Alibaba Cloud
Web Application Firewall

クイックスタート

Document Version20190920

目次

1 概要

Alibaba Cloud WAF を有効化した後、Web サイト設定を作成し、DNS 設定を更新して Web サイトに WAF をデプロイする必要があります。 WAF が有効化されていると、WAF 保護ポリシーを設定して複雑な Web 攻撃を処理したり、デフォルト設定を使用して一般的な Web 攻撃や HTTP フラッド攻撃から保護できます。 Alibaba Cloud WAF は、Web 業務のセキュリティイベントとリスクを理解するのに役立つ総合的な保護の視覚化を提供します。

以下のタスクを実行することで Alibaba Cloud WAF の使用を開始します。

タスク	説明	推奨方法	前提条件
1. Web サイト設定の自動追加	Alibaba Cloud WAF コンソールで Web サイト設定を作成して、Web サイトを WAF インスタンスに関連付けます。	Web サイト設定を自動的に作成します。	・保護されるドメイン名は Alibaba Cloud DNS でホストされています。また、DNS 設定には少なくとも 1 つの有効な A レコードが含まれる必要があります。 ・(中国本土リージョンの場合) Web サイトは、産業情報技術省 (MIIT) によって ICP ライセンスが付与されています。 ・(HTTPS 対応 Web サイトの場合) Web サイトの有効な SSL 証明書と秘密鍵へのアクセス権があるか、または証明書が Alibaba Cloud SSL Certificate Service にアップロードされています。

タスク	説明	推奨方法	前提条件
(オプション) 2. DNS 設定の更新	DNS ホストでドメイン名の DNS 設定 (CNAME レコード) を変更して、Web トラフィックを検査するために Alibaba Cloud WAF にリダイレクトします。 注: 手順 1 で実施を促された場合は必須: Web サイト設定を自動的に追加するか、手動で Web サイト設定を追加します。	値として WAF CNAME アドレスを使用して、ドメイン名の CNAME レコードを有効にします。	・ WAF CNAME アドレスを入手しています。 ・ DNS ホストシステムでドメインの DNS 設定を更新する権限があります。
3. WAF 保護ポリシーの設定	さまざまな WAF 保護機能を有効または無効にし、Alibaba Cloud WAF コンソールでそれらの関連ルールを管理します。	デフォルトの保護設定を使用します。	Alibaba Cloud WAF は Web サイトに正常にデプロイされ、Web サイト設定の DNS 解決ステータスは正常です。
4. セキュリティレポートの表示	Alibaba Cloud WAF コンソールで Web サイトのセキュリティレポートを表示します。	・ 概要ページを使用して、業務用セキュリティサマリ統計を表示します。 ・ レポートページを使用して、詳細な攻撃保護記録とリスク警告を表示します。	Alibaba Cloud WAF は Web サイトに正常にデプロイされ、Web サイト設定の DNS 解決ステータスは正常です。

2 手順 1 : Web サイト設定の自動追加

Alibaba Cloud WAF を有効化したら、WAF コンソールで Web サイト設定を作成して、Web サイトを WAF インスタンスに関連付ける必要があります。 この手順では、Alibaba Cloud DNS の DNS 設定を使用して Web サイト設定を追加します。

Web サイト設定を作成する場合、WAF は Alibaba Cloud DNS の A レコード設定にアクセスし、すべての Web サイトドメインとそのオリジンサーバーの IP アドレスを一覧表示します。 WAF 保護を有効にするドメインのみを選択して、残りの項目を自動設定することもできます。このようにして、WAF で DNS 設定を更新 (手順 2) し、トラフィックのリダイレクトを完了することができます。

前提条件

- 保護されるドメインは Alibaba Cloud DNS でホストされています。 また、DNS 設定には少なくとも 1 つの有効な A レコードが含まれる必要があります。

