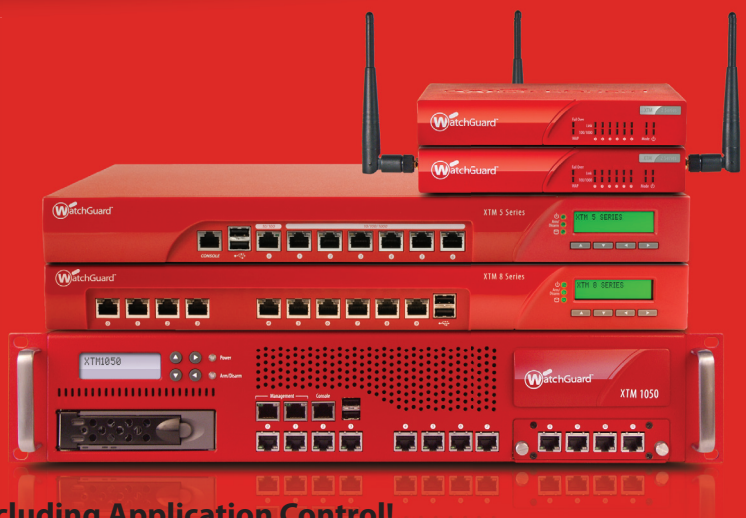
SEARCHSECURITY.COM

technical guide on WEB APPLICATION firewalls

contents

TechTarget

NOTHING GETS PAST RED



Get Comprehensive Network Protection - including Application Control!

WatchGuard's new Application Control for XTM appliances allows businesses to control what's being used on their networks – from Facebook to Skype – for tighter security and increased productivity. With sophisticated behavioral analysis and more than 2,300 signatures, it allows IT to control over 1,500 web 2.0 and business apps with ease.

- Find out how you can take back control of your network with our free white paper at **www.watchguard.com/appcontrol**.
- See how WatchGuard outperforms every other major UTM brand on the market at **www.watchguard.com/utmmarketreview**.

For more information, call **1.800.734.9905** or visit **www.watchguard.com**. Get **red.** Get secu**red.**

WatchGuard™

insight

Web Application Firewalls

Web application firewalls examine application-layer messages for security policy violations and alert to possible intrusions. They're becoming critical data protection and compliance tools that any security decision maker must understand.

SEARCHSECURITY.COM presents a comprehensive guide to Web Application Firewalls. Our experts will examine evaluation criteria, deployment considerations and management issues.

contents

A Vision of Next-Gen WAF

Imperva is the global leader in data security. Thousands of the world's leading businesses, government organizations, and service providers rely on Imperva solutions to prevent data breaches, meet compliance mandates, and manage data risk.

Hacking has become "industrialized" with a well organized infrastructure, defined roles and responsibilities, and sophisticated attack vector automation that generate large-scale attacks of unprecedented size, speed, and devastation.

The industrialization of hacking coincides with a critical shift in focus. Sensitive data is the new target. Data drives businesses more today than ever. In order to protect the business, organizations need to protect the web applications and the data. This level of defense requires the next generation web application firewall.

Learn more and download the following two whitepapers:

www.imperva.com/go/NG-WAF

White Paper: The Industrialization of Hacking

This whitepaper identifies the "Industrialization of Hacking"

White Paper: Next Generation Web Application Firewalls (NG-WAF)

This whitepaper explores Imperva's vision of next generation WAFs, or NG-WAF in three interrelated sections covering: industrialized attack mitigation, interoperability and service delivery models, and risk management. It also highlights some of the capabilities currently delivered through Imperva's SecureSphere solution.

IMPERVA®
Protecting the Data That Drives Business

3400 Bridge Parkway
Redwood Shores, CA 94065
Tel: +1 (650) 345-9000

info@imperva.com | www.imperva.com | Blog | Twitter | YouTube | iTunes | LinkedIn | Facebook

SELECTION CRITERIA

Choosing the Right Web Application Firewall

Learn about Web application firewall evaluation criteria that can help you meet PCI compliance requirements and manage deployments. BY MICHAEL COBB

ENTERPRISES TRYING to meet PCI compliance requirements may find themselves in a quandary when it comes to choosing a Web application firewall (WAF). How do you know what to look for? How do you deploy and manage the appliance or software effectively? How do you fit it into your existing infrastructure? We'll highlight the key considerations when evaluating products so your company is in compliance.

