

Tencent Cloud EdgeOne

Security Protection

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

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

Security Protection

Overview

DDoS Protection

DDoS Protection Overview

Exclusive DDoS Protection Usage

Configuration of Exclusive DDoS protection Rules

Increase DDoS Protection Level

Exclusive DDoS Traffic Alarm

Configuration IP blocklist/allowlist

Configuration Region Blocking Rule

Configuration Port Filtering

Configuration Features Filtering

Configuration Protocol Blocking Rule

Configuration Connections Attack Protection

Related References

Action

Related Concepts Introduction

Web Protection

Overview

Custom rule

Rate Limiting

CC attack defense

Custom Rate Limiting Rules

Bot Management

Overview

Bot Intelligent analysis

Bot Basic Feature Management

Client Reputation

Active Detection

Custom Bot Rule

Related References

Action

Managed rules

Exception Rules

Managed Custom Rules

Web security monitoring alarm

Refer

Web Protection Request Processing Order

Action

Match Condition

Rules Template

IP and IP Segment Grouping

Origin Protection

Custom Response Page

Alarm Notification

Security 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 <code>Moderate</code> protection level to discard traffic exhibiting clear DDoS attack characteristics. Emergency recovery during attack bypass: Implement the <code>Strict</code> 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

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

		<p>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.</p> <p>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.</p>	
	Protection Exception Rules - Skip Protection Modules	<p>Skip protection rules in web protection by module.</p> <p>For example:</p> <p>Allow internal services: Set the internal service IP list and specified API paths to allow clients on the list unrestricted access to that path.</p>	None
	Protection Exception Rules - Skip Specified Managed Rules	<p>Skip specified managed rules.</p> <p>For example:</p> <p>Allow user content uploads: Configure business paths and false-positive rules to allow requests when parameters contain user-written content.</p>	None
Bot Management	Bot Intelligent Analysis	<p>Intercept bot requests based on risk levels. (Suitable for quickly enabling bot management strategies and establishing bot access profiles).</p> <p>For example:</p> <p>Intercept misuse of CDN resources (scraping):</p>	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	<p>the features, headers, and client IP of requests. The feature provides more disposal options for bot counteraction.</p> <p>For example:</p> <p>Counteract high-risk bots accessing sensitive business:</p> <p>Match based on access paths and client profiles, configure observation, silent, and response after waiting with certain weights.</p>	
--	----------------------------------	---	--

DDoS Protection

DDoS Protection Overview

Last updated : 2024-08-05 16:38:06

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 :

Exclusive DDoS protection can only be subscribed to by EdgeOne Enterprise plan.

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 : 2023-08-17 14:25:33

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, continuous detection, cleaning, and filtering of malicious traffic.
2. Committed protection capacity, maintaining a stable session state during protection.
3. Customizable DDoS protection strategies, including IP-based and client region-based control options.

Help you mitigate DDoS attack risks and ensure business stability.

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.

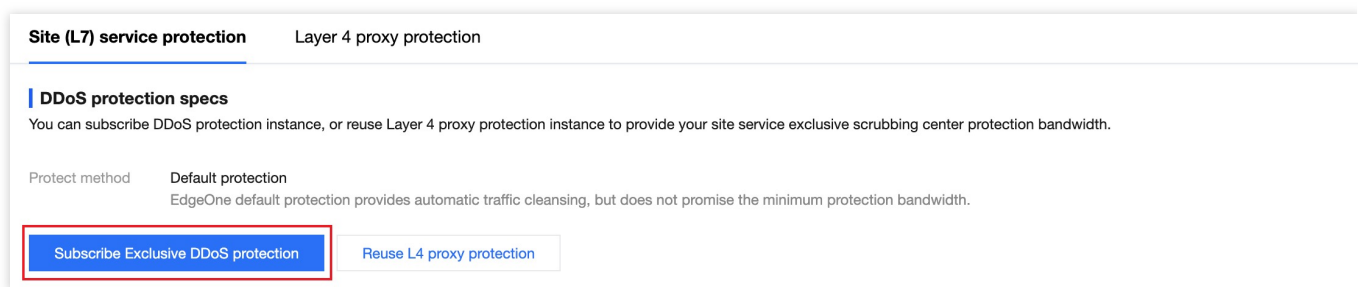
Precautions

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 Protection > DDoS Protection**.
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.

Subscribe site (L7) Exclusive DDoS protection instance

Plan type: EdgeOne Enterprise Plan

Plan ID: 

Global (MLC excluded) protection specs:

Default protection	Anycast 300 Gbps	Unlimited mitigation
--------------------	------------------	----------------------

Chinese mainland protection specs:

Default protection	<div> <div>Base protection 30 Gbps</div> <div>Elastic protection bandwidth limitation 300 Gbps</div> </div>	<div>Base protection</div> <div>Elastic protection bandwidth limitation</div>
--------------------	---	---

Chinese mainland elastic protection limitation:

Base protection bandwidth:  30 Gbps

Base protection bandwidth: fixed payment per subscription cycle. When the attack bandwidth does not exceed base protection bandwidth, no payment is required.

Elastic protection bandwidth: pay according to the actually detected DDoS attack bandwidth. When the attack bandwidth exceeds the guaranteed protection bandwidth, the payment is calculated based on the portion exceeding the guaranteed protected bandwidth. Reference: [Billing description](#)

Note: When the attack traffic received by an exclusive protection instance exceeds the elastic protection limitation you set, EdgeOne will block the exclusive protection instance.

1. After you subscribe to an Exclusive DDoS protection instance, EdgeOne will charge exclusive protection traffic fee for the subdomain with exclusive protection enabled;
2. When you subscribe to an exclusive DDoS protection instance for the first time, you will also subscribe to an exclusive protection traffic package (3TB), which can be used to defend against DDoS attacks. [Billing description](#)

Exclusive protection instance

Total subscription fee

(Subscription fees)

☒ I have read and agree to [EdgeOne Service Level Agreement](#) and [Refund Rule](#)

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.

Create L4 proxy instance

Instance name

test

1-50 characters ([a-z], [0-9] and [-]). It must start and end with a digit or letter. Consecutive hyphens (-) are not allowed.

Instance available area

☒ Global (MLC excluded) ☐ Chinese mainland ☐ Global

Security configuration

Protect method

Exclusive DDoS protection

Protection specs

Anycast 300 Gbps

Unlimited mitigation

Access configuration

IPv6 access

☐

Fixed IP

☐

Cross-MLC-border acceleration

☐

☐ I have read and agree to [EdgeOne Service Level Agreement](#) and [Refund Rule](#)

Subscription fee

Subscribe

Cancel

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.

Scenario 3: Site reuse of L7 with L4 proxy instances for DDoS protection resources

Scenario Example

Suppose your current Exchange email service is provided through multiple protocols, including HTTPS and multiple TCP/UDP protocols, and has recently suffered a DDoS attack exceeding 200Gbps. Due to its business architecture featuring both HTTPS and TCP/UDP services, hackers can launch DDoS attacks via HTTPS or TCP/UDP. Therefore, security protection is needed for both L7 sites and L4 proxies.

Precautions

When reusing L7 sites with independent L4 proxy DDoS protection, you need to configure port filtering in the independent DDoS protection to release the ports used by L7 traffic and avoid interception of L7 traffic.

The current feature is still in internal testing. If needed, you can contact Tencent Cloud sales to activate it.

Directions

Step 1: Create a new L4 proxy instance and enable protection

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 **L4 proxy**, and in the L4 proxy management instance interface, click on **Create L4 proxy**.
3. When creating a new L4 proxy instance, you can choose the corresponding protection method in the security protection configuration, switch to Exclusive DDoS protection, and in this scenario, you can choose Anycast joint defense 300Gbps.

Create L4 proxy instance

Instance name

1-50 characters ([a-z], [0-9] and [-]). It must start and end with a digit or letter. Consecutive hyphens (-) are not allowed.

Instance available area
☒ Global (MLC excluded)
☐ Chinese mainland
☐ Global

Security configuration

Protect method

Exclusive DDoS protection

Protection specs

Anycast 300 Gbps

Unlimited mitigation

Access configuration

IPv6 access ?
☐

Fixed IP ?
☐

Cross-MLC-border acceleration ?
☐

☐ I have read and agree to [EdgeOne Service Level Agreement](#) and [Refund Rule](#)

Subscription fee

Subscribe

Cancel

4. 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 an independent DDoS protection configuration for the instance;

5. After the configuration is issued, you can click on **Configure** to enter the instance configuration interface, add the required accelerated port information and origin address, and click Save to enable L4 proxy acceleration.

Step 2: Release L7 access traffic in the L4 proxy security protection instance


1. After the L4 proxy configuration is completed, you can go to the menu **Security Protection > DDoS Protection**, and in the L4 proxy protection, select the L4 proxy instance created in Step 1 and click on **Security Configuration**;

Site (L7) service protection

Layer 4 proxy protection

Layer 4 proxy instance

If you have a Layer 4 proxy instance with Exclusive DDoS Protection enabled, you can configure the DDoS protection specifications and policies of the Layer 4 proxy here.

Layer 4 proxy instanc...	Status reused by site (...)	Instance available area	Global (MLC excluded...	Chinese mainland bas...	Chinese mainland ela...	Mitigation status
	Does not support sharing to site service ⓘ	Global (MLC excluded)	Anycast 300 Gbps	-	-	Running

Total items: 1

10 / page

2. In the protection configuration, find the port filtering card, click on Setting to enter the configuration interface; click on Create, configure the release source port range as 1-65535, destination port range 443, action selection as

continue protection, release the corresponding L7 traffic, and click Save to take effect. Add another rule to release port 80 using the same steps. The complete configuration rules are as follows:

Port filtering			
Create			
Protocol	Source port range	Destination port range	Action
TCP	1-65535	443-443	Continue protection
TCP	1-65535	80-80	Continue protection
Total items: 2			
10 ▼ / page			1

Step 3: Reuse the L4 proxy protection instance to provide protection for L7 site domain names

1. After completing Step 2, click on **Security Protection > DDoS Protection**, and in the Site (L7) Service Protection, click on **Reuse L4 Proxy Protection**;

Site (L7) service protection

Layer 4 proxy protection

DDoS protection specs

You can subscribe DDoS protection instance, or reuse Layer 4 proxy protection instance to provide your site service exclusive scrubbing center protection bandwidth.

Protect method

Default protection


EdgeOne default protection provides automatic traffic cleansing, but does not promise the minimum protection bandwidth.

Subscribe Exclusive DDoS protection

Reuse L4 proxy protection

2. After selecting the L4 proxy protection resources to be reused, click Confirm to start the automatic issuance of independent DDoS instance configurations;

Reuse L4 proxy protection instance

 You can reuse exclusive protection resources of the L4 proxy instance under the current plan. After reusing, the DDoS protection policy of the L4 proxy instance will take effect for the current domain

protect resource

L4 proxy

Please select

Notes

1. After enabling Exclusive DDoS protection, the inbound and outbound traffic of the domain will be credited to the usage of exclusive DDoS protection, and will be billed independently.
2. When modifying the protection method or protection resources, the client connection will be reset.
3. After reusing exclusive protection resources of the L4 proxy instance, the L4 proxy instance cannot configure some port forwarding rules (such as: TCP 80/443, etc.)
4. After reusing exclusive protection resources of the L4 proxy instance, the DDoS protection policy of the Layer 4 proxy instance will take effect for the current domain. Please confirm that the TCP protocol or HTTP/HTTPS service port (such as: TCP 80) is not blocked in the L4 proxy instance. When WebSocket is enabled, UDP port 80 should be guaranteed not to be blocked to avoid causing interruption of Web services.

OK

Cancel

3. After the instance is issued, you can enable independent DDoS protection for all domain names in the protection configuration interface, or select `exchange.example.com` in this scenario to enable independent DDoS protection for this domain name.

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 : 2023-08-17 14:54:51

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 protection > DDoS protection** 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;

Set up L3/4 DDoS protection level

 By adjusting the DDoS protection level, you can adjust the processing method for suspected traffic. Please configure the protection level according to the specific protection scenario

- Level
- ☐ **Strict**
Block all suspected attack packets
 - ☒ **Moderate**
Intercept attack packets with obvious characteristics
 - ☐ **Loose**
Only intercept packets that are clearly attacking

OK

Cancel

Exclusive DDoS Traffic Alarm

Last updated : 2023-10-13 14:16:11

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 protection > notification push, and enter the notification push details page.
3. In the DDoS attack traffic alert card, click on the setting.
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.

Default alarm threshold **100Mbps** [Edit](#)

You can select multiple items to batch edit

All service types ▼

Enter a site n

<input type="checkbox"/> Resource	Service type	On/Off	Custom threshold
<input type="checkbox"/> 	Security acceleration	<input checked="" type="checkbox"/>	20000Mbps Edit
<input type="checkbox"/> 	L4 proxy	<input checked="" type="checkbox"/>	20000Mbps Edit

Total items: 2

20 ▼ / page

1 / 1

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 : 2023-08-17 14:57:55

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. Default platform protection and L7 site exclusive DDoS protection do not support configuration;
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 Protection > DDoS Protection** 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.

**IP blocklist/allowlist**

Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.

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 Protection > DDoS Protection 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.

**IP blocklist/allowlist**

Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.

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 : 2023-08-17 14:58:55

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 Protection > DDoS Protection** 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.



Regional blocking

Block requests to access EdgeOne from IP addresses in specified regions.

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.

Regional blocking

On/Off



Blocklist

Save

Asia (excluding Mainland China) ✕

Europe ✕

Africa ✕

Oceania ✕

South America ✕

Country/Region

☐ Chinese mainland

☒ Asia (excluding Mainland China)

All

☒ Europe

All

☒ Africa

All

☒ Oceania

All

☒ South America

All

☒ North America

All

A ☒ Anguilla

☒ Antigua and Barbuda

☒ Aruba

B ☒ Bahamas

☒ Barbados

☒ Belize

☒ Bermuda

☒ Bonaire, Sint Eustatius and Saba

C ☒ Canada

☒ Cayman Islands

☒ Costa Rica

☒ Cuba

☒ Curaçao

D ☒ Dominica

☒ Dominican Republic

E ☒ El Salvador

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

Configuration Port Filtering

Last updated : 2023-08-17 14:59:33

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 protection > DDoS protection** 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.



Port filtering

Block or allow traffic to EdgeOne by specifying the source and destination port range.

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**.

Port filtering

Create

Protocol	Source port range	Destination port range
TCP	1-65535	1-65535
TCP	110-155	110-155
Total items: 2		10 ▼ / page

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 : 2023-08-17 15:00:10

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.

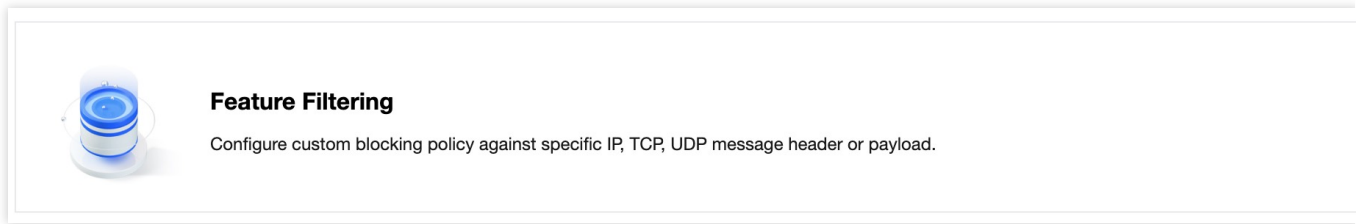
Directions

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 Protection > DDoS Protection** 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**.

Create feature filtering rule

Filter feature

Field	Logic	Value	Other p
Packet data length ▼	between ▼	512	1500
Add			

Protocol

☒ TCP
 ☐ UDP
 ☐ ALL

Action

☒ Block
 ☐ Allow
 ☐ Discard and block
 ☐ Continue protection

OK

Cancel

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 packag. Supports input of numbers in the range of 1-1500. Supports logical equal or between.	
IP Header Start Detection	Supports regex matching or 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. Check depth: The content of the data body (payload) to be matched, needs to enter a hexadecimal string starting with 0x
TCP/UDP Header Start Detection	Supports regex matching or 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 regex matching or keyword matching, where keywords are matched by offset and check depth.	

Configuration Protocol Blocking Rule

Last updated : 2023-08-17 15:08:40

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 protection > DDoS protection** 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.

**Protocol blocking**

Block requests of the specified protocol according to the traffic to EdgeOne. If your application does not use UDP, it's recommended to block all I

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.

Protocol blocking**Block ICMP protocol****Block TCP protocol****Block UDP protocol**

Configuration Connections Attack Protection

Last updated : 2023-08-17 15:10:11

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 protection > DDoS protection** 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.

**Connection attack protection**

Set refined protection policies targeting connection attacks

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.

