

Alibaba Cloud Web#用防火#

ウェブサイトアクセス

Document Version20200701

目次

| | |
|---|-----------|
| 1 Website access with CNAME..... | 1 |
| 2 Web サイトの設定..... | 2 |
| 3 WAF back-to-origin CIDR ブロックの更新..... | 11 |
| 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..... | 12 |
| 5 WAF デプロイメントガイド..... | 14 |
| 6 WAF へのアクセス..... | 20 |
| 6.1 HTTPS 証明書の更新..... | 20 |
| 6.2 HTTPS の詳細設定..... | 23 |
| 6.3 サポート対象の非標準ポート..... | 25 |
| 6.4 WAF back-to-origin フローのマーク..... | 26 |
| 6.5 複数の配信元 IP 間の負荷分散..... | 28 |
| 6.6 WAF と CDN の同時デプロイ..... | 29 |
| 6.7 WAF と Anti-DDoS Pro の同時デプロイ..... | 33 |
| 7 来訪者の送信元 IP アドレスの取得..... | 35 |

1 Website access with CNAME

2 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。

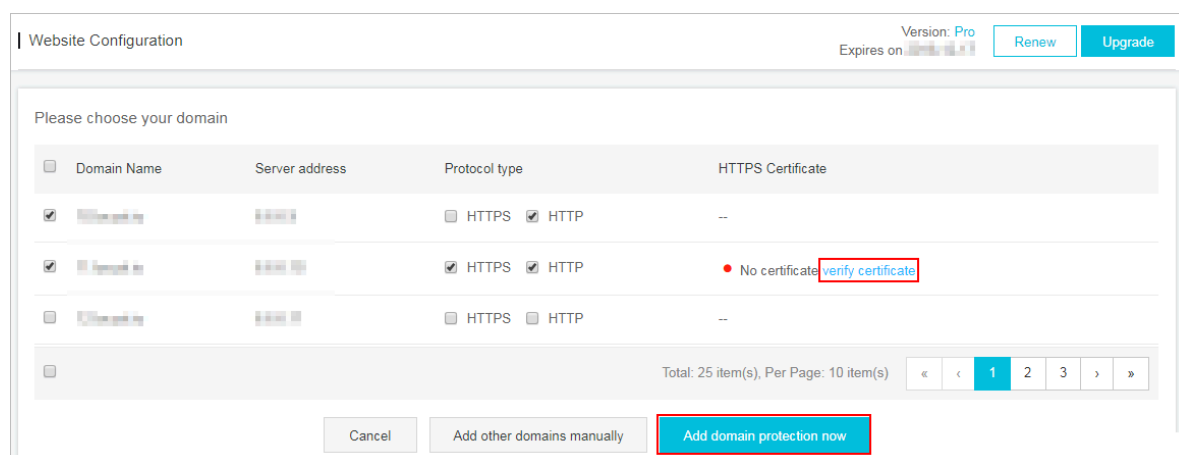
- (中国本土リージョンの場合) Web サイトは、産業情報技術省 (MIIT) によって ICP ライセンスが付与されています。

- (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。



The screenshot shows the 'Website Configuration' interface. At the top right, it indicates 'Version: Pro' and 'Expires on' with 'Renew' and 'Upgrade' buttons. Below this is a table titled 'Please choose your domain'. The table has four columns: 'Domain Name', 'Server address', 'Protocol type', and 'HTTPS Certificate'. There are three rows of domain entries. The second row is selected, and its 'HTTPS Certificate' column contains a red dot and the text 'No certificate' with a red box around the 'verify certificate' link. At the bottom of the table, there are buttons for 'Cancel', 'Add other domains manually', and 'Add domain protection now' (highlighted with a red box). A pagination bar at the bottom of the table shows 'Total: 25 item(s), Per Page: 10 item(s)' and page numbers 1, 2, 3.

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。

verify certificate

The current domain name type is HTTPS. You must import a certificate and private key to implement normal website protection.

