

Key Operational Issues to Consider for Application Firewalls



EASING THE ADOPTION OF NEW TECHNOLOGY

BY MARK KRAYNAK

THE OPERATIONAL IMPACT of deployment is a primary inhibitor to the adoption of new technology in many companies.

Application and database security is a new topic on the minds of many security groups. A key challenge in evaluating alternative solutions is estimating the cost and time to deploy and manage them.

However, some issues are difficult to anticipate because they emerge only in a broad deployment, while most evaluations are done on a smaller scale than that of the actual deployment. With application security products, the impact of these issues is heightened since many Web and database applications directly affect business operations and revenues. In fact, operational pressures are the top reason cited by managers of unsuccessful firewall deployments.

The following list describes what key deployment and operational questions you should ask your vendor and your project team to help anticipate the issues that might emerge only in a broad deployment, but which affect the ultimate success of your application firewall project.

Does the application firewall protect everything you are trying to protect?

Secondary questions:

What are the key elements of the system you are trying to protect? Does the product provide protection for all components?

Most business applications comprise

at a minimum a “front-end” application (typically a Web application) and a “back-end” database. Increasingly, Service Oriented Architectures (SOA, also referred to as “Web Services”) are being used, primarily for integration between applications and application components. Further, each of these parts typically runs on a standard server platform (i.e., an Apache or IIS Web server) and operating system (e.g., Linux or Windows).

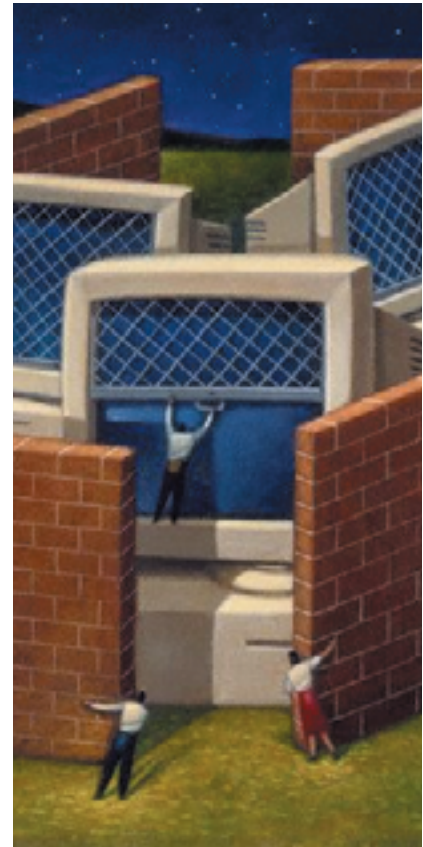
All of these elements of the business application represent a path for attackers to compromise the system. However, many of the products in the application security space are focused on protecting only one element (i.e., only Web applications or only databases). In such cases, solving the whole problem, protecting the business application and its associated proprietary information, can require multiple different security devices. From an operational perspective, this implies the need to train personnel on multiple systems and increases the administrative burden by requiring separate management of the different security systems.

Does the application firewall require changes to the network infrastructure as part of its deployment?

Secondary Questions:

What's the impact of deployment on your IP addressing scheme? On the routing scheme? Are any DNS changes required?

The first task in deploying any application firewall is setting up the network



connectivity. This isn't always as easy as it sounds.

Some application firewalls terminate user sessions to get access to the application traffic for inspection. These devices then open separate connections to the destination server. In these cases, traffic must be redirected to the application firewall (implying re-configuration of the network routers or switches).

Often, application firewalls function in the network as routers, implying changes to the routing design on the network. Depending on the specifics of

the environment, the addition of a new layer of routing can have implications on the IP addressing scheme in use.

Finally, many application firewalls rewrite, or translate, application URLs as part of their operation. This often implies a need to change the configuration of DNS inside the organization, or to propagate new DNS entries to the external DNS servers.

Does the application firewall require changes to SSL certificates?

Secondary Questions:

How does the product “see” into encrypted traffic? Will I have to replace any existing SSL termination products?

Most Internet facing applications use SSL encryption for some or all of the interaction with the users. As such, it's critical that your application firewall is able to inspect the encrypted traffic. Sometimes providing this access can simply be a matter of placing the application firewall behind a separate third-party SSL termination device. But in many cases this isn't an option, so the application firewall must have a mechanism to inspect encrypted SSL sessions.

There are two different strategies for accomplishing this: decryption and termination.

Decryption devices will load the SSL keys from the server application and use this information to decrypt the information without actively participating in the session. Generally, decryption devices require no changes to your SSL infrastructure.

Termination devices have their own SSL certificates and act as the endpoint for the encrypted session, reopening a new session (usually with the option of re-encrypting or sending clear text) to the application server.

The operational implication of this is a need to issue new certificates for the application firewalls and ensure that the certificate matches the correct domains on the user side. If the certificates aren't matched, users will get notice of such when they attempt to login to the application. It's possible to train users

to ignore these prompts, but it greatly increases the likelihood they'll ignore the warning signs of spoofed sites (used, for example, in “phishing” attacks). The result is that new certificates need to be generated, and typically the management overhead for SSL certificates increases.

Does the application firewall require changes to the application code?

Secondary Questions:

Does the product change application URLs? Does the application firewall insert content into application data streams?

Some application firewalls make changes to the application data stream, such as rewriting URLs, signing or encrypting cookies, or even inserting their own “tokens” into the pages of the application. These techniques often imply a need to re-code applications to replace hard-coded IP addresses, or to rewrite JavaScript that accesses cookie information on the client. If the application security product is removed, even temporarily, these changes may need to be reversed to maintain continuous operation.

How much security administrator time and training is required for deployment?

Secondary Questions:

How much knowledge does the administrator need regarding application design? Does the firewall require that you create rules manually? How much does the product assist administrators in developing these rules?

Many application firewalls require a detailed understanding of the application to build and/or tune the security policy by hand. This implies that the security team must work with the developers to understand how to build the rules base and then the security team must communicate these changes to the operations team.

For a new deployment, the level of application understanding required, as

well as the complexity of the application firewall, will dictate how much security administrator time and effort is required. For legacy applications, this level of understanding often doesn't exist in the organization, making it difficult to deploy products that require a detailed knowledge of the applications they protect.

For application changes, how much security administrator time and effort is required for re-configuring and re-testing?

Secondary Questions:

How much does the product automate or simplify the update process?

While most of the administrative effort for changes stems from the same requirements as those for initial deployment, the effort associated with application changes is often overlooked during evaluations. Unfortunately, it's also probably the most common reason for application firewall deployments failing.

In the test lab, or even for initial deployment, vendors or consultants can help with the initial configuration, essentially eliminating deployment issues as a concern, but what many security operations groups don't realize is that applications change far more often than networks and network protocols...how hard is it going to be to keep up?

Application changes may involve changes in modules, functions, URLs, parameter values and lengths, cookies queries, and scripts. Some application security products require manual intervention to account for these changes. ■

About the Author

Mark Kraynak is the director of product marketing at Imperva. Before joining Imperva, he held marketing and consulting positions at Check Point, CacheFlow (now BlueCoat Systems), and Ernst & Young's Center for Technology Enablement. Mark is a regular speaker on application and database security and participates in industry efforts to define the role of application firewalls in security architectures.

mark@imperva.com