WAF Concept Guide

FortiWeb

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 10, 2025
FortiWeb WAF Concept Guide

TABLE OF CONTENTS

What is Web Application Firewall? **4**
Intended Audience 4
About this guide 4
WAF Concepts **6**
Key Components of FortiWeb **7**
WAF features against OWASP Top 10 risks 7
WAF features against OWASP Top 10 API security risks 18
WAF features against OWASP Top 10 Client-Side security risks 24
WAF features against bot attacks 27
Conclusion **35**
More information **36**

What is Web Application Firewall?

A Web Application Firewall (WAF) is a specialized security solution designed to protect web applications by filtering and monitoring HTTP/HTTPS traffic between a web application and the Internet. It protects the web application from various cyber threats such as cross-site scripting (XSS), SQL injection, and other common web exploits.

Unlike traditional firewalls that focus on blocking unauthorized access at the network level, WAFs operate at the application layer (Layer 7 of the OSI model), inspecting incoming and outgoing traffic based on predefined security rules. By analyzing requests, WAFs can detect and mitigate malicious traffic in real-time, helping to safeguard web applications from vulnerabilities that could be exploited by attackers, thus enhancing overall web security and compliance.

FortiWeb, Fortinet's web application firewall (WAF), combines traditional WAF features with advanced security mechanisms like machine learning, behavioral analysis, and integration with threat intelligence services. It provides a comprehensive defense against the evolving security challenges that web applications face.

Intended Audience

This guide is intended for an audience who is interested in learning about Fortinet’s Web Application Firewall. Readers should have a basic understanding of networking and security concepts before they begin.

Interested audience may include:

- **Network Security Engineers** – Responsible for configuring, managing, and optimizing FortiWeb to secure web applications.
- **Web Application Security Specialists** – Focus on protecting web apps from OWASP Top 10 threats like SQL injection, XSS, and SSRF.
- **Network Architects** – Design secure network infrastructures, ensuring FortiWeb is properly integrated with other security solutions.
- **IT Administrators** – Handle day-to-day firewall and WAF rule management, ensuring policy enforcement and compliance.
- **SOC Analysts & Incident Responders** – Monitor logs, analyze FortiWeb alerts, and respond to security incidents.
- **MSSP Security Teams** – Managed Security Service Providers (MSSPs) who configure FortiWeb for multiple clients.

About this guide

This guide aims to provide a broad overview of WAF concepts and step by step configurations on FortiWeb to prevent common attacks. It covers the following topics:

- **Introduction to Web Application Security Threats** – Learn about common attacks (e.g., OWASP Top 10) and how they impact web applications.
- **How FortiWeb Protects Against These Attacks** – Understand FortiWeb’s key security features and how to configure them.
- **Terminology & Best Practices** – Get familiar with FortiWeb-specific terminology and security concepts to prepare for deployment.

WAF Concepts

First, let's explore the key WAF concepts we need to understand.

- **OWASP Top 10 Risks**

  The OWASP Top 10 is a widely recognized list of the most critical security risks affecting web applications. It highlights vulnerabilities such as injection attacks (SQLi, XSS), broken authentication, security misconfigurations, and server-side request forgery (SSRF). Organizations should use this as a baseline to harden their applications, implement WAF protections, and follow secure development practices.

  For use cases, see WAF Solutions against OWASP Top 10 Risks.
- **OWASP API Security Top 10 Risks**

  The OWASP API Security Top 10 focuses on vulnerabilities specific to APIs, which power modern web and mobile applications. Risks include broken authentication, excessive data exposure, improper rate limiting, and mass assignment attacks. Since APIs handle sensitive data and business logic, securing them requires strong access controls, input validation, and API gateway protections.

  For use cases, see WAF Solutions against OWASP Top 10 API Security Risks.
- **WAF Solutions Against OWASP Top 10 Client-Side Security Risks**

  The OWASP Top 10 Client-Side Security Risks focuses on attacks that target the browser specifically focus on exploiting the environment in which web pages are rendered, rather than attacking the server. These attacks aim to steal sensitive data, manipulate content, or compromise user behavior – often silently.

  For use cases, see WAF Solutions against OWASP Top 10 Client-Side Security Risks.
- **Bot Mitigation&DDoS**

  Bots account for a significant portion of global web traffic, with many engaging in malicious activities such as credential stuffing, web scraping, fraud, API abuse, and DDoS attacks. These automated threats pose serious risks to web applications, leading to data breaches, service disruptions, and financial losses. Organizations must implement effective bot mitigation strategies to protect their digital assets from these evolving threats.

  For use cases, see WAF Solutions against Bot Attacks.

In the following sections, we'll explore FortiWeb's security features designed to help defend against the risks mentioned above.

Key Components of FortiWeb

FortiWeb combines traditional WAF features with advanced security mechanisms like machine learning, behavioral analysis, and integration with threat intelligence services. It provides a comprehensive defense against the evolving security challenges that web applications face. To align with industry standards and practices, this guide will introduce FortiWeb's WAF features from the following aspects:

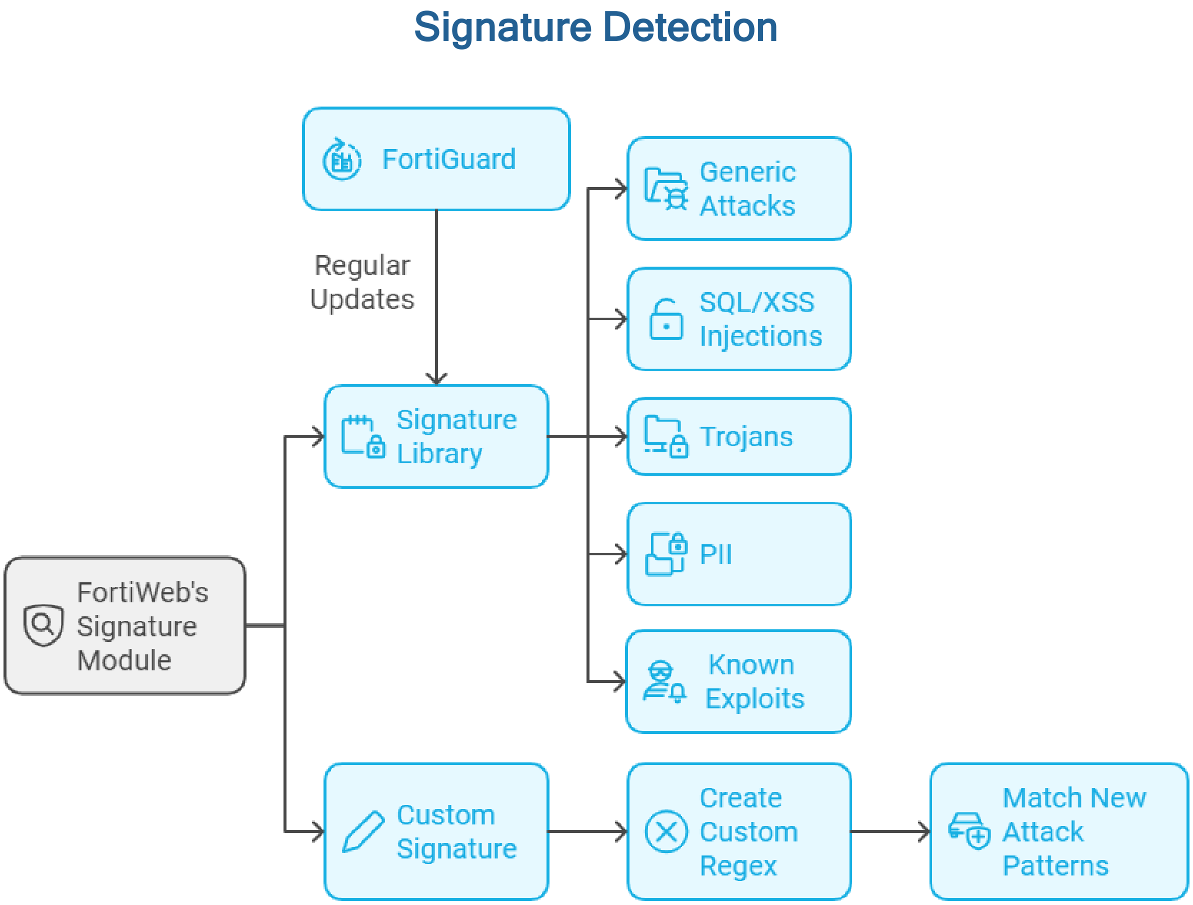
- WAF features against OWASP Top 10 risks on page 7
- WAF features against OWASP Top 10 API security risks on page 18
- WAF features against OWASP Top 10 Client-Side security risks on page 24
- WAF features against bot attacks on page 27

WAF features against OWASP Top 10 risks

The OWASP Top 10 is a widely recognized standard for web application security, highlighting the most critical security risks faced by web applications. Developed by the Open Web Application Security Project (OWASP), this document serves as a crucial resource for developers, security professionals, and organizations, providing insights into common vulnerabilities and how they can be exploited by attackers.

FortiWeb offers a comprehensive suite of security features designed to defend against the OWASP Top 10 risks. These features include advanced threat detection and mitigation techniques, such as input validation, behavior-based anomaly detection, and rate limiting, to address various forms of attacks like injection, broken access control, and cross-site scripting (XSS). Additionally, FortiWeb integrates with other security tools and employs AI-driven behavioral analysis to detect and block sophisticated attacks in real-time. Here are the specific features provided by FortiWeb that can help mitigate the OWASP Top 10 risks.

- Signature Detection
- Machine Learning based Anomaly Detection on page 9
- Data Loss Prevention (DLP) on page 10
- Syntax-based SQL/XSS Injection Detection on page 11
- Input Validation on page 11
- Man-in-the-Browser (MitB) Protection on page 12
- Protocol Constraints on page 13
- Access Control on page 14
- IP Protection on page 14
- URL Encryption on page 15
- Link Cloaking on page 16
- HTTP Security Headers on page 16
- Cookie Security on page 17
- Cross-Site Request Forgery (CSRF) Protection on page 17

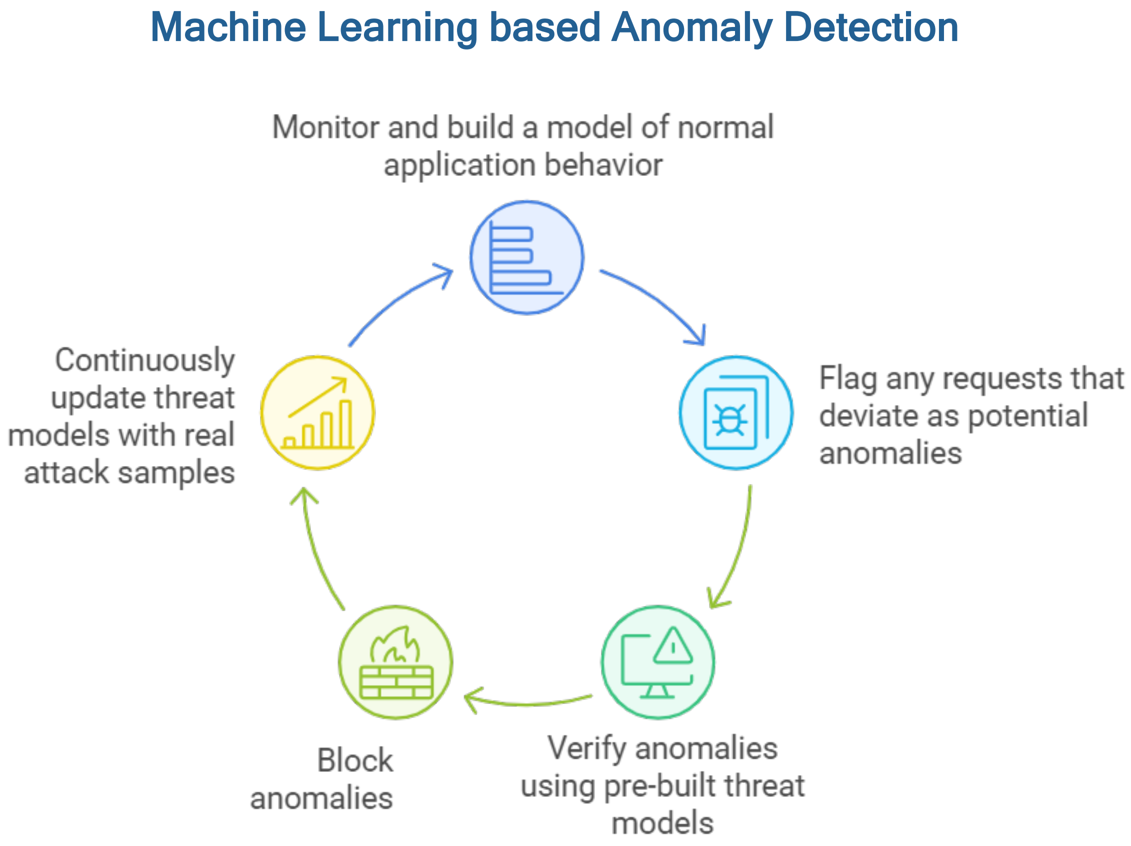


Signature library

FortiWeb's Signature module uses a signature library to block attacks that match specific characteristics, such as malicious code, SQL injection, cross-site scripting (XSS), path traversal, etc. The signature library is regularly updated to continuously improve known attack signatures.

Custom Signature

FortiWeb also provides Custom Signature module which allows you to create custom regular expressions to match the patterns of these new attacks, enabling you to block any similar attacks moving forward.

