Alibaba Cloud
Web Application Firewall

よくある質問

Document Version20190920

目次

1 WAF についてよくある質問

- Web Application Firewall は、クロスアカウント CDN + 高い防御 + WAF アーキテクチャをサポートしていますか?

Alibaba Cloud 外部のサーバーで WAF を利用できますか。

はい。WAF では、Alibaba Cloud の内部でも外部でも、インターネットを介してアクセス可能な Web サーバーやアプリケーションが保護されます。 AWS、Azure、その他のクラウドおよびデータセンターで Web サービスが保護されます。

> 注 :
> 中国本土内でアクセスされるドメイン名は、産業情報技術部で ICP ライセンスを申請する必要があります。

WAF はクラウド仮想ホストをサポートしていますか。

WAF の Business および Enterprise エディションは専用仮想ホストをサポートしています。 WAF を有効にしてから設定します。

共有ホストは共有 IP アドレスを使用します。つまり、配信元を複数のユーザーが使用するということです。 WAF を個別に設定しないことを推奨します。

HTTP フラッド攻撃を防ぐ方法を教えてください。

WAF では、通常モードと緊急モードで HTTP フラッド保護が提供されます。 実際の状況に基づいて保護モードを切り替えます。 詳細は、「HTTP フラッド保護モードの設定」をご参照ください。

保護効果を高め、誤検知率を下げるために、WAF Business エディションまたは WAF Enterprise エディションを使用して、セキュリティプロフェッショナルをカスタマイズまたはリクエストして、ターゲットとする保護ポリシーをカスタマイズします。 詳細は、「HTTP フラッド保護のカスタマイズ」をご参照ください。

WAF は HTTPS をサポートしていますか。

はい、WAF のすべてエディションで HTTPS 業務とワイルドカードドメイン名を完全にサポートしています。

必要に応じて SSL 証明書とキーをアップロードすると、WAF は HTTPS トラフィックを処理します。 WAF は、リクエストを配信元に戻す前に復号化し、データを調べてから再度暗号化します。

WAF はユーザー定義ポートをサポートしていますか。

WAF の Business および Enterprise エディションは、ユーザー定義の非標準ポートをサポートしています。 Business バージョンは最大 10 個の非標準ポートをサポートしており、Enterprise バージョンは最大 50 個の非標準ポートをサポートしています。

> 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。

WAF の QPS 制限は、WAF インスタンス全体でまとめられた QPS を目的としていますか。 それとも設定した 1 つのドメイン名に対する QPS 上限ですか。

WAF の QPS 制限は、すべての WAF インスタンスに対するものです。 たとえば、WAF の設定で 3 つのドメイン名を保護している場合、3 つのドメイン名の累積 QPS は上限を超えることはできません。 累積した QPS が WAF インスタンスの QPS 制限を超えると、レート制限がトリガーされ、パケット損失が発生する可能性があります。

悪意のある SMS に対するセキュリティが提供されるのは WAF のどのエディションですか。

WAF のすべてのエディションで悪意のある SMS に対するセキュリティが提供されます。 詳細は、「WAF エディションの選択方法」をご参照ください。

WAF の配信元 IP アドレスを ECS の内部ネットワーク IP アドレスに設定できますか。

WAF では、トラフィックはパブリックネットワークを介して配信元に返されます。 内部ネットワーク IP アドレスの直接入力はサポートしておりません。

WAF は CDN または Anti-DDoS IP と一緒に接続できますか。

WAF は CDN および Anti-DDoS サービスと完全に互換性があります。 基本アーキテクチャ: クライアント > Anti-DDoS > CDN > WAF > SLB > 配信元

Anti-DDoS または CDN とサービスを組み合わせるには、WAF の CNAME を Anti-DDoS または CDN 用配信元として入力する必要があります。 このアクションは、トラフィックが Anti-DDoS または CDN を通過した後に WAF に向けます。 その後、WAF はトラフィックを配信元に返します。

詳細は、「#unique_6」および「WAF で CDN を使用」をご参照ください。

WAF は 1 つのドメイン名の下で複数の配信元 IP アドレスを保護できますか。

はい。 個々のドメイン保護で、最大 20 個の配信元 IP が保持されます。 これらの IP はコンマで区切ります。 複数の配信元を 1 つのドメインに追加する場合、WAF はラウンドロビン方式に基づいてリクエストを負荷分散し、すべての配信元に対してヘルスチェックを実行します。 WAF

がどの配信元からの応答も得られなかった場合、WAF は通常の状態に戻るまでその配信元へのリクエストの転送を停止します。

複数の配信元が設定されている場合、WAF はどのように負荷を割り当てますか。

複数の配信元 IP アドレスを設定した場合、WAF は自動的にポーリングを使用して負荷分散を実行し、リクエストにアクセスします。

WAF はヘルスチェックをサポートしていますか。

WAF では、デフォルトでヘルスチェックは有効です。 WAF はすべての配信元 IP アドレスのアクセスステータスを確認します。 配信元 IP アドレスが応答しない場合、WAF は、IP アドレスのアクセスステータスが完全に回復するまで、リクエストを配信元 IP アドレスに転送しません。

WAF はセッション持続性をサポートしていますか。

はい、WAF はセッション持続性をサポートしています。 ただし、テクニカルサポートチームにチケットを送信して機能を有効にする必要があります。

WAF の 配信元 IP アドレスの変更中に、遅延が生じることはありますか。

特にありません。 WAF が保護する配信元 IP アドレスが変更されると、その変更は 1 分以内に有効になります。

変更した設定が WAF コンソールで有効になるのはいつですか。

概ね、変更した構成は 1 分以内に有効になります。

WAF の配信元 back-to-source IP アドレスとは何ですか。

Alibaba Cloud WAF コンソール の [管理] > [Web サイト設定] ページで、 back-to-source IP アドレスが表示されます。 詳細は、「WAF back-to-source IP アドレスの表示方法」をご参照ください。

WAF では back-to-source IP アドレスはセキュリティグループに自動的に追加されますか。

いいえ、WAF では back-to-source IP アドレスはセキュリティグループに自動的に追加されません。 配信元が他のファイアウォールまたはホストセキュリティ保護ソフトウェアと一緒にデプロイされている場合は、WAF back-to-source IP アドレスをホワイトリストに手動で追加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。

WAF の back-to-source を有効にするのに、クライアント IP アドレスからのアクセスをすべて許可する必要がありますか。

いいえ。サービスタイプによって WAF back-to-source IP アドレスまたはすべてのクライアントの IP アドレスしか許可できないためです。

Web サービスについては、WAF back-to-source IP のみ許可して配信元を保護することを推奨します。

HTTP フラッド攻撃の送信元 IP アドレスは WAF コンソールに表示されますか。

WAF Enterprise エディションの場合、サービス分析ページで HTTP フラッド攻撃の送信元 IP アドレスの全ログを表示します。

WAF が使用する帯域幅トラフィックを照会する方法を教えてください。

WAF コンソールの概要ページで、使用されている帯域幅トラフィック照会を示します。

WAF の HTTP ACL ポリシー内の IP フィールドは、ネットワークセグメントのエントリをサポートしていますか。

はい、WAF は HTTP ACL ポリシーの IP フィールドの IP ネットワークセグメントのエントリをサポートしています。

悪意のある IP ペナルティ機能を無効にした後、無効にした IP アドレスはどのくらいで回復しますか。

無効にした IP アドレスは、悪意のある IP ペナルティ機能が無効になると 6 分後にリリースされます。

WAF が提供する Anti-DDoS 機能の特徴は何ですか。

- WAF は各ユーザーに独立した IP アドレスを提供します。 これらの IP アドレスも Anti-DDoS ブラックホールポリシーの対象となり、ECS や Server Load Balancerと整合性があります。
- WAF のブラックホールしきい値は、現在のリージョンの ECS デフォルトしきい値と同じです。

Anti-DDoS Pro を購入して、Web サイトを DDoS 攻撃から保護します。

WAF は HTTPS 双方向認証をサポートしていますか。

いいえ。 WAF は HTTPS 双方向認証をサポートしておりません。

WAF は Websocket と HTTP 2.0 または SPDY プロトコルをサポートしていますか。

WAF は WebSocket プロトコルをすでにサポートしています。 ただし、現在、HTTP 2.0 と SPDY プロトコルはサポートしておりません。

WAF ではどの SSL プロトコルがサポートされていますか。

サポートしている SSL プロトコル:

- TLSv1
- TLSv1.1
- TLSv1.2

SSL 暗号スイートの例:

```
" ECDHE - RSA - AES256 - GCM - SHA384 : ECDHE - RSA - AES128 - GCM
 - SHA256 : DHE - RSA - AES256 - GCM - SHA384 : DHE - RSA - AES128 -
 GCM - SHA256 : ECDHE - RSA - AES256 - SHA384 : ECDHE - RSA - AES128
 - SHA256 : ECDHE - RSA - AES256 - SHA : ECDHE - RSA - AES128 - SHA :
 DHE - RSA - AES256 - SHA256 : DHE - RSA - AES128 - SHA256 : DHE - RSA
 - AES256 - SHA : DHE - RSA - AES128 - SHA : ECDHE - RSA - DES - CBC3
 - SHA : EDH - RSA - DES - CBC3 - SHA : AES256 - GCM - SHA384 : AES128
 - GCM - SHA256 : AES256 - SHA256 : AES128 - SHA256 : AES256 - SHA :
 AES128 - SHA : DES - CBC3 - SHA : HIGH :!  aNULL :!  eNULL :!  EXPORT
 :!  DES :!  MD5 :!  PSK :!  RC4 "
```

