Alibaba Cloud Web Application Firewall

ユーザーガイド

Document Version20190919

目次

1 Alibaba Cloud WAF を 5 分で理解

Alibaba Cloud WAF (WAF) は、Web アプリケーションのファイアウォールであり、Web サイトへの HTTP および HTTPS リクエストをモニタリングし、Web サイトのアクセス制御を実装するのに役立ちます。 WAF を使用して ACL ルールをカスタマイズしたり、内蔵のシナリオベースの保護機能を有効にします。

このトピックでは、以下のタスクについて説明します。

- WAF の有効化
- WAF の実装
- WAF 保護ポリシーの設定
- WAF セキュリティレポートの表示
- その他のベストプラクティスの参照

WAF の有効化

Alibaba Cloud WAF は有料サービスであり、月額または年額のサブスクリプション方式で請求されます。 WAF を使い始めるには、適切な業務プランをサブスクライブして支払いを完了する必要があります。 その後は、サブスクリプション期間内に仕様で規定された保護サービスを利用します。

詳細は、「請求方法」、「サブスクリプションプラン」および「Alibaba Cloud WAF の購入」をご参照ください。

> 注 :
> WAF を購入する場合、WAF で検査する通常の業務トラフィックを指定する必要があります。それにより WAF が DDoS 攻撃などの異常なトラフィックを識別できるようになります。 サブスクリプションプランごとに、帯域幅が異なります。 通常の業務トラフィックが仕様の帯域幅を超える場合は、追加の帯域幅を購入します。

Alibaba Cloud WAF をサブスクライブするには、月額または年額のサブスクリプションです。サブスクリプション方式で WAF を購入するには、該当する WAF パッケージを選択し、請求書が作成されたらすみやかに支払いを完了します。 購入したパッケージに指定された期間内で保護サービスを利用します。

> 注 :

> 注：
> サブスクリプションモデルを購入する場合、通常の業務トラフィックを提供する必要があります。DoS 攻撃などの異常なトラフィックと区別するのに役立ちます。 さまざまな WAF パッケージにより、さまざまな業務帯域幅がサポートされています。 実際の業務トラフィックがパッケージの帯域幅制限を超える場合は、帯域幅拡張パッケージを購入する必要があります。

WAF の請求方法の詳細については、「請求方法」をご参照ください。

WAF の購入方法の詳細については、「 WAF の購入」をご参照ください。

WAF を購入すると、WAF インスタンスが作成されます (WAF IP アドレスに相当)。 WAF インスタンスには、保護対象の Web サイトを 10 個まで追加可能です。 これら 10 個の Web サイトでは、トップレベルドメイン名を 1 つだけ使用します。

- 異なるトップレベルドメイン名で Web サイトを保護する場合は、追加ドメイン名パッケージを購入します。
- 1 つの WAF IP アドレスを使用してすべてのドメイン名を保護する代わりに、重要なドメイン名を排他的に保護する必要がある場合は、 専用 IP アドレスを購入します。

WAFへのアクセス

WAF を購入したら、DNS (Domain Name System) を通じて、Web サイト上のアクセストラフィックを WAF インスタンス (IP アドレス) に転送する必要があります。 悪意のあるリクエストを除外した後、WAF は正規のトラフィックを配信元に転送します。

2 つの手順で WAF にアクセスします。

- クライアントからのすべてのアクセストラフィックを WAF に転送

  WAF に Web サイト (メイン名) を追加すると、WAF は CNAME アドレスをこのドメイン名に割り当てます。 ドメイン名に CNAME レコードを適用すると、Web サイトへのアクセストラフィックが WAF インスタンスに転送されます。

  > 注：
  > WAF IP アドレスはコンソールに表示されません。 この IP アドレスを取得するには、 `ping` コマンドを実行して、ドメイン名に割り当てられた CNAME アドレスに ping を実行します。

- フィルターされたアクセストラフィックを WAF から配信元に転送

  WAF は、フィルターされたアクセストラフィックを配信元アドレス (IP アドレスまたは OSS (Object Storage Service) の CNAME アドレスなどの他のアドレス) に転送します。

を使用してドメイン名を解決する場合、WAF サービスにアクセスするのが便利です。 それ以外の場合は、アクセス操作を手動で実行する必要があります。

WAF へのアクセス方法の詳細については、「ドメイン名の追加」をご参照ください。

WAF の保護オプションの選択

WAF は、クライアントから HTTP および HTTPS を介して送信された GET および POST リクエストを分析し、アクセスルールを適用して悪意のあるアクセストラフィックを除外します。

> 注 :
> 次の機能はパッケージに含まれていない可能性があります。 機能の詳細については、各機能のリンクをご参照ください。

- HTTP ACL ポリシーを使用してアクセスルールをカスタマイズし、クライアントの IP アドレス、リクエスト URL、および共通リクエストヘッダーフィールドをフィルターします。 操作の詳細については、「ドメイン用ホワイトリストまたはブラックリストの設定」および「HTTP ACL ポリシー」をご参照ください。
- Web 保護オプションを使用して、一般的な Web 攻撃から保護することも可能です。 Web 攻撃の特徴とリクエストヘッダーとリクエスト本文の分析に基づいて、正確なフィルタリングアルゴリズムが書かれています。 これらの複雑なフィルタリングアルゴリズムは、使用するための保護オプションにカプセル化されています。 WAF は以下の保護オプションを提供します。

  > 注 :
  > WAF では、多層フィルタリングメカニズムが使用されています。 WAF を有効にして保護オプションを設定した後、リクエストが WAF に転送される場合にクライアントリクエスト

は多層フィルタリングを通過する必要があります。 デフォルトの保護シーケンスは、 HTTP ACL ポリシー > HTTP フラッド保護 > Web アプリケーション保護 です。

- Web アプリケーション保護 : SQL インジェクションや XSS クロスサイト攻撃などの一般的な Web 攻撃からユーザーを保護するのに役立ちます。 操作の詳細については、「Web アプリケーション保護ポリシーの設定」をご参照ください。
- HTTP フラッド保護: ページリクエストに対する HTTP フラッド攻撃から保護するのに役立ちます。 操作の詳細については、「 HTTP フラッド保護モードの設定」および「 HTTP フラッド保護のカスタマイズ」をご参照ください。
- インテリジェント保護エンジン: リクエストの意味解析を実行し、悪意のあるリクエストを検出します。混同攻撃や変種から始まった悪意のある攻撃からユーザーを保護するのに役立ちます。 操作の詳細については、「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 : 短時間で複数の Web 攻撃を開始するクライアントの IP アドレスを自動的にブロックするのに役立ちます。 操作の詳細については、「悪意のある IP ペナルティの有効化」をご参照ください。
- ブロックされるリージョン: ワンクリックで、中国の省または中国外部の地域からの IP アクセスリクエストをブロックするのに役立ちます。 操作の詳細については、「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: ゾンビアカウント、アカウントの盗難、アクティビティ不正行為、スパムメッセージなどのコンピューターの脅威から防御するのに役立ちます。 操作の詳細については、「データリスク管理」をご参照ください。

・ WAF はセキュリティコンプライアンスのニーズにも応えます。 WAF が提供するセキュリティコンプライアンス機能には、次のものがあります。

- Web サイト改ざん防止: 保護された Web サイトのページをロックするのに役立ちます。保護されたページは、リクエスト受信後、設定したキャッシュコンテンツを返します。 操作の詳細については、「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: ID 番号、銀行カード番号、電話番号、機密の単語など、サーバーから返されるコンテンツ内の機密情報 (異常なページまたはキーワード) をフィルターするのに役立ちます。 操作の詳細については、「データ漏えい防止」をご参照ください。

さらに、WAF は便利なモニタリングと管理機能を提供します。

・ セキュリティモニタリング: WAF コンソールの概要ページにグラフィック業務アクセスデータとセキュリティ保護統計を表示します。

- レポート: 30 日以内のドメイン名に対する攻撃の詳細とリスク警告の情報が検索可能です。操作の詳細については、「攻撃保護レポート」および「リスク警告レポート」をご参照ください。
- ログ: Web サイトのログを検索し、オンライン分析を使用してリクエストをすばやく見つけます。 操作の詳細については、「 ログの検索」をご参照ください。

WAF の使用

WAF を購入すると、配信元 IP アドレスで受信されたすべてのリクエストが WAF インスタンスから送信されます。 サーバーの IP アドレスはクライアントには見えません。

- アクセスリクエストの実際のクライアント IP アドレスを取得する場合は、「訪問者の実 IP アドレスの取得」をご参照ください。
- 配信元の IP アドレスが公開されている、または意図せずに公開されている場合、攻撃者は WAF を迂回して直接配信元を攻撃します。 このような状況に対して効果的に保護するには、配信元の保護を設定します。
- Alibaba Cloud の Anti-DDoS Pro または CDN サービスを使用する場合、 次の操作を実行します。

  注 :

  "レイヤ7 プロキシ (例えば、Anti-DDoS/CDN) が有効になっているものがありますか？" の隣の [はい] を選択する必要があります。

  - WAF で Anti-DDoS Pro を使用
  - WAF で CDN を使用
- ネイティブアプリを保護し、HTTP フラッド攻撃、悪意のある登録、偽の注文などの問題を解決するには、WAF の「 SDK ソリューション」をご参照ください。

2 WAF へのアクセス

2.1 Web サイトの設定

Web サイト設定は、Alibaba Cloud WAF でデプロイされている Web サイトの転送ルートを記述します。

自動または手動の方法を使用して Web サイト設定を追加します。

- Web サイト設定の自動作成。 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配信元サーバーの 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を単に選択して、残りの設定を自動設定にすることが可能です。 このように、WAF は DNS 設定を更新して、検査用 WAF に Web トラフィックをリダイレクトするのに役立ちます。
- Web サイト設定の手動作成。 A レコードが Alibaba Cloud DNS に作成されていない場合は、Web サイト設定を手動で作成する必要があります。 その後、DNS ホストのシステムにログインして、DNS 設定を更新して、検査用 WAF に Web トラフィックをリダイレクトします。

  DNS 設定の更新方法の詳細については、「WAF デプロイメントガイド」をご参照ください。

> 注 :
> Alibaba Cloud WAF インスタンスに追加する Web サイト設定の数は、サブスクリプションプランと追加ドメインの数によります。 詳細は、「追加ドメインクォータ」をご参照ください。

配信元サーバーアドレス、プロトコルタイプ、ポートを変更する、または HTTPS の詳細設定を行う場合は、Web サイトの設定を編集します。

WAF 保護を必要としない Web サイトについては、その DNS 設定を復元して Web サイト設定を削除します。

Web サイト設定の自動追加

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。

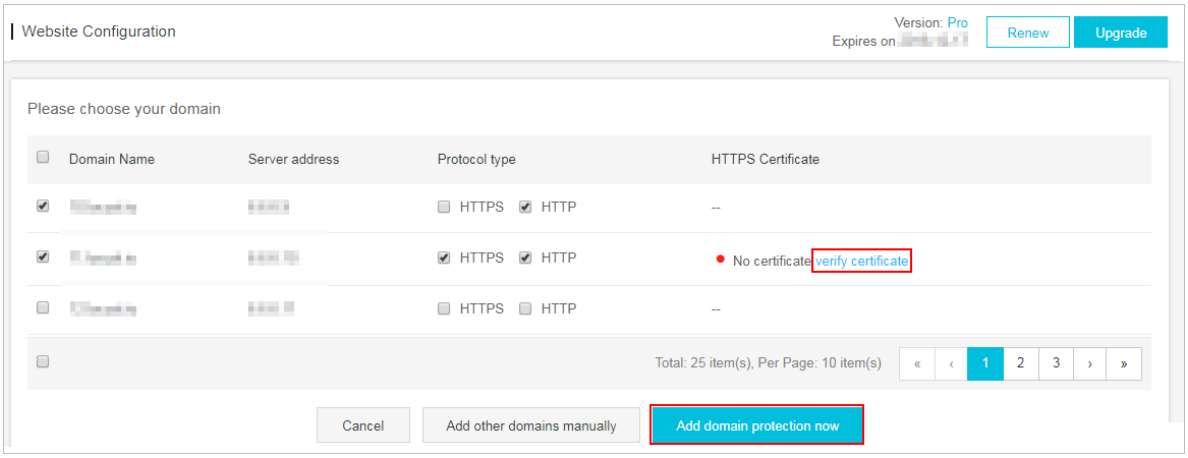
  Alibaba Cloud DNS を使用しない場合は、 Web サイトの設定を参照して Web サイト設定を手動で追加します。

- (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 :

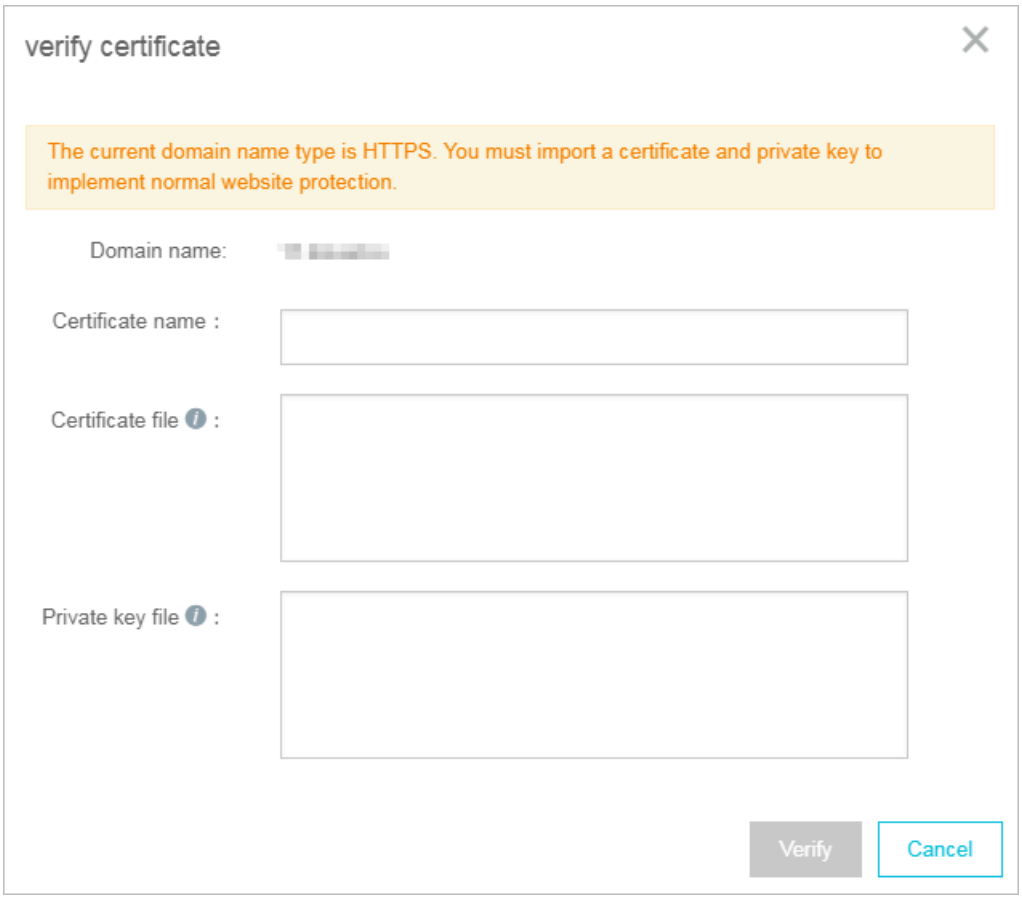
別の方法として、ここでは HTTPS を選択せず、Web サイト設定を編集し、設定を作成した後に証明書をアップロードします。 詳細は、「HTTPS 証明書の更新」をご参照ください。

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。

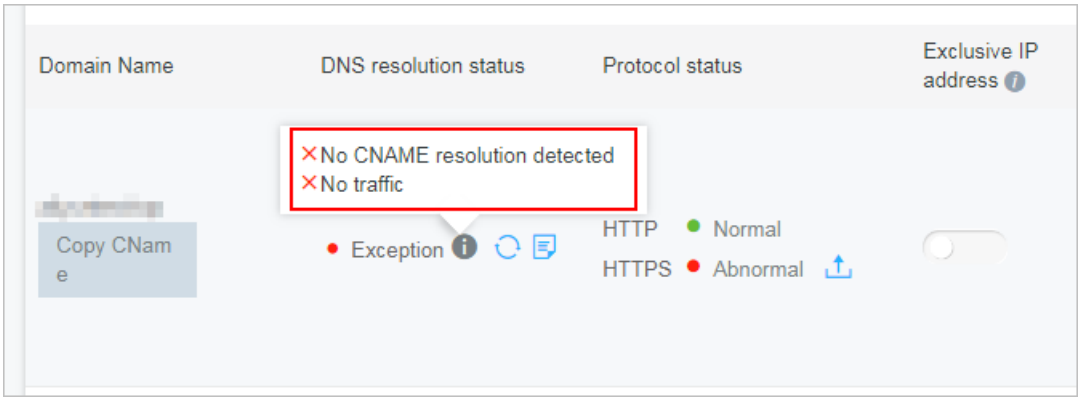
   Web サイト設定を追加した後、WAF はドメイン名の DNS 設定 (CNAME レコード) を自動的に更新して、検査用 WAF に Web リクエストをリダイレクトします。 全体のプロセスは約 10 ～15 分かかります。

   > 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。



Web サイト設定の手動追加

前提条件

- 保護する Web サイトのドメイン名を取得します。
- WAF から返されるトラフィックを受信する予定の配信元サーバー IP アドレスまたはその他の種類のアドレスを取得します。
- Web サイトが CDN、DDoS 保護、またはその他のプロキシサービスでデプロイされているかどうかを確認します。
- (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、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。

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。
4. (オプション) [ドメインを選択してください] ページで、[手動で他のドメインを追加] をクリックします。
5. [Web サイト情報の入力] のタスクで、次の設定を行います。

設定	説明
ドメイン名	保護するドメイン名を入力します。  注 : ・ `*. aliyun . com` などのワイルドカードドメインをサポートします。 ワイルドカードドメインを提示すると、関連サブドメインがすべて照合されます。 ・ 正確なドメイン (例えば、 `www . aliyun . com`) や正確なドメインと一致するワイルドカードドメイン (例えば、`*. aliyun . com`) の Web サイト設定を追加した場合、正確なドメインの設定が優先されます。 ・ .eduドメイン名はサポートしません。 Alibaba Cloud WAF を使用して末尾が .edu のドメイン名を保護する場合は、チケットを送信します。

設定	説明
プロトコルタイプ	Web サイトで使用されているプロトコルを確認します。 オプション値: HTTP、HTTPS 注 : ・ Web サイトで HTTPS が有効になっている場合は、HTTPS を確認し、HTTPS 証明書の更新を参照して、有効な証明書と秘密鍵をアップロードして WAF に HTTPS トラフィックを検査させます。 ・ HTTPS が確認されると、詳細設定 を設定し、HTTPS の強制リダイレクトまたは HTTP back-to-source を有効にして Web サイトへのアクセスを円滑にします。 詳細は、「HTTPS の詳細設定」をご参照ください。
サーバーアドレス	配信元サーバーアドレスを入力します。1 つ以上の IP アドレスまたは OSS CNAME アドレスなどの他のアドレスにします。 Web サイトが Alibaba Cloud WAF でデプロイされると、WAF は検査した Web リクエストをこのアドレスに返します。 ・ (推奨) IP を確認し、ECS インスタンス IP や SLB インスタンス IP など、配信元サーバーのパブリック IP アドレスを入力します。 注 : - 複数の IP アドレスはコンマで区切ります。 最大 20 個の IP アドレスを追加可能です。 - 複数の IP アドレスが提示された場合、WAF は検査した Web トラフィックを返すときに、ヘルスチェックとそれらのアドレス間の負荷分散を行います。 詳細は、「複数の配信元サーバー間の負荷分散」をご参照ください。 ・ 他のアドレスをオンにし、OSS の CNAME アドレスなど、WAF から返されるトラフィックの受信に使用されるサーバーアドレスを入力します。 注 : - サーバーアドレス (その他のアドレス) は Webサイトのドメイン名と同じであってはいけません。 - OSS CNAME アドレスを入力した場合、Web サイト設定を作成した後、Alibaba Cloud OSS コンソールにログインして、指定した OSS CNAME アドレスにカスタムドメイン (この場合は保護するドメイン) を関連付ける必要があります。 詳細は、「カスタムドメインの関連付け」をご参照ください。

設定	説明
サーバーポート	サーバーポートを指定します。 Web サイトが Alibaba Cloud WAF でデプロイされると、WAF は検査した Web リクエストをこのポートに返します。 ・ プロトコルタイプ に HTTP が含まれる場合、デフォルトの HTTP ポートは 80 です。 ・ プロトコルタイプ に HTTPS が含まれる場合、デフォルトの HTTPS ポートは 443 です。 ・ 他のポートを指定する場合は、[カスタム] をクリックしてそれらを追加します。 注 : 詳細は、「サポートされている非標準ポート」をご参照ください。
レイヤ 7 プロキシ (例えば Anti-DDoS または CDN) は有効ですか ?	実際の状況に応じて、[はい] または [いいえ] をオンにします。 レイヤ 7 プロキシが Alibaba Cloud WAF の前にデプロイされている場合は、[はい] をオンにする必要があります。 そうでないと、Alibaba Cloud WAF は実際のクライアント IP アドレスを取得できない可能性があります。
負荷分散アルゴリズム	複数の配信元サーバーアドレスを指定する場合は、WAF 用の負荷分散の方法 (IP ハッシュまたはラウンドロビン) を選択して、これらのアドレス間でトラフィックを分散させます
フローマーク	空いている ヘッダーフィールド 名とカスタム ヘッダーフィールド値を入力して、Alibaba Cloud WAF によって配信元サーバーに返された Web リクエストをマークします。 WAF は、指定されたヘッダーフィールドを Web サーバーの検査済み Web リクエストに追加して、WAF から返されるトラフィックを識別します。 注 : Web リクエスト自体が指定されたヘッダーフィールドを使用する場合、Alibaba Cloud WAF は元の値を指定された値で上書きします。

6. [次へ] をクリックして設定を完了します。

   Web サイト設定を作成したら、以下のタスクを実行します。

   ・ チュートリアルに従って、次のタスク DNS レコードの変更 を実行します。 詳細は、「WAF デプロイメント」をご参照ください。
   ・ (HTTPS 対応 Web サイトの場合) HTTPS 証明書と秘密鍵をアップロードします。 詳細は、「HTTPS 証明書のアップロード」をご参照ください。
   ・ [管理] > [Web サイト設定] ページに移動し、新しく追加されたウェブサイト設定を表示して、必要に応じて編集または削除します。

Web サイト設定の編集

サーバー IP アドレスの変更、プロトコルタイプまたはポートの変更など、Web サーバー設定が変わる場合や、HTTPS の詳細設定を設定する場合は、Web サイト設定を編集します。

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、操作する Web サイト設定を選択し、[編集] をクリックします。
4. [編集] ページで、Web サイト設定の手動追加の手順 5 に従って設定を完了します。

   注：
   ドメイン名 は変更できません。 別のドメイン名を関連付ける場合は、新しい Web サイト設定を追加して不要なものを削除することを推奨します。
5. [OK] をクリックして手順を完了します。

Web サイト設定の削除

Web サイトで Alibaba Cloud WAF を無効にする場合は、DNS を復元して Web サーバーにトラフィックをリダイレクトし、Alibaba Cloud WAF コンソールで Web サイト設定を削除します。

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、削除する Web サイト設定を選択し、[削除] をクリックします。

   注：
   Web サイト設定を削除する前に DNS 設定を復元する必要があります。 そうしない場合、Web サイトにアクセスできなくなる可能性があります。
4. [プロンプトメッセージ] ダイアログボックスで [OK] をクリックします。

2.2 WAF デプロイメントガイド

Web サイトに Alibaba Cloud WAF をデプロイすることは、Web サイト設定の作成後に DNS レコード (CNAME または A タイプ) を更新して、検査のために WAF に Web リクエストをリダイレクトすることを指します。

CNAME レコードまたは A レコードを使用して Web トラフィックをリダイレクトします。CNAME を使用することを推奨します。 CNAME を使用すると、ノードの障害やマシンの障害の場合に、ノードの切り替えやトラフィックを送信元へのリダイレクトさえもサポートされます。

次の内容は、Web サイト専用の Alibaba Cloud WAF のデプロイに適用します。つまり、Web サイトは CDN、DDoS 保護、およびその他のプロキシサービスを使用しません。 その他のシナリオについては、以下のドキュメントをご参照ください。

- Alibaba Cloud WAF と CDN を合わせたデプロイ: CDN と WAF を一緒に Web サイトにデプロイする方法を説明します。
- Alibaba Cloud WAF と DDoS 保護を合わせたデプロイ: Web サイトに DDoS 保護と WAF を一緒にデプロイする方法を説明します。

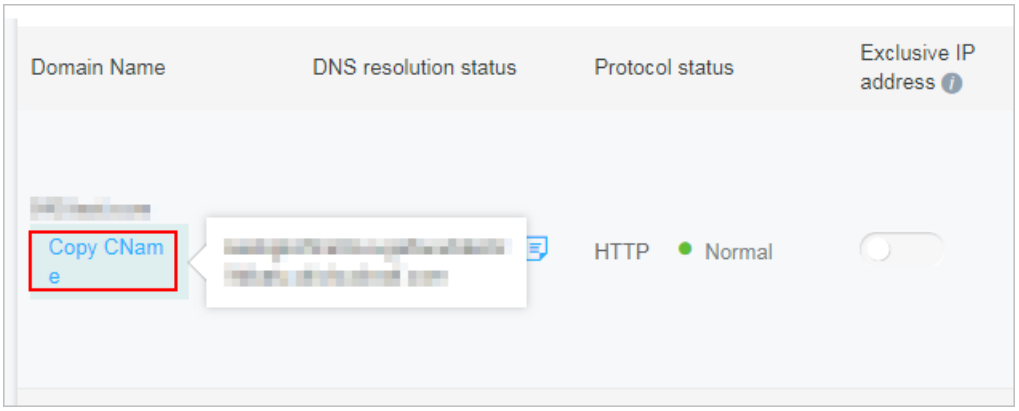
(推奨) CNAME レコードを編集して WAF をデプロイ

前提条件

- Web サイト設定が正常に作成されています。 詳細は、「Web サイト設定」をご参照ください。

- 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。

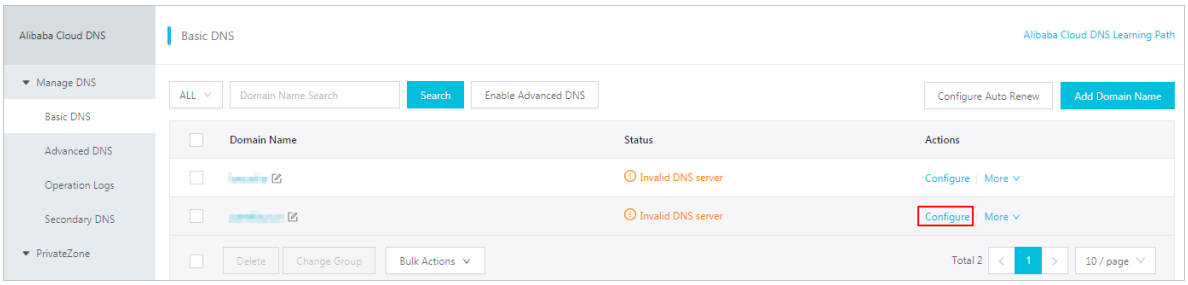
> 注：
> A レコードを更新して Webトラフィックを WAF にリダイレクトする場合は、この CNAME アドレスに ping を送信して対応する WAF IP アドレスを取得します。 詳細は、「WAF デプロイメントガイド」をご参照ください。 一般に、WAF IP アドレスはほとんど変わりません。

- DNS ホストのシステムでドメインの DNS 設定を更新する権限があります。
- (オプション) Alibaba Cloud WAF IP アドレスのホワイトリストへの登録。配信元 Web サーバーが Alibaba Cloud 以外のセキュリティソフトウェア (Fortinet FortiGate など) を有効にしている場合は、ソフトウェアで WAF IP アドレスをホワイトリストに登録して、WAF から返される正規のトラフィックがブロックされないようにする必要があります。 詳細は、「Alibaba Cloud WAF IP アドレスのホワイトリストへの登録」をご参照ください。
- (オプション) ローカルコンピューターでのリダイレクトチェックの実行 DNS 設定を変更する前に、リダイレクトチェックを実行して、設定がすべて正しいことを確認します。 これにより、誤った設定による業務中断を回避します。 詳細は、「ローカルコンピューターでのリダイレクトチェックの実行」をご参照ください。

手順

次の手順では、Alibaba Cloud DNS でCNAME レコードを更新する方法を説明します。 ドメインが Alibaba Cloud DNS でホストされている場合は、次の手順に従います。 それ以外の場合は、DNS ホストのシステムにログインして変更を加える必要があります。

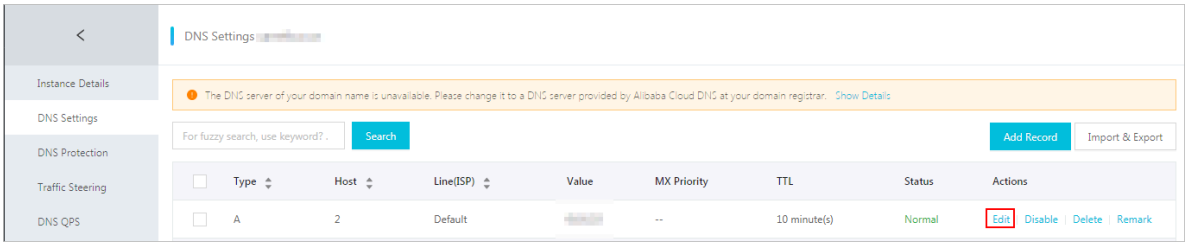
1. Alibaba Cloud DNS コンソールにログインします。
2. 操作するドメインを選択して、[設定] をクリックします。



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。

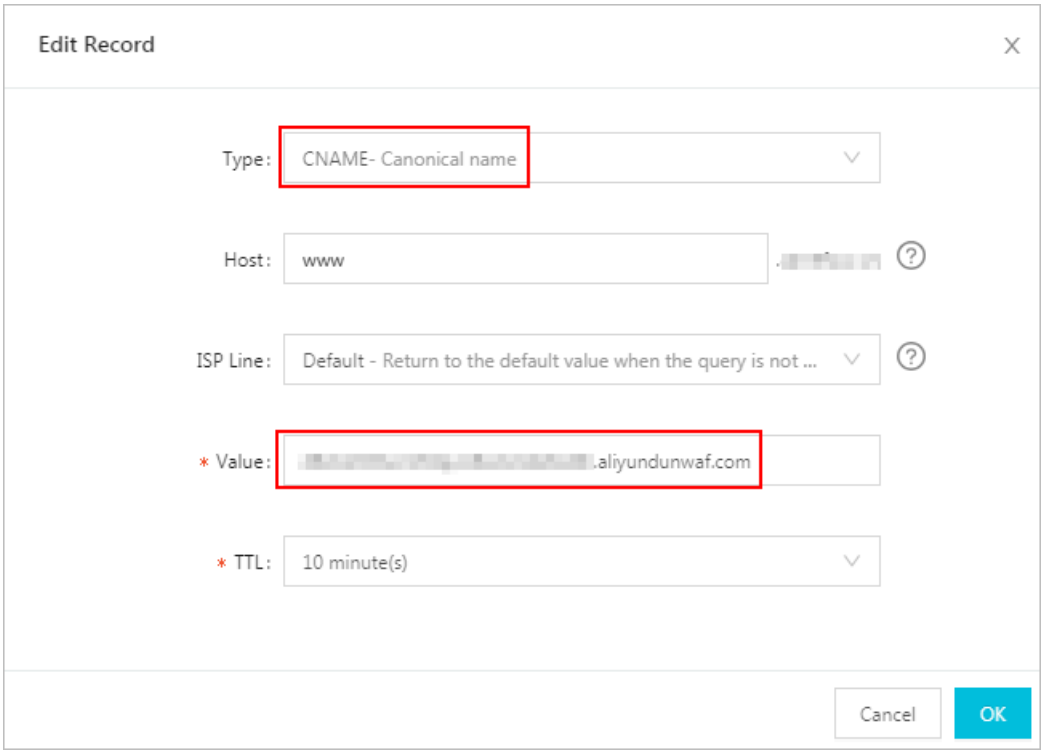
   - タイプ: CNAME を選択します。
   - 値 : WAF CNAME アドレスを入力します。
   - 他の設定はそのままにします。 TTL 値を 10 分に設定することを推奨します。 TTL 値が大きいほど、DNS の伝達は遅くなります。

