Web application firewall – Delivering must-have protection for web applications

Learn what traditional network security solutions can't do and why your organization needs a web application firewall as a cornerstone of its IT security strategy

CITRIX®

Effectively protecting the web properties that are pervasive throughout today's organizations depends on a thorough understanding of the capabilities, and also the limitations, of available security technologies. For example, although traditional network firewalls and intrusion prevention systems are useful for screening out high volumes of lower-layer threats, they are considerably less capable of defending against the increasingly targeted, application-specific threats routinely being used against organizations today. Despite delivering markedly improved granularity for controlling access to network resources, even next-generation firewalls fall short in the critical area of web property protection.

This white paper outlines the challenges of adequately defending modern web properties against cyber threats, and examines the roles that different security technologies can and, perhaps more importantly, can't fulfill in this regard. It also explains why the web application firewall is an essential component of any organization's web protection strategy and how NetScaler AppFirewall – with its unique combination of application security and application performance optimization capabilities – is the ideal solution for meeting this need.

The web application protection problem

There are numerous reasons why web properties represent a substantial risk to today's organizations. The most prominent issues are the pervasiveness of these properties, the fact that they have become the target of choice for today's hacking community and the inadequate protection afforded by so-called "application-layer" security solutions.

Web properties are pervasive

These days, organizations overwhelmingly build and buy web applications. This is definitely the case for customer- and constituent-facing applications, and increasingly true for both mobile apps and those used to enable back-office services and functions. Although revenue-generating apps still command the greatest attention, it would be unwise to underestimate how critical these other classes of apps – including those for supply chain management, finance, human resources, research and product development – are to the average business.

What does this mean for today's IT security teams? To begin with, as web applications spread throughout an organization and are increasingly used by external as well as internal users, corresponding protections are needed at more than just the network perimeter.

Another significant implication derives from the sheer diversity of web applications being deployed in organizations. With countless combinations of commercially available and custom-built web apps, it is unrealistic to expect that security technologies using only broad-spectrum rules and mechanisms – such as network-layer protocol anomaly detection – can fully protect all of them. Security teams also need tools that offer greater flexibility, far deeper granularity of inspection and control and, ideally, the ability to automatically learn/adapt to new applications.

Web properties are hackers' "target of choice"

As if pervasiveness wasn't enough to make them attractive targets for hackers, web properties are also notoriously vulnerable. This risky state of affairs is due to several factors:

- The high degree of complexity of many web properties
- The regular use of embedded, third-party libraries
- The routine incorporation of cutting-edge (read: unproven) protocols, technologies and features
- Developers and business managers who emphasize features and rapid time to market over efforts to improve code quality and reduce vulnerabilities

Expanding the target on their figurative backs, many web applications also serve as direct conduits to valuable or sensitive information, such as customer payment and ordering data, proprietary product specifications, medical records and a plethora of other personally identifiable information (PII). Once a hacker manages to punch through the user-friendly front door of the typical public-facing web application, it's a just a matter of co-opting one or more of the configured paths to associated backend databases.

Under the circumstances, it is not surprising to hear about massive web breaches leading to the compromise of millions of records, or to encounter statistics such as those from the 2014 Verizon Data Breach Investigations Report, which indicated that 35 percent of the confirmed data breaches analyzed for 2013 were attributed to web application attacks. It's also important to recognize that the web attacks that make it into the public spotlight represent only the tip of the iceberg. The actual situation is considerably worse than most business managers might expect, as the vast majority of web attacks are not deemed newsworthy or simply go unreported by the affected organizations.

Protecting app-layer services is not sufficient

Not to be overlooked is the potential confusion introduced by traditional networking frameworks and terminology. In particular, although called the "application layer," Layer 7 of the well-known OSI reference model is still – like all of the other layers in this model – about network communications. Technically, it refers to the collection of protocols and services that applications use to identify communication partners, determine resource availability and synchronize communication between two parties using the same application. Examples of application-layer protocols include HTTP (for web), FTP (for file transfer) and SMTP (for email).

The confusion results from the large number of security technologies that are marketed as providing "application-layer" protection. Although such claims may be technically accurate – for example, when an intrusion prevention system performs RFC enforcement for HTTP – they also, unfortunately, are somewhat misleading. The problem is that the protection being provided by these solutions falls considerably short of full "application" coverage, as it only indirectly helps to secure the "higher-layer" infrastructure applications (e.g., web servers and database management systems), business applications (e.g., Salesforce.com) and data that, invariably, are present as well (see Figure 1).

