Add PCI-DSS requirements for application security, and it’s easy to see why Web application firewalls, once considered niche technology, are gaining traction in corporate data centers. They prevent attacks that network firewalls, IDS/IPS and antivirus filters cannot by limiting suspect access through combinations of behavioral analysis and policy controls.

In a head-to-head review, Information Security examined six application firewall appliances, all of which delivered centralized management, enterprise reporting and comprehensive protection for applications: Barracuda Networks’ Web Application Gateway (formerly NetContinuum); Bee Ware’s iSentry; Breach Security’s WebDefend; Citrix’s Application Firewall; F5 Networks’ Big-IP 8800 Application Security Manager; and Imperva’s SecureSphere Web Application Firewall.

Each product was graded on ease of installation and configuration; administration; depth of security policy control; monitoring, alerting, auditing and reporting; and overall security effectiveness.

If the products we tested were 1U or 2U rack-mounted devices built on hardened appliances. Our first step was to gauge the ease with which each product could be installed and configured. Although each appliance supported a variety of deployment configurations (bridge, router, inline, out-of-line), we set up each as a reverse proxy, except Breach Security’s WebDefend, which is designed to operate in a non-linear environment.

Imperva and Breach were easiest to set up and configure. Thanks to their intuitive design and wizards, each took approximately an hour to get running.

Using the Site Manager through Breach’s console, we could easily verify that the domains, IP addresses and ports were correct. It even identifies the type of server on which the application is hosted (e.g., IIS). Through the logical tree structure, it’s easy to locate and add sites.

Consider how much information gets plugged into databases through applications and then regurgitated in queries, reports and content. We live in a world of HTTP and HTTPS, where everything has been ported to Web-based interfaces and consoles. Traditional network firewalls operating lower on the stack have no way of identifying malicious requests traversing TCP ports 80 and 443 to online shopping sites, Web mail or business portals such as online banking and account services.
**About this REVIEW**

*Information Security* deployed six application firewall appliances from Barracuda Networks, Bee Ware, Breach Security, Citrix, F5 Networks and Imperva.

Each product was installed in our test lab between a network firewall and in front of or alongside the application servers (see “Inside The Lab,” below), which included an Apache Web server and Microsoft Internet Information Server, each hosting a variety of applications including Web mail, an online forum and a Web site with shopping cart capabilities.

Client machines subjected to attack included systems running Microsoft XP SP2 with Internet Explorer and Linux (Debian 3.1) with Mozilla Firefox. We focused on common attacks against applications including buffer overflows, cookie tampering, SQL injection, session hijacking, cross-site scripting (XSS), cross-site request forgery (CSRF), forms tampering, remote code execution, malicious code (Internet worms), denial of service, brute force login and forceful browsing.

Additionally, we configured application-side security features, such as Web site cloaking, and attempted to gain network and application configuration via nefarious reconnaissance practices such as identifying operating systems and Web server details through HTTP header data and scanning utilities like Nmap.

Breach’s WebDefend was deployed in an out-of-line mode next to our Web servers using a span port.

—SANDRA KAY MILLER

**INSIDE THE LAB** All application firewall appliances were deployed as reverse proxies (except for Breach Security’s, which was attached to a span port) on a network between a traditional stateful inspection firewall and a variety of applications servers, including Microsoft IIS and Apache Web servers, Microsoft SQL, e-commerce applications with credit card transaction capability and an online forum. Browsers included Internet Explorer, Firefox, Netscape and Opera.

