ALIBABA CLOUD

Alibaba Cloud

Web応用防火壁

ウェブサイトアクセス

Document Version: 20200824

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Website access with CNAME 05
1.1. Web サイトの設定 05
1.2. 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 12
1.3. WAF デプロイメントガイド 13
1.4. 配信元サーバーの保護 18
1.5. WAF back-to-origin CIDR ブロックからのアクセスを許可 20
2.WAF へのアクセス 23
2.1. WAF と CDN の同時デプロイ 23
2.2. WAF と Anti-DDoS Pro の同時デプロイ 25
3.サポート対象の非標準ポート 27
4.来訪者の送信元 IP アドレスの取得 28

1.Website access with CNAME

1.1. 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。

> 説明 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

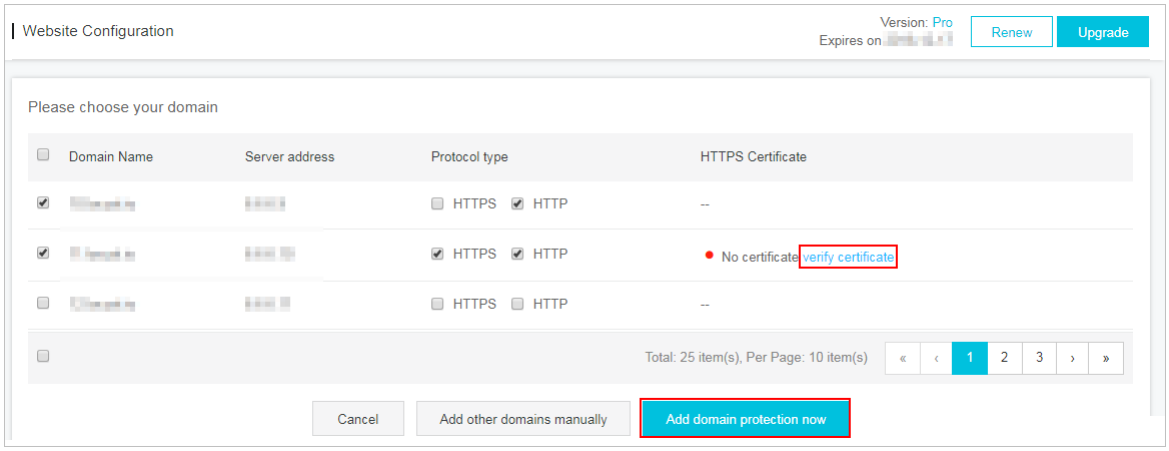
- 保護されるドメインは Alibaba Cloud DNS でホストされています。 また、DNS 設定には少なくとも 1 つの有効な A レコードが含まれる必要があります。

  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。
- （可选）(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。
- （可选）(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. （可选）(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。

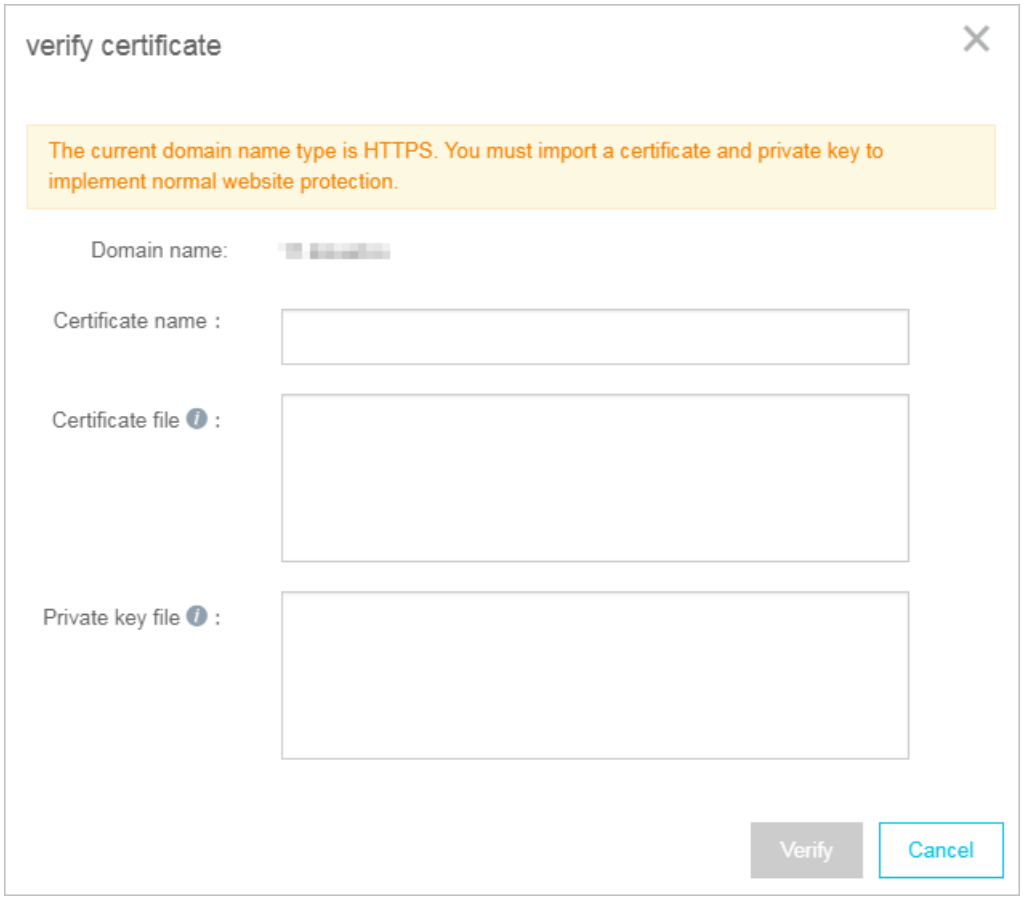
> 説明　別の方法として、ここでは HTTPS を選択せず、Web サイト設定を編集し、設定を作成した後に証明書をアップロードします。 詳細は、「 HTTPS 証明書の更新」をご参照ください。

