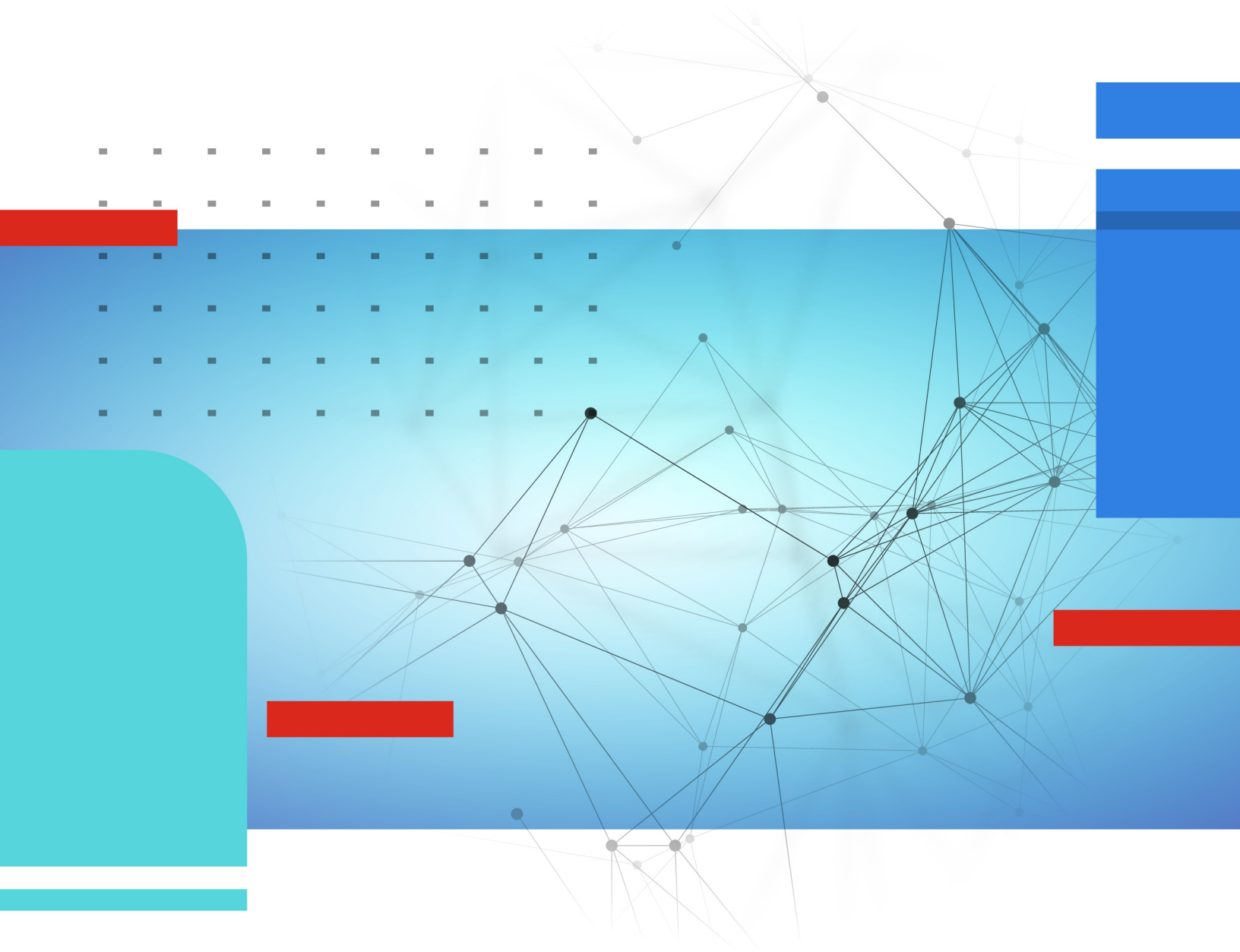
WAF Solutions against Bot Attacks

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 Solutions against Bot Attacks

TABLE OF CONTENTS

WAF solutions against bot attacks

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.