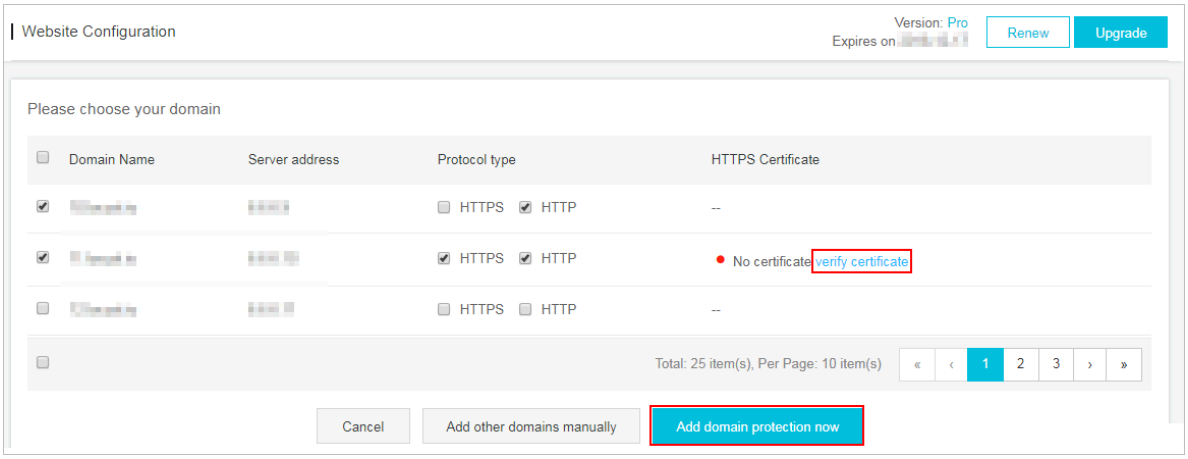
  Alibaba Cloud DNS を使用しない場合は、 Web サイトの設定を参照して Web サイト設定を手動で追加します。
- (中国本土リージョンの場合) Web サイトは、産業情報技術省 (MIIT) によって ICP ライセンスが付与されています。
- (HTTPS 対応 Web サイトの場合) Web サイトの有効な SSL 証明書と秘密鍵へのアクセス権があるか、証明書が Alibaba Cloud SSL Certificate Service にアップロードされています。

手順

1. Alibaba Cloud WAF コンソールにログインします。
2. ページ上部でリージョン [中国本土]、[国際] を選択します。
3. 管理 > Web サイト設定 ページで、[ドメインの追加] をクリックします。

   WAF は、現在の Alibaba Cloud アカウントのAlibaba Cloud DNS に A レコードが設定されているすべてのドメイン名を自動的に一覧表示します。 A レコードが Alibaba Cloud DNS に作成されていない場合は、[ドメインを選択してください] ページが表示されません。 この

場合は、Web サイト設定を手動で作成することを推奨します。 詳細は、「Web サイトの設定」をご参照ください。



4. [ドメインを選択してください] ページで、WAF 保護を有効にする ドメイン名 とプロトコルタイプを確認します。
5. (オプション) プロトコルタイプに HTTPS が含まれている場合は、最初に証明書を確認して設定を追加する必要があります。

注 :