Domain name: [dropdown]

Certificate name : [input field]

Certificate file ⓘ : [input field]

Private key file ⓘ : [input field]

Verify Cancel

- 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。



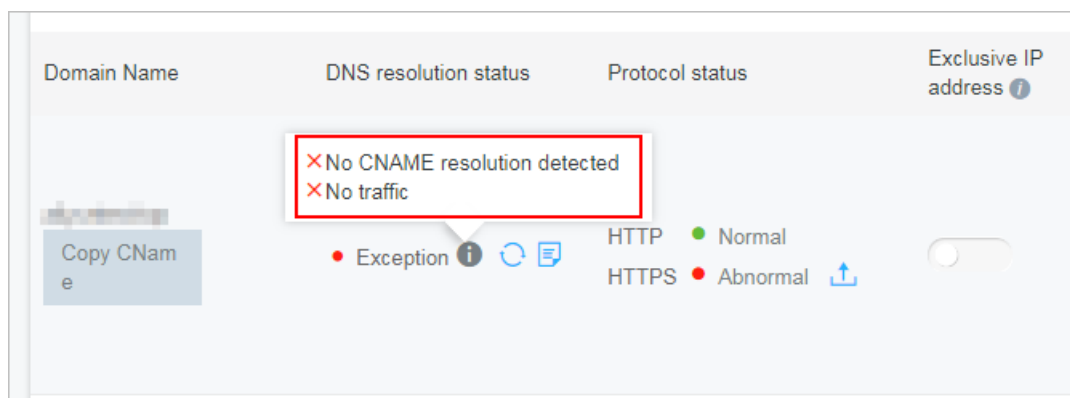
注：

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りますことを示します。

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 | <p>保護するドメイン名を入力します。</p> <p> 注：</p> <ul style="list-style-type: none"> • *.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 | <p>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</p> <div data-bbox="507 371 1434 763" style="background-color: #f0f0f0; padding: 10px;"> <p> 注:</p> <ul style="list-style-type: none"> 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。 </div> |
| サーバーアドレス | <p>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。</p> <ul style="list-style-type: none"> (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。 <div data-bbox="544 1081 1434 1429" style="background-color: #f0f0f0; padding: 10px;"> <p> 注:</p> <ul style="list-style-type: none"> 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。 </div> <ul style="list-style-type: none"> 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。 <div data-bbox="544 1581 1434 1977" style="background-color: #f0f0f0; padding: 10px;"> <p> 注:</p> <ul style="list-style-type: none"> 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。 </div> |

| 設定 | 説明 |
|---|---|
| サーバーポート | <p>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。</p> <ul style="list-style-type: none"> • 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。 <p> 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。</p> |
| レイヤ 7 プロキシ (例えば Anti-DDoS または CDN) は有効ですか？ | <p>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。</p> |
| 負荷分散アルゴリズム | <p>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</p> |
| フローマーク | <p>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。</p> <p> 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。</p> |

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。

3 WAF back-to-origin CIDR ブロックの更新

Alibaba Cloud Web Application Firewall (WAF) では、より優れた Web アプリケーション保護を提供するために、グローバル WAF サーバーのスペックを拡張し、サービス機能をさらに向上しています。スペックの拡張後、WAF の WAF back-to-origin CIDR ブロックは拡張されます。

Web のオリジンサーバーにアクセス制御用の IP ホワイトリストまたはセキュリティグループ設定がある場合、WAF back-to-origin CIDR ブロックからのアクセスのみ許可するには、次の新しい 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。そうしない場合、WAF によってオリジンサーバーに転送されるトラフィックが、アクセス制御ポリシーによってブロックされ、期待どおりに Web サイトにアクセスできません。



注：

新しい back-to-origin CIDR ブロックを追加するだけでなく、今回、一部の既存の CIDR ブロックも更新されています。新しい CIDR ブロックを慎重に確認します。

中国本土インスタンス用の新しい **WAF back-to-origin CIDR** ブロック

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

国際インスタンス用の新しい **WAF back-to-origin CIDR** ブロック

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, 47.89.7.224/27, 8.208.2.192/27

また、Web Application Firewall 管理コンソールにログインし、**[管理] > [Web サイト設定]** ページに移動して、最新の WAF back-to-origin CIDR ブロックを確認することもできます。

