CSO
FROM IDG
November 24, 2017 www.csoonline.com

Review

# Calling Barracuda's WAF a firewall is seriously selling it short

The Barracuda Web Application Firewall (WAF) is more than a firewall, it's like the core of an independent bastion of cybersecurity, able to inspect both inbound and outgoing traffic.

**By John Breeden II**

Most cybersecurity products within the network security sector concentrate on one particular aspect of security and then build up tools and procedures around that area. By contrast, the Web Application Firewall (WAF) from Barracuda Networks does an excellent job of covering the entire network, or at least the parts that administrators feel need the most protection.

At its core, the Barracuda WAF is a firewall that is capable of monitoring Layer 7 network traffic, so it can look all the way down to the application level, as well as monitor the bulk of the traffic moving through Layer 4. It is deployed as hardware, a virtual appliance or within the Amazon Web Services (AWS) or Microsoft Azure public cloud. If deployed virtually or through the cloud, it will update is drivers and expand its capacity automatically based on need. If the hardware version is used, Barracuda will upgrade the box to the latest and greatest equipment every four years, free of charge.

Calling the Barracuda WAF a firewall is seriously selling it short. It's more like the core of an independent bastion of cybersecurity, able to inspect both inbound and outgoing traffic. The WAF functions like a reverse proxy and is placed at the front of the data pathway. It intercepts all traffic, inspecting it for attacks and blocking them before they make it to any servers. In fact, it only allows traffic through that conforms to security policies, and that includes both incoming and outbound flows.

The inbound stream is generally inspected for malware, advanced persistent threats being controlled by humans, application cloaking, geofencing and other IP controls. It also can act as a defense against application-based DDoS attacks, something we tested during our review.

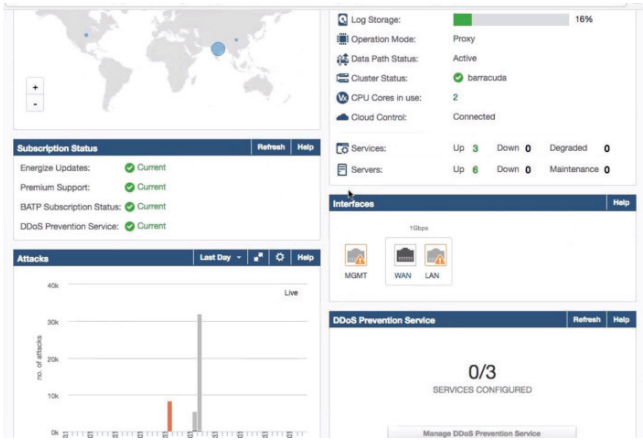
All outbound data is inspected to prevent sensitive information from leaving the network. It can recognize and stop credit cards, social security numbers and any other customized intellectual property from getting past the gateway to the outside world.

## The Interface

With so many defensive capabilities, it would be very easy for management of the WAF to get out of control, had Barracuda not perfected the simplicity of the interface. Users activate various capabilities within the firewall by creating services. Services can be created in quite a few areas including request limits, cookie security, URL protection, perimeter management, cloaking, data theft controls, URL normalization and many others.

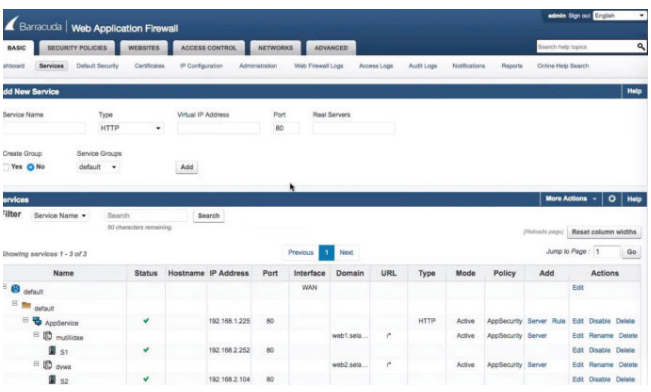
Spinning up a new service is extremely easy. Users only need to migrate to that part of the interface and click on the correct tab that matches what they need to do. The WAF automatically applies a proven, default security policy around each service, so all services are instantly configured in a way that protects the underlying application or data.

Once the default policy is in place, users can modify it based on their unique needs. For example, the default policy for an app with an entry form is to limit the size of that user input to a certain number of characters or a certain size file. But if you know your application will need to go beyond that, it's easy enough to change the parameters. The process is the same for services that deal with either



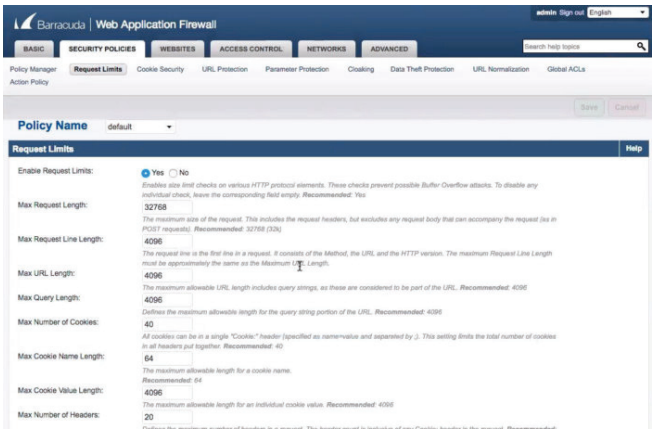

John Breeden II/IDG

The main interface for the Barracuda Web Application Firewall is completely customizable, enabling users to concentrate on whatever aspects of network security they feel is most important.




