Tencent Cloud EdgeOne

DDoS & Web Protection

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

DDoS & Web Protection Overview

Last updated：2024-08-01 21:37:22

Security protection provides secure policy configuration and security event alert options for applications integrating with EdgeOne. This helps you verify traffic and requests at the edge, preventing external attacks and security risks from impacting your business and sensitive data.

After integrating with EdgeOne's security acceleration service and subscribing to relevant security protection services, you can configure the following security policies:

Note:

DDoS protection is designed for network-layer defense against DDoS attacks and is suitable for L4 proxy applications (TCP/UDP applications). Configuration for DDoS protection is only available for users with Exclusive DDoS Protection Usage enabled.

If you need to configure Referer blocklist/allowlist, User-Agent (UA) blocklist/allowlist, IP blocklist/allowlist, or region blocking through Web protection, please navigate to **Web Protection > Custom Rules >Basic Access Control**. For more details, see Web Protection - Custom Rules.

The available rule configurations and execution methods may vary based on the EdgeOne plan you have subscribed to. See Comparison of EdgeOne Plans for package specifications.

Category	Function	Application Scenario	Default Configuration
DDoS Protection(DDoS protection at the network layer)	DDoS Protection Level	Automatic protection cleansing for DDoS attacks targeting L4 services (TCP/UDP applications). For example: Daily Protection: Utilize the `Moderate` protection level to discard traffic exhibiting clear DDoS attack characteristics. Emergency recovery during attack bypass: Implement the `Strict` protection level to discard all traffic suspected of DDoS attacks.	Protection Level: **Moderate**
	IP Blocklist/Allowlist	Discard or permit traffic from specified IP addresses.	None

		For example: Internal Call Permit: Permit the internal service IP `11.11.11.11` , allowing high-frequency access between services.	
	Configuration Region Blocking	Block client access from specified regions. For example: Ban access from overseas: Discard traffic with source IPs located outside mainland China.	None
	Configuration Port Filtering	Discard or allow traffic based on specified source/destination ports. For example: Discard high-risk reflection port: Drop traffic with `source port matching UDP 53` , prohibiting access to private UDP protocol applications.	None
	Configuration Features Filtering	Discard traffic containing specified data or parameters. For example: Discard unusually long UDP packets: Discard UDP traffic with a length exceeding 500.	None
	Configuration Protocol Blocking Rule	Discard traffic of specified IP protocols. For example: Block external PING commands: Configure blocking of ICMP protocol traffic.	None
	Configuration Connections Attack Protection	Intercept abnormal TCP behaviors such as high-frequency connections and abnormal connections.	None

Web Protection	Platform-hosted rate limiting (formerly CC Attack Defense)	Mitigate HTTP/HTTPS DDoS attacks, including high-frequency access and slow request attacks.	**Adaptive Frequency Control** Limit Level: Adaptive Loose - Disposal Method: JavaScript Challenge **Slow Attack Protection** Disabled **Intelligent Client Filtering** Disposal Method: JavaScript Challenge
	Managed Rules	Intercept vulnerabilities targeting web applications (SQL injection, cross-site scripting, remote code execution, etc.). For example: Intercept Apache log4j vulnerabilities: Enable rules related to log4j vulnerabilities in open-source components for interception.	All rules are enabled for observation mode.
	Custom Rules	Handle requests based on header content and IP. For example: Hotlink Protection: Intercept requests based on Referer header matching. Regional Blocking: Intercept requests from clients with IP matching specified regions. IP Blocklist: Intercept based on specified IP or IP groups.	None
	Rate Limiting	Intercept clients accessing beyond preset access rates. For example: Intercept clients causing a large number of errors in a short time at the origin: Set the rate allowed for each IP causing origin errors and intercept IP access beyond the threshold.	None

		Intercept account ID with excessively high access frequency to a specific API: Set the frequency allowed for each account (specified account ID position) to access a specific API, intercepting account access beyond the threshold. Intercept clients with excessively high access frequency fingerprints (JA3 fingerprints): Set the access rate for each JA3 fingerprint (i.e., TLS fingerprint) and intercept access with the same fingerprint beyond the threshold.	
	Protection Exception Rules - Skip Protection Modules	Skip protection rules in web protection by module. For example: Allow internal services: Set the internal service IP list and specified API paths to allow clients on the list unrestricted access to that path.	None
	Protection Exception Rules - Skip Specified Managed Rules	Skip specified managed rules. For example: Allow user content uploads: Configure business paths and false-positive rules to allow requests when parameters contain user-written content.	None
Bot Management	Bot Intelligent Analysis	Intercept bot requests based on risk levels. (Suitable for quickly enabling bot management strategies and establishing bot access profiles). For example: Intercept misuse of CDN resources (scraping):	None

		Intercept malicious bot requests.	
	Bot Basic Management	Handle crawlers for search engines, open-source development tools, and commercial purposes. For example: Allow Google search engine crawlers: Use search engine feature rule libraries to configure allowing Google search engine crawlers. Intercept cURL tool access: Use UA feature libraries to intercept access from web development tools.	None
	Client Reputation	Handle requests from clients with a history of malicious behavior or high-risk characteristics based on IP threat intelligence. For example: Intercept VPN/proxy requests: Intercept clients identified as malicious proxies, fast-dial IPs, or proxy IP pools.	None
	Active Detection	Intercept requests with abnormal browser runtime environments and access behavior. For example: Cookie Challenge: Enable cookie verification to intercept clients not supporting cookies. Intercept automated tool access: Enable client behavior verification to identify JavaScript runtime environment anomalies and abnormal access behavior in automated tools.	None
		Counteract bot tools based on	None

	Custom Bot Rules	the features, headers, and client IP of requests. The feature provides more disposal options for bot counteraction. For example: Counteract high-risk bots accessing sensitive business: Match based on access paths and client profiles, configure observation, silent, and response after waiting with certain weights.	

DDoS Protection

DDoS Protection Overview

Last updated：2025-05-30 10:07:58

What Is a DDoS Attack

A Distributed Denial of Service (DDoS) attack refers to an attacker remotely controlling a large number of zombie hosts through the network to send a large amount of attack requests to one or more targets, blocking the target server's network bandwidth or exhausting the target server's system resources, making it unable to respond to normal service requests.

The Harm of DDoS Attacks

If a DDoS attack causes business interruption or damage, it will bring huge commercial losses.

Significant economic loss: After suffering a DDoS attack, the origin server may not be able to provide services, causing users to be unable to access your business, resulting in huge economic losses and brand losses.

Data leakage: Hackers may take the opportunity to steal your core business data while launching a DDoS attack on your server.

Malicious competition: Some industries have vicious competition, and competitors may use DDoS attacks to maliciously attack your services, thereby gaining an advantage in industry competition.

DDoS Protection Usage Scenarios

Games: The game industry is a heavy-hit area for DDoS attacks. DDoS protection can effectively ensure the availability and continuity of games, guarantee a smooth experience for game players, and escort and protect activities, new game releases, or holiday game revenue peak periods to ensure the normal operation of the game business.

Internet: Ensure the smooth access of Internet web pages, uninterrupted normal business, and provide security escort for major events such as e-commerce promotions.

Finance: Meet the compliance requirements of the financial industry and ensure the real-time and security stability of online transactions.

Government: Meet the security needs of national government cloud construction standards, provide security guarantees for major conferences, events, and sensitive periods, ensure the normal availability of people's livelihood services, and maintain government credibility.

Enterprise: Ensure the continuous availability of enterprise site services, avoid economic and corporate brand image loss problems caused by DDoS attacks, and save security costs with zero hardware and zero maintenance.

EdgeOne DDoS Protection

DDoS Protection Scope

EdgeOne provides and enables protection against L3/L4 traffic-based DDoS attacks for all connected businesses. It monitors the network traffic in real time and performs traffic cleaning and filtering immediately after a DDoS attack is detected. The DDoS protection feature offers preset protection policies based on attack profiles, behavior pattern analysis, AI intelligent recognition, and other protection algorithms to detect and filter the following types of DDoS attacks.

Protection classification	Description
Malformed message filtering	Filter frag flood, smurf, stream flood, land flood attacks, filter IP malformed packets, TCP malformed packets, UDP malformed packets.
Network layer DDoS attack protection	Filter UDP Flood, SYN Flood, TCP Flood, ICMP Flood, ACK Flood, FIN Flood, RST Flood, DNS/NTP/SSDP reflection attacks, empty connections.
DNS DDoS attack	DNS DDoS attacks mainly include DNS Request Flood, DNS Response Flood, fake source + real source DNS Query Flood, Authoritative server attack, and Local server attack.
Connection-based DDoS attack	Connection-based DDoS attacks mainly refer to TCP slow connection attacks, Connection flood attacks, Loic, Hoic, Slowloris, Pyloris, Xoic, and other slow attacks.

DDoS Protection Specifications

The default protection specification of the EdgeOne platform provides basic DDoS protection capabilities and resources for all businesses connected to EdgeOne, enabling basic protection for most site businesses and TCP/UDP applications in daily use. On this basis, for businesses that have an expected higher risk of severe DDoS attacks, need to maintain long connections, or require customized traffic control policies, EdgeOne offers exclusive DDoS protection solutions that meet the corresponding traffic filtering needs. The specific specifications are as follows:

Feature Name	Default Platform Protection	Exclusive DDoS Protection
Automatic detection and cleaning of L3/L4 attacks[1]	✓	✓

Exclusive access IP address	-	✓
Dedicated bandwidth resources for DDoS protection[2]	-	✓
Exclusive cleaning center resources	-	✓
Supporting custom traffic filtering policies[3]	-	Supports configuring the following traffic filtering policies: IP blocking Region blocking Protocol blocking Port filtering Traffic feature filtering Connection-based attack filtering

Note:

Note 1: By default, automatic cleaning and protection is performed only for the attack traffic exceeding 100 Mbps (the attack traffic is based on traffic statistics of a single region and the threshold is for reference only. Please refer to actual protection).

Note 2: The default platform protection does not guarantee the resource capacity for DDoS protection. If your business has experienced traffic-based DDoS attacks, please consider selecting an appropriate specification of exclusive DDoS protection and reserving dedicated protection resources to ensure the business availability.

Note 3: Custom traffic filtering policies are only supported for L4 proxy instances with exclusive DDoS protection enabled. For sites accessed through the domain name, network traffic filtering is not supported. If you need to filter accessing clients, please use Web Protection - Custom Rules.

Note 4: The attack traffic cleaned by DDoS protection is not billed. For details, refer to About "clean traffic" billing instructions. For the billing mode of the traffic cleaned by exclusive DDoS protection, refer to Dedicated DDoS Mitigation Fee (Pay-as-You-Go).

Note 5: The actual protection capacity of the DDoS protection feature is dynamically adjusted based on the actual capacity and resource allocation of the infrastructure. When the scale of a DDoS attack exceeds the protection capacity of the EdgeOne infrastructure, EdgeOne will implement mitigation measures including (but not limited to) traffic scheduling, traffic throttling, and access blocking to ensure the infrastructure stability.

EdgeOne Exclusive DDoS Protection Introduction

Applicable Scenarios

Exclusive DDoS protection is an enhanced DDoS protection paid feature launched by EdgeOne, providing exclusive access to the cleaning center. When the platform's default protection cannot meet the smooth operation of your business, you can use Exclusive DDoS protection to help protect your business's normal operation. After Exclusive DDoS protection is enabled, it will provide your business with protection resources including the cleaning centers for traffic cleaning, and provide the promised protection bandwidth value according to the guaranteed protection capacity and elastic protection capacity you purchased.

Note:

1. Exclusive DDoS protection can only be subscribed to by EdgeOne Enterprise plan.
2. After an L7 site subscribes to exclusive DDoS protection, all sites within the same plan will share this exclusive DDoS protection subscription.
3. Each L4 proxy requires a separate subscription to exclusive DDoS protection.

Capability Introduction

1. The default access node uses the cleaning center, providing greater DDoS protection capabilities, up to T-level.
2. Promised protection capacity, flexible selection of Global (MLC excluded), Chinese mainland, and Global protection specs according to business deployment.
3. In addition to the automatic cleaning and recognition mechanism, EdgeOne DDoS protection can provide diversified and flexible custom DDoS protection strategies according to your business protection needs. You can flexibly set them according to the special characteristics of your business to deal with constantly changing attack methods. For L4 proxy instances, the following custom rule configuration capabilities are supported:

Note:

When a request matches multiple rules at the same time, it is processed in the following rule order.

Protection module	Configurations
IP blocklist/allowlist	Limit access to EdgeOne sites by matching IP blocklist/allowlist in DDoS attacks.
Port filtering	Limit access to EdgeOne sites within a specified port range by customizing port rules in DDoS attacks.
Protocol blocking	Allow users to access EdgeOne sites only through specified protocols.
Connection attack protection	Support protection against connection-based attacks and automatically block clients with abnormal connection behavior.
Feature filtering	Support custom blocking policies for IP, TCP, and UDP message headers or payloads in DDoS attacks.
Region blocking	Limit access to EdgeOne sites by matching regions in DDoS attacks.

Exclusive DDoS Protection Usage

Last updated：2025-05-30 10:09:33

Background Introduction

If your business has the following requirements for accessing services:

1. DDoS protection services with committed protection capacity, such as financial business, gaming platform services, etc.
2. When subjected to large-scale DDoS attacks, the business under the default platform protection may change the resolution IP due to business scheduling, which may affect the smooth operation of the business. You need to continuously maintain the session state business, including maintaining the DNS resolution IP unchanged, maintaining the TCP long connection and HTTP long session state. Such as: multiplayer online gaming services, voice services, etc.
3. Need to customize network layer DDoS protection strategy or network layer control strategy. For example, discard client traffic from specified regions.

It is recommended that you purchase exclusive DDoS protection services. Exclusive DDoS protection services provide further on the basis of the default platform protection:

1. Regular access to the cleaning center for continuous detection, cleaning, and filtering of malicious traffic.
2. Committed protection capacity with stable sessions maintained during protection. You can flexibly select protection specifications of global availability zones (excluding the Chinese mainland), Chinese mainland availability zones, or global availability zones based on your business deployment.
3. Customizable DDoS protection strategies, including IP-based and client region-based control options.

Help you mitigate DDoS attack risks and ensure business stability.

Policy Configuration

Exclusive DDoS protection can provide flexible custom DDoS protection and traffic control policies to meet your business protection requirements. You can respond to ever-changing attacks by flexible settings based on special business characteristics. For L4 proxy instances, the following custom rule features are supported:

Protection Module	Feature Description
IP Allowlist	Restricts access to EdgeOne sites in DDoS attacks by matching the IP allowlist/blocklist.
Port Filtering	Restricts access to EdgeOne sites from a specified port range in DDoS attacks by using custom port rules.
Protocol Blocking	Allows access to EdgeOne sites only through specified protocols.

Connection-based Attack Protection	Supports protection against connection-type attacks by automatically blocking clients with abnormal connection behaviors.
Feature Filtering	Supports custom blocking policies for IP, TCP, and UDP message headers or payload characteristics in DDoS attacks.
Regional Blocking	Restricts access to EdgeOne sites in DDoS attacks by matching regions.

Note:

1. Only L4 proxy instances with exclusive DDoS protection enabled support custom DDoS protection policies.
2. When the access traffic matches policies of multiple protection modules simultaneously, it is handled according to the module order shown in the table.

Usage Guide

Exclusive DDoS protection can be applied to both L7 and L4 services. You can refer to the following different scenarios to understand how to enable exclusive DDoS protection for your site.

Note：

Exclusive DDoS protection only supports Enterprise plans accessed after July 1, 2023. If you have accessed the EdgeOne Enterprise version before this date and want to use exclusive DDoS protection, please contact after-sales or technical support.

Scenario 1: Enable exclusive DDoS protection for L7 sites

Scenario Example

You provide a unified login service (SSO, Single-Sign-On) through the domain name `onelogin.example.com` , mainly serving users in the Chinese mainland. Due to frequent DDoS attacks, users may not be able to log in normally. The estimated daily attack level is 30Gbps, and the peak period may reach 50Gbps. You need to access exclusive DDoS protection to ensure the provision of stable and available services.

Precautions

After the exclusive DDoS protection is created within the L7 site, it is temporarily not supported to unsubscribe in the console. If you need to unsubscribe, please contact Tencent Cloud sales.

Enabling or disabling DDoS protection during the process may affect the business (connection reset, etc.), and the impact duration is estimated to be generally 2-3 minutes for enabling or disabling. If there is local or operator DNS cache, the switch may take effect later, and the specific effective time depends on the TTL configuration of the DNS record used by the client.

Operation Steps

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. On the site details page, click **Security > DDoS Mitigation**.
3. In the Site (L7) Service Protection tab, click **Subscribe Exclusive DDoS Protection**.

4. On the Subscribe Exclusive DDoS Protection Instance page, select the protection region and protection specs you need to subscribe to. In this scenario, based on the service area and historical attack level, you can choose to subscribe to the Chinese mainland availability zone with a guaranteed 30Gbps and an elastic capacity protection peak of 50Gbps.

5. After confirming the relevant fee information, check the box to agree to the relevant user agreement, and click **Subscribe Now** to start automatically issuing exclusive DDoS protection instance configurations for you.
6. After the instance is issued, you can enable exclusive DDoS protection for all domain names in the protection configuration page, or select `onelogin.example.com` in this scenario and enable exclusive DDoS protection for this domain name.
7. If you enable exclusive DDoS protection for a single domain name, a deployment confirmation window will pop up. Click Confirm to start the deployment, and wait for the deployment to complete before it takes effect.

Scenario 2: Enable exclusive DDoS protection for L4 proxy instances

Scenario Example

You have an upcoming game release that requires L4 proxy acceleration to optimize player login experience, transmitting TCP traffic data through port 80. The game is mainly distributed overseas, and it is expected to encounter large-scale DDoS attacks (not exceeding 300 Gbps) during the launch period. By accessing exclusive DDoS protection, you can ensure the stability of the login API service during the release and operation period, avoiding player loss.

Precautions

Currently, only new L4 proxy instances are allowed to select exclusive DDoS protection, and it cannot be modified or changed after creation;
Exclusive DDoS protection for L4 proxy is temporarily not supported for dynamic enabling/disabling.

Operation Steps

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. On the site details page, click **L4 Proxy**.
3. On the L4 Proxy Management Instance page, click **Create L4 Proxy**.

4. When creating an L4 proxy instance, you can select the corresponding protection method in the security protection configuration, switch to exclusive DDoS protection, and select Anycast joint defense 300Gbps for the current scenario.

5. After confirming the relevant user agreement and price information, click **Subscribe** to complete the creation of the L4 proxy instance. After creation, the platform will automatically issue exclusive DDoS protection configurations for the instance;
6. After the configuration is issued, you can click Configure to enter the instance configuration interface, add the required acceleration port information and origin address, and click **Save** to enable L4 proxy acceleration.

Related References

Working Principle

After enabling Exclusive DDoS protection, the traffic will be processed according to the following process:
1. When the client resolves the service DNS record, it will obtain the cleaning center address.
2. When the client accesses the service, the cleaning center first cleans the traffic, automatically identifies and filters the network layer DDoS attack traffic. If the current business has access to the L4 proxy service, the filtered traffic is accelerated by the L4 proxy service.
If your site includes L7 site acceleration, the traffic will continue to be forwarded according to the following steps:
3. After SSL authentication, HTTPS protocol requests continue to be protected by Web Protection and bot management security policies;
4. Requests that pass the security module verification will continue to go through site caching, site acceleration, and origin-pull service functions.

Configuration of Exclusive DDoS protection Rules

Increase DDoS Protection Level

Last updated：2025-05-30 10:10:36

The Protection level is the default protection template provided by EdgeOne DDoS protection. DDoS protection will automatically intercept traffic attacks that match the features according to the protection level. The following are the protection strategy descriptions for each protection level:

Note：

This function is only supported when the L4 proxy is enabled for Exclusive DDoS protection. The default platform protection and L7 site Exclusive DDoS protection do not support configuration.

Protection strategies for each protection level

Comparison items		**Loose** The cleaning strategy is relatively loose, and only attack packets with clear attack features are protected. It is suggested to enable when false interception is suspected, and complex attacks may penetrate.	**Moderate (default)** The cleaning strategy adapts to the vast majority of businesses and can effectively protect against common attacks. DDoS protection defaults to moderate mode.	**Strict** The cleaning strategy is relatively strict, and it is recommended to use when attack penetration occurs in normal mode.
Data packets with clear attack features	SYN data package	Filter	Filter	Filter
	ACK data package	Filter	Filter	Filter
	UDP data package	Filter	Filter	Filter
Data packets	TCP	Filter	Filter	Filter

not conforming to protocol specifications	data package			
	UDP data package	Filter	Filter	Filter
	ICMP data package	Filter	Filter	Filter
Attack data packets based on threat intelligence		Not filter	Filter	Filter
Active verification of some access source IP		Not filter	Filter	Filter
ICMP attack packet		Not filter	Not filter	Filter

Adjust protection level

If your business has the following two situations, it is recommended that you adjust the protection level:
During the current business operation, if there is false interception in the Log analytics, in order to ensure the availability of the business, you can reduce the protection strategy level to Loose;
During the current business operation, if there is still attack penetration to the origin under the Moderate protection level, it is recommended that you increase the protection level to Strict.
You can follow the steps below to adjust:

1. Log in to the EdgeOne console, click on the site list in the left menu bar, and click on the site to be configured in the site list to enter the site details page.
2. On the site details page, click **Security > DDoS Mitigation** to enter the DDoS protection detail page.
3. In the L4 proxy protection tab, select the L4 proxy protection instance that needs to be configured, and click **Security configuration**.
4. Find the L3/4 DDoS Protection level card, click **Set**, and adjust the protection level;

Exclusive DDoS Traffic Alarm

Last updated：2025-05-30 10:11:42

The DDoS attack traffic alert function allows users to set custom attack traffic rate alert thresholds for DDoS protection instances. When the detected attack traffic rate exceeds the set threshold, the system will send an alert notification to help users understand and respond to potential DDoS attacks in a timely manner. Upon receiving the attack traffic rate alert, users should pay attention to the operation of their business, refer to the number of connections, visitor volume, normal session count, and other normal business indicators, combined with the number of online users and other business indicators, to evaluate the health of their business and determine whether it is affected by a DDoS attack.

Note：

This function is only applicable to users who have subscribed to a separate DDoS protection instance, and the alert is only for L3/L4 (network layer) attack traffic rates.

Scenario: Configure alert thresholds for L4 proxy standalone DDoS protection instances

Example Scenario

A game client's current business has purchased a standalone DDoS protection capability for L4 proxy service, with a guaranteed protection capacity of 30,000 Mbps. When encountering a DDoS attack traffic exceeding 20,000 Mbps, the client needs to be informed and pay attention in advance so that they can take measures to upgrade their protection capability in time to avoid affecting the normal access of their business.

Directions

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. On the site details page, click on **Security** > **Alarm Notification**, and enter the details page.
3. In the DDoS alarms card, click on the **set**.
4. In the alert configuration page, for the current scenario, you can select the L4 proxy instance you need to configure, enable the custom threshold switch, click on edit, modify the alert threshold to 20000 Mbps, and click save to take effect.

Note：

The default alert domain is effective for all business types. If you need to customize the alert threshold, you need to enable the custom threshold switch.

Related Reference

Monitoring Range

The monitoring range of the DDoS attack traffic alert function is corresponding to the IP. In actual operation, multiple domain services may use the same protection instance IP, so the alert is for the protection instance, not the specific domain.

The set alert threshold is only for the detected attack traffic rate, not the total business traffic rate.

Trigger Method

Note：

The attack traffic rate alert is based on the instantaneous peak, while the attack traffic rate trend chart on the console is based on the minute dimension average, so there may be differences when comparing the two.

The DDoS attack traffic alert function uses the attack traffic rate instantaneous peak as the statistical method, with the unit being Mbps. The alert function monitors the traffic situation of the protection instance, and when the attack traffic rate reaches or exceeds the user-set threshold, it sends an alert notification.

Configuration IP blocklist/allowlist

Last updated：2025-05-30 10:12:34

Overview

EdgeOne DDoS protection service supports controlling client source IP blocking or releasing access requests by configuring IP blocklist and allowlist, thus limiting users accessing your application resources. Configuring IP blocklist/allowlist sets filtering or releasing rules for source IPs. When IPs in the allowlist access, they will be directly released without going through other protection strategies in the DDoS protection module (not affecting other module's protection strategies). When IPs in the blocklist access, they will be directly blocked.

Note：

1. This function is only supported when L4 proxy enables exclusive DDoS protection. To configure IP blocklist/allowlist for web sites, please use custom rule.
2. IP blocklist/allowlist rules will take effect within 5-10 seconds after saving.
3. Up to 8 IP groupings can be configured for IP blocklist/allowlist, and up to 2000 IPs can be filled in each group.

Usage Scenarios

Allow access only from IPs in the allowlist during an attack: When suffering from a DDoS attack, only allow users trusted by the allowlist to access the site, which can significantly reduce the security risk of the website, but may affect normal IP access requests not in the allowlist.

Block attack source IP directly with blocklist: Add confirmed attack source IP to the blocklist to block all access requests from that IP, reduce DDoS cleaning traffic, and reduce attack penetration.

Scenario 1: Release trusted IP requests through IP allowlist

For all business domain names under the site `example.com` , the IP address segment `1.1.1.1/24` is the trusted access IP of the site. To avoid misblocking trusted IPs, you can add the IP to the allowlist without going through the DDoS protection module cleaning. The operation steps are as follows:

1. Log in to the EdgeOne console, click Site List in the left menu bar, click the site to be configured in the site list, and enter the site details page.
2. On the site details page, click **Security Security > DDoS Mitigation** to enter the DDoS Protection details page.
3. In the L4 Proxy Protection tab, select the L4 proxy protection instance to be configured and click on **Security configuration.**
4. In the IP Blocklist/Allowlist card, click **Set** to enter the IP Blocklist/Allowlist configuration page.

5. In the IP Blocklist/Allowlist page, click Create, enter the IP segment `1.1.1.1/24` for the current scenario, select Type as Allowlist, and click **Save** to take effect.

Scenario 2: Permanently block attack source IP access requests through IP blocklist

For all business domain names under the site `example.com` , the IP address `1.1.1.1` has been confirmed as an attack source IP. You can directly add the IP to the blocklist to block all access requests from that IP. The operation steps are as follows:

1. Log in to the EdgeOne console, click Site List in the left menu bar, click the site to be configured in the site list, and enter the site details page.
2. On the site details page, click **Security > DDoS Mitigation** to enter the DDoS Protection details page.
3. In the L4 Proxy Protection tab, select the L4 proxy protection instance to be configured and click on **Security configuration.**
4. In the IP Blocklist/Allowlist card, click **Set** to enter the IP Blocklist/Allowlist configuration page.

5. In the IP Blocklist/Allowlist page, click Create, enter the IP `1.1.1.1` for the current scenario, select Type as Blocklist, and click **Save** to take effect.

Configuration Region Blocking Rule

Last updated：2025-05-30 10:13:18

Overview

If you find that all your attacks come from a specific region, or your business only allows access from specific regions and does not trust access from other regions, EdgeOne supports one-click blocking in the cleaning room by specifying a list of regions based on the source IP geographic region, helping you to custom block access requests from specified regions. After enabling region blocking, traffic from the blocked region to the EdgeOne site will be discarded. Supports multi-region and country traffic blocking.

Note：

1. This function is only supported when the L4 proxy is enabled for Exclusive DDoS protection, and is not supported for default platform protection and Exclusive DDoS protection for L7 sites;
2. After configuring region blocking, the attack traffic from that region will still be counted and recorded by the platform, but will not flow into the business origin.

Usage Scenarios

Exclude all attack behavior outside of trusted regions: If your current business is only applicable to specific regions, you can use region blocking to one-click block access clients from other regions in DDoS cleaning, avoiding attack sources from other regions from passing through to the origin.

One-click blocking of concentrated attack behavior in a region: If the main attack source of your current site is from a specific region, you can use region blocking to one-click block all access requests from that region in DDoS cleaning, more effectively preventing the attack from passing through.

Directions

For example: The current site users are all in China, only allowing Chinese users to access the site, not trusting access requests from other regions, in order to eliminate possible attack behavior from other regions, during a DDoS attack, all requests from other regions are blocked. The operation steps are as follows:

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. On the site details page, click **Security > DDoS Mitigation** to enter the DDoS Protection details page.

3. In the L4 proxy protection tab, select the L4 proxy protection instance you need to configure and click on **security configuration**.
4. In the region blocking card, click on **set** to enter the region blocking page.

5. On the region blocking configuration page, click the edit button on the right side of the blocking list, select the blocked region, in this case, select all regions except the Chinese mainland.

6. Click **save** to complete the region blocking configuration.

Configuration Port Filtering

Last updated：2025-05-30 10:13:58

Overview

Port filtering is used to precisely formulate protection strategies by specifying ports and protocols, controlling the ports and protocols that Clients can access EdgeOne. After enabling port filtering, you can customize the combination of protocol Type, source port Range, and destination port Range according to your needs, and set the strategy actions of intercepting, allowing, and continuing protection for the matched rules.

Note：

This function is only supported when L4 proxy is enabled for Exclusive DDoS protection, and Default platform protection and Exclusive DDoS protection for L7 site do not support Configuration.

Usage Scenarios

The origin has UDP business, and UDP reflection attack is filtered through port filtering: If your current origin business has UDP connections and cannot directly block UDP protocol access, you can configure the UDP access port that needs to be intercepted during DDoS washing in port filtering to prevent the transparent transmission of UDP reflection attacks. Common UDP reflection attack ports include: 1-52, 54-161, 389, 1900, 11211.

Wash non-allowed port access sources: When your origin only opens specified ports for access, you can configure the ports that are allowed to be accessed after DDoS washing through port filtering, and directly discard all access connections from other ports to reduce attack penetration.

Directions

For example, for all business domain names under the site example.com, the business only opens TCP protocol ports 110-155 to the outside, and other ports are not allowed to access. The operation steps are as follows:

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site that needs to be configured in the site list, and enter the site details page.
2. On the site details page, click on **Security > DDoS Mitigation** to enter the DDoS protection details page.
3. In the L4 proxy protection tab, select the L4 proxy protection instance that needs to be configured, and click on protection Configuration.
4. In the port filtering card, click on **set** to enter the port filtering page.

5. In the port filtering page, click on **Create** to create a port filtering rule. In this scenario, create two rules, intercept all protocols and select TCP protocol, fill in the source port Range 1-65535, and fill in the destination port Range 10-155 ports, select different protection actions and fill in the relevant fields, and click **Save.**

Field	Description
protocol	Optional all, TCP or UDP protocol
source port Range	Refers to the port information of the Client initiating the access, supporting the filling Range: 1-65535
destination port Range	Refers to the destination port information of the Client access, supporting the filling Range: 1-65535
action	Intercept: block the request; Allow: release the request and no longer match the remaining protection strategies. Continue protection: release the current request and continue to match the remaining protection strategies.

Configuration Features Filtering

Last updated：2025-05-30 10:14:39

Overview

Feature filtering can accurately formulate protection strategies against malformed message attacks or attack message features to prevent transparent transmission of malformed messages. EdgeOne supports custom interception policies for features in IP, TCP, and UDP message headers or payloads. After enabling feature filtering, you can combine source port, destination port, message length, IP message header or payload matching conditions, and set discard, release, blacklist, and continue protection policy actions for requests that meet the conditions.

Note:

This function is only supported when L4 proxy is enabled for exclusive DDoS protection. Default platform protection and L7 site exclusive DDoS protection do not support configuration.

Usage Scenarios

After the site business accesses EdgeOne, if you need to manage access requests with fixed features, you can enable feature filtering for the site and set precise access control rules. Feature filtering access control rules consist of matching conditions and matching actions.

Matching conditions define the request features to be identified, specifically the attribute features of TCP/UDP protocol fields in access requests.

Matching actions define the actions to be executed on access requests when they hit the matching conditions, including interception, release, discard and blacklist, and continue protection.

Directions

For example: For all business domain names under the site `example.com` , only TCP business packages with a length not greater than 512 bytes are open to the public, and all requests that do not meet this feature are intercepted. The operation steps are as follows:

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. On the site details page, click **Security > DDoS Mitigation** to enter the DDoS Protection details page.
3. In the L4 proxy protection tab, select the L4 proxy protection instance to be configured and click on **Security configuration.**

4. In the feature filtering card, click on **set** to enter the feature filtering page.

5. In the feature filtering page, click **Create**.
6. In the new feature filtering dialog box, create a feature filtering rule, select different protection actions according to the needs, and fill in the relevant fields, click **OK**.

The explanations of each feature field are as follows:

Filter feature	Explanation	Other parameters
Source Port	Refers to the access source port. Supports input of port numbers in the range of 1-65535. Supports logical equal or between.	/
Target Port	Refers to the access target port. Supports input of port numbers in the range of 1-65535. Supports logical equal or between.	
Package Length	Refers to the length of the access message data package. Supports input of numbers in the range of 1-1500. Supports logical equal or between.	
IP Header Start Detection	Supports keyword matching, where keywords are matched by offset and check depth.	**Offset:** The offset of the data body (payload) after the UDP or TCP header, optional range: 0~1500, unit: Byte. When the offset is 0, the match starts from the first byte of the data body. **Payload Content:**The content of the payload to be matched. You can directly input a string (such as hello) or a hexadecimal string starting with \\x (such as \\x1A2B3C4D). Inspection Depth:**The string length of the payload content plus the offset. (For example, if the offset is 1 and the string length is 6, then the depth is 7.)
TCP/UDP Header Start Detection	Supports keyword matching, where keywords are matched by offset and check depth.	
Payload Start Detection	Refers to skipping the IP header and TCP/UDP header and starting detection from the payload carried by the message. Supports keyword matching, where keywords are matched by offset and check depth.	

Configuration Protocol Blocking Rule

Last updated：2025-05-30 10:15:22

Overview

EdgeOne supports one-click blocking of source traffic to the site by protocol type. You can configure ICMP protocol blocking, TCP protocol blocking, UDP protocol blocking, and other protocol blocking. After the configuration is complete, when the attack traffic is detected with related Access request, it will be directly truncated.

Note：

This function is only supported when the L4 proxy is enabled with Exclusive DDoS protection, and it is not supported by the default platform protection and Exclusive DDoS protection for L7 sites.

Usage Scenarios

When your website does not have a specified access protocol, you can block the specified protocol with one-click blocking, and directly filter the access requests of the corresponding protocol during traffic cleaning to prevent the corresponding requests from being transparently transmitted to the origin.

Note：

Due to the connectionless nature of the UDP protocol (unlike TCP, which has a three-way handshake process), it has a natural security flaw. If you do not have UDP business, it is suggested to block the UDP protocol.

Directions

For example, for all business domains under the site `example.com` , only TCP protocol connections are open to the outside, and other protocol requests are blocked. The operation steps are as follows:

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. On the site details page, click on **Security > DDoS Mitigation** to enter the DDoS protection details page.
3. In the L4 proxy protection tab, select the L4 proxy protection instance that needs to be configured, and click on **Security configuration**.
4. In the protocol blocking card, click on the **set** to enter the protocol blocking page.