2 一般的な Web 脆弱性の定義

クロスサイト攻撃

説明

XSS (クロスサイトスクリプティング) は通常、クライアント側で発生します。 ハッカーはこれを使用して、フィッシング用に個人情報とパスワードを盗み、悪意のあるコードを送信します。 HTML、JavaScript、VBScript、および ActionScript は、XSS 攻撃を最も受けやすい技術です。

攻撃者は、クライアントに危害を加えるコードをサーバーに入力し、コードを使用して Web ページを偽造します。 ユーザーが Web ページを開くと、悪意のあるコードをユーザーのブラウザーに挿入して攻撃を仕掛けます。 その後、攻撃者はセッション Cookie を盗んで、パスワードやその他の機密情報を含むユーザーの個人情報を入手する可能性があります。

脅威

XSS 攻撃は Web サーバーに直接危害を及ぼしませんが、攻撃は Web サイト全体に広がり、ユーザーの機密アカウント情報とパスワードを盗みます。 この場合、Web サイトにも深刻な損害が生じる可能性があります。 XSS 攻撃により、以下の損害が生じる場合があります。

- フィッシング: 最も典型的な攻撃は、ターゲット Web サイトの反射的なクロスサイトスクリプティングの脆弱性を使用して、 Web サイトユーザーをフィッシング Web サイトにリダイレクトし、フィッシング JavaScript を挿入してターゲット Web サイトでフォームの入力をモニターし、さらに高度な DHTML ベースのフィッシング攻撃を仕掛けることです。
- Web サイトへのトロイの木馬の埋め込み: 一般的な攻撃には、クロスサイトアクセス中に IFrame を介して隠れた悪意のある Web サイトを埋め込む、悪意のある Web サイトに被害者をリダイレクトする、悪意のある Web サイトのダイアログボックスを表示するなどがあります。
- なりすまし: Cookie を使用して、ユーザーが特定の Web サイトを読み込んだときに、ユーザー ID を認証します。 XSS を悪用してユーザーの Cookie を盗み、Web サイトでの操作を実行するユーザーの許可を得ます。 Web サイト管理者の Cookie が盗まれた場合、Web サイトは深刻な脅威にさらされます。
- Web サイトユーザーの情報の盗難: ユーザーの Cookie を盗んでユーザー ID を取得すると、攻撃者はユーザーのアクセス許可をさらに取得し、Web サイトの操作を実行し、ユーザーの個人情報を見る可能性があります。

- スパム: XSS の脆弱性を悪用し、SNS コミュニティ内のターゲットユーザーグループに、被害者に代わって多くの迷惑な情報を送信します。
- ユーザーの Web 操作のハイジャック: 高度な XSS 攻撃は、ユーザーの Web 操作をハイジャックし、ユーザーの閲覧履歴と送受信したデータをモニターします。
- XSS ワーム: XSS ワームは、広告の掲載、トラフィックの生成、Web サイトへのトロイの木馬ウイルスの埋め込み、いたずら、オンラインデータの破損、および DDoS 攻撃の開始に使用されます。

CRLF 攻撃

説明

HTTP レスポンス分割は CRLF インジェクション攻撃とも呼ばれます。 CR と LF は、復帰文字と改行文字に対応します。

HTTP ヘッダーは、CRLF 文字の組み合わせで区切られた複数行で構成されています。 各行は“Key: Value”の構造になっています。 ユーザーが入力した値の一部に CRLF 文字が挿入されると、HTTP ヘッダー構造が変わる可能性があります。

脅威

攻撃者は、自己定義の HTTP ヘッダー情報 (セッション Cookie や HTML コードなど) を挿入することで、XSS 攻撃またはセッション固定の脆弱性攻撃を開始します。

Web SQL インジェクション

説明

Web SQL インジェクションは、アプリのデータベースレイヤーで発生するセキュリティ脆弱性です。 Web サイト制御のアクセス許可を違法に取得するために広く使用されています。

設計が不完全なアプリケーションは、入力文字列内の SQL 命令のチェックを見落とす可能性があります。 その結果、命令は誤って通常の SQL 命令として扱われ、データベースによって実行されます。 これが起こると、データベースは攻撃を受けやすくなり、データの盗難、改ざん、削除、さらには悪意のあるコードやバックドアが Web サイトに挿入されることもあります。

脅威

SQL インジェクション攻撃により、以下の損害が生じる可能性があります。

- 機密データが盗まれる可能性があります。
- コア業務データが改ざんされる可能性があります。
- Web ページが書き換えられる可能性があります。

- データベースサーバーが攻撃によってゾンビホストに変わったり、企業の Web サイトが攻撃されることもあります。

WebShell 攻撃

説明

WebShell 攻撃は、Web ページベースのトロイの木馬ウイルスを Web サイトサーバーに書き込み、サーバーを制御するよう構成された攻撃です。

脅威

攻撃者は Web ベースのバックドア型トロイの木馬を Web サイトに書き込み、その Web サイトでファイルを操作したりコマンドを実行したりする可能性があります。

ローカルファイルインクルージョン

説明

ローカルファイルインクルージョンは、アプリコードがインクルードファイルの処理を厳密に制御できない場合に発生する脆弱性の一種です。 その結果、攻撃者はアップロードされた静的ファイルまたは Web サイトのログファイルをコードとして実行することが可能となります。

脅威

攻撃者がこの脆弱性を悪用してサーバー上でコマンドを実行し、サーバーの操作権限を取得し、Web サイトの悪意のある削除やユーザーデータやトランザクションデータの改ざんなど、一連の悪影響が引き起こす可能性があります。

リモートファイルインクルージョン

説明

リモートファイルインクルージョンは、アプリコードがインクルードファイルの処理を厳密に制御できない場合に発生する脆弱性の一種です。 その結果、攻撃者はサーバー上で実行するためのリモートコードを含むパラメーターの構築が可能となります。

脅威

攻撃者がこの脆弱性を悪用してサーバー上でコマンドを実行し、サーバーの操作権限を取得し、Web サイトの悪意のある削除やユーザーデータやトランザクションデータの改ざんなど、一連の悪影響が引き起こす可能性があります。

リモートコード実行

説明

リモートでのコードの実行は、リスクの高いセキュリティの脆弱性です。 これにより、攻撃者はサーバーコードの脆弱性を悪用して、サーバー上で悪意のあるコードを入力して実行することができます。

脅威

攻撃者はこの脆弱性を悪用してサーバー上でアセンブルされたコードを実行する可能性があります。

FastCGI 攻撃

説明

FastCGI 攻撃は Nginx の深刻なセキュリティ上の脆弱性です。 デフォルトでは、FastCGI モジュールにより、サーバーは PHP モードのファイルタイプを誤って解析することがあります。

脅威

悪意のある攻撃者は、PHP をサポートしている Nginx サーバーを破壊する可能性があります。

3 ローカル hosts ファイルを変更して WAF をテスト

hosts ファイルの場所

```
C :\ Windows \ System32 \ drivers \ etc \ hosts
```

hosts ファイルの機能

hosts ファイルは、ドメイン名と IP アドレスの対応を指定します。 ドメイン名に hosts ファイルで指定された IP アドレスがある場合、システムはこのドメイン名にアクセスするときに DNS (Domain Name System) によってその IP アドレスを解決せず、代わりに指定された IP アドレスに直接アクセスします。

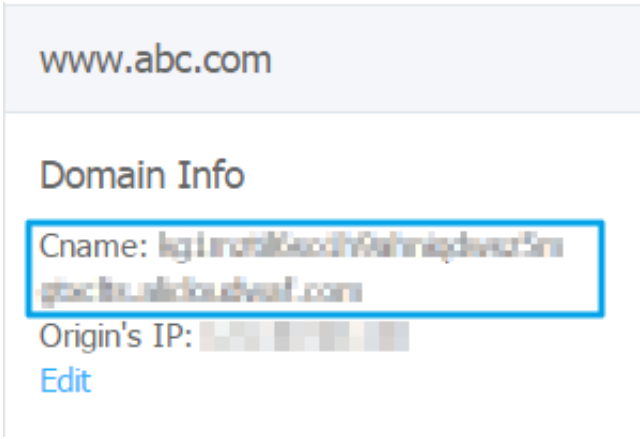
したがって、Web サイトが Anti-DDoS Pro サービスまたは WAF サービスを使用してデプロイされている場合は、オンラインの業務フローを変更することなく、ローカルの hosts ファイルを変更して Web サイトを WAF に誘導します。 これにより、業務サービスが WAF を通過した後に正常に機能するかどうかのテストが可能です。

