ALIBABA CLOUD

Alibaba Cloud

DDoS防护

DDos 保護ガイド

Document Version: 20200919

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

1.一般的な DDoS 攻撃

DDoS (分散型 DoS 攻撃) は、クライアント/サーバー技術を利用した、複数のコンピュータを組み合わせて 1 つまたは複数のターゲットに攻撃を開始するプラットフォームを形成するため、DoS 攻撃よりも桁違いに大きな脅威となります。

不正パケット

不正パケットとは、Frag フラッド攻撃、Smurf 攻撃、Stream Flood 攻撃、Land フラッド攻撃、IP 不正パケット、TCP 不正パケット、UDP 不正パケットを指します。

トランスポート層 DDoS 攻撃

トランスポート層に対する DDoS 攻撃とは、SYN フラッド、Ack フラッド、UDP フラッド、ICMP フラッド、および RST フラッド攻撃を指します。

DNS DDoS 攻撃

DNS DDoS 攻撃とは、DNS リクエストフラッド攻撃、DNS レスポンスフラッド攻撃、有効・無効な送信元 DNS クエリフラッド攻撃、DNS コンテンツサーバー攻撃およびローカルサーバー攻撃を指します。

接続 DDoS 攻撃

接続 DDoS 攻撃とは、低速 TCP 接続攻撃、帯域幅枯渇攻撃、LOIC (Low Orbit Ion Cannon)、HOIC (High Orbit Ion Cannon)、SlowLoris、PyLoris、および XOIC といった低速攻撃を指します。

Web アプリケーション DDoS 攻撃

Web アプリケーション層攻撃とは、HTTP Get フラッド、HTTP Post フラッド、および HTTP フラッド攻撃を指します。

2.DDoS 攻撃の軽減に向けたベストプラクティス

DDoS 攻撃 (分散型 DoS 攻撃) は標的システムに対する悪質なサイバー攻撃です。 通常、攻撃対象のサービスに正常にアクセスできなくすることにより、サービスを妨害します。

以下は一般的な DDoS 攻撃です。

- ネットワーク層への攻撃

  ネットワーク層に対する代表的な攻撃には UDP リフレクション攻撃があります。 主にトラフィックを増大させることにより、被害者のネットワーク帯域幅を混雑させ、被害者のサービスが顧客のアクセスに正常に応答できなくなります。

- トランスポート層への攻撃

  トランスポート層に対する代表的な攻撃には、SYN フラッド攻撃、接続攻撃があげられます。 サーバーの接続プールリソースを占有することにより、サービスを妨害します。

- セッション層への攻撃

  セッション層に対する代表的な攻撃には、SSL 接続攻撃があります。 サーバーの SSL セッションリソースを占有することにより、サービスを妨害します。

- アプリケーション層への攻撃

  アプリケーション層に対する代表的な攻撃には、DNS フラッド攻撃、HTTP フラッド攻撃、ダミー攻撃があります。 サーバーのアプリケーション処理リソースを占有し、また、サーバーの処理パフォーマンスを著しく低下させることで、サービスが妨害されます。

DDoS 攻撃を軽減するためのベストプラクティス

Alibaba Cloud のユーザーには、DDoS 攻撃の軽減に以下を推奨します。

- 公開項目を最小限にし、サービスに関係のないリソースを隔離することにより攻撃リスクを減らす
  - セキュリティグループを作成

    サービスに関係のないリクエストやアクセスを回避するため、パブリックネットワーク上のサービスに必要のないポートをできるだけ公開しないようにします。 セキュリティグループを設定することにより、不備によってシステムがスキャンまたは公開されることを防ぐことに効果があります。

    詳しくは、「セキュリティグループユーザーガイド」をご参照ください。

  - VPC (Virtual Private Cloud) の使用

    VPC により、論理的にネットワークを隔離することで、ウイルスに感染したコンピューターによる攻撃を防ぎます。

    詳しくは、「VPC ユーザーガイド」をご参照ください。

- システム設計を最適化し、パブリッククラウドの自動スケーリングおよびフェールオーバーを採用
  - Server Load Balancer のデプロイ

    ある程度のトラフィック量によるトランスポート層に対する DDoS 攻撃は、SLB (Server Load Balancer) インスタンスをデプロイして複数のサーバーに負荷を分散することで効果的に軽減できます。 なお、SLB をデプロイすると、ユーザーのサーバーへのアクセストラフィックは均等に割り振られます。各サーバーにかかる負荷は軽減し、アクセス速度を速めることができます。

    詳しくは、「SLB ユーザーガイド」をご参照ください。

- Auto Scaling のデプロイ

  Auto Scaling は保守サービスであり、お客様の要件とポリシーに応じて経済的に ECS (Elastic Compute Service) リソースを自動的に最適化します。 Auto Scaling をデプロイすることにより、システムはセッション層およびアプリケーション層への攻撃を効果的に緩和します。攻撃を受けた場合、サーバーが自動的に追加され、処理パフォーマンスが向上し、サービスへの深刻な影響を回避できます。

