Barracuda Web Application Firewall: Benefits of Proxy Based Web Application Firewalls

RELEASE 1
JUNE 2009

Introduction

Today's knowledgeable hackers have advanced well beyond the reconnaissance tactics of scanning for open ports on network firewalls and are now targeting applications directly. Sophisticated, directed attacks able to circumvent traditional methods of perimeter and core network protection have become the primary threat to organizations.

Data center security teams are now forced to focus attention on application defense to protect core data assets and critical business processes. Web Application Firewalls (WAF) have emerged as the best fit for adding a much needed new layer of protection. Two very different types of WAF products have emerged — Non-proxy based and proxy based application firewalls. Both are claiming to protect applications against the new generation of threats; however, there are some striking differences between the two, which this paper will analyze.

Comprehensive security

In proxy based application firewalls, like the Barracuda Web Application Firewall, the connection to the application is controlled by the proxy and no packets or sessions flow to the back-end until the proxy has inspected and validated the incoming data. Separate TCP sessions are used to manage and inspect user sessions versus back-end server sessions.

Non-proxy based application firewalls either work off a span port by sniffing the traffic or without fully terminating the TCP/IP protocol. These WAF products are an extension of Intrusion Prevention Systems (IPS). IPS is a common technology used by data centers to defend common desktops and servers against well known viral and worm attacks.

Cloaking

The first step in a focused attack on a Web server is reconnaissance. The hackers try small operations on the Web site to simulate error conditions and many times the error message exposes information about the Web server, application server, or the database being used. This data is then used to launch a more focused attack on the Web infrastructure. Denying hackers this information is a big step towards securing the system. A proxy based WAF, like the Barracuda Web Application Firewall, intercepts the response from the back-end server and forwards it to the client only if it is not an error. In case the response is an error, the WAF can suppress the response containing debugging information and send out a custom response. The WAF also removes headers such as server banners which can be used to identify the servers.

Since masking or removal of data is only possible in a proxy scenario, the non proxy solutions cannot provide this type of security.

Input validation

To comprehensively protect against Web application attacks, a Web application firewall must secure applications where the incoming traffic may be encrypted or encoded using a non standard character encoding.

To ensure that no attacks are smuggled inside of encrypted or encoded packets, all proxy based Web application firewalls decrypt and normalize data before running various types of checks. They also offer multiple ways of securing the inputs. For example, the Barracuda Web Application Firewall can encrypt or digitally sign cookies to prevent against cookie tampering attacks. It can also recognize which fields are read-only or hidden and ensures that these fields are not altered. For other fields, the Barracuda Web Application Firewall offers a host of protection mechanisms such as checking for various attacks on the input fields and locking down those inputs based on data type, such as numeric or alpha numeric.

Non-proxy based Web application firewalls don't provide effective input validation. Though some of them can encrypt and normalize data, not being in a proxy configuration precludes these solutions from enforcing rules on individual form parameters passed to the application. Non-proxy Web application firewalls also cannot encrypt or digitally sign the application cookie and rely heavily on signature matching for security.

Data theft protection

Since proxy based Web application firewalls intercept outbound data, they can be configured to ensure that sensitive data like credit card information or Social Security numbers are either masked or altogether blocked to protect against data leakage.

This important layer of security is possible only because the proxy based Web application firewall sits inline with the application server and secures data on both incoming and outgoing paths.

Protect against Application Layer DoS attacks

Web applications today maintain state information, such as the number of items in a shopping cart, with the help of sessions. Persistent session data requires some memory resources on the Web servers. Forcing a Web server to create thousands of session leads locks up memory resources and results in performance degradation and can lead to a server crash.

There are multiple other ways of doing application layer denial of service. The Web application firewall, entrusted with securing the application, should be able to control or throttle the rate at which requests reach the Web server and also track the rate of session creation. Only a system that proxies on behalf of the Web or application server can be utilized to control the rate of requests reaching the Web server.

The Barracuda Web Application Firewall tracks the creation of new sessions by inspecting headers and session parameters and regulates the rate at which sessions are created by the application. The extended Rate Control capabilities of the Barracuda Web Application Firewall can be utilized to ensure that requests from some clients, like those from an internal network, are treated with a higher priority.

Centralized security enforcement

To simplify operations and infrastructure, data center teams architect the ability to enforce all security policies from a single control point. Controlling and enforcing attack prevention, privacy (SSL cryptography) and AAA (Authentication, Authorization, Accounting) policy from a single control point makes security administration both safer and more efficient.

