Alibaba Cloud
Anti-DDoS Pro

Anti-DDos Basic サービス

Document Version20190603

目次

1 プロダクト紹介..... 1
1.1 Anti-DDoS Basic の概要.....1
1.2 Anti-DDoS Basic の仕組み.....2
1.3 特徴.....3
1.4 利点.....4
1.5 シナリオ.....4
2 クイックスタート.....5
2.1 Anti-DDoS Basic を使用開始.....5
3 ユーザーガイド.....10
3.1 クリーニングトリガー値の設定..... 10
3.2 トラフィッククリーニングをキャンセル..... 12
3.3 ブラックホール持続時間の確認..... 14
3.4 セキュリティ信用力の詳細を確認..... 15
3.5 DDoS 保護通知を設定.....16
3.6 DDoS イベントの詳細を表示.....17
3.7 IP アドレスがブラックホールに入っているサーバーに接続..... 18
3.8 Anti-DDoS Basic ブラックホールしきい値.....18
3.9 Web ホスティング用 Anti-DDoS Basic ブラックホールしきい値.....21
3.10 クラウドサービスの仕様とクリーニングのトリガー値.....22
3.11 Anti-DDoS Basic の誤検知をホワイトリストで回避.....22
4 FAQ..... 24
4.1 Alibaba Cloud Security のグローバルホワイトリストへの IP アドレス登録申請..... 24
4.2 Anti-DDoS Basic に関する FAQ..... 25

1 プロダクト紹介

1.1 Anti-DDoS Basic の概要

Anti-DDoS Basic は、データおよびアプリケーションを保護する無料の DDoS (分散型 DoS 攻撃) 保護サービスです。

Anti-DDoS Basic はお客様のインフラストラクチャからのトラフィックをルート変更することで DDoS 攻撃を防御および軽減します。 本サービスによって、Alibaba Cloud 上のリソースの可用性とパフォーマンスが保証されます。 また、セキュリティの可視性および制御も強化されます。 Alibaba Cloud Security のグローバルサービスである Anti-DDoS Basic は一般的な DDoS 攻撃に対して 5 Gbps の DDoS 軽減帯域幅が用意されています。

詳細については、「*Anti-DDoS Basic のプロダクト詳細*」をご参照ください。

- セキュリティ信用力プラン

  デフォルトの DDoS 軽減帯域幅に加え、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。
- 広範な保護シナリオ

  Anti-DDoS Basic は、ICMP フラッド、UDP フラッド、TCP フラッド、SYN フラッド、および ACK フラッドといったさまざまな DDoS 攻撃を防御します。
- スケーラブルな DDoS 軽減帯域幅

  信用スコアを上げることで、DDoS 軽減帯域幅を増やすことができます。
- ブラックホール持続時間の短縮

  セキュリティ信用力があれば、深刻な攻撃により開始されるブラックホールの時間は、デフォルト設定されている時間よりも短縮されます。より迅速にサービスを復旧させることができます。
- 管理可能なセキュリティ信用力

  セキュリティ信用スコアのスコア基準を理解することで、率先してスコアの改善に取り組むことができます。

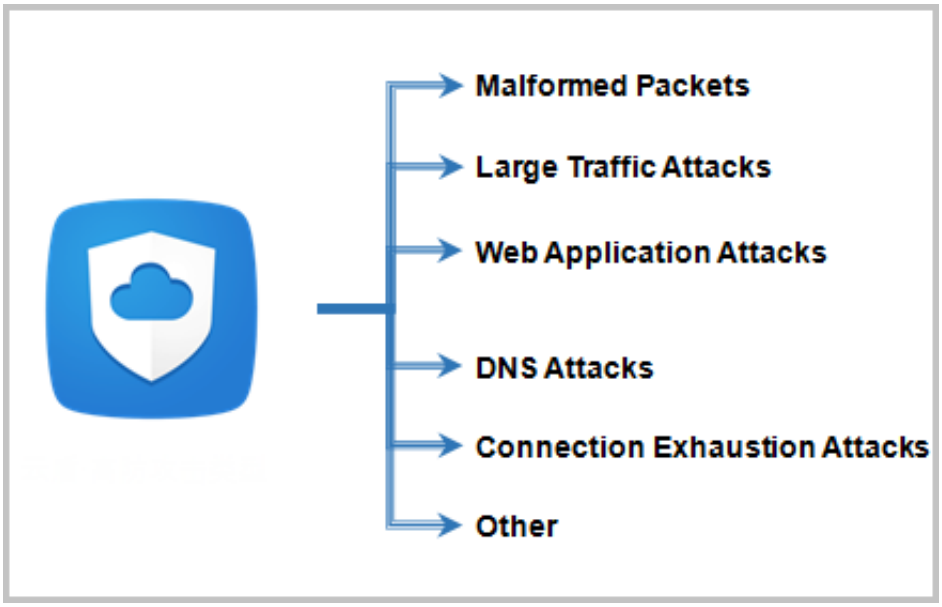
1.2 Anti-DDoS Basic の仕組み

現時点において、Anti-DDoS Basic は、BGP および DNS リダイレクトに対応しています。Anti-DDoS Basic は、主にクリーニングによって保護しますが、アクティブに、制限を設けることによっても保護します。 本サービスは、包括的に DDoS 攻撃に対処します。

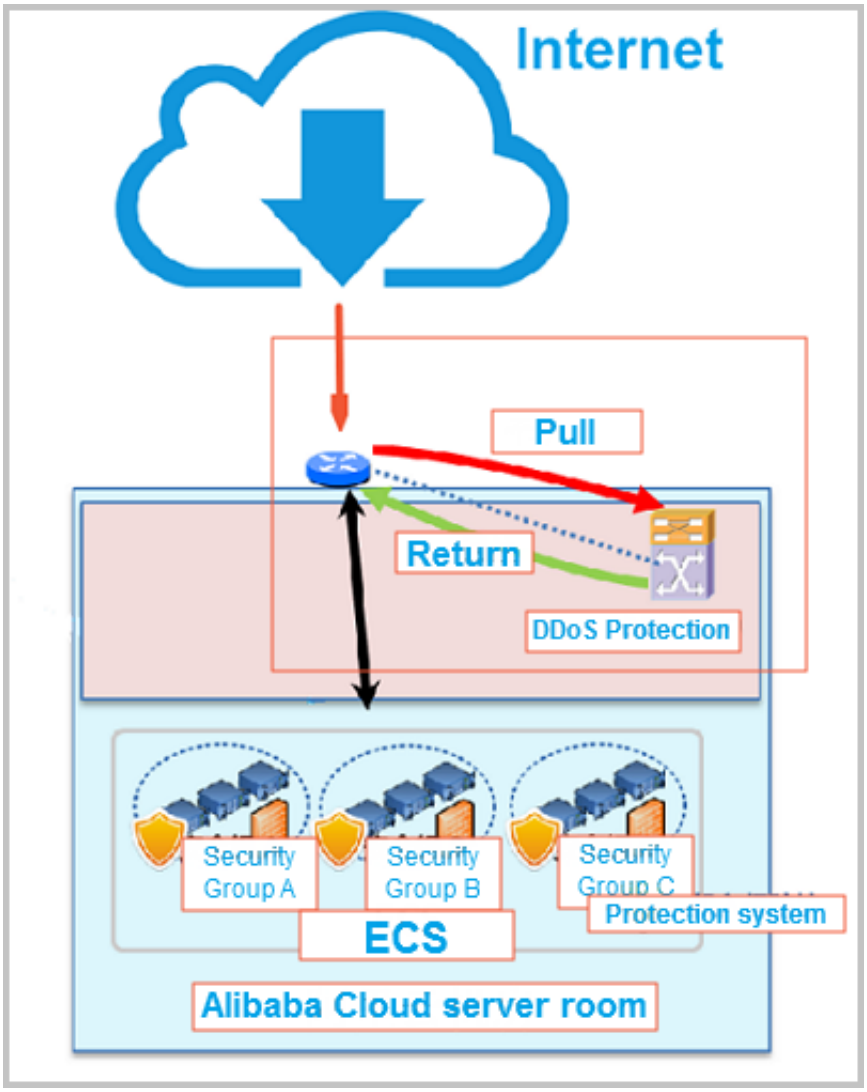
プロキシー、検出、リバウンド、権限付与、ブラックリスト/ホワイトリスト、メッセージコンプライアンスといった従来のテクノロジーに基づき、Anti-DDoS Basic には、Web セキュリティとフィルタリング、評判分析、レイヤー 7 アプリケーション分析、ユーザー行動パターン分析、機械学習、防御および対抗策といったテクノロジが実装されています。 本サービスは、脅威をブロックおよびフィルタリングし、攻撃の標的となってもユーザーが保護されることを保証します。