A Web application firewall or application-layer firewall is an appliance or software designed to protect web applications against attacks and data leakage. It sits between a Web client and a Web server, analyzing application layer messages for violations in the programmed security policy. Web application firewalls address different security issues than network firewalls and intrusion detection/prevention systems, which are designed to defend the perimeter of a network. But before you rush to buy, you'll need to understand that this is not a plug-and-play check box compliance item and requires more than just putting an appliance in front of your application servers.

Choosing a WAF

Follow these basic steps in selecting the appropriate Web application firewall for your application:

1. Use security policy objectives to define what controls your WAF must have.
2. Review the types of risk each product covers.
3. Test performance and scalability.
4. Evaluate the vendor's technical support.
5. Assess whether you have the required in-house skills to maintain and manage it.
6. Balance security, throughput, and overall cost.

–MICHAEL COBB

What you need to know

Whenever new legislation or security requirements are introduced, those tasked with ensuring compliance often tend to rush the decision-making process. Many system administrators base their decision on a single vendor's sales pitch or a particular requirement or feature they've picked up on.

The result, more than likely, will be inappropriate or less than optimal security. Even a tight deadline doesn't absolve you of due diligence. To choose a security device such as a Web application firewall, you need to answer the following questions:

- What does it need to do based on your security policy objectives and legislative requirements?
- What additional services would be valuable?
- How will it fit into your existing network—do you have the in-house skills to use it correctly and effectively?
- How will it affect existing services and users and at what cost?

New compliance requirements such as PCI DSS require you to update or at least review your security policy before you can answer the first question. A good security policy defines your objectives and requirements for securing your data. That foundation allows you to define what security devices are appropriate to meet your requirements. Since each Web application is unique, security must be custom-tailored to protect against the potential threats identified during the threat modeling phase of your secure lifecycle development program. Review which of these threats the WAFs under consideration safeguard against—such as analyzing parameters passed via cookies or URLs and providing defenses against all of the OWASP Top Ten application vulnerabilities—as well as any additional requirements mandated for compliance.

Choosing your WAF

To ensure a WAF is suitable for PCI DSS compliance purposes you should compare its capabilities with those recommended in the Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified issued by the PCI Security Standards Council.

They must be able to inspect and handle Web page content such as HTML, Dynamic HTML (DHTML), and cascading style sheets (CSS), as well as the protocols that your application uses, such as HTTP and HTTPS.

Also, check how quickly the vendor has adopted new protocols in the past. Review their development and support policy to determine if they will support custom protocols or protect a set range of application protocols. In addition, a WAF must be able to inspect Web services messages, typically SOAP and XML. Ask the WAF vendor about their processes for auto-updating and applying

dynamic signatures. Such conversations will help you assess their technical support and help services.

Lastly, ask about the additional cost of specific features. For example, some applications may require FIPS hardware key store support. A WAF vendor may support this requirement but at a dramatically higher price.

As you work through the list of requirements, take the time to understand the technical approaches and depth of treatment that each WAF uses to provide coverage of one or more security areas. Can you white list data types and ranges and create rules combining both white and black lists? How strong is the WAF against attack on itself? For example, it should run on a hardened OS, probably with components running in a non-privileged and closed runtime environment. If the product's security isn't rock solid, you should probably end the discussion right there.

Software vs. Hardware

The PCI Information Supplement states that a WAF can be implemented in software on a standard server running a common operating system or an appliance. It may be a stand-alone device or integrated into other network components. So, you can choose from the full range of WAFs on the market.

What's Next?

Web application firewalls are just the start.

TO COMBAT the ever-increasing sophistication of application attacks, the protection offered by WAFs should be integrated into application assurance platforms. This structure, promoted by vendors such as F5 and Barracuda Networks, combines WAFs, database security, XML security gateways and application traffic management to provide more holistic security coverage.

The benefits include the ability to compare information across these devices to accurately determine if traffic is potentially malicious. This makes traffic control, analysis and reporting far more effective. Administrators can configure one set of policy rules and parameters, rather than trying to enforce each policy across several different devices, greatly reducing administrative overhead.

Looking into the future, it is essential that WAFs or whatever supercedes them gain the ability to interpret inbound data the same way as the application it is protecting. This will entail some form of script engine to remove any obfuscation, so that the security device will view the request in the same form that the browser will. This will make it far easier to assess whether or not the code is malicious. Let's hope we will see this form of dynamic analysis in the next generation of security devices.