5. On the protocol blocking page, click on the switch

of the required protocol blocking, in this scenario, turn on the ICMP protocol, UDP protocol blocking, and other protocol blocking switches. Once enabled, the rule will take effect immediately, and the corresponding protocol requests will be blocked.

Configuration Connections Attack Protection

Last updated：2025-05-30 10:16:01

Overview

EdgeOne supports protection against connection-based attacks, automatically blocking clients with abnormal connection behavior. After enabling the protection for the maximum number of abnormal connections from the source IP, when the EdgeOne security acceleration platform detects a large number of abnormal connection state packets frequently initiated by the same source IP within a short period, it will add the source IP to the blocklist for punishment, with a blocking time of 15 minutes, and access can be restored after the blocking is lifted.

Note：

This function is only supported when the L4 proxy is enabled for independent DDoS protection, and it is not supported for default platform protection or independent DDoS protection for L7 sites.

Usage Scenarios

To prevent a large number of connections from exhausting the TCP connection resources or network resources of the origin, you can configure connection-based attack protection to protect the origin.

Directions

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. On the site details page, click on **Security > DDoS Mitigation** to enter the DDoS protection details page.
3. In the L4 proxy protection tab, select the L4 proxy protection instance to be configured, and click on **Security configuration.**
4. In the connection-based attack protection card, click on **set** to enter the connection-based attack protection page.

5. In the connection-based attack protection page, click on **edit** on the right side of the connection rule, and refer to Related references for the description and action of each connection rule.
6. In the configuration rule dialog box, modify the configuration, and click on **OK** to complete the rule issuance.

Related references

Supported connection rules

Per-IP new connection limit: This rule restricts the new connections from a source IP to prevent TCP connections from being exhausted by attackers.

Per-IP concurrent connection limit: This rule restricts the open simultaneous connections from a source IP to prevent TCP connections from being exhausted by attackers.

Per-IP abnormal connection limit: This rule restricts a source IP that generates many abnormal connections to access the origin.

Global new connection limit: This rule restricts the new connections between EdgeOne and the origin to prevent TCP connections from being exhausted by attackers.

Global concurrent connection limit: This rule restricts the open simultaneous connections between EdgeOne and the origin to prevent TCP connections from being exhausted by attackers.

Global data rate limit: This rule restricts the data rate at which EdgeOne transmits data to the origin to prevent the origin's network and computing resources from being consumed by forged requests from attackers.

Global packet rate limit: This rule restricts the packet rate at which EdgeOne transmits packets to the origin to prevent the origin's network and computing resources from being consumed by forged requests from attackers.

Action

Limit new connections: When under a single source IP rule, reject new connection requests from that IP; under a global policy, reject all new TCP connection requests.

Disconnect and punish: Disconnect the IP connection and block the IP for 15 minutes.

Discard overage data: Discard requests that exceed the data transmission rate or connection packet rate.

Related References

Action

Last updated：2023-08-17 15:24:05

The DDoS protection module provides multiple action methods. The processing rules for different actions are as follows:

Action	Action Description	Subsequent Actions
Deny	Directly discard the request data package and do not continue to match other rules	None
Allow	Directly pass the request data package and do not continue to match other rules	None
Discard and block	Directly discard the request data package and add the IP to the backend blocklist	None
Continue protection	Continue to execute and match other rules	ontinue to match other rules in order

Related Concepts Introduction

Last updated：2023-08-17 15:26:33

Introduction to DDoS Attacks

Distributed Denial of Service (DDoS) attacks refer to attackers remotely controlling a large number of zombie hosts through the network to send a large amount of attack requests to one or multiple targets, blocking the target server's network bandwidth or depleting the target server's system resources, making it unable to respond to normal service requests.

Network Layer DDoS Attacks

Network layer DDoS attacks mainly refer to attackers using high traffic to congest the target server's network bandwidth and consume server system resources, causing the target server to be unable to respond normally to customer visits. Common types of attacks include SYN Flood, ACK Flood, UDP Flood, ICMP Flood, and DNS/NTP/SSDP/memcached reflection attacks.

Transport Layer DDoS Attacks

Mainly include Syn Flood, Ack Flood, UDP Flood, ICMP Flood. Taking Syn Flood attack as an example, it takes advantage of the TCP protocol's three-way handshake mechanism. When the server receives a Syn request, the server must save the connection in a listening queue for a certain period of time. Therefore, it continuously sends Syn requests to the server but does not respond to Syn+Ack packets, thereby consuming server resources. When the server's listening queue is full, the server will be unable to respond to normal user requests, achieving the purpose of a denial of service attack.

Application Layer DDoS Attacks

Mainly include DNS DDoS attacks and Web application DDoS attacks. DNS DDoS attacks mainly include DNS Request Flood, DNS Response Flood, and false source + Real source DNS Query Flood. Web application DDoS attacks mainly refer to HTTP Get Flood, HTTP Post Flood, etc. HTTP Get Flood usually refers to hackers finding some resource-consuming transactions and pages from Web services or interfaces and continuously sending HTTP Get requests to these transactions and pages, causing Web application server resources to be depleted, unable to provide normal services, or causing the entire data center's entrance network bandwidth to be occupied, making the whole data center unable to provide normal services to the outside.

CC Attack

CC attack mainly refers to the attack method of maliciously occupying the target server's application layer resources, consuming processing performance, and causing it to be unable to provide normal services. Common types of attacks include HTTP/HTTPS-based GET/POST Flood, L4 CC, and Connection Flood attacks.

Protection Capability

Protection capability refers to the ability to defend against DDoS attacks. DDoS protection is provided based on Tencent Cloud's maximum DDoS protection capability in the current region.

Cleaning

When the target IP's public network traffic exceeds the set protection threshold, Tencent Cloud's DDoS protection system will automatically clean the public inbound traffic of that IP. The traffic is redirected from the original network path to Tencent Cloud's DDoS cleaning equipment through the BGP routing protocol, and the traffic of that IP is identified by the cleaning equipment, discarding the attack traffic and forwarding the normal traffic to the target IP. In general, cleaning does not affect normal access, and only in special scenarios or when the cleaning strategy is misconfigured may it affect normal access. When the traffic has been normal for a certain period of time (determined dynamically based on the attack situation), the cleaning system will determine that the attack has ended and stop cleaning.

Web Protection

Overview

Last updated：2024-08-01 21:37:22

Web Protection provides application layer protection for HTTP/HTTPS protocols. You can use EdgeOne's preset security policies or define your own security policies to identify and handle risky requests, protect sensitive data on your site, and ensure stable service operation.

Note:

EdgeOne does not charge for requests blocked by security policies.

Applicable Scenarios

Web Protection can control and mitigate various risks, with typical scenarios including:

Vulnerability attack protection: For sites involving customer data or sensitive business data, you can enable managed rules to intercept injection attacks, cross-site scripting attacks, remote code execution attacks, and malicious attack requests from third-party component vulnerabilities.

Access control: Distinguish between valid and unauthorized requests to prevent sensitive business exposure to unauthorized visitors. This includes external site link control, partner access control, and attack client filtering.

Mitigating resource occupation: Limit the access frequency of each visitor to avoid excessive resource occupation, which may cause service availability decline. EdgeOne's rate limiting can effectively mitigate site resource exhaustion and ensure stable service availability.

Mitigating service abuse: Limit session or business dimension abuse, including batch registration, batch login, excessive use of API, and other malicious usage scenarios. Strengthen the usage quota of a single session (such as users, instances, etc.) to ensure that users use service resources within a reasonable limit.

API parameter verification: Verify API parameters to ensure the legality of requests and control interface exposure risk.

Features

Web Protection provides the following features, and it is suggested to configure them based on the business type and expected client types for business:

Note:

Different protection modules' disposal order priority and the execution priority of the same priority rules within the module. For details, see Web Protection Requests Processing Order.

Protection Module	Function Introduction
Exception Rules	Requests that match the conditions skip the scanning of the specified security module and will not hit the rules in the corresponding module. For managed rules, more detailed exceptions can be configured to skip the scanning of specified managed rules.
Custom Rules	Apply the corresponding action to requests that match the specified conditions.
Platform-hosted rate limiting	Identify CC attacks (Layer 7 DDoS attack) and apply the corresponding action.
Custom Rate Limiting Rules	Count the number of requests that match the conditions within a certain period of time. When the number exceeds the specified threshold, the rule applies and handles the requests that match the conditions. After the number of requests falls below the threshold, the action remains effective for a certain period of time, and then no longer applies until triggered again.
Bot Management	Identify non-human access behavior (bot clients) and apply the corresponding action based on bot client type or behavioral features.
Managed rules	Identify attack features (including SQL injection, XSS attack, open source component vulnerability, etc.) in request headers or body, and apply the corresponding action. Rules are defined by EdgeOne and auto-renewal.

Configuring Web Protection Policy

Last updated：2024-12-16 14:29:45

Web Protection Policy Types

Tencent Cloud EdgeOne (EdgeOne) provides 3 types of web protection policies:

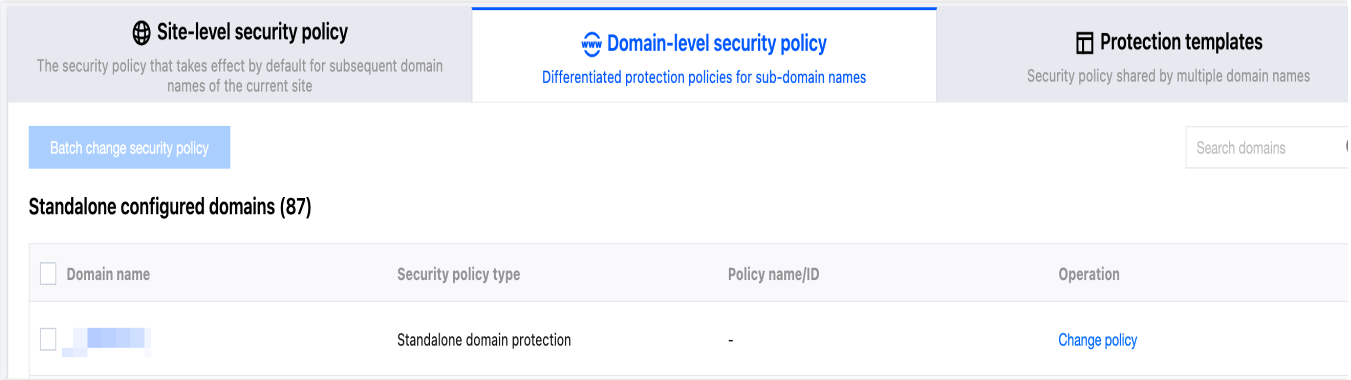
Site-level security policy: A unified policy set for the entire site, which is applicable to all domain names under the current site by default and is also the protection policy that takes effect by default for newly connected domain names under the current site.

Domain-level security policy: It is allowed to set an independent policy for each domain name to meet specific security requirements for different domain names.

Protection templates: It is allowed for users to create and apply a set of predefined protection policies. These templates can be applied to one or more domain names to simplify the configuration process.

A Method to Determine the Policy Used for a Domain Name

1. Log in to the EdgeOne console, click **Site List** in the left menu bar, and click the **site** to be configured in the site list.
2. Click **Security Protection** > **Web Protection** to go to the **Domain-level security policy** tab**.**
3. In the search box in the upper right corner, enter the domain name to find the corresponding domain name entry.
4. In the domain name entry, you can view the security policy type and the policy name or ID.



Site-level security policy
The security policy that takes effect by default for subsequent domain names of the current site
Domain-level security policy
Differentiated protection policies for sub-domain names
Protection templates
Security policy shared by multiple domain names
Batch change security policy
Search domains

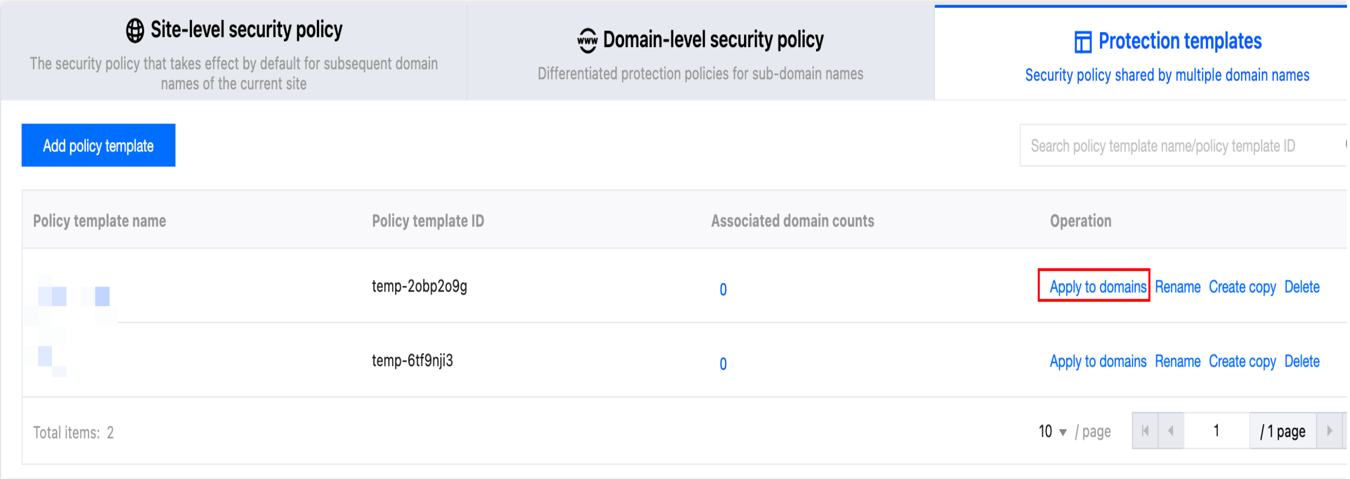
Standalone configured domains (87)

Domain name	Security policy type	Policy name/ID	Operation
[redacted]	Standalone domain protection	-	Change policy

A Method to Determine the Applicable Domain Name Range for a Protection Template

1. Log in to the EdgeOne console, click **Site List** in the left menu bar, and click the **site** to be configured in the site list.
2. Click **Security Protection >****Web Protection** to go to the **Protection templates** tab**.**

3. In the search box in the upper right corner, enter the policy template name or ID to search for the corresponding policy template.
4. In the policy template entry, you can view **Associated domain counts** and click it to display the list of domain names associated with the policy template in the pop-up window.
5. If necessary, you can click **Apply to domains** to apply the policy template to other domain names.



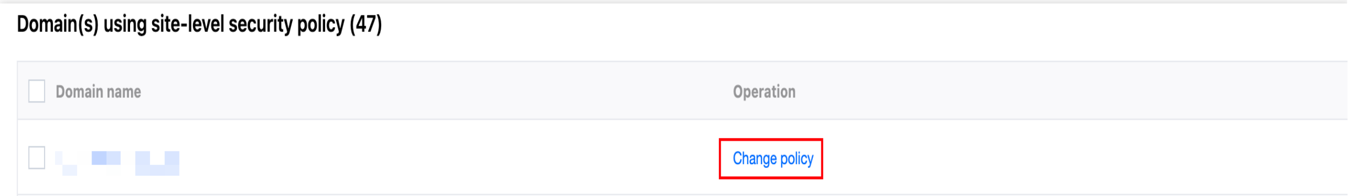
Site-level security policy
The security policy that takes effect by default for subsequent domain names of the current site
Domain-level security policy
Differentiated protection policies for sub-domain names
Protection templates
Security policy shared by multiple domain names
Add policy template
Search policy template name/policy template ID

Policy template name	Policy template ID	Associated domain counts	Operation
	temp-2obp2o9g	0	Apply to domains Rename Create copy Delete
	temp-6tf9nji3	0	Apply to domains Rename Create copy Delete

Total items: 2
10 / page
1
/ 1 page

Setting an Independent Policy for a Domain Name

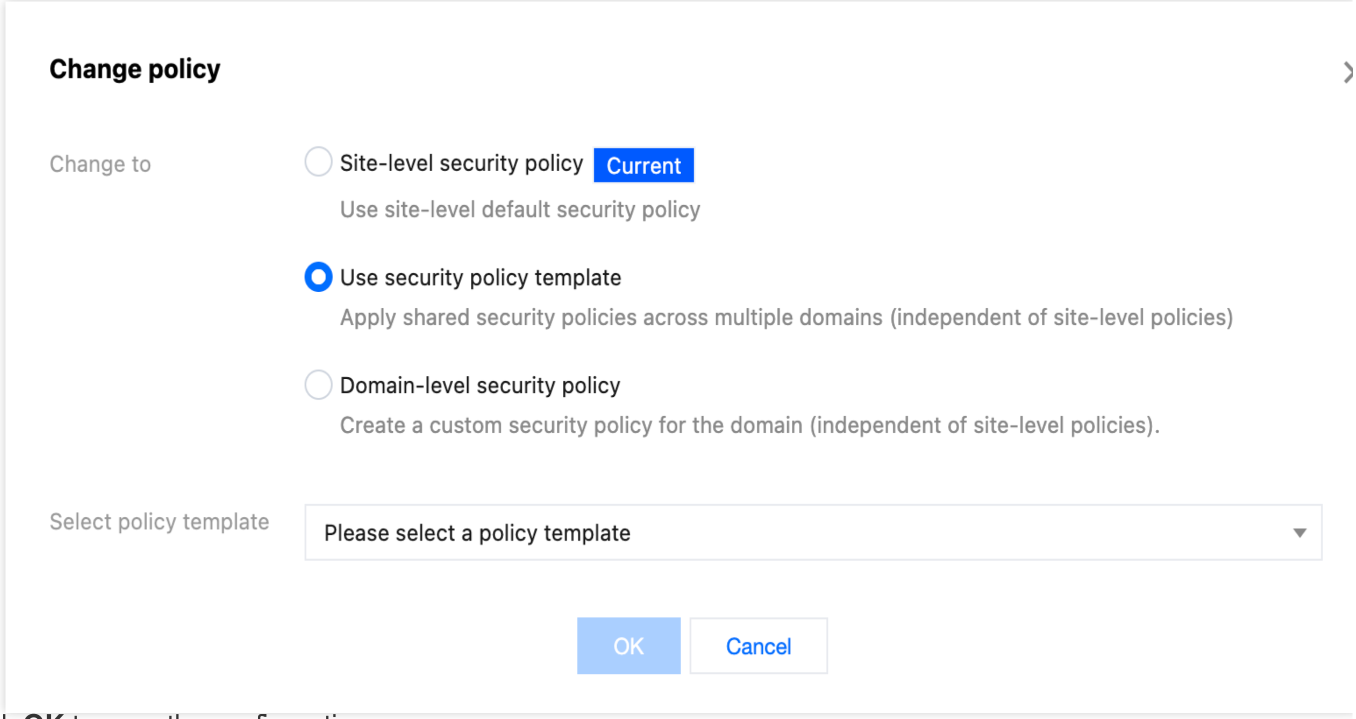
1. Log in to the EdgeOne console, click **Site List** in the left menu bar, and click the **site** to be configured in the site list.
2. Click **Security Protection** > **Web Protection** to go to the **Domain-level security policy** tab**.**
3. In the target domain name entry, click **Change policy.**



Domain(s) using site-level security policy (47)

□ Domain name	Operation
□	Change policy

4. In the pop-up window, select **Change to** and the target protection policy.



Change policy

Change to

○ Site-level security policy Current
Use site-level default security policy

● Use security policy template
Apply shared security policies across multiple domains (independent of site-level policies)

○ Domain-level security policy
Create a custom security policy for the domain (independent of site-level policies).

Select policy template: Please select a policy template

5. Click **OK** to save the configuration.

Note:

After the configuration is saved and the deployment is completed, the new protection policy will be used for the domain name. Monitor the protection effectiveness to ensure it meets your expectations and adjust the policy in time.

Custom rule(IP blocklist/allowlist、regional restrictions,etc)

Last updated：2024-11-19 17:51:41

Overview

If your site needs to customize the user access policy, such as prohibiting users from specified regions, allowing specified external sites to link to the site content, and allowing only specified users to access certain resources. Custom rules support matching client requests based on single rule matching conditions or multiple matching conditions. By allowing, intercepting, redirecting, and returning custom pages, you can control the request strategy of matched requests, which can help your site more flexibly limit the content that users can access.

Typical Scenarios and Usage

You can choose the appropriate rule type to protect your site according to different scenarios. Custom rules are divided into the following types:

Basic access control: Supports single condition matching requests, disposes or observes matched requests, and is suitable for simple scenario protection, such as configuring IP blocklist/allowlist, Referer blocklist, UA blocklist/allowlist, or regional restrictions.

Precise matching rules: Supports multiple condition combination matching requests, disposes or observes matched requests, and is suitable for complex scenario protection configuration, such as allowing only specified users to access files under specified paths.

Managed custom policy: A policy customized by Tencent security experts, which does not support console adjustment. For details, please see: Managed custom rules.

Note:

When there are multiple rules of the same type, the priority of the rules is as follows:

1. Rules within Basic access control: when a request matches multiple rules, the actions will be executed in the following order: Observe > Block.

2. Precise matching rules will be executed from high to low priority (Priority Value from small to large);

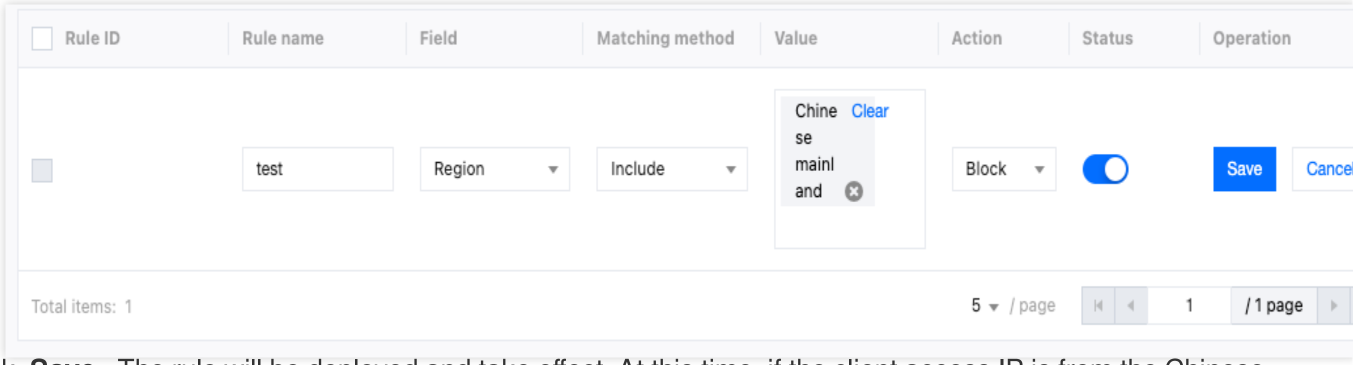
3. For the priority order of Custom rules and other Web Protection capabilities, please refer to: Web Protection Request Processing Order.

Basic Access Control

Example Scenario 1: Only allow access from specific countries/regions

To comply with the legal requirements of specified business regions, if the current business only allows access from non-Chinese mainland regions, you may need to restrict the visitor's source region. For such scenarios, you can use the regional control rules in basic access control to achieve this. The operation steps are as follows:

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. To configure differentiated security policies for a specific domain name under the current site, you can enter the **Domain-level security policy** tab and then click the **corresponding domain name** to enter the configuration page for the domain-level security policy. The subsequent steps are the same.
3. Locate the **Custom rules** tab and click **Add rule** in **Basic access control** .
4. Enter the rule name and configure the control type, matching method, and control range. In this example scenario, you can set the control type to **Region Control** , select the matching method as **Include** and the matching content as **Chinese mainland (All)** , and set the action to **Block** .



□ Rule ID	Rule name	Field	Matching method	Value	Action	Status	Operation
□	test	Region ▾	Include ▾	Chinese mainland ⊗ Clear	Block ▾	●	Save Cancel

Total items: 1 5 ▾ / page 1 / 1 page

5. Click **Save** . The rule will be deployed and take effect. At this time, if the client access IP is from the Chinese mainland, the access to the website is denied.

Example Scenario 2: Configure Referer to control external site access

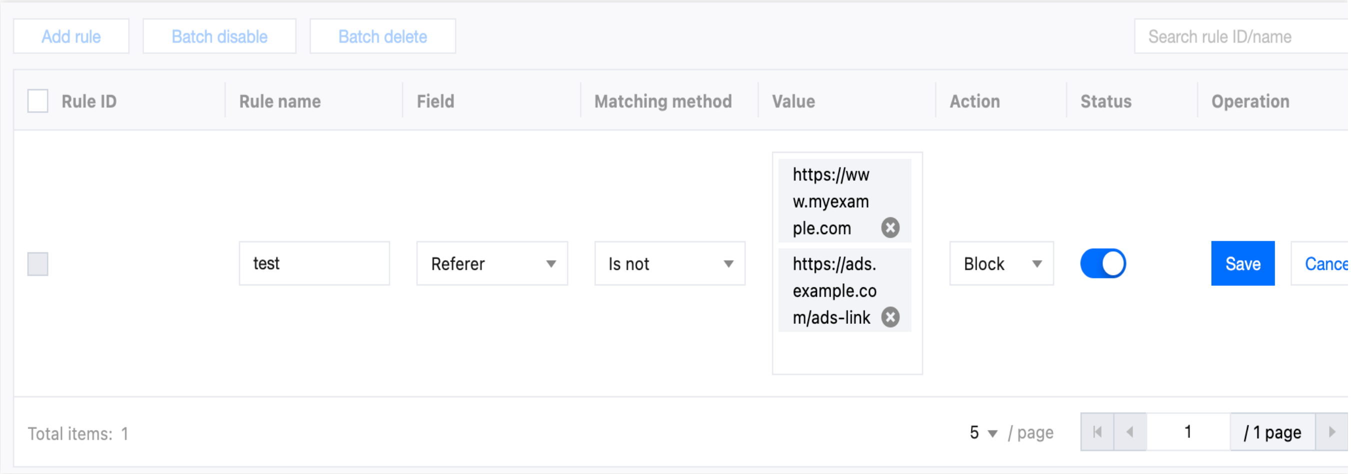
Note:

The HTTP protocol allows the Referer header to use a full URL or partial URL. You should configure the matching content according to the actual situation. For details about the Referer header, see RFC 9110.

To prevent unauthorized site access, you can use the Referer control rules in basic access control to block access requests with unauthorized Referer headers. For example, if the service at the `https://www.myexample.com` site needs to allow access requests through the advertising partner's link `https://ads.example.com/ads-link` and reject access through other site links, you can take the following steps:

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.myexample.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Custom rules** tab and click **Add rule** in **Basic access control**.

4. Enter the rule name and configure the control type, matching method, and control range. In this example scenario, you can set the control type to **Referer control** , and select the action as **Block** when the **request Referer** does not equal `https://www.myexample.com` or `https://ads.example.com/ads-link` .



☐ Rule ID	Rule name	Field	Matching method	Value	Action	Status	Operation
☐	test	Referer	Is not	https://www.myexample.com https://ads.example.com/ads-link	Block	●	Save Cance

Total items: 1   5 / page   1 / 1 page

5. Click **Save**. The rule will be deployed and take effect.

Precise Matching Rules

Example Scenario: Precisely control the exposure surface of sensitive resources on the site

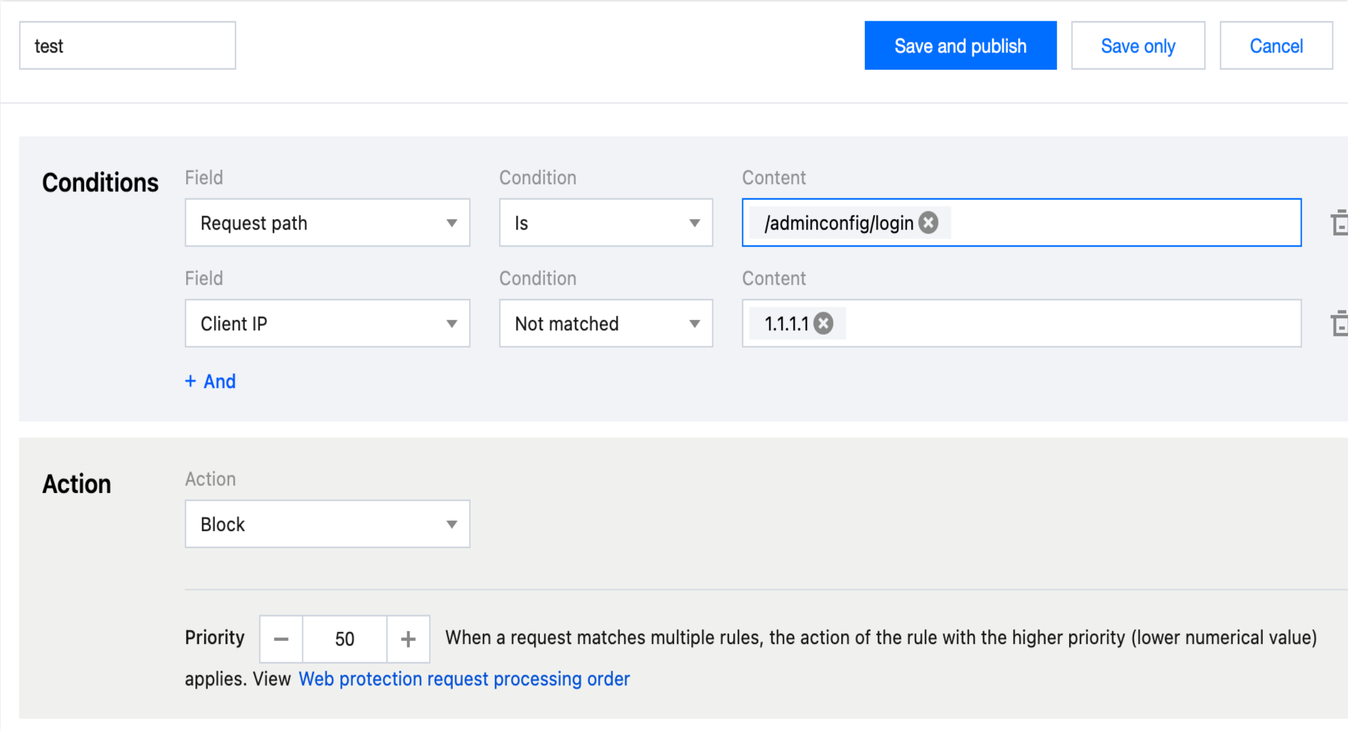
If you need to control the exposure surface of sensitive resources (such as the background management page) on the site and only allow access from specific clients or specified networks. You can use the client IP matching and request URL matching combination in precise matching rules to achieve this.

For example, the current site domain name `www.example.com` has a management background login address path of `/adminconfig/login` , and this background is only allowed to be logged in by the specified client IP user `1.1.1.1` . The operation steps are as follows:

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Custom rules** tab and click **Add rule** in **Precise matching rules** .
4. On the rule adding page, select creating a blank rule, enter the rule name, and click **Add**.
5. Configure the judgment conditions and actions. In this example scenario, you can configure the matching fields as **Request path (Path)** equals `/adminconfig/login` and **Client IP** not matching `1.1.1.1` , and set the action to **Block**.

Note:

Priority: The lower the value, the higher the priority. When a request matches multiple rules, the action of the rule with the higher priority (lower numerical value) applies.



Conditions

Field: Request path; Condition: Is; Content: /adminconfig/login

Field: Client IP; Condition: Not matched; Content: 1.1.1.1

Action

Action: Block

Priority 50 When a request matches multiple rules, the action of the rule with the higher priority (lower numerical value) applies. View Web protection request processing order

6. Click **Save and publish** . The rule will be deployed and take effect.

Related References

Supported Matching Condition Range

Custom rules can use matching conditions to control the scope of rule application. The following are the matching conditions supported by different custom rule types:

Basic access control

Rule type	Description
Client IP control	Control access requests based on client IP
Regional control	Control access requests based on client IP location
Referer control	Control access requests based on the Referer header content
User-Agent control	Control access requests based on the User-Agent
ASN control	Control access requests based on the client IP location ASN
URL control	Control access requests based on the request URL, supporting wildcard matching

Precise matching rules

Precise matching rules support the following matching conditions, and the support level for different EdgeOne plans is also not consistent.

Note:

For the description and plan restrictions of supported matching conditions, please refer to: Matching conditions.

Request domain name (Host)

Request client IP

Request client IP (prioritizing XFF header)

Request method (Method)

Request User-Agent header

Session cookie

XFF extended header

Request path (Path)

Custom request header

Request URL

Request source (Referer)

Network layer protocol

Application layer protocol

Request body

JA3 fingerprint

Supported Actions

Different custom protection rules support the following actions. For the description of different actions, please refer to Actions.

Protection rule type	Supported actions
Basic access control	Observe Intercept
Precise matching rules	Release Intercept Observe IP blocking rule Return custom response content Annotation Redirect to URL JavaScript challenge

Note:

Annotation: You can configure the **return custom response content** action for a single custom rule (only precise matching rules are supported). When a request matches the rule, EdgeOne will return the specified page and status code. You can also configure the custom response page to specify the page and status code used for all custom rules to **block requests**.

Rate Limiting

Bandwidth Abuse Protection

Last updated：2025-03-04 15:31:18

Overview

Bandwidth abuse refers to the malicious behavior of repeatedly accessing site resources through PCDN platforms or automation tools, resulting in a waste of bandwidth resources. Static resources are the main target of bandwidth abuse attacks. Images or data packages to be downloaded may be subjected to numerous crawler requests, leading to repeated downloads of resources, generating hefty download traffic bills, and even resulting in arrears and service suspension. Bandwidth abuse protection provides preset security policy options to mitigate or reduce the impact of bandwidth abuse.

Use of Bandwidth Abuse Protection

EdgeOne provides bandwidth abuse protection policies, which enable recognition and extraction of bandwidth abuse request features based on platform-wide traffic analysis to form a bandwidth abuse database. This database is used for automatic matching and interception of high-risk bandwidth abuse requests. The bandwidth abuse database is updated every 24 hours to cover the latest bandwidth abuse features.

Bandwidth abuse protection supports Monitor, Block, and JavaScript Challenge actions. Choose an appropriate option based on business compatibility. For details, see Action.

Note:

Bandwidth abuse protection only covers bandwidth abuse scenarios originating from Chinese mainland.

When the bandwidth abuse protection feature is enabled for the first time, it is recommended to use the **Monitor** action for evaluation. After evaluating the matching situation through metric analysis and web security analysis, you can choose **Block**.

If your domain name service has enabled bot management, bandwidth abuse protection will use TLS fingerprint technology to further improve the recognition accuracy of distributed bandwidth abuse crawlers.

If you find that normal traffic is mistakenly blocked by the bandwidth abuse protection feature, configure protection exception rules to restore access by blocked normal clients.

