1 概要

Cloud Anti-DDoS は、アプリケーションとインフラストラクチャを DDoS 攻撃から保護するクラウドベースのセキュリティサービスです。これにより、トラフィックを可視化し、DDoS攻撃のステータスが確認できます。このサービスは、すべての Alibaba Cloud ユーザーが無料で使用できます。

2 プロダクト詳細

Anti-DDoS は、不正なトラフィックがインフラストラクチャに侵入しないようにパケットのクリーニング及びルーティングすることで DDoS 攻撃を防御できるクラウドベースのセキュリティサービスです。また、この機能は標準でインスタンスに備わっており、アプリケーションの可用性を強化することができます。

2-1 クリーニング機能

クリーニング機能は、ある一定の閾値（ユーザにて任意に設定可能）を超過した場合に実行されます。モニタリングシステムは自動でネットワーク攻撃を検出し、サーバーで異常なトラフィックをクリーニングします。クリーニングプロセスの間、モニタリングシステムは、サーバーへのデータ転送をリアルタイムでモニターし、DDoS や他の攻撃を引き起こしかねない異常なトラフィックを適切なタイミングで検出します。正常なサービスに影響を及ぼさずに異常なトラフィックをクリーニングするために、モニタリングシステムは疑わしいトラフィックを元のネットワークパスからクリーニングプロダクトに転送し、悪意のあるトラフィックを識別、削除した後、復元された適正なトラフィックを元のネットワークパスへと差し戻します。

2-2 ブラックホール機能

ブラックホール機能は、攻撃トラフィックが下記の閾値を超過した場合に実行されます。ブラックホールがトリガーされた後、対応するサーバーによるインターネットアクセスは一定時間（2.5時間）にわたって制限されます。その後、サーバーはクリーニング状態になり、攻撃の有無を確認します。攻撃が存在する場合は、ブラックホール処理が継続されます。その場合のブラックホール状態は、攻撃の停止後に自動的に解除されます。手動による解除はサポートしていません。

各リージョンでのブラックホール閾値は、以下の通りです。

Region	1-Core ECS	2-Core ECS	4-Core or above ECS	SLB and VPC
日本	500M	500M	500M	500M
中国東部 1	500M	1G	5G	5G
中国北部 1	500M	1G	5G	5G
中国南部 1	500M	1G	2G	2G
中国北部 2	500M	1G	2G	2G
中国東部 2	500M	1G	2G	2G
香港	500M	500M	500M	500M
アメリカ西部	500M	1G	2G	2G
アメリカ東部	500M	500M	500M	500M
シンガポール	500M	500M	500M	500M

2-3 Anti-DDoS防御対象

本サービスによって防ぐことのできる攻撃は以下のとおりです。

項目	対応の説明
不正なパケット	IP Fragments, Smurf, Stream Flood, Land Flood
不正な形式のパケット	不正な形式のIP、UDP、TCP、ICMP Packets
レイヤー4攻撃	SYN Flood, ACK Flood, UDP Flood, ICMP Flood, RST Flood

ご利用上の注意事項

この資料は、Alibaba Cloudの提供するクラウドサービスの機能について説明したもので、サービスのご利用を検討する際の参考となる技術的情報を提供するものです。
今後、本資料はクラウドサービスの機能追加・変更等に合わせて、予告なく変更される場合があります。閲覧された情報は最新のものではない場合がありますので、予めご了承下さい。

改版履歴

日付	版数	変更内容
2017/1/23	1.0	初版作成

SB Cloud