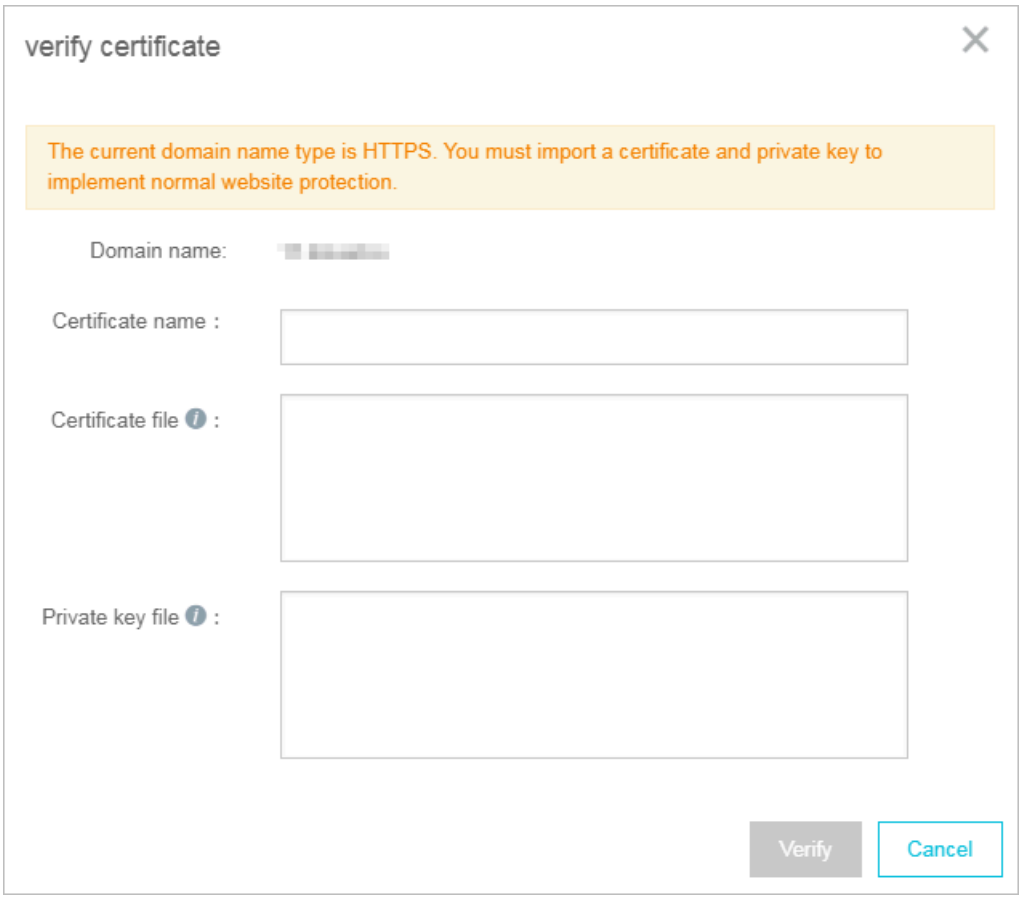
別の方法として、ここでは HTTPS を選択せず、Web サイト設定を編集し、設定を作成した後に証明書をアップロードします。 詳細は、「HTTPS 証明書の更新」をご参照ください。

a. [証明書の確認] をクリックします。

b. [証明書の確認] ダイアログボックスで、証明書と秘密鍵をアップロードします。

- 証明書が Alibaba Cloud SSL Certificate Service コンソールにホストされている場合、 [証明書の確認] ダイアログボックスの [既存の証明書を選択] をクリックし、それを選択してアップロードします。
- 手動アップロード。 [手動アップロード] をクリックし、 証明書の名前 を入力して、証明書と秘密鍵のテキスト内容をそれぞれ [証明書ファイル] と [秘密鍵ファイル] ボックスに張り付けます。

  詳細は、「HTTPS 証明書の更新」をご参照ください。



c. [確認] をクリックしてアップロードします。

6. [今すぐドメイン保護を追加] をクリックします。

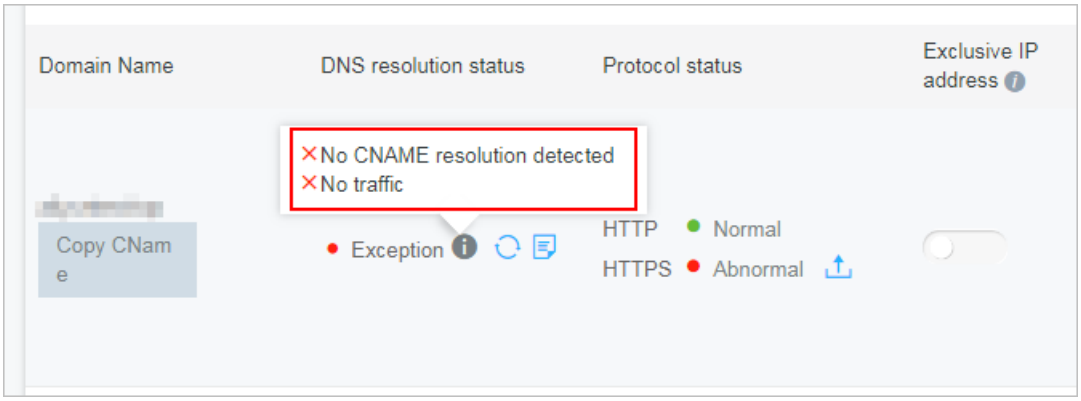
   Web サイト設定を追加した後、WAF はドメイン名の DNS 設定 (CNAME レコード) を自動的に更新して、検査用 WAF に Web リクエストをリダイレクトします。 全体のプロセスは約 10 ～15 分かかります。

