-

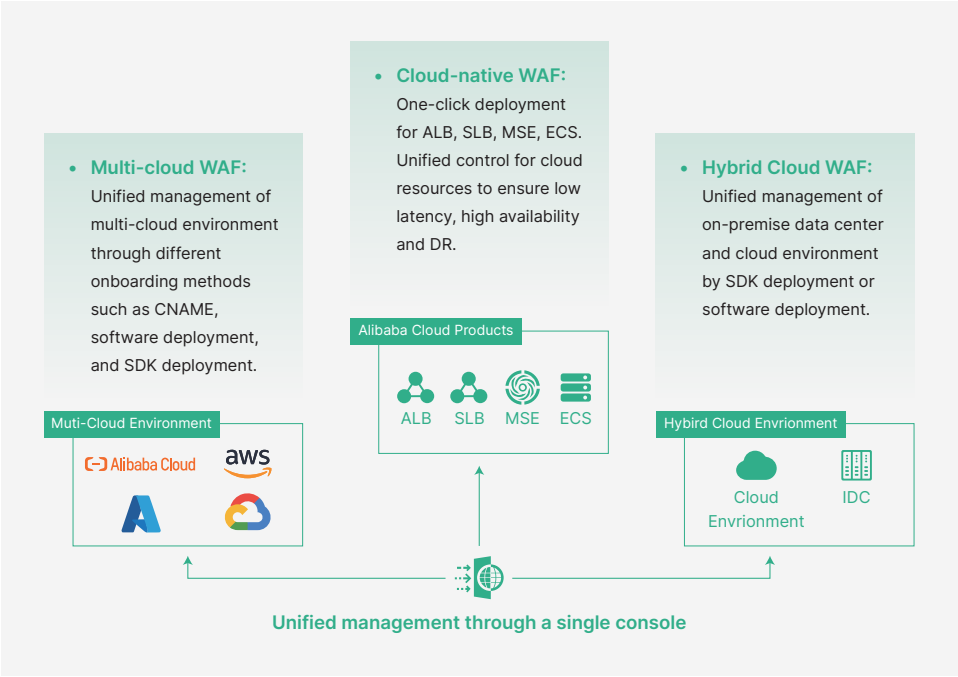
Alibaba Cloud Web Application Firewall

#WAF #Cloud Firewall
#DDoS #KMS
#Cloud Security Center

Alibaba Cloud Web Application Firewall

One-stop Solution for Web Intrusion Prevention, API Protection and Bot Management.

Alibaba Cloud Web Application Firewall was built on a global infrastructure that includes multiple clusters, and data centers distributed around the world to ensure high availability and rapid disaster recovery. Additionally, it offers a one-click bypass feature to redirect traffic to the origin server in case of an emergency or false-positive detections, an SLA of 99.95% for the entire year, with high-risk alerts push notification through DingTalk.



Web Intrusion Protection: AI-based Proactive Defense

Intrusion Protection

- 23 deep decoding capabilities, 100+ applications, 300+ high-risk fingerprint libraries.
- Provide protection against common web attacks, including SQL injection, XSS, Webshell upload, directory traversal, and backdoor implantation.
- Automatically blocks malicious scans and probes to prevent server performance issues, data leaks, and website tampering, among other risks.

Virtual Patch for Vulnerabilities

- Provide virtual patches for security vulnerabilities in web applications (such as CVE/CNVD, etc.).

0-day Emergency Response

- Automatic defense against the latest web vulnerabilities (0-day) within a few hours.
- Global/Regional bans within milliseconds.
- If a single user is attacked, all nodes are protected by 'immunity protection'.

Intelligent learning Engine

- Based on multiple intelligent engines including traffic white baseline, deep learning, and proactive defense. Effectively identify unknown attack features with 100 million+ attack samples learned per day.

Threat Intelligence

- Threat intelligence based on Alibaba Cloud's network attack data (botnet library, IP address library, crawler library, HTTP proxy library, etc.).

Bot Management

Comprehensive scenario-based protection and control for web pages, H5, apps, APIs, official accounts and mini programs, addressing business risks such as cheating, coupon fraud, and information scraping, and mitigating CC attacks (HTTP Flood).

Accurately identify bad bots

More than 7,000 device environments, traffic, messages, and behavioral fingerprints are collected and reported (purely hardware-based and anonymized without violating privacy), and countermeasures are issued automatically.

Scenario-based protection, continuously combating evolving attacks.

Define protection targets based on scenarios such as ordering, registration, login, and price checking, with recommended protection policies. Visualize human-machine traffic ratio and interception analysis.

Comprehensive HTTP traffic feature management,

Meeting personalized access control and rate limiting requirements.

Wide range of countermeasure actions such as blocking, rate limiting, and deception,

deeply integrated with risk control policies to provide comprehensive protection.

API Discovery and Protections

API lifecycle management to protect sensitive personal information, keys, enterprise sensitive information, and device sensitive information.