John Breeden II/IDG

Users protect assets and applications by creating services on the WAF. Every service is bundled with a default security policy that can later be edited, so nothing is ever deployed without protection.




John Breeden II/IDG

Editing default security policies is easy. Users can also create their own policies and swap them out for defaults when needed.

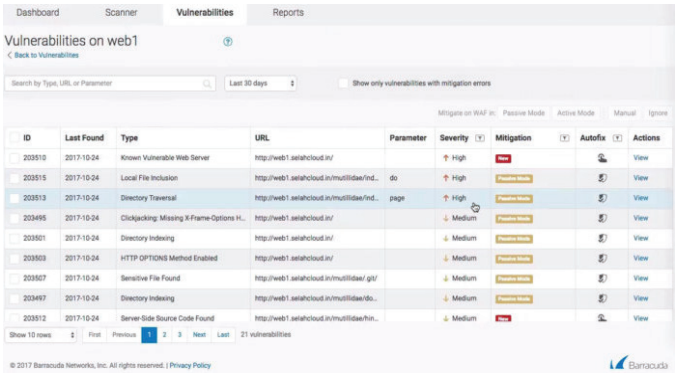
incoming or outbound traffic.

It's also possible to create wholesale policies that can replace the defaults, though not when initially deploying policies. Barracuda explained that the default policies are based on over 20 years of research about threats to network security. If users want to tweak them or replace them, that is fine, but the default security policy is put in place first. It may mean an extra step for an advanced user, but that is balanced by the fact that no mistakes will ever be made in terms of deploying a service through the WAF without adequate security that covers all the most necessary bases. And, probably 80 percent of users will never need to go beyond the defaults, or perhaps will get by with minimal, occasional tweaking.

## Vulnerability management

The WAF is also an excellent vulnerability management device. Any new application that is put into a protected network can be scanned by the WAF for vulnerabilities. This requires connecting the WAF to the additional Barracuda Vulnerability Scanner service, which is free to all firewall owners. Any vulnerabilities found by the WAF have rules created to plug those holes. It's interesting to note that the application itself isn't actually fixed, so no code is changed. The WAF, which is intercepting all traffic to and from the app, simply programs rules into its configuration so that nobody can take advantage of those vulnerabilities. It handles the fix without having to touch the program.

Within the console, rules that are created to fix an app's vulnerabilities are designated with the three-letter prefix bvm with an underscore, which stands for Barracuda Vulnerability Management. Later on, if an application is directly fixed, those rules can be removed, or users can simply trigger a new scan to confirm that the vulnerability has been squashed. But here again, most users can probably just let the WAF plug those holes and operate safely.

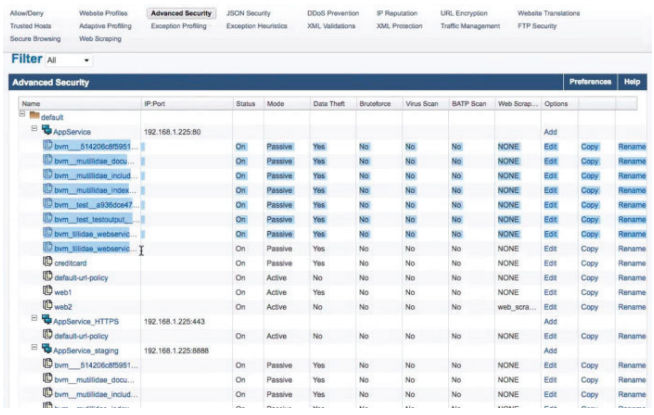



John Breeden II/IDG

Any vulnerabilities located by the WAF, or attacks made against protected applications, are logged along with any actions taken by the appliance or its administrators.

## Load balancing

Load balancing, which is only loosely affiliated with security, is also possible with the WAF. We configured multiple servers to share an application's traffic. This can be done using round robin logic, weighted round robin logic or even manually based on various traffic counts or thresholds. Deploying non-security services through the WAF is just as easy as working with cybersecurity rules.




John Breeden II/IDG

Barracuda offers a free scanning service for examining new applications for potential vulnerabilities. Located vulnerabilities trigger rules to be created on the WAF to plug holes, identified by the letters bvm, which stands for Barracuda Vulnerability Management, at the front of the rule's name.

## DDoS protection

Finally, we tested the WAF's ability to handle DDoS attacks, an unexpected feature that does not make it into a lot of firewalls. Here DDoS protection is divided up into two principal areas, application-based attacks and web-based attacks. In the former, attackers attempt to flood an application with so much data that it either crashes or overloads the server. But because the WAF is intercepting all traffic, this is easy to handle as multiple requests will break the established rules. For the more common type of attack where web traffic is sent to overload a server with junk data, the WAF will need to be connected to the Barracuda traffic scrubbing service. This requires an extra license, but enables the WAF to forward suspected DDoS traffic through the service and then remediate the situation by blocking the overloading requests.

We tested DDoS application-level attacks, sending thousands of junk data into an open field on a protected online application. With over 5,000 requests per second, the application never hiccupped. Checking the log files, it was clear that the WAF was blocking the DDoS attempt. And, we had full access to the application as a legitimate user even at the height of our attack.

## The last word

The Barracuda Web Application Firewall packs a lot of network security into a single package. Yet, for all its power, the interface is surprisingly simple, programmed with failproof security policies by default, and does not require an inordinate amount of training or expertise to use its most advanced features. It's a proverbial multi-kill with one stone type of defensive security appliance that organizations of any size could use.

*John Breeden II is an award-winning journalist and reviewer with over 20 years of experience covering technology. He is the CEO of the Tech Writers Bureau, a group that creates technological thought leadership content for organizations of all sizes.*