Barracuda

Solution Brief

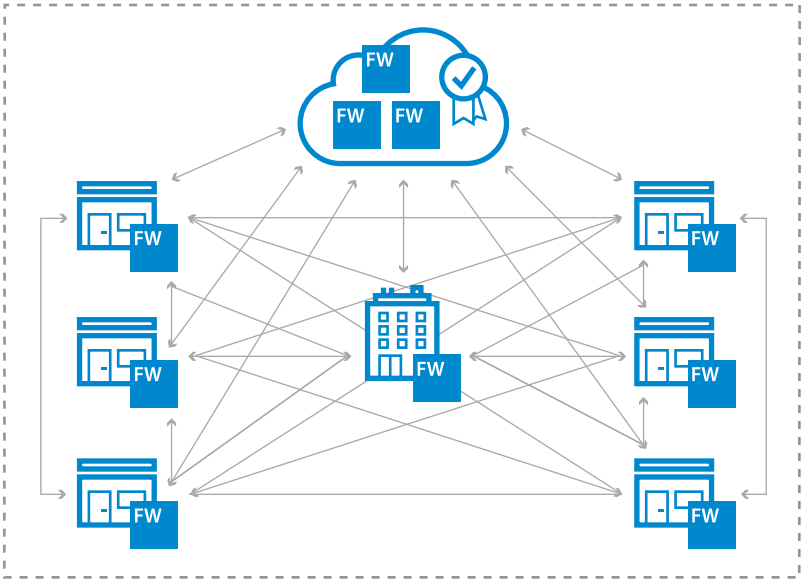
Secure Branch-to-Public-Cloud Connectivity with SD-WAN

Whether you are planning to migrate to the cloud or already have applications there, public cloud computing provides many benefits. But to leverage them, you need to ensure that branch offices have secure, reliable, low-latency access to applications and data hosted in the public cloud. Most wide area networks (WAN) today are still designed for a pre-cloud era, with all internet traffic backhauled to a central datacenter/breakout point where security policy is enforced. In the cloud era, this design causes too much latency, incurs unacceptably high bandwidth costs, and makes cloud-hosted applications perform poorly or become unusable.

The Need for Direct Internet Breakout

To benefit from public cloud infrastructure and Software as a Service (SaaS) offerings, you need to rethink branch office connectivity. Backhauling application traffic hundreds and even thousands of kilometers to a central hub for security inspection and then breaking out to the internet from there is not cost-effective. Furthermore, it hinders the performance of all your applications.

To intelligently enforce security inspection for direct internet breakouts, you need a different architecture—one that enables management of security enforcement, networking, and application prioritization transparently across the whole organization, including all public cloud deployments. Barracuda CloudGen Firewalls provide a unique blend of scalable central management, local security enforcement, and advanced uplink intelligence and QoS for every branch office. This enables direct internet breakout with direct VPN tunnels to your cloud deployments and applications at every branch office.

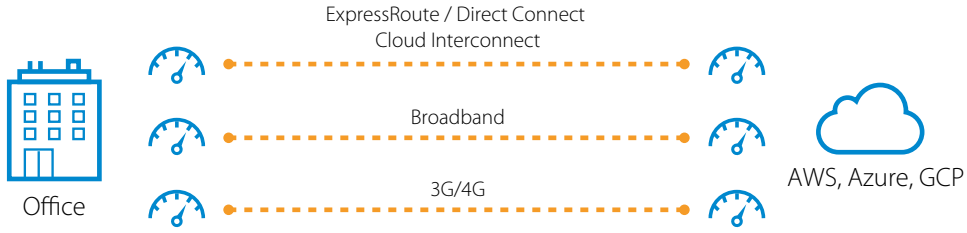


100% Centrally Managed Infrastructure

Always-On Connectivity and Application Availability, Regardless of Branch Location or Significance

You also need to rethink branch office connectivity if you want to benefit fully from the cloud. In addition to its core security and application regulation capabilities, Barracuda CloudGen Firewalls optimize traffic flows both to the cloud and within your WAN. Its full SD-WAN functionality optimizes performance across your entire network. You can replace expensive leased lines with multiple inexpensive broadband internet uplinks that are used simultaneously for logical VPN tunnels. In the event of an uplink failure, the Barracuda CloudGen Firewall instantaneously and transparently shifts sessions to the remaining uplinks, without session loss or work interruption.

In order to achieve the best possible application performance, Barracuda CloudGen Firewalls proactively measure the available bandwidths and latency between VPN endpoints for each of the physical uplinks to the cloud and other remote locations. The results are directly available to the firewall policy engine, which dynamically selects the most suitable uplink for each application based on predefined application criteria. In case an uplink shows measured bandwidth or latency outside of defined limits, the firewall temporarily disqualifies this path until the permanent measurements indicate the uplink becomes usable again. Additionally, if the measured bandwidth of an uplink is not sufficient to sustain business-critical traffic (e.g., VoIP), the CloudGen Firewall automatically shifts sessions for non-critical traffic to secondary links, to free up high-quality bandwidth for critical traffic. All of these technologies, along with built-in traffic compression and data-duplication, come standard in every Barracuda CloudGen Firewall, from small, fanless desktop or home-office models, to 2U rackmount datacenter models, virtual editions, and public cloud editions for Amazon Web Services, Microsoft Azure, and Google Cloud Platform.



Barracuda CloudGen Firewalls at a Glance

- Secure SD-WAN for all models and all platforms
- WAN compression and data deduplication
- Failover and link balancing
- Dynamic bandwidth and latency detection
- Performance-based transport selection
- Adaptive session balancing across multiple transports of a VPN tunnel
- Adaptive bandwidth reservation
- Application-based routing
- Application control
- Deep application context
- File content enforcement
- Custom application awareness
- User identity awareness
- Web filtering
- Botnet and spyware protection
- Intrusion detection and prevention
- DoS and DDoS protection

Summary

Barracuda CloudGen Firewalls provide a unique amalgamation of next-generation security, fully integrated SD-WAN, and public-cloud readiness. This enables the most cost-effective, uninterrupted access to companies' resources hosted in the public cloud. Full integration into Barracuda Firewall Control Center architecture with Zero-Touch Deployment guarantees hassle-free centralized management of thousands of remote devices. Advanced security functions include application enforcement, IPS, URL filtering, antivirus, sandboxing (ATP), and Denial-of-Service protection.