Cloud Deployments Demand Cloud Generation Firewalls

Securing your AWS environment means finding the right tool for the job.

93%

Today, 93% of organizations are already utilizing cloud services in some form.

80%

Organizations report that by the end of 2017, 80% of their IT budgets will be committed to the cloud.

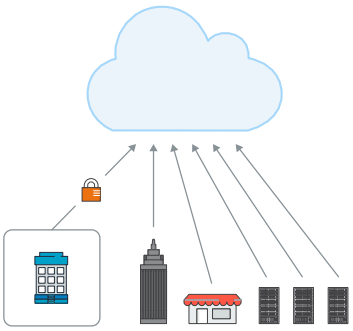
49%

Yet almost half of organizations report they have slowed their cloud adoption due to a lack of cloud-specific cybersecurity skills.

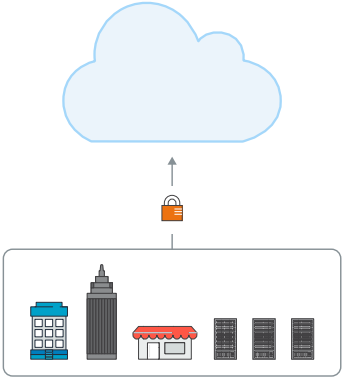
*Source: McAfee, from September 2016 survey report "Building Trust in a Cloudy Sky."

When you're building cloud environments, you need a security solution *built* for the cloud.

Network security is *different* on the cloud. While you might be tempted to re-purpose the enterprise firewall from your previous on-premises network, it's crucial to understand the difference between data center network security solutions, and security solutions that are truly engineered for today's cloud use cases.



Traditional enterprise firewalls are not engineered for a hybrid network with multiple entry points to the cloud.



Cloud Generation Firewalls protect your cloud environment from attacks.

Cloud security solutions are *engineered* for the cloud

True hybrid cloud security

- Cloud requirement: Visibility and control of security policies that are common across on-premises and cloud platforms
- The gap with legacy systems: Deployment architectures and the management experience differ between cloud instances and on-premises environments

Easy deployment and monitoring

- Cloud requirement: An easy way to deploy, manage, and monitor distributed firewalls across on-premises and cloud deployments
- The gap with legacy systems: Features, functionality, and the management experience differ between cloud instances and on-premises deployments

Flexible licensing and pricing

- Cloud requirement: Frictionless pricing and licensing that align with cloud consumption models and AWS "well-architected" principles (Metering, PAYG, BYOL)
- The gap with legacy systems: Traditional licensing models were designed for on-premises deployments. However, they lack flexibility and prevent customers from taking advantage of the agility offered by the cloud

The bottom line: Enterprise firewalls are built for *on-premises* use cases. Old-school firewalls include complicated features that simply aren't needed to protect cloud deployments, and they function differently than a firewall architected specifically for cloud use cases.

Three Key Characteristics of a Cloud Generation Firewall

1

Support for cloud deployment best practices

- Autoscaling
- API integration
- Rapid deployment and high availability
- Network traffic optimization
- Well-architected
- AWS Partner Network (APN) Competency Certified

2

A license-less billing model built for the cloud

- No large up-front multi-year license costs
- True utility-based pricing
- Pay only for security metered on throughput, rather than time

3

Support for cloud use cases

- Remote connectivity
- Highly-distributed, fully-meshed networks
- Many points of entry to be protected
- Workload migration

Cloud Generation Firewalls are engineered to support the specific deployment models, economic models, and use cases of today's cloud environments.

What does this look like?

Cloud Generation Firewalls include features engineered for cloud deployments

- VPN tunnels
- Multi-tier Architecture
- AWS Direct Connect
- Traffic control
- Access to resources

Cloud Generation Firewalls employ an economic model built for the cloud

Complete consumption flexibility:

- 90-day Free Trial
- Bring Your Own License (BYOL)
- Pay As You Go (PAYG)
- Metered billing (Throughput)

Cloud Generation Firewalls are custom designed for cloud use cases

- Cloud-native integrations: CloudFormation Templates, CloudWatch, SNS, SQS, ELB, S3, IAM
- Cloud connectivity and traffic optimization
- Scalable cloud application security
- Centralized management at scale

Unchain yourself from legacy architecture with a Cloud Generation Firewall engineered for AWS

The Barracuda NextGen Firewall (NGF) is a Cloud Generation Firewall engineered for the cloud age. NGF is an enterprise-grade firewall that secures your network perimeter while enabling rapid deployment and operation within distributed, highly dynamic, and security-critical environments on AWS. Features include:

Autoscaling

Scale up or down depending on network traffic, and pay only for the traffic.

High Availability

Place your Cloud Generation Firewall and data in multiple locations with Amazon EC2 instances. Deploying in multiple regions allows you to have 99.999% uptime.

Support for Fully Meshed Networks

Cloud Generation Firewalls offer security for all points of entry into your distributed network, with perimeter security around your entire network and security between all VPCs.

Easy Deployment, Automatic Upgrades

Deploy in minutes, not days, via the AWS Marketplace. To upgrade, simply make a configuration change, and your upgrade is ready.

Auto-Configuration

Auto-configuration and auto-deployment via AWS CloudFormation templates.

Frictionless Licensing

Metered billing with true consumption pricing based on throughput, not time.

Let go of legacy architecture. Choose the right tool for the job to protect your AWS deployment.

Free 90-day trial! Get started today with a Cloud Generation Firewall for AWS.

Simple to purchase, deploy and manage, Barracuda's NextGen Firewall for AWS makes securing your perimeter easy by combining comprehensive Application Control, Availability, and Quality of Service features with next-generation firewall capabilities that help stop bad traffic from coming in—while simultaneously enabling optimized performance for mission critical applications in the cloud. Sign up for a free trial today in AWS Marketplace.

Start free trial

Multi Region Support