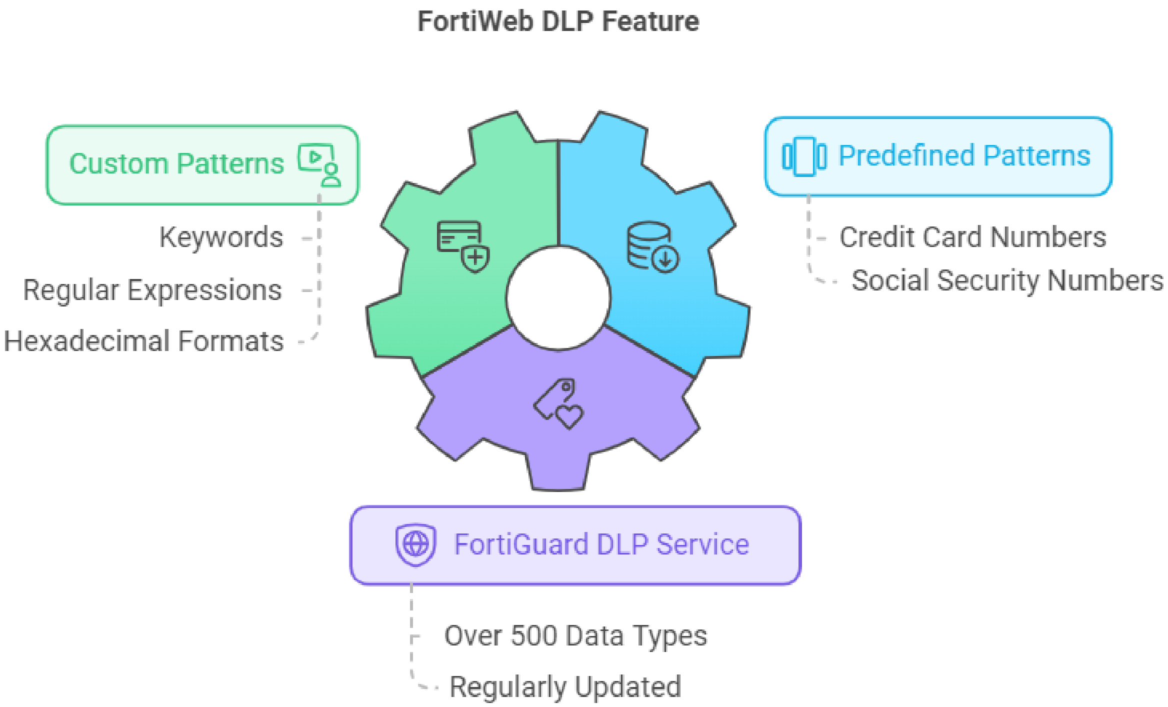

Machine Learning based Anomaly Detection
Monitor and build a model of normal application behavior
Flag any requests that deviate as potential anomalies
Verify anomalies using pre-built threat models
Block anomalies
Continuously update threat models with real attack samples

FortiWeb's Machine Learning Anomaly Detection uses a two-layer approach to effectively identify and block web application attacks.

- The first layer employs a Hidden Markov Model (HMM) to monitor and build a model of normal application behavior, flagging any requests that deviate as potential anomalies.
- The second layer then verifies these anomalies using pre-built, continuously updated threat models trained on thousands of real attack samples, such as SQL Injection and Cross-site Scripting (XSS).

This dual-layer system ensures accurate detection of malicious activity while minimizing false positives.

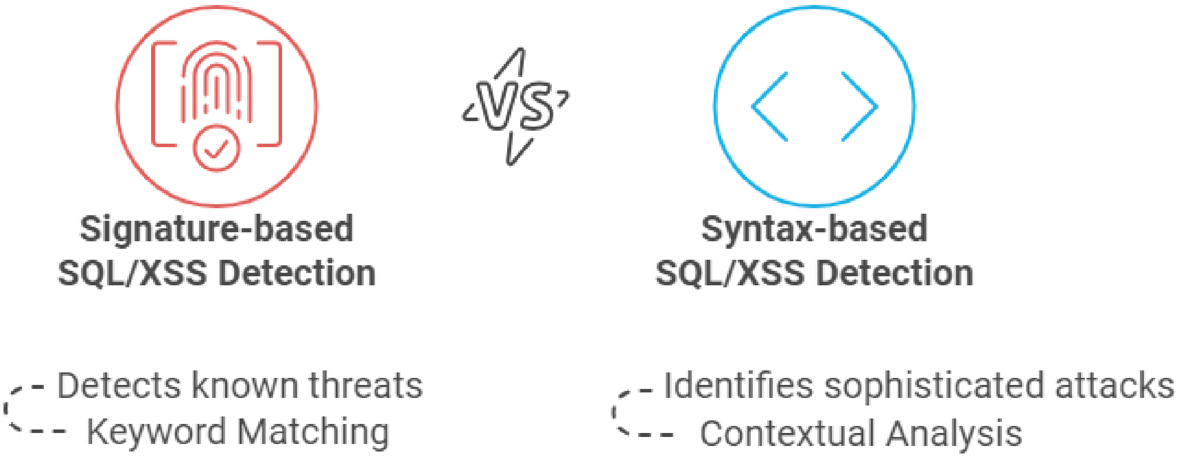
Data Loss Prevention (DLP)



FortiWeb's Data Loss Prevention (DLP) feature is designed to protect against the leakage of sensitive data from web applications.

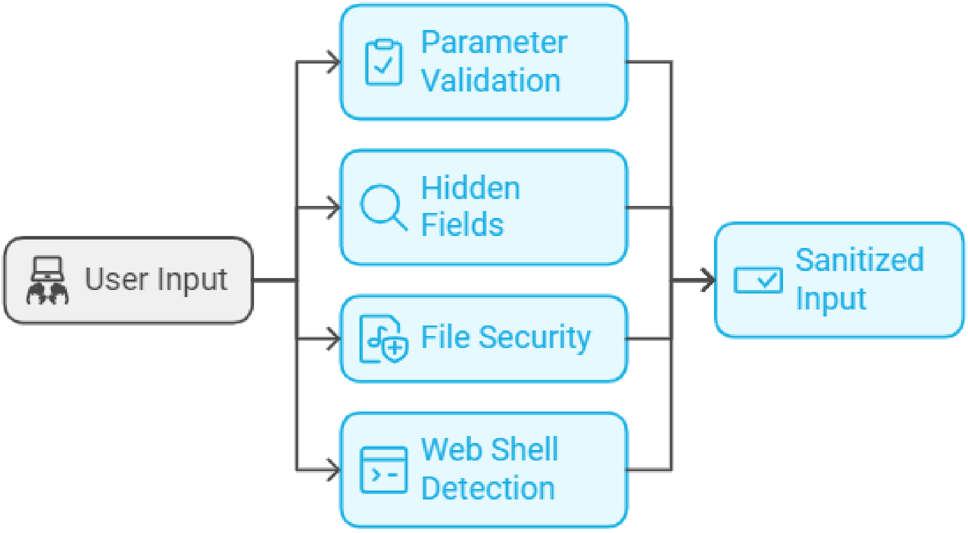
- It integrates with the FortiGuard DLP service which includes over 500 predefined, regularly updated data patterns.
- It has predefined patterns that helps prevent the leakage of sensitive data such as credit card numbers and Social Security Numbers (SSNs).
- It also supports custom patterns through keywords, regular expressions, or hexadecimal formats.

Syntax-based SQL/XSS Injection Detection


Signature-based SQL/XSS Detection
VS
Syntax-based SQL/XSS Detection
Detects known threats
Keyword Matching
Identifies sophisticated attacks
Contextual Analysis

FortiWeb's Syntax-based SQL/XSS Injection Detection feature focuses on identifying and blocking malicious inputs by analyzing the syntax and patterns of user inputs, providing real-time protection against SQL/XSS Injections.

Input Validation

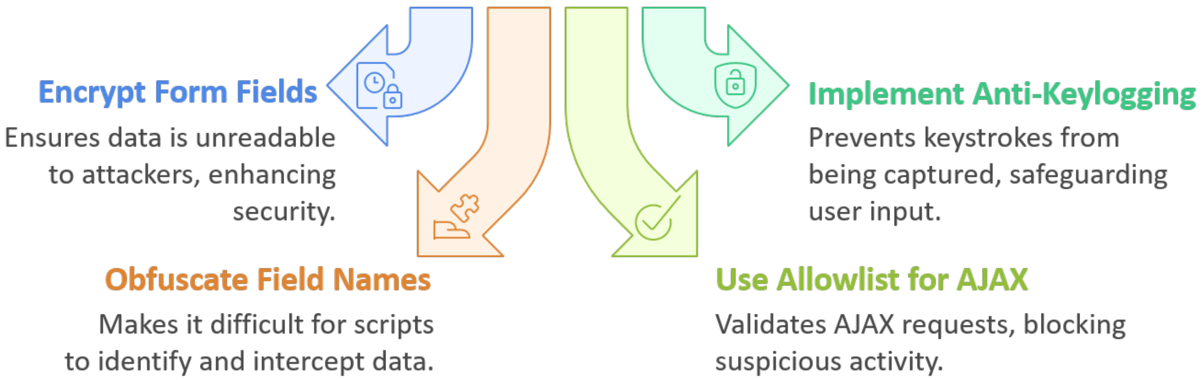


FortiWeb's Input Validation features are designed to protect web applications from various injection attacks and other threats that exploit user inputs. These features ensure that all data submitted by users, such as form fields, URL parameters, and cookies, is properly validated and sanitized before being processed by the application.

The Input Validation modules include Parameter Validation, Hidden Fields, File Security, and Web Shell Detection.

Man-in-the-Browser (MitB) Protection

How to protect sensitive form data from MiTB attacks?



Encrypt Form Fields

Ensures data is unreadable to attackers, enhancing security.

Implement Anti-Keylogging

Prevents keystrokes from being captured, safeguarding user input.

Obfuscate Field Names

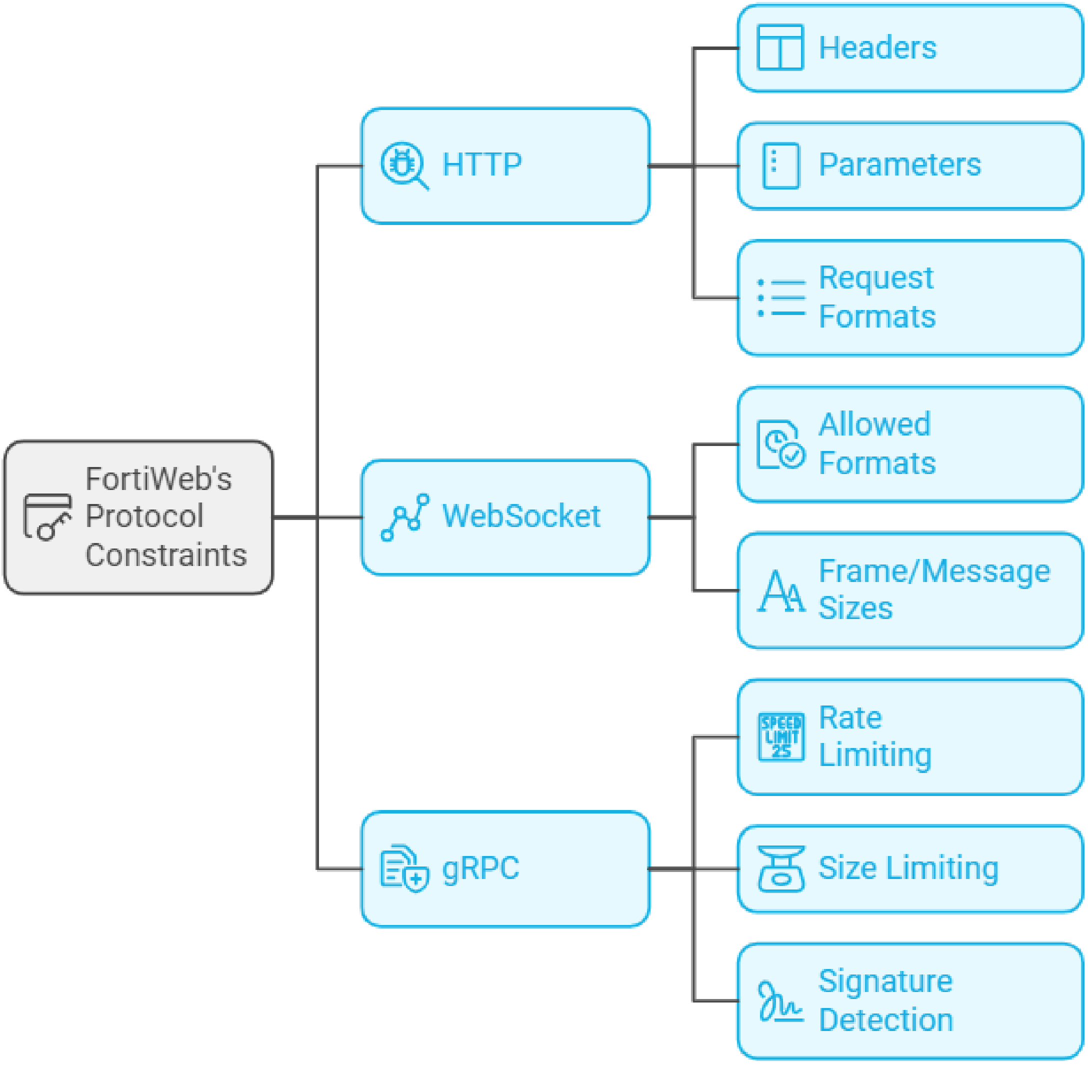
Makes it difficult for scripts to identify and intercept data.