Note:

Since the bandwidth abuse protection feature recognizes high-risk requests based on historical information, there may be an information lag when bandwidth abuse behavior changes. If you believe that bandwidth abuse attacks are still bypassing the protection after the bandwidth abuse protection policy is enabled, consider the following mitigation methods:

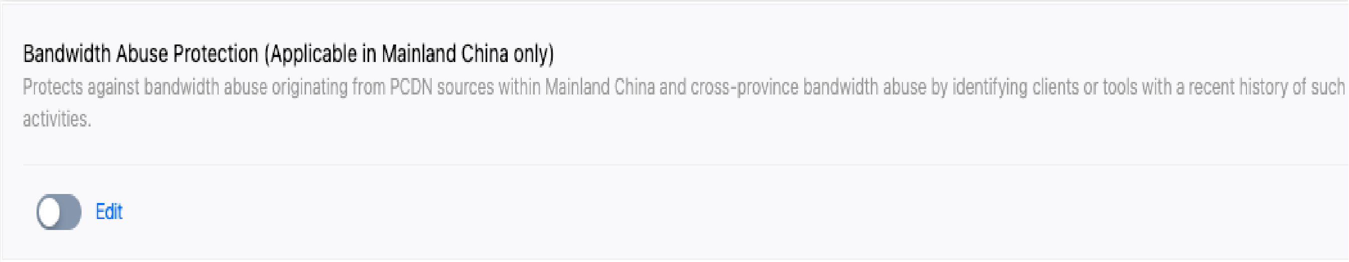
Contact technical support. We will analyze the request traffic as soon as possible and update the policy.

In web protection, configure custom rate limiting rules to recognize and block clients that repeatedly access static resources by using statistical dimensions such as client IP addresses and request URLs.

In bot management, configure bot intelligent analysis to dynamically recognize crawlers' access behavior and mitigate the impact of bandwidth abuse. (A plan for the standard edition or above is required. For details, see Comparison of EdgeOne Plans.)

Directions

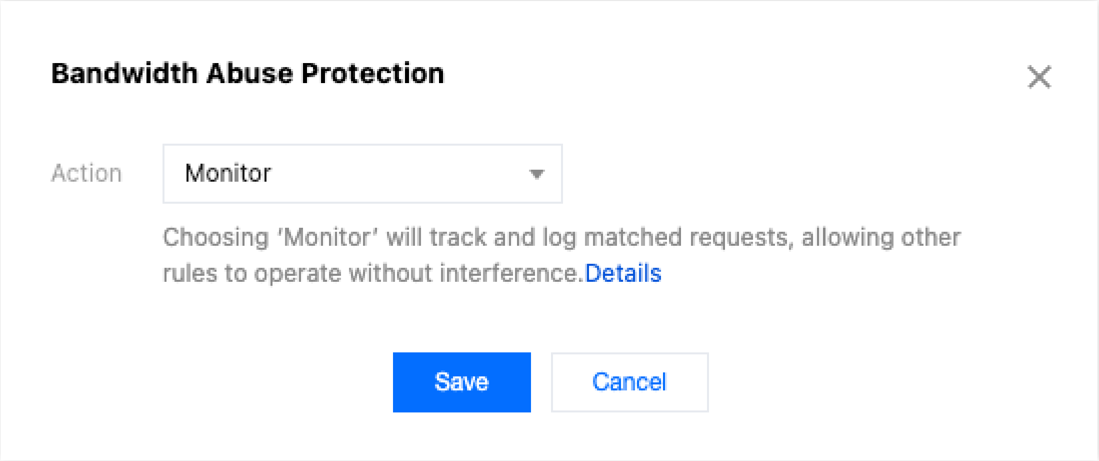
1. Log in to the EdgeOne console, click **Site List** in the left menu bar, and click the **site** to be configured in the site list.
2. Click **Security Protection** > **Web Protection**. The default is site-level security policy. If you need to configure a differentiated protection policy for a specific domain name under the current site, go to the **Domain-level security policy** tab, click the **corresponding domain name** to go to the domain-level security policy configuration page, and follow the same subsequent steps.
3. Locate the **Rate Limiting** card and click **Edit** on the right side of **Bandwidth Abuse Protection**.



Bandwidth Abuse Protection (Applicable in Mainland China only)

Protects against bandwidth abuse originating from PCDN sources within Mainland China and cross-province bandwidth abuse by identifying clients or tools with a recent history of such activities.

4. Choose the action for **bandwidth abuse protection**. It is recommended to choose **Monitor** initially. After evaluating the matching situation through metric analysis and web security analysis, you can choose **Block**.



Bandwidth Abuse Protection

Action: Monitor

Choosing 'Monitor' will track and log matched requests, allowing other rules to operate without interference.Details

Platform-Managed Rate Limiting Rules (Formerly CC Attack Defense)

Last updated：2024-12-23 15:17:46

Overview

Collapse Challenge (CC) attack, also known as HTTP/HTTPS DDoS attack. Attackers occupy the connection and session resources of Web services, causing the service to be unable to respond to user requests normally, resulting in denial of service. To avoid CC attacks, EdgeOne provides a pre-set CC attack protection strategy and enables it by default to ensure the stability of your site online.

Note:

The primary objective of CC attack protection is to ensure the availability of services. For security scenarios that do not lead to errors at the origin server or a decrease in site availability, such as resource scraping, bulk logins, and automated shopping cart orders, please fortify your security policies further by using Rate Limiting and Bot Management.

EdgeOne adopts a "clean traffic" billing model, meaning that requests intercepted by the security protection features are not charged. Charges are only applied to the traffic and request volume processed after the security protection features. For the definition of the "clean traffic" billing model, see Tencent Cloud EdgeOne.

Using Platform-Managed Rate Limiting

Platform-managed rate limiting identifies CC attacks through rate baseline learning, header feature statistical analysis, and client IP intelligence, then takes action. EdgeOne provides three pre-set CC attack protection strategies:

Adaptive frequency control: Used to deal with CC attack behavior that occupies server resources through high-frequency and large amount of concurrent connection requests, and can limit access frequency based on a single IP source.

Slow attack protection: Used to deal with CC attack behavior that occupies server resources through a large amount of slow connection requests, and can limit access connection minimum rate based on a single session, eliminating slow connection clients.

Intelligent client filtering: Integrates rate baseline learning, header feature statistical analysis, and client IP intelligence to generate real-time dynamic attack defense rules. Perform human-machine verification for requests from high-risk clients or carrying high-risk header features. Intelligent client filtering is enabled by default and executes JavaScript challenges for clients that meet the rules.

Adaptive Frequency Control

Adaptive frequency control establishes and updates the rate baseline by continuously monitoring and analyzing your website's traffic pattern. The system counts the current domain name's request rate based on the configuration, establishes the rate baseline based on the last 7 days of requests (updated every 24 hours), and limits the request rate of a single client accessing the domain name according to the configured limitation level.

Note:

Adaptive frequency control is suitable for web-based business. For sites providing high-frequency API services, to avoid normal high-frequency requests being mistakenly blocked, it is recommended to avoid using moderate and emergency limitation levels. Configure protection exception rules for APIs requiring support for high-frequency access to bypass the CC attack protection module, and configure custom rate limiting rules to precisely limit the exposure of APIs.

Directions

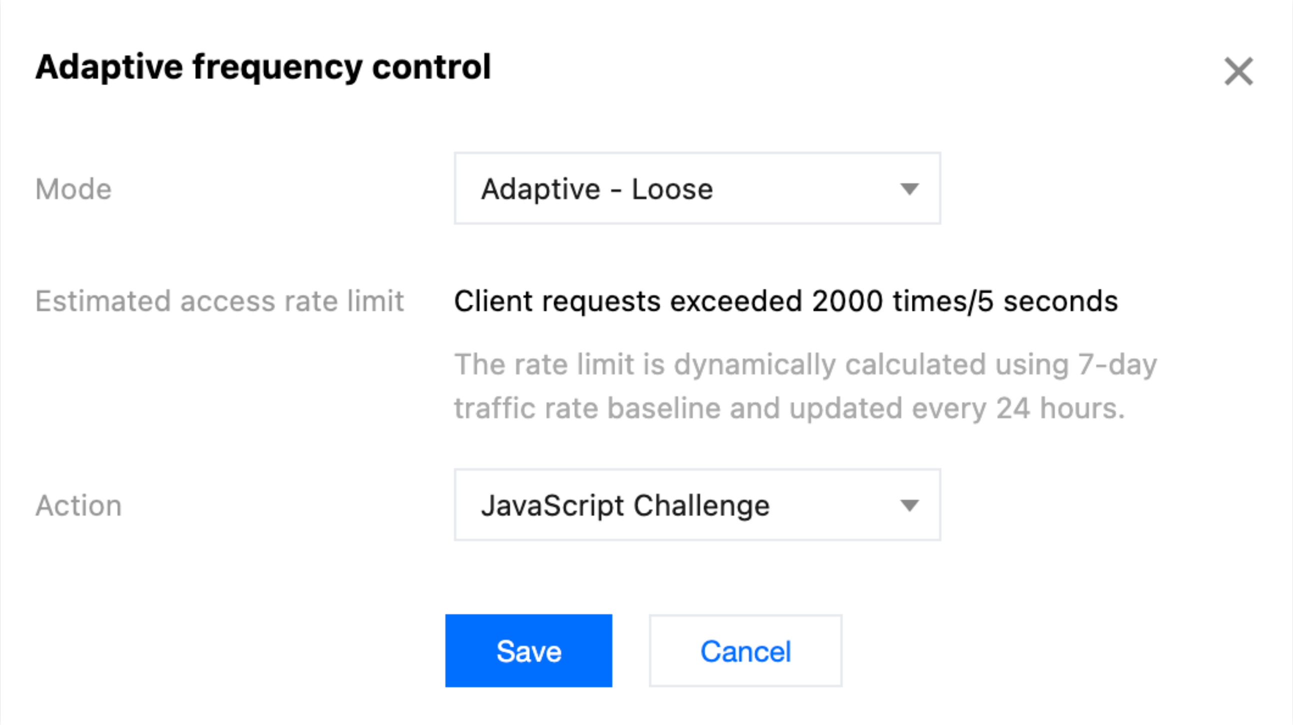
1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Protection**. By default, it is a site-level security policy. To configure differentiated security policies for a specific domain name under the current site, you can enter the **Domain-level security policy** tab and click the corresponding domain name to enter the configuration page for the domain-level security policy. The subsequent steps are the same.
3. Locate the **Rate Limiting** tab and click **Edit** on the right side of **Adaptive frequency control**.
4. Configure the limiting level and action for high-frequency Access request limiting. A description of each limitation level and rate threshold is as follows:

Limitation Type	Limitation Level	Applicable Scenarios	**Initial Access Rate Limit**
Adaptive	Loose (Default Configuration, Suggested)	Applicable to most web business scenarios that do not require real-time data interaction or queries.	2,000 times / 5 seconds
	Moderate	Applicable to business scenarios with simpler page content and less dynamic data or dynamic loading content.	200 times / 10 seconds
	Emergency	Applicable to web scenarios that mainly provide static contents. When an attack occurs or other restriction levels cause business impact, this restriction level can	40 times / 10 seconds

		be selected for emergency protection. Due to the strict rate limit of this level, there may be a risk of accidental killing, its long-term use is not recommended.	

Note:

The action of **Adaptive Frequency Control** supports **observation** and **JavaScript** challenge methods. For more information on different action methods, see action.



Adaptive frequency control

Mode: Adaptive - Loose

Estimated access rate limit: Client requests exceeded 2000 times/5 seconds

The rate limit is dynamically calculated using 7-day traffic rate baseline and updated every 24 hours.

Action: JavaScript Challenge

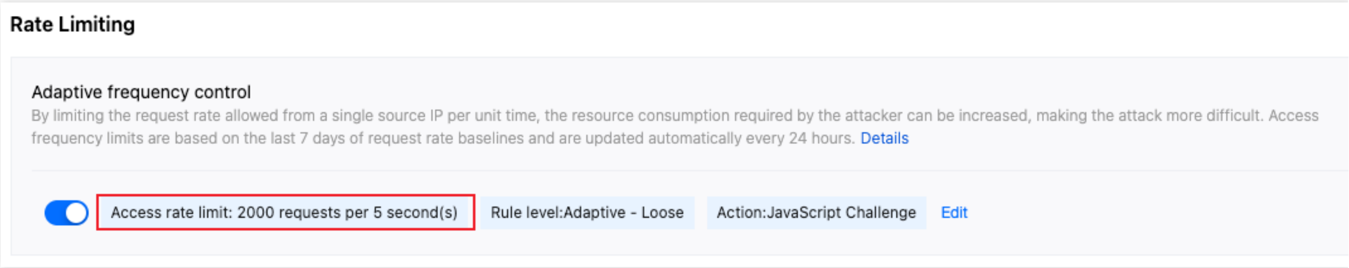
5. Click **Save** to complete the rule configuration.

Baseline Calculation and Update Method

Adaptive frequency control counts the request rate of the current domain name based on the configured limitation level, and creates the rate baseline based on the maximum daily traffic of the past 7 days. Baseline learning adopts a dynamic update mechanism, recalculation is made every 24 hours, and a 7-day time window is retained.

Rate statistics adopt a distributed method, with each EdgeOne node **counting the request rate based on the Client IP** and limiting the rate according to the threshold range of the current limitation level (adaptive - moderate and adaptive - emergency limitation levels have **fixed upper and lower limits, while the loose restriction level has a fixed lower limit**). Due to the distributed statistical characteristics, the actual rate of requests converging to the origin server may exceed the upper limit.

For the **access rate limit**, only the initial access rate limit is displayed on the console's **Policy Template** and **Site-level Policy** pages. In fact, for each domain name, the baseline is independently updated based on the traffic pattern of current network business to derive a unique range of normal access rate limits.



Rate Limiting

Adaptive frequency control

By limiting the request rate allowed from a single source IP per unit time, the resource consumption required by the attacker can be increased, making the attack more difficult. Access frequency limits are based on the last 7 days of request rate baselines and are updated automatically every 24 hours. Details

Access rate limit: 2000 requests per 5 second(s) | Rule level:Adaptive - Loose | Action:JavaScript Challenge | Edit

Enabling Suggestions

To fully leverage the advantages of adaptive frequency control, we recommend following the progressive enabling method below:

1. Initial configuration: Enable adaptive frequency control and select the " **Adaptive - Loose** " level, with the action being **Monitor** . The loose level is suitable for most web business scenarios. Its higher initial access rate limit can effectively reduce the risk of false interception, while providing ample space for the system to learn your traffic pattern.
2. Learning period (7 days is recommended): During this phase, the system will deeply analyze your traffic pattern, count the source IP access rate based on historical access traffic with a 24-hour update cycle, and gradually establish an accurate rate baseline.
3. Policy optimization: After the learning period, the system will have established a relatively accurate traffic baseline. You can view the traffic hitting adaptive frequency control in **Web Security Analysis**, and decide whether to adjust or tighten the policy according to the protection effect and business needs.

Viewing the Traffic Hitting Adaptive Frequency Control

To view the traffic hitting adaptive frequency control rules:

1. Log in to the EdgeOne console and click **Web Security Analysis** in the left sidebar.
2. Select the time period from the initial access to adaptive frequency control to the current time as the **learning period** .
3. Click **Add Filter** and select **Web Protection - CC Attack Protection Rule** equal to **High Frequency Access Request Limit** .
4. Click OK to apply the filter conditions and observe the protection effect in **Statistical Trends** and **Statistical Details** .

Functional Limitations and Solutions

Adaptive frequency control may require additional adjustments in certain special cases:

1. Low-frequency attacks: When the attack frequency is below the lower limit of the set limitation level, adaptive frequency control may not achieve effective interception. In this case, it is recommended to use web security analysis for identifying and locating low-frequency attack behaviors, such as accessing specific sensitive pages/APIs multiple

times in a row, and intercept requests that meet the characteristics according to custom rules or custom rate limiting rules.

2. Legitimate high-frequency access: Legitimate high-frequency access (such as API calls) may exceed the upper limit of adaptive frequency control and be mistakenly intercepted. For business types that require real-time client data queries such as retail, e-commerce, and game platforms, and scenarios like travel, ticketing, and open third-party API services, it is recommended to disable the adaptive frequency control feature to avoid false interception.

3. Special business scenarios: During major events such as game updates, promotional activities, and ticket sales, adaptive rate control may affect the normal access peak in a short period. When short-term access behavior significantly differs from the norm, it is recommended to disable the adaptive rate control feature to avoid false interception. You can use custom rules and custom rate limiting rules for precise protection according to multi-dimensional characteristics.

Configure Slow Attack Protection

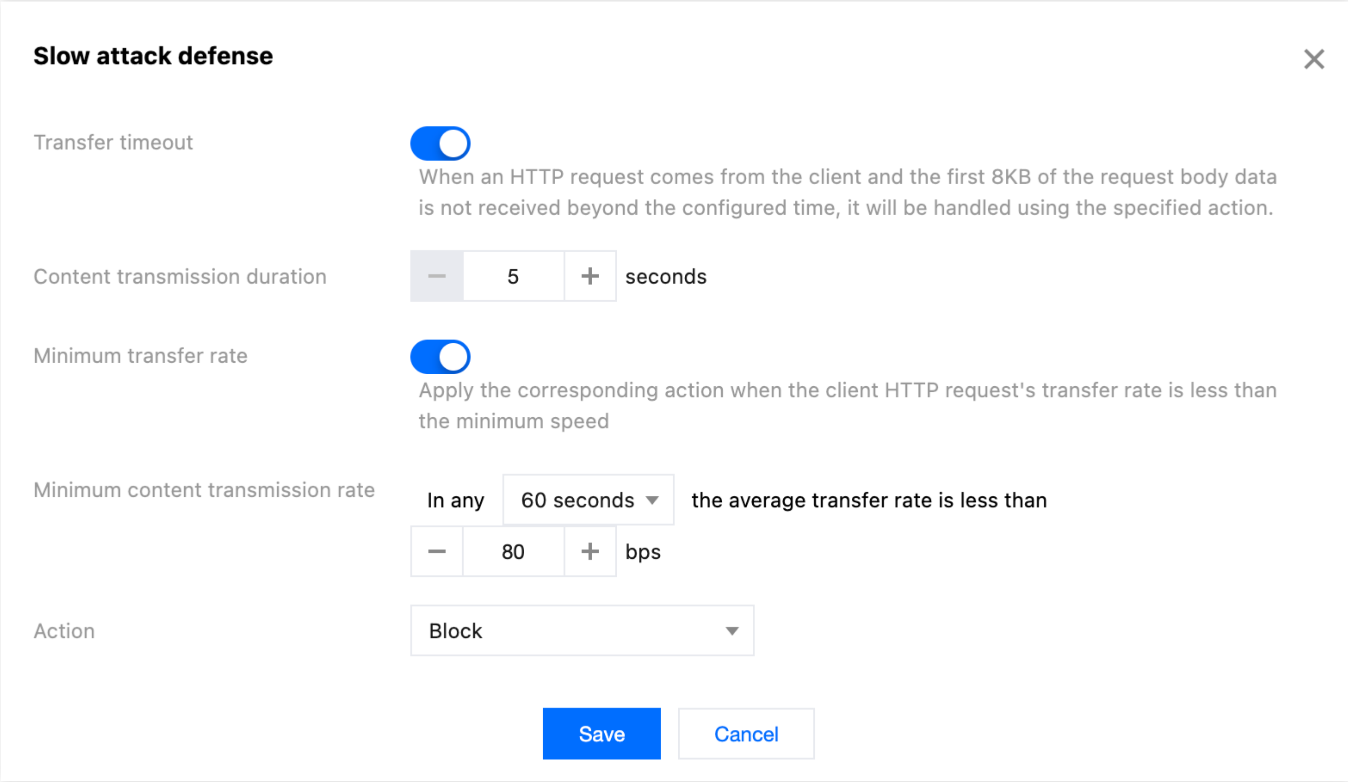
By limiting the minimum data rate and setting timeout, mitigate the consumption of site resources in slow transmission attack scenarios, and avoid the decline of service availability. EdgeOne slow attack protection supports content transmission timeout and minimum content transmission rate options. When the content transmission rate is slow or there is no data transmission for a long time, apply the corresponding action to the client.

Directions

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security > Web Protection**. By default, it is a site-level security policy. To configure differentiated security policies for a specific domain name under the current site, you can enter the **Domain-level security policy** tab and click the corresponding domain name to enter the configuration page for the domain-level security policy. The subsequent steps are the same.
3. Locate the **Rate Limiting** tab and click **Edit** on the right side of **Slow attack defense**.
4. Configure the matching method for slow attack protection rules, and choose from the following limitations:

Content transmission duration: Mitigate slow attacks that occupy connections without transmitting content data. Specify the content transmission timeout duration, and clients that fail to complete the transmission of the first 8KB of content data within the configured time will apply the corresponding action; the supported configuration is 5-120 seconds.

Minimum content transmission rate: Mitigate attacks that occupy connections and session resources by transmitting content at an extremely slow rate. Specify the minimum transmission rate, and when the content transmitted within the statistical time window is less than the configured rate, apply the corresponding action. The minimum supported transmission rate is 1 bps, and the maximum is 100 Kbps.



Slow attack defense

Transfer timeout: on

When an HTTP request comes from the client and the first 8KB of the request body data is not received beyond the configured time, it will be handled using the specified action.

Content transmission duration: 5 seconds

Minimum transfer rate: on

Apply the corresponding action when the client HTTP request's transfer rate is less than the minimum speed

Minimum content transmission rate: In any 60 seconds the average transfer rate is less than 80 bps

Action: Block

Note:

The action of Slow Attack Protection supports observation and JavaScript challenge methods. For more information on different action methods, see action.

5. Click **Save** to complete the rule configuration.

Intelligent Client Filtering

Intelligent client filtering integrates rate baseline learning, request header feature statistical analysis, and client IP intelligence to dynamically generate protection rules in real-time. It performs real-time human-machine recognition for traffic from high-risk clients or carrying high-risk request header features. Intelligent client filtering is enabled by default and performs JavaScript challenges for clients that meet the rules.

Intelligent client filtering is an advanced protection mechanism that integrates rate baseline learning, request header feature analysis, and client IP reputation evaluation technology. This feature can dynamically generate protection rules in real-time and perform real-time human-machine identification for traffic from high-risk clients or carrying high-risk request header features. Intelligent client filtering is enabled by default and automatically implements JavaScript challenges for suspicious clients that meet the rules.

Note:

Intelligent client filtering uses the business rate baseline as one of the references. When significant changes (new business access, traffic switching, new feature launch, or marketing activities) occur in the business, changes in the baseline may lead to false interception. It is recommended to temporarily adjust the action to "Monitor" in such cases, and enable it once the business traffic stabilizes.

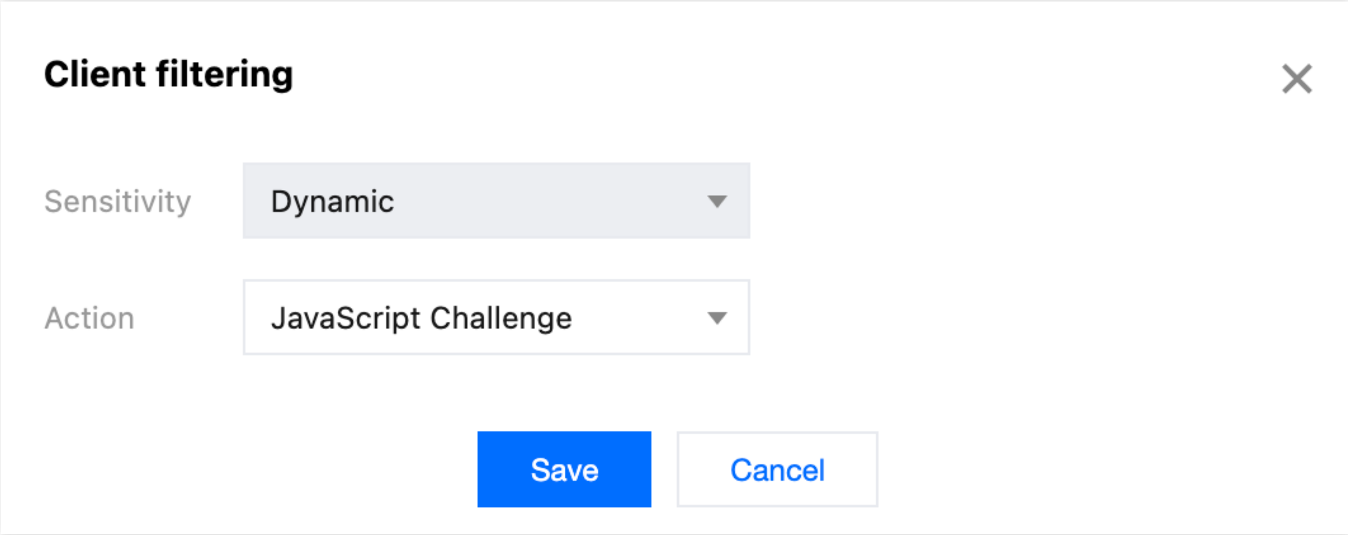
Intelligent client filtering is only supported by the Standard plan and Enterprise plan.

Policy Mechanism

Intelligent client filtering uses real-time learning algorithms to continuously analyze the request traffic of the past 1 - 12 hours, and establishes and stores the baseline model of normal user traffic. When abnormal traffic is detected, the system analyzes the aggregation of current request features and compares it with historical traffic to identify potential abnormal traffic and take corresponding action.

Modify the Action Method for Intelligent CC Attack Protection

If you need to modify the action method triggered by intelligent client filtering, you can follow these directions:
1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Protection**. By default, it is a site-level security policy. To configure differentiated security policies for a specific domain name under the current site, you can enter the **Domain-level security policy** tab and click the corresponding domain name to enter the configuration page for the domain-level security policy. The subsequent steps are the same.
3. Locate the **Rate Limiting** tab and click **Edit** on the right side of **Client filtering**.
4. Configure the actions.



Client filtering

Sensitivity: Dynamic

Action: JavaScript Challenge

Note:
Intelligent client filtering supports four actions, including **Disable (Not Enable),** Monitor and **JavaScript Challenge**. For more information on different actions, see Action.
5. Click **Save** to complete the rule configuration.
Note:
View the requests that match the **intelligent client filtering** rules. For details, see Web Security Analysis.

Viewing the Traffic Hitting Intelligent Client Filtering Rules

To view the traffic hitting intelligent client filtering rules:
1. Log in to the EdgeOne console and click **Web Security Analysis** in the left sidebar.

2. Click **Add Filter** and select **Web Protection - CC Attack Protection Rule** equal to **Intelligent Client Filtering** .
3. Click OK to apply the filter conditions and observe the protection effect in **Statistical Trends** and **Statistical Details** .

Functional Limitations and Solutions

Intelligent client filtering may require additional adjustments in certain special cases:

Business traffic fluctuates drastically: In scenarios such as large-scale attacks, major business activities, or other situations causing significant traffic pattern changes, intelligent client filtering may require a learning period of 4 to 24 hours to achieve optimal protection. During this period, it is recommended to use custom rules or custom rate limiting rules to enhance protection.

Custom Rate Limiting Rules

Last updated：2024-08-26 09:20:03

Overview

In site operation, problems such as malicious resource occupation, business abuse, and brute force cracking often occur. If these problems are ignored, they will lead to a decline in service quality, generate high-cost bills, and may even cause sensitive data leakage. To effectively manage these risks, client access frequency is an important indicator. Malicious clients usually access at a higher frequency to quickly achieve the purpose of cracking login, occupying resources, and crawling content. Using appropriate threshold limits for client access frequency can effectively distinguish between normal clients and malicious clients, thereby mitigating the risks of resource occupation and abuse.

Note:

When managing and combating crawlers, the effect of using only rate limiting strategy is limited. Please combine Bot management function to formulate a complete crawler management strategy.

Typical Scenarios and Usage

Rate limiting is commonly used to distinguish between normal client access and malicious access. By selecting appropriate statistical methods, limit thresholds, and disposal methods, rate limiting can help you mitigate security risks. Rate limiting configuration is divided into the following types:

Precise rate limiting: User-defined access frequency control strategy. Supports multiple condition combinations to match requests, limit the request rate of each request source, and is suitable for most scenarios to distinguish between normal user access and malicious high-frequency access.

Managed custom policies: Policies customized by Tencent security experts, which do not support console adjustment of policies. For details, please refer to Managed Custom Rules.

Accurate Matching Rules

Example Scenario 1: Limit the access frequency of the login API interface to mitigate credential stuffing and brute force cracking attacks

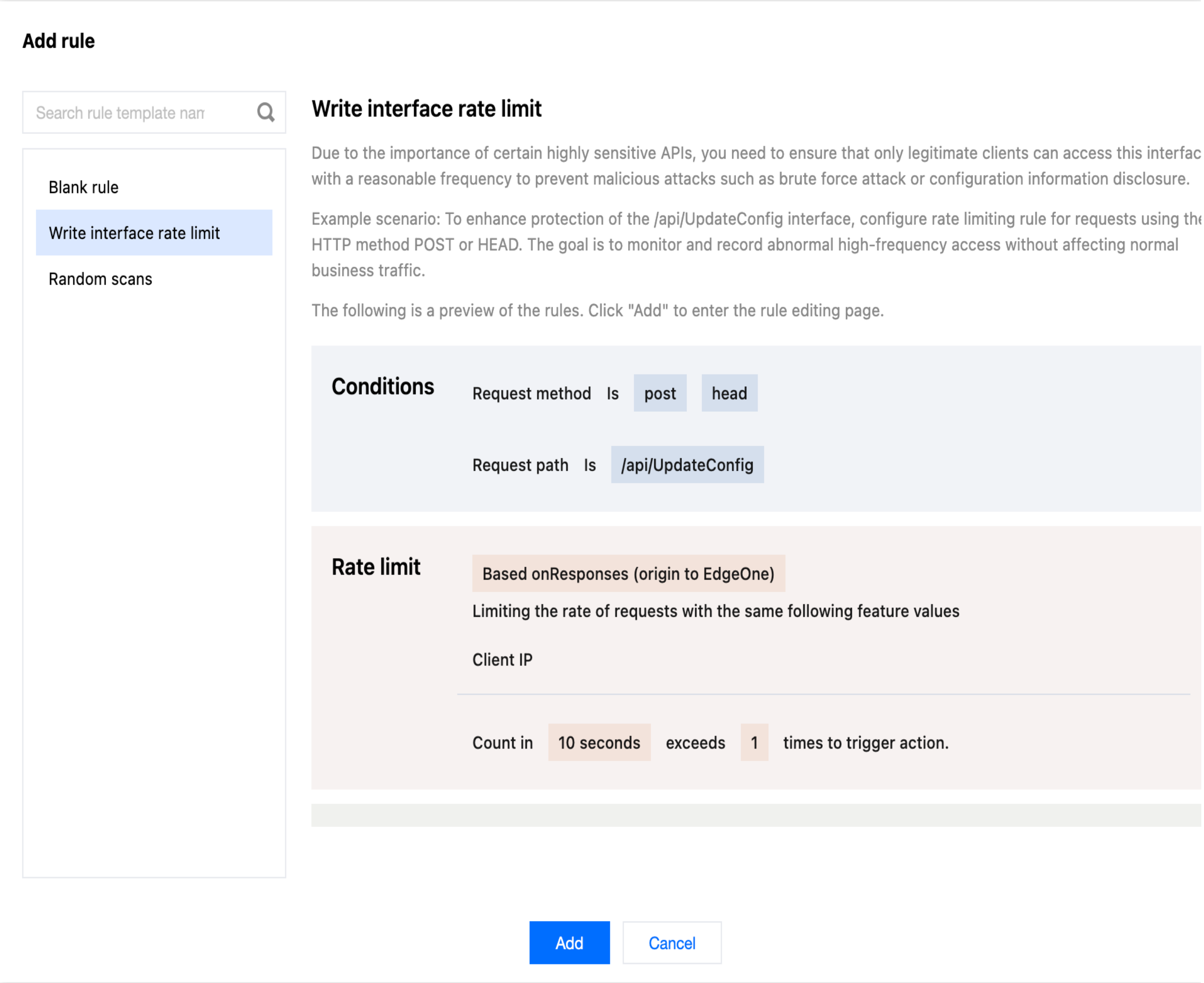
In the face of credential stuffing and brute force cracking attacks, attackers often frequently use access to the login API interface to try to obtain or crack information. By limiting the request frequency of the login interface, we can significantly mitigate the attacker's cracking attempts, effectively defend against such attacks, and protect sensitive information from being leaked.

For example: The domain name `www.example.com` provides an external interface `/api/UpdateConfig`, the allowed access call frequency is 100 times/minute, and when the frequency limit is exceeded, the IP will be blocked for 10 minutes. The operation steps are as follows:

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy . Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Rate Limiting** tab and click **Add rule** under **Rate limit**.
4. Enter the rule adding page, select the **Write interface rate limit** rule template, and click **Add**.

Note:

The configuration fields and example values in the rule template are for illustrative purposes only. You should conduct an evaluation and adjust the judgment conditions, rate thresholds, and actions according to your specific business requirements and normal traffic levels.



Add rule

Write interface rate limit

Due to the importance of certain highly sensitive APIs, you need to ensure that only legitimate clients can access this interfac with a reasonable frequency to prevent malicious attacks such as brute force attack or configuration information disclosure.

Example scenario: To enhance protection of the /api/UpdateConfig interface, configure rate limiting rule for requests using the HTTP method POST or HEAD. The goal is to monitor and record abnormal high-frequency access without affecting normal business traffic.

The following is a preview of the rules. Click "Add" to enter the rule editing page.

Conditions: Request method Is post head

Request path Is /api/UpdateConfig

Rate limit: Based onResponses (origin to EdgeOne)

Limiting the rate of requests with the same following feature values

Client IP

Count in 10 seconds exceeds 1 times to trigger action.

5. Configure the judgment conditions, rate thresholds, and actions. In this example scenario, you can configure the matching fields as **Request method** equals `POST` `HEAD` and **Request path** equals `/api/UpdateConfig` , adjust the statistical method to **Based on Responses (origin to EdgeOne)** , and configure the rate threshold as the count exceeding **100 times** in a counting cycle of **1 minute** to trigger an action. Adjust the triggered action to **Block** with a duration of **10 minutes** .
6. Click **Save and publish** . The rule will be deployed and take effect.

