



Application Intelligence: Expert Guide to Web Application Security Must-Haves

Web application security requirements should align with an organization's overall security policy. In addition, there are some basic steps you can follow to produce a short list of essential security features for any Web application.

In this expert E-Guide, find answers to four key Web application security questions. Also discover best practices for application-level firewall selection and deployment.

Sponsored By:





Application Intelligence: Expert Guide to Web Application Security Must-Haves

Table of Contents:

[Security must-haves after building a Web application](#)

[Best practices for application-level firewall selection and deployment](#)

[Resources from SonicWALL](#)

Security must-haves after building a Web application

By Michael Cobb, featured expert

Question:

We've just finished building a Web application and I'd like to know what security devices you'd recommend to protect it.

Answer:

Without knowing a lot more about the data you're trying to protect and the systems that it interacts with, it's impossible to recommend specific perimeter, network and application data security devices. There are, however, basic steps to follow to produce a short list of essential security features for any Web application.

Firstly, it's important to classify the data that the Web application uses. Where is it stored and how is it accessed and processed? Next, identify and evaluate the risks to this data and the systems and applications that handle it. This process is known as threat modeling and should really be carried out during the application-design stage. By analyzing a Web application from an attacker's point of view, you will gain a better understanding of how and why it may be targeted, and how best to mitigate any identified risks. The process also results in documentation that identifies and justifies the Web application's security requirements.

These Web application security requirements should align with the organization's overall security policy, which defines the objectives of how to legally protect its data. From here, decide how best to protect the Web application against any identified threats and reduce the risk to sensitive information. I have no doubt that rewriting some of the application's code, logic and functionality will remove some of the vulnerabilities. That effort should be supplemented by additional security devices, but your policy and strategy should make it clear what you need these devices to protect and from what.

When looking at threat-mitigation devices after building a Web application, review which types of threats they safeguard against. Some will provide safeguards against multiple threats, such as viruses, spyware and malware. Others may focus on a specific threat subsegment, such as securing instant messaging communication channels. Pay close attention to the depth of coverage and the technical approaches that each vendor uses to provide protection of one or more security areas. One problem with many attacks on application data is that they travel over valid client requests and responses; SQL injection is a classic example of this. Therefore, traditional perimeter defense technologies, such as packet-filter firewalls, are no longer adequate.

Performance and scalability are other important considerations. Some security devices may be limited as to how many transactions they can scan per hour. Other appliances may have networking limitations or only provide capabilities to protect a narrow range of application protocols. I think the key questions to answer when selecting a security device are:

1. What does it need to do based on corporate security policy objectives and requirements?
2. How will it fit into the existing network? Do the in-house skills exist to use it correctly and effectively?

3. How will it affect existing services and users, and at what cost?

4. What additional services does it provide that are of use?

Obviously all devices used to protect or process data need to be installed correctly. Installation needs to follow a four-step security lifecycle: secure, monitor, test and improve. This is a continuous process that, once followed through to completion, loops back on itself in a constant cycle of protection. Before any device is connected to the network, ensure that it has been hardened, applying patches as well as taking the time to configure the device for increased security. Be sure to reference your security policy during configuration to ensure the device is set up to do the job intended and in accordance with corporate security guidelines. Having spent time selecting and installing network defenses, it is important to conduct a penetration test to ensure they actually work as expected and deliver the desired protection. By simulating an attack, you can evaluate whether your site still has potential vulnerabilities.

For future reference, you must, of course, document any changes made based on the findings of a pen test and ensure configurations aren't changed unintentionally or without due process. You must also control physical as well as logical access to all network security devices. Relying just on perimeter security will not keep applications secure. Defenses must be built at every level: physical, network, and critically, application. Using the threat modeling process will ensure that security is also built into Web applications, increasing their resilience and reducing their reliance on perimeter security devices.

[TOUGH QUESTION #3]

HOW DOES ONE OF THE WORLD'S LARGEST AUDITING FIRMS PROVIDE 80,000 SECURE CONNECTIONS?



**SONICWALL
SECURES
THE ENTERPRISE.**

Today's successful companies deliver critical applications in a reliable and secure manner. SonicWALL security solutions provide granular control, proactive protection, and centralized management to meet these needs. With its multi-gigabit Reassembly-Free Deep Packet Inspection firewall, application intelligence and control, and SSL VPN leveraging a GRID network of 4 million touch points, SonicWALL offers the flexibility to economically address key business challenges including mobility, cloud-based applications, and remote connectivity.

[Learn more at sonicwall.com/80kstrong](http://sonicwall.com/80kstrong)



NETWORK
SECURITY



SECURE
REMOTE ACCESS



WEB AND E-MAIL
SECURITY



BACKUP AND
RECOVERY



POLICY AND
MANAGEMENT

SONICWALL™

PROTECTION AT THE SPEED OF BUSINESS™

Best practices for application-level firewall selection and deployment

by Joel Dubin, Contributor

Application-level firewalls have become a hot topic of conversation among those interested in compliance. The Payment Card Industry Data Security Standard (PCI DSS), which had only recommended application-level firewalls as a best practice, will require companies to either install them or conduct code reviews as of June 30.

Nowadays, most organizations have some sort of perimeter firewall that protects the network against malicious Internet traffic, but these types of firewalls aren't equipped to protect organizations against threats that come through applications.

Recently, application-layer firewalls have emerged as a defense against Web application attacks, which are the most common type of intrusion, according to reports by antimalware vendors Sophos plc and Symantec Corp. Traditional network firewalls can't detect application attacks because they piggy-back on open ports used by legitimate applications. Network firewalls check ports and packet headers, but they don't check applications and application data, which can hide malicious activity as it zips through open firewall ports unnoticed. Since most Web traffic goes through either port 80 or port 443, blocking these ports isn't realistic.