–MICHAEL COBB

Software WAFs are usually cheaper and more flexible. Appliances are typically easier to install and configure, partly because their operating system has already been hardened, whereas a software firewall will require you to harden it. (A WAF won't protect you against poor configurations or vulnerabilities in your servers.)

If you opt for a software-based product, choose one that works on a platform with which your IT department is familiar. Either way, check out what type of training and support is provided by the firewall vendor—and at what cost.

There are, of course, open source software WAFs, such as ModSecurity and AQTRONIX WebKnight. If they meet your requirements you can greatly reduce your costs, but you will still need staff to learn, install, configure, and maintain it. Many open source projects have excellent support forums but unlike a purchased

Primer: PCI DSS

What you need to know about PCI DSS.

THE PAYMENT CARD INDUSTRY Data Security Standard (PCI DSS) was developed by the PCI Security Standards Council, an open forum launched in 2006. The council is part of PCI, a joint industry organization set up by a group of the major credit card companies, and is responsible for the ongoing development, management, education and awareness of the PCI DSS.

However, it doesn't enforce the PCI DSS, nor does it set the penalties for any violations. Enforcement is left to the specific credit card companies and acquirers. PCI DSS does not replace individual credit card company's compliance programs but has been incorporated as the technical requirements for data security compliance. The PCI DSS must be met by all merchants that accept credit and debit cards issued by the major credit card companies.

Under the PCI DSS, an organization must be able to assure their customers that their credit card data, account information, and transaction information is safe from hackers or any malicious system intrusion by adopting various specific measures to ensure data security. These include building and maintaining a secure IT network, protecting cardholder data and maintaining a vulnerability management program and information security policy.

The standard's compliance requirements are ranked in four levels, and the level of compliance required of a merchant is based upon the annual volume of payment card transactions it processes. Level 1, the highest level, can also be imposed on organizations that have been attacked or are otherwise deemed as high risk. A single violation of any of the requirements can trigger an overall non-compliant status, resulting in fines, and, possibly, suspension or revocation of card processing privileges until the merchant is PCI compliant.

For more details, visit the PCI Security Standards Council website.

–MICHAEL COBB

product you won't be able to call a help desk in an emergency.

Performance and scalability are other important considerations when evaluating hardware or software options. Some devices may be limited as to how many transactions per hour it can handle. Other appliances may have bandwidth limitations. You will need to choose a scalable and flexible firewall if you're planning on increased Web activity or adding applications in the near future.

Software products often provide an easier upgrade path than appliances, but hardware WAFs are better suited for high-volume sites, which require high throughput.

If you are running a large-scale application, which requires more than one WAF, then centralized management may be a critical feature so firewall policies can be deployed and managed from a single location.

Software products often provide an easier upgrade path than appliances, but hardware WAFs are better suited for high-volume sites, which require high throughput.

Our advice is not to get hung up on whether the WAF is hardware or software, as long as it can meets your objectives and you have the in-house skills to configure and manage it.

Help is on hand

Plan on devoting plenty of time to fully evaluate WAF products. Once you have narrowed down your choices to those that meet your basic requirements, how do you compare the different options?

The Web Application Security Consortium (WASC) creates and advocates standards for Web application security. They have developed the Web Application Firewall Evaluation Criteria (WAFEC) for comparisons. Their testing methodology can be used by any reasonably skilled technician to independently assess the quality of a WAF solution.

Use their criteria as part of your evaluation process. Follow WASC's recommendation to pay close attention to the deployment architecture used, support for HTTP, HTML and XML, detection and protection techniques employed, logging and reporting capabilities, and management and performance.

WAF Deployment

Congratulations. You've chosen, purchased and installed a WAF with the necessary compliance capabilities. But that doesn't mean that you're compliant. Proper positioning, configuration, administration and monitoring are essential.

Installation needs to follow the four-step security lifecycle: Secure, monitor, test and improve. This is a continuous process that loops back on itself in a persistent cycle of protection. Before any device is connected to your network,

you need to ensure that you have documented the network infrastructure and hardened the device or the box it will run on. This means applying patches as well as taking the time to configure the device for increased security.

Configuration will stem directly from the business rules that you've established in your security policy (such as allowed character sets). If you approach firewall configuration this way, the rules and filters will define themselves. WAFs can expose technical problems within a network or application, such as false positive alerts or traffic bottlenecks.

Careful testing is essential, particularly if your site makes use of unusual headers, URLs or cookies, or specific content that does not conform to Web standards. Extra testing time should be allowed if you are running multi-language versions of your application, as it may have to handle different character sets.