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_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

- 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 xxxxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com 応答の WAF IP アドレスを確認します。

```
C:\Users\web-admin>ping xxxxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com

Pinging xxxxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com [111.77.42.195] with 32
bytes of data:
Reply from 111.77.42.195: bytes=32 time=2ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
```

- 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。

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
0.0.0.0 cert.bandicam.com
#       ::1           localhost
111.77.42.195 www.aliyundemo.cn
```

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。

```
C:\Users\web-admin>ping www.aliyundemo.cn

Pinging www.aliyundemo.cn [111.77.42.195] with 32 bytes of data:
Reply from 111.77.42.195: bytes=32 time=2ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
```

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、

5 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。

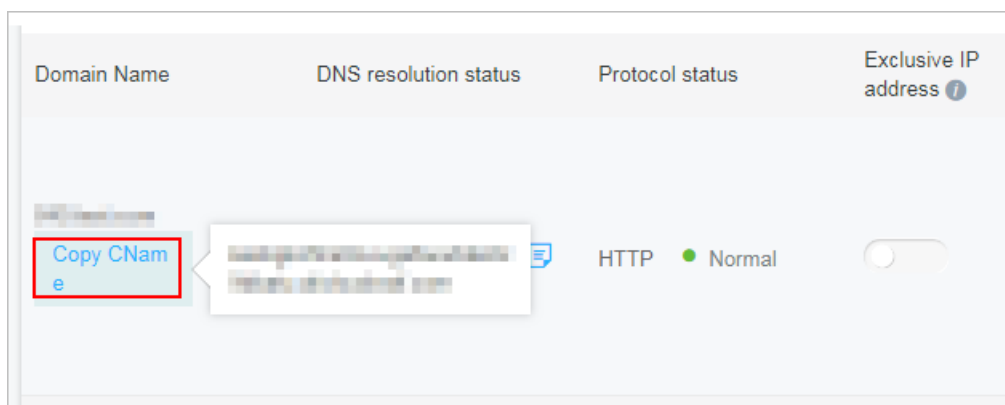
- [Alibaba Cloud WAF と CDN を合わせたデプロイ](#): CDN と WAF を一緒に Web サイトにデプロイする方法を説明します。
- [Alibaba Cloud WAF と DDoS 保護を合わせたデプロイ](#): Web サイトに DDoS 保護と WAF を一緒にデプロイする方法を説明します。