**Imperva required more manual intervention for the configuration of our servers, Web sites, services and applications. It presented a logical tree structure similar to that of Breach, but lacked the useful at-a-glance verification and instead spread the information among four different tabs. Nonetheless, these were minor points and we found it overall to be on a par with Breach in this category.**

**Bee Ware’s initial installation was similar to our other test subjects, and the configuration wizard stepped us through assigning the basics such as host name, date and time, network interfaces and assigning the destination IP address for our target back-end server. The documentation showed some rough translation issues from the original French, but the configuration wizard led us through a fairly straightforward setup.**

**F5’s Application Security Manager (ASM) is a part of its Big-IP port-based multilayer switch built on F5’s proprietary TMOS platform, which is designed for traffic management, acceleration and load balancing. After a fairly painless installation onto our network, the configuration required us to spend the better portion of a day understanding how the ASM module integrated with the other modules, such as the Local Traffic Manager.**

**While all of this first appeared extremely complex, F5 features a clean and informative interface coupled with outstanding documentation and technical support. The complexity was offset by the rich load balancing and traffic management features necessary for delivering application security in big pipe environments.**

**Citrix required a lot of manual entry, but offered a clean Windows-based configuration utility. It wasn’t as time consuming as Barracuda’s Web Firewall’s setup or as complex as F5, which required extensive understanding about network traffic management prior to setting up the security features.**

**Barracuda is somewhat complex and took a long time to set up. Even though we used Barracuda’s Web application wizard, an extensive amount of manual security configuration was required to effectively protect our test applications against our attacks. Since Barracuda boasts of its ability to be set up in a production environment without causing disruption, we initially deployed the box in passive mode, producing logs that identified actions that would have been taken if it was in active response mode—for example, blocking traffic from an IP that was performing a brute force login, forceful browsing or bot activity. This allowed us to effectively tune the appliance prior to switching to active mode—a real plus for security managers without the time or resources to first deploy in a mirrored test environment.**
Imperva offers highly granular administrative rights delegation and greatest ease of assigning rights and permissions. An expandable tree allowed us to instantly view administrative groups under which individuals are listed. Rights and permissions can be set globally, per group or per individual through a comprehensive list of available resources and applications. We could quickly set view/edit privileges. Individuals can be assigned to multiple groups as well, giving them different levels of access.

F5's comprehensive set of administrative tools supports its traffic management and load balancing capabilities, and the application security module. It helps tame the overwhelming task of administration by compartmentalizing objects such as virtual servers, URLs and databases for easier, more flexible delegation.

Similarly, Barracuda groups applications and resources into role-based administration silos to facilitate delegation. Navigation throughout the extensive feature set was relatively easy, despite complexity second only to F5. Roles define the user’s permissions for command groups (meaning what type of actions) and are accessible for a particular site, so administrative duties can be delegated in a large or distributed environment.

Bee Ware keeps things simple by breaking down administrative tasks into two basic groups—administrators and webmasters. Administrators have access to global configurations and can create, disable or delete services and policies. Webmasters only have configuration rights to the services and policies for which they have been assigned permission. This provides the autonomy needed for different groups to make changes to their HTTP-based content as well as the overall security and oversight to prevent damage to active content pages.

Citrix's administrative capabilities are basic, but well-managed through a simple and intuitive management GUI. We were able to quickly add users for administrative purposes, but our options were limited to either an application administrator or an application guest, whose account could view, but not modify, configuration settings. We felt this was essentially useless.

Breach breaks out administrative tasks into two groups as well—system administrators with access to everything, and site administrators who only have rights to sites assigned to them. Additionally, Breach includes two view-only accounts—a Super Viewer who can see everything and a Viewer with read-only access to sites to which they are assigned.

Assigning sites was effortless, as all active sites are displayed in one window and could be assigned with a mouse click.

**THE PERVERSIVENESS OF WEB-BASED APPLICATIONS PRESENTS MANAGEMENT CHALLENGES THAT MAKE DELEGATED ADMINISTRATION AN IMPORTANT FACTOR.**

Security policy control

The real power behind these products lies in their ability to let organizations control access to dynamic applications. Unlike traditional network firewalls that simply permit or deny packets based upon policy, application firewalls must deliver more sophisticated control at the application layer through a variety of contextual rule sets and behavioral analysis.

All of the products included some sort of learning function, either the automatic learning of URLs or learning behavior and traffic patterns. Another significant policy designation was the firewall's ability to operate in a transparent mode, which allowed us to fine-tune actions prior to initializing full security measures, such as blocking and redirecting.