Key Bot-Related Threats

- **Credential Stuffing**
  Credential stuffing occurs when attackers use stolen username-password combinations from previous data breaches to gain unauthorized access to user accounts. Bots automate these login attempts, testing thousands of credentials across multiple platforms.
- **Web Scraping**
  Scraping bots systematically extract competitive intelligence, pricing information, or proprietary data from websites without authorization. While some scrapers are harmless, others engage in data theft, intellectual property violations, and unfair competitive practices.
- **Account Takeover (ATO) Attacks**
  Automated bots attempt to hijack user accounts by exploiting weak credentials or security flaws. ATO attacks often involve credential stuffing, brute-force attacks, or session hijacking to gain control over user accounts, leading to identity fraud, financial theft, and data breaches.
- **API Abuse & Enumeration**
  APIs are a common target for bot-driven attacks, where automated scripts exploit API endpoints to extract data, test credentials, or identify vulnerabilities. Attackers may attempt API enumeration, where bots systematically guess API parameters to gain unauthorized access to sensitive information.
- **DDoS Attacks**
  Distributed Denial of Service (DDoS) attacks involve massive volumes of bot-generated traffic overwhelming web services, disrupting operations, and causing downtime. Attackers often use botnets—networks of compromised devices—to flood websites and APIs with malicious traffic.
- **Fake Account Creation & Spam**
  Bots are frequently used to create fake user accounts, generate spam content, and manipulate online platforms. These activities can lead to fraud, reputational damage, and resource exhaustion for businesses.

FortiWeb's Multi-Layered Bot Protection

To effectively mitigate malicious bot activity, FortiWeb employs a combination of AI-driven detection, behavioral analysis, and real-time threat intelligence:

- **Known Bots Detection** – FortiWeb's **Known Bots** feature utilizes global threat intelligence to block traffic from known malicious botnets, stopping automated attacks at the network edge.
- **Proactive Bot Deception** – The **Bot Deception** feature uses hidden links and traps to expose and intercept automated crawlers and unauthorized scrapers that do not behave like legitimate users.
- **Behavioral AI & Anomaly Detection** – FortiWeb provides several advanced detection methods:

    - **Threshold-Based Detection**: Flags abnormal behavior based on predefined metrics like request rates and repetitive patterns.
    - **Biometric-Based Detection**: Analyzes user interactions such as mouse movements, scrolling, and typing rhythms to distinguish bots from real users.
    - **Machine Learning-Based Detection**: Builds dynamic behavioral models from legitimate traffic to automatically identify and respond to anomalies.
- **CAPTCHA & JavaScript Challenges** – FortiWeb employs progressive challenge mechanisms to verify human users, effectively blocking bots that cannot process JavaScript or solve CAPTCHA tests.
- **Scrubbing Center-Based Bot Detection** – FortiWeb integrates with the **Advanced Bot Protection** service powered by FortiAppSec, a Fortinet SaaS solution designed to detect and mitigate sophisticated automated threats. It defends against data harvesting, credential stuffing, account takeovers, application-layer DDoS, and other forms of fraudulent bot activity using real-time bot intelligence and cloud-based traffic analysis.
- **DoS Attack Mitigation** – FortiWeb delivers robust protection against both application-layer and network-layer denial-of-service (DoS) attacks, including HTTP floods, TCP SYN floods, and excessive connection attempts.

Watch the following videos on FortiWeb's Bot Mitigation features:

- Mitigating Bots with FortiWeb: Overview
- FortiWeb Bot Protection: Integrating with FortiAppSec for Advanced Bot Protection
- FortiWeb Bot Protection: Biometrics based Bot Detection
- FortiWeb Bot Protection: Bot Deception
- FortiWeb Bot Protection: Mitigating Known Bots
- FortiWeb Bot Protection: Machine Learning based Protection
- FortiWeb Bot Protection: Threshold based Detection

For best practices of configuring your WAF to effectively defend against the bot attacks, see WAF Solutions against Bot Attacks.