Stress testing the WAF using tools with Microsoft's Web Application Stress and Capacity Analysis Tools or AppPerfect Load Tester will also help reveal any bottlenecks caused by the positioning of the WAF.

The testing should match the "live" application environment as closely as possible. This will help expose any system integration issues the WAF may cause prior to deployment. Stress testing the WAF using tools with Microsoft's Web Application Stress and Capacity Analysis Tools or AppPerfect Load Tester will also help reveal any bottlenecks caused by the positioning of the WAF.

WAF Management

Once you're up and running, assess how any future Web application firewall changes may impact your Web applications, and vice versa. You must, of course, document the changes you make to your network infrastructure for future reference and troubleshooting. This involves tracking any changes made to their configuration now and in the future.

Changes to the production environment should always occur during a monitored maintenance window. Make sure all affected parties throughout the organization are advised in advance of the timing and scope of the changes. To ensure that configurations aren't changed unintentionally or without due process, you must control physical as well as logical access to your security devices. Strict adherence to change control, business continuity, and disaster recovery policies will all play a part in protecting the WAF and your business.

Because application-layer firewalls examine the entire network packet rather than just the network addresses and ports, they have more extensive logging capabilities and can record application-specific commands. So, don't let this capability and information go to waste. Log file analysis can warn you

of impending or current attacks. Ensure that you define what information you want your firewall to log—preferably the full request and response data, including headers and body payloads. Make sure your staff have the expertise—and adequate time—to review and analyze it.

Web applications will never be 100 percent secure. Even without internal pressures to deploy Web applications quickly, there will be vulnerabilities that are open to threats. By having a Web application firewall in place as part of a layered security model, you can observe, monitor and look for signs of intrusion. It can also mean the difference between scrambling to fix a vulnerability or having the breathing room to repair the vulnerability to your own timetable.

Michael Cobb, CISSP-ISSAP, is the founder and managing director of Cobweb Applications Ltd., a consultancy that offers IT training and support in data security and analysis. Send comments on this article to feedback@infosecuritymag.com.

Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. Free.

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.

INFORMATION SECURITY®

www.SearchSecurity.com

Breaking news, technical tips, security schools and more for enterprise IT professionals.

SearchSecurity.com

www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.

SearchFinancialSecurity.com

www.SearchFinancialSecurity.com

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.

SearchSecurity.co.UK

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

SearchMidmarketSecurity.com

www.SearchMidmarketSecurity.com

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.

SearchSecurityChannel.com

www.SearchSecurityChannel.com

TechTarget®
The IT Media ROI Experts

PCI 6.6

How to Choose Between Source Code Reviews or Web Application Firewalls

Learn which technology best helps your organization with PCI DSS compliance requirements?

BY MICHAEL COBB

BEFORE YOU DECIDE whether a source code review or Web application firewalls best meet your PCI DSS compliance needs, I recommend taking time to fully understand PCI's Web application requirements, including the clarification documents, and consider how the approved options mesh with your architecture and resources. It is now clear that enterprises have multiple paths to compliance and, if executed properly, any of the options will not only help achieve compliance, but also improve Web application security.

Of course, there is no one-size-fits-all approach to application security. Unless you are in the fortunate position to be able to both conduct code reviews and run a WAF, it looks like the choice may simply come down to people. Does the enterprise have staff that can:

- Configure and maintain an application-layer firewall?
- Perform a code review?
- Use a third-party vulnerability detection tool and fix any problems the review uncovers?

Of course, the decision could also depend upon architecture considerations and how well a WAF would work with existing systems and devices. A factor to consider, particularly for those leaning towards a third-party code review, is how comfortable the organization may be with the status of its code. Payment card applications develop over time and may include some legacy code of unknown origin and unclear purpose. Security staff may not want to remove legacy code and run the risk of breaking a mission-critical application. Placing a firewall in front of an application might be less costly, or less disruptive, than rewriting it in light of a code review.

Another approach is to use threat modeling to identify and evaluate the risks to an application. Take the top three critical risks and decide how best to

remediate them: code review, vulnerability assessment or WAF. Be aware, though, that implementing a WAF will not eliminate the need for you to have a secure software development process in place (Requirement 6.3)! Application vulnerability assessments and code reviews both strengthen the development and quality assurance cycle.

