

Alibaba Cloud

游戏盾

Product Introduction

Document Version: 20220531

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings> Network> Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.What is Game Shield	05
2.Working principle	06
3.Architecture	08
4.Features - smart scheduling	10
5.Features - Stratified Governance	11
6.Product benefits	12
7.Development history	13

1.What is Game Shield

Compared to the Anti-DDoS Pro service, it effectively defends against large-scale DDoS attacks (T-level) and provides a complete solution for connection flood attacks that are unique to the gaming industry, at lower protection cost and with better results.

On March 29, 2017, Alibaba Cloud Security announced a new risk control model for the gaming industry at the Yunqi Conference in Shenzhen: Game Shield. Game Shield has innovative risk management methods and algorithms to help users in the gaming industry mitigate massive DDoS attacks and connection flood attacks at a lower cost and solve the problem of unequal resources in the previous attack and defense framework.

Compared to the traditional single-point DDoS defense solution, Game Shield uses data and algorithms to implement smart scheduling, quickly splitting “normal player” traffic and “hacker attack” traffic to different nodes to mitigate massive DDoS attacks, and through end-to-end encryption, preventing minor DDoS attacks that simulates user behavior from reaching the client.

Meanwhile, in traditional defenses, it is easy for hackers to lock onto an IP for attack and minimize their own damage during the attack. The smart scheduling and identification functions of Game Shield allow users to “hide” themselves and “expose” hackers - each attack impairs hackers, and the attack devices and broilers can no longer be available. This reverses the previous situation where the DDoS offensive and defensive resources were unequal.

2.Working principle

An elastic security network is the key to GameShield, which defends against DDoS attacks through edge devices.

Overview

GameShield offers an elastic security network that can only be accessed by using SDK and prevents DDoS attacks and HTTP flood attacks. A client can access the elastic security network of GameShield through a local proxy server. This allows a gamer (Token) to access the port (Dport) with the origin IP address (Dip) through a node group (GroupName).

SDK code sample: `YunCeng.getProxyTcpByDomain(Token, GroupName, Dip, Dport)`

Parameter description


Parameter	Description
Token	The ID of a gamer. It is used to identify the malicious gamers or hackers who initiate DDoS attacks. Default value: Default.
GroupName	The node group ID of a game business. Example: access.v812vCOE21.ftnormal01al.com. In the GameShield console, after you add a game and a business, you must configure node groups. For each node group, you need to determine the number of nodes based on the number of simultaneous gamers. You can specify multiple node groups for each game.
Dip	The IP address of an origin server. You must configure it in GameShield.
Dport	The port of the server. You do not need to configure it in GameShield. You can pass it to GameShield based on your business requirements.

Endpoints for different protocols

You can use a client SDK to deploy a local proxy server on the client so that the proxy server can map any server-side IP addresses and ports to local services. In this way, the proxy server forwards all related data flows between the client and the server and performs routing and data encryption. This architecture provides strong protection for your business, such as data encryption and defense against DDoS attacks and HTTP flood attacks.

The following table describes the endpoints for different protocols.

Protocol	Endpoint used for direct access	Endpoint used for proxy-based access
TCP	tcp://192.168.0.1:8080	tcp://127.0.0.1:8729 (random port)
HTTP	http://www.aliyundoc.com	http://127.0.0.1:2892 (random port)

Protocol	Endpoint used for direct access	Endpoint used for proxy-based access
HTTPS	https://www.aliyundoc.com	<p>https://127.0.0.1:2892 (Certificate verification may fail.) -> https://www-yxd.aliyundoc.com:2892</p> <div><p> Note You can use a domain name such as www-yxd.aliyundoc.com to solve the issues raised by hostname mismatch and HTTPS certificate verification failures. For more information, see Best practice for dealing with HTTPS business.</p></div>
WebSocket	ws://192.168.0.1:88	ws://127.0.0.1:2891 (random port)

