Barracuda®

single point of contact

Barracuda CloudGen Firewalls

Features and Capabilities Driving Significant IT Cost Reductions

White Paper

Contents

Introduction

When choosing a network firewall, your top concern is security. You want a solution that uses the most advanced scanning and detection technology available—one that will continue to evolve to always stay ahead of the latest advanced threats. And if you choose a Barracuda CloudGen Firewall, no matter which model or deployment option you choose, you'll have best-of-breed security tailored to your needs.

In a perfect world, that's all you would need to know. But in the real world, costs matter—a lot. That's why we engineer the Barracuda CloudGen Firewalls to include features and capabilities that deliver dramatic reductions in your overall IT costs—securing your money as well as they secure your data.

Cost-Saving Capabilities

The Barracuda CloudGen Firewall includes powerful features to efficiently reduce and offset high line latencies and slow response times. Enterprise-grade WAN acceleration features such as data compression, byte caching, traffic compression, and protocol optimization significantly improve site-to-site WAN traffic. Additional cost-optimization features include state-of-the-art Layer 7 application control, Quality of Service (QoS), adaptive traffic prioritization and traffic routing, link aggregation, and failover capabilities. All of these capabilities included at no extra charge.

Data Compression

Data compression replaces redundant entries with short replacement characters. Depending on the nature of the data, this can dramatically reduce the required bandwidth volume .

All site-to-site traffic routed between two Barracuda CloudGen Firewalls is compressed to efficiently reduce WAN latency and improve performance. By implementing the ZLIB compression algorithm, the Barracuda CloudGen Firewall accelerates data transmission by reducing the transfer volume in order to achieve higher available bandwidth for critical data.

Data Deduplication

Data deduplication is also referred to as byte-level caching, network sequence caching, or dictionary compression. It is a technique to eliminate redundant data in a stream of network traffic, thus significantly reducing the number of bytes sent over the WAN. The network stream is chunked into equally sized pieces, for which a cryptographic MD5 hash is computed. The hash and the data is then stored in a local dictionary. If a previously sent data chunk appears again for transmission, the much shorter hash stored in the dictionary is sent instead.

Barracuda CloudGen Firewalls also support bidirectional byte caching, where data chunks that were sent in one direction are immediately deduplicated in the other direction as well, using the same hashes. Data deduplication is performed independent of protocol, and works on the transport layer. As a result, it transparently accelerates any TCP traffic that is exchanged between sites via Barracuda CloudGen Firewall site-to-site VPN tunnels.

Traffic Manipulation with Application and User Awareness

To optimize bandwidth utilization and employee productivity, you need to be able to monitor user behavior on the network—ensuring that time and bandwidth are not being wasted on non-productive internet use.

The Barracuda CloudGen Firewall combines deep packet inspection (DPI) and behavioral traffic analysis to reliably detect and classify Layer 7 applications and protocols, even when these protocols use advanced obfuscation, port hopping techniques, or encryption. This lets you eliminate undesired traffic, and to throttle bandwidth-eating traffic such as media streaming or video chat applications, which can interfere with business-critical applications.

By integrating Application Control into its core firewall, routing, and quality-of-service functions, Barracuda CloudGen Firewalls make it easy for you to define and enforce policies based on users and groups, security policy, location, and time of day. Policy actions can include blocking, allowing, and throttling. You can even enable or disable specific application features, such as Facebook Chat. Barracuda Energize Updates delivers continuous protocol and application signature updates, to ensure the ongoing effectiveness of application control capabilities.

Quality of Service

Your business-critical applications should not have their performance limited because other non-essential applications are hogging bandwidth. Barracuda CloudGen Firewalls provide robust quality-of-service (QoS) technologies that let you apply quality and service guarantees to selected traffic flows within the WAN, while de-prioritizing applications that are tolerated but not essential.

