Web Application Firewall

Ext.prc.002.02 | 01.06.2024

UPM 24.x

ZINFI Confidential & Proprietary
Shared Under NDA

Contents

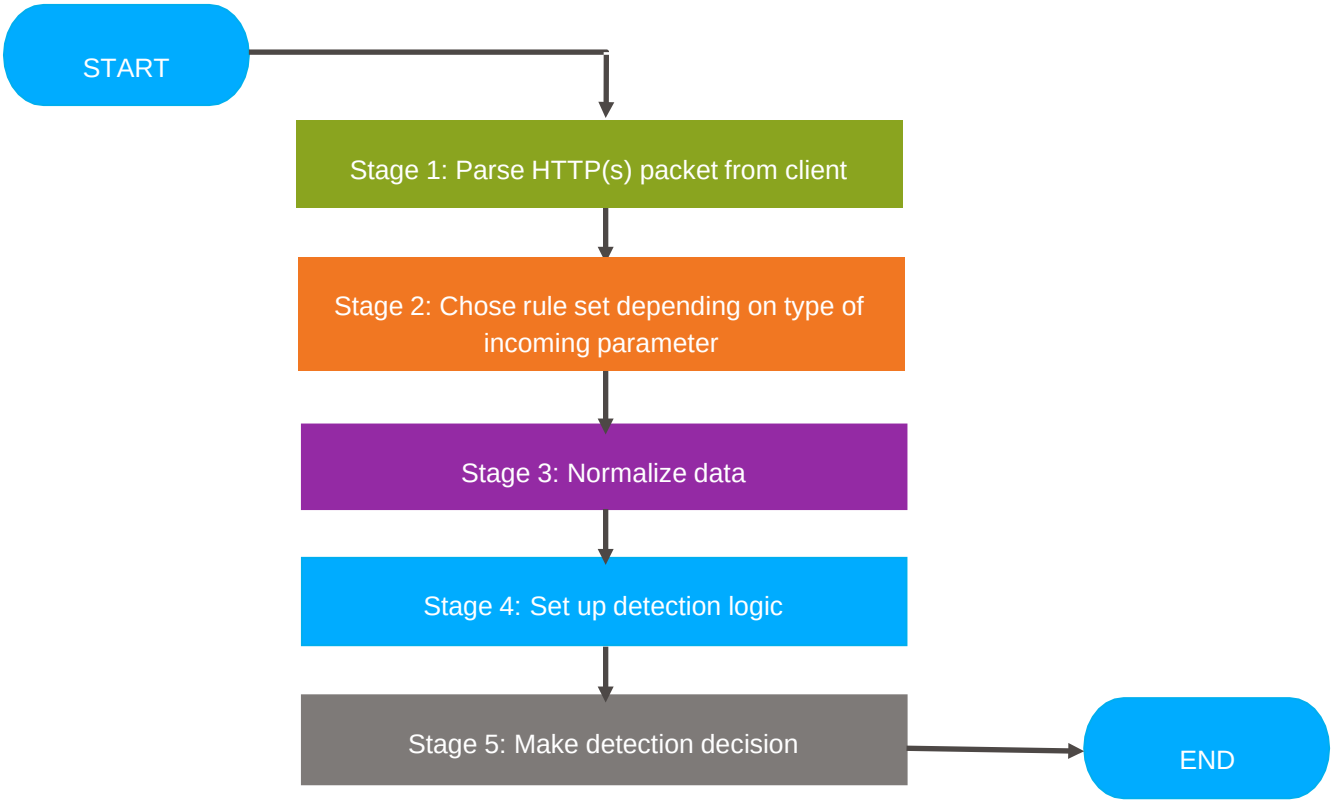
Introduction

Attacks on web-based applications and servers are more complex and frequent than ever. The ZINFI Unified Partner Management (UPM) platform's web application firewall (WAF) provides comprehensive, application layer security, virtually eliminating these problems and rigorously protecting UPM instances from such threats. UPM's WAF provides full protection from most of the threats identified by the Open Web Application Security Project (OWASP) and has been specifically designed to protect UPM instances and their underlying infrastructure, including servers, plug-ins, protocols, network connectivity and more.

UPM's WAF is designed as a shielding safeguard intended to defend UPM instances accessed via the hypertext transfer protocol (secured) (HTTP/HTTPS). It is capable of preventing attacks that network firewalls or intrusion prevention systems cannot. The WAF is layered on top of the UPM web application and is capable of monitoring application activity, issuing alerts and blocking traffic that is malicious or that does not comply with specific rules.