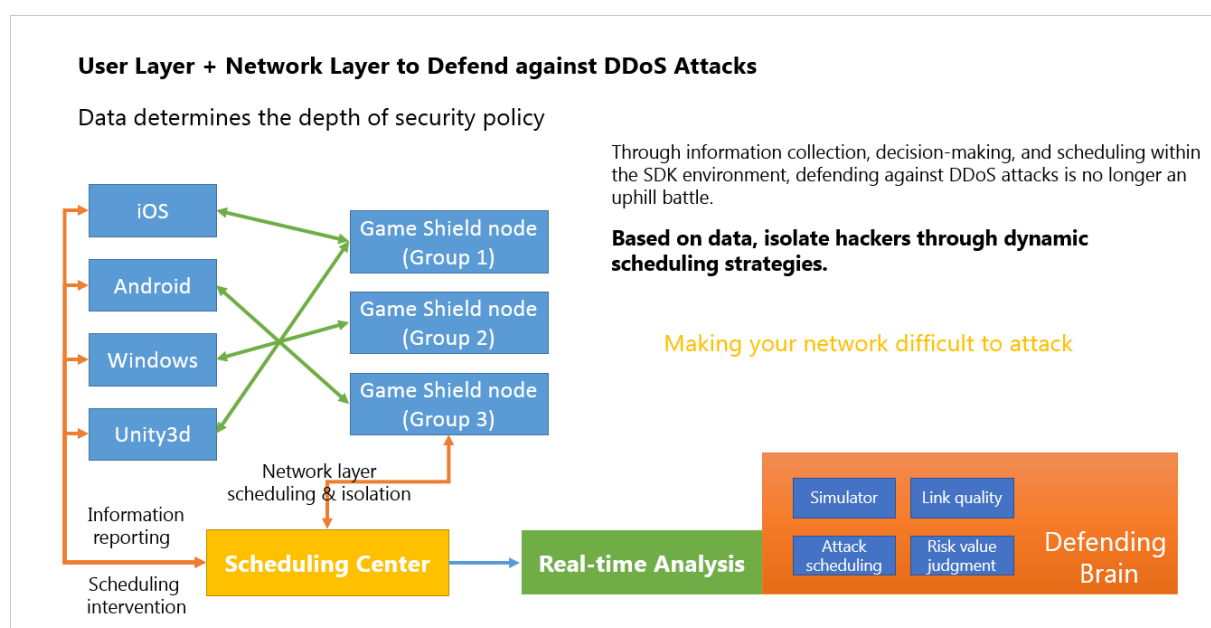
3. Architecture

GameShield is a security solution in the Alibaba Cloud Anti-DDoS series. It is designed for the gaming industry. GameShield aims to address issues, such as complex DDoS attacks and HTTP flood attacks that are faced by the gaming industry.

GameShield consists of two modules:

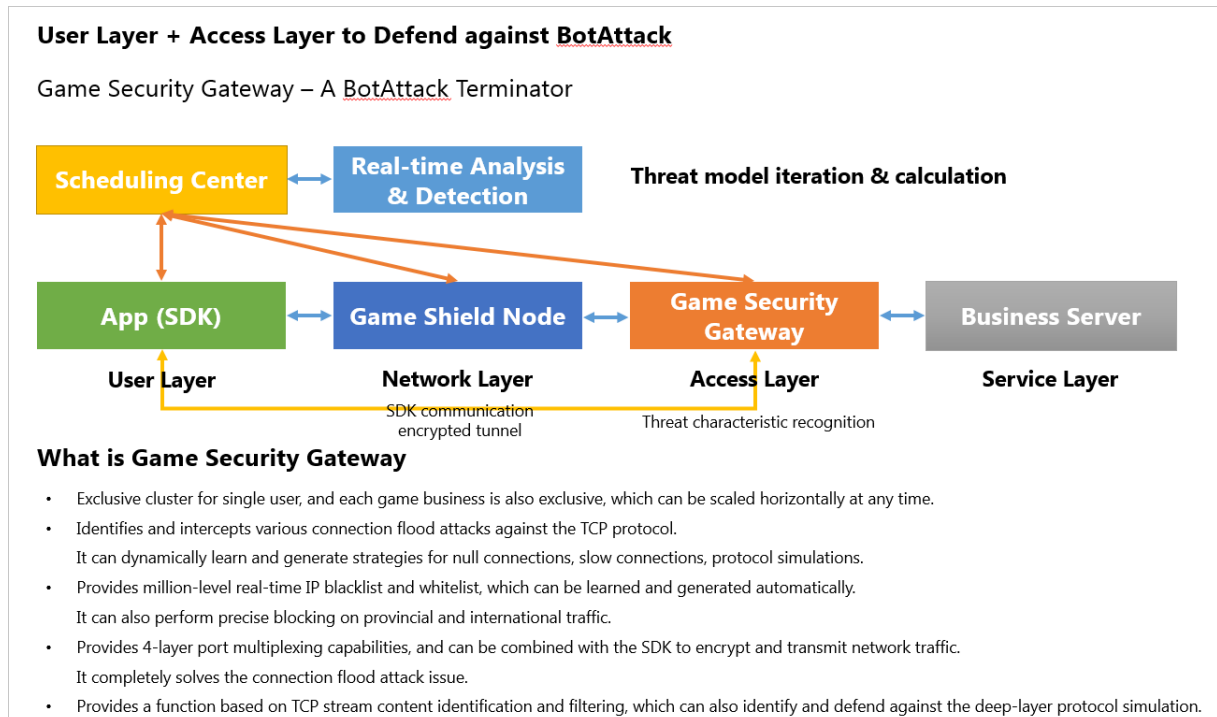
- **Distributed anti-DDoS node:** GameShield utilizes these nodes to defend against attacks greater than 600 Gbit/s.
- **Game Security Gateway:** GameShield can decode proprietary protocols. This allows GameShield to defend against HTTP flood attacks that are specific to the gaming industry.

How GameShield defends against DDoS attacks



Unlike the standard Anti-DDoS Pro or Anti-DDoS Premium data center, GameShield does not defend against attacks by using massive bandwidth, but uses the distributed anti-DDoS nodes. These nodes split and disperse attacks so that the attacks are not concentrated on a specific point. GameShield isolates attackers by using dynamic scheduling policies based on data generated by Software Development Kit (SDK) calls and traffic data.

How GameShield defends against HTTP flood attacks



In general, HTTP flood attacks in the gaming industry are different from those targeting websites. Website-targeted HTTP flood attacks are based on the HTTP or HTTPS. These protocols are standardized, and it is easy to perform data analysis and protocol analysis on these attacks. However, most of the protocols in the gaming industry are proprietary or uncommon. Therefore, to defend against game-targeted HTTP flood attacks, GameShield uses the professional cloud-based Game Security Gateway, which is formerly known as NetGuard, or NG for short.

Game Security Gateway establishes a firewall between user services and attackers. Game Security Gateway can distinguish real players from attackers based on the TCP connection behavior of attackers, post-connection dynamic information, and all traffic data.

- Game Security Gateway supports big data analytics. It analyzes user behaviors based on the characteristics of real users and directly intercepts abnormal clients with invalid protocols. It can also block specific traffic from regions in and outside China at any time by using blacklists or whitelists, which allow millions of entries.
- Game Security Gateway can establish an encrypted communication tunnel with SDKs. All network communications between clients and servers use the encrypted communication tunnel. Only the traffic authenticated by SDKs and Game Security Gateway is allowed. This eliminates TCP-layer HTTP flood attacks (attacks that simulate protocol layer attacks).

Note SDK 5.1.7 or later is required.

4.Features - smart scheduling

Innovation on Technology: Splitting Traffic through the Smart Scheduling Algorithm

DDoS attack and defense is a battle of resources. From the network, the CDN, the server to the database, DDoS attacks can occur if a resource difference exists.