   > 注 :
   > 手動で DNS 設定を変更するように求められた場合は、手順 2 : DNS 設定を更新してトラフィックを WAF にリダイレクトする必要があります。

7. 管理 > Web サイト設定 ページで、新しく追加したドメイン名とその DNS 解決ステータス を表示します。

   - " Normal " は、Alibaba Cloud WAF が Web サイトに正常にデプロイされたことを示します。 手順 3 : WAF 保護ポリシーの設定の実行に進みます。
   - " Exception " は、しばらく待つか、DNS サービス プロバイダーで DNS 設定を確認する必要があることを示します。

     DNS 設定が正しくない場合は、手順 2 : DNS 設定の更新を実行します。 詳細は、「 DNS 解決ステータスの例外」をご参照ください。



3 手順 2 : DNS 設定の更新

Web サイト設定が作成されると、Alibaba Cloud WAF は Web サイト専用の CNAME アドレスを生成します。 この手順では、値として WAF CNAME アドレスを使用して Web サイト用 CNAME レコードを有効にし、検査のために WAF に Web リクエストをリダイレクトします。

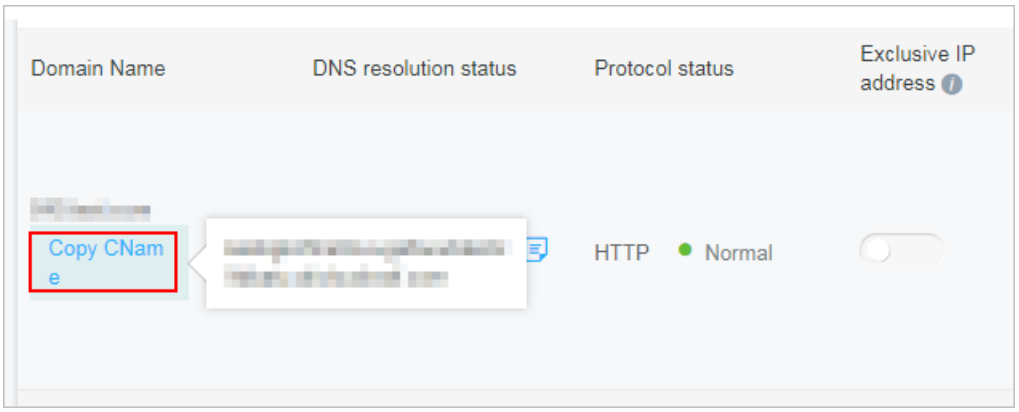
- 手順 1 : Web サイト設定の追加で DNS 設定が更新されており、DNS 解決ステータスが "Normal" の場合は、手順 3 : WAF 保護ポリシーの設定に進みます。
- 手順 1 : Web サイト設定の追加で DNS 設定を手動で更新するように求められた場合、または DNS 解決ステータスが "Exception" となっている場合は、この手順を実行します。

  次の手順では、例として Alibaba Cloud DNS を取り上げ、DNS 設定、特に CNAME レコードを更新する方法を説明します。 ドメインの DNS が Alibaba Cloud DNS でホストされている場合は、手順に従います。 それ以外の場合は、次の手順を参照して DNS ホストのシステムにログインして DNS 設定を更新します。

   注 :
  WAF CNAME アドレスを使用して DNS 設定を更新することを推奨します。 ただし、A レコードの使用もサポートしています。 A レコードを使用して DNS 設定を更新する必要がある (たとえば、CNAME レコードが MX レコードと競合する) 場合は、「WAF デプロイメントガイド」をご参照ください。

前提条件

- WAF CNAME アドレスを入手します。
  1. Alibaba Cloud WAF コンソールにログインします。
  2. ページ上部でリージョン [中国本土]、[国際] を選択します。
  3. 管理 > Web サイト設定 ページで、操作するドメイン名の上にポインタを移動します。[CName のコピー] ボタンが表示されます。