Custom rule

Last updated : 2024-05-28 14:03:42

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:

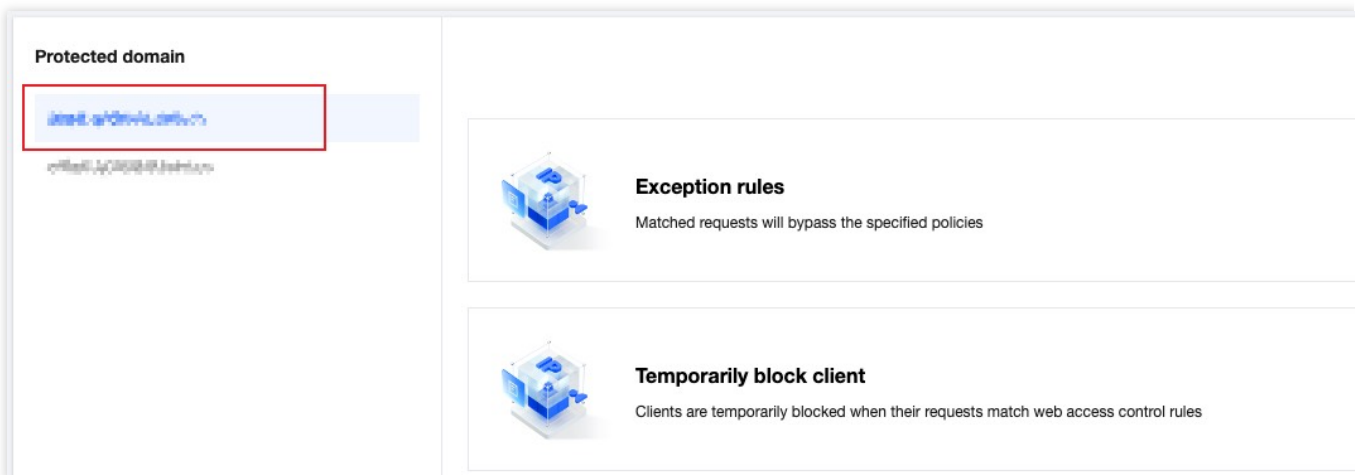
1. Rules within Basic access control: when a request matches multiple rules, the actions will be executed in the following order: Observe > Block.
2. Precise matching rules will be executed from high to low priority (Priority Value from small to large);
3. For the priority order of Custom rules and other Web Protection capabilities, please refer to: [Web Protection Request Processing Order](#).

Basic Access Control

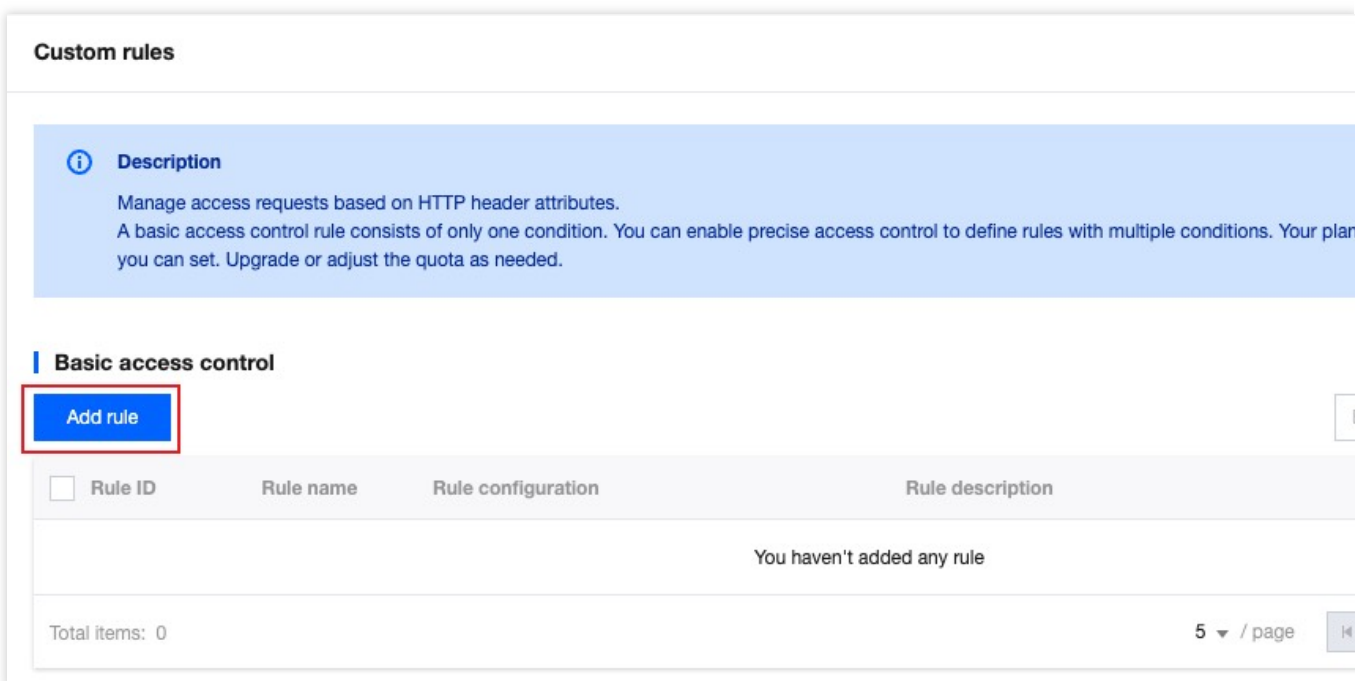
Example Scenario 1: Only allow access from specific countries/regions

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. On the site details page, click on **Security > Web Protection**, and enter the Web Protection details page on the left side of the protection domain list, and select the domain name to be protected.



3. Find the custom rule card and click on the settings. Enter the custom rule page and click on the add rule in basic access control.



4. In the new basic control rule interface, fill in the rule name, and configure the rule type, matching method, and matching content. The rule type is the matching condition, and the requests matching this rule type will be processed according to the configured action.

In this scenario, you can choose the rule type as region control, the matching method as Client IP region Contain, the matching content as Chinese mainland (all), and the action as Block.

Add basic access control rule ✕

Rule name

test

Rule type

Regional control ▼

Manage access requests based on client IP location

Enable rule

☒

Matching method

Client IP location contains ▼

Content

Chinese mainland ✕ Clear

Action

Block ▼

When the request is blocked, an error code and error page will be returned.

OK

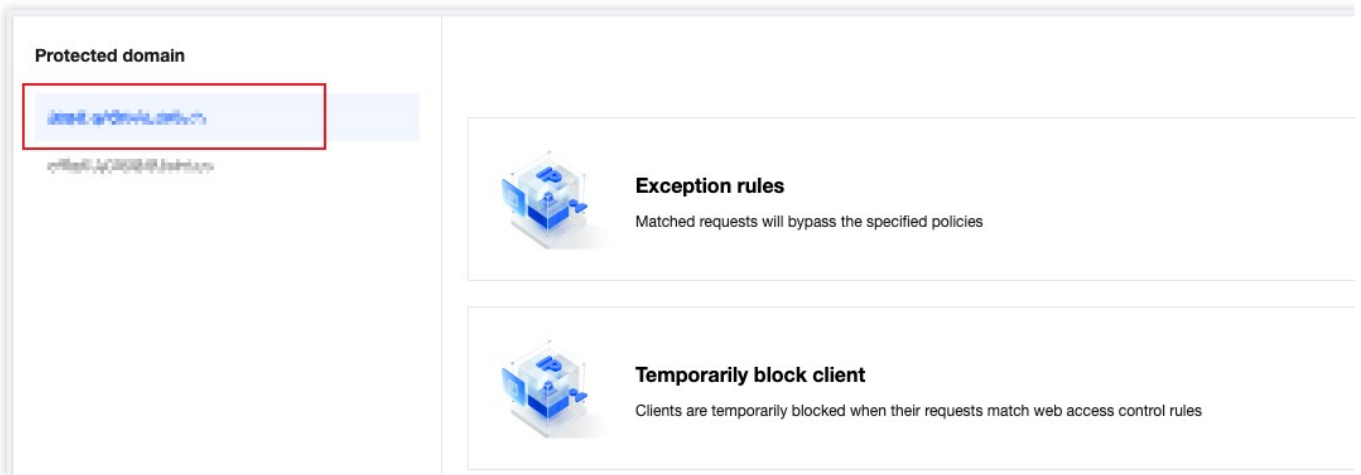
Cancel

5. After clicking confirm, the rule will be deployed and take effect. At this time, if the client access IP is a Chinese mainland user, they will not be allowed to access the website.

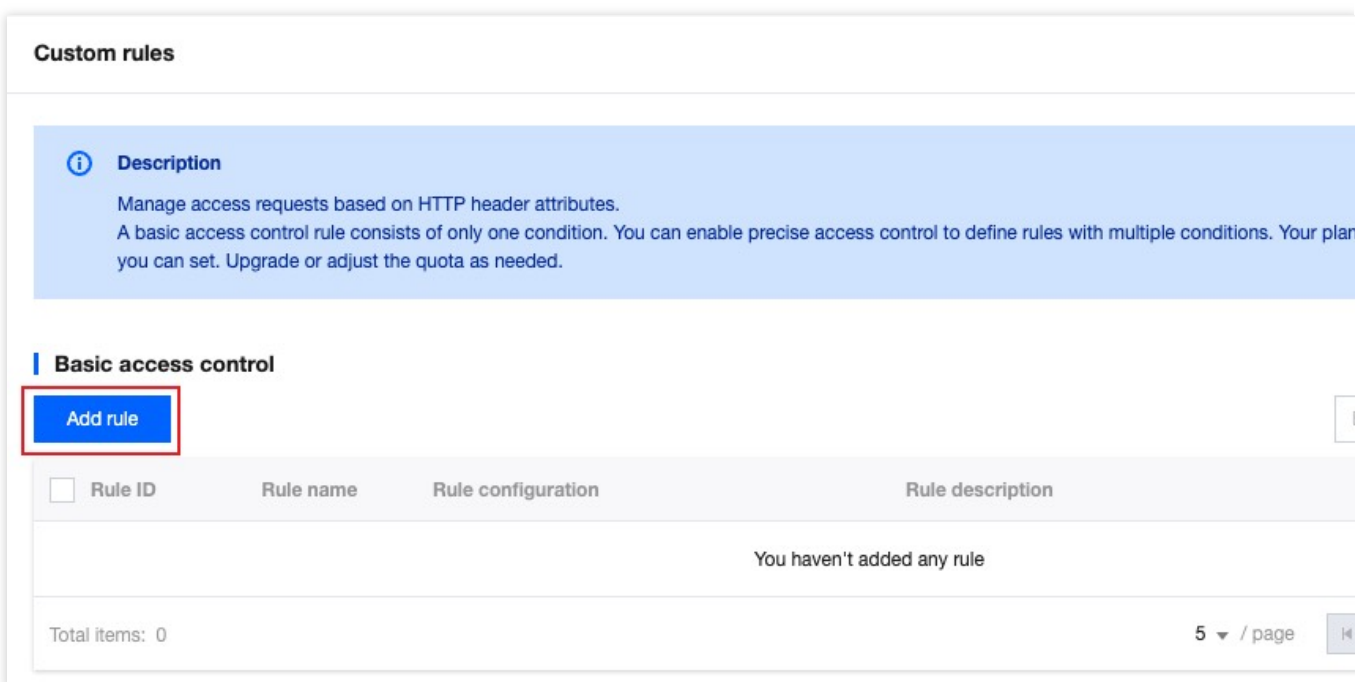
Example Scenario 2: Configure Referrer to control external site access

To prevent unauthorized site access and hotlinking, you can use the Referrer control rule in basic access control to block access requests with unauthorized Referrer headers. For example, the domain name `www.myexample.com` needs to allow access requests linked through the advertising partner `ads.example.com`, while denying access to content linked through other sites. 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. On the site details page, click on **Security > Web Protection**, and enter the Web Protection details page on the left side of the protection domain list, and select the domain name to be protected.



3. Find the custom rule card and click on the settings. Enter the custom rule page and click on the add rule in basic access control.



4. In the new basic control rule interface, fill in the rule name, and configure the rule type, matching method, and matching content. The rule type is the matching condition, and the requests matching this rule type will be processed according to the configured action.

In this scenario, you can choose the rule type as Referer control, when the request Referer does not equal to include: `www.myexample.com` , `ads.example.com` , the action is Block.

Add basic access control rule ✕

Rule name

test

Rule type

Referer control ▼

Manage access requests based on Referer

Enable rule

☒

Matching method

Referer does not equal ▼

Content

www.myexample.com ✕

ads.example.com ✕

Action

Block ▼

When the request is blocked, an error code and error page will be returned.

OK

Cancel

5. After clicking confirm, the rule will be deployed and take effect.

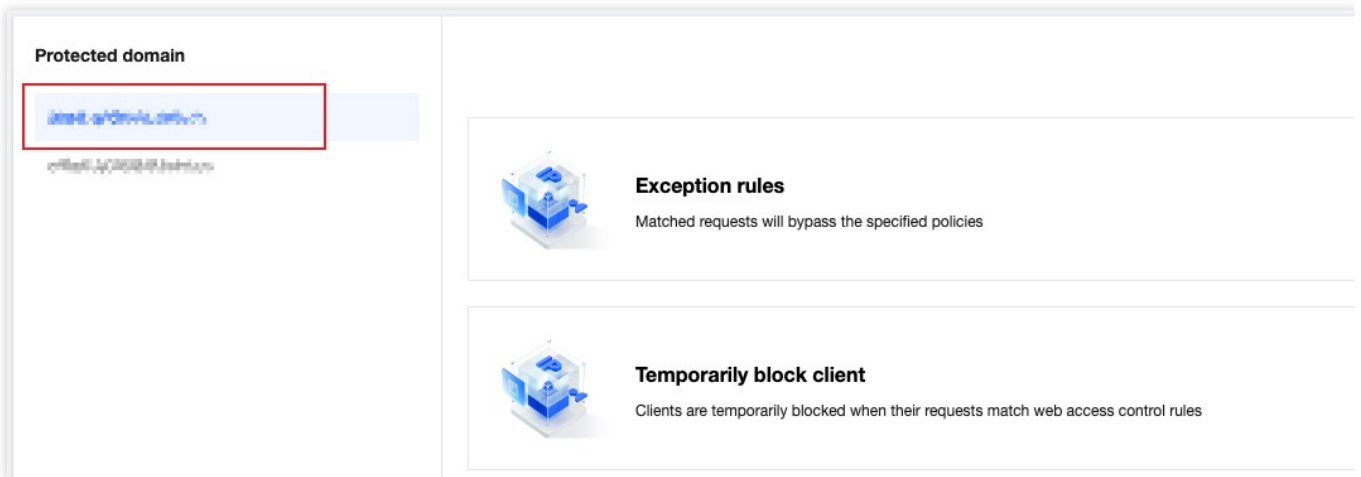
Precise Matching Rules

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

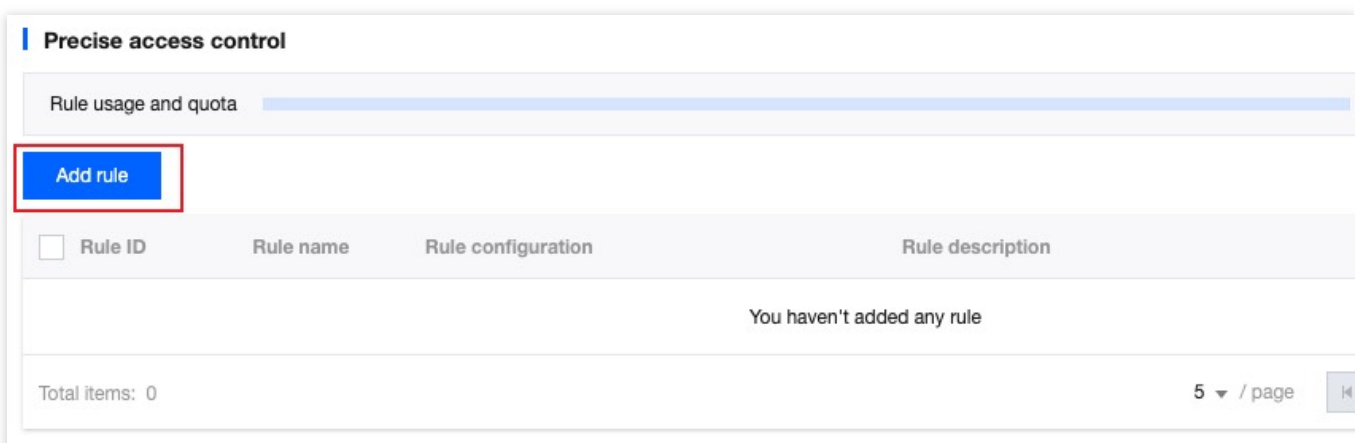
If you need to control the exposure surface of sensitive resources (such as the background management page) on the site and only allow access from specific clients or specified networks. You can use the client IP matching and request URL matching combination in precise matching rules to achieve this.