Resource type	User	Hacker
Bandwidth resource	G-level limited bandwidth and black hole routing mechanism triggered by peaks	T-level overwhelming bandwidth resource
Broilers resource	Limited server resource	Large-scale leading broiler resource
Technical resource	A complete area requiring protection	Only one point needs to be broken
Capital resource	Limited budget + high protection costs	Nearly no cost

From the cloud layer, the burstable security network to the current Game Shield, after years of working with gaming industry users side by side, Alibaba Cloud's security team has used data and algorithms to change the pattern of large-scale DDoS attack defense.

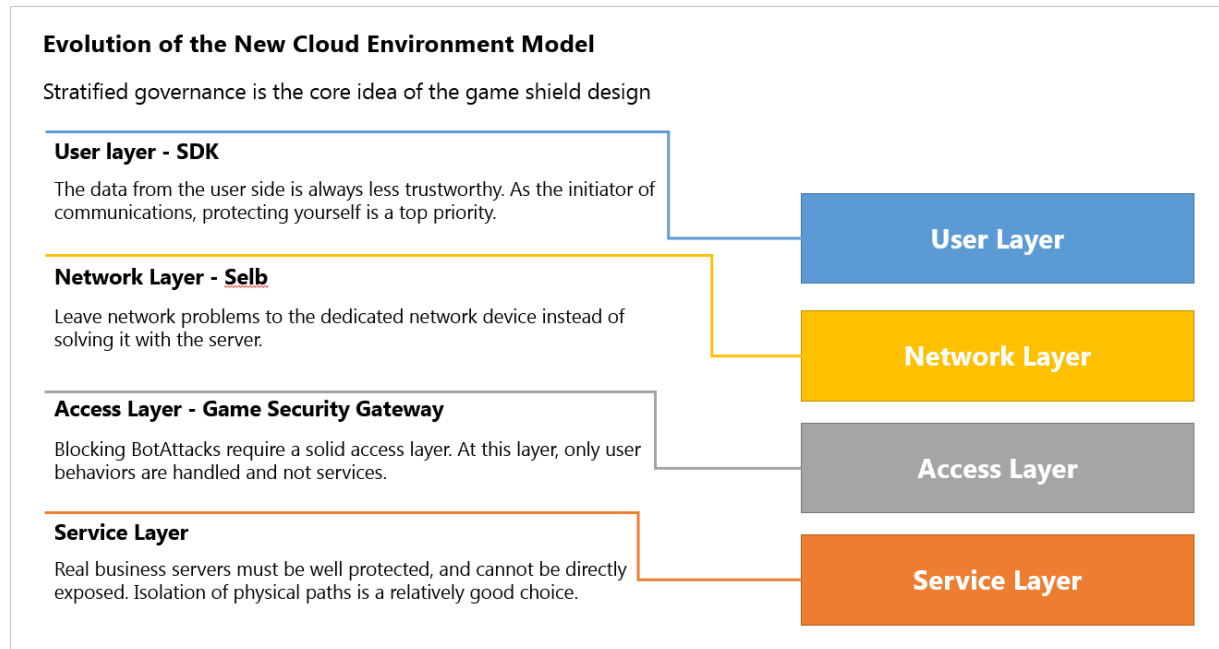
Today, when dealing with hackers, Game Shield not only defend passively but also has the ability to counterattack. It effectively identifies which client is a hacker and which client is a normal user. By using more flexible scheduling algorithms, it splits the user's normal traffic and hackers' attack traffic to different places, so it can hold off massive DDoS attacks again and again.

During the evolution of Game Shield, the Alibaba Cloud security team has successfully balanced the four major kinds of resource inequality:

- How to defense overwhelming T-level bandwidth resources
- How to break hackers' broiler resources
- How to fill the gaps that enable hackers to attack only a point while users must guard the whole area
- How to reduce the capital cost

5.Features - Stratified Governance

Innovation on Risk Control Mode: From Single-Point Defense to Stratified Governance



Stratified governance is the basis for solving these problems. Inequality of any resource is derived from the fact that a target is too easy found by the attacker, and the defender is too easy of a target.


