Tencent Cloud EdgeOne

Security Protection

Contents

Security Protection
DDoS Protection
DDoS Protection Overview

Last updated: 2023-09-07 15:21:37

What is a DDoS attack?

A Distributed Denial of Service (DDoS) attack is a malicious attempt to make a targeted server unavailable by blocking its network bandwidth or overwhelming its system with a flood of internet traffic.

The Harm of DDoS Attacks

If a DDoS attack results in business interruption or damage, it can lead to substantial commercial losses.

- **Significant Financial Loss:** Following a DDoS attack, the origin server may be unable to provide services, preventing users from accessing your business, thereby resulting in substantial financial and brand damage.
- **Data Leakage:** During a DDoS attack on your server, hackers may seize the opportunity to steal your business's core data.
- **Malicious Competition:** In some industries, fierce competition exists, and competitors may resort to DDoS attacks to maliciously disrupt your services, thereby gaining an advantage in the industry competition.

Use Cases for DDoS Protection

- **Gaming:** The gaming industry is a prime target for DDoS attacks. DDoS protection effectively ensures the availability and continuity of games, safeguarding a smooth experience for players. It also provides protection during events, new game releases, or peak revenue periods during holidays, ensuring the normal operation of the gaming business.
- **Internet:** Ensuring smooth and uninterrupted access to internet web pages, particularly during significant events such as major ecommerce promotions, is crucial for maintaining normal business operations.
- **Finance:** Anti-DDoS Pro helps the finance industry meet the compliance requirements and provide fast, secure, and stable online transaction services to customers.
- **Government:** Fulfilling the security requirements of national government cloud construction standards, providing security assurance for major conferences, events, and

sensitive periods, ensuring the normal availability of public services, and maintaining government credibility.

- **Enterprises:** Ensure the continuous availability of enterprise site services, prevent economic and brand image losses caused by DDoS attacks, and save on security costs with zero hardware and maintenance.

Introduction to EdgeOne's Default DDoS Protection

DDoS Protection is a service provided by Tencent Cloud EdgeOne to defend against L3/L4 traffic-based DDoS attacks. EdgeOne offers fundamental DDoS protection capabilities to meet daily security operation needs. The platform-level basic DDoS protection is enabled by default, monitoring network traffic in real-time. Upon detecting a traffic-based DDoS attack, it immediately initiates cleansing, providing EdgeOne with second-level protection. The default DDoS protection provides a basic security policy, which is based on attack profiling, behavior pattern analysis, AI intelligent recognition, and other protection algorithms, effectively responding to common DDoS attack behaviors.

Protection Type	Description
Malformed message filtering	Filters out Frag Flood, Smurf, Stream Flood, and Land Flood attacks, as well as IP, TCP and UDP malformed packets.
Network Layer DDoS Attack Defense	Filters out UDP Flood, SYN Flood, TCP Flood, ICMP Flood, ACK Flood, FIN Flood, RST Flood, DNS/NTP/SSDP reflection attacks, and null connections.
DNS DDoS Attack	DNS DDoS attacks primarily encompass DNS Request Flood, DNS Response Flood, False Source + Real Source DNS Query Flood, Authoritative Server Attacks, and Local Server Attacks.
Connection-based DDoS Attacks	Connection-based DDoS attacks primarily refer to TCP slow connection attacks, connection exhaustion attacks, and slow attacks such as Loic, Hoic, Slowloris, Pyloris, and Xoic.

Introduction to EdgeOne's Independent DDoS Protection

Scenarios

Exclusive DDoS Protection is a paid feature offered by EdgeOne to enhance DDoS mitigation, providing exclusive access to a cleaning center. When the platform's default protection cannot meet the demands of your business's normal operation, you can use Exclusive DDoS Protection to help ensure your business runs smoothly. Once activated, it provides an exclusive high-defense IP for traffic cleaning, offering a promised protection bandwidth value based on the guaranteed protection capacity and elastic protection capacity you purchase.

> **Note:**
> Exclusive DDoS protection is only available for subscription with the EdgeOne Enterprise plan.

Capability Overview

1. The default access node utilizes a cleansing center, offering enhanced DDoS protection capabilities, reaching up to terabyte levels.
2. Committed protection capacity can be flexibly selected based on business deployment conditions, with options for global availability zones (excluding Mainland China), Mainland China availability zones, and global availability zones protection specifications.
3. In addition to automatic cleansing and identification mechanisms, EdgeOne DDoS Protection offers diverse and flexible custom DDoS protection strategies tailored to your business's defensive needs. You can flexibly set these strategies based on the unique characteristics of your business to counter constantly changing attack methods. For Layer 4 proxy instances, the following custom rule configuration capabilities are supported:

   > **Note:**
   > When a request matches multiple rules simultaneously, it is processed in the following rule order:

Protection Module	Note
IP Blocklist/Allowlist	In the event of a DDoS attack, access to EdgeOne sites is restricted by matching IP addresses against a blocklist and allowlist.
Port Filtering	In the event of a DDoS attack, access to EdgeOne sites can be restricted by specifying a custom port range.
Protocol Blocking	You can configure EdgeOne sites to only allow user access via specified protocols.
Connection	Protection against connection-based attacks is provided,

Protection	automatically blocking clients exhibiting abnormal connection behavior.
Feature Filtering	In the event of a DDoS attack, you can customize interception strategies based on the characteristics of IP, TCP, and UDP packet headers or payloads.
Regional Blocking	In a DDoS attack, access to EdgeOne sites is restricted by matching regions.

Exclusive DDoS Protection Usage

Last updated: 2023-09-07 15:21:43

Background

If your business has the following requirements for access services:

1. Requires DDoS protection services with guaranteed protection capacity. For example: financial services, gaming platform services, etc.
2. In the event of a large-scale DDoS attack, businesses under the platform's default protection may experience changes in their resolved IP due to business scheduling, which could affect normal operations. You may need to maintain a continuous session state, including keeping the DNS resolution IP unchanged, maintaining long TCP connections, and HTTP long session states. For example: multiplayer online gaming services, voice services, etc.
3. Requires customized network layer DDoS protection strategies or network control strategies. For example: needing to discard client traffic from specified regions.

We recommend that you purchase the Exclusive DDoS Protection Service. The Exclusive DDoS Protection Service provides further enhancements on top of the platform's default protection:

1. Regularly connect to the cleansing center to continuously detect, cleanse, and filter malicious traffic.
2. Guaranteed protection capacity, maintaining session stability during protection.
3. Customizable DDoS protection strategies, including control options based on IP and client regions.

Assists in mitigating the risk of DDoS attacks, ensuring business stability.

Usage Guide

Exclusive DDoS protection can be applied to both layer-7 and layer-4 services. You can refer to the following different scenarios to understand how to enable exclusive DDoS protection for your site.

> **Note:**
> Exclusive DDoS protection is only available for Enterprise plans accessed after July 1, 2023. If you accessed the EdgeOne Enterprise version before this date and wish to use exclusive DDoS protection, please contact customer service.

Scenario One: Enabling Exclusive DDoS Protection for Layer-7 Sites

Scenario Example

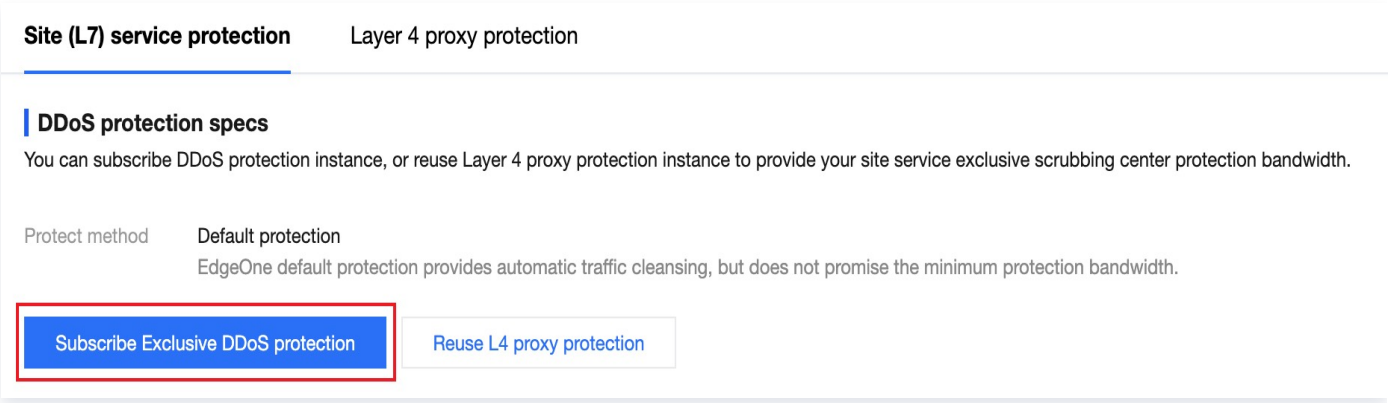
You provide HTTPS unified login services (SSO, Single-Sign-On) through the site domain `onelogin.example.com`, primarily serving users in the Chinese mainland. Frequent DDoS attacks can prevent users from logging in normally. The estimated daily attack volume is 30Gbps, which may reach 50Gbps during peak periods. Therefore, independent DDoS protection is required to ensure the provision of stable and available services.

Supports and Limits

- Once the independent DDoS protection within the Layer 7 site is created, it currently does not support unsubscription within the console. Please contact Tencent Cloud business if you need to unsubscribe.
- During the process of enabling or disabling DDoS protection, there may be impacts on the business (such as connection resets). The estimated duration of the impact is generally about 2-3 minutes for enabling or disabling. If there is local or ISP DNS cache, the switch may take effect later. The specific effective duration depends on the TTL configuration of the DNS record used by the client.

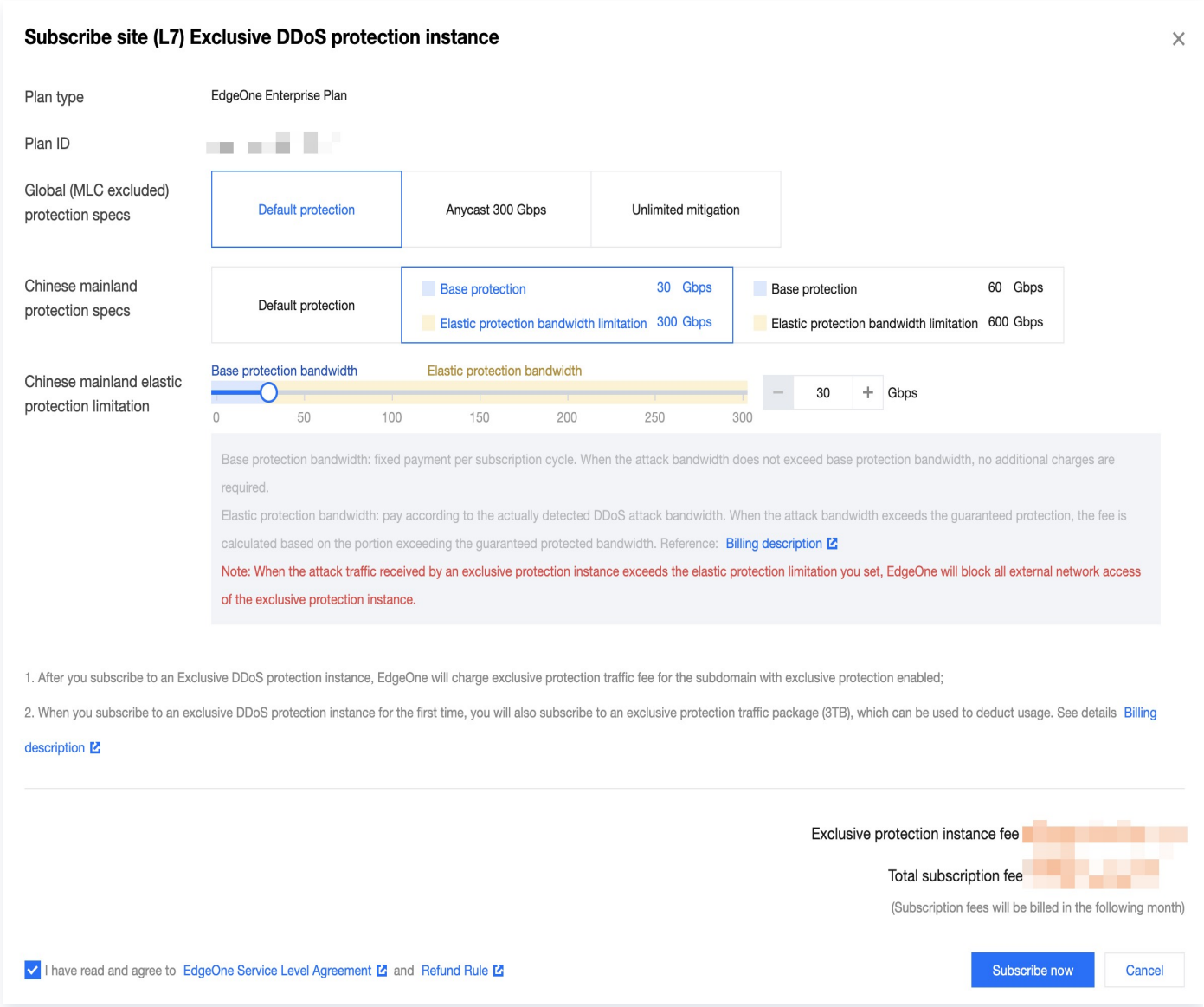
Instructions

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click on **Security** > **DDoS Mitigation**.
3. On the site (Layer 7) service protection tab, click **Subscribe to Exclusive DDoS Protection**.



4. On the page for subscribing to an exclusive DDoS protection instance, select the protection region and protection specifications you need to subscribe to. In this scenario, based on the service area and historical attack volume, you can choose to subscribe to a

guaranteed 30Gbps in the China mainland available zone, with an elastic capacity protection peak of 50Gbps.



5. After confirming the relevant fee information, select **I agree to the related user agreement**, and click **Subscribe Now**. The system will then automatically distribute the configuration for your exclusive DDoS protection instance.
6. Once the instance is deployed, you can enable Exclusive DDoS protection for all domains within the protection configuration page, or select `onelogin.example.com` within this scenario to enable Exclusive DDoS protection for this domain.
7. If you enable exclusive DDoS protection for a single domain, a deployment confirmation window will pop up. Click **Confirm** to start the deployment. The changes will take effect once the deployment is complete.

Scenario Two: Enabling Independent DDoS Protection for Layer-4 Proxy Instances

Scenario Example

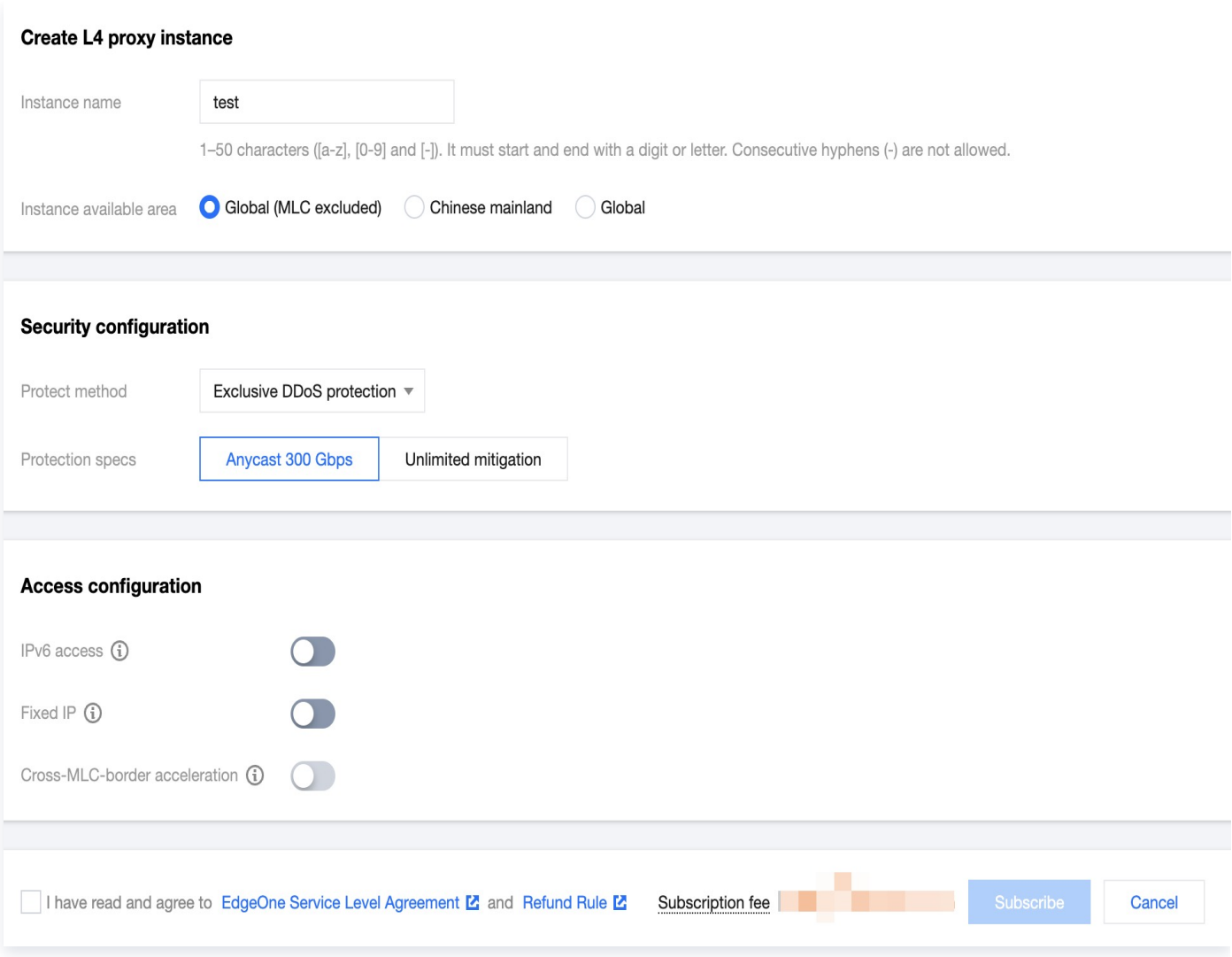
You have an upcoming game release that requires the use of L4 proxy acceleration to optimize player login experience. This involves forwarding TCP traffic data through port 80. The game is primarily distributed overseas and is expected to face large-scale DDoS attacks (not exceeding 300 Gbps) during its launch period. By integrating independent DDoS protection, you can ensure the stability of the login interface service during the release and operation periods, thereby preventing player attrition.

Supports and Limits

- Currently, the use of exclusive DDoS protection is only allowed when creating a new Layer 4 proxy instance. Once created, it cannot be modified or changed.
- Once the independent DDoS protection for Layer 4 proxy is created, it does not support dynamic enabling/disabling.

Instructions

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **L4 proxy**.
3. On the Layer 4 Proxy Management Instance page, click **Create L4 Proxy**.
4. When creating a new L4 proxy instance, you can choose the corresponding protection method in the security protection configuration, switch to independent DDoS protection. In the current scenario, for example, you can choose Anycast 300 Gbps.



5. After confirming the relevant user agreement and pricing 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 this instance.
6. After the configuration is deployed, you can click **Configuration** to enter the instance configuration interface, add the port information and origin server address that need to be accelerated, and click **Save** to start the L4 proxy acceleration.

Scenario Three: Layer-7 site reuses Layer-4 proxy instance DDoS protection resources.

Scenario Example

Assume your current Exchange email service provides services through multiple protocols, including HTTPS and several TCP/UDP protocols, and has recently suffered a DDoS attack exceeding 200Gbps. Due to its business architecture characteristics that include both HTTPS and TCP/UDP services, hackers can initiate DDoS attacks through either HTTPS or TCP/UDP. Therefore, security protection needs to be provided for both layer-7 sites and layer-4 proxies.

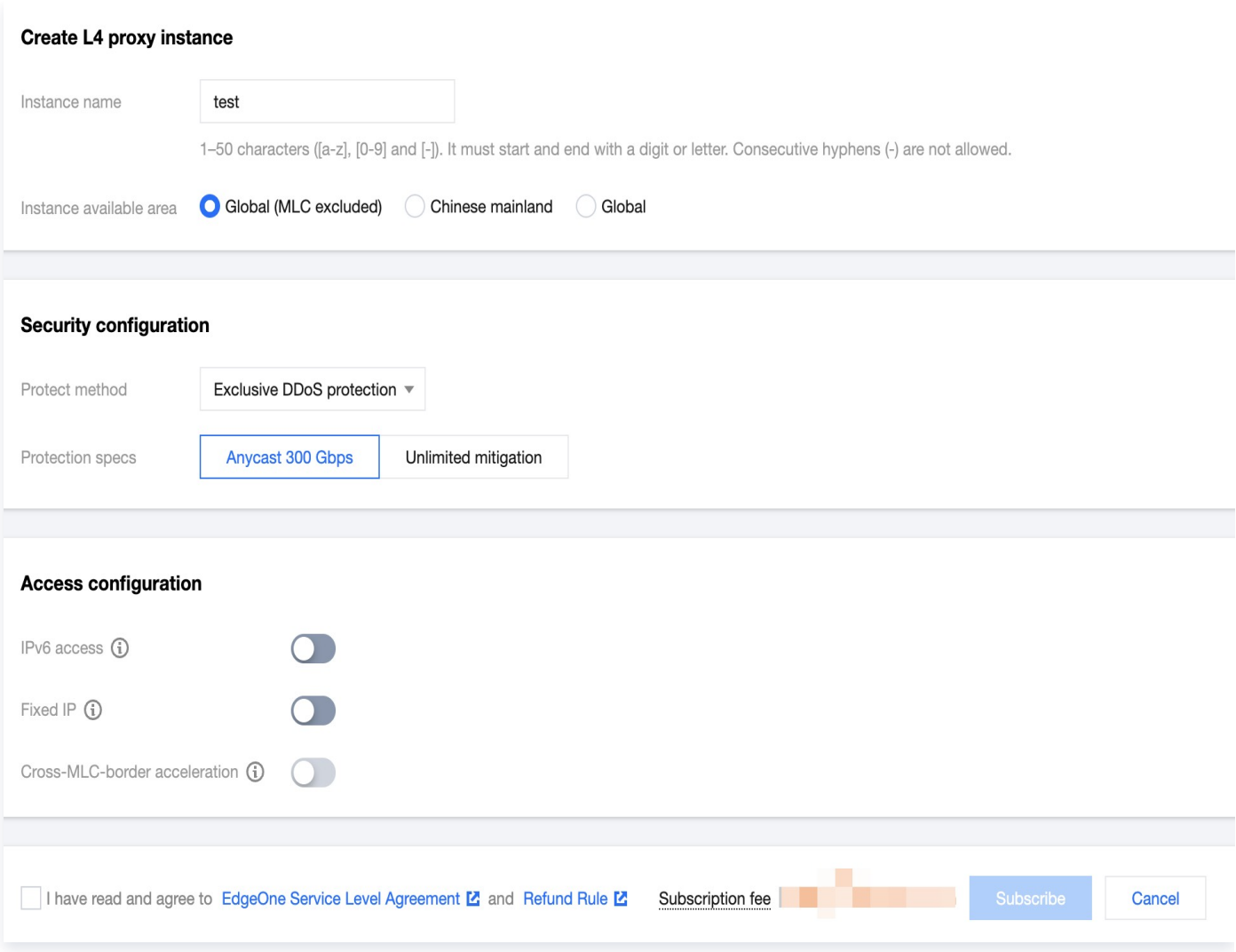
Supports and Limits

- When a layer-7 site reuses the layer-4 proxy's exclusive DDoS protection, it is necessary to configure port filtering within the exclusive DDoS protection to allow the ports used when accessing layer-7 traffic, to avoid interception of layer-7 traffic.
- This feature is currently in beta testing. If needed, you can contact Tencent Cloud to activate it.

Instructions

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

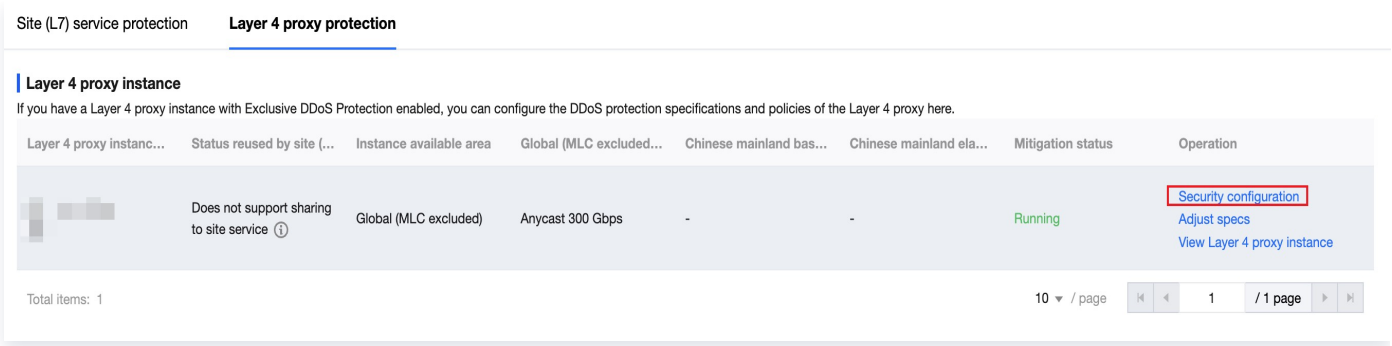
1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **L4 proxy**.
3. On the Layer 4 Proxy Management Instance page, click **Create L4 Proxy**.
4. On the page for creating a new L4 proxy instance, you can select the corresponding protection method, switch to independent DDoS protection. In the current scenario, for example, you can select Anycast joint defense 300Gbps.



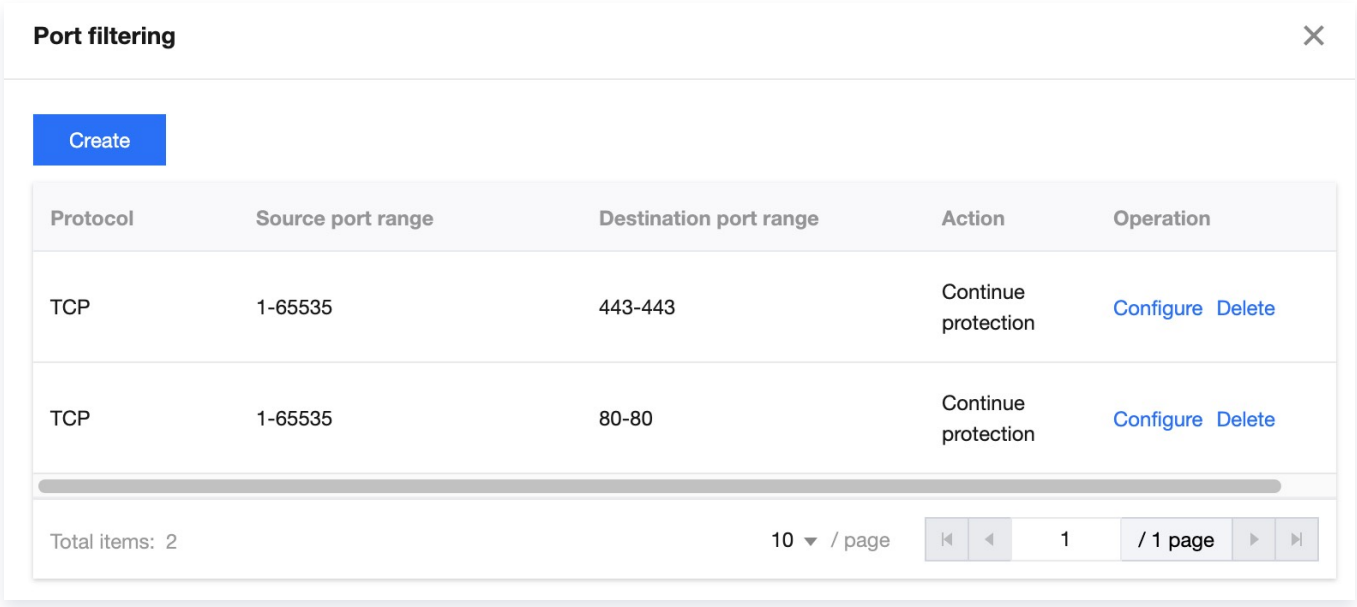
5. After confirming the relevant user agreement and pricing information, click **Subscribe** to complete the creation of the L4 proxy instance. After creation, the platform will automatically issue an independent DDoS protection configuration for this instance.
6. After the configuration is deployed, you can click **Configuration** to enter the instance configuration interface, add the port information and origin server address that need to be accelerated, and click **Save** to start the L4 proxy acceleration.

Step 2: In the L4 proxy security protection instance, allow L7 access traffic.

1. Once the L4 proxy configuration is complete, navigate to **DDoS Mitigation** > **L4 Proxy Protection** tab, select the L4 proxy instance created in Step 1, and click on **Protection Configuration**.

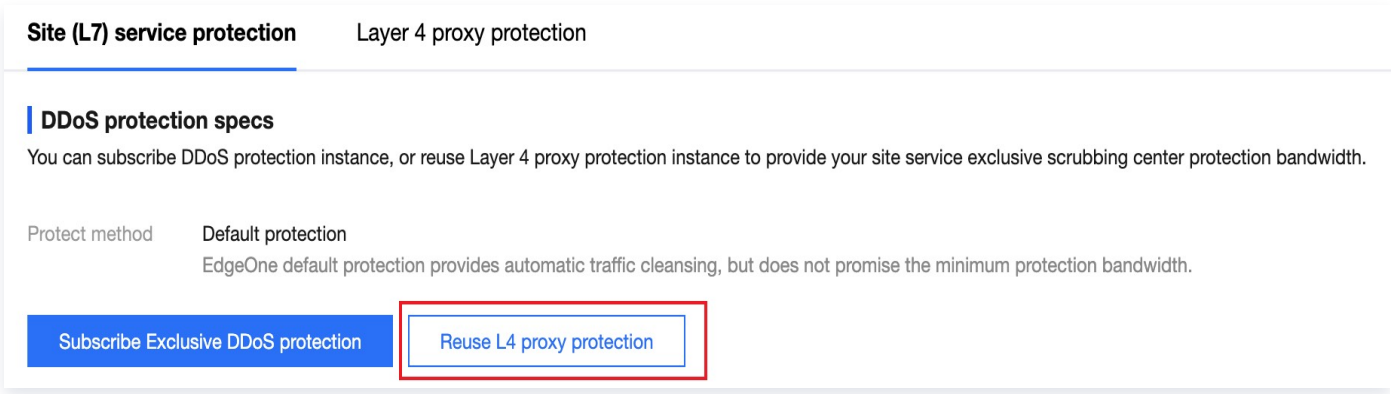


2. In the protection configuration, locate the port filtering card and click **Set** to enter the configuration interface. Click **Create** to configure a rule that allows source port range 1–65535 and destination port range 443, with the action set to continue protection, allowing the corresponding layer 7 traffic. Click **Save** to apply the changes. Follow the same steps to add another rule to allow port 80. The complete configuration rules are as follows:



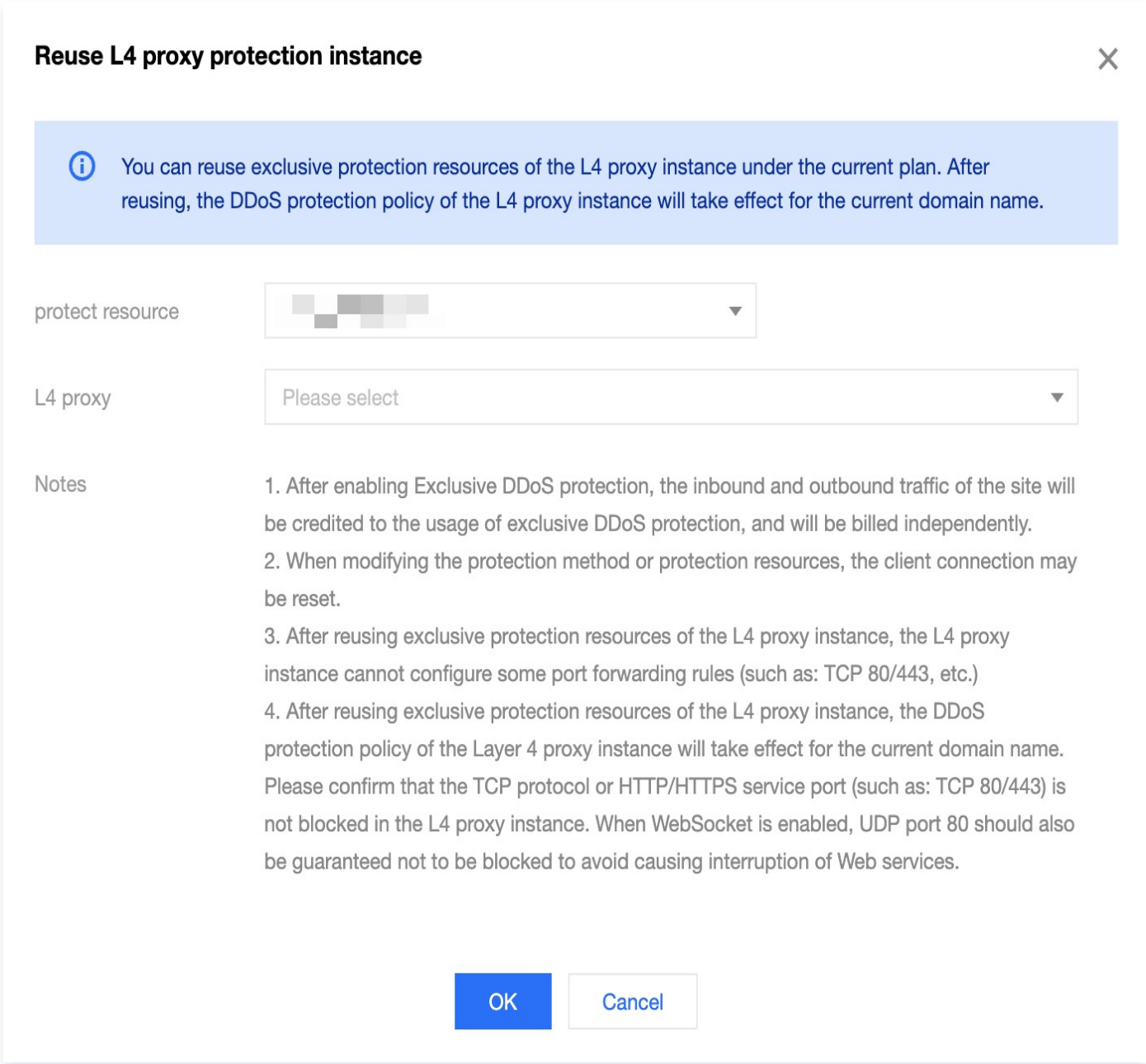
Step 3: Reuse L4 proxy protection instance to provide protection for Layer 7 site domain.