Defending against Credential Stuffing attacks

A retail website experiences a sudden spike in login attempts. Most fail, but some succeed, leading to account takeover and misuse of stored credit card details. They found out that a botnet is used to test millions of stolen username/password combinations (from previous data breaches) against login pages of their application.

Challenges

- Unauthorized access to user accounts
- Financial theft or unauthorized purchases
- Account lockouts for legitimate users
- Increased fraud detection costs

Solutions by FortiWeb

Bots used in credential stuffing attacks exhibit distinct and detectable behaviors that differ from those of legitimate users. FortiWeb offers a range of features specifically designed to identify and block such malicious requests.

Threshold-Based Bot Detection

The Illegal User Scan in FortiWeb's Threshold-Based Detection feature is designed to detect "user testing" behavior commonly associated with credential stuffing and account enumeration attacks. It identifies login attempts where an attacker submits a high number of different usernames or email addresses—particularly those that do not exist—within a short time frame.

To effectively use this feature, go to **Bot Mitigation > Threshold Based Detection** and configure the Illegal User Scan settings as follows. When the number of detected login attempts exceeds the defined threshold, FortiWeb flags the activity as an illegal user scan and applies the configured action (e.g., block, alert, log).

Illegal User Scan	Enable
Request URL	/login Narrow the scope to the login endpoint to avoid false positives from other parts of the site.
Occurrence	20-30 Prevents abuse by detecting too many unique usernames in a short time.
Within (Seconds)	10 or 30 Use a small time window to catch high-speed automation typical of bots.

In addition to Illegal User Scan, FortiWeb's Threshold-Based Detection can also detect other forms of bot activity, including crawling, vulnerability scanning, slow attacks, and content scraping.

For more details, see Configuring threshold based detection.

Machine Learning-Based Bot Detection

FortiWeb's Machine Learning-Based Bot Detection builds a behavioral model by learning what normal login activity looks like. It then uses this model to detect anomalies—such as high-volume login attempts from unusual IP addresses or devices—that may indicate automated "user testing" behavior. The following behavioral dimensions are commonly associated with credential stuffing and are used to identify bots:

HTTP request	Bots testing large username/password sets send many HTTP requests in a short time (usually POST to /login).
HTTP error responses	Repeated login failures (e.g., 401 Unauthorized) are a clear signal of username/password testing attempts.
TCP connection	Bots often open excessive connections to retry logins with different credentials.
Seconds with throughput	Sustained traffic during the whole sampling period often indicates automated, high-frequency login attempts.

Average duration with throughput	Bots usually maintain long, consistent traffic bursts unlike human behavior (which is more bursty or varied).

In addition to these dimensions, FortiWeb's machine learning model analyzes a broader set of behavioral indicators to detect other types of bot attacks beyond credential stuffing. For more details, see Configuring ML Based Bot Detection policy.

Biometric-Based Bot Detection

When a credential stuffing bot successfully logs in (i.e., it hits a valid username/password pair), FortiWeb can still recognize and mitigate it based on what happens after login — by analyzing user behavior patterns.

FortiWeb injects JavaScript into pages to track:

- Mouse movement
- Keyboard input
- Touch events
- Scrolling behavior
- Field focus changes and durations

If the session lacks these human signals, FortiWeb identifies it as a bot—even if the credentials were correct.

Behavior Expected from a Human	Bot-Like Behavior Detected by FortiWeb
Moves mouse, scrolls, pauses between actions	No mouse movement, rapid clicks, or unnatural scrolling
Navigates pages slowly or explores features	Immediately hits APIs or specific endpoints in a fixed sequence
Types or edits fields with variable timing	Inputs are automated and unnaturally fast or uniform
Has irregular delays between requests	Requests sent in uniform time intervals (like a script or loop)
Loads JS, CSS, and other frontend assets	May skip JS/CSS and go straight to JSON/XML APIs for scraping

For detailed information on this feature, see Configuring biometrics based detection.