The “layer by layer” manner in governance represents the splitting of traffic, the splitting of services, and the splitting of targets, which increases the costs and thresholds for attackers and minimizes the costs for users. “Layer” represents a kind of funnel model. In the past, we used bandwidth to combat DDoS attacks. In Game Shield, we use the most suitable ‘weapons’ for what they are best at.

- **User layer (SDK):** The data at the user level is always less trustworthy. As the initiator of communications, protecting yourself is a top priority.
- **Network layer (Selb):** Leave network concerns to the dedicated network devices, rather than solely relying on the server way.
- **Access layer (Game Security Gateway):** Do you still remember the impact of connection flood attacks? The access layer is prepared to defense them. At this layer, only user behavior is processed; businesses are not processed.
- **Service layer:** The real business server must be well protected and cannot be directly exposed. Isolation of physical paths is a relatively good choice.

Game Shield has changed the traditional method of defending against DDoS attacks where it becomes a battle of bandwidth and is a comprehensive risk control solution for the gaming industry. Under the risk control theory of Game Shield, if we solve the problem on the user side, we can defend against DDoS attacks of any size, thus achieving the balance of attack and defense costs.

6.Product benefits

Comparison Items	Game Shield	Traditional DDoS Traffic Cleansing Data Centers
Massive DDoS attacks on the gaming industry	Gets away from arms race of DDoS attack and defense, professionally defending massive DDoS attacks on the gaming industry . Distributed anti-DDoS nodes . High-quality BGP access to provide a highly available network environment for games.	Only relies on one local data center, and bandwidth is not expandable, making it unable to defend against larger DDoS attacks.
Fingerprint encryption/link encryption	Supports TCP/HTTP/HTTPS . Suitable for all kinds of service scenarios, such as mobile games, client games, and so on . Supports in-cloud/out-of-cloud client. Integration game SDK. Full-link encryption for data packets, and anti-cracking. End-to-end encryption for security access of games. Supports protection against attacks on simulated game protocols. Supports decoding for proprietary game protocols. Supports real-time adjustment of protection algorithms.	The traditional data center cleaning relies on hardware devices for identification and cannot decode proprietary game protocols.
Supports decoding proprietary game protocols	DPI (deep packet inspection) technology, automatically establishes protocol features through machine learning, and only releases requests that meet the protocol features.	The traditional data center cleaning relies on hardware devices for identification and cannot decode proprietary game protocols.
Custom game protection algorithm	Defends against empty connections, slow connections, malicious kicker attacks, global botnet repository, and SHIELD attack tracing for games.	Most traditional data centers use firewall devices or hardware devices, making the update of defense algorithms slow and the data centers do not have the ability to adjust the defense algorithms.

 **Note** HTTP flood protection support for the HTTP/HTTPS protocol is provided by the Web Application Firewall product, which is purchased separately.

7. Development history

History of Game Shield

Game Shield has experienced three major technological evolutions since its inception. From the first generation's "Cloud layer" to the current Game Shield, major improvements have taken place both in terms of its technical architecture and functional implementation.

One of the reasons for these changes is the inequality problem of attacking and defense resources; while another reason is based on our reflection on the routing rules and infrastructure of existing networks.

In simple terms, Game Shield balances the attacking and defense resources by dispatching traffic in a risk control mode. In essence, Game Shield is more like a way to change traffic directions beyond routing and DNS.

Cloud Layer: First Experiment

The predecessor of Game Shield is the Cloud layer project. It was born from a rescue experiment in early 2015.

A company had been repeatedly attacked by hackers and traditional DDoS defense methods had all been ineffective. In such an emergency, the company sought cooperation from Alibaba Cloud's security team and proposed a new method that could avoid hacker attacks through fast traffic scheduling.