1. In the **DDoS Mitigation** > **L4 Proxy Protection** tab, click on **Reuse L4 Proxy Protection**.



2. After selecting the Layer 4 proxy protection resources to be reused, click **Confirm** to

initiate the automatic distribution of independent DDoS instance configurations.



3. Once the instance is deployed, you can enable Exclusive DDoS protection for all domain names within the protection configuration interface, or select `exchange.example.com` within this scenario to enable Exclusive DDoS protection for this domain.

References

How does it work

Upon enabling Exclusive DDoS protection, traffic will be processed according to the following procedure:

1. When the client resolves the DNS record of the service, it will obtain the scrubbing center address.

2. When the client accesses the service, the cleansing center first cleanses the traffic, automatically identifying and filtering out network layer DDoS attack traffic. If the current business has accessed the L4 proxy, the filtered traffic is forwarded and accelerated by the L4 proxy service.

If your site includes Layer-7 site acceleration, traffic will continue to be forwarded in the following manner:

3. After SSL authentication, HTTPS protocol requests continue to be protected through web protection and bot management security strategies.
4. Requests verified through the security module will continue to undergo site caching, site acceleration, and back-to-source services among other functional modules.

Configuration of Exclusive DDoS protection Rules
Increase DDoS Protection Level

Last updated: 2023-09-07 15:22:01

The DDoS mitigation level is a default protection policy template provided by EdgeOne DDoS protection. Based on the mitigation level, DDoS protection will automatically intercept traffic attacks that match certain characteristics. The protection policies for each mitigation level are described below:

> **Note:**
> This feature is only supported when the Layer-4 proxy enables Exclusive DDoS protection. Both the default platform protection and Layer-7 site Exclusive DDoS protection do not support configuration.

Protection policies for each mitigation level

Comparison Item		Loose	Moderate (Default)	Strict
		This protection level uses a loose cleansing policy and defends against only explicit attack packets. We recommend that you choose this protection level when normal requests are blocked. Complex attack packets may pass through the security system.	The cleansing policy is suitable for the vast majority of businesses and can effectively defend against common attacks. The DDoS protection is set to moderate mode by default.	The cleansing policy is strict. It's recommended to use this mode when attack packets pass through the security system the Normal mode.
Data packets	SYN packet	Filter	Filter	Filter

with explicit attack attributes	ACK packet	Filter	Filter	Filter
	UDP packet	Filter	Filter	Filter
Data packets not compliant with protocol specifications	TCP packet	Filter	Filter	Filter
	UDP packet	Filter	Filter	Filter
	ICMP packet	Filter	Filter	Filter
Attack packets based on threat intelligence		Not filter	Filter	Filter
Actively verifies the source IP addresses of some access attempts.		Not filter	Filter	Filter
ICMP Attack Packets		Not filter	Not filter	Filter

Adjusting the mitigation level

If your business encounters the following two situations, it is recommended to adjust the mitigation level:

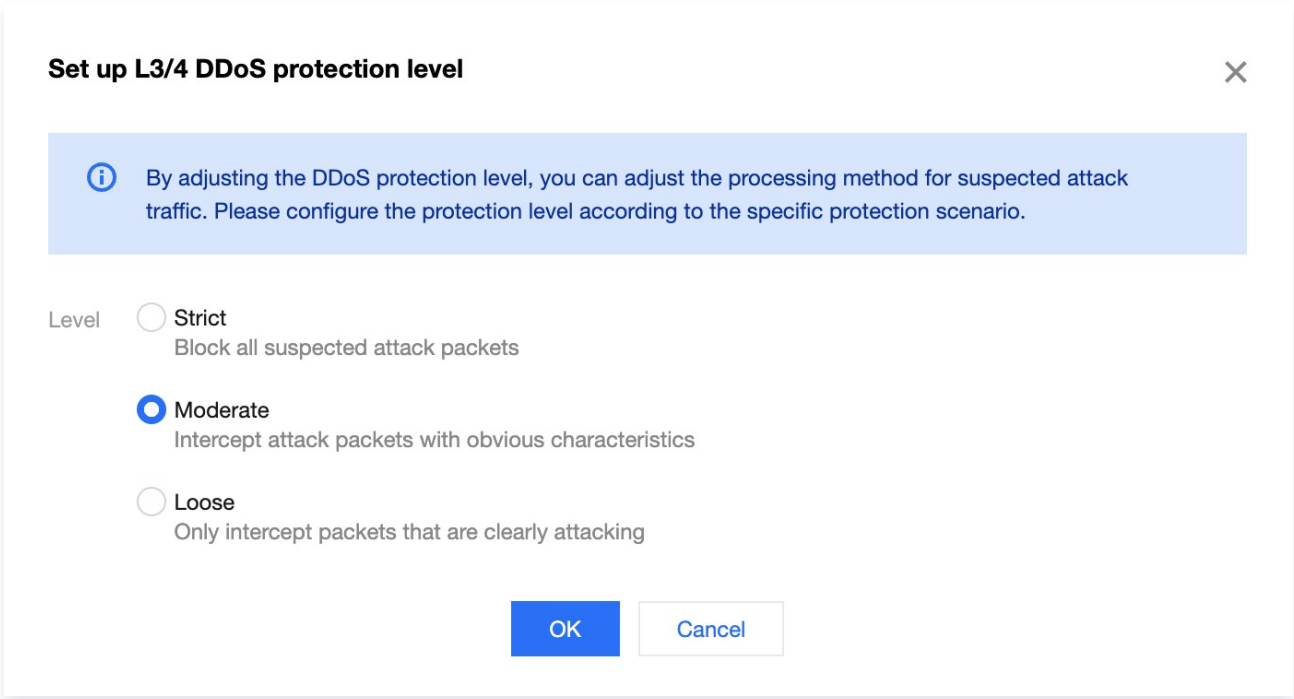
- If false positives are identified in the security log analysis during the current business operation, to ensure the availability of the business, you can adjust and lower the protection policy level to Loose.
- If attacks are still found to be passing through to the origin server during the current business operation under the moderate protection level, it is recommended that you increase the protection level to strict.

You may adjust according to the following steps:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security** > **DDoS Mitigation** to access the DDoS mitigation details page.
3. On the Layer-4 Proxy Protection tab, select the Layer-4 proxy protection instance you

want to configure and click **Protection Configuration**.

4. In the L3/4 DDoS mitigation level card, click **Settings** to adjust the mitigation level.



5. Click **OK** to apply changes after switching.

Configuration IP blocklist/allowlist

Last updated: 2023-09-07 15:22:07

Overview

EdgeOne's DDoS protection service enables you to control access requests by configuring an IP blocklist and allowlist, thereby limiting who can access your business resources. By setting up an IP blocklist and allowlist, you can filter or allow rules based on the source IP. When an IP from the allowlist attempts to access, it will be directly permitted, bypassing other DDoS protection policy filters (without affecting the protection policies of other modules). Conversely, when an IP from the blocklist attempts to access, it will be directly blocked.

Note:

1. This feature is only supported when the Layer-4 proxy enables Exclusive DDoS protection. Both the default platform protection and Layer-7 site Exclusive DDoS protection do not support configuration.
2. The IP blocklist/allowlist rules take effect within 5-10 seconds after being saved.
3. You can configure up to 8 IP groups in the IP blocklist/allowlist, with a maximum of 2000 IPs per group.

Use Cases

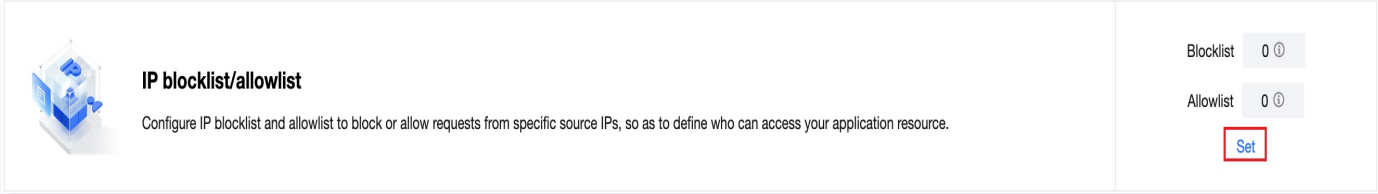
- **Allow Access Only from IPs on the Allowlist During an Attack:** During a DDoS attack, only users trusted on the allowlist are permitted to access the site. This significantly reduces the security risk to the website, but it may affect the access requests from normal IPs not on the allowlist.
- **Blocklist directly intercepts source attack IPs:** Adding confirmed source attack IPs to the blocklist will block all access requests from that IP, reducing DDoS scrubbing traffic and minimizing attack penetration.

Scenario 1: Adding trusted IP addresses to the allowlist to permit requests.

For all business domains under the site `example.com`, the IP address segment `1.1.1.1/24` is a trusted access IP for this site. To avoid mistakenly intercepting trusted IPs, you can add this IP to the allowlist, bypassing the DDoS protection module's cleansing process. The steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.

2. On the site details page, click **Security** > **DDoS Mitigation** to access the DDoS mitigation details page.
3. On the Layer-4 Proxy Protection tab, select the Layer-4 proxy protection instance you want to configure and click **Protection Configuration**.
4. In the IP blocklist/allowlist card, click on **Settings** to navigate to the IP blocklist/allowlist configuration page.

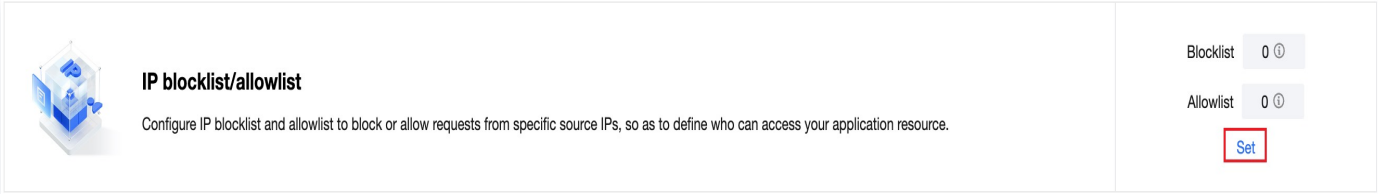


5. On the IP blocklist/allowlist page, click **Create**. For the current scenario, enter the IP range `1.1.1.1/24`, select the type as allowlist, and click **Save** to activate it.

Scenario 2: Permanently blocking access requests from attack source IPs using the IP blocklist.

For all business domains under the site `example.com`, the IP address `1.1.1.1` has been confirmed as the source of the attack. You can directly add this IP to the blocklist to block all access requests originating from this IP. The steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security** > **DDoS Mitigation** to access the DDoS mitigation details page.
3. On the Layer-4 Proxy Protection tab, select the Layer-4 proxy protection instance you want to configure and click **Protection Configuration**.
4. In the IP blocklist/allowlist card, click on **Settings** to navigate to the IP blocklist/allowlist configuration page.



5. On the IP blocklist/allowlist page, click **Create**. For the current scenario, enter IP `1.1.1.1`, select the type as blocklist, and click **Save** to activate it.

Configuration Region Blocking Rule

Last updated: 2023-09-07 15:22:13

Overview

If you find that all your attacks originate from a specific region, or your business only allows access from certain regions and does not trust access from other regions, EdgeOne supports one-click blocking in the scrubbing data center by specifying a regional list, helping you to custom block access requests from source IPs in specified regions. After enabling regional blocking, traffic from the blocked region to the EdgeOne site will be discarded. Traffic blocking is supported in multiple regions and countries.

Note:

1. This feature is only supported when the Layer-4 proxy enables Exclusive DDoS protection. Both the default platform protection and Layer-7 site Exclusive DDoS protection do not support configuration.
2. Attack traffic from the blocked regions will not be allowed to your origin server, but still be recorded.

Scenarios

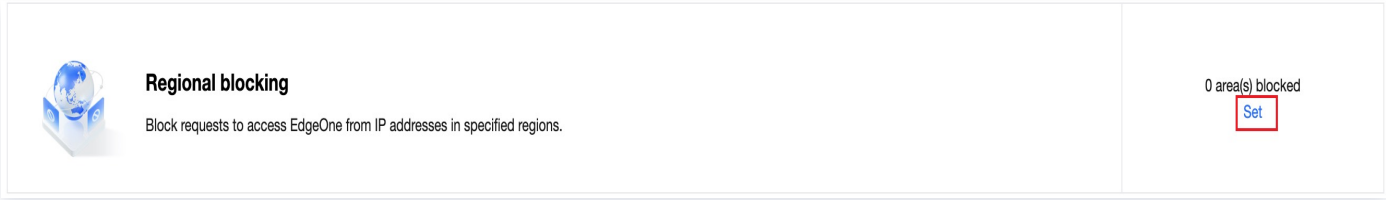
- **Exclude all attack behaviors outside trusted regions:** If your business is only applicable to specific regions, regional blocking can be used to block access clients from other regions in DDoS scrubbing, preventing attack sources from other regions from being transmitted to the origin server.
- **One-click blocking of concentrated attacks from specific regions:** If the main source of attacks on your site is from a specific region, you can use regional blocking to block all access requests from that region in the DDoS scrubbing center, effectively preventing attacks from that region from being transmitted.

Instructions

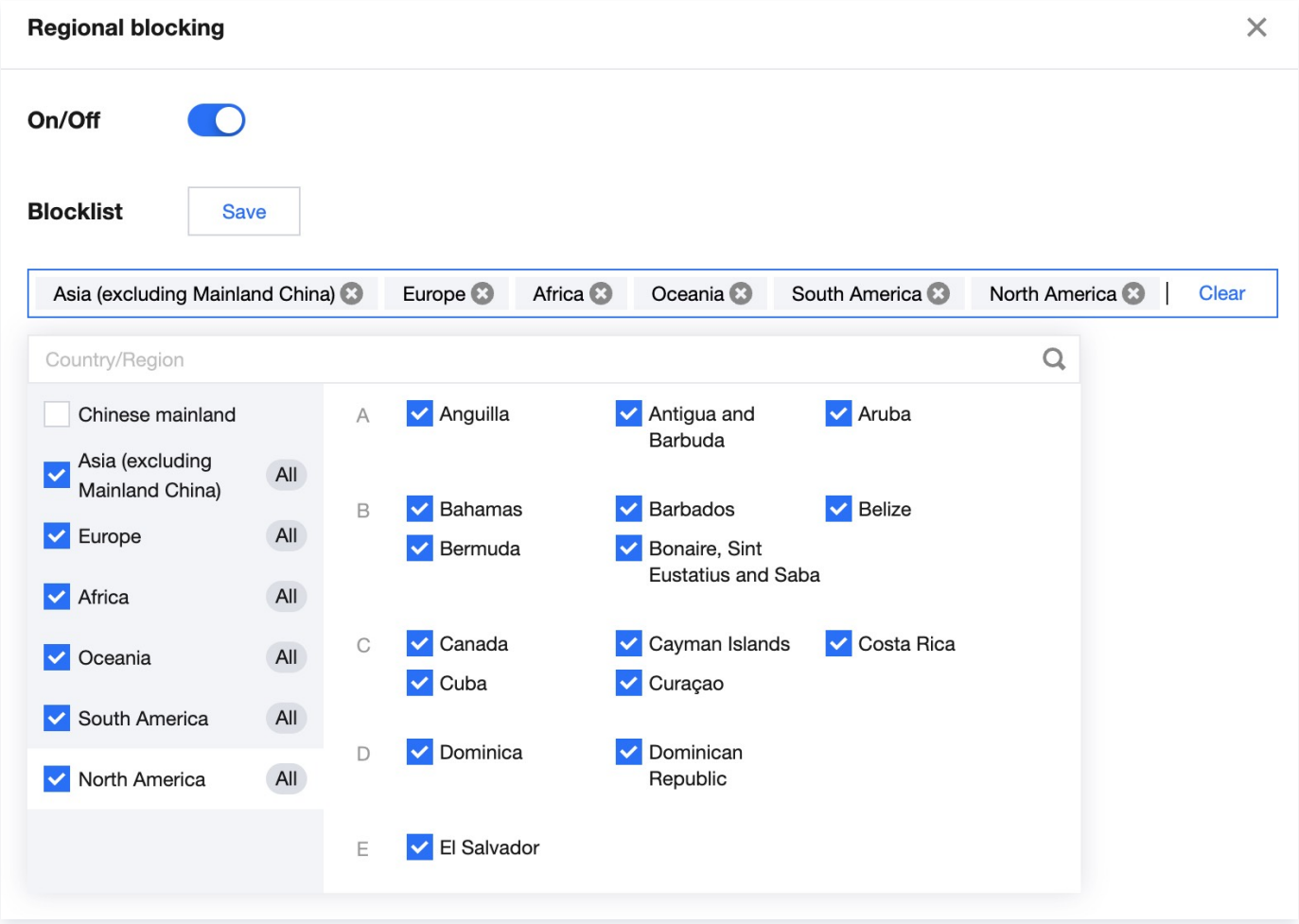
For instance, if your site's users are all located in mainland China and you only allow access from this region, distrusting requests from other regions, you can block all requests from other regions to prevent potential attacks when a DDoS attack occurs. The steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security** > **DDoS Mitigation** to access the DDoS mitigation details page.

3. On the Layer-4 Proxy Protection tab, select the Layer-4 proxy protection instance you want to configure and click **Protection Configuration**.
4. Click **Set** in the "Regional blocking" section.



5. On the regional blocking configuration page, click **Edit** on the right side of the blocking list, select the blocking region. For this scenario, select all regions except mainland China.



6. Click **Save** to complete the regional blocking configuration.

Configuration Port Filtering

Last updated: 2023-09-07 15:22:20

Overview

Port filtering is utilized to precisely formulate protection strategies by specifying ports and protocols, thereby controlling the ports and protocols that clients can use to access EdgeOne. Once port filtering is enabled, you can customize the combination of protocol types, source port ranges, and destination port ranges as per your requirements. Furthermore, you can set up actions such as interception, allowance, or continued protection for rules that match.

> **Note:**
> This feature is only supported when the Layer-4 proxy enables Exclusive DDoS protection. Both the default platform protection and Layer-7 site Exclusive DDoS protection do not support configuration.

Scenarios

- **UDP business exists at the source station, and UDP reflection attacks are filtered through port filtering:** If your current source station business has UDP connections and cannot directly block UDP protocol access, you can configure the UDP access ports that need to be intercepted during DDoS cleaning in port filtering to prevent UDP reflection attacks from being transparently transmitted. Common UDP reflection attack ports include: 1-52, 54-161, 389, 1900, 11211.
- **Filtering Unpermitted Port Access Sources:** When your origin server only allows access through specified ports, you can use port filtering to configure the ports that are allowed access after DDoS cleansing. This directly discards all access connections from other ports, reducing attack penetration.

Instructions

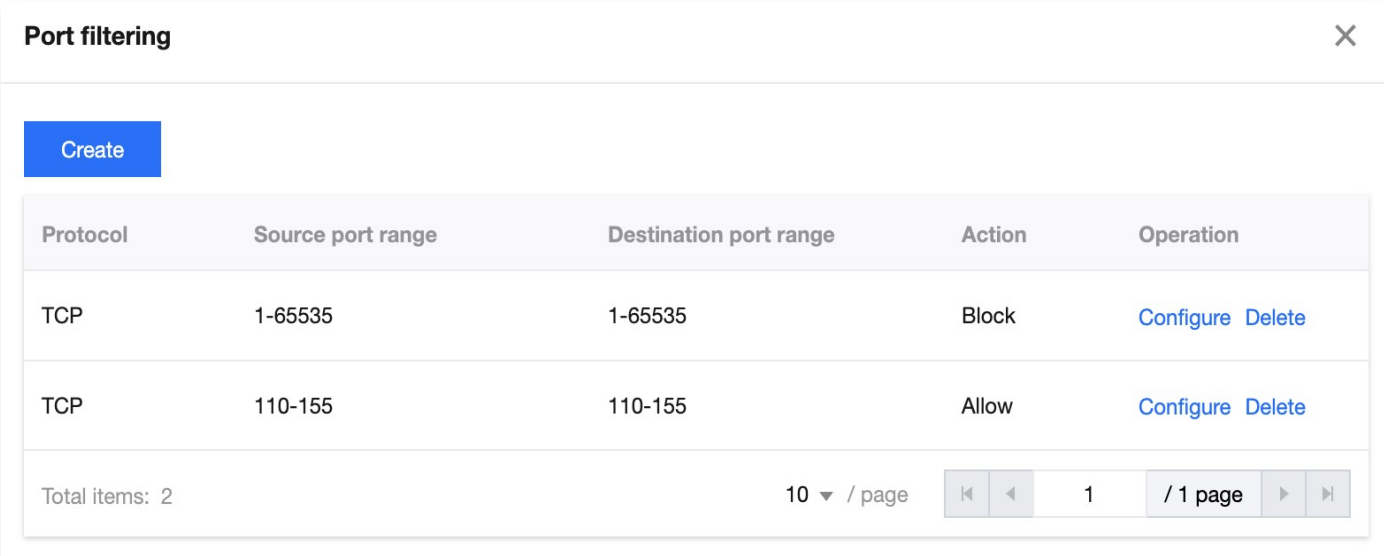
For instance, for all business domains under the site `example.com`, only ports 110-155 of the TCP protocol are open to the public, and access to all other ports is prohibited. The operation steps are as follows:

1. Log in to the EdgeOne console. In the left-hand menu, click on **Site List**. Within the site list, click on the **site** that needs configuration to enter the site details page.
2. On the site details page, click on **Security** > **DDoS Mitigation** to access the DDoS Mitigation details page.
3. On the Layer-4 Proxy Protection tab, select the Layer-4 proxy protection instance you

want to configure and click **Protection Configuration**.

4. In the Port Filtering card, click on **Settings** to navigate to the Port Filtering page.

5. On the Port Filtering page, click **Create** to establish port filtering rules. In this scenario, create two rules. Intercept all protocols selected as TCP, fill in the source port range as 1–65535, and the destination port range as 10–155. Select different protection actions and fill in the relevant fields, then click **Save**.



Parameter	Note
Agreements	You can choose from all, TCP, or UDP protocols.
Source port range	Refers to the port information from which the client initiates access, with a supported range of 1 to 65535.
Destination port range	This refers to the destination port information accessed by the client, with a supported range of 1 to 65535.
Action	• Interception: Halt the request. • Allow: Permit this request and cease matching with the remaining protection policies. • Continue Protection: Allow the current request and continue matching the remaining protection policies.

Configuration Features Filtering

Last updated: 2023-09-07 15:22:28

Overview

Feature filtering allows for the precise formulation of protective strategies against business message features or attack message features to prevent malformed message attacks from being transmitted. EdgeOne supports the customization of interception strategies based on the features in the IP, TCP, and UDP message headers or payloads. Once feature filtering is activated, you can combine the matching conditions of the source port, destination port, message length, IP message header or payload, and set actions such as discard, allow, discard and block, continue protection for the requests that meet the conditions.

> **Note:**
> This feature is only supported when the Layer-4 proxy enables Exclusive DDoS protection. Both the default platform protection and Layer-7 site Exclusive DDoS protection do not support configuration.

Scenarios

After your site is integrated with EdgeOne, if you need to manage access requests with specific characteristics, you can enable feature filtering for the site and set precise access control rules. The feature filtering access control rules consist of matching conditions and matching actions.

- A condition defines the characteristics of the request to be identified, specifically referring to the attribute features of the TCP/UDP protocol fields in the access request.
- The matching action defines the operation performed on the access request when it hits the matching condition, including interception, allowance, discard and block, and continued protection.

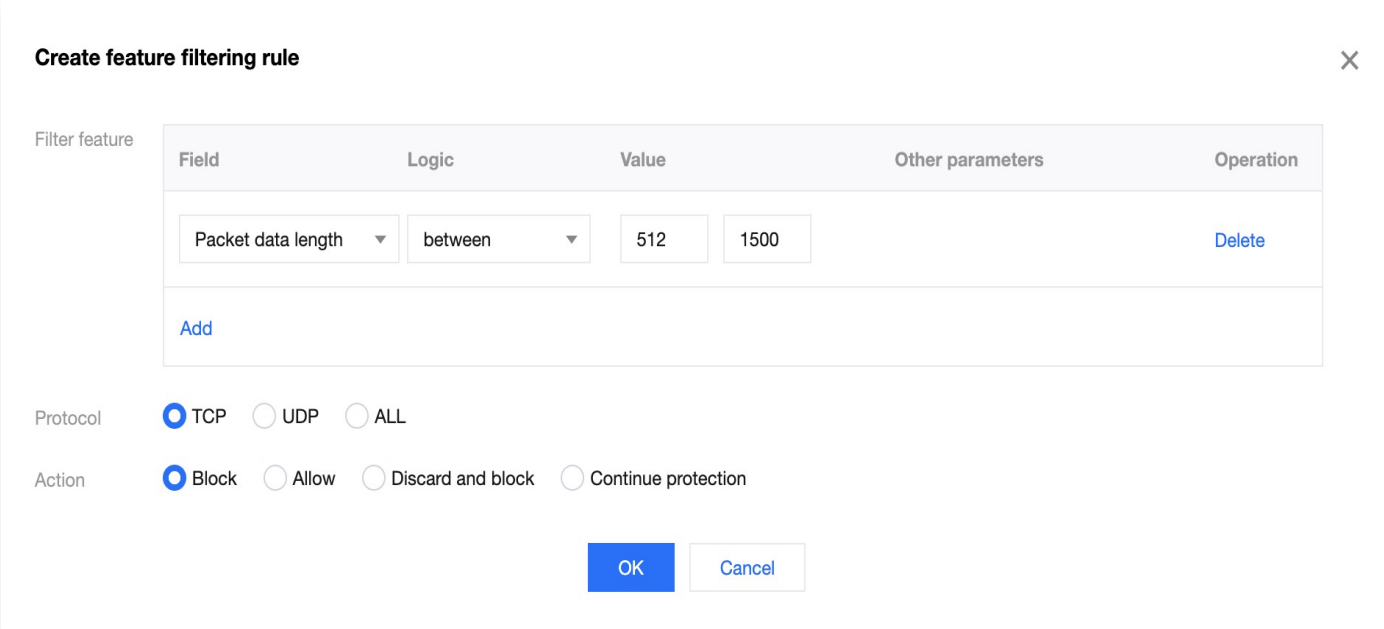
Operation Steps

For instance, for all business domain names under the site `example.com`, the requirement for the length of the outgoing TCP business packets is not more than 512 bytes. All requests that do not meet this feature are blocked. The operation steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security** > **DDoS Mitigation** to enter the DDoS Mitigation details page.

3. On the Layer-4 Proxy Protection tab, select the Layer-4 proxy protection instance you want to configure and click **Protection Configuration**.
4. In the Feature Filtering card, click on **Settings** to navigate to the Feature Filtering page.

5. In the Feature Filtering page, click on **Create**.
6. In the dialog box for creating a new feature filter, establish a feature filtering rule. Depending on your needs, select different protective actions and fill in the relevant fields, then click **Confirm**.



The table below lists the fields of a feature:

Filter feature	Note	Extra Parameter(s)
Source Port	Refers to the source port of access • Supports the input of port numbers within the range of 1-65535. • Supports logical equality or between	-
Destination port	Refers to the target port access	

	• Supports the input of port numbers within the range of 1–65535. • Supports logical equality or between	
Packet data length	Refers to the packet length of the access message. • Supports input of numbers within the range of 1–1500. • Supports logical equality or between	
Detect from IP header	Supports regex matching or keyword matching, where keywords are matched through offset and inspection depth.	• **Offset:** The offset of the data body (payload) after the UDP or TCP header, with an optional range of 0~1500, in bytes. When the offset is 0, the matching starts from the first byte of the data body. • **Inspection Depth:** The content of the data body (payload) to be matched should be entered as a hexadecimal string starting with 0x.
Detect from TCP/UDP header	Supports regex matching or keyword matching, where keywords are matched through offset and inspection depth.	
Detect from payload	• 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 through offset and inspection depth.	

Configuration Protocol Blocking Rule

Last updated: 2023-09-07 15:22:34

Overview

EdgeOne provides the capability to block source traffic to the site with a single click based on the protocol type. You can configure blocking for ICMP, TCP, UDP, and other protocols. Once configured, any detected attack traffic associated with these protocols will be immediately severed.

> **Note:**
> This feature is only supported when the Layer-4 proxy enables Exclusive DDoS protection. Both the default platform protection and Layer-7 site Exclusive DDoS protection do not support configuration.

Scenarios

When your website does not have a specific access protocol, you can block the specified protocol with one click. This allows you to directly filter access requests corresponding to the protocol during traffic cleaning, preventing such requests from being passed through to the source station.

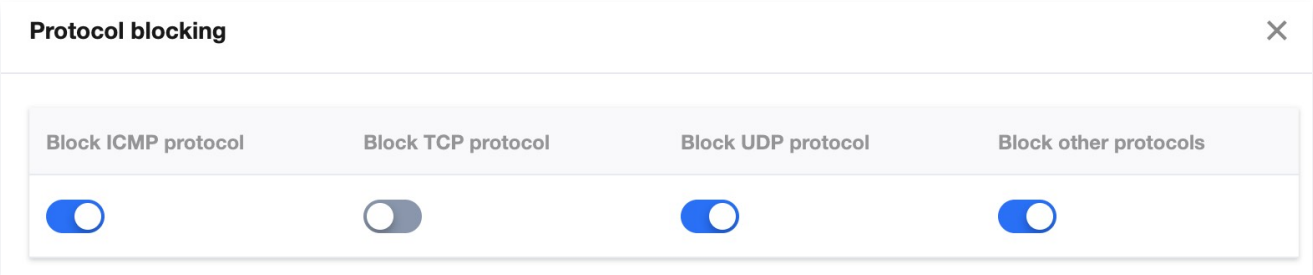
> **Note:**
> Due to the connectionless nature of the UDP protocol (unlike TCP, which has a three-way handshake process), it inherently has security vulnerabilities. If you do not have any UDP-based services, it is recommended to block all UDP protocols.