Advanced Bot Protection (via FortiAppSec)

Advanced Bot Protection, integrated via FortiAppSec, provides FortiWeb with enhanced capabilities to detect and mitigate sophisticated bot-driven threats such as credential stuffing, account takeover attempts, and automated login abuse.

This cloud-based service uses real-time threat intelligence and a global bot behavior database to identify malicious automation patterns that may bypass traditional on-premise detection techniques. When suspicious activity is detected—such as repeated login attempts from distributed sources or high-volume credential testing—FortiWeb can coordinate with the cloud-based scrubbing center to inspect, challenge, or block the bot traffic before it reaches your application.

Advanced Bot Protection can:

- Detect abnormal patterns typical of Credential Stuffing (e.g., repeated login attempts using different usernames or passwords across multiple sessions or IP addresses)
- Analyze behavior using advanced analytics and global threat intelligence
- Offload bot traffic to the scrubbing center to minimize impact on the origin server

For detailed information on this feature, see Configuring Advanced Bot Protection policy.

CAPTCHA and reCAPTCHA challenges

Bot Confirmation is integrated into Threshold-Based Bot Detection, Machine Learning-Based Bot Detection, and Advanced Bot Protection in FortiWeb. It enables FortiWeb to present a CAPTCHA or reCAPTCHA challenge—such as a puzzle—to verify whether the client is human when suspicious, automation-like behavior is detected.

The goal of this feature is to distinguish bots from legitimate users while minimizing disruption. Clients exhibiting normal interaction patterns will not be prompted—challenges are only triggered when behavior closely resembles that of a bot.

In addition to CAPTCHA and reCAPTCHA challenges, which determine whether the client is a human, **Bot Confirmation** in FortiWeb also supports Real Browser Enforcement to verify whether a request originates from a real browser. For an example of how Real Browser Enforcement is applied, see the scenario "Defending against Content Scraping bots on page 8".

Next step

- Add the **Threshold-Based Bot Detection** and **Biometric-Based Bot Detection** rules to a **Bot Mitigation Policy**. See Configuring bot mitigation policy.
- Apply the **Bot Mitigation** policy, **Machine Learning-Based Bot Detection** policy, and **Advanced Bot Protection** policy to a web protection profile and then reference the profile in a server policy. See:
- Configuring a protection profile for inline topologies
- Configuring an HTTP server policy

Conclusion

Together, these mechanisms allow FortiWeb to effectively stop credential stuffing attempts—not only by blocking failed login attempts but also by recognizing bots that have successfully logged in with stolen credentials. FortiWeb's intelligent bot mitigation capabilities ensure strong protection against automated attacks while maintaining a seamless experience for legitimate users.

Defending against Content Scraping bots

Bots can be deployed to extract product details, pricing, or intellectual property from a competitor's website. For example, a travel booking site finds that a competitor is using bots to constantly monitor and undercut its flight or hotel pricing in near real-time.

Challenges

- Competitive disadvantage through price undercutting
- Server performance degradation due to excessive bot traffic
- Violation of terms of service or copyright

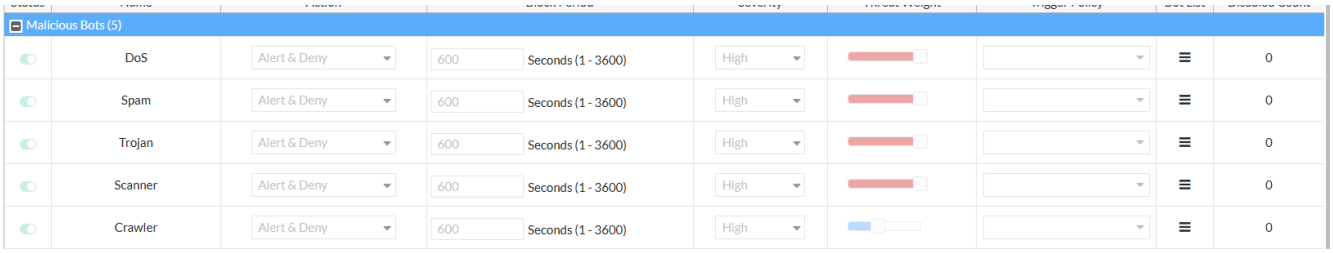
Solutions by FortiWeb

Content scraping bots pose a significant risk to business competitiveness, system performance, and data integrity. FortiWeb provides a comprehensive, multi-layered defense against these threats.

