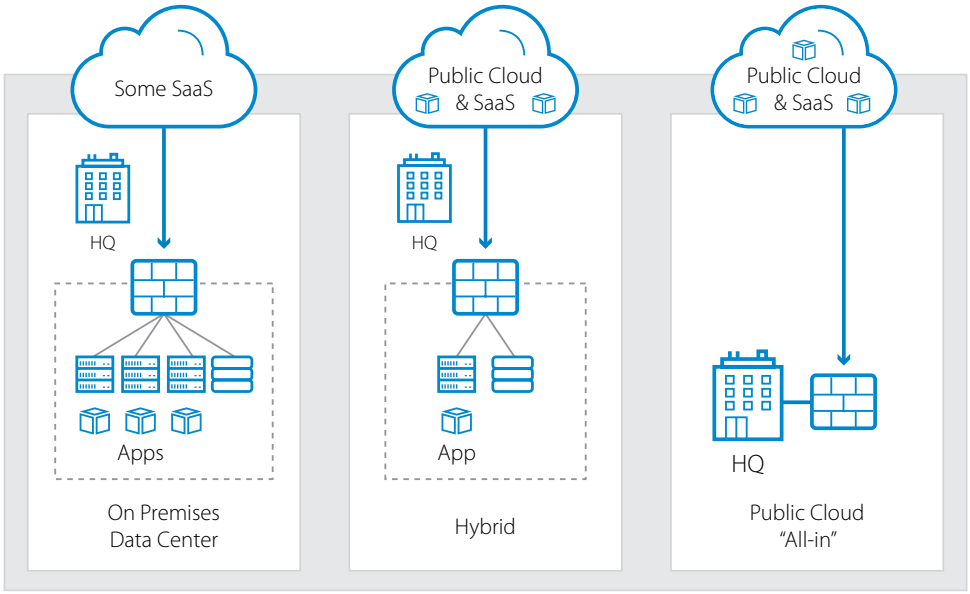
Secure Migration to Public Cloud Platforms and Hybrid Environments

How Barracuda CloudGen Firewalls Simplify and Accelerate Your Network's Evolution

White Paper

Where Will Your Applications Be in Two Years?

If your organization is like most, the answer to this question includes public-cloud hosting for some or all of the applications you depend on to operate. The benefits of using cloud-based platforms are simply too great to ignore, and those who fail to leverage them risk significant competitive disadvantages.



Migration to the cloud typically proceeds along three phases.

- In Phase 1—where a majority of organizations see themselves today—applications and data reside in on-premises data centers. However, even Phase-1 organizations are already reliant on cloud-hosted SaaS applications such as SalesForce, Microsoft Office 365, and many others. As a result, they are already coming up against architecture and security challenges related to the need for constant access to resources hosted outside the traditional network perimeter.
- In Phase 2, some workloads move to a public-cloud environment, but business-critical apps and data, as far as possible, are kept in on-premises data centers. The traditional network perimeter is still important, but it is smaller in this hybrid model. The importance of fast, reliable connectivity to the internet from any location grows more pronounced, requiring attention to security strategies and architectural adjustments.
- The final phase is the jump to a pure-cloud environment and a "serverless" infrastructure. Your traditional perimeter effectively disappears. Instead, your network extends across a constantly shifting landscape of cloud-hosted resources, applications, and data. This requires a fundamental rethinking of network architecture and security.

In facing the challenges posed by cloud migration, it's critical to understand the roles played by your network firewall. Guarding against threats that attempt to cross a defined threshold is no longer sufficient. Instead, today's network firewalls must have new capabilities and intelligence to centrally manage dispersed networks, maintain a consistent security posture on-premises and in the cloud, and ensure seamless availability of applications and workloads wherever they reside. The role of the firewall is changing just as dramatically as your network architecture and your security posture.

The Risks of Migrating Legacy Security to the Cloud

The development of traditional next-generation firewalls took place long before the cloud became a central part of modern network architectures. They were designed to optimally protect "walled-garden" style networks—with all applications and data kept in a controlled environment, and all data traffic backhauled to the head office, through a single, secure Internet breakout with centrally administered rules.

In the cloud era, network architectures—and the role of the firewall within them—are completely different. Today the tasks of the firewall have evolved from just keeping the bad traffic out to making sure access to the cloud and to headquarters is available from any location in the wide area network at any time.