Instructions

For instance: For all business domain names under the site `example.com`, only TCP protocol connections are open to the public, and requests from other protocols are blocked. The operation steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** you wish to configure to enter the site details page.
2. On the site details page, click **Security** > **Anti-DDoS**.
3. On the Layer-4 Proxy Protection tab, select the Layer-4 proxy protection instance you want to configure and click **Protection Configuration**.
4. Click **Set** in the "Protocol Blocking" section to access the protocol blocking page.

5. On the Protocol Blocking page, click the switch to block the desired protocol. In this scenario, for instance, enable the ICMP, UDP, and other protocol blocking switches. Once enabled, the rules will take effect immediately, and the corresponding protocol requests will be blocked.



Configuration Connections Attack Protection

Last updated: 2023-09-07 15:22:41

Overview

EdgeOne provides protection against connection-based attacks by automatically blocking clients exhibiting abnormal connection behavior. Once the maximum number of abnormal connections from a source IP is enabled for protection, the Edge Security Acceleration Platform will block the source IP and add it to the blacklist if it detects a large number of abnormal connection status messages being initiated from the same source IP in a short period of time. The block lasts for 15 minutes, after which access can be restored once the block is lifted.

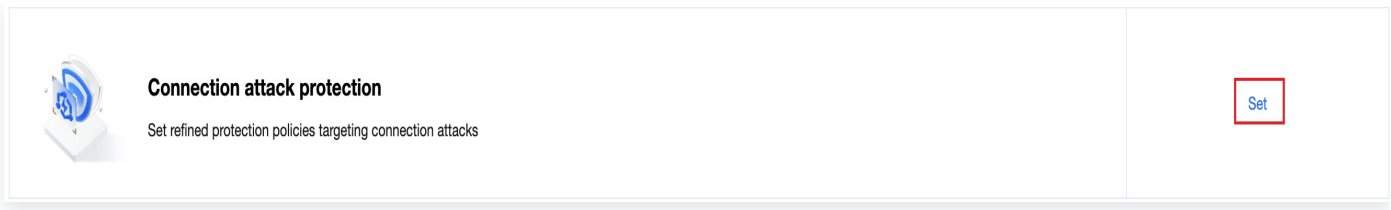
> **Note:**
> This feature is only supported when the Layer-4 proxy enables Exclusive DDoS protection. Both the default platform protection and Layer-7 site Exclusive DDoS protection do not support configuration.

Scenarios

To prevent the exhaustion of TCP connection resources or network resources at the origin server due to a large number of connections, you can protect the origin server by configuring connection-based attack protection.

Instructions

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security** > **Anti-DDoS**.
3. On the Layer-4 Proxy Protection tab, select the Layer-4 proxy protection instance you want to configure and click **Protection Configuration**.
4. In the Connection Attack Protection card, click **Settings** to enter the Connection Attack Protection page.



5. On the Connection Attack Protection page, click **Edit** on the right side of the connection rule. For explanations and handling methods of each connection rule, please refer to Related References.
6. In the rule configuration dialog box, after modifying the settings, click **OK** to complete the rule distribution.

References

Supported Connection Rules

- **Per-IP New Connection Limit:** This rule restricts the number of new connections a single source IP can initiate within a given time frame, preventing attackers from exhausting TCP connection resources through a large number of empty connections.
- **Per-IP Concurrent Connection Limit:** This rule restricts the number of open connections from a single source IP at the same time, preventing attackers from exhausting TCP connection resources through a large number of concurrent connections.
- **Abnormal Connection Limit (Per Source IP):** This rule restricts the number of abnormal connections from a single source IP to EdgeOne at any given time, preventing high-risk clients with a large number of abnormal connection statuses from connecting to the origin and posing a security risk. Abnormal connections can be determined by a combination of different dimension rules such as the proportion of SYN packets, the number of SYN packets, connection timeouts, and abnormal empty connections.
- **Global New Connection Limit:** This rule restricts the number of new connections to the origin site through EdgeOne within a given time frame, preventing attackers from exhausting TCP connection resources through a large number of empty connections.
- **Global Concurrent Connection Limit:** This rule restricts the number of open simultaneous connections between EdgeOne and the origin site at any given time, preventing attackers from exhausting TCP connection resources through a large number of concurrent connections.
- **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 data to the origin to prevent the origin's network and computing resources from being consumed by forged requests from attackers.

Action

- **Limiting New Connections:** Under a single source IP rule, new connection requests from that IP are denied. Under a global policy, all new TCP connection requests are denied.

- **Disconnect and Block:** Disconnect the IP connection and block the IP for 15 minutes.
- **Discarding Excess Data:** Discard requests that exceed the data transfer rate or connection packet rate.

Related References
Action

Last updated：2023-09-07 15:22:48

The Anti-DDoS module offers a variety of handling methods. The processing rules for different handling methods are as follows:

Handling Method	Handling Method Description	Subsequent Action
Intercept (Deny)	Directly discard the request data packets and do not continue to match other policies.	-
Permit (Allow)	Directly allow the access of this request data packet, without further matching other policies.	-
Discard and block	Directly discard the request packet and add the IP to the backend blocklist.	-
Continue protection	Continue to execute matching other policies	Continue to match other policies in sequence

Related Concepts Introduction

Last updated: 2023-09-07 15:22:54

Introduction to DDoS Attacks

A Distributed Denial of Service (DDoS) attack is a malicious attempt to make a targeted server unavailable by blocking its network bandwidth or overwhelming its system with a flood of internet traffic.

Network Layer DDoS Attack

A network layer DDoS attack attempts to make a targeted server unavailable to its intended users by blocking its network bandwidth and exhausting its system layer resources with a flood of internet traffic.
Common attacks include SYN Flood, ACK Flood, UDP Flood, ICMP Flood, and DNS/NTP/SSDP/Memcached reflection attacks.

Transport Layer DDoS Attack

These primarily include Syn Flood, Ack Flood, UDP Flood, and ICMP Flood. Taking Syn Flood attack as an example, it exploits the three-way handshake of the TCP protocol. When the server receives a Syn request, it must keep this connection in a listening queue for a certain period. Therefore, it continuously sends Syn requests to the server without responding to Syn+Ack messages, thereby consuming the server's resources. When the server's listening queue is full, it will be unable to respond to normal user requests, achieving the purpose of a denial-of-service attack.

Application Layer DDoS Attack

This primarily includes DNS DDoS attacks and Web Application DDoS attacks.

- DNS DDoS attacks primarily encompass DNS Request Flood, DNS Response Flood, and a combination of fake and real source DNS Query Flood.
- Web application DDoS attacks primarily include HTTP Get Flood and HTTP Post Flood. An HTTP Get Flood typically involves hackers identifying resource-intensive transactions and pages from a web service or interface, and incessantly sending HTTP Get requests to these transactions and pages. This can lead to the exhaustion of resources on the web application server, preventing it from providing normal services, or it can result in the data center's entrance network bandwidth being fully occupied, rendering the entire data center unable to provide services externally.

CC Attack

CC attacks primarily aim to maliciously occupy the application layer resources of a target server, consuming its processing capabilities and preventing it from providing normal services. Common types of attacks include HTTP/HTTPS-based GET/POST Flood, Layer 4 CC, and Connection Flood attacks.

Protection Capacity

Protection capability refers to the ability to defend against DDoS attacks. Anti-DDoS promises to provide full-force protection based on the maximum DDoS protection capability of Tencent Cloud in the current region.

Cleansing

When the public network traffic of a target IP exceeds the set protection threshold, Tencent Cloud's DDoS protection system will automatically cleanse the public inbound traffic of that IP. The traffic is redirected from the original network path to Tencent Cloud's DDoS cleansing devices via the BGP routing protocol. The cleansing devices identify the traffic for that IP, discard the attack traffic, and forward the normal traffic to the target IP. Under normal circumstances, cleansing does not affect regular access. Only in special scenarios or when the cleansing strategy configuration is incorrect, it may impact normal access. If the traffic continues without abnormalities for a certain period (determined dynamically based on the attack situation), the cleansing system will deem the attack over and stop cleansing.

Web protection Overview

Last updated: 2023-09-07 15:23:01

Web Protection offers application layer protection for HTTP/HTTPS protocols. You can utilize EdgeOne's pre-set security policies or define your own to identify and manage risky requests, safeguard your site's sensitive data, and ensure stable service operation.

Use Cases

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

- **Vulnerability Attack Protection**: For sites involving customer data or sensitive business data, managed rules can be enabled to intercept malicious attack requests such as injection attacks, cross-site scripting attacks, remote code execution attacks, and third-party component vulnerabilities.
- **Access Control**: Differentiate between legitimate and unauthorized requests to prevent sensitive operations from being exposed to unauthorized visitors. This includes control over external site links, partner access control, and filtering of attacking clients.
- **Resource Utilization Mitigation**: Limit the access frequency of each visitor to prevent excessive resource consumption, which could lead to a decrease in service availability. The CC attack protection and rate limiting provided by EdgeOne can effectively alleviate site resource exhaustion, ensuring stable and available services.
- **Mitigating Service Abuse**: Restrict session or business dimension abuse, including scenarios of malicious use such as bulk registration, bulk login, and excessive API usage. It also reinforces usage limits for single sessions (such as users, subscription instances, etc.) to ensure that service resources are used within reasonable limits.
- **API Parameter Verification**: Verify API parameters to ensure the legality of requests and control interface exposure risks.

Web Protection Features

Web Protection offers the following features. It is recommended to configure them based on the type of business and the expected types of client access:

Protection Module	Feature Overview
Managed rules	Identify attack features in the request header or body (including various attack feature categories such as SQL injection, XSS attacks, open source component vulnerabilities, etc.) and take

	appropriate action. These rules are defined and automatically updated by EdgeOne.
CC Attack Protection	Identify CC attacks (Layer 7 DDoS attacks) and take appropriate action.
Custom Rules	Process requests matching specified conditions in a designated manner.
Rate Limiting	The number of requests matching the conditions within a certain period is counted. When this exceeds the specified threshold, the rule is activated and the requests matching the conditions are processed. After the number of requests falls below the threshold, the processing action remains effective for a period of time, then ceases to be effective until triggered again.
Bot Management	Identify non-human access behavior (Bot clients) and take action based on the type or behavior characteristics of the Bot client.
Protection Exception Rules	Requests that match the conditions will bypass the specified security module scan and will not trigger the rules within the corresponding module. For managed rules, more detailed exceptions can be configured to skip the scan of specified managed rules.

CC attack defense

Last updated: 2023-09-07 18:18:30

Overview

CC (Collapse Challenge) attacks, also known as HTTP/HTTPS DDoS attacks, are orchestrated by attackers to occupy the connection and session resources of web services, resulting in the inability to respond to user requests and service denial. To safeguard against CC attacks, EdgeOne offers pre-configured CC attack mitigation strategies that are enabled by default, ensuring the stable online presence of your site.

Note:

1. Attack mitigation aims to ensure business availability and alleviate the degradation of origin site access quality due to malicious resource occupation.
2. To restrict access to sensitive interfaces or mitigate business abuse, please formulate strategies in conjunction with the Rate Limiting feature.
3. To manage the access of crawlers and automated tools, please specify strategies in conjunction with Bot Management.

Utilizing CC Attack Protection

CC attack mitigation identifies CC attacks through rate baseline learning, header feature statistical analysis, and client IP intelligence, and takes appropriate action. EdgeOne offers three pre-configured CC attack mitigation strategies:

- **Access Rate Limit:** This is designed to counteract CC attack behaviors that occupy server resources through high-frequency and large-scale concurrent connection requests. It can limit access frequency based on a single IP source.
- **Slow Attack Mitigation:** This is designed to counter CC attacks that occupy server resources through a large number of slow connection requests. It can eliminate slow connection clients based on the minimum access connection speed limit per session.
- **Smart Client Filtering:** This integrates rate baseline learning, header feature statistical analysis, and client IP intelligence to dynamically generate protection rules in real-time. It performs human-machine recognition for requests from high-risk clients or those carrying high-risk header features. Smart client filtering is enabled by default and executes a JavaScript challenge for clients that comply with the rules.

Configuring High Frequency Access Request Limits

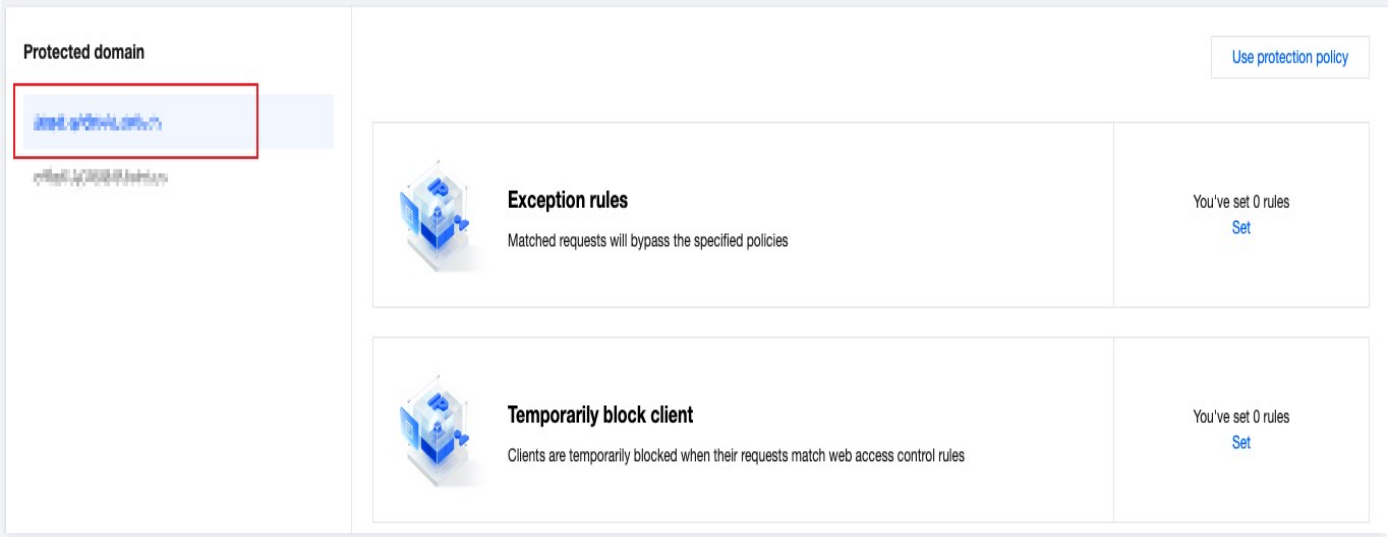
Access rate limit rules restrict the access speed of a domain based on the configured limit level. The limit level offers two types: **Adaptive** and **Fixed**.

- **Adaptive Type**: This calculates the current request rate of the domain, establishes a rate baseline based on the most recent 7 days of requests (the rate baseline is updated every 24 hours), and in conjunction with the configured limit level, restricts the request rate of a single client accessing the domain.
- **Fixed Type**: Limits the request rate of a single client accessing the domain name based on a fixed threshold.

> ⚠ **Note:**
> The access rate limit is applicable to web-based businesses. When a site also provides API interface services, it is recommended to configure protection exception rules for APIs that need to support high-frequency access to prevent normal requests with high frequency from being intercepted. This bypasses the CC attack protection module, and by configuring rate limiting, it precisely limits the exposure of the API interface, avoiding the use of moderate, emergency attack, and strict restriction levels.

Instructions

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security > Web Protection** to access the Web Protection details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.



3. Locate the CC Attack Protection card and click on **Settings**. This will take you to the CC Attack Protection configuration page. Click on **Edit** on the right side of the High-Frequency

Access Request Limit.

4. Configure the restriction level and handling method for high-frequency access requests. The explanations for each restriction level are as follows:

Item	Mode	Scenarios	Rate Cap	Initial Rate Limiting
Adaptive	Loose (Default configuration, recommended)	This is applicable to most Web business scenarios.	Unlimited At least 7,000 calls/minute	2000 requests/5 sec
	Medium	This is suitable for scenarios where the page content is relatively simple, and there is less dynamic data or dynamically loaded content.	1,200-2,400 requests/min	200 requests/5s
	Critical Attack	In the event of an attack, or when other restriction level protections cause business impact due to protective penetration, this restriction level can be selected for emergency protection. Given the strict rate limit of this level, there is a risk of false positives, hence it is not recommended for long-term use.	60-1200 times/min	50 requests/5s

> **Note:**
> The available action methods include **Observe** and **JavaScript Challenge**. For detailed explanations of different action methods, please refer to: Action Methods.

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

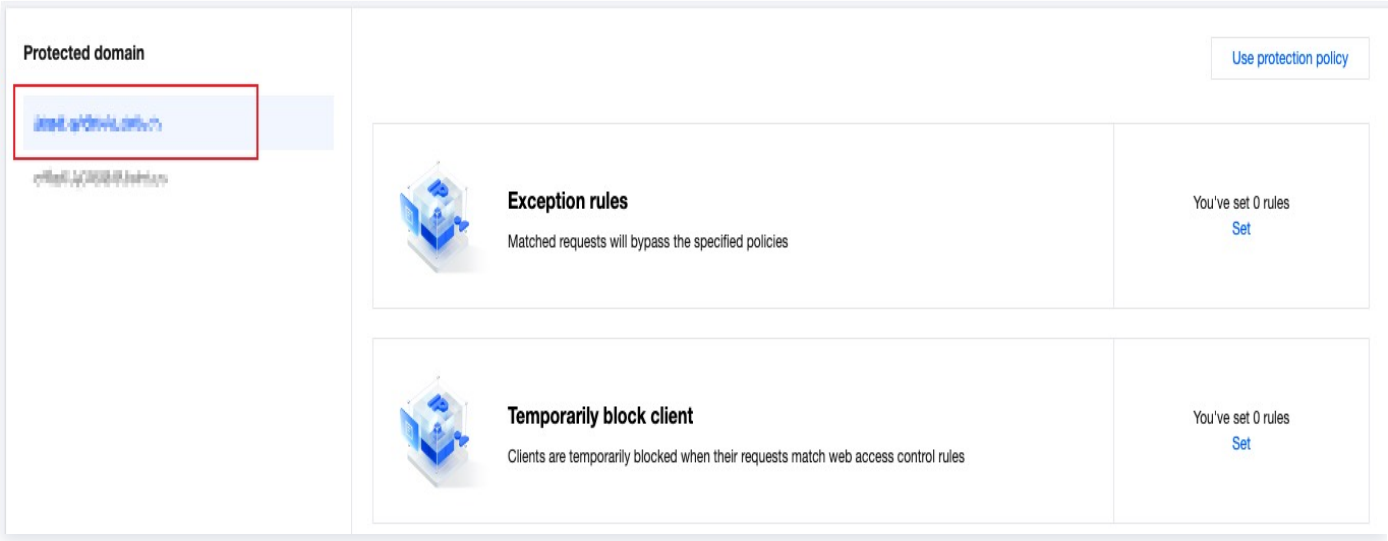
Configuring Slow Attack Protection

By limiting the minimum request rate and setting timeouts, the impact of slow transmission attacks on site resources can be mitigated, preventing a decline in service availability. EdgeOne's slow attack protection supports **Body Transmission Timeout** and **Minimum Body**

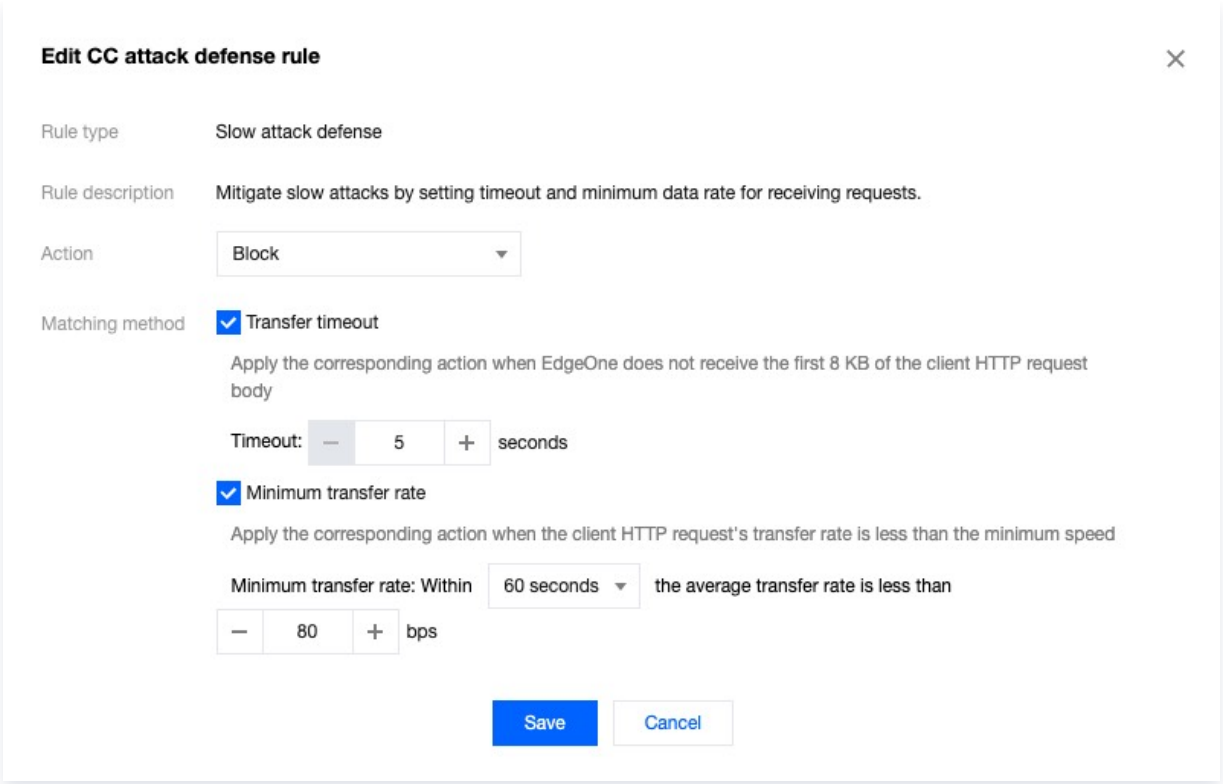
Transmission Rate options. When the body transmission rate is slow, or there is no data transmission for a long time, actions are taken against the client.

Instructions

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security > Web Protection** to access the Web Protection details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.



3. Locate the CC Attack Mitigation card and click on **Settings**. Upon entering the CC Attack Mitigation configuration page, click on **Edit** on the right side of Slow Attack Mitigation.
4. When configuring the matching method for slow attack mitigation rules, the following restrictions can be selected:
   - **Body Transmission Duration:** This mitigates slow attacks that occupy connections without transmitting body data. Specify the **timeout duration** for body transmission. Clients that fail to complete the transmission of the first 8KB of body data within the configured time will be handled in the specified manner. The configuration supports a range of 5–120 seconds.
   - **Minimum transfer rate:** Mitigates attacks that occupy connection and session resources through extremely slow content transmission. You can specify the minimum transfer rate. If the content of the request transmitted within the statistical time window is less than the configured rate, it will be handled in the specified manner. The transfer rate configuration supports a minimum of 1 bps and a maximum of 100 Kbps.



> **Note:**
> Configure the action, supporting two methods: **Block and Observe**. For detailed explanations of different actions, please refer to Action.

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

Intelligent Protection Against CC Attacks

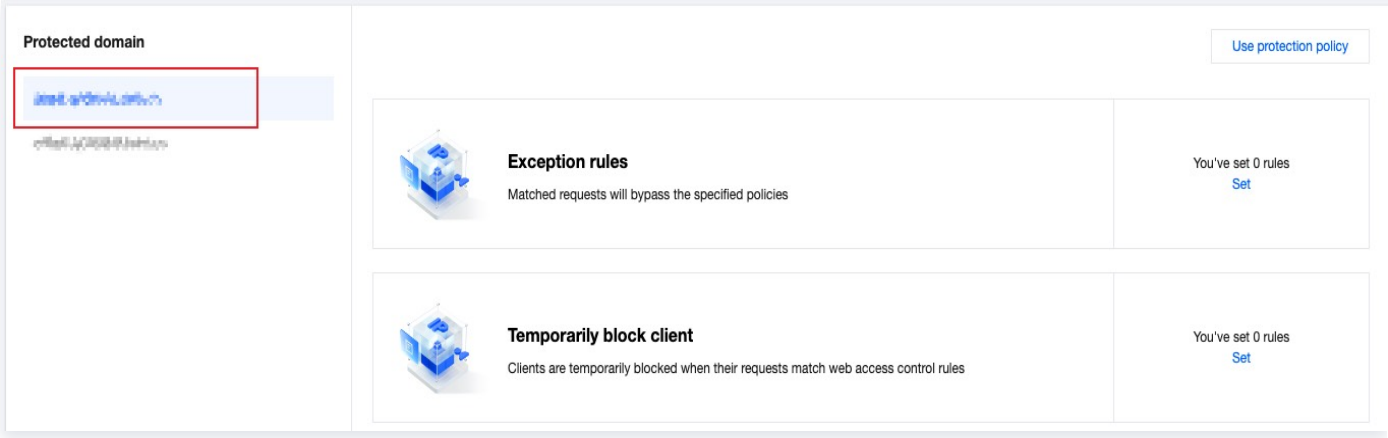
By integrating rate baseline learning, header feature statistical analysis, and client IP intelligence, real-time dynamic protection rules are generated. This targets requests from high-risk clients or those carrying high-risk header features for human-machine identification. Smart client filtering is enabled by default and executes a JavaScript challenge for clients that meet the rules.

> **Note:**
> Smart client filtering uses the business rate baseline as one of its references. Significant business changes (such as new access, volume adjustment, new business, or new activities) may cause false positives in the baseline, leading to erroneous interceptions. In such cases, you can temporarily change the handling method to observation and enable it once the business stabilizes.

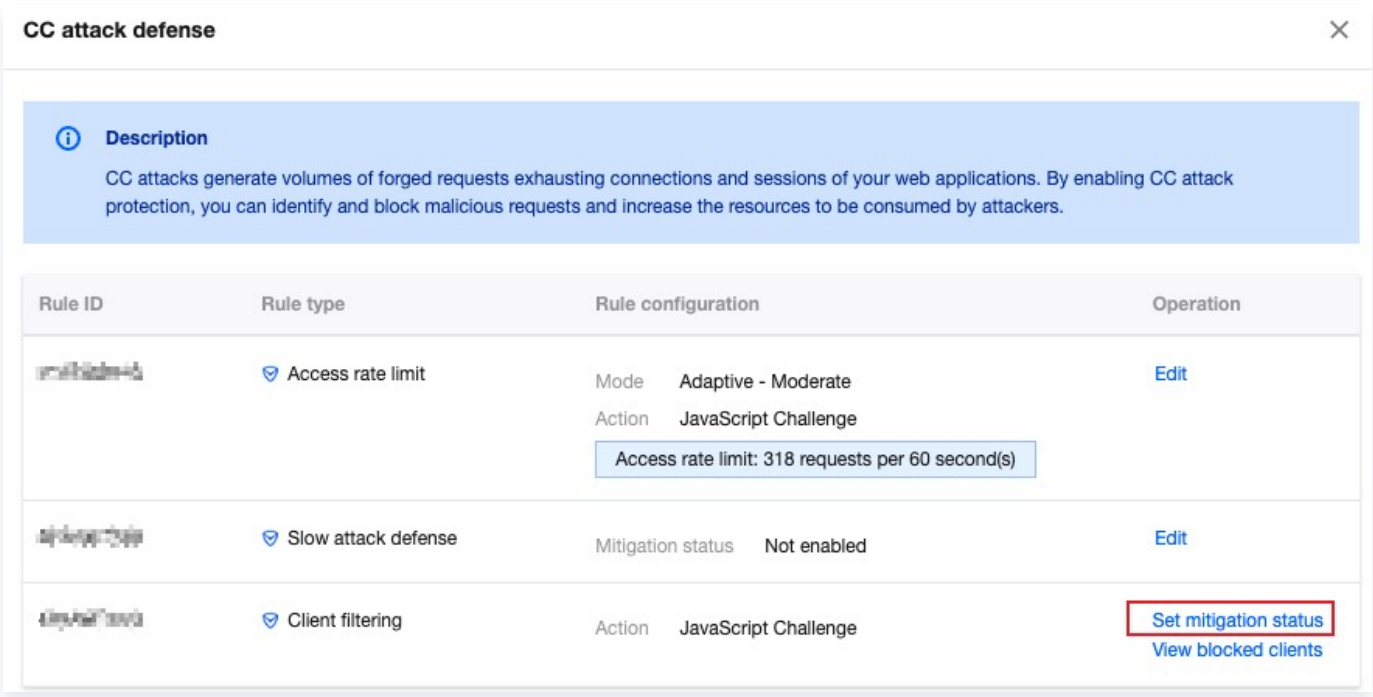
Modifying the Disposition Method for Intelligent CC Attack Mitigation

Should you need to modify the handling method after triggering the intelligent client filtering, you can follow the steps outlined below:

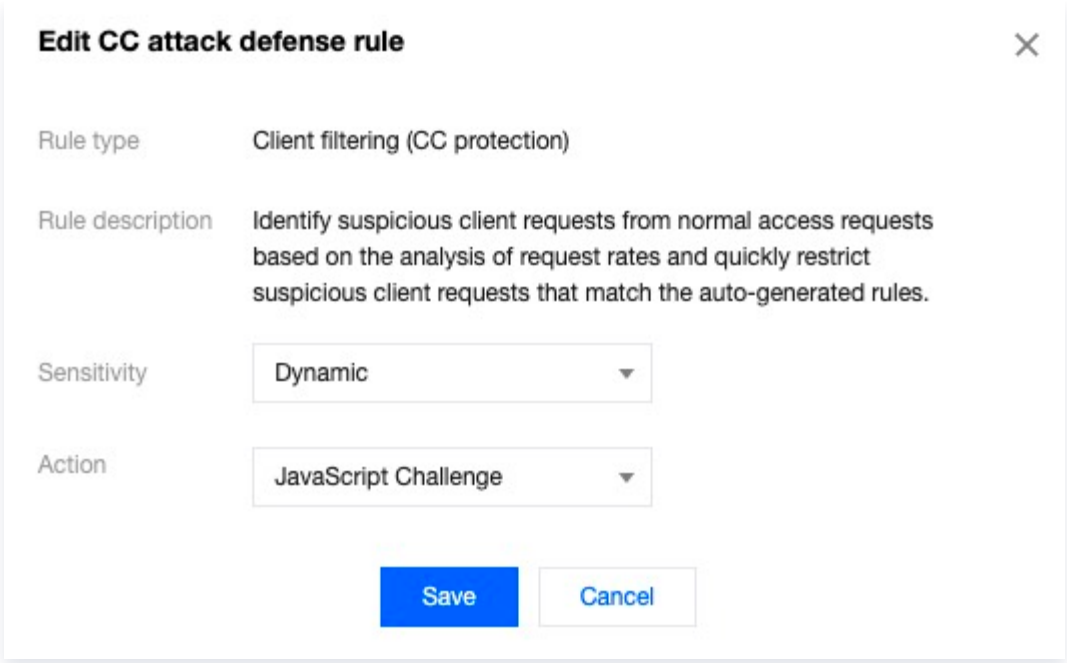
1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security > Web Protection** to access the Web Protection details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.



3. Locate the CC Attack Mitigation card and click on **Settings**. This will take you to the CC Attack Mitigation configuration page. Click on **Set Protection Status** on the right side of Intelligent Client Filtering.



4. Modifying the action of matching rules supports disabling (not enabling), observing, and JavaScript challenges. For detailed explanations of different actions, please refer to Action.