Many of these choices are likely to be too costly for the small e-commerce site, so my recommendation here would be to outsource the payments to a third-party payment provider, which affectively outsources all of the expensive security requirements, including Web security, as well as the actual PCI DSS compliance. As long as you don't handle any of the card payments anywhere else, you don't need to be PCI DSS compliant.

Compliance vs. security

No matter what choices you make, many would debate whether PCI compliance equates to acceptable levels of security.

No matter what choices you make, many would debate whether PCI compliance equates to acceptable levels of security. Those responsible for security need to understand the limitations and capabilities of each option. Source code analysis alone may deliver compliance, but it's not the answer to application security. No one thing is. PCI DSS focuses on payment card applications and components related to PCI. It doesn't look at an organization and its entire networked operations in a holistic manner, requiring security to be implemented across the board.

Even with the clarifications provided by the PCI Requirement 6.6 Information Supplement, many merchants are still unsure of what actions are good enough to gain compliance. This leads to the classical compliance dilemma. If you promulgate a standard intended to increase security, you must be prepared to answer the question: "What must I do to comply with the standard?" Which quickly evolves into: "What is the minimum I can do to be in compliance?" If you view PCI compliance from the "check the box and move on" viewpoint, then a WAF appears the quick and easy option.

The PCI DSS, however, does give organizations the foundation for creating a secure architecture and business model they can operate on. It has also put security on the board room agenda. If you're concerned with security, getting PCI compliance will be a byproduct. Until your developers program securely, a layered security solution will always be the best approach for mitigating risks, in this case, one that includes code review, vulnerability assessment and a WAF. The WAF will be more effective once results from a vulnerability scan have been integrated into its configuration. This will provide protection while the source code is analyzed and corrected to eliminate the vulnerabilities.

Will vulnerabilities still come to light even after a PCI review? Sure, but not

TABLE OF CONTENTS
SELECTION CRITERIA
PCI 6.6
MIDMARKET
FIREWALL MANAGEMENT
CHANNEL
SPONSOR RESOURCES

as many and hopefully not as serious. Costs and business drivers may result in lower levels of assessment and protection, but those are the real world business decisions that have to be taken.›

Michael Cobb, CISSP-ISSAP is the founder and managing director of Cobweb Applications Ltd., a consultancy that offers IT training and support in data security and analysis. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. Mike is the guest instructor for several SearchSecurity.com Security Schools and, as a SearchSecurity.com site expert, answers user questions on application security and platform security.

MIDMARKET

PCI 6.6 Web Application Security Mandates Burden Smaller Companies

Midmarket IT organizations must comply with PCI 6.6 and choose between a Web app firewall or source code review.

BY MICHAEL S. MIMOSO

IT'S BEEN MORE than two years since section 6.6 of the Payment Card Industry Data Security Standard (PCI DSS) became a requirement. PCI 6.6 requires organizations that process credit card transactions to address Web application security; it mandates that companies conduct either manual or automated source code reviews, or install a Web application firewall between a Web application and client endpoints.

Web applications are a popular attack vector. SQL injection attacks are becoming rampant, and are most dangerous because the vulnerabilities they exploit often provide a direct route to an organization's sensitive data.

"Many organizations start with a Web application firewall to get a checkmark. That is not necessarily raising the bar in terms of security, but they would be meeting the compliance factor."

–DANNY ALLAN, director of security research, IBM Rational

The PCI Security Standards Council imposed a June 30, 2008 deadline for compliance with PCI 6.6; for the 18 months prior, it was a recommendation. It was a wake-up call for organizations to address Web application security, and a stress point for smaller Level 3 and Level 4 merchants who may not have the resources or expertise to either conduct a source code review or properly configure a Web app firewall.

Manual source code reviews are extremely expensive and time consuming. Automated vulnerability scans are less so, but still tax the bottom line. Web app firewalls, meanwhile, are likely the quickest way to a compliance checkmark, and some experts say this is a fitting starting point until an organization matures sufficiently to tackle its proprietary software.

"Many organizations start with a Web application firewall to get a checkmark. That is not necessarily raising the bar in terms of security, but they

would be meeting the compliance factor," says Danny Allan, director of security research with IBM Rational.

Allan points out that organizations should want to do both, but the most likely scenario is one where an organization is grappling with how to compare the two options afforded by 6.6 and deciding which is the best immediate fit.