手順

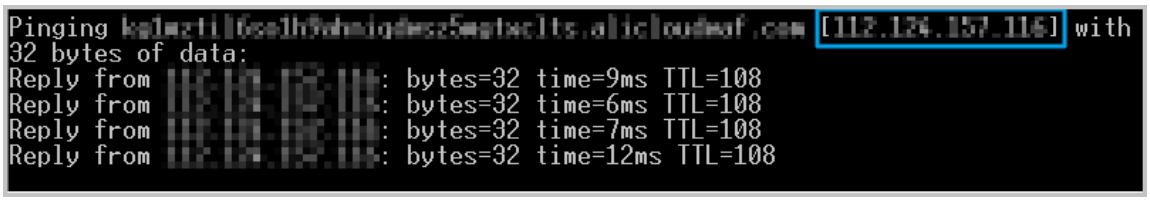
1. WAF に割り当てられた IP アドレスを見つけます。

   ドメイン名が設定されると、WAF は解決目的で CNAME レコードを生成します。 ping コマンドを使用して CNAME レコードの IP アドレスを取得します。この IP アドレスは WAF IP です。 例として www.abc.com を使用します。

   a. Alibaba Cloud WAF 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、WAF CNAME アドレスを表示します。

   b. ping コマンドを使用して、CNAME レコードの IP アドレスを取得します。

2. *C :\ Windows \ System32 \ drivers \ etc * フォルダーを検索します。
3. メモ帳で hosts ファイルを開き、ドメイン名に WAF の IP アドレスを指定します。

   hosts ファイルの形式は `< IP > < domain name >` です。 たとえば、www.abc.com を `xx . xx . xx . xxx . xx . xx . xx . xxx www . abc . com` に指定します。

4. 変更した hosts ファイルを *C :\ Windows \ System32 \ drivers \ etc * フォルダーに保存します。

4 DNS 解決ステータスの例外

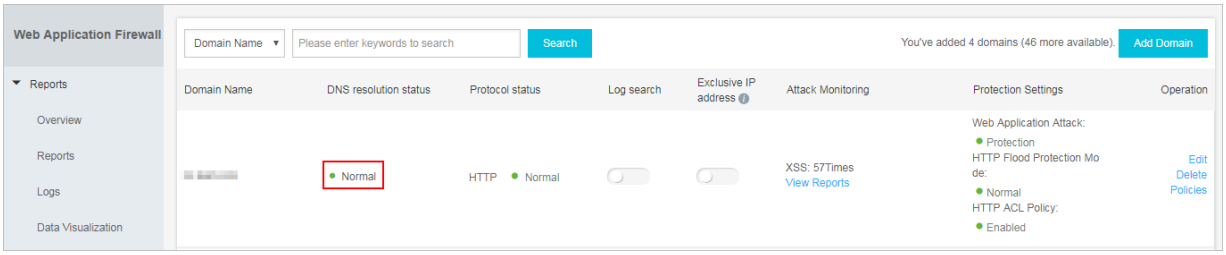
Web サイト設定が Alibaba Cloud WAF で作成されると、WAF は自動的に次の確認を行います。

- CNAME に対するドメイン: 毎時実行され、ドメイン名が WAF CNAME アドレスに対して解決されたかどうかを検出します。
- Webトラフィック: 数分ごとに実行され、ドメイン名への Web トラフィックが WAF を通過するかどうかを検出します。

確認のうち 1 つが OK であれば、DNS 解決ステータスは正常で、Alibaba Cloud WAF が Web サイトに完全に実装されていることを示しています。

DNS 解決ステータスを表示するには、Alibaba Cloud WAF コンソールにログインし、[管理] > [Web サイト設定] ページに移動します。

正常ステータスは以下のように表示されます。



DNS 解決ステータスが例外の場合、Alibaba Cloud WAF は正しく設定されていない可能性があります。 本ページでは、WAF が DNS 解決ステータスを判定する方法を説明し、一般的な例外ステータスを一覧表示します。

WAF での DNS 解決ステータスの判定方法

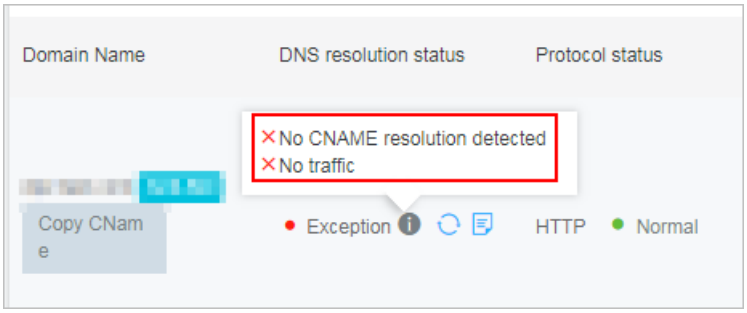
Alibaba Cloud WAF は、次の条件で DNS 解決ステータスを判定します。 条件のうち 1 つを満たす場合、DNS 解決ステータスは正常になります。

- 条件 A: ドメイン名が WAF CNAME アドレスに対して解決されている。
- 条件 B: ドメイン名の Web トラフィックが WAF を通過している。 過去 5 秒間に少なくとも 10 個のリクエストが検出されていれば、OK です。 1 分あたり 2 ～ 3 回のリクエストはトラフィックがないと見なされます。 Web トラフィックの履歴を表示するには、HTTP フラッドの攻撃保護レポートを確認します。 詳細は、「WAF セキュリティレポート」をご参照ください。

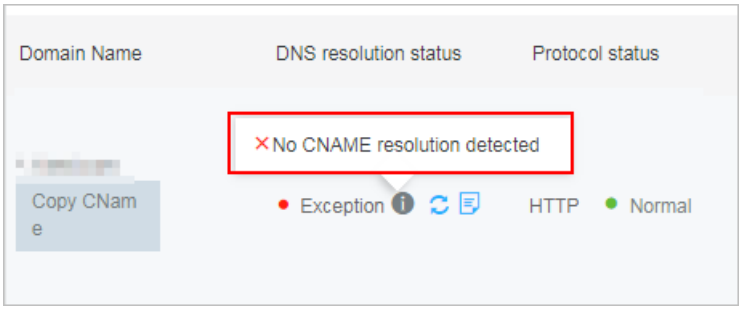
CNAME レコードを使用して Web トラフィックを WAF にリダイレクトすることを推奨します。 CNAME を使用すると、ノードの切り替えや、ノード障害やマシン障害時に配信元へのトラフィックのリダイレクトもサポートされ、業務可用性と障害回復能力が向上します。 CNAME レコードが現在の DNS 設定と競合する場合は、A レコードを使用してトラフィックのリダイレクトを行います。

一般的な例外ステータス

- 完全修飾ドメイン名 (example.abc.com などのFQDN) の場合、CNAME に対するドメイン確認と Web トラフィック確認が両方とも失敗した場合、例外ステータスが次のように表示されます。



- ワイルドカードドメイン名 (たとえば、*.abc.com) の場合、例外ステータスは次のように表示されます。



- Web サイトが WAF の前に CDN または他のプロキシサーバーとともにデプロイされている場合、ドメイン名は WAF ではなく CDN および他のプロキシサーバーに対して解決されます。 その結果、CNAME に対するドメイン確認は失敗します。 また、WAF が受信する CDN が返すトラフィックが少なく、Web トラフィック確認が失敗する可能性があります。 この場合、例外メッセージには、WAF が正しく設定されていないことが明確に示されません。

  WAF と CDN をまとめてデプロイする方法の詳細については、「#unique_7」をご参照ください。

WAF が機能しているかどうかの手動テスト

1. Alibaba Cloud WAF で設定したドメイン名、たとえば `www . aliyundemo . cn` にアクセスします。 Web ページは正常にアクセス可能です。

2. /alert(xss) 文字列をドメイン名の末尾に追加してテスト用 URL を作成し、この URL (この例では、 www.aliyundemo.cn/alert(xss)) にアクセスします。このリクエストが Alibaba Cloud WAF によってブロックされていることを知らせる 405 ページを受信した場合、WAF によって Web サイトは保護されています。

5 HTTP フラッド保護の緊急モード

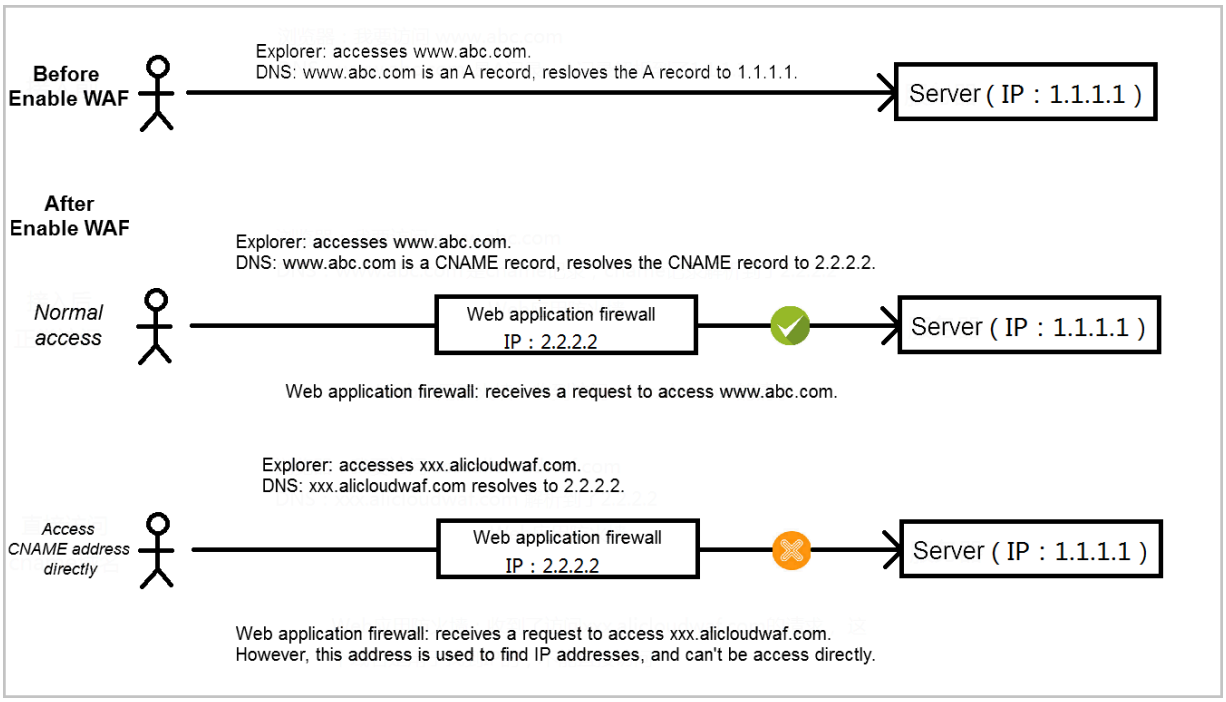
通常モードで大量の高度な HTTP フラッドを軽減できない場合は、緊急モードの HTTP フラッド保護を有効にします。