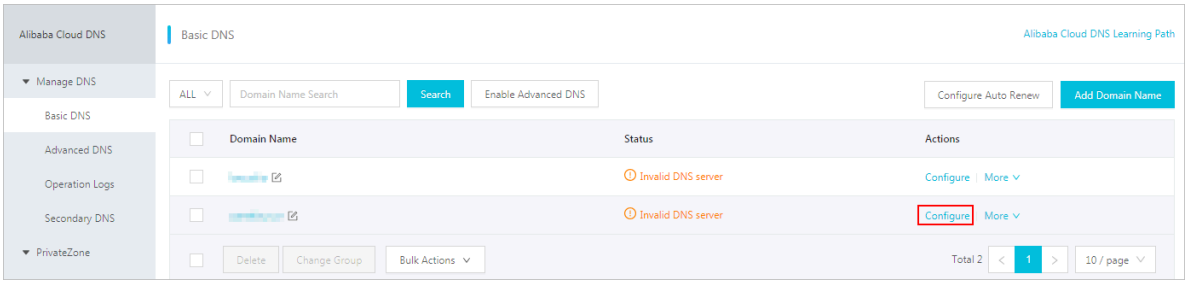
  4. [CName のコピー] をクリックして WAF CNAME アドレスをクリップボードにコピーします。

> 注 :
> A レコードを更新して Webトラフィックを WAF にリダイレクトする場合は、この CNAME アドレスに ping を送信して対応する WAF IP アドレスを取得します。 詳細は、「WAF デプロイメントガイド」をご参照ください。 一般に、WAF IP アドレスはほとんど変わりません。

- DNS ホストのシステムでドメインの DNS 設定を編集する権限があります。 この例では、ドメイン名は、WAF サブスクリプションと同じ Alibaba Cloud アカウントを使用して Alibaba Cloud DNS でホストされています。

手順

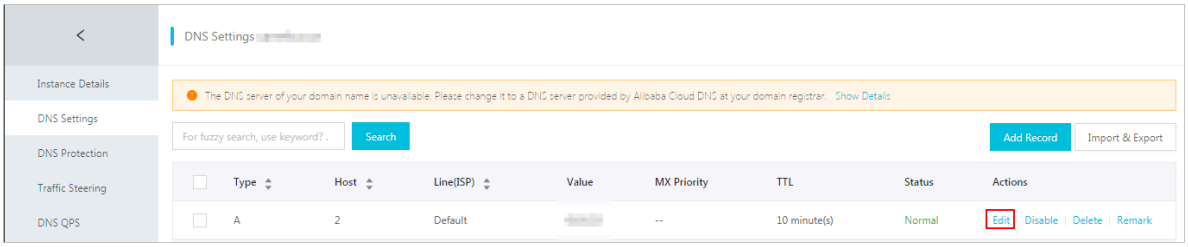
1. Alibaba Cloud DNS コンソールにログインします。
2. 操作するドメインを選択して、[設定] をクリックします。



3. 操作する ホスト (ホスト名) を選択し、[編集] をクリックします。

   `abc . com` を例に取ります。 次のようにホスト名を選択します。

   - www : www で始まるサブドメインと一致します。この場合は `www . abc . com` です。
   - @ : ルートドメインに一致します。この場合は `abc . com` です。
   - * : ルートドメインとすべてのサブドメインの両方を含むワイルドカードドメイン名に一致します。この場合は `blog . abc . com` 、 `www . abc . com` 、 `abc . com` などです。



4. [レコードの編集] ダイアログボックスで、次の操作を行います。

   - タイプ: CNAME を選択します。
   - 値 : WAF CNAME アドレスを入力します。
   - 他の設定はそのままにします。 TTL 値を 10 分に設定することを推奨します。 TTL 値が大きいほど、DNS の伝達は遅くなります。