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. On the site details page, click on **Security protection > Web Protection**, and enter the Web Protection details page on the left side of the protection domain list, and select the domain name to be protected.



3. Find the custom rule card and click on the settings. Enter the custom rule page and click on the add rule in precise matching policy.



4. In the new custom protection rule interface, fill in the rule name, and configure the matching field and perform action.

In this scenario, you can configure the matching field as the request path (Path) equal to `/adminconfig/login` and the client IP not matched `1.1.1.1` user, and the perform action as Block.

Note :

Click on more configuration to modify the priority of this rule. The lower the value, the higher the priority.

Edit custom protection rule

Rule name

Specify scope

Define conditions for the rule to match requests

Field	Condition	Content
<input type="text" value="Request path"/>	<input type="text" value="Is"/>	<input type="text" value="/adminconfig/login"/>
<input type="text" value="Client IP"/>	<input type="text" value="Not matched"/>	<input type="text" value="1.1.1.1"/>

+ And

Action

Perform the specified action when the rule applies.

Action

Priority

When a request matches multiple rules, the action of the rule with the higher priority is performed first.

[protection request processing order](#)

OK

Cancel

5. After clicking confirm, 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 client IP

Request client IP (priority matching XFF header)

Custom request header

Request URL

Request Referer header

Request User-Agent header

Request path (Path)

Request method (Method)

Request Cookie

XFF extended header

Network layer protocol

Application layer protocol

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 Redirect Return custom error pages ^{p.s.} JavaScript challenge
--	---

Note :

p.s. :

If you want to customize the response request page and status code, custom rules support the following configuration methods:

Use the return custom error pages action: You can configure the return custom error pages action for a single custom rule (only support precise matching rules). When EdgeOne responds to requests that match this rule, it will return the specified page and status code.

Use custom error pages: You can use custom error pages configuration to specify the page and status code used by all custom rules when intercepting requests.

Rate Limiting

CC attack defense

Last updated : 2024-04-16 16:30:16

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 CC Attack Protection

CC attack protection 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:

High-frequency access request restriction: 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.

Configuring High-frequency Access Request Restriction

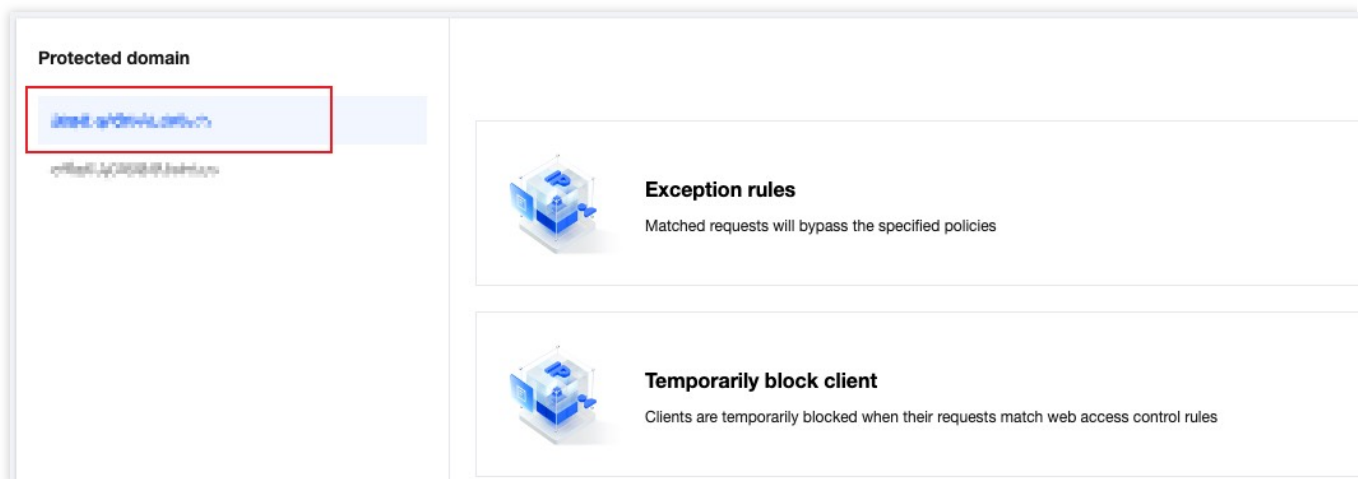
The high-frequency access request limiting rule calculates the request rate of the current domain based on the configured limitation level, establishes a rate baseline (the rate baseline is updated every 24 hours) based on the requests in the last 7 days, and combines the configured limitation level to limit the request rate of a single client accessing the domain.

Note :

High-frequency access request restriction is suitable for Web-based businesses. When the site also provides API interface services, in order to prevent normal requests with higher frequency from being intercepted, it is suggested to configure [exception rules](#) for API interfaces that need to support high-frequency access, skip the CC attack protection module, and limit the API interface exposure through [rate limiting](#) configuration to avoid using moderate, attack emergency, and strict restriction levels.

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. On the site details page, click **Security > Web protection**, enter the detail page of Web Protection, and in the domain list on the left side, select the domain that needs to enable protection.



3. Find the CC attack protection card and click on setting. Enter the CC attack protection Configuration page, and click on the edit button next to the high-frequency Access request limiting.
4. Configure the limiting level and action for high-frequency Access request limiting, with descriptions for each limiting level as follows:

Limitation Type	Limitation Level	Applicable Scenarios	Rate Limitation	Initial Rate Limiting
Adaptive	Loose (Default Configuration, Suggested)	Applicable to most Web business scenarios.	No limitation At least 7000 times/minute	2000 times/5 seconds

	Moderate	Applicable to business scenarios with simpler page content and less dynamic data or dynamic loading content.	1200-2400 times/minute	200 times/10 seconds
	Attack Emergency	When an attack occurs, or when other limitation levels' protection causes business impact due to bypass, you can select this limitation level for emergency protection. Since the rate limiting of this level is relatively strict, there may be false intercepted risks, and it is not recommended for long-term usage.	60-1200 times/minute	40 times/10 seconds

Note :

The action supports observation and JavaScript challenge methods. For more information on different action methods, see [action](#).

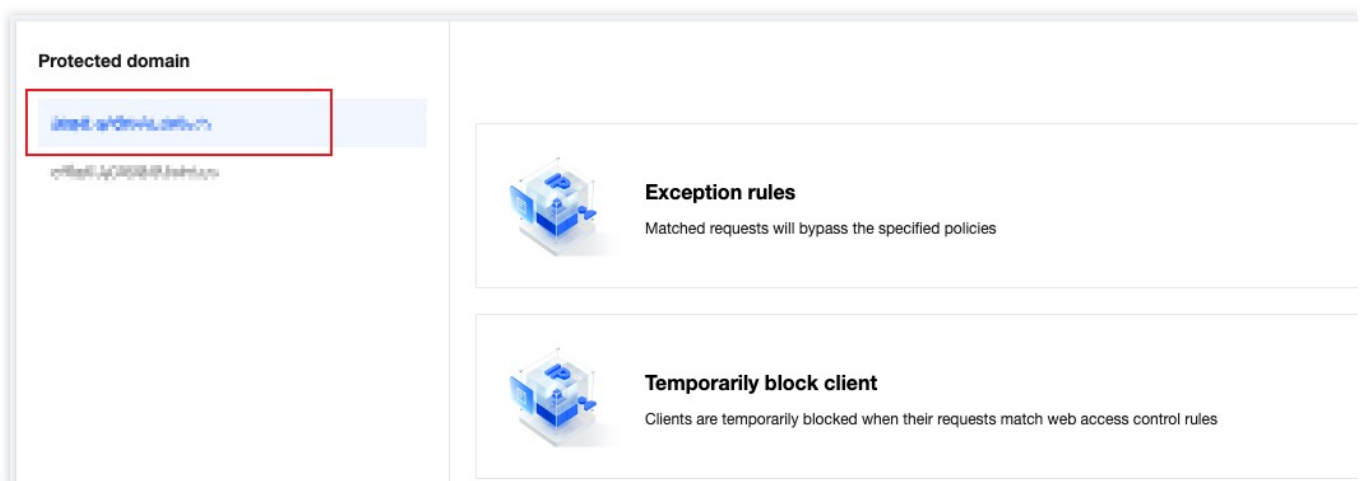
5. Click save to complete the rule configuration.

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. On the site details page, click on **security > Web Protection** to enter the Web Protection details page. On the left side of the page, select the domain that needs to be protected from the domain list.



3. Find the CC attack protection card and click on the setting. Enter the CC attack protection configuration page and click on the edit button on the right side of the slow attack protection.

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.

Edit CC attack defense rule

Rule type	Slow attack defense
Rule description	Mitigate slow attacks by setting timeout and minimum data rate for receiving requests.
Action	<div>Block</div>
Matching method	<div><input checked="" type="checkbox"/> Transfer timeout</div> <div>Apply the corresponding action when EdgeOne does not receive the first 8 KB of the client HTTP body</div> <div>Timeout: <div><div>—</div><div>5</div><div>+</div></div> seconds</div> <div><input checked="" type="checkbox"/> Minimum transfer rate</div> <div>Apply the corresponding action when the client HTTP request's transfer rate is less than the minimum</div> <div>Minimum transfer rate: Within <div>60 seconds</div> the average transfer rate is less than <div><div>—</div><div>80</div><div>+</div></div> bps</div>

Save

Cancel

Note :

The action supports observation and JavaScript challenge methods. For more information on different action methods, see [action](#).

5. Click save to complete the rule configuration.

Intelligent CC Protection

Integrating rate baseline learning, header feature statistical analysis, and client IP intelligence, real-time dynamic attack defense rules are generated. Human-machine identification is performed for requests from high-risk clients or carrying high-risk header features. Intelligent client filtering is enabled by default and executes a JavaScript challenge for clients that meet the rules.

Note :

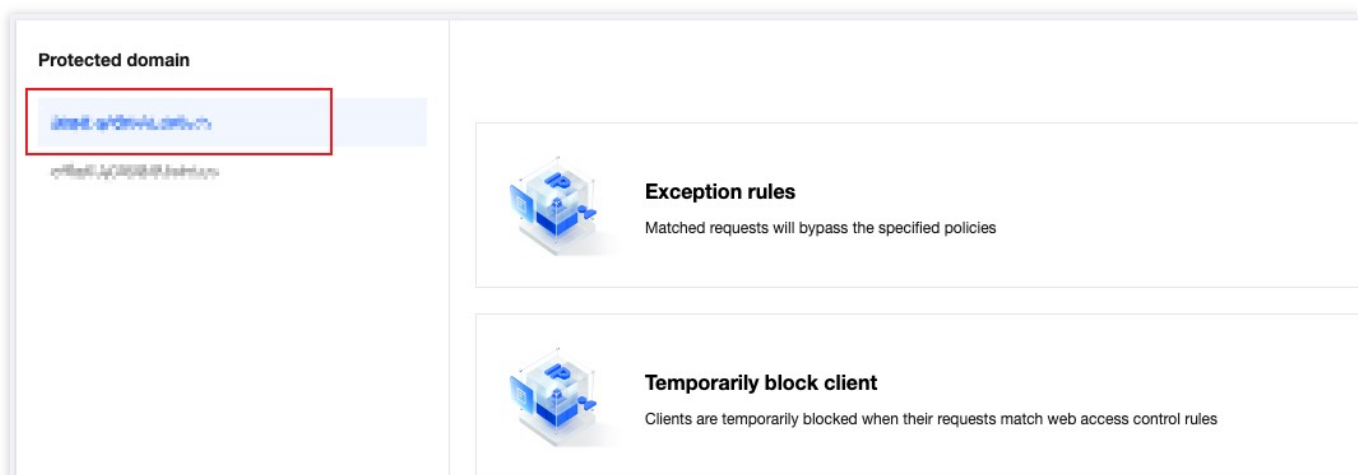
Intelligent client filtering uses the business rate baseline as one of the references. Significant business changes (such as access, cut volume, new business, and new activities) may cause false interceptions. You can temporarily change the action method to observation until the business stabilizes.

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

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. In the site details page, click on **Security > Web Protection** to enter the Web Protection details page. On the left side of the page, select the domain that needs to be protected from the domain list.



3. Find the CC attack protection card and click on the setting. Enter the CC attack protection configuration page and click on the setting protection state button on the right side of the intelligent client filtering.

CC attack defense**Description**

CC attacks generate volumes of forged requests exhausting connections and sessions of your web applications. By protection, you can identify and block malicious requests and increase the resources to be consumed by attackers.

Rule ID	Rule type	Rule configuration
ruleid-123456	Access rate limit	Mode Adaptive - Moderate Action JavaScript Challenge Access rate limit: 318 requests per 60 second(s)
ruleid-789012	Slow attack defense	Mitigation status Not enabled
ruleid-345678	Client filtering	Action JavaScript Challenge

4. Modify the action method for the matching rules, which supports Off (not enabled), observation, and JavaScript challenge. For details on different action methods, please refer to the [action section](#).

Edit CC attack defense rule ✕

Rule type

Client filtering (CC protection)

Rule description

Identify suspicious client requests from normal access requests based on the analysis of request rates and quickly restrict suspicious client requests that match the auto-generated rules.

Sensitivity

Dynamic ▼

Action

JavaScript Challenge ▼

Save

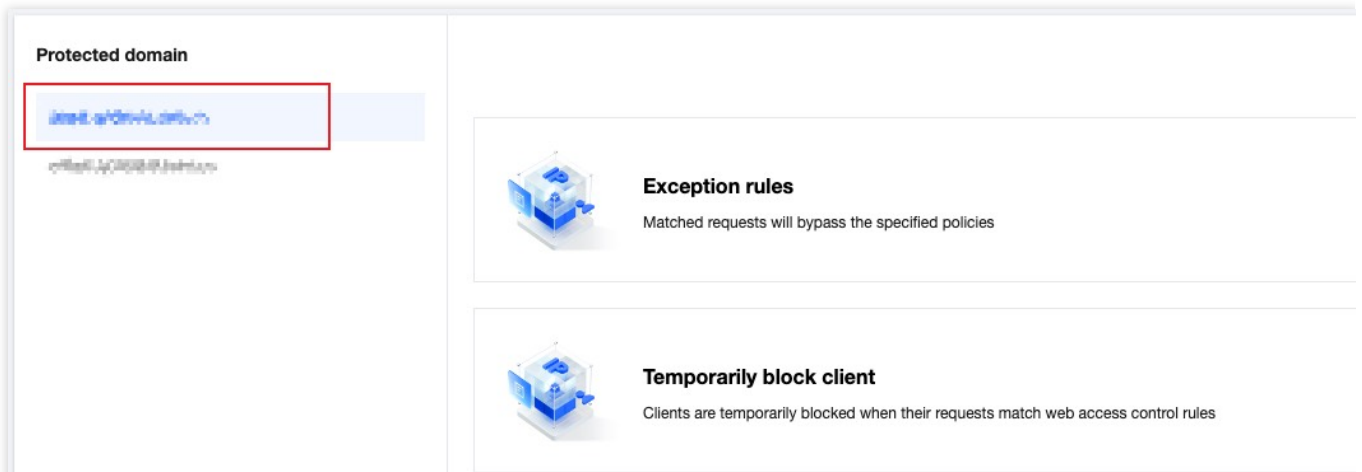
Cancel

5. Click save to complete the rule configuration.

View or release the blocked client list

If you need to view the client list blocked by intelligent client filtering, you can follow these directions:

1. Log in to the [EdgeOne console](#), click on the site list in the left menu bar, and click on the site that needs to be configured to enter the site details page.
2. In the site details page, click on security protection > Web Protection to enter the Web Protection details page. On the left side of the page, select the domain that needs to be protected from the domain list.



3. Find the CC attack protection card and click on the setting. Enter the CC attack protection configuration page and click on the view blocked clients button on the right side of the intelligent client filtering.

CC attack defense

Description

CC attacks generate volumes of forged requests exhausting connections and sessions of your web applications. By protection, you can identify and block malicious requests and increase the resources to be consumed by attackers.

Rule ID	Rule type	Rule configuration
123456789	Access rate limit	<div>Mode Adaptive - Moderate</div> <div>Action JavaScript Challenge</div> <div>Access rate limit: 318 requests per 60 second(s)</div>
987654321	Slow attack defense	<div>Mitigation status Not enabled</div>
567890123	Client filtering	<div>Action JavaScript Challenge</div>

4. In the blocked clients page, click on the add to allowlist button in the operation column to quickly configure the IP as an exception rule.