デフォルトでは、HTTP フラッド保護は通常モードに設定されていて、一般的な HTTP フラッドに対して保護します。 WAF は HTTP フラッドを標準的に軽減します。 配信元 CPU が上昇したり、データベースやアプリケーションからのレスポンスが失われる場合は、緊急モードを有効にする必要があります。

緊急モードは、正規のトラフィックを誤検知する可能性があります。 カスタマイズした HTTP フラッド保護ポリシーの場合、Business または Enterprise プランを選択することを推奨します。

6 WAF CNAME アドレスに直接アクセスできないのはなぜですか 。

WAF または Anti-DDoS Pro によって生成された CNAME ドメイン名は DNS 解決に使用され、直接アクセスすることはできません。



CNAME に直接アクセスすると、504 エラーページが表示されることがあります。

7 クライアントの実際の IP を取得する方法

HTTP リクエストがレイヤー 7 プロキシを通過すると、このパケットの送信元 IP は、クライアントの実際の IP (クライアント IP) ではなく、プロキシ IP に変更されます。 実際には、クライアント IP は HTTP ヘッドフィールドの x-forwarded-for フィールドに書き込まれます。

Alibaba Cloud WAF は次のように動作します。

WAF がドメイン “www.abc.com” を保護しているとします。 通常、クライアントからのパケットは、クライアントのブラウザー > WAF > 配信元サーバー (Apache、Nginx、IIS など) のパスを辿ります。 このアーキテクチャでは、 WAF はクライアントおよび配信元サーバー間のリバースプロキシとして機能します。

しかし、複数のプロキシ (たとえば、CDN や Anti-DDoS Pro) を含むネットワークアーキテクチャでは、 `x-forwarded-for` フィールドに複数の IP アドレスが追加されます。 これは、各プロキシがクライアント IP、または最後のプロキシ IP を追加するためです。

これにより、 `x-forwarded-for` フィールドは `X-Forwarded-For: Client IP, Proxy 1, Proxy 2, Proxy 3, ...` と表示されます。 ただし、クライアント IP が x-forwarded-for フィールドの先頭のアドレスであることに変わりはありません。

手順

クライアントの実際の IP アドレスを取得するには、次の手順に従います。

1. `x-forwarded-for` フィールドのコンテンツのリクエストコマンドを送信します。

   以下は、一般的な言語のリクエストコマンドの例です。

   - ASP の場合

     ```
     Request.ServerVariables("HTTP_X_FORWARDED_FOR")
     ```

   - ASP.NET(C#) の場合

     ```
     Request.ServerVariables["HTTP_X_FORWARDED_FOR"]
     ```

   - PHP の場合

     ```
     $_SERVER["HTTP_X_FORWARDED_FOR"]
     ```

   - JSP の場合

     ```
     request.getHeader(“HTTP_X_FORWARDED_FOR”)
     ```

2. `x - forwarded - for` の出力はカンマで区切られています。 最初の IP アドレスがクライアント IP です。

8 Alibaba Cloud DNS バージョンの WAF のプロダクト仕様

Alibaba Cloud DNS バージョンの WAF のプロダクト仕様は次の表のとおりです。

プロダクトパラメーター	説明	DNS バージョン
HTTP	HTTP (80) ポートをサポート	サポートあり
HTTPS	HTTP (443) ポートをサポート	サポートなし
クラウド外のデータセンター	Alibaba Cloud 外の Web サイトをサポート	サポートあり
基本 Web アプリケーション保護	SQL インジェクションやコマンド実行などの一般的な Web 攻撃から保護	サポートあり
ゼロデイ脆弱性防御	最新の Web 脆弱性に対して迅速に保護	サポートあり
サービスの可用性	サーバーがデプロイされているデータセンターを保護	単一のデータセンターをサポート
カスタム Web 保護ポリシー	Web サイトの Web 保護ポリシーをカスタマイズ	サポートなし
HTTP フラッド保護ポリシー	セキュリティプロフェッショナルを提供し、特定のサービスインターフェイスの保護ルールをカスタマイズ	サポートなし
HTTP フラッド保護しきい値	1 秒間に防御できる最大攻撃リクエスト	1,000
HTTP ACL ポリシー	追加できるアクセス制御ルールの数	5 (IP/URL)
保護ドメイン名の数	保護できるドメイン名の数	2
1 日の QPS しきい値	1 秒あたりの通常のリクエスト	100
帯域幅しきい値	1 秒あたりの最大帯域幅 (Mbps)	10 (Alibaba Cloud 外の配信元) 200 (Alibaba Cloud 内の配信元)
back-to-source IP アドレスの数	同じドメイン名に対して同時に配信元に返される IP アドレスの最大数	2

カスタム要件	さまざまなカスタム要件をサポート	サポートなし

DNS バージョンのプロダクト仕様が要件に合わない場合は、コンソールでサービスをアップグレードします。

9 エラー 405 を修正するにはどうすればよいですか 。

WAF をデプロイすると、Web サイトにセキュリティ上の脅威をもたらす可能性のある URL にアクセスしようとした場合、405 エラーが報告され、その URL へのアクセスが拒否されます。

ただし、URL へのアクセスが通常のビジネスリクエストであることを確認した後、HTTP ACL ポリシーの設定で、アクセスルールを追加します。 これにより、特定の URL またはソース IP アドレスにアクセスできます。

10 WAF ブラックホールを修正する方法

ブラックホールについて

Web Application Firewall (WAF) が、Anti-DDoS Basic の無料保護機能を超える大量トラフィックの DDoS 攻撃を受けた場合、WAF はブラックホール状態に陥ります。

WAF IP アドレスがブラックホール状態に陥ると、WAF を経由するトラフィック (通常のアクセスまたは攻撃) はすべてブロックされます。つまり、ブラックホール期間中は WAF インスタンスが保護するドメイン名にアクセスできません。

> 注 :
> サイトがブラックホール状態に陥った場合、そのサイトはブラックホール期間終了後にのみ回復します。 デフォルトのブラックホール期間は 150 分です。 WAF ブラックホールしきい値は、ECS が置かれるリージョンのデフォルトしきい値と同じです。

ブラックホールおよびブラックホールポリシーの詳細については、「Alibaba Cloud ブラックホールポリシー」をご参照ください。

ブラックホールを回避する方法

デフォルトでは、各 WAF インスタンスは専用 IP アドレスをユーザーに割り当てます。 この WAF IP アドレスがブラックホール状態に陥ると、ブラックホール期間中、この WAF インスタンスが保護するドメイン名にアクセスできません。 これを回避するには、重要なドメイン名に対する追加の専用 IP アドレスを購入します。 この場合、この重要なドメイン名は DDoS 攻撃を受けている他のドメイン名の影響を受けません。

> 注 :
> 大量トラフィックの DDoS 攻撃に対する最善の解決策は、Anti-DDoS Pro を使用してドメイン名を保護することです。

WAF ブラックホール についてよくある質問

WAF がブラックホール状態に陥ります。 すぐに回復しますか。

ブラックホールは Alibaba Cloud が ISP から購入するサービスであり、ISP がブラックホールをトリガーする時間と頻度に厳しい制限を加えています。したがって、手動でブラックホール状態を無効化することはできず、システムが自動的にサーバーを解放するのを待つ必要があります。

実際には、ブラックホールがすぐに無効化されたとしても、WAF が依然として大量トラフィックの DDoS 攻撃を受けている場合は、ブラックホールは再度トリガーされます。

WAF が複数のドメイン名で設定されている場合、攻撃を受けている特定のドメイン名を知る方法を教えてください。

通常、ハッカーは WAF で保護されたドメイン名を解決して WAF インスタンスの IP アドレスを取得し、この IP アドレスに対して DDoS 攻撃を開始します。 大量トラフィックの DDoS 攻撃は、WAF IP アドレスを標的にしています。 トラフィックに基づいて、攻撃を受けているドメイン名を特定することはできません。

ただし、ドメイン名を分けて、攻撃を受けているドメイン名を調べることができます。たとえば、一部のドメイン名を WAF に、残りをその他（ECS オリジン、CDN、または SLB）に名前解決します。WAF がブラックホールからなくなっていれば、ハッカーの標的はその他に名前解決されたドメイン名にあることになります。しかし、運用がやや複雑で、配信元およびその他の資産を公開してしまう可能性があり、さらに深刻なセキュリティ問題になりかねません。必要な場合を除き、この方法で攻撃を受けているドメイン名を特定しないようにします。

WAF がブラックホール状態に陥らないように WAF IP アドレスを変更すると、効果がありますか。

WAF IP アドレスを変更しても問題は解決しません。 ハッカーはドメイン名の ping によって新しい IP アドレスを入手し、別の DDoS 攻撃を開始します。 したがって、IP アドレスを変更してもあまり効果はありません。