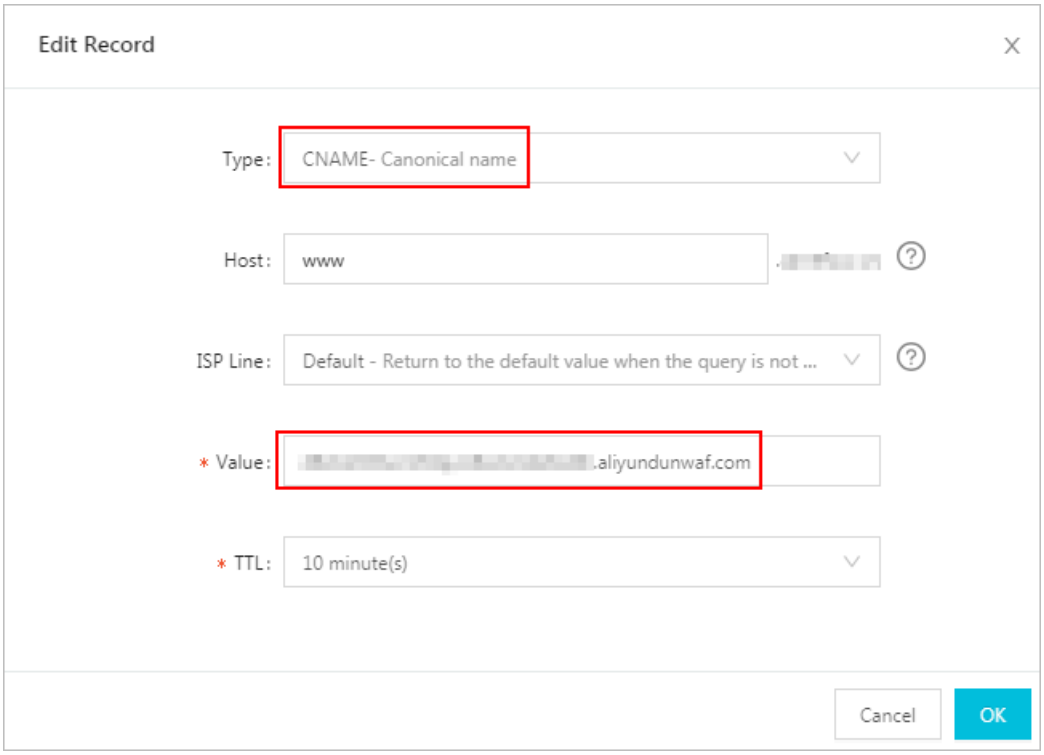
   DNS レコードの編集に関する注意事項:

   - ホスト名の場合、CNAME レコードは一意です。 WAF CNAME アドレスに編集する必要があります。
   - 異なるレコードタイプは互いに矛盾します。 たとえば、ホスト名の場合、CNAME レコードを A レコード、MX レコード、または TXT レコードと共存させることはできません。 レコードタイプを直接変更できない場合は、まず競合するレコードを削除してから新しい CNAME レコードを追加します。

   注 :

削除と追加のプロセス全体を短時間で実行する必要があります。 そうでない場合、ドメインにアクセスできなくなります。

- MX レコードが使用されている場合は、A レコードを使用して Web トラフィックを WAF にリダイレクトできます。 詳細は、「WAF デプロイメントガイド」をご参照ください。



5. [OK] をクリックして DNS 設定を完了し、DNS 変更が有効になるのを待ちます。
6. (オプション) DNS 設定を確認します。 ドメインに ping を送信するか、 の DNS Check を使用して DNS 変更が有効かどうかを検証します。