PCI DSS has also focused attention on application-level firewalls. The infamous Section 6.6, which covers Web application security, calls for companies to protect code used for processing credit cards by either conducting code reviews of their applications or using an application-level firewall.

Unfortunately, PCI DSS Section 6.6 interprets application security as an either-or proposition, but it's more complex than that. Application security isn't about a code review or a firewall; in some cases it could mean both. Unlike network security, which is about closing ports and turning off unneeded services, application security is about secure coding and design.

As with any security tool or practice, an application-layer firewall should only be seen as part of a larger security program, not as a single defense against Web application attacks. It should be one part of a multi-layered defense that includes application vulnerability, penetration testing and reviewing code for security flaws throughout the entire software development lifecycle.

Selecting and deploying application-level firewalls

There are four features every organization should look when considering application-level firewalls. Let's take a look at these features individually, as well as some application level firewalls on the market today.

First, is it really an application level-firewall, or is it just a deep-packet inspector? The distinction is important. To be compliant with PCI, it must be a real application-level firewall, not an imposter.

A true application-layer firewall inspects the traffic from applications for malicious code, such as SQL injection or cross-site scripting (XSS). Sure, this requires deep packet inspection, but deep packet inspection looks only for things like malware and spyware embedded in traffic, not necessarily at malicious code sent through an application. Unlike traditional network firewalls, which only examine packet headers, deep packet inspection looks inside packets and their contents. While this definitely beefs up the capability of firewalls, and shouldn't be discounted as a defense against attacks, it still has some limitations.

Another common misconception is to confuse application-level firewalls with Web security gateways and content filtering products. Don't turn off your Blue Coat, Vontu or Vericept systems just because you installed an application-level firewall. The two products do different things. Content filtering products block inappropriate websites, or Web-based email, all of which can contain malware. But again, they can't catch Web application attacks, which are only sometimes part of a website's content. Both products may use URL filtering, but an application-level firewall looks for malicious code in the URL, like JavaScript used in XSS attacks, while a content filter only looks at the Web address itself.

Despite that, Web security gateways, content filtering products and application-level firewalls have been slowly blending together into unified appliances. The evolution is natural, as threats have also blended and now require a multi-layered defense. The content filter may or may not block a malicious site, for example, but the application-level firewall will block the malicious code it carries.

At a bare minimum, an application level firewall should protect against injection attacks, like SQL injection and XSS, session hijacking, scanning and crawling, cookie tampering and path traversal attempts. An application-level firewall can block Denial of Service (DoS) attacks by checking for spikes or irregular traffic patterns and should also be able to handle both standard HTTP, as well as SSL traffic.

Second, does the application-layer firewall allow fine-grained protection through access controls? Access controls are a big part of compliance. Not only PCI, but SOX and HIPAA require a full-accounting of who has access to corporate systems and what they have access to. An application-level firewall can play a role in monitoring that access.

The second feature to look for in an application-level firewall is its ability to integrate with identity and access management systems. This allows the firewall to be tuned to allow employee access to certain Web applications, but not anybody else in the organization. Some employees may need access to Web-based email or WebEx to do their jobs. This can be adjusted if the firewall is integrated with the company's directory service, like Active Directory or LDAP. Access to applications can be added to an employee's profile.

An application-level firewall itself, like its network firewall counterpart, should also have role-based access to only allow authorized system administrators access for maintenance and upgrades.

The third key issue for application-level firewalls is their compatibility with a corporation's network. An application-level firewall is another piece of equipment that can be a drag on a network. If not configured properly, or if it's incompatible with corporate architecture, it can cause performance problems. Will it be a drag on your network, slowing down visitors to your web sites, or will it be transparent, as it were invisible on your network?

Generally, application-level firewalls run in tandem with network firewalls, usually behind them inside the network. Incoming traffic passes first through the network firewall, then through the application-level firewall. Always check the firewall's throughput and thoroughly load test it in your environment before considering a full production installation. Any slowdowns, bottlenecks or performance issues should be straightened out before deployment to production.

Finally, just like their network counterparts, application-level firewalls should have the capability to log traffic. Besides being a security best practice, it's essential for tracking down incidents and, in some cases, may be required for compliance. Will the logging be adequate to track down incidents or produce reports of inappropriate access? PCI is strict in its requirement of network monitoring. This is at the heart of an application-level firewall's features.

Application-layer firewalls, like other new security technologies, are becoming more popular and getting absorbed into existing security products. And, as application security becomes more important, their popularity increases. But review products carefully to make sure they use the right features to protect your company from application attacks.

About the author:

Joel Dubin, CISSP, is an independent computer security. He is a Microsoft MVP, specializing in web and application security, and is the author of The Little Black Book of Computer Security, Second Edition, available on Amazon. He also hosts a regular radio show on computer security on WIIT in Chicago and runs The IT Security Guy blog at <http://www.theitsecurityguy.com>.

Resources from SonicWALL



[Lessons Learned From Web 2.0](#)

[10 Cool Things Your Firewall Should Do](#)

[IT Briefing: Mitigating Against Web 2.0 Attacks](#)

About SonicWALL

SonicWALL is committed to improving the performance and productivity of businesses of all sizes by engineering the cost and complexity out of running a secure network. Over one million SonicWALL appliances keep tens of millions of worldwide business computer users safe and in control of their data. SonicWALL's award-winning solutions include network security, secure remote access, content security, backup and recovery, and policy and management technology. For more information, visit the company web site at <http://www.sonicwall.com>.