DDoS 攻撃と HTTP フラッド攻撃に違いはありますか。 WAF が DDoS 攻撃を防御できないのはなぜですか。

大量トラフィックの DDoS 攻撃は、IP アドレスに対するレイヤー 4 攻撃です。一方 HTTP フラッド攻撃はレイヤー 7 攻撃 (たとえば、HTTP GET や POST フラッド) です 。

WAF は HTTP フラッド攻撃を防御します。 ただし、大量トラフィックの DDoS 攻撃の場合、すべてのトラフィックをクリーニングするには十分な帯域幅のリソースが必要です。 したがって、DDoS 攻撃から保護するには、Anti-DDoS Pro を使用します。

11 どのように WAF の back-to-source IP アドレスを表示しますか。

WAF の back-to-source IP アドレスが配信元によってブロックされる、または遅くなるのを防ぐために、WAF の back-to-source IP アドレスを配信元のセキュリティグループ、ファイアウォール、またはその他のホストセキュリティ保護ソフトウェアのホワイトリストに追加します。

次の手順に従って、WAF の back-to-source IP アドレスセグメントを表示します。

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] ページに移動します。
3. ページの上隅にある [Alibaba Cloud WAF IP 範囲] をクリックします。

WAF の back-to-source IP アドレスセグメントを配信元サーバーのセキュリティグループ、ファイアウォール、またはその他のホストセキュリティ保護ソフトウェアのホワイトリストに追加して、配信元サーバーの保護をデプロイします。 詳細は、「配信元の保護」をご参照ください。

12 HTTPS アクセス例外

本ページでは、Web サイトを WAF に接続した後の HTTPS アクセス例外のトラブルシューティング方法について説明します (HTTP アクセスは正常です)。 現象には、ページを開くのに失敗、証明書が信頼できないというシステムプロンプト、一部のポートの呼び出しの失敗、および特定のマシンタイプ、オペレーションシステム、およびアプリケーションに対するアクセスエラーが含まれます。

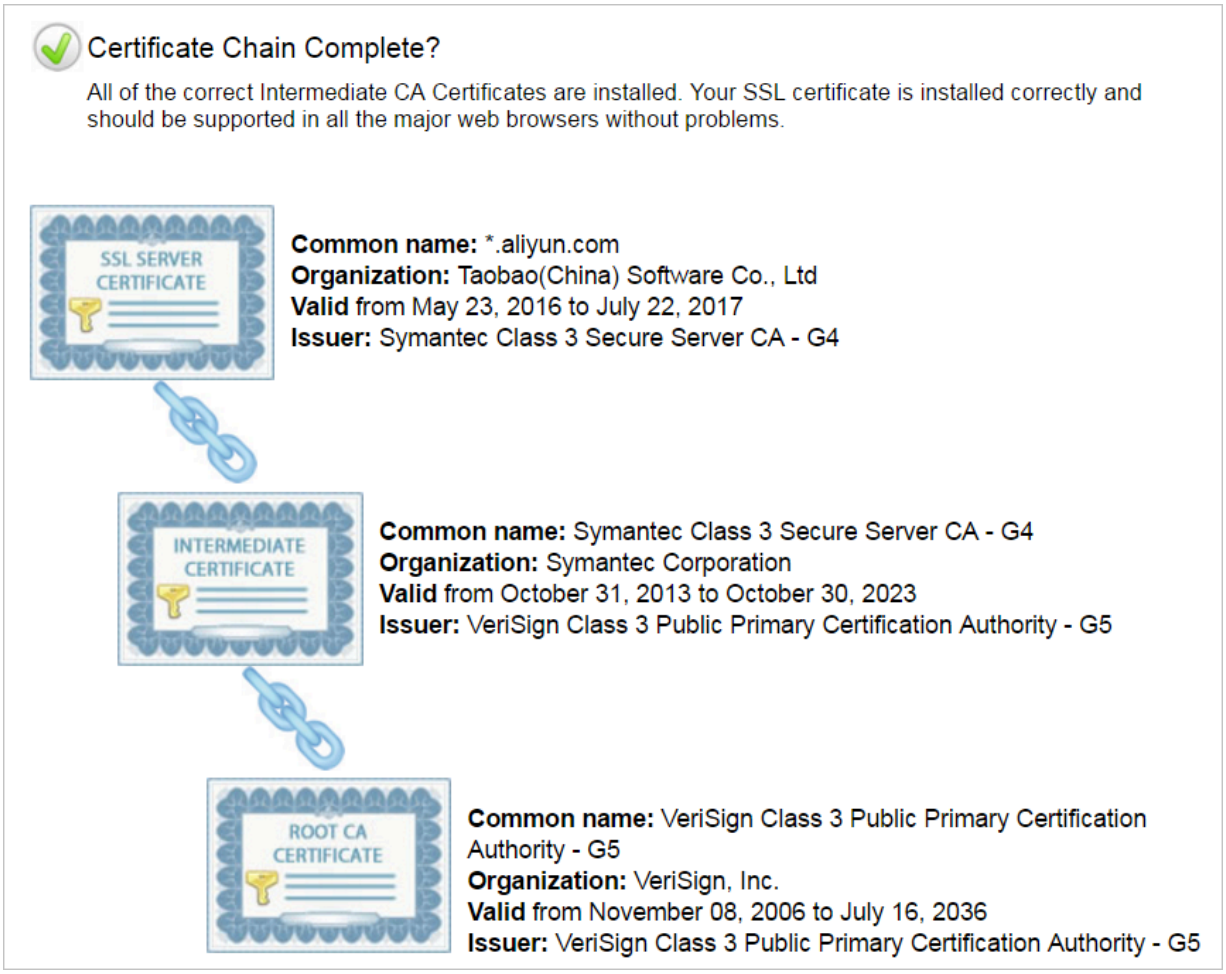
HTTPS が有効で証明書がアップロードされていますか。

WAF を使用して HTTPS サービスを保護する場合は、WAF コンソールで [HTTPS] を選択し、サーバーの証明書とまったく同じ証明書またはキーをアップロードする必要があります。 WAF が Anti-DDoS Pro、SLB、CDN などのプロダクトと同期して使用されている場合でも、WAF コンソールで証明書またはキーをアップロードする必要があります。 WAF 証明書は他のプロダクトから独立しています。

> 注 :
> コンソールで証明書をアップロードすると、設定が有効になるのに最大 5 分かかります。 この間も、アクセス例外が発生する可能性があります。 ホストをバインドし、WAF を設定、有効にしたら DNS 解決を切り替えます。

証明書チェーンは完全ですか。

たいていの場合、証明書サービスプロバイダーから複数の証明書 (サーバー証明書や 1 つ以上の CA ルート証明書など) が提供され、これらをまとめて完全な証明書チェーンが形成されます。 例として Alibaba Cloud 証明書を取り上げると、受け取ることのできる証明書チェーンは次の図のようになります。



(前の図に示すように)、完全な証明書チェーンを WAF に確実にアップロードします。 また、アップロードするときに証明書の順序に注意します。 たとえば、サーバー証明書は上部に、ルート証明書は下部に、そして複数の証明書のテキストコンテンツをまとめる必要があります。 以下は、アップロードする必要のある証明書の内容の例です。

```
----- BEGIN   CERTIFICAT  E -----
 MIIFdDCCBF  ygAwIBAgIQ  Fmr88Z0mn6  rEleGaC6UV  EzANBgkqhk
 iG9w0BAQsF  ADCB
 Obc3E + 7h0u6cUXaQ  AmFNZ2a ...
----- END   CERTIFICAT  E -----
----- BEGIN   CERTIFICAT  E -----
 MIIFYjCCBE  qgAwINMTYw  NjA3MDAwMD  AwmlTaWduL  CBJbmMuMRL
 nN5bWNiLmN  vbS9
 wY2EzLWc1L  m1hbnRlY1B  LSS0yLTU ...
----- END   CERTIFICAT  E -----
----- BEGIN   CERTIFICAT  E -----
 MIIG / TCCBeWgAwI  BAgIQLMUH0  3pBzhUCrOR  0SsKM + DANBgkqhki
 G9w0BAQsFA  DB +
 NzIDMgUHVi  bGljIFByaW  1 ...
----- END   CERTIFICAT  E -----
```

証明書チェーンが不完全な場合、証明書が信頼できないというプロンプトがページに表示されることがあり、一部の Android 携帯電話、オペレーションシステム、またはアプリでアクセスエラーや例外が発生する可能性があります (環境によってはアクセスが正常な場合もあります)。

インターネット上で利用可能なサードパーティ製の検査ツール (たとえば、GeoCerts™ SSL チェッカー) を使用して、現在利用可能な証明書チェーンが完成しているか確認します。

> 注：
> この方法で解決できることはドメイン名のステータスの確認だけです。 ドメイン名を WAF ではなく配信元に対してすでに解決している場合は、WAF で証明書のステータスを確認できません。

SNI 問題

特定のクライアントまたはアプリケーションによっては通常 HTTPS サービスにアクセスできない場合、"SSL ハンドシェイク失敗 / エラー"、または "証明書が信頼できません" というプロンプトが表示されます。理由として、クライアントが SNI をサポートしていない可能性があります。これらのクライアントまたはアプリケーションは、旧式の Android 機器、旧バージョンの JAVA で開発された呼び出しプログラム (特に SSL プロトコルを使用するプログラム)、Windows XP 上で動作する IE ブラウザー、一部の旧バージョンの携帯電話、および一部のサードパーティ支払コールバックインターフェイスである可能性があります。