   i. [証明書の確認] をクリックします。

ii. **[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。



iii. **[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。

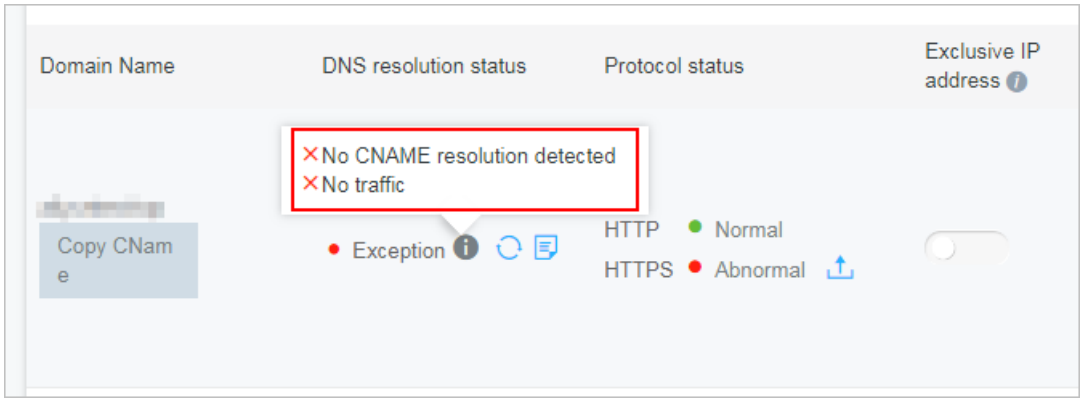
   > 説明　手動で DNS 設定を変更するように求められた場合は、手順 2 : DNS 設定を更新してトラフィックを WAF にリダイレクトする必要があります。

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. （可选）(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

設定	説明
ドメイン名	保護するドメイン名を入力します。 説明 ◦ *.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。
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 説明 ◦ 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。

設定	説明
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。 説明 ■ 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。 説明 ■ 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。
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。 説明 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。

設定	説明
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。 説明 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。

   説明 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。

   > 説明　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。

1.2. 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。

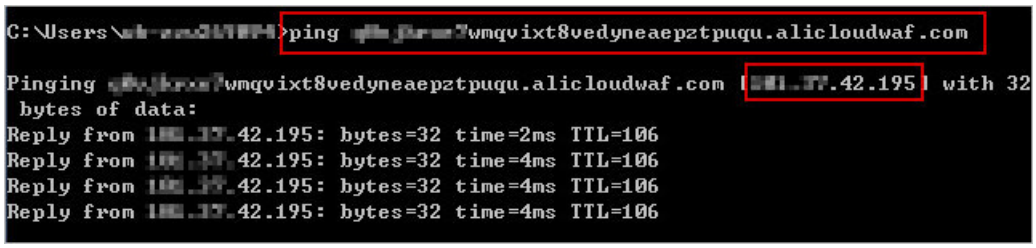
ローカルホストファイルの変更

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。

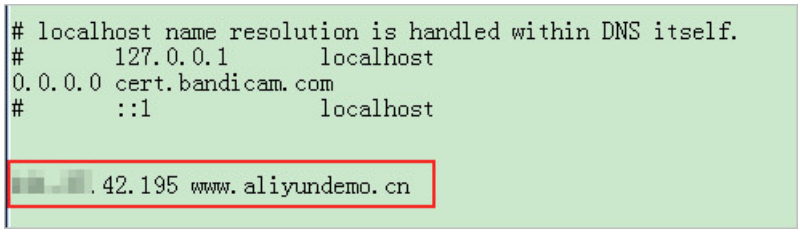
1. *hosts* ファイルをメモ帳で開きます。 *hosts*ファイルは *C:\Windows\System32\drivers\etc\hosts* ディレクトリにあります。
2. 最後の行に、次の内容を追加します。 `WAF_IP_address Domain_name_protected`

   `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。 `xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`

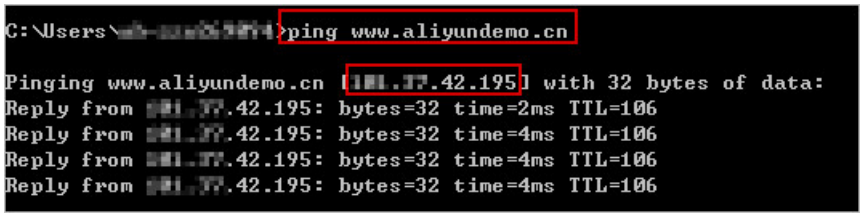
   i. Windows で cmd コマンドラインツールを開き、次のコマンドを実行して WAF IP アドレスを取得します。 `ping xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com` 応答の WAF IP アドレスを確認します。

   ii. 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、

1.3. 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。

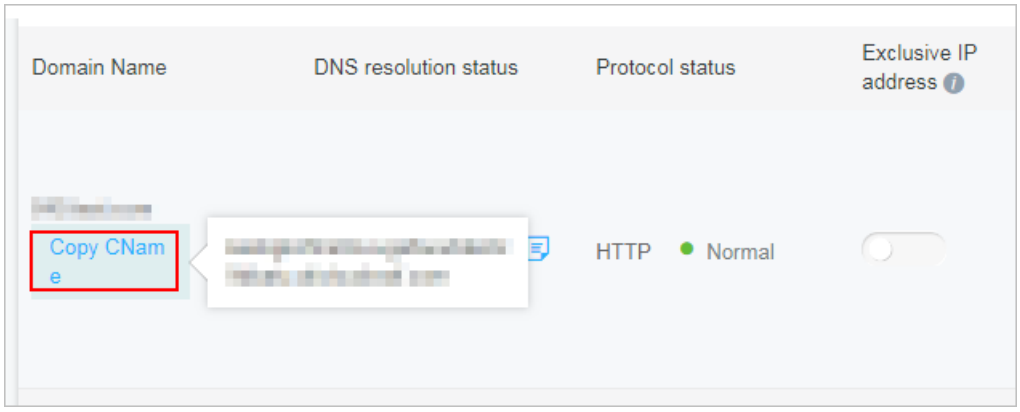
次の内容は、Web サイト専用の Alibaba Cloud WAF のデプロイに適用します。つまり、Web サイトは CDN、DDoS 保護、およびその他のプロキシサービスを使用しません。 その他のシナリオについては、以下のドキュメントをご参照ください。