Use Allowlist for AJAX

Validates AJAX requests, blocking suspicious activity.

FortiWeb's MitB Protection safeguards user inputs from Man-in-the-Browser attacks by implementing advanced security measures such as input obfuscation, encryption, anti-keylogger mechanisms, and an Ajax request allow list. These features work together to prevent malware from intercepting or altering sensitive information like passwords and payment details, ensuring that user data remains secure even if the browser is compromised.

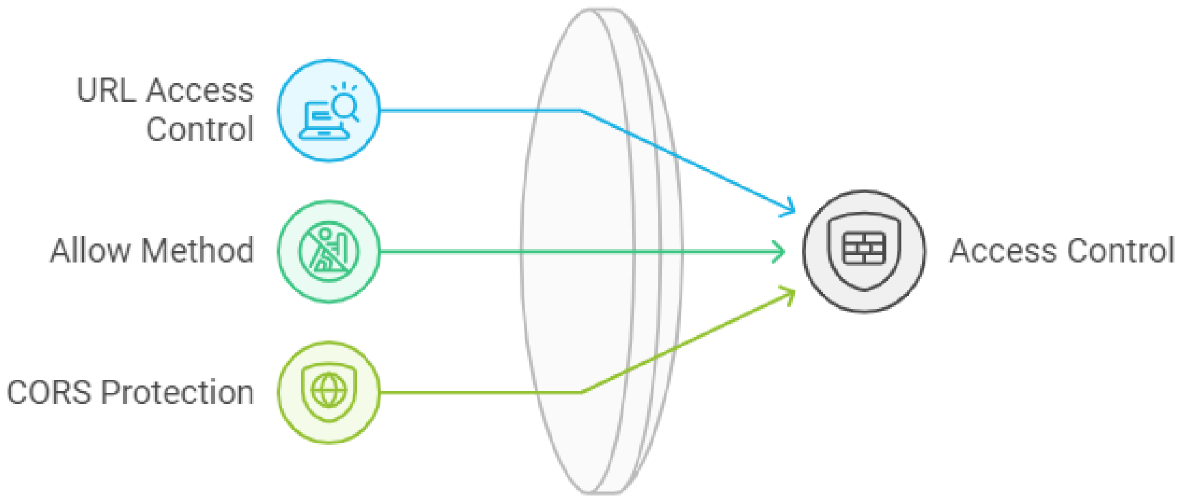
Protocol Constraints



FortiWeb's Protocol Constraints are security features that enforce strict adherence to protocols like HTTP, HTTPS, WebSocket, and gRPC to prevent attacks exploiting protocol weaknesses.

- For HTTP, FortiWeb checks elements such as headers, parameters, and request formats.
- For WebSocket, it secures WebSocket traffic by controlling allowed formats and frame/message sizes.
- For gRPC, it applies controls like rate limiting, size limiting, and signature detection.

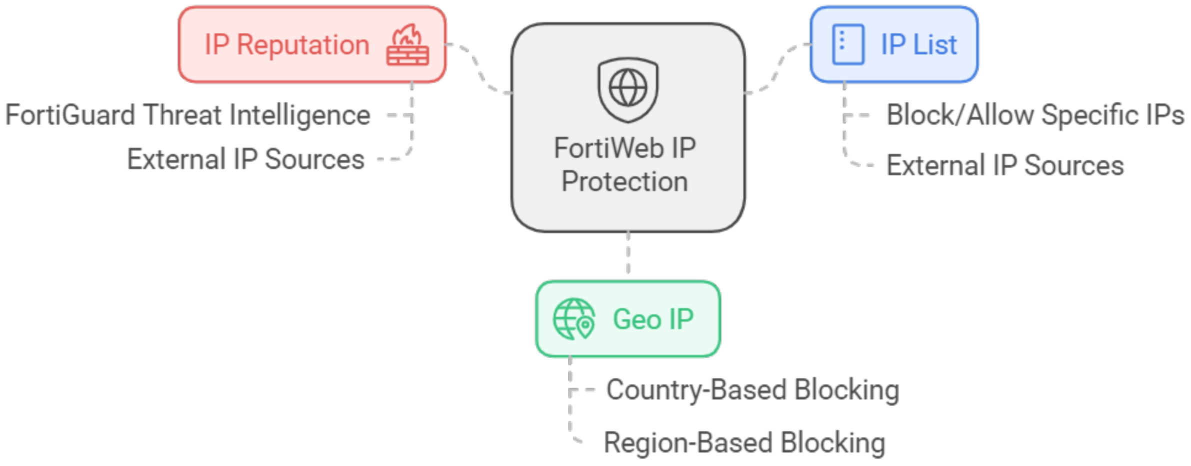
Access Control



FortiWeb's Access Control features include URL Access Control, Allow Method, and CORS (Cross-Origin Resource Sharing) Protection.

These capabilities provide granular control over how web applications handle requests based on the URL, HTTP methods, and cross-origin requests, ensuring that only authorized and legitimate interactions are permitted.

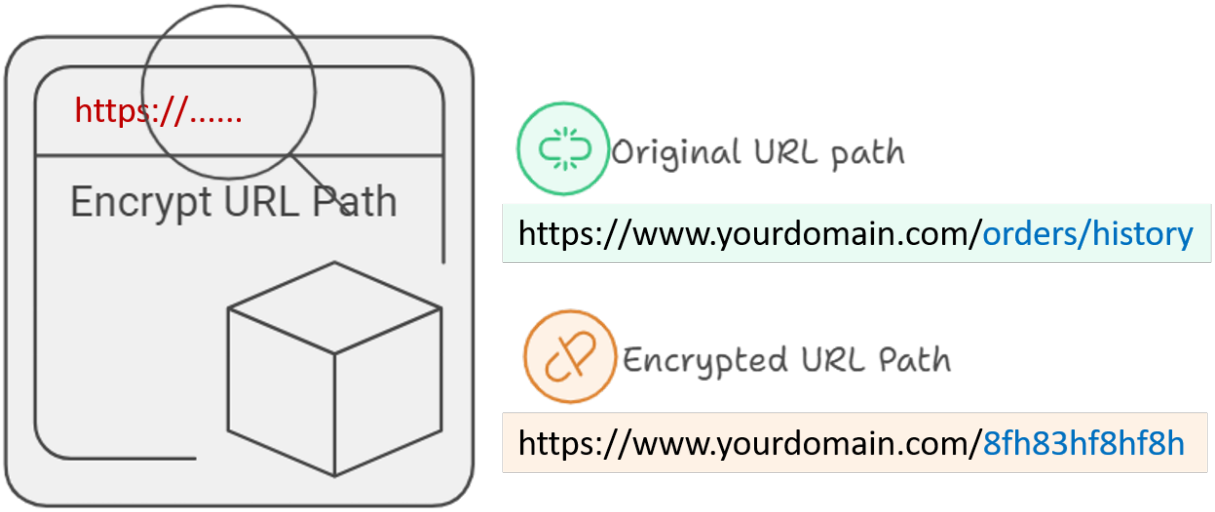
IP Protection



FortiWeb’s IP Protection features include IP List, Geo IP, and IP reputation.

It integrates with FortiGuard’s real-time threat intelligence to automatically block IPs associated with malicious activities and allows for the use of external IP sources to enhance protection. This multi-layered approach ensures that only trusted, legitimate IP addresses can access your web applications, effectively mitigating risks from unauthorized or harmful traffic.

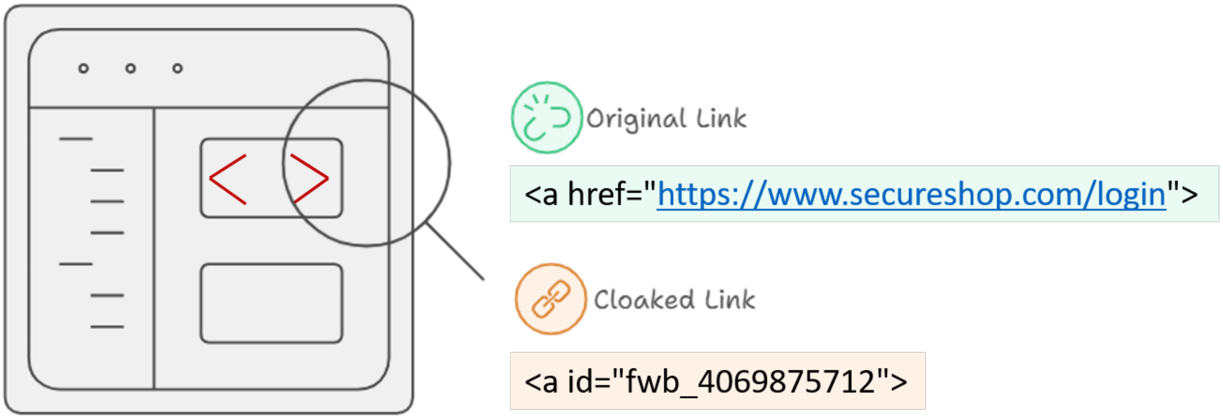
URL Encryption


https://......
Encrypt URL Path
Original URL path
https://www.yourdomain.com/orders/history
Encrypted URL Path
https://www.yourdomain.com/8fh83hf8hf8h

FortiWeb's URL Encryption feature enhances web application security by encrypting URLs to obscure their actual paths and make them difficult for attackers to guess.

For example, the URL "https://www.secureshop.com/orders/history" might be encrypted to "https://www.secureshop.com/8fh83hf8hf8h", masking the original structure and content of the URL. This prevents attackers from easily identifying and accessing sensitive pages through forceful browsing or URL manipulation.

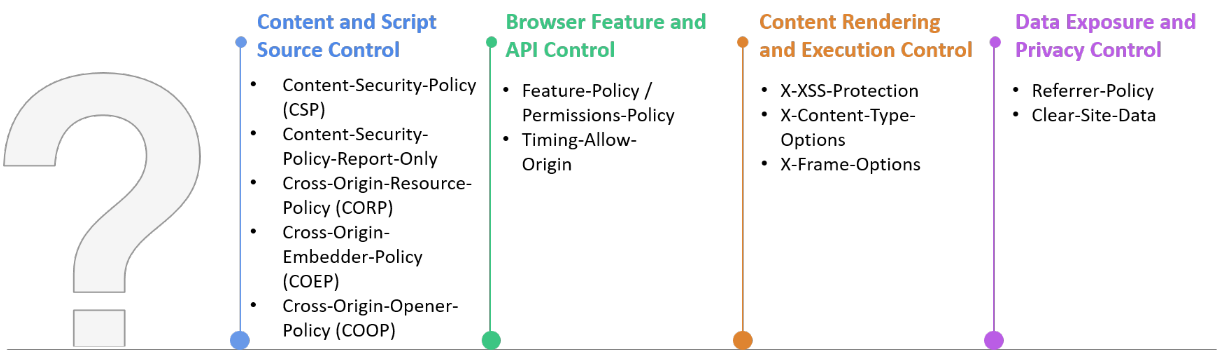
Link Cloaking



FortiWeb’s Link Cloaking feature protects sensitive or critical URLs from being indexed by web crawlers while maintaining a seamless experience for users. This is achieved by cloaking the links within the HTML content so that they are not easily readable or accessible to automated systems like search engine bots.

HTTP Security Headers

Which HTTP Security Headers should be implemented?



Content and Script Source Control

- Content-Security-Policy (CSP)
- Content-Security-Policy-Report-Only
- Cross-Origin-Resource-Policy (CORP)
- Cross-Origin-Embedder-Policy (COEP)
- Cross-Origin-Opener-Policy (COOP)

Browser Feature and API Control

- Feature-Policy / Permissions-Policy
- Timing-Allow-Origin

Content Rendering and Execution Control

- X-XSS-Protection
- X-Content-Type-Options
- X-Frame-Options

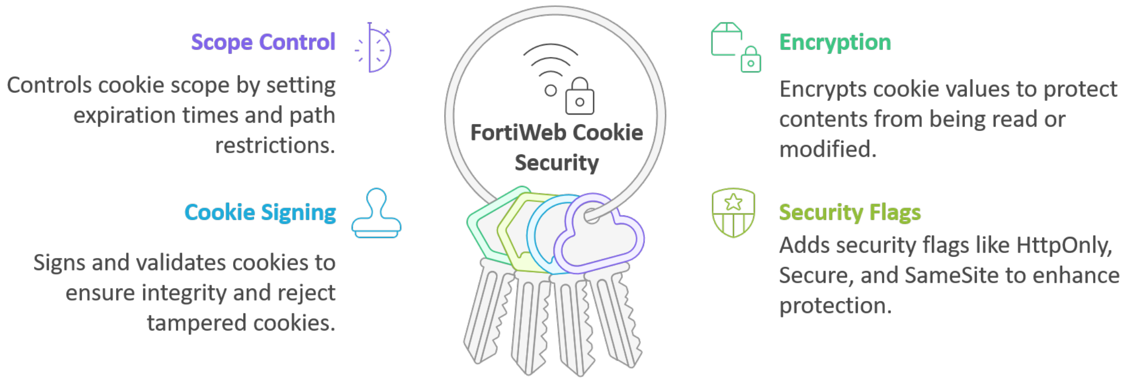
Data Exposure and Privacy Control

- Referrer-Policy
- Clear-Site-Data

FortiWeb's HTTP Security Headers feature adds security-focused HTTP headers, including X-Frame-Options, X-Content-Type-Options, Content-Security-Policy, Feature-Policy, Referrer-Policy, and X-XSS-Protection, to server responses.

