Barracuda®

QUEENS PARK
CyberSecurity Solutions Ltd.

Secure Branch Office Connectivity and Optimized Access to SaaS Applications

Barracuda Cloud Generation Firewalls and SD-WAN

White Paper

Next-Generation Firewalls for the Cloud Era

More than ever, today's businesses rely on connectivity. We're growing more reliant on advanced dispersed networks. And new network topologies are emerging, to accommodate the accelerating adoption of SaaS solutions and public cloud platforms. It is increasingly critical to ensure predictable application performance, reliability, and secure connectivity at all times and at all locations.

To help ensure high connectivity and bandwidth while controlling bandwidth costs, next-generation firewalls must take on new operational tasks. They must ensure uninterrupted network availability and robust access to cloud-hosted applications, while also simplifying the management of dispersed network infrastructures.

Barracuda Cloud Generation Firewalls are designed to optimize distributed networks, scaling easily across any number of locations, platforms, and applications, and leveraging state-of-the-art technologies like SD-WAN and Zero Touch Deployment.

Ensure Secure Connectivity and predictable Application Performance at Every Remote Location

Total internet traffic is increasing rapidly, while tolerance for latency is declining. If your organization uses costly MPLS lines to optimize data transfer between central and branch offices, and also for backhauling internet traffic through central offices, you may be facing serious bandwidth challenges.

SaaS applications like Microsoft Exchange Online in Office 365 demand a latency of less than 50ms. But even with MPLS lines—which are costly, and not available everywhere—it's hard to maintain low latency when you're backhauling all network traffic from remote offices to headquarters and from there into the internet/cloud.

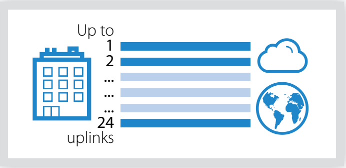
And if you're migrating workloads to public cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP), you need solutions with the specific features and scalability to help you fully leverage the benefits of cloud computing.

Cloud Generation firewalls must meet a completely new set of requirements around connectivity, scalability, security, integration, and deployment. Choosing solutions that don't meet these requirements could leave you with a cumbersome infrastructure that's hard to manage and can't leverage the full benefits of the public cloud.

Secure Branch Connectivity and SD-WAN Connectivity

Barracuda CloudGen Firewall is the first solution to combine a complete set of next-generation security capabilities with the connectivity optimization and cost savings of a full-featured SD-WAN solution into a single, easy-to-manage appliance available in physical, virtual, or cloud configurations.

Secure SD-WAN significantly increases WAN network reliability and performance by using and aggregating up to 24 active, load-sharing connections of any type (Broadband, 4G, MPLS, even 3G).



Aggregate up to 24 Uplinks indepent of type

Advanced data caching, traffic compression, and other WAN optimization capabilities give you an increase in available bandwidth. And you can always ensure there's enough bandwidth for business-critical applications by making dynamic, on-the-fly adjustments of QoS and application usage policies depending on dynamic bandwidth and latency measurements.

When CloudGen Firewall units are deployed in multiple locations, they can create a fault-tolerant, high-performance WAN network using only low-cost broadband lines. This optimizes your costs by combining multiple carriers/ISPs to get the required bandwidth and allowing for the reduction or elimination of expensive leased MPLS lines. Even with small rollouts of only a few devices, you can achieve a return on investment after just a few months. Typically, organizations can save thousands of dollars over just a few years.

Calculate potential savings at
savings.barracuda.com

Barracuda CloudGen Firewall F-Series appliances include Zero-Touch Deployment capabilities to streamline rollout to large numbers of branch offices that may lack qualified IT personnel. The appliances are shipped directly to the remote location without pre-configuration. Local staff simply unpack the appliance and plug it in, at which point it automatically connects to your Firewall Control Center. Full configuration settings are then sent securely to the appliance via an encrypted VPN tunnel, and the appliance becomes part of your security infrastructure. With Zero Touch Deployment, rollouts to hundreds and even thousands of remote locations are executed quickly, managed easily, and completed with fewer IT resources.

Summary: Optimized Site-to-Site Connectivity

- Create secure pathways across both multiple WAN connections and multiple carriers leveraging SD-WAN
- Easily establish secure VPN connections across multiple sites using only broadband
- Ensure application performance by transparently spanning up to 24 physical uplinks to create highly redundant VPN tunnels.
- Increase available bandwidth thanks to built-in caching and traffic compression.
- Fast rollout with Zero Touch Deployment

Barracuda CloudGen Firewalls combine highly resilient VPN technology, intelligent application based traffic management, and WAN optimization capabilities. This helps you reduce line costs, increase overall network availability, and improve site-to-site connectivity.