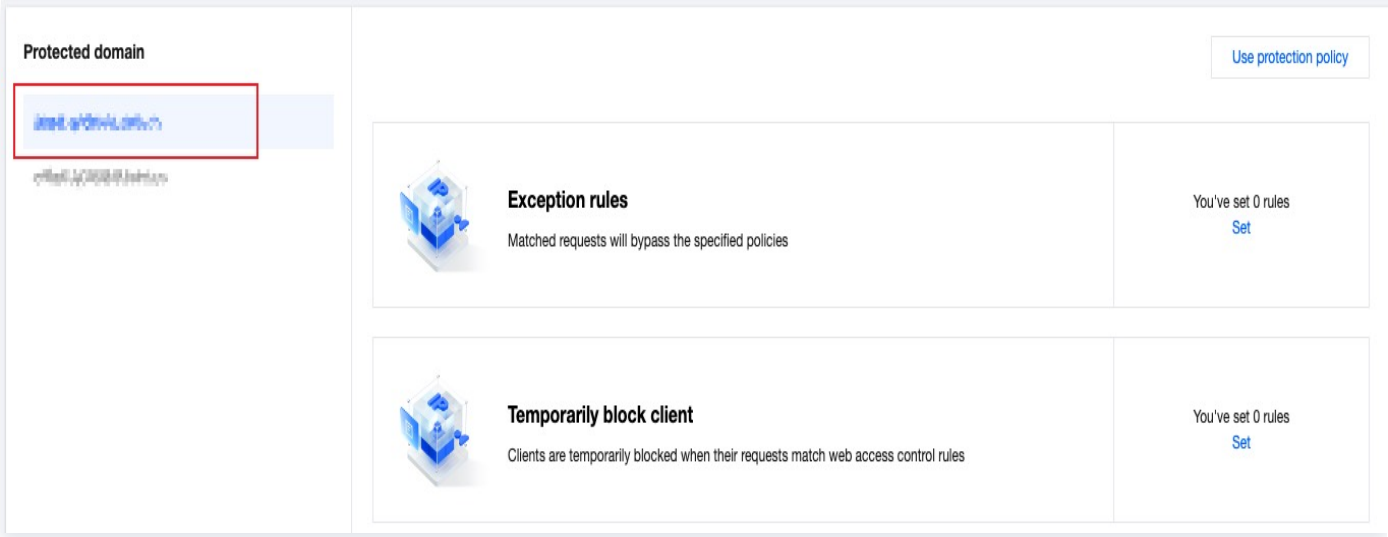


5. Click **Save** to complete the rule configuration.

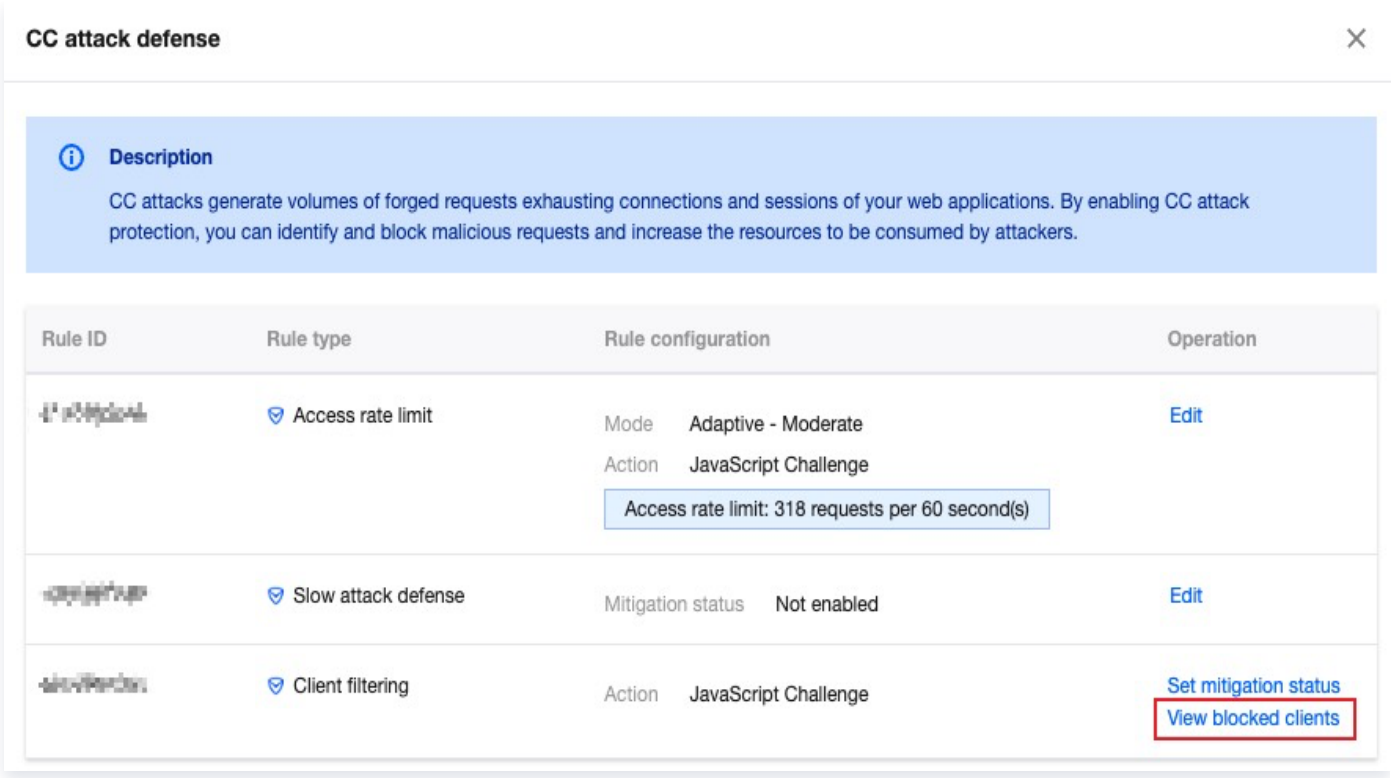
Viewing or allowing the intercepted client list

If you need to view the list of clients intercepted by the smart client filtering, you can proceed as follows:

1. Log in to the EdgeOne console. In the left-hand menu, click on **Site List**. Within the site list, click on the **site** that needs configuration to enter the site details page.
2. On the site details page, click **Security > Web Protection** to access the Web Protection details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.



3. Locate the CC Attack Protection card and click **Set**. Navigate to the CC Attack Protection configuration page and click **View Blocked Clients** on the right side of Intelligent Client Filtering.



4. In the intercepted client page, clicking **Add to Allowlist** in the operation column allows for the swift configuration of the IP as an exception to the protection rule.

Custom rule

Last updated: 2023-09-08 10:53:46

Overview

If your site requires custom user access control policies, such as prohibiting access from specific regions, allowing links to your site's content from specified external sites, or only allowing certain users to access certain resources, custom rules can help. These rules support matching client requests based on a single rule condition or a combination of multiple conditions. By allowing, blocking, redirecting, or returning custom pages, you can control the request policy for matched requests. This provides a more flexible way to limit the content that users can access on your site.

Typical Use Cases and Methods of Application

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

- **Basic Access Control:** Supports single condition request matching, and handles or observes the matched requests. This is suitable for protection in simple scenarios, such as configuring access IP blacklists/whitelists, Referer blacklists, UA blacklists/whitelists, or regional restrictions.
- **Precise Matching Rules:** Supports combination of multiple conditions to match requests, and handles or observes the matched requests. This is suitable for protection configuration in complex scenarios, such as allowing only specific users to access files under a specified path.
- **Managed Custom Policies:** These are policies customized by Tencent security experts and cannot be adjusted via the console. For more details, please see: Managed Custom Rules.

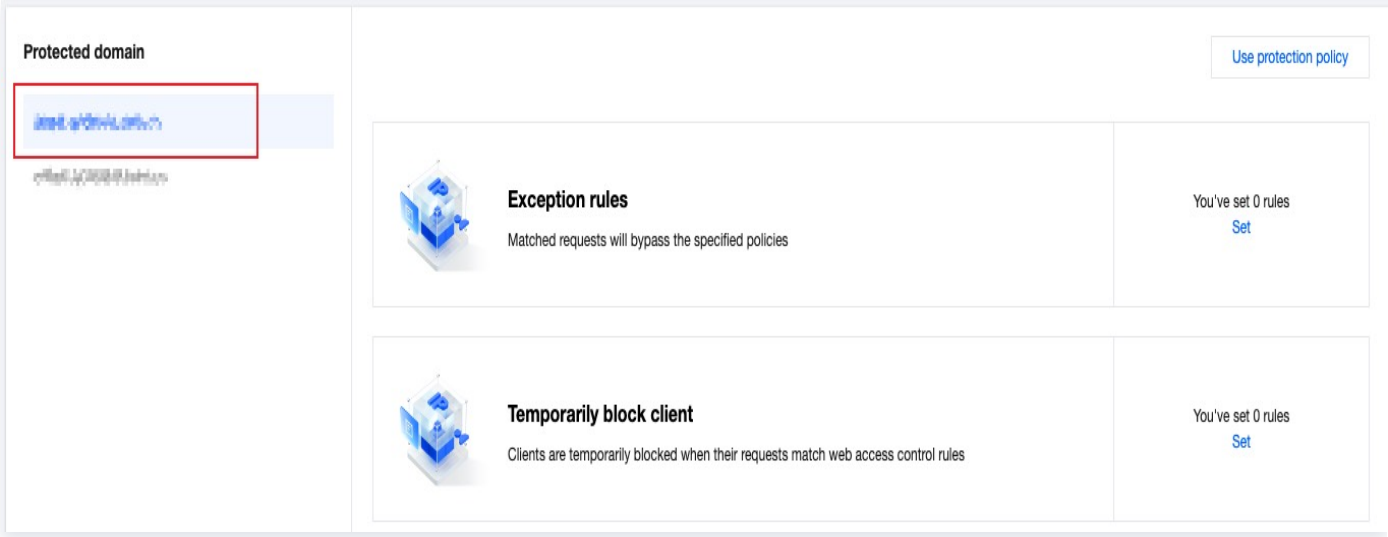
Basic access control

Example Scenario One: Only Allow Access from Specific Countries/Regions

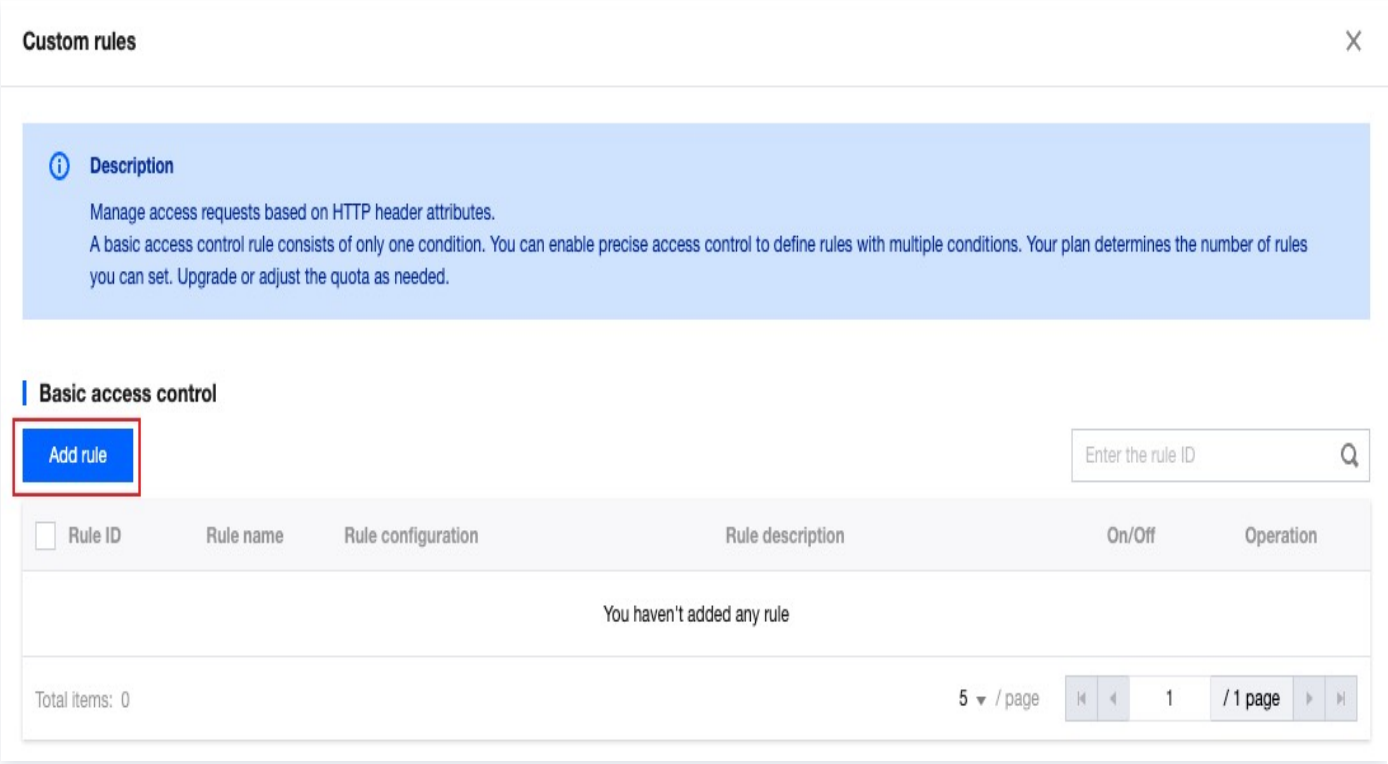
To comply with the regulatory requirements of a specific business region, if your current business only allows access from **regions outside the Chinese mainland**, you may need to restrict the visitor's source region. For such scenarios, you can implement this through the regional control rules in Basic Access Control. The operation steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security > Web Protection** to access the Web Protection

details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.



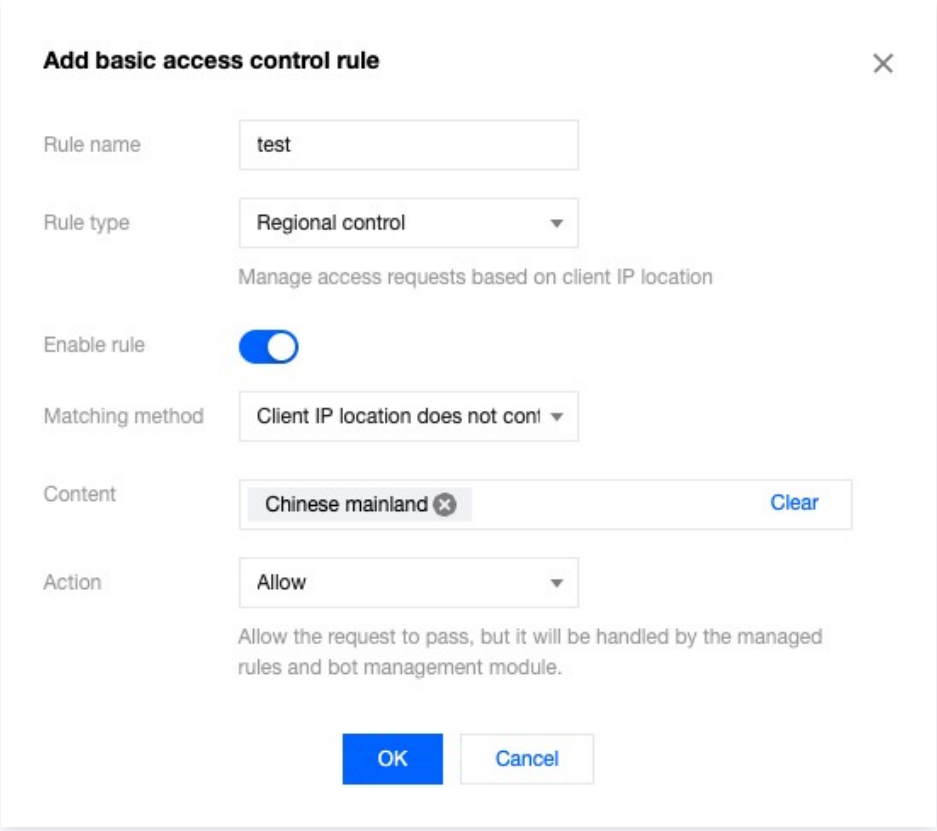
3. Locate the **Custom Rules** section and click **Set**. On the Custom Rules page, click **Add Rule** under Basic Access Control.



4. Within the interface for creating a new basic control rule, after entering the rule name, configure the rule type, matching method, and matching content. The rule type is the matching condition, and requests that match this rule type will be processed according to the handling method configured for this rule.

   For instance, in the current scenario, you can choose the rule type as regional control, select the matching method as 'client IP region does not include', select the matching

content as 'mainland China', and the handling method as 'allow'.

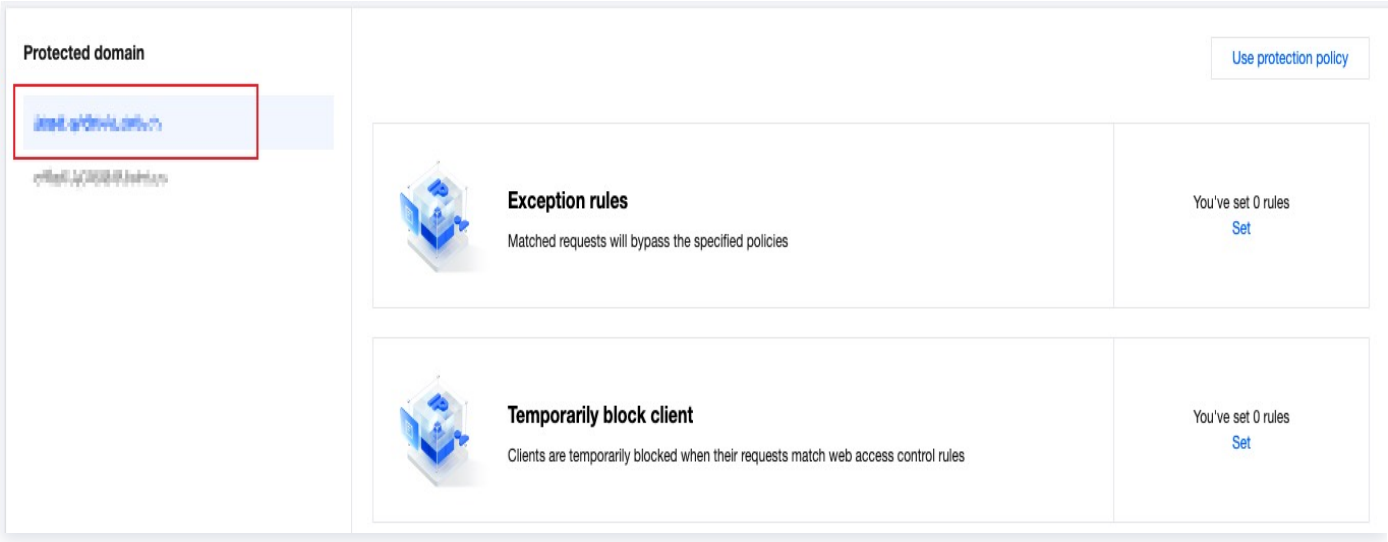


5. Upon clicking **OK**, the rule will be deployed and take effect. At this point, if the client's access IP is from Mainland China, they will not be allowed to access the website.

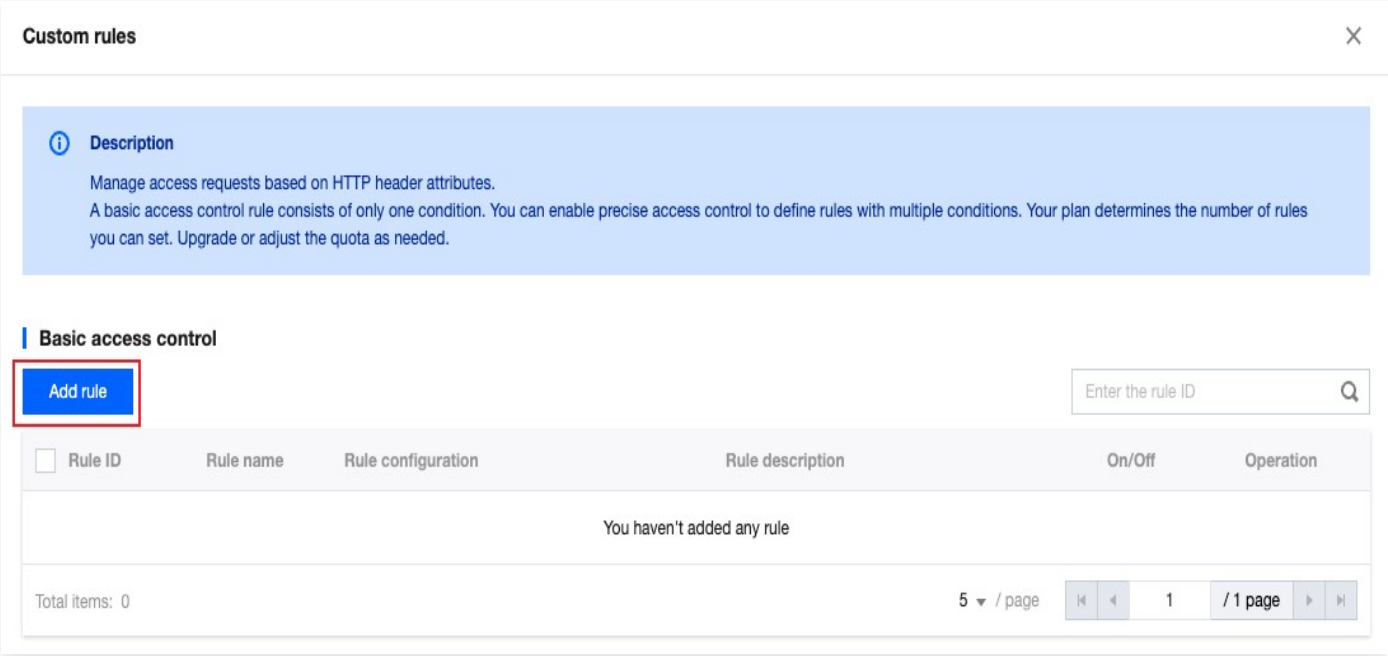
Example Scenario Two: Configuring Referer to Control External Site Access

To prevent unauthorized site access via hotlinking, you can use the Referer control rule in Basic Access Control to block access requests carrying unauthorized Referer headers. For instance, if the site domain `www.myexample.com` needs to allow requests accessed via links from the advertising partner `ads.example.com`, while rejecting content accessed via links from other sites. The operation steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security** > **Web Protection** to access the Web Protection details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.

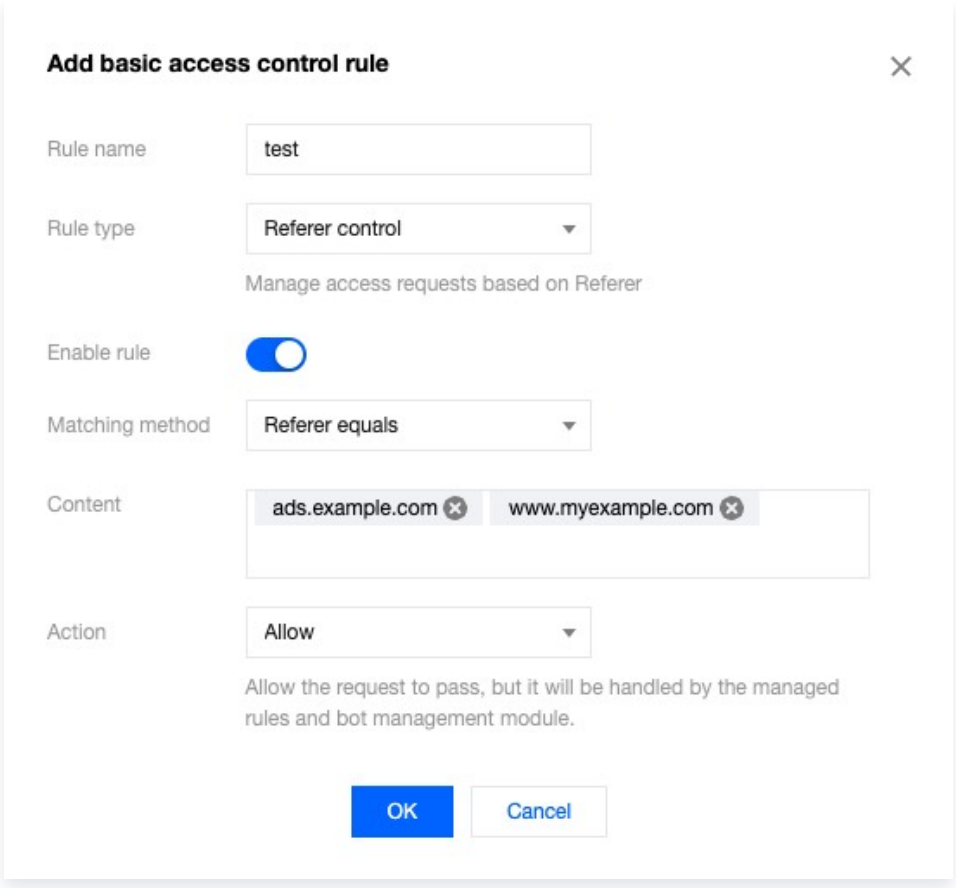


3. Locate the **Custom Rules** section and click **Set**. On the Custom Rules page, click **Add Rule** under Basic Access Control.



4. Within the interface for creating a new basic control rule, after entering the rule name, configure the rule type, matching method, and matching content. The rule type is the matching condition, and requests that match this rule type will be processed according to the handling method configured for this rule.

   For the current scenario, you can choose the rule type as **Referer Control**, select the Referer content that is only allowed to be accessed, including: `www.myexample.com`, `ads.example.com`, and choose the handling method as Allow.



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

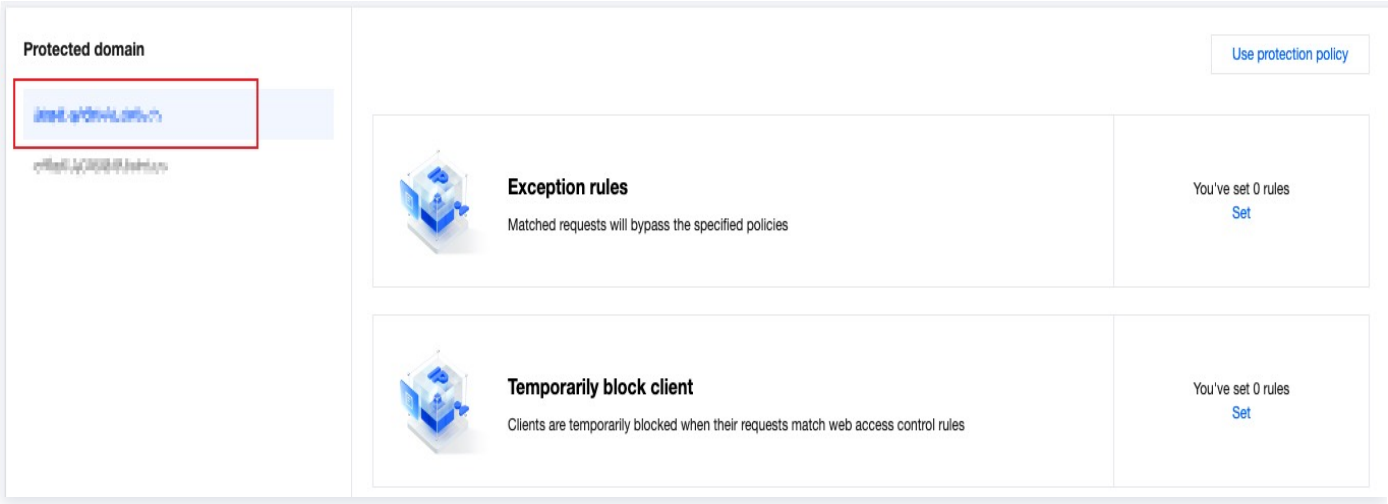
Exact Match Rules

Sample Scenario: Precise Control of Site Sensitive Resource Exposure

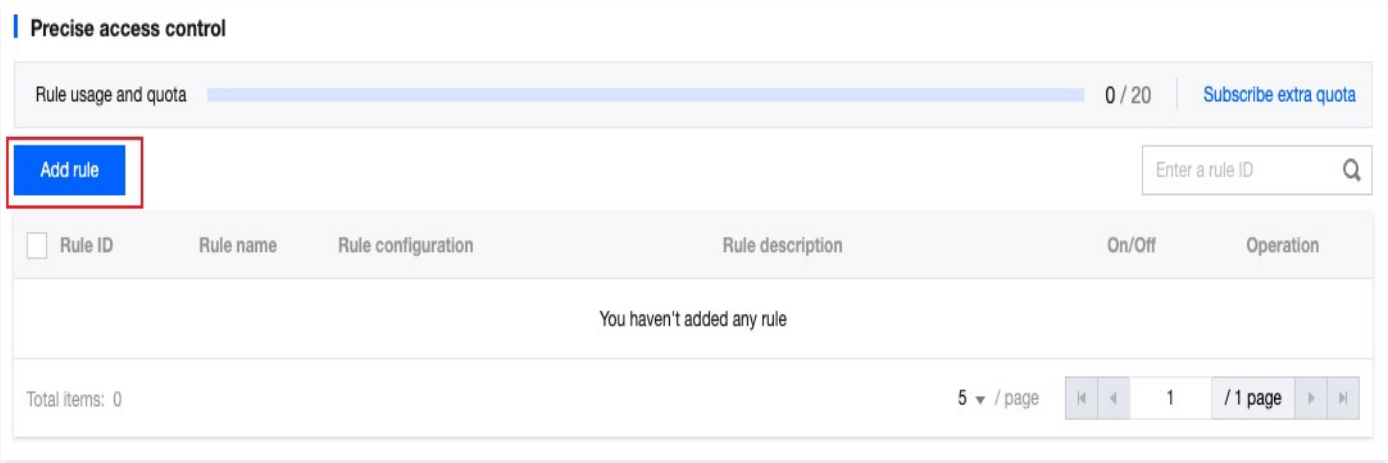
If you need to control the exposure of sensitive site resources (for example, backend management pages) and only allow access from specific clients or specified networks, you can use the **Exact Match Rule** with a combination of **Client IP** matching and **Request URL** matching to achieve this.

For instance, the admin login path for the current site domain `www.example.com` is `/adminconfig/login`. Only the specified client IP user `1.1.1.1` is allowed to log in. The operation steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security > Web Protection** to go to the Web Protection details page. In the list of protected domains on the left, select the domain for which you want to enable protection.



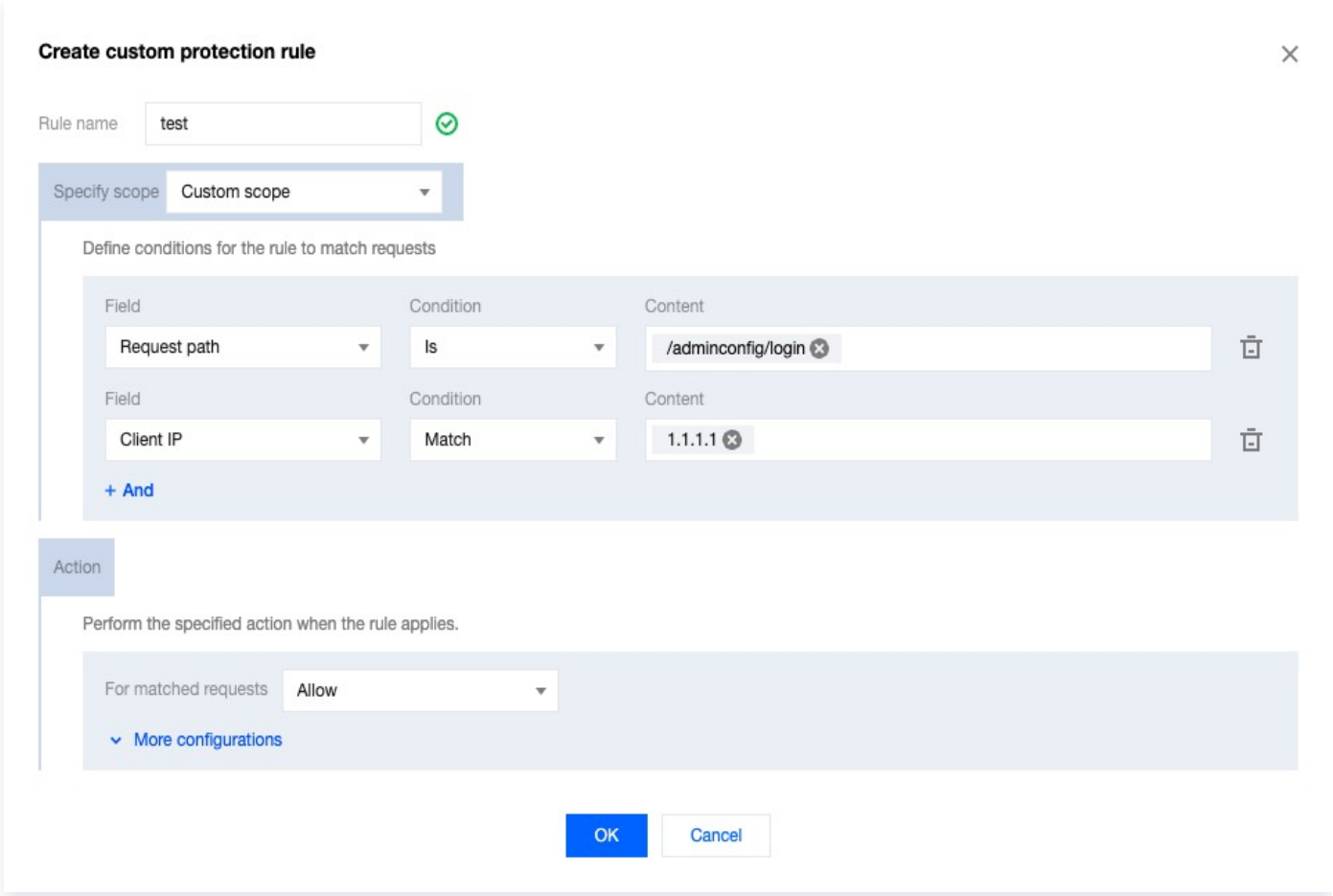
3. Locate the **Custom Rules** card and click **Set**. On the Custom Rules page, click **Add Rule** under the Precise Matching Strategy.