   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。

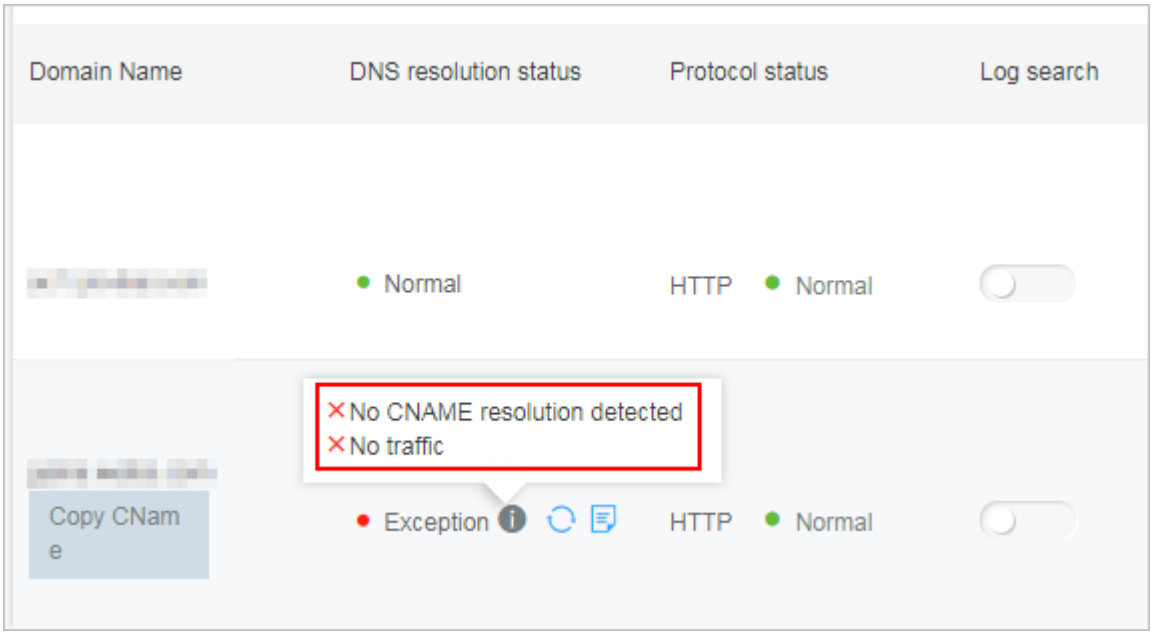
   a. Alibaba Cloud WAF コンソールにログインします。

   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。



配信元の保護

配信元サーバーの IP アドレスが公開されると、攻撃者はそれを悪用して Alibaba Cloud WAF を迂回し、配信元を直接攻撃を開始する可能性があります。 このような攻撃を防ぐために、ECS セキュリティグループまたは SLB ホワイトリストを設定して、Alibaba Cloud WAF の IP アドレスから送信されていない Web リクエストをすべてブロックすることを推奨します。 詳細は、「配信元サーバーの保護」をご参照ください。

A レコードを編集して WAF をデプロイ

A レコードの方法は、以下の違いを除いて CNAME と同じです。

- 前提条件: WAF CNAME アドレスを取得したら、以下を実行して関連 WAF IP アドレスを取得します。
  1. Windows オペレーティングシステムで、cmd コマンドラインツールを開きます。
  2. 次のコマンドを実行します。`ping “copied WAF Cname address”`
  3. 結果に WAF IP アドレスを表示します。
- 手順: 手順 4 レコードの編集で、以下を行います。
  - タイプ: A を選択します。
  - 値: WAF IP アドレスを入力します。
  - 他の設定はそのままにします。

2.3 Alibaba Cloud WAF IP アドレスのホワイトリストへの登録

Web サイトが Alibaba Cloud WAF でデプロイされると、すべての Web トラフィックは検査のために WAF にリダイレクトされ、WAF は検査したトラフィックを配信元サーバーに返します。

配信元サーバーの観点からは、すべての Web リクエストが特定の数の WAF IP アドレスから届くため、疑わしいと言えます。 配信元サーバーに FortiGate などのセキュリティソフトウェアがインストールされている場合、セキュリティソフトウェアは WAF IP アドレスおよび WAF から返された Web トラフィックに対するブロックアクションをトリガーすることがあります。 したがって、配信元サーバーのセキュリティソフトウェアですべての WAF IP アドレスをホワイトリストに登録して、通常の業務中断を回避する必要があります。

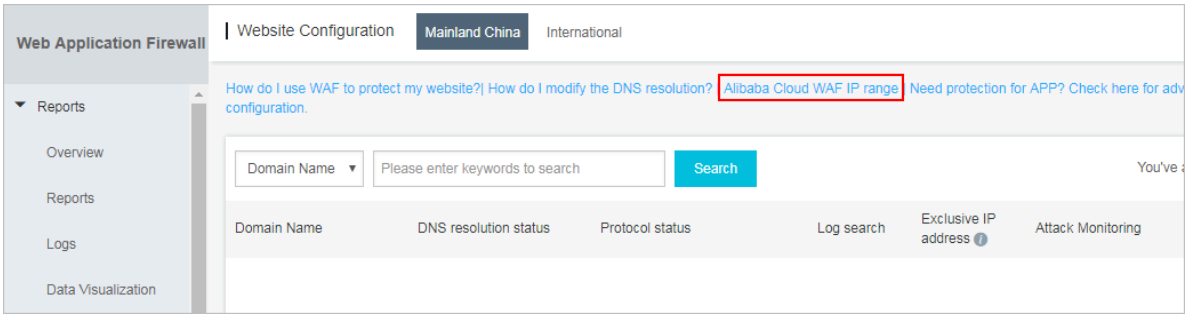
 注 :

Alibaba Cloud WAF をデプロイした後に、配信元サーバーの他のセキュリティソフトウェアをアンインストールすることを推奨します。

手順

Alibaba Cloud WAF コンソールで Alibaba Cloud WAF IP アドレスを表示します。 手順は次のとおりです。

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] ページに移動します。
4. [Alibaba Cloud WAF IP の範囲] をクリックして、すべての WAF IP アドレスを表示してコピーします。



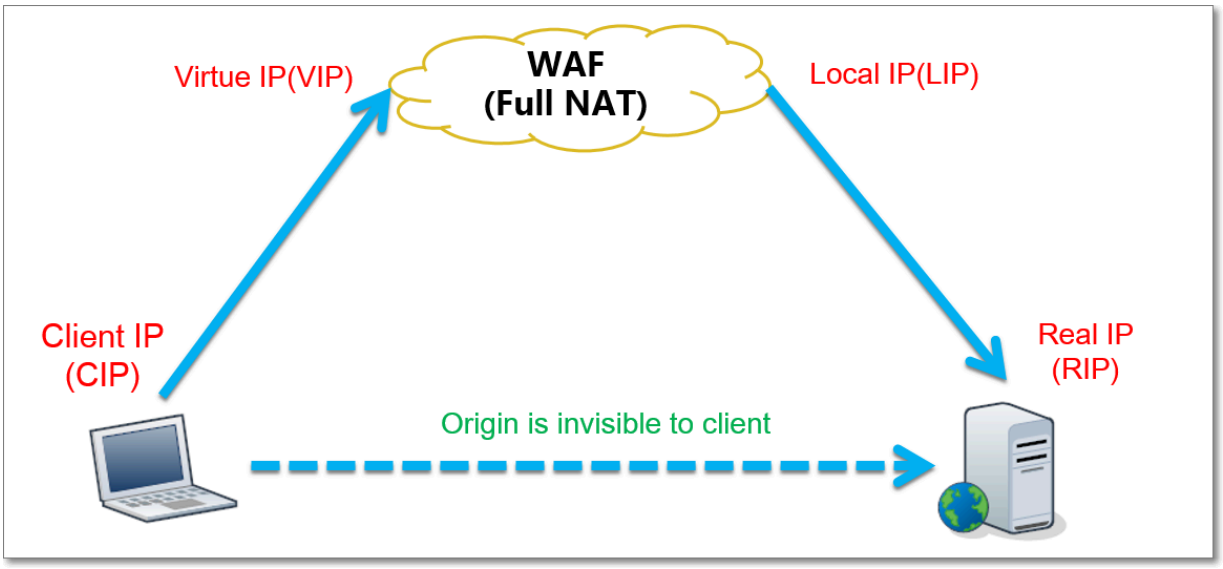
次の結果が表示されます。

5. 配信元サーバーでセキュリティソフトウェアを開き、コピーした WAF IP アドレスを IP ホワイトリストに追加します。

よくある質問

Alibaba Cloud WAF の IP アドレスとは何ですか。

Alibaba Cloud WAF は、クライアントと配信元サーバーの間のリバースプロキシとして機能します。 配信元サーバーから見ると、すべての Web リクエストは Alibaba Cloud WAF IP アドレスから配信され、正しいクライアント IP アドレスは HTTP ヘッダーの XFF (X-Forwarded-For) フィールドに書き込まれます。



Alibaba Cloud WAF IP アドレスをホワイトリストに登録する必要があるのはなぜですか。

配信元サーバーの観点からは、Alibaba Cloud WAF IP アドレスからの Web リクエストはより集中しており、頻度も高いです。 配信元サーバーのセキュリティソフトウェアは、Alibaba Cloud WAF IP アドレスが攻撃を開始していると判断し、それらに対してブロックアクションをトリガーする可能性があります。 Alibaba Cloud WAF IP アドレスがブロックされていると、正しいクライアントは応答を受け取ることができません。 したがって、Web サイトに WAF をデプロイしたら、Alibaba Cloud WAF IP アドレスをホワイトリストに登録する必要があります。 そうでないと、通常の Web アクセスに影響が出る可能性があり、Web ページを開くことができなくなったり、応答が遅くなります。

Alibaba Cloud WAF をデプロイした後は、WAF からの Web リクエストのみを許可し、他のリクエストをブロックして通常の Web 業務アクセスを保証し、配信元への直接攻撃を回避することを推奨します。 配信元サーバー IP アドレスが公開されている場合、攻撃者は WAF を迂回して配信元サーバーを直接攻撃します。 詳細は、「配信元サーバーの保護」をご参照ください。

2.4 ローカルコンピューターでのリダイレクトチェックの実行

Web サイト用の Web サイト設定を Alibaba Cloud WAF に作成済みで、Web トラフィックを検査するために WAF にリダイレクトするよう DNS 設定を更新する場合は、ローカルコンピューターでリダイレクトチェックを実行して、WAF がトラフィックを処理できるか確認することを推奨します。 リダイレクトチェックでは、ローカルホストファイルを変更して、ローカル

コンピューターが Alibaba Cloud WAF インスタンスを直接参照できるようにする必要があります。 この結果、WAF インスタンスが正しく機能しているかどうかをテストすることができます。

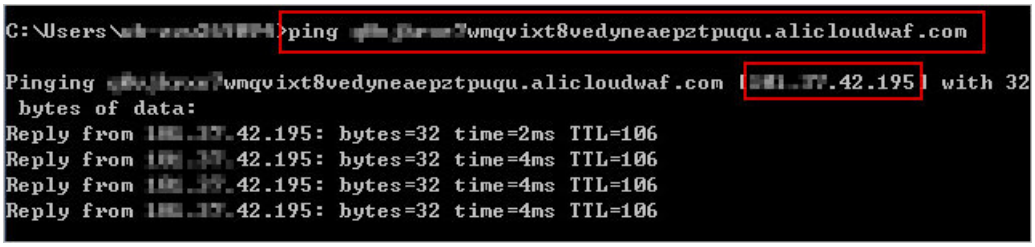
ローカルホストファイルの変更

ローカル *hosts* ファイル (『What is the hosts file?』) を変更し、ローカルリクエストを WAF に転送します。 Windows システムの場合、手順は以下のとおりです。

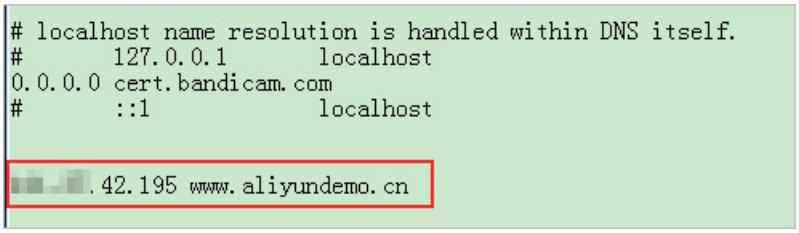
1. *hosts* ファイルをメモ帳で開きます。 *hosts* ファイルは *C :\ Windows \ System32 \ drivers \ etc \ hosts* ディレクトリにあります。
2. 最後の行に、次の内容を追加します。 `WAF_IP_add ress Domain_nam e_protecte d`

   `www . aliyundemo . cn` 用の Web サイト設定を作成し、Alibaba Cloud WAF に次の CNAME アドレスが割り当てられているとします。 `xxxxxxxxxw mqvixt8ved yneaepztpu qu . alicloudwa f . com`

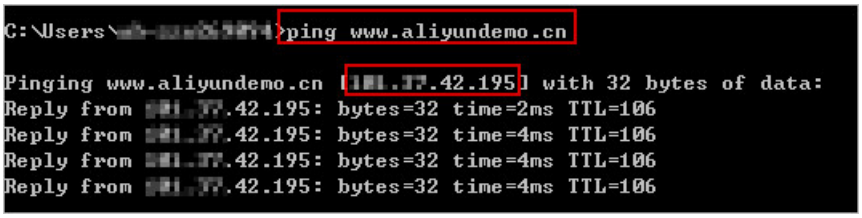
   a. Windows で cmd コマンドラインツールを開き、次のコマンドを実行して WAF IP アドレスを取得します。 `ping xxxxxxxxxw mqvixt8ved yneaepztpu qu . alicloudwa f . com` 応答の WAF IP アドレスを確認します。



   b. 次の行を *hosts* に追加します。 IP アドレスは前の手順で取得した WAF IP アドレスであり、ドメイン名は保護ドメイン名です。



3. 変更を `hosts` に保存します。 cmd で保護ドメイン名の ping を実行します。



WAF が正しく機能する場合、表示される IP アドレスは前の手順で設定した WAF IP アドレスになります。 配信元 IP アドレスが表示される場合は、ローカル DNS キャッシュの更新を試します。 Windows では、cmd で `ipconfig` または `flushdns` を実行します 。

WAF 転送の確認

ホストファイルの変更が有効になったら、ローカルコンピューターから保護ドメイン名にアクセスします。 WAF が正しく設定されていれば、Web サイトは正常にアクセスされます。

さらに、いくつかの簡単な攻撃コマンドを作成することで保護効果を確認します。 たとえば、`/?  alert ( xss )` を URL に追加してテスト用 Web 攻撃リクエストを作成します。 `www . aliyundemo . cn /?  alert ( xss )` にアクセスしようとすると、

2.5 HTTPS 証明書の更新

Alibaba Cloud WAF で Web 業務の HTTPS トラフィックを検査できるようにするには、Web サイト設定で HTTPS をプロトコルタイプに含め、有効な HTTPS 証明書を WAF にアップロードする必要があります。 証明書が変更された場合は、Alibaba Cloud WAF コンソールでタイムリーに証明書を更新する必要があります。

統合管理のために証明書ファイルを Alibaba Cloud SSL Certificate Serviceにアップロードした場合は、再度アップロードする代わりに次の手順で直接再利用します。

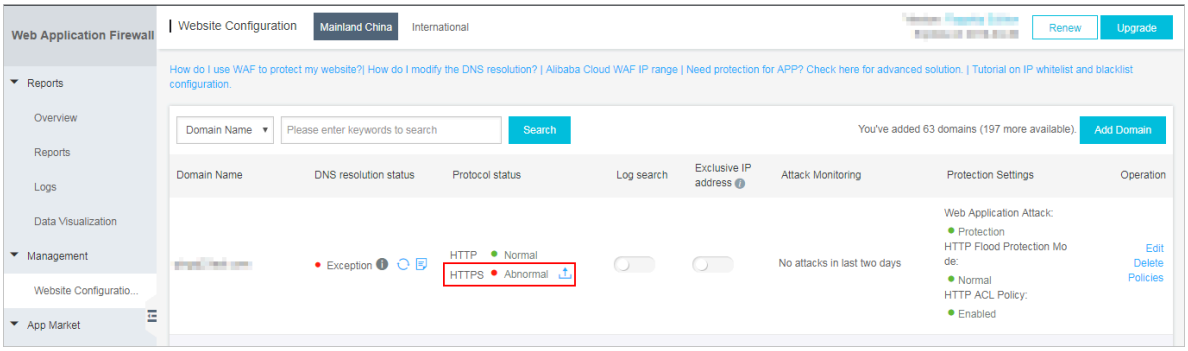
それ以外の場合は、証明書と秘密鍵のファイルを用意して、次の操作を完了する必要があります。

一般的に、以下のファイルが必要です。

- *.crt (公開鍵) または *.pem (証明書)
- *.key (秘密鍵)

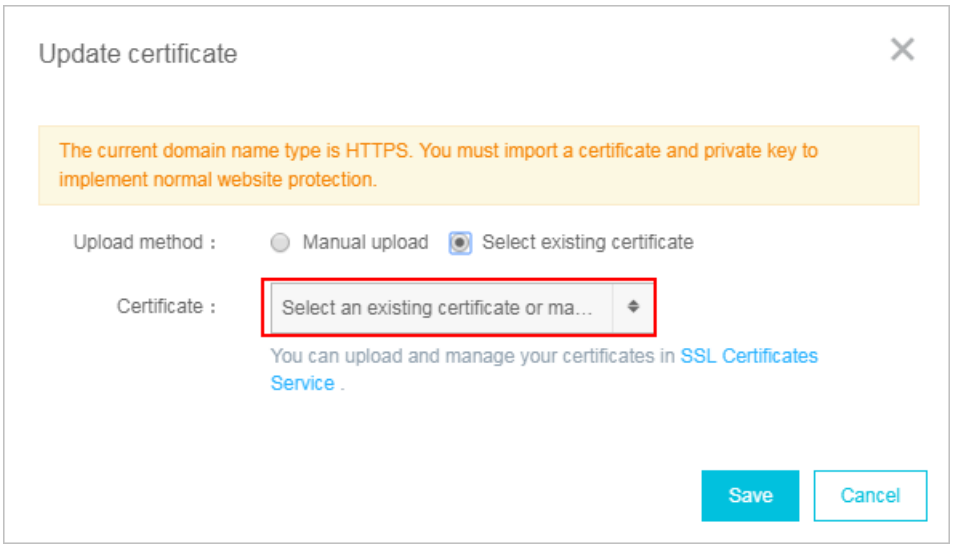
1. Alibaba Cloud WAF コンソールにログインします。
2. ページ上部でリージョン [中国本土]、[国際] を選択します。

3. [管理] > [Web サイト設定] ページで、操作するドメイン名を検索し、[HTTPS]、[プロトコルステータス] の隣の [証明書の更新] ボタン (⬆) をクリックします。



4. [証明書の更新] ダイアログボックスで、[アップロード方法] を選択します。

- アップロードする HTTPS 証明書が Alibaba Cloud SSL Certificate Serviceにホストされている場合、[既存の証明書を選択] をオンにし、アップロード用にそれを選択します。



- 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、証明書ファイルと秘密鍵ファイルのテキストコンテキストをそれぞれ [証明書ファイル] および [秘密鍵ファイル] ボックスに貼り付けます。

> 注：
>
> - PEM、CER、CRT などの一般的な形式の証明書の場合は、テキストエディタツールを使用して証明書ファイルを直接開いてテキストコンテンツをコピーします。 PFX や P7B などの他の形式の証明書の場合は、証明書ファイルを PEM 形式に変換してから、変換した証明書ファイルからテキストコンテンツをコピーします。

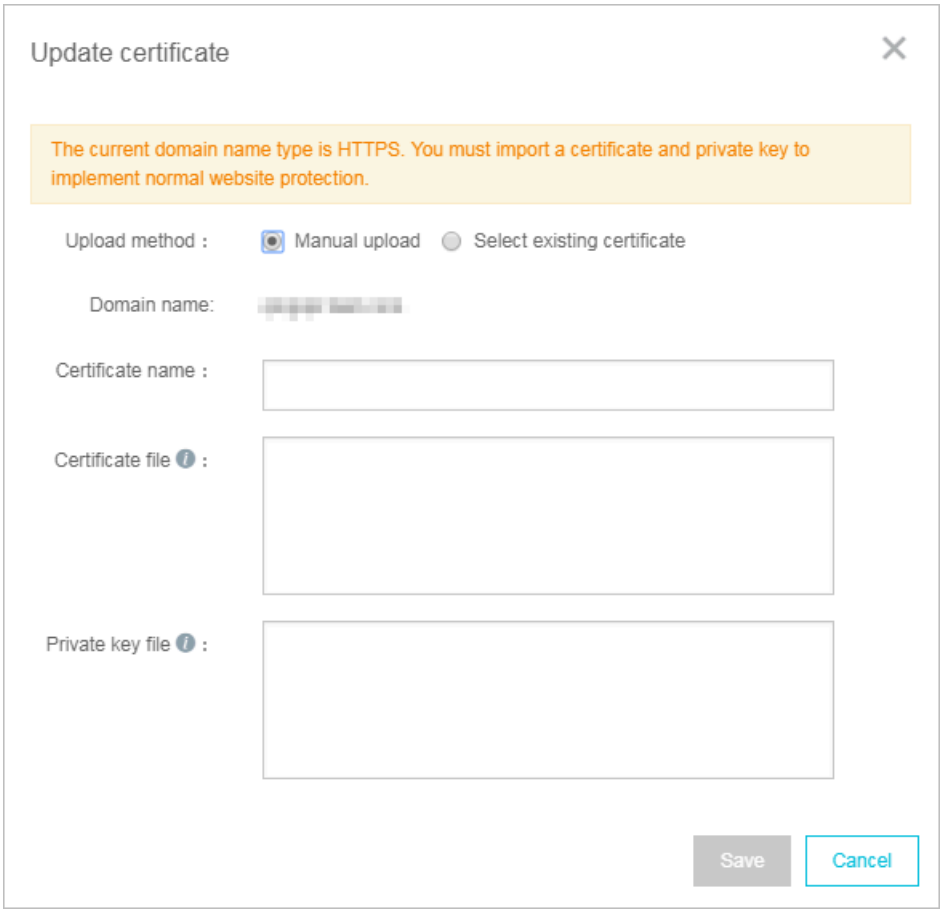
- 証明書チェーンファイルなどの複数の証明書ファイルが HTTPS 証明書にある場合は、複数の証明書ファイルからテキストコンテンツをマージして [証明書ファイル] ボックスに貼り付けます。

証明書ファイルのテキストコンテンツの例

```
----- BEGIN   CERTIFICAT  E -----
 xxxxxxxxxx  xxxxxxxxxx  xxxxxxxxxx  xxxxxxxxxx  xxxxxxxxxx
 8ixZJ4krc + 1M + j2kcubVpsE  2
 cgHdj4v8H6  jUz9Ji4mr7  vMNS6dXv8P  Ukl / qoDeNGCNdy  TS5NIL5ir +
 g92cL8IGOk  jgvhlqt9vc
 65Cgb4mL + n5 + DV9uOyTZTW / MojmlgfUek  C2xiXa54nx  Jf17Y1TADG
 SbyJbsC0Q9  nIrHsPl8YK  k
 vRWvIAqYxX  Z7wRwWWmv4  TMxFhWRiNY  7yZIo2ZUhl  02SIDNggIE  eg ==
----- END   CERTIFICAT  E -----
```

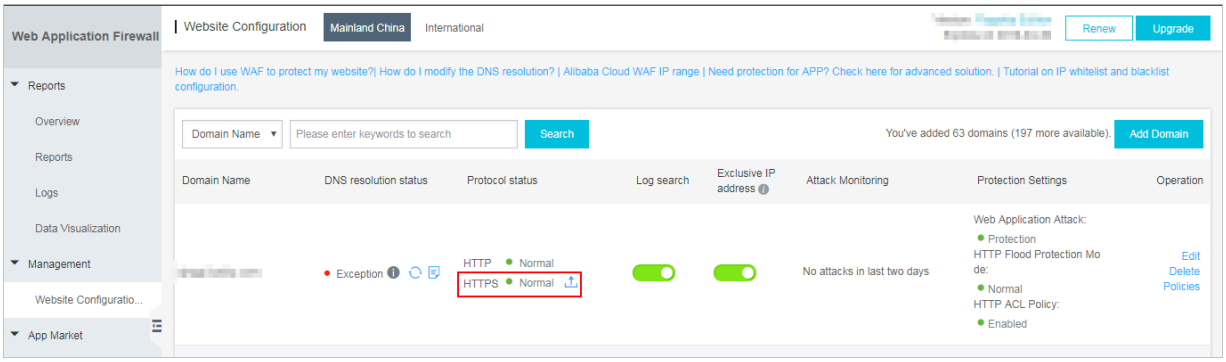
秘密鍵ファイルのテキストコンテンツの例

```
----- BEGIN   RSA   PRIVATE   KEY -----
 DADTPZoOHd  9WtZ3UKHJT  RgNQmioPQn  2bqdKHop + B / dn /
 4VZL7Jt8zS  DGM9sTMThL  yvsmLQKBgQ
 Cr + ujntC1kN6p  GBj2Fw2l / EA / W3rYEce2ty  hjgmG7rZ + A /
 jVE9fld5sQ  ra6ZdwBcQJ  aiygoIYo
 aMF2EjRwc0  qwHaluq0C1  5f6ujSoHh2  e + D5zdmkTg / 3NKNjqNv6x
 A2gYpinVDz  FdZ9Zujxvu  h9o
 4Vqf0YF8bv  5UK5G04RtK  adOw ==
----- END   RSA   PRIVATE   KEY -----
```



5. [保存] をクリックして手順を完了します。

HTTPS プロトコルのステータスは "Normal" と表示されます。

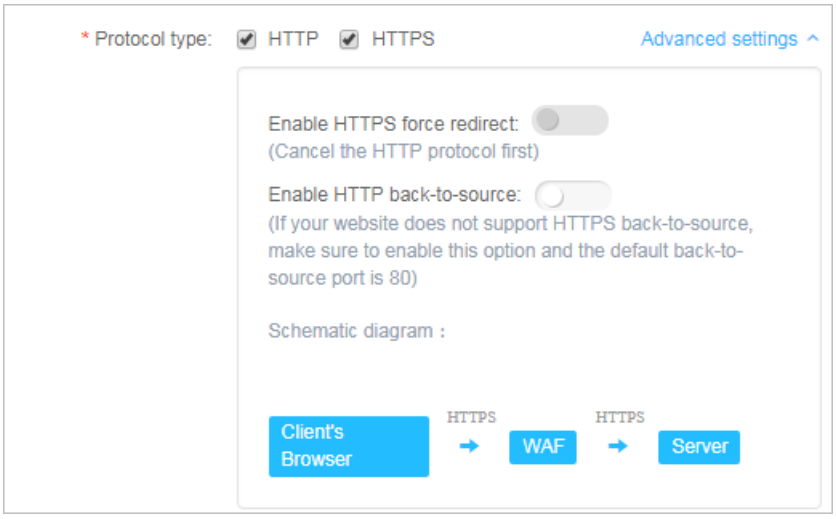


2.6 HTTPS の詳細設定

Alibaba Cloud WAF は便利な HTTPS オプションを提供して、配信元を再構築することなく HTTP back-to-source と HTTPS 強制リダイレクトの実装を支援します。

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を検索し、[編集] をクリックします。

4. [プロトコルタイプ] の [HTTPS] をオンにし、[詳細設定] メニューを展開します。

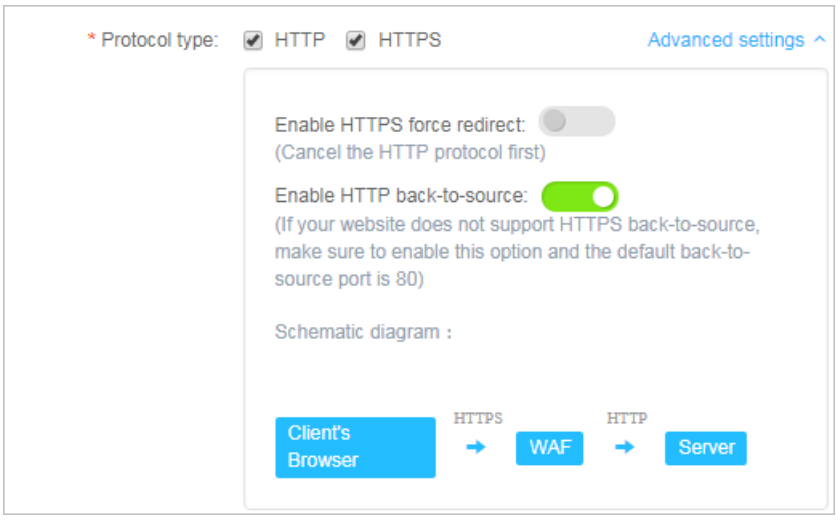


- HTTP back-to-source の有効化

  [HTTP back-to-source] を有効にして、Alibaba Cloud WAF と配信元サーバーの間の HTTP 通信を有効にします。 これにより、WAF は検査したトラフィックを配信元サーバーのデフォルトポート 80 に返します。

  注 :
  HTTP back-to-source を使用しても、配信元サーバーや HTTPS 設定を変更する必要はありません。 ただし、正しい証明書と秘密鍵が Alibaba Cloud WAF にアップロードさ

れていることを確認する必要があります。 Alibaba Cloud SSL Certificate Service で証明書を無料で申請します。



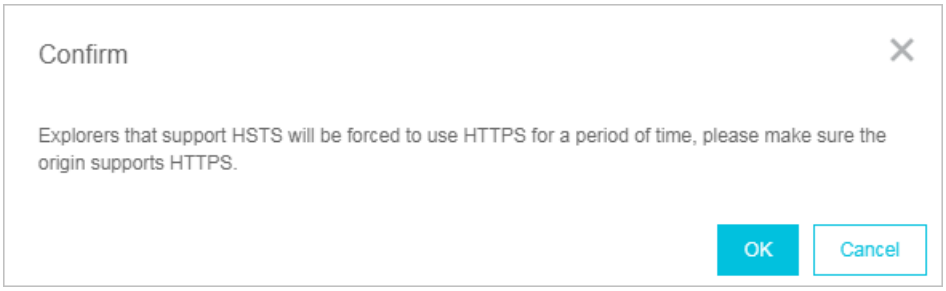
- HTTPS 強制リダイレクトの有効化

  クライアントに HTTPS を使用してサイトにアクセスさせる場合は、HTTPS 強制リダイレクトを有効にします。

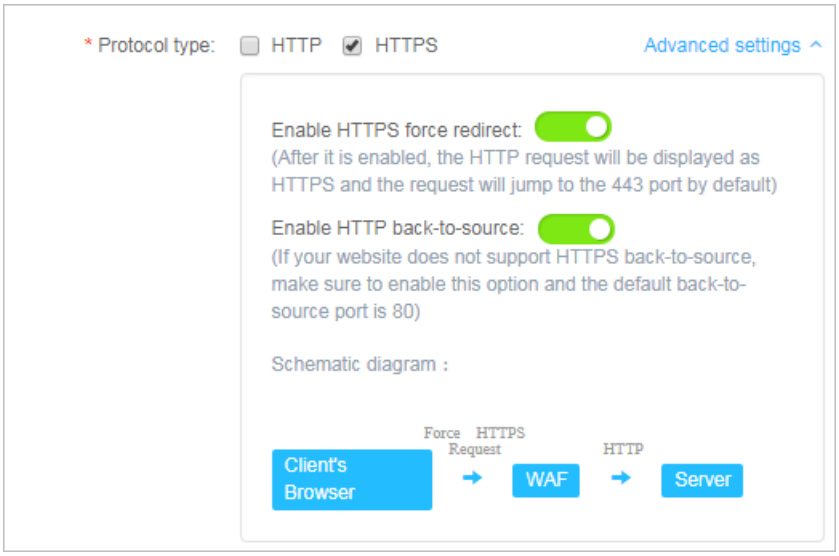
  注 :
  HTTPS 強制リダイレクトを有効にするには、HTTP プロトコルをキャンセルする必要があります。

  HTTPS 強制リダイレクトが有効になっていると、HSTS (HTTP Strict Transport Security) をサポートしている一部の Web ブラウザでは、一定期間 HTTPS の使用が強制

されます。 したがって、配信元サーバーが HTTPS をサポートしていることを確認する必要があります。



HTTPS 強制リダイレクトが有効になっていると、HTTP リクエストはすべて HTTPS として表示され、ポート 443 に転送されます。



2.7 サポート対象の非標準ポート

Alibaba Cloud WAF は、デフォルトで Webトラフィックを配信元サーバーの次のポートに返します。HTTP 接続の場合は、ポート 80 と 8080、HTTPS 接続の場合は、ポート 443 と 8443 です。 Business または Enterprise サブスクリプションプランでは、他のポートを指定できます。 このトピックでは、指定できる最大ポート数と使用できるカスタムポートについて説明します。

最大ポート数

Alibaba Cloud WAF サブスクリプションごとに、すべての Web サイト設定で指定可能な最大ポート数は次のとおりです。

- Business プラン: 最大 10 個のポート (ポート 80、8080、443、8443 を含む) を指定します。

- Enterprise プラン: 最大 50 個のポート (ポート 80、8080、443、8443 を含む) を指定します。

サポート対象のポート

> 注 :
> Alibaba Cloud WAF は、サポート対象のポートをリクエストする Web トラフィックのみを検査します。 サポートされていないポート (たとえば、4444) がリクエストされた場合、リクエストは破棄されます。

- Alibaba Cloud WAF の Business または Enterprise サブスクリプションプランの場合、次の HTTP ポートがサポートされています。

  80, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702
- Alibaba Cloud WAF の Business または Enterprise サブスクリプションプランの場合、次の HTTPS ポートがサポートされています。

  443, 4443, 5443, 6443, 7443, 8443, 9443, 8553, 8663, 9553, 9663, 18980

2.8 WAF back-to-origin フローのマーク

保護用 Web Application Firewall で Web サイトドメイン設定を追加するときに、Web サイトドメインにフローマークを設定します。 Web サイトドメインのトラフィックが WAF を通過するときに、WAF は指定されたフローマークをリクエストに追加します。 したがって、配信元サーバーは対応する情報を容易に収集できます。