- Proactively discover API risks such as rouge/deprecated APIs, lack of authentication, excessive data exposure, and sensitive information leakage.
- Automatically classify/grade API interfaces to effectively detect the flow of sensitive data in the business.
- Identify API interface vulnerabilities and provide detailed risk analysis and control suggestions.
- Based on intelligent models, establish API call baselines and promptly alerts users of abnormal attack events.

BENEFITS TO YOUR BUSINESS

One-stop Solution for Web Application Protection

- Manage multi-cloud and hybrid cloud through one console.
- Achieve web security, BOT management, and API security with one product.
- Address the issue of dispersed business protection across multiple regions and areas.

Real-time Risk Monitoring and Vulnerability Defense

- 7×24h real-time monitoring of abnormal indicators, ensuring rule updates within 24 hours to all devices.
- Automatic defense against the latest web vulnerabilities (0-day vulnerabilities) within a few hours, without manual patching.

Cloud-native Security, easy to deploy

- One-click enablement for CDN, ALB, and ECS users, without changing DNS.
- No changes to the original network architecture.
- Real-time configuration synchronization with ALB and CDN.

Attack Analysis and Tracing

- Support full log storage, and provide scenario-based log analysis reports and a visual dashboard for real-time analysis, display, and tracing purposes.

Flexible Billing Models to Reduce Costs

- Pay-as-you-go, with an ultimate service experience.
- Support multiple payment methods such as annual/monthly package, pay-as-you-go, SeCU (Security Capacity Unit) resource package, elastic post-payment, etc.

CERTIFICATIONS

The only WAF product in mainland China to receive full accreditations from international authoritative research institutions.

- Selected for Forrester's "Now Tech: Web Application Firewalls, Q2 2022".
- The only one in Asia Pacific selected for Gartner's "Magic Quadrant for Web Application Firewalls 2019" report, with intelligent algorithms recognized as a strong capability.
- Leader in the "IDC MarketScape: 2019 China Web Application Security Market Vendor Assessment" report.
- Ranked first for four consecutive years since the 2019 Frost & Sullivan Greater China Cloud WAF market share rankings.

-

Alibaba Cloud Anti-DDoS

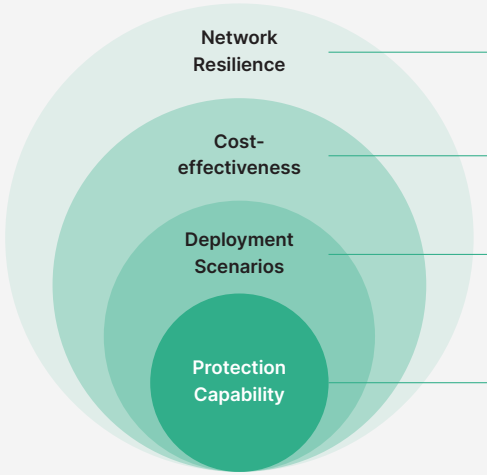
#WAF #Cloud Firewall
#DDoS #KMS
#Cloud Security Center

Alibaba Cloud Anti-DDoS

Alibaba Cloud Anti-DDoS service is based on Alibaba Cloud's global scrubbing centers, combined with intelligent DDoS detection and protection systems developed at Alibaba. This service automatically mitigates attacks and reinforces the security of your applications, reducing the threat of malicious attacks.

KEY CAPABILITIES

What to look out for when selecting DDoS protection products?



- Network Resilience → Disaster Recovery: Elastic scaling and dynamic scheduling. Monitoring and Alerting: Rapid response to new types of attacks and rapid deployment of polices.
- Cost-effectiveness → ROI
- Deployment Scenarios → Compatible with multiple business scenarios and low latency.
- Protection Capability → Effective mitigation effectiveness and broad protection coverage.

Why Alibaba Cloud?

Network Resilience

- Global Defense Capability: 14 global nodes, over 10T defense resources.
- Real-time Monitoring: 1-second detection and 2-second processing of abnormal traffic, and 3-second processing completion.
- ntelligent Scheduling: Cross-border Acceleration, Intelligent Scheduling Linkage in CDN Scenarios.

Cost-effectiveness

- Pay-as-you-go
- Tiered Pricing
- Global Protection

Deployment Scenarios

- Proxy Mode
- Cloud-Native Protection
- SDCDN

Protection Capability

- Intelligent Protection Capability: Intelligent Protection Engine, Automatic Distribution of Strategy Protection.
- Layer 7 Defense Capability: AI Intelligent CC Protection Strategy, Protection Performance up to 25 million QPS.

CERTIFICATIONS

- The only mainland China company selected in The Forrester Wave: DDoS Mitigation Solutions, Q1 2021. Intelligent Defense Engine was highly recognized.
- Selected twice for the Forrester Now Tech Market Presence Segment: DDoS Mitigation Solutions report.
- Ranked first in the Frost & Sullivan DDoS Greater China market share for three consecutive years, surpassing the total of all other vendors combined.

