Web Application Firewall

Preguntas frecuentes

Edición	01
Fecha	2025-01-20

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registradas y permisos

El logotipo HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Es posible que la totalidad o parte de los productos, las funcionalidades y/o los servicios que figuran en el presente documento no se encuentren dentro del alcance de un contrato vigente entre Huawei Cloud y el cliente. Las funcionalidades, los productos y los servicios adquiridos se limitan a los estipulados en el respectivo contrato. A menos que un contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en el presente documento constituye garantía alguna, ni expresa ni implícita.

Huawei está permanentemente preocupada por la calidad de los contenidos de este documento; sin embargo, ninguna declaración, información ni recomendación aquí contenida constituye garantía alguna, ni expresa ni implícita. La información contenida en este documento se encuentra sujeta a cambios sin previo aviso.

Huawei Cloud Computing Technologies Co., Ltd.

Dirección: Huawei Cloud Data Center Jiaoxinggong Road
Avenida Qianzhong
Nuevo distrito de Gui'an
Gui Zhou, 550029
República Popular China

Sitio web: https://www.huaweicloud.com/intl/es-us/

Índice

1 Acerca de WAF

1.1 Funciones de WAF

1.1.1 ¿Puede WAF proteger una dirección IP?

Una instancia WAF puede proteger direcciones IP.

Modo en la nube

Una instancia WAF en la nube solo puede proteger servidores basados en nombres de dominio, pero no en direcciones IP.

La dirección IP del servidor de origen configurada en WAF solo puede ser una dirección IP pública.

Para reducir el número de direcciones IP públicas, puede comprar Elastic Load Balance (ELB) o configurar balanceadores de carga para que funcionen como proxies de las direcciones IP privadas de backend y establezca la EIP (dirección IP pública) como la dirección IP de origen WAF.

Modo dedicado

Una instancia WAF dedicada o de equilibrio de carga puede proteger sitios web a través de nombres de dominio o direcciones IP.

La dirección IP del servidor de origen configurada en WAF puede ser una dirección IP pública o una dirección IP interna.

Para obtener más información sobre cómo agregar un nombre de dominio a WAF, consulte **¿Cómo agrego un nombre de dominio/dirección IP a WAF?**

1.1.2 ¿WAF puede proteger servidores en la nube o en las instalaciones?

Sí. Una instancia WAF en la nube puede proteger servidores en cualquier plataforma en la nube. Esto significa que WAF puede proteger tanto servidores en la nube como en las instalaciones, siempre que los servidores estén conectados a Internet.

Una instancia WAF en la nube protege sus servidores basándose en nombres de dominio, independientemente de si su servidor está en la nube o no, dónde reside su servidor o a qué proyecto o cuenta pertenece su servidor.

1.1.3 ¿Qué objetos protege WAF?

WAF puede proteger sitios web a través de nombres de dominio o direcciones IP.

- Las instancias en modo cloud de WAF pueden proteger sitios web solo a través de nombres de dominio.

  La dirección IP del servidor de origen configurada en WAF debe ser una dirección IP pública. Por ejemplo, si un balanceador de carga Elastic Load Balance (ELB) de Huawei Cloud está configurado para servidores de origen, una instancia de WAF en la nube puede proteger los servidores de origen siempre y cuando el balanceador de carga tenga una dirección IP pública enlazada.
- Las instancias WAF dedicadas pueden proteger sitios web a través de nombres de dominio o direcciones IP.

1.1.4 ¿Qué sistemas operativos soporta WAF?

WAF se implementa en la nube, lo que es irrelevante para un sistema operativo. Por lo tanto, WAF es compatible con cualquier sistema operativo. Un servidor de nombres de dominio en cualquier sistema operativo se puede conectar a WAF para su protección.

1.1.5 ¿En qué capas proporciona protección WAF?

WAF proporciona protección en siete capas, a saber, la capa física, la capa de enlace de datos, la capa de red, la capa de transporte, la capa de sesión, la capa de presentación y la capa de aplicación.

1.1.6 ¿Puedo usar WAF para verificar el estado de los servidores?

No. Si desea comprobar el estado de los servidores, se recomienda la combinación de ELB y WAF para sus cargas de trabajo. Después de configurar un balanceador de carga en ELB, puede habilitar las comprobaciones de estado para los servidores y usar el EIP del balanceador de carga como la dirección IP del servidor para establecer conexiones entre los servidores y WAF.

1.1.7 ¿WAF admite el almacenamiento en caché de archivos?

WAF almacena en caché solo las páginas web estáticas que están configuradas con protección contra manipulaciones web y envía las páginas web almacenadas en caché que no se manipulan a los visitantes web.

Si desea almacenar en caché todos los contenidos del sitio web, puede desplegar CDN y desplegar WAF entre CDN y el servidor de origen. Para obtener más información, consulte **Configuración de dominio con CDN y WAF desplegados**.

1.1.8 Acerca de la protección WAF

¿Qué es una dirección IP de protección?

Una dirección IP de protección en WAF es la dirección IP de un sitio web que utiliza WAF para proteger.

¿WAF admite la detección de vulnerabilidades?

La función básica de protección web de WAF puede detectar y bloquear amenazas como ataques de vulnerabilidad de herramientas de seguridad de terceros. Si habilita el elemento de escáner al configurar reglas básicas de protección web, WAF detecta escáneres y rastreadores, como OpenVAS y Nmap.

Para obtener más información acerca de cómo configurar una regla de protección web básica, consulte **Configuración de reglas de protección de web básica**.

¿WAF soporta los protocolos utilizados en MS Exchange?

WAF admite HTTP y HTTPS para iniciar sesión en Exchange en la web, pero no admite protocolos relacionados con el correo, como el protocolo simple de transferencia de correo (SMTP), el protocolo de oficina postal versión 3 (POP3) o el protocolo de acceso a mensajes de Internet (IMAP) utilizado por MS Exchange.

¿Puede la WAF defenderse contra los ataques de inyección de XOR?

Sí. WAF puede defenderse contra ataques de inyección XOR.

¿Por qué no se pueden bloquear los ataques en algunos escenarios después de que el nombre de dominio esté conectado a WAF?

Existe una alta probabilidad de que la inspección de encabezado en Protección Web básica no esté habilitada. La carga útil de ataque se transporta en el campo de encabezado definido por el usuario. El **Header Inspection** debe estar habilitado para bloquear este tipo de ataques. Para obtener más información, consulte **Configuración de reglas de protección de web básica**.

¿Qué es el parámetro bind_ip en los registros WAF?

Después de que su sitio web esté conectado a WAF, WAF funciona como un proxy inverso entre el cliente y el servidor de origen. WAF examina el tráfico a su sitio web, filtra el tráfico malicioso y reenvía el tráfico de salud a sus servidores de origen. **bind_ip** indica las direcciones IP WAF utilizadas por WAF para reenviar tráfico sano. Las direcciones IP de WAF deben estar en la lista blanca de su servidor de origen. Para obtener más detalles sobre cómo incluir direcciones IP de WAF en la lista blanca, consulte **¿Cómo incluyo rangos de direcciones IP en la lista blanca de WAF en la nube?**

¿Puede WAF proteger todos los nombres de dominio asignados a la dirección IP de mi sitio web si he conectado la dirección IP a WAF?

No.

En modo dedicado, la dirección IP del servidor de origen se puede conectar a WAF, y la dirección IP puede ser una dirección IP privada o interna. WAF protege solo el tráfico al que se accede a través de la dirección IP, pero no puede proteger el tráfico del nombre de dominio asignado a la dirección IP. Para proteger un nombre de dominio, conecte el nombre de dominio a WAF.

¿Por qué hay un gran número de solicitudes de tiempo de espera?

En modo de nube, WAF es compartido por usted y otros clientes. El crecimiento del servicio de otros clientes puede causar una alta latencia de reenvío de WAF. Si espera una baja

latencia, se recomiendan instancias de WAF dedicadas. En modo dedicado, las instancias de WAF son para su uso exclusivo, por lo que la latencia de reenvío de WAF no puede verse afectada por otros clientes.

1.1.9 ¿WAF admite la autenticación SSL bidireccional?

No. Puede configurar un certificado SSL unidireccional en WAF.

NOTA

Si establece **Client Protocol** en **HTTPS** al agregar un sitio web a WAF, se le pedirá que cargue un certificado y lo use para su sitio web.

Se recomienda utilizar un balanceador de carga ELB e instancias WAF dedicadas y, a continuación, configurar la autenticación bidireccional en el balanceador de carga. El procedimiento es el siguiente:

1. **Compre una instancia WAF dedicada**.
2. Conecte su sitio web a WAF y configure ELB. Para obtener más información, consulte **Proceso de conexión (modo dedicado)**.
3. Configure la autenticación bidireccional en el ELB. Para obtener más información, consulte **Autenticación mutua de HTTPS**.

1.1.10 ¿WAF admite el protocolo de capa de aplicación y el control de acceso basado en contenido?

WAF admite el control de acceso sobre el contenido en la capa de aplicación. HTTP y HTTPS son ambos protocolos de capa de aplicación.

1.1.11 ¿Puede WAF verificar el cuerpo que agrego a una solicitud POST?

La detección integrada de WAF comprueba los datos POST, y los web shells son los archivos enviados en las solicitudes POST. WAF comprueba todos los datos, como los formularios y los archivos JSON en las solicitudes POST basándose en las políticas de protección predeterminadas.

Puede configurar una regla de protección precisa para comprobar el cuerpo agregado a las solicitudes POST. Para obtener más información, consulte **Configuración de una regla de protección precisa**.

1.1.12 ¿Puede WAF limitar la velocidad de acceso de un nombre de dominio?

No. Puede personalizar una regla de protección contra ataques de CC para restringir el acceso a una URL específica en su sitio web basándose en una dirección IP, una cookie o un Referer, lo que mitiga los ataques de CC.

Para obtener más información, consulte **Configuración de una regla de protección contra ataque CC**.

1.1.13 ¿Puede WAF bloquear paquetes de datos en formato de multipart/form-data?

Sí. Puede **enviar un ticket de servicio** para solicitar la configuración para bloquear paquetes de datos en formato multipart/form-data.

El multipart/form-data indica que el navegador utiliza un formulario para cargar archivos. Por ejemplo, si se agrega un archivo adjunto a un correo electrónico, el archivo adjunto generalmente se carga en el servidor en formato demultipart/form-data.

1.1.14 ¿Se puede implementar una instancia WAF en la VPC?

Sí. Puede implementar instancias de WAF de motor dedicadas en una VPC.

1.1.15 ¿Puede WAF bloquear las solicitudes de URL que contengan caracteres especiales?

No. WAF solo puede detectar y restringir las direcciones IP de origen.

1.1.16 ¿Puede WAF bloquear el Spam y los registros de usuarios maliciosos?

WAF no puede bloquear los ataques relacionados con el negocio, como el spam y los registros de usuarios maliciosos. Para evitar estos ataques, configure el mecanismo de verificación de registro en su sitio web.

WAF está diseñado para mantener las aplicaciones web estables y seguras. Examina todas las solicitudes HTTP y HTTPS para detectar y bloquear ataques de red sospechosos, tales como inyecciones de lenguaje de consulta estructurado (SQL), ataques de scripting entre sitios (XSS), carga de shell web, inyecciones de comandos o código, inclusión de archivos, acceso no autorizado a archivos sensibles, vulnerabilidades de terceros, ataques Challenge Collapsar (CC), rastreadores maliciosos y falsificación de solicitudes entre sitios (CSRF).

1.1.17 ¿Puede WAF bloquear solicitudes para llamar a otras API desde páginas web?

Si los datos de solicitud para llamar a otras API en la página web se incluyen en los nombres de dominio protegidos por WAF, los datos de solicitud pasan a través de WAF. WAF comprueba los datos de la solicitud y los bloquea si se trata de un ataque.

Si los datos de solicitud para llamar a otras API en la página web no se incluyen en los nombres de dominio protegidos por WAF, los datos de solicitud no pasan a través de WAF. WAF no puede bloquear los datos de la solicitud.

1.1.18 ¿Puedo configurar el cookies de sesión en WAF?

No. WAF no admite cookies de sesión.

WAF le permite configurar reglas de protección contra ataques de CC para limitar la frecuencia de acceso de una ruta específica (URL) en un solo campo de cookie, identificar con precisión los ataques de CC y mitigar eficazmente los ataques de CC. Por ejemplo, si un usuario cuyo ID de cookie es **name** accede a la página **/admin*** bajo el nombre de dominio protegido durante más de 10 veces en 60 segundos, puede configurar una regla de protección

contra ataques CC para prohibir que el usuario acceda al nombre de dominio durante 600 segundos.

Para obtener más información acerca de cómo configurar una regla de protección contra ataques de CC, consulte **Configuración de reglas de protección contra ataques de CC**.

¿Qué son las cookies?

Cookies son datos (normalmente cifrados) almacenados en el terminal local de un usuario por un sitio web para identificar al usuario y rastrear sesiones. Las cookies son enviadas por un servidor web a un navegador para registrar información personal del usuario.

Una cookie consiste en un nombre, un valor y varios atributos opcionales que controlan el período de validez de la cookie, la seguridad y el alcance de uso. Las cookies se clasifican en cookies de sesión y cookies persistentes. Los detalles son los siguientes:

- Cookie de sesión

  Una cookie de sesión solo existe en la memoria temporal mientras el usuario navega por el sitio web. No tiene fecha de caducidad. Cuando se cierra el navegador, las cookies de sesión se eliminan.

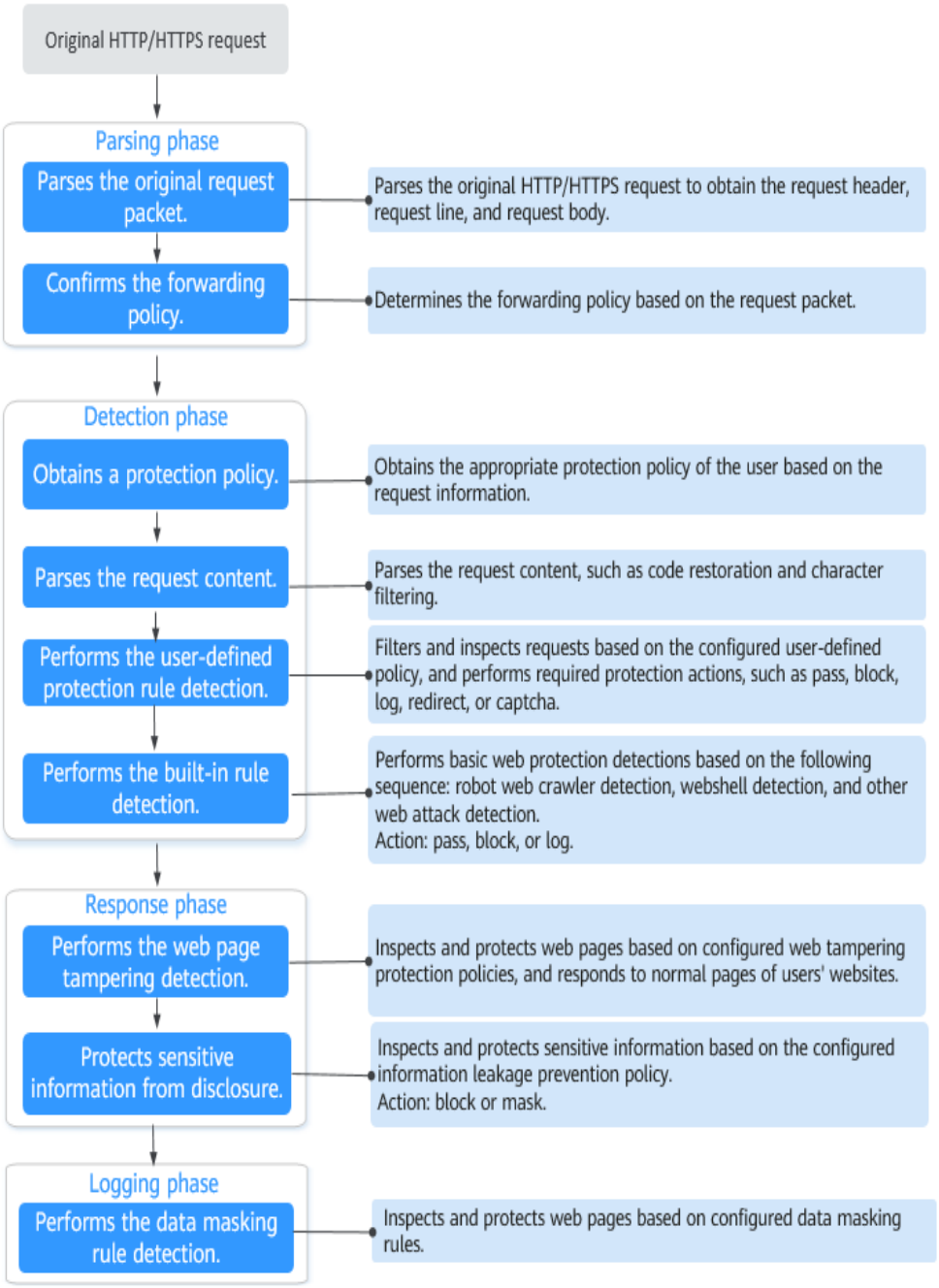
- Cookie persistente

  Una cookie persistente tiene una fecha de caducidad y se almacena en discos. Las cookies persistentes se eliminarán después de un período de tiempo específico.

1.1.19 ¿WAF bloquea las solicitudes POST personalizadas?

No. WAF no bloquea las solicitudes POST definidas por el usuario. **Figura 1-1** muestra el proceso de detección de las reglas de protección incorporadas WAF para las solicitudes HTTP/HTTPS originales.

Figura 1-1 Proceso de detección del motor WAF



Para obtener más información sobre el proceso de protección WAF, consulte **Guía de configuración**.

1.1.20 ¿Puede WAF limitar el acceso a través de nombres de dominio?

No. WAF admite las reglas de listas negras y blancas para bloquear, registrar solo o permitir solicitudes de acceso desde direcciones IP o segmentos de direcciones IP especificados.

Puede configurar reglas de listas negras y blancas para bloquear, registrar únicamente o permitir solicitudes de acceso desde las direcciones IP o segmentos de direcciones IP correspondientes a los nombres de dominio.

1.1.21 ¿Tiene WAF el módulo IPS?

A diferencia de los firewalls tradicionales, WAF no tiene un sistema de prevención de intrusiones (IPS). WAF admite la detección de intrusos solo de solicitudes HTTP/HTTPS.

1.1.22 ¿Cuáles son las diferencias entre las funciones de protección contra manipulaciones web de WAF y HSS?

1.1.23 ¿Qué protocolos de marco de servicio de web soporta WAF?

WAF se despliega en la nube.

Web Application Firewall (WAF) mantiene los servicios web estables y seguros. Examina todas las solicitudes HTTP y HTTPS para detectar y bloquear los siguientes ataques: inyección de lenguaje de consulta estructurado (SQL), secuencias de comandos en sitios cruzados (XSS), shells web, inyecciones de comandos y código, inclusión de archivos, acceso a archivos confidenciales, vulnerabilidades de terceros, ataque Challenge Collapsar (CC), rastreadores maliciosos y falsificación de solicitudes entre sitios (CSRF).

WAF puede examinar las siguientes solicitudes:

- WebSocket y WebSockets (habilitado de forma predeterminada)
  - La inspección de solicitud de WebSocket está habilitada de forma predeterminada si **Client Protocol** está establecido en **HTTP**.
  - La inspección de solicitud de WebSockets está habilitada de forma predeterminada si **Client Protocol** está establecido en **HTTPS**.
- HTTP/HTTPS

AVISO

Actualmente, HTTP/2 (HTTP2.0) se puede habilitar en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok

1.1.24 ¿Puede WAF proteger los sitios web a los que se accede a través de la autenticación HSTS o NTLM?

Sí. WAF puede proteger aplicaciones HTTP y HTTPS.

- Si un sitio web utiliza la política HTTP Strict Transport Security (HSTS), el cliente (como un navegador) se ve obligado a usar HTTPS para comunicarse con el sitio web. Esto reduce el riesgo de secuestro de sesión. Los sitios web configurados con la política HSTS utilizan el protocolo HTTPS. Por lo tanto, WAF puede proteger estos sitios web.
- Windows New Technology LAN Manager (NTLM) es un método de autenticación a través de HTTP. NTLM utiliza un protocolo de enlace de tres vías para autenticar una

conexión. NTLM autentica un cliente (como un explorador) de la misma manera que lo hace la autenticación de inicio de sesión remoto de Windows.

WAF puede proteger las aplicaciones que utilizan NTLM para autenticar la conexión entre un servidor y un cliente, como un explorador.

1.1.25 ¿Pueden mis instancias WAF ser escalables automáticamente?

No.

Puede desplegar WAF en la nube o modo dedicado para satisfacer sus necesidades de servicio.

1.1.26 ¿Cuáles son las diferencias entre WAF Forwarding y Nginx Forwarding?

Nginx reenvía directamente las solicitudes de acceso al servidor de origen, mientras que WAF detecta y filtra el tráfico malicioso y luego reenvía solo las solicitudes de acceso normales al servidor de origen. Detalles:

- Reenvío de WAF

  Después de que un sitio web se conecta a WAF, todas las solicitudes de acceso pasan a través de WAF. WAF detecta solicitudes HTTP (S) para identificar y bloquear una amplia gama de ataques, tales como inyección SQL, ataques de scripting entre sitios, cargas de shell web, inyección de comando / código, inclusión de archivos, acceso a archivos sensibles, ataques de vulnerabilidad de aplicaciones de terceros, ataques de CC, rastreadores maliciosos, ataques de falsificación de solicitudes entre sitios (CSRF). A continuación, WAF envía tráfico normal al servidor de origen. De esta manera, la seguridad, la estabilidad y la disponibilidad de sus aplicaciones web están garantizadas.

  Figura 1-2 Cómo protege WAF un sitio web

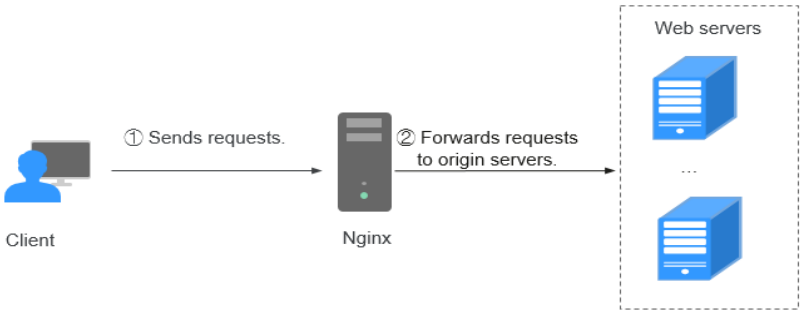
  

- Reenvío de Nginx

  Nginx funciona como un servidor proxy inverso. Después de recibir la solicitud de acceso desde el cliente, el servidor proxy inverso reenvía directamente la solicitud de acceso al servidor web y devuelve el resultado obtenido desde el servidor web al cliente. El servidor proxy inverso se instala en la sala de equipos del sitio web. Funciona como un proxy para que el servidor web reciba y reenvíe solicitudes de acceso.

  El servidor proxy inverso evita los ataques maliciosos de Internet a los servidores de intranet, almacena en caché los datos para reducir las cargas de trabajo en los servidores de intranet e implementa el control de seguridad de acceso y el equilibrio de carga.

Figura 1-3 Cómo funciona Nginx



1.1.27 ¿WAF almacena en caché los datos del sitio web?

WAF protege los datos del usuario en la capa de la aplicación. Soporta la configuración de caché en páginas web estáticas. Cuando un usuario accede a una página web, el sistema devuelve una página almacenada en caché al usuario y comprueba aleatoriamente si la página ha sido manipulada.

WAF no almacena en caché los datos del sitio web. Si desea almacenar en caché el contenido del sitio web, use CDN o despliegue tanto WAF como CDN.

Para obtener detalles sobre la combinación de WAF y CDN, consulte **Combinar WAF y CDN: Mejor protección y acceso más rápido**.

1.1.28 ¿WAF es un firewall de hardware o un firewall de software?

WAF es un firewall de software. Después de comprar WAF, solo necesita conectar su nombre de dominio para usar WAF para proteger sus aplicaciones web.

Para obtener más información, consulte **Adición de un nombre de dominio a WAF**.

1.1.29 ¿Cuáles son las diferencias entre WAF y CFW?

Web Application Firewall (WAF) y Cloud Firewall (CFW) son diferentes productos proporcionados por Huawei Cloud. WAF se utiliza para proteger su servicio web, mientras que CFW se utiliza para proteger el tráfico de fronteras de Internet y VPC.

Tabla 1-1 enumera las diferencias entre WAF y CFW.