4. Within the interface for creating a new custom protection rule, after entering the rule name, configure the matching fields and the action to be executed.

   For instance, in the current scenario, you can configure the matching field as the request path (Path) equal to `/adminconfig/login` and the client IP matches `1.1.1.1`, with the action set to allow.

> **Note:**
> Click **More Settings** to modify the priority of this rule. The lower the value, the higher the priority.



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

References

Supported Range of Matching Conditions

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

- Basic access control

Rule	Note
Client IP Control	Manage access requests based on client IP
Regional control	Manage access requests based on client IP location
Referer control	Manage access requests based on Referer
User-Agent control	Manage access requests based on User-Agent
ASN Management	Control Access Requests Based on Client ASN Ownership

URL Management	Control access requests based on the request URL, supporting wildcard matching.

- Exact Match Rules

  The exact match rules support the following match conditions, and the level of support varies across different EdgeOne plans.

  > **Note:**
  > For information on supported matching conditions and package limitations, please refer to: Matching Conditions.

  - Request Client IP
  - Request Client IP (prioritizing XFF header match)
  - Custom Request Header
  - Request URL
  - Request Referer Header
  - User-Agent Request Header
  - Request path
  - Request method
  - Cookie
  - XFF header
  - Network layer protocol
  - Application layer protocol:

Supported Handling Methods

Different custom protection rules support different disposal methods. For explanations of different disposal methods, please see Disposal Methods.

Protection Rule Types	Supported Handling Methods
Basic access control	• Observe • Reject
Exact Match Rules	• Allow • Reject • Observe • IP blocking • Redirection

	• Return Custom Page • JavaScript Challenge

Note:
If you want to customize the response page and status code for requests, custom rules support the following configuration methods.

- Using the **Return Custom Page** handling method: You can configure the **Return Custom Page** handling method for a single custom rule (only supports exact match rules). When responding to requests that match this rule, EdgeOne will return the page and status code you specified.
- **Custom Page Use:** You can use the **custom page** configuration to specify the page and status code used by all custom rules when **blocking requests**.

Rate Limiting

Last updated: 2023-09-07 15:24:51

Overview

During the operation of a website, issues such as malicious resource occupation, business abuse, and brute force cracking often arise. If overlooked, these issues can lead to a decline in service quality, generate substantial cost bills, and may even result in sensitive data leakage. To effectively manage these risks, the frequency of client access is a crucial metric. Malicious clients typically access at a higher frequency to swiftly achieve their objectives of cracking logins, occupying resources, and scraping content. By implementing appropriate threshold limits on client access frequency, one can effectively distinguish between normal and malicious clients, thereby mitigating the risks of resource occupation and abuse.

> ⚠ **Note:**
> In managing and combating web crawlers, relying solely on rate limiting strategies may yield limited results. Please combine this with the Bot Management feature to formulate a comprehensive crawler management strategy.

Typical Use Cases and Configuration Methods

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

- **Precise Matching Rules**: User-defined access frequency control policies. These rules support the combination of multiple conditions to match requests, limiting the request rate from each source. They are suitable for distinguishing between normal user access and malicious high-frequency access in most scenarios.
- **Managed Custom Policies**: These are policies customized by Tencent security experts and do not support console adjustments. For more details, please refer to Managed Custom Rules.

Exact Match Rules

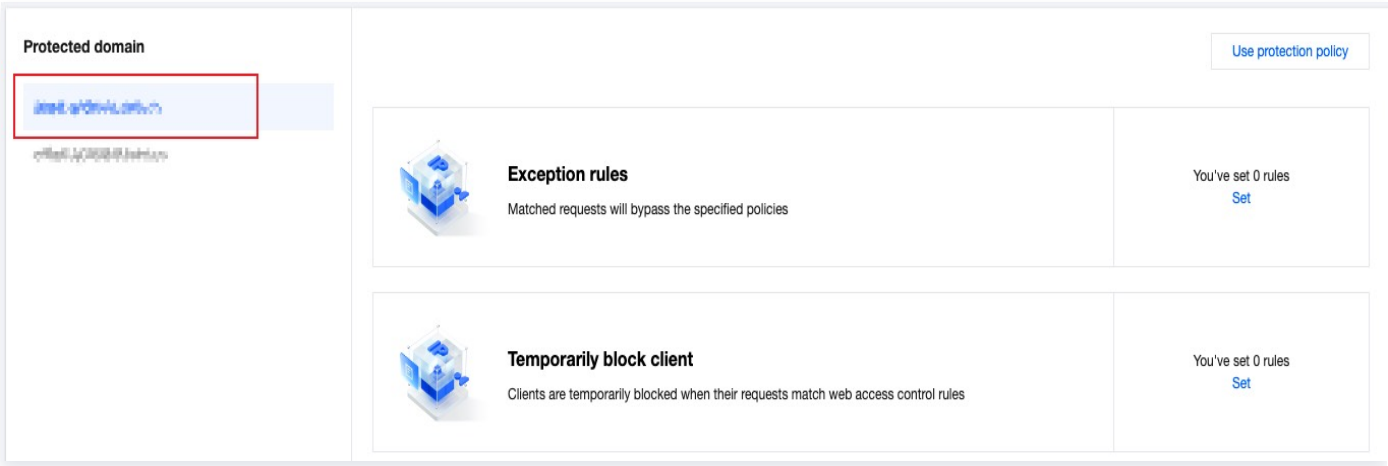
Example Scenario One: Limit the access frequency to the login API interface to mitigate against brute force and password cracking attacks.

In scenarios facing credential stuffing and brute force attacks, attackers typically attempt to access or crack information by frequently using the login API interface. By limiting the request

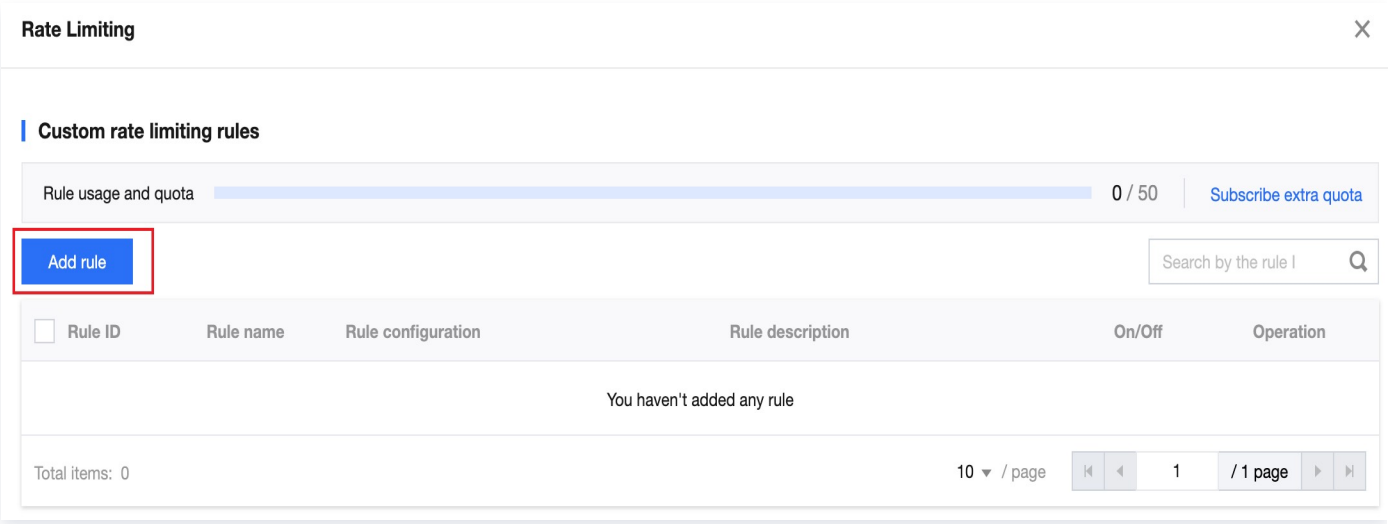
frequency to the login interface, we can significantly alleviate the attacker's cracking attempts, thereby effectively defending against such attacks and protecting sensitive information from being leaked.

For instance, the site domain `www.example.com` provides an external interface `/api/UpdateConfig`. The permitted access call frequency for this interface is 100 times per minute. If this 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. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security Protection > Web Protection** to enter the Web Protection details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.

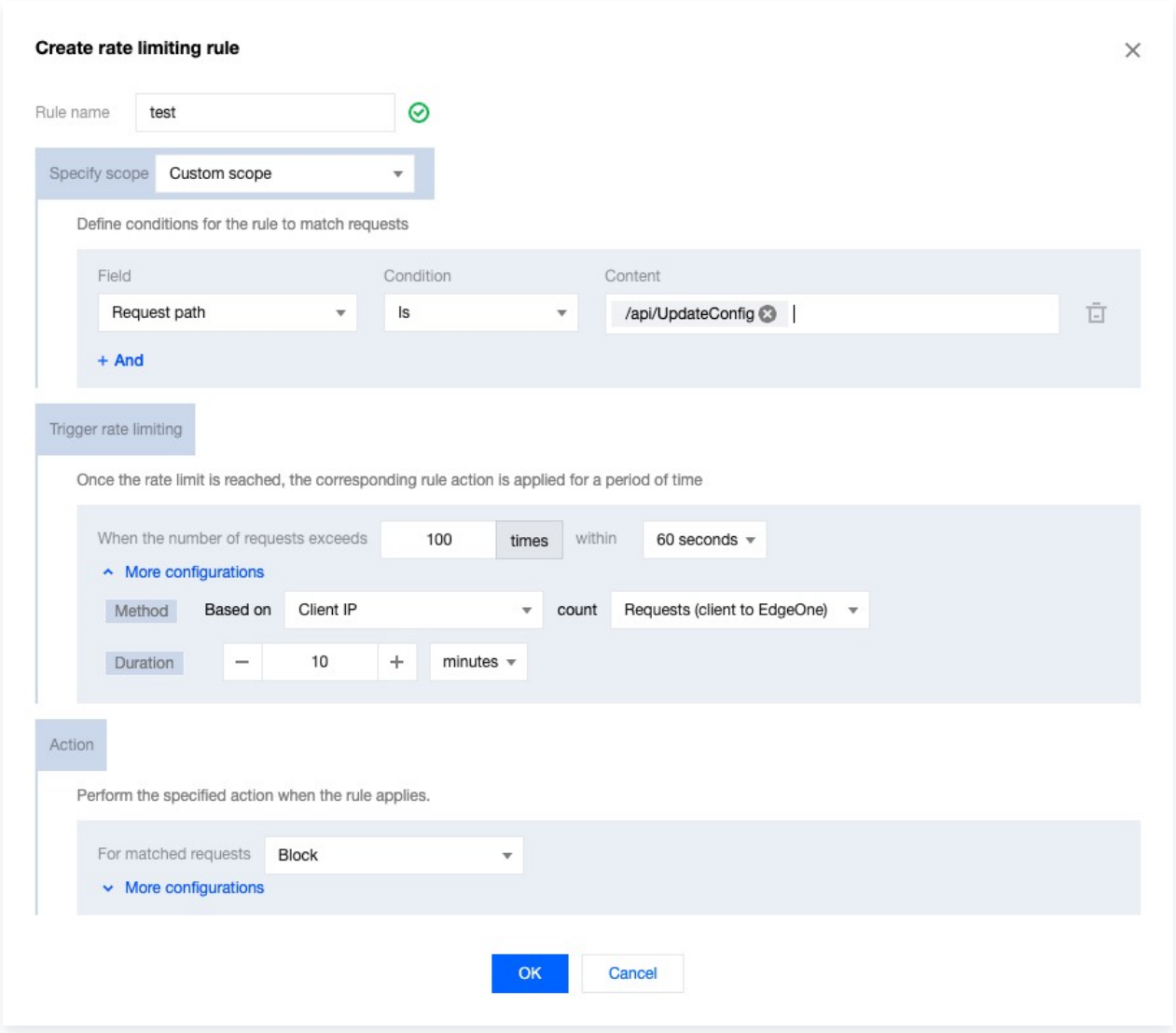


3. Locate the rate limiting card and click **Set**. Upon entering the rate limiting configuration page, click **Add Rule** under the precise rate limiting rules.



4. Within the pop-up rule page, configure as follows:
   4.1. Fill in the rule name, and select **Custom Protection Object** as the matching object.

4.2. Under the match condition list option, configure the match conditions for the rule. In this scenario, for instance, select the match field **Request Path (Path)** equals `/api/UpdateConfig` .
4.3. Configure the triggering method for this rule. In this scenario, for example, the rule is triggered when the count exceeds 100 times within a 60-second period. Click on **More Settings** to expand the configuration for the statistical method. The statistical method is triggered when a single client IP requests the EdgeOne node. Once triggered, this state is maintained for 10 minutes.
4.4. Select "Block" for the action to be executed. The complete rule configuration is as follows:

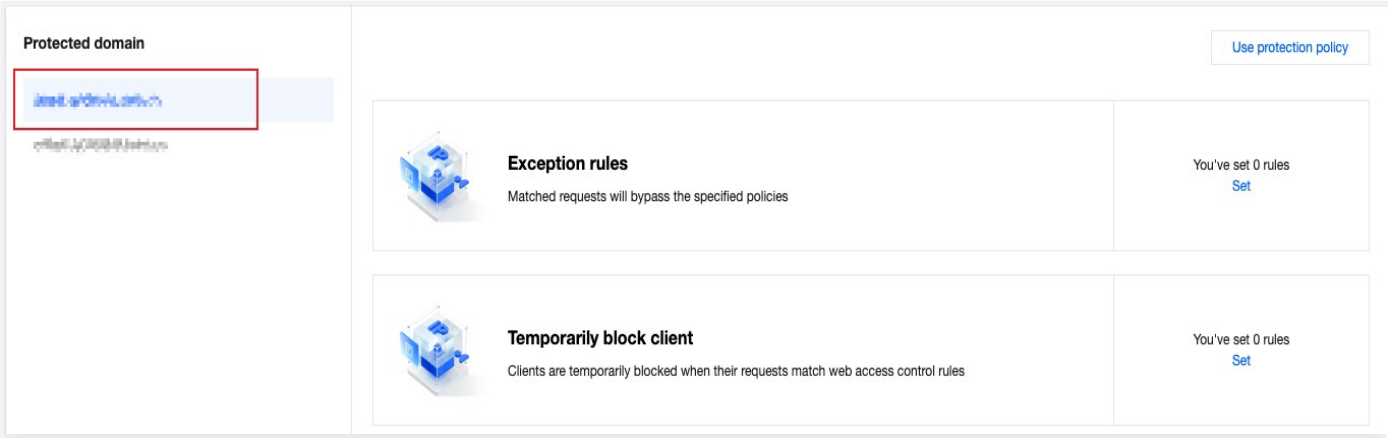


5. Upon clicking **OK**, the rule will be deployed and take effect.

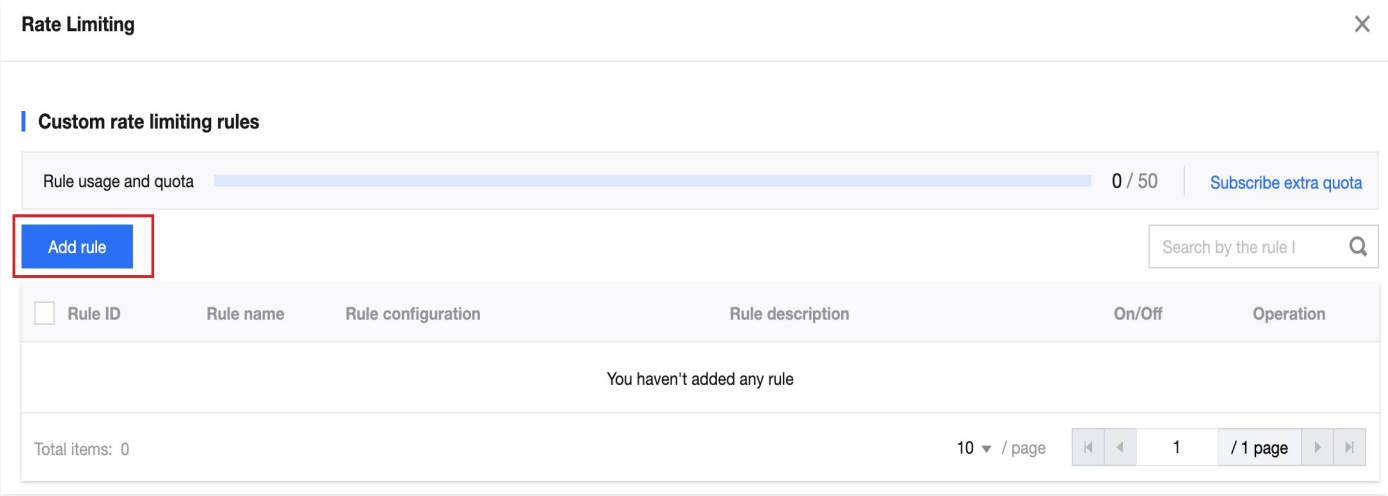
Example Scenario Two: Limit the request rate that results in a 404 status code to alleviate random resource scanning.

Malicious clients often randomly scan site image resources in an attempt to scrape content, which can lead to the origin server responding with a `404` error due to non-existent access paths. By limiting the request frequency that results in a `404` status code from the origin server, EdgeOne can prevent malicious attackers from massively scanning and requesting static resources. This reduces the number of error responses from the origin server, alleviates server pressure, and enhances the security and stability of static resource sites. For instance, for the static image resources `.jpg` , `.jpeg` , `.webp` , `.png` , `.svg` of the site domain `www.example.com` , 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. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security Protection > Web Protection** to enter the Web Protection details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.

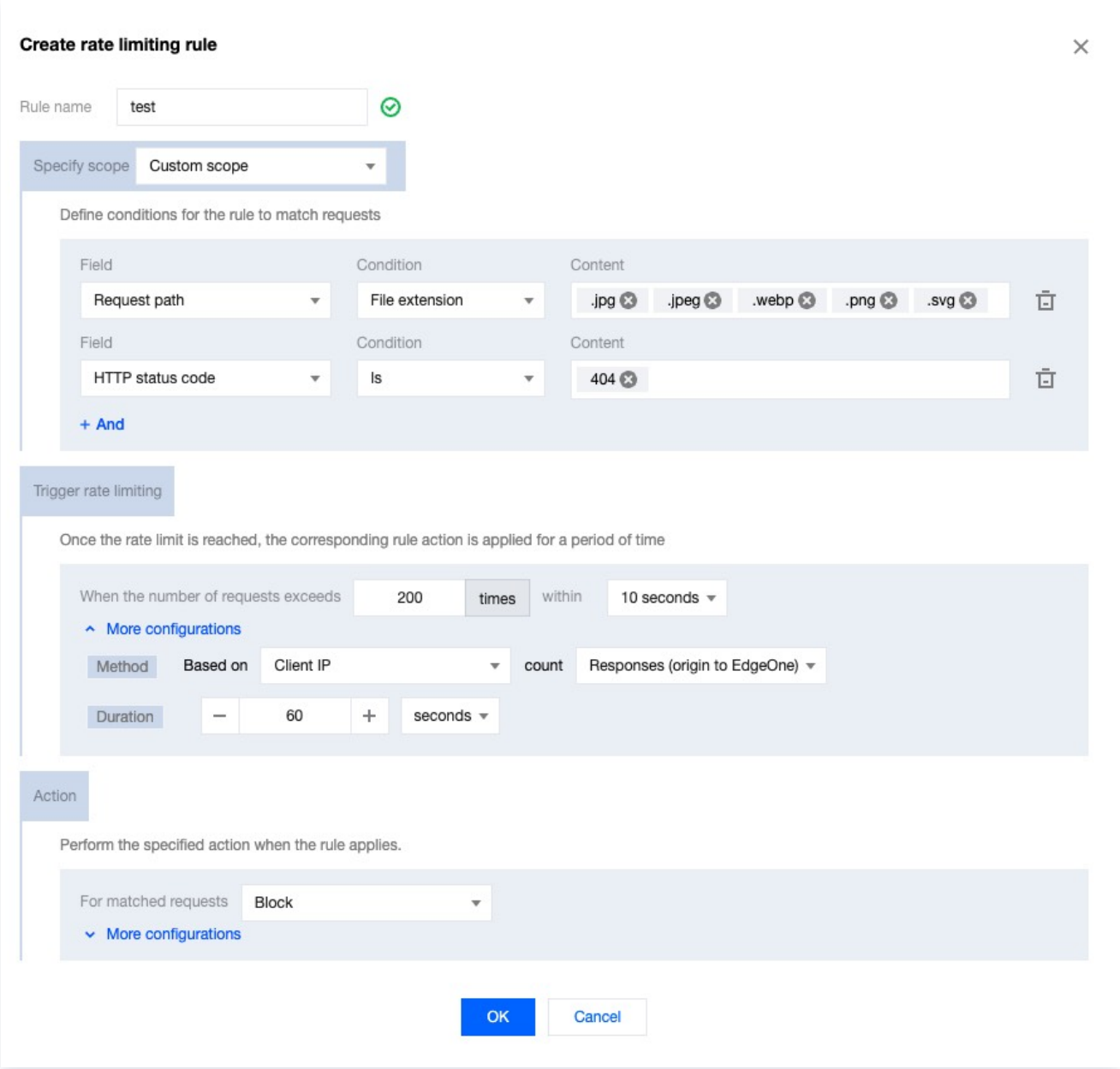


3. Locate the rate limiting card and click **Set**. Upon entering the rate limiting configuration page, click **Add Rule** under the precise rate limiting rules.



4. Within the pop-up rule page, configure as follows:

4.1. Fill in the rule name, and select **Custom Protection Object** as the matching object.
4.2. In the match condition list option, configure the match conditions for the rule. In this scenario, for instance, select the **Request Path (Path)** match field, and the **File Extension Match** content includes static resource types such as `.jpg` , `.jpeg` , `.webp` , `.png` , and `.svg` image files.
4.3. Click **+And** to add a new match condition. In the newly added match condition, select the match field for HTTP status code equal to 404 requests.
4.4. Configure the triggering method for this rule. In this scenario, for example, the rule is triggered when the count exceeds 200 times within a 10-second technical cycle. Click on **More Settings** to expand the configuration for the statistical method, which is based on the dimension of a single client IP. When the origin server responds to the EdgeOne node and the rule is triggered, this triggered state is maintained for 60 seconds.
4.5. Select "Block" as the action to be executed. The complete configuration rule is as follows:



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

References

When creating rate limiting rules, it is necessary to configure the rule matching object, trigger method, and handling method. The explanations for each configuration item are as follows:

- **Matching Objects**: Set matching condition combinations based on request origin, header characteristics, response status codes, etc. Rate limiting rules only control the business that matches these conditions. For detailed explanations of matching conditions and the level of support in different packages, please refer to Matching Conditions.
- **Trigger Method**: The rule will count statistics according to the statistical rules configured in the trigger method. When the cumulative number of requests within the technical cycle exceeds the threshold, the rule is triggered and the corresponding limit action is executed. Statistics are 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). You can define the following parameters for the trigger method:

- Counting Period: The length of the rolling time window used for counting. It supports a minimum of 10 seconds and a maximum of 60 seconds, configured in increments of 10 seconds.
- Statistical Method: This differentiates the source of requests, with rate limiting applied to the request rate for each source. It supports both client IP and client IP with priority matching to the XFF header.
- Rate Threshold: The number of requests allowed from each source (such as a client IP) within a counting cycle.
- Trigger State Retention Duration: The duration for which the request from the source matching the conditions continues to be limited after the rule is triggered. It supports a minimum of 1 second and a maximum of 48 hours.

- **Action**: When requests exceed the limit threshold, corresponding restrictive actions are taken. These include blocking, observing, and JavaScript challenges. For detailed explanations of these actions, please refer to Action.

> **Note:**
> If multiple rate limiting rules exist, a single request can match multiple rule contents simultaneously, and the decision to trigger each rule is based on different statistical methods. Once a rule is triggered and the request is intercepted, the remaining rules will not be triggered. When multiple rules are penalized simultaneously, they are executed in the order of the triggered rule's priority, with rules having a lower priority number matched first.

Exception rules

Last updated: 2023-09-07 15:24:57

Overview

The protection exception rules offer a centralized configuration option for access allowlists, enabling the swift configuration of legitimate requests to avoid interception by other modules. Moreover, when EdgeOne's built-in preset protection policies (such as CC attack protection, managed rules, etc.) fail to accurately distinguish legitimate requests, the protection exception rules can provide you with fine-tuned configurations, precisely specifying the requests or request parameters that need to be allowed.

> **Note:**
> This feature is only supported by the EdgeOne Enterprise Plan.

Typical Use Cases and Configuration Methods

Protection exception rules can specify normal requests that match certain characteristics to bypass the scanning of specified modules or rules, based on existing protection policies.

> **Note:**
> 1. Supports bypassing **custom rules, rate limits, CC attack protection, and managed rules** protection modules.
> 2. To bypass the Bot Management module, please configure using **Bot Management** > **Protection Exception Rules** or **Custom Bot Rules**.

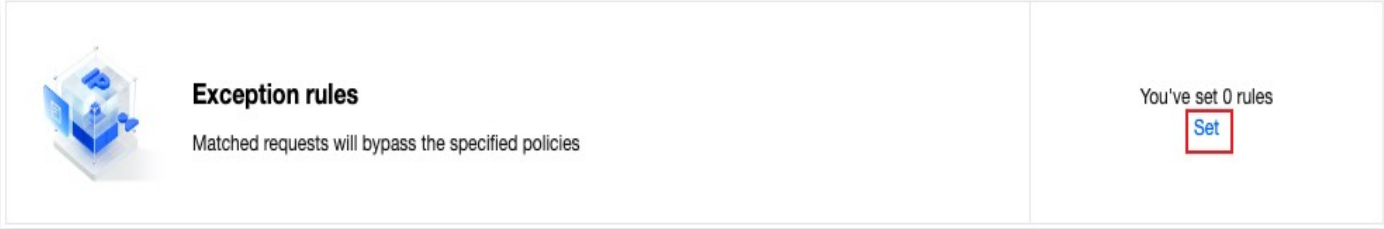
Example Scenario One: Specifying high-frequency API interface requests to bypass CC attack protection scanning

The current site domain is `api.example.com`, and the API interface for event reporting is `/api/EventLogUpload`. During a sudden increase in business, there may be scenarios of sudden high-frequency access. Such access patterns are easily recognized as attacks by the CC attack protection and intercepted. For this interface, you can configure protection exception rules to bypass the CC attack protection module and avoid false positives. The operation steps are as follows:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click on **Security Protection > Web Protection** to access the list of

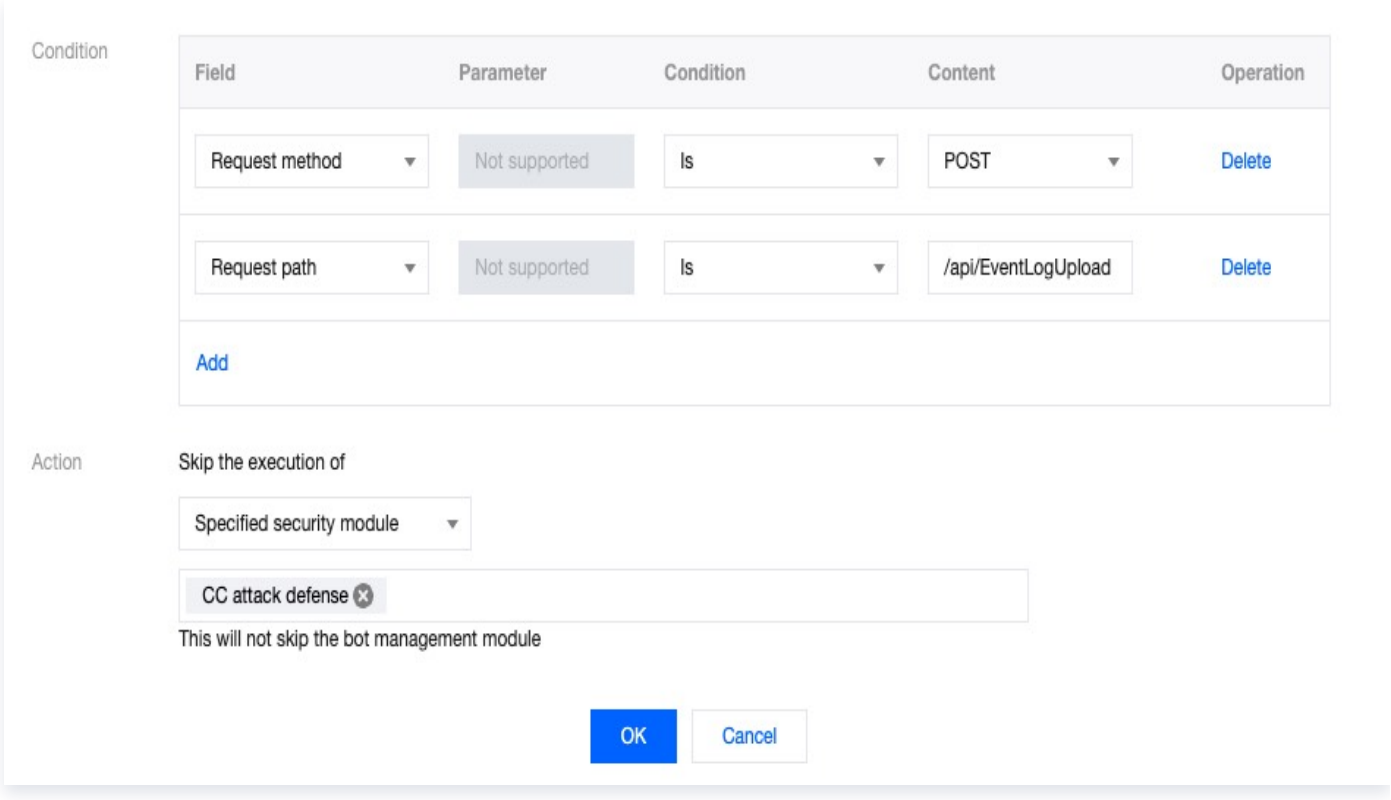
protected domains on the left side of the Web Protection details page. Select the domain for which you wish to enable protection, for instance, `api.example.com`.

3. Locate the Protection Exception Rules card and click **Set**. Navigate to the **Web Protection Exception Rules** list and click **Add Rule**.



4. In the pop-up window for creating a new web protection exception rule, fill in the rule name and select **Complete Request Bypass Rule** as the exception type.

5. Configure the request matching conditions and disposal methods. For example, in a typical scenario, set the matching field to request method equals `POST`, and request path equals `/api/EventLogUpload`. The disposal method is set to CC attack protection in the specified security protection module. Multiple matching fields can be configured, and the simultaneous existence of multiple conditions implies an "AND" relationship. For a detailed introduction to matching conditions, refer to: Matching Conditions.



