WEB APPLICATION SECURITY FOR THE DATA CENTER

Securing Applications From Threats Requires An Integrated Solution That Enhances Enterprise Firewall And Intrusion Prevention Technologies
INTRODUCTION

Most organizations focus their limited resources on locking down access and controlling their networks to protect their data centers from external threats. The latest generation of enterprise firewalls and intrusion prevention systems (IPS) primarily focus on securing the network and controlling access to it. These are great technologies, however there are limits to what they can offer to provide complete protection against threats that target applications, application services, and users.

As soon as an application is opened to the Internet, it is a target. All that stands between an attacker and an organization’s sensitive data is an unassuming login screen. No matter how many layers of network security are in place, this entry point could expose customer data, proprietary information, or sensitive financial information if the application hasn’t been hardened or protected by some other means.

In this solution guide we’ll explore the top challenges organizations face when it comes to securing applications and the data they host, including web application vulnerabilities, advanced persistent threats (APTs), and scaling application encryption.

APPLICATIONS ARE EASY TARGETS

There is no question that a firewall is your first line of defense for network security. Today’s latest firewall technologies are almost bulletproof, at least at the layer 2 and 3 levels. Attackers and cyber criminals know this and have had to adapt their techniques. Not that they won’t try to look for firewall vulnerabilities, rather they know that high-value targets like financial institutions, retailers, and government agencies have tightened their security policies and the days of easy data breaches at the firewall are over.

The fastest growing categories of attacks and data breaches are those that target applications, and application layer services. These represent many of the remaining weak spots and there are countless possibilities to exploit code vulnerabilities, and application modules.

WEB APPLICATION ATTACKS

Verizon’s 2017 Data Breach Investigations Report revealed that over 40 percent of all data breaches were caused by web application vulnerabilities. The Open Web Application Security Project (OWASP) has consistently reported since 2010 that almost every web-based application has one or more vulnerabilities listed in their Top 10 list of application security risks. They have also reported that 95 percent of all websites are attacked annually using cross-site scripting and injection techniques. Acunetix, an industry leading web application vulnerability scanning provider, noted that in 2016, 55% of their customers’ websites have at least one critical vulnerability that can be exploited for an attack.

PROTECTING APPLICATIONS FROM APTS

APTs are custom-developed, targeted attacks. They can evade straightforward detection, using previously unseen (or “zero-day”) malware, exploit vulnerabilities (unpatched security holes), and come from brand-new or seemingly innocent hosting URLs and IPs. Their goal is to compromise their target system with advanced code techniques that attempt to circumvent security barriers and stay under the radar as long as possible.

Web-based applications can be a significant vector in APTs. Many web applications allow the uploading of files that could be risks. Antivirus scans can check for previously identified attack types, however APTs generally are tailored to circumvent traditional AV detection and many slip past this first line of defense.

SECURE APPLICATION TRAFFIC GROWTH

Although not a threat, many enterprises are aggressively expanding SSL to all their web-facing applications. Even seemingly benign applications are getting the “secure” treatment in order to patch known or unknown vulnerabilities to other more important systems. Sandvine’s Encrypted Traffic Report 2016 saw encrypted traffic volume increase to 30 percent in 2015 and estimated 50 percent growth in 2016. Combined with this explosive expansion in traffic, the complexity of moving to more advanced encryption keys as the technology expands from 1,024 keys to 2,048 and now 4,096, is doubling and even quadrupling secure packet sizes. Servers and load balancers are struggling to keep up with this demand using today’s current crop of secure application delivery solutions.

COMPLETE APPLICATION SECURITY EXTENDS PAST THE FIREWALL

Each of the areas presented in the previous section provide unique challenges that need more than a firewall or an IPS to completely address. Most firewall and IPS systems today, including our FortiGate product line, have features that can solve many of these new problems. However, in general they are limited to signature detection and need additional solutions to provide complete protection for unknown and zero-day attacks. FortiGate has many services that can be enabled such as deep packet inspection and data loss prevention (DLP), but even with those, there are still loopholes and there are performance impacts that need to be considered in enterprise deployments.
Backdoors to Your Firewall and IPS

Even advanced firewalls and IPS systems can’t completely protect your network and applications from today’s latest threats. Attackers have adapted to exploit vulnerabilities that traditional firewalls weren’t designed to detect.

The most used application-level protection features of FortiGate and other firewalls are IP reputation and signature detection. Usually subscription-based services, IP reputation and attack signatures are very effective measures that block attacks before any processing is applied by the firewall. If an attack is from a known source or it matches a predefined signature, it is blocked automatically without the firewall having to perform any further inspection. FortiGate offers these services through our award-winning FortiGuard Labs.