(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：

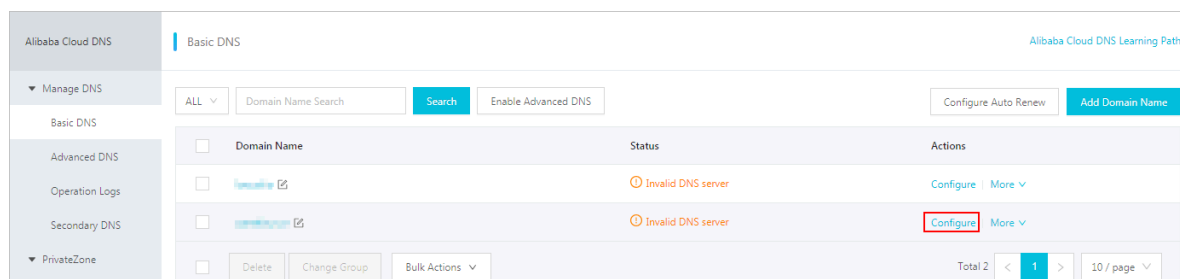
A レコードを更新して Web トラフィックを WAF にリダイレクトする場合は、この CNAME アドレスに ping を送信して対応する WAF IP アドレスを取得します。詳細は、「[WAF デプロイメントガイド](#)」をご参照ください。一般に、WAF IP アドレスはほとんど変わりません。

- 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。

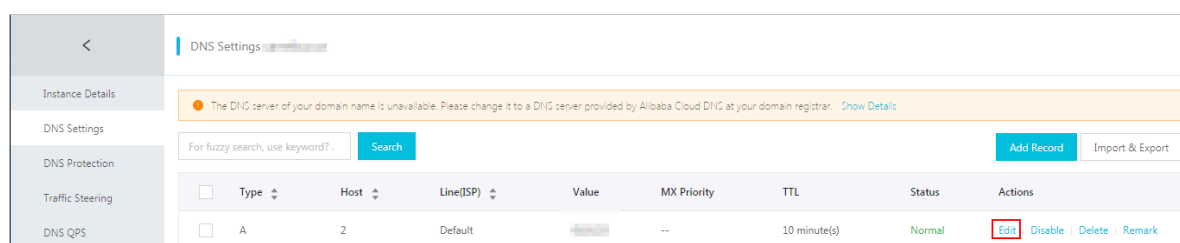
1. **Alibaba Cloud DNS コンソール**にログインします。
2. 操作するドメインを選択して、[設定] をクリックします。



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。

The screenshot shows the 'Edit Record' dialog box with the following fields:

- Type: CNAME- Canonical name
- Host: www
- ISP Line: Default - Return to the default value when the query is not ...
- * Value: [redacted] .aliyundunwaf.com
- * TTL: 10 minute(s)

Buttons: Cancel, OK

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。

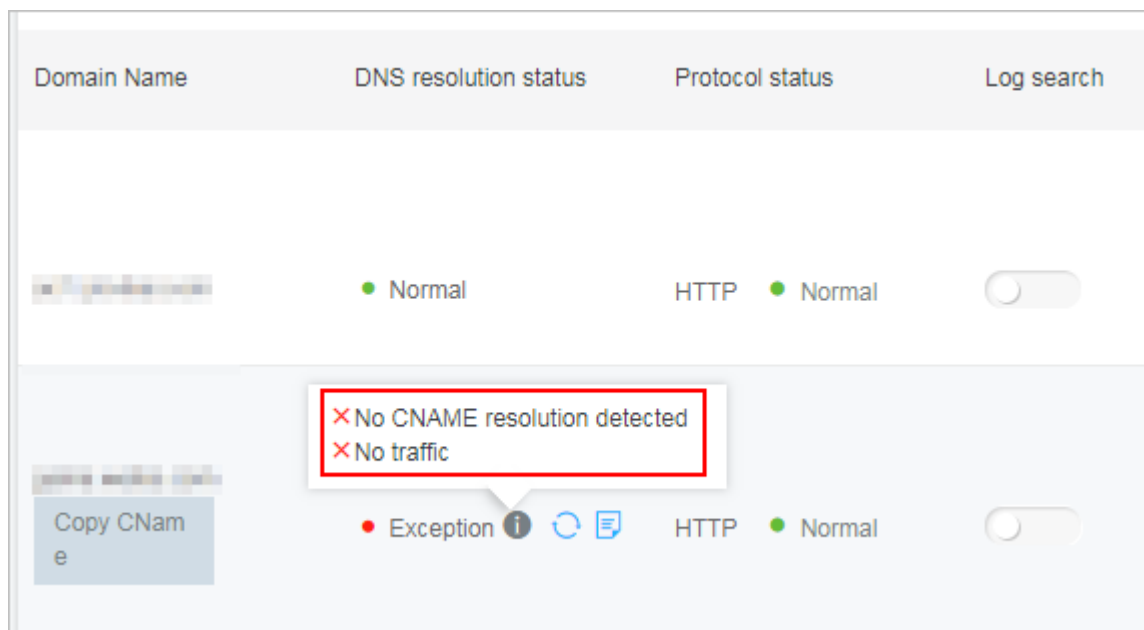
- **Normal:** Alibaba Cloud WAF は正常にデプロイされ、Web トラフィックは WAF によってモニタリングされています。
- **Exception:** "CNAME 解決が検出されませんでした"、"トラフィックなし"、または "DNSチェックに失敗しました" の例外メッセージの場合、DNS 設定が正しくない可能性があります。

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。

6 WAF へのアクセス

6.1 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。

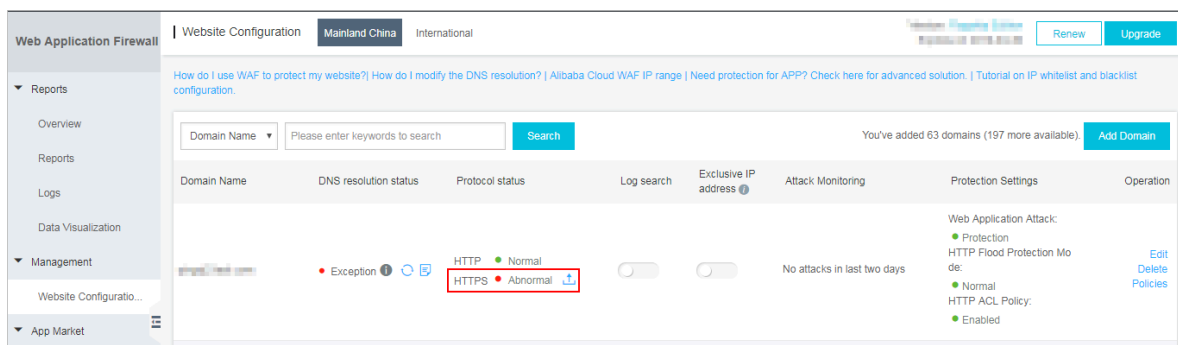
統合管理のために証明書ファイルを [Alibaba Cloud SSL Certificate Service](#)にアップロードした場合は、再度アップロードする代わりに次の手順で直接再利用します。

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。