Alibaba Cloud によって構築された現 Anti-DDoS システムは、TB レベルの攻撃を防御することができます。 一方で、Alibaba Cloud は各リージョンでの保護ノードの拡充も進めています。

Alibaba Cloud 独自開発の Alibaba Cloud Security に基づいて、SYN フラッド攻撃、UDP フラッド攻撃、ACK フラッド攻撃、ICMP フラッド攻撃、DNS クエリフラッド攻撃、NTP Reply フラッド攻撃、HTTP フラッド攻撃といったレイヤー 3 からレイヤー 7 に対する攻撃を防御する Anti-DDoS サービスを提供します。 Anti-DDoS Basic サービスによって保護される攻撃は、下図のとおりです。



Anti-DDoS Basic は、Alibaba Cloud データセンターのインターネットへの出口に DDoS 攻撃検出およびクリーニング機能を配置します。主にバイパスデプロイメントアーキテクチャを採用しています。 Anti-DDoS Basic サービスのネットワークトポロジは下図のとおりです。



1.3 特徴

Alibaba Cloud Security の Anti-DDoS Basic サービスには、以下の機能があります。

タイプ	機能	説明
攻撃に対する保護	不正なメッセージのフィルタリング	Frag フラッド攻撃、Smurf 攻撃、Stream フラッド攻撃、および Land フラッド攻撃をフィルタリングします。
攻撃に対する保護	不正なメッセージのフィルタリング	不正な IP パケット、TCP パケット、および UDP パケットをフィルタリングします。
攻撃に対する保護	トランスポート層への DDoS 攻撃に対する保護	SYN フラッド、ACK フラッド、UDP フラッド、ICMP フラッド、および RSTFLOOD 攻撃をフィルタリングします。

タイプ	機能	説明
管理	攻撃のエビデンス収集	異常なトラフィックパケットを自動取得します。
管理	攻撃イベント管理	攻撃イベントおよび攻撃トラフィックの統計を用いた管理を行うことができます。

1.4 利点

Alibaba Cloud Security Anti-DDoS Basic サービスには、以下の利点があります。

高信頼性ネットワーク回線保護

- DDoS 攻撃下でも安定したアクセス速度
- 他のユーザーからの影響を受けない十分な帯域幅を保証
- 高品質な帯域幅により、サービスの可用性および安定性を保証

高精度な保護

- 攻撃を正確に識別し、迅速に保護
- 独自の研究開発アルゴリズムに基づくクリーニングシステムにより、低い誤検知率を保証
- 互いに干渉することのないシングルポイントクリーニングとマルチポイントクリーニング

メンテナンスフリー

- クリーニングに高価な設備を購入が不要
- 自動的に起動 (デフォルトで有効)
- インテリジェントなサービス学習および動的な保護ルール設定

無料

- Anti-DDoS Basic は無料のサービスです。
- Alibaba Cloud におけるお客様のセキュリティ信用力に応じて、さらに多くの保護帯域幅を無料で提供します。

1.5 シナリオ

Alibaba Cloud Anti-DDoS Basic は、インターネット DDoS 攻撃からの保護に適用します。

適用範囲: Alibaba Cloud 上の ECS、SLB、EIP、NAT、および WAF サービスを無料で DDoS 攻撃から保護

制限: 5 GB 以下の DDoS 攻撃に対応

2 クイックスタート

2.1 Anti-DDoS Basic を使用開始

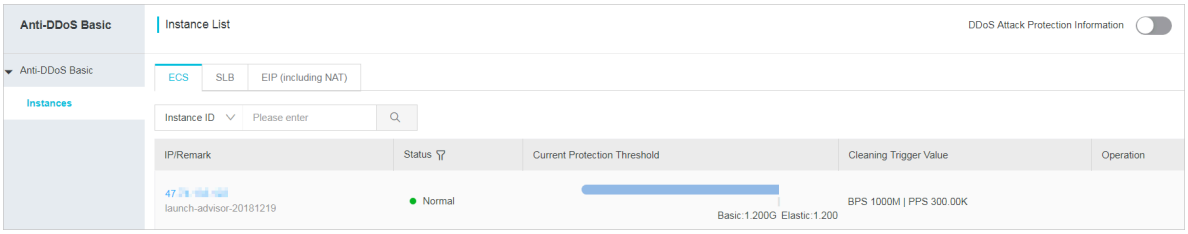
Anti-DDoS Basic は、ECS、Server Load Balance、または EIP のインスタンスを作成すると、デフォルトで有効化および初期化されます。 本サービスは、無料で 5 Gbps の軽減帯域幅を提供します。

Alibaba Cloud Security Anti-DDoS Basic コンソールより実行できる操作は、以下のとおりです。

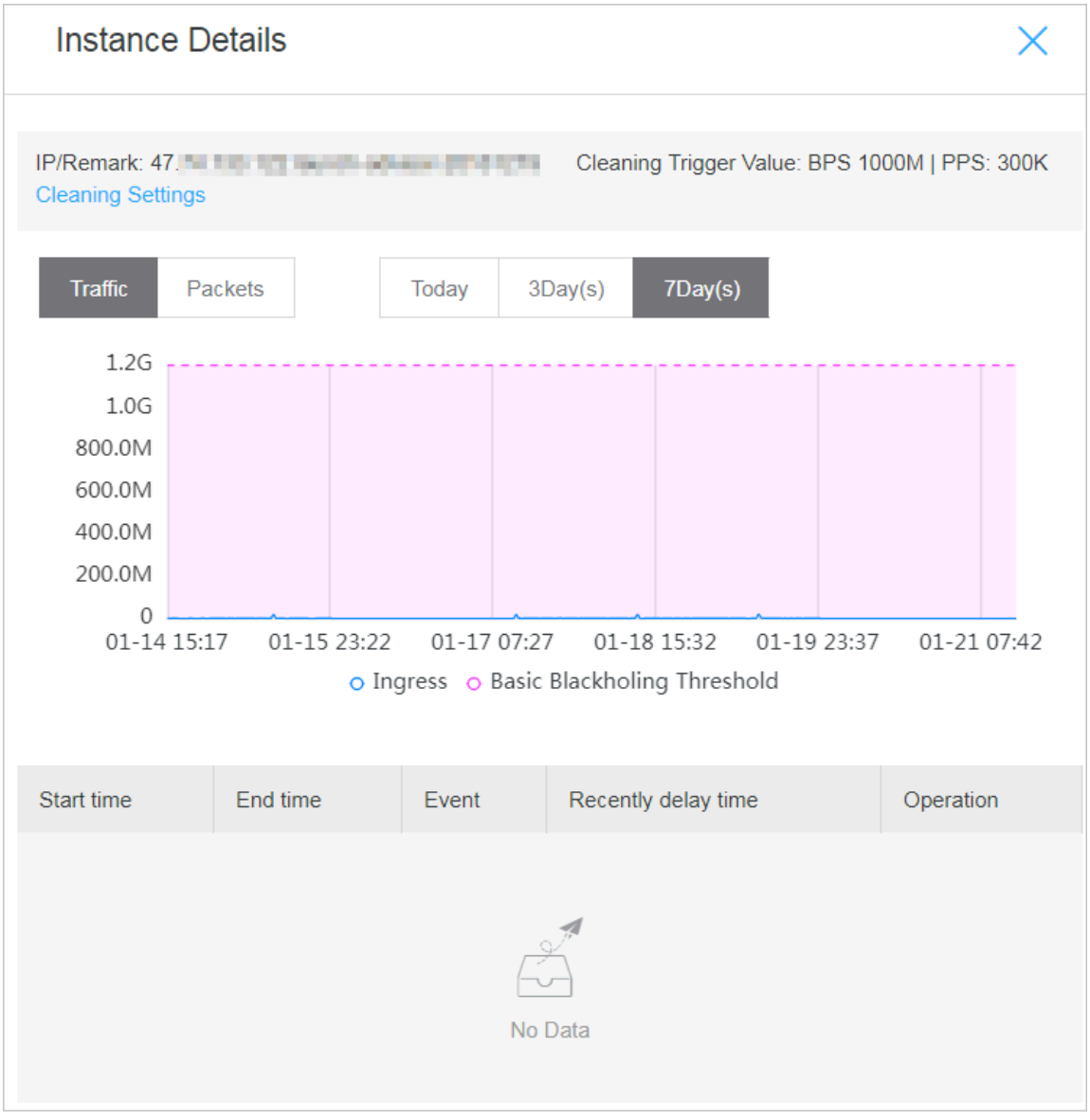
- クリーニングトリガー値を設定します。 IP が DDoS 攻撃を受け、攻撃トラフィックがクリーニングしきい値を超えると、トラフィッククリーニングが自動的に開始されるため、サービス可用性が保証されます。
- 保護しきい値を確認します。 保護しきい値には、基本保護しきい値および拡張保護しきい値があります。
  - 攻撃トラフィックが、基本保護しきい値よりも少ない場合、攻撃トラフィックのクリーニングは無料になります。 デフォルト基本保護しきい値は IPアドレスのリージョンごとに異なります。
  - 攻撃トラフィックが、基本保護しきい値以上かつ拡張保護しきい値以下の場合、Alibaba Cloud の無料で提供する利用可能な保護帯域幅が使用されます。 拡張保護のしきい値は、IP アドレス、トラフィック使用量、およびセキュリティ信用力に応じて決定されます。 無料の保護帯域幅を使い切ると、保護しきい値は基本保護しきい値にまで下げられます。 「詳細」をご参照ください。