Since a non-proxy Web application firewall does not terminate TCP connections, it does not have the ability to challenge incoming users for credentials, issue cookies upon successful credential exchange, redirect sessions to particular destinations, or restrict particular users to particular resources. Conversely, proxy based solutions, like the Barracuda Web Application Firewall, offer complete capability to be an AAA authority and/or integrate with existing AAA infrastructure. The system challenges for credentials for validation against authentication servers like LDAP or RADIUS, while forwarding and restricting access only to authorized resources based on the user's login credentials.

Control the response

Not all security violations are equal and thus cannot be responded to in the same manner. It may be desirable to respond to a security violation with a custom message or a connection reset, based on the severity of the violation. In some cases, an administrator may want to follow up with the main action with a longer block time.

This flexibility is available only in proxy based solutions. Non-proxy based WAFs rely solely on sending TCP resets back to the attacker and temporary network ACLs as their protective mechanisms. Attacking packets will get through to the attacked server and blocking actions are time-limited.

SSL architectural considerations

Application attacks use SSL cryptography and common encoding techniques to hide their attacks and bypass traditional protections. Any WAF product needs to be able to decrypt and decode HTTPS sessions. Proxy and non-proxy WAFs are quite different in the way they handle SSL cryptography and key management.

Non-proxy WAF vendors claim that they too have technology which is capable of 'seeing' into an SSL encrypted packet as it passes by the non-proxy device. But decrypting and analyzing data requires some effort and by the time a non-proxy WAF is ready to make a decision, the attack will have reached the back-end servers and completed the transaction.

Proxy based WAFs, by contrast, are designed to serve as an SSL termination endpoint. Proxies tightly couple TCP, SSL, and HTTP termination giving them complete visibility into application content and allowing them to perform deep inspection on the entire session payload, including headers, URLs, parameters, and form fields. The Barracuda Web Application Firewall not only offloads SSL processing, but can also perform certificate based client authentication and SSL re-encryption to the back-end when security policy demands it.

Accelerate and scale application delivery

Data center teams will not deploy products that adversely effect end user response time and, once again, the difference between proxy and non-proxy WAF devices is striking. Because the Barracuda Web Application Firewall fully terminates TCP, SSL, and HTTP, it is able to reduce end user response time. The system can cache, in its memory, static content from the application, offloading servers and saving download time. It can pool TCP connections to the back-end servers and offload SSL processing, thereby reducing server load and end user response time. Finally, the system can compress outbound sessions using standard GZIP algorithms to reduce download times.

None of these features are available on non-proxy WAF products.

Summary

Today's non-proxy based products are clearly an improvement over their IDS/IPS predecessors, but, ultimately deliver only a small part of the overall capability needed to protect an application. Their limited approach to application security simply isn't sufficient when it comes to protecting mission-critical business applications and confidential data.

Proxy based WAFs offer complete and comprehensive protection to enterprise Web applications. With the proxy based Barracuda Web Application Firewall, bad traffic never passes to the back-end. The system offers high transaction rates and is extremely simple to install and maintain. The Barracuda Web Application Firewall includes stateful failover capability or an optional fail-open capability to ensure continuous fail-safe operation. As data center teams move to simplify and strengthen application security policy enforcement, the Barracuda Web Application Firewall offers a comprehensive data center class solution.

For questions about the Barracuda Web Application Firewall, please visit http://www.barracuda.com/waf or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit http://www.barracuda.com/products.

About Barracuda Networks Inc.

Barracuda Networks Inc. built its reputation as the worldwide leader in content security appliances by offering easy to use and affordable products that protect organizations from email, Web and IM threats. Barracuda Networks has leveraged its success in the security market to offer networking products that improve application delivery and network access as well as world-class solutions for message archiving, backup and data protection. Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar, are amongst the 70,000 organizations protecting their networks with Barracuda Networks' solutions. Barracuda Networks' success is due to its ability to deliver easy to use, comprehensive solutions that solve the most serious issues facing customer networks without unnecessary add-ons, maintenance, lengthy installations or per user license fees. Barracuda Networks is privately held with its headquarters in Campbell, Calif. Barracuda Networks has offices in 10 international locations and distributors in more than 80 countries worldwide. For more information, please visit http://www.barracudanetworks.com.

BARRACUDA NETWORKS

Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
+1 408.342.5400
www.barracuda.com
info@barracuda.com