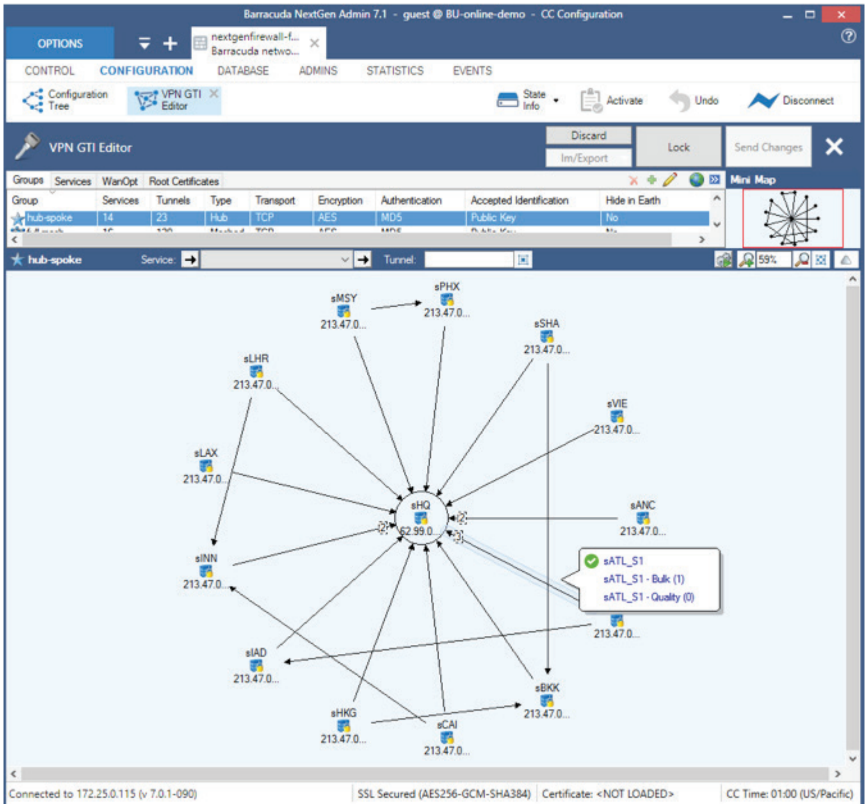
QoS technologies include traffic shaping, traffic prioritization, and bandwidth partitioning, which assigns a bandwidth limit to specific types of traffic. Real-time traffic analysis gives you the insight you need to apply optimal QoS-based policies.

Tunnel Independent Network Architecture (TINA)

Barracuda CloudGen Firewalls include a proprietary VPN protocol, TINA, that lets you build logical VPN tunnels based on up to 24 simultaneously used physical uplinks. This means that you can use inexpensive internet uplinks as the basis for extremely reliable, failsafe network connectivity provided. Powerful, multi-transport Traffic Flow Management features deliver the unprecedented capability to manipulate even encrypted traffic:

- Physical Transport lines (internet uplinks) can be identified and classified according to cost and quality. For example, you can classify a high-cost 4G line as reserved for overflow traffic only.
- You can use Multiple encapsulation transports (ESP, UDP, TCP and TCP/UDP-hybrid mode), as well as encryption mechanisms, in one logical VPN tunnel at the same time, effectively making TINA VPN tunnels immune to intermittent NAT devices or proxies (HTTPS, SOCKS) between two tunnel endpoints.
- The transports of a logical VPN tunnel may be used either simultaneously or on demand, fully configurable based on load, availability, and traffic contents.

A single, easy-to-use graphical user interface lets you visualize your entire WAN network of VPN lines, and allows simple, drag-and-drop tunnel creation across the enterprise:



Group	Services	Tunnels	Type	Transport	Encryption	Authentication	Accepted Identification	Hide in Earth
hub-spoke	14	23	Hub	TCP	AES	MD5	Public Key	No
full-mesh	16	120	Meshed	TCP	AES	MD5	Public Key	No

Connected to 172.25.0.115 (v 7.0.1-090) | SSL Secured (AES256-GCM-SHA384) | Certificate: <NOT LOADED> | CC Time: 01:00 (US/Pacific)

Figure 1: Graphical VPN Tunnel Editor

Link Aggregation and Failover

To increase available WAN bandwidth, Barracuda CloudGen Firewalls can aggregate up to 24 available internet links. Seamless failover from one internet uplink to another in case of connection loss ensures uninterrupted connectivity using low-costs uplinks.