1. *Anti-DDoS Basic コンソール*にログインします。
2. リージョンを選択します。
3. Anti-DDoS Basic > インスタンスページのECS、SLB、または EIP (含む NAT)のいずれかのタブを選択します。

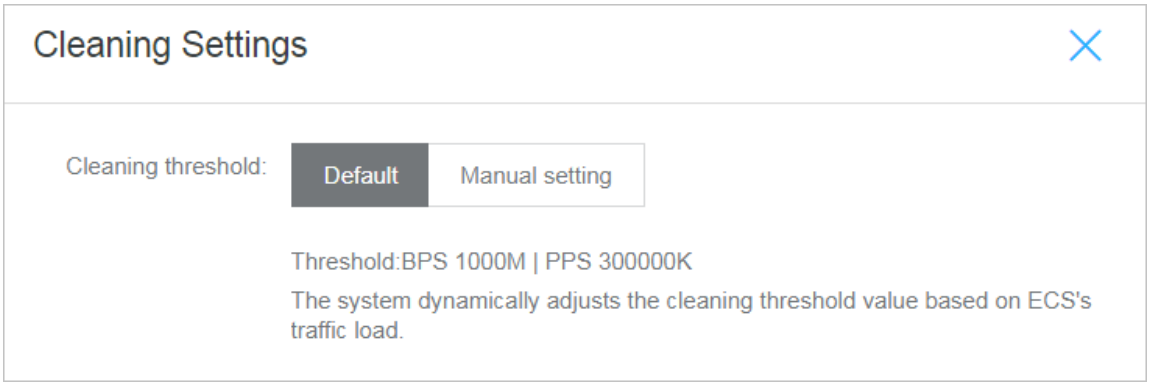
4. インスタンス一覧よりインスタンスを選択します。



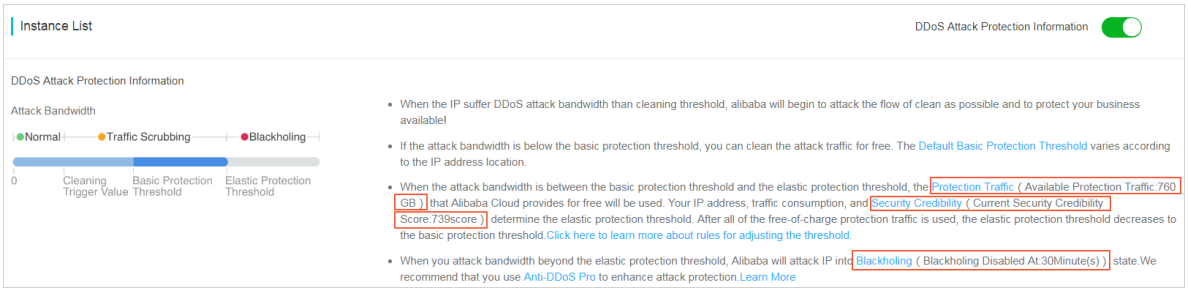
・ インスタンス IP をクリックすると、過去 7 日間のトラフィックおよびパケットの傾向、また、DDoS 攻撃イベントが表示されます。



・ インスタンスの詳細ダイアログボックスのクリーニング設定をクリックします。 手動でクリーニングしきい値を設定するか、システムのデフォルトのクリーニングしきい値を使用するかを選択します。



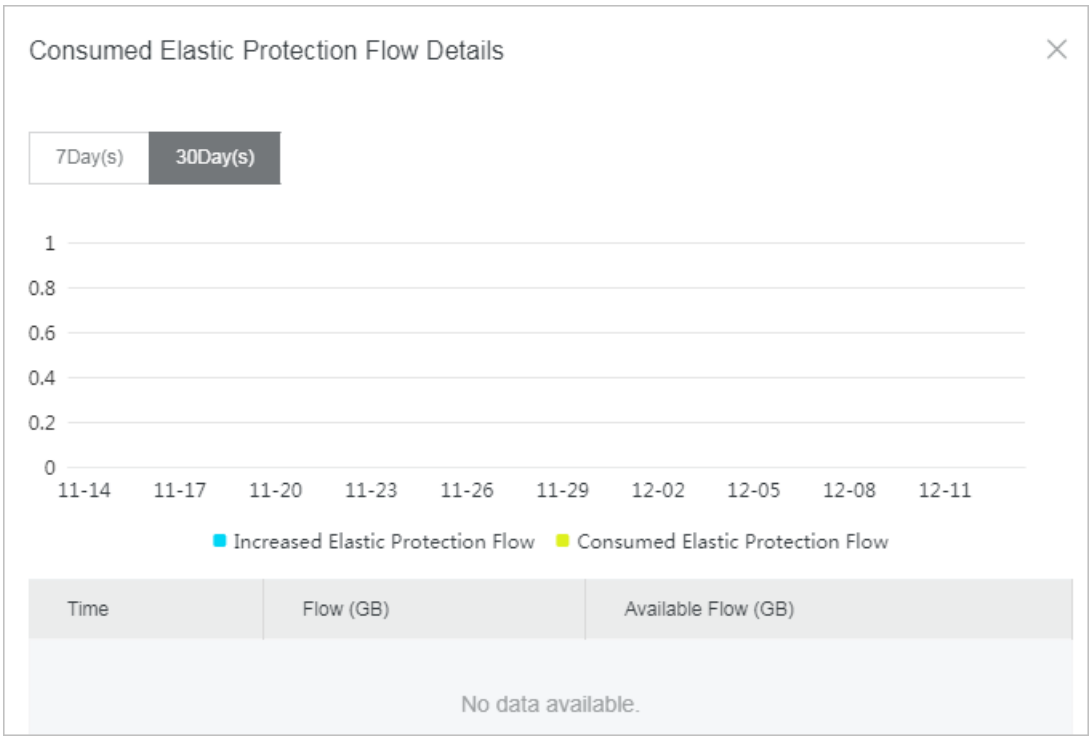
5. DDoS 攻撃保護情報を表示します。 下図の情報を表示するには、右上隅のDDoS 攻撃保護情報をオンにします。



・ 利用可能な保護帯域幅を表示

注：

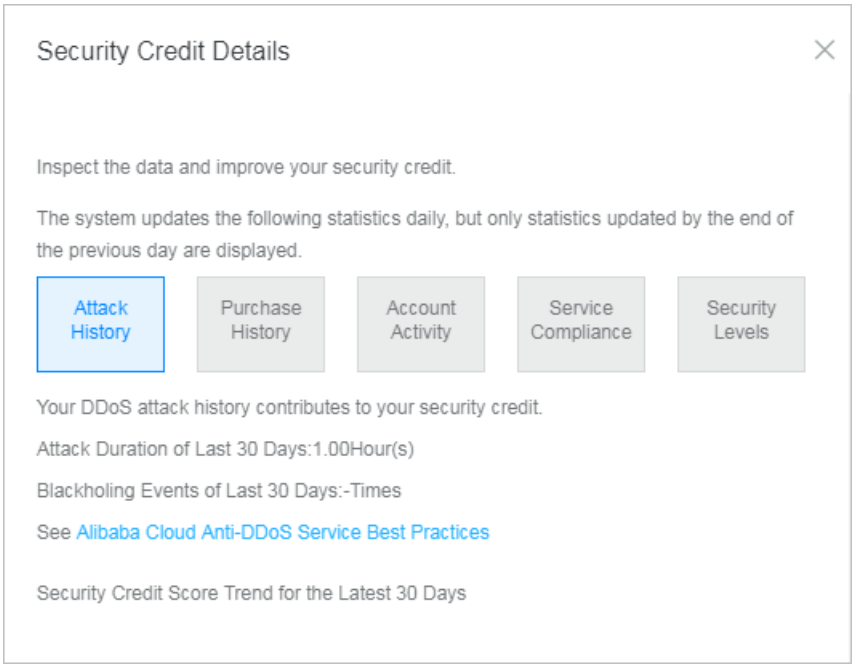
過去 30 日間の使用拡張保護帯域幅の詳細を表示するには、保護帯域幅をクリックします。