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



iv. **[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。

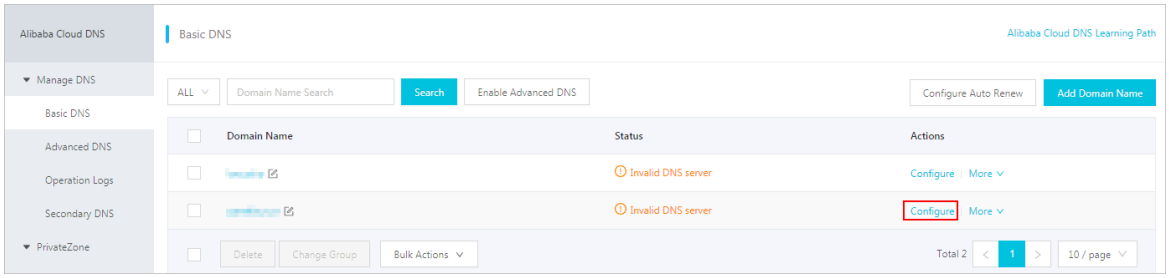
> 説明　A レコードを更新して Webトラフィックを WAF にリダイレクトする場合は、この CNAME アドレスに ping を送信して対応する WAF IP アドレスを取得します。 詳細は、「WAF デプロイメントガイド」をご参照ください。 一般に、WAF IP アドレスはほとんど変わりません。

- 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。
- （可选）(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。
- （可选）(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。

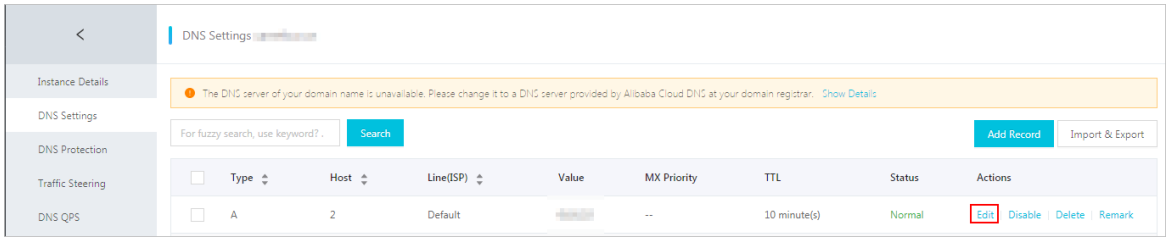


3. 操作する **ホスト (ホスト名)** を選択し、**[編集]** をクリックします。

   `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。



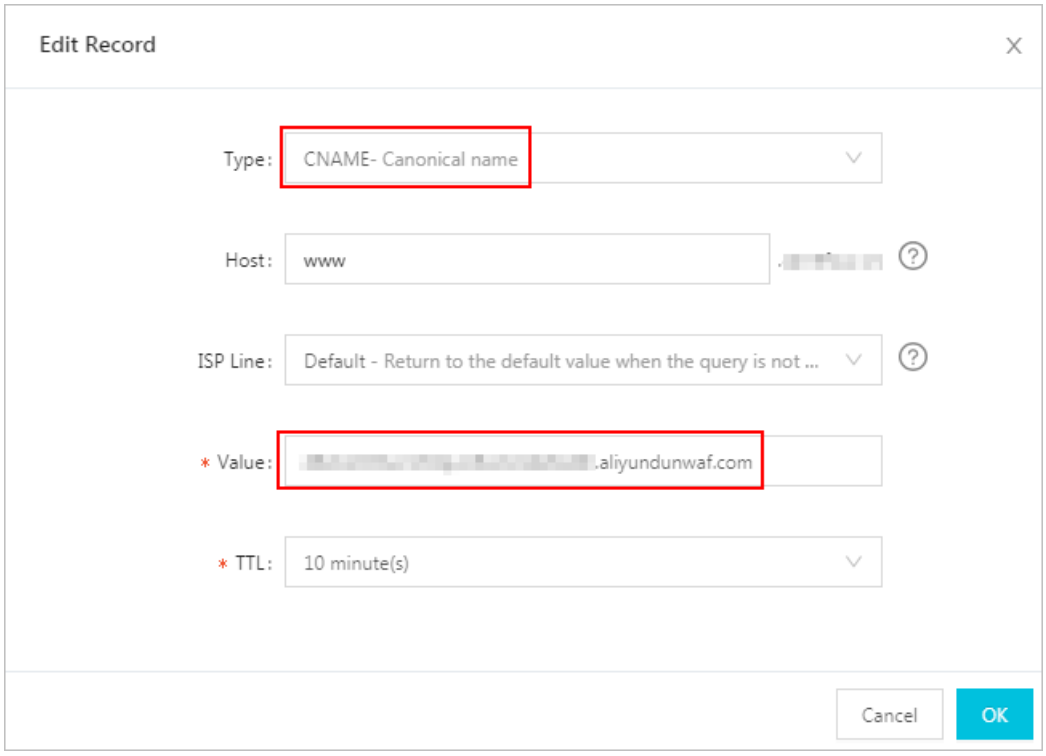
4. [レコードの編集] ダイアログボックスで、次の操作を行います。
   - タイプ: CNAME を選択します。
   - 値：WAF CNAME アドレスを入力します。
   - 他の設定はそのままにします。 TTL 値を 10 分に設定することを推奨します。 TTL 値が大きいほど、DNS の伝達は遅くなります。