  詳細については、「Auto Scaling ユーザーガイド」をご参照ください。

- DNS 解決を GEO DNS で最適化し、DNS トラフィック攻撃によるリスク回避に効果があります。 また、サービスを複数の DNS サービスプロバイダーにホスティングされることを推奨します。
  - 要求されていない DNS 応答情報をシールド
  - 高速な再伝送データパケットを破棄
  - TTL を有効化
  - 未知の DNS クエリリクエストおよびレスポンスデータを破棄
  - 要求されていない、または突然の DNS リクエストを破棄
  - DNS クライアント検証を有効化
  - 応答情報をキャッシュ
  - ACL 許可を使用
  - ACL、BCP38、および IP レピュテーションを使用

- その他の帯域幅を準備

  サーバーのパフォーマンステストを実行して、通常のサービス環境に耐え得る帯域幅およびリクエスト数を評価します。 帯域幅を購入する際、利用可能な帯域幅に余裕を持たせるようにします。攻撃を受けたときに、通常の帯域使用量を超えても正規ユーザーに影響しないようにします。

- サーバーのセキュリティを強化し、接続パフォーマンスといったサーバーのパフォーマンスを改善

  サーバーのセキュリティを強化し、攻撃対象を減らし、攻撃者の攻撃コストが高くつくようにします。

  - サーバー上のシステムファイルが最新のものであることを確認し、システムパッチは速やかに適用します。
  - すべてのサーバーのホストを確認して訪問者の出所を特定します。
  - 不要なサービスおよびポートをフィルタリングします。 たとえば、Web サーバーはポート 80 のみを有効にし、それ以外のポートはすべて無効にします。あるいは、ファイアウォールにブロックポリシーを設定します。
  - SYN 準結合の同時接続数を制限、また、SYN 準結合のタイムアウトを短縮することにより、SYN/ICMPトラフィックを制限します。
  - ネットワークデバイスおよびサーバーのログを注意深く確認します。 サーバーに脆弱性や時間に変更があれば、攻撃を受けている可能性は残ります。
  - ファイアウォールの外側のネットワークファイルとのファイル共有を制限します。 ハッカーによってシステムファイルが攻撃される機会を減らします。 ハッカーによってシステムファイルがトロイの木馬に置き換えられると、ファイル転送機能は必ず麻痺します。
  - ネットワークリソースを保護するためネットワークデバイスを最大限に活用します。 ルーターを設定する際は、トラフィック制御、パケットフィルタリング、準結合タイムアウト、ガベージパケット廃棄、送信元からの偽の送信元データパケット廃棄、SYN しきい値、ICMP および UDPブロードキャストの無効化といった設定を戦略的に行います。
  - 新たな TCP 接続、疑わしい悪意のある IP の接続および伝送速度を iptable といったソフトウェアファイアウォールで制限します。

- サービスモニタリングおよび緊急対応を実施
  - Anti-DDoS Basic のモニタリングの重視

    サービスが DDoS 攻撃を受けた場合、Anti-DDoS Basic より SMS またはメールでアラートが送信されます。 サービスが大量のトラフィック攻撃を受けた場合には、電話による警告通知も利用できます。 アラートを受信したらただちに緊急対応処理を実行することを推奨します。

    警告メッセージの送信先および音声によるアラートの設定方法については、「Anti-DDoS Basic メッセージの宛先設定」をご参照ください。
  - CloudMonitor

    CloudMonitor を使用して、Alibaba Cloud リソースのモニタリングメトリックまたはカスタム化モニタリングメトリックの収集と取得できます。また、サービスの可用性もテストできます。さらに、各メトリックにアラームを設定することもできます。

    詳細については、「CloudMonitor ユーザーガイド」をご参照ください。
- 適切な商用セキュリティソリューションを選択します。 Alibaba Cloud は、無料の Anti-DDoS Basic、および Anti-DDoS Pro IP や Game Shield といった商用セキュリティソリューションを提供しています。 他社のセキュリティソリューションを採用することもできます。
  - WAF (Web Application Firewall)

    WAF は、Web アプリケーションのトランスポート層、セッション層、およびアプリケーション層に対する攻撃の保護に効果的です。

    詳細については、「WAF ユーザーガイド 」をご参照ください。
  - Game Shield

    Game Shield は、ゲーム業界における一般的な DDoS 攻撃および HTTP フラッド攻撃に対して提案されたゲーム業界向けのソリューションです。 Game Shield は、Anti-DDoS Pro IP よりも適切性、防御効果に優れ、低コストです。