現在、たいていのブラウザー、アプリケーション、WeChat および Alipay コールバックインターフェイスは SNI をサポートしています。 ドメイン名を配信元に対して解決するときにアクセスが正常に戻る場合、SNI 互換性の問題である可能性があり、ドメイン名を WAF に対して解決すると例外が発生します。 クライアントをアップグレードするか、コールバックインターフェイスを配信元に対して直接解決します。

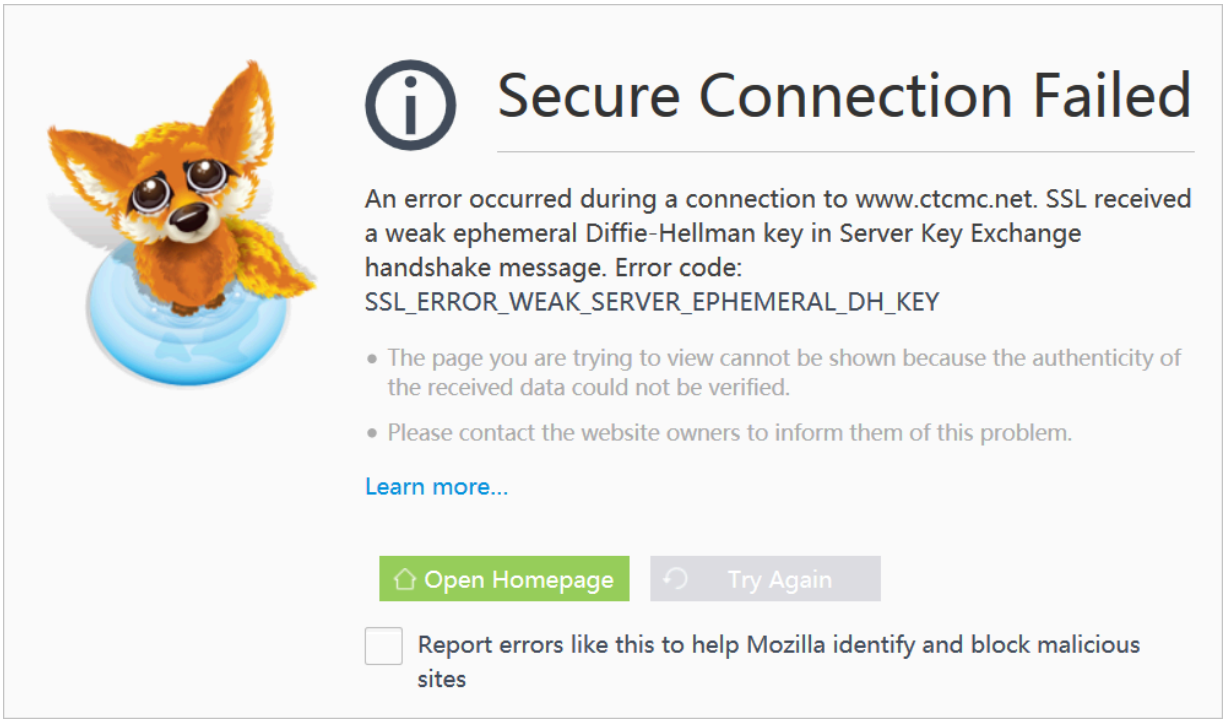
詳細は、「SNI 互換性による HTTPS アクセスの例外 (信頼できない証明書)」をご参照ください。

Windows Server 2003 / IIS6 サーバー

WAF に接続されている Windows Server 2003 または IIS 6 サーバーから HTTPS サービスにアクセスすると、白い画面または 502 エラーが発生することがあります。 これらのシステムの TLS バージョンと暗号化スイートは非常に旧式のため、セキュリティパフォーマンスがとても低く、WAF のデフォルト HTTPS back-to-source アルゴリズムと互換性がありません。 WAF は、Windows Server 2003 用 HTTPS back-to-source リクエストをサポートしていません。 Microsoft は Windows Server 2003 を使用して HTTPS サイトを構築しないことを公式に推奨しています。 通信セキュリティのため、オペレーティングシステムを Windows Server 2008 以降にアップグレードすることを推奨します。

短い DH 鍵によるリンク障害

短い DH (ディフィーヘルマン) 鍵はセキュリティ上の問題として知られています。 WAF は短い鍵をサポートしていません。 同様に、WAF を使用していなくても、新しいバージョンの Firefox ブラウザー (51.0.1 など) を使用して配信元にアクセスすると、同様のエラーが表示されることがあります。



関連するコンポーネント (JDK バージョンなど) をアップグレードして、サーバーの DH 鍵アルゴリズムを確実に 2048 ビット以上にすることを推奨します。

> 注：
> 鍵の長さはサーバーの暗号化アルゴリズムによって決まり、証明書とは無関係です。 操作方法がわからない場合は、サーバー開発者に連絡するか、関連する解決策を検索します。 以下のエラーメッセージに基づいて関連する解決策を見つけます。 `SSL routines : ssl3_check _cert_and_ algorithm : dh key too small`

HTTP リダイレクトが必要なサービスで HTTP が有効になっていますか。

配信元を設定して HTTP アクセスリクエストを HTTPS に強制的にリダイレクトしている場合は、WAF で HTTP と HTTPS を両方とも選択する必要があります。 そうでない場合、これらの HTTP リクエストは WAF にリダイレクトされた後で正常に配信元に転送されず、システムはエラーを返します。

13 ログインステータスが消失する問題を修正するにはどのようにすればよいですか

現象

WAF を使用していると、一部のサイトでログインステータスが失われたり、ログインステータスに関連したその他の例外が発生することがあります。 これらの例外の根本原因は次のとおりです。

- 特に WAF の後に SLB がアタッチされているアーキテクチャにおいて、ドメイン名に複数の配信元 (ECS) はありますが、セッションが同期されません。
- 検証のための X-forwarded-for からの実際の IPアドレス取得に失敗します。

解決策

- サーバーのセッション同期を設定します。
- WAF が SLB に接続されている場合は、レイヤー 7 HTTP 方式を使用してトラフィックを転送し、cookie ベースのセッション維持を有効にします。
- x-forwarded-for から実際の IP アドレスを取得します。

  詳細は、「訪問者の実際の IP アドレスの取得」をご参照ください。

14 ECS への侵入に対処するにはどのようにすればよいですか

ECS インスタンスは、WAF で保護された後も侵入を受ける可能性があります。 以下の原因が考えられます。

番号	原因	解決策
1	WAF に接続する前に ECS インスタンスに侵入されています。この場合、最初に ECS インスタンスをクリーンアップする必要があります。	次のセクションで説明する「サーバークリーンアップ」を実行します。
2	WAF を設定後に DNS 解決が更新されていません。 この結果、トラフィックは WAF を経由せずに直接 ECS に渡されます。	Web サイトが WAF の保護下にあるように DNS 解決が更新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。
3	WAF の使用開始前に、ECS インスタンスの IP アドレスが公開されていますが、セキュリティグループが設定されていません。 その結果、ハッカーは IP アドレスを使って ECS インスタンスを直接攻撃します。	セキュリティグループを設定して WAF を迂回する攻撃を防ぎます。 詳細は、「配信元の保護」をご参照ください。
4	WAF で保護されていない他のサイトが ECS インスタンスに存在します。 その結果、ECS インスタンスはこれらのサイトを標的とする攻撃の影響を受けます。	ECS インスタンス上のすべての HTTP サービスが WAF で保護されていることを確認します。
5	ECS インスタンスが ssh パスワードの総当たり攻撃など Web 攻撃以外の侵入に遭っています。	ECS インスタンスとデータベースが強力なパスワードを採用していることを確認します。

サーバークリーンアップ

注：
トロイの木馬やウイルスを除去する前に、まず、「スナップショットを作成」してデータのバックアップをとることで、操作ミスによるデータの損失を回避します。

トロイの木馬およびウイルスの除去

1. `netstat` でネットワーク接続を確認し、疑わしいリクエストがあるかどうかを分析します。 該当する場合、ECS インスタンスを停止します。

2. ウイルス対策ソフトウェアを使用してウイルスをスキャンして除去します。

次のコマンドを実行して Linux のトロイの木馬を除去します。

```
chattr  - i  / usr / bin /. sshd
rm  - f  / usr / bin /. sshd
chattr  - i  / usr / bin /. swhd
rm  - f  / usr / bin /. swhd
rm  - f  - r  / usr / bin / bsd - port
cp  / usr / bin / dpkgd / ps  / bin / ps
cp  / usr / bin / dpkgd / netstat  / bin / netstat
cp  / usr / bin / dpkgd / lsof  / usr / sbin / lsof
cp  / usr / bin / dpkgd / ss  / usr / sbin / ss
rm  - r  - f  / root /. ssh
rm  - r  - f  / usr / bin / bsd - port
find  / proc / - name   exe  |  xargs   ls  - l  |  grep  - v   task
| grep   deleted |  awk  '{ print  $ 11 }' |  awk  - F / '{ print  $
NF }' |  xargs   killall  - 9
```