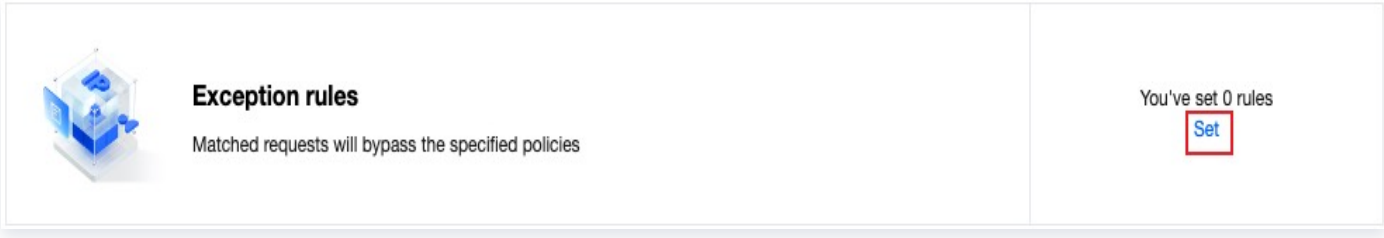
6. Click **Confirm** to complete the addition of this rule. At this point, the `POST` requests of the API interface reported by this event log will not be intercepted by the CC attack protection module, avoiding the possibility of false interceptions caused by high-frequency log reporting, while other interfaces can normally receive detection and protection.

Example Scenario Two: Preventing Personal Blog Content from Being Incorrectly Intercepted by Vulnerability Protection

The domain `blog.example.com` under the current site is used for blog content sharing, and this blog is built on WordPress. The blog content may share technical related text (for example: SQL and Shell command examples), and the protection rules may be triggered when publishing a blog due to the blog content text matching the characteristics of an SQL injection attack. Through the protection exception rules, you can configure a 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 the SQL injection attack rule scan, avoiding false positives and interception of blog content. The operation steps are as follows:

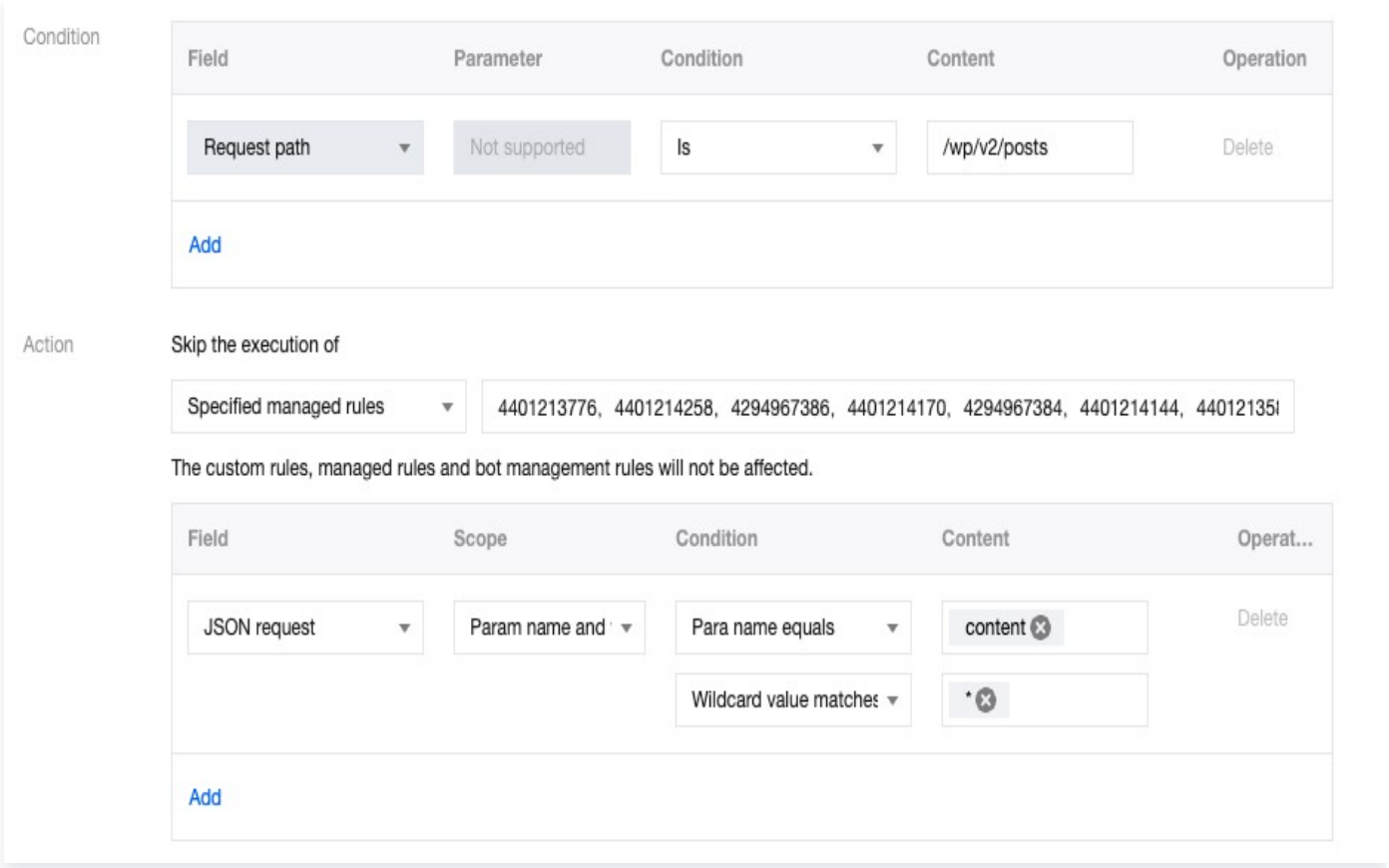
1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click on **Security Protection > Web Protection** to access the list of protected domains on the left side of the Web Protection details page. Select the domain for which you wish to enable protection, for instance, `api.example.com`.
3. Locate the Protection Exception Rules card and click **Set**. Navigate to the **Web Protection**

Exception Rules list and click **Add Rule**.



4. In the pop-up window for creating a new web protection exception rule, enter the rule name and select 'Skip rule scanning for certain request fields' as the exception type.

5. Configure the request matching conditions and disposal methods. As per the reference scenario, you can set the matching field to the request path equal to `/wp/v2/posts`. The disposal method can be set to specify the managed rule package to include all SQL injection protection rules, and not to scan the JSON request content for specified parameter names equal to `content`, and parameter values wildcard matched to `*`. For a detailed introduction to matching conditions, refer to Matching Conditions.



6. Click **OK** to complete the addition of this rule. Now, when the request path equals `/wp/v2/posts` for blog post publication, the blog content will not undergo SQL injection attack protection rule verification, preventing normal text content from being mistakenly scanned as an attack behavior.

References

The table below describes the types of exception fields supported when certain request fields bypass rule scanning:

Category	Option
JSON request	• All Parameters • Matching Parameters with Specified Names • Param name and value
Cookie Header	• All Parameters • Matching Parameters with Specified Names • Param name and value
HTTP header	• All Parameters • Matching Parameters with Specified Names • Param name and value

URL Encoded Content or Query Parameters	• All Parameters • Matching Parameters with Specified Names • Param name and value
Request URI	• Query String Section • Path Segment • Full path
Request body	• Request body • File path segment

Note:
The matching condition parameters are completed by specifying both the parameter name and value matching conditions simultaneously. Both the parameter name and value support complete matching and wildcard pattern matching.

Managed Custom Rules

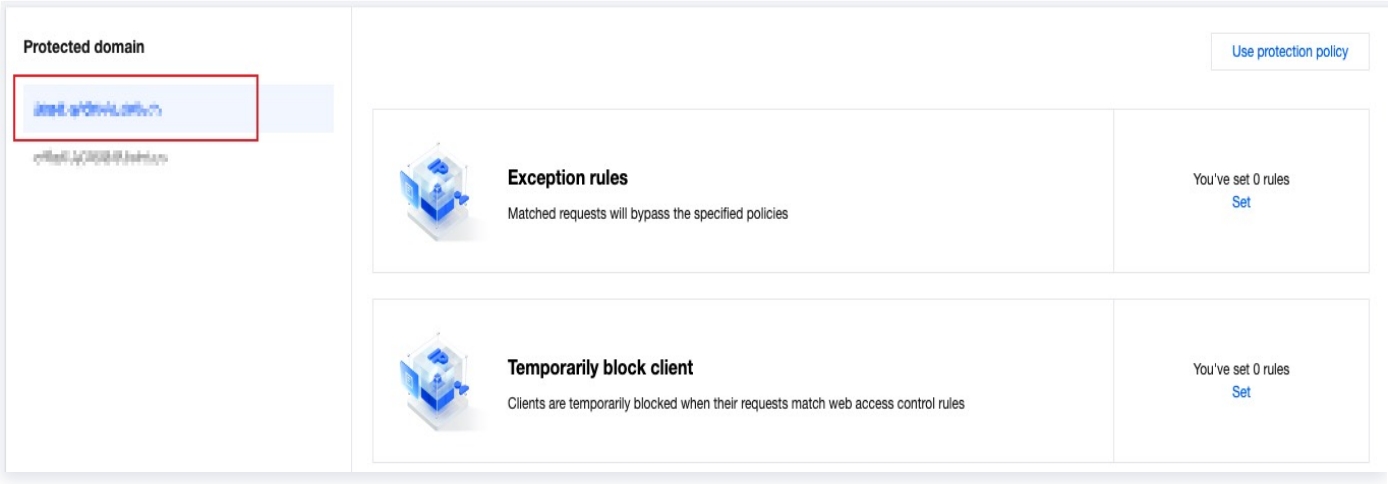
Last updated: 2023-09-07 15:25:04

When utilizing the security expert services provided by EdgeOne (including event assurance, emergency attack and defense, security hosting, and policy customization services), Tencent's security experts will tailor security policies for your business based on the business scenario and attack methods. The hosted custom policy only provides rule display and does not support console adjustment of matching conditions or disposal methods. If your business changes, or if you have special security protection demands, please contact Tencent Cloud Technical Support.

> **Note:**
> Custom rules and rate limiting support hosted custom rules.

The customized rules will be displayed in the hosted custom policy list. If you currently have customized hosted rules, you can view them by following these steps:

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security > Web Protection** to access the Web Protection details page. From the list of protected domains on the left, select the domain for which you wish to enable protection.



3. Locate the custom rules or rate limiting card, and click **Set**. You will then see the hosted custom rules.

Related References
Web Protection Request Processing Order

Last updated: 2023-09-08 11:07:11

Upon receiving a request, Web Protection first processes it through various security modules in the following order. Only requests that have passed the security module scan will continue to be processed by other functional modules.

Module Processing Sequence	Request Processing Method
Protection Exception Rules	When a request matches multiple rules, all corresponding rules will be activated.
Custom Rules	When a request matches multiple rules, they are executed from highest to lowest priority (priority values from smallest to largest) Note 1.
Rate Limiting	All rules hit by the request are counted, and rules that meet the rate conditions are independently activated Note 2. Rules that meet the rate conditions are executed from high to low priority (priority values from small to large)Note 2.
CC Attack Protection	When a request hits multiple rules, all matched rules will be activated.
Bot Management	For more information, please refer to 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 priorities are equal, the rules are executed in the following order: Observation > Allow > Managed Challenge > JavaScript Challenge > Redirect > Return to Specified Page > IP Ban > Block.
Note 2: A hit on an active rate limiting rule does not affect the statistical count of other rate limiting rules. When a single request hits multiple rate limiting rules, it is matched

and handled according to the priority order of the active rate limiting rules. When multiple rate limiting rules of the same priority level are active and matched by a request simultaneously, they are executed in the order of handling methods: Observe > Allow > Managed Challenge > JavaScript Challenge > Redirect > Return to Specified Page > Block IP > Intercept.

Action

Last updated: 2023-09-07 18:25:52

The Web Protection module offers a variety of action options. The actions supported may vary between different functional modules, please refer to the specific module documentation for details.

Action	Action Description	Subsequent Actions
Observe (Monitor)	Logs are merely recorded, no action is taken.	Continue to match other rules
Intercept (Deny)	Return an error page and error status code.	-
Permit (Allow)	Bypass other rules of the current function (Custom Rule, Rate Limit).	Continue to match other effective rules
Redirection (Redirect)	Redirect to a specified page, you can designate a site URL deployed on EdgeOne.	-
Return to Specified Page (ReturnCustomPage)	Return a custom page file, supporting the upload of local page files not exceeding 4KB in size.	-
Block IP (BlockIP)	Discard traffic from the specified client IP for a certain duration.	-
JavaScript Challenge (JSChallenge)	Respond with a redirected page (HTTP 302) carrying JavaScript code to verify client browser behavior. Only client IPs that pass the verification can continue to access.	Requests that pass the challenge continue to match other rules.
Managed Challenge	Dynamically select the appropriate challenge type based on request characteristics, aiming to reduce the use of CAPTCHA. EdgeOne's managed challenges include JS challenges and	Requests that pass the challenge continue to

	redirect CAPTCHA pages, suitable for various firewall rules.	match other rules.

Match Condition

Last updated: 2023-09-07 18:26:26

Overview

Web Protection controls access by matching various conditions of the request. The following sections provide a detailed explanation of the various matching condition options, their descriptions, and related configuration methods and limitations.

Utilizing Matching Conditions

You can specify the scope of a rule's effectiveness using its matching conditions, controlling the scope of protection exception rules, custom rules, rate limits, and custom bot rules.

> **Note:**
> When multiple matching conditions are configured, the rule only takes effect when all matching conditions are met.

Matching Condition Options and Descriptions

> **Note:**
> The matching conditions that can be configured may vary depending on the rule type and the EdgeOne plan you have subscribed to. For specific support information, please refer to the corresponding feature introduction documentation.

Matching Condition Options	Conditions Explanation	Standard	Enterprise Plan
Request Client IP	Matches the source IP address of the request. Supports matching based on region, ASN, IP, and CIDR block. • When matching using IP and CIDR blocks, IP groups can be referenced. • A single matching condition can be configured with up to eight IP groups.	This feature is supported.	This feature is supported.
Request Client IP (prioritizing	When a request carries a valid XFF (X-Forwarded-For) header, the first IP in the XFF	Unavailable	This feature is

XFF header match)	header is matched; otherwise, the source IP address is matched.		supported.
Custom Request Header	Matches the specified header of the request, providing additional parameter options to match the value of a specific header name. • Ignoring the case. • Supports equals to, not equals to, includes, excludes, matches wildcard pattern, does not match wildcard pattern, length greater than, length less than, content is empty, does not exist, and regular expression match. • A maximum of 128 match values are supported.	Unavailable	This feature is supported.
Request URL	Matching the request's URL. • Ignoring the case. • Supports equals to, not equals to, includes, excludes, matches wildcard pattern, does not match wildcard pattern, length greater than, length less than, content is empty, does not exist, and regular expression match. • A maximum of 128 match values are supported.	Matching conditions do not support regex matching.	This feature is supported.
Request Source (Referer Header)	Matching the Referer header of the request. • Ignoring the case. • Supports equals to, not equals to, includes, excludes, matches wildcard pattern, does not match wildcard pattern, length greater than, length less than, content is empty, does not exist, and regular expression match. • A maximum of 128 match values are supported.	Matching conditions do not support regex matching.	This feature is supported.
Request Content Type (Accept Header)	Matching the Accept header of the request. • Ignoring the case. • Supports equals to, not equals to, includes, excludes, matches wildcard pattern, does not match wildcard pattern, length greater than, length less than, content is empty, does not exist, and regular expression match. • A maximum of 128 match values are	Unavailable	This feature is supported.

	supported.		
Request path	Matches the path part of the request URL (excluding query parameters). • Ignoring the case.	Unavailable	This feature is supported.
Request method	Matching the request method. • Ignoring the case. • Multiple selections are supported: GET, POST, HEAD, PUT, DELETE, TRACE, OPTIONS, CONNECT.	Matching conditions do not support regex matching.	This feature is supported.
Cookie	Match the specified request Cookie header parameter value. The Cookie parameter name must be specified. • Ignoring the case. • Supports equals to, not equals to, includes, excludes, matches wildcard pattern, does not match wildcard pattern, length greater than, length less than, content is empty, does not exist, and regular expression match. • A maximum of 128 match values are supported.	Unavailable	This feature is supported.
XFF header	Matching the XFF (X-Forwarded-For) header of the request. • Ignoring the case. • Supports equals to, not equals to, includes, excludes, matches wildcard pattern, does not match wildcard pattern, length greater than, length less than, content is empty, does not exist, and regular expression match. • A maximum of 128 match values are supported.	Unavailable	This feature is supported.
Network layer protocol	Match the type of IP protocol used in the request. • Multiple selections are supported: IPv4, IPv6.	Unavailable	This feature is

			supported.
Application layer protocol	Match the application layer protocol used in the request. • Multiple selections are supported: HTTP, HTTPS.	Unavailable	This feature is supported.
Response status code	Matching the HTTP status code of the response. • Supports rate limiting only when configured based on response statistics. • A maximum of 20 status codes can be matched simultaneously.	Unavailable	This feature is supported.

Bot Management

Last updated: 2023-09-07 15:25:28

Overview

Based on request and session characteristics, client reputation intelligence, and smart behavior analysis, the Bot Management feature identifies and restricts access from bot clients (non-browser clients such as proxies, crawlers, scanners, search engine bots, and API clients), identifies and handles high-risk malicious requests (such as malicious scans, botnets, ATO attack sources, high-risk proxies, and brute force attacks), and reduces false positives and blocking for low-risk crawlers and legitimate APIs.

Follow steps below to optimize bot management rules.

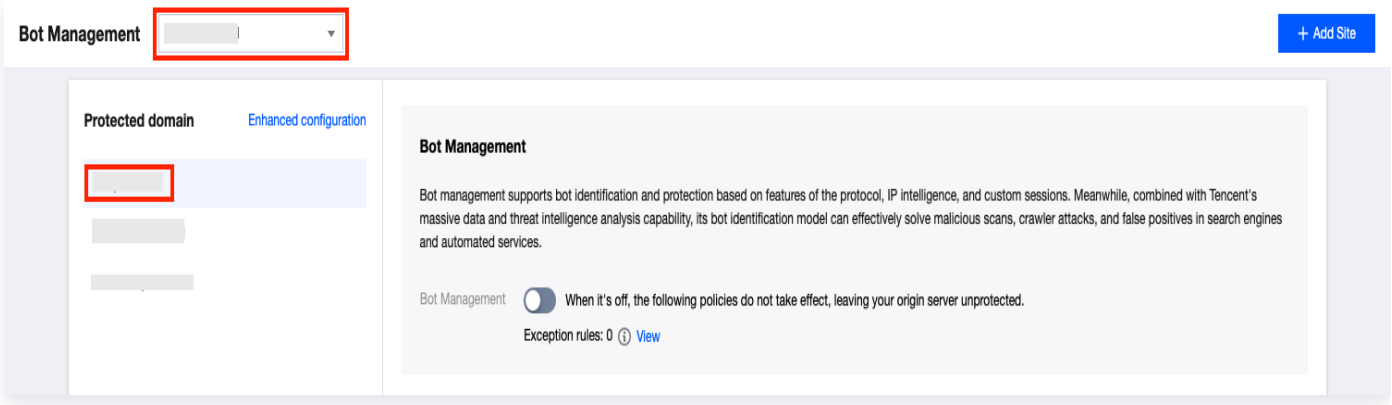
1. Change the rule action to **Observe**. In this way, the bot management feature allows matched requests and records a rule match log.
2. Send a known normal or need-to-block request.
3. Check the rule matching logs recorded by bot management. For normal requests, set the action to **Observe** or **Ignore**. For need-to-block requests, set the action to **CAPTCHA** (**JavaScript Challenge** or **Managed challenge**) or **Block**.

Basic Bot Protection Settings

EdgeOne can process requests by characteristic, such as UA, search engine, or IDC.

> **Note**
> Configuration suggestion: The feature identifies bot requests based on the characteristics of static client requests.
> - UA feature rules: Identifies clients of a specific type. This rule category is applicable to most general scenarios. We recommend that you configure a rule, set the Action to Observe first, and then adjust settings according to the result.
> - Search engine rules: Identifies bot clients of search engines. This rule category is applicable to non-webpage sites (such as API services). If your business is open to search engines, we recommend that you do not use this rule category.
> - IDC rules: Identifies clients from specified IDCs or ISPs. We recommend that you configure a rule, set the Action to Observe first, and then adjust settings according to the result.

1. Log in to the EdgeOne console. Choose **Security** > **Bot Management** on the left sidebar, and select the required site and subdomain name.

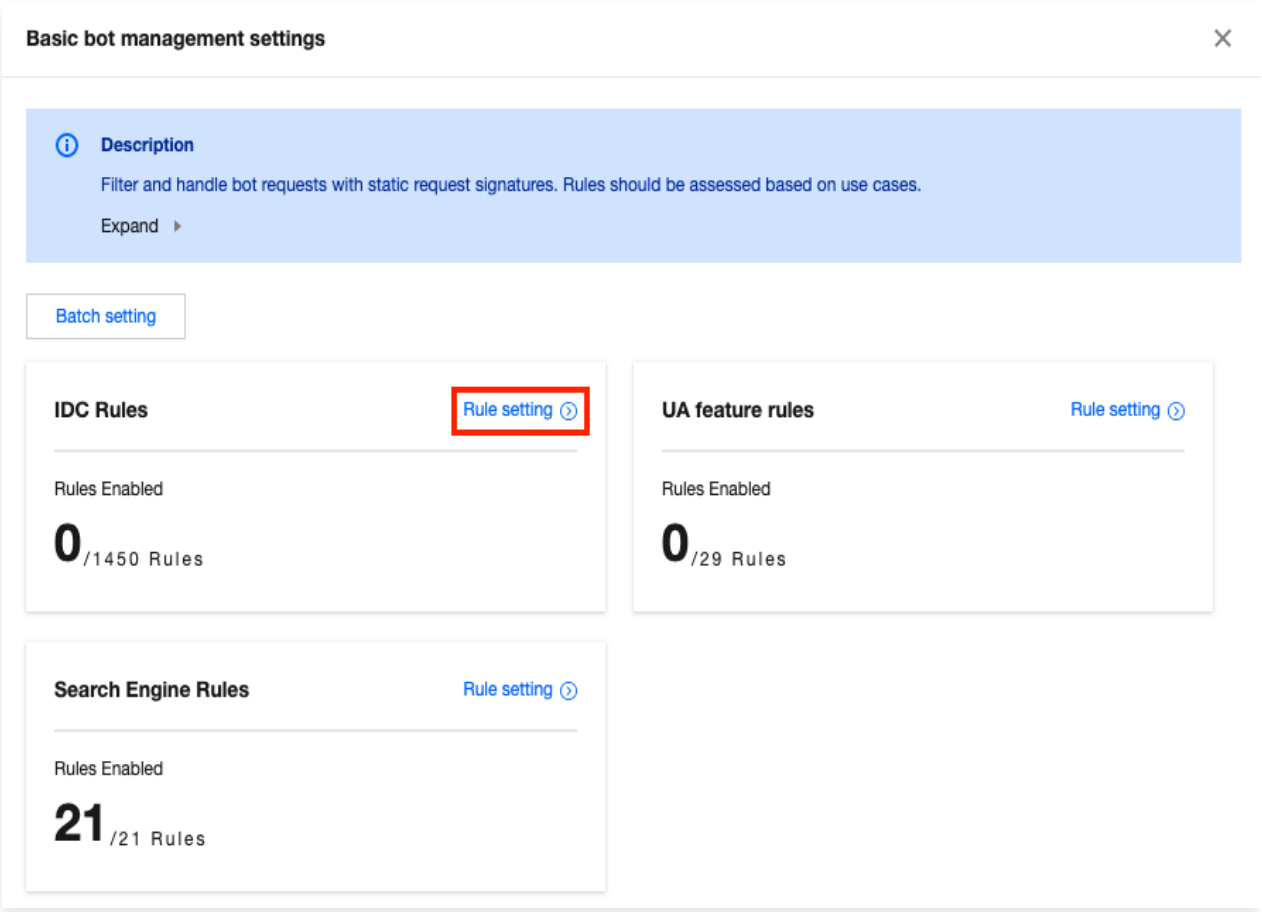


f3b9476dce0711edb580525400088f3a.png

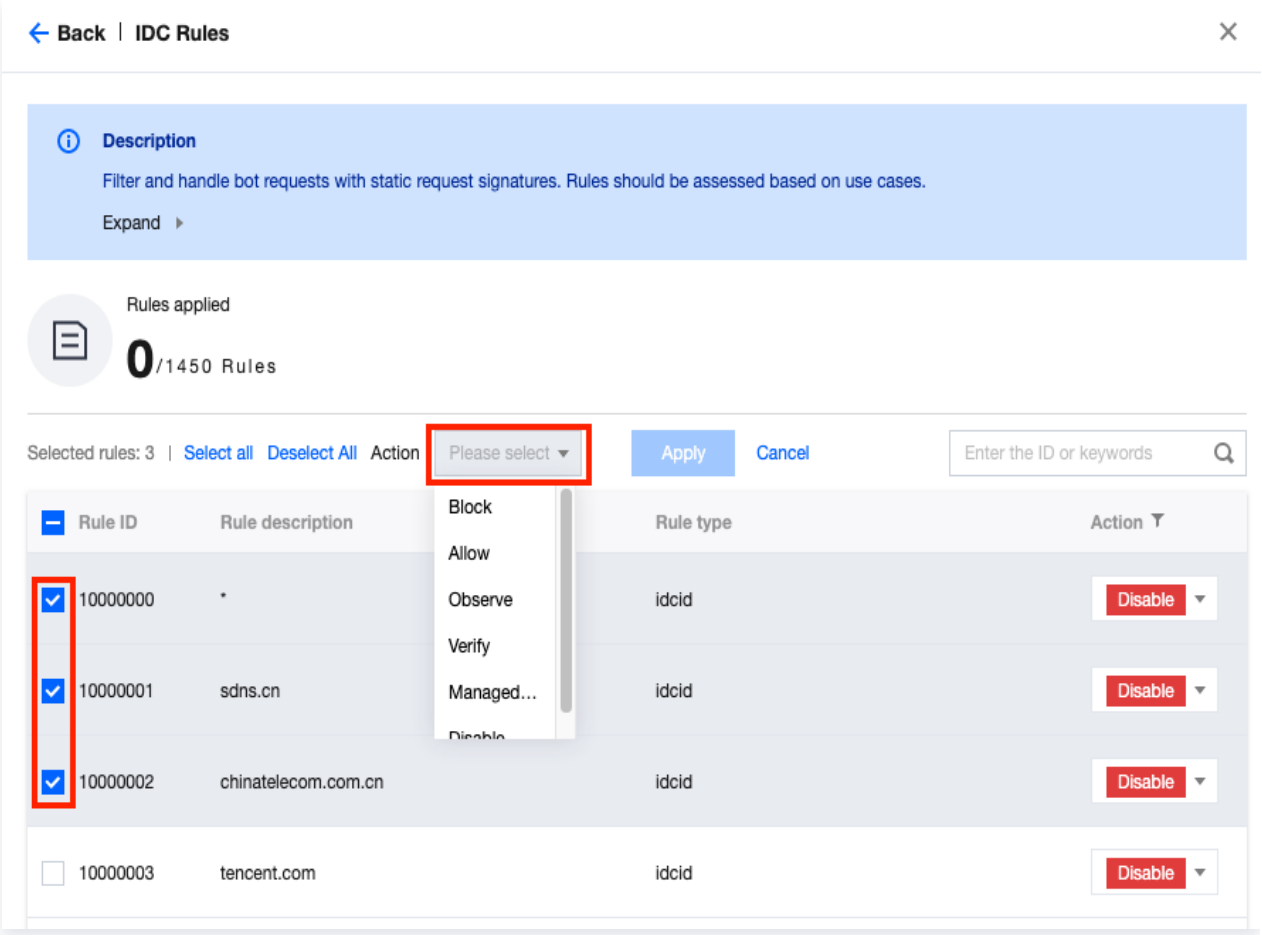
2. In the Bot Basic Protection Settings card, click **Settings** to adjust the rule configuration.
3. On the **Basic bot protection settings** page, you can set a single rule category or batch set rule categories.

   3.1 Set a single rule category

   3.1.1 Click **Rules** on the target rule category card to configure its rules.



   3.1.2 Select a **Rule ID**, click the **Action** drop-down list, and select an action.



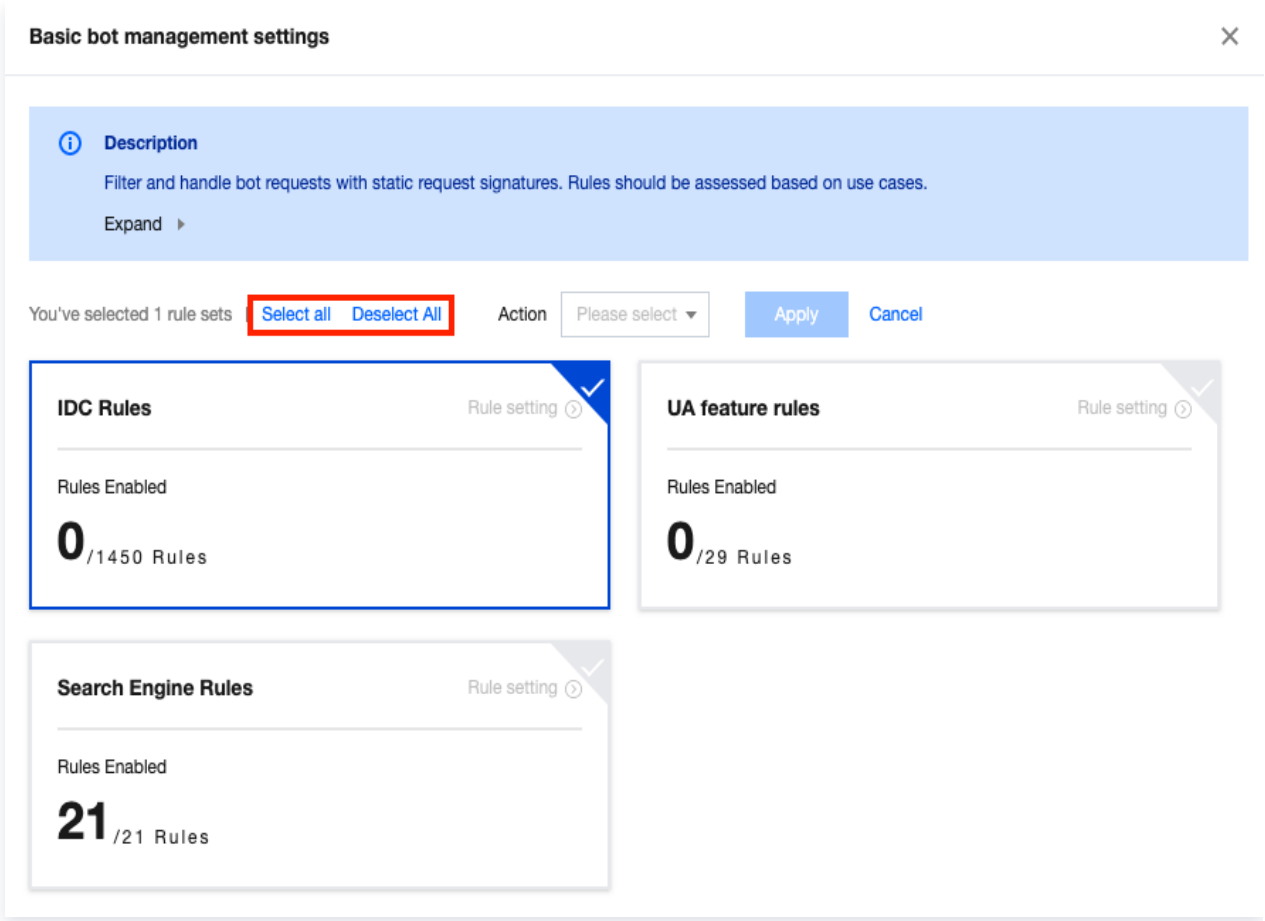
3.1.3 Click **Apply** to activate the configuration.