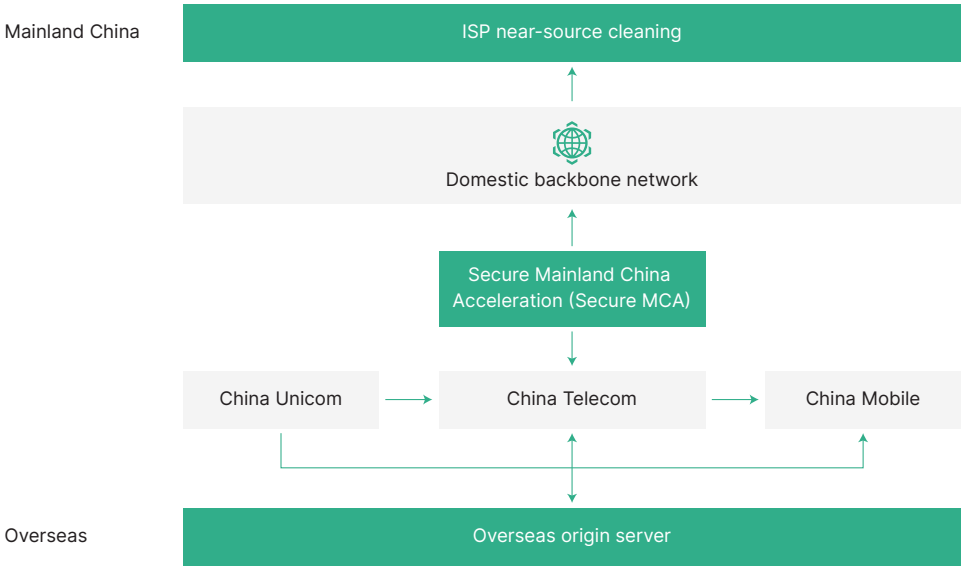
TYPICAL DEPLOYMENT ARCHITECTURE

Severs and the end-users are both located outside mainland China

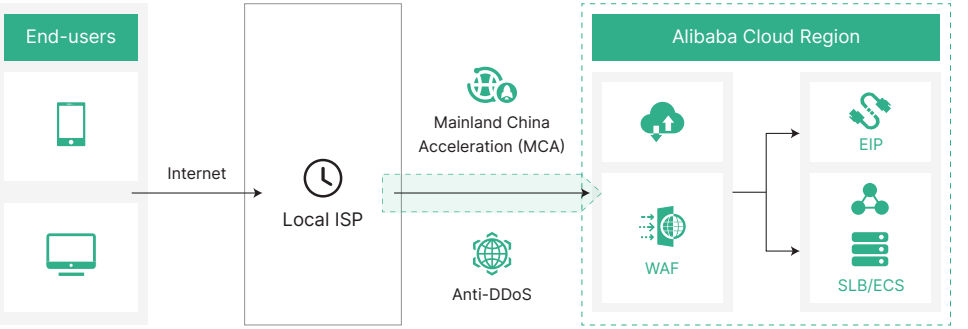
Protection Architecture	End-users outside of mainland China →	Anti-DDoS →	Overseas origin server
Onboarding Process	1 Domain and port configuration	2 DDoS protection instance back-to-origin IP whitelist + origin server protection	3 DNS resolution to DDoS protection CNAME
Recommended Products	Anti-DDoS Premium Insurance	Anti-DDoS Premium Unlimited	

Servers are outside mainland China, the end-users are located in mainland China

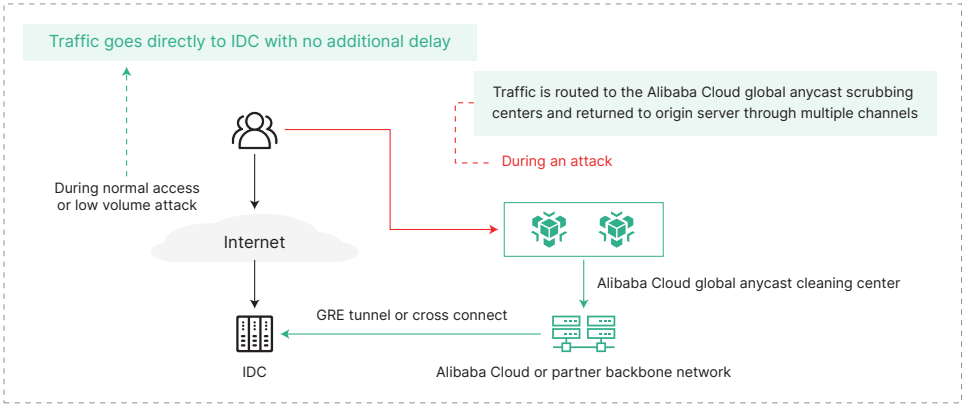
Solution 1: Secure Mainland China Acceleration (Secure MCA) solution, which performs DDoS attack mitigation during cross-border acceleration. It uses ISP DC for near-source cleaning, doesn't require traffic scheduling, and has no delay.



Solution 2: Anti-DDoS Premium + Mainland China Acceleration (MCA). During normal access, MCA is used to ensure low access latency. In case of a DDoS attack, it intelligently switches to Anti-DDoS Premium for attack mitigation.



Cloud-native Defense Scenario



SDCDN