Some vendors responded to this evolution by simply porting their virtual next-generation firewall images to the cloud. But they (and their customers) soon found that firewalls designed for traditional architectures do not integrate easily or seamlessly with public cloud platforms, do not meet the requirements for cloud-typical applications, and do not offer consumption models optimized for the cloud. As a result, these kludgy solutions prevent users from gaining the full benefits of the cloud, by creating bottlenecks, complicating security and network management, and requiring complex deployment, integration, and configuration work whenever new virtual server resources are spun up.

To enjoy the full benefits of migrating to the cloud, you need firewalls that are designed from the ground up for the dispersed, cloud-connected network architectures that must replace traditional, walled-garden, hub-and-spoke designs. You need cloud-generation firewalls.

Requirements: Firewalls for the Cloud Generation

These are the six core design principles for cloud-generation firewalls:

- Their design must take into account the cloud-native features of different IaaS platforms. A cloud-generation firewall must easily and seamlessly integrate with platform-specific features such as Azure Security Center, Azure OMS, AWS Autoscaling, AWS Elastic Load Balancing, and AWS CloudWatch. These capabilities are critical for fully leveraging the benefits of the cloud, and make it simple for you to use multiple IaaS platforms simultaneously.
- Reliable, secure, high-speed, always-on connectivity to the cloud is critical for conducting business across your entire distributed network. For this reason, true cloud-generation firewalls must include a robust set of SD-WAN and traffic intelligence capabilities to optimize bandwidth use and minimize latency for critical traffic. They should be able to bond multiple physical internet uplinks into one logical VPN tunnel to the cloud, in order to ensure high uplink availability and automated failover. They should dynamically detect real-time bandwidth and latency across multiple uplinks, and ensure that critical traffic is always routed via the optimal link. And they must employ a robust, easy-to-use VPN protocol that securely transmits data cloud-to-cloud, cloud-to-branch, and branch-to-branch, regardless of the type of connection.
- Today's workloads are increasingly distributed across multiple locations and platforms, requiring large numbers of firewalls, in a variety of form factors. Cloud-generation firewalls must be able to deliver a complete set of advanced security features and capabilities, regardless of their size or the number of users.

- In the post-backhauling network, each remote location on the wide area network—including growing numbers of IoT devices—requires its own cloud-generation firewall. To let you deploy hundreds, or even thousands of firewalls across your network in a practical, efficient way, cloud-generation firewalls must have deployment-automation capabilities. Zero-touch deployment includes the ability for each firewall to simply connect to the network and immediately download and execute its own precise configuration script. Without the need for skilled IT personnel on site, massive simultaneous deployments are practically effortless. Cloud instances must use bootstrapping and deep platform integration to deploy quickly and simply.
- The configuration and maintenance of a large number of SD-WAN and next-generation firewalls across multiple cloud platform infrastructures can be very complex and time-consuming for even large and well-funded IT departments. Cloud-generation firewalls must provide powerful, single-pane-of-glass central management that allows enforcement of shared policies, easy setup using configuration templates, comprehensive control, daily administrative tasks, and lifecycle management from a single management console. They must enable administrators to govern hundreds or even thousands of firewalls as a single, unified system.
- The flexibility of the cloud calls for flexible billing models, and many users are already familiar with the variety of billing options offered by cloud service providers. True cloud-generation firewalls must support consumption models optimized for the cloud. You should have choices, including bring-your-own-license (BYOL), pay-as-you-go (PAYG), and metered billing—which lets you deploy as many firewalls as you need, and only pay for actual protected traffic by volume.

Firewalls Designed for the Cloud

Barracuda CloudGen Firewalls are designed for today's networks, not yesterday's. They are purpose-built from the ground up to meet all the requirements listed above.

CloudGen Firewalls are available as hardware or virtual appliances, and on public cloud platforms including Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform.

Today, Barracuda is the number one firewall in the public cloud, protecting more customers in Microsoft Azure than the next three firewall vendors combined.

Barracuda had the first firewall on Azure and was Microsoft Partner of the Year 2016 in the Azure Certified ISV Solution category.

Barracuda CloudGen Firewall is AWS Security Competency certified, and Barracuda closed the largest third-party security deal ever on AWS in 2017.

Today, Barracuda also has the first firewall on Google Cloud Platform.