HTTP ヘッダーフィールド名とフローマークで指定したフィールド値に従って、トラフィックが WAF を通過するときに、WAF はすべてのリクエストの HTTP ヘッダーにフィールドと値を追加します。 トラフィックをマークすることで、WAF によって転送されたトラフィックを容易に識別でき、その後正確な配信元サーバー保護ポリシー (アクセス制御) の設定や保護効果の分析が可能です。

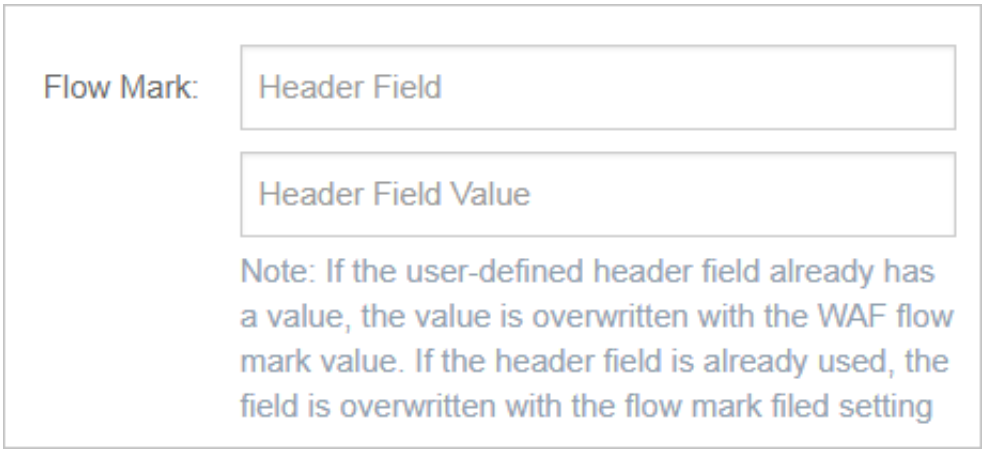
> 注：
> フローマークとして指定したユーザ定義の HTTP ヘッダーフィールドがすでにリクエストに存在する場合、WAF はリクエストの指定されたフローマークフィールド値でフィールド値を上書きします。

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] ページに移動し、ドメイン設定レコードを選択して、 [編集] をクリックします。

   > 注：
   > 新しい Web サイトドメイン設定レコードを追加するときにフローマークを指定することもできます。
4. フローマーク設定項目に、ヘッダーフィールド名とフィールド値を入力します。

   > 注：
   > すでに使用されているユーザー定義の HTTP ヘッダーフィールドを指定しないでください。指定した場合、リクエスト内のフィールドの値は、WAF によってフローマークフィールド値で上書きされます。

5. [OK] をクリックします。 設定が有効になると、WAF は Web サイトドメインにリクエストを転送するときに、指定された HTTP ヘッダーフィールドと値を追加します。

2.9 複数の配信元 IP 間の負荷分散

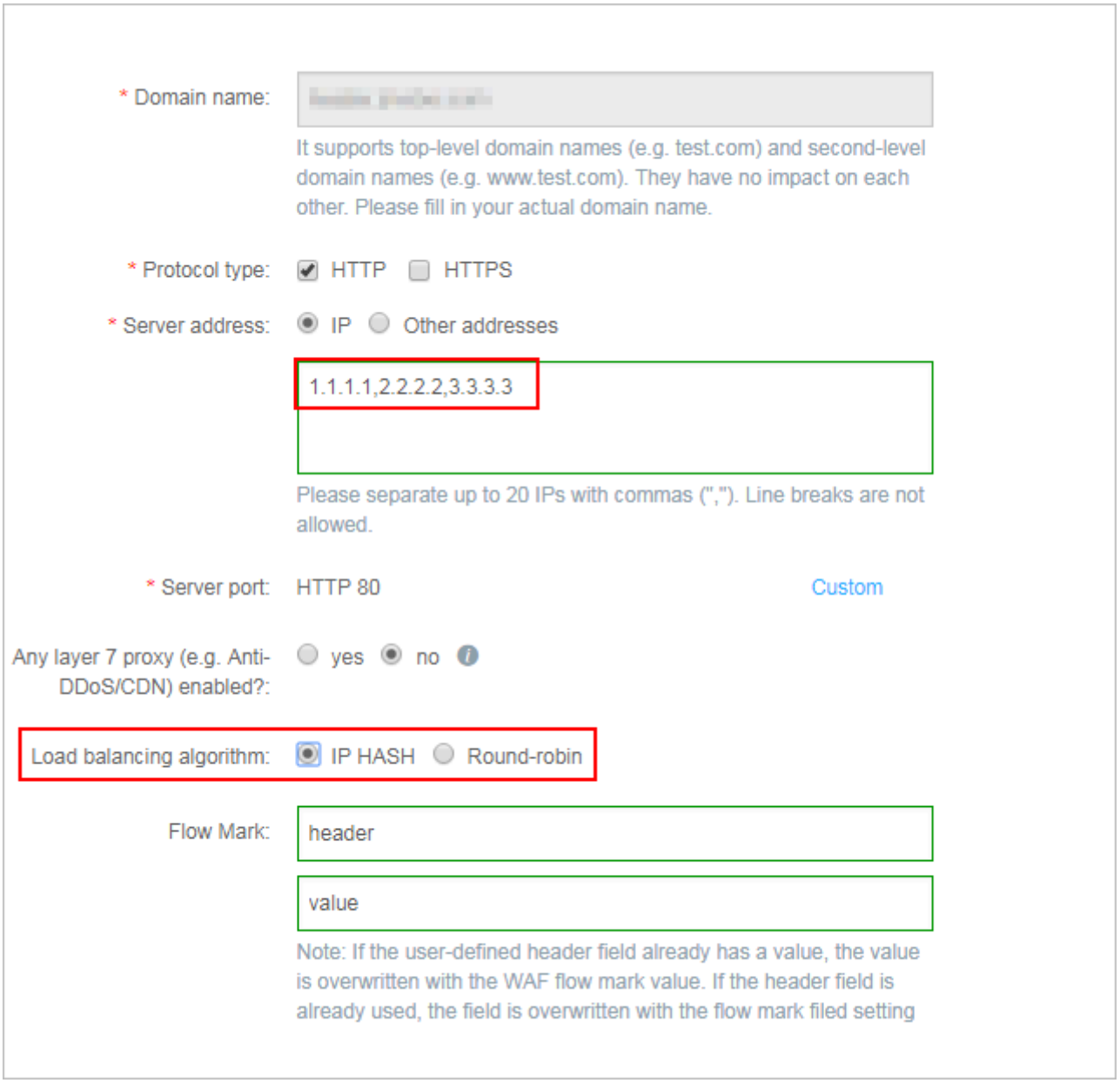
Web サイト設定で最大 20 個の配信元 IP アドレスを指定可能です。

複数の配信元 IP アドレスが指定されている場合、WAF は検査した Web トラフィックを返すときに、それらのアドレス間で負荷分散を行います。 WAF は、すべての配信元 IP でヘルスチェックも行います。 1 つの IP にアクセスできない場合、WAF は再度アクセスできるようになるまでその IP へのリクエストの割り当てを停止します。

1.1.1.1、2.2.2.2、および 3.3.3.3 の 3 つの配信元 IP があるとします。 以下のように Web サイトを設定します。

注 :

DDoS 保護や CDN など、WAF と一緒に他のレイヤー 7 プロキシを有効にしている場合は、Web サイト設定で [レイヤー 7 プロキシ (例えば、Anti-DDoS/CDN) が有効になっているものがありますか？] で [はい] を選択します。



複数の配信元 IP が指定されている場合は、IP ハッシュやラウンドロビンなどの負荷分散アルゴリズムを選択します。

注：

IP ハッシュを使用する場合は、配信元 IP アドレスが別々であることを確認します。 そうでない場合、負荷分散が正しく機能しない可能性があります。

2.10 WAF と Anti-DDoS Pro の同時デプロイ

Alibaba Cloud WAF と Anti-DDoS Pro は完全に互換性があります。 次のアーキテクチャを使用して、WAF と Anti-DDoS Pro を一緒にデプロイします。Anti-DDoS Pro (エントリレイヤー、DDoS 攻撃保護) > WAF (中間レイヤー、Web 攻撃保護) > 配信元。

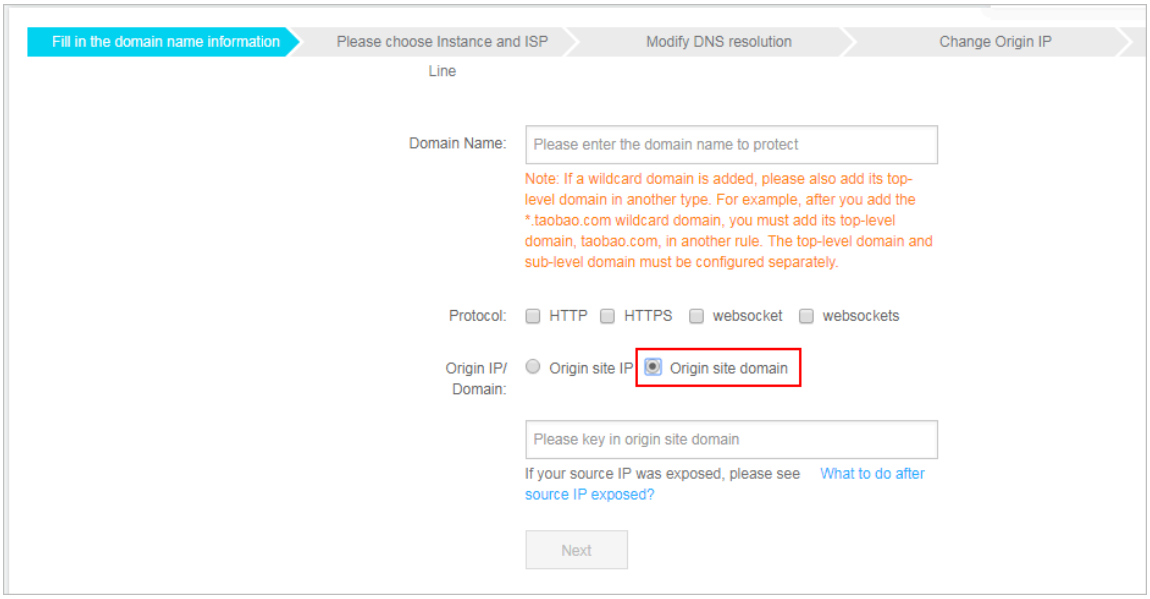
1. Alibaba Cloud WAF で Web サイト用の Web サイト設定を作成します。
   - サーバーアドレス : [IP]をオンにし、ECS インスタンスおよび Server Load Balancer インスタンスのパブリック IP アドレスまたは外部サーバーの IP アドレスを入力します。
   - レイヤー 7 プロキシ (たとえば、Anti-DDoS/CDN) が有効になっているものがありますか？ で [はい]をオンにします。

   詳細は、「Web サイト設定」をご参照ください。
2. Anti-DDoS Pro で、Web サイト用の Web サービスアクセス設定を作成します。 手順は次のとおりです。

   a. [アクセス] > [Web サービス]ページで、[ドメインの追加]をクリックします。

   b. ドメイン名情報の入力タスクで、以下を行います。
      - ドメイン名 : 保護するドメイン名を入力します。
      - プロトコル : サポートしているプロトコルをチェックします。
      - 配信元 IP / ドメイン : 配信元サイトドメインをオンにし、WAF CNAME アドレスを入力します。

      > 注 :
      > WAF CNAME アドレスの表示方法については、「WAF デプロイメントガイド」をご参照ください。



   c. [次へ]をクリックします。

   d. インスタンスと ISP ラインを選択してくださいタスクを完了します。

3. ドメイン名の DNS 設定を更新します。 DNS ホストのシステムにログインし、CNAME レコードを追加して Web トラフィックを Anti-DDoS Pro CNAME アドレスにリダイレクトします。

   詳細は、「」をご参照ください。

Web サイトへの Web リクエストはすべてクリーンアップのために Anti-DDoS Pro にリダイレクトされ、配信元サーバーに届く前に、検査のために WAF にリダイレクトされます。

2.11 WAF と CDN の同時デプロイ

Alibaba Cloud WAF と CDN (Content Delivery Network) を一緒にデプロイして、Web サイトをスピードアップし、同時に Web 攻撃から保護します。 次のアーキテクチャを使用することを推奨します: CDN (エントリレイヤー、Web サイトスピードアップ) > WAF (中間レイヤー、Web 攻撃保護) > 配信元。

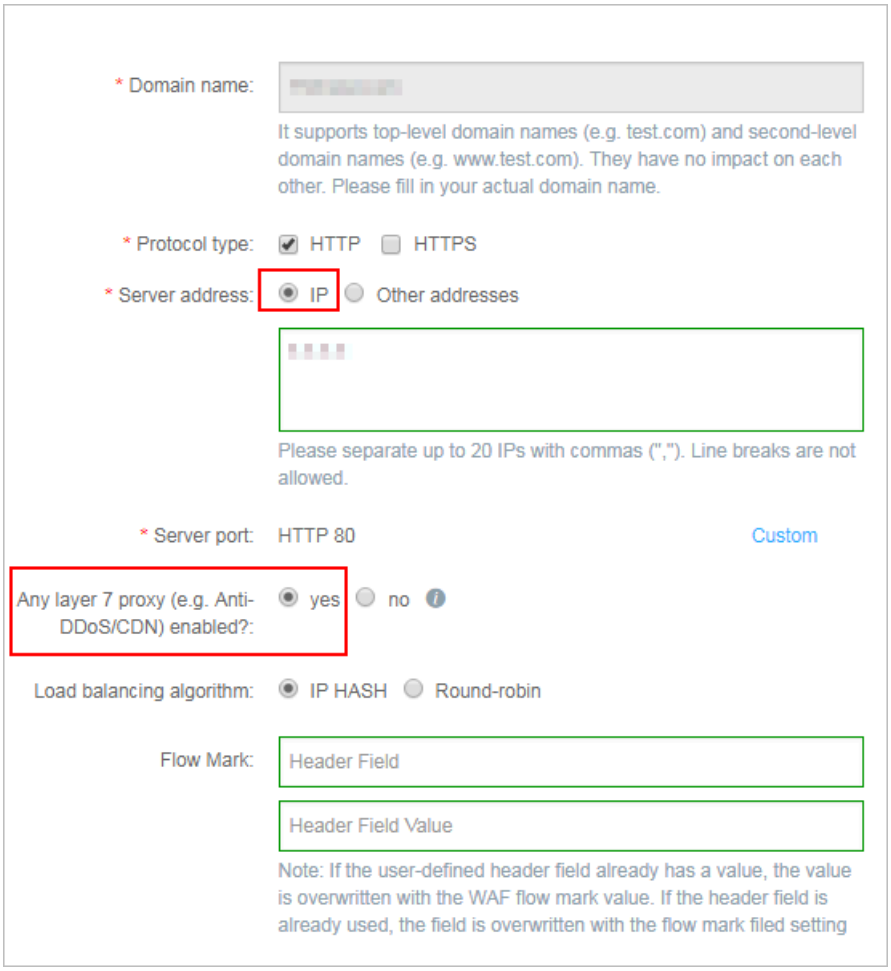
手順

Alibaba Cloud CDN を使用するとします。 次の手順に従って、WAF と CDN を一緒にデプロイします。

1. 「Alibaba Cloud CDN の使用の開始」を参照して、ドメイン名に CDN を実装します。

2. Alibaba Cloud WAF で Web サイト設定を作成します。
   - ドメイン名 : CDN で使用可能なドメイン名を入力します。 ワイルドカードがサポートされています。
   - サーバー アドレス : ECS および Server Load Balancer インスタンスのパブリック IP アドレスまたは配信元サーバーの外部サーバーの IP アドレスを入力します。
   - レイヤー 7 プロキシ (たとえば、Anti-DDoS/CDN) が有効になっているものがありますか？で [はい]をオンにします。

   詳細は、「Web サイト設定」をご参照ください。



3. Web サイト設定が正常に作成されると、WAF は専用の CNAME アドレスを生成します。

> 注 :
> WAF CNAME アドレスの表示方法の詳細は、 「WAF デプロイメントガイド」をご参照ください。

4. CDN 設定を変更して、配信元サイトアドレスを WAF CNAME アドレスに変更します。

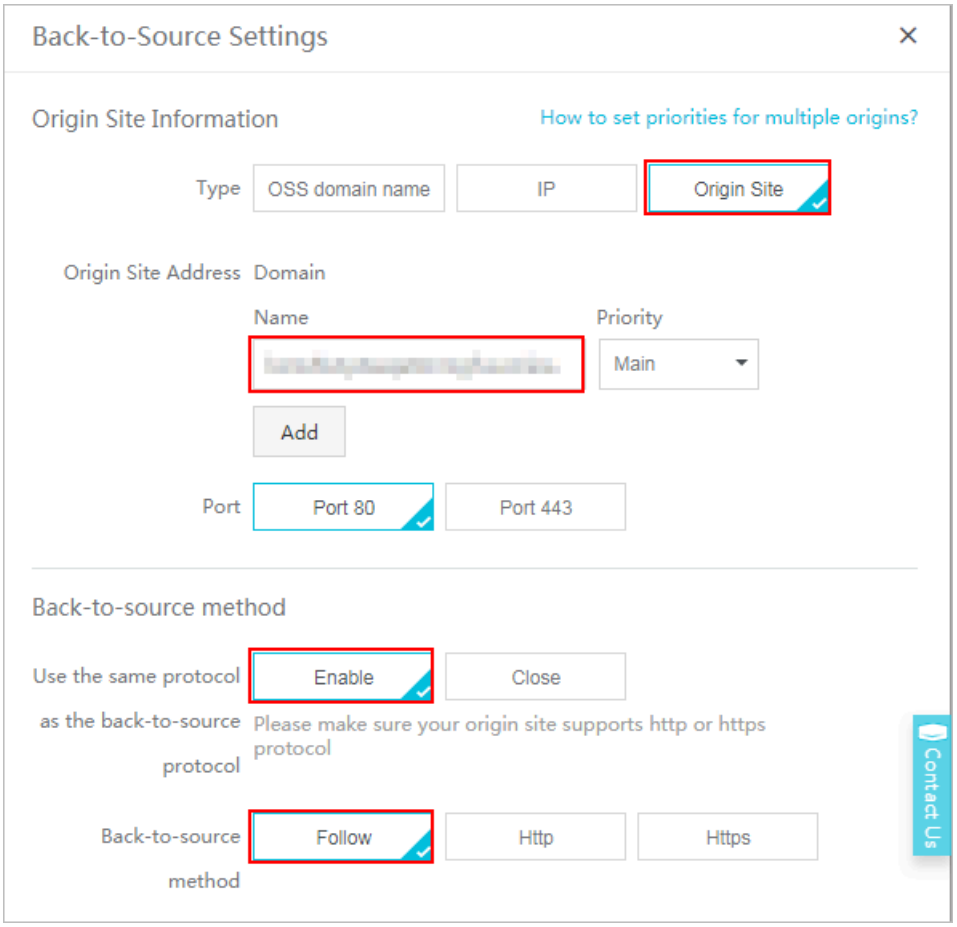
   a. Alibaba Cloud CDN コンソールにログインします。

   b. ドメイン名ページに移動し、設定するドメインを選択して [設定]をクリックします。

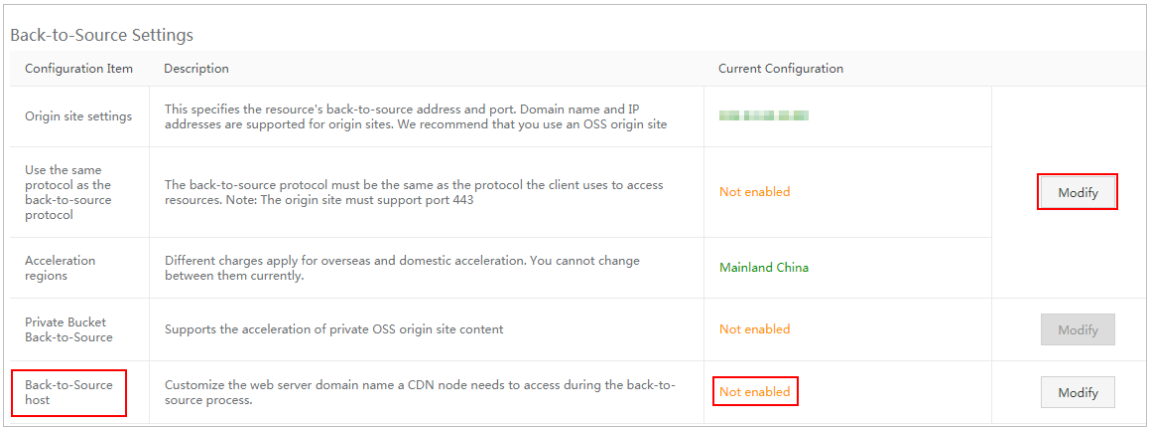
   c. 配信元サイト設定の下の [変更]をクリックします。

   d. 配信元サイト情報を変更します。

      - タイプ : [配信元サイト]をクリックします。
      - 配信元サイトアドレス IP : WAF CNAME アドレスを入力します。
      - back-to-source プロトコルと同じプロトコルを使用 : [有効] をクリックします。



   e. Back-to-Source 設定の下で、Back-to-Source ホストが無効になっていることを確認します。



操作が完了すると、トラフィックは CDN を通過し、動的コンテンツは引き続き WAF によってチェックおよび保護されます。

3 保護設定

3.1 Web アプリケーション保護

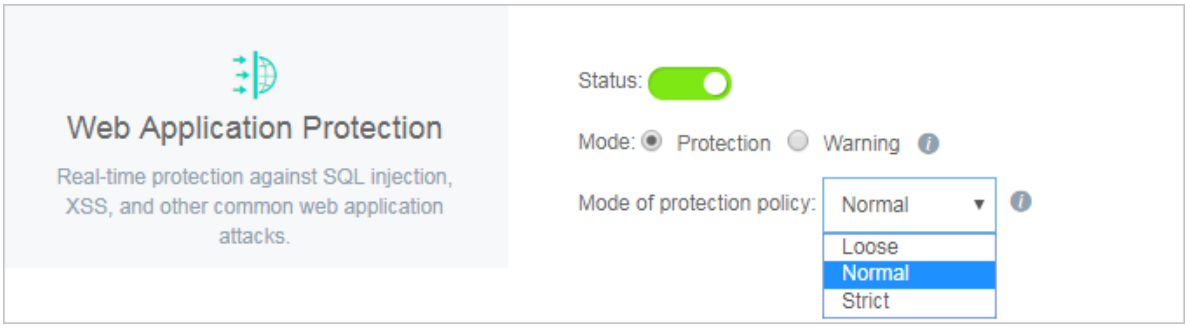
Alibaba Cloud WAF は、SQL インジェクションや XSS クロスサイト攻撃などの一般的な Web アプリケーション攻撃から Web リソースを保護します。 実際のニーズに合わせて、緩い、標準、厳しいなどの保護レベルを選択できます。

ドメインを WAF 保護リストに追加したら、それに対する Web アプリケーション保護を有効にし、実際のニーズに基づいていつでも適切な保護ポリシーを選択します。 Web アプリケーション保護機能を使用しない場合は、無効にします。

次の操作に進む前に、ドメインが WAF 保護リストに追加されていることを確認します。 詳細は、「WAF デプロイメントガイド」をご参照ください。

1. Alibaba Cloud WAF コンソールにログインします。
2. [管理] > [Web サイト設定]ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー]をクリックします。
4. [Web アプリケーション保護]を有効にし、[モード]をオンにします。

> 注 :
> この機能を使用しない場合は、このページで無効にします。



- 保護 : 攻撃が検出されるとリクエストはブロックされます。
- 警告 : 攻撃が検出されると警告が出されます。リクエストをブロックするかどうかは、ユーザーが判断します。

5. [保護ポリシーモード]ドロップダウンボックスで、保護ポリシーを選択します。
   - デフォルトでは、通常 モードが選択されています。
   - 通常モードで多くの誤検知や制御できないユーザー入力 (リッチテキストエディターやテクノロジフォーラムなど) が見つかるときは、 緩い モードを有効にします。
   - パストラバーサル、SQL インジェクション、およびコマンド実行攻撃に対するより厳しい保護が必要な場合は、厳しい モードを有効にします。

3.2 新しいインテリジェント保護エンジン

新しいインテリジェント保護エンジンは、リクエストのセマンティック分析を行います。 セマンティック検出を使用すると、エンジンは Web リクエスト内の偽装または隠された悪意のあるコンテンツを検出し、難読化コード、亜種などの方法を使用した悪意ある攻撃を効果的に遮断します。

機能説明

新しいインテリジェント保護エンジンは、リクエストのセマンティック分析を行い、セマンティック分析結果を例外および攻撃セットと照合して、偽装されたり隠された Web 攻撃の動作を検出します。

> 注 :
> 新しいインテリジェント保護エンジンは、HTTP フラッド攻撃ではなく、主に SQL インジェクションやその他の Web 攻撃方法から保護します。 Web 攻撃に対する保護要件が高い場合は、新しいインテリジェント保護エンジンを有効にすることを推奨します。

新しいインテリジェント保護エンジンには、次の機能があります。

- セマンティクス: 新しいインテリジェント保護エンジンは、類似する攻撃の類似する動作特性をまとめ、1 つの攻撃クラスの攻撃動作と特性を攻撃特徴として集約します。攻撃の複数の動作特性を特定の配列と組み合わせにグループ化して、個々の攻撃クラスを表すことで、攻撃動作のセマンティック構造を作成します。
- 例外と攻撃セット: Alibaba Cloud Security の大量の運用データを利用して、この機能は正常な Web アプリケーションのモデルを作り、異常を検出します。 大量の Web アプリケーション攻撃から例外モデルと攻撃モデルを抽出して、例外と攻撃のセットを形成します。

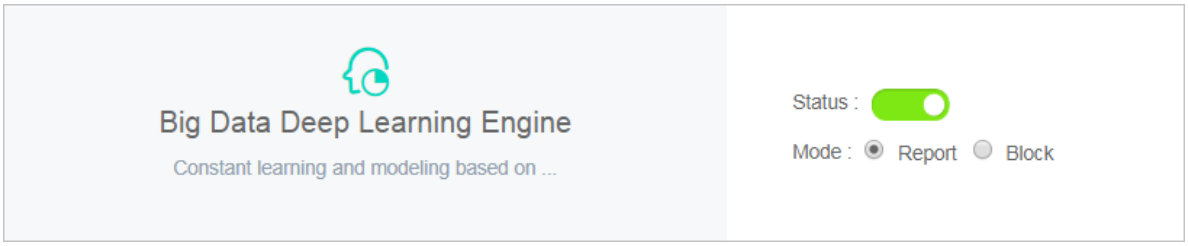
手順

次の手順に従って、新しいインテリジェント保護エンジンを有効にします。

注：
次の操作に進む前に、ドメインが WAF 保護リストに追加されていることを確認します。 詳細は、「WAF デプロイメントガイド」をご参照ください。

1. Alibaba Cloud WAF コンソールにログインします。
2. [管理] > [Web サイト設定] ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー] をクリックします。
4. [新しいインテリジェント保護エンジン] を有効にします。

注：
この機能を使用しない場合は、このページで無効にします。



3.3 HTTP フラッド保護

HTTP フラッド保護は、Web サイトに対する HTTP フラッド攻撃をブロックするのに役立ちます。

機能説明

HTTP フラッド保護は、さまざまなモード (通常モードや緊急モードなど) で HTTP フラッド攻撃をブロックするのに役立ちます。 Web サイトを WAF 保護リストに追加した後、HTTP フラッド保護を有効にし、Web サイトに適した保護モードを選択できます。 Business エディションおよび Enterprise エディションは、高度な HTTP フラッド保護をサポートしています。 詳細は、「よくある質問」をご参照ください。

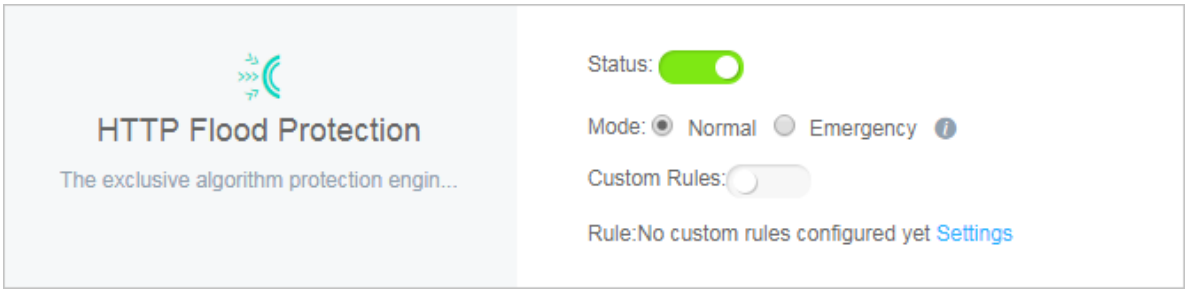
注：
緊急モードは Web ページには適用できますが、API またはネイティブアプリには適用できません。誤検知が多数発生する可能性があるためです。 API またはネイティブアプリの場合は、#unique_43を使用します。

手順

次の手順に従って、HTTP フラッド保護を設定します。

> 注：
> 次の操作に進む前に、ドメインが WAF 保護リストに追加されていることを確認します。 詳細は、「WAF デプロイメントガイド」をご参照ください。

1. Alibaba Cloud WAF コンソールにログインします。
2. [管理] > [Web サイト設定]ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー]をクリックします。
4. HTTP フラッド保護を有効にし、保護モードを選択します。



- 通常: デフォルトで使用されます。通常モードでは、非常に疑わしいリクエストのみをブロックし、誤検知の量は比較的少ないです。 誤検知を避けるため、Web サイトへの明らかなトラフィックの例外がない場合は、このモードを使用することを推奨します。
- 緊急: 通常モードで多くの HTTP フラッド攻撃がブロックされていない場合は、緊急モードに切り替えます。 緊急モードでは、WAF は HTTP フラッド攻撃に対して厳格な検査ルールを課しますが、誤検知を引き起こす可能性があります。

> 注：
> - 緊急モードでもまだ多くの攻撃が見逃されている場合は、ソース IP アドレスが WAF の Back-to-Source IP アドレスであるかどうかを確認します。 配信元が直接攻撃された場合は、「配信元サーバーの保護」を参照して、WAF の Back-to-Source IP アドレスのみがサーバーにアクセスできるようにします。
> - 保護効果を高め、誤検知率を下げるために、Business エディションまたは Enterprise エディションを使用してカスタマイズするか、セキュリティエキスパートに Web サイトの保護アルゴリズムのカスタマイズを依頼します。

よくある質問

さまざまな WAF エディションの HTTP フラッド保護機能の違いは何ですか。

WAF は、複雑な HTTP フラッド攻撃に対する保護能力に基づいて分類されています。

- Pro エディション: デフォルトの保護モード (通常と緊急) をサポートし、明らかな攻撃特性を持つ HTTP フラッド攻撃をブロックします。
- Business エディション: カスタムアクセス制御ルールをサポートし、特定の攻撃特性を持つ HTTP フラッド攻撃から保護します。 詳細は、「#unique_43」をご参照ください。
- Enterprise エディション: セキュリティエキスパートがカスタマイズした保護ルールを提供して、強固な保護効果を保証します。

WAF のアップグレード方法の詳細については、「更新とアップグレード」をご参照ください。

特定の HTTP フラッド攻撃から保護するために WAF を Business エディションにアップグレードする必要があるのはなぜですか。

Alibaba Cloud WAF は、人物の識別、ビッグデータ分析、モデル分析などの手法を使用して攻撃を識別し、それに応じて攻撃をブロックします。 プログラムのやり取りとは異なり、セキュリティの攻撃と保護は人同士の対立です。 Web サイトにはそれぞれ独自のパフォーマンスボトルネックがあります。 ハッカーは、効果のない攻撃であることがわかると、Web サイトを分析し、その後で標的型攻撃を開始する可能性があります。 この場合、Alibaba Cloud Security のエキスパートは攻撃を分析して、より高いレベルの保護とより優れた保護効果を提供します。

3.4 カスタム HTTP フラッド保護

Alibaba Cloud WAF の Business エディションと Enterprise エディションは、HTTP フラッド保護ルールのカスタマイズをサポートして、レートベースのアクセス制御を適用しています。

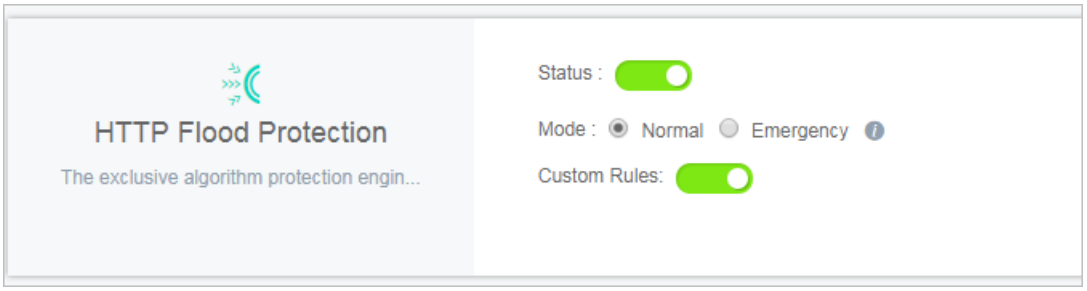
コンソールでカスタム保護ルールを適用することで、サーバーにアクセスする特定の URL の頻度を制限することができます。 たとえば、次のルールを定義します。1 つの送信元 IP アドレスが `www . yourdomain . com / login . html` に 10 秒以内に 20 回を超えてアクセスする場合、この IP アドレスを 1 時間ブロックします。