Example Scenario 2: Limit the request rate causing 404 status code to mitigate random resource scanning

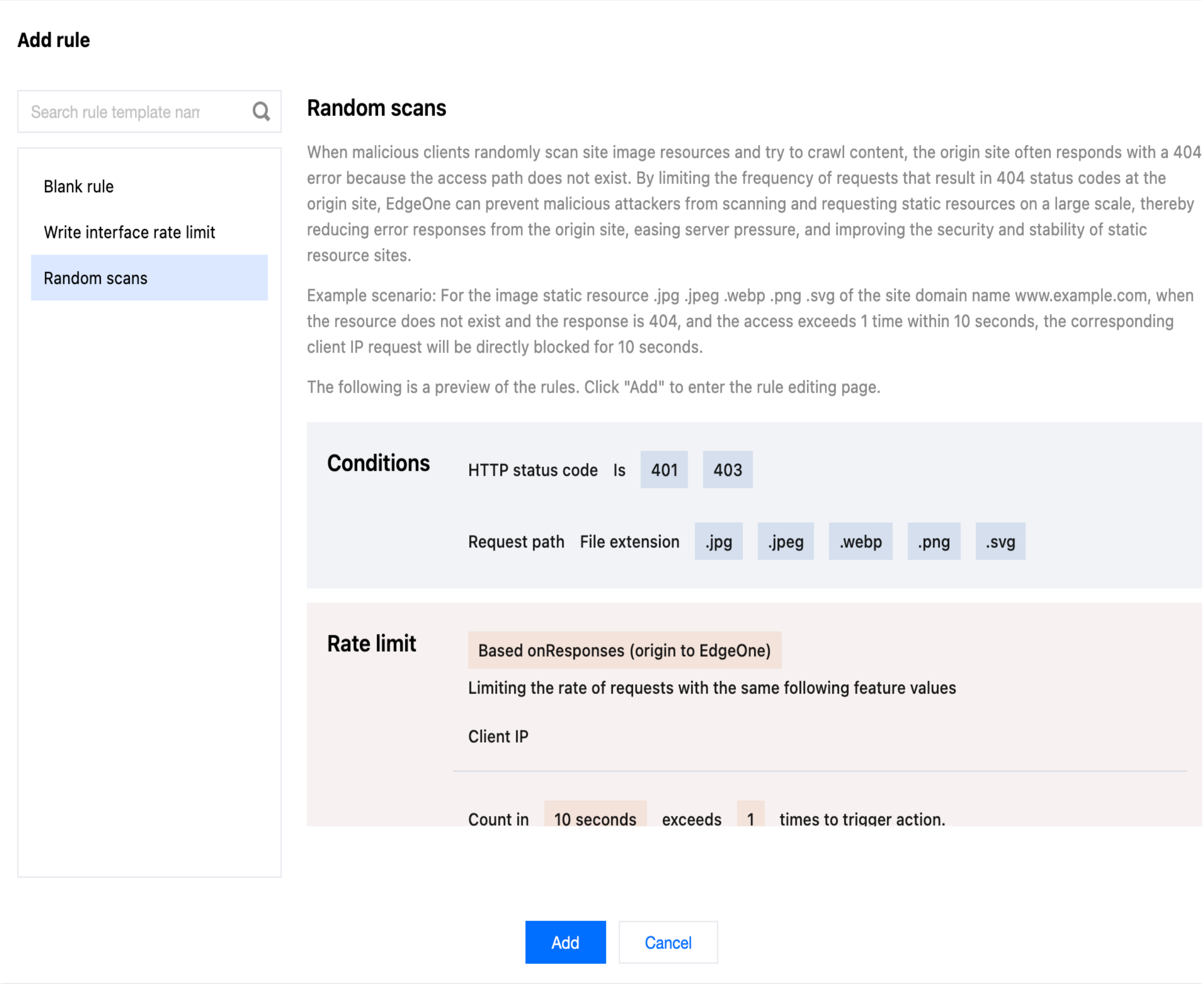
When malicious clients randomly scan site image resources and try to crawl content, they often cause the origin server to respond with a 404 error due to non-existent access paths. By limiting the request rate that causes the origin server's 404 status code, EdgeOne can prevent malicious attackers from scanning and requesting static resources on a large scale, thereby reducing the origin server's error response, alleviating server pressure, and improving the security and stability of static resource sites. For example: For the domain name `www.example.com` 's image static resources `.jpg``.jpeg``.webp``.png``.svg` , when the resource does not exist and responds with a

404, if the access exceeds 200 times within 10 seconds, the corresponding client IP request will be directly blocked for 60 seconds. The operation steps are as follows:

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy . Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Rate Limiting** tab and click **Add rule** under **Rate limit**.
4. Enter the rule adding page, select the **Random scans** rule template, and click **Add**.

Note:

The configuration fields and example values in the rule template are for illustrative purposes only. You should conduct an evaluation and adjust the judgment conditions, rate thresholds, and actions according to your specific business requirements and normal traffic levels.



Add rule

Search rule template nam

Blank rule
Write interface rate limit
Random scans

Random scans

When malicious clients randomly scan site image resources and try to crawl content, the origin site often responds with a 404 error because the access path does not exist. By limiting the frequency of requests that result in 404 status codes at the origin site, EdgeOne can prevent malicious attackers from scanning and requesting static resources on a large scale, thereby reducing error responses from the origin site, easing server pressure, and improving the security and stability of static resource sites.

Example scenario: For the image static resource .jpg .jpeg .webp .png .svg of the site domain name www.example.com, when the resource does not exist and the response is 404, and the access exceeds 1 time within 10 seconds, the corresponding client IP request will be directly blocked for 10 seconds.

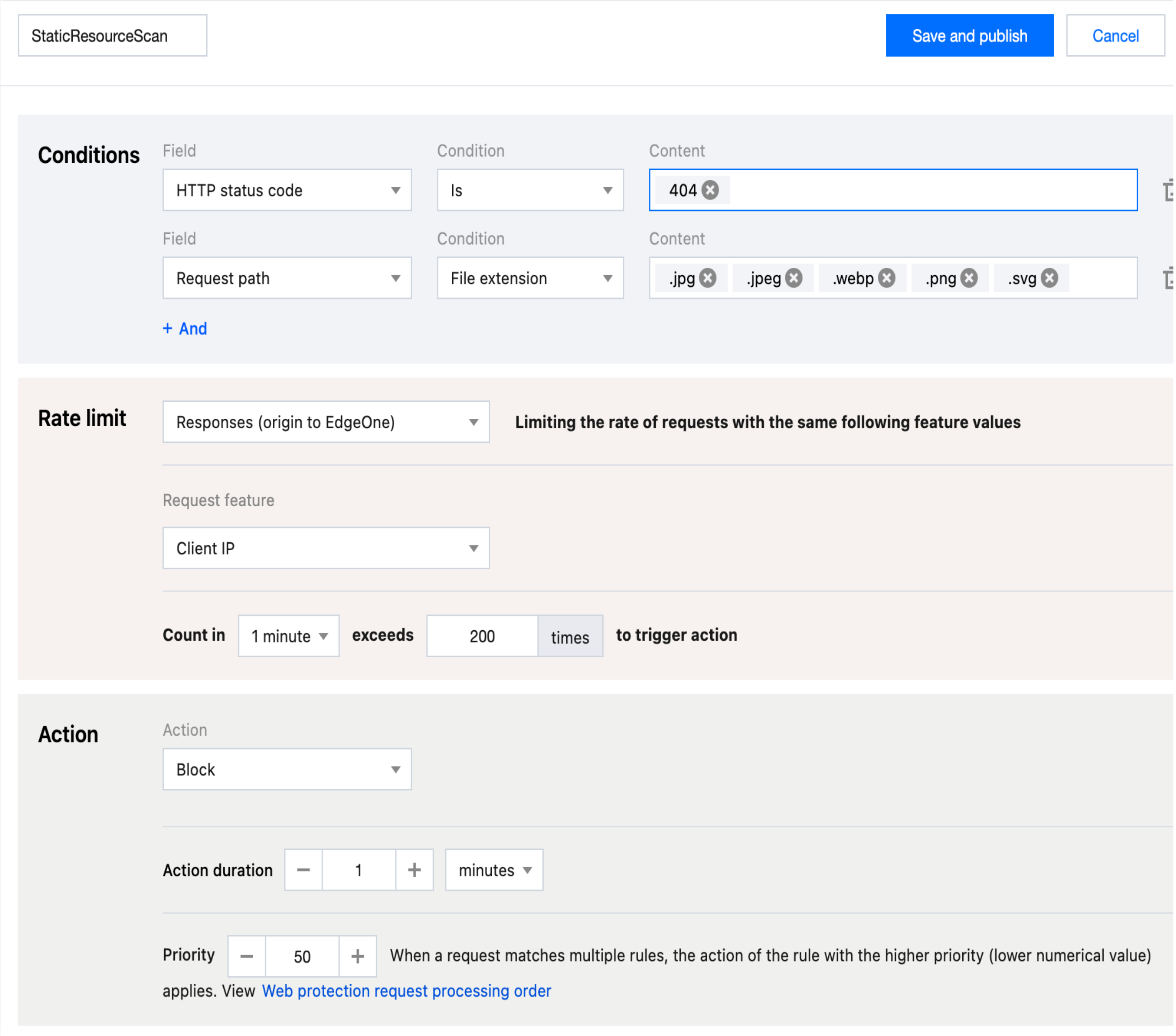
The following is a preview of the rules. Click "Add" to enter the rule editing page.

Conditions
HTTP status code Is 401 403
Request path File extension .jpg .jpeg .webp .png .svg

Rate limit
Based onResponses (origin to EdgeOne)
Limiting the rate of requests with the same following feature values
Client IP
Count in 10 seconds exceeds 1 times to trigger action.

5. Configure the judgment conditions, rate threshold, and actions. In this example scenario, you can configure the matching fields as **HTTP status code** (supported by the Enterprise plan) equals `404` and **Request path** with the **file extension** including `.jpg` , `.jpeg` , `.webp` , `.png` , and `.svg` . Adjust the statistical method to

Based on Responses (origin to EdgeOne) , and configure the rate threshold as the count exceeding **200 times** within a counting cycle of **1 minute** to trigger an action. Adjust the triggered action to **Block** with a duration of **1 minute** .


StaticResourceScan

Conditions

Field: HTTP status code | Condition: Is | Content: 404

Field: Request path | Condition: File extension | Content: .jpg .jpeg .webp .png .svg

Rate limit

Responses (origin to EdgeOne)

Limiting the rate of requests with the same following feature values

Request feature: Client IP

Count in 1 minute **exceeds** 200 times **to trigger action**

Action

Action: Block

Action duration 1 minutes

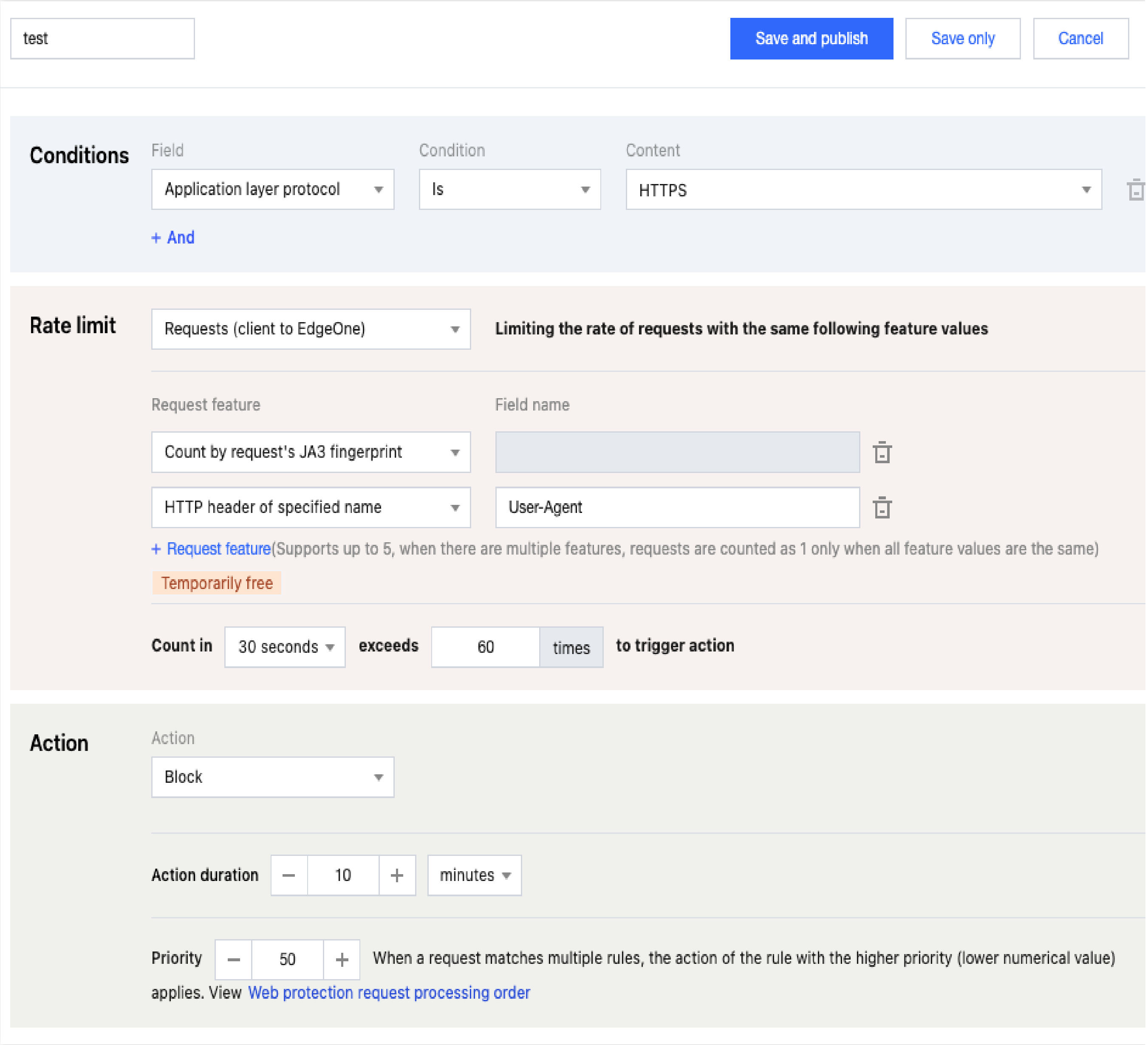
Priority 50 When a request matches multiple rules, the action of the rule with the higher priority (lower numerical value) applies. View Web protection request processing order

6. Click **Save and publish** . The rule will be deployed and take effect.

Example Scenario Three: Restricting High-Concurrency Search Engine Crawlers Access to Web Sites to Mitigate Impact on Regular Operations

A certain Y search engine provider employs a large-scale distributed crawler architecture, which lacks restrictions on access behavior. This leads to aggressive crawling activities, generating substantial traffic in a short period, potentially impacting normal operations and consuming significant resources. Therefore, rate limiting is used to identify and restrict such crawler access, mitigating its effects. For instance, the site `www.example.com` is affected by high-frequency visits from the Y search engine crawler. Through web security analysis, it is found that the distributed architecture used by the Y search engine crawler clusters in `JA3 fingerprint` and `User-Agent` characteristics. Hence, rate limiting rules are configured. When the number of access requests with the same JA3 fingerprint and User-Agent exceeds 60 within a 30-second statistical window, requests with identical JA3 fingerprint and User-Agent characteristics are intercepted, with the interception lasting for 10 minutes. The operational steps are as follows:

1. Log in to the Edgeone console and click **Site List** in the left sidebar. In the Site List, select the **Site** that requires configuration to proceed to the Site Details page.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy . Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Rate Limiting** tab and click **Add rule** under **Rate limit** .
4. On the rule adding page, select creating a blank rule, enter the rule name, and click **Add** .
5. Configure the judgment conditions, rate thresholds, and actions. In this example scenario, you can configure the matching field as **Application layer protocol** equals `HTTPS` and the statistical method as **Requests (client to EdgeOne)** . Select the request features as **JA3 fingerprint** and **User-Agent in the HTTP header** , and configure the rate threshold as the count exceeding **60 times** within a counting cycle of **30 seconds** to trigger an action. Configure the triggered action to **Block** with a duration of **10 minutes** .



test

Conditions

Field	Condition	Content
Application layer protocol	Is	HTTPS

Rate limit

Requests (client to EdgeOne)

Limiting the rate of requests with the same following feature values

Request feature	Field name
Count by request's JA3 fingerprint	
HTTP header of specified name	User-Agent

(Supports up to 5, when there are multiple features, requests are counted as 1 only when all feature values are the same)

Temporarily free

Count in 30 seconds exceeds 60 times to trigger action

Action

Action: Block

Action duration 10 minutes

Priority 50 When a request matches multiple rules, the action of the rule with the higher priority (lower numerical value) applies. View Web protection request processing order

6. Click **Save and publish** . The rule will be deployed and take effect.

Related References

When establishing rate limit rules, it is necessary to configure the rule specify scope, triggering method, and action. The explanations for each configuration item are as follows:

Note:

If your current rate rule needs to be matched based on **a specific known** value of the HTTP header, you can configure **judgment conditions > specified matching fields** for matching the **specified parameter value of HTTP header** .

If your current rate rule needs to be matched based on **a type of** HTTP headers that possibly contain the same value, you can configure **rate thresholds > request features** for matching the **HTTP header of specified name**

.

Specify Scope

Based on the origin of the request, header characteristics, response status codes, and other factors, a combination of matching conditions [1] is established. The rate limit rule is only applied to manage the operations that meet these conditions. For more information of the matching conditions and the level of support provided by different packages, please refer to Matching Conditions.

Trigger Method

Note:

1. If the rate limit threshold is not reached, the request will not be handled or logged.
2. Specific configuration options and the configurable range vary with different subscription plans. For details, see Comparison of EdgeOne Plans.
3. In the counting cycle options, the **1 second** option only supports the request features **Client IP** and **Client IP (prioritizing XFF header)** .

The rule will based on the statistical rules configured in the trigger method. When the cumulative number of requests within the counting cycle exceeds the threshold, the rule is activated and executes the corresponding limiting action[2].

The tally is based on the technical cycle and statistical method, counting the number of requests for different feature values under the specified feature dimension (such as client IP) [1]. You can define the following parameters for the trigger method:

Counting Cycle: The length of the rolling time window used for counting. It supports a minimum of 1 second and a maximum of 1 hour.

Statistical Method: The method of distinguishing request sources, where the rate limit is to limit the request rate for each source. Refer to the statistical dimension for details.

Rate Threshold: The number of requests allowed per source (such as client IP) within the counting cycle.

Trigger State Retention Duration: After the rule is triggered, the duration for which requests matching the conditions of this source are continuously limited[3]. It supports a minimum of 1 second and a maximum of 30 days.

Request Features

Supports statistical analysis based on one or more request characteristics. When the request features within the statistical dimension reach the rate threshold set in the trigger method, the rate limit rule is activated. You may specify the following statistical dimensions[1]:

Client IP: Requests originating from the same source IP will be accounted for in a singular counter. Upon exceeding the threshold, the rule's disposition action is triggered.

Client IP (prioritizing XFF header): Requests originating from the same client IP will be accounted for in a single counter, triggering the rule's disposition action upon exceeding the threshold. When the X-Forwarded-For header is present and contains a valid IP list, the first IP in the X-Forwarded-For header will be prioritized for statistics.

Designated Cookie Name: Extracts the value of the specified cookie name from the request header. Requests with identical cookie values are counted in the same counter. When the threshold is exceeded, the rule's disposition action is triggered.

For instance, when a site employs a cookie labeled `user-session` to mark visitation sessions, you can configure the value of the cookie named `user-session` as a statistical dimension, thereby tracking the request rate of each session. If the request rate within a single session surpass the threshold, the disposal action configured in the rule will be triggered.

Designated Name HTTP Header: Extracts the value of the specified name in the request header, with requests bearing identical header values being accounted for in the same counter. When this threshold is surpassed, the rule's disposition action is triggered. For instance, you may specify the Origin header to limit the access frequency from each external domain. When the access frequency from a particular external domain exceeds the threshold, the disposition action configured by the rule is initiated.

Specified Name URL Query Parameter: Extracts the value of the specified name parameter from the request URL query parameters. Requests with the same query parameter value are counted in the same counter, triggering the rule's disposition action when exceeding the threshold.

For instance, when a site uses a query parameter named `user-session` to mark access sessions, you can configure the specified name `user-session` as a statistical dimension, tallying the request rate for each session. When the request rate within a single session surpasses the threshold, it triggers the disposition action configured by the rule.

Request JA3 Fingerprint[4]: Compute the JA3 fingerprint for each request, tallying the count of requests with identical JA3 fingerprints, and triggering the rule's disposition action when the threshold is exceeded. Each request corresponds to a unique JA3 fingerprint value, with no key-value model present, thus eliminating the need for specified parameter input. Considering the characteristics of JA3, it is recommended that you configure it at the same time as the User-Agent header statistics dimension to better distinguish clients.

Access Path of Request : Extracts the access path (URL path, excluding the URL query parameters) from the request. Requests with the same access path will be counted in the same counter. When the threshold is exceeded, the action of the rule is triggered.

Notes:

1: Depending on the package you subscribe to, the configurable matching conditions, statistical dimensions, and action options may vary. For more details, please refer to the Package Options Comparison.

2: If multiple rate limit rules exist, a single request can match multiple rule contents simultaneously, and the decision to trigger the rule will be based on the statistical methods of different rules. Once a rule is triggered and blocked, the remaining rules will not be triggered. When multiple rules are triggered simultaneously, they are executed in the order of priority of the triggered rules, with the rules with smaller priority values matching first. For more information, see the Web Protection Request Processing Order.

3: Once a rule is triggered, it only applies to requests that match the current rule.

4: A JA3 fingerprint is identification information formed based on the client's TLS information, which can effectively distinguish requests from different Bot networks. When a request is initiated based on a non-SSL HTTP protocol, the JA3 fingerprint of the request is empty. If you need to use a JA3 fingerprint, please ensure that the Bot management function has been enabled for your current domain.
5: If you need to perform statistics on requests with the same characteristics through a combination of multiple statistical dimensions, you need to subscribe to the EdgeOne Enterprise Edition package.

Action

When requests exceed the established threshold, corresponding restrictive actions are implemented. These include block, monitor, JSChallenge, redirect and ReturnCustomPage[1]. For more information, please refer to the section on Disposal Methods.

Bot Management

Overview

Last updated：2024-08-01 21:37:22

Bot management is a service that maintains the quality of your website traffic. Among your website visitors, there may be a portion of visits that are not initiated by real users, but by automated programs, which we usually call bots. Although some bots (e.g., search engine crawlers) are beneficial to the website, they may also cause the following issues:

1. **Abnormal website traffic or performance degradation:** A large amount of bot traffic may consume a lot of server resources, affecting the access experience of real users. In this case, bot management helps to identify and control these bots, optimizing website performance and improving user experience.
2. **Abnormal data statistics, such as traffic and click-through rates:** This may be caused by bots simulating user behavior. Bot management can more accurately distinguish between real user and bot behavior, allowing you to obtain more realistic data.
3. **Website content or user information leakage or abuse:** Bots may try to crawl and copy website content or obtain user personal information. Bot management can effectively block unauthorized access, protecting the security of website content and user information.

If you encounter the above issues while operating a website, then bot management is the tool you need.

Feature Overview

Bot management mainly includes the following features,Bot management will process requests in the following order.

Note：

Bot management functions are only supported when the domain name of the site has bot management capabilities enabled. After enabling, the billing standard for bot management can be found in VAU Fee (pay-as-you-go).

Module	Configurations
Custom bot rules	Customizable and flexible bot management rules, supporting multiple identification mechanisms and providing flexible disposal options. For example, delay the response of half of the automated shopping cart crawlers and silently dispose of the other half.
Basic feature management	Identify bot tools and control them by combining the User-Agent header and client IP within the request with the corresponding features of search engines and tools. For example, allow search engine bots to access website resources.
Client reputation	Identify malicious bots and provide control by combining the client IP with the threat intelligence database.

	For example, intercept bot behavior that uses flash dial IP and other proxy device pools for malicious access.
Bot intelligence	Quickly deploy bot identification mechanisms, integrate multiple bot feature identification mechanisms, quickly deploy, identify and analyze website traffic patterns. It provides a clear view of user and bot visitors by automatically analyzing and classifying traffic and allows for appropriate disposal decisions for different types of traffic.
Active detection	Identify human browser clients (not applicable to native mobile apps) by verifying the client's runtime environment and access behavior through Cookie and JavaScript.

Bot Intelligent analysis

Last updated：2024-08-26 09:38:50

Overview

Bot Intelligent Analysis is suitable for situations where rapid deployment, identification, and analysis of website traffic patterns are needed. Bot Intelligent Analysis is based on a clustering analysis algorithm and a big data model intelligent engine, aiming to help you comprehensively judge the risk of requests from multiple perspectives and more conveniently use Bot management to quickly identify and deal with known or unknown bots, avoiding fixed single strategies being bypassed. Bot Intelligent Analysis will comprehensively analyze multiple factors and classify requests into normal requests, normal bot requests, suspicious bot requests, and malicious bot requests, and support the configuration of corresponding action methods for different types of requests.

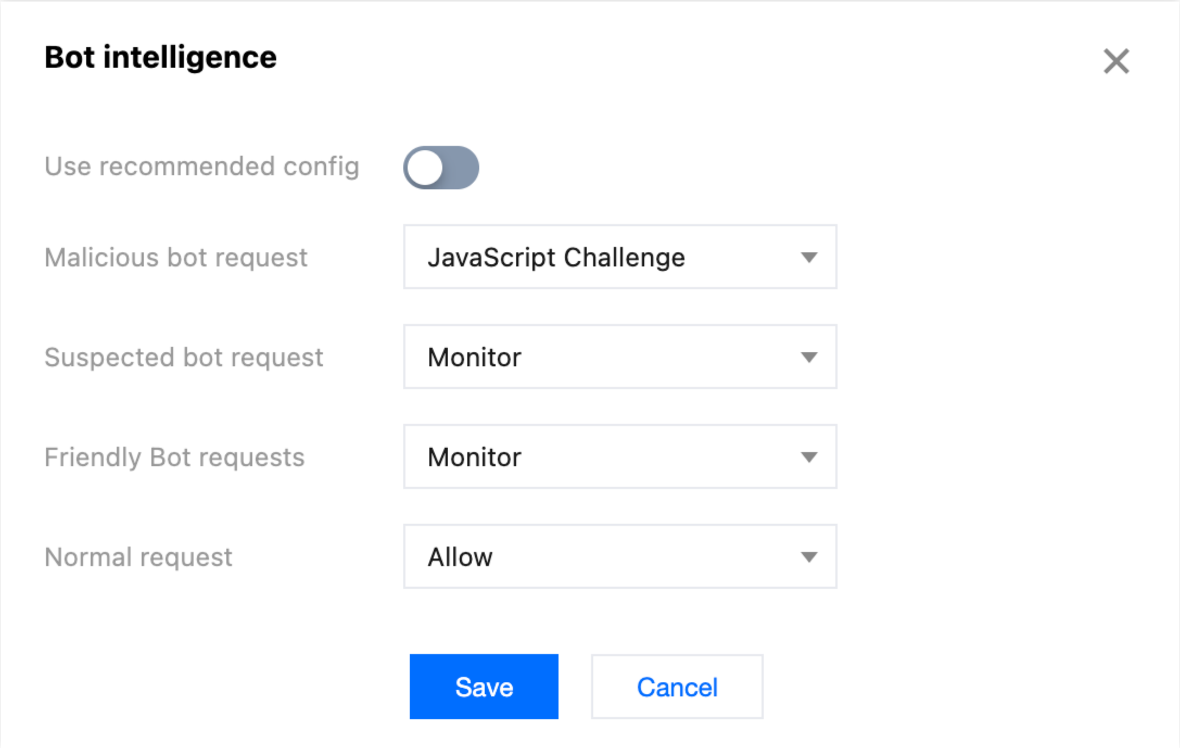
Note:

Bot Intelligent Analysis integrates the request characteristics in Bot Basic Management and Client Reputation Analysis functions and combines dynamic clustering analysis to form request risk tags. Bot Intelligent Analysis can help you understand the overall visitor situation and quickly deploy Bot management strategies. If you have very clear policy requirements for request features (for example, allowing specific search engine requests, intercepting Web development tool requests, etc.), you can further use Bot basic management, Client reputation, and Custom bot rules for policy adjustment.

Directions

For example, the e-commerce site `shop.example.com` found that the product display page had a sudden increase in access volume, and it was judged that it might have suffered a large number of bot visits. The Bot Intelligent Analysis strategy can quickly enable Bot management functions to intercept bot tools. You can follow the steps below:

1. Log in to the EdgeOne console, click the site list in the left menu bar, click the site to be configured in the site list, and enter the site details page.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `shop.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Bot Management** tab and click **Edit** under **Bot intelligence** to enter the configuration page.
4. Configure the corresponding action for each bot analysis tag. In this example scenario, you can configure the action to **JavaScript Challenge** for malicious bot requests, and maintain it as **Monitor** for suspected bot requests and friendly bot requests.



Bot intelligence

Use recommended config: off

Malicious bot request: JavaScript Challenge

Suspected bot request: Monitor

Friendly Bot requests: Monitor

Normal request: Allow

5. Click **Save** to complete the configuration.

Related References

Request Bot Tags

Bot Intelligent Analysis classifies requests into the following types based on the analysis results:

Malicious bot requests: Requests from bots with higher risks, suggested to be configured as interception or challenge actions.

Suspicious bot requests: Requests from bot clients with certain risks, suggested to be configured as at least observation or challenge actions.

Normal bot requests: Valid crawler requests, including requests from search engine crawlers.

Normal requests: Client requests without obvious bot features, only support release action.

Factors Affecting Bot Intelligent Analysis Judgment

The Bot intelligence engine will comprehensively evaluate requests based on the following main factors:

1. **Request rate:** The request rate will affect the identification of bots, and too high request rate may indicate malicious bot behavior.
2. **IP Intelligence Library:** The engine will refer to IP intelligence library to identify whether there are malicious behavior records or blocklist information.
3. **Search Engine Features:** Based on whether the source IPs match valid search engine crawlers, such as Google, Baidu, etc.

4. **Access URL sequence:** Analyze the sequence and pattern of accessed URLs to evaluate whether the request is similar to normal user behavior or normal bot behavior.

5. **JA3 Fingerprint**Note 1: Use JA3 fingerprint technology to identify the features of client TLS connections, such as identifying non-browser clients like Python tools.

6. **BotnetID Fingerprint**Note 2: By analyzing the BotnetID fingerprint and comparing it with known malicious BotnetIDs, malicious crawler behavior from botnets can be identified.

Note:

Note 1: JA3 is a fingerprint generation method for features in the TLS handshake process of clients. By collecting information provided by clients during the TLS handshake process (such as supported encryption suites, extensions, etc.), a unique hash value is generated as a fingerprint. JA3 fingerprints can help us identify clients that initiate requests using specific tools or libraries, such as requests initiated using Python libraries. By comparing the client's JA3 fingerprint with the fingerprints of known malicious tools or libraries, we can more accurately identify potential malicious bot behavior.

Note 2: BotnetID is an identification method based on bot network behavior characteristics. Bot networks (Botnets) are usually composed of multiple controlled malicious devices, which may be used to launch attacks or perform other malicious activities. By analyzing client behavior characteristics and their similarity to known bot networks, a BotnetID can be generated. By comparing the client's BotnetID with known malicious bot network IDs, we can more accurately identify potential malicious bot behavior.

Bot Basic Feature Management

Last updated：2024-08-26 09:38:50

Overview

Many public or commercialized programs, including search engine crawlers, have fixed or default User-Agent header features and have specific purposes. Bot Basic Feature management policies include most public bot type features, and you can directly manage bot tools that meet these features, which can help you:
1) Allow search engine crawlers to access and avoid being blocked wrongly;
2) Identify specific-purpose commercialized tools and limit their access.

EdgeOne will regularly update the features of automated tools to ensure that your management strategy continues to cover control scenarios.

Usage Scenarios

By default, the Bot Basic Feature management strategy is in a disabled state. When you have the following scenario demands, you can enable and adjust the bot basic management protection strategy as needed:

Control requests from IDC (data center)

Most of the access to To C applications comes from mobile networks, broadband providers, or educational networks, and normal requests do not come from data centers (IDC). Therefore, requests from cloud providers or data centers are mostly from proxies or crawlers. You can choose to control requests from data centers (IDC) and intercept or perform JavaScript challenges to mitigate the risk of malicious access.

Control valid bot requests with search engine features

Search engine crawlers are currently one of the few valid bot types. In order for sites to distinguish valid crawlers from search engines, most search engine providers provide the IP segment and UA features used by their crawler engines. EdgeOne's search engine feature rules include search engine public IP features, User-Agent header features, rDNS resolution features, and other matching methods. You can configure bot requests with search engine features to be released to avoid being intercepted by bot management policies.

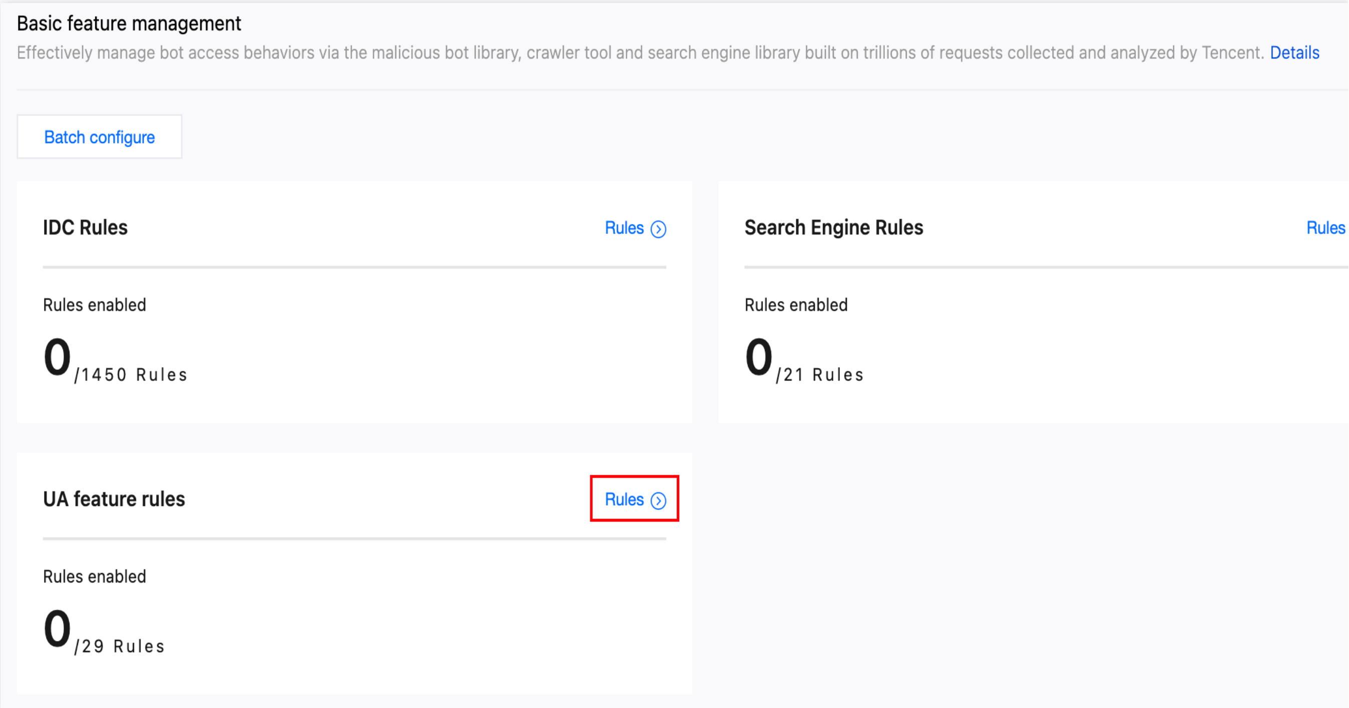
Control requests from commercial or open-source tools

Commercial software or open-source tools often carry specific User-Agent features. EdgeOne classifies these automated tools based on their usage and regularly updates the corresponding User-Agent library. If you do not allow bot requests from these commercial or open-source tools, you can intercept them.