```
DADTPZoOHD9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7jt8zSDGM9sTMThL
yvsmLQKBgQ
Cr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJ
aiygoIYo
aMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDz
FdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

Update certificate
✕

The current domain name type is HTTPS. You must import a certificate and private key to implement normal website protection.

Upload method : Manual upload Select existing certificate

Domain name:

Certificate name :

Certificate file ⓘ :

Private key file ⓘ :

Save
Cancel

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。

Web Application Firewall
Website Configuration
Mainland China
International
Renew Upgrade

How do I use WAF to protect my website? | How do I modify the DNS resolution? | Alibaba Cloud WAF IP range | Need protection for APP? Check here for advanced solution. | Tutorial on IP whitelist and blacklist configuration.

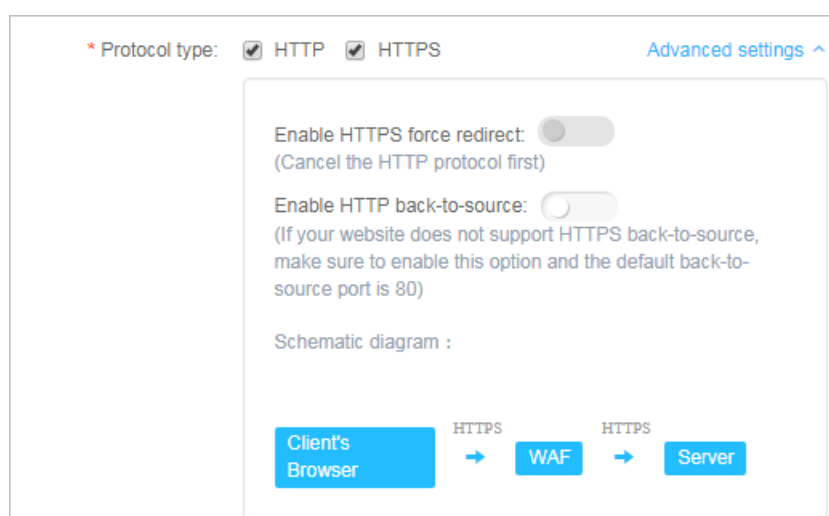
Domain Name Please enter keywords to search You've added 63 domains (197 more available)

| Domain Name | DNS resolution status | Protocol status | Log search | Exclusive IP address ⓘ | Attack Monitoring | Protection Settings | Operation |
|----------------------|--|--|-------------------------------------|-------------------------------------|-----------------------------|--|---|
| <input type="text"/> | ● Exception ⓘ | HTTP ● Normal HTTPS ● Normal <input type="button" value="↓"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | No attacks in last two days | Web Application Attack: ● Protection HTTP Flood Protection Mode: ● Normal HTTP ACL Policy: ● Enabled | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Policies"/> |

