Comprehensive Security for the Network Perimeter and Beyond

With Barracuda's Cloud Generation Firewalls and Advanced Threat Protection

White Paper

From Next Generation Firewalls to Cloud Generation Firewalls

Organizations just like yours are adopting SaaS offerings such as Office 365 and Salesforce at a rapid pace, as well as migrating workloads to public cloud platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform. As a result, they are developing new network topologies, which in turn are creating new operational tasks for network firewalls. They must now ensure uninterrupted network availability and robust access to business-critical, cloud-hosted applications. In addition, they must enable simplified management of dispersed, hybrid network infrastructures. At the same time, the threat environment is evolving quickly, requiring innovative security capabilities to respond to new and sophisticated advanced persistent threats and ransomware variants, such as WannaCry and Petya/Not Petya.

Barracuda Cloud Generation Firewalls are designed to optimize the performance and management of distributed networks and to effortlessly scale across any number of locations and applications. At the same time, they provide complete next-generation security coverage and granular application controls to protect your network perimeter from internet-based threats.

Evolving Threat Landscape

Modern attacks are rapidly growing in volume and sophistication. New malware strains are designed to evade traditional detection techniques, and they are often propagated through targeted zero-hour-attacks.

According to Osterman Research, we can expect over 200 new strains of ransomware per quarter through 2023. For attackers, this is a huge business opportunity, and they are just getting started. Ransomware alone is projected to create more than $1 billion in revenue for these criminals in 2017. It is critical to develop and implement new security capabilities to detect and block these attacks.

In addition, we all need to maintain and update security measures that address traditional network threats, vulnerabilities, and exploits, including SQL injections, cross-site scripting, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, trojans, viruses, worms, spyware, and many more. As these threats continue to evolve, we cannot afford to assume that traditional security measures will continue to be effective without evolving as well.

Comprehensive Security Features at Every Location

Barracuda firewalls are built on proven technologies to ensure real-time network protection against a broad range of threats. The Barracuda CloudGen Firewall is a stateful firewall that provides network segregation and malformed packet detection, along with effective protection against DoS and DDoS attacks.

Barracuda combines deep packet inspection (DPI) and behavioral traffic analysis to reliably detect and classify thousands of applications and sub-applications, regardless of advanced obfuscation, port hopping techniques, or encryption. This lets you block unwanted applications for defined user groups, enable or disable specific application sub-functions such as Facebook Chat or YouTube Postings, and to intercept SSL-encrypted application traffic delivered via HTTPS connections.

Barracuda CloudGen Firewall makes it easy to limit access to certain network resources to certain users or user groups. It supports authentication of users via a wide range of authentication schemes, and lets you define and enforce user-aware firewall rules.

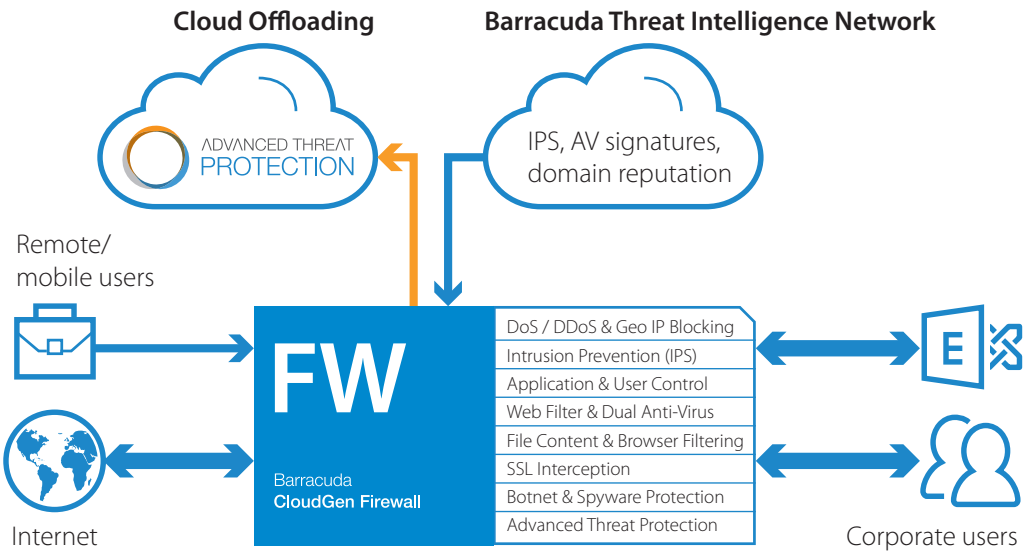
CloudGen Firewall includes an intrusion detection and prevention system (IDS/IPS) that strongly enhances network security by providing complete and comprehensive real-time network protection against a broad range of network threats, vulnerabilities, exploits, and exposures in operating systems, applications, and databases. IDS/IPS prevents network attacks such as SQL injections and arbitrary code executions, access control attempts and privilege escalations, cross-site scripting and buffer overflows, directory traversal, probing and scanning attempts, backdoor attacks, Trojans, rootkits, viruses, worms, and spyware.