Adjust Basic Feature Management Protection Strategy

For example, in an e-commerce site `shop.example.com` , to prevent users from placing orders and rushing to purchase through tools, you should disable the automated shopping cart bot. You can take the following steps:

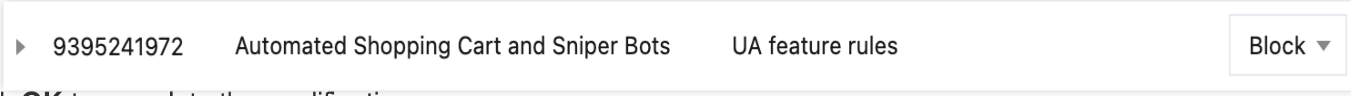
1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **Site** you wish to configure.
2. Click **Security** > **Web Security**.By default, it is a **Site-level security policy**. Click **Domain-level security policy Tab**, in the Domain-level security policy, click **Target Domain** to enter the Target Domain security policy Configuration Interface, for example: `shop.example.com` .
3. Navigate to **Bot Management** card, select **Basic feature management** in the **UA feature rules**, click the top right corner **Rules.**



Basic feature management

Effectively manage bot access behaviors via the malicious bot library, crawler tool and search engine library built on trillions of requests collected and analyzed by Tencent. Details

4. On the rules page, you can modify the action for a specified rule ID individually. If you need to perform batch configuration, you can click **Batch configure**, batch check the rule IDs to be configured, select the action, and then apply. In this example scenario, you can control the automated shopping cart bot by modifying the action of this rule to **Block**.



9395241972 Automated Shopping Cart and Sniper Bots UA feature rules Block

5. Click **OK** to complete the modification.

Client Reputation

Last updated：2024-08-26 09:38:50

Overview

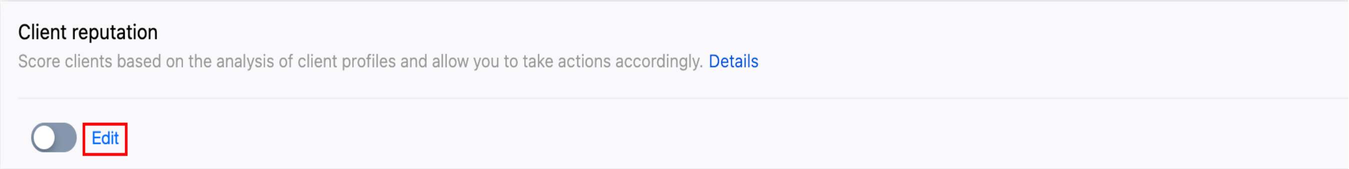
Malicious bots usually initiate requests through proxy pools, botnets, or specific devices. EdgeOne's client reputation analysis uses Tencent's nearly 20 years of network security experience and big data intelligence accumulation to determine the real-time state of IP, adopt scoring mechanisms, quantify risk values, and precisely identify access from malicious dynamic IPs. It accurately identifies high-risk clients, updates the latest threat intelligence every 24 hours, and provides threat confidence reports for different IP addresses. According to the different types of attack clients, it provides 5 risk classifications and confidence levels. You can help control multiple categories (network attack sources, exploited network proxy devices, vulnerability scanning tools, brute force cracking behaviors, etc.) of high-risk client access by customizing the protection strategy for each threat confidence level, reducing business risks and effectively intercepting such malicious behaviors.

Example Scenario

In the Web security analysis module, you observe that under the site `api.example.com` , the login interface `/api/login` has high-frequency access, and there are a large number of failed access requests in a short period of time. However, due to the large number of access IPs, mainly from broadband operator networks, a single IP request is only 1-2 times. Judging from the access features, it is suspected that dial-up IPs are used for brute force cracking login attempts. To strengthen the security policy, we suggest intercepting higher confidence network proxy clients and setting medium confidence clients to observe.

Directions

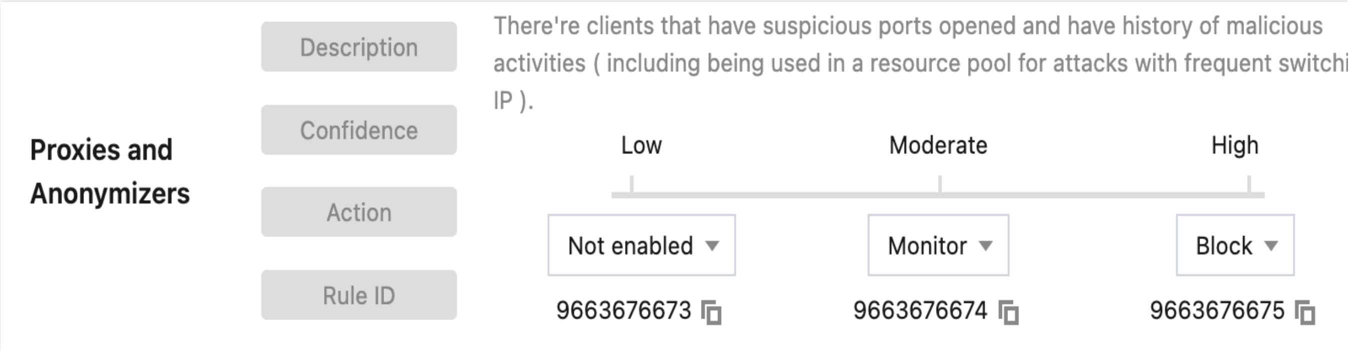
1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. Click **Security > Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `shop.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Bot Management** tab and click **Edit** under **Client reputation** to enter the configuration page.



Client reputation

Score clients based on the analysis of client profiles and allow you to take actions accordingly. Details

4. Client reputation is classified into network attack, network proxy, scanner, account takeover attack, and malicious bot. For different client types, you can select the corresponding action based on the client credibility level. In this example scenario, dial-up IPs belong to a typical network proxy client. When high-frequency access from dispersed IPs is monitored at the site, you can **block** high-credibility network proxy clients, and set the action to **Monitor** for moderate-credibility clients.



Proxies and Anonymizers

Description: There're clients that have suspicious ports opened and have history of malicious activities (including being used in a resource pool for attacks with frequent switchi IP).

Confidence	Low	Moderate	High
Action	Not enabled ▼	Monitor ▼	Block ▼
Rule ID	9663676673	9663676674	9663676675

5. Click **OK** to complete the configuration.

Related References

Risk Classification

Client reputation analysis is based on real-time threat intelligence libraries and can effectively identify clients with the following 5 types of malicious behavior history:

Network attack: Clients with recent attack behavior (such as DDoS, high-frequency malicious requests, site attacks, etc.). For example, attacks initiated by the Mirai botnet can be classified into this category.

Network proxy: Clients that have recently opened suspicious proxy ports and have been used as network proxies, including dial-up IP proxy pools and IoT proxy networks used to initiate malicious requests.

Scanner: Clients with recent scanner behavior targeting known vulnerabilities. For example, vulnerability scanning tools for Web applications.

Account takeover attack: Clients with recent malicious login cracking and account takeover attack behavior. For example, attackers who use brute force to crack user login credentials.

Malicious bot: Clients with recent malicious bot, hotlinking, and brute force cracking behaviors. For example, illegal bots that collect website content.

Credibility Level

For each category of client reputation rules, each credibility level corresponds to a client address list. The credibility level reflects the frequency and consistency of the client address's recent malicious behavior in that category:

Higher credibility: The client address has recently engaged in stable, high-frequency malicious behavior in that category. It is recommended to intercept such clients.

Moderate credibility: The client address has recently engaged in significant frequency malicious behavior in that category. It is recommended to configure such clients for JavaScript challenge or observation.

General credibility: The client address has recently engaged in stable malicious behavior in that category. It is recommended to configure this type of client as an observation, and then adjust it to a JavaScript challenge or a hosting challenge based on the analysis results.

Active Detection

Last updated：2025-05-29 10:21:21

Overview

In addition to analyzing the received client requests, identifying features in the headers and client IP, EdgeOne also provides an active detection bot identification method. Active detection can perform Cookie verification and session tracking on the client, as well as client behavior verification for interaction, and further identify whether the current visitor is a tool based on the client's interaction feedback. Active detection has the following advantages:

It has a strong identification effect on tools that can simulate browser behavior (such as: Headless Chrome, etc.).

Compared with other front-end verification methods (such as: CAPTCHA human-machine verification), the integration of active detection is less intrusive to the business, and users can hardly perceive it, which can bring you better bot identification results and integration experience.

If your current site service provides login/registration/payment services and has high business value (for example: you can obtain the value within the account after obtaining the account, and you can obtain scarce goods or services through payment, etc.), it is recommended that you enable active detection for key business interfaces.

Note:

1. Due to the characteristics of the active detection mechanism, before enabling it, please confirm that your business is a **Web browser client**, or restrict the active detection rules to resources that **only allow Web browser access** through matching conditions to avoid compatibility issues affecting mobile app access.
2. This function is still in beta. If you need to enable it, please contact us.

Supported capabilities

Active detection supports the following two capability configurations:

Cookie verification and session tracking: Through the HTTP session state (Cookie mechanism), a dynamic session token is issued to each visitor, and the visitor's request must carry a valid session token. In this way, requests from different visitors can be tracked and their behavior characteristics can be identified. In addition to verifying the legality of the Cookie in the request, Cookie verification will also identify tampered session information and high-frequency collection of Cookie information behavior, reducing the security risks caused by session hijacking.

Client behavior verification: Advanced automation tools (such as: Headless Chrome) can already simulate browser behavior. Client behavior verification will inject JavaScript code into the HTML response page, collect the client's JavaScript runtime environment, device environment, and client interaction behavior, and thus identify the tool environment and normal request visitors.

Client Interaction Process

Scenario 1: Intercept ordinary Web tool crawlers and access to the media site

Scenario Example

The media site `media.example.com` only allows H5 clients and browsers to obtain site content, and all legal clients support `Cookies` . Therefore, clients that do not support `Cookies` need to be intercepted, including crawlers that have hijacked other visitors' sessions. For clients that maliciously tamper with `Cookies` , use the silent mode to counteract, maintain the connection but no longer respond to requests.

Directions

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. Click **Security** > **Web Security**. By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `media.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Bot Management** tab and click **Add rule** under **Active detection** to enter the configuration page.
4. Configure the judgment conditions and actions. In this example scenario, you can configure the matching fields as **Request path (Path)** matching the regular expression `/*` and **Request method (Method)** equals `GET` .
Configure the operation to **Validate cookie** and the verification method to **Update and validate**.
For requests carrying no cookies or an expired cookie, configure the trigger threshold to 300 times within 10s and the action to **Block**.
For requests carrying an invalid cookie, configure the action to **Drop w/o response**.

For action details of the bot management module, see Action. Other related configurations are described as follows:

Configuration item	Description
Verification method	**Update Cookie and verify:** For requests that do not carry valid session information or have expired session information, EdgeOne will create a session in the response with the

	Set-Cookie header and continuously update the session information. It is recommended to use this verification method for paths accessed by GET. **Only verify:** EdgeOne only verifies whether the session information carried in the request is legal. When the session information in the request expires or the request does not carry valid session information, it will not create a new session by updating the Cookie. It is recommended to use the only verification method for APIs accessed by POST (such as: registration, login, add to cart, etc.).
Validation result	For requests that have failed the Cookie verification, the processing can be done according to the check result as follows: **No Cookie or expired Cookie:** The session information carried in the Cookie header has a time limit and is only valid for a certain period of time. If the request does not carry valid session information or the session information has expired, the session information needs to be updated to pass the Cookie verification. When the client frequently uses requests without session information to access, there may be a risk of harvesting Cookies and hijacking sessions. You can choose to dispose of requests from the request sources (client IP) that do not carry valid session information when the session information is not carried at a specified rate. **Trigger threshold:** You can configure the upper limit of the number of sessions that can be created without carrying a Cookie or an expired Cookie within a certain period of time, and limit the initiation rate of new sessions. When the trigger threshold is exceeded, it will be processed according to the configured action. **Invalid cookie:** The session information issued by EdgeOne has encryption verification capabilities, and tampering with session information often means malicious requests. You can choose to dispose of requests with tampered session information.
Cookie-based session check	Requests that pass the Cookie verification are divided into high-risk, medium-risk, and low-risk categories according to the specified rate features. You can configure different actions for each risk level to more effectively identify and mitigate malicious behaviors: **High risk:** In a single session (corresponding to the same EO-Bot-SessionId value in the Cookie header), more than 1000 requests in each 5-minute statistics window. When client behavior verification is enabled, also verify that the same client verification token (corresponding to the same EO-Bot-Token value in the Cookie header) is used more than 200 times in 1 minute. **Medium risk:** In a single session (corresponding to the same EO-Bot-SessionId value in the Cookie header), more than 500 requests in each 5-minute statistics window. When client behavior verification is enabled, also verify that the same client verification token (corresponding to the same EO-Bot-Token value in the Cookie header) is used more than 100 times in 1 minute. **Low-risk:** In a single session (corresponding to the same EO-Bot-SessionId value in the Cookie header), more than 100 requests in each 5-minute statistics window. When client behavior verification is enabled, also verify that the same client verification token (corresponding to the same EO-Bot-Token value in the Cookie header) is used more than 20 times in 1 minute.

5. Click **Save and publish**. The rule will be deployed and take effect.

Scenario 2: Strengthening the e-commerce site's password reset page and API using client behavior verification to combat against Account Take Over (ATO) attacks from bulk password reset attempts

Scenario Example

The password reset API `/api/password_reset` of the e-commerce site `shop.example.com` has a large number of failed reset requests from a large amount of IPs with low frequency and no obvious `User-Agent` or header aggregation. Therefore, the active detection function is used to strengthen the bot protection rules for the password reset API `/api/password_reset` and the password reset page `/account/forgot_password.html` , using silent mode to combat against automated bulk password reset tools.

Directions

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. Click **Security** > **Web Security**. By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `shop.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Bot Management** tab and click **Add rule** under **Active detection** to enter the configuration page.
4. Configure the judgment conditions and actions. In this example scenario, you can configure the matching field as **Request path (Path)** equals `/account/forgot_password.html` . Configure the operation to **Validate client behavior**, the Proof-of-work strength to **High**, and the delay to **Delay for 100 ms** :

For **clients not enabled JS**, configure the action to **Add long latency** when the requests are greater than **10 times** within **10s**.

For **clients timed out**, configure the action to **Drop w/o response**.

For **Bot clients**, configure the action to **Drop w/o response**.

Note:

Client behavior verification will be performed by injecting JavaScript only when the response `Content-Type` is `text/html` . Other requests will be handled based on the current verification result.

For action details of the bot management module, see Action. Other related configurations are described as follows:

Configuration item	Description
Proof-of-work strength	Client behavior verification supports adjusting the strength of proof of work verification. By adjusting the strength, the balance between the client's computational load and the identification effect on bots can be achieved.
Execution method	The JavaScript code used for detection will run after the whole page is loaded, and it also supports delaying the execution of the JavaScript detection code for a certain time. This helps to avoid affecting the normal page rendering, ensuring that the browser loads the page first before performing the verification, thus avoiding affecting the user's browsing experience.
Validation result	**Client does not enabled JS (not completed detection):** For clients that do not support JavaScript or requests initiated before the verification is completed, they are classified into this category. Since JavaScript verification usually takes some time, you can allow a certain rate of requests to pass before the client completes the verification, and dispose of clients that have not passed the verification and initiate high-frequency requests. **Client timed out:** The client supports JavaScript and has started the verification, but it cannot be completed within 60 seconds. 60 seconds is enough for normal browser clients to complete the client behavior verification, while IoT proxies with less computing power have a higher probability of verification timeout. This option can be used to distinguish and dispose of requests from distributed bot networks with low computing power. **Bot client:** The client has successfully completed the JavaScript verification, and the detection module finds that the client's running environment is abnormal, and it is not a normal human accessing through a browser.

5. Click **Save and publish**. The rule will be deployed and take effect.

Custom Bot Rule

Last updated：2025-05-30 10:26:24

Overview

When you need to customize fine-grained policies for specific bot behaviors or features based on existing Bot management policies, custom bot rules can provide you with flexible matching conditions (such as client IP, header information, request method, static feature recognition, and client reputation analysis results), and can be combined with disposal strategies that randomly select actions by weight, helping you create accurate management strategies to effectively manage the risks brought by bot access to the site.

Note:

Custom bot rules support randomly configuring multiple actions by weight. For example, you can configure 25% of requests as observation, 25% of requests as interception, 25% of requests as release, and 25% of requests as Managed Challenge. This approach can confuse bot tools' perception of bot effectiveness while also helping to reduce risk during the Canary testing phase.

Scenario 1: Silent Processing to Avoid Risks when Bot Requests for Sensitive API Interfaces Surge

Scenario Example

In Web security analysis, a large number of sudden request accesses to the login interface are found. After reviewing the abnormal clients, the requests mainly come from multiple proxy clients in the `222.22.22.0/24` IP segment, trying to log in to accounts using various types of clients. To urgently mitigate business risks and consume malicious tool resources, silent processing can be used to handle requests from related sources (maintaining client TCP connections but no longer responding to HTTP requests).

Directions

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Bot Management** tab and click **Add rule** under **Custom rules** to enter the configuration page.
4. Enter the rule name and configure the judgment conditions and actions. In this example scenario, you can configure the matching fields as **Client IP** equal to the `222.22.22.0/24` IP range and **User-Agent** including `cURL` ,

and select the action as **Drop w/o response** .++

Note:

Priority: The lower the value, the higher the priority. When a request matches multiple rules, the action of the rule with the higher priority (lower numerical value) applies.

5. Click **Save and publish** . The rule will be deployed and take effect.

Scenario 2: Implement a Combination of Multiple Disposal Methods for Bot Management Policies on the Login Page to Reduce the Risk of Account Theft (ATO: Account-Take-Over)

Example Scenario

In order to control the risk of account theft and prevent batch login methods from stealing accounts, the business needs to conduct human-machine verification for access to the login page while ensuring the best possible user experience. Clients with a higher credibility level of account takeover risk (including brute force and other account theft methods) can be controlled: a certain proportion of login page accesses will be subject to human-machine verification, while other requests will be subject to a short time wait, ensuring that when tools attempt batch logins, they will trigger a human-machine challenge after a certain number of attempts and avoid high-frequency attempts through short time waits.

Directions

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. Click **Security > Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Bot Management** tab and click **Add rule** under **Custom rules** to enter the configuration page.++
4. Enter the rule name and configure the judgment conditions and actions. In this example scenario, you can configure the matching field as **Client reputation** equal to **Account Take Over Attackers-High confidence** . For the action, first select **Managed Challenge** and then click **Add action** to add the **Add short latency** action. Set the weight to 20% for **Managed Challenge** and 80% for **Add short latency**.

5. Click **Save and publish** . The rule will be deployed and take effect.

Scenario 3: Optimize the Bot Intelligent Analysis Policy and Allow Requests with Specified Bot Intelligent Analysis Features

Example Scenario

After the site enables Bot intelligent analysis, it identifies Bot tags for site requests based on the general policy model. By default, it identifies scenarios where the request User-Agent does not match the request TLS fingerprint and marks them with Bot risk tags. When a client accesses the site through a local proxy (e.g., local SOCKS proxy), the request User-Agent and TLS fingerprint mismatch will occur. If the site service allows the client to access through this method, you should optimize the Bot intelligent analysis policy and allow requests with specific Bot intelligent analysis features to avoid false blocking.

Directions

1. Log in to the EdgeOne console, click **Site List** in the left sidebar, and then click the target **site** in the site list.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. Locate the **Bot Management** tab and click the switch under **Bot Intelligent Analysis** to enable this feature.

4. Locate the **Bot Management** tab and click **Add rule** under **Custom rules** to enter the configuration page.
5. Enter the rule name and configure the judgment conditions and actions. In this example scenario, you can configure the matching field as **Bot intelligent analysis feature** equal to **TLS Fingerprint Inconsistency** and select the action as **Allow**.

6. Click **Save and publish**. The rule will be deployed and take effect.

Related References

Action

Last updated：2023-09-21 09:57:52

The bot management module provides multiple action methods. The processing rules for different action methods are as follows:

Action	Purpose	**Action description**	**Subsequent action**
Block	Used to block request access to the site (including Cache or non-Cache content).	Responded with an intercept page and intercept status code.	No longer match other Rules.
Allow	Used to skip the remaining rules of the current Security module.	In the current module, the remaining rules no longer match the request.	Continue to match other Effective rules.
Observe	Used for evaluating or Canary security policy.	Only records log, does not take action.	Continue to match other rules.
JavaScript challenge	Used to identify Clients that do not support JavaScript Note 1, commonly found in DDoS attack sources, scanning tools, etc.	Responded with a redirect (HTTP 302) page, the page carries JavaScript code to verify the browser behavior of the Client, and only visitors who pass the verification can continue to access.	Requests that pass the challenge continue to match other rules.
Managed challenge	Used for bot confrontation, first perform JavaScript challenge verification, and then perform CAPTCHA human-machine verification for requests that pass the verification.	First, perform a JavaScript challenge; for Clients that pass the verification, respond with a redirect (HTTP 302) page, carry a CAPTCHA verification, and the user completes the verification through interactive operation. Only visitors who pass both verifications can continue to access.	Requests that pass the challenge continue to match other rules.
Drop w/o response	Belongs to a more intense bot confrontation mechanism, limiting bot	Maintain TCP connections, but no longer respond to any HTTP Data.	No longer match other management strategies.

	concurrent ability by consuming bot network connections.		
Add short latency	Mainly used to limit bot concurrent ability, with obfuscation feature [Note 2].	Randomly wait 1-5 seconds before responding.	No longer match other management strategies.
Add long latency	Mainly used to limit bot concurrent ability, with obfuscation feature [Note 2].	Randomly wait 8-10 seconds before responding.	No longer match other management strategies.

Note:

Note 1:
Browser Clients that support JavaScript can normally pass the JavaScript challenge verification, while Clients that do not support JavaScript (such as cURL) cannot pass the verification.

Note 2:
Generally speaking, when bot operators detect that their bots are being restricted by bot management policies, they may adjust the characteristics of their bots to bypass bot policies, thereby increasing the difficulty of bot identification. Therefore, long-term operational bot confrontation mechanisms usually have obfuscation features, that is, it is difficult for bot operators to intuitively judge whether their bots are restricted by bot management policies. Confrontation mechanisms with obfuscation features can reduce the cost and difficulty of bot operators without increasing the difficulty of bot identification.

Supports multiple action methods for random execution

Random execution of multiple action methods can help your bot management strategy achieve higher obfuscation intensity, making it more difficult for bot operators to detect. Custom bot rules support the use of multiple action methods to handle requests, and you can configure multiple action methods and their corresponding weights. When the rule matches the request, one of the action methods will be randomly selected for processing based on the weight configuration.

Note:

This capability is only available for configuration within custom bot rules.

Get Bot management tag via HTTP Headers of origin-pull requests

Last updated：2025-05-26 15:05:19

Function Overview

When the Bot management feature of EdgeOne is enabled, the platform will automatically append an HTTP request header `EO-Bot-Tag` to origin requests, containing the Bot label identification results of the requesting client, assisting the origin site in log analysis and security policy linkage.

Note:

After subscribing to Bot management, this feature will be enabled by default.

Application Scenarios

Enhanced Logging: Directly record Bot identification information into the origin site logs for subsequent analysis and tracing.

Risk Level Control: The origin site can dynamically adjust interception, rate limiting, and recording strategies based on tag content.

Attack Situation Recognition: Comprehensive Bot, fingerprint, and behavior labels assist the origin site in client profiling and threat assessment.

Request Header Description

Header Name

EO-Bot-Tag: If the original request already contains the `EO-Bot-Tag` header, EdgeOne will automatically overwrite it.

Transmission Format

Single JSON Object: The structure is uniformly a JSON object containing multiple key-value pair fields.

Tag Field Definition

Field Name	Type	Example	Description
bot type	string	"Unknown Bot", "Tool"	The type of crawler or tool recognized by the **UA feature rules** under the **Bot Management** module **Basic Feature Management**.
bot name	string	"GoogleBot", "cURL"	The name of the crawler or tool recognized by the **UA feature rules** under the **Bot Management** module **Basic Feature Management**.
botnetID	string (hash)	"f0cd7aee88e2b81bca1a063cd1154f02"	The hash of the detected Botnet fingerprint.
JA3 signature	string (hash)	"f436b9416f37d134cabc04886327d3e8" or ""	JA3 fingerprint (a hash fingerprint calculated based on TLS handshake behavior) (When the request is of HTTP protocol, the communication does not include the TLS protocol, and the JA3 fingerprint is an empty string).
applied action	string	"monitor" or "trans"	The action taken by EdgeOne's **Web Security** feature on the request. Requests that do not hit any security rules will be marked as trans.
category	object	{"client_reputation":[{"type":"bot","credibility":"medium"}]} or {"idc":{"name": "pccw.com"}}	The crawler risk classification information recognized by the **Client Reputation Analysis, IDC Rules, or Search Engine Rules** features in the **Bot Management** module: 1. The parameter name is the feature name where the crawler risk information was identified. 2. The parameter value contains multiple fields: - type field: crawler risk classification - credibility field: risk assessment credibility
behavior	string	`"evil_bot"` , `"suspect_bot"` , `"normal"`	The crawler behavior risk label identified by the Bot Intelligent Analysis function in the **Bot Management** module.

Applied action Field Values

Value	Description
monitor	Observation mode, records but does not intervene
delay	Responds after a short delay
slow	Responds after a significant delay
allow	Directly allowed

Behavior Field Values

Value	Description
evil_bot	Malicious Bot
suspect_bot	Suspicious Bot
normal	Normal Traffic

Examples

Example 1: Common Bot Tool Request

```
EO-Bot-Tag: {
  "bot type": "Tool",
  "bot name": "cURL",
  "botnetID": "d0b8e949bdd3475fec4cd41081577958",
  "JA3 signature": "f436b9416f37d134cadd04886327d3e8",
  "applied action": "monitor",
  "category": {
    "idc": {
      "name": "pccw.com"
    }
  },
  "behavior": "evil_bot"
}
```

Example 2: Suspicious Client Request

```
EO-Bot-Tag: {
  "bot type": "Unknown Bot",
  "botnetID": "f0cd7aee88e2b814ba1a063cd1154f02",
  "JA3 signature": "",
  "applied action": "monitor",
  "category": {
    "client_reputation": [
      {
        "type": "bot",
        "credibility": "medium"
      }
    ]
  },
  "behavior": "suspect_bot"
}
```

Notes

The `EO-Bot-Tag` header should only be added to requests where the Bot management feature is enabled.
The order of fields within the JSON object has no fixed requirements; the origin site should parse based on field names.
The `category` field may contain various sources (such as `idc` , `client_reputation` , etc.), and its internal structure may be nested arrays or objects.
The `JA3 signature` field will always exist, even if it has no value, its content will be an empty string.

Managed rules

Last updated：2025-04-25 16:30:47

Overview

Exposed site vulnerabilities may lead to origin intrusion, sensitive data loss, and may further seriously damage your relationship with users. Managed rules provide comprehensive and real-time vulnerability attack protection for your website, covering common vulnerabilities and attack types in OWASP TOP 10 Note 1, such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), etc. Through continuous updates, this rule set can effectively deal with emerging security threats, ensuring that your site operating environment and sensitive data are reliably protected.

Note:

Note 1:OWASP TOP 10 lists common and severe security risks in web applications. These risks represent a major part of current network security threats, so covering these scenarios is crucial for protecting the security of web applications. EdgeOne's vulnerability attack protection rule set covers all OWASP Top 10 risk scenarios and automatically updates the rule list for 0-day vulnerabilities.

Note 2: By default, managed rules only scan the first 10 KB of the request body. If you subscribe to the Enterprise package and need to scan more request body data, please contact us.

Note 3: Different plans support different managed rules. For details, see Comparison of EdgeOne Plans.

Optimize Managed Rule Policy

If you need to customize the configuration of protection rule policies according to your actual business situation and protection requirements, you can configure them in the following ways:

Note:

During access to new sites or creation of policy templates or security policies, the evaluation mode is enabled by default for managed rules. Requests matching the rules will be only logged for observation but not actually handled. You should complete policy evaluation and optimization as soon as possible, and then disable the Evaluation mode to implement the protection rules and block malicious requests.

Scenario 1: Configure the Global Protection Level Policy by Rule Group

EdgeOne divides managed rules into different rule groups according to the vulnerability types they protect. Configuration can be done by rule group to set handling methods for all rules within the group based on protection level. For example: If the domain name `www.example.com` frequently exposes vulnerabilities in open-source components, the protection level of the open-source component vulnerability rule group can be set to strict and the handling method to interception. Then the effective configuration will be to intercept all rules with high-risk and lower risk levels.

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Security**. By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. In the Managed Rules - Rule set Card, search for "Open-Source component vulnerability", separately configure protection level and action, adjust the protection level to **strict**, set the handling method to **Block**, and click **save** to complete the rule configuration.

Scenario 2: Customize Optimization Protection Strategy by Single Rule

EdgeOne supports differentiated configuration of protection policies for individual rules. For example, for the domain name `www.example.com` , there is a file upload scenario. Currently, the file upload attack protection rule group is configured with a strict protection level to intercept. However, in business scenarios, there are legitimate file upload requests whose filenames contain the `<>` symbol. The expected outcome is to allow them normally. At this point, it is necessary to separately configure this rule to monitor (only record logs).

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Security**. By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `www.example.com` , to enter the configuration page for the security policy of the target domain name.
3. In the Managed Rules - Rule set Card, click **View by rule**.
4. Search for search keywords `<>` to find the corresponding specific rule, and modify the action of the rule to **monitor**.

Updating a Version of Managed Rules

EdgeOne, based on independent development and third-party threat intelligence, formulates new vulnerability protection rules for the request characteristics of 0-day vulnerabilities and adds them to the set of managed rules. Users can deploy new protection rules to cover new vulnerability threats by updating the version of managed rules. Properly configuring automatic updates and new rule deployment options can reduce the risk of external 0-day vulnerability attacks on your site, which is crucial for continuously protecting your site.

Note:

Not all 0-day vulnerabilities can be protected through traffic. EdgeOne provides web vulnerability protection that can identify traffic based on the HTTP/HTTPS protocol.

EdgeOne periodically updates the rule set based on Tencent's threat intelligence and vulnerability POC information. If you have independent threat intelligence sources and want to protect vulnerabilities not covered by managed rules, use Custom Rules to configure you security policy according to the intelligence and POC information. If you have more custom rule requirements, please contact us for technical support.

Updating a Rule Set and Deploying New Rules

When new rules are added to the rule set, the list of managed rules will be updated accordingly. New rules cannot be directly used in the existing version of managed rules. To use new rules, you need to update the version of managed rules to the latest one. According to the protection level (Notify Only, Do Not Automatically Update) or protection mode (Automatically Update) configuration of corresponding classifications of new rules, new rules will be deployed to your site.

Note:

Regarding updates to published rules: For published rules, EdgeOne will also optimize them based on rule recognition and POC intelligence updates to ensure that rule recognition accuracy and false alarm situations meet protection expectations. When existing rules are updated, the version of managed rules will not be updated; the action of the rules will remain unchanged after the update.

When a new version update is released, your managed rules will be updated as follows:

1. Check the automatic update configuration: If you enabled automatic update, the managed rules will automatically apply the latest rule list; if you chose manual update, the managed rules will retain the current rule list, and you can arrange the timing to update the version of managed rules by yourself.
2. Check the protection mode and action configuration for each rule classification: If you select the "Auto-Protect" option for a classification, when the new version includes updates for the classification, the action of corresponding rules will be configured based on your protection mode level. After the update, the action of each rule in the classification will be consistent with the protection level and action configuration of the rule classification.

Example of Rule Update Process: Automatic Deployment of New Rules When "Automatic Update" Is Enabled and "Automatic Protection" Mode Is Used

In the new version of managed rules, a new rule for the **SQL Injection Attack** classification with a **Loose** rule level is added. When this version is released, EdgeOne detects that the web protection policy of the current site has **Automatic Update** enabled. Therefore, it further checks the rule configuration of the **SQL Injection Attack** classification. Since the protection mode for the **SQL Injection Attack** classification of this policy is **Automatic Protection - Strict**, rules with a rule level of **Loose**, **Normal**, or **Strict** need to be configured as **Interception** according to the action of the rule classification. Since the rule level of the new rule is **Loose**, which falls under the above rule range, it is configured as **Interception**.

(The rule ID, classification, name and other items used in this example are for illustrative purposes only. The actual rule ID and rule name should prevail.)

Scenario 1: Automatic Operation of Vulnerability Protection Policy

The site has strict protection requirements for 0-day vulnerabilities from SQL injection attacks and requires automated protection against known vulnerabilities. Due to business sensitivity, requests suspected of attacks are also intercepted first. You may refer to this example to **automatically operate** your security policy:

Automatically update the rule list when a new version is available.

Automatically deploy new rules. The new rules will be classified based on EdgeOne's rule level and be deployed and take effect according to your configured protection level and action.

The scheme in the example has the following features:

For high-risk 0-day vulnerabilities, when an appropriate protection level is configured, the configuration scheme can intercept requests exploiting the vulnerabilities as soon as the managed rules are updated.

After an appropriate protection level is configured, the managed rules will automatically operate the policy, resulting in low continuous operation costs.

Only enabled rules are monitored, and other rules do not generate logs or alarms to reduce operational interference.

Note:

When using the scheme in the example, consider the following configuration recommendations and risks:

It is recommended to carefully evaluate the **protection level** of each rule classification. When a vulnerability corresponding to a disabled protection rule is exploited, it cannot be detected through logs or alerts, potentially leading to data risks.

It is recommended to select an appropriate operational policy for different rule classifications based on the interactive mode of actual business and the middleware used and use the **automatic protection** and **manual protection** options in combination.

If you find that the rules have intercepted your normal business, configure Protection Exception Rules for temporary handling as needed, and timely evaluate and fix potential business component vulnerabilities.

It is recommended to configure Web Security Monitoring and Alerting synchronously to monitor the request data that hits the managed rules. When a large number of requests hit the managed rules, timely evaluate the request logs and adjust the protection level.