- セキュリティ信用スコアを表示

注：

セキュリティ信用スコアの詳細を確認するには、セキュリティ信用力をクリックします。



信用スコアが高いほど、より多くの DDoS 軽減帯域幅が割り当てられます。 信用スコアのポリシーを理解し、より高い信用スコアを維持するよう推奨します。

- ブラックホールの持続時間の設定を表示

> 注：
> ブラックホールをクリックすると、Alibaba Cloud のブラックホール戦略に関する詳細情報が表示されます。

3 ユーザーガイド

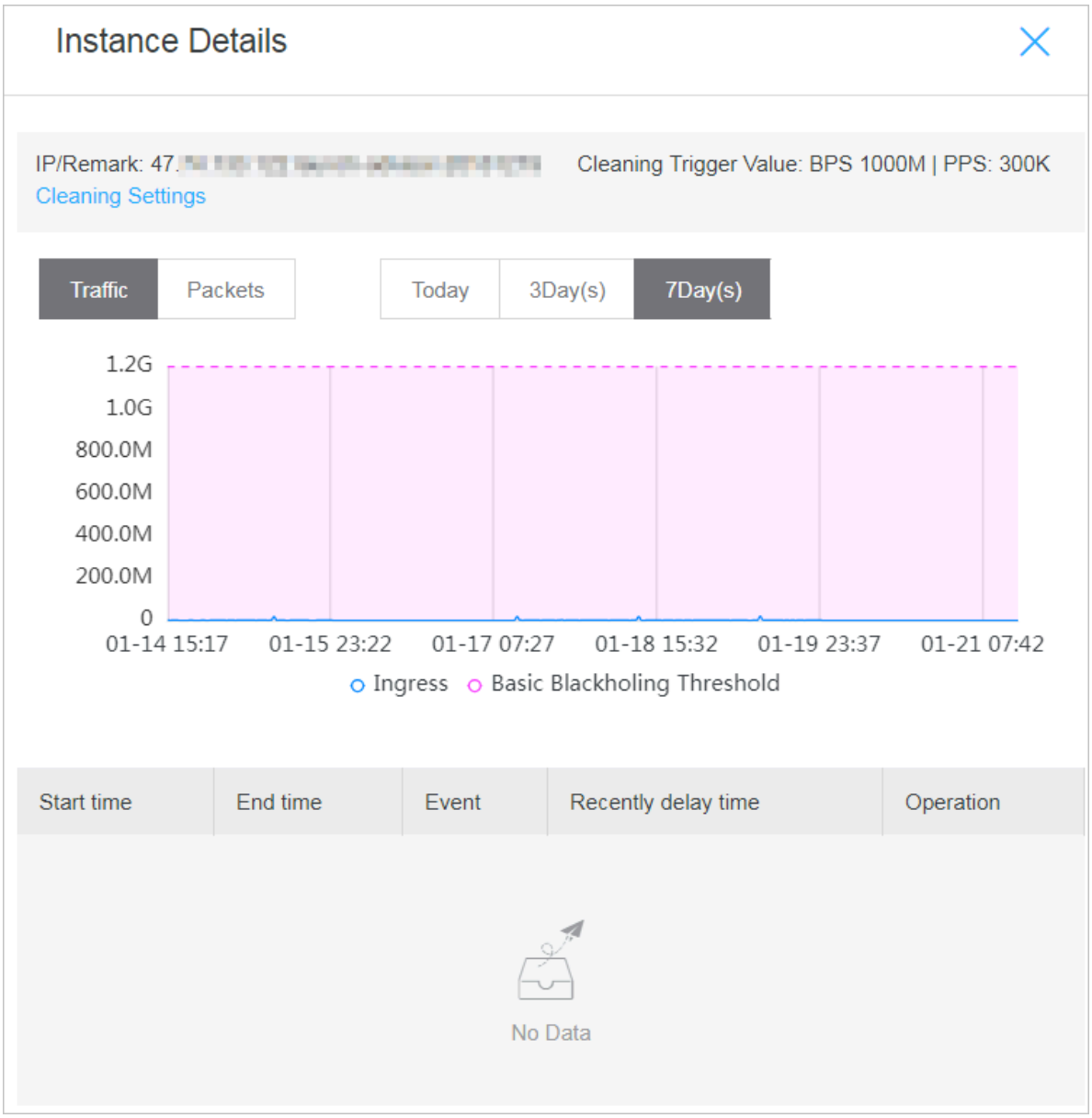
3.1 クリーニングトリガー値の設定

Alibaba Cloud Security の Anti-DDoS Basic は、DDoS 攻撃の内、SYN フラッド攻撃、UDP フラッド攻撃、ACK フラッド攻撃、ICMP フラッド攻撃、および DNS フラッド攻撃を軽減します。 Anti-DDoS Basic でクリーニングトリガー値を設定するには、以下の手順を実行します。

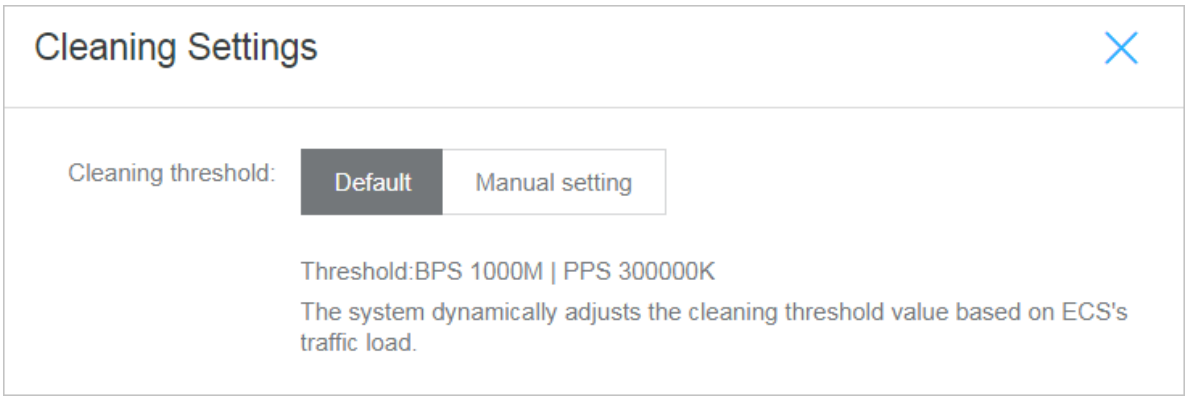
1. *Anti-DDoS Basic コンソール*にログインします。
2. リージョンを選択します。
3. Anti-DDoS Basic > インスタンス ページで、ECS、SLB、または EIP (含む NAT) のいずれかのタブを選択します。
4. 対象のインスタンスを特定します。

   注 :
   ターゲットインスタンスは、インスタンス ID、インスタンス名、または インスタンス IP で検索できます。

5. インスタンスの IP アドレスをクリックします。表示されるインスタンスの詳細ダイアログボックスより、クリーニングの設定をクリックします。



6. クリーニングの設定ダイアログボックスでクリーニングしきい値モードとしてデフォルト または 手動設定 を選択します。



- デフォルト: Anti-DDoS Basic サービスは、トラフィック負荷状況に応じて動的にクリーニングしきい値を調整します。
- 手動設定: 帯域幅およびパケットのしきい値を指定します。 トラフィックがしきい値を超えると、Anti-DDoS Basic のトラフィッククリーニングがトリガーされます。 (Web サイトに広告がある場合は、適宜クリーニングしきい値を調整されることを推奨します)。