Tabla 1-1 Diferencias entre WAF y CFW

Categoría	WAF	CFW
Definiciones	Web Application Firewall (WAF) mantiene los servicios web estables y seguros. Examina todas las solicitudes HTTP y HTTPS para detectar y bloquear los siguientes ataques: inyección de lenguaje de consulta estructurado (SQL), secuencias de comandos en sitios cruzados (XSS), shells web, inyecciones de comandos y código, inclusión de archivos, acceso a archivos confidenciales, vulnerabilidades de terceros, ataque Challenge Collapsar (CC), rastreadores maliciosos y falsificación de solicitudes entre sitios (CSRF).	For details, see *Cloud Firewall User Guide*.
Mecanismo de protección	WAF funciona como un proxy inverso entre el cliente y el servidor de origen. Todas las solicitudes de acceso al sitio web se envían primero a WAF. WAF detecta y filtra el tráfico de ataques maliciosos y devuelve el tráfico normal al servidor de origen para garantizar que el servidor de origen sea seguro, estable y esté disponible.	CFW puede implementar un control refinado sobre todo el tráfico, incluida la protección de fronteras de Internet, el tráfico cruzado de VPC y cruce de VPC, para evitar la intrusión externa, los ataques de penetración interna y el acceso no autorizado desde el interior hacia el exterior.

Categoría	WAF	CFW
Modo de despliegue	WAF se puede implementar en modo en la nube y modo dedicado. ● WAF en la nube es una buena opción si sus servidores de servicio se despliega en Huawei Cloud, en cualquier otra nube, incluso en centros de datos locales solo mientras tengan nombres de dominio. Los escenarios de aplicación para diferentes ediciones son los siguientes: – Arrancador Esta edición es adecuada para la protección de sitios web personales. – Edición estándar Esta edición es adecuada para sitios web pequeños y medianos que no tienen requisitos de seguridad especiales. – Edición profesional Esta edición es adecuada para sitios web o servicios de empresas medianas que están abiertos a Internet, se centran en la seguridad de los datos y tienen altos requisitos de seguridad. – Edición platino Esta edición es adecuada para sitios web de grandes y medianas empresas que tienen servicios a gran escala o tienen requisitos de seguridad especiales. ● **Dedicated mode**: Las instancias de WAF dedicadas son una buena opción si sus servidores de servicio se despliega en Huawei Cloud siempre y cuando tengan nombres de dominio o direcciones IP. Las instancias de WAF dedicadas son sitios web adecuados para grandes empresas que tienen una gran escala de servicio y tienen requisitos de seguridad personalizados.	Protección para frontera de Internet y frontera de VPC

Categoría	WAF	CFW
Objetos de protección	● Modo en la nube: nombres de dominio ● Modo dedicado: nombres de dominio o direcciones IP	Dirección IP elástica (EIP)
Funciones	WAF identifica y bloquea una amplia gama de ataques sospechosos, tales como inyecciones de lenguaje de consulta estructurado (SQL), ataques de scripting entre sitios (XSS), carga de shell web, inyecciones de comandos o código, inclusión de archivos, acceso no autorizado a archivos sensibles, vulnerabilidades de terceros, ataque Challenge Collapsar (CC), rastreadores maliciosos y falsificación de solicitudes entre sitios (CSRF).	● Gestión de activos y defensa contra intrusiones: CFW detecta y defiende contra intrusiones en activos en la nube que son accesibles a través de Internet en tiempo real. ● Control de acceso: Puede controlar el acceso en las fronteras de Internet. ● Análisis de tráfico y auditoría de log: CFW controla, analiza y visualiza el tráfico de VPC, audita logs y rastrea las fuentes de tráfico.

1.1.30 ¿Hay algún impacto en los servidores de origen si habilito HTTP/2 en WAF?

Sí. HTTP/2 no es compatible entre WAF y el servidor de origen. Esto significa que si habilita HTTP/2 en WAF, WAF puede procesar solicitudes HTTP/2 de clientes, pero WAF solo puede reenviar las solicitudes al servidor de origen usando HTTP 1.0/1.1. Por lo tanto, el ancho de banda del servicio de los servidores de origen puede aumentar ya que la multiplexación en HTTP/2 puede volverse inválida para los servidores de origen.

1.1.31 ¿Cómo WAF detecta la inyección SQL y los ataques XSS?

Una inyección de lenguaje de consulta estructurado (SQL) es un ataque web común. El atacante inyecta comandos SQL maliciosos en cadenas de consulta de la base de datos para engañar al servidor para ejecutar comandos. Al explotar estos comandos, el atacante puede obtener información confidencial, agregar usuarios, exportar archivos o incluso obtener los permisos más altos para la base de datos o el sistema.

Los ataques XSS aprovechan las vulnerabilidades dejadas durante el desarrollo de la página web para inyectar código de instrucciones maliciosas en las páginas web para que los atacantes puedan engañar a los visitantes para que carguen y ejecuten programas maliciosos de página web fabricados por los atacantes. Estos programas maliciosos de páginas web son generalmente JavaScript pero también pueden incluir Java, VBScript, ActiveX, Flash, o incluso HTML común. Después de que un ataque tenga éxito, el atacante puede obtener

varios contenidos, incluidos, entre otros, permisos más altos (por ejemplo, permisos para ciertas operaciones), contenido privado, sesiones y cookies.

¿Cómo WAF detecta los ataques de inyección SQL?

WAF detecta y compara palabras clave SQL, caracteres especiales, operadores y símbolos de comentarios.

- Palabras clave de SQL: union, Select, from, as, asc, desc, order by, sort, and, or, load, delete, update, execute, count, top, between, declare, distinct, distinctrow, sleep, waitfor, delay, having, sysdate, when, dba_user, case, delay, y the like
- Especial characters: ',; ()
- Operadores matemáticos: ±, *****, /, **%** y |
- Operadores: =, >, <, >=, <=, **!**=, += y **-=**
- Símbolos de comentario: – o /**/

¿Cómo detecta WAF ataques XSS?

WAF comprueba las etiquetas de script HTML, los procesadores de eventos, los protocolos de script y los estilos para evitar que los usuarios malintencionados inyecten declaraciones XSS malintencionadas a través de las solicitudes del cliente.

- Palabras clave XSS (como **javascript**, **script**, **object**, **style**, **iframe**, **body**, **input**, **form**, **onerror** y **alert**)
- Caracteres especiales (<, >, ', y ")
- Enlaces externos (href="http://xxx/",src="http://xxx/attack.js")

NOTA

El texto enriquecido se puede cargar usando la carga de varias partes en lugar del cuerpo. En la carga multiparte, el texto enriquecido se almacena en formularios y se puede decodificar incluso si se codifica usando Base64. Analice sus servicios y no utilice comillas ni corchetes angulares en la medida de lo posible.

1.1.32 ¿Una instancia WAF dedicada admite la protección entre VPC?

Las instancias de WAF dedicadas no pueden proteger los servidores de origen en las VPC que son diferentes de donde se encuentran esas instancias de WAF. Para proteger estos servidores de origen, compre instancias dedicadas de WAF en la misma VPC que para los servidores de origen.

1.1.33 ¿Cuáles son las diferencias entre la prevención de inyección SQL en WAF y DBSS?

WAF puede defenderse contra ataques de inyección SQL evitando la ejecución de comandos SQL maliciosos. Para obtener más información, consulte **Cómo WAF protege contra ataques de inyección SQL**.

DBSS proporciona una biblioteca de inyección SQL, que facilita la generación de informes de alarmas para excepciones de base de datos basadas en la función del comando SQL o la gravedad del riesgo.

1.2 Uso de WAF

1.2.1 ¿Por qué la herramienta de análisis de vulnerabilidades informa de los puertos no estándar deshabilitados para mi sitio web protegido por WAF?

Síntomas

Cuando una herramienta de análisis de vulnerabilidades de terceros analiza el sitio web cuyo nombre de dominio se ha conectado a WAF, el resultado del análisis muestra que algunos puertos estándar (por ejemplo, 443) y puertos no estándar (por ejemplo, 8000 y 8443) son vulnerables.

Causa posible

WAF utiliza el mismo motor de puerto no estándar para todos los usuarios de WAF. Por lo tanto, si una herramienta de análisis de vulnerabilidad de terceros realiza un análisis de su sitio web, se informa de los puertos no estándar habilitados en WAF. Esto significa que estas vulnerabilidades de puerto en los resultados de análisis no afectan a la seguridad del servidor de origen. WAF protegerá su sitio web después de que indique la dirección IP del servidor de origen a la dirección IP del motor WAF a través del registro CNAME.

Sugerencias sobre el manejo

No se requiere ninguna medida.

1.2.2 ¿Cuáles son las restricciones al uso de WAF en Proyecto empresarials?

Cada proyecto de empresa es independiente de los demás.

- Las políticas creadas solo pueden ser utilizadas por sus propios proyectos. Por ejemplo, si crea la política A para un proyecto principal, las reglas creadas para los subproyectos no pertenecen a la política A. Debe crear una política para subproyectos por separado.
- Los certificados creados solo pueden ser utilizados por sus propios proyectos. Un proyecto principal y subproyecto solo pueden utilizar sus propios certificados.

1.2.3 ¿WAF afecta a los puertos de correo electrónico o a la recepción y envío de correo electrónico?

WAF protege las páginas de aplicaciones web. Después de que su sitio web esté conectado a WAF, no hay impacto en su puerto de correo electrónico o envío o recepción de correo electrónico.

1.2.4 ¿Cómo obtengo la dirección IP real de un visitante web?

Después de conectar un sitio web a su instancia WAF, WAF funciona como un proxy inverso entre el cliente y el servidor. La dirección IP real del servidor está oculta y solo la dirección IP de WAF es visible para los visitantes de la web.

Generalmente, un proxy tal como CDN, WAF, y servicio anti-DDoS se despliega entre el cliente y el servidor. Los visitantes Web no pueden acceder directamente al servidor. Por ejemplo, **web visitor** > **CDN/WAF/anti-DDoS** > **origin server**.

Al reenviar solicitudes al servidor descendente, el servidor proxy transparente añade un campo **X-Forwarded-For** al encabezado HTTP para identificar la dirección IP real del visitante web en el formato **X-Forwarded-For: real IP address of the web visitor, proxy 1-IP address, proxy 2-IP address, proxy 3-IP address, ...->...**.

Por lo tanto, puede obtener la dirección IP real del visitante web desde el campo **X-Forwarded-For**. La primera dirección IP en este campo es la dirección IP real del visitante web.

Para obtener más información, consulte **Obtención de la dirección IP real de un visitante web**.

1.2.5 ¿Cómo bloquea las solicitudes WAF?

WAF comprueba tanto el encabezado como el cuerpo de la solicitud. Por ejemplo, WAF detecta el cuerpo de la solicitud, como los datos de formulario, XML y JSON, y bloquea las solicitudes que no cumplen con las reglas de protección.

Para obtener más información sobre el proceso de protección WAF, consulte **Guía de configuración**.

1.2.6 ¿Se permitirá el tráfico después de que WAF se cambie al modo bypasssed?

Para las instancias de WAF en la nube, si cambia la instancia de trabajo **Mode** a **Bypassed**, las solicitudes se envían directamente al servidor backend original sin pasar a través de WAF.

Cambie el modo WAF a **Bypassed** solo si se cumple una de las siguientes condiciones:

- Los servicios del sitio web deben ser restaurados al estado cuando el sitio web no está conectado a WAF.
- Es necesario investigar los errores del sitio web, como 502, 504, u otros problemas de incompatibilidad.
- No se configura ningún proxy entre el cliente y WAF.

Tiempo efectivo del modo de trabajo de bypassed de WAF

Después de cambiar el **Mode** de trabajo WAF a **Bypassed**, su efecto será de 3 a 5 minutos.

Procedimiento para la conmutación del mecanismo de trabajo WAF

Paso 1 **Inicie sesión en la consola de gestión**.

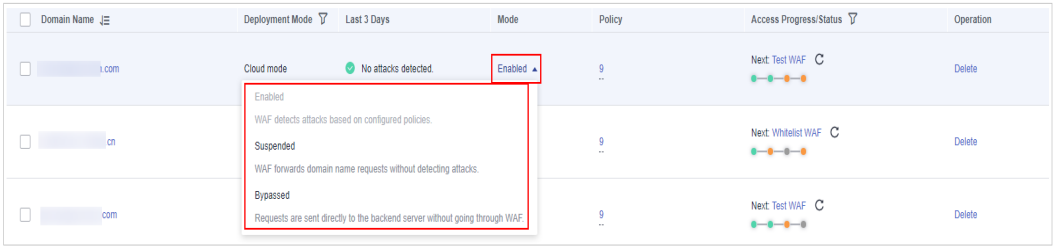
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en ☰ en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 En el panel de navegación, seleccione **Website Settings**.

Paso 5 En la fila que contiene el nombre de dominio de destino, haga clic en ▼ en la columna **Mode**.

Figura 1-4 Cambio de modo de trabajo de WAF



----Fin

1.2.7 ¿Qué son la inclusión de archivos locales y la inclusión de archivos remotos?

Puede ver eventos de seguridad como la inclusión de archivos en eventos de protección WAF para localizar rápidamente las fuentes de ataque o analizar los eventos de ataque.

Los desarrolladores de programas escriben funciones usadas repetidamente en un solo archivo. Cuando estas funciones necesitan ser utilizadas, el archivo es invocado directamente. El proceso de invocación de archivos se denomina inclusión de archivos. Las vulnerabilidades de inclusión de archivos se clasifican en dos categorías, según si el archivo es un archivo alojado remotamente o un archivo local disponible en el servidor web:

- Inclusión de archivos locales
- Inclusión de archivos remotos

Una vulnerabilidad de inclusión de archivos permite al atacante acceder a archivos confidenciales o no autorizados disponibles en el servidor web o ejecutar archivos maliciosos en el servidor web mediante el uso de dicho archivo. Esta vulnerabilidad se debe principalmente a un mecanismo de validación de entrada incorrecto, en el que la entrada del usuario que se pasa al archivo incluye comandos sin una validación adecuada. El impacto de esta vulnerabilidad puede provocar la ejecución de código malicioso en el servidor o revelar datos presentes en archivos confidenciales.

Para obtener más información sobre los registros de eventos de protección, consulte **Consulta de registros de eventos de protección**.

1.2.8 ¿Cuál es la diferencia entre QPS y el número de solicitudes?

Consultas por segundo (QPS) indica el número de solicitudes por segundo. Por ejemplo, una solicitud HTTP GET también se denomina consulta. El número de solicitudes es el número total de solicitudes en un intervalo de tiempo específico.

Consultas por segundo (QPS) es el número de solicitudes que un servidor puede manejar por segundo.

NOTA

QPS se utiliza para medir el número de consultas, o solicitudes, por segundo.

Para obtener más información sobre QPS en la página **Dashboard**, consulte **Tabla 1-2**.

Tabla 1-2 Cálculo de QPS

Rango de tiempo	Descripción promedio de QPS	Pico QPS Descripción
Ayer o **Hoy**	La curva QPS se realiza con los QPS promedio cada dos minutos.	La curva QPS se realiza con cada pico QPS cada dos minutos.
Últimos 3 días	La curva QPS se realiza con los QPS promedio cada cinco minutos.	La curva QPS se realiza con cada pico QPS cada dos minutos.
Últimos 7 días	La curva de QPS se realiza con el valor máximo entre los QPS promedio en cada cinco minutos a un intervalo de 10 minutos.	La curva QPS se realiza con cada pico QPS cada 10 minutos.
Últimos 30 días	La curva QPS se realiza con el valor máximo entre los QPS promedio en cada cinco minutos en un intervalo de una hora.	La curva de QPS se realiza con los QPS pico en cada hora.

Para obtener más información sobre el rendimiento de QPS de diferentes ediciones WAF, consulte **Diferencias de ediciones**.

1.2.9 ¿Qué son las solicitudes simultáneas?

El número de solicitudes simultáneas se refiere al número de solicitudes que el sistema puede procesar simultáneamente. Cuando se trata de un sitio web, las solicitudes simultáneas se refieren a las solicitudes de los visitantes al mismo tiempo.

Para obtener más información, consulte **Diferencias de edición**.

1.2.10 ¿Puede el WAF bloquear las solicitudes cuando se monta un certificado en ELB?

Si el certificado está montado en ELB, todas las solicitudes enviadas a través de WAF se cifran. Para los servicios HTTPS, debe cargar el certificado en WAF para que WAF pueda detectar la solicitud descifrada y determinar si desea bloquear la solicitud.

1.2.11 ¿WAF admite políticas de autorización personalizadas?

WAF admite políticas de autorización personalizadas. Con IAM, usted puede:

- Crear usuarios de IAM para empleados en función de la estructura organizativa de su empresa. Cada usuario de IAM tiene sus propias credenciales de seguridad, lo que proporciona acceso a los recursos WAF.

- Otorgar únicamente los permisos necesarios para que los usuarios realicen una tarea.
- Confiar una cuenta de Huawei Cloud o un servicio en la nube para realizar operaciones profesionales y eficientes en sus recursos WAF.

Para obtener más información, consulte **Creación de un grupo de usuario y concesión de permisos**.

1.2.12 ¿WAF afecta a mis cargas de trabajo existentes y a la ejecución del servidor?

Habilitación de WAF no interrumpe las cargas de trabajo existentes ni afecta al estado de ejecución de los servidores de origen. No se requiere ninguna operación adicional (como el apagado o el reinicio) en los servidores de origen.

AVISO

Si está utilizando una instancia WAF en la nube, solo necesita cambiar el registro de resolución DNS de su sitio web para permitir que el tráfico pase a través de WAF. La modificación de la resolución DNS puede afectar a los servicios de acceso al sitio web. Se aconseja realizar la operación durante las horas de menor actividad. Para obtener más información, consulte **Conexión a un nombre de dominio a WAF**.

WAF ofrece las instancias en la nube y dedicadas para proteger sus sitios web. Puede agregar nombres de dominio o direcciones IP a WAF. Antes de comenzar, familiarícese con las siguientes diferencias:

- Modo en la nube: protege sus aplicaciones web que tienen nombre de dominio y se implementan en Huawei Cloud, cualquier otra nube o centros de datos locales.
- Modo dedicado: protege las aplicaciones web desplegadas en Huawei Cloud y accesibles a través de nombres de dominio o direcciones IP.

1.2.13 ¿Cómo configuro mi servidor para permitir solo solicitudes de WAF?

Puede configurar una regla de control de acceso en el servidor de origen para permitir que solo las direcciones IP de origen WAF tengan acceso al servidor de origen. Esto evita que los hackers eludan WAF para atacar el servidor de origen a través de las direcciones IP del servidor de origen, garantizando la seguridad, estabilidad y disponibilidad del servidor de origen.

Para obtener más detalles, consulte las siguientes secciones:

- Configure una política de control de acceso en el servidor de origen para incluir en la lista blanca las direcciones IP de WAF.
  - Modo en la nube: Consulte **¿Cómo incluyo rangos de direcciones IP en la lista blanca de WAF en la nube?**
  - Modo dedicado: Consulte **Incluir en la lista blanca las direcciones IP de origen de sus instancias de WAF dedicadas**.
- Deshabilite otros firewalls y software de seguridad en los servidores de origen.

1.2.14 Why Do Cookies Contain the HWWAFSESID or HWWAFSESTIME field?

After a domain name or IP address is connected to WAF, WAF inserts fields such as **HWWAFSESID** and **HWWAFSESTIME** into the cookie of customer requests. These fields are used for WAF statistics and security features and do not affect user services.

1.2.15 ¿Puedo cambiar entre el modo de Cloud de WAF y el modo dedicado?

No se admite la conmutación directa, pero puede completar las configuraciones requeridas y luego usar el modo WAF que desee. Cuando agrega un nombre de dominio o una dirección IP a WAF, puede seleccionar el modo en la nube o el modo dedicado para satisfacer las diferentes necesidades del negocio. Una vez que seleccione un modo WAF y conecte el nombre de dominio a WAF, el modo WAF no se puede cambiar directamente.

Si desea utilizar otro modo WAF para el nombre de dominio, implemente sus servicios en el modo WAF que desee primero. A continuación, quite el nombre de dominio o la dirección IP de la instancia WAF actual y agréguelo a la instancia WAF en el modo WAF que desee. Por ejemplo, está utilizando una instancia WAF en la nube para proteger el nombre de dominio www.example.com. Si desea utilizar una instancia WAF dedicada para proteger www.example.com, asegúrese de que sus servicios actuales son compatibles con el modo dedicado WAF. Luego, puede comprar una instancia WAF dedicada y quitar el nombre de dominio protegido www.example.com de la instancia WAF en la nube. A continuación, agregue www.example.com a la instancia de WAF dedicada.

AVISO

1.2.16 ¿Puedo agregar un nombre de dominio o una dirección IP a WAF bajo diferentes cuentas?

Si su nombre de dominio se ha agregado a WAF en modo en nube, no se puede agregar de nuevo. Por lo tanto, un nombre de dominio no se puede agregar a WAF bajo diferentes cuentas.

Sin embargo, si utiliza instancias dedicadas con balanceo de carga, puede agregar nombres de dominio o direcciones IP a instancias WAF en diferentes cuentas.

WAF ofrece las instancias en la nube y dedicadas para proteger sus sitios web. Puede agregar nombres de dominio o direcciones IP a WAF. Antes de comenzar, familiarícese con las siguientes diferencias:

- Modo en la nube: protege sus aplicaciones web que tienen nombre de dominio y se implementan en Huawei Cloud, cualquier otra nube o centros de datos locales.
- Modo dedicado: protege las aplicaciones web desplegadas en Huawei Cloud y accesibles a través de nombres de dominio o direcciones IP.

AVISO

Cada combinación de un nombre de dominio/dirección IP y un puerto se cuenta para la cuota de nombres de dominio de la edición WAF que está utilizando. Por ejemplo, www.example.com:8080 y www.example.com:8081 usan dos nombres de dominio de la cuota. Si desea proteger los servicios web a través de varios puertos con el mismo nombre de dominio/dirección IP, agregue el nombre de dominio/dirección IP y cada puerto a WAF.

1.2.17 ¿Cómo configuro WAF si se implementa un servidor proxy inverso para mi sitio web?

En este caso, el servidor proxy inverso no se verá afectado después de que el sitio web esté conectado a WAF. WAF funciona como un proxy inverso entre el cliente y el servidor de su sitio web. Las direcciones IP reales de su servidor web están ocultas a los visitantes, y solo las direcciones IP de WAF son visibles para ellos.

Para más detalles, consulte **¿Cómo agrego un nombre de dominio/dirección IP a WAF?**

1.2.18 ¿Cómo reenvía las solicitudes de acceso WAF cuando un nombre de dominio comodín y un nombre de dominio único están conectados a WAF?

WAF reenvía preferentemente las solicitudes de acceso al único nombre de dominio. Si no se puede identificar el nombre de dominio único, las solicitudes de acceso se reenviarán al nombre de dominio de comodín.

Por ejemplo, si conecta el nombre de dominio único a.example.com y el nombre de dominio comodín *.example.com a WAF, WAF reenvía preferentemente las solicitudes de acceso al nombre de dominio único a.example.com.

Si está configurando un nombre de dominio comodín, preste atención a lo siguiente:

- Si la dirección IP del servidor de cada nombre de subdominio es la misma, introduzca un nombre de dominio de comodín. Por ejemplo, si los nombres de subdominio ***a.example.com***, ***b.example.com*** y ***c.example.com*** tienen la misma dirección IP del servidor, puede agregar el nombre de dominio de comodín ****.example.com*** a WAF para proteger los tres.
- Si las direcciones IP del servidor de los nombres de subdominio son diferentes, agregue nombres de subdominio como nombres de dominio únicos uno por uno.

1.2.19 ¿Gzip en el servidor de origen afecta a WAF?

Si gzip está habilitado en el servidor de origen, WAF puede bloquear incorrectamente las solicitudes de acceso normales desde el servidor de origen. Si la solicitud bloqueada es una solicitud de acceso normal, puede manejar el evento como una falsa alarma haciendo referencia a **Manejo de alarmas falsas**. Después de que un evento es manejado como una falsa alarma, WAF deja de bloquear el tipo correspondiente de evento. No se mostrará este tipo de evento en la página **Events** y ya no recibirá notificaciones de alarma en consecuencia.

1.2.20 Does WAF Affect Data Transmission from the Internal Network to an External Network?

No. After a website is connected to WAF, all website access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to keep your origin server is secure, stable, and available.

1.2.21 ¿Necesito realizar algunos cambios en WAF si se cambia el grupo de seguridad para servidor de origen (Dirección)?

No se requieren modificaciones en WAF, pero se requiere que incluya las direcciones IP de WAF en los servidores de origen.

El procedimiento varía en función del tipo de instancia WAF que esté utilizando:

- Modo en la nube: **Incluir en la lista blanca direcciones IP de WAF**
- Modo dedicado: **Incluir en la lista blanca las direcciones IP de origen de sus instancias WAF dedicadas**

1.2.22 ¿Cómo se balancea la carga cuando se configuran varios servidores de origen en WAF?

Si ha configurado varias direcciones IP del servidor de origen, WAF utiliza el algoritmo round robin ponderado para distribuir las solicitudes de acceso de forma predeterminada. También puede personalizar un algoritmo de balanceo de carga según sea necesario. Para obtener más información, consulte **Cambio de algoritmo de balanceo de carga**.

1.3 Las regiones y las AZ

1.3.1 ¿Qué son las Regiones y las AZ?