At the time, this method had not been verified in any actual implementation. Alibaba Cloud's DDoS protection and security technology team collaborated with the user's technical team in a manner like "feeling the way in the dark" and after putting this new protection method into practice, it succeeded in combating a series of attacks.

The "Cloud layer" era began.

At the time, the hackers' attack tactics were relatively simple. They found a target IP address, and hit the IP into the black hole routing status through a wave of large DDoS attacks (10~50GBps). The preparation time for a hacker to launch a next wave of attacks was about 10-15 minutes. The rapid scheduling of distributed IPs within seconds by the "Cloud layer" suppressed the hacker's continued minute-level attacks and won a small victory.

Afterwards, the "Cloud layer" model won several other victories. Meanwhile, however, new forms of attacks are constantly being developed. "Cloud layer", despite achieving a second-level IP scheduling speed, must adapt its algorithms and efficiency to keep pace with hacker attacks. In this context, the era of Game Shield has arrived!

Game Shield: Enter the battlefield

It has always been the case that over 50% of domestic DDoS and connection flood attacks target the gaming industry. Thus, the gaming industry has become the best target for DDoS attackers, and it is also the best industry for testing and scheduling algorithms.

Therefore, Alibaba Cloud's security team decided to apply the accumulated technical experience from the "Cloud layer" era to the gaming industry and turn it into a risk control model that all users can use and take advantage of.

A long time before Game Shield was born, Alibaba Cloud's security team rigorously analyzed the attack and defense patterns in the gaming industry, and learned the characteristics of registration, login, and players of the game services. On this basis, it reconstructed the smart scheduling algorithm of Game Shield.

Game Shield not only inherits the fast scheduling capability of the Cloud layer, it can also perform normalized process analysis through collecting terminal information and network communications. Based on the resources and features on the cloud, Game Shield can calculate, process, and store massive amounts of terminal data. Compared with the offline environment, Alibaba Cloud has achieved substantial breakthroughs by taking advantage of cloud computing platforms in computing and data processing: the image of each terminal device is completed, and finally settled into a new scheduling factor of "terminal threat value" .

The core of all data processing at Game Shield is the AirTraffic Control (ATC) system, of which the cognitive foundation is based on deep machine learning (DL) and Long Short-Term Memory (LSTM). It can quickly isolate malicious users from the dispatch system.

On the front lines of the gaming industry, Game Shield has proven its capabilities and continues to upgrade itself under the heaviest of attacks. Meanwhile, threat identification and affected area control have replaced scheduling to become the new technical keywords.

Refinement and Stratified Governance: A Small Step Ahead

This is only the beginning. Attackers are also gradually increasing their own resource input. If you want to stay a small step ahead of hackers, data and algorithms alone are not enough. You must truly understand their attack trends and attack tactics.

Game Shield was refined through implementation in actual scenarios and finally evolved into streamlined solution: NetGuard was born.

With the help of the AI modeling and analysis capabilities accumulated in the previous two phases, Game Shield challenges the attacks against the business layer.

Game Shield serial learns the characteristics of specific business data to quickly identify malformed and sudden abnormal traffic, and blocks it on the trunk. Meanwhile, Alibaba Cloud's security team proposed a three-dimensional protection system that consists user-layer, network-layer, access-layer, and business-layer linkages, so that Game Shield can help users build the most suitable security architecture.

The core of the three-dimensional protection system of Game Shield lies in stratified governance. First, large traffic attacks rely on the network layer to solve, while technical connection flood attacks are solved through access layer. The three-dimensional protection system can breakthrough bandwidth limitations, control the range and time of the attack, and accurately identify the user's behavior.

A Tilted Balance

From 2015 to 2017, two years experience and technical polishing have enabled Game Shield to apply a new security risk control mode to help gaming industry users solve significant problems.

Nevertheless, from Cloud layer to Game Shield, it is only the first step of Alibaba Cloud's security team tilting the balance of DDoS attacks. The true direction for advancement is to build a safe and credible network that carries "clean traffic" and to extend this network further out.