Although these are very effective to block attacks from known sources and previous attack patterns, zero-day and APTs bypass these detection systems. In some cases APTs are so customized, that malicious code is developed specifically for a single target with no forewarning until the malware is deployed. Signatures and IP reputation also can’t fully protect web applications from attacks as many code-based vulnerabilities have almost unlimited ways to bypass any predefined signatures.

In the face of these threats, Fortinet has risen to the occasion with purpose-built solutions to supplement the protections in firewalls and IPS platforms. These include web application firewalls for application security, advanced application delivery controllers (ADCs) to meet the demands of secure application traffic, and sandboxing integration to isolate malicious code for inspection.

PCI COMPLIANCE, FIREWALLS, AND WAFS

We’ve done our best to highlight the case that you’re going to need more than a firewall to completely protect your applications and data. If you’re in one of the many industries that deal in e-commerce and banking, you must consider PCI compliance for your network and application security.

Although PCI DSS standards are not directly mandated by law, many laws, especially at the state and local level, specifically mention PCI compliance to meet legal requirements. A firewall alone is not going to be enough. To pass PCI DSS 6.6 compliance, you’re going to need a web application firewall to meet all the OWASP Top 10 Application Threats that are referred to in that section. Below is a list of the OWASP Top 10 and how a WAF stacks up against a firewall.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Firewall</th>
<th>WAF</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Injection (SQL, OS, and LDAP)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2 Broken Authentication and Session Management</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>3 Sensitive Data Exposure</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4 XML External Entities (XXE)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5 Broken Access Control</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6 Security Misconfiguration</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>7 Cross-Site Scripting</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>8 Insecure Deserialization</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>9 Using Components with Known Vulnerabilities</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>10 Insufficient Logging and Monitoring</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
APPLICATION SECURITY SOLUTIONS

Fortinet is much more than our enterprise-class FortiGate firewalls. We offer many solutions that provide network and application security for a data center. The following section covers many of the advanced threats and challenges that data centers face today along with the solutions offered by Fortinet. For more details on the products presented, white papers, case studies and other useful information, please visit [Fortinet.com](http://Fortinet.com).

Fortinet’s Web Application Security Solution

Fortinet’s Security Fabric enabled Web Application Security Solution delivers a high-performance set of products that protects an organization’s valuable information throughout the data center by using a combination of Fortinet web application firewalls and application delivery controllers.

WEB APPLICATION SECURITY THREATS

- Public facing applications are attractive targets
- Sensitive customer and proprietary data exposed
- Almost every web application has vulnerabilities
- Firewalls and IPS can only detect known threats
- 95 percent of all websites have experienced cross-site scripting and SQL injection attacks

WEB APPLICATION VULNERABILITY PROTECTION

Web applications are attractive targets to hackers as they are public-facing applications that require being open to the Internet. As many provide major e-commerce and business-driving tools, they can contain cardholder, company, and other sensitive data.

Perimeter security technologies such as IPS and firewalls have focused on network and transport layer attacks. Many vendors, including Fortinet have added application layer enhancements, usually referred to as “Deep Packet Inspection” (DPI) to extend signature detection to the application layer. Although DPI is useful in protecting against attacks on the web server infrastructure (IIS, Apache, etc.), it cannot protect against attacks on custom web application code such as HTML and SQL.

WEB APPLICATION FIREWALLS (WAFS)

Securing web applications requires a completely different approach than signature detection alone. Only a web application firewall can provide complete application protection by understanding application logic and what elements exist on the web application such as URLs, parameters, and what cookies it uses. Using behavioral monitoring of application usage, the WAF can deeply inspect every application in your data center to build a baseline of normal behaviors and trigger actions to protect your applications when anomalies arise from attacks.
FortiWeb Web Application Firewalls provide specialized, layered web application threat protection for medium/large enterprises, application service providers, and SaaS providers. FortiWeb Web Application Firewalls protect web-based applications and Internet-facing data from attacks and breaches. Using advanced techniques it provides bidirectional protection against malicious sources, DoS attacks, and sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, file inclusion, cookie poisoning, and numerous other attack types.

- WAF throughputs ranging from 25 Mbps to 20 Gbps
- Multiple, correlated threat detection methods include protocol validation, behavioral identification, FortiGate quarantined IP polling, and subscription-based FortiGuard IP reputation, antivirus and web attack signatures
- Included vulnerability scanner and support for virtual patching with third-party scanner integration
- Sandbox integration for protection from Advanced Persistent Threats
- Simplified deployment with automatic setup tools and integration with FortiGate

**SECURE APPLICATION DELIVERY**

Users have come to expect applications to be there when they need them and to respond immediately. It is a given now that they also expect that you are protecting their and your organization’s sensitive data. In order to provide the security that almost every application needs, data center managers are deploying SSL on almost every application, however this comes at a cost in user capacities, speed, and latency.