Custom Rate Limiting Rules

Last updated : 2023-12-18 15:31:41

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:

Accurate matching rules: 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

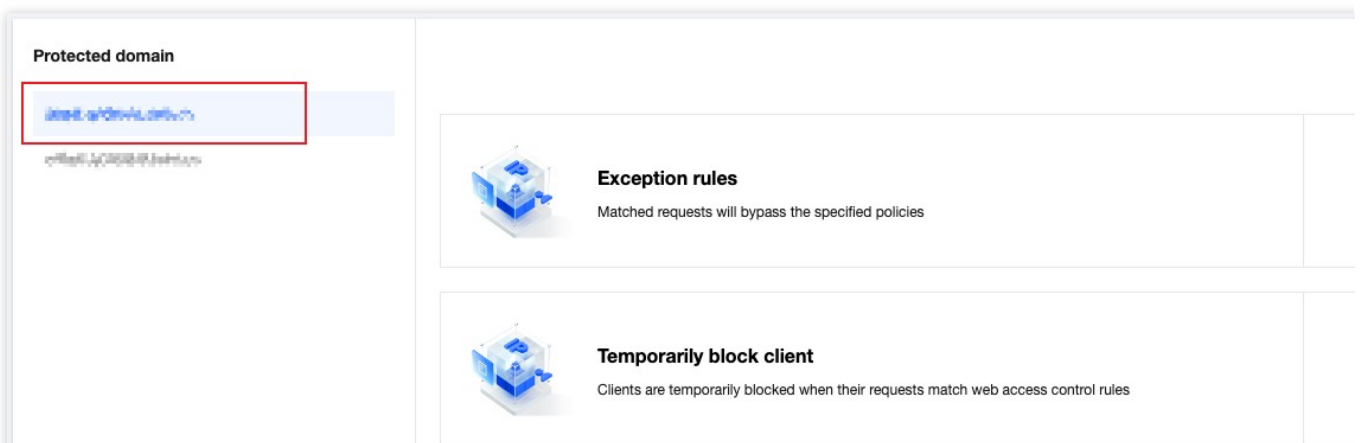
Example Scenario 1: Limit the access frequency of the login API interface to mitigate credential stuffing and brute force cracking attacks

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

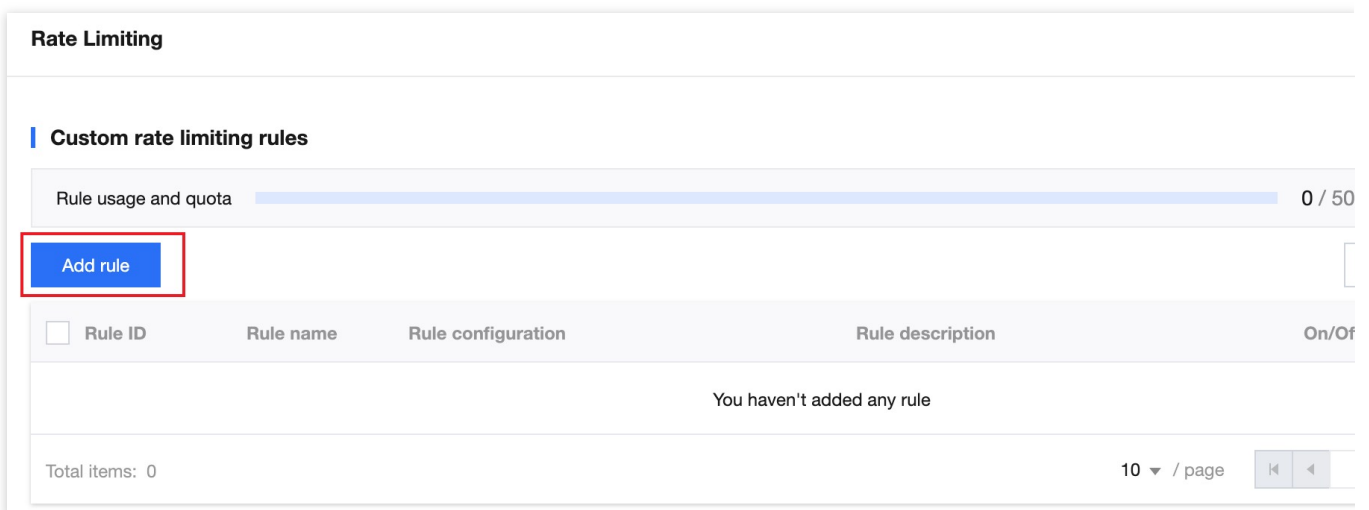
significantly mitigate the attacker's cracking attempts, effectively defend against such attacks, and protect sensitive information from being leaked.

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. In the site details page, click Security Protection > Web Protection to enter the Web Protection details page, and select the domain name to be protected in the left protection domain list.



3. Find the rate limiting card and click Settings. Enter the rate limiting configuration page and click Add Rule in the Accurate Rate Limiting Rules.



4. In the pop-up rule page, configure according to the following steps:
 - 4.1. Fill in the rule name and select the custom protection object for the matching object.
 - 4.2. In the matching condition list option, configure the matching condition of the rule. In this scenario, select the request path equal to `/api/UpdateConfig`.
 - 4.3. Configure the triggering method of this rule. In this scenario, configure the counting period of 60 seconds, and trigger when the count exceeds 100 times. The statistics method is triggered when a single client IP requests to the EdgeOne node, and after triggering, the triggering state is maintained for 10 minutes.

4.4. Select Intercept for the execution action. The complete rule configuration is as follows:

Create rate limiting rule

Rule name

Specify scope

Custom scope

Define conditions for the rule to match requests

Field	Condition	Content
Request path	Is	/api/UpdateConfig

+ And

Trigger rate limiting

Once the rate limit is reached, the corresponding rule action is applied for a period of time

When the number of requests exceeds

100

times

within

60 seconds

More configurations

Method

Based on

Client IP

count

Requests (client to EdgeOne)

Duration

-

10

+

minutes

Action

Perform the specified action when the rule applies.

For matched requests

Block

More configurations

OK

Cancel

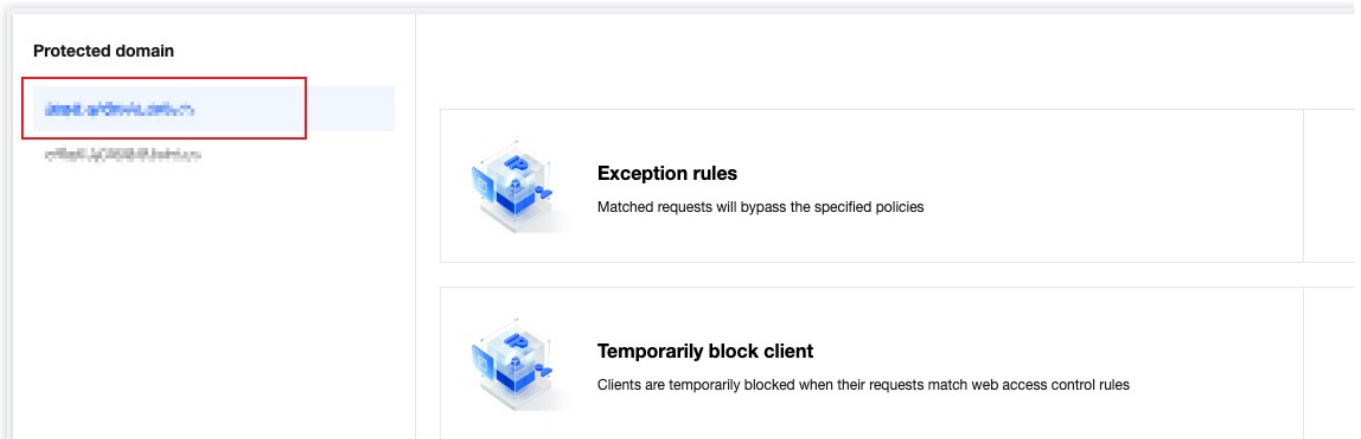
5. After clicking OK, the rule will be deployed and take effect.

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

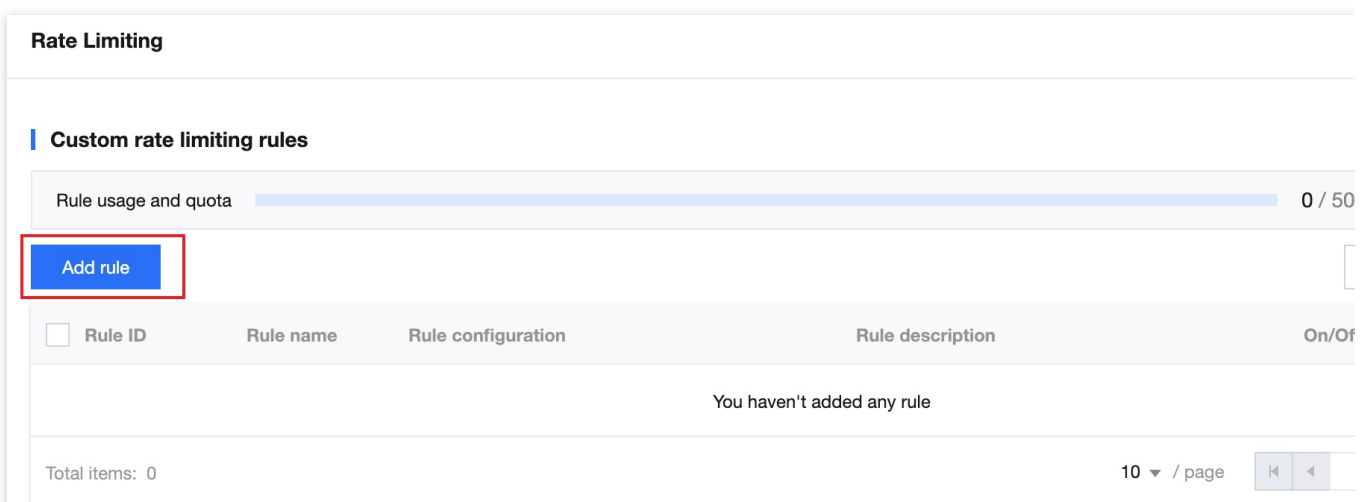
When malicious clients randomly scan site image resources and try to crawl content, they often cause the origin server to respond with a 404 error due to non-existent access paths. By limiting the request rate that causes the origin server's 404 status code, EdgeOne can prevent malicious attackers from 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. In the site details page, click Security Protection > Web Protection to enter the Web Protection details page, and select the domain name to be protected in the left protection domain list.



3. Find the rate limiting card and click Settings. Enter the rate limiting configuration page and click Add Rule in the Accurate Rate Limiting Rules.



4. In the pop-up rule page, configure according to the following steps:
 - 4.1. Fill in the rule name and select the custom protection object for the matching object.
 - 4.2. In the matching condition list option, configure the matching condition of the rule. In this scenario, select the request path (Path) file extension matching content including `.jpg` `.jpeg` `.webp` `.png` `.svg` image static resource types.
 - 4.3. Click +And to add a new matching condition. In the new matching condition, select the HTTP status code equal to 404 requests.

4.4. Configure the triggering method of this rule. In this scenario, configure the counting period of 10 seconds, and trigger when the count exceeds 200 times. The statistics method is based on a single client IP dimension, and is triggered when the origin server responds to the EdgeOne node. After triggering, the triggering state is maintained for 60 seconds.

4.5. Select Intercept for the execution action. The complete configuration rule is as follows:

Create rate limiting rule

Rule name

Specify scope

Custom scope

Define conditions for the rule to match requests

Field	Condition	Content
<input type="text" value="Request path"/>	<input type="text" value="File extension"/>	<input type="text" value=".jpg"/> <input type="text" value=".jpeg"/> <input type="text" value=".webp"/> <input type="text" value=".png"/> <input type="text" value=".svg"/>
<input type="text" value="HTTP status code"/>	<input type="text" value="Is"/>	<input type="text" value="404"/>

+ And

Trigger rate limiting

Once the rate limit is reached, the corresponding rule action is applied for a period of time

When the number of requests exceeds

within

More configurations

Method

Based on

count

Duration

-

+

Action

Perform the specified action when the rule applies.

For matched requests

More configurations

OK

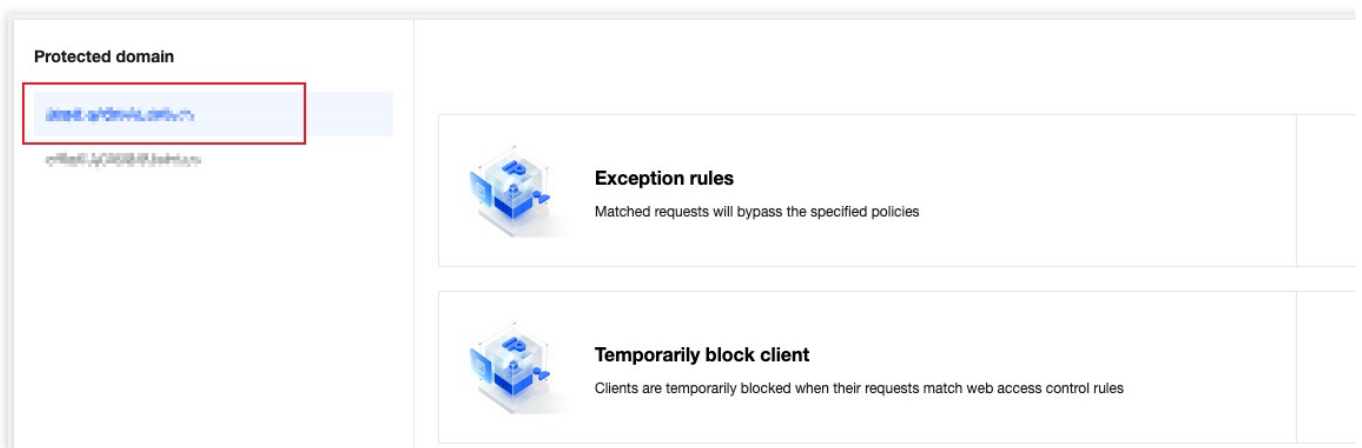
Cancel

5. After clicking OK, the rule will be deployed and take effect.

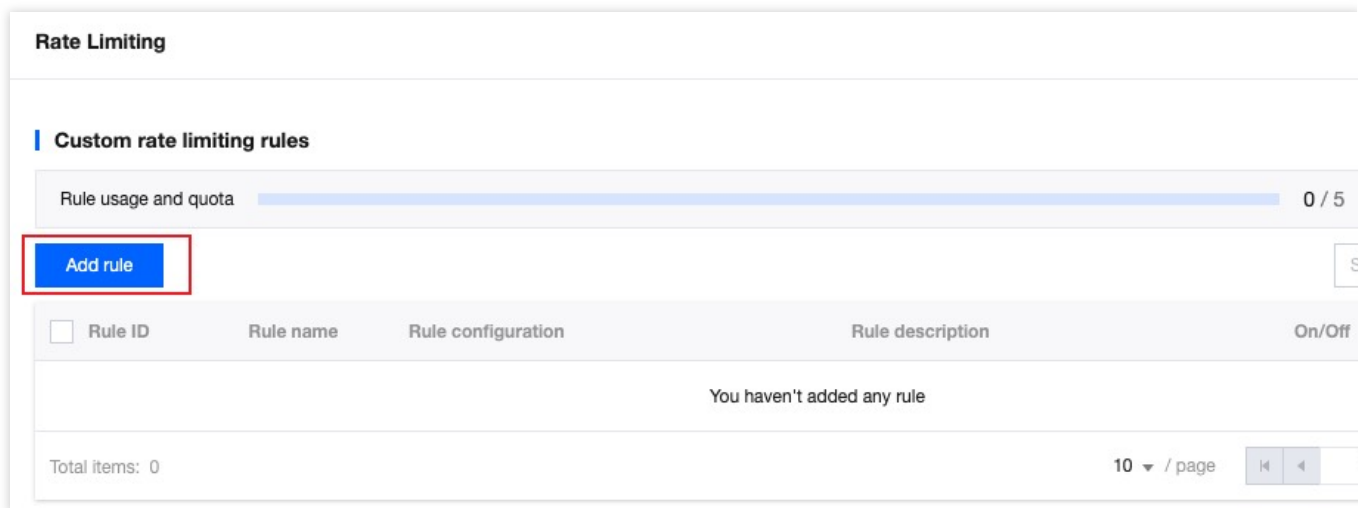
Example Scenario Three: Restricting High-Concurrency Search Engine Crawlers Access to Web Sites to Mitigate Impact on Regular Operations

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. On the site details page, click on Security > Web Protection to navigate to the Web Protection details page. From the list of Protected domain on the left, select the domain for which you wish to enable protection, for instance: `www.example.com`.



3. Locate the Rate Limiting card and click on **Set**. This will navigate you to the Rate Limiting Configuration page. Click on **Add Rule** within the Custom Rate Limit Rules.