> 注 :
> クリーニングしきい値は実際のアクセストラフィック量より高めに設定します。 しきい値が高すぎても、DDoS 攻撃の防御に役立つわけではありません。しきい値が低すぎる場合には、予期しないトラフィッククリーニングで正常なアクセスが影響を受ける可能性があります。
>
> IP アドレスに対するトラフィックがクリーニングしきい値に達した場合、Anti-DDoS Basic コンソールにクリーニング情報が表示されます。 正常なアクセスリクエストが影響を受けた場合は、トラフィックのクリーニングをキャンセルしてクリーニングしきい値を適切に調整します。

3.2 トラフィッククリーニングをキャンセル

Alibaba Cloud のサーバーには、デフォルトで無料の DDoS 軽減帯域幅が用意されています。 トラフィック攻撃の標的になると、トラフィッククリーニングサービスが自動的に有効になります。 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。

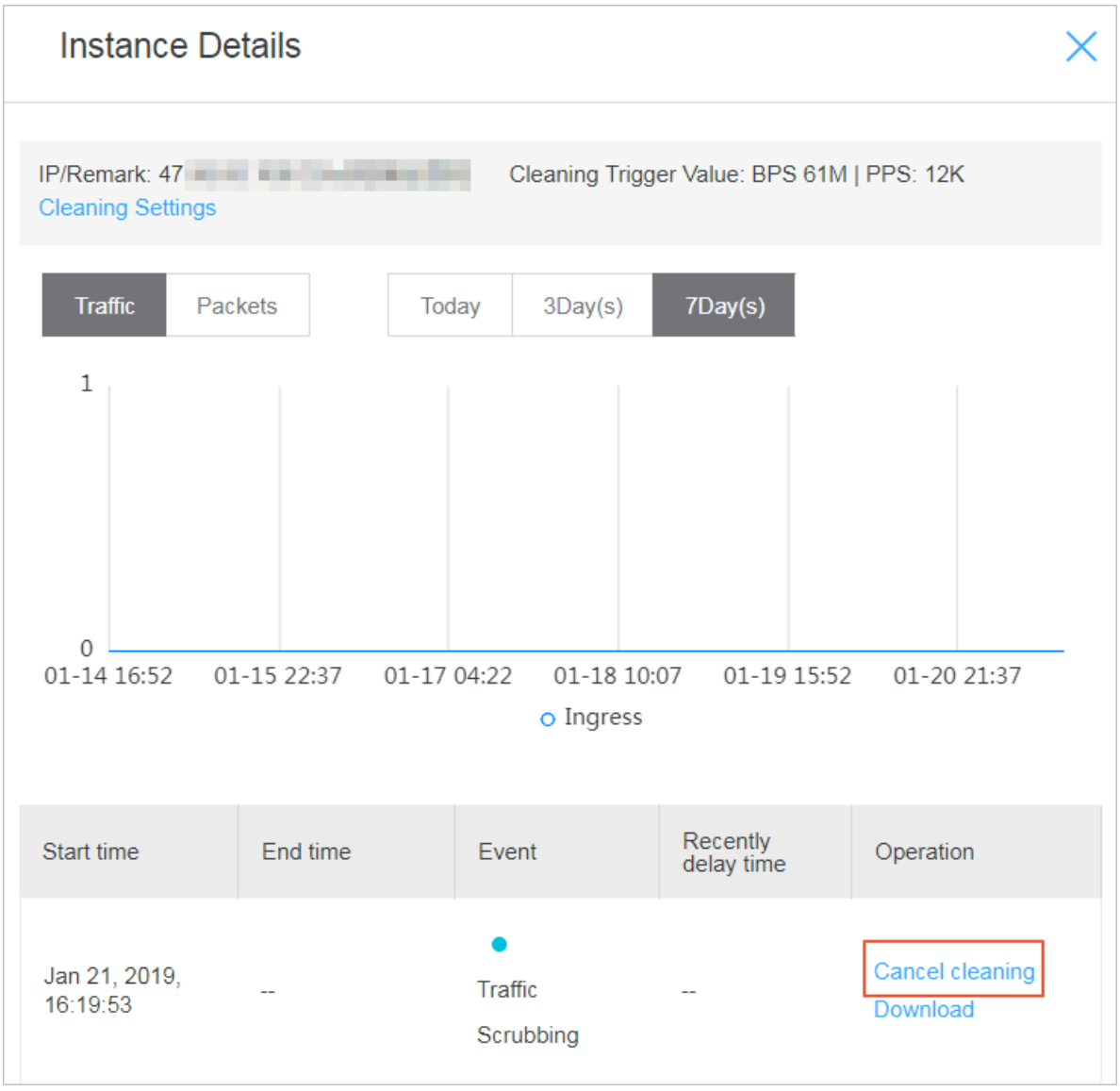
検知センターは、クラウドサーバーの受信トラフィックデータをモニタリングし、DDoS 攻撃といった異常なトラフィックをタイムリーに検出します。 異常が検出されると、管理センターは、トラフィック迂回ポリシーに基づいて、クリーニングセンターに不審なトラフィックをクリーニ

ングするよう指示します。 悪質なトラフィックは除去され、正当なトラフィックは元のインスタンスに返されます。 正当なトラフィックのみがターゲットシステムに転送されるようになります。

インスタンス IP が異常ステータスであれば、トラフィッククリーニングを手動でキャンセルします。

> 注：
> 各アカウントは 1 日に 3 回まで手動でトラフィッククリーニングを無効にできます。

1. *Anti-DDoS Basic コンソール*にログインします。
2. リージョンを選択します。
3. インスタンスタイプのタブを選択します。クリーニングステータスのインスタンス IP をクリックして、インスタンス詳細ダイアログボックスを表示します。



4. DDoS イベントリストより クリーニング ステータスであるイベントのクリーニングのキャンセル をクリックします。

> 注：
> ネットワーク監督部門に報告する際のエビデンスとして、採取したトラフィックデータファイルをダウンロードするには、ダウンロードをクリックします。

3.3 ブラックホール持続時間の確認

サーバーが大規模な DDoS 攻撃を受け、ブラックホール機能がトリガーされると、サーバーのセキュリティ信用力に基づいて、サーバーのパブリック IP アドレスは一定期間無効になります。

デフォルトのブラックホール持続時間は 2.5 時間で、この間、IP の無効化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。 ブラックホールステータスの持続時間に影響を与える主な要因は次のとおりです。

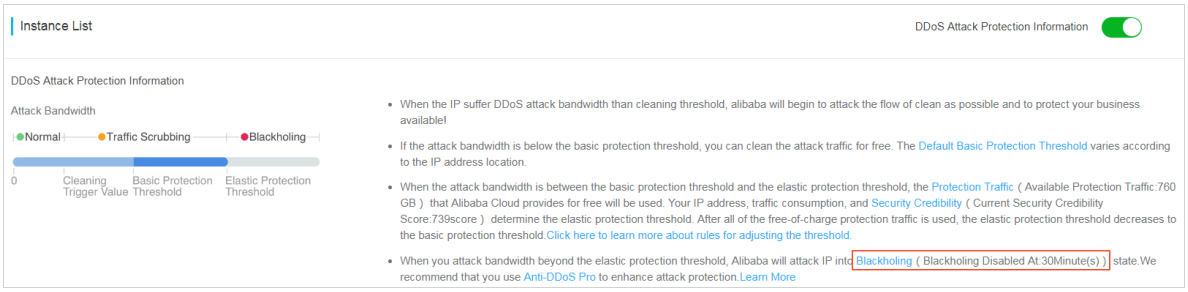
- 攻撃が続いているかどうか。 攻撃が続く場合には、ブラックホールの持続時間は延長されます。 ブラックホールの持続時間は、延長された時間を基に再計算されます。
- 頻繁に攻撃を受けているかどうか。 初めて攻撃を受けた場合、ブラックホールの持続時間は自動的に短縮されます。 逆に、頻繁に攻撃を受けている場合には、再び攻撃される可能性が高いため、ブラックホールの持続時間は自動的に延長されます。

設定されているブラックホールしきい値と持続時間は、Anti-DDoS Basic コンソールにログインして表示します。

> 注：
> - あまりにも頻繁にブラックホールに入る場合、Alibaba Cloud 側で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。
> - ブラックホールはインターネットサービスプロバイダ (ISP) の提供するサービスです。各 ISP はブラックホールを解除する時間制限を設けています。 ブラックホール持続時間は一般に 30 分以上で、アカウントの特定のブラックホール持続時間は同アカウントのセキュリティ信用力に基づいて自動的に調整されます。