Known Bots

FortiWeb's **Known Bots** feature leverages FortiGuard threat intelligence to identify and block:

- Known malicious scrapers
- Bots with identifiable signatures (user-agent strings, IPs, behaviors)
- Common tools like curl, python-requests, outdated browser versions, etc.



If the bot scraping your travel site:

- Uses a known bad IP address or ASN
- Sends requests with obvious or default user-agent headers
- Behaves like a generic crawler or scanner

Then FortiWeb can block it via the **Crawler** or **Scanner** profiles under **Malicious Bots**.

FortiWeb regularly updates bot signatures and IP reputation data from FortiGuard, ensuring that the latest bots can be effectively identified and mitigated in real time.

For more details, see Configuring known bots.

Bot Deception

FortiWeb's **Bot Deception** inserts invisible or fake elements (such as hidden links or fields) into your web application responses. These elements are not seen or interacted with by legitimate users using normal browsers.

However, scraping bots that:

- Parse and fetch all page elements, regardless of visibility
- Don't process CSS/DOM correctly (i.e., don't ignore hidden content)

- Crawl all links blindly, including those not exposed to real users

will interact with these deceptive elements and reveal themselves as bots.

Bot Deception is an effective anti-scraping solution that operates invisibly without impacting user experience. It delivers low false positives and detects bots even when they use rotating IPs or mimic browser headers.

For more details, see Configuring bot deception.

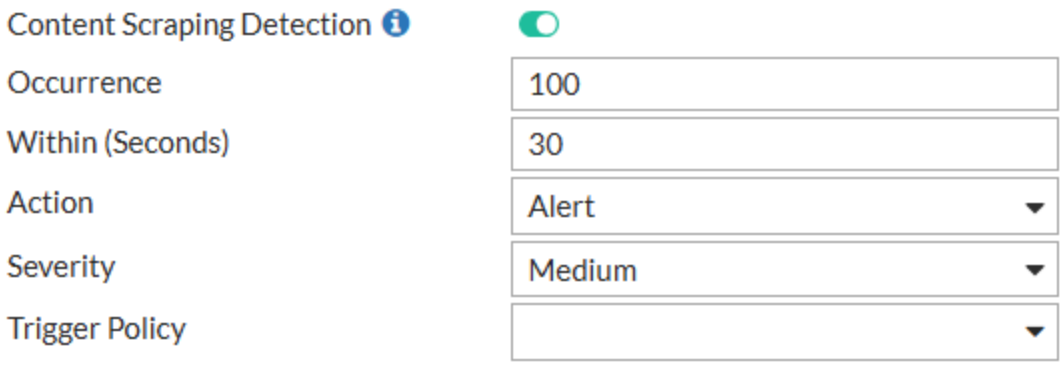
Threshold-Based Bot Detection

FortiWeb's **Threshold-Based Detection** monitors request volume, type, and frequency within a defined time window. It is effective for identifying scraping patterns, such as:

- High-frequency `GET` requests to product listing or pricing pages
- Access to large numbers of URLs in a short period
- Repeated requests to the same endpoint (e.g., /search, /flights, /hotels)

When these behaviors exceed the configured threshold (e.g., >100 requests to /pricing in 10 seconds), FortiWeb can take action (block, alert, log, etc.).

Below is the **Content Scraping Detection** settings in FortiWeb.



In addition to Content Scraping, FortiWeb's Threshold-Based Detection can also detect other forms of bot activity, including crawling, vulnerability scanning, slow attacks, and illegal user scan. For more details, see Configuring threshold based detection.