   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。

     > 説明　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. （可选）(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。

> 説明　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。

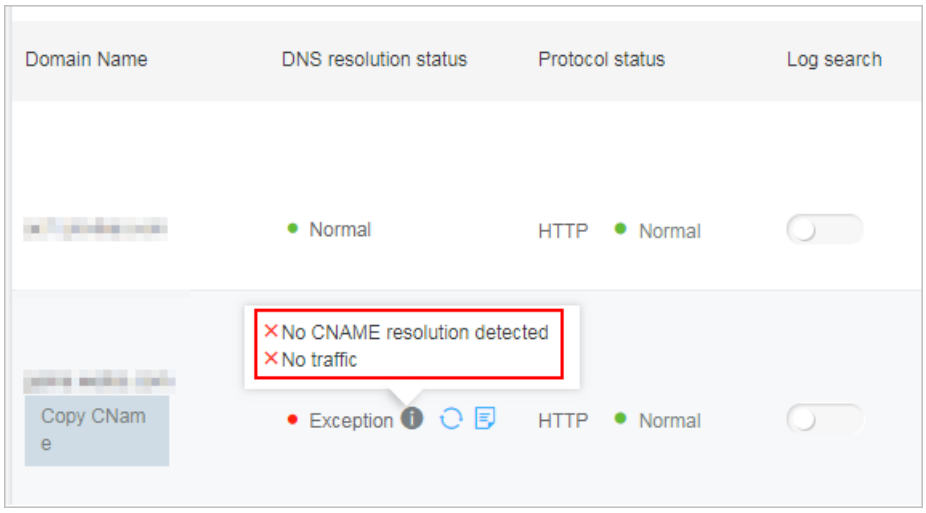
7. DNS 解決ステータスを確認します。
   i. Alibaba Cloud WAF コンソールにログインします。

ii. **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。

  > 説明 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。
  i. 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。
  ii. 次のコマンドを実行します。 `ping “copied WAF Cname address”`
  iii. 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。

1.4. 配信元サーバーの保護

配信元サーバーの IP アドレスが公開されている場合、攻撃者はそれを悪用して Alibaba Cloud WAF を迂回し、配信元サーバーに対して直接配信元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には、配信元サーバーにセキュリティグループ (ECS 配信元) またはホワイトリスト (SLB 配信元) を設定します。

背景

> 説明　本ページで説明されている設定は必須ではありません。 ただし、IP 公開によって発生する可能性があるリスクを排除するために設定することを推奨します。

次のように、配信元サーバーにこのようなリスクがあるかどうかを確認します。

Telnet を使用して、Alibaba Cloud 以外のホストから配信元サーバーのパブリック IP アドレスのリスナーポートへの接続を確立します。 接続が成功したかどうかを確認します。 接続に成功した場合、配信元サーバーは露出のリスクに直面しています。 ハッカーはパブリック IP アドレスを取得すると、WAF を迂回して配信元サーバーに到達可能です。 接続に失敗した場合、配信元サーバーは安全です。

たとえば、WAF が有効な配信元サーバ IP のポート 80 と 800 への接続をテストします。 接続が正常に確立された場合、配信元サーバーは安全ではありません。

```
Last login: Tue Jul 31 13:48:10 on ttys000
[                          1$ telnet 4           80
Trying (          )5...
Connected to (          )5.
Escape character is '^]'.
^ZConnection closed by foreign host.
```

