Barracuda Web Application Firewall vs. Intrusion Prevention Systems (IPS)

RELEASE 1
FEBRUARY 2010

Securing Web Applications

As hackers moved from attacking the network to attacking the deployed applications, a category of products known as Intrusion Prevention Systems (IPS) emerged as a solution to provide the necessary protection. However, as these attacks have grown in sophistication and target Web-based applications, the security offered by IPS solutions falls short on multiple accounts due to their core technological design of matching attack signatures against the traffic coming into your network. Since one Web application differs from another, using simplistic pattern matching does not suffice. Securing against the latest Layer 7 Web attacks requires the security solution to be aware of Web application constructs and also to be aware of application context. This is the core of the next generation of products that secure Web applications – Web Application Firewalls.

There is some confusion regarding the differences between these two technologies. IPS vendors often add to the confusion by claiming that their solutions provide complete Web application protection. This paper examines the essential differences between Web Application Firewalls and IPS solutions, especially with regard to Web application protection.

Application Protection – Technology Comparison

IPS solutions work at the network layer and can detect network level attacks such as stealth port scans, CGI attacks and attacks aimed at the protocols. They allow or deny packets after comparing them to known attack signatures. Because the IPS has no knowledge of the Web Application Layer constructs, the data structure and encoding cannot be considered during this comparison. This approach fails to prevent many attacks, or generates false positives, depending on the security policies.

The Barracuda Web Application Firewall fully terminates and proxies every connection. Because the firewall has complete visibility into the application layer constructs, it can apply strict security checks on the decoded request content. It also provides the flexibility to tighten or relax the security policies for individual elements, a requirement for securing complex Web applications.

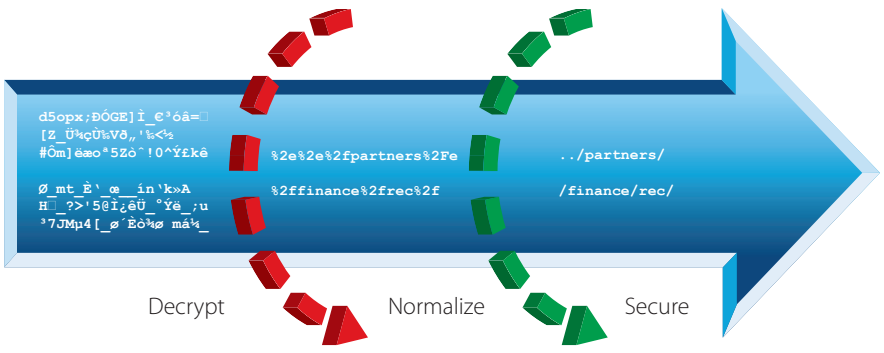
Application State Awareness

Securing against certain attacks, such as cookie tampering, session hijacking and hidden form field tampering requires that application constructs such as cookie or session be understood, and that their values be monitored to prevent tampering.

Since IPS products work at the network level and have no application state knowledge, they are incapable of blocking these application layer attacks. The Barracuda Web Application Firewall understands the Web traffic constructs and keeps track of the application state and client sessions. This enables it to enforce the full application state validation needed to secure the Web application.

Securing Encrypted or Encoded Traffic

Because most IPS products work at the network layer, they cannot validate encrypted sessions or interpret application encoding schemes. This prevents IPS technology from protecting the most mission-critical applications in a network.



Web application constructs that security appliances must identify to secure against Layer 7 attacks:

- *URLs*
- *Query/form parameters*
- *HTTP headers*
- *HTTP cookies*
- *Session context*
- *POST*
- *Response content*
- *Authentication services and other application resources*

Good hackers know this and take full advantage of it. They use SSL to hide their activities from the security snoops. Hackers also use encoding schemes such as URL encoding, Unicode and hexadecimal to evade the security provided by IPS products, rendering their application protection useless against all but the simplest attacks. The Barracuda Web Application Firewall, by contrast, was designed from the ground up with Web applications in mind. As a result, it automatically decrypts and normalizes all traffic before attempting any security inspection.

Protection from Attack Variants and Zero Day Attacks

Most modern IPS products share a common heritage with signature-based intrusion detection system (IDS) solutions. They watch incoming network traffic and compare it against a database of signatures describing all previously known exploits. If a close match is discovered, the traffic is blocked.

This signature-based approach requires each new threat to be discovered and added to the known threat signature database before it can be prevented. Even known signatures can escape detection by slightly modifying the attack signature.

The Barracuda Web Application Firewall, however, uses both a positive security model and a signature-based model. It ensures that every user request and response conforms to expected application usage and allows only valid traffic, which prevents both known and unknown application attacks with no signatures and no false positives.

For example: On a page *login.asp*, the Barracuda Web Application Firewall can enforce the field *login-id* to only accept numbers [0-9] and a maximum value of 999999. This defeats all known and unknown injection attacks.