ECS インスタンスの脆弱性の確認および修正

1. サーバーアカウントが正常であることを確認します。 サーバーアカウントが異常な場合は、ECS を停止して異常アカウントを削除します。
2. ECS へのリモートログインがあるか確認します。 ある場合は、10 文字を超える大文字と小文字のアルファベット、数字、および特殊文字で構成される強力なログインパスワードを設定します。
3. Jenkins、Tomcat、PhpMyadmin、WDCP、および Weblogic のバックエンドのパスワードが強力なものであることを確認します。 サービスを使用しない場合は、管理ポート 8080 を無効にします。
4. Struts や ElasticSearch などの Web アプリケーションの脆弱性を確認します。 Web サイトが WAF によって保護されていることを確認します。 トロイの木馬とウイルスの除去およびパッチのインストールには、Server Guard の使用を推奨します。
5. 次の脆弱性が存在するかどうかを確認します。Jenkins 管理者がパスワードを使用せずにリモートでコマンドを実行している。 該当する場合、パスワードを設定するか、8080 ポートを管理するページを閉じます。
6. 次の脆弱性が存在するかどうかを確認します。 パスワードを使用せずにファイルが Redis に書き込まれている可能性がある。 ハッカーによって作成された SSH ログインキーファイルが `/ root /` 配下にあるかどうかを確認します。 ファイルが存在する場合は、ファイルを削除します。 Redis を変更し、ユーザーにパスワードを使って Redis にアクセスさせ、より強力なパスワードを設定させるようにします。 パブリックネットワークへのアクセスが不要な場合は、 `bind  127 . 0 . 0 . 1` を使用してローカル アクセスのみを許可します。
7. パスワードが設定されている MySQL、SQLServer、FTP、および Web 管理バックエンドを確認し、必ず強力なパスワードを設定してください。

Alibaba Cloud セキュリティサービスの有効化

- **ECS インスタンス上のすべての Web サイトで WAF が有効になっていることを確認します。**
- **ホストスキャン、トロイの木馬のスキャンと除去、および脆弱性の修正には Alibaba Cloud Security Threat Detection Service を使用します。**

15 SNI 互換性による HTTPS アクセスの例外 (信頼できない証明書)

背景

HTTP サーバーに仮想ホストを導入する目的は、複数のドメイン名が 1 つの IP アドレスを再利用して IPv4 アドレスの供給を分散させることです。 サーバーは、クライアントリクエストに指定されたホストに応じて、リクエストを異なるドメイン名 (仮想ホスト) に割り当て、処理します。 IP アドレスが複数のドメイン名 (仮想ホスト) で共有されている HTTPS サーバーでは、ブラウザーが HTTPS サイトにアクセスすると、最初にサーバーとの SSL 接続が確立されます。 SSL 接続を確立するための最初の手順は、サーバーからの証明書をリクエストすることです。 サーバーはドメイン名に関係なく証明書を送信します。 これは、ブラウザーがアクセスしたドメイン名をサーバーが判別できないためです。

SNI (Server name indication) は、複数のドメイン名と証明書を使用して単一サーバーの問題を解決するために使用される SSL/TLS 拡張です。 サーバーが SSL 接続を確立するために接続される前に、アクセスされるサイトのドメイン名 (ホスト名) が最初に送信されるので、サーバーはドメイン名に基づいて適切な証明書を返します。

現在、ほとんどのオペレーティングシステムとブラウザーは SNI 拡張をサポートしています。 この機能は OpenSSL 0.9.8 に組み込まれており、新しいバージョンの Nginx も SNI をサポートしています。

現象

クライアントが SNI をサポートしていない場合、WAF にアクセスしたときに HTTPS アクセスが異常になることがあります。

SNI をサポートしていないブラウザーを使用して WAF を使用する Web サイトにアクセスすると、WAF はクライアントがリクエストしたドメイン名を知らないため、クライアントとやり取りするための対応する仮想ホスト証明書を取得できません。 Web Application Firewall は、埋め込みのデフォルト証明書のみを使用して、クライアントとのハンドシェイクを実行します。 この場合、クライアントのブラウザーには "証明書が信頼できません" というメッセージが表示されます。

クライアントが SNI をサポートしていない場合は、次の現象が発生する可能性があります。

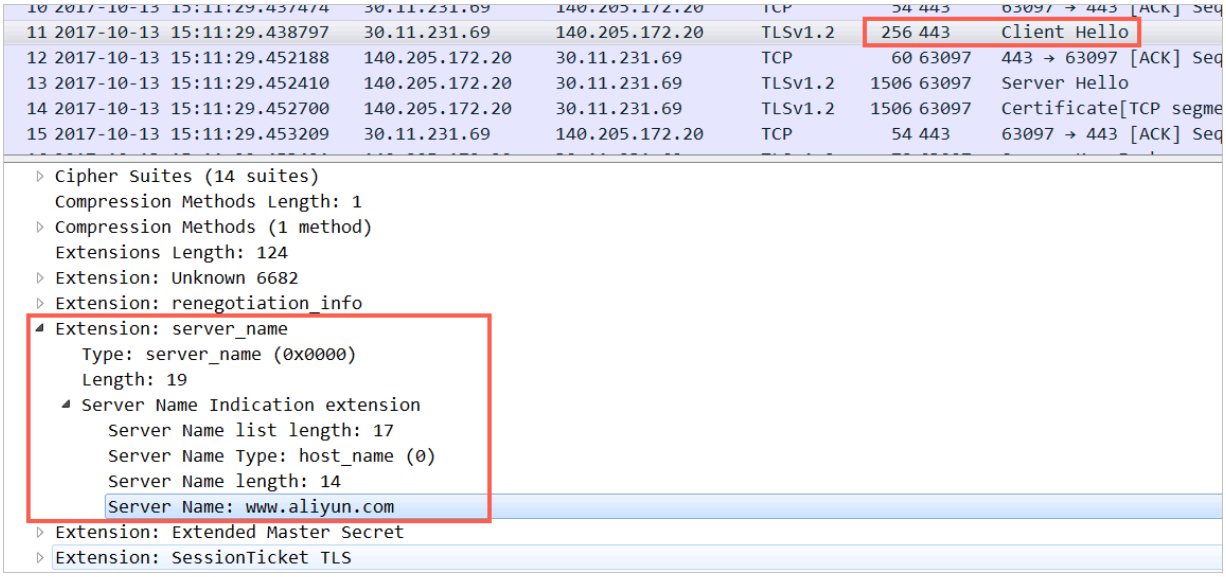
- モバイルアプリクライアントでは、iOS クライアントには通常アクセスできますが、Android クライアントは通常開くことができません。

- Web ページを開くと、ブラウザーに証明書が信頼できないことを示すメッセージが表示されます。

解決策

クライアント上で SSL ハンドシェイクパケットをキャプチャして、クライアントが SNI をサポートしているかどうかを確認します。 Chrome ブラウザーを使用してAlibaba Cloud の公式 Web サイトにアクセスするとします。

次の図に示すように、SNI 拡張が Client Hello パケットに表示される場合、クライアントはSNI 拡張をサポートしています。



それ以外の場合、クライアントは SNI 拡張をサポートしていません。 SNI をサポートしていないクライアントの場合、

- ブラウザーをアップグレードするか、Chrome や Firefox などの新しいバージョンのブラウザーを使用することを推奨します。
- WeChat および Alipay からのサードパーティコールバックの場合、配信元 IP アドレスを使用して Web Application Firewall を迂回します。

SNI 互換性

> 注：
> SNI は TLS1.0 以降のバージョンと互換性がありますが、SSL ではサポートされていません。

- SNI は以下のデスクトップブラウザーをサポートしています。
  - Chrome 5 以降のバージョン
  - Chrome 6 以降のバージョン (Windows XP)
  - Firefox 2 以降のバージョン
  - IE 7 以降のバージョン (Windows Vista / Server 2008 以降のバージョンで動作、Windows XP OSの IE のどのバージョンも SNI をサポートしていません)
  - Konqueror 4.7 以降のバージョン
  - Opera 8 以降のバージョン
  - Windows Vista / Server 2008 以降のバージョンまたは Mac OS X 10.5.6 以降のバージョンのSafari 3.0
- SNI は以下のライブラリをサポートしています。
  - GNU TLS
  - Java 7 以降のバージョン (クライアントとしてのみ機能)
  - HTTP クライアント 4.3.2 以降のバージョン
  - libcurl 7.18.1 以降のバージョン
  - NSS 3.1.1 以降のバージョン
  - OpenSSL 0.9.8j 以降のバージョン
  - OpenSSL 0.9.8f 以降のバージョン (フラグを設定する必要があります)
  - QT 4.8 以降のバージョン
  - Python 3、Python 2.7.9 以降のバージョン
- SNI は以下のモバイルブラウザーをサポートしています。
  - 3.0 Honeycomb 以降のバージョンの Android ブラウザー
  - iOS 4 以降のバージョンの iOS Safari
  - Windows Phone 7 以降のバージョン
- SNI は以下のサーバーをサポートしています。
  - Apache 2.2.12 以降のバージョン
  - Apache Traffic Server 3.2.0 以降のバージョン
  - HAProxy 1.5 以降のバージョン
  - IIS 8.0 以降のバージョン
  - lighttpd 1.4.24 以降のバージョン
  - LiteSpeed 4.1 以降のバージョン
  - Nginx 0.5.32 以降のバージョン

- SNI は以下のコマンドラインをサポートしています。
  - cURL 7.18.1 以降のバージョン
  - wget 1.14 以降のバージョン

16 長時間接続タイムアウト

現象

一部のサービスシナリオでは、クライアントがリクエストを送信すると、サーバーは処理のために 60 秒以上経ってから応答を返します。 処理中、サーバーはクライアントとデータをやり取りしません。

