ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

防護配置

Document Version: 20210817

Alibaba Cloud

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 `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.最佳實踐

1.1. Web防護功能最佳實務

本文介紹了阿里雲雲盾Web Application Firewall的Web攻擊防護最佳實務，主要從應用情境、防護策略、防護效果、規則更新四個方面進行介紹。

應用情境

Web Application Firewall（Web Application Firewall，簡稱WAF）主要提供針對Web攻擊的防護，例如SQL注入、XSS、遠程命令執行、Webshell上傳等攻擊。關於Web攻擊的詳細資料，請參考OWASP 2017 Top 10。

> **說明** 主機層服務的安全問題（例如Redis、MySQL未授權訪問等）導致的伺服器入侵不在WAF的防護範圍之內。

防護策略

在將網站成功接入WAF防護後，登入Web Application Firewall控制台，在**管理 > 網站配置**頁面選擇已防護的網站，並單擊**防護配置**，即可查看Web應用攻擊防護的防護狀態，如圖所示。

Web應用攻擊防護功能預設開啟，並使用正常模式的防護規則策略。其中，

- **狀態**
  - **開啟**表示WAF的Web應用攻擊防護模組已開啟。
  - **關閉**表示該防護模組處於關閉狀態。
- **模式**：分為防護和預警兩種模式。
  - **防護**模式表示當遭受Web攻擊時，WAF自動攔截攻擊請求，並在後台記錄攻擊日誌。
  - **預警**模式表示當遭受Web攻擊時，WAF不會攔截攻擊請求，僅在後台記錄攻擊日誌。
- **防護規則策略**：分為寬鬆、正常、嚴格三種模式，僅在啟用防護模式後生效。
  - **寬鬆**防護規則策略的防護粒度較粗，只攔截攻擊特徵比較明顯的請求。
  - **正常**防護規則策略的防護粒度較寬鬆且防護規則策略精準，可以攔截常見的具有繞過特徵的攻擊請求。
  - **嚴格**防護規則策略的防護粒度最精細，可以攔截具有複雜的繞過特徵的攻擊請求。

使用建議：

- 如果您對自己的業務流量特徵還不完全清楚，建議先切換到預警模式進行觀察。一般情況下，建議您觀察一至兩周，然後分析預警模式下的攻擊日誌。
  - 如果沒有發現任何正常業務流量被攔截的記錄，則可以切換到防護模式啟用攔截防護。
  - 如果發現攻擊日誌中存在正常業務流量，可以聯絡阿里雲安全專家溝通具體的解決方案。
- PHPMyAdmin、開發技術類論壇接入WAF防護可能會存在誤攔截的問題，建議聯絡阿里雲安全專家溝通具體的解決方案。
- 業務操作方面應注意以下問題：
  - 正常業務的HTTP請求中盡量不要直接傳遞原始的SQL語句、JAVA SCRIPT代碼。
  - 正常業務的URL盡量不要使用一些特殊的關鍵字（UPDATE、SET等）作為路徑，例如 `www.example.com/abc/update/mod.php?set=1` 。

- 如果業務中需要上傳檔案，不建議直接通過Web方式上傳超過50M的檔案，建議使用OSS或者其他方式上傳。

- 開啟WAF的Web應用攻擊防護功能後，不要禁用預設精準存取控制規則中的Web防護通用防護模組，如圖所示。

防護效果

開啟WAF的Web應用攻擊防護功能後，您可以在**統計 > 安全報表**頁面，查看攻擊的攔截日誌，如圖所示。

在**安全報表**頁面，您可以查看昨天、當天、7天以及一個月內的攻擊詳情。同時，單擊**查看攻擊詳情**，可以查看具體的攻擊資訊，如圖所示。

該截圖中的攔截日誌即為一條已被WAF攔截的SQL注入攻擊請求。

> **說明** 如果您發現WAF誤攔截了正常業務流量，建議您先通過精準存取控制功能對受影響的URL配置白名單策略，然後聯絡阿里雲安全專家溝通具體解決方案。

規則更新

對於互連網披露的已知漏洞和未披露的0day漏洞，雲盾WAF將及時完成防護規則的更新，並發布防護公告。

您可以登入Web Application Firewall控制台，前往**總覽 > 安全**頁面，查看最新發行的防護公告，如圖所示。

該截圖中公告欄展示了針對weblogic遠程命令執行漏洞的防護規則的更新公告。

> **說明** Web攻擊往往存在不止一種概念證明方法（Proof of Concept，簡稱PoC），阿里雲安全專家會對漏洞原理進行深度分析從而確保發布的Web防護規則覆蓋已公開和未公開的各種漏洞利用方式。