As mentioned previously, the trend in secure traffic growth will strain even the best-architected data centers to keep up with this demand. Coupled with this is that SSL encryption keys are getting more complicated as they expand from the older 1,024-bit keys to 2,048, and now 4,096.

**ADCS WITH SSL OFFLOADING**

Application Delivery Controllers (ADCs) offer the feature to offload SSL traffic from servers to the ADC itself. Most manufacturers can do this using software encryption and decryption, however only hardware-accelerated appliances have the dedicated ASIC processors to handle the speeds of a modern data center. Most software-based devices can handle a few hundred to a few thousand transactions per second vs. hardware-based appliances that can manage tens-of-thousands of secure transactions per second.

By offloading this processor-intensive traffic from the servers to the ADC, secure applications can scale up to 100 times while at the same time reducing response rates for end users.
FortiADC hardware and virtual ADCs provide unmatched server load balancing performance whether scaling an application across a few servers in a single data center or serving multiple applications to millions of users around the globe. With included SSL offloading, HTTP compression, global server load balancing, firewall, and link load Balancing, they offer the performance, features, and security needed at a single all-inclusive price.

- L4 throughput from 500 Mbps to 60 Gbps.
- Complete layer 4 to 7 server load balancing solution with intelligent policy-based routing
- Web application firewall and IP reputation (subscriptions required)
- Scripting for custom load balancing and content rewriting rules
- Antivirus and FortiSandbox integration to detect infections and APTs in web application file attachments
- SSL forward proxy for increased secure traffic inspection with FortiGate firewalls
- Qualified for Microsoft Exchange and Skype for Business

**ADVANCED THREAT PROTECTION FOR APPLICATIONS**

Malware can come in any form and can be one of the most difficult threats to detect. Some forms of it can be simple to detect as they may route a user to a website to download malicious code. Newer methods are much more obfuscated and rely on many different vectors to infect users or data center infrastructure elements.

This complexity, combined with the almost limitless options for zero-day malware attacks can make it almost impossible for firewalls and IPS systems to detect all these threats. Additionally, many of them may be buried in seemingly harmless code that in some cases may take years to be fully exposed.

**SANDBOXING**

Even with the best threat detection defenses, sometimes it’s just best to let the code “explode” to see what it’s going to do. This is where a sandbox comes in and acts like a bomb squad. The suspicious code is isolated in a virtual bomb detonation chamber and allowed to do what it was intended to do. Since the sandbox is completely isolated from your network and applications, if the code is malware, it’s not going to do any harm to your real environment.

Once the code is extracted and installed in the sandbox, it’s easy to examine the changes it makes to do the damage it was intended to do. If it is assessed to be a threat, the malware is quarantined and blocked from entering your network.

**FORTISANDBOX AND FORTICLOUD SANDBOX – ADVANCED THREAT DETECTION**

With the increasing volume and sophistication of cyber-attacks, it takes only one threat to slip through security for a data breach to occur. CISOs have adopted sandboxing as an essential component of their security strategies to help combat previously unknown threats.

While attack surfaces are becoming more dynamic due to the rise of IoT and cloud-based services, a continuing shortage of cyber security talent is driving organizations to integrate sandboxing with greater controls and a high degree of automation.

FortiSandbox and FortiCloud Sandbox are a key parts of Fortinet’s integrated and automated Advanced Threat Protection solution.

- Critical protection against advanced and emerging threats
- Automated sharing of threat intelligence in real time to disrupt attacks early in the cycle without human intervention
- Broad integration with Fortinet and third-party security solutions to help protect an organization’s dynamic attack surface
- Flexible form factors to help support various industry requirements
INTEGRATED APPLICATION SECURITY WITH THE FORTINET SECURITY FABRIC

Only Fortinet can offer the security, performance, and integration for a total network and application security solution that can meet the needs of your data center. Starting with the award-winning FortiGate firewall as a foundation, Fortinet offers the additional products and services you need to provide complete protection that goes beyond firewalls to protect your applications, users, and sensitive data.

No matter how complex your needs are, a comprehensive Fortinet security solution that includes WAF, application delivery, and sandbox integration is easy to setup and manage. We provide you the tools you need to centrally manage your Fortinet solutions and tools for consolidated threat analysis and reporting.

Fabric-enabled Web Application Security

- One vendor
- Integrated Security
- Only from Fortinet

SUMMARY

A firewall is the first line of network defense in your data center, however many new trends that target applications and end users require additional protections that a firewall or an IPS can’t provide. Signature-based detection, IP reputation, and deep packet inspection can stop some of these advanced threats, but they are limited in what they can offer. Additional products like web application firewalls, application delivery controllers, and sandboxing are needed to address these new threats to your data center and users.

Fortinet offers a wide range of products that not only complement our class-leading FortiGate firewalls, they also are designed to work together seamlessly in Fortinet’s Security Fabric ecosystem. For more information on the products presented in this white paper, please visit Fortinet.com.