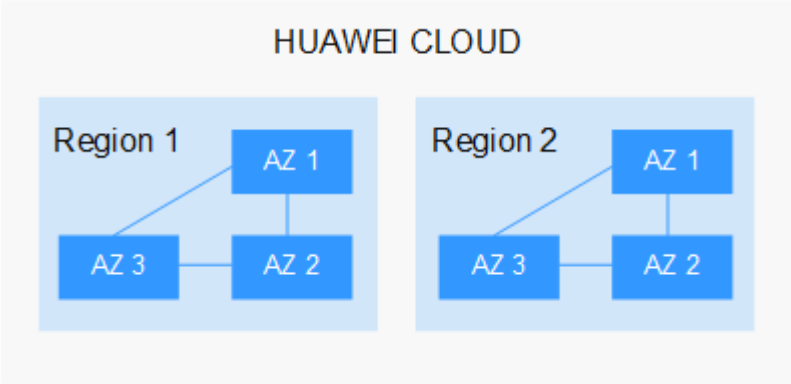
Conceptos

Una región y una zona de disponibilidad (AZ) identifican la ubicación de un centro de datos. Puede crear recursos en una región específica y AZ.

- Las regiones se dividen de las dimensiones de la ubicación geográfica y la latencia de la red. Los servicios públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), se comparten dentro de la misma región. Las regiones se clasifican como regiones universales y regiones dedicadas. Una región universal proporciona servicios en la nube universales para los tenants estándares. Una región dedicada proporciona servicios del mismo tipo solo o para tenants específicos.
- Una AZ contiene uno o más centros de datos físicos. Cada AZ cuenta con instalaciones independientes de electricidad, de refrigeración, de extinción de incendios y a prueba de humedad. Dentro de una AZ, los recursos de computación, red, almacenamiento y otros se dividen de forma lógica en múltiples clústeres. Las AZ dentro de una región están interconectadas mediante fibras ópticas de alta velocidad para permitirle construir sistemas de alta disponibilidad entre AZ.

Figura 1-5 muestra la relación entre las regiones y las zonas de disponibilidad.

Figura 1-5 Región y AZ



Huawei Cloud ofrece servicios en muchas regiones de todo el mundo. Puede seleccionar una región y una AZ según sea necesario.

Selección de una región

Al seleccionar una región, tenga en cuenta los siguientes factores:

- Localización

  Se recomienda seleccionar una región cercana a usted o a sus usuarios objetivo. Esto reduce la latencia de la red y mejora la velocidad de acceso.

  – Si usted o sus usuarios se encuentran en la región Asia Pacífico y fuera de China continental, seleccione la región **CN-Hong Kong**, **AP-Bangkok** o **AP-Singapore**.
  – Si usted o sus usuarios están en África, seleccione la región **AF-Johannesburg**.
  – Si usted o sus usuarios están en América Latina, seleccione la región **LA-Santiago**.

- Precio del recurso

  Los precios de los recursos pueden variar en diferentes regiones. Para obtener más información, consulte **Detalles de precios del producto**.

Selección de una AZ

Al determinar si se deben desplegar recursos en la misma AZ, tenga en cuenta los requisitos de recuperación ante desastres (DR) y latencia de red de sus aplicaciones.

- Para una alta capacidad de DR, despliegue recursos en diferentes AZ en la misma región.
- Para una baja latencia de red, implemente recursos en la misma AZ.

Regiones y puntos de conexión

Antes de usar una API para invocar a recursos, especifique su región y punto de conexión.

1.3.2 ¿Puedo usar WAF en todas las regiones?

Por lo general, una instancia WAF adquirida en cualquier región puede proteger los servicios web en todas las regiones. Para hacer que una instancia WAF reenvíe el tráfico de su sitio web más rápido, seleccione la región más cercana a sus servicios.

Si usted compra WAF en la región de Beijing, los servicios en otras regiones (por ejemplo, Shanghai) también pueden ser protegidos por WAF. Sin embargo, se necesita más tiempo para

que WAF reenvíe el tráfico de servicios en Shanghai. Por lo tanto, se recomienda comprar dos instancias WAF, una en Beijing y otra en Shanghai, para proteger los servicios en Beijing y Shanghai, respectivamente, mejorando la eficiencia del reenvío.

1.3.3 ¿En qué regiones está disponible WAF?

WAF está disponible en todas las regiones en Huawei Cloud.

AVISO

- Después de comprar una instancia WAF, la región no se puede cambiar. Para cambiar la región, cancele la suscripción de la instancia WAF que ha comprado y compre otra.
- Solo se puede comprar una edición WAF bajo una cuenta en la misma gran región, como CN Este, incluidas las regiones CN Este-Shanghai1 y CN Este-Shanghai2.

Puede comprar instancias WAF en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok
- AP-Singapore
- LA-Sao Paulo1
- LA-Santiago
- LA-Mexico City1
- LA-Mexico City2
- AF-Johannesburg

Por lo general, una instancia WAF adquirida en cualquier región puede proteger los servicios web en todas las regiones. Para hacer que una instancia WAF reenvíe el tráfico de su sitio web más rápido, seleccione la región más cercana a sus servicios.

1.4 Configuración de direcciones IPv6

1.4.1 ¿Qué ediciones de WAF en qué regiones admiten la protección IPv6?

WAF soporta protección IPv6.

- Puede comprar instancias WAF en la nube de platino o profesionales para proteger sus direcciones IPv6.
- La protección IPv6 está disponible en las siguientes regiones:
  - AP-Singapore
- Para instancias de WAF dedicadas, las EIP están vinculadas a los balanceadores de carga configurados para ellos. Si los balanceadores de carga admiten direcciones IPv6, las instancias WAF correspondientes también admiten direcciones IPv6.

1.4.2 ¿Cómo puedo comprobar si la dirección IP del servidor de origen configurada en WAF es una dirección IPv6?

Antes de realizar esta operación, asegúrese de que se ha agregado un nombre de dominio a WAF y que el nombre de dominio se ha conectado a WAF.

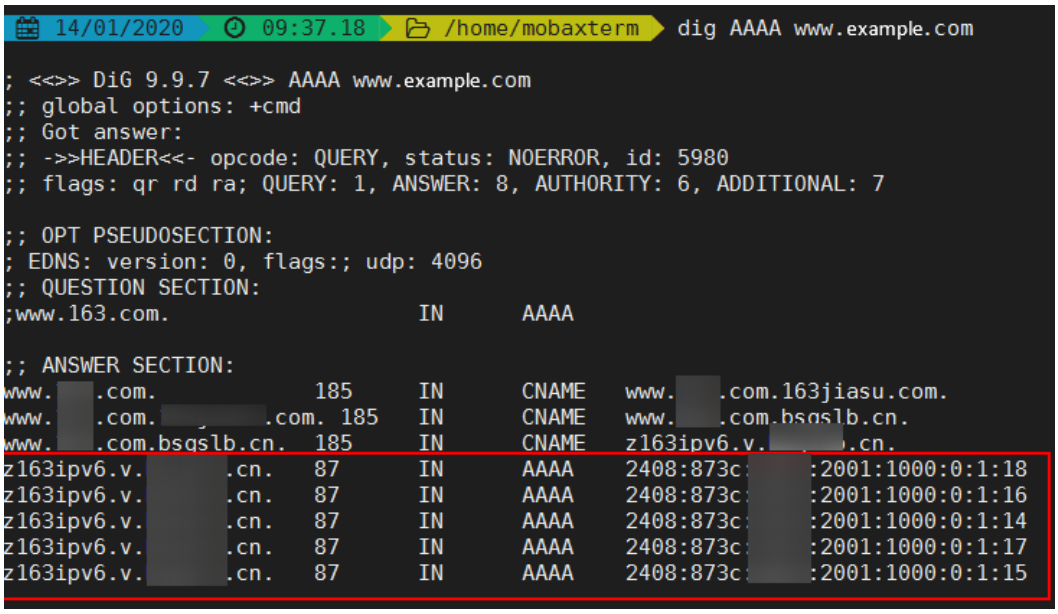
Si se ha agregado un nombre de dominio *www.example.com* puede utilizar el siguiente método para comprobar si la dirección IP del servidor de origen configurada es una dirección IPv6:

Paso 1 Abra la herramienta de línea de comandos de cmd en el sistema operativo de Windows.

Paso 2 Ejecute el comando **dig AAAA www.example.com**.

Si el resultado del comando contiene una dirección IPv6, la dirección IP del servidor de origen configurada es una dirección IPv6.

Figura 1-6 Resultado de la prueba



----Fin

1.4.3 ¿Puedo configurar la dirección del servidor de origen en una dirección IPv6 en WAF?

Sí. La dirección del servidor de origen configurada en WAF puede ser una dirección IPv4 o IPv6. Si ha configurado una dirección IPv4, cámbiela a una dirección IPv6 del servidor de origen en el momento que desee.

WAF soporta el modo de doble pila IPv6/IPv4 y el mecanismo NAT64. Los detalles son los siguientes:

AVISO

Solo las ediciones profesional y platino son compatibles con la protección IPv6.

1.4.4 ¿Cómo reenvía WAF el tráfico a un servidor de origen IPv6?

Si la dirección del servidor de origen es una dirección IPv6, WAF accede al servidor de origen a través de la dirección IPv6. WAF agrega resolución de direcciones IPv6 en conjuntos de registros de CNAME de forma predeterminada. Las solicitudes de acceso IPv6 se reenvían primero a WAF. WAF detecta y filtra el tráfico de ataques maliciosos y devuelve el tráfico normal al servidor de origen para garantizar que el servidor de origen sea seguro, estable y esté disponible.

WAF soporta el modo de doble pila IPv6/IPv4 y el mecanismo NAT64. Los detalles son los siguientes:

AVISO

Solo las ediciones profesional y platino son compatibles con la protección IPv6.

1.5 Enterprise Project

1.5.1 ¿Puedo usar WAF en proyectos empresariales?

Eso depende de qué modo se despliega su instancia de WAF. Los detalles son los siguientes:

- Modo en la nube

  Puede utilizar su WAF en la nube para diferentes proyectos empresariales.
- Modo dedicado

  Si su instancia WAF dedicada puede comunicarse con la VPC a la que pertenecen sus servidores de origen, la instancia se puede utilizar en todos los proyectos empresariales. De lo contrario, el WAF dedicado que adquiere en un determinado proyecto de empresa no se puede utilizar para otros proyectos de empresa.

  NOTA

  Para la instancia WAF dedicada que no puede comunicarse con la VPC a la que pertenecen sus servidores de origen, si aún desea usarla para otros proyectos de empresa, vaya a la página **Proyecto empresarial Management** y mueva la instancia WAF al proyecto de empresa de destino. A continuación, puede utilizar o actualizar la instancia WAF dedicada en el proyecto de empresa.

1.5.2 ¿Puedo utilizar una instancia WAF en un proyecto de empresa específico para otros proyectos empresariales?

Sí, pero necesita migrar la instancia WAF al proyecto de empresa que desee. Para ello, **habilite el Centro de empresa** y gestione sus instancias WAF por proyecto empresarial.

- Modo en la nube

  Si selecciona un proyecto de empresa específico durante la compra o actualización de la instancia WAF, la instancia WAF no se puede utilizar directamente para otros proyectos empresariales.
- Modo dedicado

Una instancia de WAF dedicada en un proyecto empresarial específico no se puede usar directamente para otros proyectos empresariales. Mientras tanto, puede migrar la instancia WAF al proyecto de empresa que desee en la página **Enterprise Project Management** y, a continuación, usar la instancia WAF.

2 Compra de WAF

2.1 ¿Cuáles son las diferencias entre los permisos de una cuenta y los de usuarios de IAM?

Los recursos de una cuenta están aislados de los de usuarios de IAM

Los nombres de dominio agregados por un usuario de IAM pueden ser vistos por la cuenta que crea el usuario de IAM, pero los nombres de dominio agregados por una cuenta no pueden ser vistos por los usuarios de IAM creados con la cuenta.

Para obtener más información sobre los permisos de la cuenta WAF, consulte **Gestión de permisos**.

2.2 ¿Puedo compartir mi WAF con varias cuentas?

WAF no puede ser compartido por varias cuentas. Cada cuenta necesita comprar individualmente una instancia de WAF. Sin embargo, una instancia WAF puede ser compartida por varios usuarios de IAM.

Compartir WAF entre varios usuarios de IAM

Supongamos que ha creado una cuenta, *domain1*, al registrarse en Huawei Cloud, y que ha utilizado *domain1* para crear dos usuarios de IAM, *sub-user1a* y *sub-user1b*, en IAM. Si ha concedido permisos WAF a *sub-user1b*, *sub-user1b* puede utilizar el servicio WAF de *sub-user1a*.

Para obtener más información sobre la concesión de permisos, consulte **Creación de un grupo de usuarios y concesión de permisos**.

2.3 Diferencias entre las ediciones de WAF

WAF ofrece ediciones estándar, profesionales, platino, así como dedicadas (modo dedicado) para usted.

Para obtener más información sobre las características de cada edición, consulte **Diferencia de edición**.

2.4 ¿Cómo calcula WAF el uso de cuotas de nombres de dominio?

El número de nombres de dominio protegidos por WAF se calcula de la siguiente manera:

- El número de dominios es el número total de nombres de dominio de nivel superior (por ejemplo, example.com), nombres de dominio únicos/dominios de segundo nivel (por ejemplo, nombres de dominio www.example.com), y carácter comodín (por ejemplo, *.ejemplo.com). Por ejemplo, una instancia WAF estándar (anteriormente edición profesional) puede proteger 10 nombres de dominio. Por lo tanto, puede agregarle 10 nombres de dominio individuales o nombres de dominio carácter carácter comodín, o agregarle un nombre de dominio de nivel superior y nueve nombres de dominio de subdominio o nombres de dominio carácter comodín relacionados con el nombre de dominio de nivel superior.
- Si un nombre de dominio se asigna a puertos diferentes, se considera que cada puerto representa un nombre de dominio diferente. Por ejemplo, **www.example.com:8080** y **www.example.com:8081** se cuentan para su cuota como dos nombres de dominio distintos.

Para obtener más información, consulte **Diferencias de edición**.

3 Ancho de banda de servicio/ Especificaciones

3.1 Cambio de las especificaciones de instancia WAF

3.1.1 ¿Cómo puedo cambiar la edición de instancia WAF a una más baja y reducir el número de paquetes?

WAF proporciona WAF en la nube de estándar, profesional y platino. Puede reducir el número de nombres de dominio, ancho de banda y paquetes de expansión de reglas que ha comprado. Para cambiar la edición WAF actual a una inferior o reducir las especificaciones de la edición WAF, haga clic en **Change** en la esquina superior derecha de la página. En la página **Change WAF Specifications** mostrada, cambie las especificaciones.

- Para cambiar la edición WAF: En la fila **Edition**, haga clic en **Edition change** en la columna **Details**. En el panel de **Change Edition** que se muestra, seleccione una edición y haga clic en **OK**.
- Para cambiar paquetes de expansión: en la columna **Details** de las filas **Domain Name Quota**, **Bandwidth Quota** y **Rule Quota** aumente o disminuya el número de paquetes de expansión, respectivamente.

⚠ ATENCIÓN

- No se pueden cambiar las especificaciones de una instancia WAF caducada. Para ello, renueve primero la instancia WAF.
- Solo se pueden cancelar la suscripción a los paquetes de expansión no utilizados.

- Para obtener más información sobre las especificaciones, consulte **Diferencias de edición**.
- Para obtener más información sobre la cancelación de la suscripción, consulte **¿Cómo puedo cancelar mi suscripción a WAF?**

- Para obtener más información sobre las recompras, consulte **¿Puedo conservar las configuraciones originales cuando cancelo la suscripción de una instancia WAF y luego compro otra?**

3.1.2 ¿Puedo agregar más reglas de protección?

WAF ofrece ediciones estándar, profesionales y platino para usted. Para obtener más información, consulte **Diferencias de ediciones**. Si la edición que está utilizando no puede cumplir con sus requisitos de servicio, puede actualizarla.

3.1.3 ¿Cómo puedo aumentar el ancho de banda del servicio WAF?

Si el tráfico normal de su sitio web excede el límite de ancho de banda ofrecido por la edición que seleccione, el reenvío de tráfico del sitio web puede verse afectado negativamente.

Por ejemplo, pueden producirse limitaciones de tráfico y pérdidas de paquetes aleatorias. Es posible que los servicios de su sitio web no estén disponibles, estén congelados o respondan muy lentamente.

NOTA

Si se excede el límite de ancho de banda del servicio WAF, WAF no envía notificaciones de alarma. Si se excede el límite de QPS admitido por la edición WAF que está utilizando, WAF seguirá enviando notificaciones de alarma una vez que detecte ataques en su sitio web. Para obtener más información, consulte **Habilitación de notificación de alarma**.

En este caso, actualice su edición o compre paquetes de expansión de ancho de banda adicionales.

Para obtener más información sobre cómo actualizar la edición, consulte **Actualizar la edición**.

3.1.4 ¿Cuáles son los impactos cuando el QPS supera la tasa máxima permitida?

Si el pico de tráfico de su sitio web excede las especificaciones de QPS máximo que está utilizando, WAF dejará de comprobar el tráfico y lo reenviará directamente al servidor de origen. No hay protección para su sitio web o aplicaciones.

Tabla 3-1 enumera las especificaciones QPS admitidas por cada edición WAF.

Tabla 3-1 Especificaciones de QPS soportadas por WAF

Edición	Tasa máxima de solicitudes de servicio normales	Tasa máxima de defensa de ataque CC
Standard	2,000 QPS	100,000 QPS
Professional	5,000 QPS	300,000 QPS
Platinum	10,000 QPS	1,000,000 QPS
Dedicated mode	10,000 QPS	500,000 QPS

Para obtener más información, consulte **Diferencias de edición**.

3.1.5 ¿Puedo cambiar las especificaciones WAF durante la renovación?

No. Puede renovar su instancia WAF en la nube, pero no puede cambiar sus especificaciones durante la renovación. Puede renovar sus suscripciones a la edición WAF actual, dominio adquirido, ancho de banda y/o paquetes de expansión de reglas.

Puede cambiar las especificaciones de su instancia WAF de la siguiente manera antes de renovarla:

- Actualizar las especificaciones de WAF
  - Actualizar su instancia WAF de la edición actual a una edición superior.
  - Aumentar la cantidad de nombres de dominio, ancho de banda o paquetes de expansión de reglas.

  Para obtener más información, consulte **Actualización de edición y especificaciones de WAF en la nube**.
- Especificaciones WAF más bajas
  - Cancelar la suscripción de su edición de instancia actual y suscribirse a una edición inferior
  - Reducir la cantidad de paquetes de expansión de reglas, ancho de banda o nombre de dominio.

AVISO

Asegúrese de que la nueva instancia WAF está en la misma región que la instancia WAF original. De lo contrario, debe agregar manualmente el dominio protegido por la instancia WAF original a la nueva instancia WAF y configurar reglas de protección para el dominio según los requisitos de protección. Para más detalles, consulte **¿Puedo conservar las configuraciones originales cuando cancelo la suscripción de una instancia WAF y luego compro otra?**

3.1.6 ¿Cuántas reglas puedo agregar a una instancia WAF?

El número de reglas que puede agregar varía en función de los tipos de protección en la edición WAF que esté utilizando. **Tabla 3-2** enumera las especificaciones incluidas en las diferentes ediciones.

Tabla 3-2 Escalamiento de servicio aplicable

Escalamiento de servicio	Estándar (anteriormente edición profesional)	Profesional (anteriormente edición empresarial)	Platino (anteriormente edición premium)	Pago por uso	Modo dedicado
Tasa máxima de solicitudes de servicio normales	● 2,000 QPS ● Conexiones WAF a servidor: 6,000 por nombre de dominio	● Solicitudes de servicio: 5000 QPS ● Conexiones WAF a servidor: 6,000 por nombre de dominio	● Solicitudes de servicio: 10,000 QPS ● Conexiones WAF a servidor: 6,000 por nombre de dominio	N/A	● Especificaciones: WI-500. Rendimiento: – Rendimiento: 500 Mbit/s; QPS: 10,000 – Conexiones WAF-a-servidor soportadas: 60,000 por instancia o 5,000 por dominio ● Especificaciones: WI-100. Rendimiento: – Rendimiento: 100 Mbit/s; QPS: 2,000 – Conexiones WAF-a-servidor soportadas: 60,000 por instancia o 5,000 por dominio

Escalamiento de servicio	Estándar (anteriormente edición profesional)	Profesional (anteriormente edición empresarial)	Platino (anteriormente edición premium)	Pago por uso	Modo dedicado
Umbral de ancho de banda del servicio (el servidor de origen se implementa en la nube)	100 Mbit/s	200 Mbit/s	300 Mbit/s	N/A	● Especificaciones: WI-500. Rendimiento: – Rendimiento: 500 Mbit/s; QPS: 10,000 – Conexiones WAF-a-servidor soportadas: 60,000 por instancia o 5,000 por dominio ● Especificaciones: WI-100. Rendimiento: – Rendimiento: 100 Mbit/s; QPS: 2,000 – Conexiones WAF-a-servidor soportadas: 60,000 por instancia o 5,000 por dominio
Umbral de ancho de banda del servicio (el servidor de origen no se implementa en Huawei Cloud)	30 Mbit/s	50 Mbits/s	100 Mbit/s	N/A	N/A

Escalamiento de servicio	Estándar (anteriormente edición profesional)	Profesional (anteriormente edición empresarial)	Platino (anteriormente edición premium)	Pago por uso	Modo dedicado
Cantidad de dominios	10 (Soporta un nombre de dominio de nivel superior.)	50 (Soporta cinco nombres de dominio de nivel superior.)	80 (Soporta ocho nombres de dominio de nivel superior.)	30 (Soporta tres nombres de dominio de nivel superior.)	2,000 (Soporta 2000 nombres de dominio de nivel superior.)
Cantidad de direcciones IP de retorno a origen (el número de direcciones IP WAF back-to-source que pueden ser permitidas por un nombre de dominio protegido)	20	50	80	20	N/A
Tasa máxima de defensa de ataque CC	100,000 QPS	300,000 QPS	1,000,000 QPS	N/A	500,000 QPS
Número de reglas de defensa contra ataques CC	20	50	100	200	100
Número de normas de protección precisas	20	50	100	200	100
Número de reglas del cuadro de referencia	N/A	50	100	200	100

Escalamiento de servicio	Estándar (anteriormente edición profesional)	Profesional (anteriormente edición empresarial)	Platino (anteriormente edición premium)	Pago por uso	Modo dedicado
Número de reglas de la lista negra o de la lista blanca de direcciones IP	20	100	1,000	200	1,000
Número de reglas de control de acceso de geolocalización	20	50	100	200	100
Número de reglas de protección contra manipulaciones web	20	50	100	200	100
Número de normas de prevención de fugas de información	N/A	50	100	200	100
Número de reglas de enmascaramiento de falsas alarmas	1,000	1,000	1,000	2,000	1,000
Número de reglas de enmascaramiento de datos	20	50	100	200	100

3.1.7 ¿Dónde y cuándo puedo comprar un paquete de expansión de dominio, ancho de banda o regla?

Puede comprar paquetes de expansión de dominios, ancho de banda y reglas al comprar o actualizar una instancia WAF en la nube en edición estándar, profesional o platino.

Para obtener más información, consulte **Paquete de expansión de nombres de dominio**, **Paquete de expansión de ancho de banda**, y **Paquete de expansión de regla**.

Comprar paquetes de expansión mientras compra WAF en la nube

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 Si es usuario por primera vez, haga clic en **Buy WAF Now**.

NOTA

Si no es usuario por primera vez, haga clic en **Buy WAF** en la esquina superior derecha.

Paso 5 En la página **Buy Web Application Firewall**, especifique **Region** y seleccione una edición.

Paso 6 Especifique el número de paquetes de expansión de dominio, ancho de banda y reglas.

Paso 7 Establezca **Required Duration** y pague el pedido.

NOTA

Una instancia WAF y sus paquetes de expansión tienen la misma duración requerida.

----Fin

Compra de paquetes de expansión durante la actualización

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda y elija **Web Application Firewall** en **Security**.

Paso 4 En la esquina superior derecha, haga clic en **Change**.

Paso 5 En la columna **Details** de las filas **Domain Name Quota**, **Bandwidth Quota** y **Rule Quota** aumente o disminuya el número de paquetes, respectivamente.

Paso 6 En la esquina inferior derecha de la página, haga clic en **Next** y paga el pedido.

NOTA

Una instancia WAF y sus paquetes de expansión tienen la misma duración requerida.

----Fin

3.2 Acerca del ancho de banda de servicio

3.2.1 ¿Cómo selecciono el ancho de banda del servicio al comprar WAF?

WAF limita solamente el ancho de banda del servicio. No hay limitaciones en el ancho de banda de protección o ancho de banda compartido. Para obtener más información sobre el ancho de banda del servicio, consulte **Diferencias de edición**.

¿Qué es el ancho de banda de servicio?

El ancho de banda de servicio en WAF es la cantidad de tráfico (unidad: Mbit/s) que una instancia WAF puede proteger.

Antes de comprar WAF, confirme el tráfico máximo total de entrada y salida de los sitios web que están protegidos por WAF. Asegúrese de que el ancho de banda de la edición WAF que seleccione es mayor que el tráfico máximo total entrante o el tráfico máximo total saliente, el que sea mayor.

¿Qué es el tráfico?