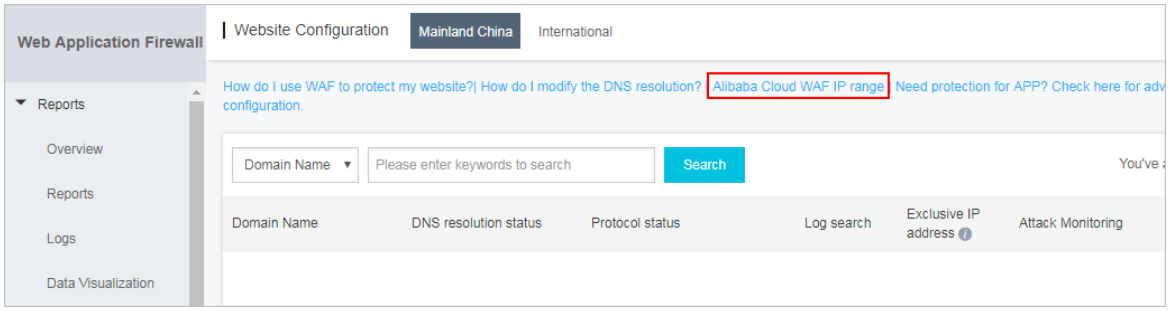
注記

セキュリティグループの設定には一定のリスクがあります。 次の点を考慮します。

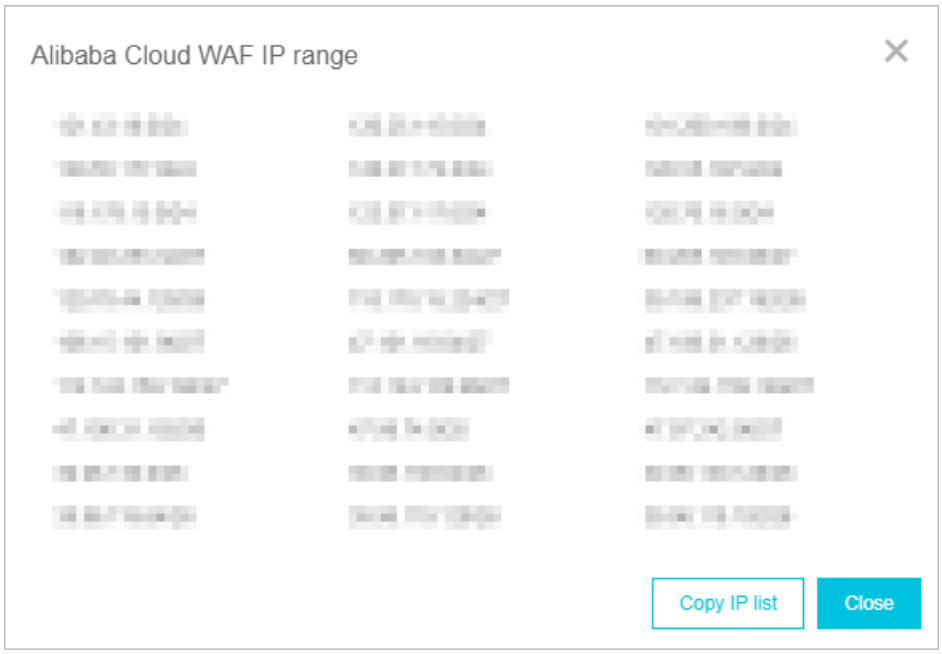
- 配信元サーバー (ECS または SLB インスタンス) でホストされているすべてのドメイン名が Alibaba Cloud WAF にデプロイされていることを確認します。
- WAF で検査されたトラフィックがスタンバイルートを介して配信元サーバーに返される Alibaba Cloud WAF クラスター障害の場合、配信元サーバーでセキュリティグループポリシーが有効になっていると、サイトへのアクセスが影響を受けます。
- Alibaba Cloud WAF の IP アドレスを拡張する場合、配信元サーバーでセキュリティグループポリシーが有効になっていると、訪問者に 5xx エラーページが頻繁に返されることがあります。

手順

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]** ページに移動します。
3. **[Alibaba Cloud WAF IP 範囲]** をクリックして WAF IP アドレスを表示します。



4. **[Alibaba Cloud WAF IP 範囲]** ダイアログボックスで、**[IP リストのコピー]** をクリックします。



5. 配信元サーバーのアクセス制御を設定して WAF IP アドレスのみを許可します。
   - **ECS 配信元の場合**
     a. ECS インスタンスリストに移動し、配信元インスタンス見つけ、**[管理]** をクリックします。
     b. 左側のナビゲーションウィンドウで、**[セキュリティグループ]**をクリックします。
     c. 操作するセキュリティグループを探し、**[ルールの追加]** をクリックします。
     d. **[セキュリティグループルールの追加]** をクリックし、次の設定を完了して最も優先度の高い WAF IP アドレスを許可します。
        - **NIC:** インターネットネットワーク
        - **ルールの方向:** Ingress
        - **アクション:** 許可
        - **プロトコル種別:** カスタム TCP
        - **権限付与タイプ:** Ipv4 CIRD ブロック
        - **ポート範囲:** 80/443
        - **権限付与オブジェクト:** 手順 4 でコピーした WAF IP アドレスを貼り付けます。
        - **優先度:** 1

e. 別のセキュリティグループルールを追加し、次のように設定して、優先順位が最も低いアクセスをすべてブロックします。
   - **NIC:** インターネットネットワーク
   - **ルールの方向:** Ingress
   - **アクション:** 禁止
   - **プロトコル種別:** カスタム TCP
   - **ポート範囲:** 80/443
   - **権限付与タイプ:** Ipv4 CIRD ブロック
   - **権限付与オブジェクト:** 0.0.0.0/0
   - **優先度:** 100

> 説明　配信元インスタンスが他の IP またはアプリケーションと対話する場合は、対応するルールを追加してアクセスを許可する必要があります。

- **SLB 配信元の場合**

  SLB インスタンスの設定は ECS と似ています。 WAF IP アドレスをホワイトリストに追加します。詳細は、「アクセス制御の設定」をご参照ください。

  - アクセス制御リストの作成
  - WAF IPアドレスを IP ホワイトリストに追加
  - IP ホワイトリストの有効化

1.5. WAF back-to-origin CIDR ブロックからのアクセスを許可

WAF は、指定された back-to-origin CIDR ブロックを使用して、通常のトラフィックをオリジンサーバーに転送します。 back-to-origin CIDR ブロックからのインバウンドトラフィックを許可するには、WAF コンソールに Web サイトを追加するときに、オリジンサーバーのセキュリティソフトウェア、またはアクセス制御ポリシーを設定する必要があります。

背景

オリジンサーバーに FortiGate などのセキュリティソフトウェアを使用する場合は、ソフトウェアのホワイトリストに、WAF back-to-origin CIDR ブロックを追加する必要があります。 これにより、WAF によってオリジンサーバーに転送される通常のトラフィックが、アクセス制御ポリシーによってブロックされるのを防ぐことができます。

セキュリティ上の理由により、WAF back-to-origin CIDR ブロックからのインバウンドトラフィックのみを許可する場合は、オリジンサーバーのアクセス制御ポリシーを設定することを推奨します。 これにより、攻撃者が WAF をバイパスして、直接オリジンサーバーを攻撃するのを防ぐことができます。 詳細については、「配信元サーバーの保護」をご参照ください。

2020 年 4 月 30 日に追加された back-to-origin CIDR ブロック

2020 年 4 月 30 日、WAF クラスターがスケールアウトされた後、次の back-to-origin CIDR ブロックが追加されました。

- 中国本土のリージョン： `39.96.158.0/24,47.110.182.0/24,120.77.139.0/25,47.102.187.0/25`

- 中国本土以外のリージョン： 47.56.50.0/24,161.117.161.0/25,147.139.22.0/25,8.209.192.0/25

> 警告 オリジンサーバーの IP アドレスホワイトリストやセキュリティグループの設定で WAF back-to-origin CIDR ブロックのみがアクセスできるようになっている場合、新しい WAF back-to-origin CIDR ブロックをホワイトリストに追加する必要があります。 追加しない場合、WAF によって転送された back-to-origin トラフィックが、オリジンサーバーのアクセス制御ポリシーによってブロックされ、アクセスが拒否される可能性があります。