Machine Learning-Based Detection

FortiWeb's **Machine Learning-Based Bot Detection** builds a behavioral model by learning what normal user activity looks like across 13 behavioral dimensions. Several of these dimensions are particularly effective in distinguishing between legitimate user behavior and the automated, high-frequency, and selectively targeted patterns typical of scraping bots.

Dimension	How It Helps Detect Scraping Bots
HTTP Request	Scrapers often make a large number of GET requests to product or content pages in a short time.
HTTP HEAD Methods	Some scrapers use HEAD requests to check resources without downloading the

Dimension	How It Helps Detect Scraping Bots
	full content, which normal users rarely do.
HTTP Requests Without Referers	Bots often omit the Referer header because they don't navigate like users (e.g., clicking links from within the site).
HTTP Requests Without User-Agent	Scrapers may send requests with missing or generic User-Agent strings, unlike normal browsers.
HTML Pages	Scrapers may avoid HTML and instead fetch structured data (JSON, XML), which indicates non-standard access behavior.
JavaScript/CSS Resources	Scrapers typically skip JS/CSS and only pull raw content, whereas real browsers load full pages.
JSON/XML Resources	Scrapers often target API endpoints or structured data sources and make high-frequency requests.
Seconds with Throughput	Scrapers maintain sustained activity throughout the sampling period, unlike bursty human traffic.
Average Duration with Throughput	Bots tend to produce consistent traffic over time, while human sessions are more varied and shorter.

In addition to these dimensions, FortiWeb's machine learning model analyzes a broader set of behavioral indicators to detect other types of bot attacks beyond scraping bots. For more details, see Configuring ML Based Bot Detection policy.

Advanced Bot Protection (via FortiAppSec)

FortiWeb integrates with **Advanced Bot Protection**, a cloud-based service powered by FortiAppSec, to defend against sophisticated and evasive bots—including those used for content scraping, API abuse, credential stuffing, and other forms of automated attacks.

This service leverages real-time bot intelligence gathered from Fortinet's global threat network and a cloud-based scrubbing center to detect and mitigate bots that may bypass traditional, on-premise detection methods. It is particularly effective against distributed scraping operations that rotate IPs, mimic human behavior, or use headless browsers.

Advanced Bot Protection can:

- Detect abnormal patterns typical of scraping bots (e.g., repeated requests to structured data endpoints like pricing APIs)
- Analyze behavior using advanced analytics and global threat intelligence
- Offload bot traffic to the scrubbing center to minimize impact on the origin server

By incorporating this cloud-native defense, FortiWeb enhances its ability to stop even zero-day or previously unknown bots in real time.

For detailed information on this feature, see Configuring Advanced Bot Protection policy.

Real Browser Enforcement

Content scraping is typically carried out by non-browser clients, such as scripts, headless browsers, or automated tools like curl or python-requests, which do not behave like real users interacting through browsers.

To address this, FortiWeb integrates **Bot Confirmation** into **Threshold-Based Bot Detection**, **Machine Learning-Based Bot Detection**, and **Advanced Bot Protection**. One of the key mechanisms it uses is **Real Browser Enforcement**, which tests whether the client behaves like a real browser.

When **Real Browser Enforcement** is enabled, FortiWeb:

- Injects JavaScript into the HTTP response
- Requires the client to execute browser-like actions (e.g., DOM interaction, JS execution)
- Waits for the client to return the expected result within a defined Validation Timeout

Real Browser Enforcement significantly reduces false positives by ensuring that only non-browser automation tools are challenged or blocked, while legitimate users can proceed uninterrupted—even if their behavior is borderline.

You can enable **Real Browser Enforcement** when configuring Threshold-Based Bot Detection rules, as well as within the Machine Learning-Based Bot Detection and Advanced Bot Protection policies.

In addition to **Real Browser Enforcement**, which verifies whether a request originates from a real browser, Bot Confirmation in FortiWeb also supports CAPTCHA and reCAPTCHA challenges to determine whether the client is a human. For an example of how these challenges are applied, see the scenario "Defending against Credential Stuffing attacks on page 5".