El tráfico de ataques debe eliminarse en sus estimaciones. Por ejemplo, si se accede a su sitio web normalmente, WAF enruta el tráfico de vuelta al ECS de origen, pero si su sitio web está bajo ataque, WAF bloquea y filtra el tráfico ilegítimo, y enruta solo el tráfico legítimo de vuelta al ECS de origen. El tráfico entrante y saliente del ECS de origen que ve en la consola de ECS es el tráfico normal. Si hay varios ECS, recopile estadísticas sobre el tráfico normal de todos los ECS. Por ejemplo, si tiene seis sitios y el ancho de banda máximo de salida de cada sitio no supera los 50 Mbit/s, entonces el ancho de banda máximo total no supera los 300 Mbit/s. En este caso, puede comprar la edición WAF platino (anteriormente edición premium).

NOTA

En general, el tráfico saliente es mayor que el tráfico entrante.

¿Qué sucede si el tráfico del sitio web supera el límite de ancho de banda del servicio?

Si el tráfico normal de su sitio web excede el límite de ancho de banda de servicio de la edición que seleccionó, el tráfico puede estar limitado o puede haber pérdida de paquetes aleatoria. Como resultado, los servicios no están disponibles, se congelan o se retrasan durante un cierto período de tiempo.

En este caso, actualice su edición o compre más paquetes de expansión de ancho de banda.

Un paquete de expansión de ancho de banda puede proteger hasta 20 Mbit/s de tráfico para aplicaciones en Huawei Cloud o 50 Mbit/s para aplicaciones que no estén en Huawei Cloud; o 1,000 Consultas por Segundo (QPS). Cada solicitud de HTTP Get es una consulta.

Para obtener más información sobre los paquetes de expansión de ancho de banda, consulte **Paquetes de expansión de ancho de banda**.

3.2.2 ¿Dónde puedo consultar el uso del ancho de banda del servicio WAF actual?

Puede consultar el uso de ancho de banda entrante de la dirección IP del servidor de origen en el servidor de origen.

3.2.3 ¿El ancho de banda del servicio se calcula en función del tráfico entrante o saliente?

El ancho de banda de servicio en WAF es la cantidad de tráfico (unidad: Mbit/s) que una instancia WAF puede proteger.

Antes de comprar WAF, confirme el tráfico máximo total de entrada y salida de los sitios web que están protegidos por WAF. Asegúrese de que el ancho de banda de la edición WAF que seleccione es mayor que el tráfico máximo total entrante o el tráfico máximo total saliente, el que sea mayor.

El tráfico de ataques debe eliminarse en sus estimaciones. Por ejemplo, si se accede a su sitio web normalmente, WAF enruta el tráfico de vuelta al ECS de origen, pero si su sitio web está bajo ataque, WAF bloquea y filtra el tráfico ilegítimo, y enruta solo el tráfico legítimo de vuelta al ECS de origen. El tráfico entrante y saliente del ECS de origen que ve en la consola de ECS es el tráfico normal. Si hay varios ECS, recopile estadísticas sobre el tráfico normal de todos los ECS. Por ejemplo, si tiene seis sitios y el ancho de banda máximo de salida de cada sitio no supera los 50 Mbit/s, entonces el ancho de banda máximo total no supera los 300 Mbit/s. En este caso, puede comprar la edición WAF platino (anteriormente edición premium).

NOTA

En general, el tráfico saliente es mayor que el tráfico entrante.

Para obtener más información sobre el ancho de banda, consulte **Paquete de expansión de ancho de banda**.

3.2.4 ¿Tiene WAF un límite en el ancho de banda de protección o el ancho de banda compartido?

WAF no limita el ancho de banda de protección o el ancho de banda compartido. WAF limita el ancho de banda del servicio y el QPS.

El ancho de banda de servicio en WAF es la cantidad de tráfico (unidad: Mbit/s) que una instancia WAF puede proteger.

Antes de comprar WAF, confirme el tráfico máximo total de entrada y salida de los sitios web que están protegidos por WAF. Asegúrese de que el ancho de banda de la edición WAF que seleccione es mayor que el tráfico máximo total entrante o el tráfico máximo total saliente, el que sea mayor.

Para obtener más información, consulte **Diferencias de edición**.

3.2.5 ¿Dónde puedo ver los anchos de banda entrante y saliente de un sitio web protegido?

En la página **Dashboard**, puede ver el uso del ancho de banda sobre el sitio web o la instancia protegida. El procedimiento es el siguiente:

AVISO

Actualmente, puede ver estadísticas de ancho de banda en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

NOTA

Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable de **Enterprise Project** y ver los datos de las estadísticas de seguridad del proyecto.

Paso 4 En la lista desplegable del sitio web o de la instancia, seleccione el sitio web o la instancia que desea comprobar y seleccione un intervalo de tiempo (ayer, hoy, últimos 3 días, últimos 7 días o últimos 30 días).

Paso 5 En el área **Security Event Statistics**, seleccione la pestaña **Bytes Sent/Received** y vea los anchos de banda entrante y saliente.

----Fin

4 Facturación, renovación y recompra después de darse de baja

4.1 ¿Puedo cambiar entre pagos anuales/mensuales y pagos por uso para WAF?

Para las instancias de WAF en la nube, se admite el cambio entre pagos anuales/mensuales y pagos por uso.

AVISO

Para comprar instancias de WAF de pago por uso, **envíe un ticket de servicio** para habilitar el servicio.

Cambio de pago por uso a anual/mensual

AVISO

Para una instancia de WAF en la nube facturada sobre una base de pago por uso, puede deshabilitar el modo de facturación anual/mensual y, a continuación, habilitar una instancia de WAF en el modo de facturación anual/mensual.

- Después de deshabilitar el modo de facturación de pago por uso, la facturación de WAF se detiene. El **Mode** de WAF cambia a **Suspended**. En esta situación, WAF reenvía el tráfico de tu sitio web sin detectarlo.
- Para evitar cargas de trabajo de configuración repetidas, se recomienda que las instancias WAF en la nube nuevas y originales estén bajo el mismo proyecto en la misma región.

El modo de facturación de pago por uso es un método de pago pospago. Para una instancia en la nube de pago por uso, se le factura el número de nombres de dominio agregados, el número de reglas personalizadas y el número de solicitudes que utiliza en todo el período de facturación.

Si quiere usar WAF durante mucho tiempo, cambia su modo de facturación de pago por uso a anual/mensual para reducir los costos. Realice los siguientes pasos:

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 Deshabilitar la instancia WAF facturada sobre una base de pago por uso.

1. En el panel de navegación de la izquierda, elija **Instance Management** > **Product Details**.
2. Haga clic en **Disable Pay-per-Use Billing**.
3. En el cuadro de diálogo que se muestra, seleccione. "The involved domain names have been resolved to corresponding origin servers, or they have been brought offline" y haga clic en **Confirm**.

   El **Mode** de trabajo de la instancia WAF para todos los nombres de dominio en la página de configuración del sitio web cambia a **Suspended**.

Paso 5 Compre una instancia de WAF facturada anualmente/mensualmente.

Para obtener más información, consulte **Compra de una instancia WAF facturada anualmente/mensualmente**.

Paso 6 Habilite la instancia WAF.

1. En el panel de navegación de la izquierda, seleccione **Website Settings**.
2. En la fila que contiene el sitio web deseado, localice la columna **Mode** y haga clic en **Enabled**. A continuación, haga clic en **Confirm** en el cuadro de diálogo mostrado.

   Si la información en **Mode** cambia a **Enabled**, WAF comienza a detectar su sitio web.

----Fin

Cambio de anual/mensual a pago por uso

AVISO

- Para una instancia de WAF en la nube facturada anualmente/mensualmente, después de que caduque o cancele su suscripción, puede habilitar otra instancia de WAF facturada según pago por uso.
- Para evitar cargas de trabajo de configuración repetidas, se recomienda que las instancias WAF nuevas y originales estén bajo el mismo proyecto en la misma región o proyecto.

Anual/Mensual es un modo de facturación prepago en el que se factura una instancia WAF en función de la duración del servicio. Este modo rentable es ideal cuando la duración del uso de la instancia WAF es predecible.

Si necesita un modo de facturación más flexible, en el que su WAF se facturará según el uso, puede cambiar el modo de facturación de anual/mensual a de pago por uso. Antes de hacerlo,

asegúrese de que la suscripción anual/mensual haya caducado o de que se haya cancelado la suscripción de la instancia anual/mensual en la nube. Realice los siguientes pasos:

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 Cancele la suscripción de la instancia anual/mensual de WAF o confirmar que la suscripción anual/mensual ha caducado.

Para ver los detalles sobre la instancia WAF que está utilizando, consulte la información que se muestra en la esquina superior derecha de la página **Dashboard**.

Para obtener más información sobre la cancelación de la suscripción, consulte **¿Cómo puedo cancelar mi suscripción a WAF?**

Paso 5 Habilite una instancia de WAF facturada según el pago por uso.

Para obtener más información, consulte **Compra de una instancia WAF facturada en base a pago por uso**.

Paso 6 Habilite la instancia WAF.

1. En el panel de navegación de la izquierda, seleccione **Website Settings**.
2. En la fila que contiene el sitio web deseado, localice la columna **Mode** y haga clic en **Enabled**. A continuación, haga clic en **Confirm** en el cuadro de diálogo mostrado.

   Si la información en **Mode** cambia a **Enabled**, WAF comienza a detectar su sitio web.

----Fin

4.2 ¿Cómo se factura el WAF?

WAF en la nube se puede facturar de forma anual/mensual (prepago) o de pago por uso (pospago). Las ediciones estándar, profesional y platino se facturan anualmente/mensualmente. Para el WAF en la nube facturado anualmente/mensualmente, el nombre de dominio, el ancho de banda y los paquetes de expansión de reglas se proporcionan a un costo adicional. Se le facturará la instancia WAF y los paquetes de expansión que seleccionó en función del modo de facturación que especificó.

AVISO

Para comprar instancias de WAF de pago por uso, **envíe un ticket de servicio** para habilitar el servicio.

Para obtener más información sobre los precios de WAF, consulte **Detalles de precios**.

For price details, see **Product Pricing Details**.

4.3 ¿Puede WAF continuar protegiendo un nombre de dominio cuando caduca?

Después de que caduque su instancia de WAF en la nube, hay un período de retención.

- Durante este período, WAF solo reenvía el tráfico, pero no lo compara con sus políticas de protección.
- Cuando finalice este período, se borrarán los recursos, es decir, se eliminarán todas las configuraciones de sus nombres de dominio. Durante el período de borrado, los nombres de dominio se apuntan de nuevo a los servidores de origen de forma predeterminada. Sin embargo, es posible que los servicios de sus nombres de dominio no se ejecuten correctamente porque puede haber incoherencias entre los protocolos y puertos configurados.

Para evitar que se produzcan problemas de seguridad, se recomienda renovar la instancia WAF en la nube antes de que expire su período de retención. Si la instancia de WAF en la nube caduca, no afecta a otros servicios.

4.4 ¿Cómo puedo renovar mi instancia WAF?

En este tema se describe cómo renovar la suscripción a una instancia de WAF facturada anualmente/mensualmente cuando está a punto de caducar. Después de la renovación, puede continuar usando su instancia WAF.

Antes de que caduque su suscripción a WAF, el sistema enviará un mensaje SMS o correo electrónico para recordarle que la renueve.

Si no renueva su suscripción antes de que caduque, se aplicará un período de retención.

- Durante este período, WAF solo reenvía el tráfico, pero no lo compara con sus políticas de protección.
- Cuando finalice este período, se borrarán los recursos, es decir, se eliminarán todas las configuraciones de sus nombres de dominio. Durante el período de borrado, los nombres de dominio se apuntan de nuevo a los servidores de origen de forma predeterminada. Sin embargo, es posible que los servicios de sus nombres de dominio no se ejecuten correctamente porque puede haber incoherencias entre los protocolos y puertos configurados.

Para evitar pérdidas innecesarias causadas por problemas de seguridad, renueve su suscripción antes de que expire el período de retención.

NOTA

- Si ha seleccionado **Auto-renew** al comprar WAF, el sistema genera automáticamente un pedido de renovación y renueva su suscripción antes de que caduque.
- Si utiliza una cuenta de miembro, conceda permiso al administrador de BSS para que pueda renovar la suscripción caducada mediante la cuenta de miembro.

Prerrequisitos

- Ha comprado WAF.

- Su instancia en modo cloud ha caducado.

Procedimiento

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

Paso 4 En la esquina superior derecha de la página, seleccione **Billing & Costs** > **Renewal**. Se muestra la página **Renewals**.

Paso 5 En la página de gestión de renovación, complete la renovación.

Para obtener más información, consulte **Reglas de renovación**.

----Fin

4.5 ¿Cómo puedo cancelar mi suscripción a WAF?

En este tema se describe cómo cancelar la suscripción de una instancia de WAF facturada anualmente/mensualmente.

Si desea darse de baja de un WAF dedicado facturado sobre una base de pago por uso, en la consola WAF, elija **Instance Management** > **Dedicated Engine**. A continuación, elimine la instancia WAF dedicada que ya no necesita. La facturación se detiene tras la eliminación.

Si desea darse de baja de una instancia de WAF en la nube facturada sobre una base de pago por uso, en la consola de WAF, elija **Instance Management** > **Product Details**, deshabilite la facturación de pago por uso para la instancia de WAF en la nube.

NOTA

- Si usa una cuenta de miembro, concede permiso al Administrador de BSS para que pueda cancelar la suscripción de WAF usando la cuenta de miembro.
- Si desea darse de baja de una instancia WAF dedicada, **elimínelo**. La facturación se detiene cuando se elimina la instancia.

Prerrequisitos

- Se proporciona un reembolso incondicional de cinco días para las instancias de WAF en la nube. Esto significa que puede obtener un reembolso completo siempre y cuando cancele la suscripción de un WAF en la nube dentro de los 5 días posteriores a la compra.
- Antes de darse de baja de una instancia de WAF en la nube, asegúrese de haber resuelto el nombre de dominio del sitio web protegido a las direcciones IP del servidor de origen, o el sitio web se volverá inalcanzable después de la cancelación de la suscripción.
- Ha habilitado el puerto de servicio en el servidor de origen antes de cancelar la suscripción de un WAF en la nube.

Precauciones

Para reutilizar las configuraciones de una instancia WAF, asegúrese de que la instancia WAF original de la que canceló su suscripción y la nueva instancia WAF que está comprando estén en la misma región. De lo contrario, debe conectar el nombre de dominio a la nueva instancia WAF y configurar de nuevo las reglas de protección. Para obtener más información, consulte **¿Puedo conservar las configuraciones originales cuando cancelo la suscripción de una instancia WAF y luego compro otra?**.

Procedimiento

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 En la parte superior derecha de la página, haga clic en **Billing & Costs** para ir a la página **Billing Center**.

Paso 3 En el panel de navegación de la izquierda, elija **Orders** > **Unsubscriptions and Returns/ Exchanges**.

Paso 4 Complete las operaciones de cancelación de suscripción.

Para obtener más información, consulte **Reglas de cancelación de suscripción**.

----Fin

4.6 ¿Puedo conservar las configuraciones originales cuando cancelo la suscripción de una instancia WAF y luego compro otra?

Para una instancia de WAF facturada anualmente/mensualmente, después de darse de baja de ella, puede habilitar otra instancia de WAF facturada anualmente/mensualmente o de pago por uso.

- Si elige el modo de facturación de pago por uso, las configuraciones de la instancia WAF original se pueden guardar y usar para la instancia WAF recién habilitada.
- Si elige el modo de facturación anual/mensual, las configuraciones de la instancia WAF original se pueden guardar y usar para la instancia WAF recién habilitada solo cuando se encuentren en la misma región. Si no están en la misma región, dichas configuraciones no se guardan.

AVISO

Para comprar instancias de WAF de pago por uso, **envíe un ticket de servicio** para habilitar el servicio.

Instancia de WAF no suscrita e instancia de WAF recién adquirida facturada anual/mensualmente en la misma región

Después de darse de baja de una instancia de WAF, sus configuraciones se conservan durante 24 horas.

Después de darse de baja de WAF, WAF suspende la protección de sus nombres de dominio. Después de comprar WAF de nuevo, solo tiene que cambiar el modo de trabajo WAF del nombre de dominio a **Enabled**. A continuación, WAF comienza a proteger el nombre de dominio basándose en las reglas de protección configuradas en WAF.

- Para obtener más información sobre la cancelación de la suscripción, consulte **¿Cómo puedo cancelar mi suscripción a WAF?**
- Para obtener más información sobre cómo comprar una instancia WAF, consulta **Comprar WAF**.
- Para obtener más información sobre cómo cambiar el modo de trabajo WAF, consulte **Cambiar un modo de trabajo**.

AVISO

Para conservar las configuraciones de la instancia de WAF original después de darse de baja, compre una nueva instancia de WAF en un plazo de 24 horas.

Instancia de WAF no suscrita e instancia de WAF recién adquirida facturada anual/mensualmente no en la misma región

Después de darse de baja de una instancia WAF, sus configuraciones no se guardan.

Después de comprar una instancia WAF de nuevo, agregue el nombre de dominio a la nueva instancia WAF y configure de nuevo las reglas de protección.

- Para obtener más información sobre la cancelación de la suscripción, consulte **¿Cómo puedo cancelar mi suscripción a WAF?**
- Para obtener más información acerca de cómo empezar, consulta **Pasos iniciales**.

4.7 ¿Cómo sé cuándo caduca mi WAF?

Después de comprar una instancia WAF, su tiempo de caducidad se mostrará en la esquina superior derecha de cada página WAF. También puede habilitar las notificaciones de caducidad. Cuando el servicio está a punto de caducar, el sistema envía una notificación a los destinatarios que configura.

5 Configuración de acceso al nombre de dominio del sitio web

5.1 Nombre de dominio y configuración de puerto

5.1.1 ¿Cómo agrego un nombre de dominio/dirección IP a WAF?

Después de conectar un nombre de dominio o dirección IP del sitio web que desea proteger a WAF, WAF funciona como un proxy inverso entre el cliente y el servidor. La dirección IP real del servidor está oculta y solo la dirección IP de WAF es visible para los visitantes de la web.

WAF ofrece las instancias en la nube y dedicadas para proteger sus sitios web. Puede agregar nombres de dominio o direcciones IP a WAF. Antes de comenzar, familiarícese con las siguientes diferencias:

- Modo en la nube: protege sus aplicaciones web que tienen nombre de dominio y se implementan en Huawei Cloud, cualquier otra nube o centros de datos locales.
- Modo dedicado: protege las aplicaciones web desplegadas en Huawei Cloud y accesibles a través de nombres de dominio o direcciones IP.

AVISO

- Puede introducir un nombre de dominio único de varios niveles (por ejemplo, nombre de dominio de nivel superior example.com o nombre de dominio de segundo nivel www.example.com) o un nombre de dominio de comodín (*.ejemplo.com). Los procesos de conexión de nombres de dominio a diferentes tipos de instancia WAF son los mismos.
  - Si la dirección IP del servidor de cada nombre de subdominio es la misma, introduzca un nombre de dominio de comodín. Por ejemplo, si los nombres de subdominio ***a.example.com***, ***b.example.com*** y ***c.example.com*** tienen la misma dirección IP del servidor, puede agregar el nombre de dominio de comodín ****.example.com*** a WAF para proteger los tres.
  - Si las direcciones IP del servidor de los nombres de subdominio son diferentes, agregue nombres de subdominio como nombres de dominio únicos uno por uno.
- No se puede agregar un nombre de dominio al modo en la nube de WAF repetidamente.

  Cada combinación de un nombre de dominio y un puerto no estándar se cuenta para la cuota de nombres de dominio de la edición WAF que está utilizando. Por ejemplo, www.example.com:8080 y www.example.com:8081 usan dos nombres de dominio de la cuota. Si desea proteger los servicios web a través de varios puertos con el mismo nombre de dominio, agregue el nombre de dominio y cada puerto a WAF.

Para obtener más información, consulte **Diferencias de edición**.

La siguiente figura muestra el proceso de conectar un sitio web a WAF en cada modo.

Figura 5-1 Proceso de conexión de un sitio web a WAF

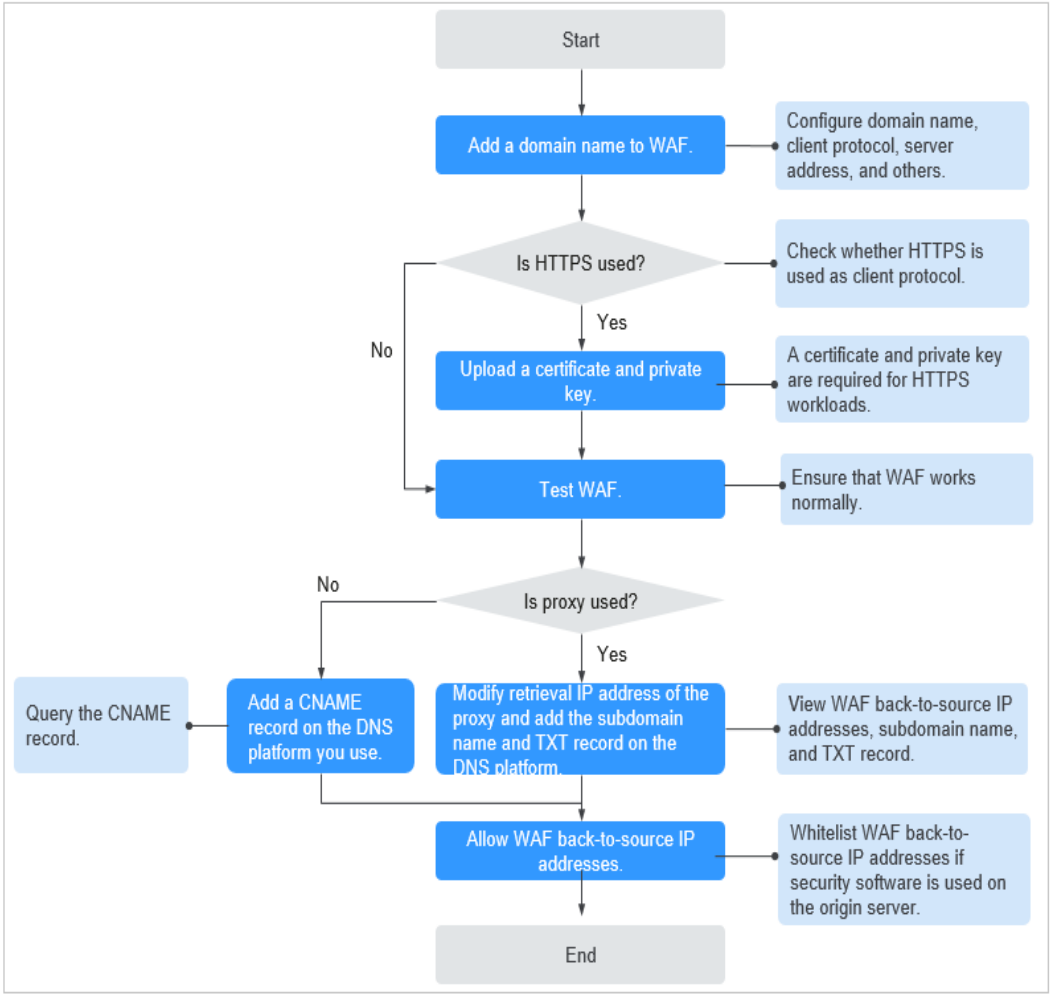
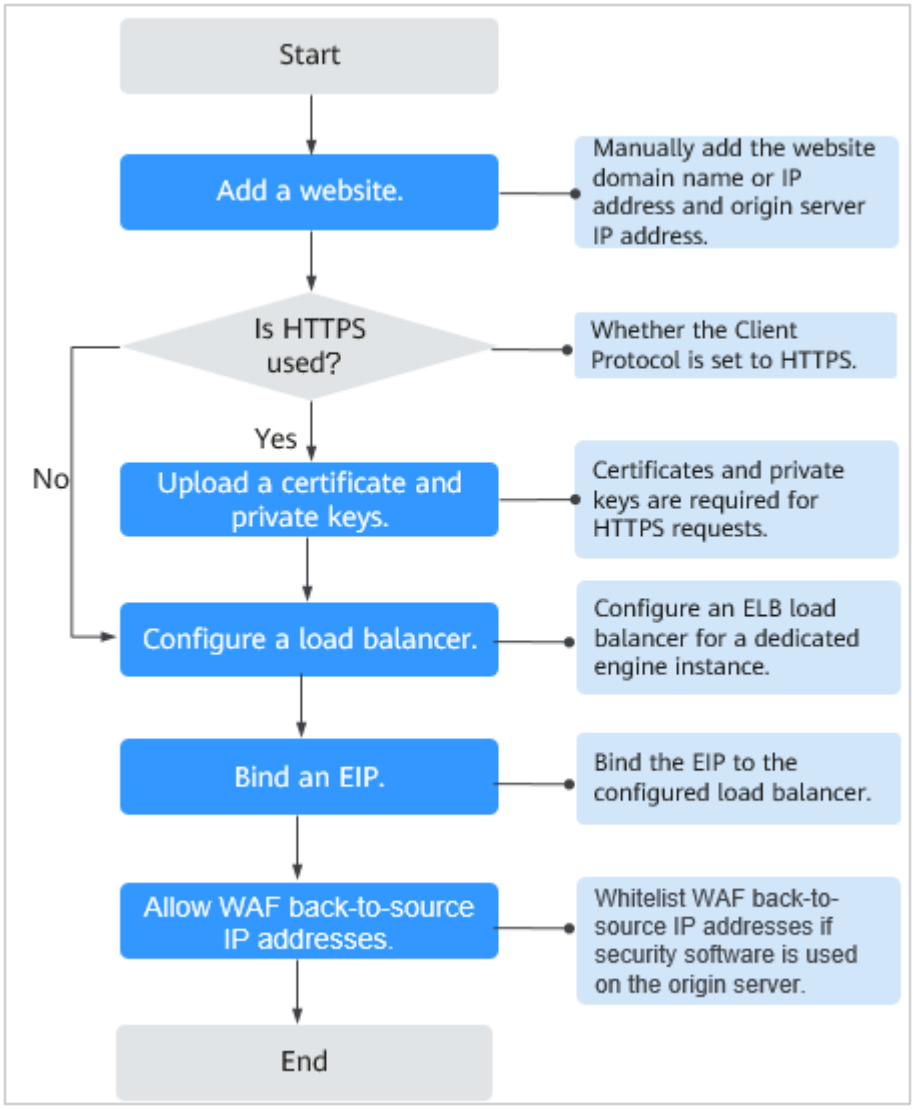


Figura 5-2 Proceso de conexión de un sitio web a una instancia WAF dedicada



Para obtener más información, consulte **Adición de un nombre de dominio a WAF**.