Configuration Procedure

1. Log in to the EdgeOne console, click **Site List** in the left sidebar, and click the **site** to be configured on the site list.
2. Click **Security Protection** > **Web Protection** . The default is site-level security policy. If you need to configure a differentiated protection policy for a specific domain name under the current site, go to the **Domain-level security policy** tab, click the **corresponding domain name** to go to the domain-level security policy configuration page, and follow the same subsequent steps.
3. In the **Managed Rule > Automatic Update** card, click **Option Switch** . In the pop-up window, select **Automatic Update to the Latest Version** . After confirming the policy behavior, click **Save** .

4. In the **Managed Rule > Rule Set** card, search for **SQL Injection Attack Protection** and change the protection mode to **Automatic Protection - Strict,** click **Save**. Then automatic update rules can take effect for SQL injection attack protection type rules.

Scenario 2: Assisted Operation of Vulnerability Protection Policy

The site has strict protection requirements for 0-day vulnerabilities from SQL injection attacks. However, to avoid false interceptions, new vulnerability rules will not be enabled directly as interception. When a new rule is launched, it is required to adopt the Monitor mode by default. Only after confirmation by the security operation team will the new rule be adjusted as interception. The scheme in this example is suitable for business scenarios where there are high vulnerability protection requirements and it is able to operate security policies and timely evaluate vulnerability risks.

You can refer to this example to **assist in operating** your security policies:

Automatically update the rule list when a new version is available.

Do not automatically enable new rules as interception mode. The default action for new rules is **Monitor** , and only logs are recorded. You can manage the enabling scope and timing of rules and adjust them to interception manually.

The scheme in the example has the following features:

For ultra-high-risk 0-day vulnerabilities, the managed rules will not automatically intercept them, but need to be manually enabled to provide protection.

You need to perform daily operation and maintenance of the managed rule configuration. You need to be able to judge whether specific security vulnerabilities are applicable to the site's backend architecture.

You can freely choose the scope of rules to monitor and record request logs. Through the Monitor mode, you can keep an eye on vulnerabilities that do not need interception.

Note:

It is recommended to select an appropriate operational policy for different rule classifications based on the interactive mode of actual business and the middleware used and use the **automatic protection** and **manual protection** options in combination.

If you find that the rules have intercepted your normal business, configure Protection Exception Rules for temporary handling as needed, and timely evaluate and fix potential business component vulnerabilities.

It is recommended to configure Web Security Monitoring and Alerting synchronously to monitor the request data that hits the managed rules. When a large number of requests hit the managed rules, timely evaluate the managed rule policy and optimize the configuration.

Configuration Procedure

1. Log in to the EdgeOne console, click **Site List** in the left sidebar, and click the **site** to be configured on the site list.

2. Click **Security Protection** > **Web Protection** . The default is site-level security policy. If you need to configure a differentiated protection policy for a specific domain name under the current site, go to the **Domain-level security**

policy tab, click the **corresponding domain name** to go to the domain-level security policy configuration page, and follow the same subsequent steps.
3. In the **Managed Rule > Automatic Update** card, click **Option Switch** . In the pop-up window, select **Automatic Update to the Latest Version** . After confirming the policy behavior, click **Save** .

4. In the **Managed Rules > Rule Set** card, search for **SQL Injection Attack Protection** and modify the protection mode to **manual protection**.

Scenario 3: Manual Operation of Vulnerability Protection Policy

The site does not use managed rules at all and only needs to temporarily enable protection in a few scenarios. The scheme in this example will not automatically update the rule list. When new rules are released, you will be notified through the message center, and you can upgrade to the latest version as needed.
The scheme in the example has the following features:
For high-risk 0-day vulnerabilities, the managed rules will not automatically intercept them.
You need to perform daily operation and maintenance of the managed rule configuration. You need to be able to judge whether specific security vulnerabilities are applicable to the site's backend architecture.
You can freely choose the scope of rules to monitor and record request logs.

Note:

During the manual update process, more policies will be enabled simultaneously. To reduce the risk of false interception, configure the rules as needed to the Monitor mode or enable the Managed Rule - Evaluate mode.
If you find that the rules have intercepted your normal business, configure Protection Exception Rules for temporary handling as needed, and timely evaluate and fix potential business component vulnerabilities.
It is recommended to configure Web Security Monitoring and Alerting synchronously to monitor the request data that hits the managed rules. When a large number of requests hit the managed rules, timely evaluate the managed rule policy and optimize the configuration.

Configuration Procedure

1. Log in to the EdgeOne console, click **Site List** in the left sidebar, and click the **site** to be configured on the site list.
2. Click **Security Protection** > **Web Protection** . The default is site-level security policy. If you need to configure a differentiated protection policy for a specific domain name under the current site, go to the **Domain-level security policy** tab, click the **corresponding domain name** to go to the domain-level security policy configuration page, and follow the same subsequent steps.
3. In the **Managed Rule > Automatic Update** card, click **Option Switch** . In the pop-up window, select **Notify Only, Do Not Automatically Update** . After confirming the policy behavior, click **Save** .

4. If the rule list needs to be updated after a rule update occurs, you can go to the **Managed Rule > Automatic Update** card to click **Update Now** . After confirmation in the pop-up window, the managed rule list for the current policy will be updated immediately.

Use Deep Analysis to Automatically Identify Unknown Vulnerabilities

Deep analysis uses advanced semantic analysis technology to deeply understand the intent of SQL and XSS statements. It can not only effectively deal with known attack methods but also has the ability to protect against unknown attacks. This method goes beyond the traditional pattern-matching detection method and improves the recognition accuracy of complex and new attacks. With deep analysis, you will get a higher level of security protection, reduce the risk of false positives and false negatives, and ensure that your website is free from malicious attacks and data leakage threats.

Note:

Deep analysis function is only supported by the Standard plan and the Enterprise plan.

Enable Deep Analysis

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Security**. By default, it is a site-level security policy. To configure differentiated security policies for a specific domain name under the current site, you can enter the **Domain-level security policy** tab and click the **corresponding domain name** to enter the configuration page for the domain-level security policy. The subsequent steps are the same.
3. In the **Managed Rules - Deep Analysis** tab, click **Edit**.
4. Select the protection mode as Enable, click **Save** to enable Deep Analysis.

Observe (default): Only log the identified malicious requests without intercepting them.

Enable: Intercept identified malicious requests.

Off: Turn off deep analysis.

Related Reference

Evaluation Mode（Global Observation Mode）

Note:

The Evaluation mode is enabled by default. To handle requests by the block action, you should disable the Evaluation mode.

When the evaluation mode is enabled, under all managed rule policies configured as block, requests are only logged but not actually handled. This mode can help you comprehensively assess the current vulnerability policy configuration and prevent false blocking of normal business requests that contain vulnerability characteristics.

For new business access, it is recommended to maintain the evaluation mode and observe complete client access scenarios for 48 hours (adjust the duration based on your actual assessment). When normal business requests are found to match a specific rule continuously, the rule is adjusted to Observe.

Protection Level Description

Configuration Suggestions

Managed rules provide multiple protection levels for different attack and vulnerability types, including Loose, Normal, Strict, and Ultra-Strict. When selecting a protection level, the corresponding level and all levels below it will be enabled. For example, selecting the Strict protection level will enable the rules of Loose, Normal, and Strict levels, achieving layered protection. It is recommended to enable the corresponding protection level according to the business scenario:

Loose: Meet the most basic protection needs and try to avoid false positives. It is recommended that all external HTTP services enable at least all rules of this level.

Normal (recommended): Comprehensive protection, suitable for most scenarios. It is recommended to enable this level for services involving customer data. This level of rules may generate false positives in specific scenarios, which can be debugged and optimized through observation mode.

Strict: Full protection, suitable for stricter protection scenarios, ensuring no attacks bypass. It is recommended to use this level for services involving financial data (such as online banking). Under this protection level, rules may generate some false positives, and it is recommended to debug and optimize them in combination with observation mode and custom rules.

Ultra-Strict: Suitable for access scenarios under strict control environments. This level of rules may cause more false positives, so please enable them according to specific protection needs and deploy them in combination with exception rules, observation, and custom rules.

If you need more fine-grained control, you can also use custom protection levels to customize the actions of different rules according to specific business needs.

Rule Group Protection Level and Rule Risk Level Mapping

Rule Group Protection Level	Valid Configuration Corresponding Rule Risk Level
Very strict	Ultra-high risk, high risk, medium risk, low risk
Strict	High risk, medium risk, low risk
Normal	Medium risk, low risk
loose	Low risk
Custom	Do not configure the configuration disposal method according to the group dimension of rules. The configuration shall be subject to the sub-rule.

Exception Rules

Last updated：2024-08-26 09:31:35

Overview

Exception rules provide a centralized allowlist configuration option, allowing for quick configuration of valid requests to be released, avoiding interception by other modules. In addition, when EdgeOne's built-in preset protection strategies (such as CC attack defense, managed rules, etc.) do not accurately identify valid requests, exception rules can provide you with fine-tuning configuration, accurately specifying the requests or request parameters that need to be released.

Note:

In the Exception rules for protection, partial request skip the scan function, which is only supported by the EdgeOne Enterprise plan. If you need to use it, contact us.

Typical Scenarios and Usage

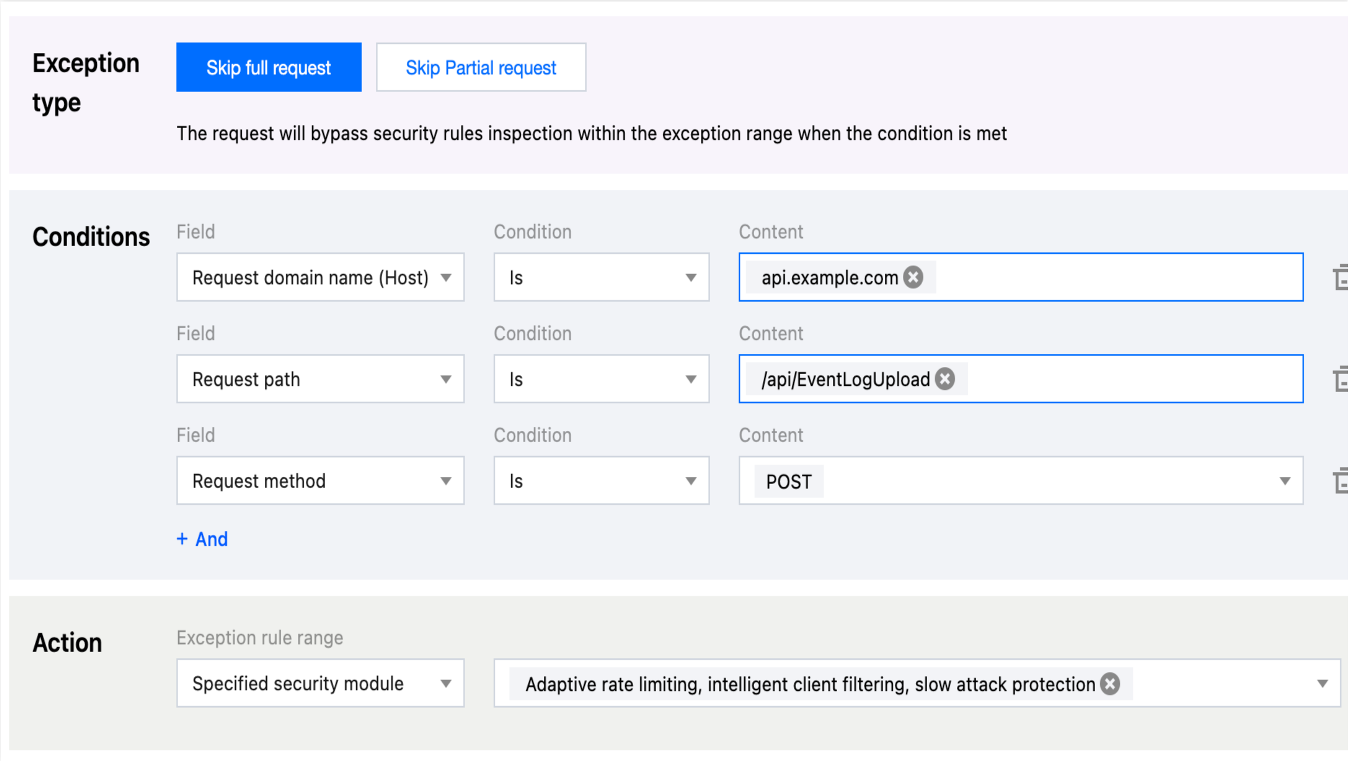
Based on the existing protection policies, the exception rules can specify normal requests matching certain characteristics to skip scanning of specified modules or rules. The supported protection modules include **custom rules, rate limiting, CC attack protection, Bot management, and managed rules** .

Example Scenario 1: Specify Trusted Client IPs (IP allowlists) to Skip Web Protection Feature Scanning

The current site domain name `api.example.com` trusts a specific IP range to access test devices and internal services. The trusted IP range is `123.123.123.0/24` . For access requests from the trusted IP range, no scanning related to the Web protection feature is performed to avoid false blocking. The steps are as follows:

1. Log in to the EdgeOne console, click **Site List** in the left sidebar, and then click the **Site** in the site list.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `api.example.com` , to enter the configuration page for the security policy of the target domain name.
3. In the **Exception rules** tab, click **Add rule** .
4. Enter the rule name and select the exception type as **Skip full request**.
5. Configure the judgment conditions and actions. In this example scenario, you can configure the matching fields as **Request domain name (Host)** equal to `api.example.com` and **Client IP** equal to `123.123.123.0/24` . Select the action as all options in the specified security module, including `Managed rules` , `rate limiting`

, `custom rules` , `adaptive frequency control, intelligent client filtering, slow attack protection` , and `Bot management` .



Exception type: Skip full request | Skip Partial request

The request will bypass security rules inspection within the exception range when the condition is met

Conditions

Field	Condition	Content
Request domain name (Host)	Is	api.example.com
Request path	Is	/api/EventLogUpload
Request method	Is	POST

+ And

Action

Exception rule range: Specified security module — Adaptive rate limiting, intelligent client filtering, slow attack protection

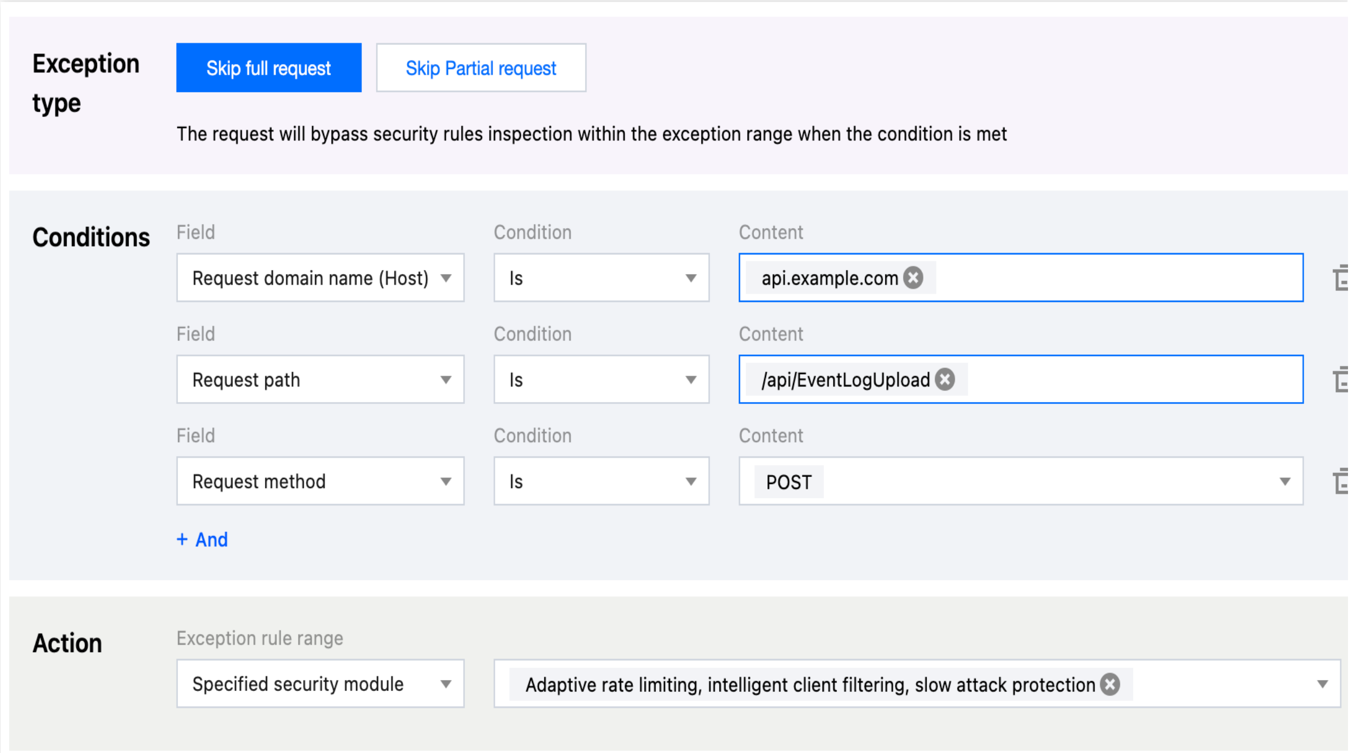
6. Click **Save and publish** . The rule will be issued and take effect immediately. At this time, requests from the specified trusted IP range `123.123.123.0/24` are not blocked by the security features of the Web protection module. This method avoids false blocking of the testing and internal service requests.

Example Scenario 2: Specify High-Frequency API Interface Requests to Skip CC Attack Defense Scanning

The current site domain name is `api.example.com` , and the API interface for event reporting is `/api/EventLogUpload` . In the event of a business surge, there may be a burst of high-frequency access scenarios. Such access patterns are highly likely to be identified as attacks by CC attack defense and intercepted. For this interface, you can configure exception rules to skip the CC attack defense module to avoid false interception. The operation steps are as follows:

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `api.example.com` , to enter the configuration page for the security policy of the target domain name.
3. In the **Exception rules** tab, click **Add rule** .
4. Enter the rule name and select the exception type as **Skip full request** .

5. Configure the judgment conditions and actions. In this example scenario, you can configure the matching fields as **Request domain name (Host)** equal to `api.example.com` , **Request method** (Method) equal to `POST` , and **Request path** (Path) equal to `/api/EventLogUpload` . Select the exception rule range as `Adaptive frequency control, intelligent client filtering, and slow attack protection` in the specified security module. You can configure multiple matching fields, and there is an AND relationship between the matching fields. For details of the matching conditions, see Match Conditions.


Exception type

The request will bypass security rules inspection within the exception range when the condition is met

Conditions

Field	Condition	Content
Request domain name (Host)	Is	api.example.com
Request path	Is	/api/EventLogUpload
Request method	Is	POST

Action

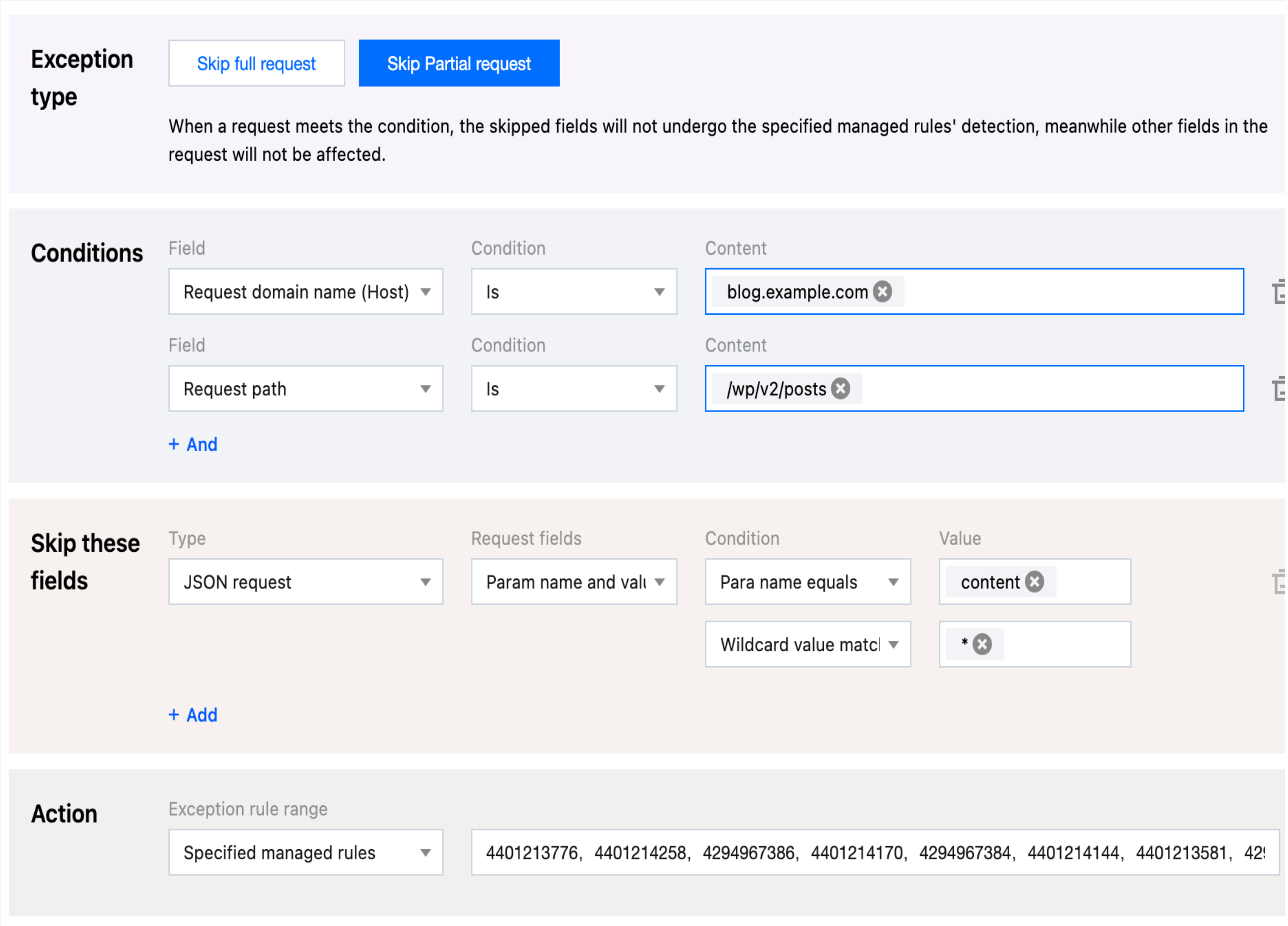
Exception rule range: Specified security module — Adaptive rate limiting, intelligent client filtering, slow attack protection

6. Click **Save and publish** . The rule will be issued and take effect immediately. At this time, the `POST` requests from the API for reporting the event logs are not blocked by feature modules such as adaptive frequency control. This method avoids false blocking due to high-frequency log reporting, and meanwhile enables normal detection and protection for other APIs.

Example Scenario 3: Avoid False Interception of Personal Blog Content by Vulnerability Protection

The current site domain name is `blog.example.com` , which is used for blog content sharing. The blog is based on WordPress. The blog content may share technical content related text (such as: SQL and Shell command examples), and when publishing the blog, the blog content text may trigger the attack defense rule due to matching SQL injection attack features. Through exception rules, you can configure request parameter allowlist, match the blog publishing API interface path `/wp/v2/posts` , and specify that the text parameter `Content` in the publishing content request does not participate in SQL injection attack rule scanning, avoiding false alarms and interception of blog content. The operation steps are as follows:

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. Click the **Domain-level security policy** tab and then click the **target domain name** such as `blog.example.com` , to enter configuration page for the security policy of the target domain name .
3. In the **Exception rules** tab, click **Add rule** .
4. Enter the rule name and select the exception type as **Skip Partial request** .
5. Configure the judgement conditions, skipped fields, and actions. In this example scenario, you can configure the matching fields as **Request domain name (Host)** equal to `blog.example.com` and **Request path** equal to `/wp/v2/posts` . Select the exception rule range as **Specified managed rules**, including all SQL injection attack protection rules. Configure no scanning for the parameter content with the parameter name equal to `content` and the parameter value matching the wildcard `*` in JSON requests. For details of the matching conditions, see Match Conditions.



Exception type: Skip full request | **Skip Partial request**

When a request meets the condition, the skipped fields will not undergo the specified managed rules' detection, meanwhile other fields in the request will not be affected.

Conditions

Field	Condition	Content
Request domain name (Host)	Is	blog.example.com
Request path	Is	/wp/v2/posts

+ And

Skip these fields

Type	Request fields	Condition	Value
JSON request	Param name and valı	Para name equals	content
		Wildcard value matcl	*

+ Add

Action

Exception rule range: Specified managed rules | 4401213776, 4401214258, 4294967386, 4401214170, 4294967384, 4401214144, 4401213581, 42!

6. Click **Save and publish** . The rule will be issued and take effect immediately. At this time, when a blog post is published through the `/wp/v2/posts` ++++ request path, the blog content is not verified by the SQL injection

attack protection rules. This method prevents normal text content from being wrongly identified as an attack through scanning.

Related References

The exception field types supported when skipping rule scanning for partial request fields are as follows:

Category	Option
JSON Request Content	All parameters Match specified parameter name Match condition parameter
Cookie Header	All parameters Match specified parameter name Match condition parameter
HTTP Header Parameters	All parameters Match specified parameter name Match condition parameter
URL Encoded Content or Query Parameters	All parameters Match specified parameter name Match condition parameter
Request Path URI	Query parameter part Partial path Complete path
Request Body Content	Complete request body Segmented file name

Note:

Match condition parameters are completed by specifying both parameter name and parameter value match conditions, and both parameter name and value support full match and wildcard match.

Managed Custom Rules

Last updated：2024-08-26 09:31:35

When you use the security expert services provided by EdgeOne (including Activity Guarantee, Emergency Attack and Defense, Security Managed and Customized Rules services), Tencent Security Experts will customize security policies for your business based on the business scenario and attack methods. Managed custom rules are displayed in the rule list of the corresponding feature module. They can only be displayed and do not support adjustment of the matching conditions or actions. If your business changes or you have special security protection requirements, contact us.

Note:

Custom rules and rate limiting support Managed Custom Rules.

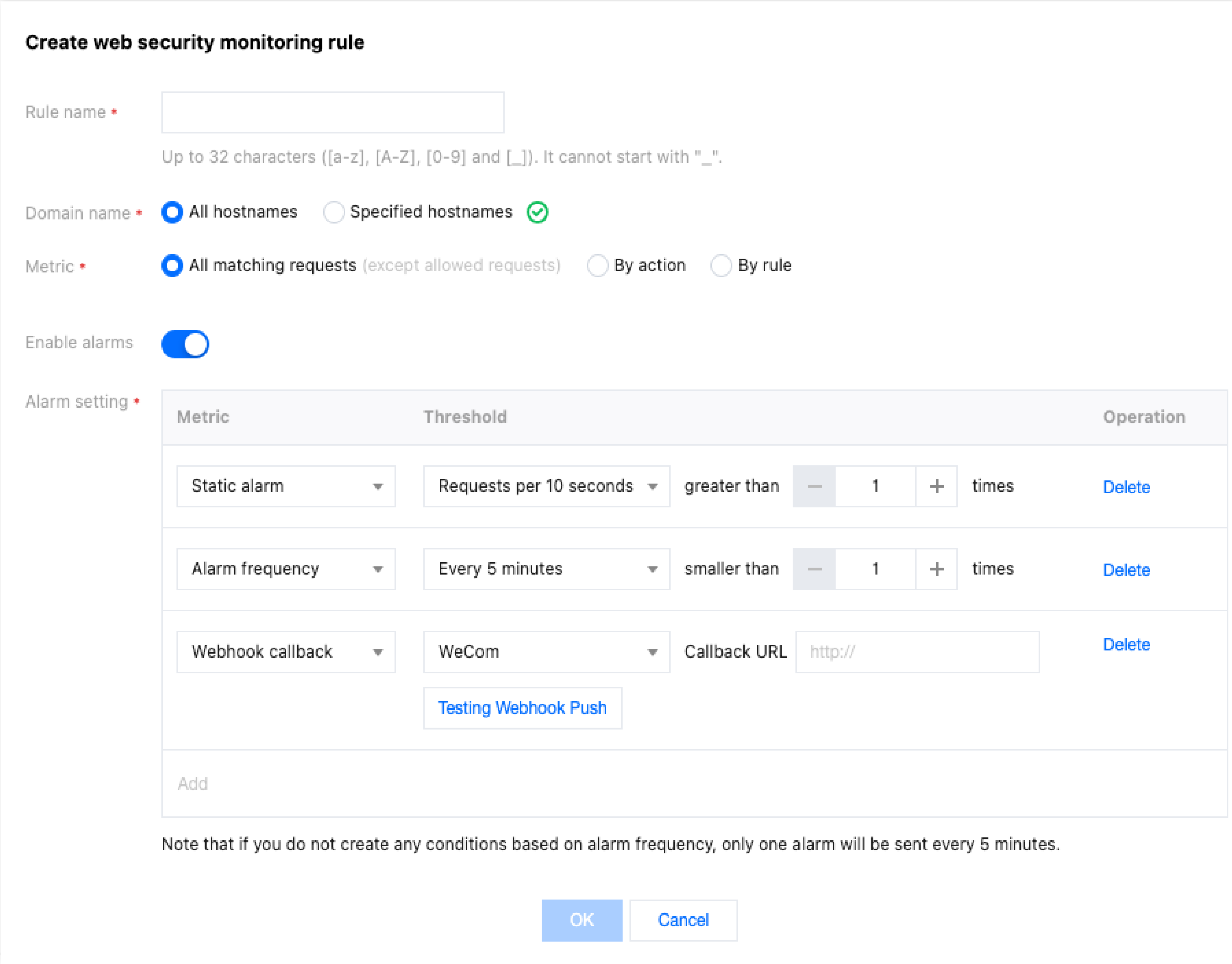
Web security monitoring alarm

Last updated：2024-04-16 16:49:45

Overview

Web security monitoring rules can provide you with real-time, customized security event notifications, and support Webhook shipping, seamlessly integrating alarms with common enterprise communication tools, improving security operation efficiency, and helping you quickly discover and respond to potential risks. You can flexibly configure the monitoring range, threshold, and alarm frequency based on your business needs and risk assessment.

Configuration Item Description



Create web security monitoring rule

Rule name *

Up to 32 characters ([a-z], [A-Z], [0-9] and [_]). It cannot start with "_".

Domain name * ● All hostnames ○ Specified hostnames ✓

Metric * ● All matching requests (except allowed requests) ○ By action ○ By rule

Enable alarms: on

Alarm setting *

Metric	Threshold				Operation
Static alarm	Requests per 10 seconds	greater than	1	times	Delete
Alarm frequency	Every 5 minutes	smaller than	1	times	Delete
Webhook callback	WeCom Testing Webhook Push	Callback URL	http://		Delete

Add

Note that if you do not create any conditions based on alarm frequency, only one alarm will be sent every 5 minutes.

OK Cancel

Configuration Item	Description

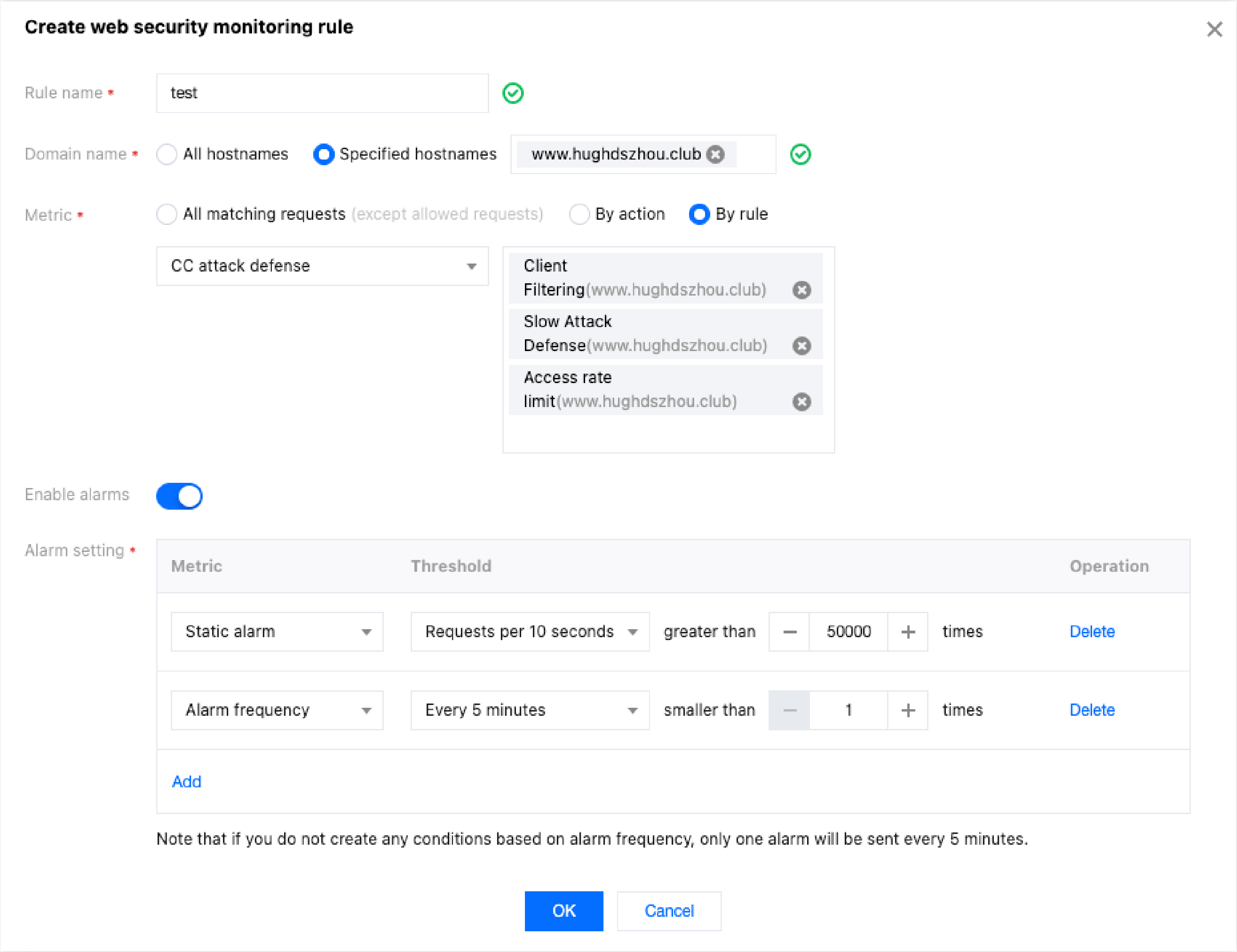
Rule name (Required)		Must meet the following requirements: A combination of letters, digits, and underscores; Less than 32 characters; Cannot start with an underscore.
Domain name (Required)		**All domains:** Includes all domains under this site, including domains added later. **Specified domains:** Only monitors specific domains under this site. **Note:** Threshold statistics are only effective for individual domains and will not merge the number of requests within multiple domains.
Metric (Required)		Supports selecting the statistical request range by action or by rule. **All action requests:** All requests that hit the security module rules and are processed (excluding allowed), are counted in the monitoring rule statistics. **Only count requests with specified action:** Requests that hit Web protection or Bot management rules and are ultimately processed in the selected way, are counted in the monitoring rule statistics. **Only count requests that hit specified rule:** Requests that hit specified Web protection or Bot management rules. **Note:** Allowing will not record logs, so it will not be included in monitoring statistics.
Alarm switch		Controls whether this Web security monitoring rule is effective. When the alarm switch is enabled, alarms will be sent through the message push channels provided by the Message Center (Message Center/Email/SMS/WeChat/Voice/WeCom Service Account). The specific message push channels can be configured in the Message Center Console. When the alarm switch is disabled, this Web security monitoring rule will no longer send alarms, including Message Center-related channels and Webhook push. **Note:** EdgeOne Web security monitoring alarm messages correspond to the "Security Event Notification" type messages in the Message Center.
Alarm setting	Static alarm (Required)	Supports configuring the threshold quantity of requests reached within a specified time window. When the specified threshold is reached, an alarm is triggered.
	Alarm frequency (Optional)	Configure the frequency of pushing alarms. When not custom configured, the default is up to 1 alarm notification every 5 minutes for each rule.
	Webhook push (Optional)	In addition to the message push channels provided by the Message Center, an additional Webhook interface callback method is provided.