Next step

- Add the **Known Bots**, **Bot Deception**, and **Threshold-Based Bot Detection** rules to a **Bot Mitigation Policy**. See Configuring bot mitigation policy.
- Apply the **Bot Mitigation** policy, **Machine Learning-Based Bot Detection** policy, and **Advanced Bot Protection** policy to a web protection profile and then reference the profile in a server policy. See:
- Configuring a protection profile for inline topologies
- Configuring an HTTP server policy

Conclusion

By integrating Known Bots filtering, Bot Deception, Threshold-Based Detection, Machine Learning-Based Detection, and Advanced Bot Protection, FortiWeb empowers organizations to accurately detect and stop scraping bots without disrupting legitimate users.

Defending against Inventory Hoarding & Scalping

Scalper bots can rapidly add high-demand items (e.g., concert tickets, GPUs, limited-edition sneakers) to carts or complete purchases before real users can. For example, during a flash sale, a bot buys out all PlayStation 5 consoles within seconds, which later appear on secondary markets at double the price.

Challenges

- Poor customer experience (legitimate users can't buy)
- Brand damage and social media backlash
- Resale at inflated prices on secondary markets

Solutions by FortiWeb

FortiWeb offers a multi-layered bot mitigation framework specifically designed to combat sophisticated automated threats like scalper bots. The following features work together to detect, challenge, and block scalper bots while preserving a seamless experience for legitimate users.

DoS Protection

FortiWeb's DoS Protection is designed to detect and block abusive traffic patterns at both the network layer and application layer. While its primary purpose is to prevent service disruptions—such as HTTP floods or excessive concurrent connections—some of its capabilities are also effective against scalper bots, which often generate rapid, high-volume requests during flash sales.

Relevant DoS Settings for Mitigating Scalper Bots

DoS Settings	How It Helps Against Scalpers
HTTP Request Rate Limits	Scalper bots often send large volumes of requests in milliseconds. FortiWeb can throttle or block clients exceeding normal rates.
Concurrent Connection Limits	Blocks clients that open too many simultaneous connections to gain a performance advantage.
Slow HTTP Attack Detection	While less relevant to scalping, it helps prevent bots trying to overload the system stealthily.

Note: DoS Protection does not analyze user behavior (e.g., mouse movement, scrolling, or interaction timing), so it may not detect scalper bots that mimic legitimate activity or stay within rate thresholds while acting unnaturally (e.g., instant cart submission or checkout).

It's recommended to use DoS Protection as a first layer to block obvious abusive traffic. For comprehensive protection, combine it with:

- **Biometric-Based Bot Detection** – to analyze real vs. automated behavior post-login
- **Machine Learning-Based Detection** – to identify deviations from normal user flow
- **Bot Confirmation** – to enforce CAPTCHA checks before taking actions

For detailed information on this feature, see DoS protection.

Biometric-Based Detection

Scalper bots often exhibit behaviors that differ significantly from those of legitimate users. These include **extremely fast and precise** interactions (e.g., instant form submissions with no delay), **skipping human-like actions** such as mouse movement, scrolling, or hesitation, and **relying on automation tools** like headless browsers or scripts that cannot fully replicate natural user interaction.

FortiWeb's **Biometric-Based Detection** injects JavaScript into web pages to collect data on user interactions, including:

- Mouse movement
- Keyboard input
- Click behavior
- Touch gestures
- Scroll behavior
- Focus changes and dwell time on fields

If a client fails to exhibit normal biometric signals—such as navigating too quickly, skipping UI interactions, or submitting forms without mouse or keyboard activity—FortiWeb can flag the session as a bot and apply the configured action (e.g., block, CAPTCHA, alert).

For detailed information on this feature, see Configuring biometrics based detection.

Machine Learning-Based Detection

FortiWeb's **Machine Learning-Based Bot Detection** builds a behavioral model by learning what normal user activity looks like across 13 behavioral dimensions. It can detect scalper bots effectively, focusing on dimensions that reveal automated, sustained, and unnatural session behavior.