- Si **Access Status** para un sitio web protegido es **Inaccessible**, rectifique la falta haciendo referencia a **¿Por qué es inaccesible mi nombre de dominio o dirección IP?**
- Si su sitio web se vuelve inaccesible después de estar conectado a WAF, rectifique el problema consultando **¿Cómo soluciono los errores 404/502/504?**

5.1.2 ¿Qué puertos no estándar admite WAF?

WAF puede proteger aplicaciones web que utilizan WebSocket/WebSockets (activado por defecto), HTTP o HTTPS a través de los puertos estándar 80 y 443 o puertos no estándar. Los puertos no estándar compatibles con WAF varían dependiendo de la edición WAF que esté utilizando.

Cada combinación de un nombre de dominio y un puerto no estándar se cuenta para la cuota de nombres de dominio de la edición WAF que está utilizando. Por ejemplo, www.example.com:8080 y www.example.com:8081 usan dos nombres de dominio de la

cuota. Si desea proteger los servicios web a través de varios puertos con el mismo nombre de dominio, agregue el nombre de dominio y cada puerto a WAF.

Puertos soportados por WAF

WAF proporciona ediciones estándar, profesional y platino. **Tabla 5-1** lista los puertos soportados por las ediciones WAF.

Tabla 5-1 Puertos soportados por WAF

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
Estándar	Puertos estándares	80	443	Ilimitado
	Puertos no estándar (89 en total)	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 7009, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8999, and 9001	4443, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8712, 8803, 8804, 8805, 8843, 9443, 8553, 8663, 9553, 9663, 18000, 18110, 18381, 18443, 18980, 19000, and 28443	Ilimitado
Profesional	Puertos estándares	80	443	Ilimitado

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
	Puertos no estándar (266 en total)	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 1000, 1090, 1135, 1139, 1688, 3128, 3333, 3501, 3601, 4444, 5000, 5080, 55222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 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, 7080, 77081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9021, 9023, 9027, 9037, 9050, 9077, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 9770, 10000, 10001, 10080, 11000, 12601, 13000, 14000, 18080, 18180, 18280, 19101, 19501, 21028, 23333, 27777, 28080, 30002, 30086, 33332, 33334,	447, 882, 1818, 4006, 4430, 4443, 5100, 5443, 6443, 7072, 7073, 7443, 8033, 8043, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8842, 8843, 9053, 9090, 9443, 9553, 9663, 9999, 10300, 10301, 11001, 11003, 13001, 13003, 13080, 14003, 14443, 18000, 18010, 18110, 18381, 18443, 18980, 19000, 20000, 28443, and 60009	Ilimitado

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
		33702, 40010, 48299, 48800, 52725, 52726, 60008, and 60010		
Platino	Puertos estándares	80	443	Ilimitado

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
	Puertos no estándar (253 en total)	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 1000, 1090, 1135, 1139, 1688, 3128, 3333, 3501, 3601, 4444, 5000, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 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, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8006, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8888, 8889, 8899, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9021, 9023, 9027, 9037, 9050, 9077, 9080, 9081, 9082, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 10000, 10001, 10080, 11000, 12601, 13000, 14000, 18080, 18180, 18280, 23333, 27777, 28080, 30086, 33702, 48299, and 48800	447, 882, 1818, 4006, 4430, 4443, 5443, 6443, 7072, 7073, 7443, 8033, 8043, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8842, 8843, 8848, 8910, 8920, 8950, 9053, 9090, 9182, 9184, 9190, 9443, 9553, 9663, 9999, 10300, 10301, 11001, 11003, 13001, 13003, 13080, 14003, 18000, 18010, 18110, 18381, 18443, 18980, 19000, 28443, and 60009	Ilimitado
Motor dedicado	Puertos estándares	80	443	Ilimitado

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
	Puertos no estándar (206 en total)	81, 82, 83, 84, 86, 87, 88, 89, 97, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 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, 7080, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9945, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 10000, 10001, 10080, 12601, 19101, 19501, 19998, 21028, 28080, 30002, 33332, 33334, 33702, 40010, 48800, 52725, 52726, 60008, and 60010	4443, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8843, 9443, 9553, 9663, 9999, 18000, 18010, 18110, 18381, 18443, 18980, 19000, and 28443	Ilimitado

5.1.3 ¿Cómo uso una instancia WAF dedicada para proteger los puertos no estándar que no son compatibles con la instancia dedicada?

Para utilizar una instancia WAF dedicada para proteger un puerto no estándar que no es compatible con la instancia dedicada, configure un balanceador de carga ELB para distribuir el tráfico a cualquier puerto no estándar que es compatible con la instancia dedicada. Para ver los puertos no estándar compatibles, consulte **¿Qué puertos no estándar admite WAF?**

Por ejemplo, un cliente envía solicitudes a través de HTTP a la instancia WAF dedicada y protege el sitio web cuyo nombre de dominio es www.example.com:1234. La instancia dedicada no puede proteger el puerto no estándar 1234. En este caso, puede configurar un balanceador de carga para distribuir el tráfico a cualquier otro puerto no estándar (por ejemplo, el puerto 81) que pueda ser protegido por la instancia dedicada. De esta manera, el tráfico designado para el puerto no estándar 1234 será verificado por WAF.

AVISO

Para garantizar que la configuración surta efecto, se recomienda un nombre de dominio comodín correspondiente al nombre de dominio protegido para el campo **Domain Name**. Por ejemplo, si desea proteger www.example.com:1234, establezca **Domain Name** en ***.example.com**.

Realice los siguientes pasos:

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Agregue el nombre de dominio del sitio web que desea proteger en la consola WAF.

1. Haga clic en ☰ en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.
2. En el panel de navegación de la izquierda, seleccione **Website Settings**.
3. En la esquina superior izquierda de la lista de sitios web, haz clic en **Add Website**. En la página mostrada, seleccione **Dedicated mode**, introduzca el nombre de dominio comodín ***.example.com** correspondiente a **www.example.com:1234** en el cuadro de texto **Domain Name** y seleccione un puerto (por ejemplo, 81) en la lista desplegable **Protected Port**.
4. Seleccione **Yes** para **Proxy** y haga clic en **OK**.
5. Cierre el cuadro de diálogo que aparece.

   Puede ver los sitios web agregados en la lista de sitios web protegidos.

Paso 3 Configure un balanceador de carga en la consola ELB.

1. Haga clic en ☰ en la esquina superior izquierda de la página y elija **Elastic Load Balance** en **Network** para ir a la página **Load Balancers**.
2. Haga clic en el nombre del balanceador de carga que desee en la columna **Name** para ir a la página **Basic Information**.
3. Localice la fila **IP as a Backend**, habilite la función. En el cuadro de diálogo que se muestra, haga clic en **OK**.

4. Seleccione la pestaña **Listeners**, haga clic en **Add Listener** y configure el puerto de escucha en **1234**.
5. Haga clic en **Next: Configure Request Routing Policy**.
6. Haga clic en **Next: Add Backend Server**. A continuación, seleccione la pestaña **IP as Backend Servers**.
7. Haga clic en **Add IP as Backend Server**. En el cuadro de diálogo que se muestra, configure **Backend Server IP Address** y **Backend Port**.
   - **Backend Server IP Address**: Ingrese la dirección IP del motor WAF dedicado, que puede obtener de la lista de motores dedicados.
   - **Backend Port**: 81, que es el mismo que el puerto no estándar que seleccionó en **Paso 2.3**.
8. Haga clic en **OK**.
9. Haga clic en **Next: Confirm**, confirme la información y haga clic en **Submit**.

Paso 4 Desvincule una dirección IP elástica (EIP) del servidor de origen y vincule el EIP al equilibrador de carga configurado para la instancia WAF dedicada.

----Fin

5.1.4 ¿Puede WAF proteger varios nombres de dominio que apuntan al mismo servidor de origen?

Sí. Si hay varios nombres de dominio que apuntan al mismo servidor de origen, puede conectar estos nombres de dominio a WAF para su protección.

WAF protege los nombres de dominio o direcciones IP. Si varios nombres de dominio utilizan el mismo EIP para proporcionar servicios, todos estos nombres de dominio deben estar conectados a WAF.

5.1.5 ¿Cómo configuro nombres de dominio para protegerse al agregar nombres de dominio?

Antes de usar WAF, debe agregar nombres de dominio para protegerse a WAF en función de sus requisitos de protección de servicios web. WAF admite la adición de nombres de dominio únicos y nombres de dominio de comodín. En esta sección se describe cómo configurar los nombres de dominio para protegerse.

Conceptos básicos

- Nombre de dominio de comodín

  Un nombre de dominio de comodín es un nombre de dominio que contiene el comodín * y comienza con *.

  Por ejemplo, ***.example.com** es un nombre de dominio comodín correcto, pero ***.*.example.com** no lo es.

  NOTA

  Un nombre de dominio comodín cuenta como un nombre de dominio.

- Nombre de dominio único

  Un nombre de dominio único también se llama un nombre de dominio común y es un nombre de dominio específico (un nombre de dominio no comodín).

Por ejemplo, **www.example.com** o **example.com** es un nombre de dominio único.

NOTA

Por ejemplo, **www.example.com** cuenta como un nombre de dominio y también lo hace **a.www.example.com**.

Selección de un tipo de nombre de dominio

WAF admite nombres de dominio únicos y nombres de dominio comodín.

El nombre de dominio adquirido del proveedor de servicio de DNS es un nombre de dominio único (example.com). El nombre de dominio agregado a WAF puede ser example.com, un nombre de subdominio (por ejemplo, a.example.com), o un nombre de dominio de comodín (*.example.com). Puede seleccionar un tipo de nombre de dominio basado en los siguientes escenarios:

- Si los servicios de un nombre de dominio que se va a proteger son los mismos, introduzca un solo nombre de dominio. Por ejemplo, si todos los servicios de www.example.com a proteger son servicios en el puerto 8080, establezca **Domain Name** en un solo nombre de dominio **www.example.com**.
- Si la dirección IP del servidor de cada nombre de subdominio es la misma, introduzca un nombre de dominio comodín que se va a proteger. Por ejemplo, si las direcciones IP del servidor correspondientes a a.ejemplo.com, b.ejemplo.com y c.ejemplo.com son las mismas, **Domain Name** se puede establecer en un nombre de dominio comodín ***.example.com**.
- Si las direcciones IP del servidor de los nombres de subdominio son diferentes, agregue nombres de subdominio como nombres de dominio únicos uno por uno.

NOTA

Se recomienda establecer el nombre de dominio que se va a proteger para que sea el mismo que el nombre de dominio que se establece en el proveedor de DNS.

5.1.6 ¿Debo configurar el mismo puerto que el del servidor de origen al agregar un sitio web a WAF?

No. Cuando agrega un nombre de dominio a WAF, configure el puerto del servidor al puerto del sitio web protegido. El puerto de servidor de origen es el puerto de servicio utilizado por WAF para reenviar las solicitudes de su sitio web. A continuación se describen más detalles sobre la configuración del puerto:

- Si **Client Protocol** es **HTTP**, WAF protege los servicios en el puerto estándar 80 de forma predeterminada. Si **Client Protocol** es **HTTPS**, WAF protege los servicios en el puerto estándar 443 de forma predeterminada.
- Para configurar un puerto distinto de los puertos 80 y 443, seleccione un puerto no estándar de la lista desplegable **Protected Port**.

Para obtener más información sobre los puertos no estándar soportados por WAF, consulte **¿Qué puertos no estándar soporta WAF?**

5.1.7 ¿Cómo configuro puertos no estándar al agregar un nombre de dominio protegido?

Cuando agrega un nombre de dominio a WAF, **Port** debe estar configurado en el puerto de servicio de su sitio web. Puede configurarlo haciendo referencia a las siguientes instrucciones:

- Si **Client Protocol** es **HTTP**, WAF protege los servicios en el puerto estándar 80 de forma predeterminada. Si **Client Protocol** es **HTTPS**, WAF protege los servicios en el puerto estándar 443 de forma predeterminada.
- Para configurar un puerto distinto de los puertos 80 y 443, seleccione un puerto no estándar de la lista desplegable **Protected Port**.

Ejemplo de configuración 1: Protección del tráfico al mismo puerto estándar con diferentes direcciones IP del servidor de origen asignadas

1. Anule la selección de **Non-standard Port**.
2. Seleccione **HTTP** o **HTTPS** para **Client Protocol**. **Figura 5-3** y **Figura 5-4** mostrar configuraciones de puerto estándar cuando el protocolo cliente es HTTP o HTTPS.

Figura 5-3 Puerto 80

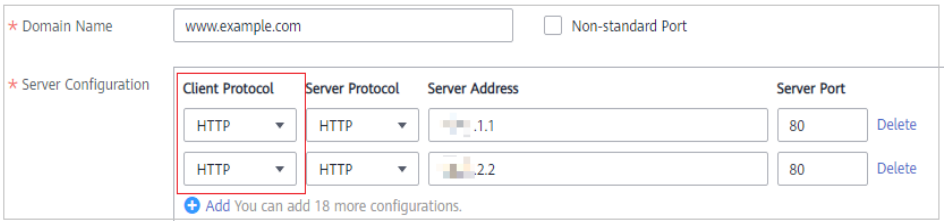
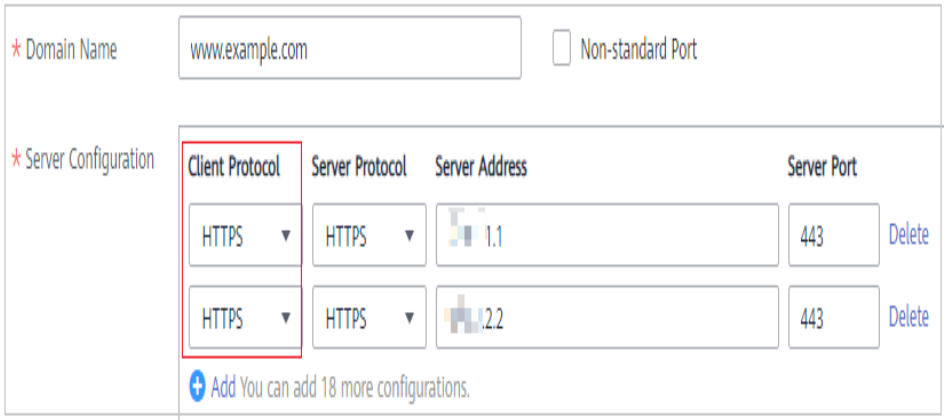


Figura 5-4 Puerto 443



NOTA

Si **Client Protocol** está establecido en **HTTPS**, se requiere un certificado.

3. Los visitantes de su sitio web pueden acceder al sitio web sin agregar un puerto al final del nombre de dominio. Por ejemplo, introduzca **http://www.example.com** en la casilla de dirección del navegador para acceder al sitio web.

Ejemplo de configuración 1: Protección del tráfico a un puerto no estándar con diferentes direcciones IP del servidor de origen asignadas

1. Seleccione **Non-standard Port** y seleccione un puerto no estándar que se va a proteger en la lista desplegable de **Port**. Para obtener más información sobre los puertos no estándar soportados por WAF, consulte **¿Qué puertos no estándar soporta WAF?**
2. Seleccione **HTTP** o **HTTPS** para **Client Protocol** para todos los puertos de servidor. **Figura 5-5** y **Figura 5-6** mostrar la configuración del puerto HTTP o HTTPS no estándar, respectivamente.

Figura 5-5 Otro puerto HTTP además del puerto 80

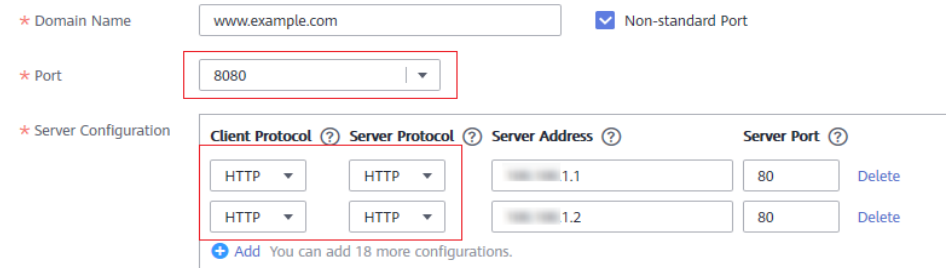
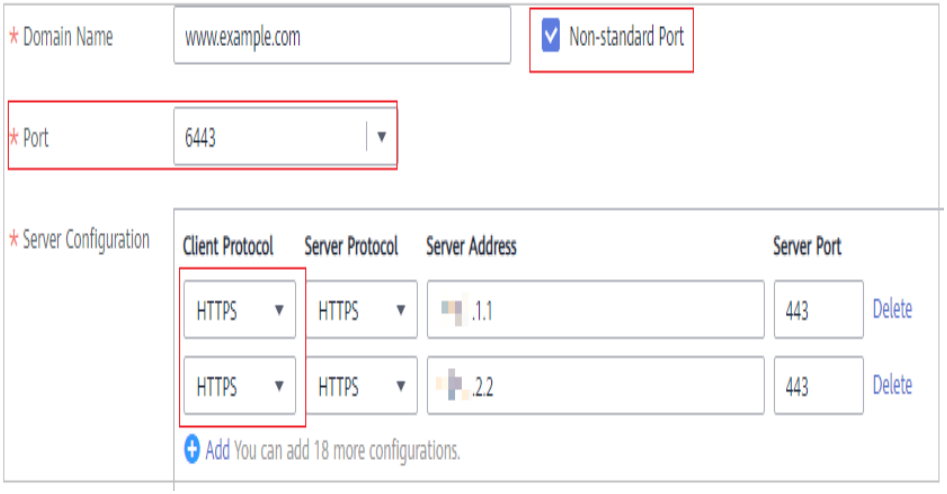


Figura 5-6 Otro puerto HTTPS además del puerto 443



NOTA

Si **Client Protocol** está establecido en **HTTPS**, se requiere un certificado.

3. Los visitantes deben agregar el puerto no estándar configurado al nombre de dominio cuando accedan a su sitio web. De lo contrario, se devuelve el error 404. Si el puerto no estándar es 8080, escriba *http://www.example.com:8080* en el cuadro de dirección del navegador.

Ejemplo de configuración 3: Protección de diferentes puertos de servicio

Si los puertos de servicio que se van a proteger son diferentes, configure los puertos por separado. Por ejemplo, para proteger los puertos 8080 y 6443 para su sitio **www.example.com**, agregue el dominio por separado para cada puerto, como se muestra en **Figura 5-7** y **Figura 5-8**.

Figura 5-7 Puerto de protección 8080

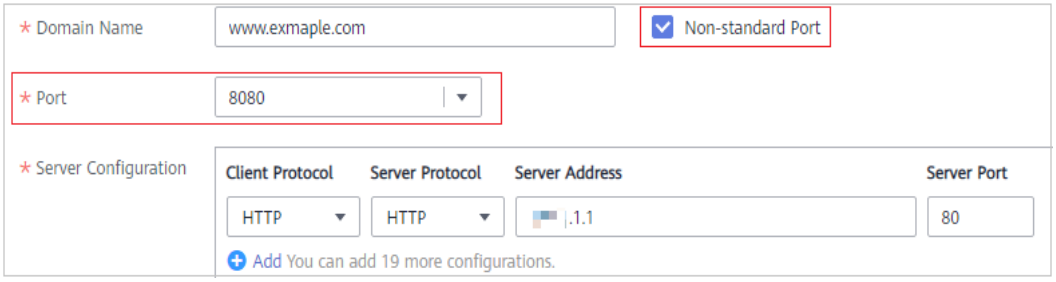
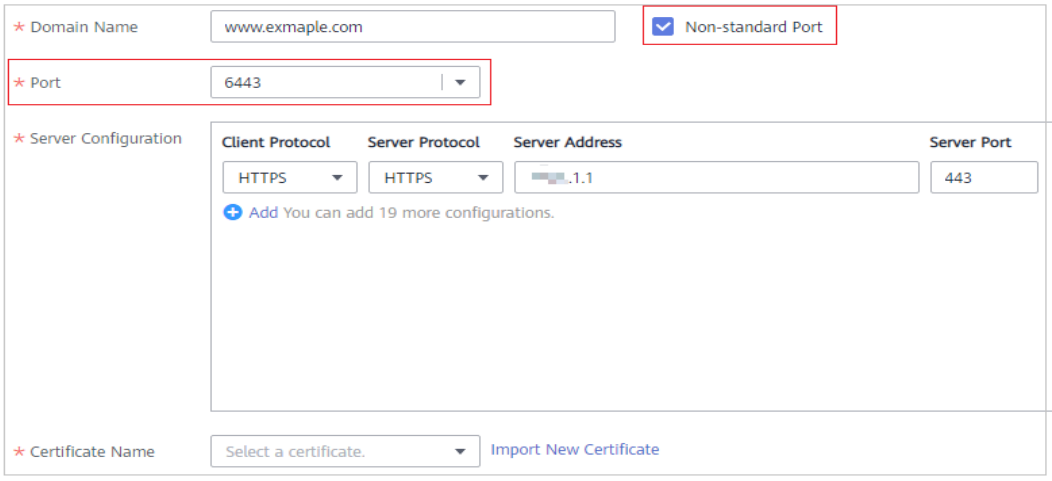


Figura 5-8 Puerto de protección 6443



5.1.8 ¿Qué puedo hacer si uno de los puertos de un servidor de origen no requiere protección WAF?

WAF protege su aplicación web a través de su nombre de dominio y el puerto de servicio correspondiente. Cuando se agrega un nombre de dominio a WAF, se especifica el nombre de dominio y el puerto que se va a proteger. Después de que el sitio web esté conectado a WAF, el tráfico no se reenviará a WAF a través de otros puertos.

Para obtener más información, consulte **Adición de un nombre de dominio a WAF**.

5.1.9 ¿Qué datos se requieren para conectar un nombre de dominio /dirección IP a WAF?

Prepare la información necesaria para conectar un nombre de dominio o una dirección IP a WAF según el modo de instancia de WAF que planea comprar.