Full Security Stack

Intrusion Detection and Prevention

All Barracuda CloudGen Firewalls include an Intrusion Detection and Prevention system (IDS/IPS) that strongly enhances network security by providing complete and comprehensive real-time protection against a broad range of network threats, vulnerabilities, exploits, and exposures in operating systems, applications, and databases. It prevents network attacks such as:

- SQL injections and arbitrary code executions
- Access control attempts and privilege escalations
- Cross-Site Scripting and buffer overflows
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Directory traversal and probing and scanning attempts
- Backdoor attacks
- Trojans, rootkits, viruses, worms, and spywareTCP split handshake protection

Barracuda CloudGen Firewall includes additional advanced attack and threat protection features including:

- IP and RPC defragmentation
- FTP evasion protection
- URL and HTML decoding

Barracuda CloudGen Firewalls identify and block advanced evasion attempts and obfuscation techniques that are used by attackers to circumvent and trick traditional intrusion prevention systems.

DoS and DDoS Protection

In today's world of omnipresent botnets, one of the main challenges for perimeter protection is to ensure ongoing network availability for legitimate requests while effectively detecting and repelling malicious denial-of-service attacks.

With built-in TCP SYN Flood Protection, the Barracuda CloudGen Firewall essentially functions as a generic TCP proxy, forwarding only legitimate TCP traffic to the inside of the network. It also lets you define a rate limit that sets the maximum number of sessions per source address to be handled by the firewall. Packets arriving at a rate faster than allowed will simply be dropped.

In a massive DDoS attack, the attackers may simply aim for saturating the link by transmitting vast numbers of UDP packets. The integrated environmental monitoring feature of Barracuda CloudGen Firewalls diagnoses such conditions by link and target address monitoring. If the response of a remote target address to regular ICMP probing fails, the system can be configured to activate different routes and uplinks (for example a backup line, ISDN, or xDSL). This lets you shut down DoS and DDoS attacks while leaving legitimate traffic unimpeded and ensuring crucial site-to-site and site-to-internet connectivity remains operational.

Web Filtering

All licensed Barracuda CloudGen Firewalls include highly granular, real-time visibility into online activity broken down by individual users and applications. This makes it easy for you to create and enforce effective internet content and access policies. It protects user productivity, blocks malware downloads and other web-based threats, and supports compliance by blocking access to unwanted websites and servers.

Malware Protection

Malware protection built into the Barracuda CloudGen Firewalls shields the internal network from malicious content by scanning web content (HTTP and HTTPs), email (SMTP,SMTPS, POP3S), and file transfers (FTP, SFTP) via two fully integrated antivirus engines. Malware protection is based on regular signature updates as well as advanced heuristics to detect malware or other potentially unwanted programs even before signatures are available. Malware protection covers viruses, worms, Trojans, malicious Java applets, and programs using known exploits in common document formats, macro viruses, and many more, even when they use stealth or morphing techniques for obfuscation.

Botnet and Spyware Protection

Botnet and spyware protection features guard against botnet infections by blocking access to malicious sites and servers, and detects potentially infected clients using a DNS sinkhole, which blocks clients from accessing malicious domains by monitoring outbound DNS requests passing through the firewall. DNS requests to malicious domains are redirected to an internal sinkhole, which preventing data exfiltration while identifying the victim. Once an infected client is detected, it is automatically isolated for remediation. An alert can also be created or reported by the Barracuda Report Creator.

Advanced Threat Protection

On top of all traditional signature based security solutions, the Barracuda Advanced Threat Protection (ATP) security layer uses cloud-based sandboxing with full system emulation to prevent any malicious file entering the network. During the sandboxing process, the potentially malicious file is executed on the fly in a controlled environment, and the system continuously monitors file activity. The process of uploading and sandboxing happens in the background and is fully transparent to users and administrators.

Cost-Effective Central Management

Barracuda CloudGen Firewalls are designed to be centrally managed across thousands of locations and multiple deployments including hardware, virtual, and in the cloud. With Barracuda Firewall Control Center, managing thousands of devices requires no more time or effort than managing a single device. Below are some highlights of the central management architecture.

Zero-Touch Deployment

Barracuda Firewall Control Center lets you easily manage configuration settings, services, licensing, hardware settings, and software updates via a single pane of glass. This includes the preparation and licensing of new units, even before the actual hardware is delivered. A bui9lt-in API lets you automate the creation of new configurations, or you can do it on the fly via the included wizards.