この機能を使用するには、WAF を Business Edition または Enterprise Edition にアップグレードする必要があります。 詳細は、「更新とアップグレード」をご参照ください。

次の操作に進む前に、ドメインが WAF 保護リストに追加されていることを確認します。 詳細は、「WAF デプロイメントガイド」をご参照ください。

1. Alibaba Cloud WAF コンソールにログインします。

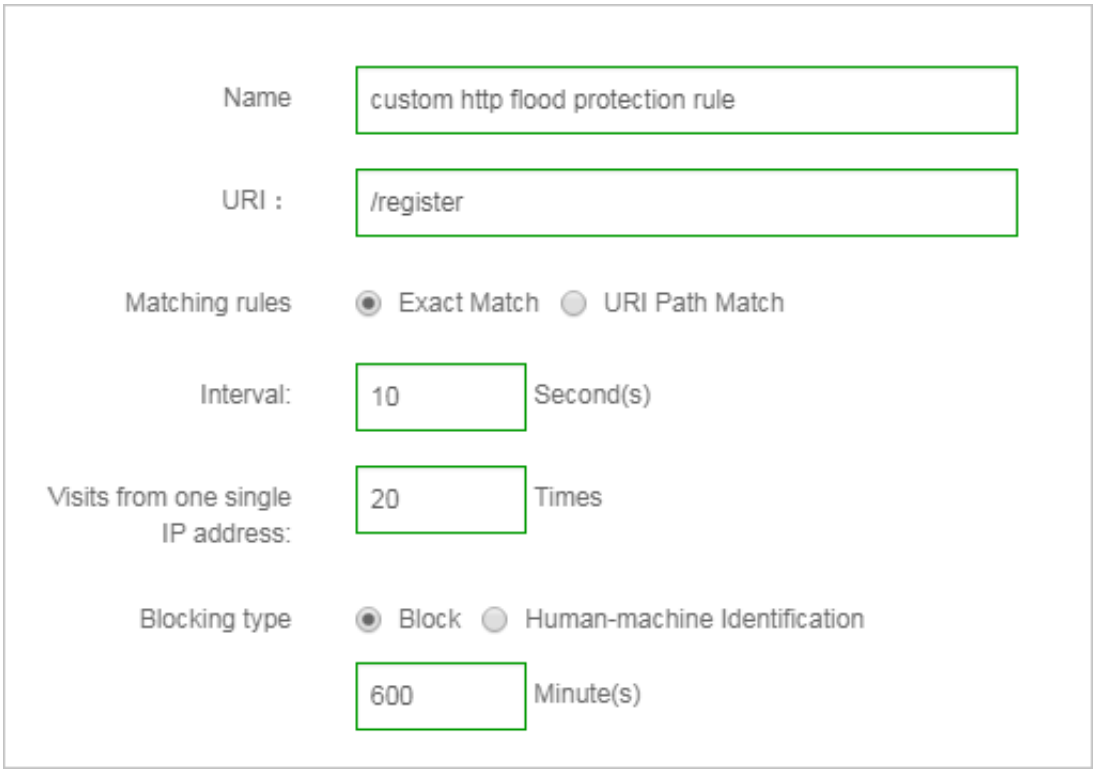
2. [管理] > [Web サイト設定] ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー] をクリックします。
4. HTTP フラッド保護 (通常モード) とカスタムルールを有効にし、[設定] をクリックします。



5. [新しいルール] をクリックしてルールを追加します。 パラメーターは次のとおりです。

設定	説明
名前	このルールの名前。
URI	保護される URI パス。 たとえば、`/ register` です。 パスには "?" でつないだパラメーターが含まれます。 たとえば、`/ user ? action = login` を使用します。
一致ルール	・ 完全一致: リクエスト URI は、ここでカウントされる設定 URI と完全に同じである必要があります。 ・ URI パス一致: リクエスト URI がここで設定した URI 値で始まる場合に、リクエストがカウントされます。 たとえば、URIとして `/ register` を使用した場合、`/ register . html` がカウントされます。
間隔	訪問数を計算するためのサイクル。 1 つの IP アドレスからの訪問数と同期して機能します。
1 つの IP アドレスからの訪問数	サイクル間隔中に 1 つの送信元 IP アドレスから URL への許可された訪問数。

設定	説明
ブロックタイプ	条件を満たすと実行されるアクション。 操作はブロックまたはヒューマンマシン識別のいずれかです。 ・ ブロック: 条件を満たすと、クライアントからのアクセスをブロックします。 ・ マンマシン識別: 条件を満たすと、リダイレクトによってクライアントにアクセスします。 検証されたリクエストのみ配信元に転送されます。



上図の設定の場合、1 つの IP アドレスは 10 秒間に 20 回を超えてターゲットアドレスにアクセスでき (完全一致)、その後 IP は 600 分間ブロックされます。

WAF はクラスター内の複数のサーバーからデータを収集して単一の IP からのアクセス頻度を計算するため、統計処理にはある程度の遅延が生じることがあります。

ルールが正常に追加された後、ルールを編集または削除できます。

3.5 HTTP ACL ポリシー

HTTP ACL ポリシーを使用して、アクセス制御ルールをカスタマイズし、クライアント IP、リクエスト URL、および一般的に使用される HTTP フィールドによって HTTP リクエストをフィルターします。

機能説明

HTTP ACL ポリシーは、HTTP アクセス制御のカスタマイズをサポートしており、IP、URL、リファラー、UA、パラメーターなど、一般的に使用される HTTP フィールドの基準の組み合わせに基づいて HTTP リクエストをフィルターします。 この機能は、アンチリーチや Web サイト管理コンソールの保護など、さまざまな業務シナリオに適用します。

HTTP ACL ポリシールール

HTTP ACL ポリシールールはそれぞれ、一致条件とアクションで構成されています。 ルールを作成する場合、一致フィールド、論理演算子、および対応する一致コンテンツを設定して一致条件を定義し、一致する場合にトリガーされるアクションを選択します。

一致条件

一致条件は、一致フィールド、論理演算子、および一致コンテンツで構成されています。 一致コンテンツは正規表現の説明をサポートしていませんが、null 値に設定することは可能です。

次の表は、HTTP ACL ポリシールールでサポートされているすべての一致フィールドの一覧です。

注 :

WAF Pro インスタンスの場合、IP、URL、リファラー、ユーザーエージェントのみが一致フィールドでサポートされ、各ドメイン名に対して最大 20 個のルールが許可されます。 WAF Business または Enterprise インスタンスの場合、リストされる一致フィールドはすべてサポートされ、各ドメイン名にそれぞれ最大 100 個または 200 個のルールを定義できます。

一致フィールド	説明	サポートされる論理演算子
IP	クライアント IP アドレス。	· Has · Does not have
URL	リクエストされる URL	· Includes · Does not include · Equals to · Does not equal to

Referer	現在のリクエストページへのリンクがある、以前の Web ページのアドレス。	· Includes · Does not include · Equals to · Does not equal to · Length less than · Length equals · Length more than · Does not exist
User-Agent	クライアントのブラウザーに関する情報を識別するユーザーエージェント文字列。	· Includes · Does not include · Equals to · Does not equal to · Length less than · Length equals · Length more than
Params	"?" の後から始まるリクエスト URL のパラメーター。 たとえば、URL `www . abc . com / index . html ? action = login` のパラメーターは、 `action = login` です。	· Includes · Does not include · Equals to · Does not equal to · Length less than · Length equals · Length more than
Cookie	リクエスト URL 内の Cookie。	· Includes · Does not include · Equals to · Does not equal to · Length less than · Length equals · engths more than · Does not exist

Content-Type	リクエストの本文のメディアタイプ (POST および PUT リクエストで使用されます)。	· Includes · Does not include · Equals to · Does not equal to · Length less than · Length equals · Length more than
X-Forwarded-For	リクエスト URL 内の x-forward-for フィールド。 X-Forwarded-For (XFF) は、HTTP プロキシまたはロードバランサーを介して Web サーバーに接続しているクライアントの元の IP アドレスを識別します。	· Includes · Does not include · Equals to · Does not equal to · Length less than · Length equals · Length more than · Does not exist
Content-Length	オクテット (8 ビットバイト) でのリクエスト本文の長さ	· Value less than · Value equals · Value more than
Post-Body	リクエストのレスポンスコンテンツ。	· Includes · Does not include · Equals to · Does not equal to
Http-Method	GET、POST などのリクエストメソッド。	· Equals to · Does not equal to
Header	カスタマイズされたヘッダーフィールド。	· Includes · Does not include · Equals to · Does not equal to · Length less than · Length equals · Length more than · Does not exist

> 注:
> ルールはそれぞれ、最大 3 つの条件の組み合わせを許可します。 ルール内の複数の条件は "AND" でつなぎます。つまり、リクエストはルールに一致するように条件をすべて満たす必要があります。

アクション

ルールが一致した後に、以下のアクションを実行します。

- ブロック: 条件に一致するリクエストをブロックします。
- 許可: 条件に一致するリクエストを許可します。
- 警告: 条件に一致するリクエストを許可し、アラームをトリガーします。

> 注:
> 許可または警告を指定すると、Web アプリケーション保護、HTTP フラッド保護、新しいインテリジェント保護、リージョンブロック、およびデータリスク管理の実行に進むかどうかをさらに判断します。

ルールの並べ替え

一致ルールは特定の順序に従います。 上位のルールが最初に一致します。

ルールの順序を調整して最適な保護パフォーマンスを実現します。

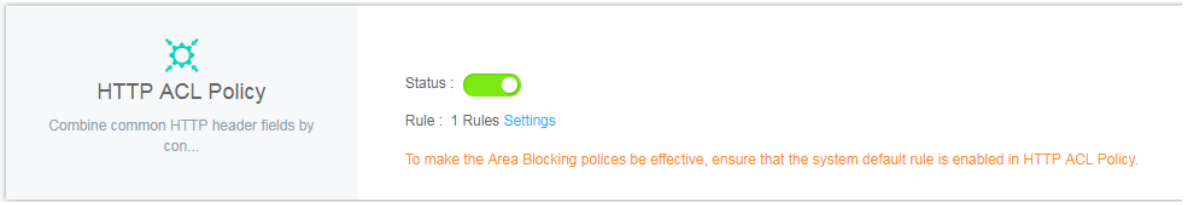
手順

これらの手順に従って、保護ドメイン名の HTTP ACL ポリシールールを追加します。

> 注:
> 次の操作を実行する前に、保護用 WAF にドメインが追加されていることを確認します。 詳細は、「WAF デプロイメントガイド」をご参照ください。

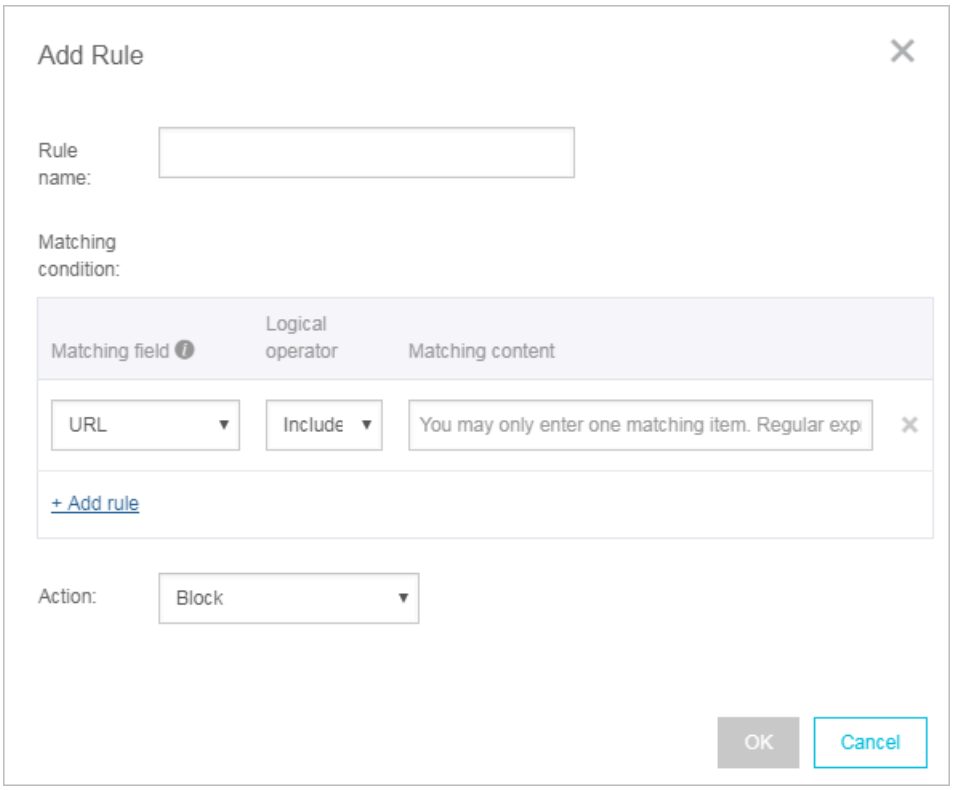
1. Alibaba Cloud WAF コンソールにログインします。
2. [管理] > [Web サイト設定]] ページに移動し、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー] をクリックします。

4. [HTTP ACL ポリシー] を有効にし、[設定]をクリックします。



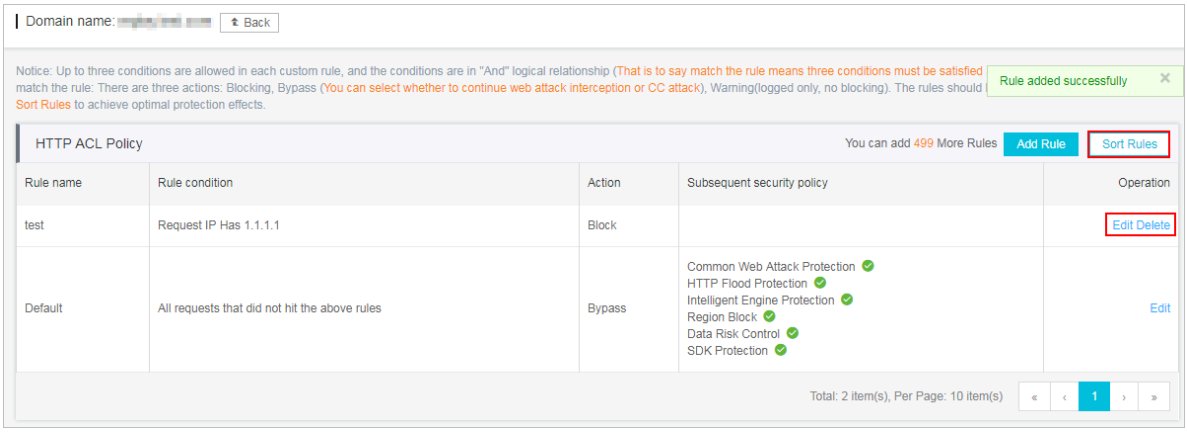
5. [ルールの追加] をクリックし、目的のルールを設定して [OK] をクリックします。

> **注：**
> 設定の詳細については、「HTTP ACL ポリシールール」をご参照ください。 設定例の詳細については、「設定例」をご参照ください。



6. 作成したルールについては、そのコンテンツを編集 するか、またはそれを 削除します。 複数のルールを作成している場合は、[ルールの並べ替え] をクリックして、それらのデフォルトの

順序を変更します。 [上に移動]、[下に移動]、[一番上に移動]、および[一番下に移動] を使用して、最初に一致するルールを決定します。



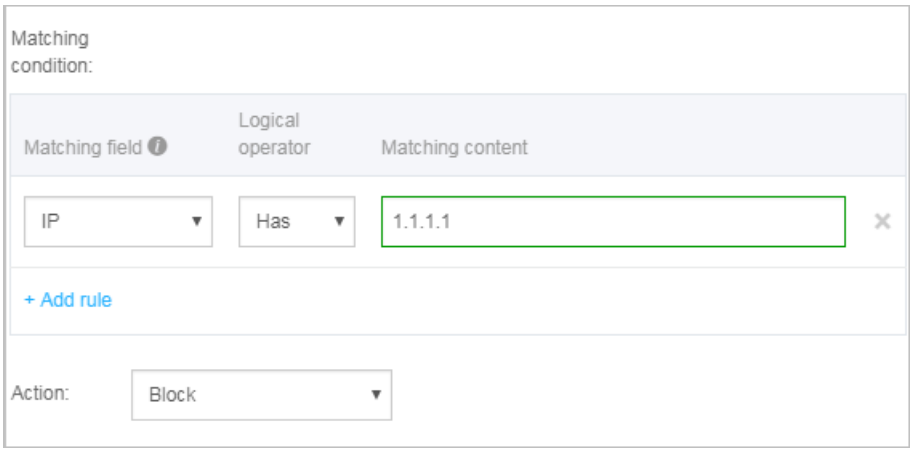
設定例

HTTP ACL ポリシーはさまざまな設定方法をサポートします。 業務特性に基づいて最良のルールを実現します。 HTTP ACL ポリシーを使用して特定の Web 脆弱性を修正することも可能です。

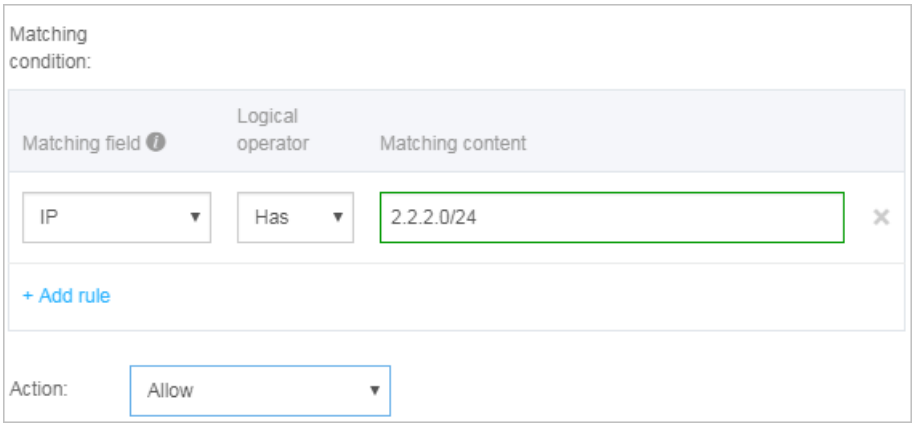
以下に例をいくつか示します。

IP ブラックリストとホワイトリストの設定

次の設定を使用して 1.1.1.1 からのアクセスをすべてブロックします。



次の設定を使用して 2.2.2.0/24 からのアクセスをすべて許可します。



注：

[Web アプリケーション攻撃保護の実行] も [HTTP フラッド攻撃保護の実行] もオンにしてはいけません。

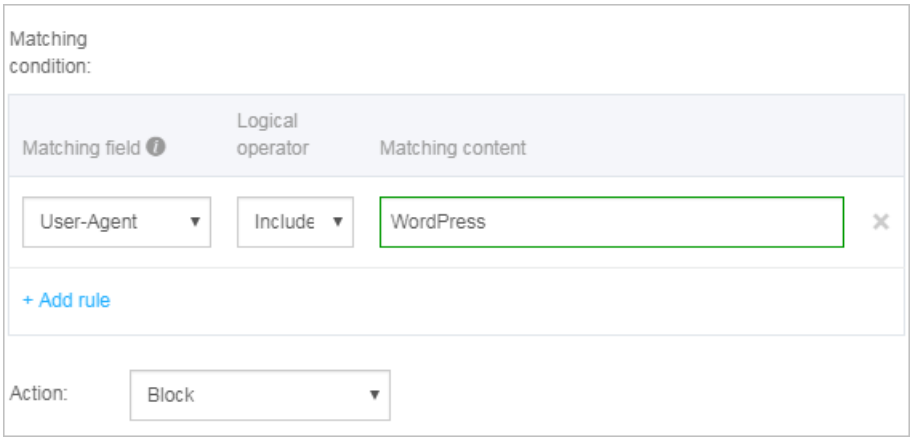
詳細は、「IP ホワイトリストとブラックリストのセットアップ」をご参照ください。

悪意のあるリクエストのブロック

次の図は、WordPress バウンス攻撃の例を示しています。UA に WordPress が含まれてることが特徴です。

UA
WordPress/4.2.10; http://ascsolutions.vn; verifying pingback from 191.96.249.54
WordPress/4.0.1; http://146.148.63.90; verifying pingback from 191.96.249.54
WordPress/4.6.1; https://www.nokhostinsabt.com; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://eadastage.lib.umd.edu; verifying pingback from 191.96.249.54
WordPress/3.5.1; http://danieljromo.com
WordPress/4.2.4; http://wd.icopy.net.tw; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://kmgproje.com; verifying pingback from 191.96.249.54
WordPress/4.1.6; http://www.vv-atalanta.nl; verifying pingback from 191.96.249.54
WordPress/4.5; http://23.83.236.52; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://playadelrey.news; verifying pingback from 191.96.249.54
WordPress/4.1; http://hostclick.us; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://mosaics.pro; verifying pingback from 191.96.249.54
WordPress/4.0; http://www.chinavrheadset.com; verifying pingback from 191.96.249.54

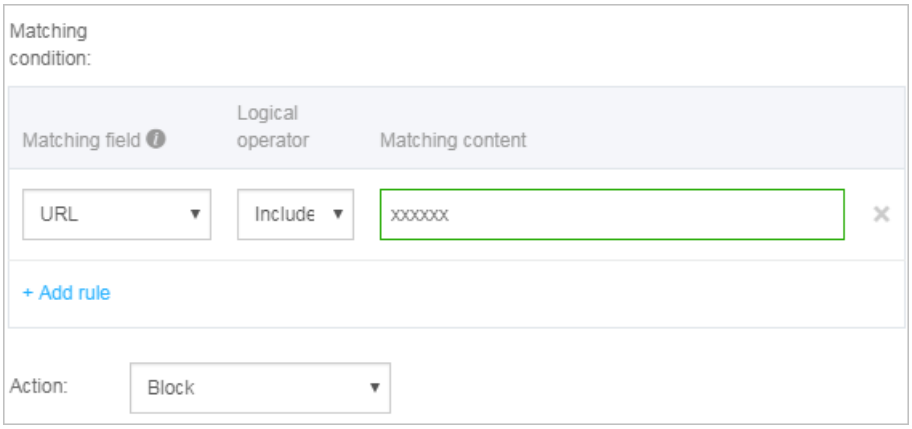
以下の設定を使用して、この種の攻撃を防御します。



詳細は、「WordPress のピンバック攻撃の防止」をご参照ください。

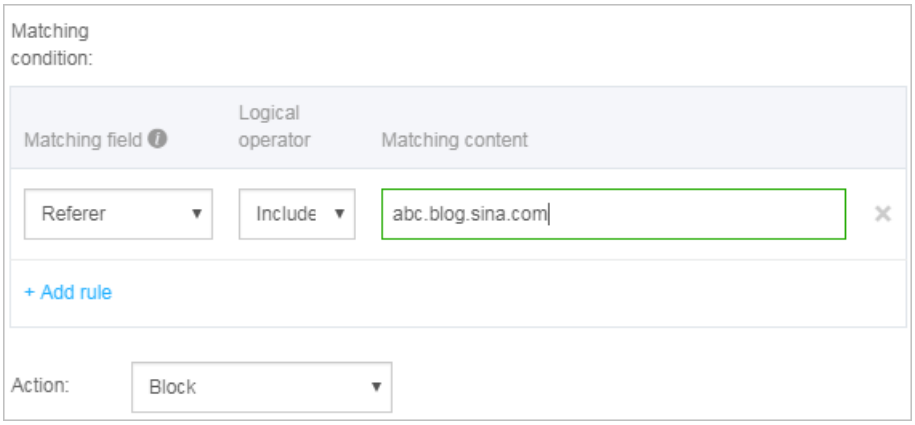
特定の URL のブロック

多数の IP アドレスで特定の存在しない URL を必要としている場合は、次の設定を使用します。



アンチリーチ

リファラーベースのアクセス条件を設定します。 たとえば、 *abc . blog . sina . com* がサイトで大量の写真を使用していると分かった場合は、次の設定を使用します。



3.6 ブロックリージョン

この機能を使用して、中国本土、香港、マカオ、台湾、および世界中の最大 247 か国の特定の地域をリージョンブラックリストに追加します。 指定した地域からのリクエストはすべてブロックされます。

ブロックリージョン機能を有効にするには、WAF を Enterprise エディション以上にアップグレードする必要があります。 アップグレードの詳細については、「更新とアップグレード」をご参照ください。

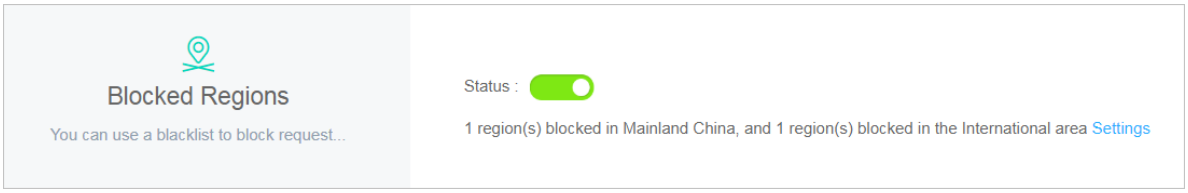
ブロックリージョンを有効にし、指定するには、次の手順を実行します。

> 注：
> ターゲットドメインが保護用 WAF に追加されていることを確認します。 詳細は、「CNAME アクセスガイド」をご参照ください。

1. Web Application Firewall コンソールにログインします。

2. [管理] > [Web サイト設定]ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー] をクリックします。
4. [ブロックリージョン] オプションを有効にします。

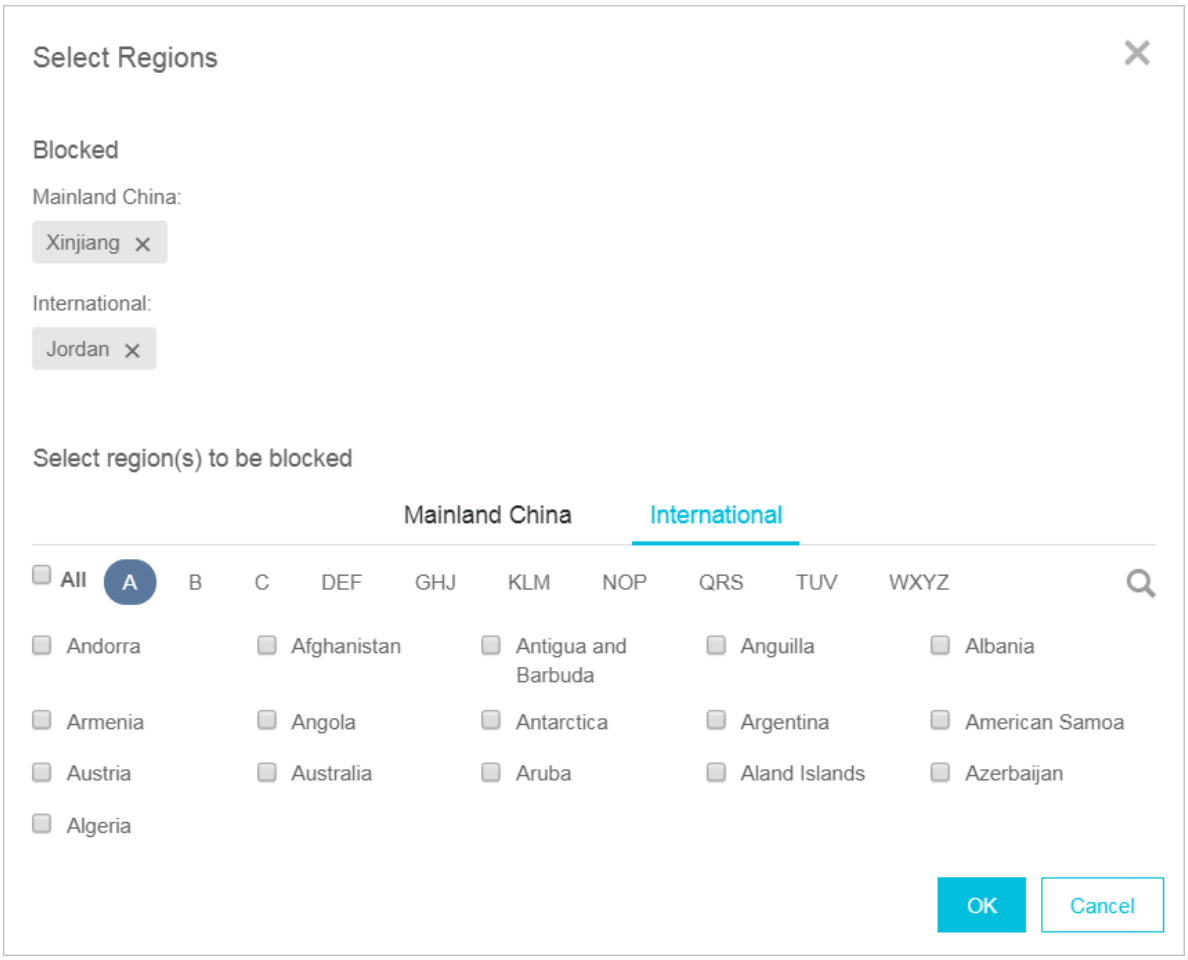
> 注：
> 地域ブロックポリシーを有効にするには、HTTP ACL ポリシーでシステムのデフォルトルールが有効になっていることを確認します。



5. [設定] をクリックし、[中国本土] または [国際] スコープを選択し、ブロックする地域を選択します。 [OK] をクリックします。

> 注：

[国際] スコープを選択した場合、国名の頭文字またはクイック検索で国や地域をすばやく見つけられます。



設定確認後、ブロックされた地域の IP アドレスからのリクエストはすべて WAF によってブロックされます。

注：
IP の送信元地域情報は、Alibaba Taobao IP アドレスライブラリに基づいています。

3.7 ホワイトリストまたはブラックリストの設定

WAF の HTTP ACL ポリシーを設定することで、ホワイトリストやブラックリストを設定することができます。 ホワイトリストとブラックリストは、HTTP ACL ポリシーが設定されている特定のドメインでのみ有効です。

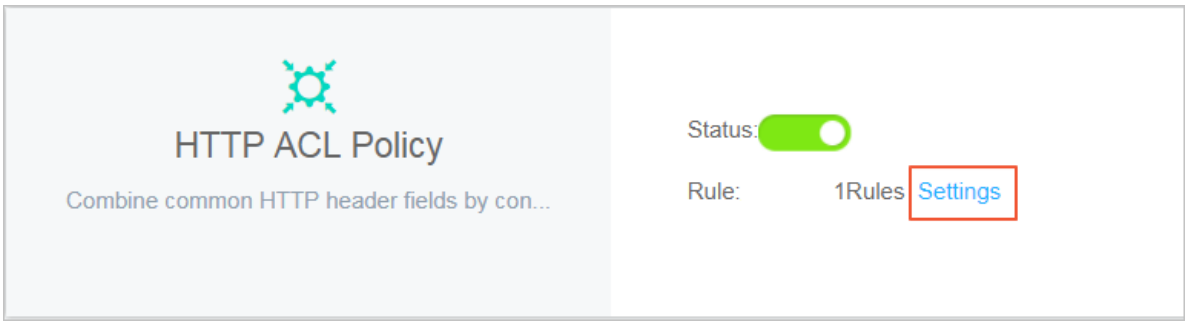
手順

次の手順に従って、ホワイトリストまたはブラックリストを設定します。

注：

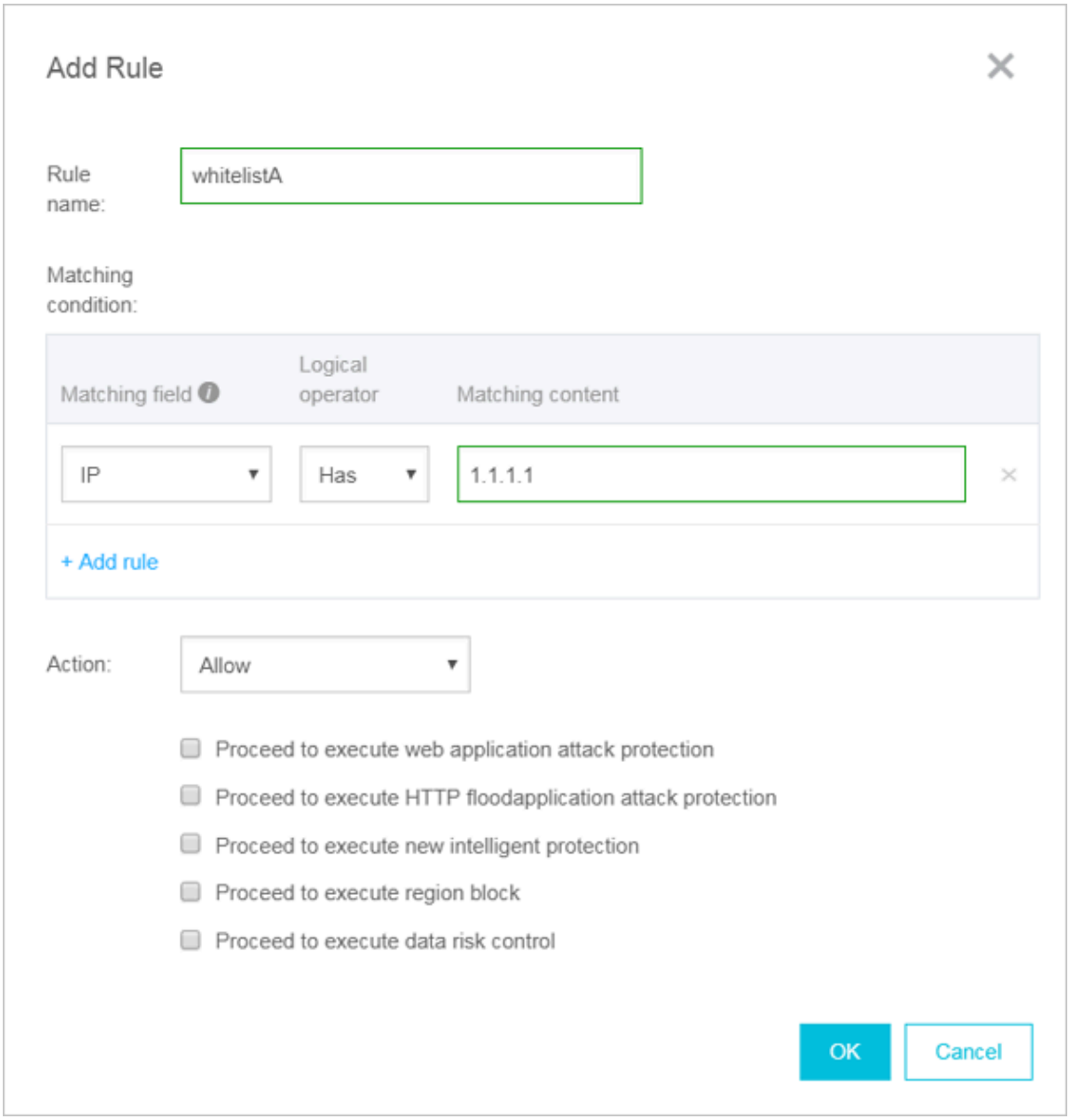
次の操作に進む前に、ドメインが WAF 保護リストに追加されていることを確認します。 詳細は、「WAF デプロイメントガイド」をご参照ください。