- Modo en la nube

Tabla 5-2 Se requiere información de nombre de dominio

Información	Parámetro	Descripción	Ejemplo
Si se utiliza un proxy para el nombre de dominio	Proxy	Este parámetro debe establecerse en **Yes** si se ha desplegado un proxy de web de capa 7, como CDN y servicio de aceleración en la nube, para su sitio web antes de conectar el sitio web a WAF.	-
Parámetros de configuración	Nombre de dominio	El nombre de dominio es utilizado por los visitantes para acceder a su sitio web. Un nombre de dominio se compone de letras separadas por puntos (.). Es una dirección legible por humanos que se asigna a la dirección IP legible por máquina de su servidor.	www.example.com
	Puerto protegido	El puerto de servicio correspondiente al nombre de dominio del sitio web que desea proteger. ● Puertos estándares – 80: puerto predeterminado cuando el protocolo de cliente es HTTP – 443: puerto predeterminado cuando el protocolo de cliente es HTTPS ● Puertos no estándar Puertos distintos de los puertos 80 y 443 **AVISO** Si su sitio web utiliza un puerto no estándar, compruebe si la edición WAF que planea comprar puede proteger el puerto no estándar antes de realizar una compra. Para más detalles, consulte **¿Qué puertos no estándar admite WAF?**	80
	HTTP/2	HTTP/2 solo se puede usar para el acceso entre el cliente y WAF con la condición de que al menos un servidor de origen tenga **HTTPS** usado para **Client Protocol**.	-
	Protocolo del cliente	Protocolo utilizado por un cliente (por ejemplo, un navegador) para acceder al sitio web. WAF soporta HTTP y HTTPS.	HTTP

Información	Parámetro	Descripción	Ejemplo
	Protocolo de servidor	Protocolo utilizado por WAF para reenviar solicitudes del cliente (como un navegador). Las opciones son **HTTP** y **HTTPS**.	HTTP
	Dirección de servidor	Dirección IP pública o nombre de dominio del servidor de origen para que un cliente (como un navegador) acceda. En general, una dirección IP pública se asigna al registro A del nombre de dominio configurado en el DNS y un nombre de dominio al registro CNAME.	XXX.XXX.1.1
(Opcional) Certificado	Nombre del certificado	Si establece **Client Protocol** en **HTTPS**, debe configurar un certificado en WAF y asociar el certificado con el nombre de dominio. **AVISO** Solo se pueden utilizar certificados .pem en WAF. Si el certificado no está en formato PEM, conviértelo en formato PEM consultando **¿Cómo puedo convertir un certificado en formato PEM?**	-

- Modo dedicado

Tabla 5-3 Nombre de dominio o detalles de la dirección IP requeridos

Información	Parámetro	Descripción	Ejemplo
Parámetros de configuración	Sitio web protegido	• Nombre de dominio: utilizado por los visitantes para acceder a su sitio web. Un nombre de dominio se compone de letras separadas por puntos (.). Es una dirección legible por humanos que se asigna a la dirección IP legible por máquina de su servidor. • IP: dirección IP del sitio web.	www.example.com

Información	Parámetro	Descripción	Ejemplo
	Puerto protegido	El puerto de servicio correspondiente al nombre de dominio del sitio web que desea proteger. ● Puertos estándares – 80: puerto predeterminado cuando el protocolo de cliente es HTTP – 443: puerto predeterminado cuando el protocolo de cliente es HTTPS ● Puertos no estándar Puertos distintos de los puertos 80 y 443 **AVISO** Si su sitio web utiliza un puerto no estándar, compruebe si la edición WAF que planea comprar puede proteger el puerto no estándar antes de realizar una compra. Para más detalles, consulte **¿Qué puertos no estándar admite WAF?**	80
	Protocolo del cliente	Protocolo utilizado por un cliente (por ejemplo, un navegador) para acceder al sitio web. WAF soporta HTTP y HTTPS.	HTTP
	Protocolo de servidor	Protocolo utilizado por WAF para reenviar solicitudes del cliente (como un navegador). Las opciones son **HTTP** y **HTTPS**.	HTTP
	VPC	Seleccione la VPC a la que pertenece la instancia WAF dedicada.	vpc-default
	Dirección de servidor	Dirección IP privada del servidor del sitio web al que accede un cliente (por ejemplo, un navegador).	192.168.1.1

Información	Parámetro	Descripción	Ejemplo
(Opcional) Certificado	Nombre del certificado	Si establece **Client Protocol** en **HTTPS**, debe configurar un certificado en WAF y asociar el certificado con el nombre de dominio. **AVISO** ● Solo se pueden utilizar certificados .pem en WAF. Si el certificado no está en formato PEM, conviértelo en formato PEM consultando **¿Cómo puedo convertir un certificado en formato PEM?** ● Actualmente, los certificados adquiridos en Huawei Cloud SCM solo se pueden enviar al **default** proyecto empresarial. Para otros proyectos empresariales, los certificados SSL enviados por SCM no se pueden utilizar.	-

5.1.10 ¿Cómo puedo eliminar de forma segura un nombre de dominio protegido?

Para eliminar un sitio web, consulte **Eliminación de un sitio web protegido de WAF**. Antes de comenzar, familiarícese con las siguientes precauciones:

- En modo nube, si desea quitar un sitio web protegido de WAF, vaya a la plataforma DNS y traduzca el nombre de dominio a la dirección IP del servidor de origen antes de quitarlo. De lo contrario, el tráfico destinado al nombre de dominio no se dirigirá al servidor de origen.
- Si selecciona **Forcible delete the WAF CNAME record.**, WAF no comprobará la resolución de su nombre de dominio y eliminará el registro WAF CNAME inmediatamente. Antes de activar esta opción, asegúrese de haber resuelto el nombre de dominio en el servidor de origen, o su sitio web se volverá inaccesible.
- Se tarda un tiempo en quitar un sitio web de WAF, pero una vez que se inicia esta acción, no se puede cancelar. Tenga cuidado al quitar un sitio web de WAF.

5.1.11 ¿Puedo cambiar el nombre de dominio que se ha agregado a WAF?

Después de agregar un nombre de dominio a WAF, no puede cambiar su nombre. Si desea cambiar el nombre de dominio protegido, se recomienda eliminar el original y agregar el nombre de dominio que desea proteger.

5.1.12 ¿Cuáles son las precauciones para configurar varias direcciones de servidor para servidores backend?

- Al configurar varias direcciones de servidor para el mismo nombre de dominio, preste atención a lo siguiente:
  - Para la asignación de nombres de dominio a puertos no estándar

    El protocolo de cliente, el protocolo de servidor y el servidor para cada pieza de configuración del servidor deben ser los mismos.
  - Para la asignación de nombres de dominio a puertos estándar

    El protocolo de cliente, el protocolo de servidor y el servidor para cada pieza de configuración de servidor pueden ser diferentes.
- Cuando se agrega un nombre de dominio, WAF admite la adición de múltiples direcciones IP de servidor. WAF dirige las solicitudes legítimas de vuelta a los servidores de origen en modo de sondeo, reduciendo la presión sobre los servidores y protegiendo los servidores de origen. Por ejemplo, se agregan dos direcciones IP del servidor backend (IP-A e IP-B). Cuando hay 10 solicitudes para acceder al nombre de dominio, cinco solicitudes son reenviadas por WAF al servidor identificado por IP-A, y las otras cinco solicitudes son reenviadas por WAF al servidor identificado por IP-B.

5.1.13 ¿WAF admite nombres de dominio de comodín?

Sí. Al agregar un nombre de dominio a WAF, puede configurar un nombre de dominio único o un nombre de dominio de comodín según sus requisitos de servicio. Los detalles son los siguientes:

- Nombre de dominio único

  Configure un solo nombre de dominio para protegerlo. Por ejemplo, www.example.com
- Nombre de dominio de comodín

  Puede configurar un nombre de dominio comodín para permitir que WAF proteja los nombres de dominio de varios niveles bajo el nombre de dominio de comodín.
  - Si la dirección IP del servidor de cada nombre de subdominio es la misma, introduzca un nombre de dominio comodín que se va a proteger. Por ejemplo, si los nombres de subdominio ***a.example.com***, ***b.example.com***, and ***c.example.com*** tienen la misma dirección IP del servidor, puede agregar directamente el nombre de dominio comodín ****.example.com*** a WAF para su protección.
  - Si cada nombre de subdominio apunta a diferentes direcciones IP del servidor, agregue nombres de subdominio como nombres de dominio únicos uno por uno.

Para obtener más información, consulte **Adición de un nombre de dominio**.

5.1.14 ¿Cómo dirijo el tráfico del sitio web a WAF?

En modo nube, después de agregar su sitio web a WAF, resuelva el nombre de dominio a WAF para que el tráfico pueda pasar a través de WAF. A continuación, WAF filtrará las solicitudes maliciosas y reenviará solo las solicitudes legítimas al servidor de origen.

Cómo funciona WAF

- No proxy utilizado

  DNS resuelve su nombre de dominio a la dirección IP del servidor de origen antes de que el sitio se conecte a WAF. DNS resuelve su nombre de dominio en el CNAME de WAF

después de que el sitio se conecta a WAF. A continuación, WAF inspecciona el tráfico entrante y filtra el tráfico malicioso.

- Un proxy (como el servicio anti-DDoS) utilizado

  Si se utiliza un proxy como el servicio anti-DDoS en su sitio antes de conectarse a WAF, DNS resuelve el nombre de dominio de su sitio a la dirección IP anti-DDoS. El tráfico va al servicio anti-DDoS y el servicio anti-DDoS luego enruta el tráfico de regreso al servidor de origen. Después de conectar su sitio web a WAF, cambie la dirección de back-to-source del proxy (como el servicio anti-DDoS) al CNAME de WAF. De esta manera, el proxy reenvía el tráfico a WAF. A continuación, WAF filtra el tráfico ilegítimo y solo enruta el tráfico legítimo de vuelta al servidor de origen.

  NOTA

  - Para asegurarse de que WAF puede reenviar solicitudes correctamente, realice una verificación local haciendo referencia a **Pruebas de WAF** antes de modificar la configuración DNS.
  - Para evitar que otros usuarios configuren sus nombres de dominio en WAF por adelantado (esto causará interferencias en la protección de su nombre de dominio), agregue el nombre de subdominio y el registro TXT en su plataforma de gestión DNS. WAF puede determinar qué usuario posee el nombre de dominio basándose en el nombre de subdominio y el registro TXT. Para obtener más información sobre el método de configuración, consulte **¿Cuáles son los impactos si no hay ningún nombre de subdominio y registro TXT configurados?**

Guía de operación

Después de agregar un nombre de dominio, WAF genera un registro CNAME, o CNAME, nombre de subdominio y registro TXT para que DNS resuelva el nombre de dominio en WAF para que el tráfico del sitio web pueda pasar a través de WAF para su detección. Para obtener más información, consulte **Tabla 5-4**.

Tabla 5-4 Guía de operación

Escenario	Valor de parámetro generado	Operación relacionada con la resolución de nombres de dominio
No proxy utilizado	CNAME	El DNS obtiene el CNAME de WAF.
Proxy utilizado	CNAME, nombre de subdominio y registro TXT	• Cambie la dirección IP de origen del proxy, como el servicio anti-DDoS, al CNAME de WAF. • (Opcional) Agregue un nombre de subdominio WAF y un registro TXT en su proveedor DNS.

Procedimiento

Para obtener más información, consulte **Conexión de un nombre de dominio a WAF**.

5.1.15 ¿Qué puedo hacer si se muestra el mensaje "Illegal server address" al agregar un nombre de dominio?

Síntoma

Cuando un usuario agrega un nombre de dominio a proteger, el sistema muestra un mensaje que indica que la dirección del servidor de origen no es válida.

Causas posibles

- **Server Address** se establece en una dirección IP privada reservada para uso interno.
- **Server Address** y **Domain Name** se establecen en la misma dirección IP.

Sugerencias sobre el manejo

Establezca **Server Address** en la dirección IP del servidor de origen real (dirección IP pública) o en un nombre de dominio de origen independiente, que no puede ser el mismo que el nombre de dominio protegido.

5.1.16 ¿Por qué estoy viendo que mi cuota de dominio es insuficiente cuando todavía hay cuota restante?

La cuota de nombres de dominio contiene nombres de dominio de nivel superior y de segundo nivel. Esto ocurre cuando su cuota para el nombre de dominio de nivel superior se agota, pero intenta agregar un nombre de dominio de nivel superior a WAF.

En la página **Website Settings**, puede ver la cuota de nombre de dominio.

5.2 Gestión de certificados

5.2.1 ¿Por qué no se puede ver el certificado SSL de Huawei Cloud SCM en WAF?

Después de que un certificado SSL es administrado por Huawei Cloud SCM, debe enviar el certificado a WAF para que pueda ser utilizado en Huawei Cloud WAF.

Actualmente, los certificados adquiridos en Huawei Cloud SCM solo se pueden enviar al **default** proyecto empresarial. Para otros proyectos empresariales, los certificados SSL enviados por SCM no se pueden utilizar.

Para obtener más información sobre cómo enviar un certificado SSL de SCM a WAF, consulte **Enviar un certificado SSL a otros servicios en la nube**.

5.2.2 ¿Cómo selecciono un certificado al configurar un nombre de dominio carácter comodín?

Cada nombre de dominio debe corresponder a un certificado. Un nombre de dominio comodín solo se puede usar para un certificado de dominio comodín. Si solo tiene certificados de dominio único, debe agregar nombres de dominio uno por uno en WAF.

5.2.3 ¿Cómo modifico un certificado?

Si el certificado adquirido está a punto de caducar, se recomienda comprar un nuevo certificado antes de la fecha de caducidad y actualizar el certificado asociado con el nombre de dominio en WAF.

Realice las siguientes operaciones:

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Website Settings**.

Paso 5 En la columna **Protected Website**, haga clic en el nombre de dominio del sitio web para ir a la página de información básica.

Paso 6 Haga clic en junto a **Server Information**. Si **Client Protocol** es **HTTPS**, seleccione un nuevo certificado en la lista desplegable de certificados o importe un nuevo certificado.

----Fin

5.2.4 ¿Necesito importar los certificados que se han subido a ELB a WAF?

Puede seleccionar un certificado creado o importar un nuevo certificado. Necesita importar el certificado que se ha subido a ELB a WAF.

5.2.5 ¿Cómo puedo convertir un certificado en formato PEM?

Solo se pueden utilizar certificados .pem en WAF. Si el certificado no está en formato in.pem, conviértelo a.pem localmente haciendo referencia a **Tabla 5-5** antes de cargarlo.

Tabla 5-5 Comandos de conversión de certificados

Formato	Método de conversión
CER/CRT	Cambie el nombre del archivo de certificado **cert.crt** a **cert.pem**.

Formato	Método de conversión
PFX	● Obtener una clave privada. Por ejemplo, ejecute el siguiente comando para convertir **cert.pfx** en **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** ● Obtener un certificado. Por ejemplo, ejecute el siguiente comando para convertir **cert.pfx** en **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Convertir un certificado. Por ejemplo, ejecute el siguiente comando para convertir **cert.p7b** en **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Cambie el nombre del archivo de certificado **cert.cer** a **cert.pem**.
DER	● Obtener una clave privada. Por ejemplo, ejecute el siguiente comando para convertir **privatekey.der** en **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** ● Obtener un certificado. Por ejemplo, ejecute el siguiente comando para convertir **cert.cer** en **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTA

- Antes de ejecutar un comando OpenSSL, asegúrese de que la herramienta **OpenSSL** se haya instalado en el host local.
- Si su PC local ejecuta un sistema operativo Windows, vaya a la interfaz de línea de comandos (CLI) y, a continuación, ejecute el comando de conversión de certificados.

5.2.6 ¿Por qué mis proyectos empresariales personalizados no pueden utilizar el certificado SSL enviado por Huawei Cloud SCM?

Actualmente, los certificados adquiridos en Huawei Cloud SCM solo se pueden enviar al **default** proyecto empresarial. Para otros proyectos empresariales, los certificados SSL enviados por SCM no se pueden utilizar.

Para obtener más información, consulte **Enviar un certificado SSL a otros servicios en la nube**.

5.3 Server Configuration

5.3.1 ¿Cómo configuro el protocolo de cliente y el protocolo de servidor?

En esta sección de preguntas frecuentes se describe cómo configurar el protocolo de cliente y servidor.

WAF proporciona varios tipos de protocolo. Utilice www.example.com como ejemplo. Puede configurar su instancia WAF utilizando cualquiera de los siguientes métodos:

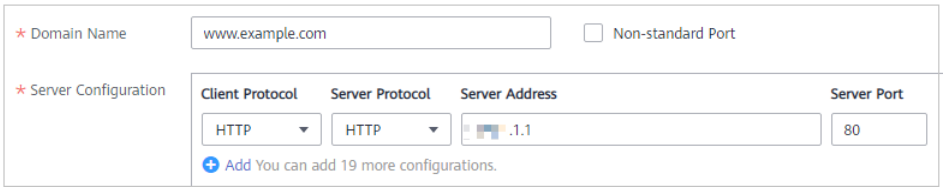
Acceso HTTP - Respuesta de redirección 302

Establezca **Client Protocol** y **Server Protocol** en **HTTP** **Figura 5-9** muestra un ejemplo.

AVISO

Esta configuración permite que los visitantes de la web accedan a http://www.example.com a través de HTTP solamente. Si acceden a él a través de HTTPS, recibirán el código 302 encontrado y serán redirigidos a http://www.example.com.

Figura 5-9 Modo HTTP



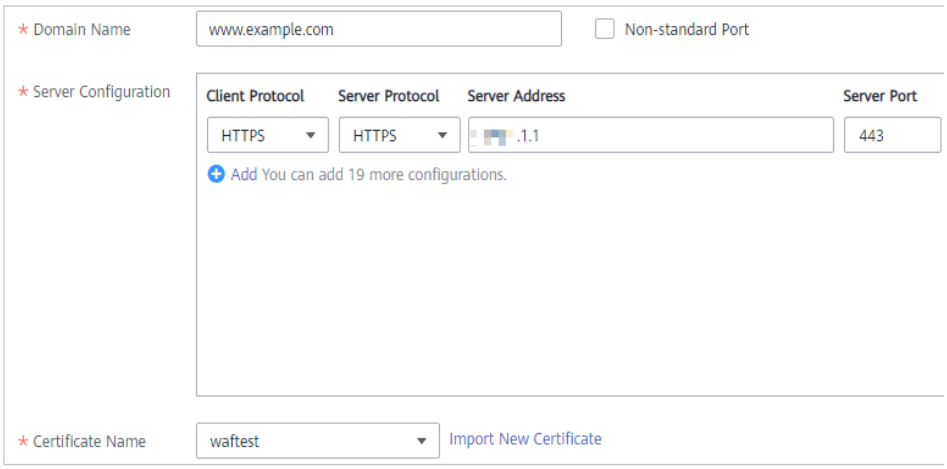
Conversión forzada de HTTPS

Establezca **Client Protocol** y **Server Protocol** en **HTTPS**. **Figura 5-10** muestra un ejemplo. Cuando se utiliza el protocolo HTTP para acceder al servidor, todas las solicitudes iniciales del cliente se convierten a la fuerza de HTTP a HTTPS.

AVISO

- Si los visitantes de la web acceden a su sitio web a través de HTTPS, el sitio web devuelve una respuesta correcta.
- Si los visitantes de la web acceden a http://www.example.com a través de HTTP, recibirán el código 302 encontrado y serán dirigidos a https://www.example.com.

Figura 5-10 Modo HTTPS



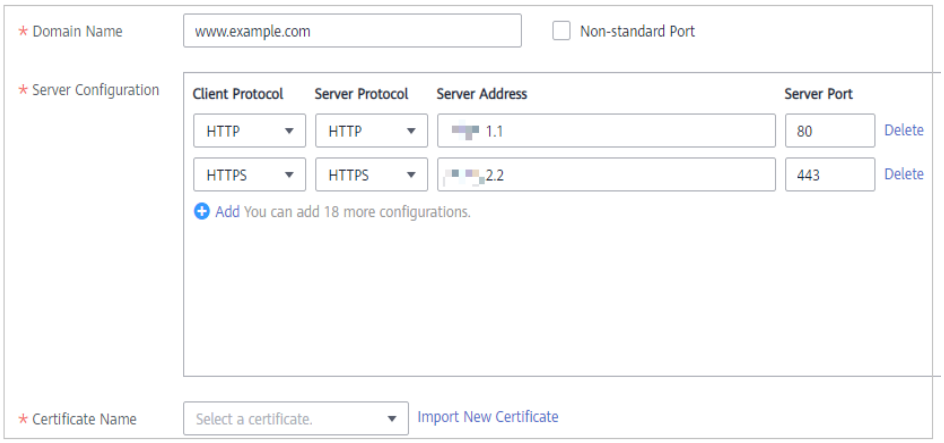
HTTP y HTTPS

Establezca **Client Protocol** y **Server Protocol**. **Figura 5-11** muestra un ejemplo.

AVISO

- Si los visitantes de la web acceden a su sitio web a través de HTTP, el sitio web devuelve una respuesta exitosa, pero no se cifra ninguna comunicación entre el navegador y el sitio web.
- Si los visitantes de la web acceden a su sitio web a través de HTTPS, el sitio web devuelve una respuesta exitosa y todas las comunicaciones entre el navegador y el sitio web están encriptadas.

Figura 5-11 Modos HTTP y HTTPS



Descarga de HTTPS

Establezca **Client Protocol** en **HTTPS** y **Server Protocol** en **HTTP**.

AVISO

Si los visitantes de la web acceden a su sitio web a través de HTTPS, WAF reenvía las solicitudes a su servidor de origen a través de HTTP.

5.3.2 ¿Por qué no puedo seleccionar un protocolo de cliente al agregar un nombre de dominio?

El puerto no estándar que ha configurado no es compatible con el protocolo de cliente (HTTP/HTTPS). El puerto no estándar que configurará debe ser compatible con el protocolo cliente (HTTP/HTTPS).

Para más detalles, consulte **¿Qué puertos no estándar admite WAF?**

5.3.3 ¿Puedo establecer la dirección del servidor de origen en un registro CNAME si estoy usando WAF en la nube?

Sí. Si la dirección IP del servidor de origen se establece en un registro CNAME, se realiza una resolución de DNS adicional después de agregar un nombre de dominio. Es decir, el CNAME se resuelve primero a una dirección IP. La resolución DNS aumenta el retraso. Por lo tanto, se recomienda una dirección IP de red pública para el servidor de origen.

Para obtener más información, consulte **Adición de un nombre de dominio a WAF**.

5.4 Resolución de nombres de dominio

5.4.1 ¿Cómo modifico el registro DNS en Huawei Cloud DNS?

Si su sitio web puede ser accesible directamente a través de un cliente (como un navegador) antes de agregar el nombre de dominio del sitio web a WAF, después de agregar el nombre de dominio a WAF, apunte el nombre de dominio al CNAME de WAF usando su plataforma DNS. De esta manera, el tráfico destinado a su sitio web va primero a WAF. A continuación, WAF comprueba el tráfico, bloquea los ataques y reenvía solo el tráfico normal al servidor de origen.

En este tema se utiliza Huawei Cloud DNS como ejemplo para describir cómo modificar el registro DNS. Los métodos para modificar el registro DNS en otra plataforma son similares.

Prerrequisitos

- Ha agregado el nombre de dominio a la instancia WAF en la nube.
- Para asegurarse de que WAF reenvía las solicitudes correctamente, verifique la conexión de WAF y el nombre de dominio localmente antes de modificar la configuración DNS haciendo referencia a **Pruebas de WAF**.

Restricciones

- El registro CNAME debe ser único para el mismo registro de host. Necesita cambiar el registro CNAME existente de su nombre de dominio al registro WAF CNAME.
- Los conjuntos de registros de diferentes tipos en la misma zona pueden entrar en conflicto entre sí. Por ejemplo, para el mismo registro de host, el registro CNAME entra en conflicto con otros registros como A record, MX record y TXT record. Si el tipo de registro no se puede cambiar directamente, puede eliminar los registros en conflicto y agregar un registro CNAME. La eliminación de otros registros y la adición de un registro CNAME debe completarse en el menor tiempo posible. Si no se agrega ningún registro CNAME después de eliminar el registro A, la resolución del dominio puede fallar. Para obtener más información, consulte **¿Por qué un mensaje indica un conflicto con un registro existente cuando agrego un conjunto de registros?**
- Para evitar que otros usuarios configuren su nombre de dominio en WAF antes de agregarlo a WAF (esto causará interferencia en la protección de su nombre de dominio), agregue el nombre de subdominio y el registro TXT en su plataforma de gestión DNS. WAF determinará qué usuario posee el nombre de dominio basándose en el nombre de subdominio y el registro TXT. Para obtener más información sobre el método de configuración, consulte **¿Cuáles son los impactos si no hay ningún nombre de subdominio y registro TXT configurados?**

- Un conjunto de registros modificado tiene efecto cuando expira la duración de la caché especificada por el TTL del conjunto de registros original. Si el portador establece una duración de memoria caché más larga, el conjunto de registros tendrá efecto después de que transcurra este período de tiempo.

Procedimiento

Vaya a la página **Website Settings** en la consola WAF y haga clic en en la columna **Access Status** en la fila del dominio para copiar el registro CNAME.

Realice los siguientes pasos para modificar el registro DNS:

5.4.2 ¿Cómo verifico la propiedad del dominio usando el DNS de Huawei Cloud?

La verificación por DNS normalmente requiere operaciones del administrador del nombre de dominio. Si está gestionando su nombre de dominio en Huawei Cloud y el nombre de dominio está en su cuenta, realice la verificación con el DNS de Huawei Cloud.

AVISO

Si su nombre de dominio está alojado en otras plataformas, como www.net.cn, www.xinnet.com y www.dnspod.cn, realice la verificación en la plataforma correspondiente. Por ejemplo, si su nombre de dominio está alojado en Alibaba Cloud, realice la verificación en Alibaba Cloud.

Por ejemplo, lo siguiente muestra cómo agregar un registro TXT **2019030700000022ams1xbyevdn4jvahact9xzpicb565k9443mryw2qe99mbzpb** para el nombre de dominio **domain3.com**. El procedimiento para verificar la propiedad del dominio con Huawei Cloud DNS es similar.

Prerrequisitos

Ha obtenido la información de configuración (registro de host y valor de registro) necesaria para la verificación del nombre de dominio.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Elija **Domain Name Service** en **Network** para ir a la página **Domain Name Service**.

Paso 3 En el panel de navegación de la izquierda, elija > **Public Zones**.

Paso 4 En la página **Public Zones** que se muestra, haga clic en nombre de dominio **domain3.com**.

Paso 5 En la página de la pestaña **Record Sets**, en la esquina superior izquierda, haga clic en **Add Record Set**.

NOTA

Si hay un registro TXT del nombre de dominio **domain3.com** en la lista de nombres de dominio, haga clic en **Modify** en la columna **Operation**. Modifique el registro en el cuadro de diálogo **Modify Record Set** que se muestra.