These headers enforce security policies in client browsers, mitigating risks such as clickjacking, MIME-type sniffing, and cross-site scripting (XSS), thereby improving protection during request handling.

Cookie Security



Scope Control

Controls cookie scope by setting expiration times and path restrictions.

Cookie Signing

Signs and validates cookies to ensure integrity and reject tampered cookies.

Encryption

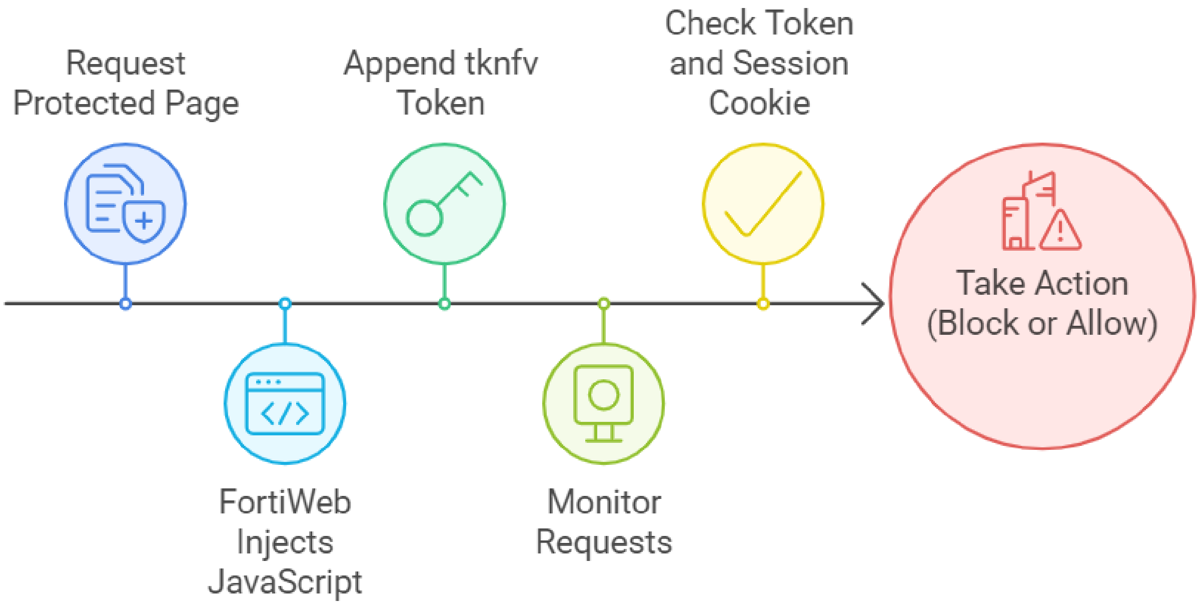
Encrypts cookie values to protect contents from being read or modified.

Security Flags

Adds security flags like HttpOnly, Secure, and SameSite to enhance protection.

FortiWeb's Cookie Security module protects web application cookies by encrypting their contents, enforcing HTTPOnly, SameSite and Secure flags to prevent access by scripts and ensure transmission over HTTPS, and verifying cookie integrity with digital signatures. These features also include session cookie protection, and setting cookie expiration and path restrictions. Together, they safeguard against common cookie-related attacks like session hijacking, XSS, and man-in-the-middle attacks, ensuring cookies remain secure and tamper-proof throughout their lifecycle.

Cross-Site Request Forgery (CSRF) Protection


Request Protected Page
FortiWeb Injects JavaScript
Append tknfv Token
Monitor Requests
Check Token and Session Cookie
Take Action (Block or Allow)

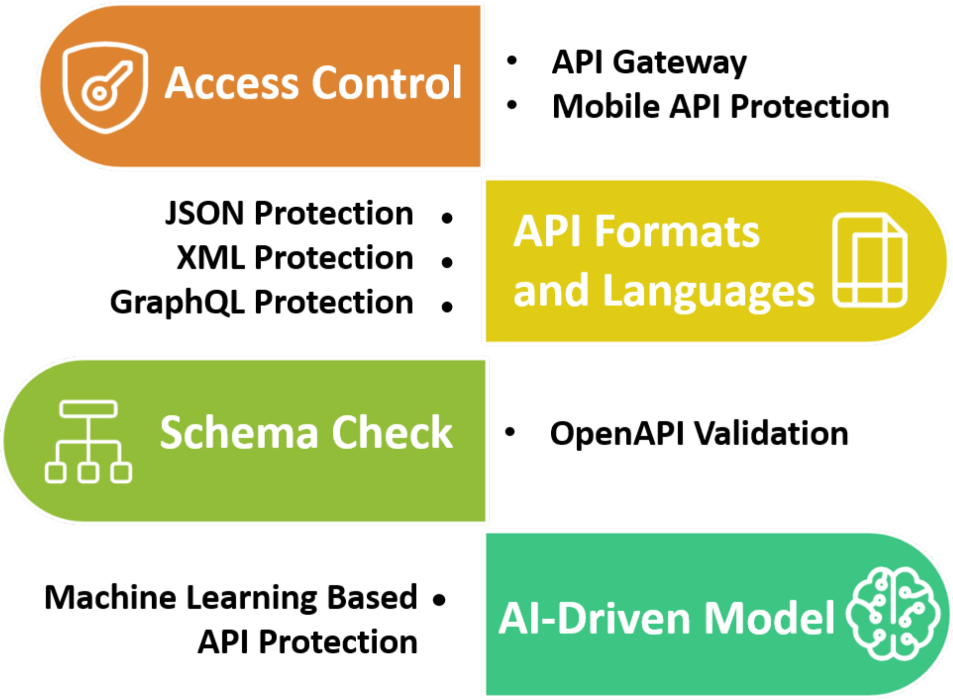
FortiWeb’s Cross-Site Request Forgery (CSRF) Protection is designed to safeguard web applications from CSRF attacks, where an attacker tricks a user into performing actions on a web application without their consent.

When a protected page is requested, FortiWeb injects JavaScript to append the tknfv token to HTML links, forms, and AJAX requests. The token is tied to the session cookie managed by Client Management. FortiWeb monitors requests to the URLs in the list, and if a request lacks the token or the token doesn't match the session cookie, it takes the specified action, such as blocking the request. Proper configuration ensures effective protection without false positives.

WAF features against OWASP Top 10 API security risks

The OWASP API Security Top 10 is a list of the most critical security risks specific to Application Programming Interfaces (APIs). As APIs become increasingly integral to modern applications, they have also become a prime target for attackers. The OWASP API Security Top 10 provides guidance on the most common vulnerabilities that can affect APIs, helping organizations better secure their API endpoints.

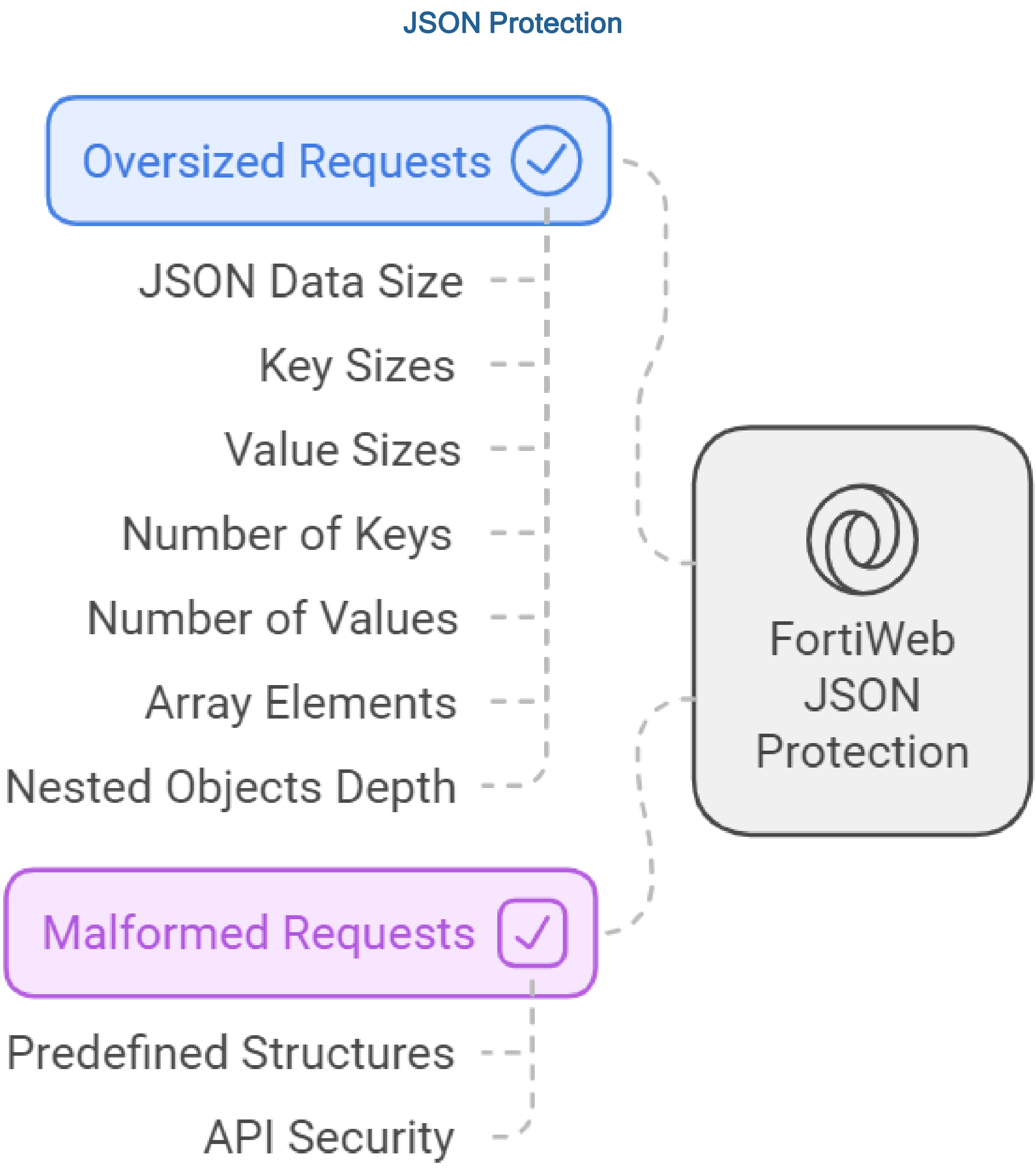
FortiWeb provides a robust set of features to protect APIs against the OWASP API Security Top 10 risks. Its advanced security mechanisms, AI-driven behavioral analysis, and integration with Fortinet's security fabric, allow for comprehensive protection of APIs.



Here's a breakdown of the specific features provided by FortiWeb that can help mitigate each of the OWASP API Security Top 10 risks.

- JSON Protection
- XML Protection
- GraphQL Protection

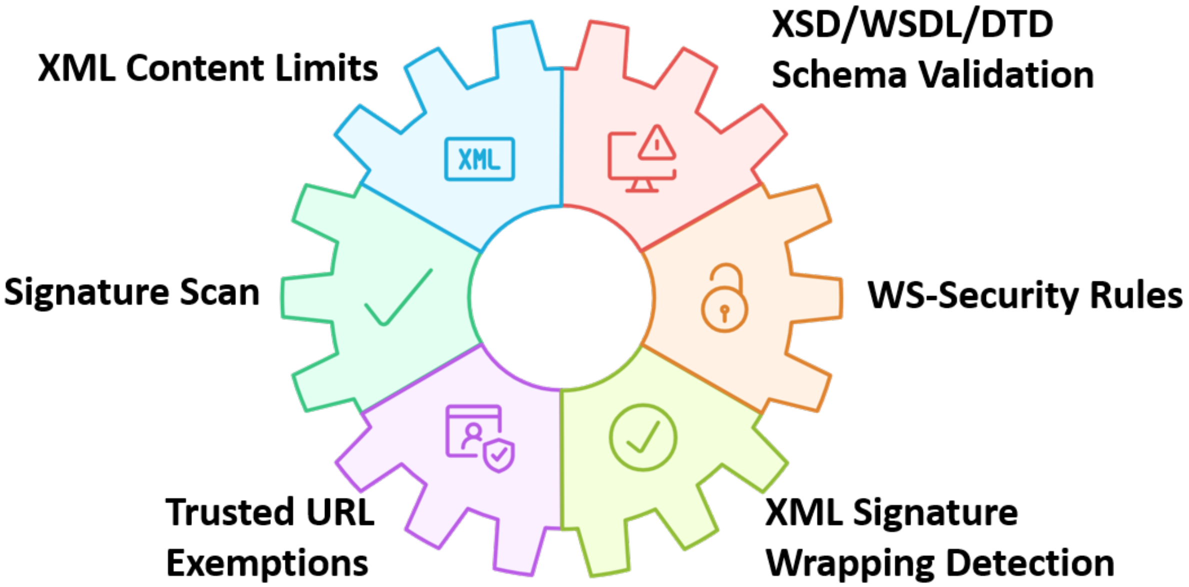
- OpenAPI Validation
- Mobile API Protection
- API Gateway
- Machine Learning (ML) Based API Protection



FortiWeb's JSON Protection allows you to configure detailed validation rules for JSON data, helping to secure your application against malicious input. You can control the size of the JSON document, key, and value sizes, as well as the number of keys, values, and array elements, and the depth of nested objects. These settings help prevent attacks such as buffer overflows and DoS by restricting oversized or malformed JSON requests. Additionally, FortiWeb supports JSON schema validation, ensuring that incoming requests conform to predefined structures, enhancing the security and reliability of your API.