4. Within the emergent rule page, configure as per the following steps:

4.1. Enter the rule name, and select the specify object as a **custom scope**.

4.2. Within the selection of matching condition lists, configure the rule's matching conditions. For the current scenario, select the application layer protocol equal to HTTPS as the matching field.

4.3. Configure the trigger method for this rule. In the current scenario, set the request from the client to EdgeOne, where the JA3 fingerprint in the request feature and the User-Agent feature in the HTTP header are identical. Set the count cycle to trigger when the count exceeds 60 times within 30 seconds.

4.5. The selected action to execute is Block. The complete configuration rule is as follows:

Create rate limiting rule

Rule name

Specify scope

Custom scope

Define conditions for the rule to match requests

Field	Condition	Content	
Application layer protocol	Is	HTTPS	
+ And			

Trigger rate limiting

Once the rate limit is reached, the corresponding rule action is applied for a period of time

Requests (client to EdgeOne)

Limiting the rate of requests with the same following feature values

Request feature	Value	
Request's JA3 fingerprint		
HTTP header of specified name	User-Agent	
+ Request feature (Supports up to 5, when there are multiple features, requests are counted as 1 only when all feature values are the same) Free		

The count value is in

30 seconds

Exceeds within

60

times

Trigger action

Action

Perform the specified action when the rule applies.

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](#)

OK

Cancel

5. After clicking **OK**, the rule will be deployed and activated.

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 require a match based on a known, fixed value of an HTTP header, you may configure the match object, specifying the match condition to equal the value of the designated HTTP header parameter.

If your current rate rule require a match based on a category of HTTP headers that may possess identical values, you may configure the statistical dimension, using the designated name of the HTTP header for matching.

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:

When the rate limit threshold is not met, requests will not be processed and logged.

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 action². 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 limited³. It supports a minimum of 1 second and a maximum of 30 days.

Statistical Dimensions

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 dimensions¹:

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 surpasses 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.

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 ReturnCustomPage¹. 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 : 2023-09-21 10:46:44

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. Therefore, 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 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 Protection > Bot Management to enter the Bot Management details page.
3. In the Bot Intelligent Analysis card, click Settings to enter the configuration page. In this scenario, you can configure the [action method](#) for malicious bot requests as JavaScript challenge, and keep the suspicious bot requests and normal bot requests as observation only.

[Use recommended config](#)

Tag	Action
Malicious bot request	JavaScript Challenge
Suspected bot request	Observe
Normal bot request	Observe
Normal request	Allow

[Save](#) [Cancel](#)

4. 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 our 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 : 2024-07-16 16:33:57

Overview

Many public or commercialized programs, including search engine crawlers, have fixed or default User-Agent header features and have specific purposes. Bot 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 Basic bot 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 Management Protection Strategy

For example, your current site `shop.example.com` is an e-commerce website. In order to prevent users from placing orders and snatching purchases through tools, you need to disable the automatic shopping cart bot. You can follow the steps below:

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 Protection > Bot Management** to enter the Bot Management details page.
3. In the Basic Bot Management Settings card, click **Set** to enter the configuration page.



Basic bot 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.

4. Select UA feature rules and click on the detailed rules in the upper right corner.
5. In the detailed rules page, you can modify the [action](#) for a specified rule ID individually; if you need to configure in batches, you can also click Batch Settings, select the rule IDs to be configured in batches, choose the action, and apply.

In this scenario, you can modify the action for the automatic shopping cart robot to **Block**.

▶ 9395241972	Automated Shopping Cart and Sniper Bots	UA feature rules	Block
--------------	---	------------------	-------

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

Client Reputation

Last updated : 2024-04-28 11:09:57

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. In the site details page, click **Security Protection > Bot Management** to enter the Bot Management details page.
3. In the client reputation analysis card, click **Set** to enter the configuration page.
4. Client reputation is divided into network attacks, network proxies, scanners, account takeover attacks, and malicious bots. You can customize the corresponding [action](#) for different types of clients based on the client reputation credibility level.

In the current scenario, dial-up IPs are typical network proxy type clients. When observing that the site receives a high frequency of dispersed IP access, you can intercept higher confidence network proxy clients and set medium confidence clients to observe.

ProxyIP1	Description	There're clients that have suspicious ports opened and have history of malicious behavior including being used in a resource pool for attacks with frequent switching		
	Confidence	Low	Moderate	High
	Action	Not enabled ▾	Observe ▾	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.

Medium 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 : 2023-09-21 10:23:49

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.

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

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. In the site details page, click **security protection > bot management** to enter the bot management details page.
3. In the Active detection card, click **set** to enter the configuration page.
4. Click **Add Rule** and select the matching field. In this scenario, you can select the matching field as the request path regex match `/*`, and the request method is equal to GET.
5. Click **operation**, add an operation; select the operation as Cookie verification and session tracking, and the execution action can refer to: [action](#). Other related configuration instructions are as follows:

Configuration item	Description
Verification method	<p>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.</p> <p>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.).</p>
Check result	<p>For requests that have failed the Cookie verification, the processing can be done according to the check result as follows:</p> <p>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.</p> <p>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,</p>

	<p>and limit the initiation rate of new sessions. When the trigger threshold is exceeded, it will be processed according to the configured action.</p> <p>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.</p>
Session rate and Periodic feature verification	<p>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:</p> <p>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.</p> <p>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.</p> <p>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.</p>

In this scenario, you can configure the verification method to update the Cookie and verify, and configure the trigger threshold to be 300 times in 10 seconds when the check result is no Cookie or expired Cookie, then intercept the request; when there is an invalid cookie request, process it silently. The configuration results are as follows:

IF

Field	Condition	Content
Request method	Is	GET
Request path	Is	/*

[+ And](#)

Operation

Operation	Verification Method	Cookie-based session check
Validate cookie	Update and validate	<input checked="" type="checkbox"/>

Validation result

Validation result	Threshold	Convert
No cookie/Cookie expired	Within 10s greater than 300 times	Block
Invalid cookie		Drop w/o response

[+ Operation](#)

6. Click **Save and Publish** to complete the configuration.

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 to enter the site details page.
2. In the site details page, click **security protection > Bot Management** to enter the Bot Management details page.
3. In the Active detection card, click **set** to enter the configuration page.
4. Click **Add rule** and select the matching field. In this scenario, you can choose the matching field as the request path equals `/account/forgot_password.html`.

5. In the rule configuration page, click **operation**, add an operation; select the operation as Client behavior verification, and refer to the [action](#) for the execution method. The related configuration instructions are as follows:

Note:

Client behavior verification will only inject JavaScript for verification when the response's `Content-Type` is `text/html`, and other requests will be disposed of based on the current verification result.

Configuration item	Description
Proof-of-work verification	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	<p>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.</p> <p>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.</p> <p>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.</p>

In this scenario, you can configure the proof-of-work strength as high, the execution method as delaying 100ms, and allow more than 10 times/10 seconds for clients that have not enabled JS (not completed detection) to Add long latency for the response. Maintain a Drop w/o response mode against client detection timeout and bot clients. The configuration result is shown below:

IF

Field	Condition	Content
Request path	Is	<input type="text" value="/api/password_reset"/> <input type="text" value="/account/forgot_password.html"/>

+ And

Operation	Proof-of-work strength	Delay
Validate client behavior	High	Delay for 100 ms

Validation result	Threshold	Convert
Client not enabled JS	Within 10s <input type="text" value="greater than"/> 10 <input type="text" value="times"/>	Add long latency
Client timed out		Drop w/o response
Bot client		Drop w/o response

+ Operation

6. Click **Save and Publish** to complete the configuration.

Custom Bot Rule

Last updated : 2024-01-02 10:41:28

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 to enter the site details page.
2. On the site details page, click **security protection > Bot management** to enter the Bot management details page.
3. In the custom bot rule card, click **set** to enter the configuration page.
4. Click **Add Rule**, and for the example scenario, you can follow the steps below to configure:

4.1 After filling in the rule name, add the matching condition that the client IP matches the `222.22.22.0/24` IP segment and the `User-Agent` contains `cURL`.

4.2 In the perform action section, select Silent processing as the action. The configured rule is shown below.

Create custom bot rule

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

Specify scope

Define conditions for the rule to match requests

Field	Condition	Content	
Client IP	Match	222.22.22.0/24	✕
User-Agent	Is	cURL	✕

+ And

Action

Perform the specified action when the rule applies.

Action:

+ Add action (Multiple actions are executed based on the assigned weight)

▼ More configurations

OK Cancel

5. Click **OK** to complete the rule configuration and issue.

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 to enter the site details page.
2. On the site details page, click **security protection > Bot management** to enter the Bot management details page.
3. In the custom bot rule card, click **set** to enter the configuration page.
4. Click **Add Rule**, and for the example scenario, you can follow the steps below to configure:
 - 4.1 After filling in the rule name, add the matching condition that the request client reputation equals account takeover IP risk - higher confidence level.
 - 4.2 In the perform action section, first select Managed Challenge as the action, then click Add Action and add the action of Add short latency. Set the weight of Managed Challenge to 20% and the weight of Add short latency to 80%. The configured rule is shown below.

Create custom bot ruleRule name 

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



Specify scope

Define conditions for the rule to match requests

Field	Condition	Content
Client reputation	Is	AccountTakeOverIP1-High confidence 

[+ And](#)**Action**

Perform the specified action when the rule applies.

Action	Weight	
Managed challenge	20%	
Add short latency	80%	

[+ Add action](#)(Multiple actions are executed based on the assigned weight)[▼ More configurations](#)**OK**

Cancel

5. Click confirm to complete the rule configuration and issue.

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.

Managed rules

Last updated : 2024-04-16 16:30:16

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 10KB of the request body. If you subscribe to the Enterprise package and need to scan more request body data, please contact your Tencent Cloud sales rep for expansion.

Note 3: Different plans support different managed rules. For details, see [Comparison of EdgeOne Plans](#).

Optimize Managed Rule Policy

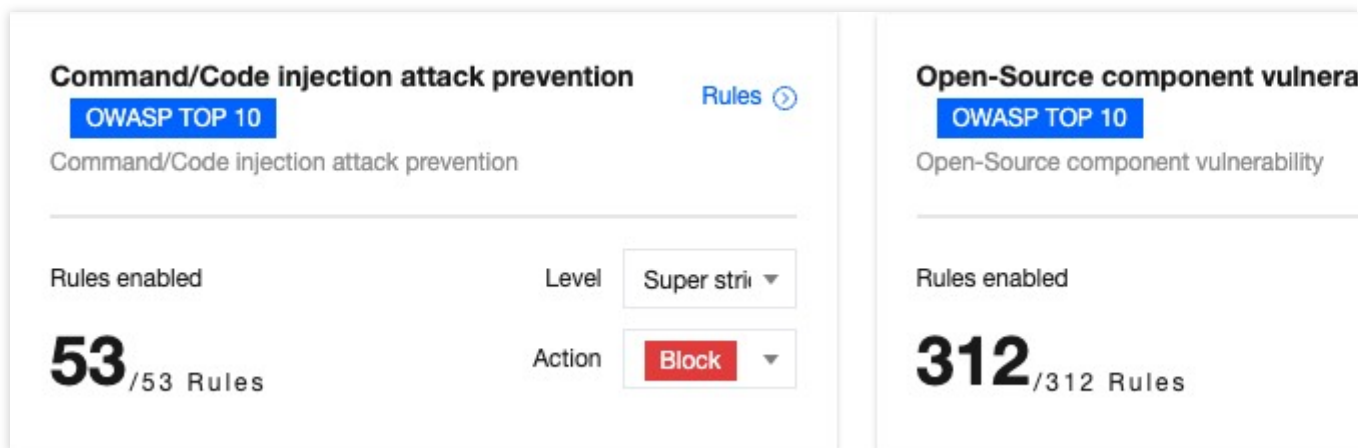
If you need to customize the configuration of protection rule policies according to your actual business situation and protection requirements, you can configure them in the following ways:

Scenario 1: Configure global protection level policy by rule type

According to the rule types divided by managed rules, you can enable interception for all rules in that type according to the protection level. For example, the current domain name [www.example.com](#) often exposes open source component vulnerabilities, and you can intercept all rules within the open source component vulnerabilities and all rules with strict and below protection 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. In the site details page, click **Security Protection > Web Protection**.

3. In the Web Protection details page, select the domain name that needs to be protected from the protection domain list on the left.
4. Find the Managed Rules card and click **Settings**.
5. On the Managed Rules page, find the Open Source Component Vulnerability Rules card, and configure the [Protection Level](#) and [Action](#). Adjust the protection level to Strict and the action to Intercept, then the configuration can be completed.



Scenario 2: Customize optimization protection strategy by single rule

If you need to customize the protection strategy for a single rule, you can optimize the rule by customizing it. For example, the current domain name `www.example.com` has a file upload scenario, and the current protection strategy for file upload attacks is a strict blocking policy. However, normal file uploads are intercepted because the name contains `.exe` extensions, and you want to configure this rule separately for observation and 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. In the site details page, click Security **Protection > Web Protection**.
3. In the Web Protection details page, select the domain name that needs to be protected from the protection domain list on the left.
4. Find the Managed Rules card and click **Settings**.
5. On the Managed Rules page, for example, find the File Upload Attack Protection Rule module and change the protection level to **Custom**.

Non-Compliant protocol

Non-Compliant protocol

Rules enabled: 5 / 5 Rules

Level: Super stri ▼

Action: Block ▼

File upload attack prevention

File upload attack prevention

Rules enabled: 14 / 14 Rules

In custom mode, rule actions need to be cor in

Level: Custom

6. Click the **Detailed Rules** in the upper right corner to enter the Detailed Rules Optimization page, and customize the modification of different rules' **actions**. Select Rule ID: 4401214802's action as Observe, then the configuration can be completed.

Total rules: 14 | [Select all](#)

<input type="checkbox"/>	Rule ID	Rule description	Rule level ▼	Action ▼
<input type="checkbox"/>	4401214785	Block attacks against Tomcat session deserialization vulnerabilities, by intercepting malicio...	loose	Block ▼
<input type="checkbox"/>	4401214260	Prevents the file upload vulnerability in UEditor ASP.NET Edition	normal	Block ▼
<input type="checkbox"/>	4298532437	Prevents file upload attacks by detecting parsing requests using malformed packets to byp...	normal	Block ▼
<input type="checkbox"/>	4401214802	Detects the attributes of sensitive extensions of uploaded files	normal	Observe ▼
<input type="checkbox"/>	4401215200	This rule protects against bypass methods for Tomcat or Spring Webshell uploads.	loose	Block ▼
<input type="checkbox"/>	4401215347		loose	Block ▼
<input type="checkbox"/>	4401215365		strict	Block ▼
<input type="checkbox"/>	4295073822	Prevents file upload attacks by blocking some potentially malicious upload file extensions	strict	Block ▼
<input type="checkbox"/>	4401214803	Prevents file upload attacks by blocking some potentially malicious upload file extensions	normal	Block ▼
<input type="checkbox"/>	4298068457	Prevents the file upload attacks of using multiple "Content-Disposition" lines for bypass	normal	Block ▼

Total items: 14 10 / page 1 / 2 pages

Use Deep Analysis to Automatically Identify Unknown Vulnerabilities

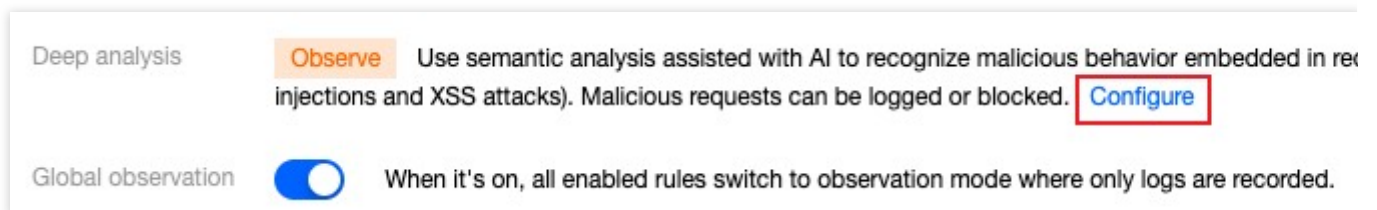
Deep analysis uses advanced semantic analysis technology to deeply understand the intent of SQL and XSS statements. It can not only effectively deal with known attack methods but also has the ability to protect against unknown attacks. This method goes beyond the traditional pattern-matching detection 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:

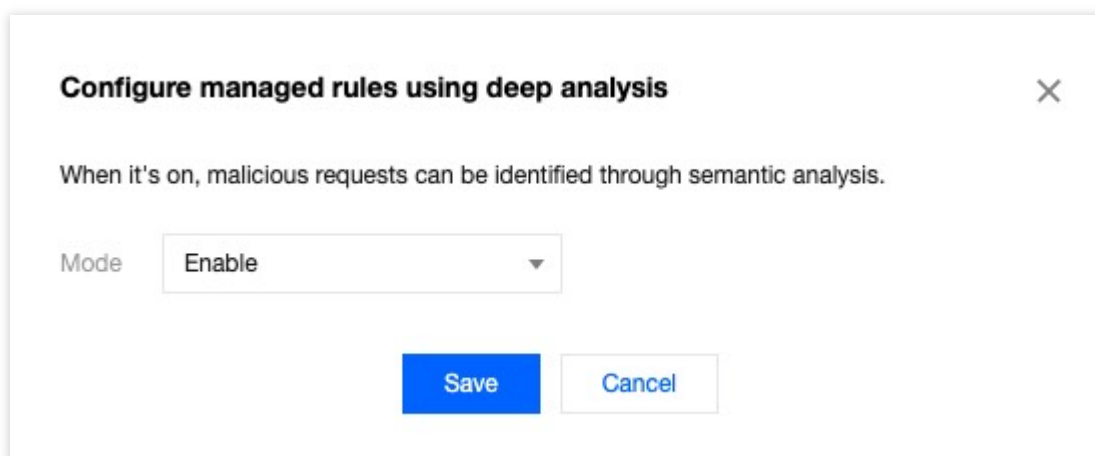
Deep analysis function is only supported by the Standard plan and the Enterprise plan.