When migrating workloads to IaaS platforms, you need to consider the "shared responsibility" security model. In this model, the cloud providers are responsible for the security of the cloud infrastructure, while you are responsible for the security of your data, applications and pathways to the public cloud. In the cloud era, network firewalls must do more than secure your network—they must also ensure you have uninterrupted network availability and robust access to cloud-hosted applications.

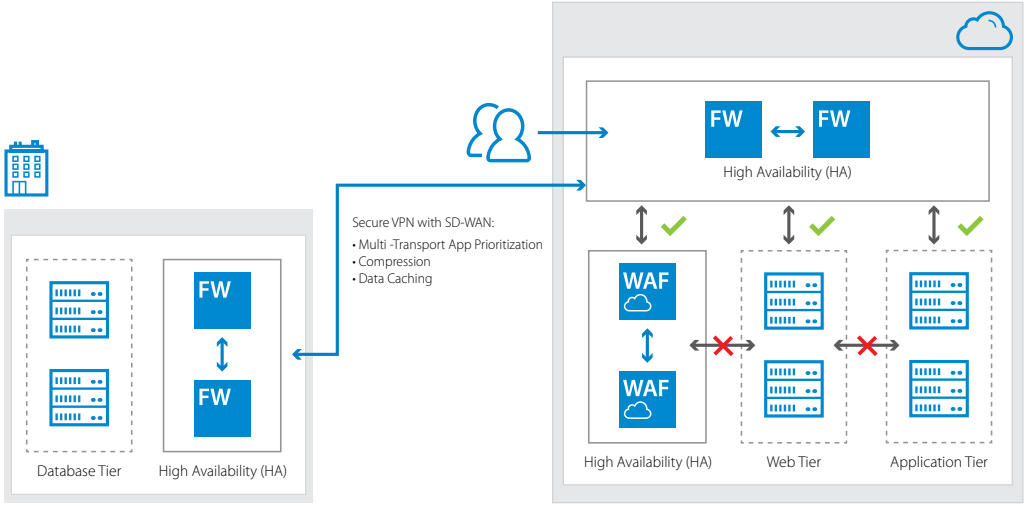
Barracuda CloudGen Firewalls protect and enhance your dispersed network infrastructure. They deliver advanced security by tightly integrating a comprehensive set of next-generation firewall technologies, including Layer 7 application profiling, intrusion prevention, web filtering, malware and advanced threat protection, antispam protection, and network access control.

In addition, Barracuda CloudGen Firewalls combine highly resilient VPN technology with intelligent traffic management and WAN optimization capabilities. This lets you reduce line costs, increase overall network availability, improve site-to-site connectivity, and ensure uninterrupted access to applications hosted in the cloud.

Scalable centralized management helps you reduce administrative overhead while defining and enforcing granular policies across your entire dispersed network. Barracuda's cloud-ready firewalls are ideal for multi-site enterprises, managed service providers, and other organizations with complex, dispersed network infrastructures.

Network Segmentation for Hybrid Applications

Segmenting networks into multiple network tiers provides security, visibility, and compliance for applications hosted in the public cloud. For compliance reasons, workloads such as database servers that hold sensitive data might need to be hosted on-premises, while application servers or web servers can be hosted in the public cloud. Barracuda CloudGen Firewalls secure, restrict, and monitor the communications between these tiers, while limiting the potential damage to an organization in the event of an attack.



If all workloads co-exist in the same cloud infrastructure, connectivity of Virtual Private Clouds (VPC) is manageable. However, if you need to use more than one cloud infrastructure at the same time, Barracuda CloudGen Firewalls let you segment networks transparently across multiple cloud infrastructure providers, so your cloud workloads work together seamlessly.

Deep Integration with Public Cloud Platforms

The most popular cloud platforms each have their own unique features, capabilities, and benefits. Barracuda CloudGen Firewalls are deeply integrated with the IaaS ecosystems, ensuring smooth and simple deployment, configuration, and scaling. Features include cloud-native automation and integration with the full suite of native management and monitoring capabilities, including Amazon CloudWatch, AWS CloudFormation templates, AWS Direct Connect, Azure Security Center, Microsoft OMS, Azure ExpressRoute, and many more.

Flexible Licensing Options Optimized for the Cloud

Barracuda CloudGen Firewalls make security and connectivity economical regardless of your network architecture. On premises, they can be deployed as appliances or on virtual machines. On IaaS platforms, they can be deployed as licensed virtual instances (BYOL) or using license-free PAYG or metered-billing models that scale elastically with your workload. Both pay-as-you-go and metered billing give you the flexibility to pay for actual firewall usage, on either an hourly or a volume-based billing.