Watch the video on JSON Protection by clicking this link.

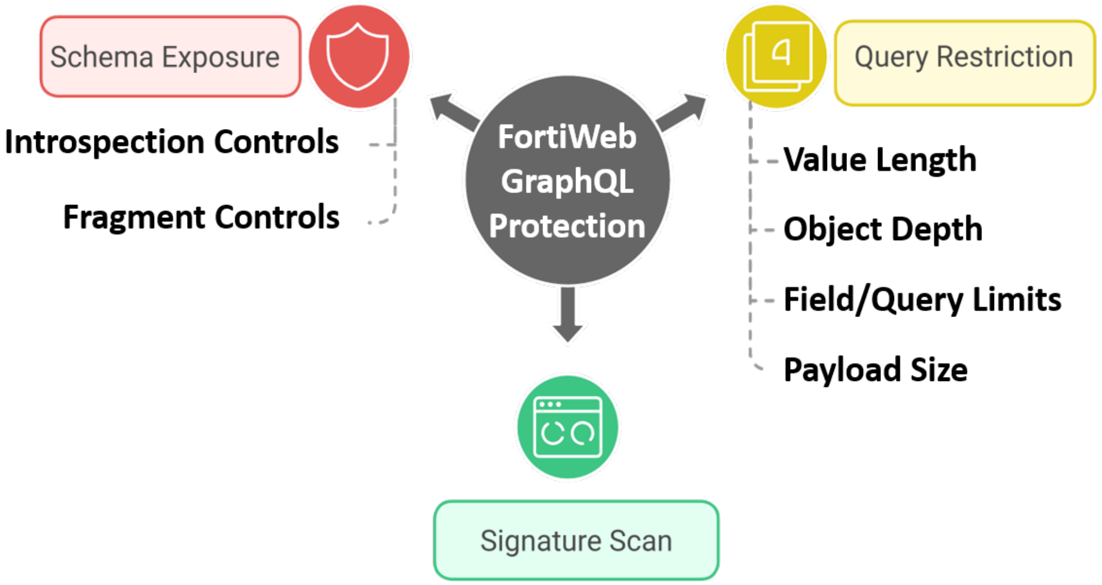
XML Protection



FortiWeb’s XML protection feature secures web applications by enforcing limits on XML content, blocking malicious entities like XML External Entities (XXE) and Schema Location injections, and validating messages against schemas (XSD, WSDL, DTD). It also provides WS-Security rules for encrypting, decrypting, and digitally signing parts of SOAP messages, ensuring message integrity. Additionally, FortiWeb detects XML Signature Wrapping (XSW) attacks by verifying signed nodes using XPath and certificates. You can configure exemptions for trusted URLs while maintaining protection for the rest of the application, making it ideal for safeguarding e-commerce platforms handling XML data.

Watch the video on XML Protection by clicking this link.

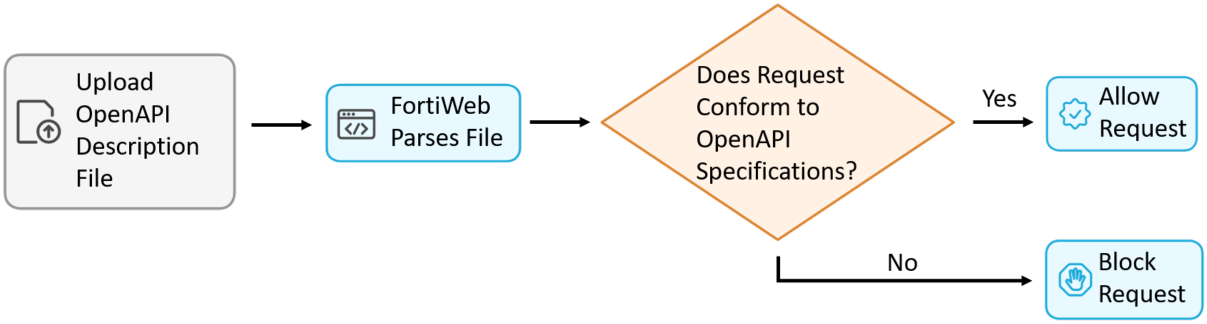
GraphQL Protection



FortiWeb's GraphQL protection safeguards APIs by limiting query size, complexity, and resource consumption to defend against malicious queries, signature attacks, and performance bottlenecks. Key features include restrictions on payload size, value length, object depth, and the number of fields or queries in alias or array batches. It also offers controls over introspection queries and fragments to minimize schema exposure.

Watch the video on GraphQL Protection by clicking this link.

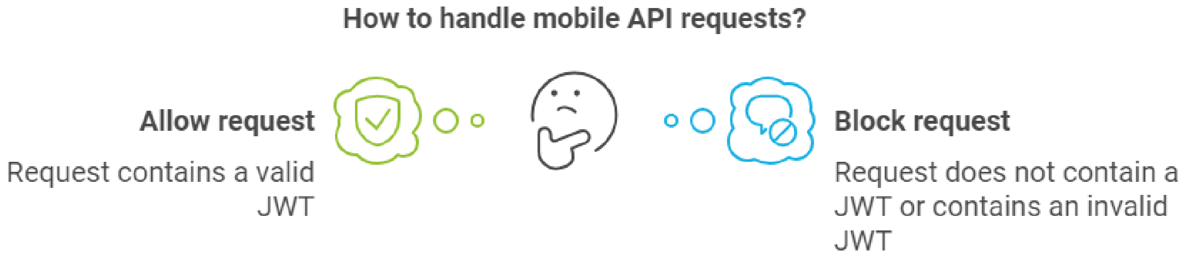
OpenAPI Validation


Upload OpenAPI Description File
FortiWeb Parses File
Does Request Conform to OpenAPI Specifications?
Yes
Allow Request
No
Block Request

FortiWeb’s OpenAPI validation feature allows you to upload an OpenAPI description file (also known as a Swagger file) that defines your API’s structure, endpoints, and data types. Once uploaded, FortiWeb parses this file and uses it as a baseline to validate incoming requests. It blocks any requests that do not conform to the API specifications defined in the OpenAPI file, such as requests with unexpected endpoints, invalid parameters, or mismatched data types. This ensures that only legitimate requests that match the predefined API schema are allowed, improving security by preventing attacks like parameter tampering and malformed requests.

Watch the video on OpenAPI Validation by clicking this link.

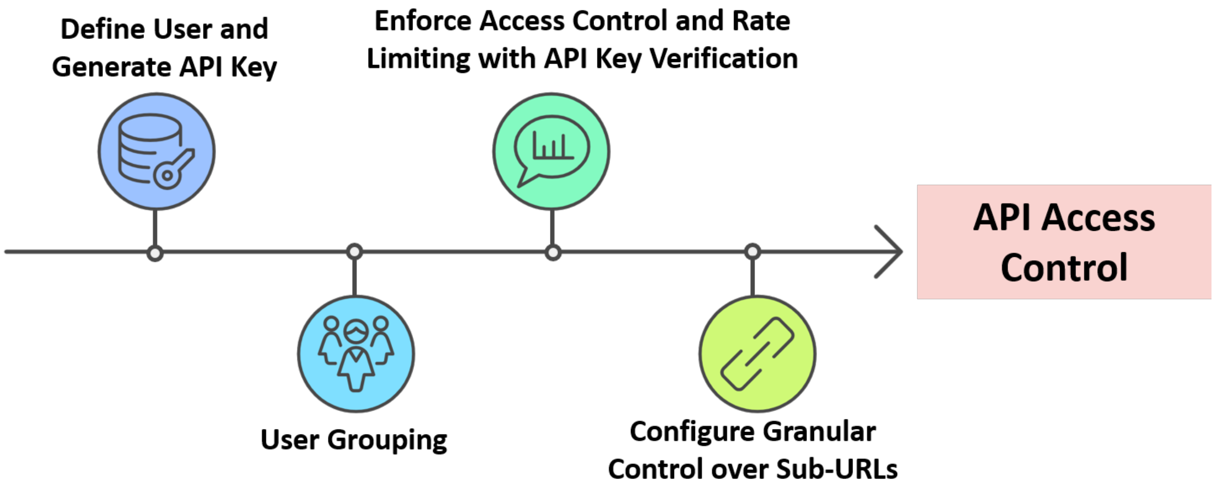
Mobile API Protection


How to handle mobile API requests?
Allow request
Request contains a valid JWT
Block request
Request does not contain a JWT or contains an invalid JWT

FortiWeb’s Mobile API protection feature validates JSON Web Tokens (JWTs) in requests from mobile applications. It checks if a request contains a JWT, whether the token is valid, and flags the request accordingly (no token, valid token, or invalid token). Based on these flags, actions are enforced ensuring only authorized mobile traffic is allowed and enhancing security for mobile API interactions.

Watch the video on Mobile API Protection by clicking this link.

API Gateway

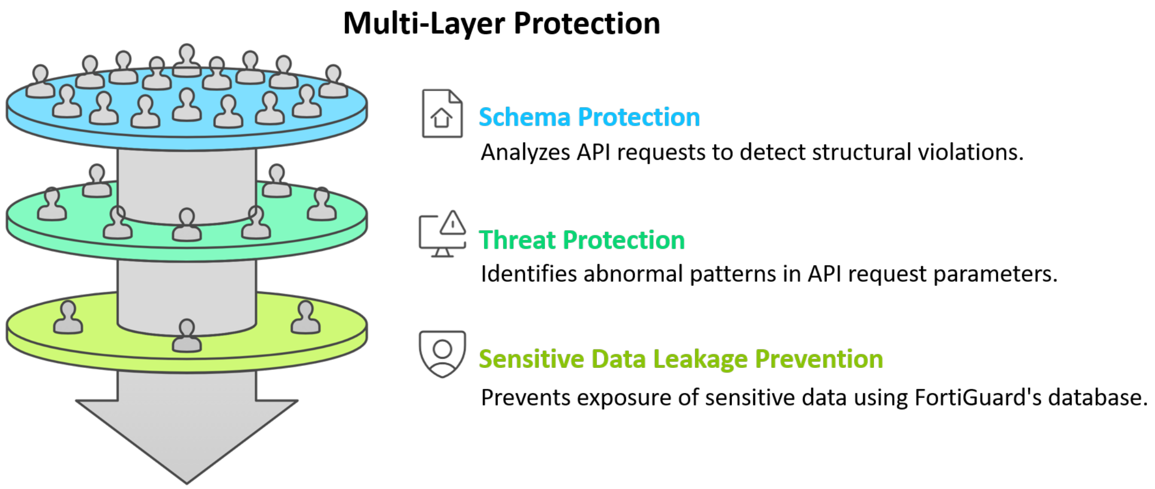

Define User and Generate API Key
Enforce Access Control and Rate Limiting with API Key Verification
API Access Control
User Grouping
Configure Granular Control over Sub-URLs

FortiWeb’s API gateway provides robust API management by enforcing access control through API key verification, ensuring only authorized users from defined user groups can access the API. It manages rate limits, user grouping, and sub-URL settings, and executes specified actions if any API call violates these rules, providing secure and controlled API access.

Sub-URL Settings allow you to create additional rules for more granular control over specific API subpaths. When a user’s API call matches a predefined frontend URL prefix, you can apply sub-URL rules to control access or actions based on specific subpaths under that prefix.

Watch the video on API Gateway by clicking this link.

Machine Learning (ML) Based API Protection



Multi-Layer Protection

Schema Protection

Analyzes API requests to detect structural violations.

Threat Protection

Identifies abnormal patterns in API request parameters.

Sensitive Data Leakage Prevention

Prevents exposure of sensitive data using FortiGuard's database.

The machine learning based API Protection learns the REST API data structure from user traffic samples and then build mathematical models to screen out malicious API requests, and prevent sensitive data leakage in API responses.

Multi-Layer Protection for API Requests

- **Schema Protection:** The Schema Protection model consists of two main functions – API discovery and API protection. It analyzes the method, URL, and endpoint data of the API request samples to detect schema violations.
- **Threat Protection:** The Threat Protection model learns parameter value patterns and then identify API requests with abnormal parameter values.
- **Sensitive Data Leakage Prevention:** Integrates with FortiGuard's extensive, customizable database of over 500 predefined data patterns and policies to detect potential exposure of sensitive information in API responses.

