WHITE PAPER

Application Security Gateways

Overview

As businesses place more applications on the Web, they expose more of their sensitive customer data to hackers. Browser-based applications tunnel through the entire security perimeter of an organization, giving users unprecedented access to internal systems. It's little wonder that the majority of attacks today target the application directly.

For most organizations, the Web application has in itself become the security perimeter, and the only way to ensure the security of those applications is an Application Security Gateway, also known as an application firewall.

However, Application Security Gateways can only be effective if they are tailored to match closely to an application. Poorly-tailored gateways will inevitably block legitimate user or customer traffic or let in hackers.

F5's TrafficShield, an Application Security Gateway, is a new class of device that protects applications from hackers and other malicious attacks. It enforces granular security policies to protect Web applications as well as confidential information from both random and targeted application security attacks. And thanks to breakthrough technology that automatically generates an extremely accurate model of all legitimate user interaction with an application, TrafficShield is able to filter all application requests and deny anything that is not legitimate user activity.

Challenge

Today every aspect of business is migrating to the Web. Unfortunately, every time a new Web-based application is created, back-end systems previously sheltered from direct access are now connected to the Internet – and potentially the world. The result is that a company's critical data is exposed to an external attack.

Meanwhile, hackers are finding new ways to penetrate traditional defenses. According to a recent CSI/FBI study (Source: Computer Security Institute), 52% of respondents reported company system penetration from the outside in 2004, despite the fact that 98% of the respondents had firewalls in place. Reported financial losses from these attacks – including system penetration, misuse of Web applications, Web site defacement, theft of proprietary information and Denial of Service totaled over $141 million among the 269 company respondents.

Traditional firewalls – which have historically done an excellent job preventing outsiders from accessing company networks – are no longer sufficient. As IDC noted even back in 2002, "firewalls offer little protection at the application layer because ports within the firewall have to be left open for communication."

Recently, the traditional firewall vendors have begun touting 'application-layer security', incorporating functionality from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) into their products. Unfortunately these solutions have proven ineffective for two fundamental reasons:

- **They rely on attack signatures or other patterns of abnormal user behavior.** This leaves systems exposed to new types of attacks ('zero-day attacks'), and threats cloaked as normal traffic. More importantly, it leaves them blind to targeted attacks exploiting the specific vulnerabilities of an application, for which there is no generic pattern.

- **They operate at the network layers, not the application layers.** Despite their claims, many network security products are inherently limited because of the information they are able to interpret. Firewalls and IPS systems look at packets on the wire, not entire requests, so they lack the application-specific knowledge to tell a good request from a bad one. In fact, many cannot even look into simple SSL encryption.

Accordingly, businesses today are being forced to build a high degree of security into the applications themselves. Popular tools such as application scanners help identify obvious holes, but ultimately it's a labor-intensive job to scan and then patch them all. More problematically, scanning can never reveal all application vulnerabilities; there are simply too many parameters to check and too many possible entry points. Developers can patch thousands of holes, but a hacker only needs to find one to inflict major damage.

The ideal solution, therefore, would be to offload the security function to a network appliance that has enough application-specific knowledge to filter out malicious requests. This protection would work like a firewall, but would be based on the application's specific logic, not generic traffic patterns. This type of device would know exactly what the application's traffic should look like, and block anything else. In response to this need, a new class of security solutions called *Application Security Gateways* or *Application Firewalls*, has emerged.

Solution

F5's TrafficShield is a unique Application Security Gateway that provides comprehensive protection for Web servers and Web applications against application layer attacks – not only from the exploitation of known Web application and infrastructure vulnerabilities, but also more malicious, targeted attacks.

Specifically, TrafficShield can stop attacks that no other solution on the market can stop. Take, for instance, two common hacker techniques that pass straight through today's security solutions – even those solutions that claim to feature 'application security' or 'content-aware' blocking:

1. **Hackers enter as one user, then change their ID or escalate privileges once they are past the authentication 'gate'.** The most complex form of this (dynamic parameter tampering) is invisible to nearly every solution on the market.

2. **Hackers change or bookmark the URL of a Web application to enter areas which should be restricted.** Sometimes this is as simple as changing a URL from …/webapp/user to …webapp/admin. More often, the path is convoluted or even buried within an application. Users who are familiar with the application, however, can often guess or detect where to go.

Only TrafficShield can protect against these breaches because it the first to have a comprehensive understanding of the user interaction with the firewall. This means it not only has a very granular understanding of legal activities, but also a firm understanding of the user context (or state) at any given time.

Additionally, TrafficShield's accurate security policy is based on a proprietary model (called the Application Flow Model) which combines automatic analysis of Web page content with iterative adjustments based on real-life traffic analysis.

The Application Flow Model

The best way to enforce a security policy is to have a detailed model (or policy) of the ways users interact with the application. Once you have defined what is legal, all other activities can be declared illegal. An accurate model of the user activity, then, is critical to security enforcement. Without this, the policy with either permit attacks or – more likely – block users who are attempting to perform legitimate activities.