Breach provided the most predefined policy set out of the box, covering known attacks against popular applications such as IIS, Apache and SQL. We are skeptical that its controls have the robustness to be effective against unknown attacks.

The console isn’t as complex or icon-driven as the other products, but is laid out in a way that let us drill down through our applications and review and set policies. Best of all, it provided one of the best visual interfaces along with information about security events.

We were particularly engaged by the use of BreachMarks—regular expressions or custom strings used to identify sensitive information, such as credit card numbers.

The first order of business with Citrix was switching from bypass mode to operating mode—basically turning on the firewall. From the same page, we were able to choose whether to include failover protection in our security policy, assign session timeout thresholds and toggle between two diverse degrees of overall security—Enterprise, which included full filtering and blocking, or Express, with basic Web server policies.

Once traffic began passing through the appliance, we had to determine whether to enable failover protection. Initialing this option was difficult, as it required an in-depth understanding as to whether or not pages containing Web forms utilized Javascript or Get calls.

Citrix’s Adaptive Learning mode examines traffic to determine what is normal and then builds recommendations that let users apply, edit and apply, skip or ignore. Unfortunately, when a recommendation is ignored, the firewall will no longer view that particular action as a threat when encountered. We would have preferred to see a threshold set for the skip option to allow change to meet new zero-day exploits and adaptive malware.

F5's policy management is quite flexible. Initially, the wizard walked us through each aspect rule definition. F5 also supports an assortment of adaptive learning tools to assist with policy generation. We found the Learning Manager and its counterpart, the Traffic Learning Screen, to be the most helpful in determining policy. Each time we created a potential violation, such as forceful browsing or multiple failed login attempts, the Learning Manager made suggestions as to how to adapt our security policy.

F5 offers the ability to create security policy templates to facilitate large-scale deployments.

Between Barracuda's policy wizard and the dynamic application profiling, we were able to create security policies specific to the traffic generated during our testing. However, it’s easy to see how in a high-traffic environment, the constant tweaking would be bothersome and ultimately create a security risk from multiple changes.

Barracuda's passive mode is very good at displaying what results would be if policies were actively enforced. While the other products displayed what was taking place on the network, they didn’t offer the extensive understanding of the ramifications of the security policy had it been active.

While Bee Ware's security policies provided adequate protection against our assortment of attacks, setting up polices proved to be difficult. The appli-
CONSIDER THIS

WEB APPLICATION FIREWALLS have additional features, such as those related to traffic management, including SSL acceleration, caches, compression, load balancing and high availability. The growing adoption of high bandwidth technologies requires that solutions are capable of delivering security without latency. Other factors that may influence your purchase decision are regulatory compliance features and out-of-the-box policies and signatures to get you started without a lot of customization.

<table>
<thead>
<tr>
<th>Appliance Specifications</th>
<th>Load Balancing</th>
<th>Traffic Shaping</th>
<th>High Availability</th>
<th>SSL Acceleration Offloading</th>
<th>Connection Pooling</th>
<th>Cache and Compression</th>
<th>Pre-loaded Policies and Signatures</th>
<th>Regulatory Compliance Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barracuda Networks Web Application Gateway</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bee Ware iSentry</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Breach Security WebDefend</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Application Firewall</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>F5 Networks Big-IP Application Security Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Imperva SecureSphere Web Application Firewall</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Imperva delivered an impressive set of predefined attack signatures. Custom signatures can be easily created through a simple menu system that includes a wide variety of metadata choices (Web, stream, SQL).

The easy-to-navigate interface allowed us to peruse policies through a variety of filters listed in a hierarchical tree on the left side of the policies page.

MONITORING, ALERTING, AUDITING & REPORTING

All the products we examined had features specific to aid compliance auditing and reporting. Security managers want detailed information about malicious activities on their network—the who, what, why, where, when and how details. Auditing and reporting features can make or break a product’s chances of ending up at the top of the short list.