3.2 Batch set rule categories

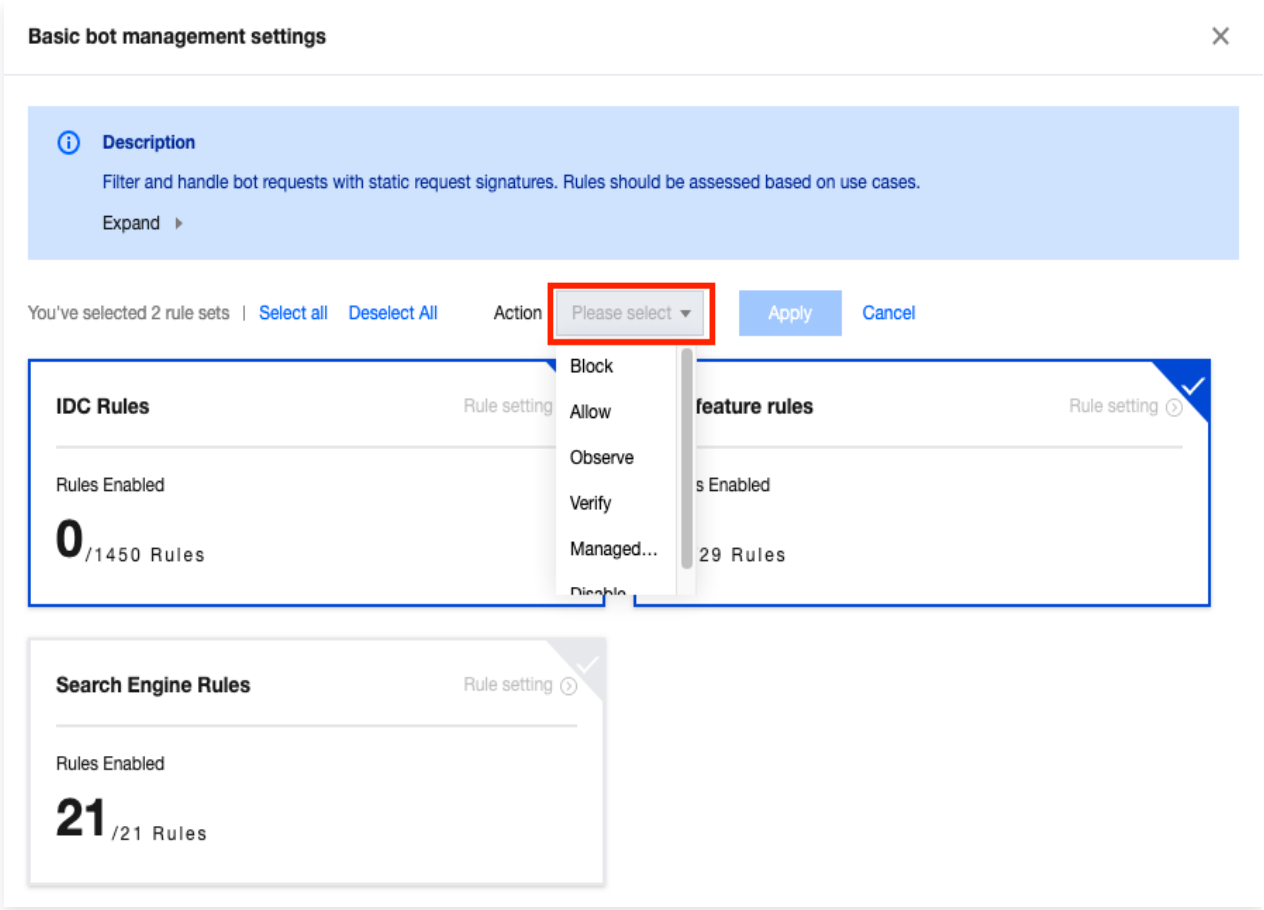
3.1.1 On the Bot Basic Protection Settings page, click **Batch Settings** to select one or more rule categories for batch action configuration.

3.1.2 In batch setting mode, select all the categories you want.

> **Note**
> In batch setting mode, you can click **Select all** or **Deselect All** to select or deselect all category cards at once.



3.1.3 Click the **Action** drop-down list and select an action.



3.1.4 Click **Apply** to activate the configuration.

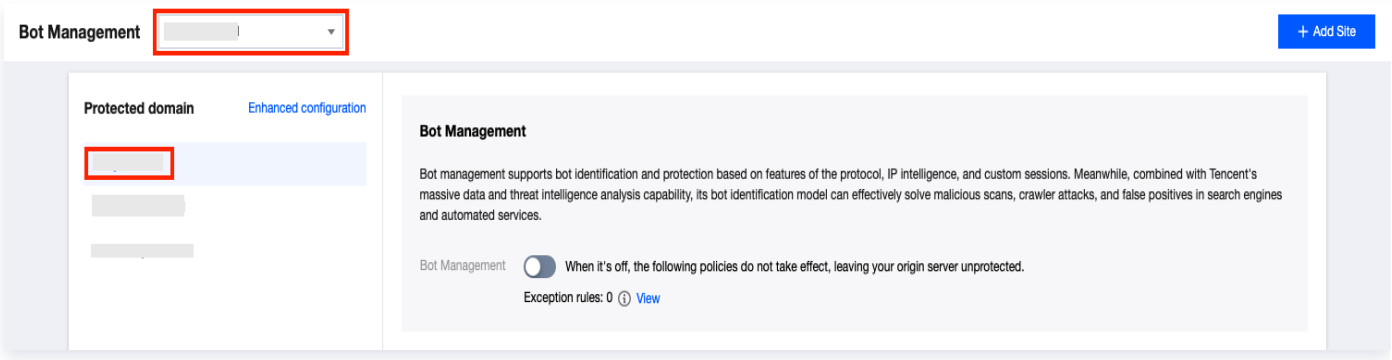
4. Click **OK** at the bottom to complete.

Custom rule

You can create different custom rules according to you business requirement.

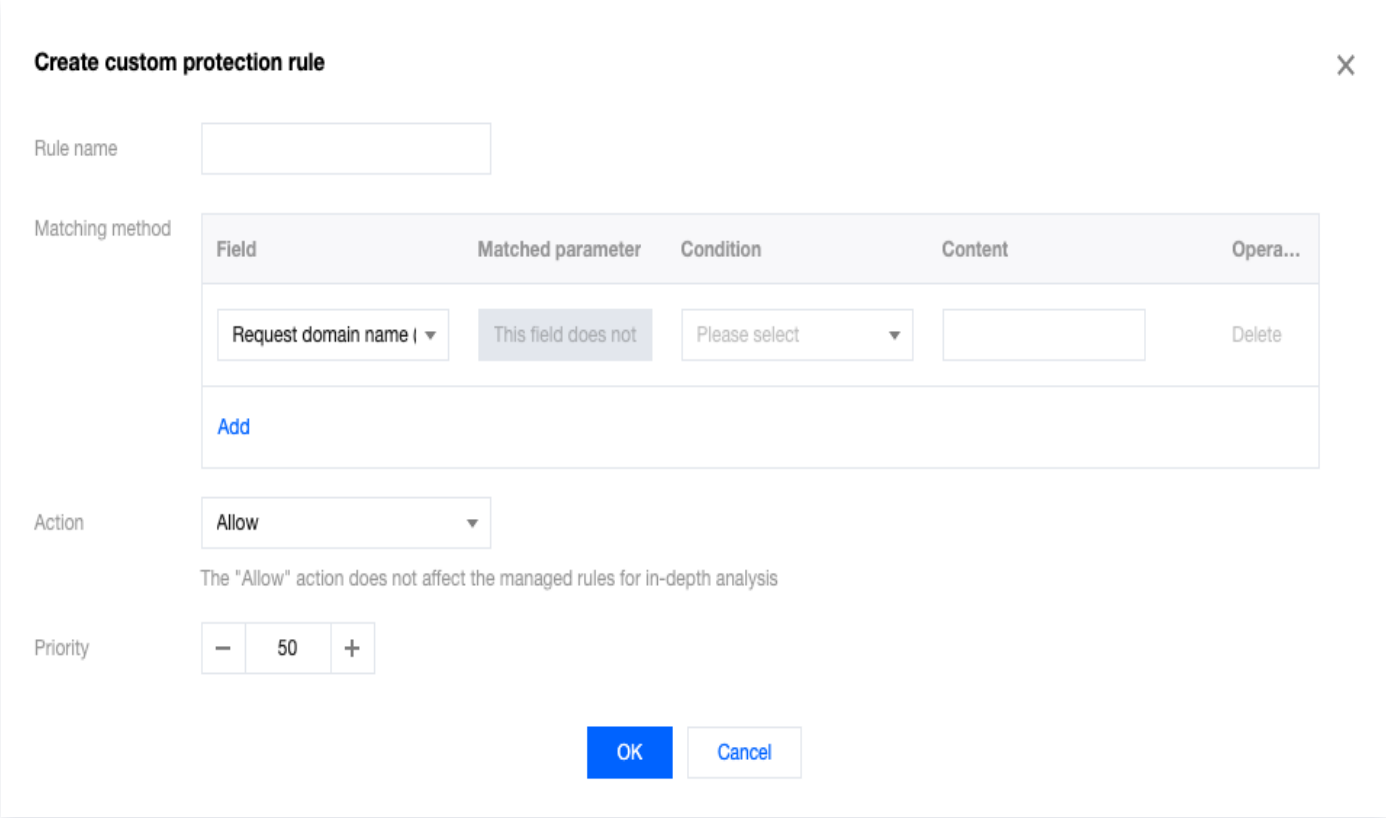
Add rule

1. Log in to the EdgeOne console. Choose **Security** > **Bot Management** on the left sidebar, and select the required site and subdomain name.



2. In the Custom Rule card, click **Settings**.
3. On the Custom Rules page, click **Add rule**. Set the rule name, matching method, action,

and priority.



Parameter Description:

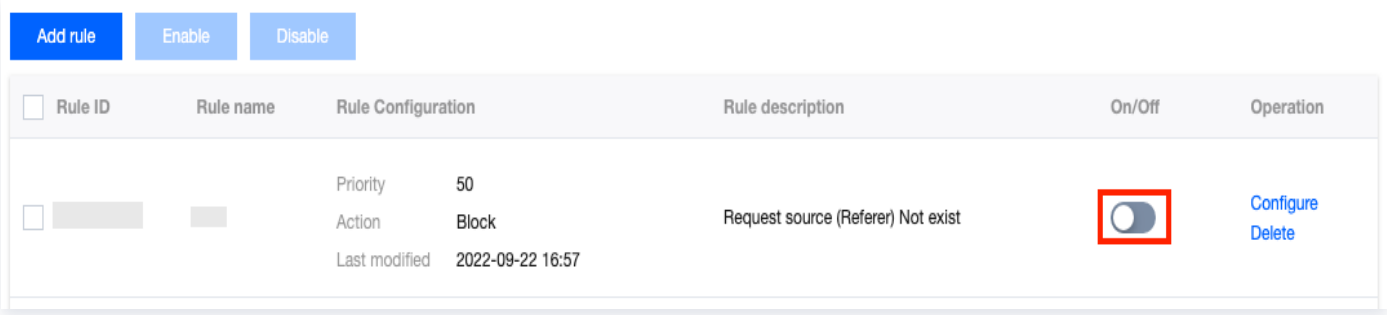
- Rule name: It contains letters, digits, and underscores. A rule name will be generated automatically if this parameter is left empty. Note that a rule name must be unique.
- Matching method: It consists of configuration items such as the protocol field (http/https) and the logical operator (include/equal to). Up to five conditions per rule are allowed, and the relation among conditions is "AND". Note that the same field can be configured only once in each rule.
- Action: Select as needed.
- Priority: This parameter determines the execution order of the entries. **Custom rules are executed in descending order of their configured priorities. If two rules have the same priority, the one that was modified more recently is executed first.**

4. Click **OK** to finalize the addition of the rule.

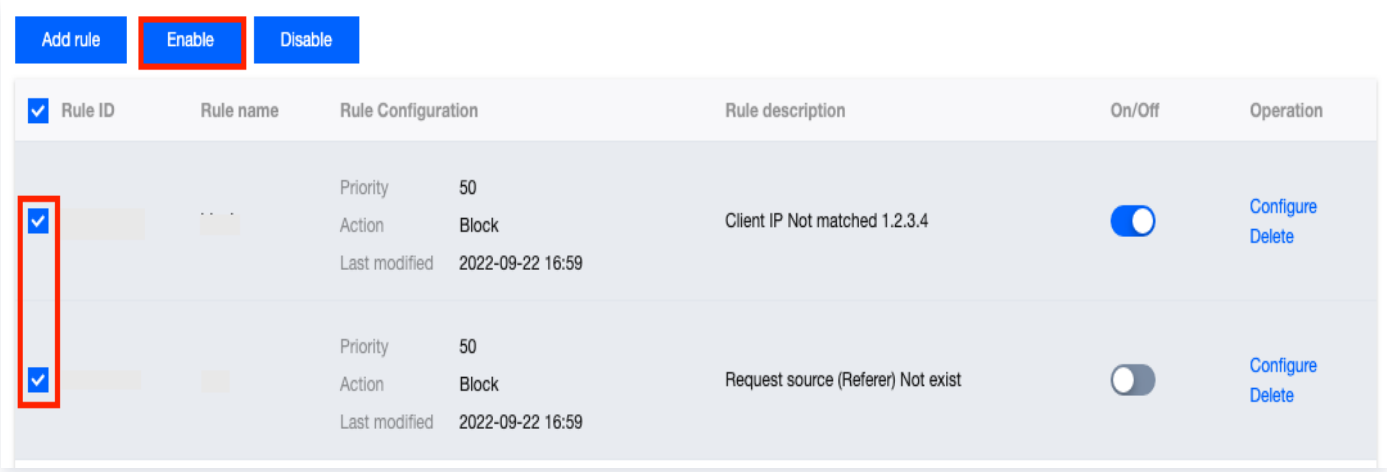
Rule switch

On the Custom Rules page, you can enable one or more rules.

- Individual: Select the required rule ID and click the policy switch to activate the corresponding rule.



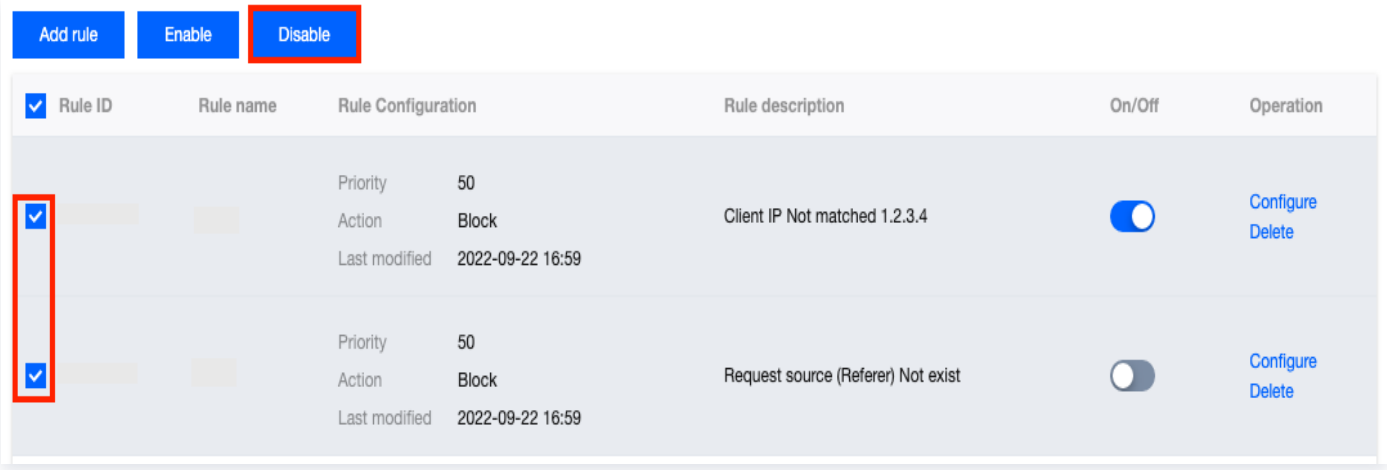
- To enable multiple rules, select the desired rules and click **Enable**. The selected rules will then be activated.



Disabling a rule

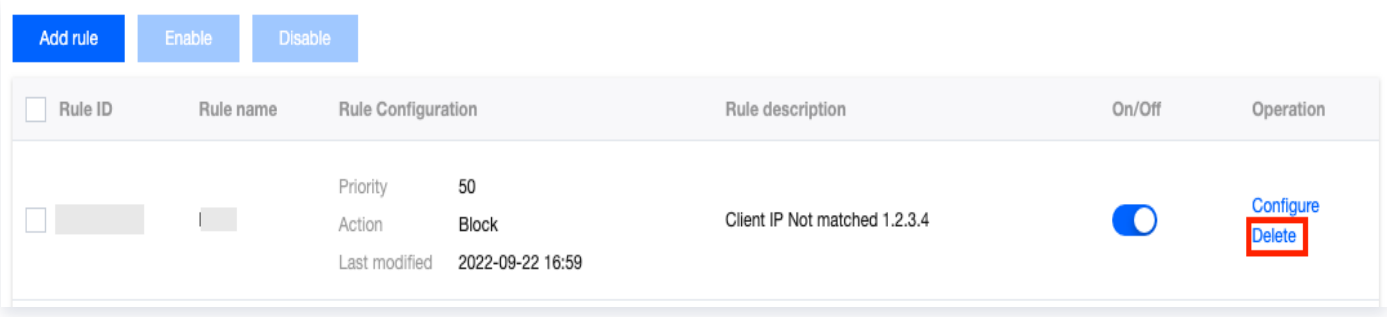
On the Custom Rules page, you can disable one or more rules.

- Individually: Select the desired Rule ID and click on the policy switch to disable the corresponding rule.
- To disable multiple rules, select the desired rules and click **Disable**.



Deleting a rule

1. On the Custom Rules page, select the desired rule and click **Delete** in the operation column.



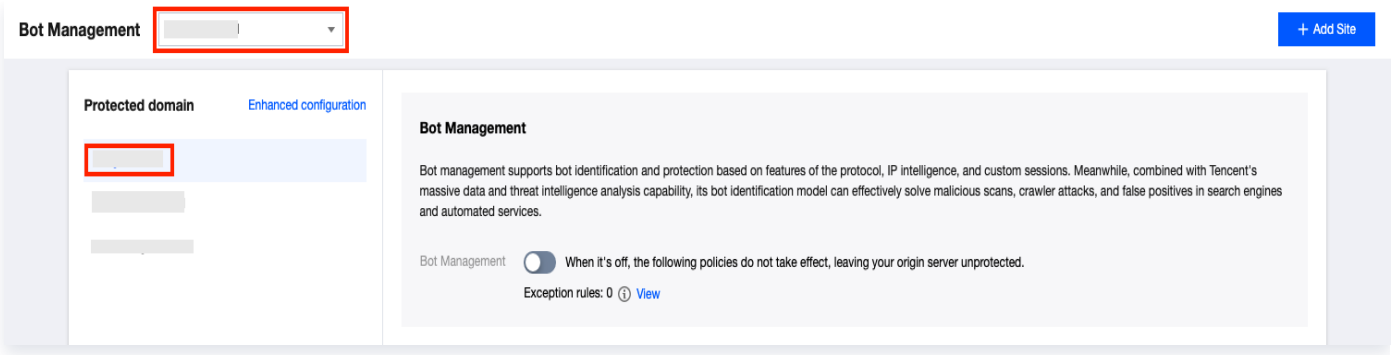
2. In the Delete Rule dialog box, click **Delete** to remove the corresponding rule.

Client Reputation

The client IP reputation is profiled based on a large amount of malicious access data and intelligence data collected recently. Actions can be configured based on the confidence level of the malicious client.

> **Note**
> Client reputation confidence: Under each type of client reputation rules, each confidence value corresponds to a client address list and reflects the frequency and consistency of a certain type of malicious behaviors performed from client addresses in the list.
> - High Confidence: The client address has recently been consistently and frequently involved in this type of malicious behavior. Requests from such addresses are almost certainly malicious and it is recommended to block them.
> - Medium Confidence: The client address has recently exhibited a significant frequency of this type of malicious behavior. There is a high probability that requests from such addresses are malicious, although occasional false positives may occur. It is recommended to configure the action as a JavaScript Challenge or Managed Challenge.
> - Low Confidence: The client address has recently demonstrated a consistent record of this type of malicious behavior. Compared to other addresses, this client address is more likely to initiate malicious actions, although there is a possibility of false positives. It is recommended to configure the action as 'Observe', and adjust to 'JavaScript Challenge' or 'Managed Challenge' as necessary through tuning steps.

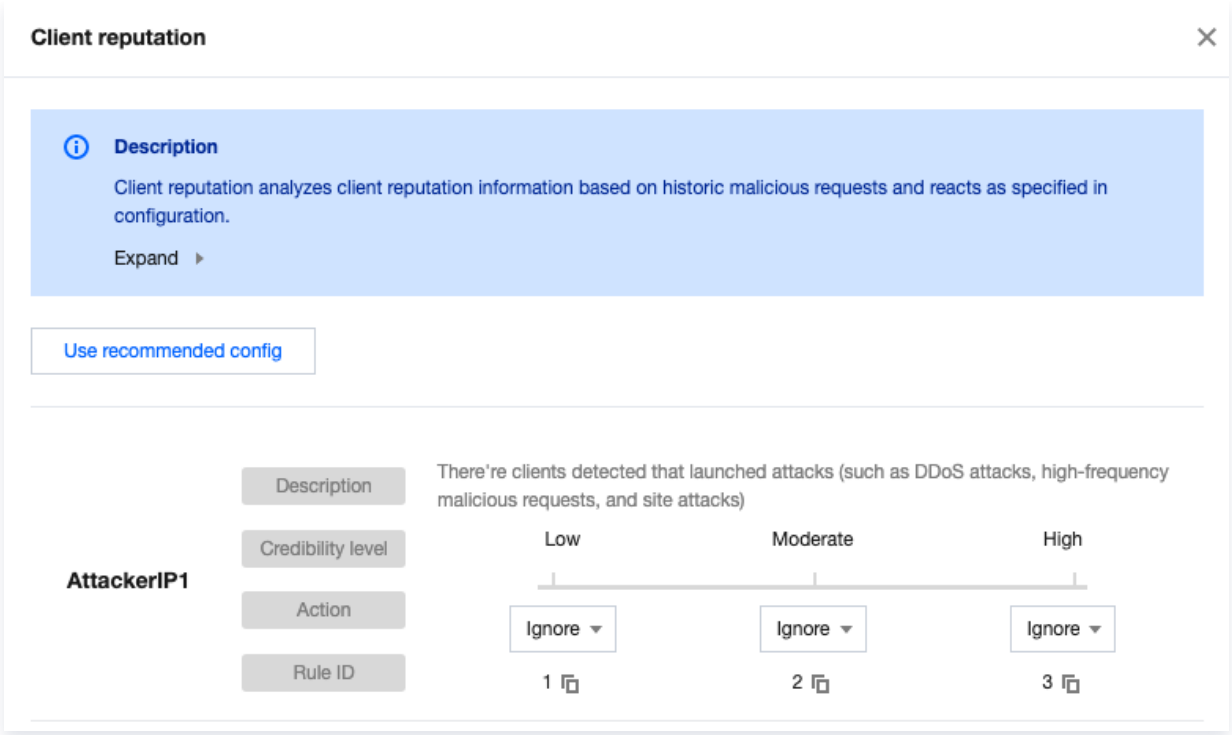
1. Log in to the EdgeOne console. Choose **Security** > **Bot Management** on the left sidebar, and select the required site and subdomain name.



2. In the **Client reputation** section, toggle on or off the switch on the right.

> **Note**
>
> - After the client reputation feature is disabled, related rules no longer take effect. Requests are allowed by default, and no logs are recorded.
> - When the client reputation feature is enabled for the first time, it is recommended to configure a detailed rule before enabling the rule. This is to prevent normal business access from being affected by unconfigured rules.

3. In the **Client reputation** section, click on **Settings** to configure the rules within the module.
4. On the **Client Reputation Configuration** page, within the malicious behavior category box that requires configuration adjustment, click on the **Action** drop-down list corresponding to different confidence levels, and select the action that needs to be configured.



5. Click **OK** to complete.

Rules Template

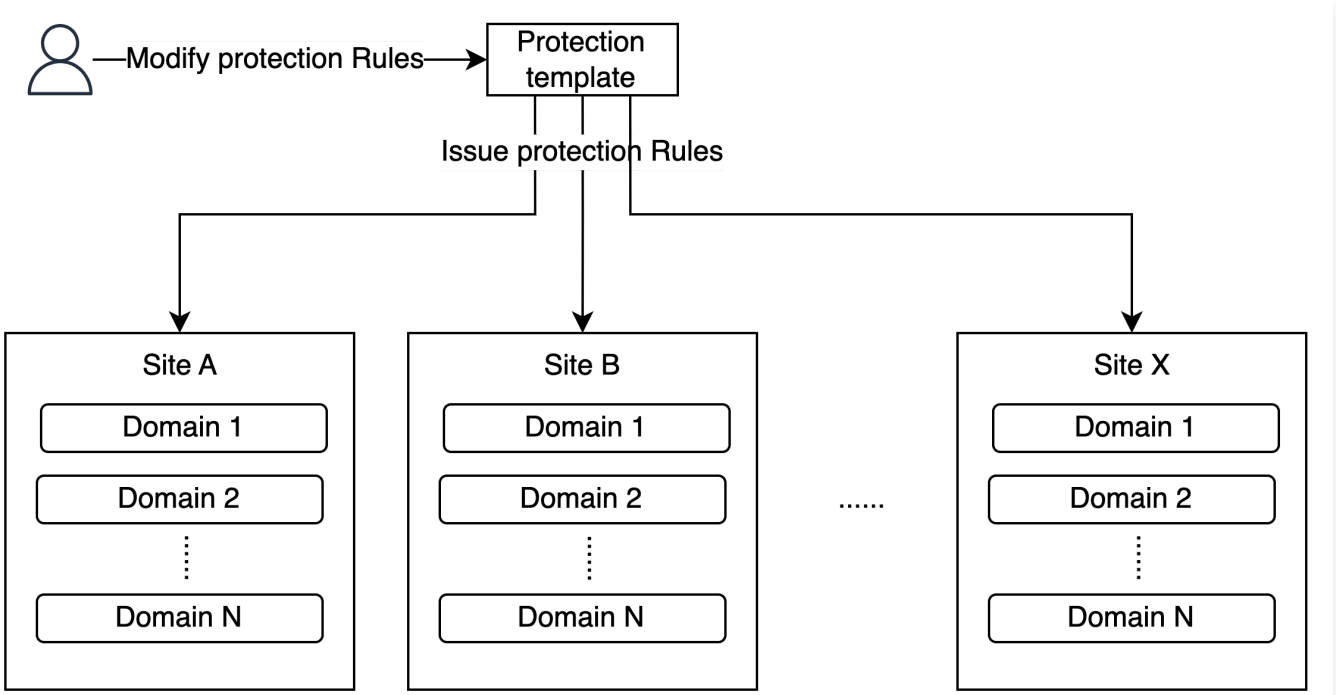
Last updated: 2023-09-07 15:25:34

Overview

When you need to connect a large number of domain names to EdgeOne Web Protection simultaneously, and if the protection policies required by these domain names are identical, modifying the Web Protection policy for each domain name individually can result in a significant maintenance workload.
EdgeOne's security protection offers a policy template feature, allowing you to save security policies as templates and apply these template policies to specified domain names. You can directly modify the corresponding security protection policy within the template management, which will then take effect on all domain names that have applied this template, significantly reducing your operational costs.

Note:

1. Policy templates only support Web Protection Policies, Bot Management Policies, and Custom Pages.
2. Utilizing a policy template will overwrite the existing protection policies within the current domain name, and the current protection policies will be lost.
3. Upon utilizing a policy template, the current list of temporarily blocked clients within Intelligent CC Attack Protection will be cleared. Any newly added temporarily blocked client lists after application will not affect other domain names within the policy template.

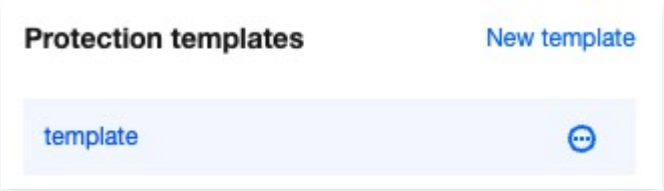


Bind Protection Template

Scenario 1: Creating a policy template and applying it to specified domain names and sites.

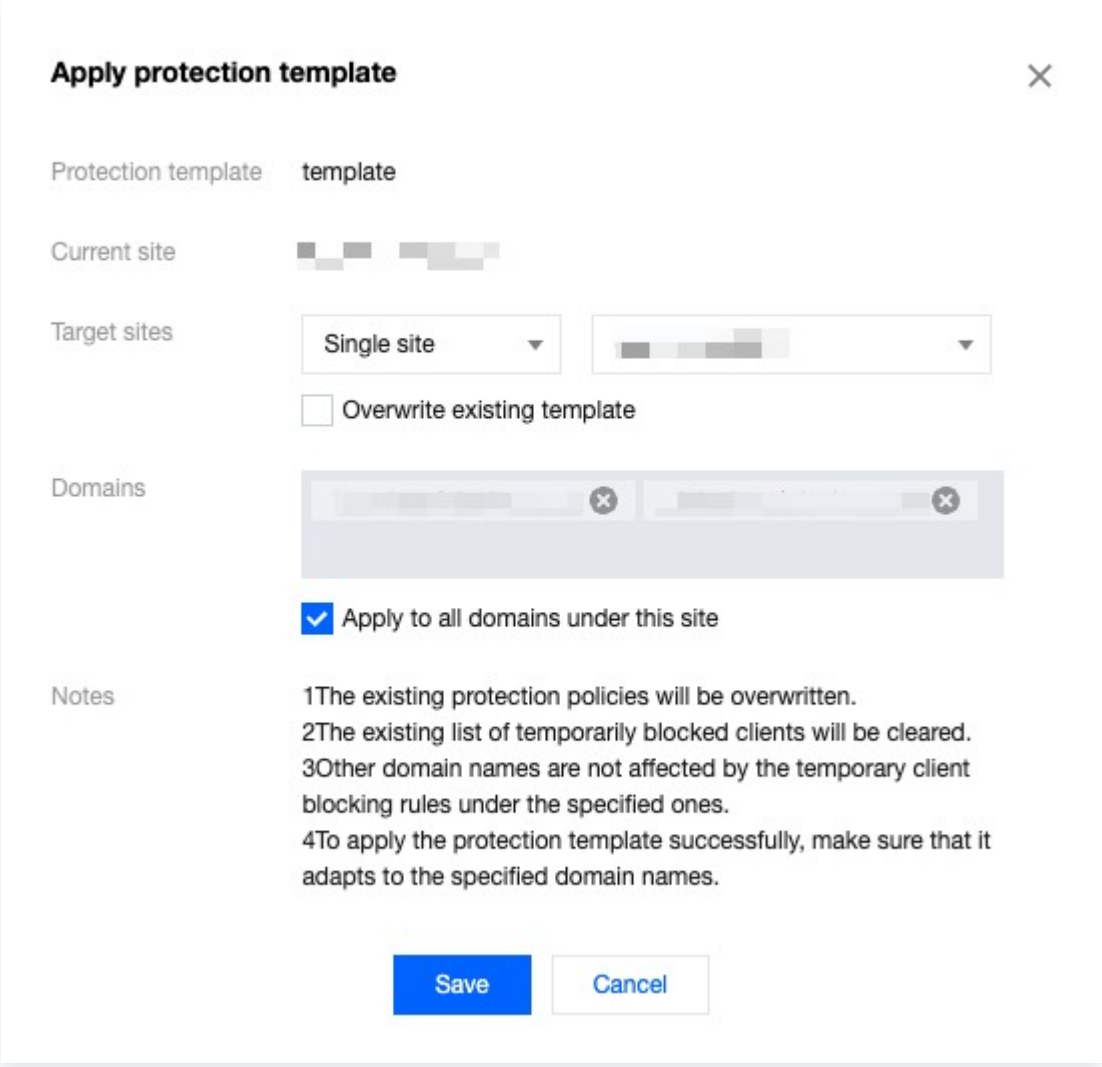
For instance, you need to create a new policy template `template` and apply this policy template to all domain names within the site `example.com`.