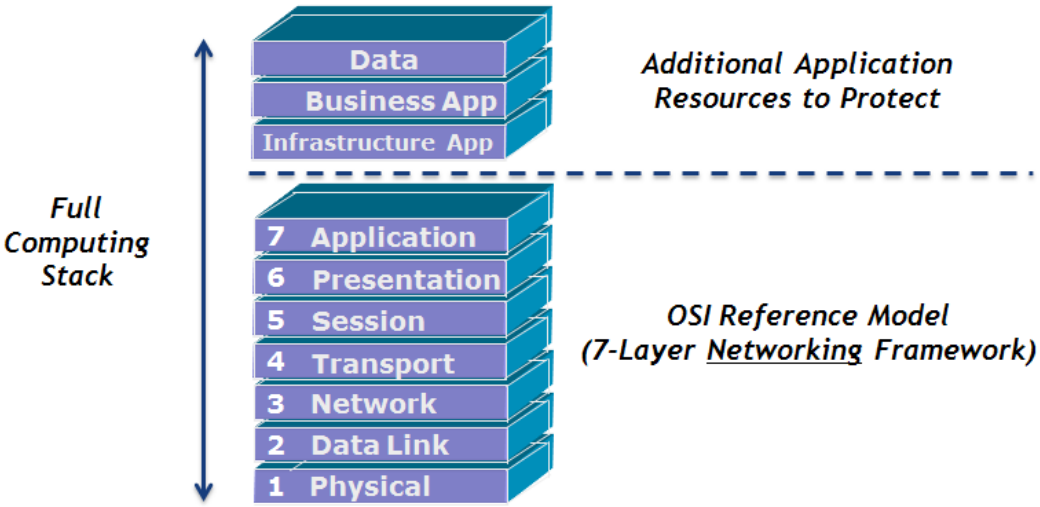

Figure 1: The full computing stack model

To thoroughly protect their important web properties, organizations need security technologies that deliver complete:

- Physical coverage – providing protection for all use cases, both perimeter and internal
- Functional coverage – providing not only policy enforcement in the form of granular access control, but also explicit detection/prevention of threats
- Logical coverage – providing protection across all layers of the computing stack, from network- and application-layer services/protocols to infrastructure applications, custom business applications and even data

Establishing comprehensive coverage such as this requires investing in more than just ordinary network firewalls and intrusion prevention systems (IPSs).

Existing network security technologies

Commonly deployed network security technologies clearly have a role to play in defending an organization's business-critical web properties. It is important to understand, however, that they have limitations and, alone, fail to provide an adequate level of protection.

Network firewalls

The primary function of an ordinary network firewall is access control – policing which application traffic is allowed to come and go across the network boundary where it's deployed. Being stateful conveys the ability to dynamically match and allow return traffic corresponding to authorized outbound sessions (and vice versa). However:

- Because it is based solely on network-layer attributes (e.g., port, protocol and source/destination IP addresses), an ordinary firewall's access control capability is not especially granular. As a result, the firewall cannot always distinguish and, therefore, control the individual applications using a given port/protocol – such as the vast array of HTTP web apps that use TCP port 80.
- Ordinary network firewalls are not equipped to explicitly detect/prevent threats. The only protection they provide against malware, attacks and other unauthorized activities is a by-product of the access control policies they are configured to enforce. For example, if a threat relies on a communication path that is not "open," it will, by default, be prevented (without ever being detected).

The net result is that ordinary network firewalls provide relatively limited protection for an organization's web properties.

Network intrusion prevention systems

Typically offering little in the way of access control capabilities, network IPS technology is focused instead on detecting threats. The broad-spectrum mechanisms this technology relies on include signatures for known threats and vulnerabilities, and protocol and behavior anomaly detection for suspected malicious activities and unknown threats. Coverage is typically provided up to and including the application services layer and for all common Internet protocols, including HTTP(s), DNS, SMTP, SSH, Telnet and FTP.