Direct Internet Breakout at Every Location for Predictable SaaS Application Performance

Backhauling internet traffic to a central breakout is no longer sustainable once you decide to leverage SaaS applications such as Exchange Online or SharePoint Online in Office 365. These cloud-connected applications increase overall traffic while requiring very low latency. To manage these demands, you need a different architecture, one that enables local internet breakouts at every location for direct access to cloud services.

Barracuda CloudGen Firewalls provide a unique set of technologies to support SaaS application availability. Application-aware security and prioritization ensures that business-critical SaaS applications like Office 365 are assigned the highest priority. You can also set traffic to bypass SSL inspection when needed to comply with Microsoft's requirements. Application-based link selection makes sure there will always be enough bandwidth by assigning critical SaaS application traffic to the best available uplink.

Every firewall on the market today can block and allow traffic for specific applications. But Barracuda Cloud Generation Firewalls combine application control, security settings, Quality of Service, and routing and uplink selection to optimize accessibility of critical applications.

Cloud Ready for Public Cloud Adoptions

The ongoing shift of IT workloads to cloud services in order to increase flexibility and reduce costs requires a reliable, cost-effective extension of the company WAN to the cloud. This applies to headquarters as well as to direct Internet breakouts at every branch location. Barracuda CloudGen Firewall models come fully featured for all common Cloud IaaS providers, including Amazon Web Services, Microsoft Azure, and Google Cloud Platform, as virtual appliances, and in a variety of hardware appliances for even small offices. Barracuda Firewalls fit your existing architecture while making you ready for a swift and easy transition to a new, cloud-integrated infrastructure.

Barracuda's CloudGen Firewall Feature Set at a Glance

Barracuda provides all the connectivity features required to ensure high Quality of Service with low IT overhead for dispersed networks.

- Secure SD-WAN and Traffic Intelligence
- WAN Compression
- Failover and Link Balancing
- Dynamic Bandwidth Detection
- Dynamic Latency Detection
- Performance-based Transport Selection
- Adaptive session balancing across multiple transports of a VPN tunnel
- Adaptive Bandwidth Reservation
- Application-Based Routing
- Zero-Touch-Deployment

The Cloud Generation Firewall for Today and the Future

Barracuda CloudGen Firewall let you easily establish optimized site-to-site connectivity and at the same time reduce network bandwidth cost and IT overhead. Simplified rollout and centralized management from a single pane of glass enable administrators to handle large deployments very efficiently.

The broad range of deployment options—hardware or virtual appliance, AWS, Azure, and Google Cloud Platform—give you maximum flexibility and make your network cloud-ready as you adopt more SaaS or IaaS services. With Barracuda CloudGen Firewalls, investments in network infrastructure are long-term and secure.

Securing Access to Corporate Resources for Remote Users

Remote and mobile users increasingly require access to corporate information and applications. Barracuda CloudGen Firewalls offer several options for fast and secure access to corporate resources.

- **Network Access Client** provides richer performance and functionality than standard IPsec client software for Windows, macOS, and Linux devices.
- **Browser Remote Access** provides simple browser-based remote access for desktop and mobile devices via Barracuda's SSL VPN Portal. The portal supports most commonly used devices, including Apple iOS, Android, Blackberry, etc.
- **CudaLaunch** a simple-to-use connectivity app designed for BYOD and mobile devices. The application is available for Windows, macOS, iOS, and Android and can be downloaded at the corresponding App Stores.

Browser Remote Access and CudaLaunch require the optional Advanced Remote Access Subscription for Barracuda CloudGen Firewalls. The subscription also adds a Personal Firewall and Health Checks for Windows to the Network Access Client.

Conclusion

Barracuda's Cloud Generation Firewalls redefine the role of the Firewall from a pure perimeter security solution to a distributed network optimization solution that can scale across any number of locations and applications, and connect on-premises and cloud infrastructures.

In addition to typical security and application regulation functions, Barracuda's CloudGen Firewall regulates traffic flows and provides SD-WAN features to economically route traffic across the extended network while improving performance. Replacing expensive, leased MPLS lines with inexpensive broadband and smart VPN tunnels providing traffic compression across multiple uplinks significantly minimizes WAN cost.

Today the fast growing adoption of SaaS solutions, like Office 365 and Salesforce, requires modern network topologies to ensure productivity. Backhauling becomes expensive, complex, and limiting as an organization expands. Barracuda's Cloud Generation Firewalls establish secure direct internet breakouts for all remote offices and branch offices locations, optimizing connectivity to cloud-based Software as a Service (SaaS) applications.

Finally, Barracuda's Cloud Generation Firewalls help you to be "Cloud Ready"—no matter how you choose to deploy your infrastructure and workloads in the future.

About Barracuda Networks

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. 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.

QPCSS LTD
QUEENS PARK
CyberSecurity Solutions Ltd.

Queens Park CyberSecurity Solutions

8a Bravington Road
Maida Vale
London
London
W9 3AH
United Kingdom
02039710740 info@qpcsl.com www.qpcsl.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