1. *Anti-DDoS Basic コンソール*にログインします。
2. Anti-DDoS Basic > インスタンスページの右上隅の DDoS 攻撃保護情報 をオンに切り替えます。

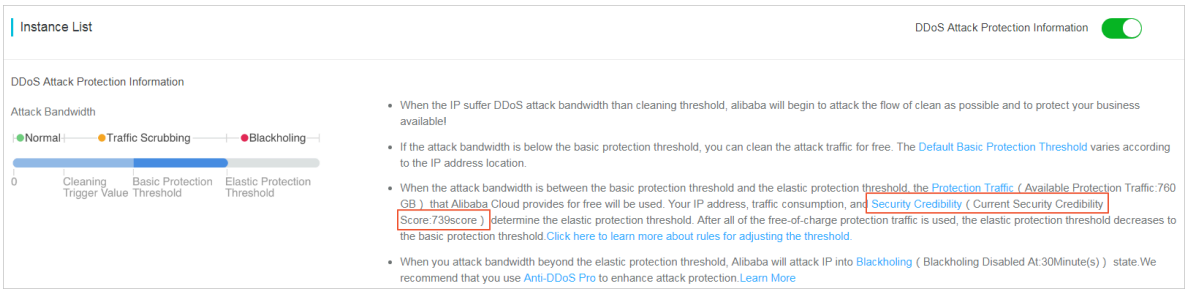
3. 現在のブラックホール持続時間が表示されます。



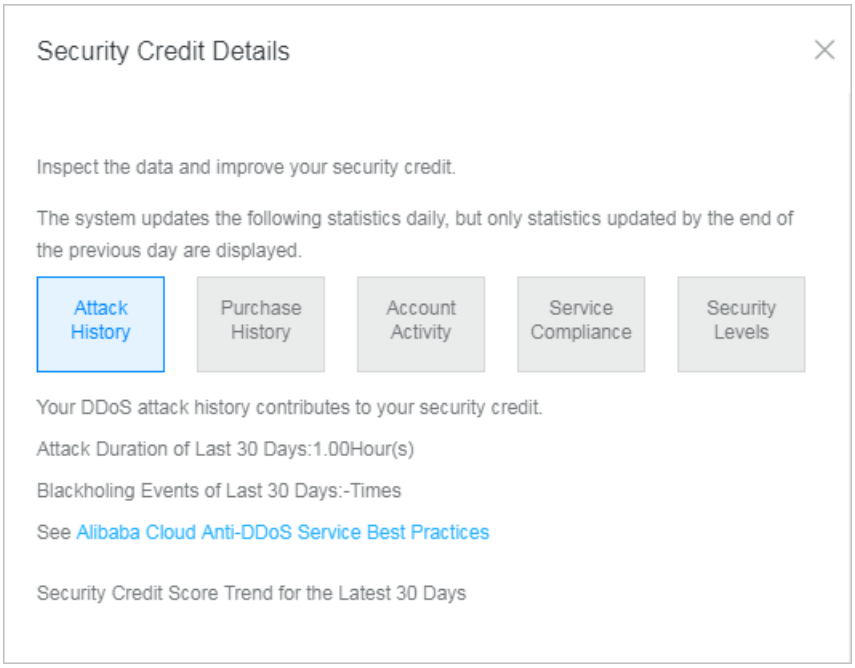
3.4 セキュリティ信用力の詳細を確認

Anti-DDoS Basic コンソールで現在のセキュリティ信用スコアと詳細を確認する方法は、以下のとおりです。

1. *Anti-DDoS Basic コンソール*にログインします。
2. Anti-DDoS Basic > インスタンスページの右上隅のDDoS 攻撃保護情報をオンにします。
3. 現在のセキュリティ信用スコアが表示されます。



4. セキュリティ信用スコアの詳細を確認するには、セキュリティ信用力をクリックします。



セキュリティ信頼性の基準に基づいてセキュリティ信用スコアを管理し、さらに多くの DDoS 保護帯域幅を無料で入手されることを推奨します。

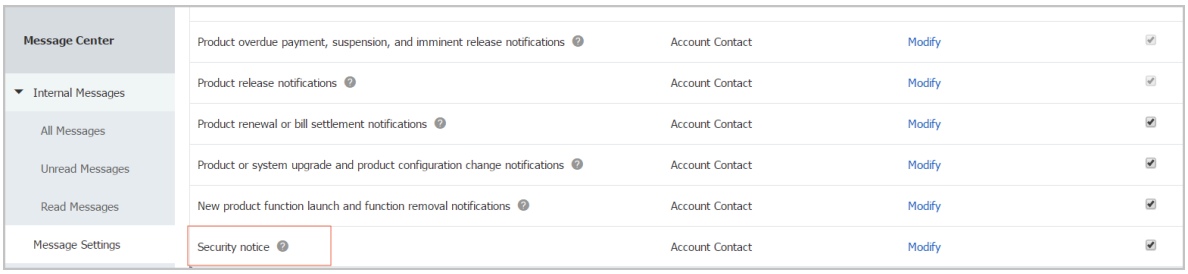
3.5 DDoS 保護通知を設定

Alibaba Cloud には、DDoS 保護通知機能があります。 アカウント下のサーバーが DDoS 攻撃を受けたり、トラフィッククリーニングやブラックホール機能がトリガーされたりした場合に、システムより通知が送信されるように指定することができます。

メッセージの宛先管理

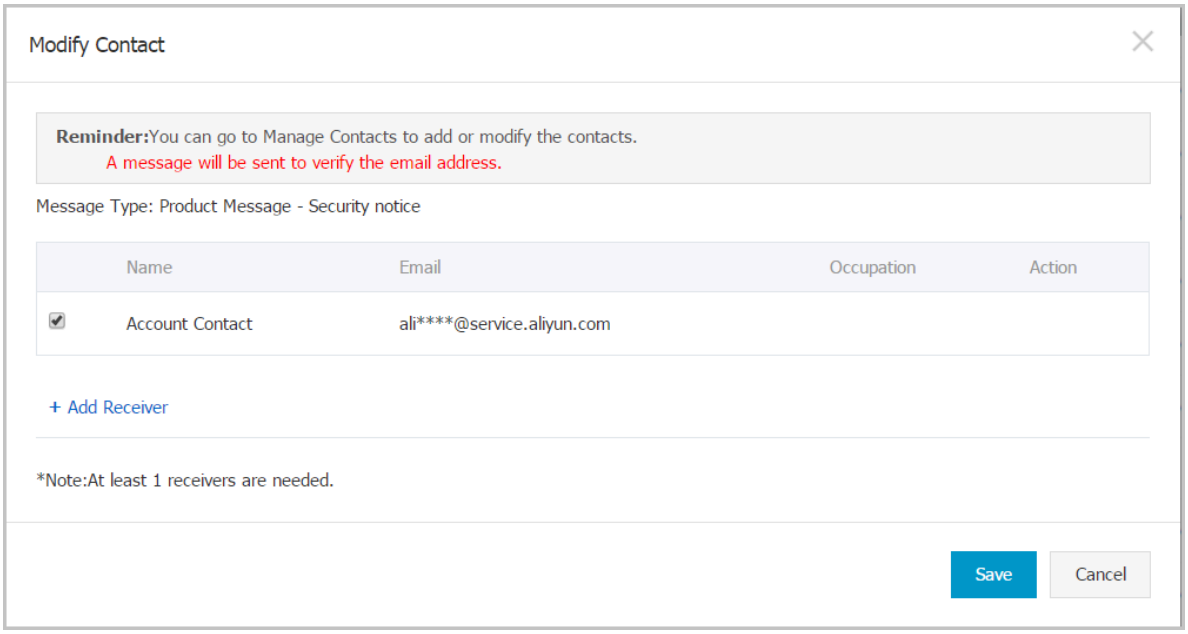
セキュリティ通知方法 (内部メッセージ、メール、または SMS) と宛先を設定するには、以下の手順を実行します。

1. *Message Center コンソール*にログインします。
2. メッセージ設定 をクリックし、セキュリティ通知を特定します。



3. 変更をクリックして、メッセージの宛先を選択します。

> 注：
> 新たにメッセージの宛先を追加するには、宛先を追加をクリックします。



3.6 DDoS イベントの詳細を表示

ECS または SLB インスタンスのパブリック IP が大規模な DDoS 攻撃を受け、攻撃トラフィックが対応するブラックホールしきい値を超えると、その IP アドレスはブラックホールとなり、サーバーは利用できなくなります。