Imperva sports a highly configurable real-time interface, in which we were able to monitor all our applications, alerts, events, connections and the overall health of our systems at a glance under the Monitoring tab.

A separate and equally functional tab offers more than 100 types of reports from which to choose—from a list or using Imperva’s robust filtering capabilities.

The Admin tab put everything neatly at our fingertips. With a mouse click we could access users, sessions and, most important, the Application Defense Center—a catch-all for updates and information on signatures, policies, protocols, reports, etc.

Breach also offers an assortment of useful reports, many which are obviously focused on PCI compliance reporting. Monitoring our shopping cart application, it took only minutes to compile detailed reports about how credit card information transmitted through specific Web pages.

The Event Viewer offers nine filtering options to drill down on an incredible amount of information, as well as the ability to create customized filters.

Citrix provided adequate monitoring, alerting and logging capabilities. Monitoring is accessed via a dashboard icon on the main interface, as are reports and logs. There are two basic types of logs: The firewall log provides information about security-related events, and the audit log records all activities you select when you configure the box.

Compared to Imperva, the Citrix dashboard is plain and uninformative. We were disappointed by the weak reporting features, which offered only four types of administrative reports—an Executive Summary, a Security Summary, a Configuration Summary and an Inspection Report, which listed the attacks.

In addition to Web Application logs, Barracuda provides syslogs, network firewall logs and Web firewall logs, each with its own page under the Logs tab on the dashboard. Overall, the logging displays were visually confining and dull. Reporting capabilities were as disap-

AT THE CORE |

Security Policy Control

THE GOOD NEWS We especially like BreachMarks tagging. F5 features a good policy toolset, particularly for adaptive learning, and Imperva has an array of out-of-the-box policies and attack signatures.

THE BAD NEWS Bee Ware’s policy creation is time consuming, poorly organized and difficult to navigate.
“Imperva is the closest thing to a silver bullet for application security, based on its combination of adaptive learning and other techniques.”

pointing as those offered by Citrix, limited to alerts, diagnostics and error reports. They lacked the rich level of detail and customization found in Imperva and Breach.

F5 delivers excellent monitoring, alerting, historical and forensic capabilities, but the reporting tools are only mediocre. Executive, Events, Security and Attack reports, despite the phenomenal amount of information gleaned through the multiple types of monitors that continuously track HTTP, HTTPS, TCP, FTP and other network protocols.

Bee Ware’s monitoring capabilities were limited to real-time application activity and security logs, which are viewed via the administrative interface or exported as syslog log files. Alerting was limited to SNMP traps and syslog messages. Security administrators require instant notification through a variety of methods, such as SMS and email, the moment a critical event occurs.

Bee Ware only offered two basic types of logs—security and access. Each provides a table of events and each event could be clicked on for additional information. We found the logs to be more helpful than the reports for which they provided the data. Reports were limited and poorly designed in their graphical display.

**OVERALL SECURITY EFFECTIVENESS**

The Web has opened a multitude of new avenues for hackers to exploit Internet protocols and the applications that utilize them. The core functionality of all the products delivered comprehensive security for HTTP, HTTPS and FTP applications and XML services. In our test rail, all the products delivered a core set of security features, most notably Web site cloaking, protection against common Web vulnerabilities and exploits and data protection.

Our battery of attacks included but was not limited to SQL injections, buffer overflows, cookie tampering, forms tampering, session hijacking, cross-site scripting, remote code execution, malicious code (Internet worms), denial of service, brute force logins and forced browsing. We launched a Java-based Web crawler in an effort to fingerprint the applications and hosted sites behind the product under testing. Additionally, we purposely set up insecure pages that provided access to restricted data (credit card numbers, fake, of course) and attempted to gain access. Each product performed satisfactorily, and all are worthy of enterprise installations.