新しい back-to-origin CIDR ブロックを、適切なタイミングで IP アドレスホワイトリストに追加することを推奨します。

WAF back-to-origin CIDR ブロックを取得する

WAF インスタンスのリージョンに基づいて、次の表から back-to-origin CIDR ブロックを取得するか、次の手順に従ってWAF コンソールから、最新の back-to-origin CIDR ブロックを取得できます。

WAF インスタンスのリージョン	back-to-origin CIDR ブロック
中国本土リージョン	121.43.18.0/24,120.25.115.0/24,101.200.106.0/24,120.55.177.0/24,120.27.173.0/24,120.55.107.0/24,123.57.117.0/24,120.76.16.0/24,182.92.253.32/27,60.205.193.64/27,60.205.193.96/27,120.78.44.128/26,118.178.15.0/24,39.106.237.192/26,106.15.101.96/27,47.101.16.64/27,47.106.31.0/24,47.98.74.0/25,47.97.242.96/27,112.124.159.0/24,39.96.130.0/24,39.96.119.0/24,47.99.20.0/24,47.104.53.0/26,47.108.23.192/26,39.104.199.128/26,39.96.158.0/24,47.110.182.0/24,120.77.139.0/25,47.102.187.0/25
中国本土以外のリージョン	47.89.1.160/27,47.89.7.192/26,47.88.145.96/27,47.88.250.0/24,47.52.120.0/24,47.254.217.32/27,47.88.74.0/24,47.89.132.224/27,47.91.69.64/27,47.91.54.128/27,47.74.160.0/24,47.91.113.64/27,149.129.211.0/27,149.129.140.0/27,8.208.2.192/27,47.56.50.0/24,161.117.161.0/25,147.139.22.0/25,8.209.192.0/25 説明 Web サイトのオリジンサーバーが日本にデプロイされている場合は、8.209.192.0/25 back-to-origin CIDR ブロックを追加してください。

1.
2.
3.
4. プロダクト情報 ページの下部で、[WAF IP セグメント] セクションを見つけ、すべてのIPをコピー をクリックします。 [WAF IP セグメント] セクションに、最新の back-to-origin CIDR ブロックが表示されます。

次のステップ

WAF back-to-origin CIDR ブロックを取得したら、それらをオリジンセキュリティソフトウェアの IP アドレスホワイトリストに追加できます。

警告 WAF back-to-origin CIDR ブロックをオリジンサーバーの IP アドレスホワイトリストに追加しない場合、WAF によって送信された通常リクエストが拒否される可能性があります。 これにより、サービスが中断される場合があります。

2.WAF へのアクセス

2.1. 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。

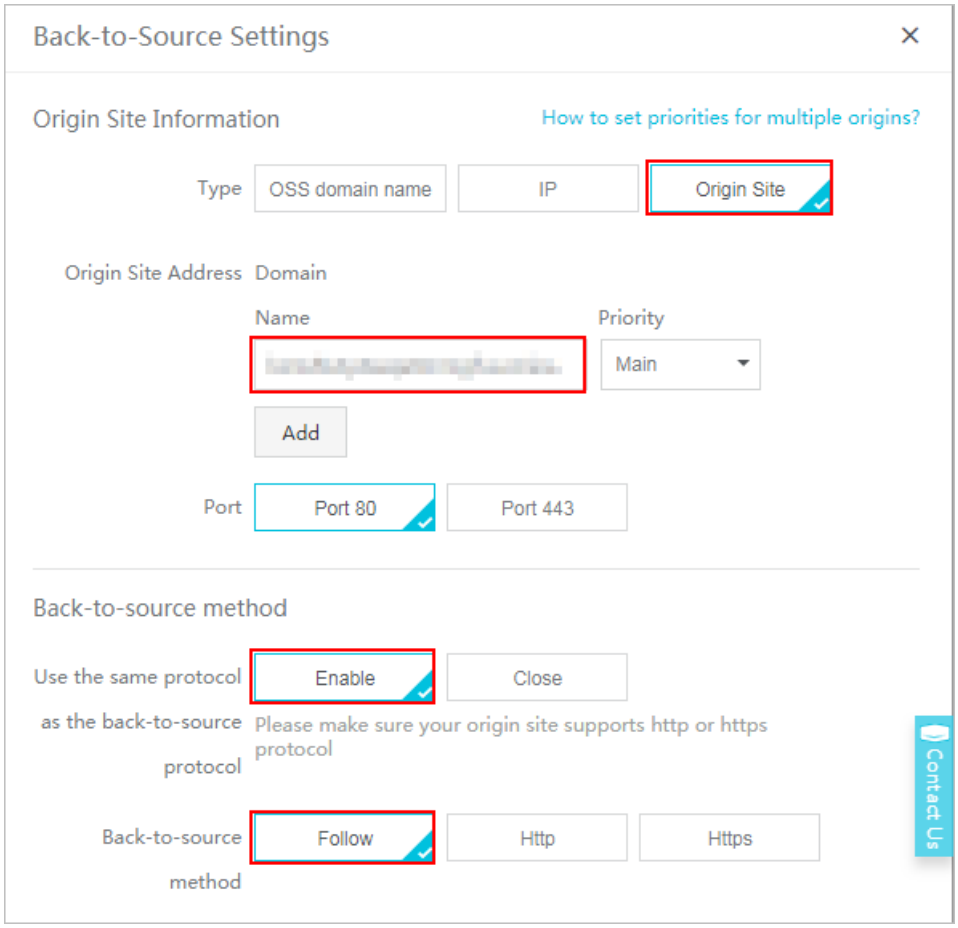
1. 「Alibaba Cloud CDN の使用の開始」を参照して、ドメイン名に CDN を実装します。
2. Alibaba Cloud WAF で Web サイト設定を作成します。
   - **ドメイン名**: CDN で使用可能なドメイン名を入力します。 ワイルドカードがサポートされています。
   - **サーバー アドレス**: ECS および Server Load Balancer インスタンスのパブリック IP アドレスまたは配信元サーバーの外部サーバーの IP アドレスを入力します。
   - **レイヤー 7 プロキシ (たとえば、Anti-DDoS/CDN) が有効に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。