1. Alibaba Cloud WAF コンソールにログインします。
2. [管理] > [Web サイト設定] ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー] をクリックします。
4. HTTP ACL ポリシー を有効にし、[設定] をクリックします。



5. [ルールの追加] をクリックします。

   - ホワイトリストの設定例。 次の設定では、IP 1.1.1.1 からのリクエストをすべて許可します。



> **注 :**
> この IP からのリクエストをすべて許可する場合は、[ルールの追加] ダイアログボックスで "〜に進む" の保護オプションを選択しないでください。 保護オプションが選択されている場合、この IP からのリクエストがブロックされたままになることがあります。

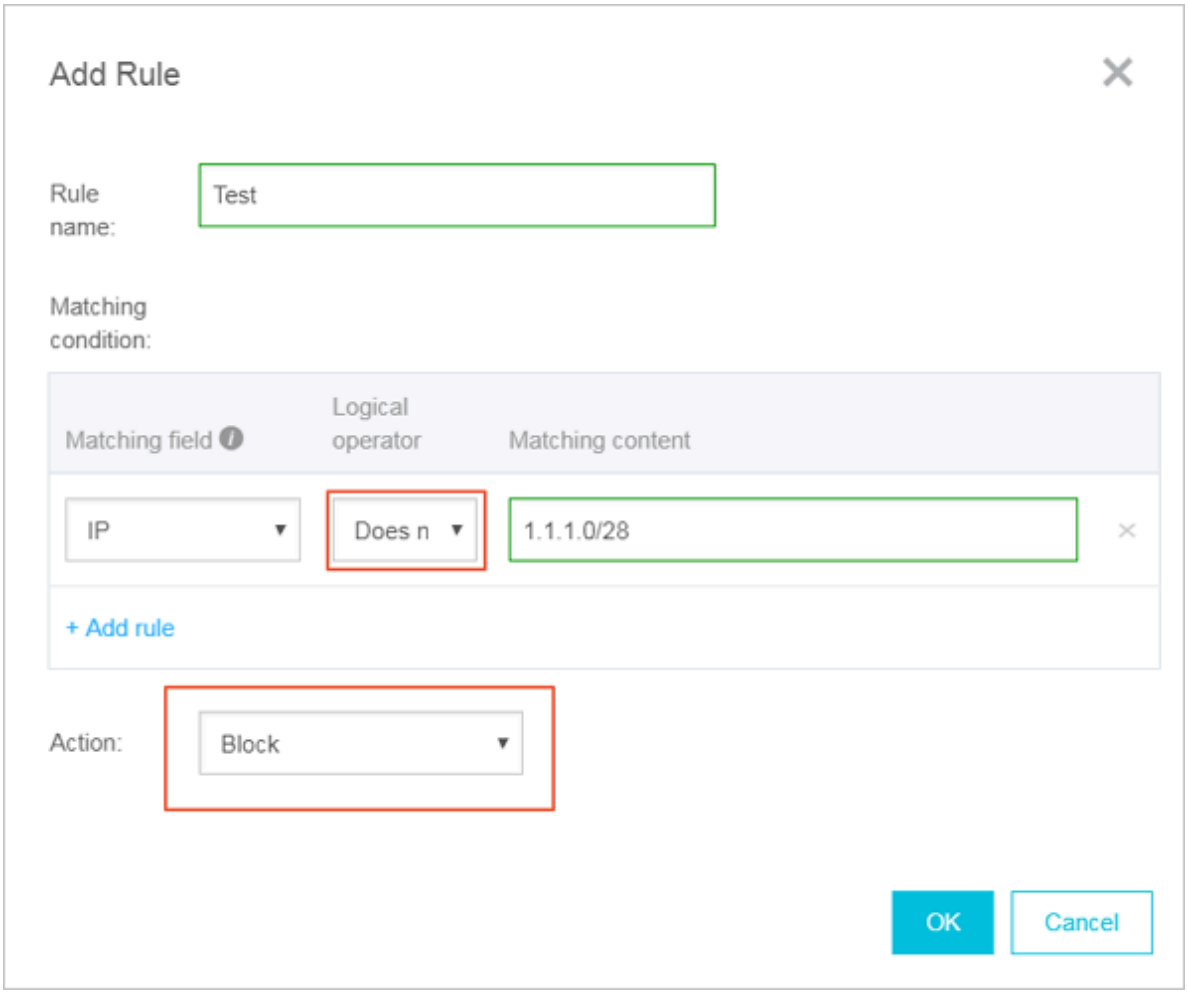
   - 同様に、この手順に従って特定のドメイン用ブラックリストを設定することも可能です。

注

- 1 つのルールで最大 3 つの一致条件をサポートします。 ルールをトリガーするには、ルール内の条件がすべて一致する必要があります。 複数の個別 IP アドレスまたは IP セグメントをホワイトリストやブラックリストに登録する場合は、複数の HTTP ACL ルールを設定する必要があります。 たとえば、1.1.1.1、2.2.2.2、および 3.3.3.3 からのアクセスリクエストをブロックするには、3 つのルールを別々に設定する必要があります。

Rule name	Rule condition	Action
blacklistC	RequestIP Has 3.3.3.3	Block
blacklistA	RequestIP Has 1.1.1.1	Block
blacklistB	RequestIP Has 2.2.2.2	Block

- HTTP ACL ルールにファイルされた IP 照合はマスク形式 (たとえば、1.1.1.0/24) をサポートし、論理演算子は "なし" をサポートします。 たとえば、次の設定を使用して、特定の IP セグメントから 1 つのドメインへのリクエストのみ許可します。



- 複数の HTTP ACL ルール間に優先順位があります。 WAF は、HTTP ACL ポリシーリストに表示される HTTP ACL ルールの順序 (上から下) に従って HTTP ACL ルールを適用します。また、[ルールの並べ替え] をクリックして HTTP ACL ルール間の優先順位を変更します。

3.8 Web サイト改ざん防止

Web サイト改ざん防止機能を使用して、機密コンテンツを含む特定のページをキャッシュします。 これらのページをキャッシュした後、WAF は、ソースコンテンツが改ざんされた場合に、事前にキャッシュしたコンテンツを訪問者に返し、確実にユーザーが正しいページを表示できるようにします。

Web サイト改ざん防止機能を使用するには、WAF Pro を Business または Enterprise エディションにアップグレードする必要があります。 操作の詳細については、「更新とアップグレード」をご参照ください。

次の手順に従って、Web サイト改ざん防止を有効にして設定します。

> 注 :
> 次の操作を実行する前に、保護対象の Web サイトが WAF に追加されていることを確認します。 操作の詳細については、「WAF デプロイメントガイド」をご参照ください。

1. Alibaba Cloud WAF コンソールにログインします。
2. [管理] > [Web サイト設定] ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー] をクリックします。
4. [Webサイト改ざん防止] を有効にしてから、[設定] をクリックします。

> 注 :
> 改ざん防止サービスが不要な場合は、このページで無効にします。

5. [新しいルール] をクリックし、[新しい URL の追加] ダイアログボックスで設定を完了します。

   - サービス名: ルールに名前を付けます。
   - URL: 保護する正確なパスを指定します。 ワイルドカード文字 (`/*` など) またはパラメーター (`/ abc ? xxx =`) はサポートされていません。 WAF はこのパス内のすべてのテキスト、HTML、および画像を保護します。

6. ルールを追加したら、[保護ステータス] でルールを手動で有効にします。 ルールを有効にしないと、設定は有効になりません。

7. 保護されたページを更新する場合は、[キャッシュの更新] をクリックしてキャッシュを更新する必要があります。 ページが更新された後、キャッシュを更新しない場合、WAF は常に最後にキャッシュされたページコンテンツを返します。

3.9 データ漏えい防止

データ漏えい防止機能により、Web Application Firewall (WAF) は、次のように規定している中国のサイバーセキュリティ法に準拠することが可能です。"ネットワーク事業者は、収集した個人情報のセキュリティを保証し、情報漏えい、損害、および損失を防止するための技術的措置およびその他必要な措置を講じなければならない。 個人情報の漏えい、損害、または損失が発生した場合、または発生する可能性がある場合には、関係するネットワーク事業者は直ちに改善策を講じ、ユーザーに適時通知し、規定に従って所轄官庁に報告しなければならない。"

機能説明

データ漏えい防止機能は、Web サイトでの機密情報の漏えい (特に携帯電話番号、ID カード番号、およびクレジットカード情報) と機密キーワードの漏えいに対する感度低下と警告対策を提供します。 指定した HTTP ステータスコードをブロックすることも可能です。

この機能を使用するには、WAF を Business または Enterprise エディションにアップグレードする必要があります。 詳細は、「更新とアップグレード」をご参照ください。

Web サイトが直面する一般的な情報漏えいは次のとおりです。

- Web サイト管理バックグラウンドへの不正アクセスなど、URL への不正アクセス。
- 水平方向の過剰アクセス権限の脆弱性や垂直方向の過剰アクセス権限の脆弱性など、過剰なアクセス権限の脆弱性。

・ Web ページ上の悪意のあるクローラーによってクロールされる機密情報。

データ漏えい防止機能では、次のタスクが行えます。

・ Web ページ上で生成した個人情報や機密データを検出して識別し、早期警告や機密情報シールドなどの保護手段を提供して、Web サイトの運用データ漏えいを防止します。 この機密データおよび個人データには、ID カード番号、携帯電話番号、および銀行カード番号などがあります。
・ Web サイトで使用される Web アプリケーションソフトウェア、オペレーティングシステム、およびバージョンをさらす可能性のある機密サーバー情報のワンクリックブロックをサポートして、機密サーバー情報の漏えいを防止します。
・ この機能は、組み込み型の違法で機密性の高いキーワードライブラリを使用して、警告、違法なキーワードシールド、およびその他の保護手段を備え、Web ページに表示される違法で機密性の高いキーワードに対処します。

利用シナリオ

データ漏えい防止機能は、応答ページに ID カード番号、携帯電話番号、キャッシュカード番号、および他の種類の機密情報があるかどうかを検出します。 機密情報の一致を検出した場合、警告を送信するか、または一致ルールに対して設定されているアクションに基づいて機密情報をフィルターします。 機密情報がフィルターされると、情報の機密部分がアスタリスク (*) に置き換えられ、保護されます。

データ漏えい防止機能は、`text /*`、`image /*`、および `applicatio n /*` などの コンテンツタイプをサポートし、Web 端末、アプリ端末、および API インターフェイスをカバーしています。

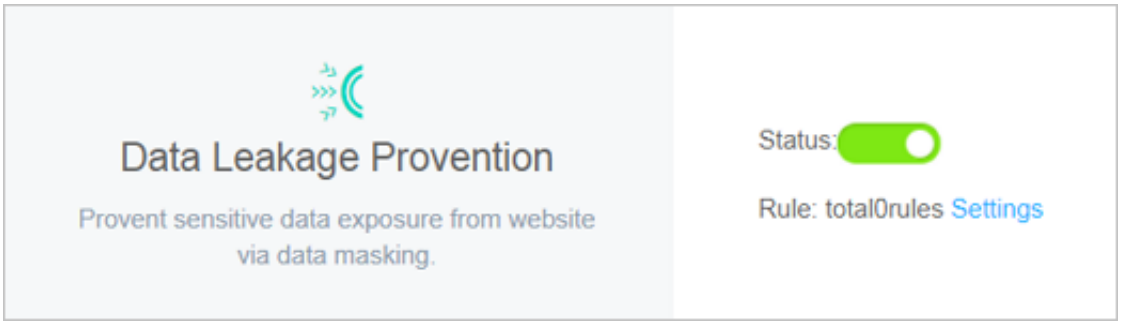
手順

次の手順に従って、データ漏えい防止を有効にして設定します。

 注 :
次の操作に進む前に、ドメインが WAF 保護リストに追加されていることを確認します。 詳細は「CNAME アクセスガイド」をご参照ください。

1. Web Application Firewall コンソールにログインします。
2. [管理] > [Web サイト設定] ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、[ポリシー] をクリックします。

4. [データ漏えい防止] 機能を有効にし、[設定] をクリックします。

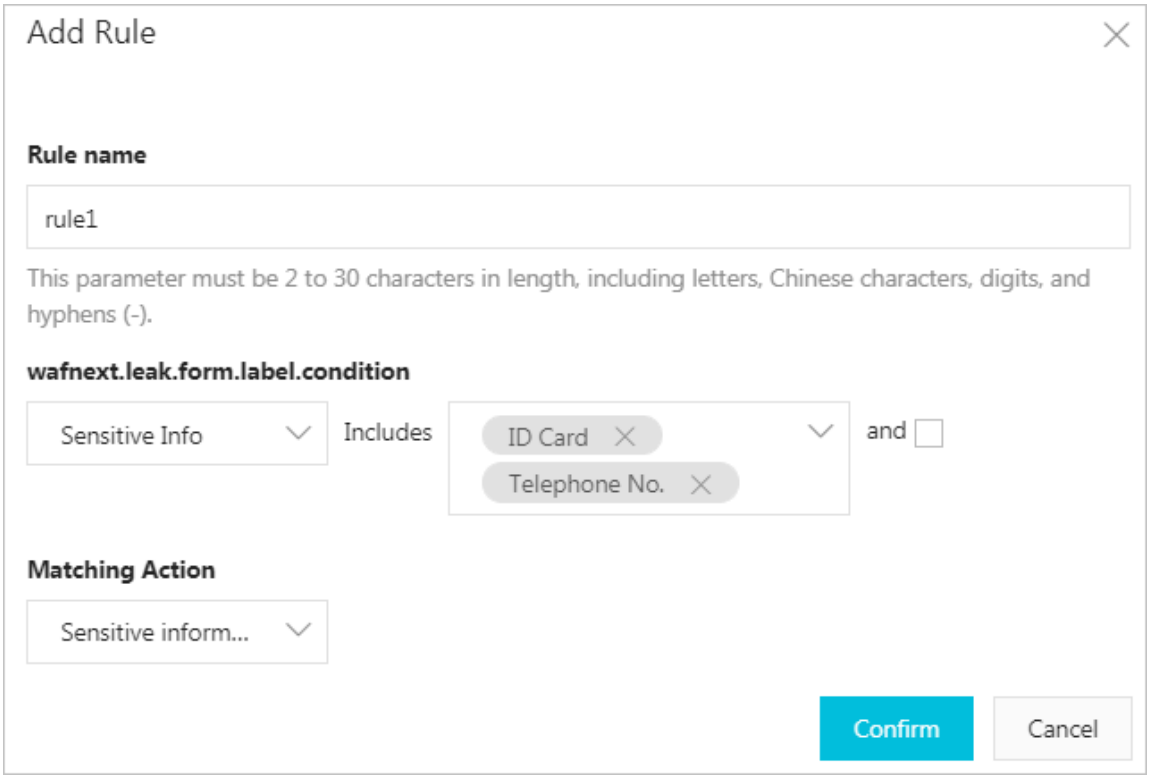


5. [ルールの追加] をクリックして機密情報保護ルールを追加します。

> 注：
> [ルールの追加] ダイアログボックスで、[追加] をクリックしてさらに URL 一致条件を追加します。

- 機密情報のマスク: 携帯電話番号、ID カード番号、およびその他の機密情報を表示する可能性のある Web ページの場合、関連ルールを設定してこの情報をマスクまたは警告し

ます。 たとえば、次の保護ルールを設定して、データマスクによって携帯電話番号と ID カード番号を保護します。

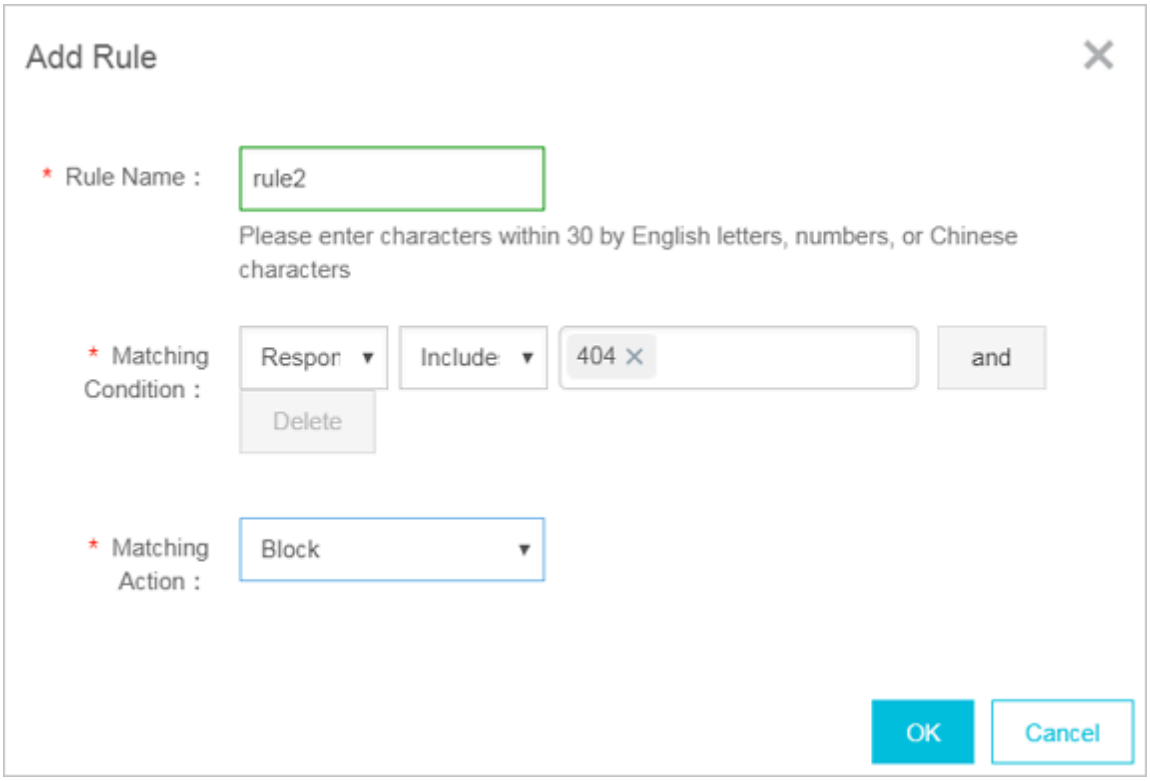


この保護ルールを設定すると、この Web サイトのすべての Web ページに表示される携帯電話番号と ID カード番号は自動的に暗くなります。

注 :

Web ページに業務連絡先電話番号、サポートホットライン番号、およびその他の一般に提供される携帯電話番号がある場合、これらも設定した携帯電話番号機密情報フィルタリングルールによって除外されることがあります。

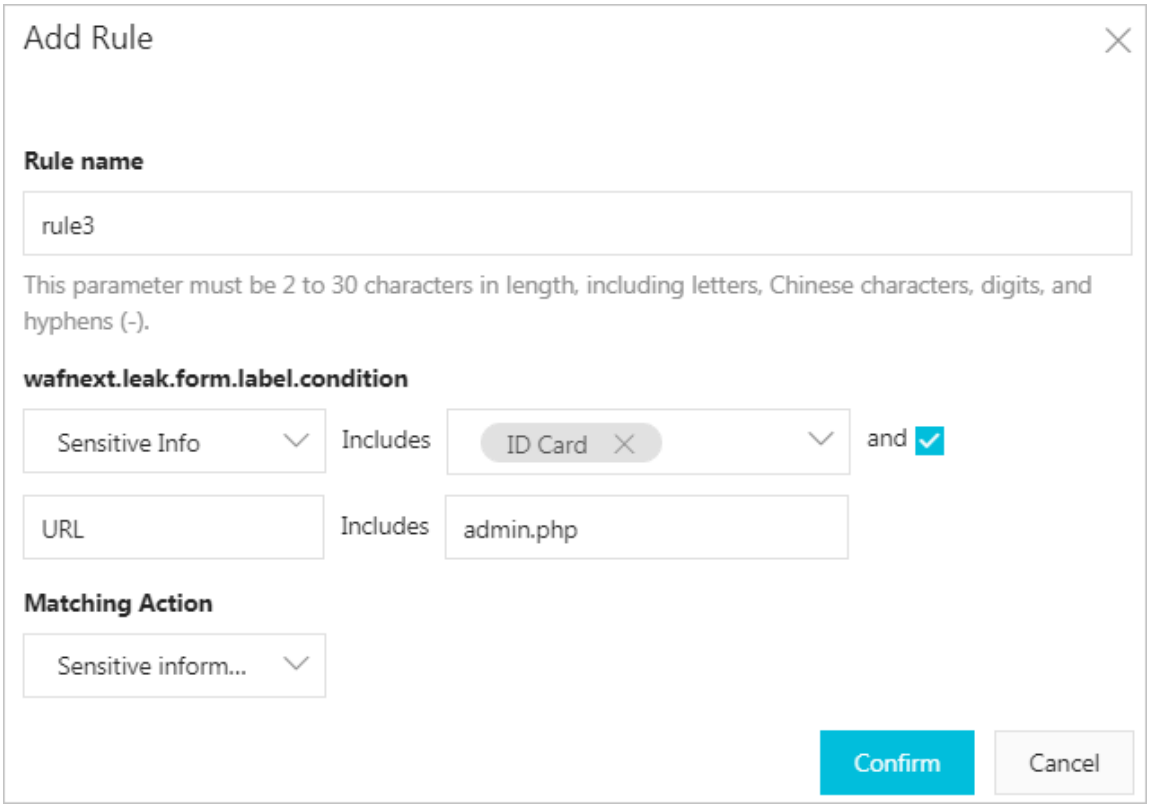
- ステータスコードブロック: 特定の HTTP リクエストステータスコードをブロックまたは警告するルールを設定して、機密サーバー情報の漏えいを防止します。 たとえば、次の保護ルールを設定して HTTP 404 ステータスコードをブロックします。



この保護ルールを設定すると、ユーザーがこの Web サイト配下に存在しないページをリクエストした場合に、指定されたページが返されます。

- 指定した URL の機密情報のフィルター: 携帯電話番号、ID カード番号、および他の機密情報を表示する可能性のある指定した Web ページ の URL の場合、関連ルールを設定してこ

の情報をフィルターまたは警告します。 たとえば、次の保護ルールを設定して、Web ページ admin.php 上で ID カード番号をフィルターします。



この保護ルールを設定すると、ID カード番号は admin.php Web ページ上で暗くなります。

6. 追加したルールについては、それを編集または削除することも可能です。

データ漏えい防止機能を有効にすると、Web Application Firewall コンソールにログインし、[レポート] > [攻撃保護] ページに移動して保護レポートを表示します。 このレポートによって、データ漏えい防止ルールで除外またはブロックされたアクセスリクエストのログを照会します。

4 保護レポート

4.1 Alibaba Cloud WAF レポートの概要

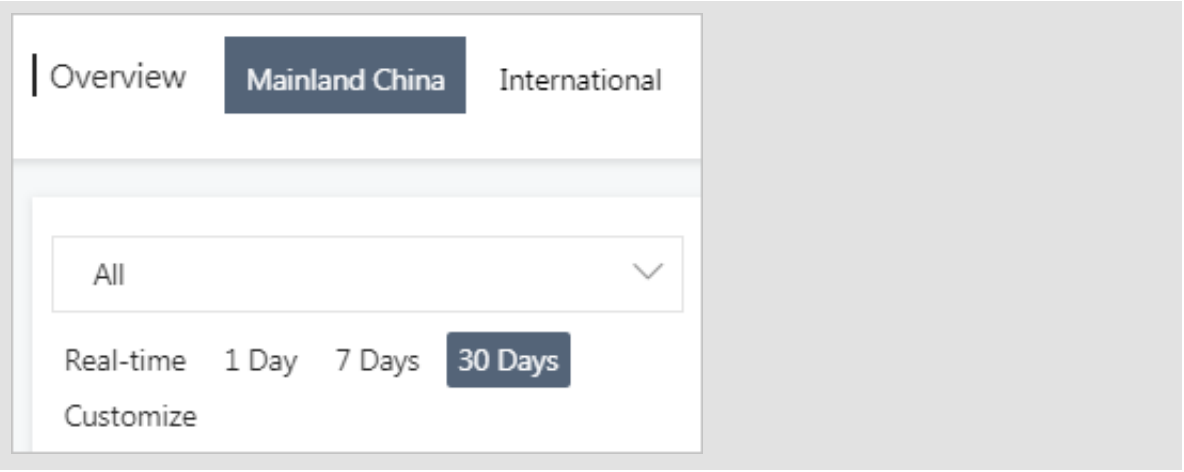
Alibaba Cloud WAF 概要ページには、業務概要とセキュリティ概要が両方表示されます。

業務概要の表示

次の手順に従って、業務概要ページを表示します。

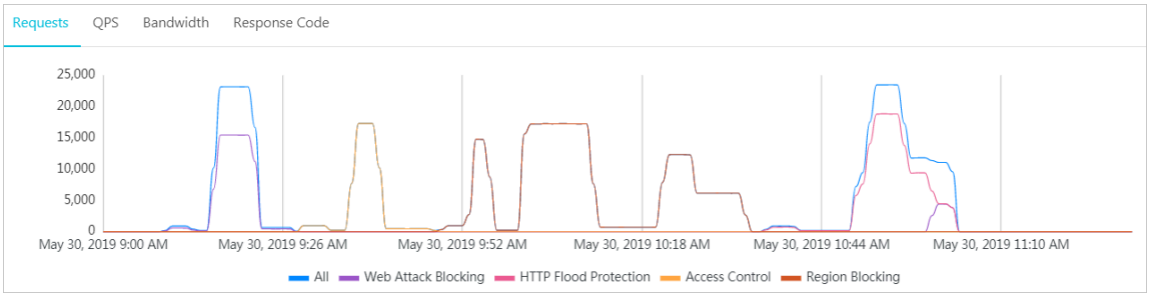
1. Web Application Firewall コンソールにログインします。
2. [レポート] > [概要] ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 業務サブページで表示するドメイン名と期間 (リアルタイム、6 時間、1 日、7 日、30 日、カスタマイズ) を 1 つまたはすべて選択します。

> 注 :
> 過去 30 日間の業務概要が表示されます。 カスタマイズ期間を設定して、過去 30 日間の指定期間の情報を表示することも可能です。

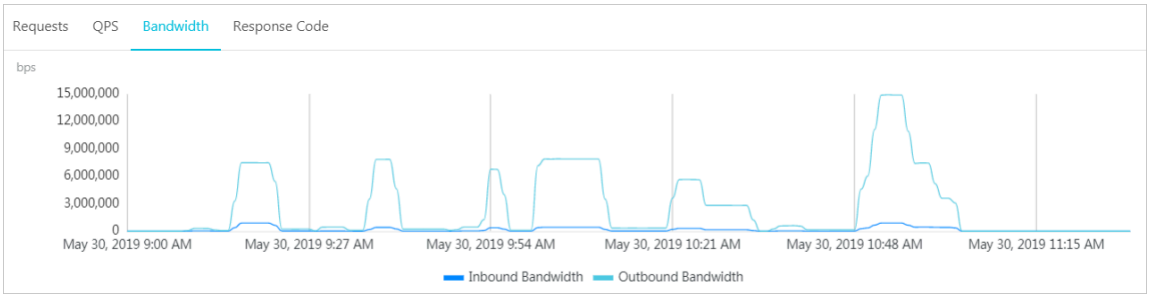


表示できる業務概要の情報は次のとおりです。

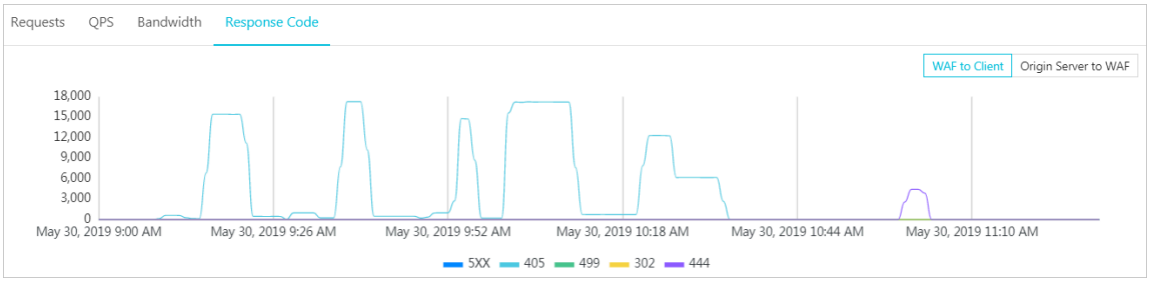
- QPS とブロックされた攻撃の数: 特定期間 (最小間隔: 1 分) の QPS、Web 攻撃、HTTP フラッド攻撃、HTTP ACL ヒット、およびデータリスク管理を表示します。 グラフの下のアイコンをクリックして、対応するレコードを消去またはグラフで表示します。



- 帯域幅: 特定期間 (最小間隔: 1 分) のインバウンドとアウトバウンドの帯域幅 (単位: ビット/秒) を表示します。 グラフの下のアイコンをクリックして、対応するレコードをキャンセルまたはグラフで表示します。

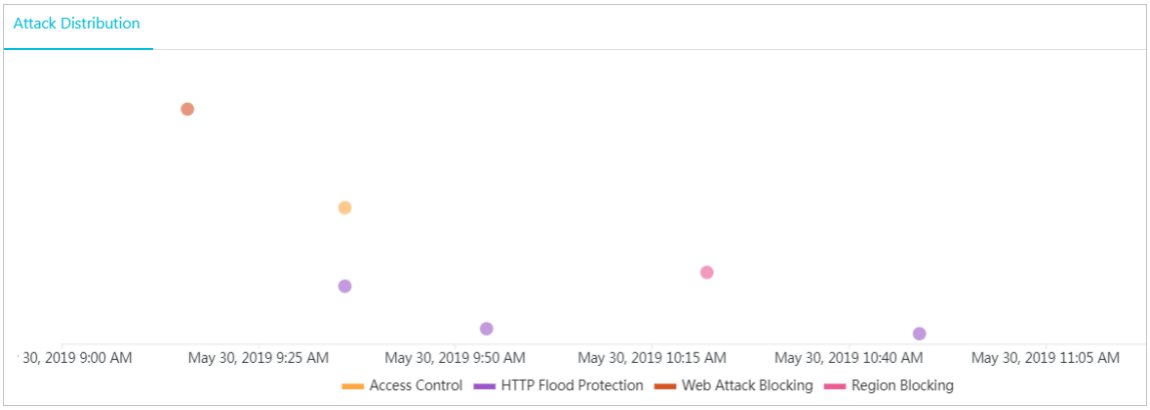


- 異常: 左側に特定期間 (最小間隔: 1 分) の異常な業務レコードを表示します。 異常な業務の分布も円グラフで表示します。 グラフの下のアイコンをクリックして、対応するレコードをキャンセルまたはグラフで表示します。