> 注：
> インスタンスのブラックホールしきい値はリージョンごとに異なります。 詳細については、「*Alibaba Cloud のブラックホールポリシー*」をご参照ください。

サーバーが利用不可能になった場合には、Anti-DDoS Basic コンソールで DDoS イベントの詳細を表示し、 IP がブラックホールになった理由を確認することができます。

1. *Anti-DDoS Basic コンソール*にログインします。
2. リージョンを選択します。
3. Anti-DDoS Basic > インスタンスページのECS、SLB、または EIP (含む NAT)のいずれかのタブを選択します。

4. インスタンス一覧より、ステータスがブラックホール有効化となっている該当インスタンスを特定します。

   注：
   インスタンスは、インスタンス ID、インスタンス名、またはインスタンス IPを指定して検索します。

5. インスタンスの IP アドレスをクリックすると、インスタンスがブラックホールとなった時間およびその間のトラフィックが表示されます。

3.7 IP アドレスがブラックホールに入っているサーバーに接続

サーバーが大規模なトラフィック攻撃を受け、そのサーバーの IP アドレスがブラックホールに入った場合、そのサーバーへの外部トラフィックはすべて破棄されます。 ただし、サーバーと同じリージョンにある Alibaba Cloud サービスからはアクセスできます。

注：
ブラックホールに入っている間、外部からのサーバーへの接続要求はブロックされます。

IP アドレスがブラックホールに入った場合も、Alibaba Cloud ECS インスタンスからはサーバーに接続できます。

1. 正常にアクセスでき、かつ、サーバーと同じリージョンにある Alibaba Cloud ECS インスタンスに接続します。

   注：
   ECS インスタンスは、ブラックホールステータスのサーバーに接続できる必要があります。インスタンスとサーバーは同じ VPC 環境にあり、セキュリティグループのアクセス制御ルールによって接続がブロックされていない必要があります。

2. ツールの使用、またはコマンドラインより、ECS インスタンスよりブラックホールステータスのサーバーに接続します。

ECS インスタンスよりサーバーに正常にアクセスできるようになったら、サーバーから ECS インスタンスにファイルを転送し、ECS インスタンスサーバー上で設定ファイルを変更します。

3.8 Anti-DDoS Basic ブラックホールしきい値

データ転送速度がデフォルトのブラックホールしきい値 (単位: bps) を超える場合には、ブラックホールが有効化され、インスタンスへのネットワークアクセスがロックされます。 ブラック

ホールに入った攻撃対象のインスタンスをブロック解除することはできません。 各リージョンのデフォルトのしきい値については、下表をご参照ください。

注：

- デフォルトのしきい値は、ECS、SLB、および EIP に適用されます。
- ECS、SLB、またはEIPインスタンスの実際のブラックホールスレッシュホールド(しきい値)は、インスタンスのタイプとネットワーク帯域幅によって決まるためデフォルト値とは異なる場合があります。最終的なブラックホールスレッシュホールドはAlibaba Cloudコンソールに表示している値を確認して下さい。詳細については、「インスタンスのブラックホールしきい値の確認方法」をご参照ください。

リージョン	1 コア CPU ECS	2 コア CPU ECS	4 コア CPU 以上の ECS	SLB および EIP
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 (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 (バージニア)	500 M	1 G	2 G	2 G
米国 (シリコンバレー)	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 ECS	2 コア CPU ECS	4 コア CPU 以上の ECS	SLB および EIP
UAE (ドバイ)	500 M	500 M	500 M	500 M

ブラックホールの持続時間は、発生したブラックホールが持続する時間で、デフォルトでは 2.5 時間です。 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 時間の間で変動します。 次の要因をご考慮ください。

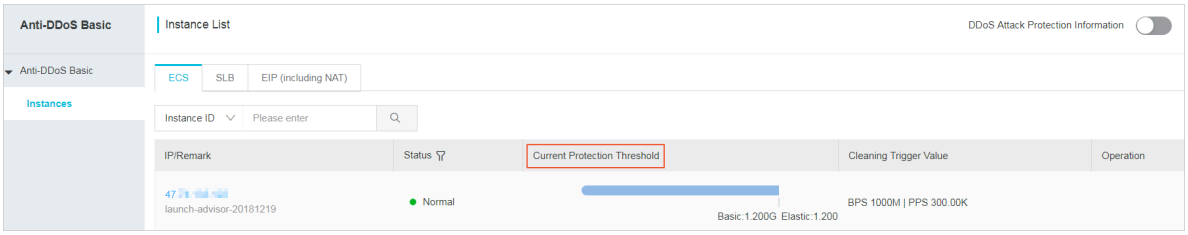
- 攻撃の継続。 攻撃が続く場合には、ブラックホールの持続時間は延長されます。
- 攻撃の頻度。 初めて攻撃を受ける ECS インスタンスの場合、ブラックホールの持続時間は自動的に短縮されますが、頻繁に攻撃を受けている場合には、ブラックホールの持続時間は自動的に延長されます。

> 注 :
> あまりにも頻繁にブラックホールに入る場合、Alibaba Cloud Security 側で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。 実際に適用される持続時間およびしきい値は、Alibaba Cloud Anti-DDoS Basic コンソールで確認します。

インスタンスのブラックホールしきい値の確認方法

ECS、SLB、または EIP インスタンスに実際に適用されるブラックホールしきい値を確認するには、以下の手順を実行します。

1. *Anti-DDoS Basic コンソール*にログインします。
2. リージョンを選択します。
3. Anti-DDoS Basic > インスタンスページより、ECS、SLB、または EIP (含む NAT) のいずれかのタブを選択します。
4. インスタンスの実際のブラックホールしきい値は、インスタンスの現在の保護しきい値欄で確認します。



3.9 Web ホスティング用 Anti-DDoS Basic ブラックホールしきい値

Web ホスティング用のブラックホールしきい値には、以下の値がデフォルト設定されています (単位: bps)。

 注 :

共有ホスティングの場合、1 つの IP アドレスを複数のホストで共有しているため、ブラックホールしきい値を決定することができません。 とはいえ、実際に適用されるしきい値は、デフォルトのしきい値より低い値でなければなりません。 共有ホスティングサーバーのブラックホールがトリガーされると、このサーバーおよび IP アドレスを共有しているすべてのサーバーにアクセスすることができなくなります。 セキュリティを重視する場合は、ECS インスタンスの購入を強く推奨します。

リージョン	ホスティングしきい値
中国 (杭州)	5 G
中国 (青島)	5 G
中国 (深セン)	2 G
中国 (北京)	2 G
中国 (上海)	2 G
中国 (香港)	500 M
米国 (シリコンバレー)	500 M
シンガポール	500 M

ブラックホールの持続時間は、ブラックホールがトリガーされてからの持続時間で、デフォルトでは 2.5 時間です。 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 時間の間で変動します。 さらに以下の要因が考慮されます。

- 攻撃の継続。 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。
- 攻撃頻度。 初めて攻撃を受ける ECS インスタンスの場合、ブラックホールの持続時間は自動的に短縮されますが、頻繁に攻撃を受けている場合には、ブラックホールの持続時間は自動的に延長されます。

 注 :

あまりにも頻繁にブラックホールに入る場合、Alibaba Cloud Security 側で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。 実

際に適用されている持続時間としきい値の情報は、Alibaba Cloud Anti-DDoS Basic コンソールで確認します。

DDoS 軽減帯域幅を増やして強化するには、「*Alibaba Cloud Anti-DDoS Pro*」をご参照ください。

3.10 クラウドサービスの仕様とクリーニングのトリガー値

Alibaba Cloud は、インターネットに公開されているクラウドプロダクトに対する DDoS 攻撃を軽減する、基本的な DDoS 保護機能を提供します。 クラウドプロダクトのパブリック IP アドレスの送受信するネットワークトラフィックが、指定のクリーニングしきい値を超えると、この IP に対するトラフィックを自動的にクリーニングし、正常にサービスを運用できるよう DDoS 攻撃から保護します。

トラフィッククリーニングの詳細については、「トラフィッククリーニング、ブラックホールとしきい値」をご参照ください。

各 Alibaba Cloud プロダクトの最大クリーニングしきい値は、インスタンスの仕様ごとに異なります。 ECS または SLB インスタンスを作成または変更すると、システムはそのインスタンス仕様に基づいて最大クリーニングしきい値を自動調整します。