たとえば、Web ページに Excel ファイルをアップロードし、サーバーにファイル内のデータを処理するよう要求したとします (処理時間は約 3 分)。 ファイルが送信されてから 120 秒以内は、クライアントとサーバーの間でデータ (HTTP や TCP パケット) をやり取りしません。 この場合、WAF はクライアントに 504 タイムアウト応答を返し、接続を切断します。

これは、WAF が (データのやり取りがない場合) 120 秒を超える長時間接続は維持せず、また、レイヤー 7 のタイムアウト間隔 (120 秒) を変更できないためです。

解決策

長時間接続では、60 秒以内に小さなデータ (セッションが維持される、Ack パケット、ハートビートパケット、キープアライブパケットなど) をやり取りするよう、リクエスト交換モードを変更することを推奨します。

ユーザー シナリオは多岐にわたるため、コード レベルでの修正案は提供していません。サービスの特徴に応じて調整する必要があります。

17 WAF トラブルシューティングマニュアル

本ページでは、現象、問題について説明し、WAF にアクセスするドメイン名に何らかの異常なアクセスが発生したときに起こる重大な問題の解決策を示します。

ツール

- Chrome ブラウザー - 開発者向けツール: Chrome ブラウザで提供されている開発者向けツールは、読み込まれるページ要素を確認するのに便利です。 F12 キーを押してツールを開き、ネットワークタブに切り替えます。
- ping: Windows および Linux オペレーティングシステムが提供する ping テストツールを使用して、ネットワーク障害を分析し、識別します。 Windows OS では、Win+R キーを押して「CMD」と入力し、ツールを開きます。 使用法: `ping domain name / IP address` 。
- traceroute (Linux)/tracert (Windows): リンクトレースツールを使用して、データ損失の発生するホップを検出します。 Windows OS では、CTRL+R キーを押して「cmd」と入力し、ツールを開きます。 使用法: `tracert -d domain name / IP address`
- nslookup: このツールを使用して、ドメイン名の解決が機能しているかどうか検出します。 Windows OS では、CTRL+R キーを押して「cmd」と入力し、ツールを開きます。 使用法: `nslookup domain name`

トラブルシューティング方法

配信元が正常かどうかの確認

次の手順に従い、WAF を迂回して、問題が配信元にあるかどうかを確認します。

1. 配信元のセキュリティグループ、ブラックリスト、ホワイトリスト、ファイアウォール、ドングル、およびクラウドロックを無効にして、WAF IP アドレスがブラックリストに追加されないようにします。
2. ローカルの hosts ファイルを変更し、ドメイン名を対応する ECS、SLB、またはサーバーのパブリックネットワーク IP アドレス (WAF で指定された配信元 IP アドレス) に誘導します。
3. WAF なしでも問題が発生するかどうか確認します。

アクセスリクエストが誤って遮断されたかどうかの確認

次の手順に従い、保護ポリシーを調整し、アクセスリクエストが誤って遮断されたかどうかを確認します。

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] ページに移動します。
3. アクセスが異常なドメイン名を見つけ、操作リストの下にある [ポリシー] をクリックします。
4. [Web アプリケーション保護] を無効にし、問題が解決したかどうかを確認します。 問題が解決した場合は、
   - Web アプリケーション保護ポリシーの設定を [緩い] にすることを推奨します。
   - URL を分析し、HTTP ACL ポリシーを使用して、正常な URL からのアクセスを許可する新しいルールを追加することも可能です。
5. 問題が解決しない場合は、HTTP フラッド保護を無効にし、問題が解決したかどうかを確認します。 問題が解決した場合は、
   - HTTP フラッド保護モードの設定を [標準] にすることを推奨します。
   - URL または IP アドレスを分析し、HTTP ACL ポリシーを使用して、正常な URL または IP アドレスからのアクセスを許可する新しいルールを追加することも可能です。

WAF に関する一般的な問題

WAF を接続しているときに問題が引き続き発生し、WAF を切断すると問題がなくなる場合は、次の手順でそのような問題を解決します。

アクセスがブロックされました (エラー 405)

現象

アクセスがブロックされていることを示すページが表示され、応答で 405 が返されます。

原因

考えられる原因は次のとおりです。

- HTTP ACL ポリシーによりアクセスがブロックされています。
- Web アプリケーション保護によりアクセスがブロックされています。

解決策

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] ページに移動します。
3. アクセスが異常なドメイン名を見つけ、操作リストの下にある [ポリシー] をクリックします。
4. HTTP ACL ポリシーを無効にして、ページ (405) が引き続き表示されるかどうかを確認します。 ページが表示されなくなった場合は、ACL ルールによりアクセスが遮断されています。ルールを削除して問題を解決します。

5. HTTP ACL ポリシーを無効にしても問題が発生する場合は、Web アプリケーション保護を無効にしても問題が引き続き発生するかどうかを確認する必要があります。 問題が解決した場合は、
   - Web アプリケーション保護ポリシーの設定を [緩い] にすることを推奨します。
   - URL を分析し、HTTP ACL ポリシーを使用して、正常な URL からのアクセスを許可する新しいルールを追加することも可能です。

接続リセット (エラー 302)

現象

一部の IP アドレスを使用してWeb サイトにアクセスすると、”接続がリセットされました” というメッセージが表示され、応答で 302 が返されます。 Set-cookie も送信されます。

原因

IP アドレスに基づくアクセスによって HTTP フラッド保護 ルールがトリガーされています。

解決策

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. アクセスが異常なドメイン名を見つけ、操作リストの下にある [ポリシー] をクリックします。
4. HTTP フラッド保護を無効にして、アクセスが回復するかを確認します。 HTTP フラッド保護を無効にした後にアクセスが回復した場合、HTTP フラッド保護ルールによりアクセスは遮断されています。
   - HTTP ACL ポリシーを設定して、正常な URL または IP アドレスからのアクセスを許可する新しいルールを追加します。
   - HTTP フラッド保護モードが緊急の場合、HTTP フラッド保護モードの設定を [通常] にすることを推奨します。

HTTPS アクセス異常

現象

HTTPS リクエストを送信後、証明書 `www . notexist . com` が返されます。

原因

WAF は SNI をサポートするブラウザーが必要です。 一般に、iOS は基本的に SNI をサポートしています。 Windows および Android オペレーティングシステムでは、SNI と互換性があることを確認しなければなりません。

解決策

「SNI の互換性から生じる HTTPS アクセスの例外 (信頼できない証明書)」をご参照ください。

ホワイトスクリーン (エラー 502)

現象

Web サイトへのアクセス中、ホワイトスクリーンが表示され、応答で 502 が返されます。

原因

配信元 (ECS、SLB、またはサーバー) でパケットロスが発生、または配信元が到達不能になった場合、WAF はホワイトスクリーンを返します。

解決策

- ブラックリスト、iptables、ファイアウォール、ドングル、およびクラウドロックなどのセキュリティソフトウェアまたはポリシーが配信元に設定されているかどうかを確認します。 設定されていれば、関連サービスを停止またはアンインストールし、ブラックリストを解除して、問題が解決するかを確認します。
- 「トラブルシューティング方法」をご参照ください。 WAF を迂回してアクセスし、アクセスが正常かどうかを確認します。 それでもアクセスが異常な場合は、配信元のプロセス、CPU、メモリ、および Web ログが異常でないかどうかを確認します。

ping の失敗とトリガーされたブラックホール

現象

ドメイン名の ping が失敗します。 さらに、WAF が DDoS 攻撃を受けてブラックホールに入ったことを示すショートメッセージを受信します。

原因

DDoS 攻撃は WAF の保護範囲ではありません。

解決策

Anti-DDoS Proを有効にして、DDoS 攻撃から防御します。

バックエンド内の複数のサーバー負荷が不均衡

原因

WAF はレイヤー 4 IP アドレスのハッシュアルゴリズムを使用します。 したがって、

- Anti-DDoS Pro が WAF に接続されていると、ECS の負荷が分散されないことがあります。
- SLB がレイヤー 4 転送を使用する場合、ECS の負荷は分散されないことがあります。

解決策

WAF および ECS を設定し、直接 SLB を使用して負荷を分散する、つまりレイヤー 7 転送、クッキーセッションの永続化、および負荷分散を有効にします。

WeChat または Alipay のコールバックに失敗

現象

WeChat または Alipay コールバックに失敗します。

原因

- 高頻度のアクセスは、HTTP フラッド保護によって遮断されます。
- HTTPS はコールバックに使用され、WeChat および Alipay は SNI をサポートしません。SNI の詳細は、「SNI 互換性から生じる HTTPS アクセスの例外 (信頼できない証明書)」をご参照ください。

解決策

- HTTP フラッド保護
  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. アクセスが異常なドメイン名を見つけ、操作リストの下にある [ポリシー] をクリックします。
  4. HTTP フラッド保護を無効にして、アクセスが回復するかを確認します。 HTTP フラッド保護を無効にした後でアクセスが回復した場合、HTTP フラッド保護ルールによりアクセスは遮断されています。
     - HTTP ACL ポリシーを設定して、正常な URL または IP アドレスからのアクセスを許可する新しいルールを追加します。
     - HTTP フラッド保護モードが緊急の場合、HTTP フラッド保護モードの設定を [通常] にすることを推奨します。
- SNI の互換性

  WeChat または Alipay を設定して、WAF を経由せずに ECS または SLB の IP アドレスを直接呼び出します。

18 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。