"There's no right answer," Allan says. "Some recommend beginning with a Web application firewall, but a WAF needs to be configured properly to work. If you're in a fluid environment [applications change and grow in complexity], that can require a fair amount of time to configure. And ultimately, you're putting a Band-Aid on the issue. The application still has the problem."

"In my mind, you want to do both [6.6 options], but this is an apples to oranges comparison. Which gives you more of a bang in the short term? That is the question that needs to be answered."

–DANNY ALLAN, director of security research, IBM Rational

Web application firewalls, also known as deep-packet inspection firewalls, look at application layer messages for violations of an established security policy. Some offer signature-based protection, while others are fed a baseline of appropriate application behaviors and monitor for deviations. They're offered either as software or in an appliance. WAFs struggle detecting certain types of attacks because they don't always understand the context under which input is entered into an application, and legitimate traffic could be dropped if a WAF believes the traffic violates policy. Also, some tools fail to detect some serious Web app threats such as cross-site scripting attacks.

"In my mind, you want to do both [6.6 options], but this is an apples to oranges comparison," Allan says. "Which gives you more of a bang in the short term? That is the question that needs to be answered."

"Smaller merchants are going to gravitate toward a WAF if it will get them a checkmark," says David Taylor, founder of the PCI Knowledge Base and research director of PCI Security Vendor Alliance. "That is where things are going. It's not wrong; it's the most cost-effective way to go. I would never tell a Level 3 or 4 merchant to spend more money than they have to."

Source code reviews, meanwhile, are the ideal solution. For some time, experts have urged organizations to include security in the software development lifecycle. Automated scanners can test applications for vulnerabilities, in particular the Open Web Application Security Project (OWASP) top 10 list of flaws. In fact, PCI DSS 6.5 says Web applications should be developed based on guidelines such as OWASP and applications should be secured against the vulnerabilities listed in the top 10, which is updated annually.

But developers generally shun security because it hampers productivity and

functionality. Manual reviews are difficult, though sometimes they're essential in order to catch problems in the context of an application's semantics. Expense aside, manual reviews require inspection, often of hundreds of thousands of lines of code, and it's virtually impossible to follow all the logic paths an application can take, says Barmak Meftah, senior VP of products and services at Fortify, a vendor of static and dynamic source code analysis tools.

"The main type of vulnerability a hacker is getting hold of is an input field—putting in malformed input and getting the app to do unintended things," he explains. "That packet is now using different paths than intended, and connecting those dots optically is impossible."

The big picture is that organizations need to look at 6.6 compliance requirements in the context of an overall vulnerability management program, says IBM Rational's Allan.

"Security threats are changing daily. PCI 6.6 is a strategic approach: How do I address this fluid changing paradigm of security attacks that is going to be different tomorrow than today?" Allan says. "This is about building good, quality code. If we keep focusing on the security aspect and not building quality apps, we're forever going to be chasing security vulnerabilities."

Michael S. Mimoso is Editorial Director of the Security Media Group at TechTarget.

FIREWALL MANAGEMENT

Building Application Firewall Rule Bases

Here are four steps for building and deploying application firewall rule bases in an organization. BY MIKE CHAPPLE

DURING THE PAST DECADE, most enterprises have made significant investments in network and perimeter security. Organizations have tightened their controls and moved toward a defense posture that dramatically limits the effectiveness of hackers' network-scanning attacks. Unfortunately, while security professionals were busy building up network controls, attackers spent their time developing new techniques to strike at the next Achilles' heel: the application layer.

A Gartner Inc. study highlighted this risk by estimating that 75% of today's successful attacks occur at the application layer.

A Gartner Inc. study highlighted this risk by estimating that 75% of today's successful attacks occur at the application layer.

Why are these attacks so successful? The answer is quite simple: they bypass all of the network-centric controls that security personnel have implemented over the last ten years, such as port blocking. Consider Web application attacks, for example. Traditional firewalls protecting a Web server contain rules that block all sorts of unwanted traffic, only allowing TCP traffic to traverse the firewall via ports 80 or 443. Unfortunately, the firewall can't distinguish desirable port 80 traffic from undesirable port 80 traffic.

This is where application firewalls come into play. These firewalls perform application-layer inspection of HTTP traffic before it reaches the Web server. The devices are able to inspect a connection and analyze the nature and type of commands that users are providing to the application. They can then analyze the traffic for signatures of known attacks or deviations from profiles of standard utilization.