6.2 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

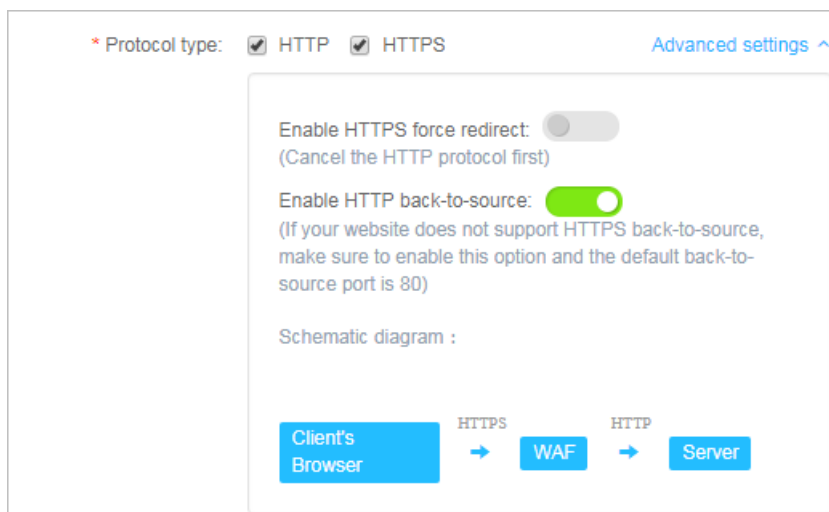
[HTTP back-to-source] を有効にして、Alibaba Cloud WAF と配信元サーバーの間の HTTP 通信を有効にします。これにより、WAF は検査したトラフィックを配信元サーバーのデフォルトポート 80 に返します。



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。



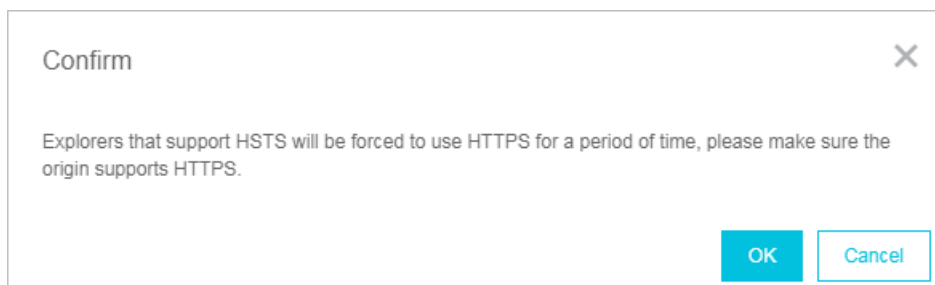
- **HTTPS** 強制リダイレクトの有効化

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。

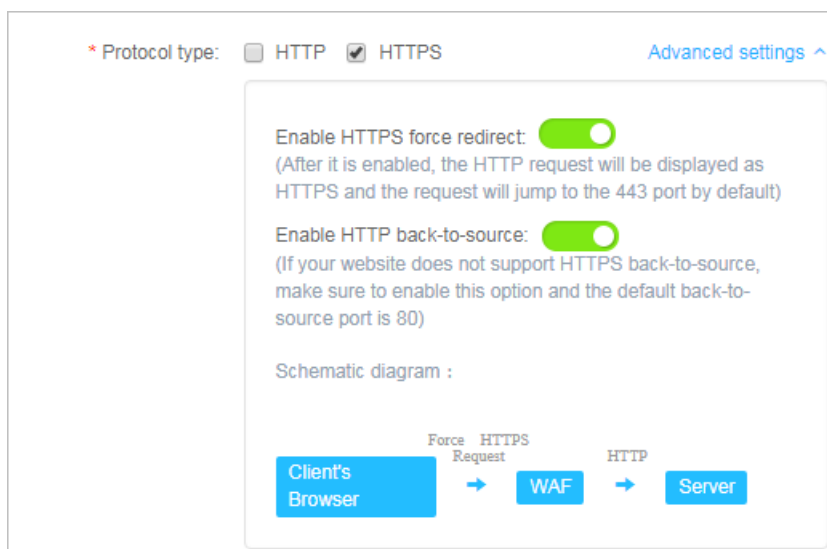
 注：

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。



6.3 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



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

6.4 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ー定義の 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。