This shielding technology does not require modification of UPM's source code. WAFs can reduce risk without actually fixing the underlying vulnerability. In cases where it might take a long time or it is otherwise infeasible to fix the vulnerability in code, UPM's WAF is still indispensable in protecting against attacks.

UPM's WAF Workflow



UPM's WAF Architecture

Negative Security Model

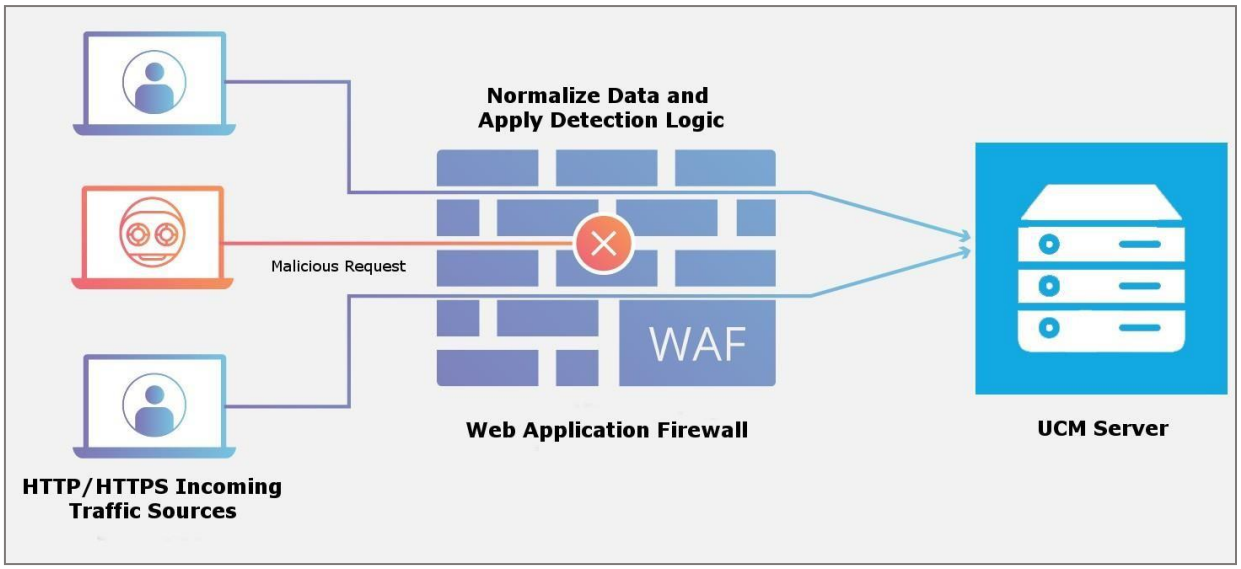
UPM's WAF compares requests to generic attack signatures and application-specific policies for the UPM instance being protected, and issues alerts or blocks violations. Web application firewalls generally follow a positive or negative security model to develop security policies for an application.

A positive security model defines what is allowed and rejects everything else.

UPM WAF's negative security model defines what is disallowed and implicitly allows everything else. This is referred to as blacklisting. The negative security model is achieved by compiling a list of attack signatures, comparing web traffic against those signatures, and blocking traffic that matches. Because the negative security model does not need to know anything about the UPM application, it offers out-of-the-box protection.

Deployment Model

Server Resident — The server resident or embedded WAF is an integrated layer on the host running the web server. UPM's WAF is implemented as an independent application. The embedded WAF removes the additional network point of failure, but puts an extra load on the server, and an important analysis is made with respect to server resource utilization prior to implementation. The architecture is shown in the below figure. The WAF, represented by the shield, is functioning as an application on the web server.



Virtual Patching

Virtual patching is a security technique that ZINFI incorporates in the secure software development lifecycle (SDLC) to ensure UPM application instances remain free of security vulnerabilities. Once identified, vulnerabilities take time to fix. In the process, we necessarily take development time away from creating new functionality to devote time to fixing a security issue. This is a costly endeavor at best. To address this problem, we utilize the WAF to help remediate UPM application vulnerabilities without the need to change the application's source code.

