Secure Content Delivery Network

Product Introduction

Product Documentation

Contents

Product Introduction
Overview

Last updated：2021-11-25 12:09:52

What Is SCDN?

Based on fast and stable content delivery network services, Tencent Cloud Secure Content Delivery Network (SCDN) provides protection capabilities against various cyber attacks. For Content Delivery Network (CDN) or Enterprise Content Delivery Network (ECDN) domain names, you can easily enable SCDN to protect your business against DDoS attacks, CC attacks, web attacks, and bots.

Note：

- SCDN provides security services based on two basic products: **CDN** and **ECDN**. Its service regions are divided into **Chinese mainland** and **Outside Chinese mainland**.

The following problems can be effectively addressed:

1. Large volumes of DDoS attacks and CC attacks may overwhelm the CDN/SCDN bandwidth, causing extensive traffic and requests not from your business and extra costs.
2. CDN/ECDN services provide limited protection and access control capabilities, such as IP access limit and access authentication. Given increasingly complex cyber threats and attacks, they can deliver an all-out protection by combining with other cloud security products, separate service configurations, and additional network transport layers.

You can easily enable SCDN without making changes to existing CDN/SCDN and DNS settings and customize your SCDN settings as needed.

Strengths

Last updated：2021-11-25 12:09:52

A Variety of Features

On the basis of providing fast and stable content delivery network services, SCDN can quickly enable all-around security solutions that integrate multiple protection capabilities against web, DDoS, and CC attacks.

Protection against DDoS attacks

With advanced characteristic recognition algorithms, this feature helps prevent large volumes of traffic attacks such as SYN floods, UDP floods, and ICMP floods, ensuring smooth operation of your business.

The distributed architecture allows SCDN nodes to schedule load balancing globally and intelligently. When the attack traffic reaches the cleansing threshold, it can schedule traffic to SCDN clusters to defeat large DDoS attacks and secure the availability of your business.

The SCDN can defend against up to 20 Tbps of DDoS attacks on the entire network, with up to 1 Tbps protection for a single node.

Protection against CC attacks

This feature uses kernel-level blocking, machine learning algorithms, and CAPTCHA to intelligently identify and block CC attacks.

A single node can defeat up to 600,000 QPS of CC attacks, preventing your service from exceptional, frequent access requests. With the distributed architecture, SCDN can combat large attacks by intelligently scheduling load balancers among nodes.

Protection against web application layer attacks

Powered by Tencent Cloud's WAF system, massive web attack samples, and AI-based rule engine, this feature smartly identifies common web attacks to prevent SQL injection, unauthorized access, cross-site scripting (XSS), cross-site request forgery (CSRF), and trojan webshell uploading, eliminating bypasses, false negatives, and false positives.

It can also actively monitor and respond to emergent network security events and provide virtual patches against high-risk web vulnerabilities and zero-day vulnerabilities within 24 hours, keeping websites away from emergent web vulnerabilities.

Note：

This feature has been available on SCDN and is free of charge for a limited time.

Protection against bots

With AI-based rule engine and rule library, this feature can identify, monitor, and block over 1,000 known bots, including web crawlers, search engines, and content aggregation tools, helping prevent user data leakage, content infringement, competition-based pricing, inventory query, black hat SEO, and business strategy disclosure caused by malicious bots.

To defeat bots that are not identified, it supports setting the UA, referrer, rate, path, and special parameters along with behavior observation, feature extraction, and business adjustment.

Note：
This feature is in beta test now.

Custom protection rules

This feature supports creating a complex access control rule by specifying fields such as client IP, URI, Referer, User-Agent, and Params, in addition to basic rules defined based on IP, Referer, and UA blocklist/allowlist. The rule can also be tailored to different application scenarios by setting the condition logic (equal to, include, or exclude) for those fields.