注意事項

DDoS 攻撃は、よく知られている業界全体の天敵です。 攻撃対象のサービスだけでなく、攻撃対象のネットワーク全体の安定性にも影響を及ぼします。また、同ネットワークの他のユーザーのサービスにも損害を与えます。

コンピュータネットワークは共有している環境です。 各当事者がそれぞれに安定性を維持していく必要があります。 操作によっては、ネットワーク全体および他のテナントのネットワークに影響を与える可能性があります。 したがって、以下にご注意ください。

- Alibaba Cloud プロダクトのメカニズムを使用した DDoS 保護プラットフォームを確立しないこと
- ブラックホールステータスにあるインスタンスをリリースしないこと
- ブラックホールステータスにあるサーバーには SLB IP、Elastic IP、NAT Gateway といった IP プロダクトを繰り返し置き換え、バインド解除、および追加をしないこと
- IP アドレスプールの使用や、攻撃トラフィックを多くの IP アドレスに割り振ることによって防御しないこと
- 攻撃に対して脆弱な、ネットワークセキュリティ防御に非対応の Alibaba Cloud プロダクト (CDN および OSS など) を表に出さないこと
- 複数のアカウントを使い回さないこと

3.Alibaba Cloud のブラックホールポリシー

本トピックでは、Alibaba Cloud Security のブラックホールポリシーについて説明します。

ブラックホールについて

サーバーへの攻撃トラフィックが、サーバーに設定されたブラックホールしきい値を超えると、そのサーバーはブラックホールステータスとなり、外部ネットワークからのサーバーへのアクセスはブロックされます。 ブラックホールに入れられたサーバーは、ブラックホールの持続時間中はアクセス不可能になります。 攻撃トラフィックが止んだとシステムが判断すれば、自動的にブラックホールステータスは解除されます。

ブラックホールは、Alibaba Cloud が事業者から購入しているサービスです。事業者は、ブラックホールを解除する時間および頻度に厳しい制限を設けています。 ブラックホールステータスを Alibaba Cloud 側で解除することはできません。 したがって、サーバーへのアクセス禁止がシステムにより自動的に解除されるのを待つ必要があります。

攻撃を無期限に拒否せずに、ブラックホールポリシーを設けている理由

DDoS 攻撃により、攻撃対象だけでなく、クラウドネットワーク全体も深刻な被害を受けます。 また、DDoS 防御のコストは多額で、中でも帯域幅は最もコストがかかります。

Alibaba Cloud は ISP から帯域幅を購入しています。 Alibaba Cloud の ISP より請求される帯域幅料金は、DDoS 攻撃トラフィックが除外されていません。使用帯域幅がそのまま請求されます。

Alibaba Cloud Security は、限られたコストの中で DDoS 攻撃から Alibaba Cloud ユーザーを無料で潜在的に防御を施しますが、攻撃トラフィックがしきい値を超える場合は、攻撃対象の IP アドレスへのトラフィックを Alibaba Cloud はブロックします。

ブラックホールのしきい値と持続時間を表示する方法

ECS、SLB、または EIP インスタンスの現在の DDoS 軽減帯域幅を確認するには、「Anti-DDoS Basic ブラックホールしきい値」をご参照ください。

ブラックホールイベントが発生してから、IP へのアクセス可能になるまでの時間については、「ブラックホール持続時間を表示」をご参照ください。

ブラックホールしきい値の最適化

無料のセキュリティ信用力プランに参加すると、セキュリティ信用スコアに応じて DDoS 軽減帯域幅が増量されます。

セキュリティ信用スコアのスコア基準を理解し、スコア改善に率先して取り組むには、「セキュリティ信用力の詳細を確認」をご参照ください。 信用スコアを上げることで、DDoS 軽減帯域幅は増量されます。

ブラックホールしきい値を設けるだけでは十分でない場合

Anti-DDoS Proサービスを購入することで、サーバーへの DDoS 攻撃を防御し、サーバーの正常な処理を保護することができます。 Anti-DDoS Pro サービスは、DDoS 攻撃からユーザーを防御するように設計されており、保護および防御をお約束します。

セキュリティ信用力プランと Anti-DDoS Pro との違い

セキュリティ信用力プランによって、信用履歴の優れているユーザーが初めて攻撃を受けた場合、保護機能は強化されます。 ブラックホールのしきい値は信用スコアに応じて調整され、保証される保護機能は固定化されていません。