		Currently supported channels include WeCom, Lark, DingTalk, and custom interface callback. After filling in the Webhook address for the corresponding channel, you can click Test Webhook Push, and EdgeOne will push a test message to the address you filled in to verify connectivity. The message content template is defined using Go text/template syntax and supports referencing Web security monitoring-related variables using {{.Notification Variables}}. For details, see Webhook Message Content Template.

Scenario 1: Monitor site for CC attack events and alert within 5 minutes

A financial business site needs to quickly respond within 5 minutes to meet regulatory compliance requirements when the business domain `www.example.com` is under CC attack. Therefore, the site's CC attack events are monitored. When the site is attacked by more than 5000 QPS CC attacks, an alarm is pushed to the security operations team for processing within 5 minutes.

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target **site** to enter the site details page.
2. On the site details page, click **Security and Acceleration** > **Alarm Notification** Push to enter the alarm notification push details page.
3. In the Web security monitoring rules card, click **Set** to enter the rule management page.
4. Click **Add rule** and configure the corresponding alarm rule. In this scenario, after entering the rule name, select the monitoring domain as `www.example.com` , the monitoring metric as high-frequency access request limit, intelligent client filtering, and slow attack protection events in CC attack defense. When the number of CC attacks exceeds 50,000 within 10 seconds, an alarm is triggered immediately and sent through the notification channels configured in the Message Center Console.



Create web security monitoring rule

Rule name * test

Domain name * ○ All hostnames ● Specified hostnames www.hughdszhou.club

Metric * ○ All matching requests (except allowed requests) ○ By action ● By rule

CC attack defense

- Client Filtering(www.hughdszhou.club)
- Slow Attack Defense(www.hughdszhou.club)
- Access rate limit(www.hughdszhou.club)

Enable alarms

Alarm setting *

Metric	Threshold				Operation
Static alarm	Requests per 10 seconds	greater than	50000	times	Delete
Alarm frequency	Every 5 minutes	smaller than	1	times	Delete
Add					

Note that if you do not create any conditions based on alarm frequency, only one alarm will be sent every 5 minutes.

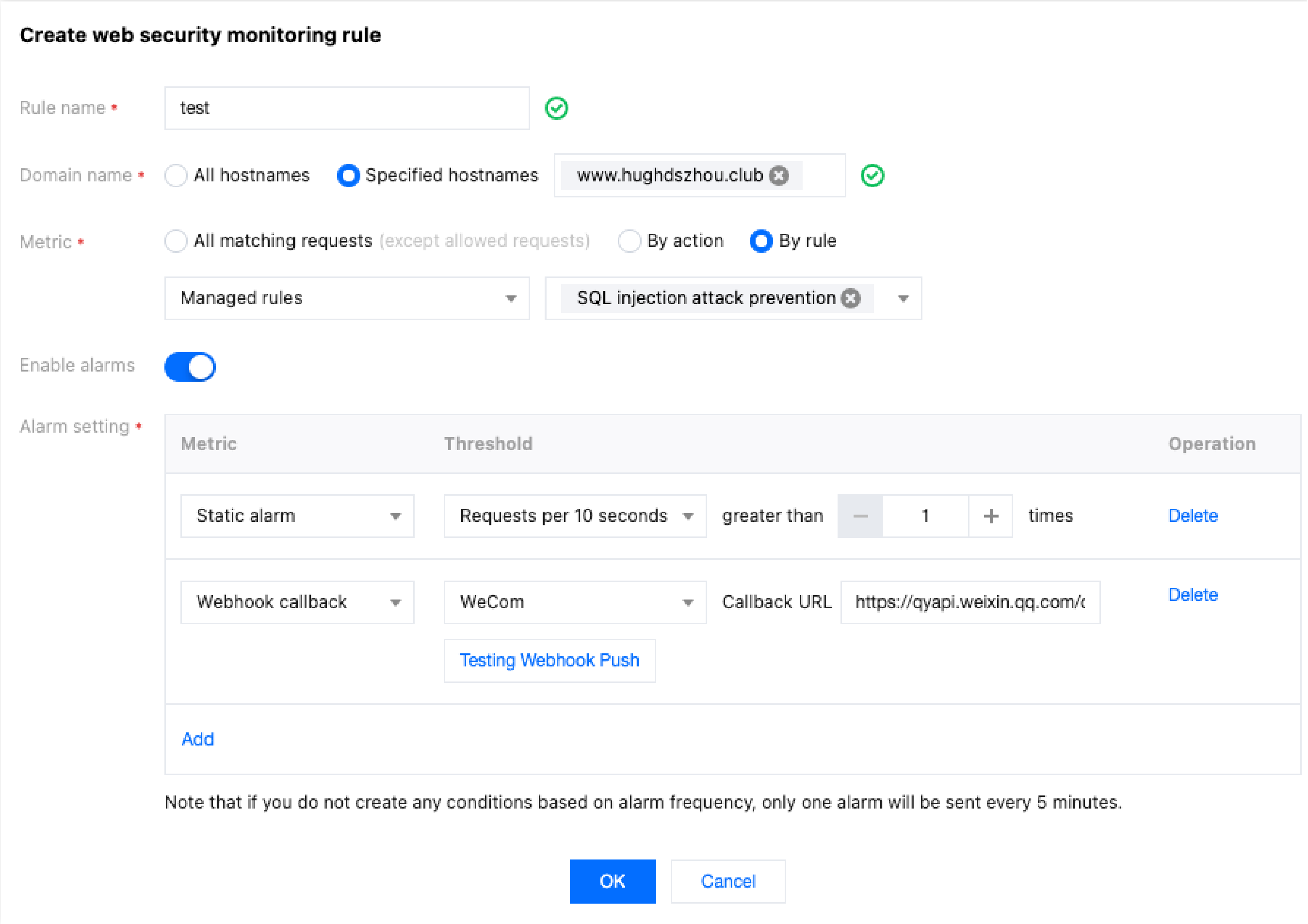
5. Click **OK** to complete the configuration.

Scenario 2: Monitor requests suspected of vulnerability attacks that hit managed rules and push Webhook alarms

The domain name of a company's official website that has been connected is `www.example.com` . The site contains sensitive customer information and needs to be constantly monitored for SQL injection-type vulnerability attacks. When any request hits the Web-managed rules for SQL injection attack defense, an alarm needs to be triggered immediately and pushed to the Enterprise WeChat robot via Webhook for further analysis.

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target site.
2. On the site details page, click **Security Protection** > **Alarm Notification Push** to enter the alarm notification push details page.
3. In the Web security monitoring rules card, click **Set** to enter the rule management page.
4. Click **Add rule** and configure the corresponding alarm rule. In this scenario, after entering the rule name, select the monitoring domain as `www.example.com` , the monitoring metric as requests hitting managed rules for SQL injection attack defense, and when the number of requests exceeds 1 within 10 seconds, an alarm is triggered

immediately and sent through the notification channels configured in the Message Center Console, as well as pushed to the specified URL via Webhook.



Create web security monitoring rule

Rule name * test

Domain name * ○ All hostnames ● Specified hostnames www.hughdszhou.club

Metric * ○ All matching requests (except allowed requests) ○ By action ● By rule

Managed rules | SQL injection attack prevention

Enable alarms: on

Alarm setting *

Metric	Threshold		Operation
Static alarm	Requests per 10 seconds	greater than 1 times	Delete
Webhook callback	WeCom Testing Webhook Push	Callback URL https://qyapi.weixin.qq.com/c	Delete

Add

Note that if you do not create any conditions based on alarm frequency, only one alarm will be sent every 5 minutes.

5. Click **OK** to complete the configuration.

Related References

Webhook Message Content Template

The message content template is defined using Go text/template syntax and supports referencing Web security monitoring-related variables using `{{.Notification variables}}`. The default message content template is as follows:

```
Notification Type: Site Security Monitoring Notification

Account ID: {{.UIN}}
Nickname: {{.AccountName}}
Site Name: {{.Zone}}
Monitoring Object: {{.Object}}
Monitoring Rule Name: {{.AlertRule}}
Alarm Time: {{.StartTime}} (GMT +8:00)
Alarm Condition: {{.Condition.TimeSpan}} seconds with more than {{.Condition.Thresh
Monitoring Item Metrics: {{.Condition.TimeSpan}} seconds with {{.MetricValue}} requ
```

Notification Variable Name	Data Type	Variable Meaning
UIN	String	Tencent Cloud Account ID
AccountName	String	Tencent Cloud Account Nickname
Zone	String	EdgeOne Site Name
AlertRule	String	Alarm Policy Name
Object	Array of String	Alarm Object (User-configured monitoring domain)
Condition	JSON object	Alarm Trigger Condition (User-configured static alarm condition)
StartTime	String	Alarm Trigger Time. The default timezone is UTC+8, example value: 2024-01-08 18:00:40
MetricValue	Integer	Alarm Trigger Metric Value

Note:

Currently, the console does not support self-service modification of message content templates. If you have related needs, please contact us.

Condition Object Structure

Alarm trigger condition, i.e., user-configured static alarm condition.

key Name	value Meaning
TimeSpan	User-configured alarm time window
Threshold	User-configured static threshold for the number of requests

Related References

Web Protection Request Processing Order

Last updated：2023-07-28 14:35:46

When Web Protection receives a request, it will first go through each security module in the following order, and only requests that have passed the security module scans will continue to be processed by other function modules.

Module processing order	Processing method of requests
Exception rules	When a request matches multiple rules, all matched rules apply.
Custom rule	When a request matches multiple rules, they are executed in order from high to low priority (priority value from small to large).Note 1
Rate limiting	All rules hit by the request are counted, and rules that meet the rate condition apply independently.Note 2 Rules that meet the rate condition are executed in order from high to low priority (priority value from small to large) .Note 2
CC attack defense	When a request hits multiple rules, all matched rules apply.
Bot management	For details, please see Bot Management.

Note:

Note 1:

When a request matches multiple custom rules, if a higher priority rule handles the request (except for observation), the request will not continue to match lower priority rules. When the priorities are the same, the actions are executed in the following order: observe > release > Managed challenge > JavaScript challenge > redirect > Return specified page > blocking IP > intercept.

Note 2:

Hitting an effective rate limiting rule does not affect the statistics of other rate limiting rules. When the same request hits multiple rate limiting rules, the matching and handling are performed according to the priority order of the effective rate limiting rules. When multiple rate limiting rules with the same priority are effective and matched by the request at the same time, the actions are executed in the following order: observe > release > Managed challenge > JavaScript challenge > redirect > Return specified page > blocking IP > intercept.

Action

Last updated：2025-03-04 15:32:42

The Web protection module provides multiple action options. Different feature modules support different actions, please refer to the specific feature module document.

Action	Use Case	Action Description	Subsequent Action
Block	Used to block requests to access a site (including cached or non-cached content).	Respond with block page and block status code.	No longer matches other policies
Allow	Used to skip the remaining rules in the current security module.	In the current module, the remaining rules will no longer match this request.	Continue to match other effective rules
Monitor	Used to evaluate or grayscale its security policies.	Logs are only recorded, no actions are taken.	Continue to match other rules
Redirect	Used to provide standby resources and improve user access experience when blocked.	Redirect to the specified URL.	No longer matches other policies
ReturnCustomPage	Used to provide block pages with a better experience. Used to be compatible with the API format and respond to error messages that the API can parse. Used to monitor business and monitor blocked requests by specifying status codes.	Returns a custom error page and status code. Supports referencing page content defined in the Custom Error Page feature.	No longer matches other policies
BlockIP	Used to punish malicious clients.	When a request matches the conditions, discard requests from that client IP within a period of time. **Note:** If the matching condition used is client IP (the XFF header is matched first), IP blocking will be	No longer matches other policies

		based on the request source client IP, rather than the XFF header. Configure with caution.	
JSChallenge	Used to identify tool clients that do not support JavaScript, frequently seen in DDoS attack sources.	Respond with an HTTP 302 redirect page, the page carries JavaScript code to verify the client browser behavior, and only the visitors that passes the verification can continue to access.	Requests that pass the challenge continue to match other rules
ManagedChallenge	Used for Bot defense, JavaScript challenge verification is first performed, and then CAPTCHA human verification is performed on requests that pass the verification.	First take the JavaScript challenge. For clients that pass the verification, they need to respond to the redirection (HTTP 302) page and carry the verification code for verification, and the user completes the verification through interactive operations. Only visitors who pass both verifications can continue to visit.	Requests that pass the challenge continue to match other rules

JavaScript Challenge

The JavaScript challenge verification process is imperceptible browser verification, neither displaying a verification page nor requiring manual intervention. The browser can automatically complete the verification and display the requested resources. This method can effectively filter DDoS attacks initiated by distributed scripts.

JavaScript Challenge Use Cases

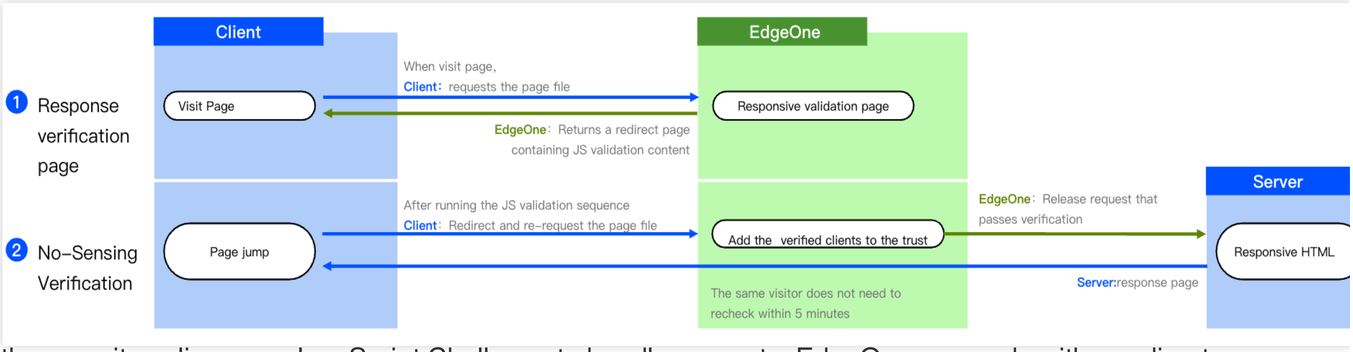
JavaScript Challenge mainly applies to protection of the following resources:
Pages visited in the browser;
Resources accessed only after you visit a page in the browser.

Note:

JavaScript Challenge is not suitable for the following scenarios:
Non-browser client access and certain scenarios, such as APIs accessed by mobile applications and APIs not called through a page. In such scenarios, the client may fail to pass verification for it cannot handle the JavaScript response content properly, thereby causing access to be blocked.
Scenarios where the request header options such as Accept are used for accessing non-HTML static resources. In such scenarios, the client may fail to pass verification for the JavaScript challenge response content does not match the Content-Type option in the Accept header, thereby causing failure of the resource access.

For the above business scenarios, you should use the **ReturnCustomPage** , **Redirect** or **Block** action, or configure protection exception rules to ensure normal business operation.

JavaScript Challenge Interaction Flow

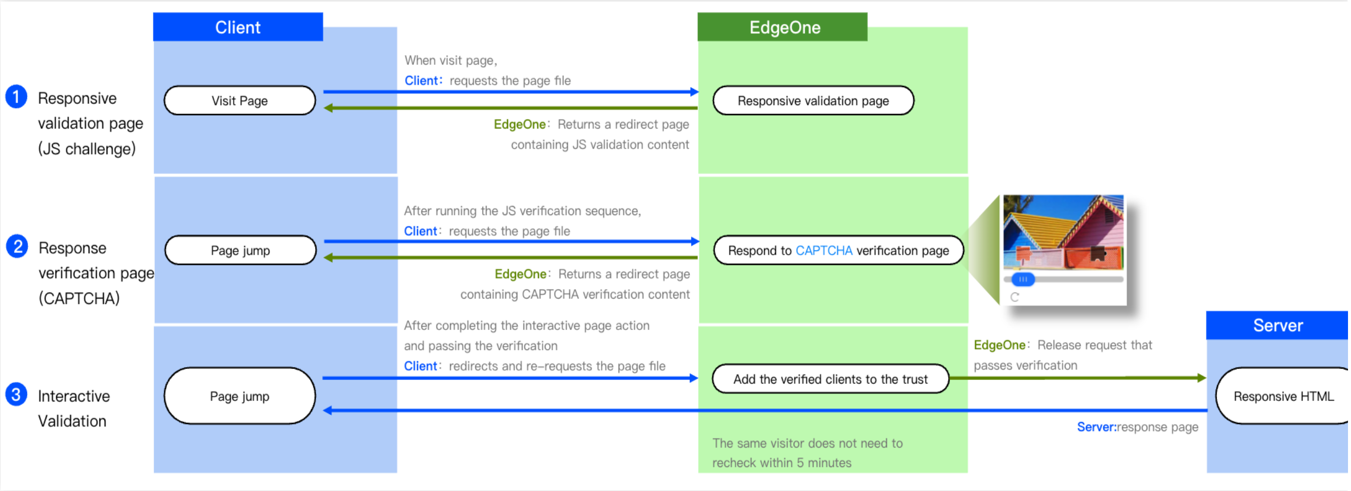

Client
EdgeOne
Server
1 Response verification page
2 No-Sensing Verification
Visit Page
When visit page,
Client: requests the page file
Responsive validation page
EdgeOne: Returns a redirect page containing JS validation content
Page jump
After running the JS validation sequence
Client: Redirect and re-request the page file
Add the verified clients to the trust
EdgeOne: Release request that passes verification
Responsive HTML
Server:response page
The same visitor does not need to recheck within 5 minutes

When the security policy uses JavaScript Challenge to handle requests, EdgeOne responds with a redirect page (HTTP 302) containing a JavaScript program to verify the browser runtime environment. After receiving this response, browsers with JavaScript enabled will execute the verification program and perform an HTTP 302 redirect. After receiving the redirect request, the EdgeOne security protection module will allow requests carrying valid identifiers (client IP and User-Agent).

Managed Challenge

Managed Challenge integrates JavaScript Challenge and CAPTCHA (human-machine verification) to verify the browser environment and human users through two-factor authentication. This method effectively filters out non-browser client access.

Managed Challenge Interaction Flow


Client
EdgeOne
Server
1 Responsive validation page (JS challenge)
2 Response verification page (CAPTCHA)
3 Interactive Validation
Visit Page
When visit page,
Client: requests the page file
Responsive validation page
EdgeOne: Returns a redirect page containing JS validation content
Page jump
After running the JS verification sequence,
Client: requests the page file
Respond to CAPTCHA verification page
EdgeOne: Returns a redirect page containing CAPTCHA verification content
Page jump
After completing the interactive page action and passing the verification
Client: redirects and re-requests the page file
Add the verified clients to the trust
EdgeOne: Release request that passes verification
Responsive HTML
Server:response page
The same visitor does not need to recheck within 5 minutes

When the security protection policy uses JavaScript Challenge to handle requests, EdgeOne first implements the JavaScript challenge mechanism, that is, responds with a redirect page (HTTP 302) containing a JavaScript program to verify the browser runtime environment. After receiving this response, browsers with JavaScript enabled will continue to respond with a redirect page (HTTP 302) that has an embedded interactive CAPTCHA verification program. After the program completes verification on the client, an HTTP 302 redirect is performed. After receiving the redirect request, the EdgeOne security protection module will allow requests carrying valid identifiers (client IP and User-Agent).

Note:

When the client frequently attempts JavaScript challenges and triggers interceptions, it will lead to the client entering the JavaScript Challenge blocklist. For a period of time, the security policy will no longer respond to JS challenges for that client and will directly respond with an interception page. To restore the client's access, please configure Protection Exception Rules.

Match Condition

Last updated：2024-08-26 16:40:42

Overview

Web Protection function is implemented by matching different conditions of requests. The following provides a detailed introduction to various matching condition options, matching condition descriptions, and related configuration methods and limitations.

Using Matching Conditions

You can use the matching conditions of the rule to specify the effective scope of the rule, and control the effective scope of protection exception rules, custom rules, rate limiting, and custom bot rules.

Note:

When multiple matching conditions are configured, the rule takes effect only when all matching conditions are satisfied.

Matching Methods

When the matching field and matching content meet the requirements of the matching method, the matching condition is satisfied.

Note:

For the request header matching fields (such as Referer header and custom headers), if the matching methods such as equal to, not equal to, include, exclude, wildcard matching, wildcard mismatch, and regular expression matching are used, the matching condition can be satisfied only when the header exists and is not empty.

Matching Method	Description
Equal to (in the list)	The **matching content** list contains the full string of the **matching field**, which is case-insensitive. The matching content can be configured with multiple values. When the matching field matches any value, the matching condition is satisfied.
Not equal to (not in the list)	The **matching content** list does not contain the full string of the **matching field** , which is case-insensitive. The matching content can be configured with multiple values. When the matching field matches none of the values, the matching condition is satisfied.

Include (keyword)	The **matching field** string contains any full string included in the **matching content** list, which is case-insensitive. The matching content can be configured with multiple values. When any value does not appear in the matching field, the matching condition is satisfied.
Exclude (keyword)	The **matching field** string does not contain any full string included in the **matching content** list, which is case-insensitive. The matching content can be configured with multiple values. When all values do not appear in the matching field, the matching condition is satisfied.
Wildcard matching	The **matching content** list contains a string for wildcard matching of the **matching field**, which is case-insensitive. The supported wildcard characters include: Asterisk `*` : Matches zero or multiple characters. Question mark `?` : Matches one character. The matching content can be configured with multiple wildcard expressions. When the matching field matches any wildcard expression, the matching condition is satisfied. When the matching content does not contain a wildcard, exact matching is used to judge the matching field.
Wildcard mismatch	The **matching content** list does not contain a string for wildcard matching of the **matching field**, which is case-insensitive. The supported wildcard characters include: Asterisk `*` : Matches zero or multiple characters. Question mark `?` : Matches one character. The matching content can be configured with multiple wildcard expressions. When the matching field matches none of the wildcard expressions, the matching condition is satisfied. When the matching content does not contain a wildcard, exact matching is used to judge the matching field.
Length greater than	The **matching field** exists and the data length (calculated by the number of characters in the string) is greater than the specified length.
Length less than	The **matching field** exists and the data length (calculated by the number of characters in the string) is less than the specified length.
Content is empty	The **matching field** exists and is an empty string.
Not exist	The **matching field** does not exist.
Regular expression matching	The **matching field** data can match the regular expression in the **matching content** .

Matching Condition Options and Descriptions

Note:

1. The supported matching conditions vary depending on the rule type and the EdgeOne plan you have subscribed to. For support details, refer to the Comparison among EdgeOne Plans.

2. In all the matching content of a single rule, the total number of the matching items should not exceed 128 (including the matching conditions that require matching multiple values simultaneously).

Match Condition options	Match Condition descriptions
Request Client IP	Match the source IP address of the request. Supports matching based on Region, ASN, IP, and CIDR Block. When using `Match` , `not match` logical symbol options, you can match Client IP, CIDR Block, and IP grouping. A single match condition can configure up to 8 IP groupings. When using `Region inclusion` , `Region exclusion` logical symbol options, you can match the Region of the Client IP. When using `ASN affiliation` , `ASN affiliation not equal to` logical symbol options, you can match the BGP autonomous system number (ASN) to which the Client IP belongs.
Request Client IP (Prioritize matching XFF Header)	When the request carries a valid XFF (X-Forwarded-For) Header, match the first IP in the XFF Header; otherwise, match the source IP address of the request. When using `Match` , `not match` logical symbol options, you can match Client IP, CIDR Block, and IP grouping. A single match condition can configure up to 8 IP groupings. When using `Region inclusion` , `Region exclusion` logical symbol options, you can match the Region of the Client IP. When using `ASN affiliation` , `ASN affiliation not equal to` logical symbol options, you can match the BGP autonomous system number (ASN) to which the Client IP belongs.
Custom request header	Match the specified header of the request, providing additional parameter options to match the header value of a specific name. Case insensitive. Supports equal to, not equal to, include, exclude, wildcard matching, wildcard mismatch, length greater than, length less than, content is empty, no existing, regular expression match.
Request URL	Match the request URL. For example: /example.html?region=cn . Case insensitive. Exclude Hostname Include URL query parameters Supports equal to, not equal to, include, exclude, wildcard matching, wildcard mismatch, length greater than, length less than, content is empty, no existing, regular expression match.

Request Source (Referer Header)	Match the request's Referer header. Case insensitive. Supports equal to, not equal to, include, exclude, wildcard matching, wildcard mismatch, length greater than, length less than, content is empty, no existing, regular expression match.
Request content type (Accept Header)	Match the request's Accept header. Case insensitive. Supports equal to, not equal to, include, exclude, wildcard matching, wildcard mismatch, length greater than, length less than, content is empty, no existing, regular expression match.
Request Path	Match the request URL's path section. For example: /example.html or /api/v2/login. Hostname is not included. Query parameters are not included. Case insensitive.
Request Method	Method for matching requests. Case insensitive. Supports multiple selections: GET, POST, HEAD, PUT, DELETE, TRACE, OPTIONS, CONNECT.
Request Cookie	Matches specified request Cookie header parameter values. Cookie parameter name must be specified. Case insensitive. Supports equal to, not equal to, include, exclude, wildcard matching, wildcard mismatch, length greater than, length less than, content is empty, no existing, regular expression match.
XFF extended headers	Match the request's XFF (X-Forwarded-For) header. Case insensitive. Supports equal to, not equal to, include, exclude, wildcard matching, wildcard mismatch, length greater than, length less than, content is empty, no existing, regular expression match.
Network layer protocol	Match the type of IP protocol used in the request. Support multiple selections: IPv4, IPv6.
Application layer protocol	Match the application layer protocol used in the request. Support multiple selections: HTTP, HTTPS.
Response status code	Match the HTTP status code of the response. Only support rate limiting; configuration is supported when selecting based on response statistics. Supports matching up to 20 status codes simultaneously.
Request body	Match the body of the request.

	Only supports matching the first 8 KB data of the request body.

API Discovery（Beta）

Last updated：2025-05-26 16:31:59

Function Overview

API Discovery helps enterprises automatically discover, count, and manage API call situations on the platform. This function is based on request flow data that has been integrated into the EdgeOne platform. By parsing HTTP request paths, request methods (such as GET, POST, etc.), and associated response features, it automatically extracts the actual accessed API paths and usage. The system classifies the received request data, removes noise, and performs trend analysis, helping enterprises accurately identify active APIs, deprecated APIs, and potential shadow APIs.
The main features of API asset identification include:
Automatic Comprehensive Identification: Based on real-time incoming traffic, it dynamically sorts all API call assets proxied by EdgeOne without manual input.
Precise Risk Positioning: Identifies high-frequency abnormal calls, unusually exposed interfaces, and deprecated interfaces as potential risk points, assisting in formulating security policies.
Optimized Resource Allocation: Guides the optimization of backend resource configuration and interface governance through evaluation of call activity and trends.

Typical Business Scenarios

Quickly discover and address shadow APIs: Security operations personnel discover unknown API calls during routine inspections, which may expose sensitive data or service risks.
Investigate and handle abnormal traffic for interfaces: Operations engineers notice a sudden increase in traffic for a specific API and need to quickly analyze the cause and formulate throttling strategies.

Operation Steps

The following example illustrates the specific usage process of "Shadow API Discovery and Handling":
1. Log in to the EdgeOne console, click **Site List** in the left sidebar, and select the site to be configured.
2. In the site detail page, click **Security Protection > API Protection** to enter the API asset identification page.
3. Set the time zone and time range to view at the top of the page (for example, "Last 7 days"), with data retrievable for up to 30 days.
4. Filter by domain or directly input API path keywords to search for specific interfaces, quickly locating suspected shadow APIs.

5. View the call counts and trends for specific APIs to identify abnormal or unknown API paths.

6. For risky APIs, click the corresponding action button, such as quickly creating **Precise Matching Rules** for interception or setting call frequency limits through **Rate Limiting Rules**.

Analysis Process and Handling Recommendations

1. If confirmed as abnormal traffic, immediately set rate limits for the corresponding interface to prevent backend resources from being abused or causing service unavailability.
2. For more detailed investigations, use EdgeOne's real-time logging feature to obtain real-time data, confirming the source and pattern of calls.
3. Based on the investigation results, further measures may be taken if necessary:

Adjust API Interface Permission Control: For sensitive or high-risk API interfaces, it is recommended to implement access control through custom rules in the EdgeOne console, such as:

Allowing access only from specific IPs or IP segments (via IP blocklist/allowlist rules).

Requiring specific headers (such as custom authentication tokens) to be present and pass format validation.

Working with application-side authentication mechanisms (such as JWT Token validation, OAuth authorization processes) and limiting illegal requests through rules in EdgeOne.

Combining access frequency statistics to implement throttling or interception for requests without valid identity credentials.

Strengthen API Security Protection Policies: Configure stricter WAF rules for high-risk interfaces, such as enabling strict parameter validation, access frequency limits, or challenge verification based on client behavior characteristics.

Usage Restrictions and Handling Recommendations

Data Update Delay: Data is updated daily, with a maximum delay of 24 hours. For more timely analysis results, combine with the real-time logging function for a comprehensive analysis.

Historical Data Retention Period: The platform retains API call data for the past 30 days.

Related Capability Linkage

API asset identification can be linked with the following EdgeOne security features to further enhance security operations efficiency:

Web Protection: Based on API identification results, directly create precise Web Application Firewall (WAF) rules to guard against API attack risks.

Analysis:Combine with traffic analysis functionality for in-depth investigation of abnormal API calls and locate the sources of abnormal traffic.

Rate Limiting:Quickly formulate rate limiting strategies for high-frequency abnormal APIs to protect business stability.

Custom Response Page

Last updated：2024-08-26 09:51:52

Feature Overview

In some cases, users may encounter exceptions and receive a response status code when accessing the site. In order to help users better understand the problems and solutions, EdgeOne provides a custom response page feature. This feature can help you inform users of the current website status through a specified custom response page, and avoid users from failing to determine the specific reason and handling method in case of request errors.

EdgeOne offers the custom response page feature in both site acceleration and security protection features. You can perform configuration according to actual scenarios.
Custom Site Origin-Pull Error Response **Pages**: You can customize the response page content for the origin-pull status codes 4xx or 5xx. For details, see Custom Error Page.
Custom Security Protection Policy Block Response **Pages**: You can customize the status code and response page content when Web protection or Bot protection block policies are triggered. For details, see Configuring Custom Response Pages in Security Protection.

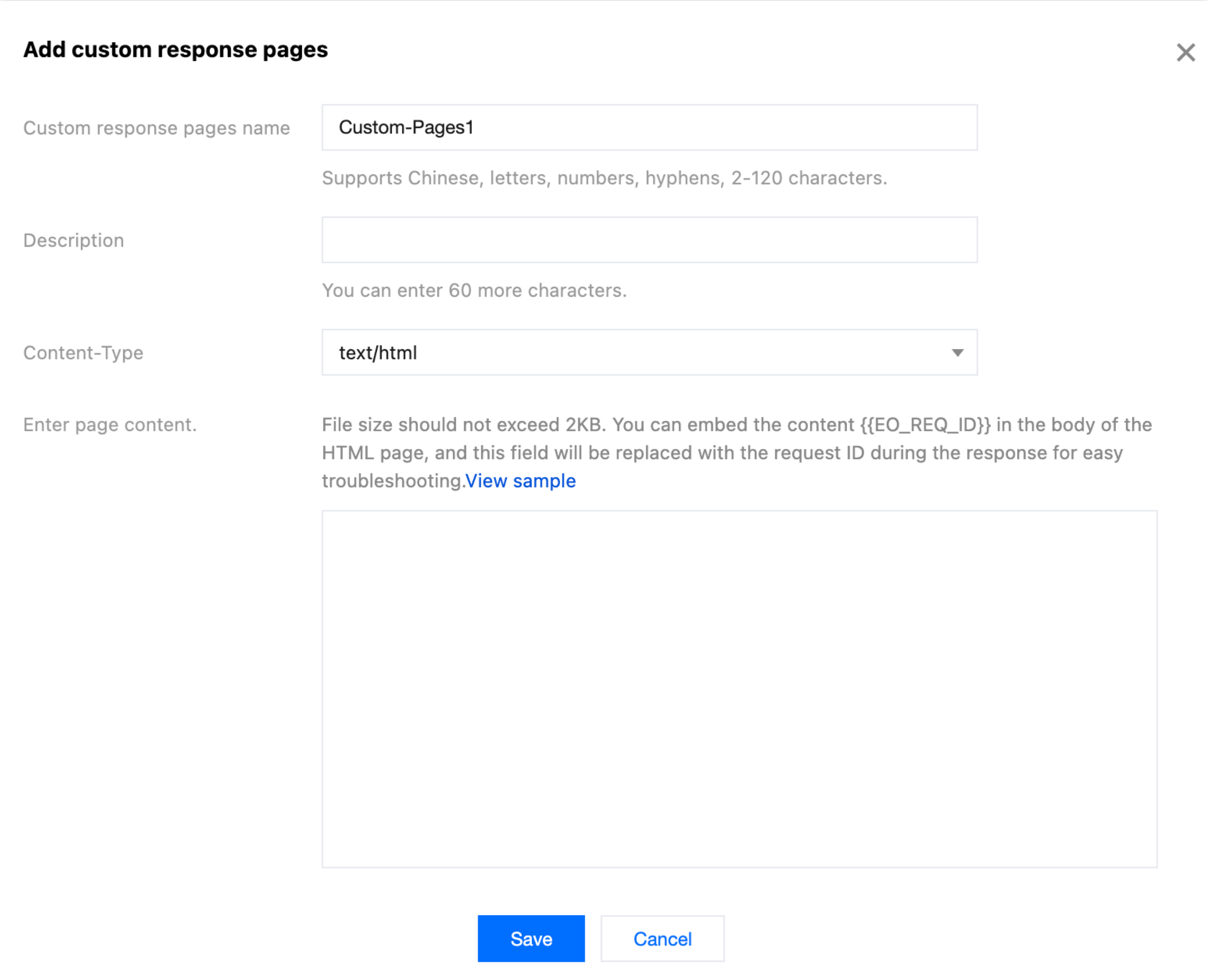
Additionally, to facilitate management and usage, EdgeOne offers the Custom Response Page Template feature, which can be used to manage the response page content and be referenced by different feature modules. By editing this response page template, you can simultaneously apply the modified response page content to all referencing feature modules.