Built-in web filtering enables highly granular, real-time visibility into online activity broken down by individual users and applications. This lets you create and enforce effective Internet content and access policies. It improves user productivity, blocks malware downloads and other web-based threats, and simplifies regulatory compliance by blocking access to unwanted websites and servers.

With the optional Malware Protection module enabled, the Barracuda CloudGen Firewall uses two fully integrated antivirus engines to shield your network from malicious content by scanning web content (HTTP and HTTPS), email (SMTP, POP3), and file transfers (FTP and Secure FTP). With advanced heuristics and regular updates, Malware Protection lets you detect new malware and other potentially unwanted programs even before signatures are available.

Barracuda's CloudGen Firewall accelerates content inspection and minimizes latency thanks to its Single Pass Mode architecture. Traffic is inspected only once inside the firewall, with no need for handoff to a proxy. This means that you never have to make the difficult choice between optimal performance and robust security.

Finally, with Barracuda's proprietary high-performance Transport-Independent Network Architecture (TINA) VPN protocol, you can encrypt all traffic from end to end.

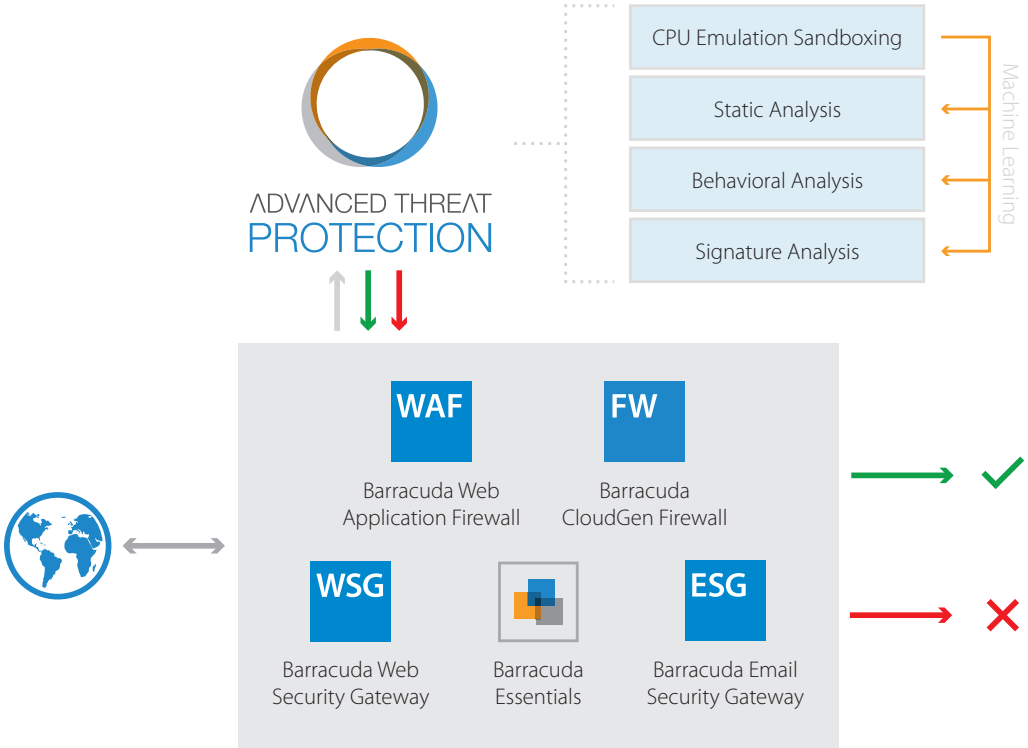


Defense-in-Depth with Barracuda Advanced Threat Protection

The polymorphic nature of modern cyber threats renders traditional signature-based defense mechanisms inadequate. Comprehensive, reliable protection against attacks like ransomware and advanced persistent threats requires a layered approach.