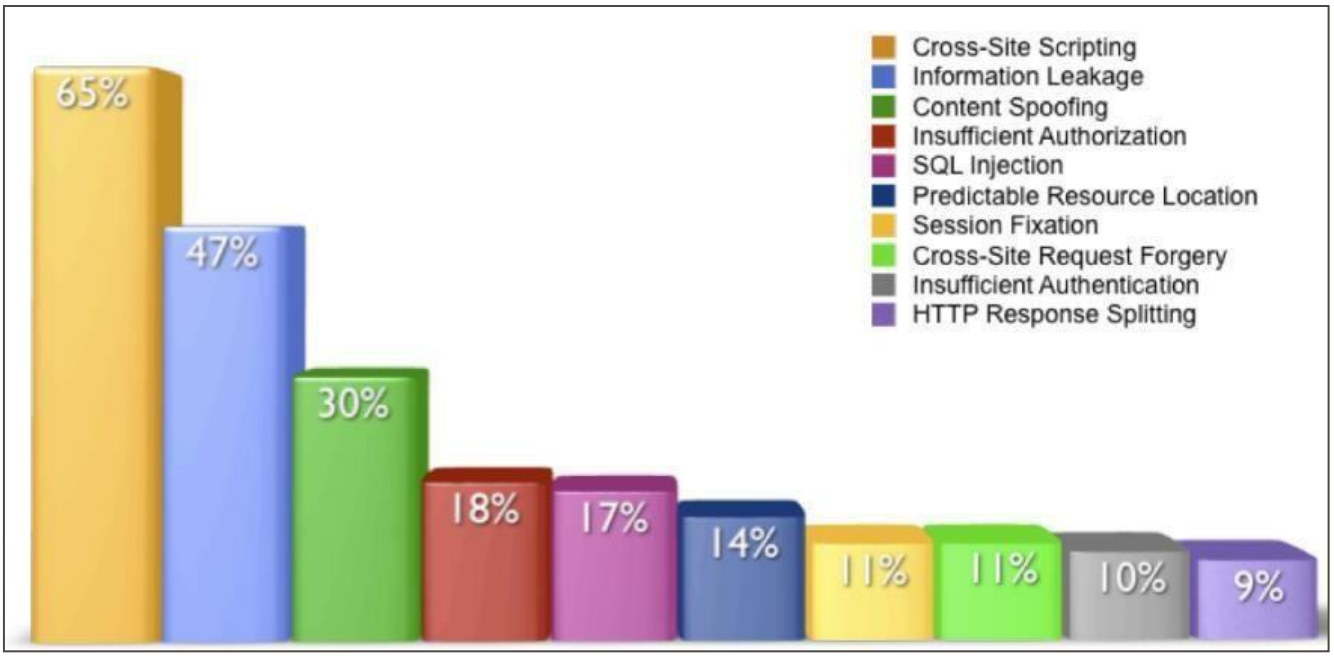
Virtual patching is generally defined as a security policy enforcement layer that prevents the exploitation of a known vulnerability. Given a custom rule that addresses a specific vulnerability, UPM's WAF can analyze transactions and intercept attacks in transit so the malicious traffic targeting the vulnerability never reaches the UPM application.

Cross-site scripting (XSS) attacks are a type of injection attack where an attacker sends a malicious script, typically browser-side JavaScript, through a web application to another end user. The user's browser then executes that script, and the malicious code carries out its nefarious purpose. XSS can be used to hijack user sessions, deface web sites, insert hostile content, redirect users and hijack the user's browser using malware.

In this context, virtual patching is best at:

- Applying protection to UPM application vulnerability by adding a new signature or policy to prevent the vulnerability or by importing vulnerability findings into the UPM's WAF for policy remediation.
- Blocking attempts to exploit known vulnerabilities.
- Narrowing the window of exposure while patches are thoroughly tested and deployed.

Drivers



Architectural Features

Security	Benefits
Deep Packet Inspection, covering applications / Layer 7	Ensures UPM application instance is always protected from SQL injection, cross-site scripting attacks and thousands of other attack vectors.
SSL	Terminates SSL connections without any overhead or additional latency. Applies our UPM's WAF policy to SSL-encrypted traffic without having to upload certificates or invest in costly hardware solutions.
For GET and POST HTTP/S requests	Covers range of HTTP/S traffic.
URL-specific custom rule sets	Allows us to include/exclude specific URLs or subdomains for UPM's WAF protection to test domains or include/ exclude specific subdomains.
DDoS mitigation integration	Allows full-stack protection against DDoS.
IP reputation database integration	Real-time intelligence on over 1 billion unique IPs used to block malicious traffic.
Restrict by IP or geolocation	Blacklists/whitelists traffic from specific IP addresses or countries to protect against hackers from specific IPs or countries
Full integration with CDN service, offering outbound content transformation	Reduces web latency.

Intrusion Detection and Incident Response

UPM's WAF serves as a kind of network of sensors to UPM's security monitoring infrastructure. It collects data and alerts on potentially malicious traffic for analysis in the detection phase of intrusion detection and incident response. The alerts and logs from UPM's WAF are sent to our security incident and event management IT department for correlation, enhancing and expanding monitoring activities to web traffic. Our UPM's WAF gives the best visibility into the UPM instance's application traffic and potential attacks.