While application firewalls have great potential, the process of deploying them should be slow and deliberate. Back when network firewalls first entered the enterprise, implementation managers typically adopted a cautious approach to these projects, conducting careful analysis and extensive testing. That same approach should be applied when deploying a Web application firewall. Careful testing builds confidence among an organization's application developers, serving as leverage security managers can use to convince them that the technology will help the enterprise more than it will hinder their day-to-day lives.

Once an organization is ready to move the product into the production environment, it's time to think about a solid firewall rule base. Here's a step-by-step approach for building and deploying application firewall rule bases in an organization:

1. **Have an adequate adjustment period.** Modern Web application firewalls have sophisticated capabilities that monitor traffic and learn patterns of normal activity. Over time, the firewall is "trained" to recognize these patterns and block anomalous traffic. The firewall, however, needs to be trained over a long enough period of time so that the rule base reflects periodic and seasonal trends in network activity. For example, an ecommerce retailer wouldn't want to train the firewall protecting its Web site during the slow summer months, and then deploy the rule base during the busy winter holiday shopping season.
2. **Develop custom rules to supplement vendor-provided signatures.** Knowledge of an organization's infrastructure is important, and customizing a firewall to meet a company's unique needs can dramatically improve the tool's effectiveness. For example, if only one Web application in an environment should accept file uploads, a rule should be set that completely blocks PUT commands (the HTTP command used for file uploads), to all other systems.
3. **Begin with an initial run in passive mode.** Testing out a rule base often requires a "soft launch." With such a strategy, the firewall is placed online with all of its proposed rules. It is then run in monitoring mode without actually blocking any traffic. Before the firewall is actually put into active mode, time should be spent evaluating the traffic that violates the firewall's rules. Those in charge of implementation should also tune the false positive rate before going into production. Since programmers never like it when security systems break their applications, this will go a long way toward improving relations with your developers!
4. **Monitor, monitor, monitor.** Once the firewall is deployed in active mode, it should be watched carefully. The logs created by blocked traffic will tell an important story. Records of the blocked attacks can show management the return on their security investment. There may also be additional false positives, and they can further assist in the fine-tuning of the rule base.

Like network firewalls, application firewalls are not a panacea. Tools such as HP WebInspect and IBM AppScan can be used to test Web applications for vulnerabilities. Complementing these efforts with periodic penetration testing is a solid defensive strategy and can put many security professionals' Web application fears to rest.

Mike Chapple, CISA, CISSP, is an IT security professional with the University of Notre Dame. He previously served as an information security researcher with the National Security Agency and the U.S. Air Force. Mike is a frequent contributor to SearchSecurity.com, a technical editor for Information Security *magazine and the author of several information security titles, including the* CISSP Prep Guide *and* Information Security Illuminated.

CHANNEL

Application Security Expertise a Plus When Offering WAF Services

Web application firewalls require the application security expertise that security solution providers can offer.

BY NEIL ROITER

APPLICATION SECURITY SAVVY solution providers can add valuable services around the selection, implementation and management of Web application firewalls (WAFs) to help customers build effective application and data protection programs.

Few organizations have the expertise to properly implement and manage Web application firewalls, which have emerged in recent years as tools for enabling organizations to meet certain compliance mandates involving data protection. Considering, many companies will depend on solution providers to help them get the most value out of their implementation.

"The market is still very under-educated overall in application security strategy."

–MARK CARNEY, managing director of strategic services, Fishnet Security

"The market is still very under-educated overall in application security strategy," said Mark Carney, managing director of strategic services for Kansas City, Mo.-based Fishnet Security Inc. "It's improving, but not at a pace where the general security community understands the level of care and feeding an application firewall needs and what it takes to make it effective against Web application vulnerabilities."

This may be true even for so-called "check box" compliance deployments that satisfy regulations such as the Payment Card Industry Data Security Standard (PCI DSS) Requirement 6.6, which requires either the implementation of a Web application firewall or, alternatively, manual or automated source code reviews or application vulnerability scans.

PCI DSS requires audits for Level 1 merchants (those that process more than 6 million transactions annually); MasterCard recently added the audit requirement for Level 2 merchants (between 1 million and 6 million transactions annually). Knowledgeable and aggressive Qualified Security Assessors (QSAs) will expect companies to demonstrate that Web application firewalls are implemented properly and are being put to use.

"There are auditors who ask, 'Do you have a Web application firewall?' and then

say, 'OK, check,'" said Brian Monkman, WAF manager for Mechanicsburg, Penn.-based ICSA Labs, an independent division of Verizon Business, which provides vendor-neutral security product testing and certification for security products, including a WAF certification program. "But there are those who ask more specific questions; the longer Web application firewalls are out there and the more mature they get, the more in-depth these questions will be."