Creating a complete and valid configuration will take only a few minutes, and then you simply mark it for automatic deployment via Zero Touch. As soon as the CloudGen Firewall unit arrives at its location and is plugged in, the unit will contact the Barracuda Zero Touch Deployment service. That service then automatically applies the previously created configuration to the remote device, establishing a permanent direct management tunnel. This procedure allows for extremely fast unit roll-out, even with untrained field personnel. All the on-site personnel need to do is physically set up the unit by connecting power and network cables. Everything else happens transparently and automatically in the background.

Object-Based Management

The Barracuda Firewall Control Center allows creation of re-usable objects for any configuration entry imaginable: IP address, networks, ranges, DNS names, content security policies, network security policies, etc. These objects can be created once and reused in subsequent configurations nodes. For example, if there is an object Internal_Network_Branchname as a network object, it can be referenced in the network settings, firewall rules, and VPN settings. If the object needs to be changed, it only needs to be changed once, preferably via the Firewall Control Center. Then, the changes will be automatically applied at every location where the object is referenced. This provides a faster, easier, and more convenient method of changing configuration services across multiple units.

Centralized Repositories

When configuring multiple CloudGen Firewalls across the WAN, there will always be components that some devices have in common, such as domain names, DNS servers, NTP servers, application security configurations, URL filter configurations, and others. The Barracuda Firewall Control Center collects all of these in a repository (global configuration node) linked to multiple Barracuda CloudGen Firewalls. Using repositories on the Firewall Control Center, an administrator can update thousands of firewalls with just a single change in the repository within a matter of seconds.

Repositories still provide the flexibility to override specific settings on specific firewalls. For example, if one location uses a different DNS server than the others, you can create an explicit overwrite for just this setting on just this firewall.

Centralized Software Updates

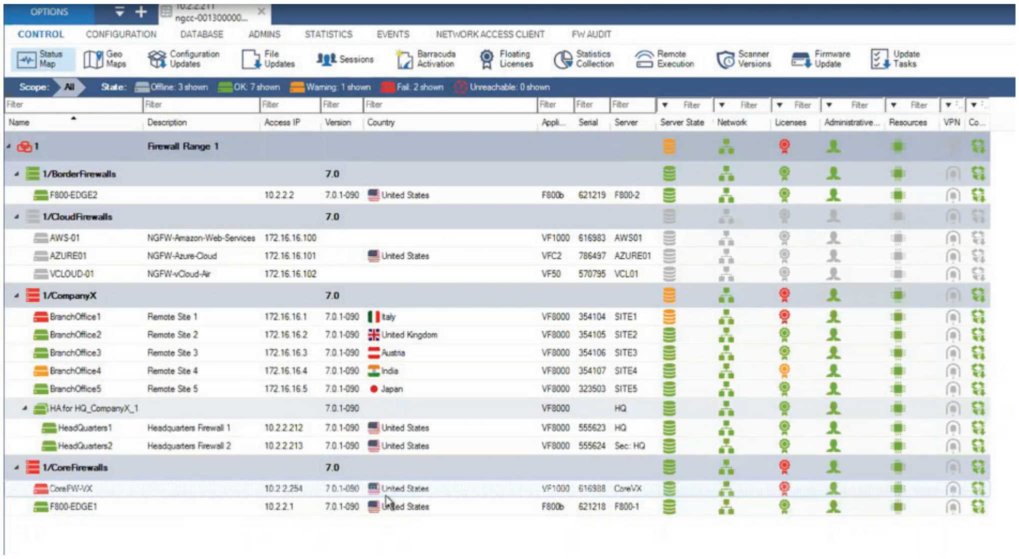
The Barracuda Firewall Control Center provides centralized software updates for all centrally managed CloudGen Firewall units. Updates can be scheduled for a specific time and for specific subsets of remote CloudGen Firewall units. In case a software update is not successful, it is automatically rolled back and reported.

Multi-Administrator Login

The Barracuda Firewall Control Center allows simultaneous login of multiple administrators in "writing mode." This is useful in multi-admin environments where there is a greater likelihood of administrators managing systems in teams. If a change needs to be made, only the dedicated configuration node needs to be locked for changing by the admin actually performing the change. All other settings outside of this locked configuration node are still viewable and modifiable by other admins logged into the system.