Sporadic coverage is also available at higher layers of the computing stack, as it is not uncommon to include signatures for known vulnerabilities and threats associated with the most popular infrastructure and business applications running in organizations today. Despite being a step in the right direction, this extended coverage is simply not sufficient and leaves IPS technology stuck in the middle, subject to both:

- False negatives – as a lack of deeper visibility into and understanding of applications leaves it blind to most higher-layer threats (such as those that work by manipulating application process logic), and
- False positives – as attempting to write broadly applicable signatures that account for a wide range of higher-layer threats across both standard and custom web applications invariably leads to countless false alarms

Although providing explicit detection/prevention of threats makes IPS technology a valuable complement to ordinary network firewalls, spotty coverage above the application services layer results in only an incremental gain in protection for an organization's web properties.

Next-generation firewalls

The next-generation firewall (NGFW) combines the capabilities of network firewalls and IPSs in a single solution. To these capabilities, the NGFW typically adds user and application identity as attributes for controlling access to/from a network. For use cases with all but the highest throughput requirements (i.e., above several Gbps), the result is a conveniently consolidated solution with a few extra bells and whistles for good measure. Relative to protecting web applications, however, a significant shortcoming remains: application awareness. The ability to reliably identify applications regardless of the port and protocol being used, also known as application awareness, is not the same as application fluency.

With application awareness, techniques such as application protocol decoding and application signatures identify the specific infrastructure and business apps responsible for all network traffic. Thus application awareness enables precision access control, where separate policies can now be set when multiple apps and services are using the same protocols and ports. For example, the "web bucket" of traffic can be sliced and diced to allow access to a handful of helpful and business-critical web applications while selectively restricting or completely blocking less-desirable web apps, such as web mail, file-sharing services and Facebook games.

Aa a prerequisite for explicit threat detection at higher layers, application fluency requires an even deeper understanding of the application being protected, including which inputs and navigation sequences are valid and how the application is intended to work (versus not to work).

The bottom line is that although NGFWs deliver enhanced access control capabilities and an opportunity to eliminate numerous single-technology appliances, organizations are still left with the explicit threat detection/protection capabilities of an ordinary IPS. The breadth and depth of coverage are simply not sufficient to protect most web properties – especially custom ones – from the increasingly sophisticated and targeted attacks that now constitute a significant portion of the threat landscape.

The web application firewall – master of the app domain

The web application firewall (WAF) picks up where other security technologies leave off, providing protection from threats that operate at the highest layers of the computing stack. Automated learning routines supplemented by manually configured policies result in a high-fidelity "understanding" of how each protected web application works, including all custom features and business logic. Deviations subsequently detected represent suspected malicious traffic, which is automatically dispositioned – for example, blocked, allowed subject to restrictions or logged – according to administrator-defined policies.

Compared to the security technologies previously discussed in this paper, WAFs are unique in their ability to:

- Validate inputs, thereby stopping dangerous SQL injection, cross-site scripting and directory traversal attacks
- Detect cookie, session or parameter tampering attacks
- Block attacks that exploit vulnerabilities in custom web properties
- Stop exfiltration of sensitive data through object-level identification and blocking

- Fully inspect SSL-encrypted traffic for all types of embedded threats
- Prevent threats that operate by exploiting logic loopholes in custom business apps
- Protect against application-layer denial and distributed denial of service (DDoS) attacks
- Dynamically cloak server response information that is potentially useful to hackers
- Deliver comprehensive XML protections, including schema validation for SOAP messages, and XPath injection defenses, and identify/block XML attachments harboring malicious content
- Enable compliance with requirement 6.6 of the Payment Card Industry Data Security Standard (PCI DSS)

Underpinning all of these application-centric protections, market-leading WAFs – such as NetScaler AppFirewall – also include support for network-layer access control rules and a signature-based component for detecting known threats. Security teams need to recognize, though, that WAF defenses, by design, are primarily focused on web protocols such as HTTP, HTTPS, XML and SOAP.

Security technology round-up

Table 1 provides a side-by-side comparison of the security technologies discussed above. Key takeaways include the following:

- Although they are useful for screening out high volumes of low-layer threats, the most commonly deployed security technologies – network firewalls and IPSs – leave a lot of ground uncovered when it comes to protecting web applications
- Although no single security technology provides complete protection for web applications, WAFs come closest
- Combining NGFWs with WAFs is an efficient way to establish powerful, full-spectrum threat protection for all of an organization's important web properties