Barracuda CloudGen Firewall Feature-Set at a Glance

Security

- Advanced Threat and Malware Protection
- Botnet and Spyware Protection
- Intrusion Detection and Prevention
- SSL Interception
- Stateful Deep Packet Inspection

Connectivity and SD-WAN

- Dynamic Bandwidth and Latency Detection
- Performance-Based Transport Selection
- Failover and Link Balancing
- Traffic Shaping and Quality of Service
- TINA VPN[1]

Remote Access

- Unlimited Number of VPN Clients
- Network Access Control (NAC) functionality
- Browser-based Mobile Portal
- CudaLaunch App for BYOD policies

[1]TINA (Transport Independent Network Architecture) is a proprietary high-performance VPN protocol that lets you create logical tunnels that make use of multiple physical transport paths.

Central Management

- 100% Scalability of Firewall Control Center
- Zero-Touch Deployment and Bootstrapping
- Drag-and-Drop VPN Graphical Tunnel Interface
- Multi-Revision Management
- Revision Control System (RCS)

The Right Tools for the Job

Wherever you are on your journey to the cloud, Barracuda offers the right tools for the job. The broad portfolio of CloudGen Firewalls includes hardware appliances in multiple form factors, virtual appliances, and cloud-hosted editions available directly on Microsoft Azure, Amazon Web Services, and Google Cloud platform. This gives you maximum flexibility in terms of sizing and deployment options to meet your specific needs without overprovisioning.

Barracuda CloudGen Firewalls combine comprehensive next-generation security features including Advanced Threat Protection (using cloud-based CPU-emulation sandboxing) with secure SD-WAN. This lets you establish a full-mesh network architecture, improve branch-to-branch, branch-to-cloud, and cloud-to-cloud connectivity, optimize MPLS usage, ensure a consistent security posture for data and workloads wherever they reside, manage rollout to remote locations economically with Zero Touch Deployment, and reduce IT overhead with powerful but simple central management.

Securing Web Applications Hosted in the Public Cloud

Today many organizations host their websites and web applications on public cloud platforms. The agility and elasticity of the cloud deliver real benefits, but you need to secure your web applications in the cloud just as well as you do on-premises.

Barracuda CloudGen WAF is a sister product to the CloudGen Firewall—a Web Application Firewall available for Azure, AWS, and Google Cloud Platform.

- Barracuda CloudGen WAF provides protection against distributed denial-of-service attacks and OWASP-listed attacks, as well as outbound data loss prevention. It also provides effective access control for your cloud-hosted websites.
- Check your websites for vulnerabilities with Barracuda Vulnerability Remediation Service, a free Barracuda service. Scan results can also be used as a WAF configuration document to automatically eliminate vulnerabilities.
- Quick and easy deployment, configuration, and scaling is a basic requirement in the cloud. Barracuda CloudGen WAF uses templates, auto-scaling, integration with cloud services, and APIs that enable automatic orchestration and deployment.

Barracuda CloudGen Firewall and Barracuda CloudGen WAF are the perfect combination to ensure seamless availability and comprehensive protection for your web applications in the cloud.

Conclusion

Barracuda CloudGen Firewalls are the right choice for organizations leveraging SaaS applications or public cloud platforms, those with large numbers of remote locations and/or IoT devices, and those wishing to position themselves optimally for a potential future move to the cloud.

> *Barracuda should be considered by enterprises that have a cloud infrastructure and want to secure it.*

Gartner Research Enterprise Network Firewall Magic Quadrant

2017

The Enterprise Security Group (ESG) states in a recently published Buyer's Guide commissioned by Amazon, "Barracuda provides a cloud-native solution with the required baseline level of integration with AWS—bootstrapping options for deployment, AES 256 encryption over all link types, traffic shaping controls, and IAM role-based access for security. Barracuda supported additional features and functionality that are above and beyond this baseline of support, based on their target market and use cases."

- Barracuda CloudGen Firewalls are purpose-built for securing cloud-connected networks.
- Barracuda offers cloud editions for the major IaaS platforms – Azure, AWS, and Google.
- Barracuda's long-standing partnerships with the major cloud vendors ensure continuous improvements.
- Barracuda offers flexible licensing models that allow leveraging the public cloud advantages to their full extent.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda®

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com