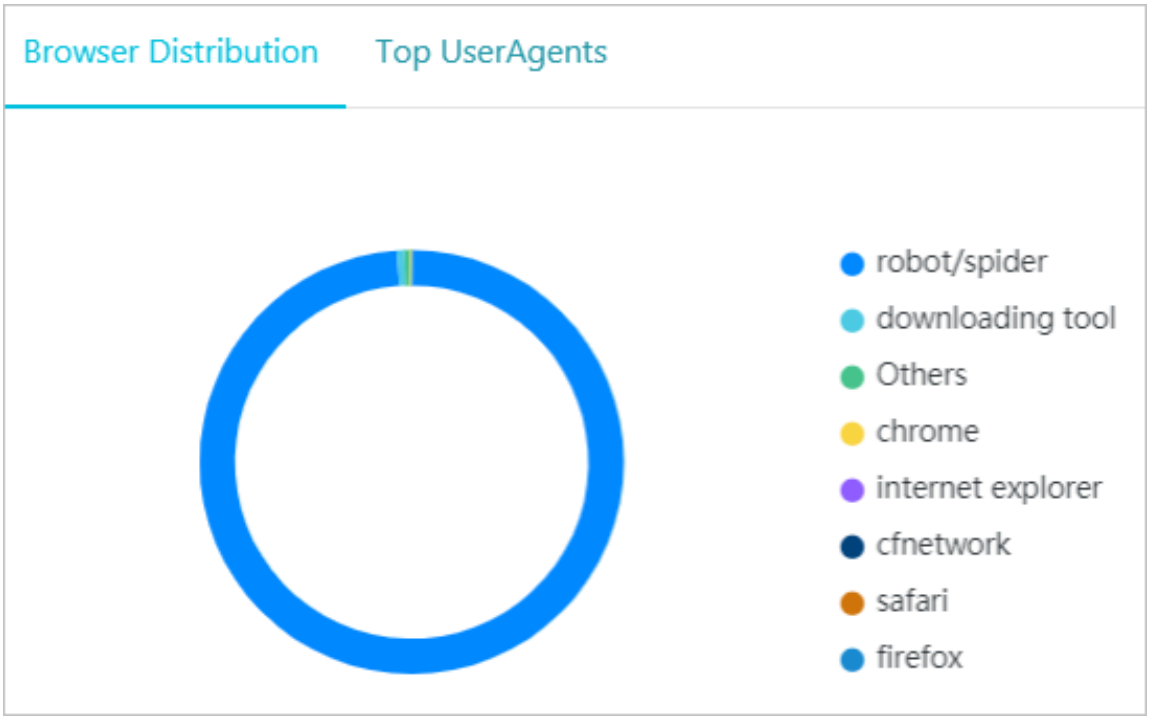


- リクエスト送信元リージョン、リクエスト送信元 IP: アクセス送信元の分布統計を表示します。 左側の棒グラフには、上位 5 つのアクセス送信元地域と上位 10 個のアクセス送信

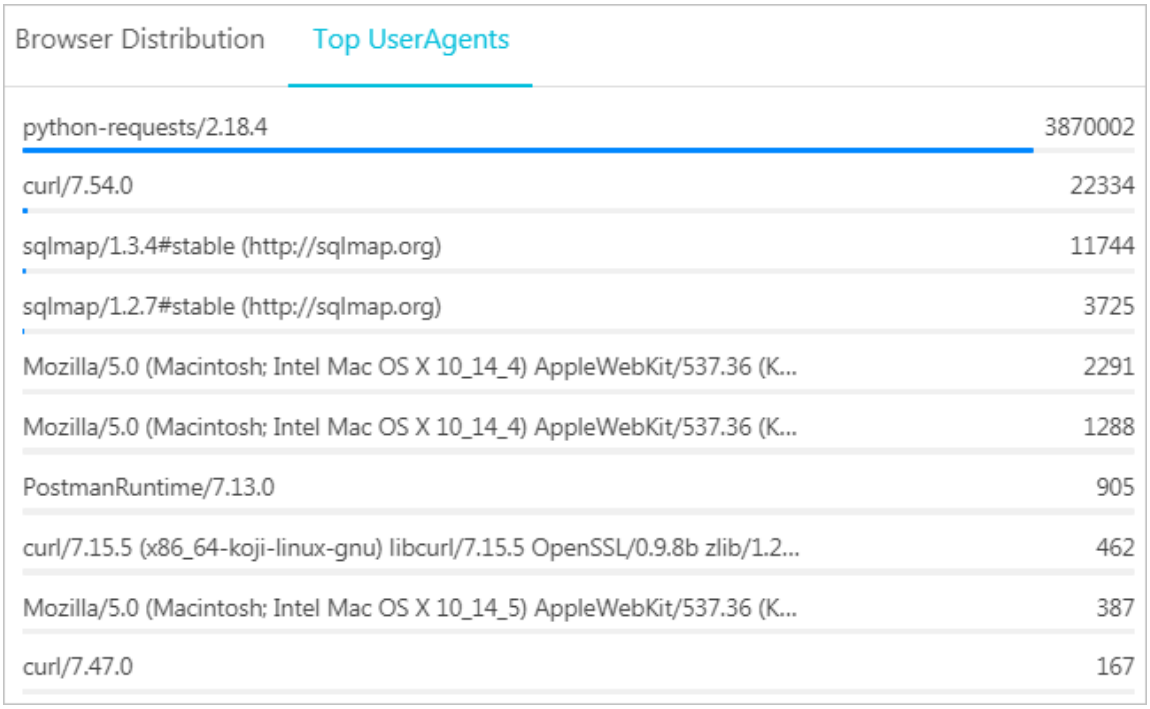
元 IP アドレスが表示されます。 右側のマップでは、対応するアクセス送信元が青いドットとして識別されます。 ドット上にマウスを置くと、特定のレコードをが表示します。



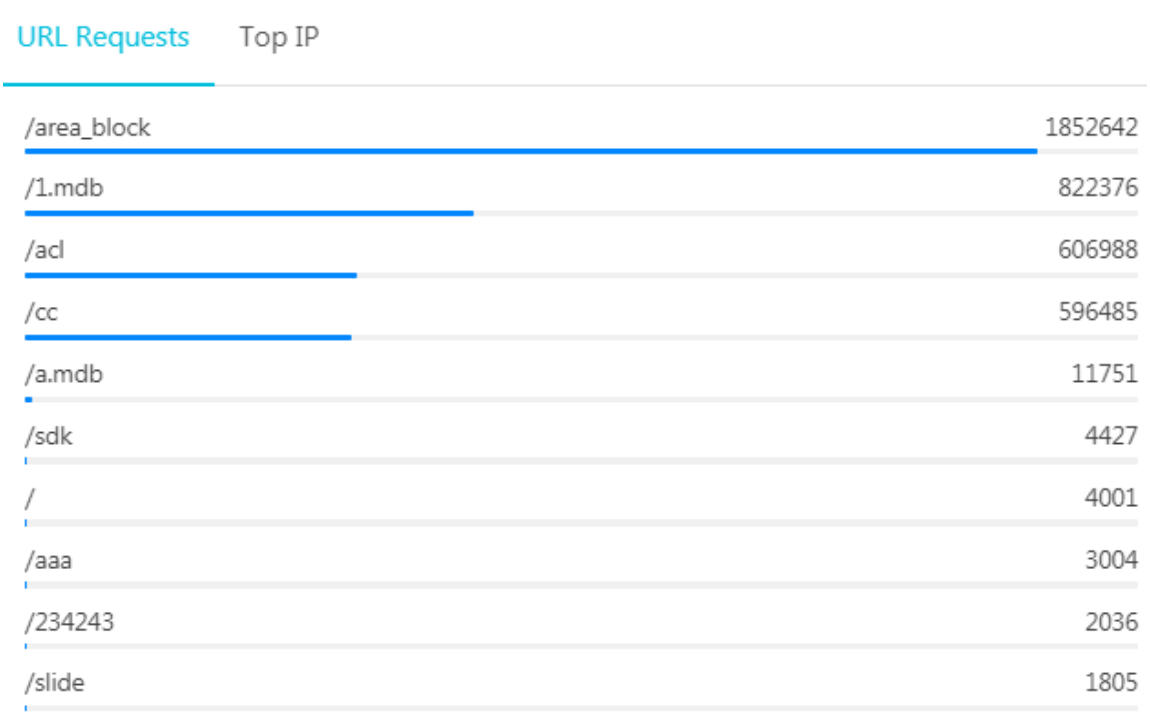
- アクセス送信元分布: モバイル OS と PC ブラウザーの分布を別々の円グラフで表示します。



- 応答時間順の上位 5 つの URL: 応答時間が最も長い上位 5 つの URL とその応答時間 (単位: ms) を一覧表示します。



- 最も頻繁にアクセスされた URL: 最も頻繁にアクセスされた上位 5 つの URL とそれらがアクセスされた回数を一覧表示します。



セキュリティ概要の表示

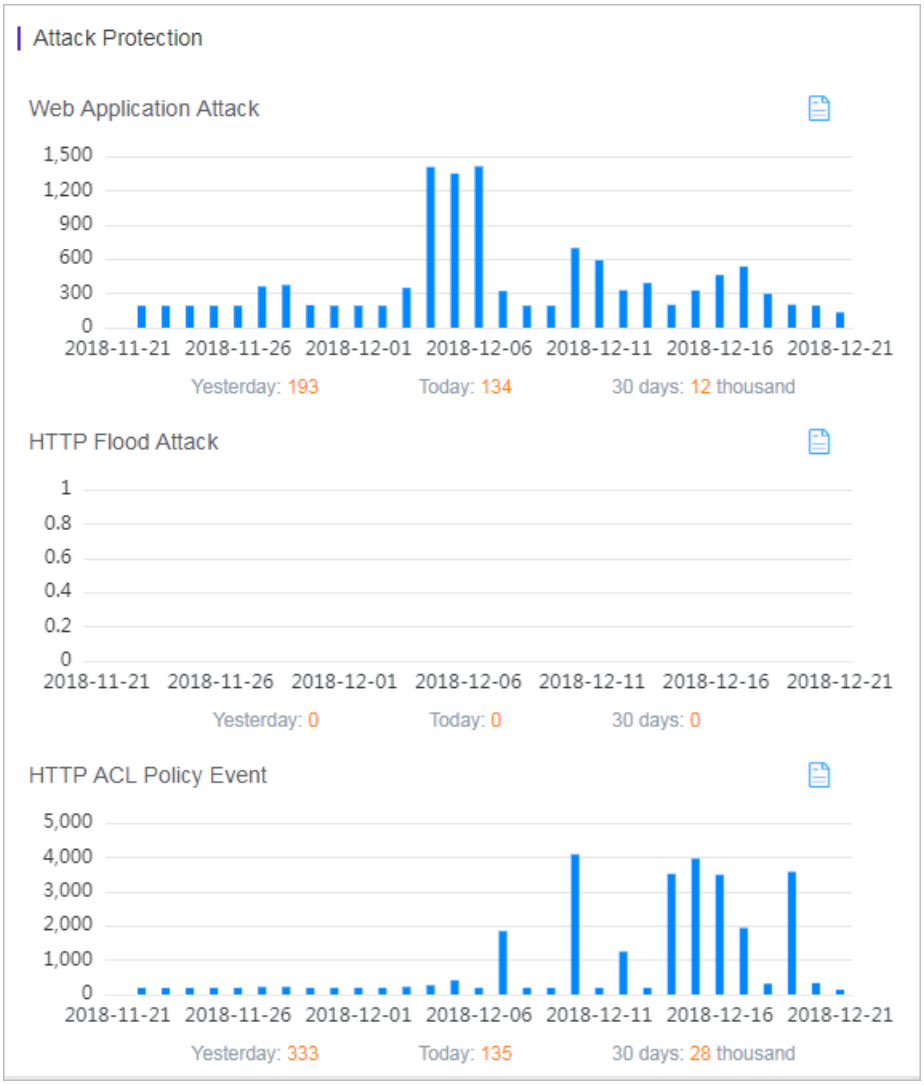
次の手順に従って、セキュリティ概要ページを表示します。

1. Web Application Firewall コンソールにログインします。

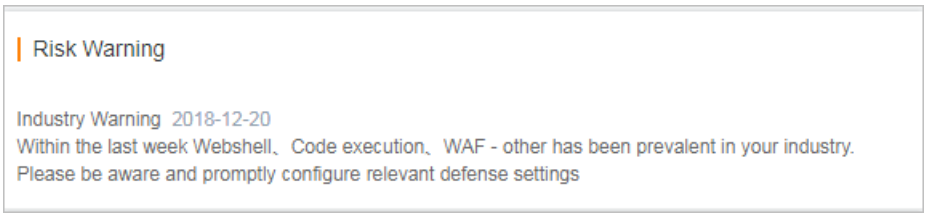
2. [レポート] > [概要ページ] に移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. セキュリティタブページのセキュリティ概要を表示します。 表示できるセキュリティ概要の情報は次のとおりです。

   ・ 攻撃防止: 過去 30 日間の Web アプリケーションの攻撃、HTTP フラッド攻撃、および HTTP ACL ポリシーイベントを棒グラフで表示します。 マウスをレコードの上に移動し

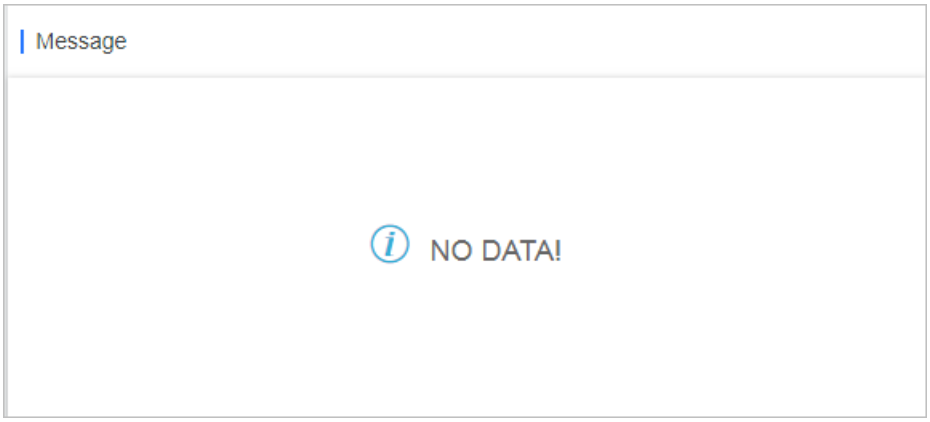
て、特定の情報を表示します。 グラフの右上隅にある [ビュー詳細] をクリックして、対応する攻撃保護レポートに移動し、その詳細レコードを表示します。



- リスク警告: WAF は Web サイトで発見した新しいセキュリティリスクと業界で発生した最新のセキュリティリスクを表示します。 推奨される保護も提供します。 [レポートの表示] をクリックしてリスク警告レポートを表示します。



- メッセージ: 最新の脆弱性に対する WAF 保護ルールの更新を表示します。 [表示] をクリックして、脆弱性の通知を表示します。



4.2 ログ検索

ログ検索機能が有効な場合、Alibaba Cloud WAF は Web サイトへの Web リクエストをすべて記録するのに役立ち、ビジネス分析やセキュリティ管理用の保存されたログの検索が可能です。

この機能を使用するには、Alibaba Cloud WAF Pro を Business または Enterprise プランにアップグレードする必要があります。 詳細は、「更新とアップグレード」をご参照ください。

> 注：
> この機能を使用するには、国際 WAF インスタンスを Enterprise エディションにアップグレードする必要があります。

ログ検索機能により、次の O&M タスクを簡単に完了します。

- WAF が特定のリクエストに対して実行するアクション (ブロックまたは許可) を確認します。
- リクエストを終了させたルールの種類を確認します。Web 攻撃保護ルール、HTTP フラッド攻撃保護ルール、またはカスタムアクセス制御ルール。
- 特定のリクエストの応答時間を確認して、配信元サーバーの応答がタイムアウトしたかどうかを確認します。
- フィールドフィルタリング条件を組み合わせて使用して、特定のリクエストを検索します。 たとえば、送信元 IP アドレス、URL キーワード、Cookie、リファラー、ユーザーエージェント、X-Forwarded-For 、サーバー応答ステータスコードなどです。

> 注：
> ログ検索機能を有効にすると、Alibaba Cloud に対し、WAF が検査するすべての Web リクエストを記録するアクセス許可を構成します (POST データは記録されません)。

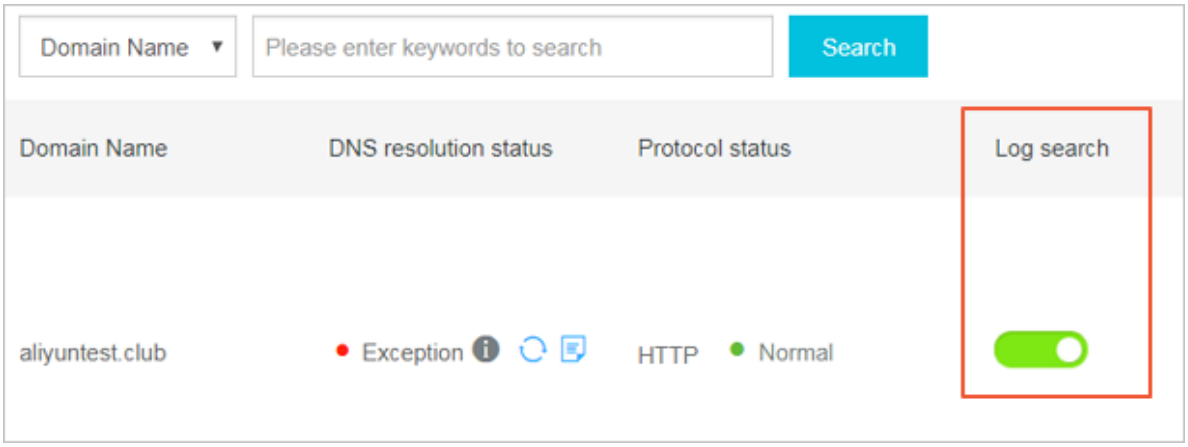
前提条件として、[Web サイト設定] ページに移動して、特定のドメイン名のログ検索機能を有効にする必要があります。 Alibaba Cloud WAF は、[ログ検索] スイッチがオンの場合にの

み、Web サイトのリクエストログの記録を開始します。 ログ検索が有効になると、[ログ] ページに移動して、ドメイン名のログを検索します。

> 注：
> 最大 100 個のドメイン名のリクエストログを表示します。

1. Alibaba Cloud WAF コンソールにログインします。
2. [管理] > [Web サイト設定] ページに移動して、WAF インスタンスのリージョン (中国本土または国際) を選択します。
3. 設定するドメインを選択して、その [ログ検索] を有効にします。

> 注：
> このページでログ検索を無効にすることも可能です。 ログ検索を無効にすると、リクエストログは記録されなくなります。 再度ログ検索を有効にしても、機能が無効になっている間はリクエストログの照会はできません。



4. [レポート] > [ログ] ページに移動します。
5. [ドメイン名]、[照会時間] を選択し、[検索] をクリックします。

> 注：

最新の 30 日間のログのみにアクセス可能です。

[詳細検索] をクリックして、より詳細な検索条件を定義することも可能です。

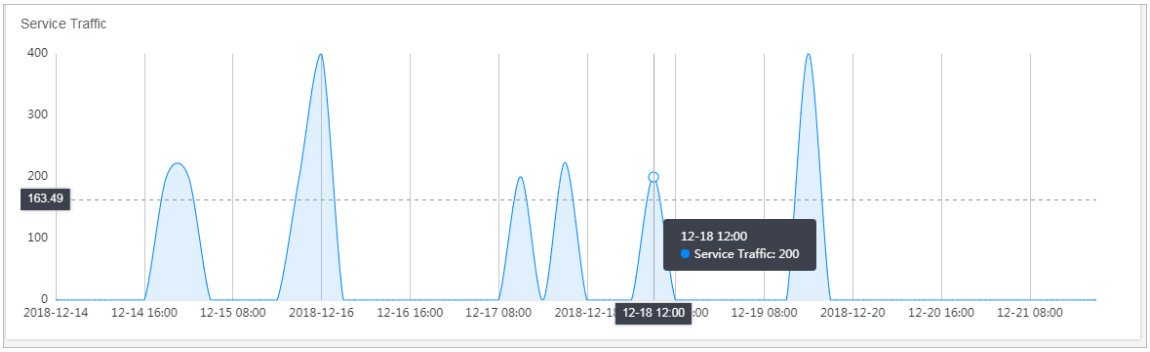
表 4-1 : 詳細検索フィールド

フィールド	説明
送信元 IP	送信元 IP アドレス。
URL キーワード	リクエストされた URL。 注 : このフィールドは "/" 記号をサポートします。 たとえば、「/NTIS/casier」と入力します。
Cookie	リクエストヘッダーに含まれるクライアント側の Cookie。
リファラー	HTTP リクエストヘッダーのリファラーフィールド。
ユーザーエージェント	クライアントのブラウザー、オペレーティングシステムなどを識別するリクエスト内のユーザーエージェント文字列。
X-Forwarded-For	リクエストヘッダーの XFF フィールド
サーバー応答コード	Alibaba Cloud WAF が配信元サーバーから受信した応答ステータスコード。 注 : 3 桁の数字をサポートしています。 「-」記号を指定して、応答ステータス情報を持たないリクエストを検索することも可能です。 たとえば、リクエストはブロックされました。
WAF が返すステータスコード	Alibaba Cloud WAF がクライアントに返した応答ステータスコード。 注 : 3 桁の数字をサポートしています。 「-」記号を指定して、応答ステータス情報を持たないリクエストを検索することも可能です。 たとえば、リクエストはブロックされました。
リクエストユニーク ID	リクエスト ID。 リクエストがブロックされた場合は、ブロックしているページでリクエスト ID が見つかります。

フィールド	説明
リクエストドメイン	ログ検索機能でワイルドカードドメイン名が有効になっている場合、このフィールドを使用して特定のドメイン名を検索します。
保護ポリシー	このオプションを使用して、Web アプリケーション攻撃保護、HTTP フラッド保護ポリシー、HTTP ACL ルール、リージョンブロック、データリスク管理などのルール一致タイプを指定します。

6. 検索結果の表示

・ [サービストラフィック] エリアで、検索時間帯別のアクセスリクエスト件数トレンドグラフを表示します。



・ [リクエストログ] 一覧で、検索条件に一致するアクセスリクエストレコードを表示します。 次の図は、HTTP フラッド攻撃保護ルールに対してブロックされたアクセスリクエストのログを示しています。

配信元の応答情報内のパラメーターの説明

- Status: Alibaba Cloud WAF がクライアントに返す応答ステータス情報を示します。
- Upstream_status: Alibaba Cloud WAF が配信元サーバーから受信した応答ステータス情報を示します。 “-“ が返された場合、応答がないことを示しています。 たとえ

ば、このリクエストが Alibaba Cloud WAF によってブロックされたか、配信元サーバー応答がタイムアウトしました。

- Upstream_ip: このリクエストの配信元サイトの IP アドレスを示します。 たとえば、Alibaba Cloud WAF が ECS インスタンスにトラフィックを返す場合、このパラメーターは配信元 ECS インスタンスの IP アドレスを返します。
- Upstream_time: 配信元サーバーが WAF リクエストへの応答に要した時間を示します。 “-“ は応答がタイムアウトしたことを示します。

7. [ログ照会] ページ右上隅の [ログのダウンロード] をクリックして、現在取得しているログのダウンロードタスクを追加します。 [ダウンロードしたファイルを表示] ページで、ログファイルをローカルクライアントにダウンロードします。

> 注 :
> 一度に最大 2,000 万行のログをダウンロード可能です。 2,000 万行を超えるログをエクスポートする場合は、複数のダウンロードタスクを実行することを推奨します。

リクエストログフィールドの説明

フィールド	名前	説明
時刻	時刻	リクエストの UTC 時刻。
ドメイン	ドメイン	リクエストされたドメイン名。
送信元 IP	送信元 IP	送信元 IP アドレス。
IP の都市	IP の都市	リクエストが発生した都市。
IP の国	IP の国	リクエストが発生した国。
メソッド	メソッド	リクエストの HTTP メソッド。
URL	アクセスリクエスト URL	リクエストされた URL。
Https	アクセスリクエストプロトコル	リクエストで指定されたプロトコル
リファラー	リファラー	HTTP ヘッダー内のリファラーフィールド。
ユーザーエージェント	ユーザーエージェント	クライアントのブラウザー、オペレーティングシステムなどを識別するリクエスト内のユーザーエージェント文字列。
X-Forwarded-For	X-Forwarded-For	HTTP プロキシまたはロードバランサーを介して Web サーバーに接続しているクライアントの配信元 IP アドレスを識別するリクエストヘッダー内の x-forward フィールド。

フィールド	名前	説明
Cookie	Cookie	クライアントの Cookie 情報を識別するリクエストヘッダー内の Cookie フィールド。
攻撃タイプ	攻撃タイプ	リクエストによってトリガーされたイベント。 ・ 0: 攻撃が見つからなかったことを示します。 ・ 1: Web アプリケーション攻撃保護ルールがトリガーされたことを示します。 ・ 2: HTTP フラッド保護ルールがトリガーされたことを示します。 ・ 3: HTTP ACL ポリシールールがトリガーされたことを示します。 ・ 4: ブロックされるリージョンルールがトリガーされたことを示します。 ・ 5: データリスク管理ルールがトリガーされたことを示します。
ステータス	応答ステータスコード	Alibaba Cloud WAF がクライアントに返した応答ステータスコード。
アップストリームステータス	ステータス	Alibaba Cloud WAF が配信元サイトから受信した応答ステータスコード。"-" は応答が受信されなかったことを示します。 たとえば、リクエストが WAF によってブロックされたか、配信元サイトがタイムアウトしました。
アップストリーム IP	アップストリーム IP	リクエストの送信元 IP アドレス。 たとえば、Alibaba Cloud WAF が ECS インスタンスにトラフィックを返す場合、このパラメーターは配信元 ECS インスタンスの IP アドレスを示します。
アップストリーム時間	アップストリーム時間	配信元サーバーがリクエストに応答するのにかかった時間。"-" は応答がタイムアウトしたことを示します。

5 設定

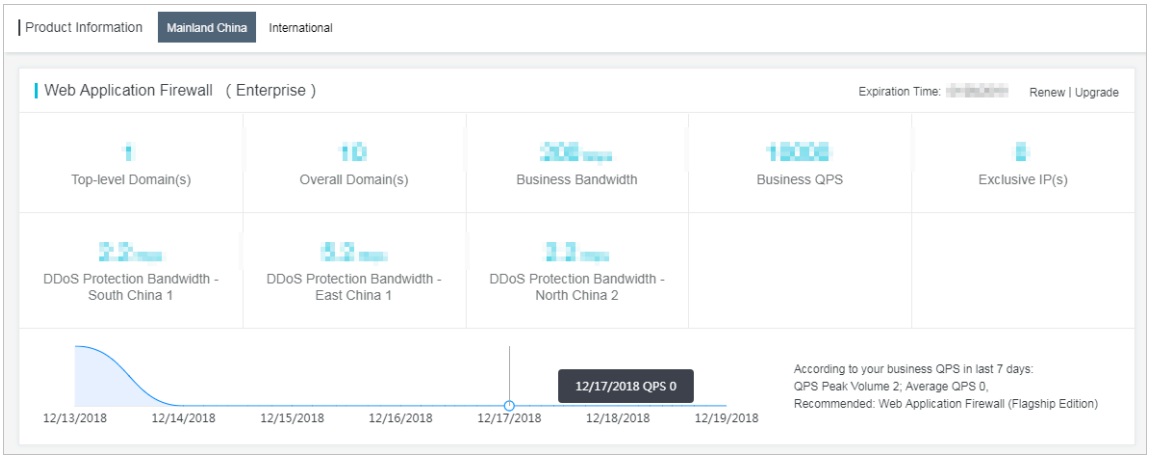
5.1 プロダクト情報の表示

Alibaba Cloud WAF のプロダクト情報ページには、サブスクリプションの詳細、組み込み保護ルールの更新、機能変更、および WAF の IP アドレスに関する直感的な情報が表示されます。

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。

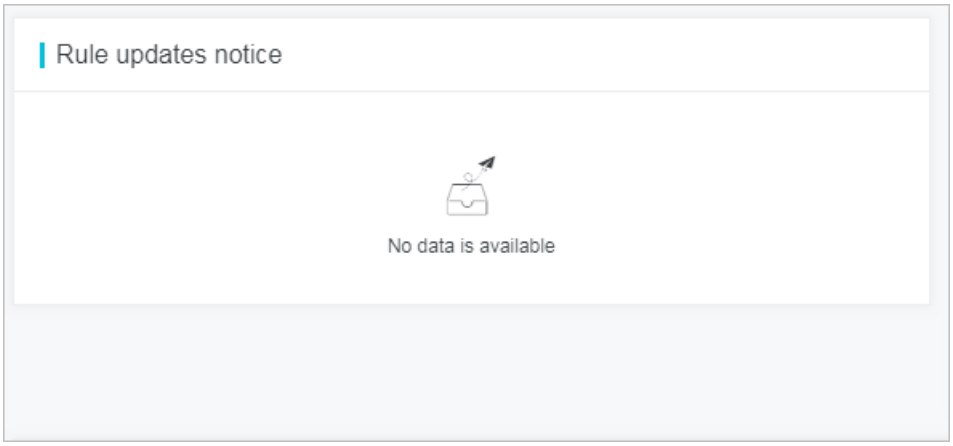
3. [設定] > [プロダクト情報] ページに移動して以下の情報を表示します。

- サブスクリプションの詳細
  - 現在のサブスクリプションプランと有効期限 (更新とアップグレードをサポート)
  - トップレベルドメインの最大数を設定可能
  - ドメイン全体の最大数を設定可能
  - アクセスされたすべてのドメインの最大業務帯域幅
  - アクセスされたすべてのドメインの最大業務 QPS
  - 専用 IP の数
  - 追加の DDoS 保護帯域幅 (リージョン別)
  - 直近 7 日間の業務 QPS グラフ



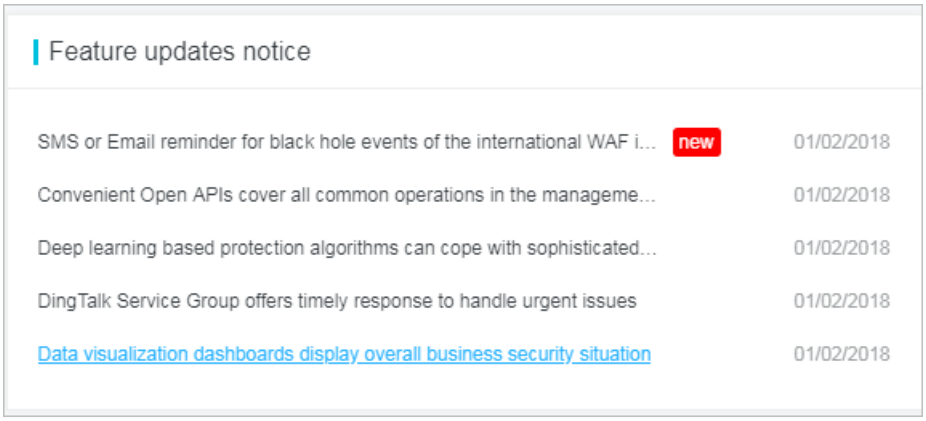
- ルール更新通知

  Alibaba Cloud WAF の組み込み保護ルールの最新の更新についてお知らせします。 タイトルをクリックして詳細を表示します。



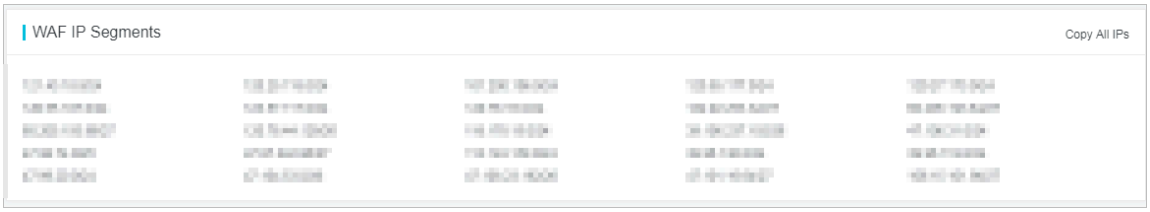
- 機能更新通知

  Alibaba Cloud WAF 機能の最新の変更について通知します。



- WAF IP セグメント

  すべての Alibaba Cloud WAF IP アドレスを一覧表示します。 [すべての IP をコピー]をクリックして、クリップボードにコピーします。



5.2 カスタムルールグループ

ルールグループは、特定の保護機能に対するオプションポリシーを構成する Alibaba Cloud WAF の組み込み保護ルールを組み合わせたものです。 WAF の特定の保護機能に対するカスタムルールグループを作成、適用して専用の保護効果を実現します。

> 注：
> カスタムルールグループは、Business または Enterprise サブスクリプションプランに含まれています。 現在、この機能は Web アプリケーション保護にのみ適用されます。 Web アプリケーション保護のデフォルトの保護ポリシーの詳細については、「Web アプリケーション保護」をご参照ください。