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. In the site details page, click **Security Protection > Web Protection**.
3. In the Web Protection details page, select the domain name that needs to be protected from the protection domain list on the left.
4. Find the Managed Rules card and click **Settings**.
5. On the Managed Rules page, click the **configure** of Deep Analysis.



6. 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

Protection Level Description

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.

Exception Rules

Last updated : 2024-01-02 10:48:20

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.

Typical Scenarios and Usage

Exception rules can be used to specify normal requests with specific features to skip scanning of specified modules or specified rules based on existing protection strategies.

Note :

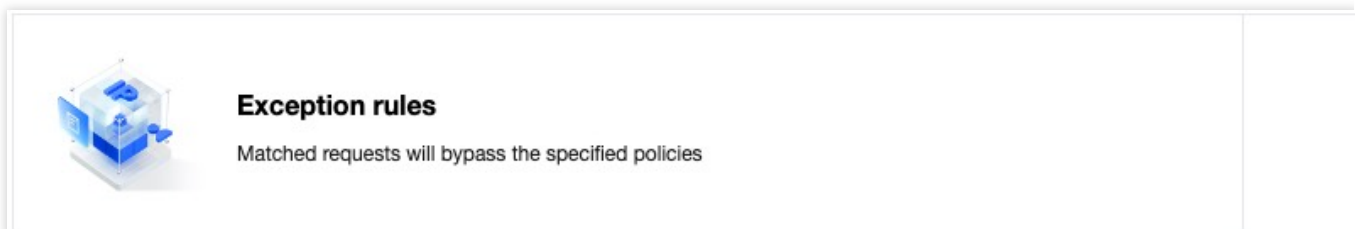
1. Supports skipping custom rules, rate limiting, CC attack defense, and managed rule protection modules.
2. If you need to skip the bot management module, please use Bot Management > Exception Rules or custom bot rules for configuration.

Example Scenario 1: 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. In the site details page, click security protection > Web Protection, enter the Web Protection details page, and select the domain name that needs to be protected in the left protection domain list, such as: `api.example.com` .

3. Find the Exception Rules card and click Settings. Enter the Web Protection Exception Rules list and click Add Rule.



4. In the Create Web Protection Exception Rule pop-up, fill in the rule name and select the exception type as Complete Request Skip Rule.

Create web exception rule

Rule name

Exception type ☒ Full request
The part of the request matched will bypass the security rules you specified

5. Configure the match condition and action. For example, configure the match field as request method equals `POST`, request path equals `/api/EventLogUpload`, and action as specifying the CC attack defense in the security protection module. Multiple match fields can be configured, and multiple simultaneous matches are considered "and" relationships. For a detailed introduction to match conditions, please refer to: [Match Condition](#).

Condition

Field	Parameter	Condition	Content
Request method	Not supported	Is	POST
Request path	Not supported	Is	/api/EventLogUpload

[Add](#)

Action

Skip the execution of

Specified security module

CC attack defense

This will not skip the bot management module

[OK](#) [Cancel](#)

6. Click Confirm to complete the addition of this rule. At this point, the `POST` request for the event log reporting API interface will not be intercepted by the CC attack defense module, avoiding the possibility of false interception due to

high-frequency log reporting, while other interfaces can be normally detected and protected.

Example Scenario 2: 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. In the site details page, click security protection > Web Protection, enter the Web Protection details page, and select the domain name that needs to be protected in the left protection domain list, such as: `api.example.com`.
3. Find the Exception Rules card and click Settings. Enter the Web Protection Exception Rules list and click Add Rule.



Exception rules

Matched requests will bypass the specified policies

4. In the Create Web Protection Exception Rule pop-up, fill in the rule name and select the exception type as Partial Request Field Skip Rule Scanning.

Create web exception rule

Rule name

Exception type ☐ Full request

The part of the request matched will bypass the security rules you specified

☒ Partial request

The full request matched will bypass the security rules you specified

5. Configure the match condition and action. Referring to the example scenario, you can configure the match field as request path equals `/wp/v2/posts`, and the action as specifying all SQL injection attack defense rules in the

managed rule package, not scanning the JSON request content with the specified parameter name equals

`content` , and the parameter value wildcard match is `*` . For a detailed introduction to match conditions, please refer to: [Match Condition](#).

Condition

Field	Parameter	Condition	Content
Request path	Not supported	Is	/wp/v2/posts
Add			

Action

Skip the execution of

Specified managed rules

4401213776, 4401214258, 4294967386, 4401214170, 4294967384, 4401214170

The custom rules, managed rules and bot management rules will not be affected.

Field	Scope	Condition	Content
JSON request	Param name and	Para name equals	content
		Wildcard value matches	*
Add			

6. Click Confirm to complete the addition of this rule. At this point, when the request path equals `/wp/v2/posts` to publish a blog post, the blog content will not be verified by the SQL injection attack defense rule, avoiding normal text content being mistakenly scanned as attack behavior.

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 : 2023-07-28 14:35:46

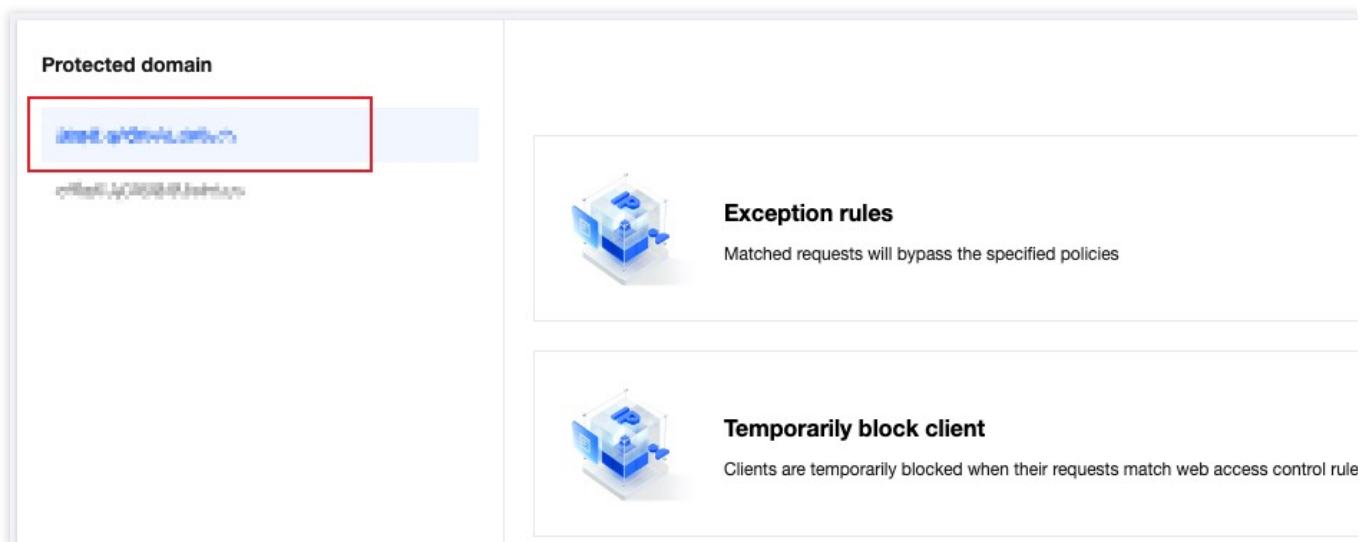
When you use the security expert services provided by EdgeOne (including Activity Guarantee, Emergency Attack and Defense, Security Managed and Customized Rules services), Tencent Security Experts will customize security policies for your business based on the business scenario and attack methods. Managed Custom Policy only provides rule display and does not support console adjustment of matching conditions or action methods. If your business changes or you have special security protection demands, please contact [Tencent Cloud Technical Support](#).

Note :

Custom rules and rate limiting support Managed Custom Rules.

Customized rules will be displayed in the Managed Custom Policy list. If you have already customized Managed rules, you can view them by following these 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 Protection > Web Protection, and in the Web Protection Details page, select the domain that needs to be protected from the left domain list.
3. Find the Custom rule or rate limiting card, click Setting, and you can see the 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

☒

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 Callback URL http://	Delete
<div>Testing Webhook Push</div>		
<div>Add</div>		

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)		<p>Must meet the following requirements:</p> <p>A combination of letters, digits, and underscores;</p> <p>Less than 32 characters;</p> <p>Cannot start with an underscore.</p>
Domain name (Required)		<p>All domains: Includes all domains under this site, including domains added later.</p> <p>Specified domains: Only monitors specific domains under this site.</p> <p>Note:</p> <p>Threshold statistics are only effective for individual domains and will not merge the number of requests within multiple domains.</p>
Metric (Required)		<p>Supports selecting the statistical request range by action or by rule.</p> <p>All action requests: All requests that hit the security module rules and are processed (excluding allowed), are counted in the monitoring rule statistics.</p> <p>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.</p> <p>Only count requests that hit specified rule: Requests that hit specified Web protection or Bot management rules.</p> <p>Note:</p> <p>Allowing will not record logs, so it will not be included in monitoring statistics.</p>
Alarm switch		<p>Controls whether this Web security monitoring rule is effective.</p> <p>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.</p> <p>When the alarm switch is disabled, this Web security monitoring rule will no longer send alarms, including Message Center-related channels and Webhook push.</p> <p>Note:</p> <p>EdgeOne Web security monitoring alarm messages correspond to the "Security Event Notification" type messages in the Message Center.</p>
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.

OK

Cancel

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

©2013-2022 Tencent Cloud. All rights reserved.

Page 113 of 146

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

☒

Alarm setting *

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

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

OK

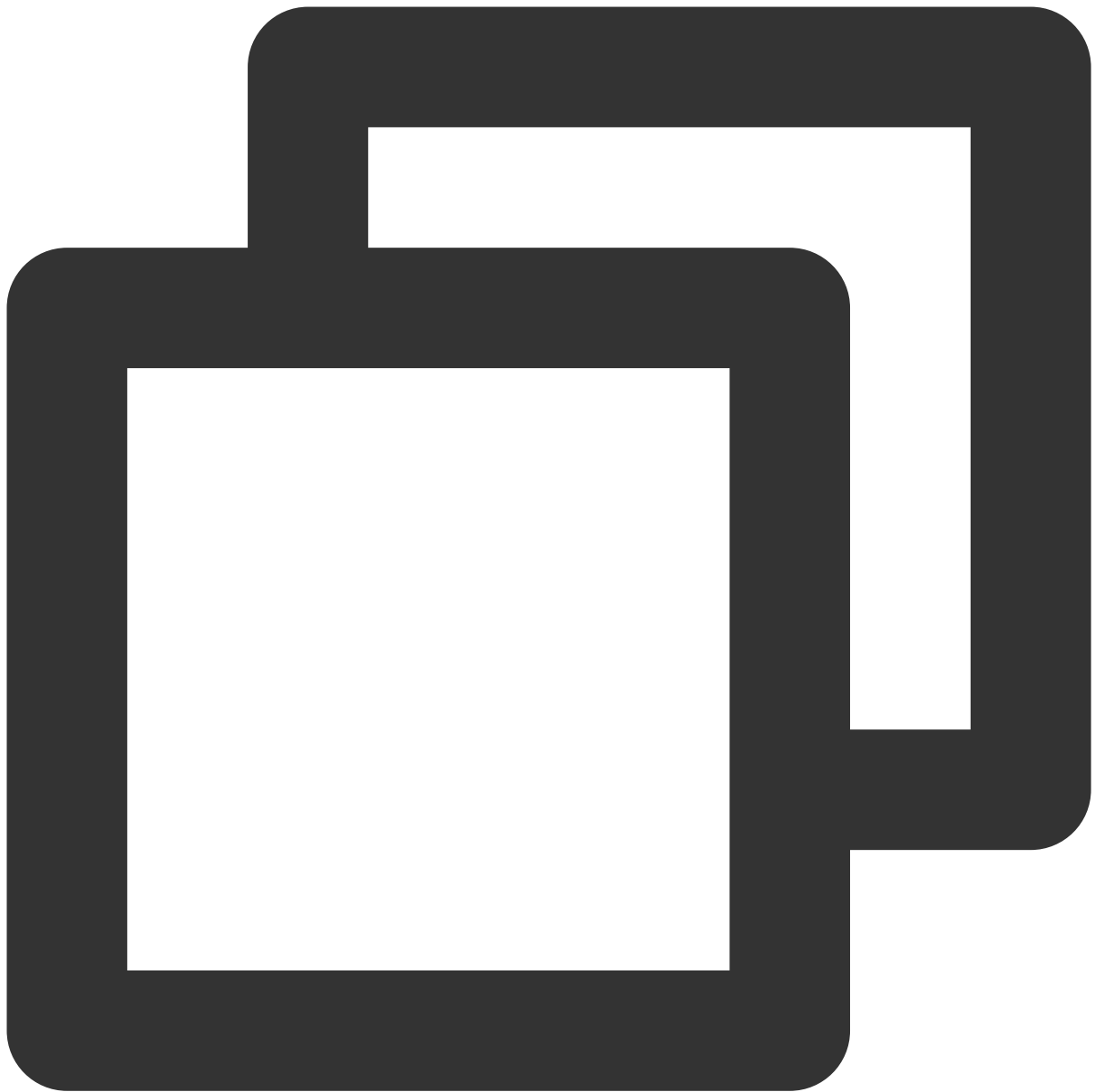
Cancel

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

Refer

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 : 2024-08-19 18:02:03

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.	No longer matches other policies
JSChallenge	Used to identify tool clients that do not support	Respond with an HTTP 302 redirect page, the page carries JavaScript code to verify the	Requests that pass the challenge

	JavaScript, frequently seen in DDoS attack sources.	client browser behavior, and only the visitors that passes the verification can continue to access.	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:

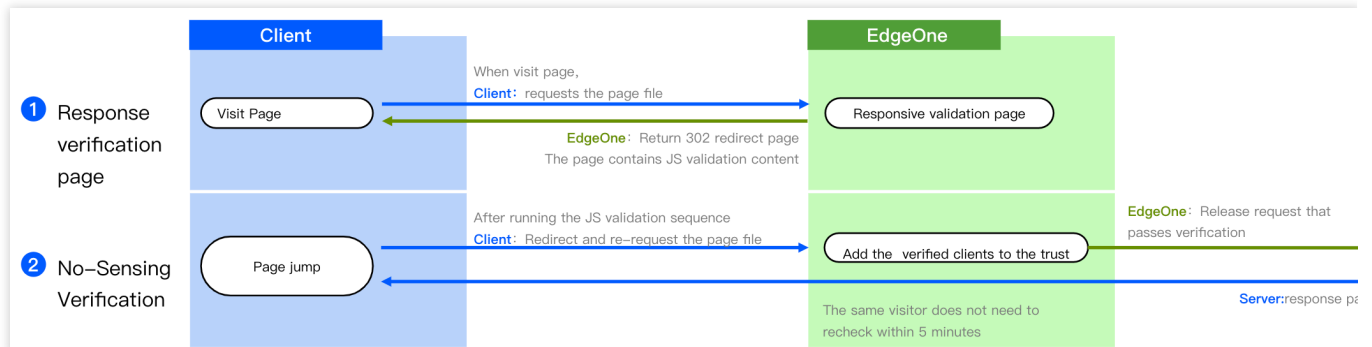
JavaScript Challenge is not suitable for the following scenarios:

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

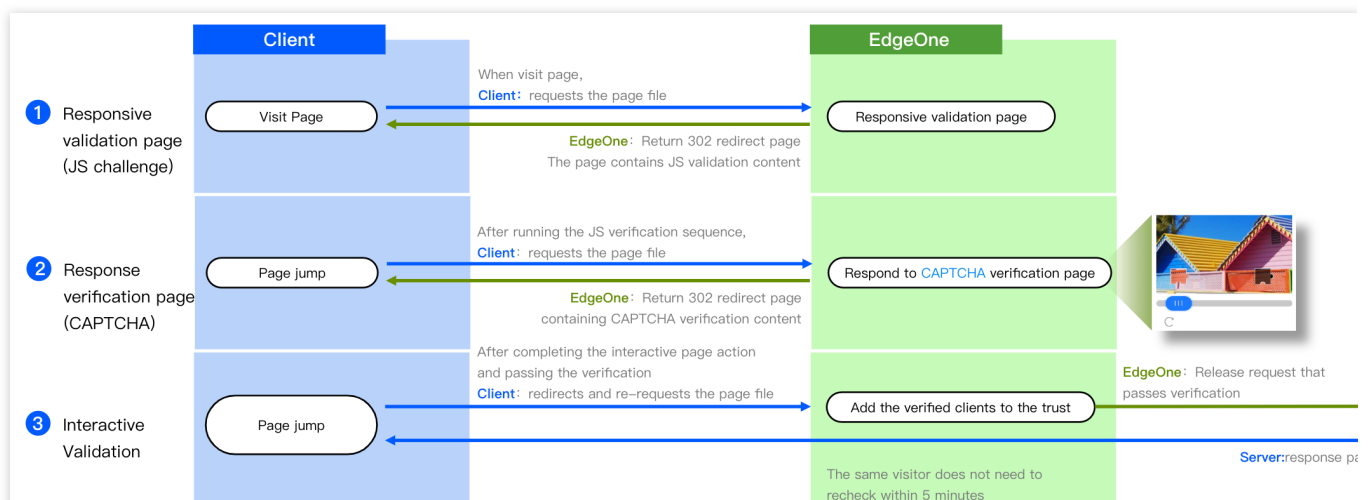


When the security protection policy uses JavaScript Challenge to handle requests, EdgeOne responds with a redirect page (HTTP 302) containing a JavaScript program to verify the browser runtime environment. Upon receiving this response, browsers with JavaScript enabled will execute the verification program and perform an HTTP 302 redirect. Upon 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



When the security protection policy uses Managed 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. Upon 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. Upon receiving the redirect request, the EdgeOne security protection module will allow requests carrying valid identifiers (client IP and User-Agent).