Organizations often need help determining how users interact with applications, as well as what critical data the applications can access, said Brian Contos, former chief security strategist for Redmond Shores, Calif.-based application and data security vendor Imperva Inc. Contos is now with McAfee. Partners can offer up-front discovery as a WAF service to determine the applications and data that are in scope.

"Data security has to be much more precise than network security," Contos said. "If you don't know where sensitive data is, it's hard to tell how users interact."

"Data security has to be much more precise than network security. If you don't know where sensitive data is, it's hard to tell how users interact."

–BRIAN CONTOS, chief security strategist, McAfee

WAFs typically "learn" through initial baselining, which involves running a test period to determine what constitutes acceptable behavior, what is questionable and what is malicious.

This represents another opportunity for solution providers, as the test findings must be analyzed and the results reported to the customer. After the results have been analyzed, the solution provider can work with the customer to build custom rules that define what to allow, what to alert on, and what to block, based on corporate policy as well as likely and potential attacks.

"It becomes a very consultative relationship and that's a lot of value add as opposed to just leveraging technology," Contos said.

That's particularly true in large, complex WAF deployments. Experts say VARs should understand the business logic behind an application, as well as technical information about how it works, the development platform it is built on and the programming language it uses in order to best help customers.

"The biggest thing to realize is that applications are complex," said Fishnet's Carney. "They are not as predictable or as straightforward as network-based traffic."

It's especially important to know if new applications are going to be deployed and existing applications changed, he said. The client will either have to be trained in how to modify WAF rules to accommodate the changes, or will have to contract the solution provider for additional services to do it for them.

"The more dynamic the environment, the more care and feeding is required," Carney said.

In dynamic environments, the solution provider can perform penetration testing using Web application scanners to reveal vulnerabilities introduced with the changes. Customers would be best served by WAF deployments that integrate with scanning tools and/or services, Monkman said. For example, WhiteHat Security Inc.'s cloud-

TABLE OF CONTENTS
SELECTION CRITERIA
PCI 6.6
MIDMARKET
FIREWALL MANAGEMENT
CHANNEL
SPONSOR RESOURCES

based application scanning service integrates with a number of leading WAFs. The service (or in other cases, product) can create a "virtual patch," a rule that blocks exploits of the particular vulnerability until the code can be fixed.

This is essential for critical production applications that can't be taken offline. Patches take time to create and test, especially if development is outsourced.

"You need someone who has an intimate understanding of secure coding, of how Web application firewalls and vulnerability scanners work, and how to integrate them," Monkman said.

That combination of expertise is in short supply, presenting an opportunity for solution providers to offer application security practices, in addition to simple WAF deployments.

"Designing security for applications, especially dynamic ones, can be best done when you have a relationship with a partner," Contos said. "As network security is becoming more commoditized, this is one of the areas I would look at for a lot of growth in the future."

TECHTARGET SECURITY MEDIA GROUP

SearchSecurity.com

EDITORIAL DIRECTOR Michael S. Mimoso

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS DIRECTOR Robert Westervelt

SITE EDITOR Jane Wright

ASSISTANT EDITOR Maggie Sullivan

ASSOCIATE EDITOR Carolyn Gibney

ASSISTANT EDITOR Greg Smith

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Nick Dowd

SALES DIRECTOR Tom Click

CIRCULATION MANAGER Kate Sullivan

PROJECT MANAGER
Elizabeth Lareau

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Andrew McHugh, Karina Rousseau

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann
peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Jeff Wakely

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

TechTarget
Where Serious Technology Buyers Decide

"Technical Guide on Web Application Firewalls" is published by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

SPONSOR RESOURCES

WatchGuard

See ad page 2

- Application Control White Paper: Take Back Control – Maintain Security Without Restricting Users
- Reputation Enabled Defense Whitepaper: Reject Threats at the Connection Level, Take the Processing Demands Off Your Network
- UTM Market Review: Compare the major UTM Brands Head-to-Head

IBM

- IBM Service Management Resource Center

Imperva

See ad page 4

- Web Application Security Demo
- Ponemon Institute: State of Web Application Security, 2010
- Web Application Security

GeoTrust

- GeoTrust SSL Solutions
- GeoTrust SSL Products
- Free 30-Day SSL Trial