Given the massive amount of information stored in databases that are touched by Web-facing applications, we found that Imperva’s application and database security provided the closest thing to a silver bullet security managers could institute. Using a combination of whitelists, blacklists and adaptive learning (“Dynamic Profiling Technology”), the device examined traffic and behavioral patterns of applications and databases to differentiate between valid traffic patterns and our attacks.

Barracuda uses a combination of Web ACLs, positive and negative security models and Dynamic Application Profiling to identify acceptable traffic. The included signatures for the negative model blocked all the common attacks (SQL, buffer overflow, tampering, etc.), while the positive model locked down all traffic unless defined through the powerful ACLs. We set a variety of ACLs that delivered superior security for our test sites.

Similarly, F5 employs both a positive security model, and a negative model for common attacks, with heuristic analysis of all traffic through the Adaptive Learning and Tuning engine. We credited the strong positive security model for initially blocking some of our legitimate traffic and returned to the transparent mode until we had established a traffic baseline through F5’s automated policy builder. Our second attempt at enabling blocking resulted in flawless operation, with all attacks stopped while allowing permitted traffic to proceed.

The granular traffic movement controls allowed us to limit access to applications through customized traffic flow policies.

We started our Citrix testing in bypass mode; while we understood the validity of not filtering in this state, we would have liked to been able to at least log traffic for a comparison once the device was switched to operating mode. Our initial testing was met with a number of false positives requiring us to disable Adaptive Learning and do some manual tuning.

Adaptive Learning made suggestions that we could accept, deny or customize. We found this especially helpful whenever any changes were made to our applications, such as the addition of new sites or pages within sites, especially those containing vulnerable aspects such as forms, logins and dynamic links. All our malicious attacks were blocked in operating mode.

Bee Ware more than held its own under testing against common attacks and exploits such as SQL injection, buffer overflows, XSS and Microsoft and Unix vulnerabilities. Additionally, the behavioral analysis-based security engine offered enough automation of policy creation to make it attractive to smaller IT shops. Bee Ware’s learning capabilities quickly identified new sites and pages added within our applications. However, until a new URL has been learned or manually added, it was rejected, leading initially to legitimate sites being blocked.

Breached uses dynamic application profiling combined with inbound and outbound traffic analysis to mitigate threats. Breach also identified imperfections in Web pages, such as miscoded URLs, images and objects that can create vulnerabilities, such as returning error pages displaying identifying information about the Web server or application.

We started our testing in learning mode with the option to automatically switch to protect mode once enough traffic has been analyzed. We were pleased to see a change without any false positives once the device initiated an active posture.

There’s no doubt that Breach is an excellent solution for PCI compliance. Focusing on security aspects specific to credit card transactions, from masking account numbers to robust SSL protection, we were pleased with the overall performance of the appliance. When we tagged our test data simulating credit card information with BreachMarks, our exploitable shopping cart application lit up our alerts. At first, we allowed the private information to traverse the firewall to verify Breach’s claims that it provides detailed records about any compromised information. This lets companies verify exactly what records have been illegally accessed.
MEETING THE NEW THREATS

All of the appliances we reviewed provide effective application layer protection; all scored well against the diverse attacks we threw at them. But we found significant enough differences depending on your organization’s requirements. Imperva presented the strongest all-around offering, followed closely by Breach Security. Both were strong across the board. F5 and Barracuda Networks are strong choices, faltering only in their monitoring, alerting and reporting categories.

The scope of our testing was limited to a single appliance placed in front of a couple of Web servers. However, when working with these products it becomes apparent that they were designed to protect clusters of servers, if not entire server farms hosting Web-facing applications. Though network management features weren’t part of our evaluation criteria, these may be important factors in your choice of an application firewall appliance.

Application firewalls represent next-generation digital security. As these technologies mature, and working in conjunction with traditional network firewalls, IDS/IPS and malware scanners, it is hoped they will reduce the threats faced by an increasingly Web application-driven society.

Technical editor Sandra Kay Miller is a frequent contributor to Information Security. Send comments on this article to feedback@infosecuritymag.com.