F5's Application Flow Model is a logical representation of the interaction between a legal user and the Web application. For each Web page presented to the user, the model describes the structure of the HTTP requests that are generated by the client-side source code of the Web page and the authorized transitions to other Web pages. The representation of the flow that transfers the user from the browsed (source) Web page to another (target) page includes:

- The current Web page
- The target Web page
- The names of the parameters that can or must appear in the request
- The characteristics of the values allowed for each parameter

The Application Flow Model represents a breakthrough in application modeling because previous approaches only created models of user requests based on scanning user traffic. F5's model automatically 'crawls' the entire application, mapping the flow or total pattern of user interaction with the Web site. This ability to map the application in addition to tracking traffic patterns is far more accurate in modeling user interactions than any other previous methods. The benefits of this model are threefold:

- **Knowledge of state** – Only the Application Flow Model tracks which pages a user is coming from, and the specific permissions associated with that context. A request which is perfectly 'legal' within the context of one page might be inappropriate for a user on another page.
- **Bidirectional** – Only the Application Flow Model looks at server responses to the client as well as client requests to the server. This is essential to verify that the user hasn't attempted to tamper with the credentials sent to him in his response.
- **Granularity** – Only the Application Flow Model creates a complete logical rendering of the transitions between every page, including every object, every parameter of each object, and every legal value within each object parameter.

Building the security policy on the basis of this model allows TrafficShield to verify that the user interaction with the Web application follows the Web application design and enables it to block any attempts that vary from it.

In other words, the Application Flow Model turns the problem of application security into a problem of *protocol enforcement*, which is exactly what firewalls have proven so effective at doing for so many years.

How The Application Flow Model Is Generated

To generate an accurate model and the security policy constraints associated with it, TrafficShield automatically performs an extremely detailed audit of the application's presentation layer, utilizing all available information including both the page's source code and the traffic associated with it.

Needless to say, this is an enormous amount of information to record and model accurately. TrafficShield is able to accomplish this using an innovative hybrid approach, involving two discrete steps:

1. **Automatic analysis of application Web page content** -- TrafficShield uses a sophisticated crawler, purpose-built to probe every aspect of an application. This complete analysis of the Web page content, including active code such as JavaScript, enables TrafficShield to 'learn' the application logic, including all the details of the interaction between the user and the Web application.

2. **Iterative policy adjustment --** TrafficShield then takes this 'snapshot' of the Web page content and examines how users interact with it over time, based on real-life traffic. TrafficShield proactively recommends adjustments to the current policy, based on the on-line analysis of the rejected traffic.

One advantage of TrafficShield's 'iterative analyze and adjust' mechanism is that the Web administrator and the security officer obtain a hands-on understanding of the effectiveness and accuracy of the various parts of a security policy for each application, based on the exact number and types of alarms generated by each URL policy, if there were any. They can monitor TrafficShield's alarms during the 'learning' mode, and only switch to 'blocking' mode once they are 100% confident that no false positives are being generated.

One common question is how TrafficShield deals with updates to the Web application. TrafficShield's policy generator:

- Continuously monitors the Web site content in order to automatically detect changes
- Analyzes the changes and translates them into a series of policy update recommendations
- Applies the suggested updates automatically, or allows the administrator to approve them manually

Note that TrafficShield proactively suggests policy changes. At no time does an administrator have to manually configure all the parameters and flows of the policy.

TrafficShield's innovative, multi-layer inspection mechanism also enables it to block only the requests that are out of compliance with the application's policy. Current solutions that employ single-layer inspection can (and do) shut out entire IP addresses or universally block access to objects. TrafficShield, however, ensures Web security and availability even when those resources are under attack.

Comprehensive Protection Against All External Threats

In order to offer comprehensive protection for the enterprise Web infrastructure, TrafficShield combines robust application-layer filtering with best-in-class network and encryption technology for a complete Web security solution:

TrafficShield Features

Negative Security Attack Filters Protect Against Random Attacks

- Script kiddies
- Known worms and vulnerabilities
- Requests for restricted object and file types
- Other known exploits

Positive Security Protection Against Targeted Attacks

- Manipulation of invalidated input
- Broken access control (Forceful Browsing)
- Buffer overflow
- Cross-site scripting
- SQL/OS injection
- Cookie poisoning

Content Scrubbing

- Identity theft protection for Web servers
- Ensure customer information is never served on a Web page
- Configurable to scrub any identifiable information such as:
    - Social security numbers
    - Credit card numbers
    - Account numbers
    - Patient health data
    - Phone numbers

Network Security Services

- SSL accelerator
- IP/Port filtering
- Reverse proxy
- Key management and failover handling
- SSL termination and re-encryption to Web servers

Cloaking

- Prevent OS and Web server fingerprinting
- Conceal any HTTP error messages from users
- Remove application error messages from pages sent to users
- Prevent leakage of server code

Only TrafficShield combines all these functions into one simple-to-manage device for complete Web application security.