Match Condition

Last updated : 2023-07-28 14:35:46

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 Condition Options and Descriptions

Note:

The matching conditions that can be configured vary depending on the rule type and the EdgeOne plan you subscribe to. For specific support situations, please refer to the corresponding function introduction document.

Matching Condition Options	Matching Condition Description	Standard Plan	Enterprise Plan
Request Client IP	Match the source IPs of the request. Support matching based on region, ASN, IP, and CIDR IP segment. When using IP and CIDR IP segment matching, you can use IP grouping. Up to 8 IP groups can be configured for a single matching condition.	Support	Support
Request Client IP (Priority 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.	Not Support	Support

Custom Request Header	Match the specified request header, and provide additional parameter options to match the header value with a specific name. case-insensitive Support equal, does not equal, contain, does not contain, wildcard match, wildcard does not match, length greater than, length less than, content is empty, does not exist, regex match. Support up to 128 matching values.	Not Support	Support
Request URL	Match the request URL. case-insensitive Support equal, does not equal, contain, does not contain, wildcard match, wildcard does not match, length greater than, length less than, content is empty, does not exist, regex match. Support up to 128 matching values.	Matching condition does not support regex match	Support
Request Source (Referer Header)	Match the Referer header of the request. case-insensitive Support equal, does not equal, contain, does not contain, wildcard match, wildcard does not match, length greater than, length less than, content is empty, does not exist, regex match. Support up to 128 matching values.	Matching condition does not support regex match	Support
Request Content Type (Accept Header)	Match the Accept header of the request. case-insensitive Support equal, does not equal, contain, does not contain, wildcard match, wildcard does not match, length greater than, length less than, content is empty, does not exist, regex match. Support up to 128 matching values.	Not Support	Support
Request Path (Path)	Match the path part of the request URL (excluding query parameters). case-insensitive	Not Support	Support
Request Method (Method)	Match the method of the request. case-insensitive Support multiple selections: GET, POST, HEAD, PUT, DELETE, TRACE, OPTIONS, CONNECT.	Matching condition does not support regex match	Support
Request Cookie	Match the specified request Cookie header parameter value. The parameter name must be specified.	Not Support	Support

	<p>Ignore case.</p> <p>Support equal, does not equal, contain, does not contain, wildcard match, wildcard does not match, length greater than, length less than, content is empty, does not exist, regex match.</p> <p>Support up to 128 matching values.</p>		
XFF Extension Header	<p>Match the XFF (X-Forwarded-For) header of the request.</p> <p>Ignore case.</p> <p>Support equal, does not equal, contain, does not contain, wildcard match, wildcard does not match, length greater than, length less than, content is empty, does not exist, regex match.</p> <p>Support up to 128 matching values.</p>	Not Support	Support
Network Layer Protocol	<p>Match the IP protocol type used by the request.</p> <p>Support multiple selections: IPv4, IPv6.</p>	Not Support	Support
Application Layer Protocol	<p>Match the application layer protocol used by the request.</p> <p>Support multiple selections: HTTP, HTTPS.</p>	Not Support	Support
HTTP Status Code	<p>Match the HTTP status code of the response.</p> <p>Only support rate limiting, support configuration when selecting based on response statistics.</p> <p>Support up to 20 status codes at the same time.</p>	Not Support	Support

Rules Template

Last updated : 2023-08-16 16:54:16

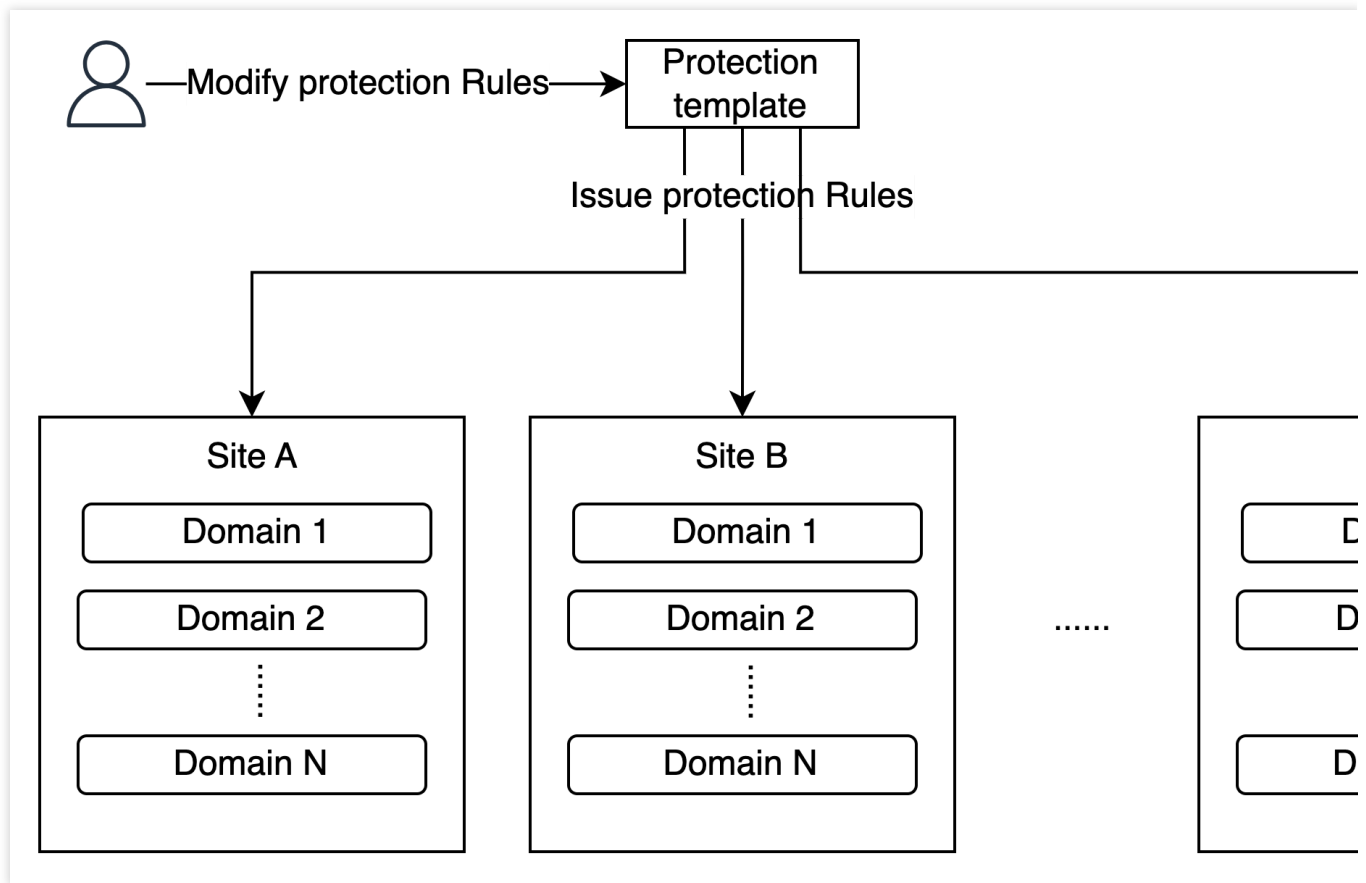
Overview

When you have a large number of domains that need to be connected to EdgeOne Web Protection at the same time, if the protection policies required by the domains are exactly the same, when you need to modify the Web Protection policies, modifying them one by one will bring a large amount of maintenance workload.

EdgeOne's security protection provides you with a policy template function, which allows you to save security policies as templates and apply the template policies to specified domains. You can directly modify the corresponding security protection policies in the template management, and it will take effect on all domains that have applied this template, greatly reducing your operation and maintenance costs.

Note :

1. Policy templates only support [Web Protection policies](#), [Bot management policies](#), and custom error pages.
2. Using policy templates will overwrite the current domain's protection policies, and the current domain's protection policies will be lost.
3. After using the policy template, the temporary client list currently blocked in the [intelligent CC attack defense](#) will be cleared, and the newly added temporary blocked client list will not affect other domains in the policy template.



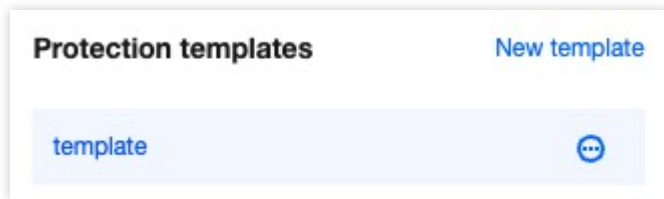
Directions

Binding Protection Template

Scenario 1: Create a new policy template and apply it to specified domains/sites

For example: You currently need to create a new policy template named "template" and apply this policy template to all domains within the site example.com. You can follow the steps below:

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. In the site details page, click on **security protection > Protection templates** to enter the policy template management interface.
3. In the left protection policy template, click on "New template", enter the template name, and press the carriage return key to create a new template.



4. After the creation is complete, click on the template name created in step 3 to enter the template editing page. You can complete the configuration and modification of related rules in this interface. For configuration, please refer to:

[Web Protection](#), [Bot management](#).

5. Apply the configured policy template to the site, supporting the following three application methods:

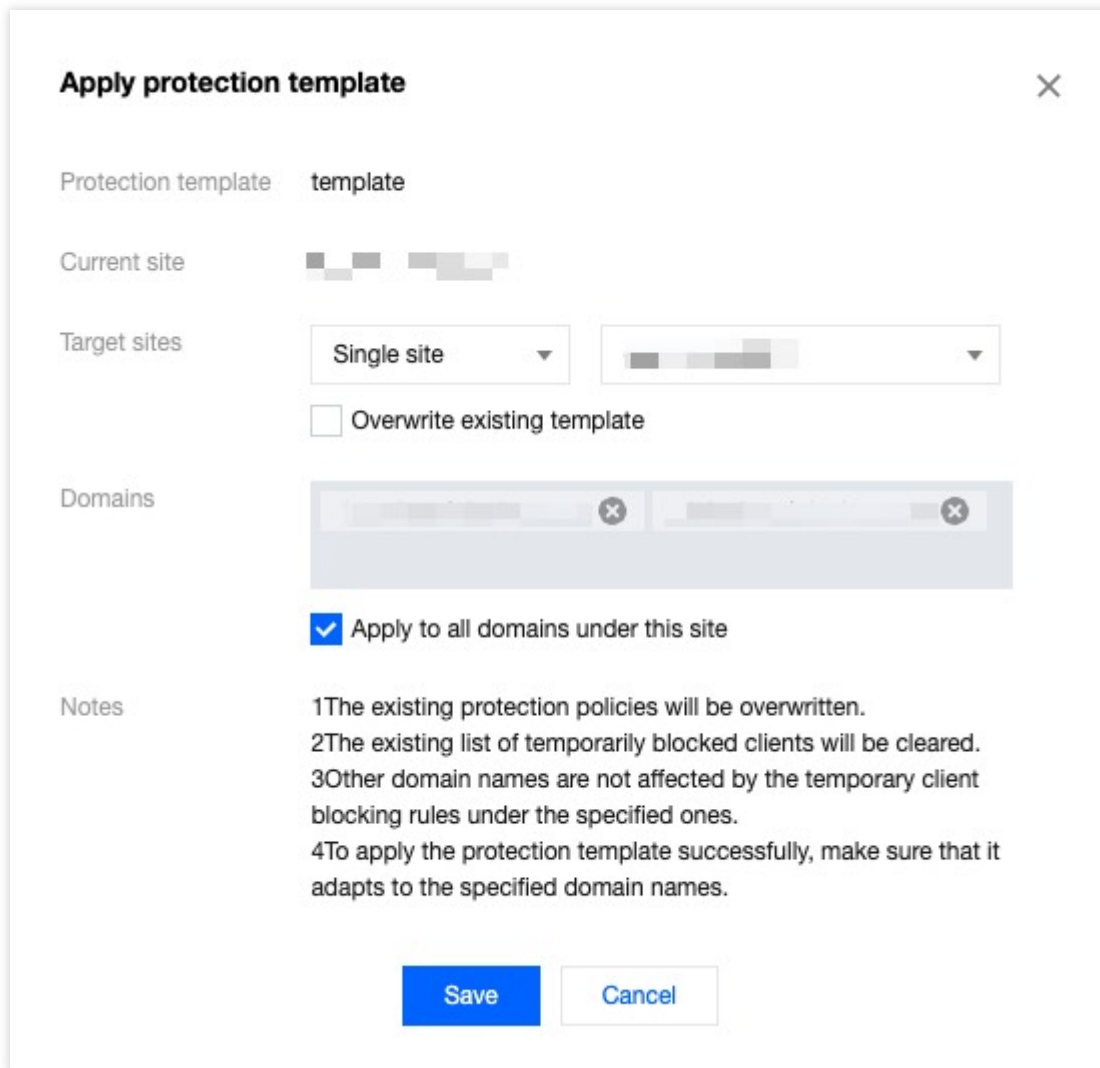
current site: Apply the current policy template to the domain or all domains under the current site;

single sites: Apply the current policy template to the domain or all domains under other specified sites;

multiple sites: Apply the current policy template to multiple specified sites' domains or all domains. When batch applying to sites, wildcard expressions can be used to match domains. For example:

In this scenario, you need to apply this policy template to all domains within `example.com`. You can click on

"Apply to Domains" in the template, select the application method as "Apply to Specified Site", and select the site as `example.com`, check **"Apply to all domains under this site"**, and configure as follows:



The screenshot shows a modal dialog titled "Apply protection template" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Protection template:** A text input field containing the value "template".
- Current site:** A text input field containing a blurred site address.
- Target sites:** A dropdown menu set to "Single site" and a text input field containing a blurred domain name.
- Overwrite existing template:** An unchecked checkbox.
- Domains:** A list of domain names with a close button (X) for each item.
- Apply to all domains under this site:** A checked checkbox.
- Notes:** A text area containing four numbered notes:
 - 1The existing protection policies will be overwritten.
 - 2The existing list of temporarily blocked clients will be cleared.
 - 3Other domain names are not affected by the temporary client blocking rules under the specified ones.
 - 4To apply the protection template successfully, make sure that it adapts to the specified domain names.
- Buttons:** "Save" and "Cancel" buttons at the bottom.