組み込み保護ルールの表示

カスタムルールグループを作成する前に、Alibaba Cloud WAF の組み込み保護ルールを理解しておくことを推奨します。

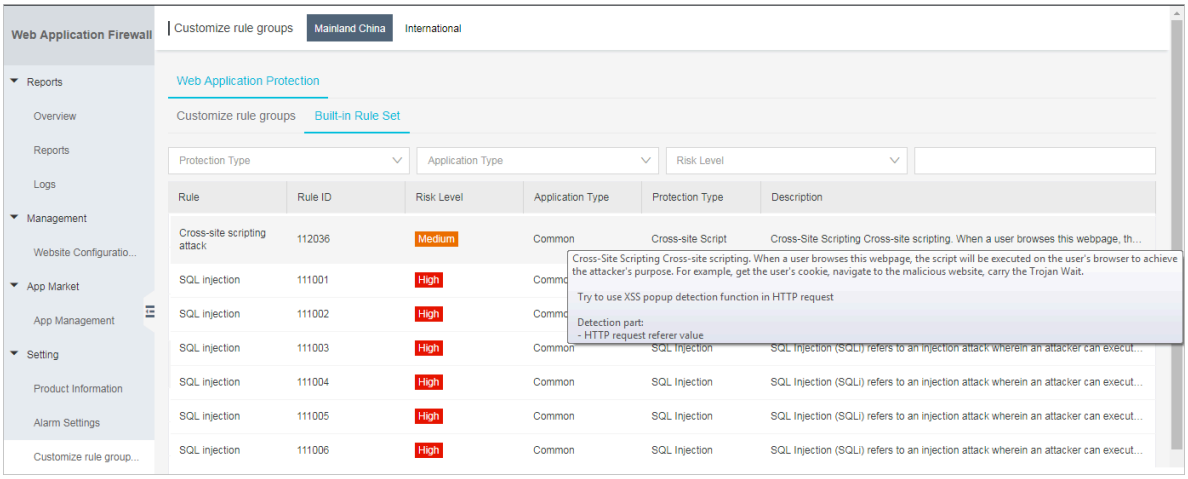
手順

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] または [国際] を選択します。

3. [設定] > [ルールグループのカスタマイズ] ページで、表示する保護機能を選択します。 現在、Web アプリケーション保護のみサポートしています。
4. [組み込みルールセット] ページタブをクリックして、Web アプリケーション保護の保護ルールを表示します。 各ルールは次の情報で構成されています。

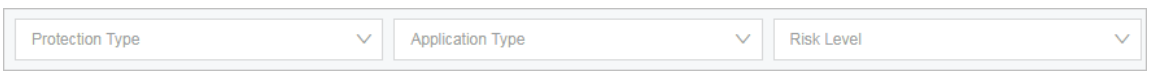
   - ルール: このルールの名前。
   - ルール ID: このルールの一意識別子。
   - リスクレベル: このルールによって防御される脆弱性のリスクレベル。
   - アプリケーションタイプ: このルールで保護されているアプリケーション。 オプション: Common、Wordpress、Discuz、Tomcat、phpMyAdmin など。
   - 保護タイプ: 防御される Web 攻撃タイプ。 オプション: SQL インジェクション、クロスサイトスクリプト、コード実行、CRLF、ローカルファイルインクルージョン、リモートファイルインクルージョン、Webshell、CSRF、その他。
   - 説明: Web 攻撃の説明、検査するコード、検査を実行するセレクタなど、このルールの説明。

   > 注:
   > 説明の上にポインタを置くと、ルールの詳細説明が表示されます。

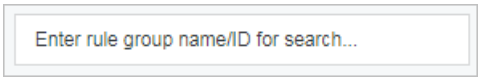


5. (オプション) フィルターを使用して検索し、特定のルールを見つけます。

   - 保護タイプ、アプリケーションタイプ、およびリスクレベルでルールをフィルターします。



   - ルール名または ID でルールを検索します。



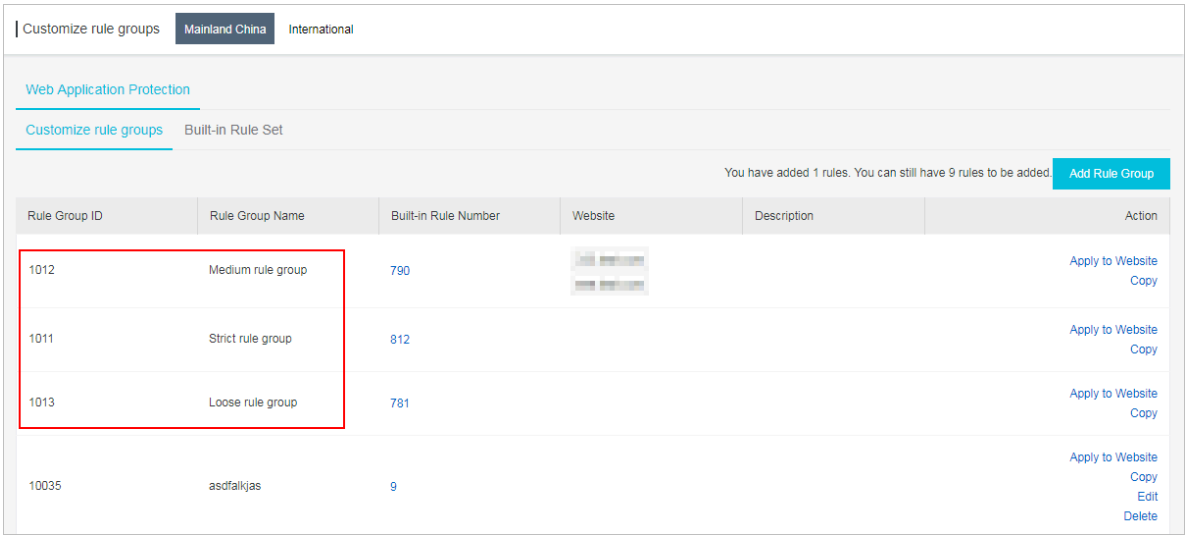
カスタムルールグループの追加

特定の保護機能に対するカスタムルールグループを作成します (現在、Web アプリケーション保護のみサポートしています)。 カスタムルールグループを作成する場合、組み込みルールを選択してグループに追加し、専用の保護ポリシーを構成します。

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] または [国際] を選択します。
3. [設定] > [ルールグループのカスタマイズ] ページで、操作する保護機能を選択します。 現在、Web アプリケーション保護のみサポートしています。

   [ルールグループのカスタマイズ] ページでは、Web アプリケーションのルールグループ ID がすべて表示されます。それらルールグループ IDのうち、"1011"、"1012"、および " 1013" はデフォルトのルールグループです。



4. 新たに 1 つ作成するか、既存のものをコピーして、カスタムルールグループを追加します。

> 注 :

Web アプリケーション保護には最大 10 個のカスタムルールグループを追加可能です。

- カスタムルールグループの作成

  a. [ルールグループの追加] をクリックします。

  b. [ルールグループの追加] ページで、以下の設定を完了します。

  - ルールグループ名: 必須。 このルールグループに名前を付けます。 保護ポリシーを選択するドロップダウンボックスにこの名前が表示されるため、わかりやすい名前を使用することを推奨します。
  - 説明: オプション。 このルールグループの説明を追加します。
  - ルール: すべての組み込みルールの左側エリアからルールを選択して、このルールグループのルールの右側エリアに追加します。

    ルールの詳細については、「組み込みルールの表示の手順 4」をご参照ください。 フィルターと検索を使用して特定のルールを見つけます。 詳細は、「組み込みルールの表示の手順 5」をご参照ください。

  c. [確認] をクリックして、ルールグループを追加します。

  新しく作成されたルールグループに、ルールグループ ID が割り当てられます。

- 既存のルールグループのコピー

  a. コピーするルールグループを見つけ、[コピー] をクリックします。

  b. [ルールグループの追加] ページで、[ルールグループ名] に新しい名前を入力し、継承されたルールを確認します。 (この手順でルールの追加、削除はできません。)

  c. [確認] をクリックして、ルールグループを追加します。

  新しくコピーされたルールグループに、ルールグループ ID が割り当てられます。 「カスタムルールグループの編集」を参照して、このルールグループ内のルールを追加または削除します。

Web サイトへのカスタムルールグループの適用

ルールグループを追加すると、特定の Web サイトの保護 [ポリシー] でそれを有効にするか、[ルールグループのカスタマイズ] ページで一括ドメインに対してそれを有効にします。

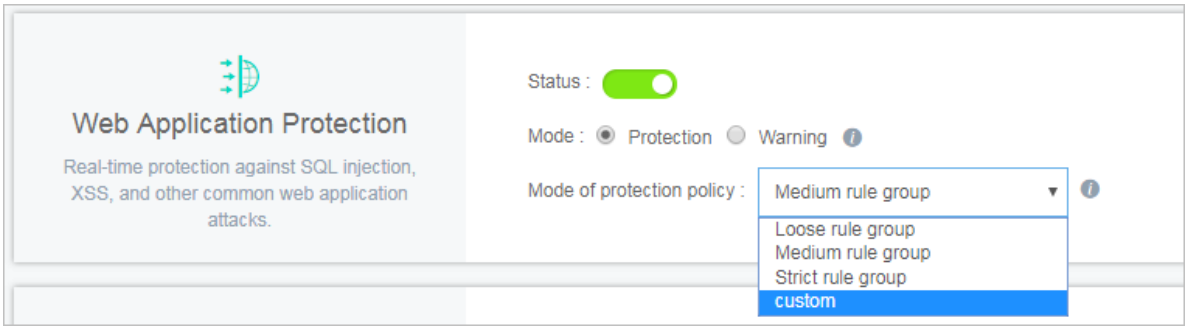
手順

Web アプリケーション保護を例にとり、次の手順に従って、Web サイト設定でカスタマイズルールグループを有効または無効にします。

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] または [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. Web アプリケーション保護の下で保護を有効にします。
5. [保護ポリシーのモード] ドロップダウンボックスを展開し、名前が新たに追加されたルールグループを選択します (この例では、[カスタマイズ] を選択します)。

   カスタマイズルールグループを無効にするには、[保護ポリシーのモード] ドロップダウンボックスで、デフォルトのポリシーを選択します。 この例では、厳しいルールグループ、標準ルールグループ、または緩いルールグループを選択します。



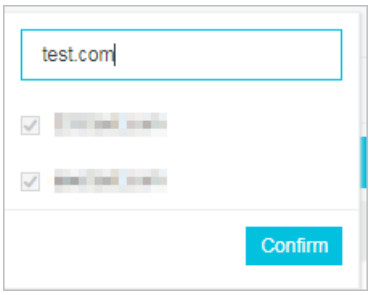
Web アプリケーション保護を例にとり、次の手順に従って、カスタムルールグループを一括ドメインに適用します。

> 注 :
> ルールグループを無効にするには、特定のドメインの保護ポリシーページに移動することを推奨します。

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] または [国際] を選択します。
3. [設定] > [ルールグループのカスタマイズ] ページで、操作する保護機能を選択します。 現在、Web アプリケーション保護のみサポートしています。
4. [ルールグループのカスタマイズ] タブページで、操作するルールグループを見つけ、[Web サイトに適用] をクリックします。

5. 指定されたルールグループを適用する Web サイトをオンにし、[確認] をクリックします。

   ドメインを検索します。



カスタムルールグループの編集

カスタムルールグループが正常に追加されたら、編集してルールを管理したり、名前と説明を変更します。 デフォルトのルールグループは編集できません。

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] または [国際] を選択します。
3. [設定] > [ルールグループのカスタマイズ] ページで、操作する保護機能を選択します。 現在、Web アプリケーション保護のみサポートしています。
4. 操作するルールグループを見つけ、[編集] をクリックします。
5. [ルールグループの編集] ページで、ルールグループを再設定します。 詳細は、「カスタムルールグループの追加」をご参照ください。
6. [確認] をクリックして、ルールグループを更新します。

カスタムルールグループの削除

不要なカスタムルールグループについては、削除します。 ルールグループを削除する前に、そのルールグループがどの Web サイトにも適用されていないことを確認する必要があります。 デフォルトのルールグループは削除できません。

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] または [国際] を選択します。
3. [設定] > [ルールグループのカスタマイズ] ページで、操作する保護機能を選択します。 現在、Web アプリケーション保護のみサポートしています。
4. 削除するルールグループを見つけ、[削除] をクリックします。

5. ヒントのダイアログボックスで、[確認] をクリックします。

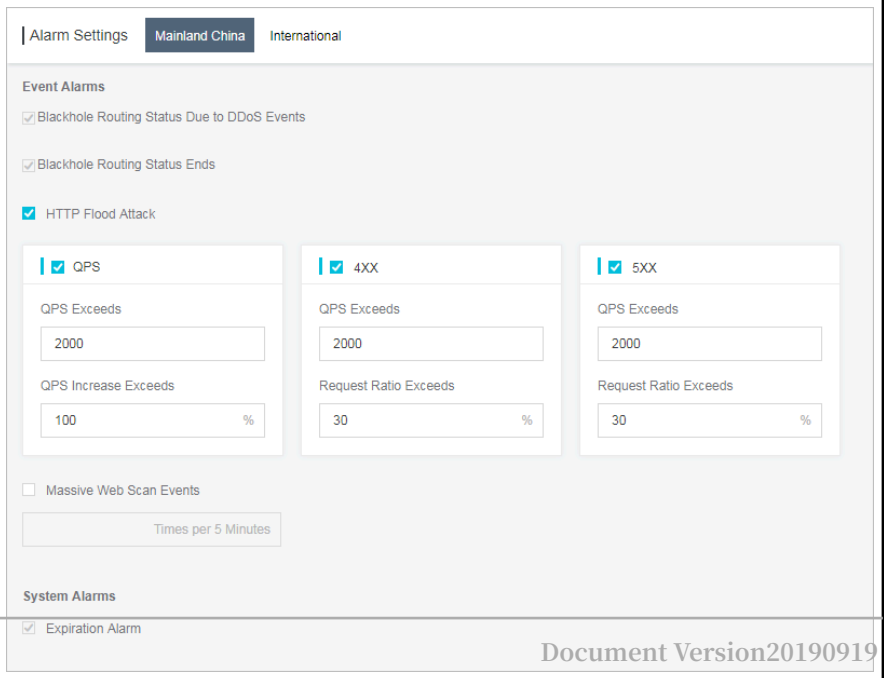
> 注：
> グループが Web サイトに適用されている場合は、削除を続行するには Web サイト設定からそれを無効にする必要があります。 詳細は、「Web サイトへのカスタムルールグループの適用」をご参照ください。

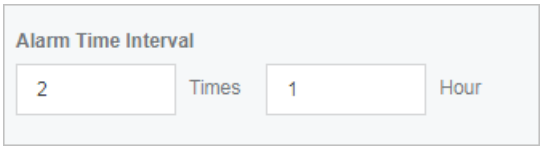
5.3 アラームの設定

Alibaba Cloud WAF は、セキュリティイベントとシステムイベントについてメールで通知します。 アラームのトリガー条件とアラーム時間間隔を設定します。

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] または [国際] を選択します。

3. **[設定] > [アラーム設定] ページで以下の設定を完了します。**

設定	説明
トリガー	どのセキュリティまたはシステムイベントがアラームをトリガーするかを指定します。 注： デフォルトのアラームを無効にしたり設定したりすることはできません。 ・ イベントアラーム - DDoS イベントによるブラックホールルーティングステータス (デフォルト) - ブラックホールルーティングステータスの終了 (デフォルト) - HTTP フラッド攻撃 アラームをトリガーする条件を指定する必要があります。 ■ QPS は定義済みの最大値 (1 ～ 10,000,000) を超え、定義済みの最大率 (0%～ 1,000%) で増加します。 ■ 4xx リクエストが定義済みの最大 QPS (1 ～ 10,000,000) を超え、定義済みの最大比率 (0% ～ 1,000%) を占めます。 ■ 5xx リクエストが定義済みの最大 QPS (1 ～ 10,000,000) を超え、定義済みの最大比率 (0% ～ 1,000%) を占めます。 - 大規模 Web スキャンイベント 5 分あたりの最大頻度を指定する必要があります。 ・ システムアラーム: 期限切れアラーム (デフォルト) 

設定	説明
アラーム時間間隔	xx (0 ～ 24時間) あたり xx (0 ～ 10) 回アラームを繰り返します。 

4. [設定を保存] をクリックします。

5.4 WAF インスタンスのリリース

WAF インスタンスが期限切れになったら、リリースします。

> 注：
> WAF インスタンスをリリースする前に、すべての保護ドメイン名が WAF インスタンスではなく配信元サイトに解決されていることを確認します。 インスタンスがリリースされると、 Web サイト設定はすべて消去されます。 リクエストが WAF インスタンスに到達しても、転送されません。

1. Alibaba Cloud WAF コンソールにログインして、リージョンを選択します。
2. ページの右上隅にある [WAF を閉じる] をクリックします。

> 注：
> このボタンは、WAF インスタンスが期限切れになったときにのみ表示されます。

3. すべての保護ドメイン名が配信元サイトに解決されていることを確認して、[OK] をクリックして、WAF インスタンスをリリースします。

6 リアルタイムログの照会と分析

6.1 WAF Log Service の有効化

Web Application Firewall インスタンスの購入後、コンソールの [アプリの管理] ページで、Web サイトのリアルタイムのログ照会および分析サービスを有効化することができます。

スコープ

WAF Log Service により、WAF が保護する Web サイトから複数のログエントリをリアルタイムで収集します。 リアルタイムのログ照会と分析を実行し、ダッシュボードに結果を表示することも可能です。 WAF Log Service は、Web サイトの業務保護ニーズと運用上の要件を完全に満たしています。 WAF Log Service を有効にした場合、必要に応じてログストレージ期間とログストレージサイズを選択します。

> 注 :
> 現時点では、WAF Log Service は WAF サブスクリプションインスタンス (Pro、Business、または Enterprise エディション) でのみ利用可能です。

利点

WAF リアルタイムログ照会と分析サービスには、次の利点があります。

- 簡単な設定: サービスを簡単に設定して、Web サイトへの訪問と攻撃を記録するログエントリを収集します。
- リアルタイム分析: WAF コンソールは Log Service と統合され、リアルタイムログ分析サービスと、設定の容易なレポートセンターを提供します。 Web サイトへの訪問と攻撃についてほとんどすべて分かります。
- リアルタイム警告: 特定のインジケーターに基づいたほぼリアルタイムのモニタリングと警告が利用可能で、重要な業務例外へのタイムリーな対応を保証します。
- コラボレーション: リアルタイムコンピューティング、クラウドストレージ、可視化、およびその他のデータソリューションとともにこのサービスを使用して、より多くのデータ価値を見いだします。

WAF Log Service の有効化

1. Web Application Firewall コンソールにログインします。

2. [アプリマーケット] > [アプリの管理] をクリックし、WAF インスタンスがあるリージョンを選択します。
3. リアルタイムログ照会と分析サービスで、[アップグレード] をクリックします。
4. 表示されたページで、[Log Service] を有効にし、ログストレージ期間とログストレージサイズを選択して、[今すぐ購入] をクリックします。
5. WAF コンソールに戻り、 [アプリマーケット] > [アプリの管理] をクリックし、リアルタイムログ照会と分析サービスで、[許可]をクリックします。
6. [同意] をクリックして、専用ログストアにログエントリを書き込む権限を WAF に付与します。

   WAF Log Service が有効になり、権限付与されます。
7. WAF コンソールに戻り、[アプリマーケット] > [アプリの管理] をクリックし、リアルタイムログ照会と分析サービスで、[設定] をクリックします。
8. [Log Service] ページで、WAF が保護する Web サイトのドメイン名を選択し、右側の ステータス スイッチをオンにして WAF Log Service を有効にします。

   Log Service は、WAF が記録した Web ログをすべてリアルタイムで収集します。 これらのログエントリはリアルタイムで照会および分析されます。

6.2 ログ収集

WAF コンソールで、指定したドメインの Web Application Firewall (WAF) のログ収集機能を有効にします。

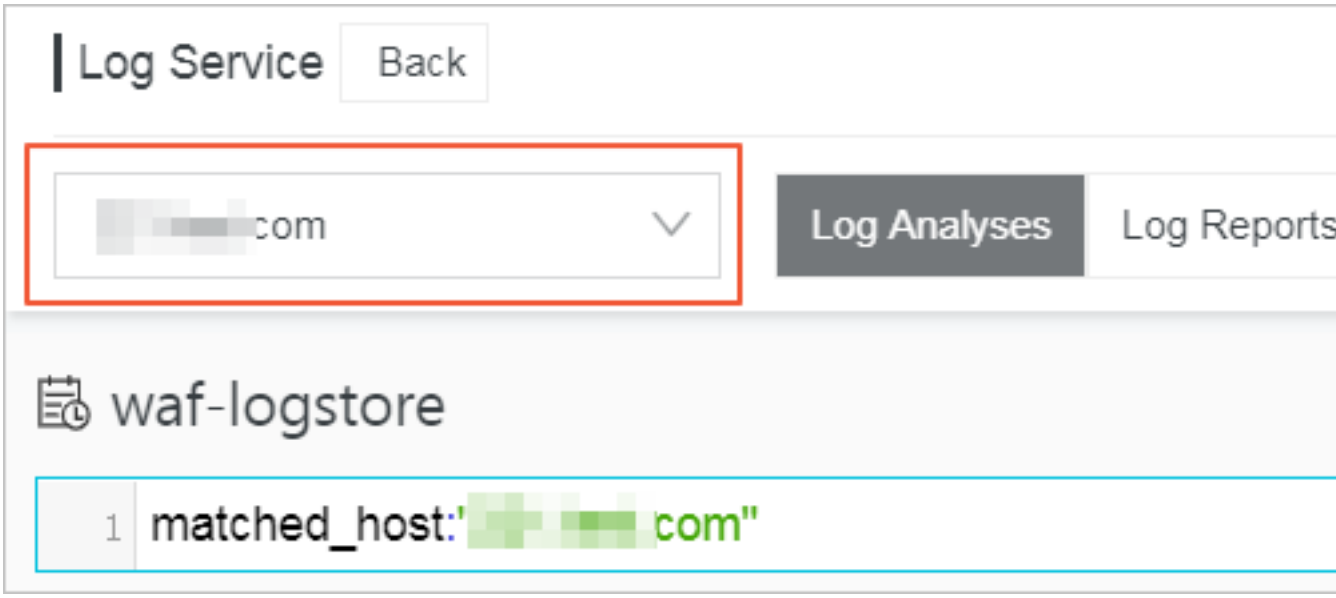
- WAFインスタンスを購入し、WAF を使用してドメインを保護します。
- Log Service を有効にします。

Log Service は Alibaba Cloud WAF が保護する Web サイトへの訪問と攻撃を記録するログエントリを収集し、リアルタイムのログ照会と分析をサポートします。 照会結果はダッシュボードに表示されます。 Web サイトへの訪問と攻撃についての分析調査をタイムリーに実行し、セキュリティエンジニアが保護戦略を開発するのに役立ちます。

1. Web Application Firewallにログインします。
2. [アプリマーケット] > [アプリの管理] をクリックし、[リアルタイムログ照会と分析サービス] をクリックします。

   注：
   WAF ログ 収集機能を初めて設定する場合は、[許可] をクリックし、許可ページの指示に従って、すべてのログエントリを専用のログストアに書き込む権限を WAF に付与します。

3. ドメインを選択し、右側の [ステータス] スイッチをオンにし、ログ収集機能を有効にします。



これでドメインに対する WAF ログ収集機能が有効になりました。 Log Service はアカウント用ログストアを自動的に作成します。 WAF はログエントリを専用ログストアに自動的に書き込みます。 次の デフォルト設定の表は、専用ログストアのデフォルト設定を示しています。

表 6-1 : デフォルト設定

デフォルト設定項目	説明
プロジェクト	プロジェクトはデフォルトで作成されます。 プロジェクト名の形式は、WAF インスタンスのリージョンによって決まります。 ・ WAF インスタンスが中国本土で作成された場合、プロジェクト名は "`waf-project- #### Alibaba Cloud ##### ID -cn-hangzhou`" です。 ・ WAF インスタンスが他のリージョンで作成された場合、プロジェクト名は "`waf-project-#### Alibaba Cloud ##### ID -ap-southeast-1`" です。
ログストア	ログストア `waf - logstore` はデフォルトで作成されます。 WAF ログ収集機能によって収集されたログエントリはすべてこのログストアに保存されます。

デフォルト設定項目	説明
リージョン	・ WAF インスタンスが中国本土で作成された場合、プロジェクトはデフォルトで杭州リージョンに保存されます。 ・ WAF インスタンスが他のリージョンで作成された場合、プロジェクトはデフォルトでシンガポールリージョンに保存されます。
シャード	デフォルトで 2 つのシャードが作成され、自動シャード分割機能が有効になります。
ダッシュボード	3 つのダッシュボードが作成されます。 ・ アクセスセンター ・ オペレーションセンター ・ セキュリティセンター ダッシュボードの詳細については、「WAF Log Service - ログレポート」をご参照ください。

制限と説明

・ 他のデータを専用ログストアに書き込むことはできません。

WAF が生成したログエントリは、専用ログストアに保存されます。 API、SDK、または他の方法を使用してこのログストアに他のデータを書き込むことはできません。

> 注：
> 専用ログストアは、照会、統計、アラート、ストリーミング消費などの機能に特別な制限はありません。

・ ログエントリのストレージ期間などの基本設定は変更できません。

・ 専用ログストアは請求されません。

専用ログストアを使用するには、アカウントに対して Log Service を有効にする必要があります。 専用ログストアは請求されません。

> 注：
> Log Service が期限切れになると、WAF ログ収集機能は、料金が適宜支払われるまで一時停止します。

・ デフォルトで Log Service が作成するプロジェクト、ログストア、インデックス、およびダッシュボードの設定を削除または変更しないでください。 Log Service は WAF ログ照

会と分析サービスを不定期に更新します。 専用ログストアのインデックスとデフォルトのレポートも自動的に更新されます。

- RAM ユーザーにより WAF ログ照会と分析サービスを使用する場合は、RAMユーザーに必要な Log Service 権限を付与する必要があります。 権限を付与する方法の詳細については、「RAMユーザーへのログ照会と分析の権限付与」をご参照ください。

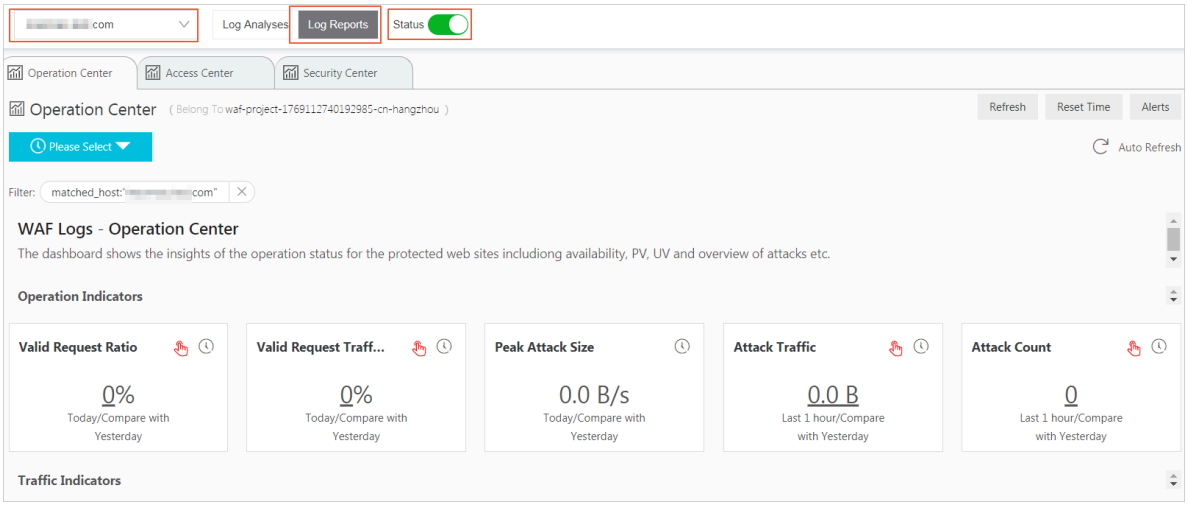
6.3 ログレポート

[ログレポート] ページは、Log Service の [ダッシュボード] ページと統合されています。 このページでは、デフォルトのダッシュボードを表示します。 時間範囲を変更するかフィルターを追加することで、Web サイトに関する業務データとセキュリティデータをフィルターします。

レポートの表示

1. Web Application Firewall コンソール にログインし、[アプリマーケット] > [アプリの管理] をクリックします。
2. [リアルタイムログ照会と分析サービス] エリアをクリックして [ログサービス] ページを開きます。
3. [DO NOT TRANSLATE]
4. ドメインを選択し、右側の [ステータス] スイッチがオンになっていることを確認します。
5. [ログレポート] をクリックします。

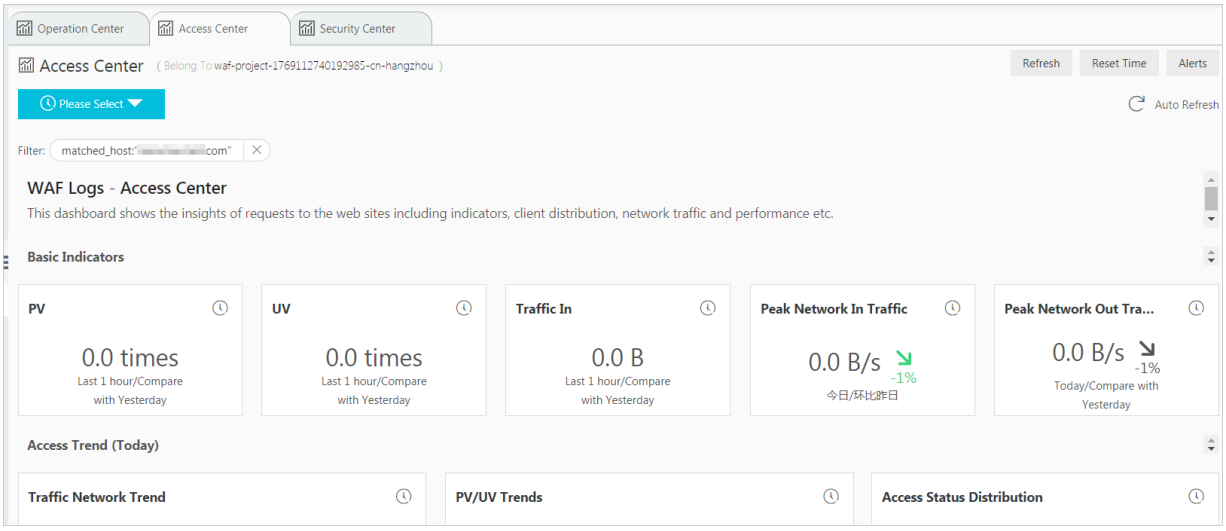
   表示されるページは、Log Service の [ダッシュボード] ページと統合されています。 フィルター が自動的に追加され、選択したドメインについて記録されているすべてのログエントリを表示します。 この例では、フィルターは `matched_ho st : www . aliyun . com` です。



WAF ログ収集機能を有効にすると、Log Service はデフォルトでオペレーションセンター、アクセスセンター、およびセキュリティセンターの 3 つのダッシュボードを作成します。

注：
デフォルトのダッシュボードの詳細については、「デフォルトのダッシュボード」をご参照ください。

ダッシュボード	説明
オペレーションセンター	有効なリクエスト率や攻撃の統計などの操作の詳細、インバウンドとアウトバウンド両方のスループットのピークや受信したリクエストの数などのトラフィックの詳細、操作の傾向、攻撃の概要、その他の情報を表示します。
アクセスセンター	ページビュー (PV) 数やユニーク訪問者 (UV) 数 、アクセス傾向、訪問者分布、その他情報などの基本的なアクセス詳細を表示します。
セキュリティセンター	攻撃の基本的なインデックス情報、攻撃タイプ、攻撃の傾向、攻撃者分布、その他の情報を表示します。



注：
ダッシュボードは、WAF Log Service で事前に定義されているレイアウトを使用してさまざまなレポートを表示します。 次の表に、レポートでサポートされているグラフの種類を示します。 Log Service でサポートされているグラフの種類の詳細については、「グラフの説明」をご参照ください。

種類	説明
数	この種類のグラフは、有効なリクエスト率や攻撃のピークなどの重要なメトリックスを表示します。
折れ線グラフと面グラフ	これらの種類のグラフは、インバウンドスループットの傾向や攻撃阻止の傾向など、指定された期間内の重要なメトリックスの傾向を表示します。
地図	この種類のグラフは、たとえば国ごとの訪問者と攻撃者の地理的分布を表示します。 攻撃者の分布を説明するヒートマップもサポートしています。
円グラフ	この種類のグラフは、攻撃者の分布やクライアントタイプの分布などを表示します。
テーブル	この種類のグラフは、攻撃者の情報などの情報を含むテーブルを表示します。
地図	この種類のグラフはデータの地理的分布を表示します。