注 :
設定が有効になるまでにある程度時間がかかります。 検証に失敗した場合は、約 10 分待ってから再度検証します。

7. DNS 解決ステータスを確認します。

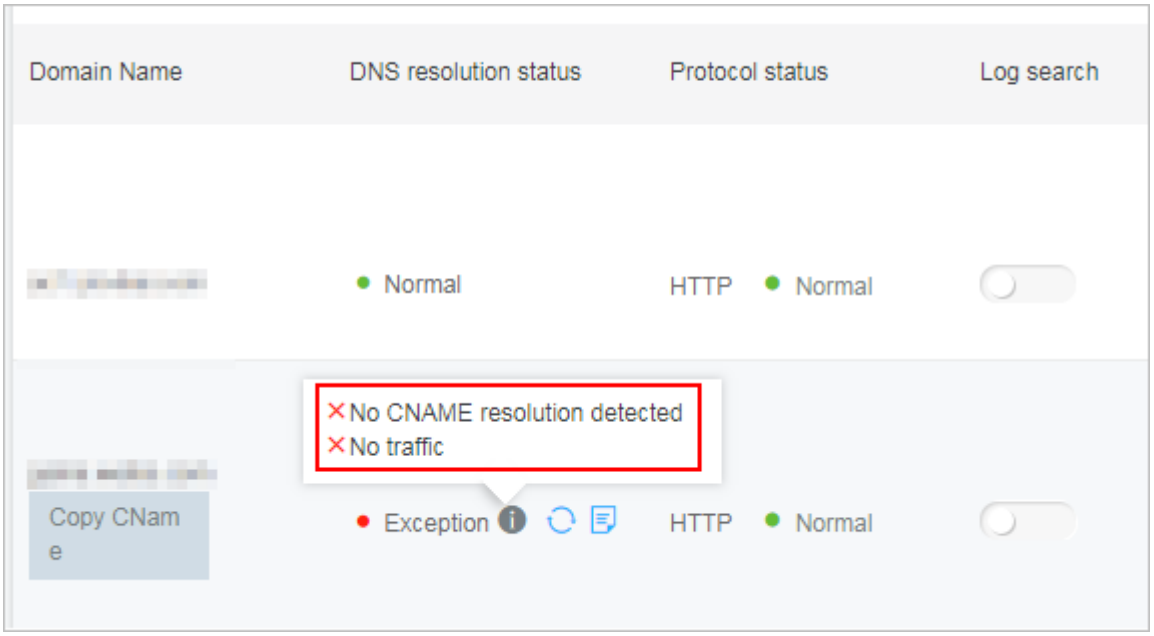
   a. Alibaba Cloud WAF コンソールにログインします。

   b. 管理 > Web サイト設定 ページで、ドメイン名の DNS 解決ステータス を確認します。

   - Normal: Alibaba Cloud WAF は正常にデプロイされ、Web トラフィックは WAF によってモニタリングされています。
   - Exception:"CNAME 解決が検出されませんでした"、"トラフィックなし"、または "DNSチェックに失敗しました" の例外メッセージの場合、DNS 設定が正しくない可能性があります。

     この場合は、DNS 設定を確認します。 DNS 設定が正しいことを確認したら、1 時間待ってから DNS 解決ステータスを更新します。 詳細は、「DNS 解決ステータスの例外」をご参照ください。

     > 注 :
     > ここでの例外は、WAF が正しくデプロイされていないことを示しています。 Web サイトへのアクセスは影響を受けません。



4 手順 3 : WAF 保護ポリシーの設定

Web サイトが Alibaba Cloud WAF でデプロイされると、WAF はデフォルトの保護設定に基づいて、Web トラフィックの検査、一般的な Web 攻撃 (SQL インジェクションや XSS スクリプトなど) および HTTP フラッド攻撃のブロックを支援します。 実際の業務状況に応じて、より多くの保護機能を有効にしてそれらのポリシーを設定します。

1. Alibaba Cloud WAF コンソールにログインします。
2. ページ上部でリージョン [中国本土]、[国際] を選択します。
3. 管理 > Web サイト設定 ページで、設定するドメイン名を選択し、[ポリシー] をクリックします。
4. さまざまな WAF 保護機能を有効または無効にして、それらの保護ルールを管理します。

> 注 :
> さまざまなサブスクリプションプランがさまざまな機能で提供されています。 以下の機能がすべてサブスクリプションに含まれているわけではありません。 詳細は、「WAF サブスクリプションプラン」をご参照ください。

- HTTP ACL ポリシー : 有効にすると、配信元の IP アドレス、リクエストされた URL、その他の一般的な HTTP リクエストヘッダーフィールドなどの条件に基づいて、Web リクエストをフィルターするための Web アクセス制御ルールを作成します。 詳細は、「HTTP ACL ポリシー」をご参照ください。
- Web アプリケーション保護 : デフォルトで有効になっています。 SQL インジェクションなどの一般的な Web 攻撃から Web サイトを保護し、検査の厳密性を設定して悪意のあるリクエストをブロックするかどうかを判定することが可能です。 詳細は、「Web アプリケーション保護」をご参照ください。
- HTTP フラッド保護 : デフォルトで有効になっています。 HTTP フラッド攻撃から Web サイトを保護し、検査の厳密性を設定することが可能です。 Business または Enterprise サブスクリプションで、レートベースのルールを作成して、指定した時間間隔あたりのリクエスト数を制限することも可能です。 レートベースのルールは、指定された時間間隔あたりの特定の IP アドレスから受信したリクエストをカウントします。 リクエスト数が制限