Outbound Data Leak Prevention

IPS solutions cannot intercept and modify outbound responses from the Web applications. Hackers frequently attempt to simulate error conditions where the server response reveals sensitive information about the application, server or the database. The information gathered can be used to launch focused attacks subsequently. The Barracuda Web Application Firewall suppresses sensitive information in responses such as stack traces and debugging information to cloak the Web applications. It also removes headers like server banners that can be used to identify the servers. Additionally, the Barracuda Web Application Firewall ensures that sensitive information like credit card information or social security numbers are either masked or blocked to protect against data leaks.

Protection Against Forceful Browsing

One of the most common hacker reconnaissance strategies is Web harvesting, either manual or using malicious robots and crawlers, in an attempt to gain access to resources that are not explicitly linked but may be easily attacked.

IPS solutions have no defense against such forceful browsing attacks. Since they cannot control the server error responses, they are unable to effectively cloak the Web applications.

The Barracuda Web Application Firewall can automatically learn the precise application profile and its security policies from request and response traffic. This includes the application structure such as valid URL space, the FORM/query parameters allowed for each page, their maximum instances and allowed values. Any request for a resource outside the generated profile or violating the profile is denied by the Barracuda Web Application Firewall, thus protecting against forceful browsing.

Granular Control

A one-size-fits-all security model, as offered by IPS products, generates too many false positives when applications need to explicitly allow certain inputs that otherwise might be deemed as attacks. For example, an online email application may treat HTML input as valid, but the IPS would treat it as an XSS injection attack. A "name" parameter may be allowed a single quote (John O'Connor) but this will match SQL injection patterns.

The Barracuda Web Application Firewall allows administrators to selectively relax the security policy to allow such inputs where they are required, while continuing to apply them everywhere else. IPS products do not offer such fine-grained exception configuration.

Securing Customized Web Applications

IPS protection is limited to well-known applications and platforms such as Microsoft, Oracle or Apache. But as many as 75% of all attacks today target vulnerabilities in customized application code built on top of these platforms for which there are no signatures. As a result, IPS solutions are not effective in these cases. This problem often is compounded by the fact that custom Web applications themselves are dynamic and complex, so as new vulnerabilities get introduced they require a different approach to securing these applications.

Because it learns legitimate application behavior in real-time, the Barracuda Web Application Firewall is able to block both known and unknown attacks in standard platforms and customized application code.

Securing Web Services and Protecting against Web 2.0 Attacks.

The adoption of Web 2.0 technologies such as Web Services, SOAP, AJAX, JSON, RIA and RSS/Atom has generated additional attack vectors that are being increasingly exploited by hackers. Examples of such new attacks includes XPATH injection, WSDL probing, XML poisoning and parsing attacks, as well as many others.

Existing attacks like XSS, CSRF and a combination of the two can be carried out in new ways with Web 2.0 application frameworks and are becoming very popular in the hacker's toolbox. Using the new client side frameworks such as AJAX, hackers are bypassing same-origin policy to get cross domain access to the victim's authenticated sites, thereby riding the victim's sessions without his/her knowledge.

IPS products do not provide any protection from such attacks. The Barracuda Web Application Firewall uses advanced checks such as referrer checking and injecting unique session tokens in responses to thwart cross-domain session riding attacks. It also features a comprehensive XML firewall that denies attacks on Web 2.0 applications based on the new technologies such as AJAX and Web Services.

Refer to the whitepaper **Barracuda Web Application Firewall: Benefits of Proxy-Based Web Application Firewalls** for a more in depth discussion on proxy-based solutions.

Architectural Limitations of IPS Products

Due to being non-proxy in nature, IPS solutions are not able to offer protection against application layer DoS attacks and do not have the deployment flexibility of the Barracuda Web Application Firewall as indicated below.

Deployment flexibility	IPS/IDS Firewall	Barracuda Web Application Firewall
Secure network partitioning	No	Yes
Integrated Load Balancer	No	Yes
Accelerated application delivery	No	Yes
TCP connection pooling	No	Yes
Application content based routing	No	Yes
SSL offloading	No	Yes
Built in authentication engine	No	Yes
Multiple applications single sign on	No	Yes

Feature Comparison

The table below gives a quick comparison between the Web security abilities of other technologies vis-à-vis the Barracuda Web Application Firewall.

Security	IPS/IDS Firewall	Barracuda Web Application Firewall
Injection attack protection (XSS, SQL)	Limited	Yes
CSRF protection	No	Yes
Normalize encoded traffic	No	Yes
Inspect HTTPS traffic	No	Yes
Session tampering/hijacking/riding protection	No	Yes
Forceful browsing prevention	No	Yes
Data theft protection, cloaking	No	Yes
Brute-force protection	No	Yes
Web services projection	No	Yes
Virus/malware upload protection	Yes	Yes
Application layer DoS protection	No	Yes
Rate control protection	No	Yes
Request, response rewrite	No	Yes
Application access logging and user audit trails	No	Yes

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. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit www.barracudanetworks.com.

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