- **Name**: Introduzca el prefijo del registro de host devuelto por el proveedor de servicios de nombres de dominio en la página de verificación de nombres de dominio.

  El registro de host devuelto varía según el proveedor de servicio de nombres de dominio. Los siguientes son dos ejemplos:

  Ejemplo:

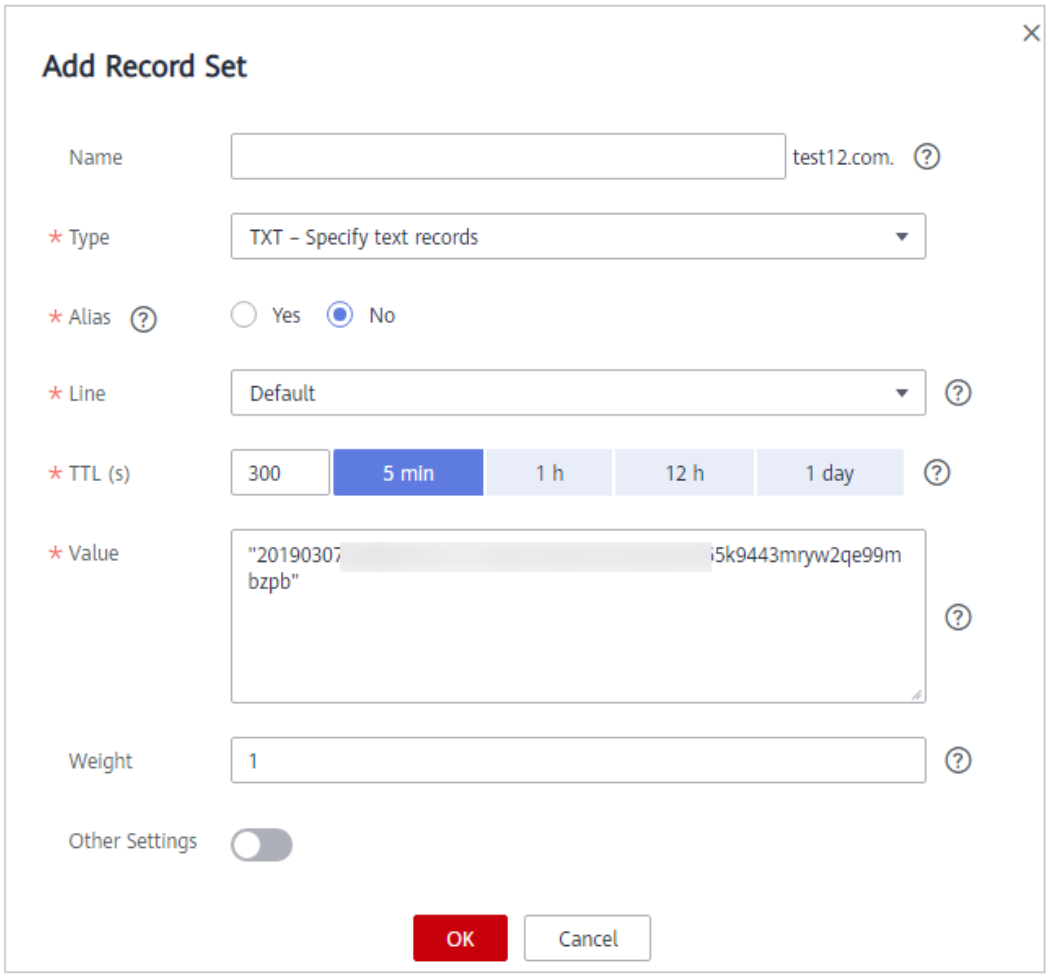
  – Si el registro de host devuelto por el proveedor de servicios de nombres de dominio es **_dnsauth.domain3.com**, establezca **Name** en **_dnsauth**.

  – Si el registro de host devuelto por el proveedor de servicio de nombres de dominio es **domain3.com**, deje **Name** vacío.
- **Type**: Seleccione **TXT – Specify text records**.
- **Line**: Seleccione **Default**.
- **TTL (s)**: El valor recomendado es **5 min**. Un valor TTL mayor hará que sea más lento para la sincronización y actualización de registros de DNS.
- **Value**: Introduzca el valor de registro devuelto por el proveedor de servicios de nombres de dominio en la página de verificación de propiedad del dominio.

  NOTA

  Los valores de registro deben comillas y pegarse en el cuadro de texto.
- Mantenga los demás ajustes sin cambios.

Figura 5-12 Adición de un conjunto de registros



Paso 6 Haga clic en **OK**.

Si el estado del conjunto de registros es **Normal**, el conjunto de registros se agrega correctamente.

NOTA

- Los registros de configuración de DNS solo se pueden eliminar después de que se haya emitido o revocado el certificado.
- Compruebe si el registro DNS está configurado correctamente. Si no es así, el certificado no puede ser emitido.
- Una vez completada la verificación de propiedad del dominio, la CA tarda un período de tiempo en confirmar la verificación. Durante este período, el certificado se encuentra en el estado de **Pending domain name verification**. El certificado introduce el estado de **Pending organization verification** solo después de que la CA haya confirmado la propiedad del dominio.

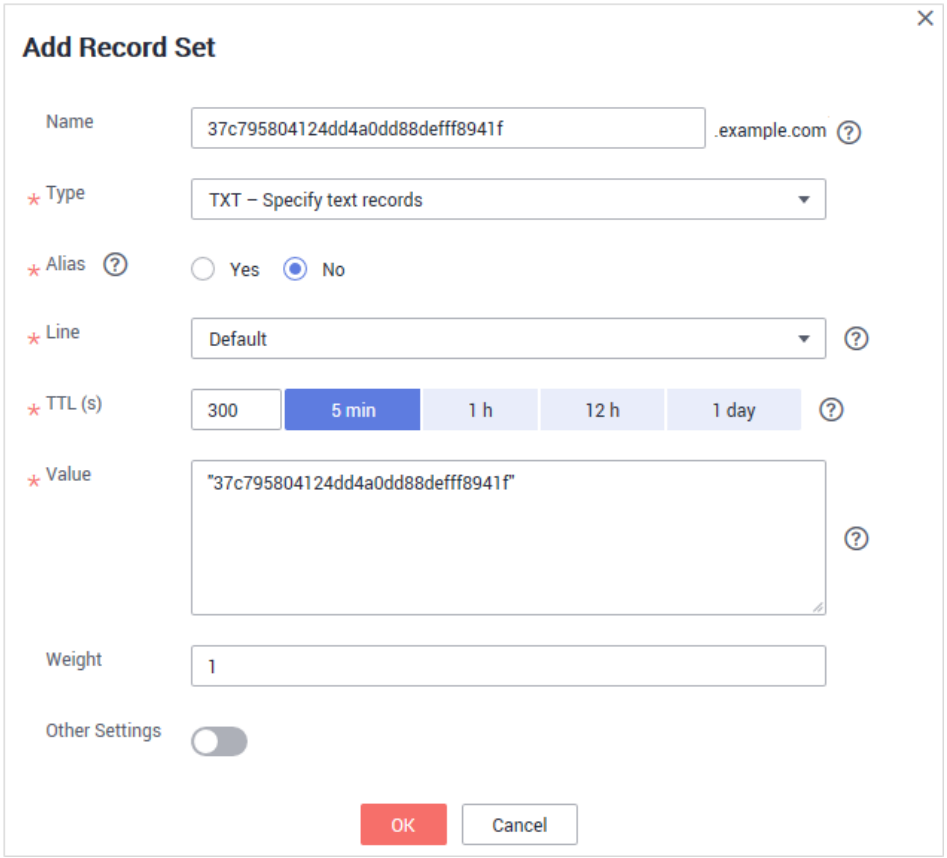
----Fin

5.4.3 ¿Cómo configuro el registro TXT en el servicio DNS de Huawei Cloud?

Después de agregar el nombre de dominio del proxy, como Anti-DDoS avanzado (AAD), en WAF, configuró el nombre de subdominio y el registro TXT en su proveedor DNS para proteger sus nombres de dominio. Si otros usuarios configuran el mismo nombre de dominio en WAF, su protección para el nombre de dominio se verá afectada negativamente.

Si utiliza el servicio DNS en Huawei Cloud, agregue comillas dobles ("") al registro TXT y péguelas en el cuadro de texto, por ejemplo, "37c795804124dd4a0dd88defff8941f".

Figura 5-13 Adición de un conjunto de registros



Para obtener más información sobre cómo configurar un nombre de subdominio y un registro TXT en el servicio DNS en Huawei Cloud, consulte **¿Cuáles son los impactos si no se configura ningún nombre de subdominio y registro TXT?**

5.4.4 ¿Cuáles son los impactos si no se configura ningún nombre de subdominio y registro TXT?

Después de agregar el nombre de dominio del proxy, como Anti-DDoS avanzado, en WAF, si el nombre de subdominio y el registro TXT no están configurados en su proveedor DNS y otros usuarios configuran el mismo nombre de dominio en WAF, La protección de su dominio será interferida.

Cómo determinar

Su nombre de dominio está en gris en la lista de nombres de dominio, y el modo de trabajo es **Suspended** y no se puede cambiar a **Enabled**. Si se produce este síntoma, su nombre de dominio ha sido ocupado por otro usuario.

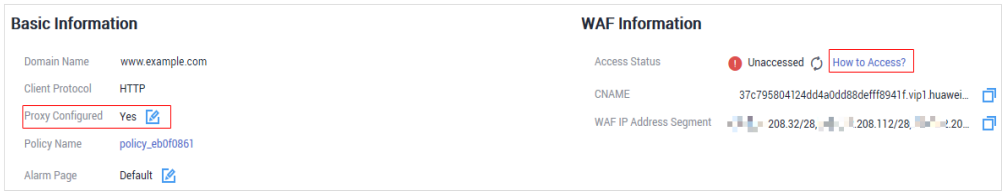
Solución

Vaya a su proveedor de DNS, agregue un nombre de subdominio y configure un registro TXT para el nombre de subdominio. El siguiente ejemplo utiliza el nombre de dominio ***www.example.com*** para describir cómo configurar el servicio DNS en Huawei Cloud.

Paso 1 Obtener los valores de **Subdomain Name** y **TXT Record**.

1. **Inicie sesión en la consola de gestión**.
2. Haga clic en ☰ en la esquina superior izquierda de la consola de gestión y elija **Security & Compliance** > **Web Application Firewall**. En el panel de navegación, seleccione **Website Settings**.
3. En la columna **Domain Name**, haga clic en Nombre de dominio ***www.example.com*** para ir a la página **Basic Information**.
4. Ubique la fila **Access Status** y haga clic en **How to Access**.

Figura 5-14 Información de acceso al nombre de dominio

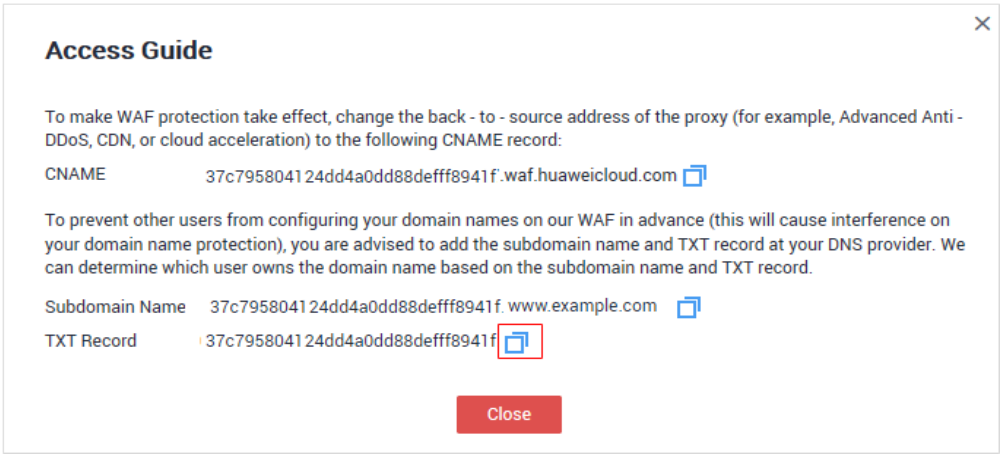


NOTA

Si un nombre de dominio que utiliza un proxy, como Anti-DDoS avanzado (AAD), se ha agregado a WAF, el valor de **Proxy Configured** es **Yes**.

5. En el cuadro de diálogo mostrado, haga clic en ⧉ para copiar el valor de **TXT Record**.

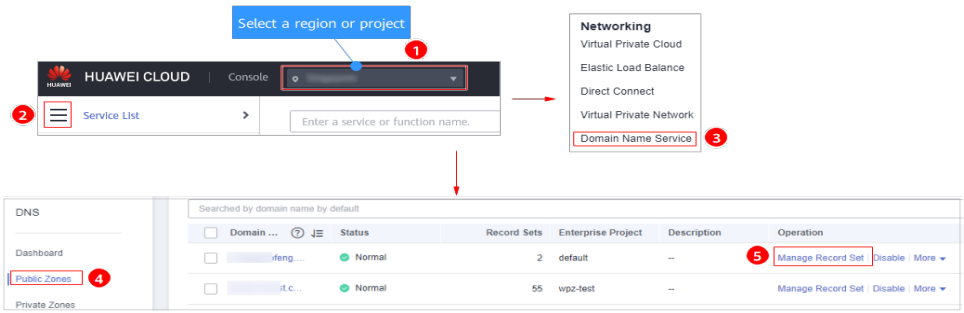
Figura 5-15 Copia de **TXT Record**



Paso 2 Agregue un nombre de subdominio WAF y un registro TXT en su proveedor de DNS.

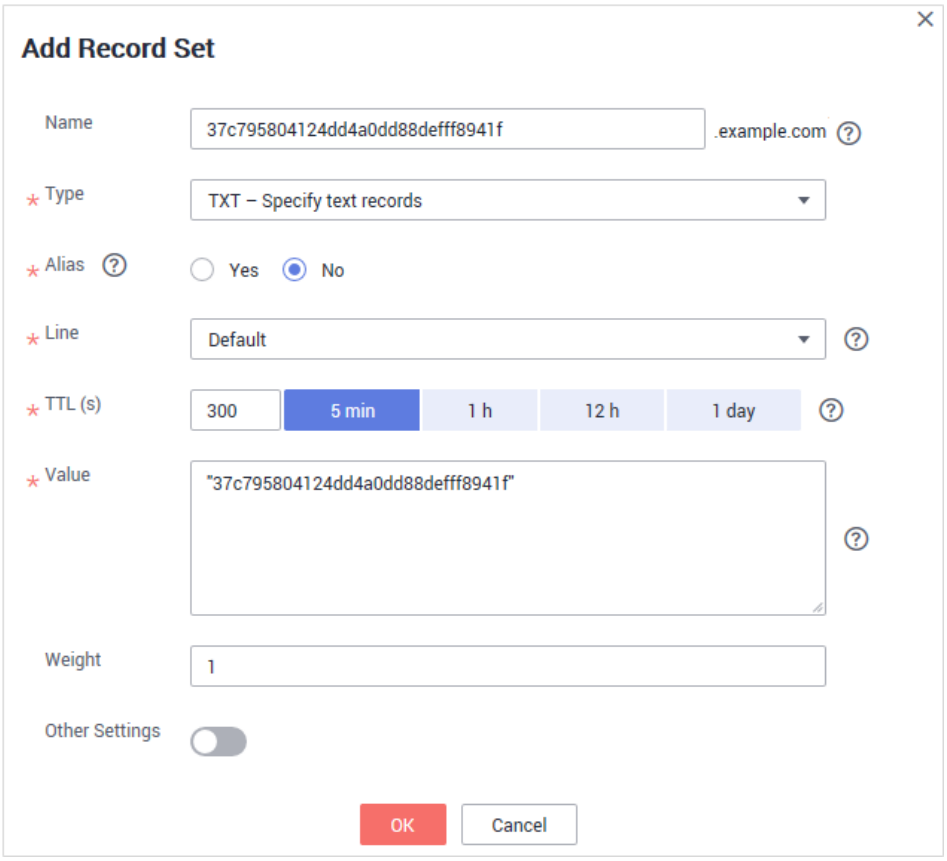
1. En la columna **Operation** del ***www.example.com*** de nombre de dominio, haga clic en **Add Record Set**. **Figura 5-16** muestra el ejemplo.

Figura 5-16 Página DNS



2. En la esquina superior izquierda, haga clic en **Add Record Set** para ir a la página **Add Record Set**.
   - **Name**: Pegue el registro TXT copiado en **Paso 1.5** al cuadro de texto.
   - **Type**: Seleccione **TXT – Specify text records**.
   - **Alias**: Seleccione **No**.
   - **Line**: Seleccione **Default**.
   - **TTL (s)**: El valor recomendado es **5 min**. Un valor TTL mayor hará que sea más lento para la sincronización y actualización de registros de DNS.
   - **Value**: Agregue comillas al registro TXT copiado desde **Paso 1.5** y péguelas en el cuadro de texto, por ejemplo, "37c795804124dd4a0dd88defff8941f".
   - Mantenga los demás ajustes sin cambios.

Figura 5-17 Adición de un conjunto de registros



3. Haga clic en **OK**.

----Fin

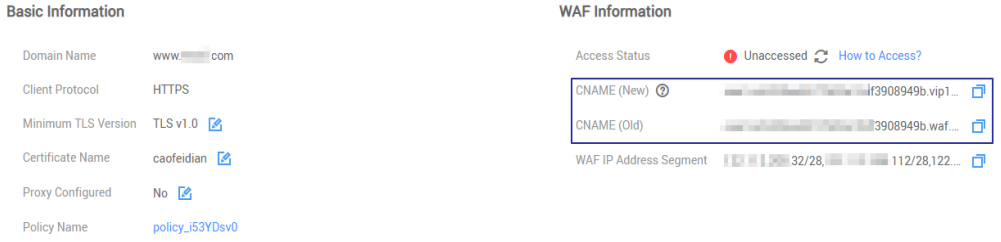
5.4.5 ¿Cuáles son las diferencias entre los CNAME antiguos y los nuevos?

Fondo

WAF actualiza los CNAMEs para mejorar la confiabilidad de la resolución de nombres de dominio.

Para asegurarse de que un nombre de dominio agregado se puede usar correctamente, WAF conserva el antiguo CNAME en la página de información básica del nombre de dominio agregado y muestra el nuevo CNAME, como se muestra en **Figura 5-18**.

Figura 5-18 Nuevo CNAME



Diferencias entre los CNAMEs antiguos y nuevos

El nuevo CNAME proporciona la función de resolución para dos DNS activos/activos heterogéneos, mejorando la fiabilidad de la resolución de nombres de dominio.

Se recomienda seleccionar un nuevo CNAME durante la resolución del nombre de dominio.

5.5 Operaciones después de conectar sitios web a WAF

5.5.1 ¿Puedo acceder a un sitio web usando una dirección IP después de que un nombre de dominio esté conectado a WAF?

Después de conectar un nombre de dominio a WAF, puede introducir la dirección IP del servidor de origen en la barra de direcciones del navegador para acceder al sitio web. Sin embargo, la dirección IP del servidor de origen se expone fácilmente. Como resultado, los atacantes pueden eludir WAF y atacar su servidor de origen.

Se recomienda configurar la protección del servidor de origen de acuerdo con las instrucciones en **Protección de servidor original**.

5.5.2 ¿Cómo puedo probar WAF?

Antes de dirigir el tráfico a WAF, realice una verificación local para asegurarse de que todas las configuraciones son correctas.

Antes de probar WAF, asegúrese de que el protocolo, la dirección y el puerto utilizados por el servidor de origen del nombre de dominio (por ejemplo, **www.example5.com**), y el archivo de certificado cargado y la clave privada si **Client Protocol** es **HTTPS** son correctos.

Para obtener más información, consulte **Pruebas de WAF**.

5.5.3 ¿Cómo puedo reenviar solicitudes directamente al servidor de origen sin pasar por WAF?

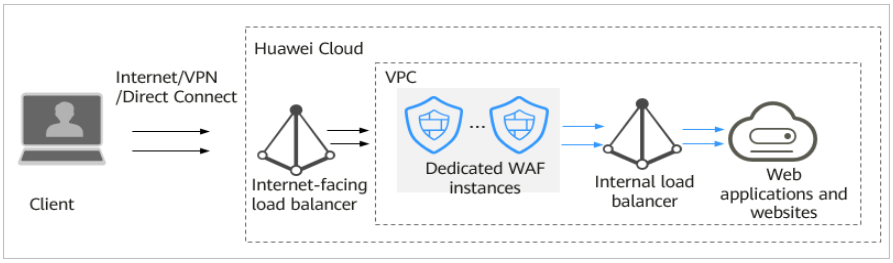
Si utiliza instancias WAF en la nube o instancias WAF dedicadas, siga los pasos de este tema para dirigir el tráfico de su sitio web directamente a sus servidores de origen.

- Modo en la nube

  Cambie **Mode** de trabajo WAF a **Bypassed**. Luego, las solicitudes de su sitio web van directamente a los servidores de origen sin pasar por WAF. Toma alrededor de 3 a 5 minutos para que el bypass WAF tenga efecto.

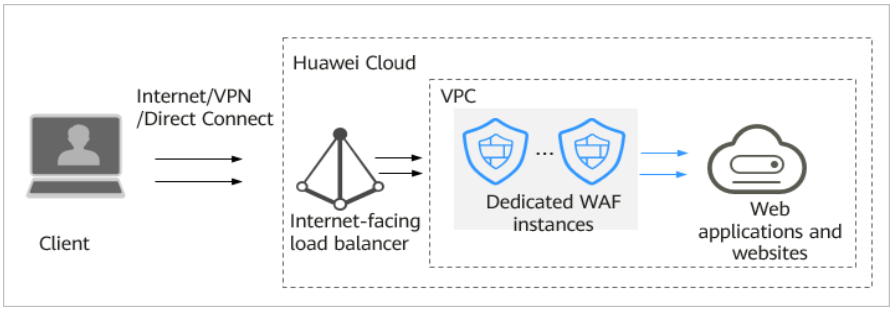
- Modo dedicado
  - Si su sitio web tiene un balanceador de carga de red privada implementado detrás de la instancia de WAF dedicada, como se muestra en **Figura 5-19**, desvincule el EIP del balanceador de carga orientado a Internet y luego vincule el EIP al balanceador de carga privado. Al hacerlo, el tráfico de su sitio web omitirá WAF e irá directamente al servidor de origen.

Figura 5-19 Arquitectura de implementación de instancias de WAF dedicadas (balanceadores de carga de red privada desplegados detrás de instancias de WAF dedicadas)



– Si su sitio web no tiene un equilibrador de carga de red privada implementado detrás de la instancia WAF dedicada, como se muestra en **Figura 5-20**, desvincule el EIP de la instancia WAF dedicada y luego vincule el EIP al servidor de origen. Al hacerlo, el tráfico de su sitio web omitirá WAF e irá directamente al servidor de origen.

Figura 5-20 Arquitectura de implementación de instancia WAF dedicada (sin balanceador de carga de red privada implementado detrás de instancias de WAF dedicadas)



Restricciones

Puede cambiar el modo de trabajo WAF a **Bypassed** solo cuando se selecciona **Cloud mode** para el sitio web y su sitio web encuentra cualquiera de los siguientes problemas:

- Los servicios del sitio web deben ser restaurados al estado cuando el sitio web no está conectado a WAF.
- Es necesario investigar los errores del sitio web, como 502, 504, u otros problemas de incompatibilidad.
- No se configura ningún proxy entre el cliente y WAF.

Configuración de WAF en la nube

El siguiente procedimiento le guiará a través de cómo configurar el modo **Bypassed** de WAF.

Procedimiento para omitir una instancia WAF dedicada en escenarios en los que se implementa un equilibrador de carga de red privada detrás de una instancia WAF

Puede desvincular el EIP del balanceador de carga de red pública y luego vincularlo al balanceador de carga privado para que el tráfico a su sitio web protegido pueda omitir WAF y vaya directamente al servidor de origen.

Paso 1 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 2 Haga clic en en la esquina superior izquierda de la página y elija **Elastic Load Balance** en **Network** para ir a la página **Load Balancers**.

Paso 3 En la página **Load Balancers**, busque la fila que contiene el balanceador de carga orientado a Internet, haga clic en **More** en la columna **Operation** y seleccione **Unbind IPv4 EIP**. **Figura 5-21** muestra un ejemplo.

Figura 5-21 Desvinculación de una EIP de un balanceador de carga orientado a Internet

Paso 4 En el cuadro de diálogo mostrado, haga clic en **Yes** para desvincular el EIP del balanceador de carga.

Paso 5 En la página **Load Balancers**, busque la fila que contiene el balanceador de carga privado, haga clic en **More** en la columna **Operation** y seleccione **Bind IPv4 EIP**.

Paso 6 En el cuadro de diálogo **Bind IPv4 EIP** que se muestra, seleccione la dirección IP pública en la que desvincula en **Paso 3** y haga clic en **OK**.

----Fin

Procedimiento para omitir una instancia de WAF dedicada en escenarios en los que no se implementa ningún balanceador de carga de red privada detrás de instancias de WAF

Puede quitar la instancia de WAF dedicada del balanceador de carga de red pública y agregar el servidor de origen al balanceador de carga orientado a Internet para que el tráfico a su sitio web pueda omitir WAF y vaya directamente al servidor de origen.

