SOLUTION BRIEF

Fortinet Web Application Security for the Cloud

Executive Summary

Cloud-based web services are essential but also vulnerable to cyberattacks. The Fortinet Security Fabric provides a fabric-based approach that uses machine learning (ML) to detect and block those attacks, which improves over time, to ultimately achieve nearly 100% accuracy. Elements in the Fortinet Security Fabric that are involved include virtual next-generation firewalls (NGFWs), a threat update feed, and a cloud-based sandbox. These work together to protect cloud-based web services.

Fabric-Based Web Services Protection:

- Blocks attacks with near-100% accuracy
- Dual machine-learning engines minimize false positives
- Includes virtual firewall, threat update feed, and cloud-based sandbox

Problem: Protecting Cloud-Based Web Services

Typically, cloud-based applications use web services to communicate inside as well as outside the cloud. This increases risk: 48% of all data breaches are caused by hacking of web-based applications.[1] Also, 94% of all web applications have high-severity vulnerabilities.[2]

"Many of the features that make web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are at odds with traditional security models and controls," notes the National Institute of Standards and Technology (NIST) Guide to Secure Web Services.[3]

Solution: Fabric-Based Security for Multi-Cloud Protection

Protecting web services requires going beyond the traditional security model of using point security solutions that usually do not work together. What is needed is a security-fabric-based approach that uses open standards and protocols to integrate different security devices into a single security system—one that can span a multi-cloud network. This is the Fortinet Security Fabric.

Rather than following the hub-and-spoke structure of the multi-cloud network, the Fortinet Security Fabric creates a meshed security network in which all the security functions can communicate among themselves, coordinated by a central management console. The elements of the Fortinet Security Fabric work together to protect web services in cloud-based applications. Following is a closer look at the elements and how they work.

FortiWeb-VM is a purpose-built, industry-leading web application firewall (WAF) offered on all major cloud platforms. It helps secure web services APIs as well as protect web applications from known and unknown threats. It also uses ML to minimize unwanted false-positive detections.

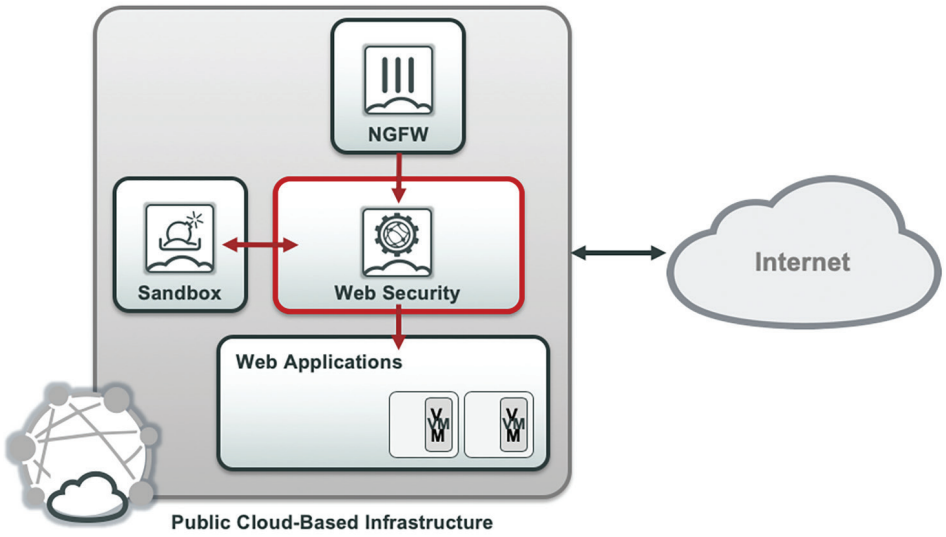

Figure 1: Securing web-based applications in the cloud. When FortiWeb detects a threat, a FortiGate NGFW can block it, or if it is a suspected zero-day threat, it can be passed to the FortiCloud Sandbox Service to detonate and analyze. FortiCloud would then update other elements of the Fortinet Security Fabric about the threat.

This is a different approach than traditional WAFs, which use application learning to observe applications and build policies based on their behavior. Any behaviors outside those policies trigger alerts. This generally leads to false positives that are resource-intensive to investigate.

Instead of using application learning, FortiWeb uses a unique ML approach that employs two separate detection engines. The first uses a statistical model to determine whether an HTTP request varies significantly from those previously observed. A request straying too far from normal is flagged, but instead of being blocked, it is sent for additional analysis to FortiWeb's second ML engine to determine whether it is a threat or simply a benign variance (such as a typo). The ML statistical model is pre-trained to evaluate events like this, learn from them, and achieve nearly 100% accuracy that improves over time.[4] The model is updated with the FortiGuard Web Application Security Service to provide protection from new threats that require retraining and testing.[5]

FortiWeb packaged rulesets are security signatures that can be used to enhance the protections included in base WAF products provided by cloud vendors. The rulesets are based on FortiWeb WAF Security Service signatures and are updated on a regular basis to include the latest threat information from the award-winning FortiGuard Labs. API-specific FortiWeb rulesets are available to enhance multi-layer security protection at the API level.

Additional Security Fabric Elements Safeguard Web Services

When FortiWeb detects threats, **FortiGate-VMs** block them. FortiGate-VMs are virtual FortiGate NGFWs, and they monitor and enforce virtual traffic on leading virtualization, cloud, and SDN platforms, including VMware vSphere, Hyper-V, Xen, KVM, Azure, and AWS. FortiGate-VMs provide firewall, intrusion prevention, VPN, antivirus, and other consolidated security functions for virtual workloads.

FortiCloud Sandbox Service performs dynamic analysis to identify previously unknown malware. Actionable intelligence generated by FortiCloud Sandbox is fed back into preventive controls within an organization's network to disarm the threat.

Web services are essential to cloud operations, and the Fortinet Security Fabric offers the broad visibility, integrated protection across multiple clouds, and automated operations that are essential to protecting web services.

[1] "2018 Data Breach Investigations Report," Verizon, March 2018.

[2] "94 Percent of Web Applications Suffer From High Severity Vulnerabilities," SecurityIntelligence, April 19, 2018.

[3] Anoop Singhal, et al., "Guide to Secure Web Services," National Institute of Standards and Technology (NIST), August 2007.

[4] Mark Byers, "FortiWeb Release 6.0: AI-based Machine Learning for Advanced Threat Detection," Fortinet, June 5, 2018.

[5] "FortiWeb 6.0: AI-based Web Application Threat Detection," Fortinet, accessed March 15, 2019.

March 19, 2019 8:39 AM

357565-0-0-EN

D:\Fortinet\Work\March\031819\sb-web-application-security-for-security-architect