Configuring the Custom Response Page Template

You can customize the Content-Type and the included content information of the response page. Refer to the following steps for configuration:
1. Log in to the EdgeOne console and click **Site List** in the left sidebar. Then click the **site** to be configured in the site list.
2. On the site details page, click **Custom** Response **Page**.
3. Click **Add Custom Response Pages** and configure the custom response page content. The related parameters are explained as follows:
Content-Type: The value of the HTTP response header `Content-Type` included in the custom response page during response. Supported values are `application/html` , `application/json` , `text/plain` , and

`application/xml` . For example, if `text/plain` is selected, the HTTP response header `Content-Type: text/plain` will be returned when EdgeOne responds with the custom response page.

Page content: The body of the custom response page, not exceeding 2 KB. It is recommended to contain `{{ EO_REQ_ID }}` in the page content. This field will automatically get the user's request ID information during response, and will be replaced with the request ID to facilitate problem locating.



Add custom response pages

Custom response pages name: Custom-Pages1

Supports Chinese, letters, numbers, hyphens, 2-120 characters.

Description:

You can enter 60 more characters.

Content-Type: text/html

Enter page content.

File size should not exceed 2KB. You can embed the content {{EO_REQ_ID}} in the body of the HTML page, and this field will be replaced with the request ID during the response for easy troubleshooting.View sample

4. Click **Save** to complete the creation of the response page.

Note:

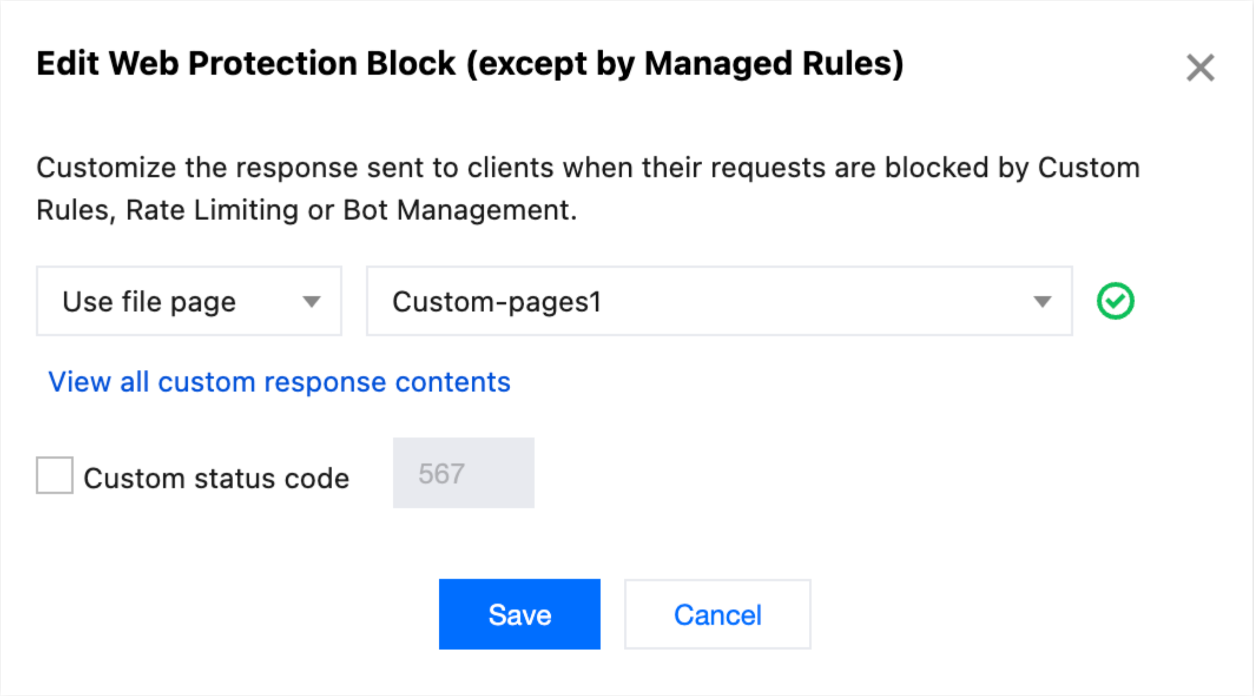
If the custom response page has already been referenced by other feature modules, it cannot be deleted. If deletion is required, navigate to the feature module referencing this page and dereference it first.

After a created custom response page is edited and saved, all feature modules referencing this custom response page will automatically apply the edited page.

Configuring Custom Response Pages in Security Protection

Assume that a custom Web protection rule configured for the current site domain `www.example.com` only allows accesses by users within the Chinese mainland, and blocks accesses by users in other regions. When the users in other regions attempt to access, you should inform them of the block reason through a custom response page. You have referred to Configuring Custom Response Page Template to configure a custom response page named `Custom-Pages1` . Then you can take the following steps to configure it:

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. Then click the **Site** to be configured in the site list.
2. Click **Security** > **Web Security** . By default, it is a site-level security policy. To configure differentiated security policies for a specific domain name under the current site, you can enter the **Domain-level security policy** tab and click the **corresponding domain name** to enter the configuration page for the domain-level security policy. The subsequent steps are the same.
3. Under the custom block page classification, select the block page module you need to configure. For example, you can select the **Web Protection Block (except by Managed Rules)** page and click **Edit** .
4. On the edit page, configure the content of the custom response page, select **Use file page** for blocking, and choose the pre-configured page named Custom-Pages1.



Edit Web Protection Block (except by Managed Rules)

Customize the response sent to clients when their requests are blocked by Custom Rules, Rate Limiting or Bot Management.

Use file page ▾ Custom-pages1 ▾ ✓

5. Then click **Save** to complete the configuration.

Alarm Notification

Last updated：2023-12-18 15:03:57

Overview

EdgeOne can push alarm notifications when security events are detected. You can subscribe to the notifications in the Message Center.

DDoS alarms: For DDoS attacks against the Enterprise DDoS mitigation plan (site access and layer-4 proxy services),

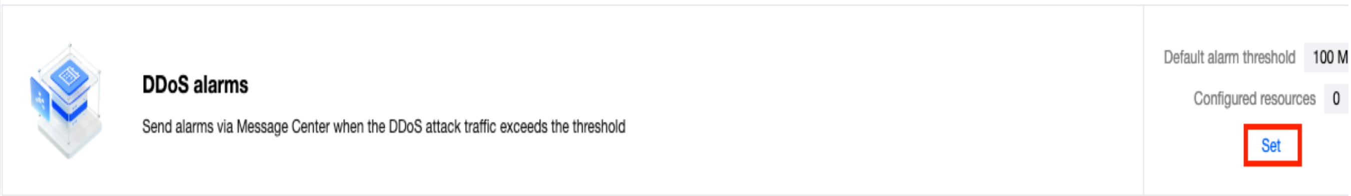
Web security monitoring rules: For security monitoring against web protection rules and bot protection rules, you can set a request condition threshold.

DDoS Attack Traffic Alarms

EdgeOne monitors the incoming traffic in real time, and cleanses traffic as soon as malicious attack traffic is detected. Alarm notifications are pushed only for DDoS attacks against the Enterprise DDoS mitigation plan (site access and layer-4 proxy services). Currently, other businesses don't support the DDoS attack traffic alarming feature.

Configuring DDoS alarm settings

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. On the site details page, click **Security** > **Alarm Setting**.



DDoS alarms

Send alarms via Message Center when the DDoS attack traffic exceeds the threshold

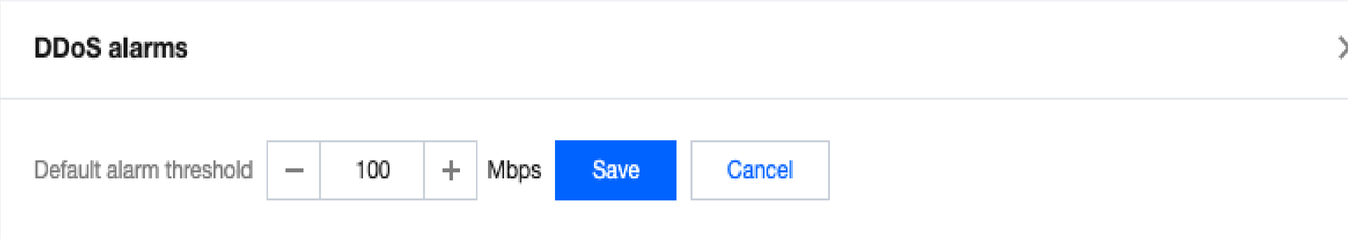
Default alarm threshold 100 M

Configured resources 0

3. On the **DDoS alarm** page, adjust the default global DDoS attack alarm threshold for the current site, and the Message Center will push attack event notifications only when the attack rate exceeds the configured threshold. To do so, click **Edit** of the default alarm threshold, modify the threshold, and click **Save**.

Note:

The **DDoS alarm** page displays all objects that can be configured and their custom DDoS alarm thresholds if you have set. For those not configured with custom thresholds, you can modify the **Default alarm threshold**.



DDoS alarms

Default alarm threshold: 100 Mbps

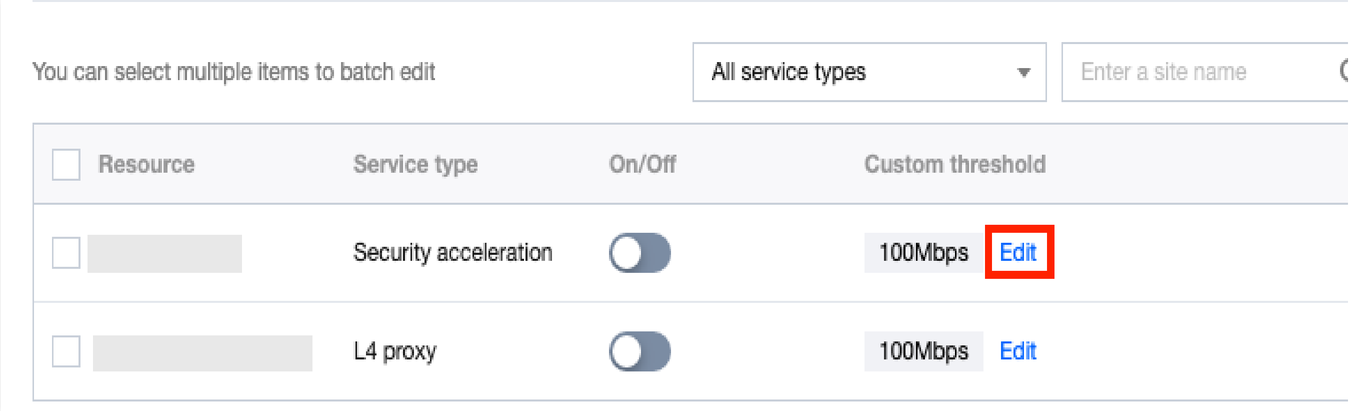
4. On the **DDoS alarm** page, configure the alarm threshold for a security acceleration or layer-4 proxy business project.

Note:

We recommend you adjust the threshold based on the attack frequency and history. The threshold is 100 Mbps by default and can be adjusted to 10 Mbps at the minimum.

4.1 Set a single alarm threshold

4.1.1 Select the target object and click **Edit** in the **Custom threshold** column. The threshold indicates the minimum attack rate above which the object will push DDoS attack notifications.



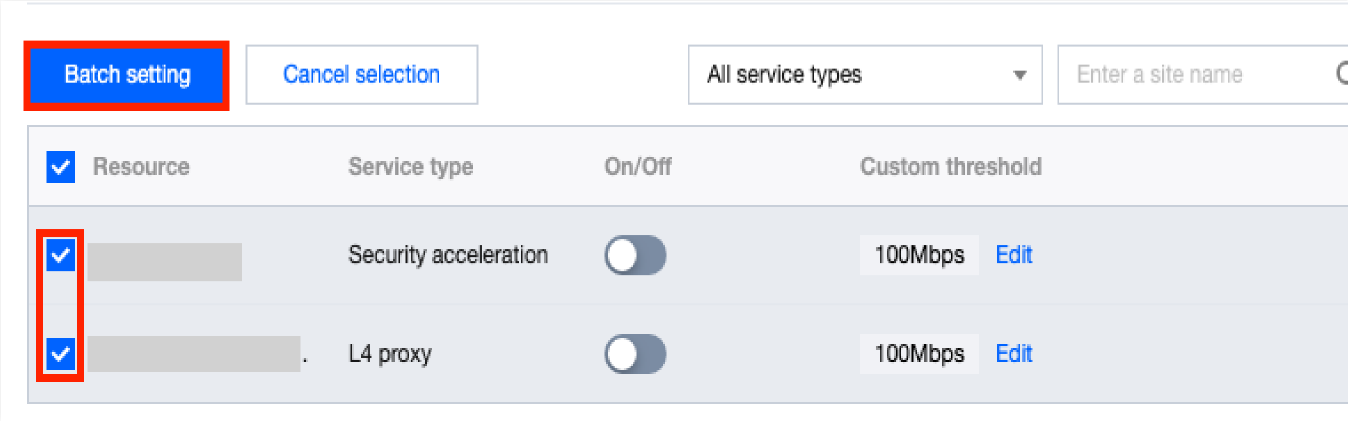
You can select multiple items to batch edit

□ Resource	Service type	On/Off	Custom threshold
□ [redacted]	Security acceleration	○	100Mbps Edit
□ [redacted]	L4 proxy	○	100Mbps Edit

4.1.2 Modify the alarm threshold, click **Save**, and the custom threshold will be enabled automatically.

4.2 Batch set alarm thresholds

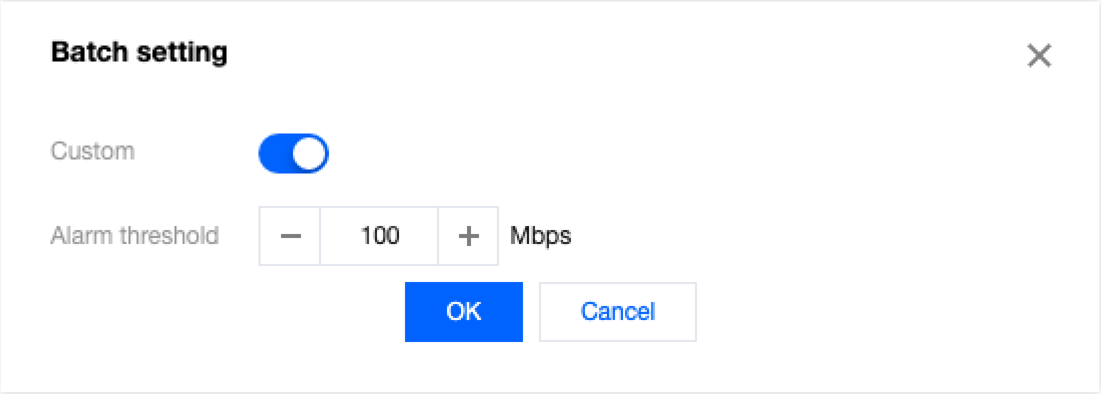
4.2.1 Select one or more objects and click **Batch setting**.



☑ Resource	Service type	On/Off	Custom threshold
☑ [redacted]	Security acceleration	○	100Mbps Edit
☑ [redacted]	L4 proxy	○	100Mbps Edit

4.2.2 Toggle on the custom threshold switch

, set the alarm threshold, and click **OK**.



Batch setting

Custom: on

Alarm threshold: 100 Mbps

Web Security Monitoring Rules

When processing requests, EdgeOne records requests that hit **web security** and **bot management** rules (including security rules configured in **policy templates**) to the web security logs.

Note:

Requests that hit a rule whose action is **Allow** are not logged.

Requests are counted by the domain name. Alarms are generated when the request count exceeds the alarm threshold.

The web security monitoring rule counts the total number of rule-hit requests from a single domain name. When the rule-hit request count exceeds the threshold, an alarm is generated.

Options of web security monitoring rules

Web security monitoring rules support flexible ranges of monitoring statistics and alarm settings. You can configure multiple monitoring rules to cover daily monitoring and alarm scenarios based on your security O&M needs.

Web security monitoring rules support the following options:

Rule name: Required. Take note of the following naming conventions:

It can contain only letters, digits, and underscores.

The character length must be less than 32.

It cannot start with an underscore.

Domain name: Required. Select the domain names to be monitored.

All hostnames: Including all domain names in the current site and the domain names that are to be added in the future.

Specified hostnames: The domain names that are selected from the site.

Monitor requests: Required. You can select a statistical range for the requests by processing method or rule.

All matching requests: All requests that match the security rules are counted, except for those matching the security rules with the action being **Allow**.

By action: Requests that match the web protection or bot management rules with the specified action are counted.

By rule: Requests that match the web protection or bot management rules are counted.

Alarm setting: Select the alarm condition. You can select the alarm frequency.

Static alarm: When the request count threshold is exceeded, alarm notifications are pushed in the specified frequency.

Alarm frequency: When the security rule satisfies the alarm condition, alarm notifications are pushed in the specified frequency.

Note:

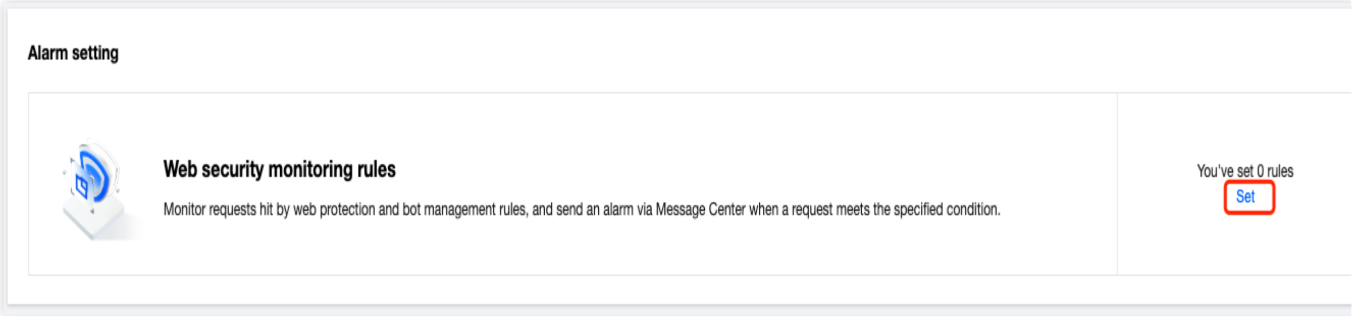
If **Alarm frequency** is not selected, alarm notifications are pushed once every five minutes for each rule by default.

Managing web security monitoring rules

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.

2. On the site details page, click **Security > Alarm Setting**.

3. In the **Web security monitoring rules** card, click **Set** to create, delete, edit, enable, or disable a web security monitoring rule.



Alarm setting

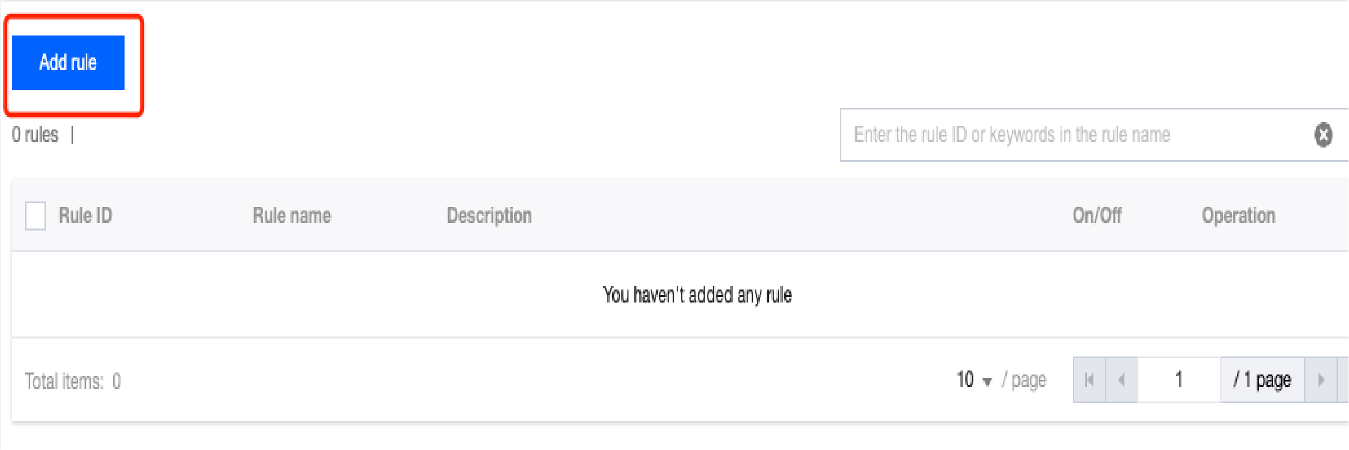
Web security monitoring rules

Monitor requests hit by web protection and bot management rules, and send an alarm via Message Center when a request meets the specified condition.

You've set 0 rules

Create a web security monitoring rule

1. On the **Web security monitoring rules** page, click **Add rule**.



0 rules |

Enter the rule ID or keywords in the rule name

□ Rule ID	Rule name	Description	On/Off	Operation
You haven't added any rule				

Total items: 0

10 ▾ / page 1 / 1 page

2. In the **Create web security monitoring rule** pop-up window, set the **Rule name**, **Domain name**, **Monitor requests**, and **Alarm setting** parameters, and click **Save**. The alarm condition takes effect immediately.

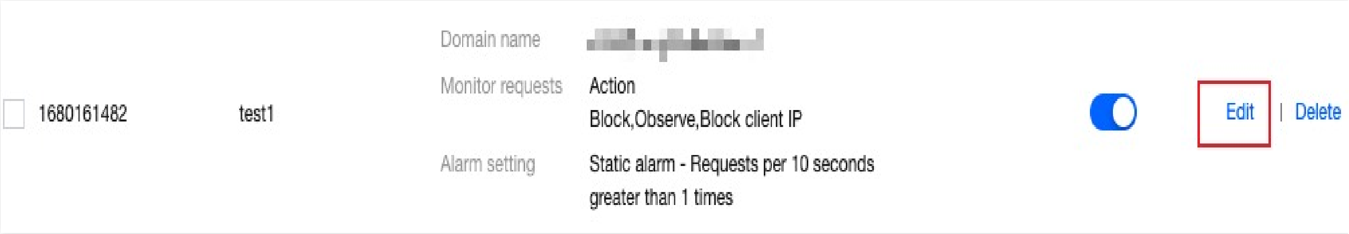
Edit a web security monitoring rule

1. On the **Web security monitoring rules** page, find the target rule and click **Edit** in the **Operation** column.
2. In the **Edit web security monitoring rule** pop-up window, modify the **Rule name**, **Domain name**, **Monitor requests**, and **Alarm setting** parameters, and click **Save**. The updated alarm condition takes effect immediately.

Delete a web security monitoring rule

Delete a single web security monitoring rule

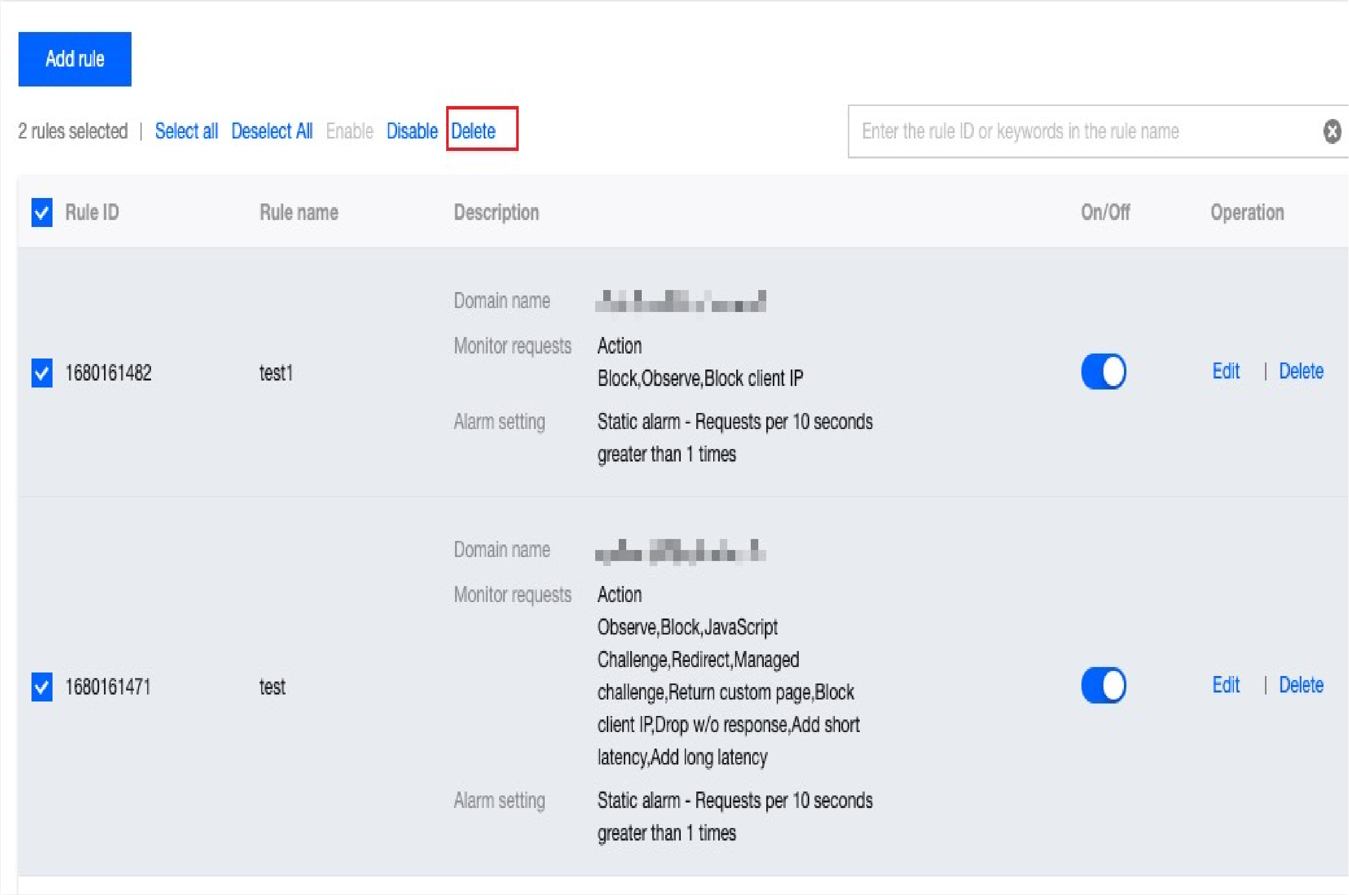
On the **Web security monitoring rules** page, find the target rule and click **Delete** in the **Operation** column.



□ 1680161482	test1	Domain name [redacted] Monitor requests Action Block,Observe,Block client IP Alarm setting Static alarm - Requests per 10 seconds greater than 1 times	●	Edit | Delete

Batch delete web security monitoring rules

On the **Web security monitoring rules** page, select the target rules and click **Delete**.


Add rule
2 rules selected | Select all Deselect All Enable Disable Delete
Enter the rule ID or keywords in the rule name

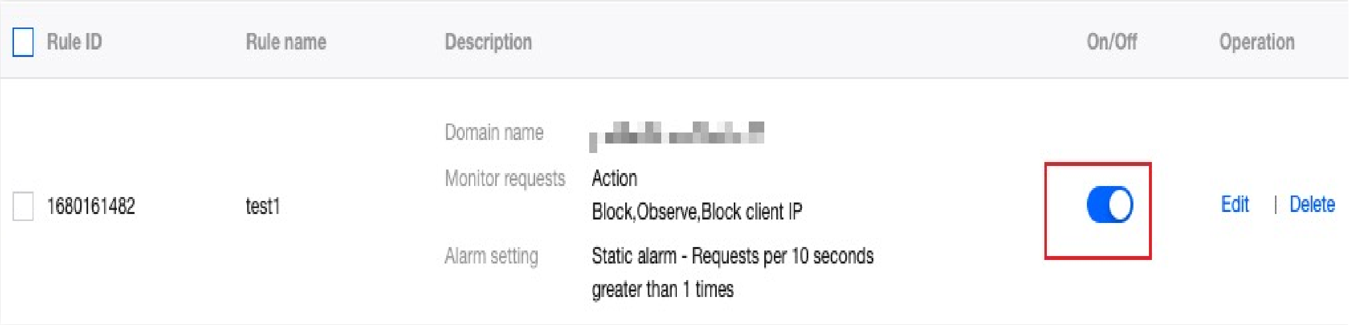
☑ Rule ID	Rule name	Description		On/Off	Operation
☑ 1680161482	test1	Domain name Monitor requests Alarm setting	[redacted] Action Block,Observe,Block client IP Static alarm - Requests per 10 seconds greater than 1 times	●	Edit | Delete
☑ 1680161471	test	Domain name Monitor requests Alarm setting	[redacted] Action Observe,Block,JavaScript Challenge,Redirect,Managed challenge,Return custom page,Block client IP,Drop w/o response,Add short latency,Add long latency Static alarm - Requests per 10 seconds greater than 1 times	●	Edit | Delete

Enable or disable a web security monitoring rule

Enable or disable a single web security monitoring rule

On the **Web security monitoring rules** page, select the target rule and toggle on or off the switch

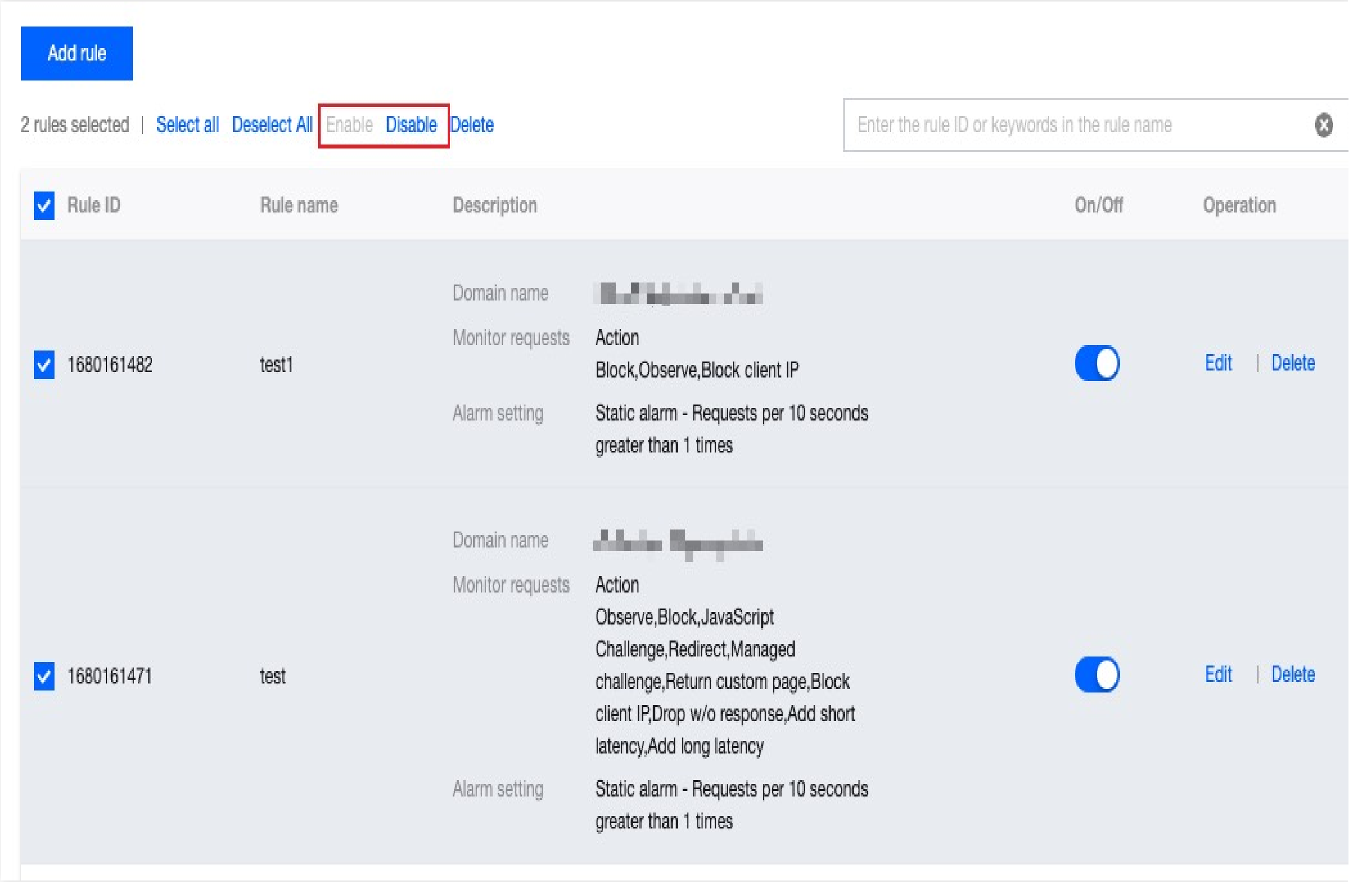
in the **On**/**Off** column.



□ Rule ID	Rule name	Description		On/Off	Operation
□ 1680161482	test1	Domain name Monitor requests Alarm setting	[redacted] Action Block,Observe,Block client IP Static alarm - Requests per 10 seconds greater than 1 times	●	Edit | Delete

Batch enable or disable web security monitoring rules

On the **Web security monitoring rules** page, select the target rules and click **Enable** or **Disable**.



Add rule

2 rules selected | Select all Deselect All Enable Disable Delete

Enter the rule ID or keywords in the rule name

☑ Rule ID	Rule name	Description	On/Off	Operation
☑ 1680161482	test1	Domain name [redacted] Monitor requests Action Block,Observe,Block client IP Alarm setting Static alarm - Requests per 10 seconds greater than 1 times	●	Edit | Delete
☑ 1680161471	test	Domain name [redacted] Monitor requests Action Observe,Block,JavaScript Challenge,Redirect,Managed challenge,Return custom page,Block client IP,Drop w/o response,Add short latency,Add long latency Alarm setting Static alarm - Requests per 10 seconds greater than 1 times	●	Edit | Delete