Deployment Options

When deploying TrafficShield in an enterprise or large government environment, the need for security of course must be managed as part of a broader risk profile. Some

applications will require immediate and strict policy enforcement, while others require a more rapid deployment.

TrafficShield can be used in a variety of security postures, from a basic intrusion protection *shield* (requiring just minutes of set-up time) to a complete positive-security *blanket* (requiring application-specific policy building). The ability to be configured at these different security levels provides security administrators with the flexibility to ensure enterprise-wide protection immediately -- without compromising the security for their most sensitive applications.

Enterprise Class System Architecture

TrafficShield's multi-layer system architecture is based on a hardened security appliance designed to meet all of an enterprise's demands for infrastructure security, including:

- Negligible latency (less than 1 ms) and high throughput
- Scalable architecture -- additional units can be added to handle larger traffic volumes
- High Availability -- units can be configured for hot, stateful failover between yoked pairs of servers (an active server and a standby server). In the unlikely event of a server failure, all session data is preserved and the failover to a backup unit is invisible to the user.
- Zero-fault configuration, easy deployment and maintenance -- TrafficShield is composed of optimized and pre-configured appliances that effectively address configuration, deployment, and maintenance issues.
- Central and secure management.
- Easy integration with enterprise security information management or management framework systems.

TrafficShield Business Benefits

Closing the Door On Web Attacks – Obviously the most important benefit of the TrafficShield solution is that it eliminates the risk of cyber-attacks through a company's Web applications. As more systems are opened to Web traffic, more and more sensitive customer data is exposed to threats which current security systems cannot prevent. And once hackers are in, the costs to your business can be staggering – costs that do not take into account the increased insurance expenditures and the legal responsibilities that accrue with deficient security.

Identity Theft and other Regulatory Compliance -- Across industries, new regulations such as the Basel Accords, HIPAA, California's SB 1386 and a host of other national and trans-national regulations are making the security of personal customer data an imperative. Currently, Web applications are the main entry point for hackers seeking customer data. Application-layer attacks that companies know about (certainly only a small portion of the total) cost them hundreds of millions of dollars per year. F5's TrafficShield is an absolute necessity for any company with sensitive customer information.

Improved Time to Market -- In addition to preventing hacks, TrafficShield can actually improve the development cycle for new applications. Right now, the deployment of new applications is hampered by the 'scan-and-fix' cycle of application security scanning tools. Code is written, scanned by one of several off-the-shelf products, then sent back to the developers to be re-written. Not only is this costly and time-consuming, it is ineffective, as scanners can only detect a limited set of known security breaches. With a product like TrafficShield, the development team can focus on rapid development of new applications and functionality, knowing that their code will sit behind a powerful security perimeter.

Plug and Protect -- The TrafficShield solution delivers on the promise of a "plug and protect" appliance. TrafficShield is delivered as a network device, which can be easily nested in a company's Web infrastructure. Once installed, the proprietary, automated learning mechanism quickly and accurately builds security policies tailored to the unique specifications of the applications it protects. Policy management and configuration are minimal, as TrafficShield automatically generates recommendations, rather than waiting for manual configuration.

Easily Quantified Return on Investment

The benefits of an application-layer security solution such as TrafficShield can be easily quantified. TrafficShield will slash costs related to security enforcement, attack damage, and damage response. Consider the savings associated with the following:

No Attack Incidents -- In addition to the costs of the attacks themselves (stolen funds, lost revenue) companies have extensive costs associated with responding to the attack and repairing the damage. This response is not limited to the IT department, as it can involve public relations, litigation, and even regulatory costs.

No Code Rewrites -- Without adequate protection around their application, application developers are forced to scour their applications for individual security holes, and hard-code plugs for those holes. Application scanners can detect some of these, but rigorous code review and rewriting is always necessary. Once TrafficShield is in place, developers can focus on the rapid deployment of new applications and new functionality.

No Reactive Patching -- Knowing that applications are often open to direct attacks, IT managers constantly monitor sites and company announcements to immediately install the latest patches. As mentioned above, a secure application firewall ensures that only legal activity is permitted on an application, reducing the reliance on patches.

No False Positives -- Blocking customers from their accounts while they are conducting legal transactions is a good way to lose those customers. Without an accurate model of legal activity (such as the Application Flow Model), companies face the tough choice of relaxing security protocols and letting in hackers, or tightening them and blocking customers.

About F5 Networks

F5 enables organizations to successfully deliver business-critical applications and gives them the greatest level of agility to stay ahead of growing business demands. As the pioneer and global leader in Application Traffic Management, F5 continues to lead the industry by driving more intelligence into the network to deliver advanced application agility. F5 products ensure the secure and optimized delivery of applications to any user - anywhere. Through its flexible and cohesive architecture, F5 delivers unmatched value by dramatically improving the way organizations serve their employees, customers and constituents, while lowering operational costs. Over 6,000 organizations and service providers worldwide trust F5 to keep their businesses running. The company is headquartered in Seattle, Washington with offices worldwide. For more information go to www.f5.com.