| | |
|--|---|
| Flow Mark: | <input type="text" value="Header Field"/> |
| | <input type="text" value="Header Field Value"/> |
| <p>Note: If the user-defined header field already has a value, the value is overwritten with the WAF flow mark value. If the header field is already used, the field is overwritten with the flow mark filed setting</p> | |

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。

6.5 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。

* Domain name:

It supports top-level domain names (e.g. test.com) and second-level domain names (e.g. www.test.com). They have no impact on each other. Please fill in your actual domain name.

* Protocol type: HTTP HTTPS

* Server address: IP Other addresses

Please separate up to 20 IPs with commas (","). Line breaks are not allowed.

* Server port: HTTP 80 [Custom](#)

Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?: yes no [i](#)

Load balancing algorithm: IP HASH Round-robin

Flow Mark:

Note: If the user-defined header field already has a value, the value is overwritten with the WAF flow mark value. If the header field is already used, the field is overwritten with the flow mark filed setting

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。

6.6 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

奨めます: 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。

* Domain name:

It supports top-level domain names (e.g. test.com) and second-level domain names (e.g. www.test.com). They have no impact on each other. Please fill in your actual domain name.

* Protocol type: HTTP HTTPS

* Server address: IP Other addresses

Please separate up to 20 IPs with commas (","). Line breaks are not allowed.

* Server port: HTTP 80 [Custom](#)

Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?: yes no [?](#)

Load balancing algorithm: IP HASH Round-robin

Flow Mark:

Note: If the user-defined header field already has a value, the value is overwritten with the WAF flow mark value. If the header field is already used, the field is overwritten with the flow mark filed setting

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。

Back-to-Source Settings

Origin Site Information [How to set priorities for multiple origins?](#)

Type OSS domain name IP Origin Site

Origin Site Address Domain

Name Priority

Add

Port Port 80 Port 443

Back-to-source method

Use the same protocol as the back-to-source protocol Enable Close

Please make sure your origin site supports http or https protocol

Back-to-source method Follow Http Https

Contact Us

- 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。

| Back-to-Source Settings | | |
|--|--|---|
| Configuration Item | Description | Current Configuration |
| Origin site settings | This specifies the resource's back-to-source address and port. Domain name and IP addresses are supported for origin sites. We recommend that you use an OSS origin site | |
| Use the same protocol as the back-to-source protocol | The back-to-source protocol must be the same as the protocol the client uses to access resources. Note: The origin site must support port 443 | Not enabled Modify |
| Acceleration regions | Different charges apply for overseas and domestic acceleration. You cannot change between them currently. | Mainland China |
| Private Bucket Back-to-Source | Supports the acceleration of private OSS origin site content | Not enabled Modify |
| Back-to-Source host | Customize the web server domain name a CDN node needs to access during the back-to-source process. | Not enabled Modify |

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。

6.7 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트리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。

The screenshot shows a multi-step configuration process. The first step, 'Fill in the domain name information', is active. It includes a 'Domain Name' input field with a placeholder 'Please enter the domain name to protect'. Below it is a note: 'Note: If a wildcard domain is added, please also add its top-level domain in another type. For example, after you add the *.taobao.com wildcard domain, you must add its top-level domain, taobao.com, in another rule. The top-level domain and sub-level domain must be configured separately.' There are four protocol options: HTTP, HTTPS, websocket, and websockets. Under 'Origin IP/Domain', the 'Origin site domain' radio button is selected and highlighted with a red box. Below it is an input field with the placeholder 'Please key in origin site domain'. A link 'What to do after source IP exposed?' is visible. A 'Next' button is at the bottom.

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。

7 来訪者の送信元 IP アドレスの取得

来訪者のブラウザが 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。



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。



注：
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;
```



注：

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_bytes_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"/>
```