Vast Resource Reserves

Powered by Tencent Cloud CDN and ECDN, SCDN delivers an all-out protection against web, DDoS, and CC attacks while accelerating content delivery and transmission. Tencent Cloud CDN has deployed high-performance cache nodes (over 2,000 in the Chinese mainland and over 800 globally), with a total reserved bandwidth of over 150 Tbps, securing Tencent Cloud data centers with quality ISP networks.

Smart Scheduling

Leveraging Tencent Cloud's proprietary GSLB scheduling system paired with smart routing technologies and real-time network-wide monitoring, SCDN schedules access traffic to optimal secure cache nodes to ensure quick responses to service traffic. When experiencing high volumes of traffic attacks, it can perform smart scheduling for load balancing to ensure high business availability.

Quick Configuration

SCDN has integrated with CDN and ECDN, allowing you to easily enable SCDN without any changes to your existing CDN and DNS configurations.

For SCDN domain names connected to CDN/ECDN, you can directly enable SCDN in the console and configure relevant settings. It will take about 5 minutes to deploy your configurations to SCDN nodes, which will not affect the acceleration services.

Use Cases

Last updated：2021-11-25 12:09:53

Use Cases

Tencent Cloud SCDN delivers an all-round protection against cyber security threats posing to different sectors.

Sector	Security Risk	SCDN Capability	SCDN Solution Strength
Governments, enterprises, and media	Websites and apps of governments, enterprises, and media are important windows for them to disclose and disseminate information and interact with the public. Attacks to such websites or information systems may result in service unavailability, content tampering, and reputation decline, interrupt normal information dissemination, and even cause PR crisis.	Protection against DDoS, CC, and web attacks.	It guarantees the high availability of government and enterprise websites and apps, resists web attacks, and prevents website content from being tampered with by attacks and causing PR risks.
Finance	There are many fields in the finance sector, such as banking, securities, fund, and stock, and they are main target fields of attacks. Financial services have very high requirements for availability. When attacks consume system and network resources and cause business interruptions, normal users cannot place transactions and orders, which will cause serious economic losses. In addition, financial origin servers generally store large amounts of sensitive data, and if they are compromised, information leaks will occur and cause greater impact and losses.	Protection against DDoS, CC, and web attacks.	It ensures the stability and high availability of financial applications, resists web attacks, and reduces the leakage risks of origin server content and data.

Sector	Security Risk	SCDN Capability	SCDN Solution Strength
Gaming and streaming media	The gaming and video industries are highly competitive and have always been major targets of DDoS attacks. Since 2017, chess and card games and online videos have developed explosively with a huge influx of capital and users. Horizontal competition triggers malicious competition, network traffic attacks are endless, and DDoS attacks are fast and violent even up to the Tbps level. For related industries, ensuring high service availability and low lag are the prerequisites for retaining players and users.	Protection against DDoS and web attacks.	It secures the stability of game content/resource package download and streaming media transmission. This helps avoid service unavailability and user attrition caused by large traffic attacks in face of frequent malicious competition.
Ecommerce	The ecommerce industry can become vulnerable to DDoS, CC, and web attacks due to malicious competition or blackmail during business peaks, especially at the middle and end of the year, causing service unavailability, declining merchant reputation, customer attrition, and huge economic losses.	Protection against DDoS, CC, and web attacks.	It protects your business from DDoS, CC, and web attacks during high-traffic events.

Use Limits

Last updated：2021-11-25 12:09:53

Connection to SCDN

To connect your domain name to Tencent Cloud SCDN, you need to connect it to Tencent Cloud CDN or ECDN and enable CDN or ECDN services. Then, you can enable SCDN for the domain name. For details about connecting domain names to CDN, see Use Limits.

SCDN Services

Feature	Description
SCDN domain name	Provides a basic package containing 20 SCDN domain names. To increase the limit, you need to purchase packages and you can increase it to 120. To use SCDN, you need to enable CDN as well. Wildcard domain names are not supported.
Statistics	Supports querying attack data over the past one year by default.
Event log	Supports querying attack events over the past seven days and retains your download task for seven days. One download task can contain up to 1,000 log entries. You can only create 100 tasks per day.