Comparison of security technologies for protecting web properties

	Network firewall	Intrusion prevention system	Next-generation firewall	Web application firewall
Works at	Layers 3-4	Layers 3-7	Layers 3-7	Layers 3-7+
Deployment architecture (typical)	Layer 3 gateway	Transparent mode	Layer 3 gateway	Reverse proxy
Access control granularity	Port, protocol, IP address	n/a	Port, protocol, IP address, user, app	Port, protocol, IP address
Threat detection / prevention techniques	n/a	Signatures, pattern matching, protocol and behavior anomaly detection	Signatures, pattern matching, protocol and behavior anomaly detection	Signatures, protocol anomaly detection, app-specific anomaly detection
Protocol coverage	Any	Any	Any	Web-centric: HTTP(s), XML, SOAP, SPDY
SSL/encrypted traffic inspection	n/a	n/a	Yes	Yes
DDoS protection	Network layer (basic)	Network layer	Network layer	Application layer
Web application protection	Minimal	Known/unknown vulns/threats primarily for network and app services layers	Known/unknown vulns/threats primarily for network and app services layers	Extensive, including full application layer coverage

NetScaler AppFirewall

Its unique web protection capabilities make the WAF an essential component of an organization's security architecture and elevate the importance of selecting a full-featured solution.

NetScaler AppFirewall is a comprehensive, ICSA-certified web application security solution that blocks known and unknown attacks against web and web services applications. By employing a hybrid security model and analyzing all bi-directional traffic, including SSL-encrypted communications, NetScaler AppFirewall counteracts a broad range of security threats without requiring any modifications to applications.

Following are NetScaler AppFirewall key protection features:

Hybrid security model. To defeat new, unpublished exploits, a positive-model policy engine that understands permissible user-app interactions automatically blocks all traffic falling outside this scope. As a complement, a negative model engine uses attack signatures to guard against known threats to applications.

XML protection. NetScaler AppFirewall not only blocks common threats that can be adapted for attacking XML-based apps (e.g., cross-site scripting, command injection), but also incorporates a rich set of XML-specific protections, including comprehensive schema validation and the ability to thwart related application-layer DoS attacks (e.g., excessive recursion).

Advanced protection for dynamic elements. Multiple, session-aware protections secure dynamic application elements such as cookies, form fields and session-specific URLs, thereby thwarting attacks that target the trust relationship between client and server (e.g., cross-site request forgery).

Tailored security policies. An advanced learning engine automatically determines the expected behavior of web applications and generates human-readable policy recommendations. Administrators can then tailor the security policy to the unique requirements of each application to avoid false-positive detection events.

Ensured compliance. NetScaler AppFirewall enables companies to comply with data security mandates such as the PCI DSS, which explicitly encourages the use of WAFs for public-facing applications that handle credit card information. Detailed reports can be generated to document all protections defined in the firewall policy that pertain to PCI mandates.

Zero-compromise performance. The industry's highest-performing web application security solution delivers 12+ Gbps of comprehensive protection without degrading application response times.

Further distinguishing NetScaler AppFirewall is the unique ability to deploy it as an integral component of the full NetScaler application delivery platform. The benefits of this approach include substantial gains in web application performance (due to advanced acceleration and server offload capabilities) and reliability (due to server load balancing, server health monitoring and site-level failover capabilities). The net result is an ideal solution that delivers unparalleled web protection along with a high-definition application experience for today's demanding users.

Conclusion

In the past, ordinary network firewalls and intrusion prevention systems may have afforded adequate protection for the handful of web applications that the average organization deemed important. With today's substantially greater dependence on web properties and the dramatic shift by hackers toward targeted, application-specific attacks, however, that is no longer the case. Even next-generation firewalls fall short, as the enhancements they deliver are primarily in infrastructure consolidation and increased granularity for setting and enforcing access control policies.

To thoroughly protect their organization's numerous externally and internally facing web properties, security teams need to supplement these other countermeasures – which are still useful for filtering high volumes of lower-layer threats – with a web application firewall solution. By maintaining an in-depth understanding of how each protected application normally operates and searching for anomalous activities and information beyond the application services/protocol layer, full-featured WAFs such as NetScaler AppFirewall deliver a degree of threat protection unavailable from all other commonly deployed security technologies, legacy and otherwise.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com

Copyright © 2016 Citrix Systems, Inc. All rights reserved. Citrix, NetScaler and NetScaler AppFirewall are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

Insight®

Work smarter

At Insight, we'll help you solve challenges and improve performance with intelligent technology solutions.

Learn more