Solution Brief

Integrating Barracuda CloudGen Firewalls with the Web Security Gateway

With more sophisticated cyber threats on the rise, businesses need to have more granular visibility and controls over their web traffic. Barracuda offers a family of CloudGen Firewalls that help businesses secure against advanced malware and zero-hour threats, while reducing cost, complexity, and management overhead. To further enhance your web-based security, the Barracuda Web Security Gateway provides additional features like social-network regulation and monitoring, remote filtering, and full visibility into SSL-encrypted traffic. Used together, Barracuda CloudGen Firewalls and the Web Security Gateway deliver complete network protection, internet content control, with alerting and granular reporting capabilities.

Introduction

Firewalls and web security gateways have long been deployed together to complement each other's capabilities. Because firewalls lacked visibility into application and web traffic, causing network blind spots and security vulnerabilities, web security gateways provided the necessary features to mitigate those risks. With the introduction of next-generation firewalls, however, these features are now included in the solution, blurring the lines between the capabilities of firewalls and web security gateways.

Further complicating things, UTM devices also now claim to offer complete solutions in one device. However, for all their promises UTMs often suffer from performance issues when all features are enabled, or suffer from vulnerabilities when some are disabled to compensate. The alternative solutions to these problems tend to require the purchase of more capable—and therefore more expensive—models.

Barracuda Provides Complete Website Security

With all of these solutions now competing for market share, buyers are often understandably confused about which one is right for them. While each has a case to make, Barracuda believes that you shouldn't have to sacrifice features, usability, or affordability to get a complete solution. That's why we recommend deploying the Barracuda CloudGen Firewalls alongside the Barracuda Web Security Gateways.

While Barracuda CloudGen Firewall and Web Security Gateway have some similar features, there are important differences to note:

- The Barracuda Web Security Gateway has more granular logging and reports over a longer period of time. Next-generation firewalls and UTMs are somewhat limited in their reporting capabilities, both in terms of event detail and the length of time that events can be stored. While external reporting applications are offered to increase the amount of historical data, these do not typically increase the granularity of the data stored. The Barracuda Web Security Gateway, on the other hand, provides up to six months of detailed historical reporting with granular insight into users' web activity.
- Another difference is the Web Security Gateway's enhanced application control. Not only can administrators simply block or allow applications, but Web Application Monitoring feature also provides insight into—and controls for—specific functions within applications. Social media, for example, is now an omnipresent concern for organizations. Whether you're a business looking to leverage yet monitor social media marketing efforts, or a school looking to screen for cyberbullying,

terrorism, or profanity, the Barracuda Web Security Gateway has application controls that enable the enforcement of custom policies. Web Application Monitoring also enables visibility into the activity of users on major search engines.

- UTMs and firewalls typically require that traffic pass back through the device via a VPN in order for policies to be applied. Not only is this inefficient, but it also becomes costly as organizations must increasingly account for the bandwidth consumption of cloud-based infrastructures. However, the Barracuda Web Security Gateway remotely filters content without having to backhaul or proxy traffic.

How to Configure Barracuda CloudGen Firewalls and Web Security Gateway

When deploying Barracuda Web Security Gateway with our CloudGen Firewall, there are some configuration concerns to consider. The different deployment modes, which determine the relationship between the two devices, include inline (or transparent proxy), forward proxy, WCCP, and transparent redirect. Inline is the most common of these deployment modes, mainly because it allows the Barracuda Web Security Gateway to view and control application traffic. The Inline deployment mode also enables malware and AV scanning of all internet traffic, and the ability to detect and block outbound spyware protocol requests. It also allows administrators to filter both web based and non-web based applications.

While the inline deployment mode is a great option for many settings, in some cases, it can create issues due to throughput disparities between the Barracuda Web Security Gateway and CloudGen Firewalls. Because the Web Security Gateway inspects traffic at a more detailed level, the CloudGen Firewall generally has higher throughput specs. Therefore, it is important to ensure that they are both capable of handling the bandwidth.

The forward proxy deployment mode can also be a good option, as it solves the bandwidth disparity issues by only directing web traffic to the Barracuda Web Security Gateway. In this case, additional security can also be achieved by setting the Barracuda CloudGen Firewall to prevent internet access to machines, except through the Web Security Gateway. By forcing the web traffic through a single egress point, you get granular visibility as well as control of the traffic. The Barracuda Web Security Gateway will terminate connections between the requesting client and the website, inspecting every packet that passes through.

The WCCP deployment mode does not require client settings, and it overcomes potential bandwidth disparity issues by only directing a portion of the network traffic to the WSG. WCCP is a content-routing protocol that provides a mechanism to redirect traffic in real time; any network hops between devices only touch the encapsulation layers without gaining visibility into the encapsulated data itself. While this provides built-in load balancing, fault tolerance, and scalability, WCCP is a propriety protocol created by Cisco. Some devices may require additional licensing fees to enable this feature, and can also encounter additional device-specific limitations.

Similar to WCCP, Barracuda CloudGen Firewalls offer a Transparent Redirect feature that also does not require endpoint settings, and directs only traffic headed for ports 80 (HTTP) and 443 (HTTPS). In this deployment mode, the Barracuda Web Security Gateway retains all of the value-added features like reporting web app and search term monitoring and remote access without having to backhaul traffic. In this case, Barracuda CloudGen Firewall provides the application control, intrusion prevention, Advanced Threat Protection, and VPN service. From a high-level view, Barracuda CloudGen Firewall is designed to keep intruders out, while prioritizing network traffic, and preventing the use of unwanted applications. The Barracuda Web Security Gateway is designed to understand, monitor, and control the activity that takes place on the web, then report on those events. By enabling the strengths of both the Barracuda Web Security Gateway and CloudGen Firewall, respectively, this is the strongest method of deployment.

Instead of compromising for the sake of using a single device, we recommend deploying a complete solution by using Barracuda Next Generation Firewalls in conjunction with the Web Security Gateway. Enhance your security and optimize your traffic with Barracuda network and content security solutions.