Barracuda Advanced Threat Protection is a cloud-based service that provides in-depth defense against ransomware, malware, and other advanced cyberattacks. It consists of multiple layers of detection, including signature matching, static analysis, behavioral analysis, and comprehensive CPU-emulation sandboxing to provide accurate detection of a variety of polymorphic attacks, including zero-day threats.

The core of Barracuda Advanced Threat Protection is a comprehensive CPU-emulation sandbox that will 'detonate' any attachment that is not conclusively analyzed by the preceding layers—advanced threat signatures, behavioral and heuristic analysis, and static code analysis. Once a new threat is identified and a signature is created, the information is pushed to the pre-filtering layers. The next time the same threat attempts to enter your network, it will be blocked without the need for repeating the resource-intensive sandbox analysis. This ensures that sandboxing is used as efficiently as possible, to deliver advanced security without significantly impacting operations. The service is connected to a global threat intelligence network that gathers threat data from diverse sources around the world, providing real-time protection against newly discovered threats, and further minimizing the amount of traffic that is subjected to sandboxing. Barracuda's threat protection framework cross-pollinates diverse threat intelligence gathered across all vectors.



Security Features at a Glance

Barracuda provides all the security features required to protect dispersed networks:

- 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
- Malware Protection
- Typosquatting and Link Protection
- Advanced Threat Protection

The Cloud Generation Firewall for Today and the Future

Every location, even the smallest remote site, requires full protection without compromise. All security features are available in every model of Barracuda CloudGen Firewall, ranging from 1 Gbps to 48 Gbps throughput, to fit any network environment—from small, remote sites to large global headquarters.

Barracuda CloudGen Firewall is available in a broad range of deployment options, including physical and virtual appliances, and as public-cloud deployments available on Amazon Web Services, Microsoft Azure, and Google Cloud Platform. This means that it integrates perfectly with your current architecture, while making you fully cloud-ready—able to seamlessly adopt future SaaS and IaaS offerings without the need to migrate to a new firewall solution. Your investment in Barracuda CloudGen Firewalls is secure for the long term.

Securing All Threat Vectors

The network perimeter is not the only attack surface that requires real-time protection. A comprehensive security strategy should address all threats across all threat vectors. Email, web browsing, and web applications need the same level of protection.

Barracuda provides a comprehensive suite of solutions to secure all these vectors, each of them offering integrated Advanced Threat Protection:

- Email Security – Barracuda Email Security Gateway and Barracuda Essentials
- Web Security – Barracuda Web Security Gateway and Barracuda Web Security Service
- Application Security – Barracuda Web Application Firewall

Barracuda CloudGen Firewall and Barracuda Web Application Firewall, build a comprehensive Ransomware Protection Suite when used together. The Web Application Firewall expands your security posture with inbound and outbound filtering, OWASP Top-10 Protection, Data Loss Prevention (DLP), and more.

Conclusion

Modern network topologies are characterized by a large number of globally dispersed locations, each of which require robust, reliable, zero-lag connectivity to SaaS applications and public-cloud platforms. Barracuda's Cloud Generation Firewalls are designed as distributed network optimization solutions that can scale across any number of locations and applications, without compromising on the core function of a next-generation firewall—protecting the network perimeter from internet-based threats.

Barracuda CloudGen Firewalls offer a comprehensive set of next-generation firewall technologies to ensure real-time network protection against a broad range of network threats, vulnerabilities, and exploits, including SQL injections, cross-site scripting, denial of service attacks, trojans, viruses, worms, spyware, and many more.

The nature of modern cyber threats, such as ransomware and advanced persistent threats, targeted attacks, and zero-day threats, require progressively sophisticated defense techniques that balance accurate threat detection with fast response times. Barracuda Advanced Threat Protection provides Defense-in-Depth, leveraging multiple layers of threat detection including CPU Emulation-based sandboxing, combined with machine learning techniques.

About Barracuda Networks

Barracuda 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.

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