Dimension	How It Helps Detect Scraping Bots
HTTP Request	Scalper bots send a high number of rapid requests, especially during flash sales or item launches.
Seconds with Throughput	Scalpers maintain sustained activity over the entire sampling period, unlike bursty human behavior.
Average Duration with Throughput	Their sessions are long and consistent, indicating automation, not human-paced interactions.
JavaScript/CSS Resources	Bots may skip loading these assets, while real browsers typically fetch them as part of page rendering.
HTTP Requests Without Referers	Scalper bots often bypass normal navigation, submitting requests directly without a referer header.
HTTP Requests Without User-Agent	Bots may send requests with missing or generic User-Agent strings, revealing automation.

In addition to these dimensions, FortiWeb's machine learning model analyzes a broader set of behavioral indicators to detect other types of bot attacks beyond Scalper bots. For more details, see Configuring ML Based Bot Detection policy.

Advanced Bot Protection (via FortiAppSec)

Advanced Bot Protection, integrated via FortiAppSec, provides FortiWeb with enhanced capabilities to detect and mitigate sophisticated bot-driven threats such as sophisticated scalper bots and other evasive forms of automated attacks.

This cloud-based service uses real-time threat intelligence and a global bot behavior database to identify malicious automation patterns that may bypass traditional on-premise detection techniques. It is especially effective against distributed scalping operations that rotate IP addresses, mimic browser behavior, or operate using headless automation tools.

Advanced Bot Protection can:

- Detect abnormal patterns typical of scalper bots (e.g., ultra-fast Add-to-Cart or Checkout requests)
- Analyze behavior using advanced analytics and global threat intelligence
- Offload bot traffic to the scrubbing center to minimize impact on the origin server

By integrating this cloud-native defense, FortiWeb significantly enhances its ability to detect and stop even stealthy or zero-day scalper bots in real time.

For detailed information on this feature, see Configuring Advanced Bot Protection policy.

CAPTCHA and reCAPTCHA challenges

Bot Confirmation is integrated into Threshold-Based Bot Detection, Machine Learning-Based Bot Detection, and Advanced Bot Protection in FortiWeb. It enables FortiWeb to present a CAPTCHA or reCAPTCHA challenge—such as a puzzle—to verify whether the client is human when suspicious, automation-like behavior is detected.

In scenarios like flash sales, you can enforce human validation at critical steps—such as Add to Cart or Checkout—to prevent scalper bots from successfully placing orders. CAPTCHA and reCAPTCHA challenges can be enabled as part of the Machine Learning-Based Bot Detection policy configuration.

The goal of this feature is to distinguish bots from legitimate users while minimizing disruption. Clients exhibiting normal interaction patterns will not be prompted—challenges are only triggered when behavior closely resembles that of a bot.

In addition to CAPTCHA and reCAPTCHA challenges, which determine whether the client is a human, **Bot Confirmation** in FortiWeb also supports Real Browser Enforcement to verify whether a request originates from a real browser. For an example of how Real Browser Enforcement is applied, see the scenario “Defending against Content Scraping bots on page 8”.

Next step

- Add the **Biometric-Based Detection** rule to a **Bot Mitigation Policy**. See Configuring bot mitigation policy.
- Apply the **Bot Mitigation** policy, **Machine Learning-Based Bot Detection** policy, and **Advanced Bot Protection** policy to a web protection profile and then reference the profile in a server policy. See:
- Configuring a protection profile for inline topologies
- Configuring an HTTP server policy

Conclusion

FortiWeb delivers a comprehensive, layered defense against such bots by combining behavior-based detection, biometric analysis, traffic rate controls, and real browser verification. When integrated with FortiAppSec's Advanced Bot Protection, FortiWeb can also identify and neutralize even the most evasive scalping operations in real time. By leveraging these capabilities, organizations can ensure fair access to inventory, preserve customer satisfaction, and safeguard the integrity of flash sales and high-demand product launches.

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

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.