Anti-DDoS Pro サービスは、DDoS 攻撃からユーザーを防御するように設計されており、保護および防御をお約束します。

各リージョンのブラックホールトリガーしきい値

各リージョンの、Anti-DDoS Basic の基本的な保護機能のブラックホールトリガーしきい値は、デフォルトでは下表のとおりです (単位: bps)。

> 説明　トリガーしきい値は、ECS、Server Load Balancer、VPC といった Alibaba Cloud のプロダクトに適用されます。

リージョン	1 コア CPU のクラシックネットワーク ECS	2 コア CPU のクラシックネットワーク ECS	4 コア CPU 以上のクラシックネットワーク ECS	Server Load Balancer と VPC
中国 (杭州)	500 M	1 G	5 G	5 G
中国 (上海)	500 M	1 G	2 G	2 G
中国 (青島)	500 M	1 G	5 G	5 G
中国 (北京)	500 M	1 G	2 G	2 G
中国 (張家口)	500 M	1 G	2 G	2 G
中国 (フフホト)	500 M	1 G	2 G	2 G
中国 (深セン)	500 M	1 G	2 G	2 G
中国 (香港)	500 M	500 M	500 M	500 M
米国 (シリコンバレー)	500 M	1 G	2 G	2 G
米国 (バージニア)	500 M	500 M	500 M	500 M
日本 (東京)	500 M	500 M	500 M	500 M
シンガポール	500 M	500 M	500 M	500 M
オーストラリア (シドニー)	500 M	500 M	500 M	500 M
マレーシア (クアラルンプール)	500 M	500 M	500 M	500 M
インド (ムンバイ)	500 M	1 G	1 G	1 G
ドイツ (フランクフルト)	500 M	500 M	500 M	500 M

リージョン	1 コア CPU のクラシックネットワーク ECS	2 コア CPU のクラシックネットワーク ECS	4 コア CPU 以上のクラシックネットワーク ECS	Server Load Balancer と VPC
UAE (ドバイ)	500 M	500 M	500 M	500 M

ブラックホール持続時間

デフォルトのブラックホール持続時間は 2.5 時間です。サーバーへのアクセス禁止を解除することはできません。 実際のブラックホールの持続時間は攻撃の程度に応じて 30 分から 24 時間の範囲内で変動します。 ブラックホールの持続時間に影響を与える主な要因は、以下のとおりです。

- 攻撃が続いているかどうか。 攻撃が続く場合には、ブラックホールの持続時間は延長されます。 ブラックホールの持続時間は、延長された時間を基に再計算されます。
- 頻繁に攻撃を受けているかどうか。 初めて攻撃を受けた場合、ブラックホールの持続時間は自動的に短縮されます。 逆に、頻繁に攻撃を受けている場合には、再び攻撃される可能性が高いため、ブラックホールの持続時間は自動的に延長されます。

> **説明** あまりにも頻繁にブラックホールに入る場合、Alibaba Cloud はブラックホールの持続時間を延長し、また、ブラックホールのしきい値を下げることができるものとします。 ブラックホールのしきい値と持続時間は、コンソールで確認することができます。

4.ブラックホールポリシー

5.トラフィッククリーニングとブラックホール

ECS インスタンスを作成すると、Anti-DDoS Basic がデフォルトで有効化されます。 Anti-DDoS Basic のサービスには、トラフィックのクリーニングとブラックホールが含まれます。

トラフィッククリーニング

トラフィッククリーニングサービスは、検知センター、クリーニングセンター、および集中管理センターの 3 つのユニットで構成されています。 検出センターは、ECS インスタンスへの受信データをモニタリングし、DDoS 攻撃といった異常なトラフィックをタイムリーに検出します。 異常が検出されると、管理センターはトラフィック迂回ポリシーに基づいて不審なトラフィックをクリーニングするようクリーニングセンターに指示します。 正当なトラフィックは元のインスタンスに戻されますが、悪意のあるトラフィックは削除されます。 これにより、正当なトラフィックだけがターゲットのシステムに転送されるようになります。

ブラックホール

攻撃トラフィックがデフォルトのトラフィックしきい値を超えると、ブラックホールトリガーサービスは自動的にブラックホールをトリガーします。 しきい値は、リージョンや CPU 構成によって異なります。 各リージョンのデフォルト設定については、「Anti-DDoS Basic ブラックホールしきい値」をご参照ください。

ブラックホールにより、攻撃の状況に応じてトラフィックが一定時間 (デフォルトでは 2.5 時間) 制限されます。

その間、トラフィッククリーニングサービスは有効です。 攻撃が続くと、ブラックホールステータスの持続時間は延長されます。 また、ブラックホールステータスは手動で無効にすることはできません。 サーバーがシステムによって自動的に解除されるまでお待ちください。

サービスの復旧に緊急を要する場合は、Alibaba Cloud Anti-DDoS Proをご利用ください。

Anti-DDoS Pro は、付加価値の高い有料サービスで、大規模な DDoS 攻撃を受けてサービスを利用できなくなった後に適用します。 攻撃トラフィックを Anti-DDoS Pro の IP アドレスにリダイレクトすることにより、ソースインスタンスの安定性と信頼性が保証されます。