Status Map

The default screen for every Barracuda Firewall Control Center displays a clickable status overview of all centrally managed Barracuda CloudGen Firewall units. The status is indicated by the icon color (red, yellow, or green) and is provided for individual units, clusters, and whole tenant installations (or "ranges"). The "worst" status is always prioritized, giving you a centralized view of the overall status, and the ability to dig deeper with only a few mouse clicks.



Name	Description	Access IP	Version	Country	Appli...	Serial	Server
1	Firewall Range 1						
1/BorderFirewalls			7.0				
F800-EDGE2		10.2.2.2	7.0.1-090	United States	F800b	621219	F800-2
1/CloudFirewalls			7.0				
AWS-01	NGFW-Amazon-Web-Services	172.16.16.100			VF1000	616983	AWS01
AZURE01	NGFW-Azure-Cloud	172.16.16.101		United States	VFC2	786497	AZURE01
VCLOUD-01	NGFW-vCloud-Air	172.16.16.102			VF50	570795	VCL01
1/CompanyX			7.0				
BranchOffice1	Remote Site 1	172.16.16.1	7.0.1-090	Italy	VF8000	354104	SITE1
BranchOffice2	Remote Site 2	172.16.16.2	7.0.1-090	United Kingdom	VF8000	354105	SITE2
BranchOffice3	Remote Site 3	172.16.16.3	7.0.1-090	Austria	VF8000	354106	SITE3
BranchOffice4	Remote Site 4	172.16.16.4	7.0.1-090	India	VF8000	354107	SITE4
BranchOffice5	Remote Site 5	172.16.16.5	7.0.1-090	Japan	VF8000	323503	SITE5
HA for HQ_CompanyX_1			7.0.1-090		VF8000		HQ
HeadQuarters1	Headquarters Firewall 1	10.2.2.212	7.0.1-090	United States	VF8000	555623	HQ
HeadQuarters2	Headquarters Firewall 2	10.2.2.213	7.0.1-090	United States	VF8000	555624	Sec: HQ
1/CoreFirewalls			7.0				
CoreFW-VX		10.2.2.254	7.0.1-090	United States	VF1000	616988	CoreVX
F800-EDGE1		10.2.2.1	7.0.1-090	United States	F800b	621218	F800-1

Figure 3: Central Management, clickable status map with drill-down functionality

Multi-Revision Management

The security landscape is constantly evolving. That's why Barracuda Networks constantly develops and releases new features and improved security functionalities for all its CloudGen Firewalls through its Energize Updates subscription. But when you have dozens or even thousands of devices managed in a company's WAN network, some devices, networks, or even branches will inevitably run older firmware versions. The Barracuda Firewall Control Center is backward-compatible to older firmware versions deployed for at least three years, effectively easing the process of applying updates and upgrades across the organization.

Flexible Pool Licensing

Pool licensing ties the license for a particular Barracuda CloudGen Firewall unit to the managing Firewall Control Center, not to the serial number and hardware combination.

Individual units may be purchased at a lower price-point for use with pool licensing. In the unlikely event of hardware failure, a new unit can readily be deployed without the need to wait for relicensing. This allows organizations with large deployments and managed security services providers to optimize license usage and provide expedited replacement with readily available hardware units.

Automated Reporting

Whether due to regulatory requirements or company policy, most organizations require regular and easy-to-read reports on network status, user behavior, and bandwidth usage or resource allocation.

The Barracuda Firewall Report Creator allows administrators to create sophisticated, fully customizable reports, either for a single location or across multiple locations. This includes reports on top application usage, top talkers, top threat senders, top threat receivers, top policy violators, top bandwidth wasters, availability and uptime of VPN connections, usage time of client-to-site VPN logins, and many more predefined reports. Creation and delivery can be fully automated.

About Single Point of Contact

Single Point of Contact is a managed security service provider dedicated to helping businesses implement the right IT security solution. While we understand there are plenty of misconceptions about cloud security, we will also work with you to ensure you completely understand the advantages of operating your business in the cloud. To learn more about how we can help protect your business from cyber-attacks, **contact us** today.

single point of contact