注：
各インスタンス IP に実際に適用されるブラックホールしきい値は、最大クリーニングしきい値やセキュリティ信用スコアといった要素を基に計算されます。

- ECS インスタンスの最大クリーニングしきい値の計算方法については、「*ECS に基本的な DDoS 保護*」をご参照ください。
- SLB インスタンスの最大クリーニングしきい値の計算方法については、「*SLB に基本的な DDoS 保護*」をご参照ください。

3.11 Anti-DDoS Basic の誤検知をホワイトリストで回避

正常なトラフィック (Web サイトサービスへの正常なアクセスなど) が、Anti-DDoS Basic によってブロックされることがあります。

お客様が NAT ネットワーク環境を使用しているとします (LAN 内のホストが、インターネットアクセスにインターネット IP アドレスを共有)。この LAN 内のホストサーバーがウイルスに感染またはウィルスが侵入し、ECS サーバーが攻撃を受けるとします。 Alibaba Cloud Security にこの攻撃が検知されると、NAT の共有インターネット IP アドレスはブロックされ、アクセスできなくなります。

Alibaba Cloud のセキュリティコントロールプラットフォームにホワイトリストを設定すれば、この誤検知を回避できます。

1. セキュリティコントロール コンソールにログインします。

   注：
   コンソールの右上隅にあるアカウントアイコンの上にマウスを移動し、セキュリティコントロールをクリックすることでもセキュリティコンソールに移動することができます。

2. ホワイトリスト管理 > アクセスホワイトリストに移動し、追加をクリックします。
3. オブジェクトタイプを選択し、送信元 IP を入力します (ログイン中の Alibaba Cloud アカウントが使用している IP ではありません)。 次に、左側のリストより現在のアカウントのオブジェクト IP を選択します (たとえば、ECS インスタンスのパブリック IP を選択します)。右方向キーをクリックして選択済みの IP を右側のリストに追加し、OKをクリックします。 このように指定した送信元 IP が選択済みのオブジェクト IP のアクセスホワイトリストに追加されると、送信元 IP からオブジェクト IP へのすべてのアクセスがセキュリティコントロールプラットフォームによって制限されることはなくなります。

   注：
   オブジェクト IP へのアクセスをすべての IP に許可するには、送信元 IPに「0.0.0.0」と入力します。

   ホワイトリストを設定すると、アクセスホワイトリストに登録されている送信元 IP からターゲットホストリソースへのアクセスはすべて、たとえ危険性のあるアクセスであっても、Alibaba Cloud のセキュリティコントロールに制御されません。 したがって、アクセスホワイトリストへの登録は慎重に行う必要があります。

   注：
   アクセスホワイトリストに追加された送信元 IP は 10 分以内に反映されます。

4 FAQ

4.1 Alibaba Cloud Security のグローバルホワイトリストへの IP アドレス登録申請

Alibaba Cloud は、セキュアなクラウド環境を提供し、不審な操作をリアルタイムにモニタリングし、ブロックします。 サードパーティーの CDN ベンダーまたはセキュリティベンダーの製品を使用した、リクエスト転送またはセキュリティスキャンの実行は、Alibaba Cloud Security によって不審な行動とみなされます。 したがって、送信元 IP アドレスを含む転送リクエストや許可されていないセキュリティスキャンは、アクセスエラーとなります。

サードパーティーの CDN や セキュリティ製品が必要であることを鑑み、Alibaba Cloud では、サードパーティーのベンダーが自社製品の IP アドレスを Alibaba Cloud Security 基本保護グローバルホワイトリストに登録する許可申請を受け付けます。 手順は以下のとおりです。

> 注 :
> ECS インスタンスのみをホワイトリストに登録する場合は、「セキュリティコントロールのアクセスホワイトリスト設定」をご参照ください。

申請の際、申請者は以下の情報を記載した公式の文書を作成する必要があります。

- ホワイトリストに登録する IP アドレスのリスト。 登録する IP アドレスの数が多い場合には、IP アドレスリストのファイルをメールに添付していただくことができます。
- 登録する IP アドレスの用途
- 関連法令、および Alibaba Cloud の関連法令を遵守する旨の誓約書。 申請者は、Alibaba Cloud ユーザーに対していかなる攻撃行為も行わないものとします。 なお、ホワイトリストに登録した IP アドレスが、Alibaba Cloud のユーザーにセキュリティ上の脅威をもたらすとみなされる場合、または、不法行為・特許権の侵害に利用されている疑いがある場合、Alibaba Cloud は登録した IP アドレスをホワイトリストから除外できるものとします。 申請者は、このことにより生じる損害に対し、すべての責任を負うものとします。
- 連絡先 (電話番号を推奨)
- 申請者の社印

申請者は、ベンダーの会社を代表して、登記事項証明書の電子コピーと公式レターを次のアドレスに電子メールで送信してください。

- To: dachao.xdc@alibaba-inc.com

- Cc: yemin.ym@alibaba-inc.com

承認

Alibaba Cloud は申請を受領後、審査の上、2 営業日以内に最初の返信をお送りします (自動返信ではありません)。 Alibaba Cloud は、申請審査の際、申請資料に疑義があった場合には、その説明を申請者に請求できるものとします。 審査には数営業日かかる場合があります。 審査の完了後、Alibaba Cloud は審査結果を申請者に通知します。

申請者は、Alibaba Cloud が、Alibaba Cloud のポリシーに則した定期保守でホワイトリストに登録する IP アドレスを除外できることに同意するものとします。 また、申請者は、関連プロダクトの IP アドレスに修正・変更があった場合、その旨を Alibaba Cloud に通知する義務を負うものとします。 登録した IP アドレスが、Alibaba Cloud ユーザーにセキュリティ上の脅威をもたらすと Alibaba Cloud が判断した場合、Alibaba Cloud はその IP アドレスを永久に除外し、申請者に法的責任を負わせる権利を留保します。

4.2 Anti-DDoS Basic に関する FAQ

現時点において、Anti-DDoS Basic は、デフォルトですべての ECS インスタンスに有効です。ECS インスタンスの Web トラフィックが指定の DDoS しきい値を超えると、Anti-DDoS クリーニングデバイスはトラフィッククリーニングを開始します。

- *Anti-DDoS Basic* のポートホワイトリストはどのような役割を果たしますか。
- *Anti-DDoS Basic* で *SYN* フラッド攻撃から保護されますか。
- *Anti-DDoS* 保護結果の表示期間は選択できますか。
- *ECS* サーバーが *20 MB* の攻撃を受けましたが、*Anti-DDoS Basic* によって防御されなかったのはなぜですか 。
- *ECS* サーバーの *AliVulfix* プロセスは何ですか。
- なぜブラックホールをすぐにキャンセルできないのですか。

Anti-DDoS Basic のポートホワイトリストはどのような役割を果たしますか。

Anti-DDoS Basic により、サービスの使用しているポートが検出されます。 ポートをポートホワイトリストに登録して Anti-DDoS Basic サービスのアラーム対象外にすることができます (ポートを公開する権限が必要です)。

Anti-DDoS Basic で SYN フラッド攻撃から保護されますか。

はい。Anti-DDoS Basic により、SYN フラッド攻撃より保護されます。

Anti-DDoS 保護結果の表示期間は選択できますか。

はい、できます。 Anti-DDoS Basic コンソールでは、24 時間以内の DDoS 攻撃イベントを照会することができます。

ECS サーバーが 20 MB の攻撃を受けましたが、Anti-DDoS Basic によって防御されなかったのはなぜですか 。

Anti-DDoS Basic は、Alibaba Cloud Security の公益サービスです。 攻撃トラフィックが 100 MB に満たない場合はブロックされません。 攻撃のトラフィックが 100 MB 未満の場合は、サーバーのパフォーマンスの最適化、または、Cloudlock といったホストファイアウォールのインストールを推奨します。

ECS サーバーの AliVulfix プロセスは何ですか。

AliVulfix プロセスは、Alibaba Cloud Security で ECS の脆弱性を検出するプロセスです。

なぜブラックホールをすぐにキャンセルできないのですか。

通常、ブラックホールは 30 分から 24 時間続きます。 頻繁に攻撃を受けているユーザーの場合、Alibaba Cloud は、ペナルティーとしてブラックホールの頻度を増やすことがあります。

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から削除できる時間に明確な制限を設けています。 したがって、ブラックホールをすぐにキャンセルすることができません。