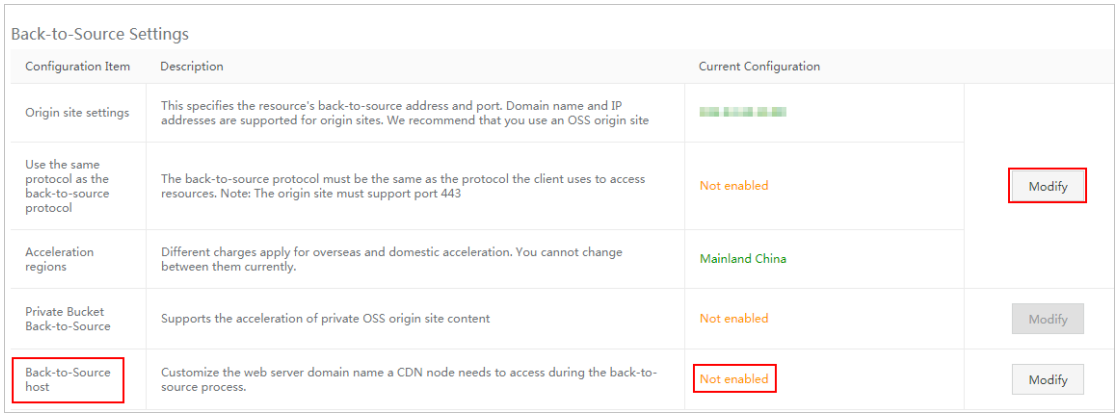
3. Web サイト設定が正常に作成されると、WAF は専用の CNAME アドレスを生成します。

> 説明　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。
   i. Alibaba Cloud CDN コンソールにログインします。
   ii. 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。
   iii. 配信元サイト設定の下の [変更]をクリックします。
   iv. 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。



v. **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。

2.2. 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。

手順

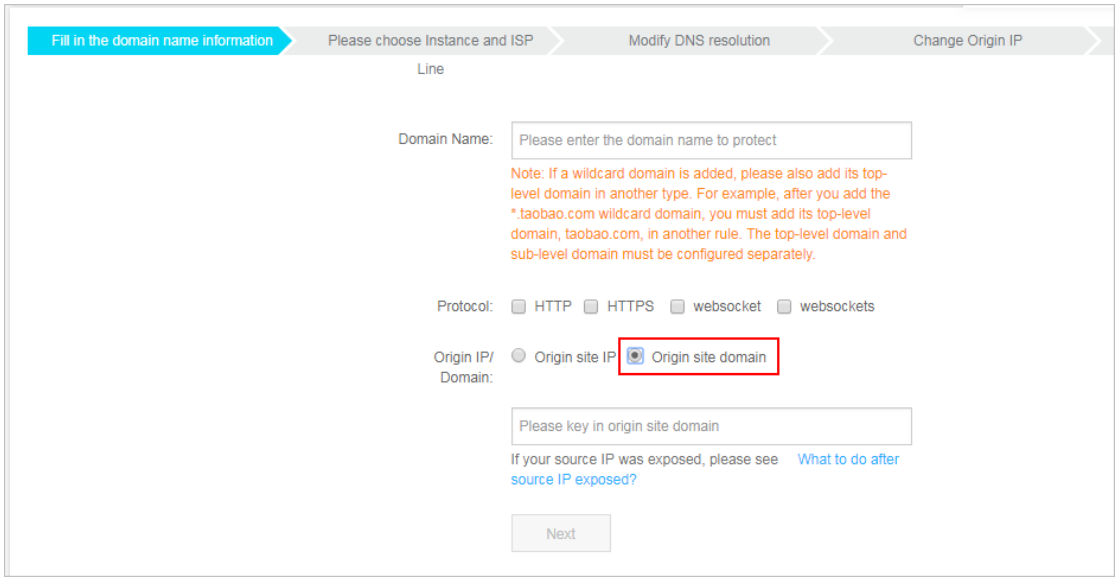
1. Alibaba Cloud WAF で Web サイト用の Web サイト設定を作成します。
   - **サーバーアドレス : [IP]をオンにし、ECS インスタンスおよび Server Load Balancer インスタンスのパブリック IP アドレスまたは外部サーバーの IP アドレスを入力します。**
   - **レイヤー 7 プロキシ (たとえば、Anti-DDoS/CDN) が有効になっているものがありますか? で [はい]をオンにします。**

   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。
   i. **[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。**

ii. 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。

> 説明　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。



iii. [次へ]をクリックします。

iv. 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。

実行結果

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。

3.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

> 説明 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

4.来訪者の送信元 IP アドレスの取得

来訪者のブラウザーが Web サイトにアクセスする際、通常は CDN、WAF、または Anti-DDoS Pro を経由するため、直接配信元サーバーに接続されることはありません。 一般的には、たとえば、「来訪者 > CDN/WAF/Anti-DDoS Pro > 配信元サーバー」のようなアーキテクチャになっています。 では、さまざまな段階を経て到達した来訪者からのリクエストについて、配信元サーバーはどのような方法で来訪者の送信元 IP アドレスを取得するのでしょうか。

オープンで透過的なプロキシサーバーは、経路上の次のサーバーにユーザーのリクエストを転送する際、X-Forwarded-For レコードを HTTP ヘッダーに追加します。 このレコードは、ユーザーの送信元 IP アドレスを記録するために使用され、 `X-Forwarded-For: user IP` の形式を取ります。 複数のプロキシサーバーがリクエストプロセスに関与している場合、 X-Forwarded-For レコードは `X-Forwarded-For: user's IP address, Proxy 1-IP address, Proxy 2-IP address, Proxy 3-IP address...` の形式で表示されます。

つまり、一般的なアプリケーションサーバーは、X-Forwarded-For レコードを使用して来訪者の送信元 IP アドレスを取得することができます。 以下のセクションでは、Nginx、IIS 6、IIS 7、Apache、および Tomcat サーバーでの X-Forwarded-For の設定方法を説明します。