を超えると、ルールによって指定されたアクションが起動されます。 詳細は、「HTTP フラッド保護」と「#unique_16」をご参照ください。

- 新しいインテリジェント保護エンジン : 有効にすると、Web リクエストに対して自動的に意味解析を実行して、難読化や変種を悪用し、巧妙に偽装または隠された悪意のある攻撃を発見します。 詳細は、「新しいインテリジェント保護エンジン」をご参照ください。
- 悪意のある IP ペナルティ : 有効にすると、短時間に複数の攻撃を開始した IP からのリクエストを自動的にブロックします。 詳細は、「悪意のある IP ペナルティ」をご参照ください。
- ブロックされるリージョン : 有効にすると、指定された地理位置情報からのリクエストをブロックします。現在は中国の省または中国以外のリージョンが対象です。 詳細は、「ブロックされるリージョン」をご参照ください。
- データリスク管理 : 有効にすると、登録、ログイン、アクティビティ、フォーラムなどの重要な業務インターフェース用の追加のセキュリティ確認ページに疑わしいユーザーをリダイレクトしてマシン詐欺を防ぎます。 ゾンビアカウント、ハッキングアカウント、投票詐欺、およびスパムメッセージから保護するのに役立ちます。 詳細は、「データリスク管理」をご参照ください。
- Web サイトの改ざん防止 : 有効にすると、指定した Web ページをロックして元のコンテンツが改ざんされないようにします。 ロックされた Web ページがリクエストされると、サーバーは指定したキャッシュページを返します。 詳細は、「Web サイト改ざん防止」をご参照ください。
- データ漏えい防止 : 有効にすると、機密データフィルタリングルールを作成して、ID カード番号、クレジットカード番号、電話番号、返した Web コンテンツのデフォルトの機密単語を隠したり、指定されたリクエストコードで Web ページをブロックします。 詳細は、「データ漏えい防止」をご参照ください。

5 手順 4 : セキュリティレポートの表示

Web サイトが Alibaba Cloud WAF でデプロイされ、WAF 保護ポリシーが設定されると、WAF セキュリティレポートにアクセスして Web 業務のセキュリティ状況についての洞察を得たり、業務分析を実施します。

1. Alibaba Cloud WAF コンソール にログインします。
2. ページ上部でリージョン [中国本土]、[国際] を選択します。
3. レポート > 概要 ページで、業務の統計とセキュリティ状況を表示します。

   以下の業務統計を表示します。

   - 直近 30 日間の合計 QPS と悪意のある QPS (保護ルールの起動)
   - 直近 30 日間のインバウンドとアウトバウンド帯域幅
   - 直近 30 日間の異常な応答数
   - 配信元の上位 5 都市および上位 10 個の IP アドレス
   - モバイルオペレーティングシステムと配信元 PC ブラウザー
   - 応答速度が最も遅い上位 5 つの URL
   - 最も頻繁にリクエストされている上位 5 つの URL

   次のセキュリティ統計を表示します。

   - 最近 30 日間の Web アプリケーション攻撃、HTTP フラッド攻撃、および Web ACL イベントの頻度
   - 新たに公開された業界または業務セキュリティイベントのリスク警告
   - Alibaba Cloud WAF 保護ルールセットの更新メッセージ

   詳細は、「セキュリティ概要」をご参照ください。

4. レポート > レポート ページで、詳細な攻撃保護レコードとリスク警告を照会します。

   次の攻撃保護レコードの詳細を照会します。

   - 直近 30 日間の Web アプリケーション攻撃
   - 直近 30 日間の HTTP フラッド攻撃
   - 直近 30 日間の Web ACL イベント

   以下のリスク警告の詳細を照会します。

   - 既知のハッカーの攻撃
   - WordPress 攻撃
   - 疑わしい攻撃
   - ロボットスクリプト
   - Web クローラー
   - SMS 悪用妨害

   詳細は、「WAF セキュリティレポート」をご参照ください。