Continuous Learning

FortiWeb supports Continuous Learning, enabling the model to automatically adapt to changes in the API schema. This includes handling scenarios such as:

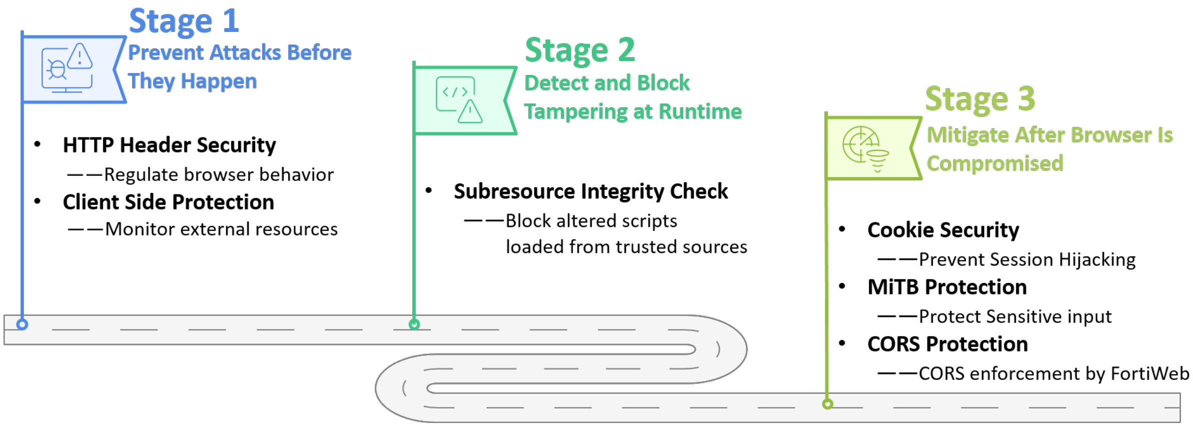
- **Introduction of new APIs:** Adding entirely new endpoints or services to the application.
- **Modifications to existing parameters:** Updating the structure, data types, or values of existing parameters in API requests or responses.
- **Addition of optional or mandatory parameters:** Recognizing newly added optional fields or required parameters in API calls.
- **Changes to URL structures:** Adjusting to modifications in API endpoint paths.
- **Updates in request or response payloads:** Adapting to altered JSON data formats used in API exchanges.

Watch the video on Machine Learning (ML) Based API Protection by clicking this link.

WAF features against OWASP Top 10 Client-Side security risks

Since modern web apps rely heavily on JavaScript, APIs, and third-party integrations, the browser becomes a critical attack surface. Attacks that target the browser specifically focus on exploiting the environment in which web pages are rendered, rather than attacking the server. These attacks aim to steal sensitive data, manipulate content, or compromise user behavior – often silently.

FortiWeb actively prevents and mitigates these attacks by controlling how browsers behave, validating resource integrity, and securing sensitive data. Its layered protection strategy provides defense before, during, and even after the browser is comprised.



Stage 1
Prevent Attacks Before They Happen

- **HTTP Header Security**
  ——Regulate browser behavior
- **Client Side Protection**
  ——Monitor external resources

Stage 2
Detect and Block Tampering at Runtime

- **Subresource Integrity Check**
  ——Block altered scripts loaded from trusted sources

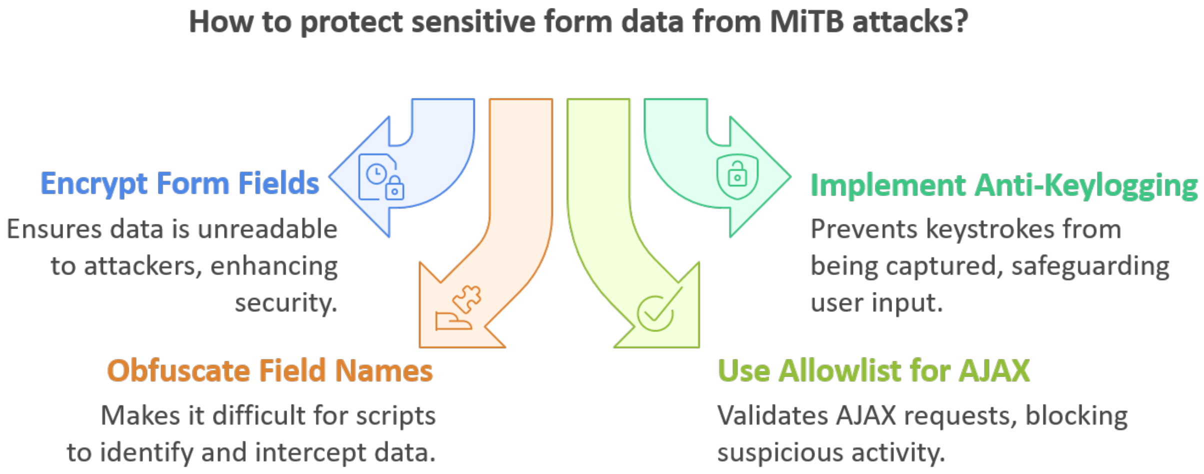
Stage 3
Mitigate After Browser Is Compromised

- **Cookie Security**
  ——Prevent Session Hijacking
- **MiTB Protection**
  ——Protect Sensitive input
- **CORS Protection**
  ——CORS enforcement by FortiWeb

Here are the key features FortiWeb employs to defend against client side security risks.

- Man-in-the-Browser (MitB) Protection on page 25
- HTTP Security Headers on page 25
- Subresource Integrity Check on page 26
- Cookie Security on page 26
- CORS Protection on page 27
- Client Side Protection on page 27

Man-in-the-Browser (MitB) Protection



How to protect sensitive form data from MiTB attacks?

Encrypt Form Fields
Ensures data is unreadable to attackers, enhancing security.

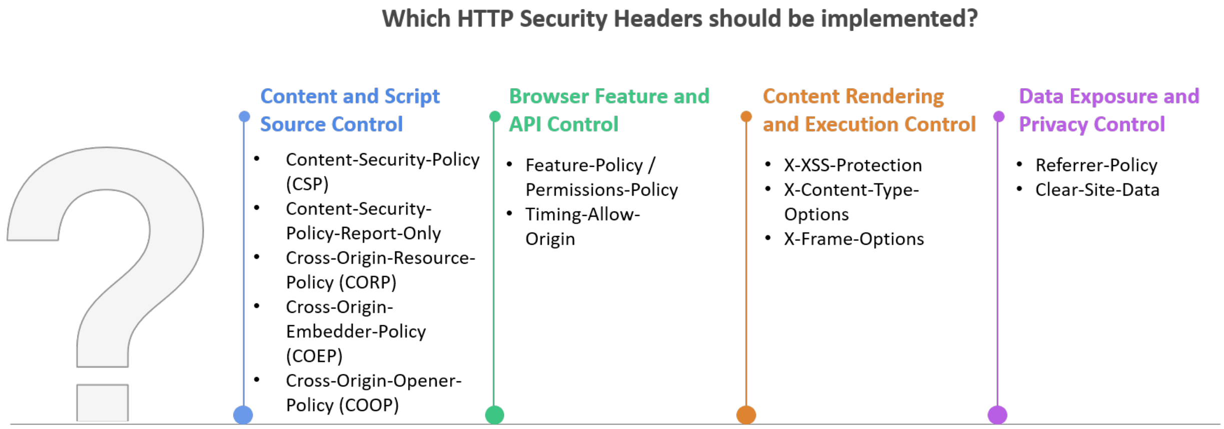
Implement Anti-Keylogging
Prevents keystrokes from being captured, safeguarding user input.

Obfuscate Field Names
Makes it difficult for scripts to identify and intercept data.

Use Allowlist for AJAX
Validates AJAX requests, blocking suspicious activity.

FortiWeb's MitB Protection safeguards user inputs from Man-in-the-Browser attacks by implementing advanced security measures such as input obfuscation, encryption, anti-keylogger mechanisms, and an Ajax request allow list. These features work together to prevent malware from intercepting or altering sensitive information like passwords and payment details, ensuring that user data remains secure even if the browser is compromised.

HTTP Security Headers



Which HTTP Security Headers should be implemented?

Content and Script Source Control
- Content-Security-Policy (CSP)
- Content-Security-Policy-Report-Only
- Cross-Origin-Resource-Policy (CORP)
- Cross-Origin-Embedder-Policy (COEP)
- Cross-Origin-Opener-Policy (COOP)

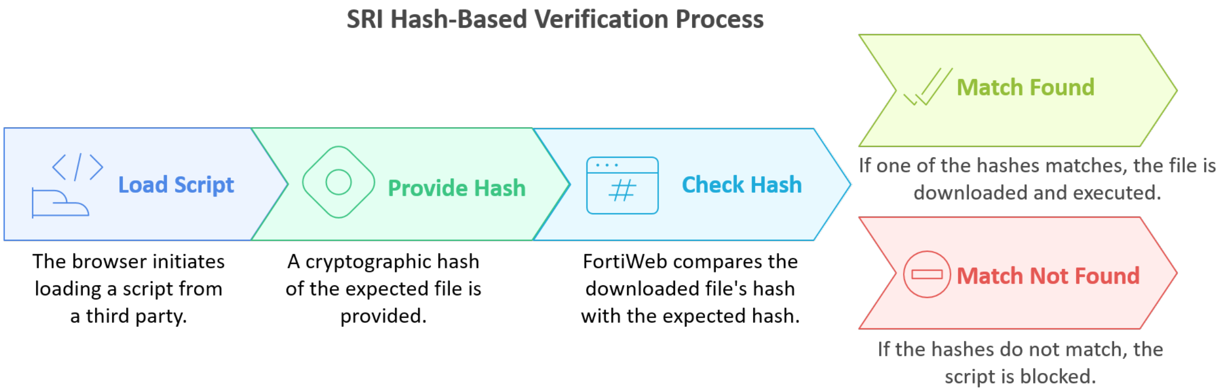
Browser Feature and API Control
- Feature-Policy / Permissions-Policy
- Timing-Allow-Origin

Content Rendering and Execution Control
- X-XSS-Protection
- X-Content-Type-Options
- X-Frame-Options

Data Exposure and Privacy Control
- Referrer-Policy
- Clear-Site-Data

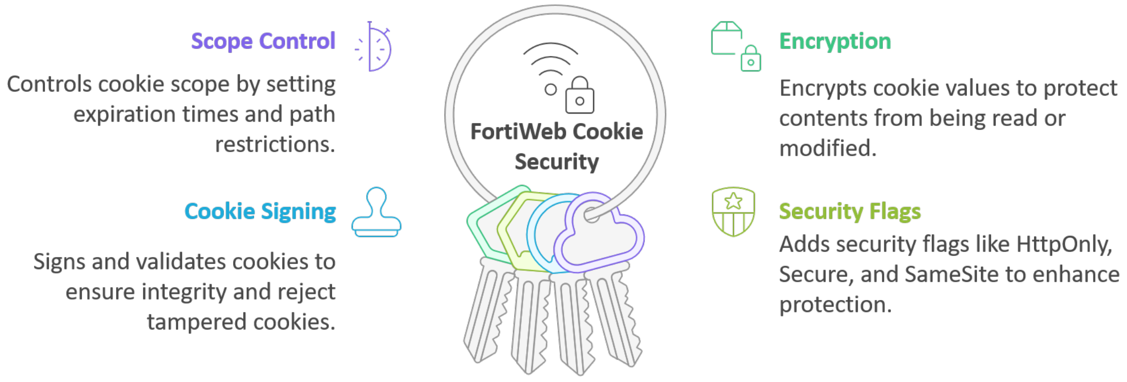
FortiWeb's HTTP Security Headers feature adds security-focused HTTP headers, including X-Frame-Options, X-Content-Type-Options, Content-Security-Policy, Feature-Policy, Referrer-Policy, X-XSS-Protection, etc. to server responses. These headers enforce security policies in client browsers, mitigating risks such as clickjacking, MIME-type sniffing, and cross-site scripting (XSS), thereby improving protection during request handling.

Subresource Integrity Check


SRI Hash-Based Verification Process
Load Script
The browser initiates loading a script from a third party.
Provide Hash
A cryptographic hash of the expected file is provided.
Check Hash
FortiWeb compares the downloaded file's hash with the expected hash.
Match Found
If one of the hashes matches, the file is downloaded and executed.
Match Not Found
If the hashes do not match, the script is blocked.

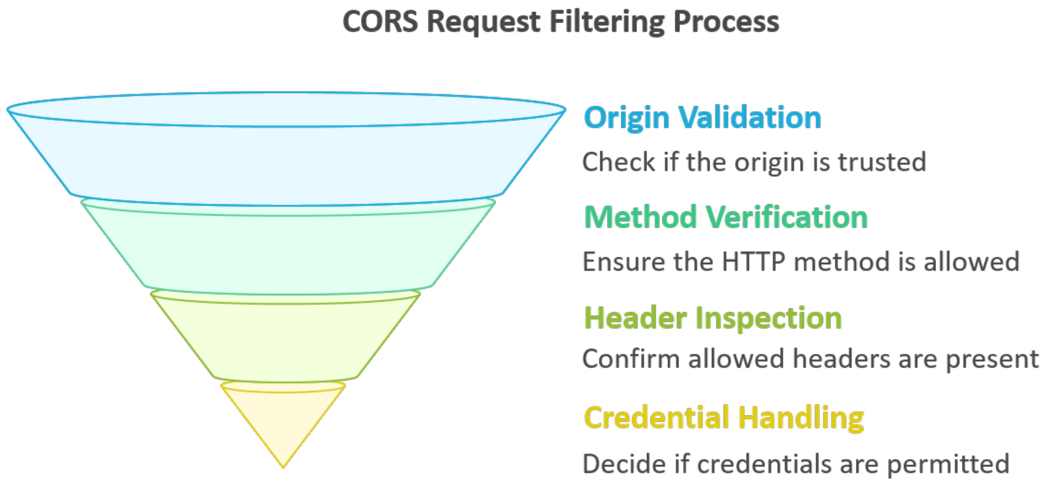
Most modern websites rely on third-party sources—like CDNs—to load scripts and stylesheets. But what if one of those external files is compromised? FortiWeb's Subresource Integrity (SRI) Check feature helps protect against this by enforcing hash-based verification. It ensures that the scripts or styles are executed only if their content matches a known, trusted cryptographic hash.

Cookie Security


Scope Control
Controls cookie scope by setting expiration times and path restrictions.
Cookie Signing
Signs and validates cookies to ensure integrity and reject tampered cookies.
FortiWeb Cookie Security
Encryption
Encrypts cookie values to protect contents from being read or modified.
Security Flags
Adds security flags like HttpOnly, Secure, and SameSite to enhance protection.