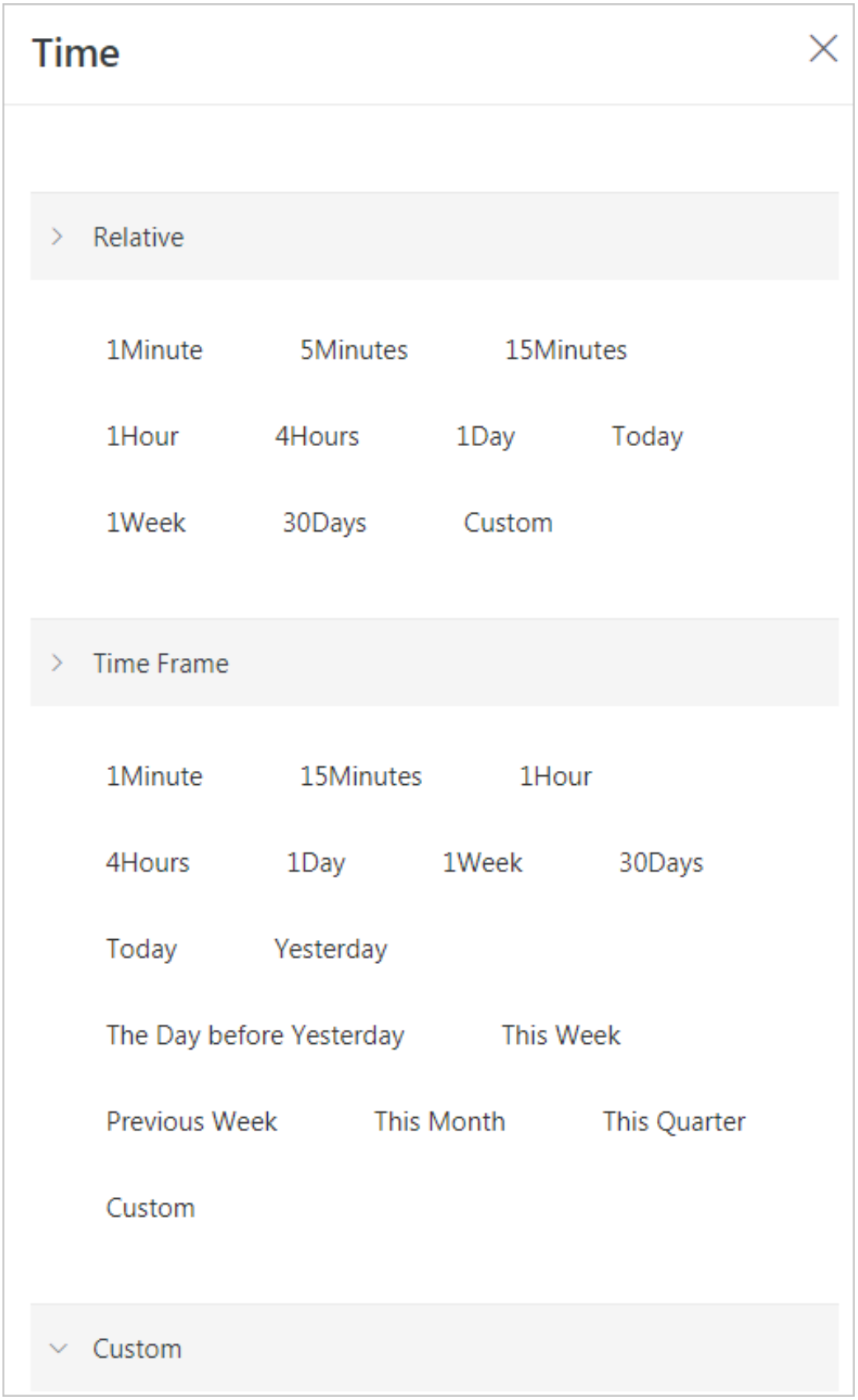
タイムセレクター

ダッシュボードページのすべてのグラフのデータは、さまざまな時間範囲に基づいて生成されています。 時間範囲を統一する場合は、 タイムセレクターを設定します。

1. [ログレポート] ページで、[選択してください] をクリックし、
2. 表示されたウィンドウで時間範囲を選択します。 相対時間、概算時間を選択するか、または時間範囲をカスタマイズします。

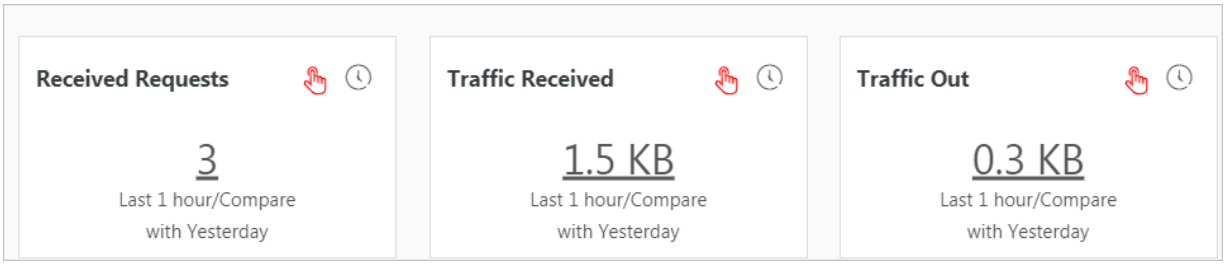
 注：

- 時間範囲を設定すると、その時間範囲がすべてのレポートに適用されます。
- 時間範囲を設定すると、現在のページに一時的なビューが生成されます。 次回レポートを表示するときには、デフォルトの時間範囲が使用されます。
- ダッシュボードで単一のレポートの時間範囲を変更するには、右上隅にある  をクリックします。


Time
Relative
1Minute
5Minutes
15Minutes
1Hour
4Hours
1Day
Today
1Week
30Days
Custom
Time Frame
1Minute
15Minutes
1Hour
4Hours
1Day
1Week
30Days
Today
Yesterday
The Day before Yesterday
This Week
Previous Week
This Month
This Quarter
Custom
Custom

データドリルダウン

ダッシュボードページの一部のグラフではドリルダウン操作が有効になっており、詳細データにすばやくアクセス可能です。



ドリルダウン操作は、右上隅に  アイコンが付いているグラフで利用可能です。 下線付きの数字をクリックして、詳細な基礎データを表示します。 たとえば、攻撃を受けたドメインと攻撃数をすばやく見つけるには、[セキュリティセンター] レポートの [攻撃を受けたホスト] グラフの番号をクリックします。

注：
または、 [Raw ログ] タブに切り替えて、関連するログエントリを見つけます。

デフォルトのダッシュボードの値の説明

- オペレーションセンター: 有効なリクエスト率や攻撃の統計などの操作の詳細、インバウンドとアウトバウンド両方のスループットのピークや受信したリクエストの数などのトラフィックの詳細、操作の傾向、攻撃の概要、その他の情報を表示します。

グラフ	種類	デフォルトの時間範囲	説明	例
有効なリクエスト率	単一値	今日 (概算時間)	すべてのリクエストのうちの有効なリクエスト率を表示します。 有効なリクエストとは、攻撃でも 400 エラーでブロックされたリクエストでもないリクエストのことです。	95%

グラフ	種類	デフォルトの時間範囲	説明	例
有効なリクエストトラフィック率	単一値	今日 (概算時間)	すべてのリクエストによって生成されたトラフィックのうち、有効なリクエストによって生成されたトラフィックの割合を表示します。	95%
ピーク攻撃サイズ	単一値	今日 (概算時間)	攻撃トラフィックのピークを表示します。測定単位は Bps です。	100 B/s
攻撃トラフィック	単一値	1 時間 (相対)	合計攻撃トラフィックを表示します。測定単位は B です。	30 B
攻撃カウント	単一値	1 時間 (相対)	攻撃の総数。	100
ピークネットワークイン	単一値	今日 (概算時間)	ピークインバウンドスループットを表示します。測定単位は KB/s です。	100 KB/s
ピークネットワークアウト	単一値	今日 (概算時間)	ピークアウトバウンドスループットを表示します。測定単位は KB/s です。	100 KB/s
受信したリクエスト	単一値	1 時間 (相対)	有効なリクエストの総数を表示します。	7,800
受信したトラフィック	単一値	1 時間 (相対)	有効なリクエストによって生成された合計インバウンドトラフィックを表示します。測定単位は MB です。	1.4 MB
トラフィックアウト	単一値	1 時間 (相対)	有効なリクエストによって生成された合計アウトバウンドトラフィックを表示します。測定単位は MB です。	3.8 MB

グラフ	種類	デフォルトの時間範囲	説明	例
ネットワークトラフィックインと攻撃	面グラフ	今日 (概算時間)	有効なリクエストと攻撃によって生成されたスループットの傾向を表示します。測定単位は Kbit/s です。	-
リクエストと阻止	折れ線グラフ	今日 (概算時間)	有効なリクエストと阻止されたリクエストの傾向を表示します。測定単位は Kbit/h です。	-
アクセスステータス分布	フローチャート	今日 (概算時間)	さまざまなステータスコード (404、304、200、その他のステータスコード) を持つリクエストの傾向を表示します。測定単位は Kbit/h です。	-
攻撃送信元 (世界)	世界地図	1 時間 (相対)	攻撃者の分布を国別に表示します。	-
攻撃送信元 (中国)	中国地図	1 時間 (相対)	中国の攻撃者の分布を省別に表示します。	-
攻撃タイプ	円グラフ	1 時間 (相対)	攻撃の分布を攻撃タイプ別に表示します。	-
攻撃されたホスト	ツリーマップ	1 時間 (相対)	攻撃されたドメインと攻撃数を表示します。	-

- アクセスセンター: PV 数と UV 数などの基本的なアクセス詳細、アクセス傾向、訪問者分布、その他情報を表示します。

グラフ	種類	デフォルトの時間範囲	説明	例
PV	単一値	1 時間 (相対)	PV の総数を表示します。	100,000
UV	単一値	1 時間 (相対)	UV の総数を表示します。	100
トラフィックイン	単一値	1 時間 (相対)	合計インバウンドトラフィックを表示します。測定単位は MB です。	300 MB

グラフ	種類	デフォルトの時間範囲	説明	例
トラフィックのピークネットワーク	単一値	今日 (概算時間)	ピークインバウンドスループットを表示します。測定単位は KB/s です。	0.5 KB/s
ピークネットワークアウトトラフィック	単一値	今日 (概算時間)	ピークアウトバウンドスループットを表示します。測定単位は KB/s です。	1.3 KB/s
トラフィックネットワーク傾向	面グラフ	今日 (概算時間)	インバウンドスループットとアウトバウンドスループットの傾向を表示します。測定単位は KB/s です。	-
PV または UV の傾向	折れ線グラフ	今日 (概算時間)	PV と UV のトレンドを表示します。測定単位は Kbit/h です。	-
アクセスステータス分布	フローチャート	今日 (概算時間)	さまざまなステータスコード (404、304、200、その他のステータスコード) を持つリクエストの傾向を表示します。測定単位は Kbit/h です。	-
アクセス送信元	世界地図	1 時間 (相対)	攻撃者の分布を国別に表示します。	-
送信元のトラフィック (世界)	世界地図	1 時間 (相対)	リクエストからのインバウンドトラフィックの分布 (国別に) を表示します。	-
送信元のトラフィック (中国)	中国地図	1 時間 (相対)	リクエストからのインバウンドトラフィックの分布 (省別に) を表示します。	-
アクセスヒートマップ	Amap	1 時間 (相対)	地理的位置ごとにリクエスト送信元の分布を示すヒートマップを表示します。	-

グラフ	種類	デフォルトの時間範囲	説明	例
ネットワークプロバイダー送信元	円グラフ	1 時間 (相対)	China Telecom、China Unicom、China Mobile、大学などの送信元にネットワークを提供するインターネットサービスプロバイダーによるリクエストの送信元分布を表示します。	-
リファラー	テーブル	1 時間 (相対)	ホストが最も頻繁にリダイレクトされている最初の 100 リファラーの URL を表示し、ホストの情報とリダイレクト頻度を表示します。	-
モバイルクライアント分布	円グラフ	1 時間 (相対)	モバイルクライアントからのリクエスト分布をクライアントタイプ別に表示します。	-
PC クライアント分布	円グラフ	1 時間 (相対)	PC クライアントからのリクエスト分布をクライアントタイプ別に表示します。	-
リクエストコンテンツタイプの分布	円グラフ	1 時間 (相対)	HTML、フォーム、JSON、ストリーミングデータなどのコンテンツタイプ別にリクエスト送信元の分布を表示します。	-
アクセスしたサイト	ツリーマップ	1 時間 (相対)	最も訪問された 30 ドメインのアドレスを表示します。	-

グラフ	種類	デフォルトの時間範囲	説明	例
クライアント上位	テーブル	1 時間 (相対)	ドメインを最も訪問した 100 クライアントの情報を表示します。 この情報には、クライアント IP アドレス、リージョンと都市、ネットワーク情報、リクエストメソッド、インバウンドトラフィック、不正アクセス数、攻撃数、その他の情報が含まれます。	-
応答が最も遅い URL	テーブル	1 時間 (相対)	応答時間が最も長い 100 個の URL の情報を表示します。 情報には、Web サイトアドレス、URL、平均応答時間、アクセス数、その他の情報が含まれます。	-

- セキュリティセンター: 攻撃の基本的な詳細、攻撃タイプ、攻撃の傾向、攻撃者分布、その他の情報を表示します。

グラフ	種類	デフォルトの時間範囲	説明	例
ピーク攻撃サイズ	単一値	1 時間 (相対)	Web サイトが攻撃を受けているときのスループットのピークを表示します。測定単位は Bps です。	100 B/s
攻撃されたホスト	単一値	今日 (概算時間)	攻撃されたドメインの数を表示します。	3
攻撃送信元の国	単一値	今日 (概算時間)	攻撃送信元となっている国の数を表示します。	2

グラフ	種類	デフォルトの時間範囲	説明	例
攻撃トラフィック	単一値	1 時間 (相対)	攻撃によって生成されたトラフィック総量を表示します。測定単位は B です。	1 B
攻撃者 UV	単一値	1 時間 (相対)	攻撃送信元となっている一意のクライアント数を表示します。	40
攻撃タイプの分布	フローチャート	今日 (概算時間)	攻撃の分布を攻撃タイプ別に表示します。	-
阻止された攻撃	単一値	1 時間 (相対)	WAF が阻止した攻撃数を表示します。	100
HTTP フラッド攻撃阻止	単一値	1 時間 (相対)	WAF が阻止した HTTP フラッド攻撃数を表示します。	10
Web 攻撃阻止	単一値	1 時間 (相対)	WAF が阻止した Web アプリケーション攻撃数を表示します。	80
アクセス制御イベント	単一値	1 時間 (相対)	WAF の HTTP ACL ポリシーによって阻止されたリクエスト数を表示します。	10
HTTP フラッド攻撃 (世界)	世界地図	1 時間 (相対)	HTTP フラッド攻撃者の国別分布を表示します。	-
HTTP フラッド攻撃 (中国)	中国地図	1 時間 (相対)	HTTP フラッド攻撃者の中国の省別分布を表示します。	-
Web 攻撃 (世界)	世界地図	1 時間 (相対)	Web アプリケーション攻撃の国別分布を表示します。	-
Web 攻撃 (中国)	中国地図	1 時間 (相対)	Web アプリケーション攻撃の中国の省別分布を表示します。	-
アクセス制御攻撃 (世界)	世界地図	1 時間 (相対)	WAF の HTTP ACL ポリシーによって阻止されたリクエストの国別分布を表示します。	-

グラフ	種類	デフォルトの時間範囲	説明	例
アクセス制御攻撃 (中国)	中国地図	1 時間 (相対)	WAF の HTTP ACL ポリシーによって阻止されたリクエストの中国の省別分布を表示します。	-
攻撃されたホスト	ツリーマップ	1 時間 (相対)	最も攻撃を受けた Web サイトを表示します。	-
HTTP フラッド攻撃戦略分布	円グラフ	1 時間 (相対)	HTTP フラッド攻撃に対して有効化されているセキュリティポリシーの分布を表示します。	-
Web 攻撃タイプ分布	円グラフ	1 時間 (相対)	Web 攻撃の分布を攻撃タイプ別に表示します。	-
攻撃者上位	テーブル	1 時間 (相対)	最近攻撃を開始した最初の 100 クライアントの IP アドレス、都道府県、およびネットワークプロバイダーを表示します。また、攻撃数とこれらの攻撃によって生成されたトラフィック量を表示します。	-
攻撃者リファラー	テーブル	1 時間 (相対)	攻撃リクエストのリファラーの情報を表示します。リファラー URL、リファラーホスト、攻撃数が含まれます。	-

6.4 ログエントリのフィールド

WAF は、アクセスリクエストや攻撃ログなど、ドメインに関する詳細なログエントリを保持します。 各ログエントリには何十ものフィールドがあります。 特定のフィールドに基づいて照会と分析を実行します。

フィールド	フィールドの説明	例
__topic__	ログエントリのトピック。 このフィールドの値は waf_access_log であり、変更できません。	waf_access_log
acl_action	pass、drop、captcha など、リクエストに対して WAF HTTP ACL ポリシーが生成したアクション。  注 : 値が null 値または"-" の場合、アクションは pass です。	pass
acl_blocks	リクエストが HTTP ACL ポリシーによってブロックされているかどうかを示します。 ・ 値が 1 の場合、リクエストはブロックされています。 ・ 値が 1 ではない場合、リクエストは渡されます。	1
antibot	適用するアンチボットサービス保護戦略の種類。以下が含まれます。 ・ ratelimit: 周波数制御 ・ sdk: アプリ保護 ・ intelligence: アルゴリズムモデル ・ acl: HTTP ACL ポリシー ・ blacklist: ブラックリスト	ratelimit

フィールド	フィールドの説明	例
antibot_action	アンチボットサービス保護戦略によって実行されるアクション。以下が含まれます。 ・ challenge: 埋め込み JavaScript スクリプトを使用した検証 ・ drop: ブロッキング ・ report: アクセスイベントのロギング ・ captcha: スライダーキャプチャを使用した検証	challenge
block_action	有効化されている WAF 保護の種類。以下が含まれます。 ・ tmd: HTTP フラッド攻撃に対する保護 ・ waf: Web アプリケーション攻撃に対する保護 ・ acl: HTTP ACL ポリシー ・ geo: リージョンのブロック ・ antifraud: データリスク管理 ・ antibot: Web クローラーのブロック	tmd
body_bytes_sent	アクセスリクエスト内の本文のサイズ。測定単位はバイトです。	2
cc_action	none、challenge、pass、close、captcha、wait、login、n などの HTTP フラッド攻撃に対する保護戦略。	close
cc_blocks	リクエストが CC 保護によってブロックされているかどうかを示します。 ・ 値が 1 の場合、リクエストはブロックされています。 ・ 値が 1 ではない場合、リクエストは渡されます。	1

フィールド	フィールドの説明	例
cc_phase	seccookie、server_ip_blacklist、static_whitelist、 server_header_blacklist、server_cookie_blacklist、server_args_blacklist、qps_overmax などの CC 保護ポリシー。	server_ip_blacklist
content_type	アクセスリクエストのコンテンツタイプ。	application/x-www-form-urlencoded
host	ソース Web サイト	api.aliyun.com
http_cookie	クライアント側の Cookie。リクエストヘッダーに含まれています。	k1=v1;k2=v2
http_referer	リクエスト送信元 URL 情報。リクエストヘッダーに含まれています。 "-" は URL 情報がないことを示します。	http://xyz.com
http_user_agent	リクエストヘッダー内のユーザーエージェントフィールド。クライアントブラウザーやオペレーティングシステムなどの情報が含まれます。	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)
http_x_forwarded_for	リクエストヘッダー内の XFF (X-Forwarded-For) 情報。HTTP プロキシまたは負荷分散を使用して Web サーバーに接続するクライアントの元の IP アドレスを識別します。	-
https	リクエストが HTTPS リクエストであるかどうかを示します。 ・ true: リクエストは HTTPS リクエストです。 ・ false: リクエストが HTTP リクエストではありません。	true
matched_host	WAF が保護する一致ドメイン名 (拡張ドメイン名)。 一致するドメインがなかった場合、値は "-" です。	*.aliyun.com
querystring	リクエスト内の照会文字列。	title=tm_content%3Darticle&pid=123
real_client_ip	クライアントの実際 IP アドレス。システムが実際の IP アドレスを取得できない場合、値は "-" です。	1.2.3.4

フィールド	フィールドの説明	例
region	WAF インスタンスの存在するリージョンの情報。	cn
remote_addr	リクエストにアクセスするクライアントの IP アドレス。	1.2.3.4
request_length	リクエストのサイズ。測定単位はバイトです。	123
request_method	アクセスリクエストで使用される HTTP リクエストメソッド。	GET
request_path	リクエストの相対パス。 照会文字列は含まれません。	/news/search.php
request_time_msec	リクエスト時間。測定単位はマイクロ秒です。	44
request_traceid	WAF が記録するアクセスリクエストの一意の ID。	7837b117154103869434 37009ea1f0
server_protocol	応答プロトコルと配信元サーバーのバージョン番号。	HTTP/1.1
status	WAF が返すクライアントへの HTTP 応答のステータス。	200
time	アクセスリクエストが発生した時刻。	2018-05-02T16:03:59+08:00
ua_browser	リクエストを送信するブラウザーの情報。	ie9
ua_browser_family	リクエストを送信したブラウザーのファミリ。	internet explorer
ua_browser_type	リクエストを送信したブラウザーの種類。	web_browser
ua_browser_version	リクエストを送信するブラウザーのバージョン。	9.0
ua_device_type	リクエストを送信するクライアントデバイスの種類。	computer
ua_os	リクエストを送信するクライアントによって使用されるオペレーティングシステム。	windows_7
ua_os_family	クライアントによって使用されるオペレーティングシステムのファミリ。	windows

フィールド	フィールドの説明	例
upstream_addr	コンマで区切られた配信元アドレスのリスト。 アドレスの形式は `IP : Port` です。	1.2.3.4:443
upstream_ip	アクセスリクエストに対応する配信元 IP アドレス。 たとえば、配信元サーバーが ECS インスタンスの場合、このフィールドの値は ECS インスタンスの IP アドレスです。	1.2.3.4
upstream_response_time	配信元サイトが WAF リクエストに応答するのにかかる時間。測定単位はバイトです。"-" はリクエストのタイムアウトを示します。	0.044
upstream_status	WAF が配信元サーバーから受信する応答ステータス。"-" は応答がないことを示します。 理由は、応答のタイムアウトまたはリクエストが WAF によってブロックされている可能性があります。	200
user_id	Alibaba Cloud のアカウント ID。	12345678
waf_action	Web 攻撃保護ポリシーからのアクション。 ・ 値が block の場合、攻撃はブロックされています。 ・ 値が bypass または他の値である場合、攻撃は無視されています。	block
web_attack_type	xss、code_exec、webshell、sqli、lfilei、rfilei などの Web 攻撃の種類。	xss

6.5 詳細設定

WAF ログ照会と分析サービスのページで [詳細設定] をクリックすると、Log Service コンソールにリダイレクトされます。 その後、Log Service の詳細機能を設定します。 たとえば、アラームと通知、リアルタイムのログ収集と消費、転送ログデータを設定したり、他のプロダクトにビジュアル表示を提供します。

手順

1. Web Application Firewall コンソールにログインし、[アプリマーケット] > [アプリの管理] をクリックします。
2. [リアルタイムログ照会と分析サービス] エリアをクリックして [Log Service] ページを開きます。
3. 右上隅の [詳細設定] をクリックします。
4. 表示されるダイアログボックスで、[移動] をクリックして Log Service コンソールを開きます。
5. Log Service コンソールで、ログプロジェクトとログストア用の次の詳細機能を設定します。
   - リアルタイムでのログの収集と消費
   - 他の Alibaba Cloud ストレージサービスへのリアルタイムでの転送ログデータ
   - 他のプロダクトへのビジュアル表示の提供

6.6 ログエントリのエクスポート

WAF ログ照会と分析サービスにより、ログ照会結果をローカルファイルにエクスポートします。

現在のページのログエントリを CSV ファイルにエクスポートするか、すべてのログエントリを TXT ファイルにエクスポートすることができます。

手順

1. Web Application Firewall コンソールにログインし、[アプリマーケット] > [アプリの管理] をクリックします。
2. [ログ照会と分析サービス] エリアをクリックして [Log Service] ページを開きます。
3. [Log Service] ページの [生ログ] タブで、右側にあるダウンロードボタン  をクリックします。

> 注：
> 照会に対する結果が見つからない場合、ダウンロードボタンは表示されません。

4. 表示される [ダウンロードログ] ダイアログボックスで、[現在のページでログをダウンロード] または [CLI コンソールですべてのログをダウンロード] を選択します。

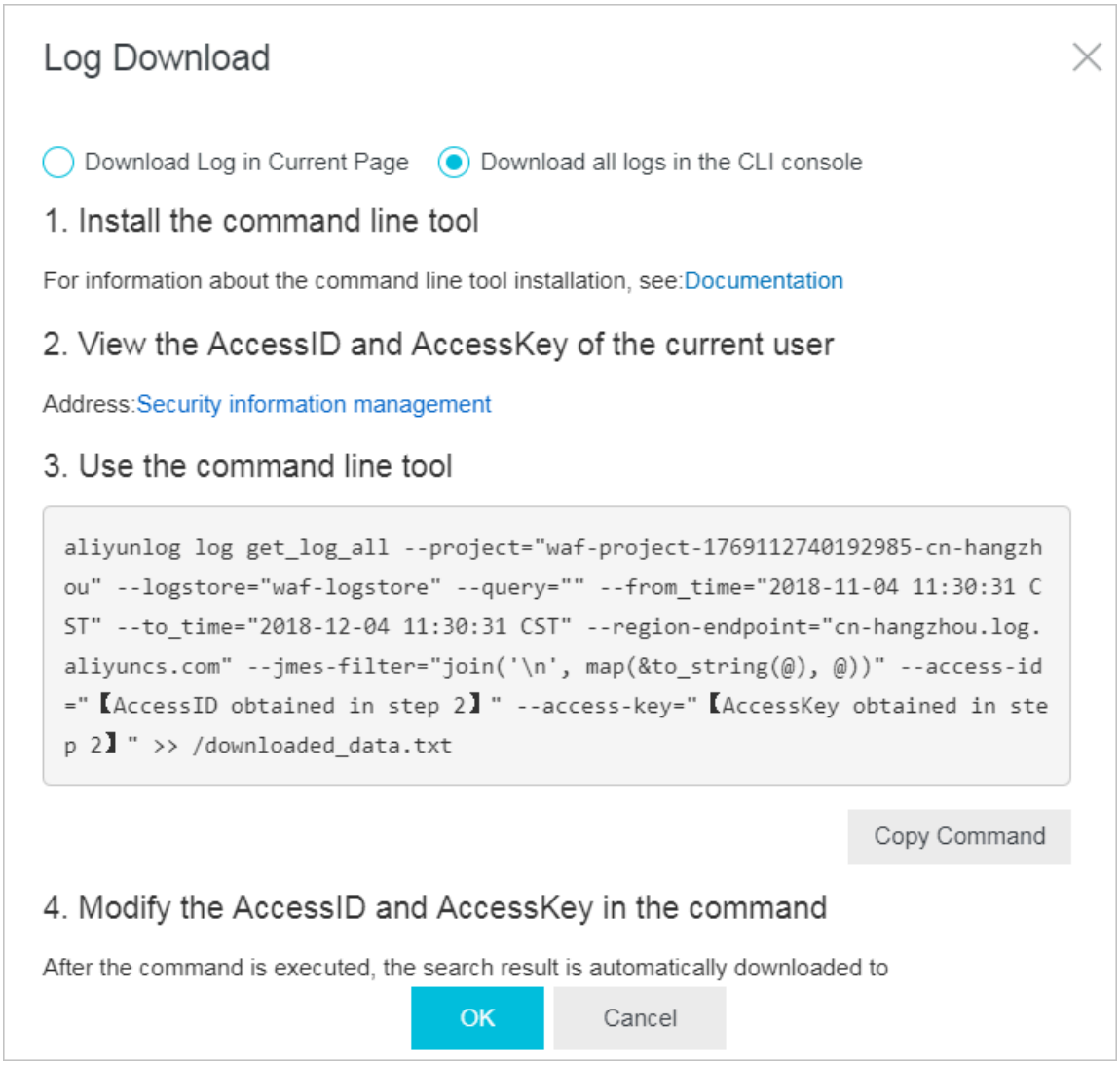
   - 現在のページでログをダウンロード: [OK] をクリックすると、現在のページの生ログエントリを CSV ファイルにダウンロードします。
   - CLI コンソールですべてのログをダウンロード

     a. コマンドラインインターフェイス (CLI) のインストールの詳細については、「CLI ガイド」をご参照ください。

     b. [セキュリティ管理] ページに移動して、現在のユーザーの AccessKey ID と AccessKey Secret を見つけます。

     c. [コマンドのコピー] をクリックしてコマンドを CLI に貼り付け、`AccessID obtained in step 2` と `AccessKey obtained in step 2`

を現在のユーザーの AccessKey ID と AccessKey Secret に置き換えてから、コマンドを実行します。



WAF が記録した生ログエントリはすべて自動的にダウンロードされ、コマンドを実行するディレクトリのdownload_data.txt ファイルに保存されます。

6.7 RAM ユーザーへのログ照会と分析の権限付与

RAM ユーザーで WAF ログ照会と分析サービスを使用する場合は、Alibaba Cloud アカウントを使用して RAM ユーザーに必要な権限を付与する必要があります。

WAF ログ照会と分析サービスを有効にして使用するには、次の権限が必要です。

操作	必要なアカウントタイプと権限
Log Service の有効化 (この操作の後もサービスは有効化されたままです)	Alibaba Cloud アカウント

操作	必要なアカウントタイプと権限
WAF に権限付与して Log Service 内の専用ログストアにリアルタイムでのログデータの書き込み (権限付与は、この操作の後も有効化されたままです)	· Alibaba Cloud アカウント · `AliyunLogF ullAccess` 権限を持つ RAM ユーザー · 特定の権限を持つ RAM ユーザー
ログ照会と分析サービスの使用	· Alibaba Cloud アカウント · `AliyunLogF ullAccess` 権限を持つ RAM ユーザー · 特定の権限を持つ RAM ユーザー

必要に応じて RAM ユーザーに権限を付与します。

シナリオ	権限	手順
すべての Log Service 操作に対する権限を RAM ユーザーに付与します。	`AliyunLogF ullAccess`	詳細は、「RAMユーザー」をご参照ください。
WAF ログ照会と分析サービスを有効にした後、RAM ユーザーにログ表示権限を付与し、Alibaba Cloud アカウントに対する権限付与を完了します。	`AliyunLogR eadOnlyAcc ess`	詳細は、「RAMユーザー」をご参照ください。
WAF ログ照会と分析サービスを有効にして使用する RAM ユーザー権限を付与します。この RAM ユーザーには、Log Service に対する他の管理権限が付与されていません。	カスタム権限付与ポリシー	詳細は、次の手順をご参照ください。

1. RAM コンソールにログインします。
2. [ポリシー] ページで [カスタムポリシー] タブをクリックします。
3. ページの右上隅の [権限付与ポリシーの作成] をクリックします。
4. [権限付与ポリシーの作成] をクリックします。 テンプレートで 権限付与ポリシー名を指定し、ポリシーコンテンツフィールドに以下を入力します。

注 :

次のポリシーコンテンツの `${ Project }` と `${ Logstore }` を WAF Log Service 内の専用プロジェクトとログストアの名前に置き換えます。

```
{
  " Version ": " 1 ",
  " Statement ": [
      {
      " Action ": " log : GetProject ",
      " Resource ": " acs : log :*:*: project /${ Project }",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateProj  ect ",
      " Resource ": " acs : log :*:*: project /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : ListLogSto  res ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 logstore /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateLogS  tore ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 logstore /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : GetIndex ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 logstore /${ Logstore }",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateInde  x ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 logstore /${ Logstore }",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : UpdateInde  x ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 logstore /${ Logstore }",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateDash  board ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 dashboard /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : UpdateDash  board ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 dashboard /*",
```

```
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateSave  dSearch ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 savedsearc  h /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : UpdateSave  dSearch ",
      " Resource ": " acs : log :*:*: project /${ Project }/
 savedsearc  h /*",
      " Effect ": " Allow "
    }
  ]
}
```

5. [権限付与ポリシーの作成] をクリックします。
6. [ユーザー] ページに移動し、RAM ユーザーを探し、[許可] をクリックします。
7. 作成した権限付与ポリシーを追加し、[OK] をクリックします。
   この RAM ユーザーは、WAF ログ照会と分析サービスを有効にして使用しますが、Log Service の他の機能は使用できません。

6.8 ログストレージの管理

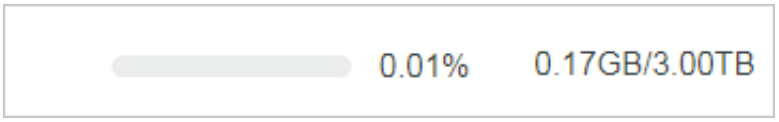
WAF Log Service を有効化すると、指定したログストレージサイズに基づいて、ログストレージが WAF Log Service に割り当てられます。 ログストレージの使用率は Web Application Firewall コンソールの Log Service ページで確認できます。

ログストレージ使用率の表示

WAF ログ照会と分析サービスによって生成したログストレージの使用率はいつでも表示可能です。

> 注 :
> ストレージ使用率の変更がコンソールで更新されるのに 2 時間かかります。 使用できるログストレージ容量が少ない場合は、ログストレージをアップグレードする必要があります。

1. Web Application Firewall コンソールにログインします。
2. [アプリマーケット] > [アプリの管理]をクリックし、WAF インスタンスが存在するリージョンを選択し、[リアルタイムログ照会と分析サービス] をクリックします。
3. [Log Service] ページの上部に、ログストレージの使用率が表示されます。



ログストレージのアップグレード

ログストレージサイズをアップグレードするには、[Log Service] ページの上部の [ストレージのアップグレード]をクリックします。

> 注：
> ログストレージが一杯になると、新しいログデータを専用ログストアに書き込むことはできません。 ログストレージが一杯になる前にログストレージをアップグレードすることを推奨します。

ログストレージの消去

必要に応じて、ログストレージ内のすべてのログエントリを削除します。 たとえば、テストフェーズ中に生成したログエントリを削除して、本番フェーズ中に生成したログエントリのみを記録することで、ログストレージを最大限に活用します。

[Log Service] ページの上部の [消去] をクリックし、[確認] をクリックしてログストレージ内のすべてのログエントリを削除します。

> 重要：
> 削除したログエントリは復元できません。 ログエントリは慎重に削除してください。

> 注：
> ログストレージは、限られた回数しか消去できません。