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security Protection** > **Policy Templates**.
3. On the Policy Template page, click **Add New Template** on the left, enter the template name, and press the Enter key to create a new template.



4. After creation, click on the **template name** you just created to enter its editing page. You can complete the configuration and modification of related rules on this page. For configuration details, please refer to Web Protection and Bot Management.
5. On the Policy Template page, click **Apply to Domains** to apply the configured policy template to the site. In this scenario, the policy template needs to be applied to all domain names within `example.com`. Select **Apply to Specified Site** as the application method, choose `example.com` as the site, and check the box to apply to all domain names.

- **Note:**
  - Apply to the current site: Implement the current policy template to the domain names within the current site or to all domain names.
  - Apply to specified sites: Apply the current policy template to domain names under other specified sites or to all domain names.
  - Bulk Apply to Sites: Apply the current policy template to multiple specified site domain names or all domain names within a site. When applying in bulk to sites, wildcard expressions can be used to match domain names.



6. Click **Save** to complete the application of the policy template.

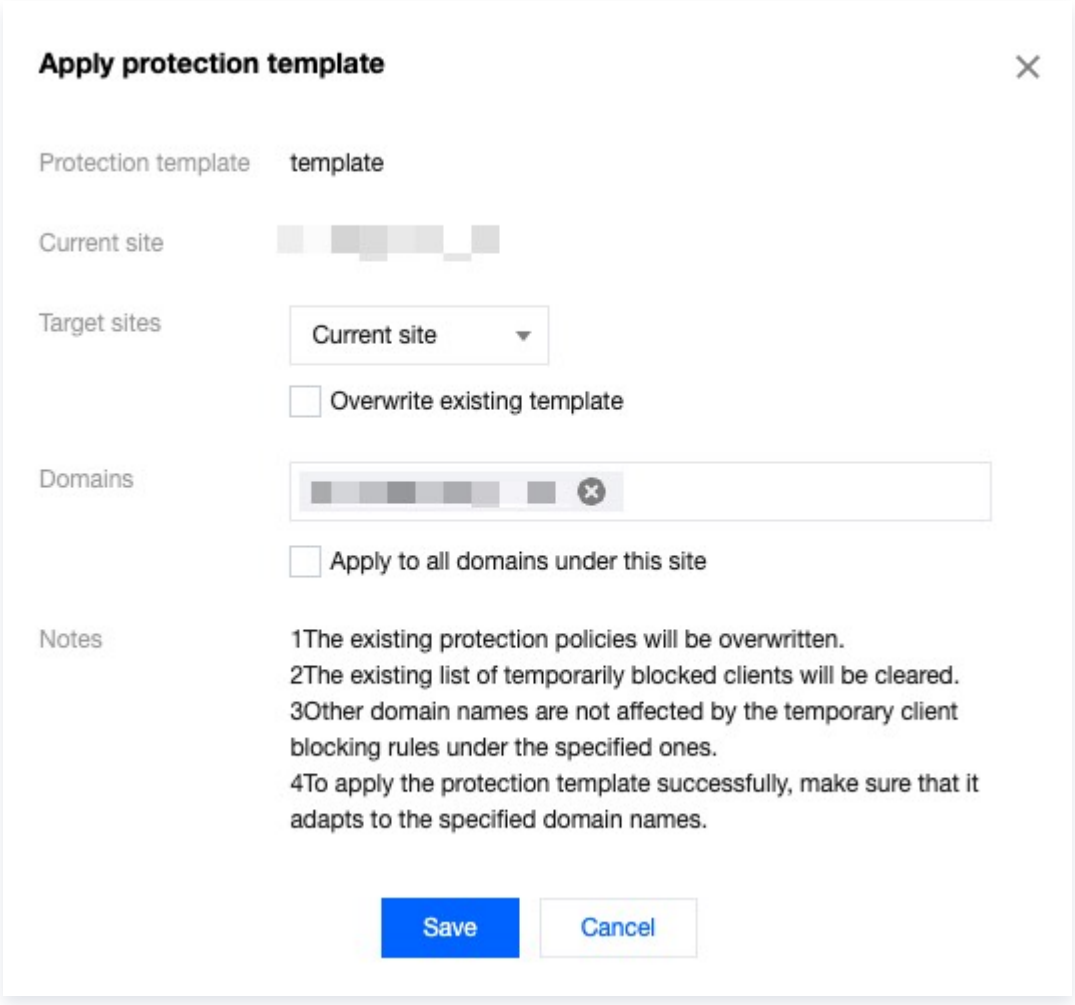
Scenario 2: Applying an existing template to a newly added domain or site.

For instance, if you currently have a Web Security Protection Policy template `template` configured under the site `example.com`, and you add a new domain name `www.example.com`

under the current site, and the Web Protection Policy for this domain name is identical to the template `template`, you can quickly apply the current policy template to this domain name by using the template policy.

Method 1: Operating within the policy template

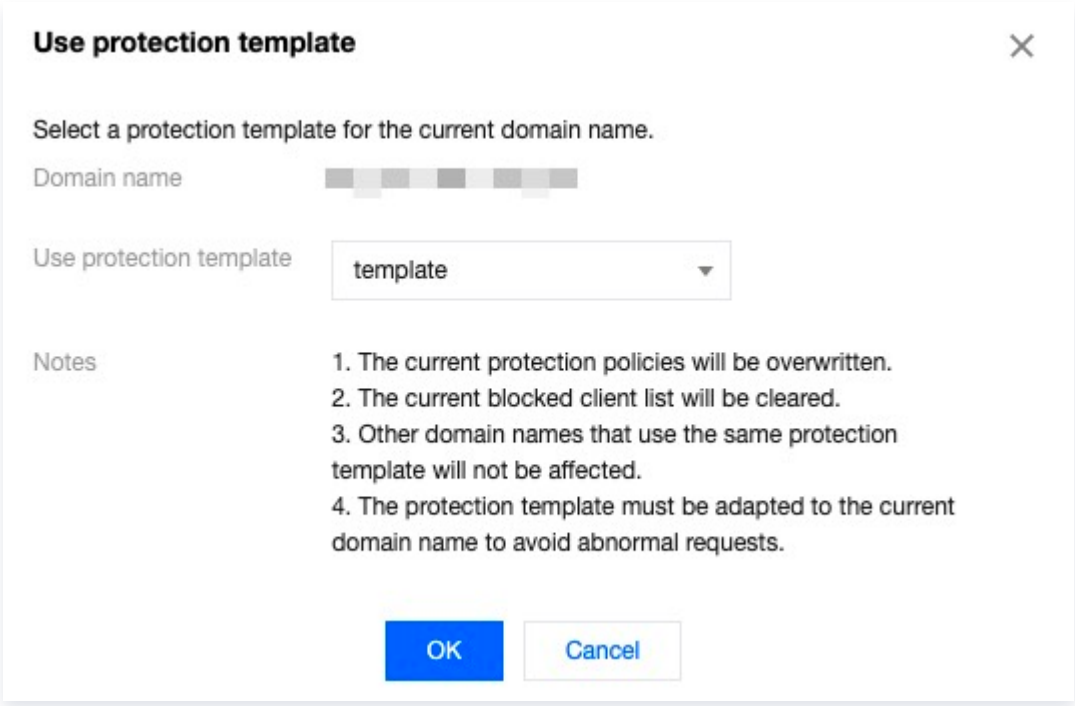
1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, click **Security Protection** > **Policy Templates**.
3. On the Policy Template page, select the corresponding protection template, such as `template`.
4. Click **Apply to Domains**. In this scenario, you can choose to apply to the current site and select the domain name `www.example.com` from the domain name list.



5. Click **Save** to complete the application of the policy template.

Method 2: Operating within the Protection Configuration

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, select the protection module that needs to be configured. In this scenario, you can click on **Security Protection** > **Web Protection**.
3. On the Web Protection page, select the domain name that needs to be configured, for example, `www.example.com`.
4. Click **Use Template Policy** in the upper right corner, select the template policy you need to apply, for example: `template`.



5. Click **OK** to apply the template policy.

Unbind protection template

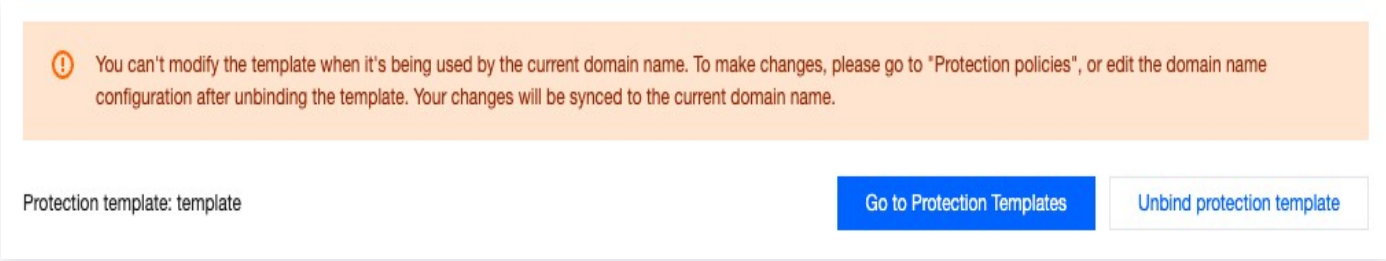
For instance, if you currently have a Web Protection policy template `template` bound to the domain `www.example.com` under the site `example.com`, and this domain requires a personalized protection policy configuration that differs from other domains, you need to unbind the corresponding policy template in order to configure a new custom rule while retaining the current security configuration.

1. Log in to the EdgeOne console. In the left sidebar, click **Site List**. Within the site list, click the **site** that needs to be configured to enter the site details page.
2. On the site details page, select the protection module that needs to be configured. In this scenario, you can click on **Security Protection** > **Web Protection**.
3. On the Web Protection page, select the domain name from the left-hand protection

domain list that needs to have the policy template unbound, for example: `www.example.com` .

4. Domain names bound to a policy template can only view configurations and cannot be modified. Click **Unbind Policy Template** to support two types of unbinding operations:
   - Preserve Current Security Policy: After unbinding, the security protection policy content configured by the current policy template will be retained.
   - Implementing a blank security policy: Clear all security policies and reconfigure.

   In the current scenario, you may choose to retain the existing security policy information



5. Click **OK** to unbind.

Origin Protection

Last updated: 2023-09-07 15:25:41

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.

Instructions

1. Log in to the EdgeOne console and choose **Security** > **Origin Protection** on the left sidebar.
2. On the Origin Protection page, click **Enable** for the Origin Protection status. Select the Site Acceleration/L4 Proxy Service, then click **Confirm Enable** to activate Origin Protection for the selected resources.

   > **Note**
   > **Select resource**: Select target resources to enable Origin Protection.

3. When 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.

Supports and Limits

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.

FAQs

Why can't I enable Origin protection for my domain name?

Origin protection only supports domain names with security acceleration enabled.

How can I enable security acceleration for a domain name?

If your EdgeOne plan supports security acceleration, you can enable advanced protection for a specific domain name in the Enhanced configuration card under **DDoS Mitigation**.

Can I use origin protection for non-security acceleration resources?

Regrettably, this feature is currently unavailable if the site's package does not support the "Security Acceleration" business model.

Alarm Notification

Last updated: 2023-09-07 15:25:49

Overview

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

- DDoS alarms: For DDoS attacks against the Enterprise DDoS mitigation plan (site access and layer-4 proxy services), you can set an alarm threshold based on the minimum DDoS attack rate.
- 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 continuously monitors external access traffic and identifies any DDoS attacks. Upon detection of an attack, the system automatically initiates traffic cleansing, filtering out malicious attack traffic without the need for manual intervention.
- Alarm notifications are pushed only for DDoS attacks against the DDoS mitigation Enterprise plan (site access and layer-4 proxy services). Currently, other businesses don't support the DDoS attack traffic alarming feature.

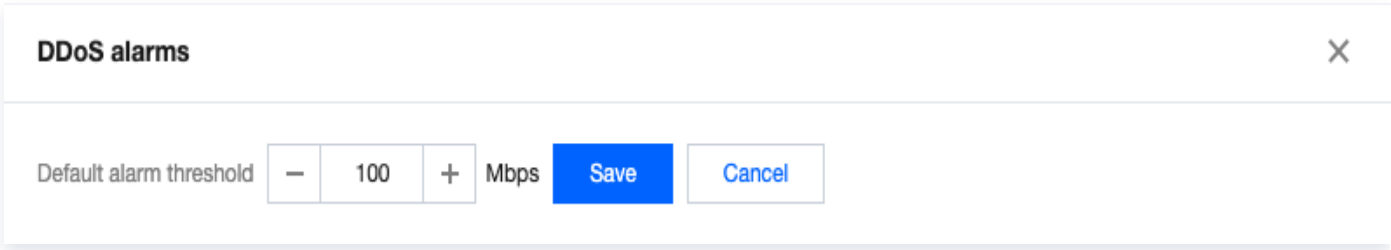
Configuring DDoS alarm settings

1. Log in to the EdgeOne console. Choose **Security** > **Alarm Notification** on the left sidebar, and select the target site.
2. In the DDoS Attack Traffic Alarm card, click on **Settings**.

3. On the DDoS attack traffic alarm page, you can adjust the global default DDoS attack alarm threshold for the current site. Notifications will only be pushed to the Message Center when the attack data rate exceeds the configured threshold. Click **Edit** next to the default alarm threshold, modify the threshold, and then click **Save**.

> **Note**
> The DDoS attack traffic alarm page displays all services that support DDoS attack traffic alarms, along with their corresponding DDoS attack alarm thresholds. For

services that have not enabled custom thresholds, you can adjust the corresponding DDoS attack alarm threshold by modifying the **default alarm threshold**.

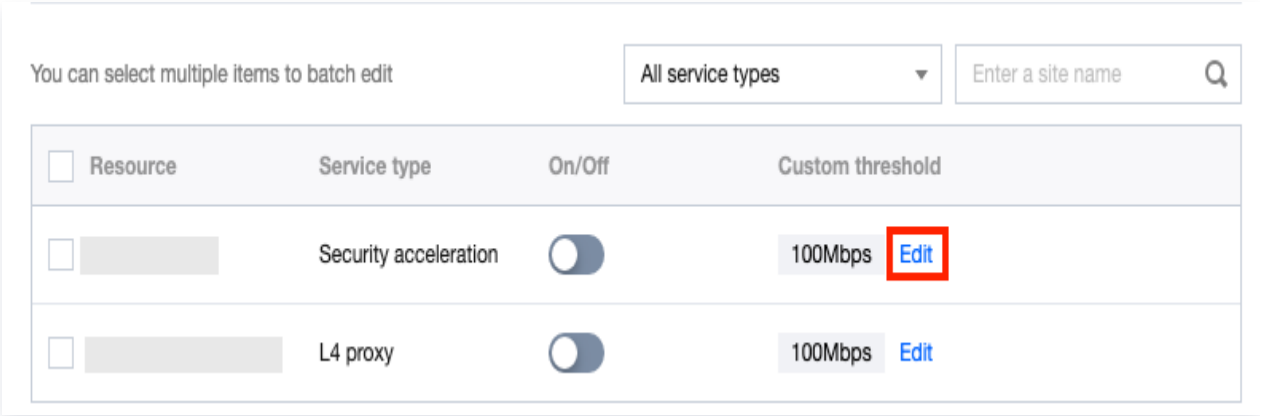


4. On the **DDoS attack traffic alarm** page, you can configure the alarm threshold for a security acceleration or layer-4 proxy business project.

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

4.1 Set a single alarm threshold

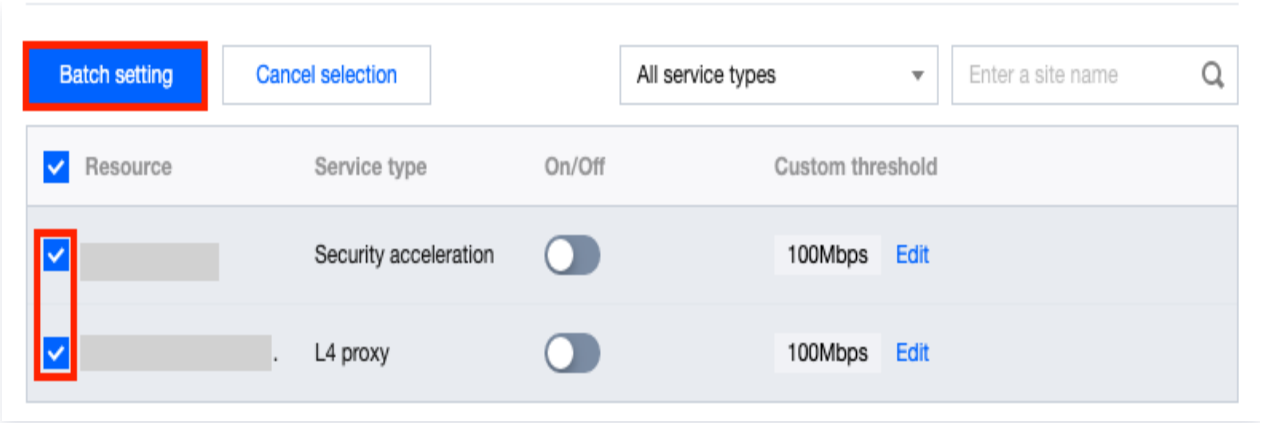
4.1.1 Select the desired service and click **Edit** in the corresponding alarm threshold column to adjust the scale of the attack (minimum attack rate) for which the service will push DDoS attack notifications.



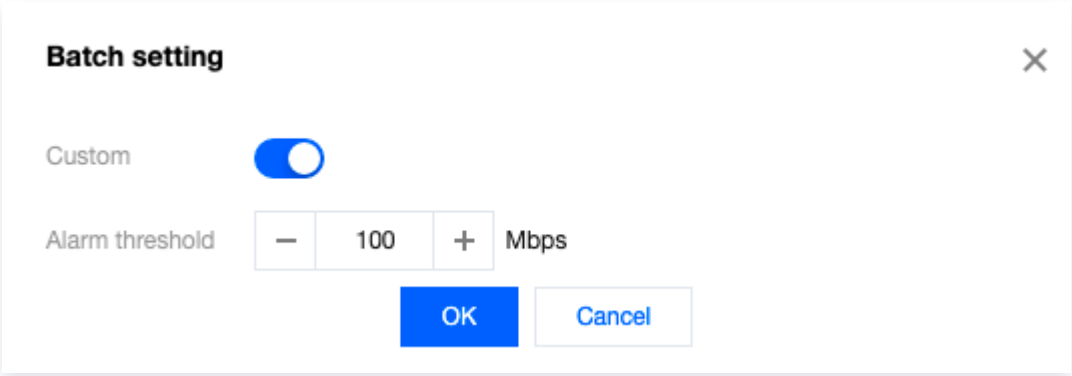
4.1.2 Modify the alarm threshold, click **Save**, and the custom threshold will be enabled automatically.

4.2 Batch set alarm thresholds

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



4.2.2 Toggle on the custom threshold switch, set the alarm threshold, and click **OK**.



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:

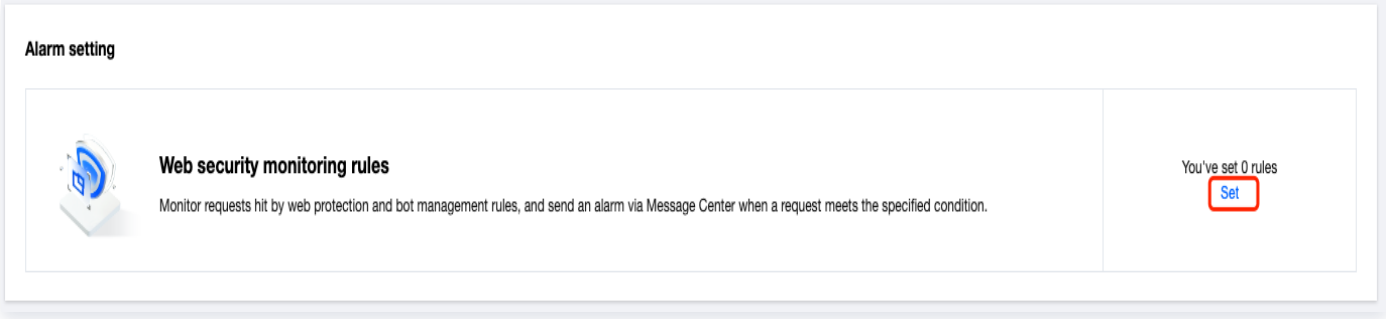
- **Rule name**: Required. Take note of the following naming conventions:
  - It can contain only letters, digits, and underscores.
  - The character length must be less than 32.
  - It cannot start with an underscore.
- **Domain name**: Required. Select the domain names to be monitored.
  - **All hostnames**: 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 Processed Requests**: All requests that have triggered the security module rules and have been processed (excluding those allowed) are included in the monitoring rule statistics.
  - **Specifically handled requests**: Only requests that hit the web protection or bot management rules and are ultimately handled in the selected manner are counted in the monitoring rule statistics.
  - Only **rule-hit requests** are counted: These are requests that hit specified web protection or bot management rules.
- **Alarm setting**: Select the alarm condition. You can select the alarm frequency.
  - **Static Alarm Condition**: Alarm notifications are dispatched based on a fixed request count threshold. When this threshold is exceeded, the alarm condition is met and notifications are sent according to the configured alarm frequency.
  - **Alarm Frequency**: When this rule meets the alarm conditions, alarm notifications are dispatched according to the configured alarm 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

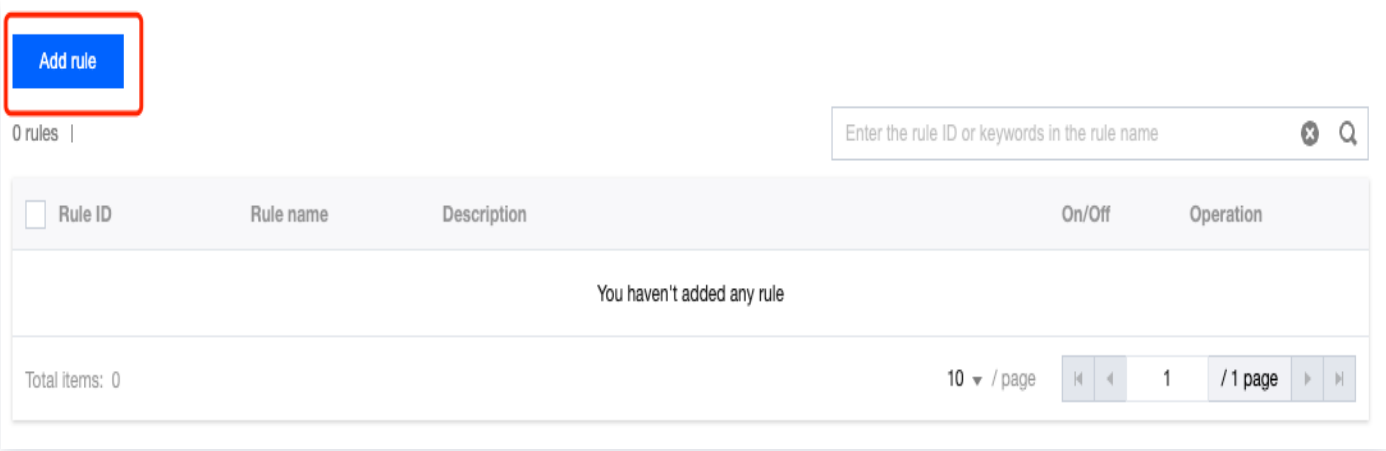
1. Log in to the EdgeOne console. Choose **Security** > **Alarm Notification** on the left sidebar, and select the target site.

2. In the Web Security Monitoring Rules card, click **Settings** to enter the configuration page. Here, you can add, delete, edit, and toggle Web Security Monitoring Rules.



Create a web security monitoring rule

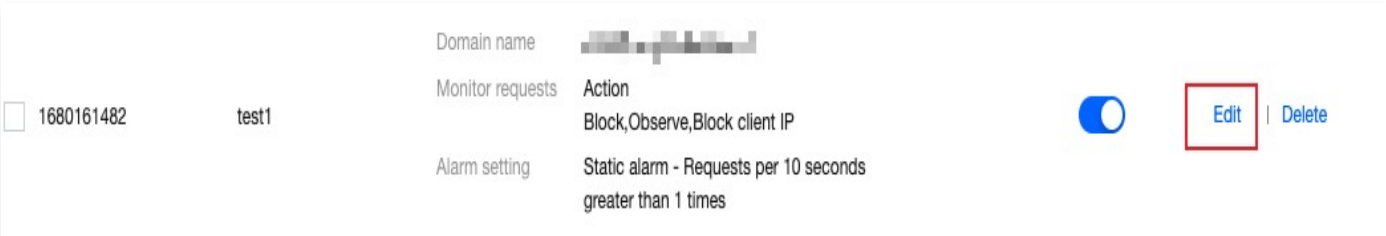
1. In the Web Security Monitoring Rules configuration page, click **Add Rule** to create a new monitoring rule.



2. Within the Web Monitoring Rules configuration pop-up, after setting the rule name, domain, monitoring statistical range, and alarm options, click **Confirm** to save the monitoring rule. The alarm conditions will take effect immediately.

Edit a web security monitoring rule

1. On the Web Security Monitoring Rules configuration page, locate the rule you wish to edit and click **Edit** in the corresponding operation column.

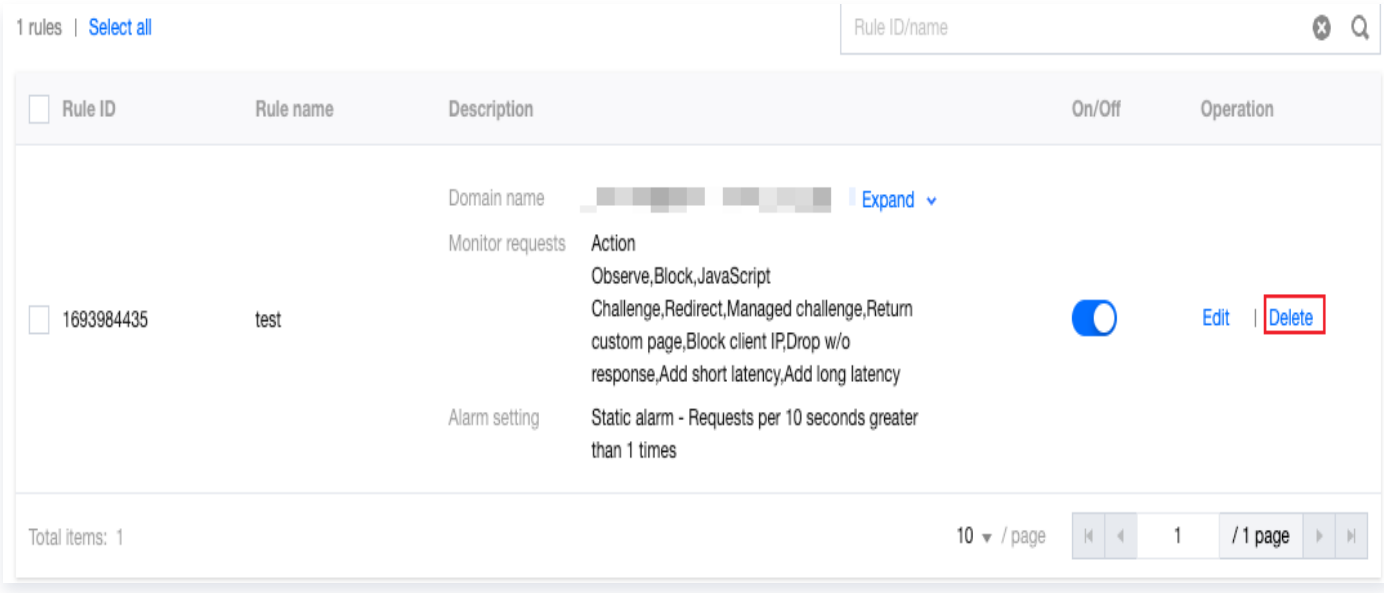


2. In the Web Monitoring Rules configuration pop-up, modify the rule name, domain, monitoring statistical range, and alarm options, then click **Confirm** to save the monitoring

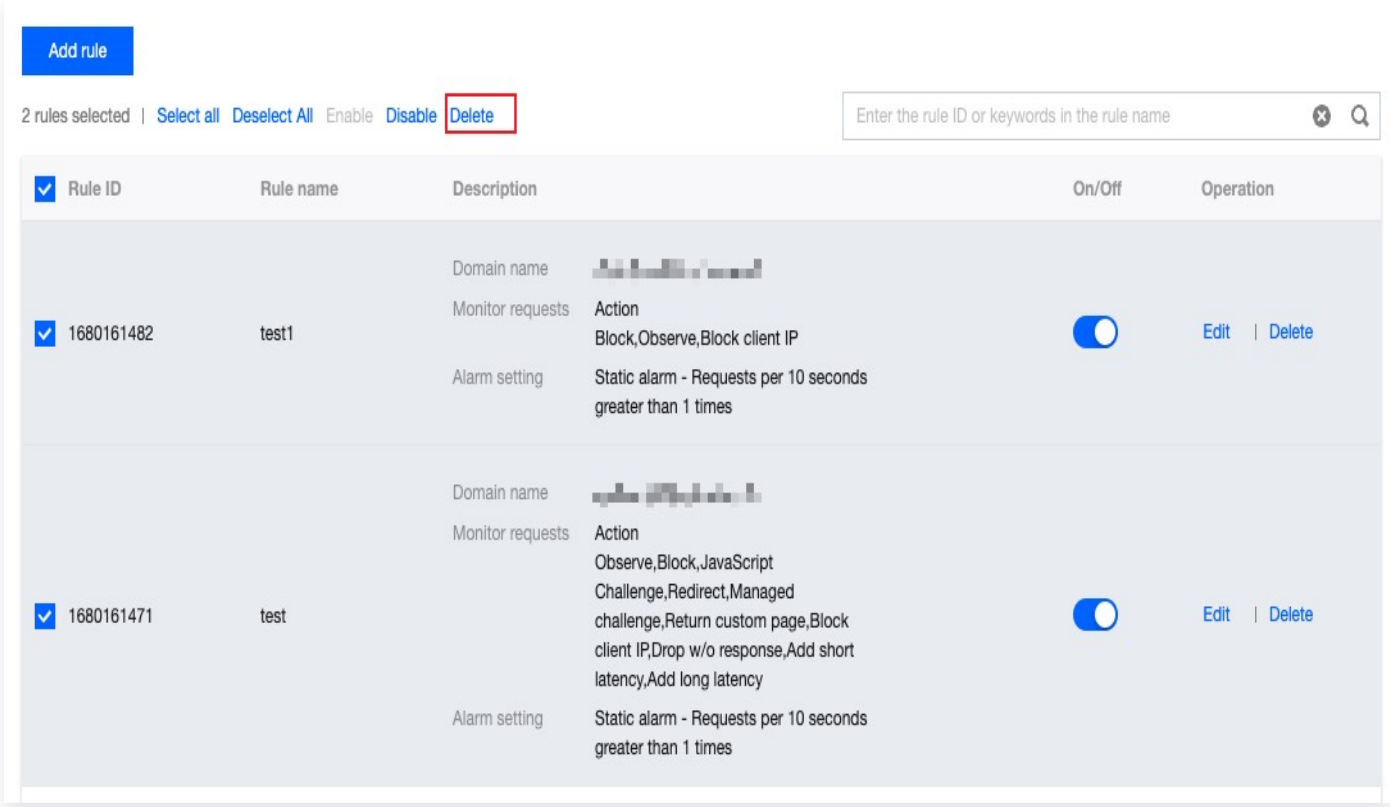
rule. The alarm conditions will take effect immediately.

Delete a web security monitoring rule

- Delete a single web security monitoring rule
  On the Web Security Monitoring Rules configuration page, locate the rule you wish to delete and click **Delete** in the corresponding operation column.



- Batch delete web security monitoring rules
  On the Web Security Monitoring Rules configuration page, select one or more rules and click **Delete Selected** to simultaneously remove all selected rules.



Enable or disable a web security monitoring rule

- Enable or disable a single web security monitoring rule
  On the Web Security Monitoring Rules configuration page, locate the rule you wish to enable or disable, then click on the corresponding in the **Alarm Switch** column.

- Batch enable or disable web security monitoring rules
  Select one or more Web Security Monitoring Rules and click **Enable Selected** or **Disable Selected** to simultaneously enable or disable all selected rules.