FortiWeb's Cookie Security module protects web application cookies by encrypting their contents, enforcing HTTPOnly, SameSite and Secure flags to prevent access by scripts and ensure transmission over HTTPS, and verifying cookie integrity with digital signatures. These features also include session cookie protection, and setting cookie expiration and path restrictions. Together, they safeguard against common cookie-related attacks like session hijacking, XSS, and man-in-the-middle attacks, ensuring cookies remain secure and tamper-proof throughout their lifecycle.

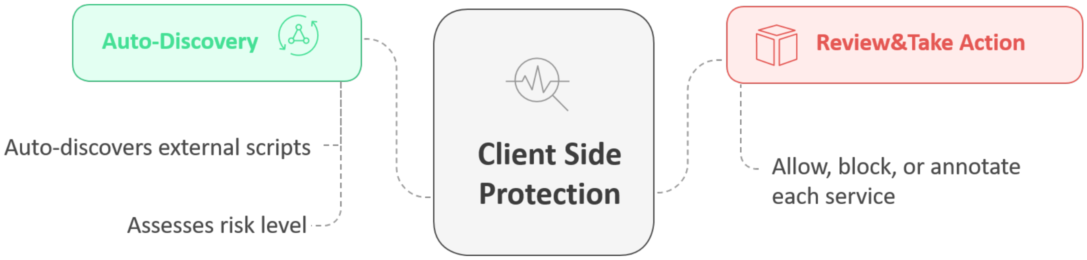
CORS Protection


CORS Request Filtering Process
Origin Validation
Check if the origin is trusted
Method Verification
Ensure the HTTP method is allowed
Header Inspection
Confirm allowed headers are present
Credential Handling
Decide if credentials are permitted

Malicious extensions or injected scripts from web frontends may try to send cross-origin requests to your application's APIs. These requests might attempt to read sensitive data, such as user details or session tokens, from your backend.

FortiWeb's CORS Protection feature allows you to enforce strict rules on which external origins can access your application's resources–blocking unauthorized cross-origin requests before they ever reach your backend.

Client Side Protection

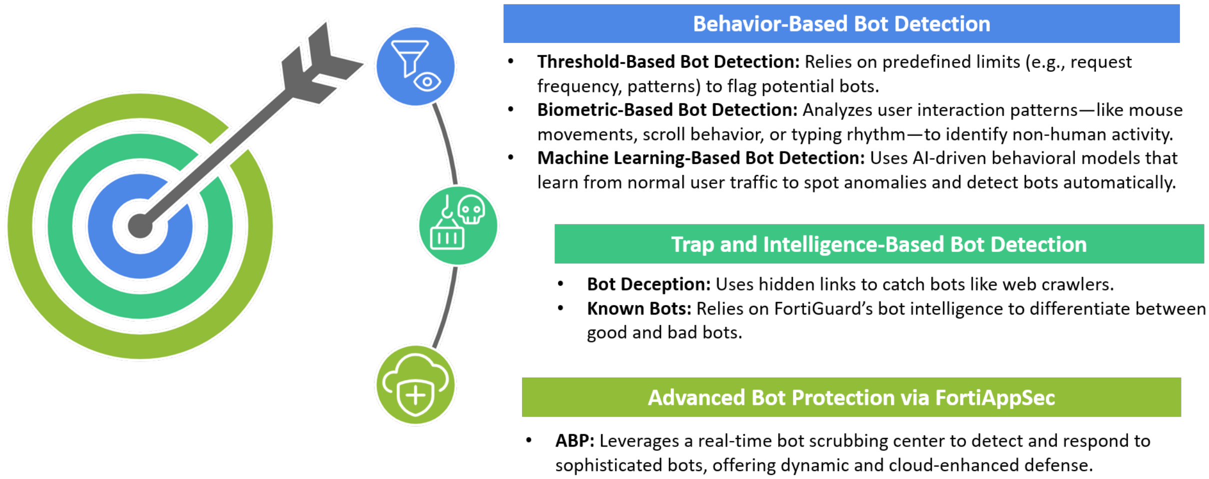


FortiWeb's Client-Side Protection feature automatically scans and analyzes all third-party services and scripts loaded by your web application. It helps you monitor client-side risks and take action directly, without requiring manual tracking of external dependencies.

WAF features against bot attacks

Bot attacks are malicious activities carried out by automated software programs, known as bots. These attacks exploit vulnerabilities in web applications, APIs, and network infrastructure to achieve various malicious goals, such as data theft, service disruption, or fraud. Unlike legitimate bots (e.g., search engine crawlers), malicious bots are designed to mimic human behavior and can execute tasks at a scale and speed that humans cannot match.

FortiWeb offers a range of features specifically designed to detect and mitigate bot attacks, providing robust protection for web applications and APIs. Using a combination of behavioral analysis, AI-based detection, and rate-limiting controls, FortiWeb can identify and block malicious bots while ensuring a seamless experience for legitimate users.



Behavior-Based Bot Detection

- **Threshold-Based Bot Detection:** Relies on predefined limits (e.g., request frequency, patterns) to flag potential bots.
- **Biometric-Based Bot Detection:** Analyzes user interaction patterns—like mouse movements, scroll behavior, or typing rhythm—to identify non-human activity.
- **Machine Learning-Based Bot Detection:** Uses AI-driven behavioral models that learn from normal user traffic to spot anomalies and detect bots automatically.

Trap and Intelligence-Based Bot Detection

- **Bot Deception:** Uses hidden links to catch bots like web crawlers.
- **Known Bots:** Relies on FortiGuard's bot intelligence to differentiate between good and bad bots.

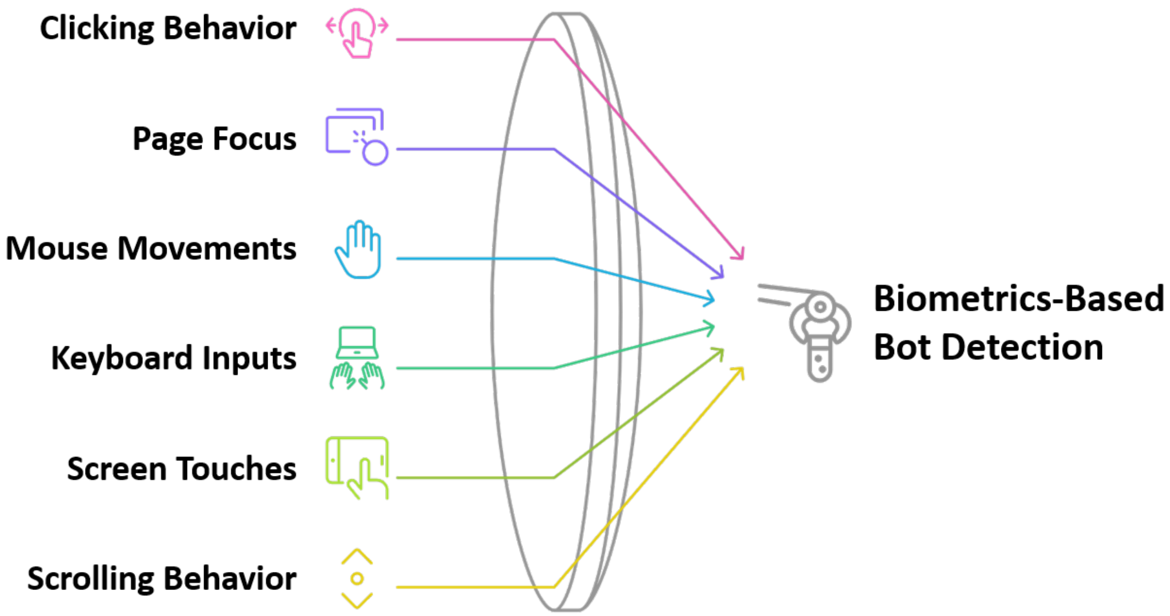
Advanced Bot Protection via FortiAppSec

- **ABP:** Leverages a real-time bot scrubbing center to detect and respond to sophisticated bots, offering dynamic and cloud-enhanced defense.

Here are the key features FortiWeb employs to defend against bot attacks.

- Biometrics-Based Bot Detection
- Threshold-Based Bot Detection
- Bot Deception
- Known Bots
- Machine Learning Based Bot Detection
- Advanced Bot Protection
- DDoS Protection on page 33

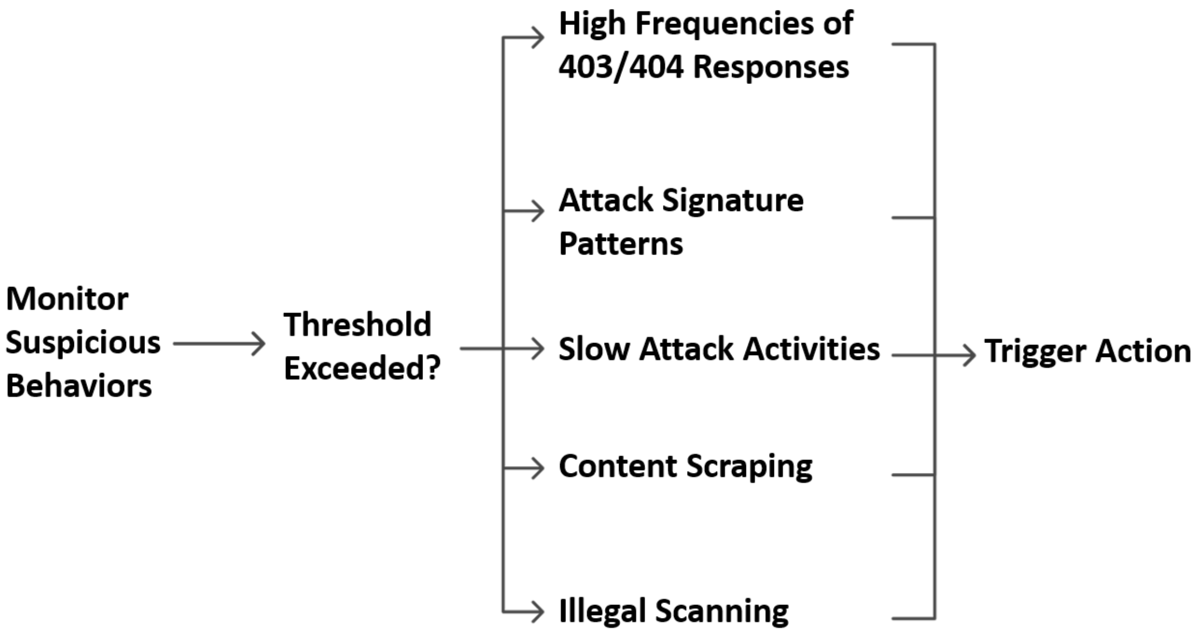
Biometrics-Based Bot Detection



FortiWeb’s Biometrics-Based Bot Detection is a sophisticated feature designed to differentiate between human users and bots by analyzing client-side interactions, such as mouse movements, keyboard inputs, screen touches, and scrolling behavior. This method provides a more nuanced approach to bot detection, particularly useful for mitigating advanced bots that can bypass simpler detection mechanisms like IP blocking or user-agent validation.

Watch the video on Biometrics-Based Bot Detection by clicking this link.

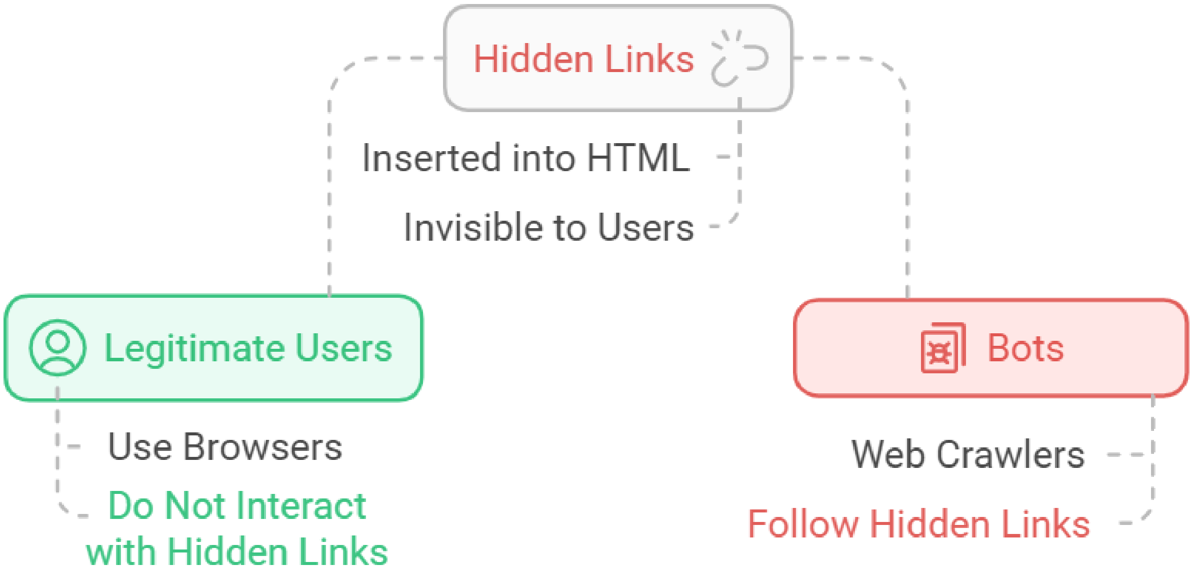
Threshold-Based Bot Detection


Monitor Suspicious Behaviors
Threshold Exceeded?
High Frequencies of 403/404 Responses
Attack Signature Patterns
Slow Attack Activities
Content Scraping
Illegal Scanning
Trigger Action

FortiWeb’s Threshold-Based Bot Detection is a feature that helps distinguish between human users and automated bots by monitoring for suspicious behaviors that occur at abnormal rates, such as the frequency of 403 and 404 response codes, attack signatures, slow attack activities, content scraping activities, and illegal user scan.

