces, CloudGen WAFs scan and secure your online applications, eliminating both known and zero-day vulnerabilities. They defeat today's most sophisticated, complex threats, including DDoS attacks, with advanced inspection capabilities that do not impact throughput. They inspect inbound traffic to combat web-based attacks including the OWASP Top 10, and outbound traffic to prevent data loss and leakage. And they improve overall app performance with built-in application delivery features including SSL offloading, load balancing, and content caching.

CloudGen WAFs are built to help you fully realize the benefits of the cloud, with simple centralized management across multiple domains and platforms, and all the scalability and flexibility that the cloud demands.

Barracuda CloudGen Firewalls and CloudGen WAFs are available with a variety of consumption and payment models, including pay-as-you-go, bring-your-own-license, and metered billing, in order to fit in with the variety of SaaS and IaaS purchasing options.

Conclusion

If you attempt to carry your incumbent, on-premises security infrastructure over to your new cloud-integrated network, without fully evaluating its fitness for the new environment, you risk finding out too late that it lacks the scalability and other features that you need to fully leverage the benefits of your cloud migration—and losing a lot of time and money trying to make it work anyway.

Realizing the benefits of cloud computing demands a completely new set of requirements around connectivity, scalability, security, integration, and deployment. Legacy security architectures based on customized platforms purpose-built for on-premises data centers and networks are just

not cut out for public cloud frameworks. Worse, the wrong choice could force you to compromise on features or performance and add to your deployment overhead—eventually making the cloud more cumbersome than your existing infrastructure.

Barracuda's Cloud Generation Firewalls for network and application security help you become "Cloud Ready." No matter how you choose to deploy your infrastructure and workloads, Barracuda CloudGen Firewalls and Barracuda CloudGen WAFs can fortify your network, secure connectivity across on-premises and cloud components, and protect your business.

About Single Point of Contact

The cloud experts at Single Point of Contact have helped hundreds of firms build and implement a cloud environment. As one of the first adapters of this technology, Single Point of Contact is one of the most experienced cloud consultants in the Bay Area. Contact us today to learn more about how the experts at Single Point of Contact can help increase security and provide a flexible solution for your companies requirements.

single point of contact