6. Click **save** to complete the policy template application.

Scenario 2: Apply an existing template to newly added domains/sites

For example: You currently have a Web security protection policy template named "template" configured under the site `example.com`, and now a new domain named `www.example.com` has been added under the current site. The Web protection policy of this domain is exactly the same as the template "template". You can quickly apply the current policy template to this domain by using the template policy. You can follow the steps below:

Method 1: Operate in the policy template

Method 2: Operate in the protection configuration

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. In the site details page, click on **security protection > Protection template** to enter the policy template management interface.
3. Select the corresponding protection template, such as "template".

4. Click on "Apply to Domain", in this scenario, you can choose the application method as "Current Site", and select the domain in the domain list as `www.example.com`.

The screenshot shows a modal dialog titled "Apply protection template" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Protection template:** A text field containing the value "template".
- Current site:** A text field containing a blurred domain name.
- Target sites:** A dropdown menu currently showing "Current site".
- Overwrite existing template:** An unchecked checkbox.
- Domains:** A text field containing a list of blurred domain names with a clear button (X) on the right.
- Apply to all domains under this site:** An unchecked checkbox.
- Notes:** A section containing four numbered instructions:
 - 1The existing protection policies will be overwritten.
 - 2The existing list of temporarily blocked clients will be cleared.
 - 3Other domain names are not affected by the temporary client blocking rules under the specified ones.
 - 4To apply the protection template successfully, make sure that it adapts to the specified domain names.

At the bottom of the dialog are two buttons: "Save" (in a blue box) and "Cancel" (in a white box with a blue border).

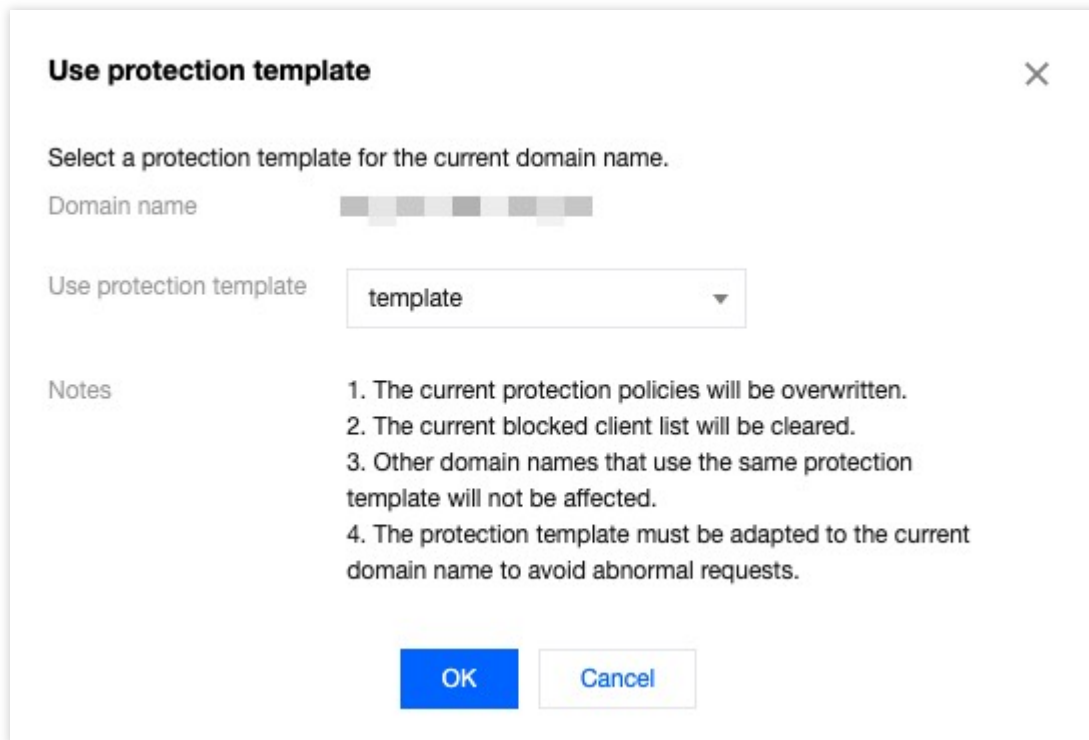
5. Click **save** to complete the policy template application.

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. In the site details page, select the protection module to be configured, for example, click on security **protection > Web Protection** to enter the Web Protection policy configuration page.

3. In the protection domain list, select the domain to be configured, such as: `www.example.com`.

4. Click on "Use Protection Template" in the upper right corner, and select the template policy to be applied, such as: `"template"`.



5. Click OK to complete the template policy application.

Unbinding Protection Template

For example: You currently have a Web protection policy template named " `template` " bound to the domain `www.example.com` under the site `example.com` . If this domain has a personalized protection policy configuration that is different from other domains, you need to add a custom rule while retaining the current security configuration. You need to unbind the corresponding policy template to configure it. You can follow the steps below:

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. In the site details page, select the protection module to be configured, for example, click on security protection > Web Protection to enter the Web Protection policy configuration page.

3. In the left protection domain list, select the domain that needs to unbind the policy template, such as: `www.example.com`.

4. Domains bound to policy templates can only view configurations and cannot be modified. Click on "Remove Policy Template" and support two unbinding operations:

Retain current security policy: After unbinding, retain the security protection policy content configured by the current policy template.

Use empty package security policy: Clear all security policies and reconfigure.

In this scenario, you can choose to retain the current security policy information.



You can't modify the template when it's being used by the current domain name. To make changes, please go to "Protection policies", or edit configuration after unbinding the template. Your changes will be synced to the current domain name.

Protection template: template

[Go to Protection Templates](#)



5. Click confirm to unbind.

IP and IP Segment Grouping

Last updated : 2023-10-13 14:20:45

Function Description

IP/subnet grouping contains IP or CIDR subnet list. You can use this IP/subnet grouping in DDoS protection, Web Protection, and Bot Management rules, or in cross-site similar rules to simplify configuration maintenance operations.

Note :

1. IP/subnet grouping supports cross-site usage. You can use the IP/subnet grouping in other sites directly after creating a new IP/subnet grouping to ensure the consistency of different site policies.
2. Up to 20,000 IP/subnet groupings can be added to the blocklist/allowlist under the same site, with a maximum of 16 IP groupings.

Scenario: Group management of IP information with business threats

Example scenario

A large game customer has connected sites `example.com` and `site.com` . Currently, through the security intelligence library and their own business security, a blocklist of IPs with business threats has been identified. These IP addresses will change dynamically, so they need to be updated in real-time and applied to all site domain names, instantly blocking these IPs.

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. On the site details page, click **Security Protection > General Settings** to enter the configuration option details page.
3. In the IP and subnet grouping card, click **Set**.



IP groups

Allow you to group and manage IP addresses for IP configuration.

4. Click **Create** to create a new group, enter the group name and the IP addresses or IP address segments included in the group, such as: `1.1.1.1/23;1.2.2.2` . Separate multiple addresses with a return.

ID	Group name	List of IP groups	Operations
	IPblacklist	1.1.1.1/23 × 1.2.2.2 ×	Save

Total items: 0 10 / page 1

5. Click **Save** to complete the IP group creation. After the group is created, in this scenario, you need to disable all IP access within the group. You can add Basic access control rules on the **Web Protection > Custom rule** page of `example.com` and `site.com` , respectively. When adding rules, select to block when the **Client IP** is equal to the group name, which will block all IP access within the group and update dynamically based on the IPs included in the group. For detailed configuration steps, refer to [Custom rule](#).

Add basic access control rule ✕

Rule name

Rule type
Manage access requests based on client IP

Enable rule ☒

Matching method

Content

Action
When the request is blocked, an error code and error page will be returned.

OK Cancel

6. (Optional) After configuring the rules, if you identify new risky IPs that need to be added to the group and applied to all sites, you can follow steps 1-3 to re-enter the site where the template was created, click **Edit**, enter the new IP addresses, and click **Save** to apply the new IPs to all protection policies that use this group.

Create Batch import

ID	Group name	List of IP groups	Operat
1734	<input type="text" value="IPblacklist"/>	<div><input style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 2px 5px;" type="text" value="1.1.1.1/23"/> <input style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 2px 5px;" type="text" value="1.2.2.2"/> <input style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 2px 5px;" type="text" value="3.3.3.3"/></div>	Save

Total items: 1 10 / page 1

Origin Protection

Last updated : 2024-01-02 10:43:44

Overview

When Origin Protection is enabled, EdgeOne notifies you of the latest update of intermediate IPs of L4 proxy and site acceleration. You can sync them to the firewall rules of your origin, allowing only traffic from these IPs to your origin.

Directions

1. Log in to [the EdgeOne console](#), click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. In the site details page, click **Security protection > Origin protection**.
3. On the page that appears, enable **Origin Protection**. Select the resources to bind with the intermediate IP addresses. Click **OK**.

Note

Select resource: Select target resources to enable Origin Protection.

4. After Origin Protection is enabled:

You can see the current intermediate IP addresses. You can update your origin firewall rules accordingly.

You will be informed of any updates of the intermediate IP addresses. Once you confirm the updates and report your update progress, the latest ones will be applied to your associated resources.

Reminders

To ensure the normal running of your business, confirm and update the intermediate IPs in the console as soon as possible after you are notified.

Note

If the intermediate IP addresses are not updated, there may be higher latency or instability issues in case of high concurrency.

Custom Response Page

Last updated : 2024-07-15 09:31:09

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 on the **site** to be configured in the site list.
2. On the site details page, click **Custom Response Page**.
3. In the custom response pages, 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](#)

Save

Cancel

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. A custom response page named `Custom-Pages1` has already been configured. You can refer to the following steps for configuration:

1. Log in to the [EdgeOne console](#) and click **Site List** in the left sidebar. Then click on the **site** to be configured in the site list.
2. On the site details page, click **Security > Custom Pages**.
3. On the custom page details page, select the domain name to be configured from the protected domain list on the left, such as: `www.example.com`.
4. Select the block page module to be configured. For example, select the Web Protection Block (except by Managed Rules) page and click **Set**.

Configurations



Managed Rule Block

Customize the response sent to clients when their requests are blocked by managed rules.



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.

5. 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 ▼

[View all custom response contents](#)☐

Custom status code

567

Save

Cancel

6. 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

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 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

All service types

Enter a site r

<input type="checkbox"/> Resource	Service type	On/Off	Custom threshold
<input type="checkbox"/>	Security acceleration	<input type="checkbox"/>	100Mbps Edit
<input type="checkbox"/>	L4 proxy	<input type="checkbox"/>	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**.

Batch setting

Cancel selection

All service types

Enter a site r

<input checked="" type="checkbox"/> Resource	Service type	On/Off	Custom threshold
<input checked="" type="checkbox"/>	Security acceleration	<input type="checkbox"/>	100Mbps Edit
<input checked="" type="checkbox"/>	L4 proxy	<input type="checkbox"/>	100Mbps Edit

4.2.2 Toggle on the custom threshold switch



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

The image shows a 'Batch setting' dialog box with a close button (X) in the top right corner. Inside the dialog, there is a 'Custom' label followed by a toggle switch that is currently turned on. Below this, there is an 'Alarm threshold' label followed by a numeric input field containing '100', flanked by minus and plus buttons, and the unit 'Mbps'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

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.

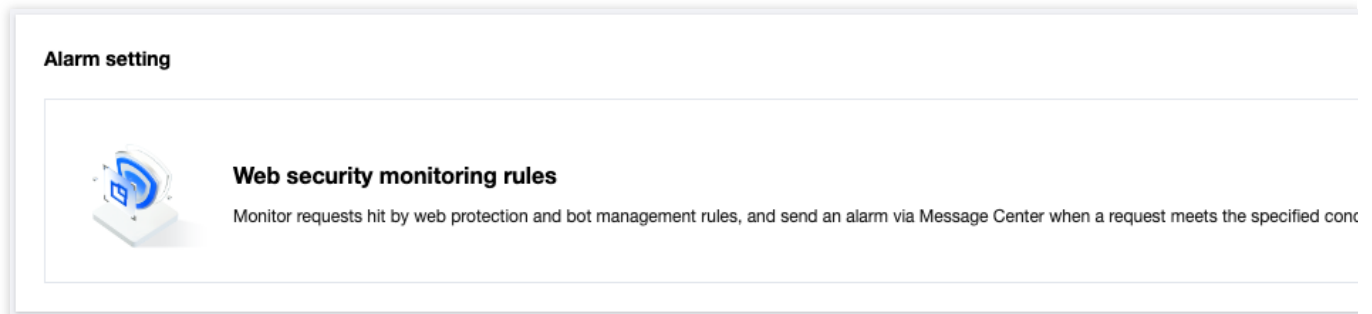
Alarm frequency: When the security rule satisfies the alarm condition, alarm notifications are pushed in the specified frequency.

Note:

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

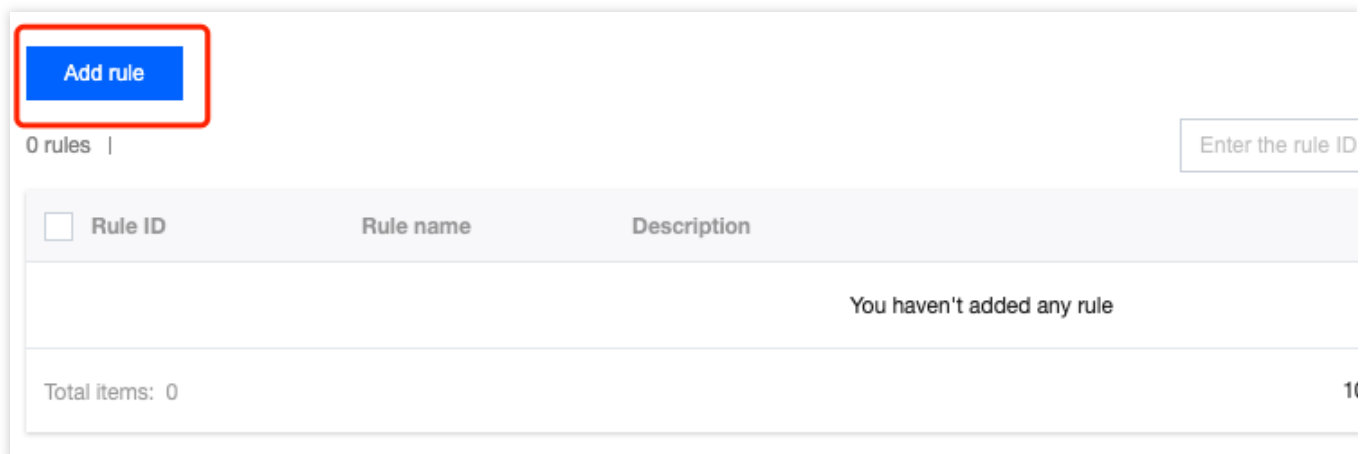
Managing web security monitoring rules

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.



Create a web security monitoring rule

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



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.

		Domain name	████████████████████
		Monitor requests	Action Block,Observe,Block client IP
		Alarm setting	Static alarm - Requests per 10 seconds greater than 1 times
<input type="checkbox"/>	1680161482	test1	

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

<input checked="" type="checkbox"/>	Rule ID	Rule name	Description
<input checked="" type="checkbox"/>	1680161482	test1	<div>Domain name</div> <div>Monitor requests</div> <div>Action</div> <div>Block,Observe,Block client IP</div> <div>Alarm setting</div> <div>Static alarm - Requests per 10 seconds greater than 1 times</div>
<input checked="" type="checkbox"/>	1680161471	test	<div>Domain name</div> <div>Monitor requests</div> <div>Action</div> <div>Observe,Block,JavaScript Challenge,Redirect,Managed challenge,Return custom page,Block client IP,Drop w/o response,Add short latency,Add long latency</div> <div>Alarm setting</div> <div>Static alarm - Requests per 10 seconds greater than 1 times</div>

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.

<input type="checkbox"/>	Rule ID	Rule name	Description
<input type="checkbox"/>	1680161482	test1	<div>Domain name</div> <div>Monitor requests</div> <div>Action</div> <div>Block,Observe,Block client IP</div> <div>Alarm setting</div> <div>Static alarm - Requests per 10 seconds greater than 1 times</div>

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

<input checked="" type="checkbox"/>	Rule ID	Rule name	Description
<input checked="" type="checkbox"/>	1680161482	test1	<div>Domain name</div> <div>Monitor requests</div> <div>Action</div> <div>Block,Observe,Block client IP</div> <div>Alarm setting</div> <div>Static alarm - Requests per 10 seconds greater than 1 times</div>
<input checked="" type="checkbox"/>	1680161471	test	<div>Domain name</div> <div>Monitor requests</div> <div>Action</div> <div>Observe,Block,JavaScript Challenge,Redirect,Managed challenge,Return custom page,Block client IP,Drop w/o response,Add short latency,Add long latency</div> <div>Alarm setting</div> <div>Static alarm - Requests per 10 seconds greater than 1 times</div>