Watch the video on Threshold-Based Bot Detection by clicking this link.

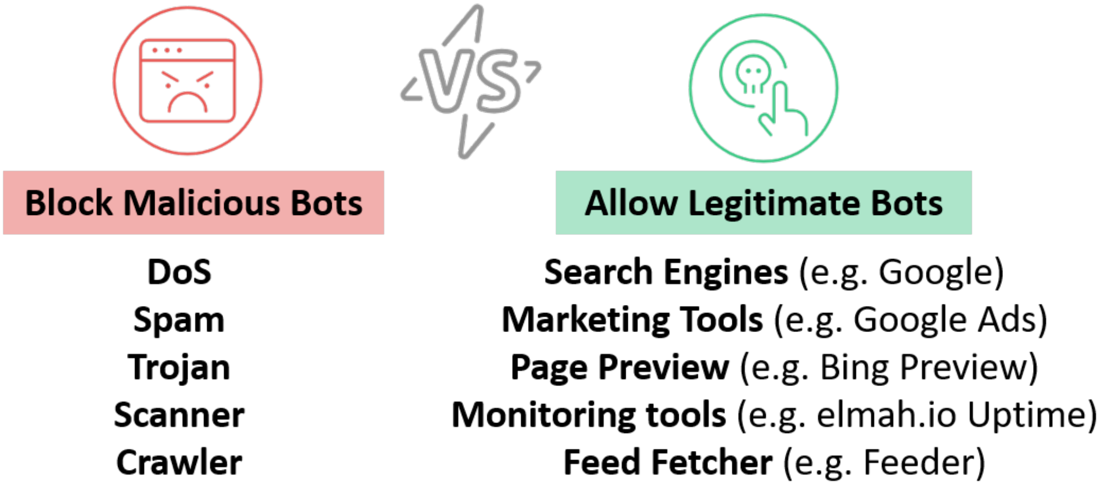
Bot Deception



FortiWeb’s Bot Deception feature is a proactive defense mechanism designed to detect and trap malicious bots, such as web crawlers, by inserting hidden links into the HTML response pages. Legitimate users, such as human visitors using a browser, will not interact with these invisible links, but bots (especially web crawlers) may inadvertently follow these links, exposing their automated behavior. Once identified, FortiWeb can take action against these bots, such as blocking their requests or logging the activity for further investigation.

Watch the video on Bot Deception by clicking this link.

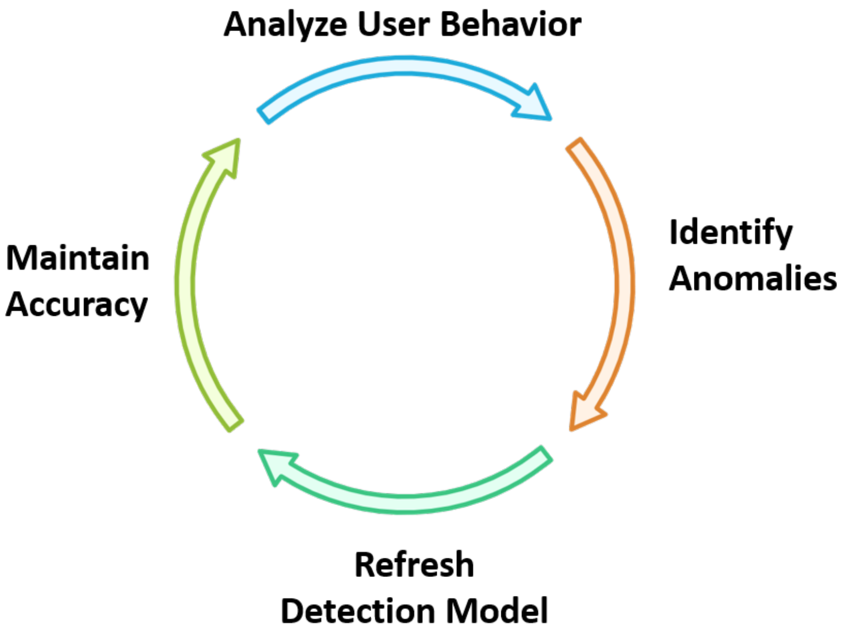
Known Bots


VS
Block Malicious Bots
DoS
Spam
Trojan
Scanner
Crawler
Allow Legitimate Bots
Search Engines (e.g. Google)
Marketing Tools (e.g. Google Ads)
Page Preview (e.g. Bing Preview)
Monitoring tools (e.g. elmah.io Uptime)
Feed Fetcher (e.g. Feeder)

FortiWeb’s Known Bots feature is designed to help manage and differentiate between legitimate bot traffic (such as search engine crawlers) and malicious bots (such as DDoS bots, spammers, or content scrapers). By doing so, it helps protect your websites, mobile applications, and APIs from unwanted bot attacks without disrupting the flow of critical and beneficial traffic.

Watch the video on Known Bots by clicking this link.

Machine Learning Based Bot Detection

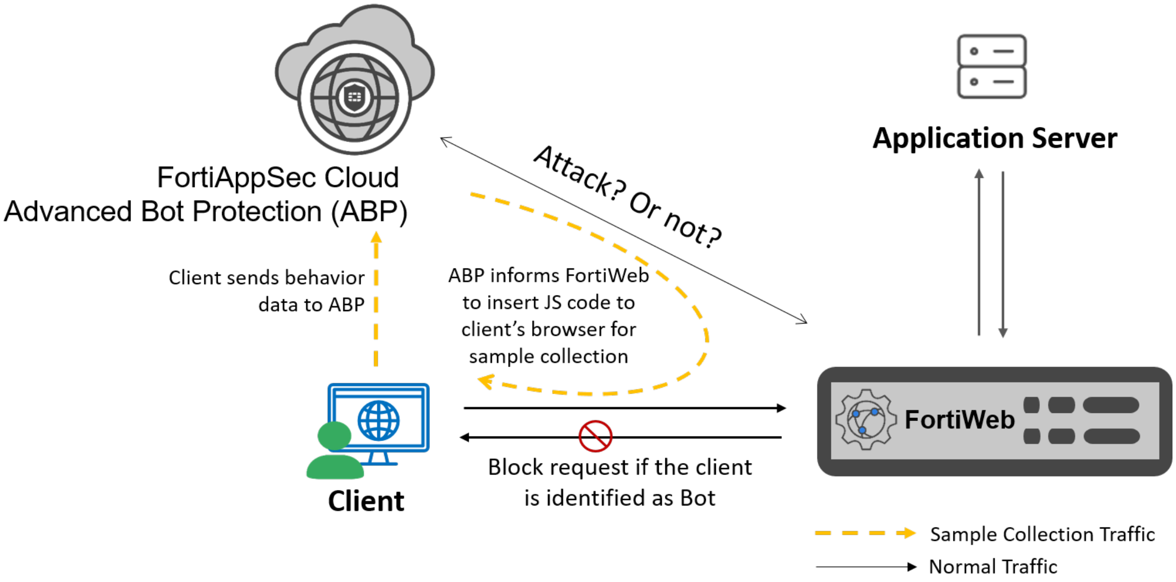


FortiWeb's AI-based machine learning bot detection enhances traditional signature and threshold-based methods by identifying sophisticated bots that might otherwise evade detection.

- It analyzes user behavior across thirteen dimensions, such as the frequency of HTTP requests and the use of illegal HTTP versions, without requiring manual threshold configuration.
- Using a Support Vector Machine (SVM) algorithm, FortiWeb automatically learns the behavior patterns of regular users, comparing incoming traffic to these patterns to identify anomalies.
- If user behavior changes significantly—due to application updates, for example—FortiWeb adapts by refreshing its model to maintain accurate detection. This automated, adaptive approach reduces the need for manual adjustments and experimentation, ensuring more effective and efficient bot detection.

Watch the video on Machine Learning Based Bot Detection by clicking this link.

Advanced Bot Protection


FortiAppSec Cloud
Advanced Bot Protection (ABP)
Application Server
Attack? Or not?
Client sends behavior data to ABP
ABP informs FortiWeb to insert JS code to client's browser for sample collection
FortiWeb
Client
Block request if the client is identified as Bot
Sample Collection Traffic
Normal Traffic

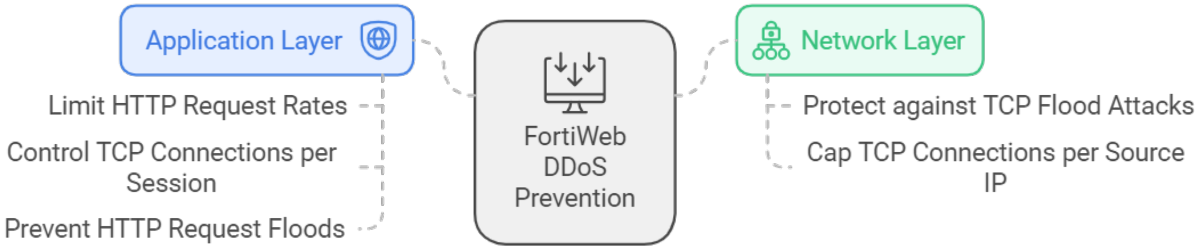
FortiWeb has integrated the FortiAppSec Cloud's Advanced Bot Protection (ABP) service. It is a Fortinet SaaS advanced bot mitigation solution designed to detect and protect against sophisticated bots.

To detect bot activity, the ABP service injects a lightweight JavaScript into the client's browser. This script collects behavioral data and request samples, which are then used to train a machine learning model capable of identifying patterns associated with normal user interactions.

All communication between FortiWeb and the ABP service is encrypted using TLS. To ensure authenticity and integrity, both FortiWeb and ABP present certificates to establish mutual TLS authentication. This safeguards the attack query process from potential interception or tampering by malicious actors.

Watch the video on Advanced Bot Protection by clicking this link.

DDoS Protection


Application Layer
Limit HTTP Request Rates
Control TCP Connections per Session
Prevent HTTP Request Floods
FortiWeb DDoS Prevention
Network Layer
Protect against TCP Flood Attacks
Cap TCP Connections per Source IP

FortiWeb provides Application Layer DoS Prevention and Network Layer DDoS Prevention.

- FortiWeb's Application Layer DoS Prevention strategies aim to mitigate malicious traffic like HTTP floods and high connection rates while safeguarding legitimate user access. This is achieved by limiting HTTP request rates, controlling TCP connections per session, and preventing HTTP request floods.

- For Network Layer DDoS Prevention, FortiWeb offers protection against TCP flood attacks by capping the number of fully-formed TCP connections per source IP. This helps prevent network-level attacks that attempt to exhaust server resources by opening an excessive number of TCP connections, thereby maintaining server stability and performance.

Conclusion

The goal of Fortinet's Web Application Firewall FortiWeb is to enhance web application security while reducing the operational burden on security teams. FortiWeb achieves this by integrating advanced AI-driven threat detection and anomaly detection, and behavior-based bot mitigation, combined with signature-based protection and API security into a Web Application Firewall (WAF) solution. These technologies work together to provide real-time threat intelligence, adaptive security policies, and automated attack mitigation, ensuring robust protection against evolving web application threats.

By leveraging FortiWeb, organizations can defend against OWASP Top 10 threats, API vulnerabilities, automated bot attacks, and DDoS threats, ensuring secure and resilient web applications. To learn more about FortiWeb’s security capabilities, refer to the FortiWeb Deployment Guide and FortiWeb Configuration Guide, or explore additional resources available in the Appendix.

More information

Feature documentation

- FortiWeb Administration Guide
- FortiWeb CLI Reference
- Deploying FortiWeb-VM on public cloud platforms
- Deploying FortiWeb-VM on private cloud platforms

4D documentation - Define, Design, Deploy & Demo

- **WAF Concept Guide**
  Provides a broad overview of Web Application Firewall (WAF) concepts and FortiWeb's core features. Includes infographics and embedded videos for easier understanding.
- **WAF Architecture Guide**
  Presents a high-level overview of FortiWeb deployment architectures across various operation and high availability (HA) modes. Explains traffic flows, key benefits, and limitations of each mode to help you choose the most suitable setup for your network topology.
- **WAF Solutions against OWASP Top10 Risks**
  Introduces the OWASP Top 10 Web Application Security Risks with real-world use cases. Offers step-by-step FortiWeb configuration guidance to mitigate each risk.
- **WAF solutions against OWASP Top 10 API Security Risks**
  Covers the OWASP Top 10 API Security Risks with real-world examples. Offers step-by-step FortiWeb configuration guidance to effectively defend against these risks.
- **WAF Solutions Against OWASP Top 10 Client-Side Security Risks**
  Explores the OWASP Top 10 Client-Side Security Risks using practical use cases. Offers step-by-step FortiWeb configuration guidance to mitigate these threats.
- **WAF solutions Against Bot Attacks**
  Explains common bot attack types through real-world scenarios. Offers step-by-step FortiWeb configuration guidance to detect and block malicious bot activity.

Videos on how to use FortiWeb

We regularly share videos on configuring FortiWeb to prevent and mitigate attacks. Stay updated by following FortiWeb's video channel: https://video.fortinet.com/products/fortiweb www.fortinet.com