> 注意 設定作業を行う前に、ECS スナップショットや Web サーバー構成ファイルなど、現在の環境をバックアップしてください。

Nginx

1. http_realip_module のインストール

負荷分散のため、Nginx では http_realip_module を使用して送信元の IP アドレスを取得します。

`# nginx -V | grep http_realip_module` コマンドを実行して、http_realip_module がインストールされているかどうかを確認します。 インストールされていない場合は、Nginx を再コンパイルして http_realip_module をロードします。

> 説明 Nginx がデフォルトの手順でインストールされている場合、http_realip_module はインストールされていません。

次のコードを使用して、 http_realip_module モジュールをインストールできます。

```
wget http://nginx.org/download/nginx-1.12.2.tar.gz
tar zxvf nginx-1.12.2.tar.gz
cd nginx-1.12.2
./configure --user=www --group=www --prefix=/alidata/server/nginx --with-http_stub_status_module
--without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
kill -QUIT `cat /alidata/server/nginx/logs/ nginx.pid.oldbin`
```

2. Nginx の設定に WAF IP アドレスを追加

`default.conf` を開き、 `location / {}` に次の内容を追加します。

```
set_real_ip_from ip_range1;
set_real_ip_from ip_range2;
...
set_real_ip_from ip_rangex;
real_ip_header X-Forwarded-For;
```

説明 `ip_range1,2,...,x` は、WAF の back-to-source IP アドレスを示し、それぞれに複数のエントリを追加する必要があります。

3. log_format の変更

log_format は、通常 `nginx.conf` の HTTP 設定の部分にあります。 *log_format* に *x-forwarded-for* を追加して、元の *remote-address* を置き換えます。 編集後の *log_format* の内容は以下のとおりです。

```
log_format main '$ http_x_forwarded_for-$ remote_user [$ time_local] "$ request"' '$ status $ body_byt
es_sent "$ http_referer"' '"$ http_user_agent"';
```

上記の操作が完了したら、 `nginx -s reload` を実行して Nginx を再起動し、設定を検証します。 設定が有効になると、Nginx サーバーは X-Forwarded-For フィールドに来訪者の IP アドレスを記録します。

IIS 6

F5XForwardedFor.dll プラグインがインストールされていれば、 IIS 6 のログから来訪者の送信元 IPアドレスを取得できます。

1. *F5XForwardedFor.dll* をサーバーの OS バージョンに応じて *x86\Release* または *x64\Release* ディレクトリから既定のディレクトリ (*C:\ISAPIFilters*) にコピーし、IIS プロセスにこのディレクトリの読み取り権限が付与されていることを確認します。
2. IIS マネージャーを開き、現在開いている Web サイトを右クリックしてプロパティを選択し、プロパティページを開きます。
3. [プロパティ] ページの **[ISAPI フィルター]** タブを選択し、**[追加]** をクリックします。
4. [追加] ウィンドウで次のパラメータを設定し、**[OK]** をクリックします。
   - **フィルター名:** F5XForwardedFor
   - **実行可能ファイル:** F5XForwardedFor.dll の完全パスを入力します。 今回の例では、*C:\ISAPIFilters\F5XForwardedFor.dll* です。
5. IIS サーバーを再起動し、設定が有効になるのを待ちます。

IIS 7

F5XForwardedFor モジュールを使用すると、来訪者の送信元 IP アドレスを取得できます。

1. *F5XFFHttpModule.dll* および *F5XFFHttpModule.ini* をサーバーの OS バージョンに応じて *x86\Release* または *x64\Release* ディレクトリから既定のディレクトリ (*C:\x_forwarded_for\x86* および *C:\x_forwarded_for\x64*) にコピーし、 IIS プロセスに各ディレクトリの読み取り権限が付与されていることを確認します。

2. IIS マネージャーで、[モジュール] をダブルクリックして開きます。
3. [ローカルモジュールの構成] をクリックします。
4. [ローカルモジュールの構成] ダイアログボックスの [登録] をクリックして、ダウンロードした DLL ファイルを登録します。
   - x_forwarded_for_x86 モジュールの登録
     - 名前: x_forwarded_for_x86
     - パス: *C:\x_forwarded_for\x86\F5XFFHttpModule.dll*
   - x_forwarded_for_x64 モジュールの登録
     - 名前: x_forwarded_for_x64
     - パス: *C:\x_forwarded_for\x64\F5XFFHttpModule.dll*
5. 登録後、新しく登録されたモジュール (x_forwarded_for_x86 および x_forwarded_for_x64) を選択し、[OK] をクリックして有効にします。
6. 登録されたDLLをそれぞれ [ISAPIおよびCGIの制限] に追加し、設定を[許可しない] から [許可] に変更します。
7. IIS サーバーを再起動し、設定が有効になるまで待ちます。

Apache

Apache で来訪者の送信元 IP アドレスを取得するには、次の手順に従います。

1. 次のコードを実行して、Apache 用のサードパーティモジュール mod_rpaf をインストールします。

```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/alidata/server/httpd/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

2. Apache の設定ファイル `/alidata/server/httpd/conf/httpd.conf` を編集し、末尾に次の情報を追加します。

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips IP address
RPAFheader X-Forwarded-For
```

   `RPAFproxy_ips ip address` は、Server Load Balancer が提供するパブリック IP アドレスではありません。 Apache のログから特定の IP アドレスを取得できます。 通常、2 つの IP アドレスが含まれます。

3. IP アドレスの追加後、次のコマンドを実行して Apache を再起動します。

```
/alidata/server/httpd/bin/apachectl restart
```

Tomcat

次の手順に従って、Tomcat サーバーの X-Forwarded-For 機能を有効にできます。

tomcat/conf/server.xml を開き、AccessLogValve を次の内容に変更します。

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T" resolveHosts="false"/>
```