Paso 1 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

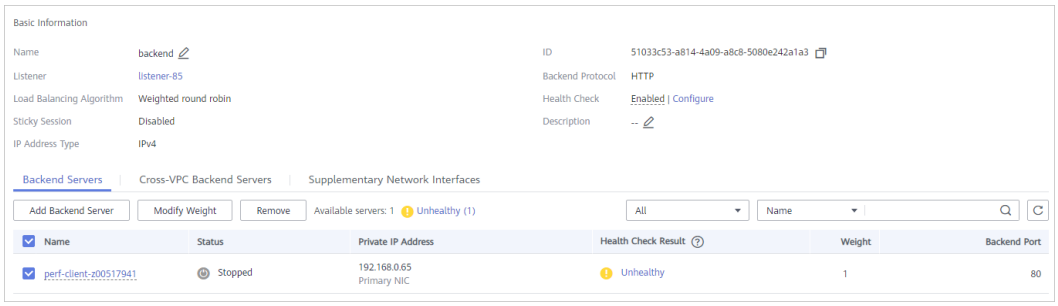
Paso 2 Haga clic en en la esquina superior izquierda de la página y elija **Elastic Load Balance** en **Network** para ir a la página **Load Balancers**.

Paso 3 Haga clic en el nombre del balanceador de carga que desee en la columna **Name** para ir a la página **Basic Information**.

Figura 5-22 Lista de balanceadores de carga

Paso 4 Haga clic en la pestaña **Backend Server Groups**, seleccione la instancia WAF dedicada que desea quitar y haga clic en **Remove** en la columna **Operation**. **Figura 5-23** muestra un ejemplo.

Figura 5-23 Eliminación de una instancia WAF dedicada de un equilibrador de carga orientado a Internet

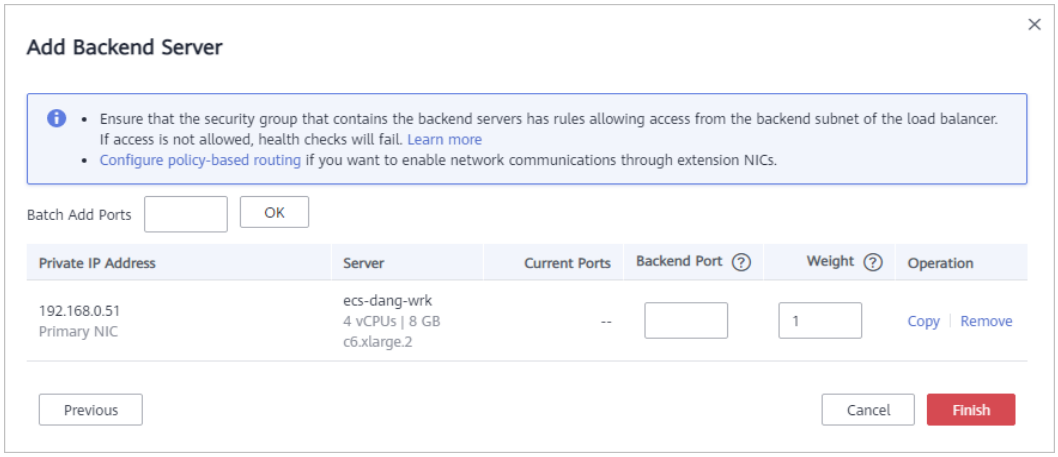


Paso 5 En el cuadro de diálogo que se muestra, haga clic en **Yes**.

Paso 6 Haga clic en **Add Backend Server** y seleccione servidores en el cuadro de diálogo **Add Backend Server** que se muestra.

Paso 7 Haga clic en **Next**, configure un puerto de backend y haga clic en **Finish**.

Figura 5-24 Adición de servidores de origen como servidores de backend



----Fin

5.5.4 ¿Por qué no se puede habilitar el modo de protección después de conectar un nombre de dominio a WAF?

Otro inquilino ha configurado el mismo nombre de dominio en WAF. Como resultado, la propiedad del nombre de dominio es ocupada por otro inquilino. En este caso, agregue un nombre de subdominio y configure un registro TXT para el nombre de subdominio en su proveedor DNS. Para más detalles, consulte **¿Cuáles son los impactos si no se configura ningún nombre de subdominio y registro TXT?**

6 Comprobación de interrupción del servicio

6.1 ¿Cómo soluciono los errores 404/502/504?

Si se produce un error, como 404 Not Found, 502 Bad Gateway o 504 Gateway Timeout, después de conectar un nombre de dominio a WAF, utilice los métodos siguientes para localizar la causa y quitar el error:

502 Bad Gateway

Escenario: El acceso al sitio web es normal una vez completada la configuración WAF. Sin embargo, después de un cierto período de tiempo, se notifica con frecuencia un error de 502 Bad Gateway.

NOTA

Si su servidor web no está implementado en Huawei Cloud, consulte con su proveedor de servicios si el servidor tiene la configuración de bloqueo predeterminada. En caso afirmativo, solicite al proveedor de servicios que quite la configuración de bloqueo predeterminada.

Las posibles causas son las siguientes:

- **Causa 1**: Su sitio web está utilizando otro software de protección de seguridad. El software considera las direcciones IP de origen de WAF como maliciosas y bloquea las solicitudes enviadas por WAF. Como resultado, el sitio se vuelve inaccesible.

  Solución: Agregue los rangos de direcciones IP WAF a la lista blanca del firewall (hardware o software), el software de protección de seguridad y el módulo de limitación de velocidad haciendo referencia a **¿Cómo incluyo rangos de direcciones IP en la lista blanca de WAF en la nube?**

- **Causa 2**: Se configuran varios servidores de backend. Sin embargo, un servidor backend es inalcanzable.

  Realice los siguientes pasos para comprobar si la configuración del servidor de origen es correcta:

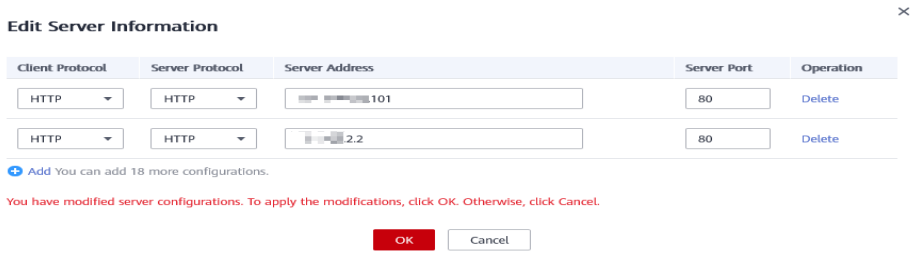
  a. Inicie sesión en la consola de gestión, haga clic en **Service List** en la parte superior de la página y elija **Security** > **Web Application Firewall**.

  b. En el panel de navegación, seleccione **Website Settings**.

c. En la columna **Protected Website**, haga clic en el nombre de dominio para ir a la página **Basic Information**.

d. En el área **Server Information**, haga clic en . En la página mostrada, compruebe si el protocolo del cliente, el protocolo del servidor, la dirección del servidor de origen y el puerto utilizado por el servidor de origen son correctos.

Figura 6-1 Configuración del servidor



e. Ejecute el comando **curl** en el host para comprobar si se puede acceder correctamente a cada servidor de origen.

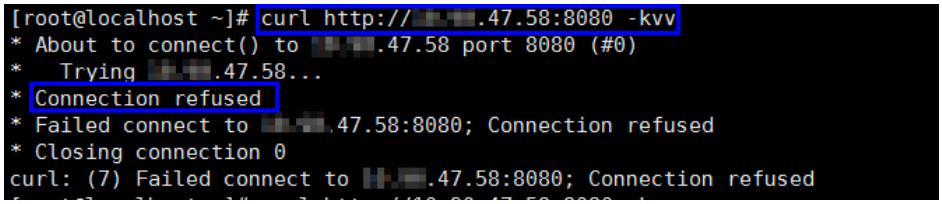
```
curl http://xx.xx.xx.xx:yy -kvv
```

xx.xx.xx.xx indica la dirección IP del servidor de origen. *yy* indica el puerto del servidor de origen. *xx.xx.xx.xx* y *yy* deben pertenecer al mismo servidor de origen.

NOTA

- El host donde se puede ejecutar el comando **curl** debe cumplir los siguientes requisitos:
  - La comunicación de la red debe ser normal.
  - Se ha instalado el comando **curl**. **curl** debe instalarse manualmente en el host que ejecuta el sistema operativo Windows. **curl** se instala junto con otros sistemas operativos.
- También puede introducir **http://*origin server address*:*origin server port*** en la barra de direcciones del navegador para comprobar si se puede acceder correctamente al servidor de origen.

Figura 6-2 Salida del comando



Si se muestra **connection refused**, el servidor de origen es inalcanzable y no se puede acceder al sitio web. Realice las siguientes operaciones:

- Compruebe si el servidor se está ejecutando correctamente. Si no lo es, reinicie el servidor.
- Agregue los rangos de direcciones IP WAF a la lista blanca del firewall (hardware o software), el software de protección de seguridad y el módulo de limitación de velocidad haciendo referencia a **¿Cómo incluyo rangos de direcciones IP en la lista blanca de WAF en la nube?**

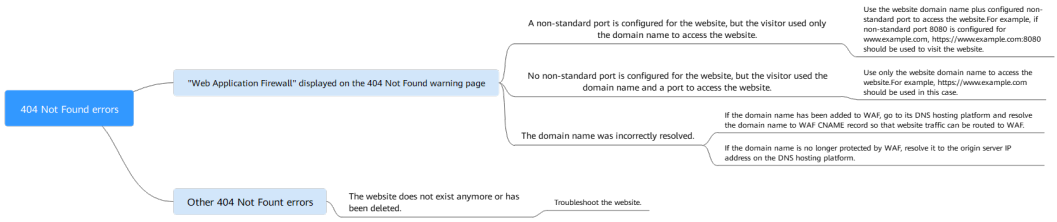
- **Causa 3**: Rendimiento del servidor de origen

  Solución: Póngase en contacto con el propietario de su sitio web para rectificar el error.

Proceso de solución de problemas y sugerencias de 404 Not Found

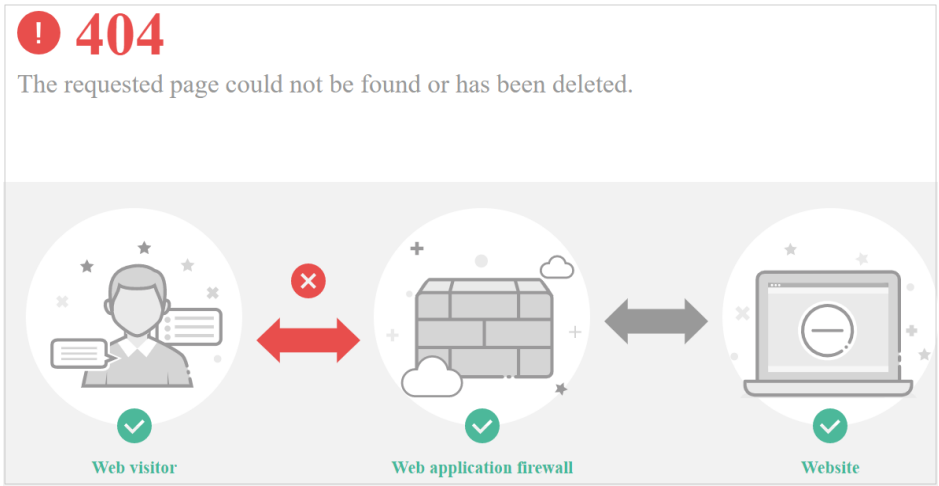
Consulte **Figura 6-3** para corregir el error 404 Not Found después de que su sitio web esté conectado a WAF.

Figura 6-3 Solución de problemas para el error 404 Not Found



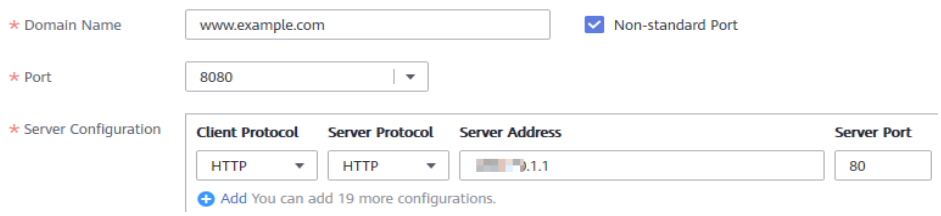
- Si se muestra la página mostrada en **Figura 6-4**, las posibles causas y soluciones son las siguientes:

  Figura 6-4 Página 404

  Cause 1: Se configura un puerto no estándar cuando se agrega el nombre de dominio a WAF, pero los visitantes usan el nombre de dominio y el puerto estándar o usan solo el nombre de dominio para acceder al sitio web. Por ejemplo, un puerto no estándar se configura como se muestra en **Figura 6-5**. Un visitante utiliza https://www.example.com o https://www.example.com:80 para acceder al sitio web. Como resultado, se muestra la página de error 404.

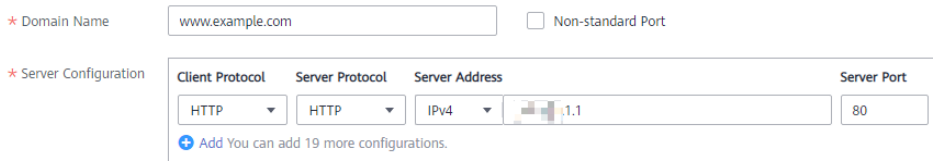
  Figura 6-5 Configuración de un puerto no estándar

Solución: Agregue el puerto no estándar a la URL y vuelva a acceder al servidor de origen, por ejemplo, **https://www.example.com:8080**.

Cause 2: No se configura ningún puerto no estándar cuando se agrega el nombre de dominio a WAF. Los visitantes usan el nombre de dominio y un puerto no estándar o el puerto no estándar configurado para el puerto del servidor de origen para acceder al sitio web. Por ejemplo, acceder **https://www.example.com:8080** cuando se configura el servicio de protección mostrado en **Figura 6-6**.

Figura 6-6 Puerto no estándar no configurado



NOTA

Si no se configura ningún puerto no estándar, WAF protege los servicios en el puerto 80/443 de forma predeterminada. Para proteger los servicios en otros puertos, vuelva a configurar la configuración del dominio.

Solución: Utilizar solo el nombre de dominio para acceder al sitio web. Por ejemplo, **https://www.example.com**.

Causa 3: El nombre de dominio se ha resuelto incorrectamente.

Solución:

– Si el nombre de dominio se ha agregado a WAF, resolver el nombre de dominio a WAF haciendo referencia a **Enrutar el tráfico del sitio web a WAF**.

– Si el nombre de dominio ya no está protegido por WAF, resuélvalo a la dirección IP del servidor de origen en la plataforma de alojamiento de DNS.

- Si la página de respuesta no es similar a la mostrada en **Figura 6-4**, las posibles causas y soluciones son las siguientes:

  Causa: El sitio web no existe o ha sido eliminado.

  Solución: Comprobar el sitio web.

Procesos y soluciones de resolución de problemas de 504 Gateway Timeout

Después de conectar su sitio web a WAF, la posibilidad de error de 504 gateway timeout aumenta a medida que aumenta el tráfico de su sitio web. En algunos otros casos, puede haber una posibilidad de error de tiempo de espera del gateway 504 si los visitantes acceden a su sitio web a través de las direcciones IP del servidor de origen. Consulte **Figura 6-7** para corregir errores de 504 gateway timeout.

Figura 6-7 Proceso de resolución de problemas de errores de 504 gateway timeout

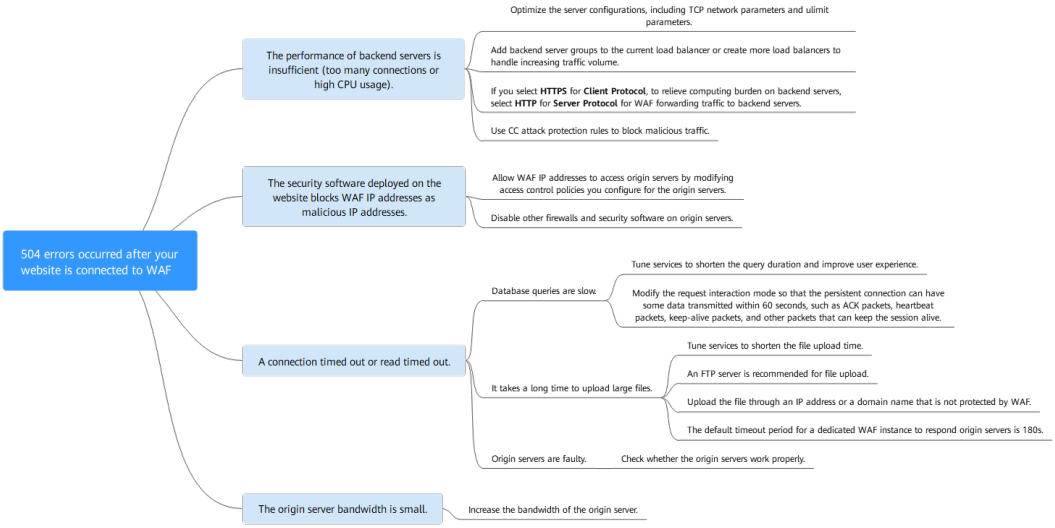


Tabla 6-1 Solución de problemas de errores de 504 gateway timeout

Causa posible	Resolución de problemas	Solución
Causa 1: Problemas de rendimiento del servidor de backend (como demasiadas conexiones o uso de CPU elevado)	Si el rendimiento del servidor de origen es insuficiente, compruebe los registros de acceso del servidor de origen y el tráfico de acceso para analizar los problemas.	• Optimice las configuraciones del servidor, incluidos los parámetros de red TCP y ulimit. • Se recomienda agregar grupos de servidores backend o crear nuevos balanceadores de carga para soportar las cargas de trabajo de servicio cada vez mayor, si su sitio web está conectado a una instancia de WAF en la nube. – Agregue más grupos de servidores de backend. – Para crear un balanceador de carga, consulte **Paso 1** a **Paso 7**. • Si configura **Client Protocol** a **HTTPS**, para aliviar la carga de los servidores backend, configure **HTTP** para **Server Protocol** para el tráfico de reenvío WAF a los servidores backend. Para obtener más información, consulte **Edición de información de servidor**. • Utilice las reglas de protección contra ataques CC para bloquear el tráfico malicioso.

Causa posible	Resolución de problemas	Solución
Causa 2 ● Las direcciones IP de origen WAF no están incluidas en la lista blanca o el puerto de servicio no está habilitado en el grupo de seguridad. ● Las direcciones IP WAF back-to-source son bloqueadas por el firewall en el servidor de origen.	Siga las siguientes soluciones para solucionar problemas: ● Compruebe si el servidor de origen tiene grupos de seguridad, firewalls y software de seguridad desplegados. ● Capture paquetes en el cliente y WAF, respectivamente, al mismo tiempo para comprobar si el firewall del servidor de origen descarta proactivamente paquetes de la conexión persistente a WAF.	● Configure una política de control de acceso en el servidor de origen para incluir en la lista blanca direcciones IP de WAF. – Modo en la nube: Consulte **¿Cómo incluyo rangos de direcciones IP en la lista blanca de WAF en la nube?**. – Modo Dedicado: **Incluir en la lista blanca las direcciones IP de origen de sus instancias WAF dedicadas** ● Deshabilite otros firewalls y software de seguridad en los servidores de origen.

Causa posible	Resolución de problemas	Solución
Causa 3: Tiempo de espera de conexión y tiempo de espera de lectura **NOTA** ● Se produce un error 504 si el servidor de origen es demasiado lento para responder, por ejemplo, una respuesta lenta a consultas de base de datos, un tiempo de carga largo para un archivo grande o un servidor de origen defectuoso. ● El período de tiempo de espera para que WAF reenvíe el tráfico a un servidor de origen es 60s o 180s. Se produce un error 504 si WAF no puede reenviar el tráfico dentro del período de tiempo de espera configurado.	Métodos de resolución de problemas: ● Omita WAF y acceda directamente al servidor de origen y luego verifique el tiempo de respuesta. ● Vea el tiempo de respuesta del servidor de origen en los registros de acceso almacenados en Log Tank Service (LTS). ● Omitir WAF, probar la función de carga de archivos y comprobar el tamaño del archivo.	● Las consultas a la base de datos son lentas. – Ajuste los servicios para acortar la duración de la consulta y mejorar la experiencia del usuario. – Modifique el modo de interacción de solicitud de modo que la conexión persistente pueda tener algunos datos transmitidos en 60 segundos, tales como paquetes ACK, paquetes de latidos del corazón, paquetes de mantenimiento activo y otros paquetes que pueden mantener la sesión activa. ● Se necesita mucho tiempo para cargar archivos de gran tamaño. – Ajuste los servicios para acortar el tiempo de carga de archivos. – Se recomienda un servidor FTP para cargar archivos. – Suba el archivo a través de una dirección IP o un nombre de dominio que no está protegido por WAF. – El período de tiempo de espera predeterminado para que una instancia WAF dedicada responda a los servidores de origen es de 180s. ● El servidor de origen está defectuoso. Compruebe si el servidor de origen funciona correctamente.

Causa posible	Resolución de problemas	Solución
Causa 4: El ancho de banda del servidor de origen es insuficiente. Cuando el tráfico de acceso es pesado, el servidor de origen no puede manejar todo el tráfico con su ancho de banda actual.	Métodos de resolución de problemas: ● Si tiene un balanceador de carga de capa 7 implementado en la parte posterior de WAF, puede consultar registros de 504 en el balanceador de carga. ● Si tiene un balanceador de carga de capa 4 implementado en la parte posterior de WAF, puede consultar los registros en el campo **Traffic exceeded the bandwidth threshold** en el balanceador de carga. ● Si tiene una EIP vinculado a las instancias WAF de backend, compruebe la supervisión del tráfico de EIP cuando los errores de 504 suban al volumen máximo.	Aumente el ancho de banda del servidor de origen.

Cree un balanceador de carga. Utilice la EIP del balanceador de carga como la dirección IP del servidor de origen y conecte el EIP a WAF.

AVISO

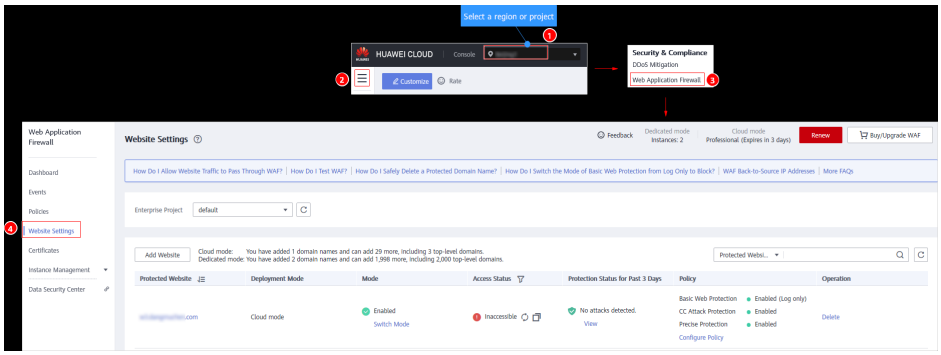
Se tarda unos dos minutos para que la modificación de la información del servidor tenga efecto.

Paso 1 **Cree un balanceador de carga compartido**.

Paso 2 **Inicie sesión en la consola de gestión**.

Paso 3 Vaya a la página **Website Settings** siguiendo los pasos en **Figura 6-8**.

Figura 6-8 Acceso a la página Configuración del sitio web



Paso 4 En la columna **Protected Website**, haga clic en el nombre de dominio para ir a la página **Basic Information**.

Paso 5 En el área **Server Information**, haga clic en . En la página mostrada, haga clic en **Add**.

Paso 6 Establezca la **Server Address** en el EIP enlazado al balanceador de carga.

Paso 7 Haga clic en **OK**.

----Fin

6.2 ¿Por qué es inaccesible mi nombre de dominio o dirección IP?

Síntomas

Si **Access Progress** de un sitio web que ha agregado a WAF es **Accessible**, se ha establecido la conexión entre WAF y el nombre de dominio o la dirección IP del sitio web.

AVISO

WAF comprueba automáticamente el estado de acceso de los sitios web protegidos cada hora. Si WAF detecta que una web protegida ha recibido 20 solicitudes de acceso en un plazo de 5 minutos, considera que la web se ha conectado correctamente a WAF.

WAF ofrece las instancias en la nube y dedicadas para proteger sus sitios web. Puede agregar nombres de dominio o direcciones IP a WAF. Antes de comenzar, familiarícese con las siguientes diferencias:

- Modo en la nube: protege sus aplicaciones web que tienen nombre de dominio y se implementan en Huawei Cloud, cualquier otra nube o centros de datos locales.
- Modo dedicado: protege las aplicaciones web desplegadas en Huawei Cloud y accesibles a través de nombres de dominio o direcciones IP.

Solución de problemas y soluciones para instancias de WAF en la nube

Consulte **Figura 6-9** y **Tabla 6-2** para corregir los errores de conexión del sitio web protegido en modo de nube.

Figura 6-9 Solución de problemas para instancias de WAF en la nube

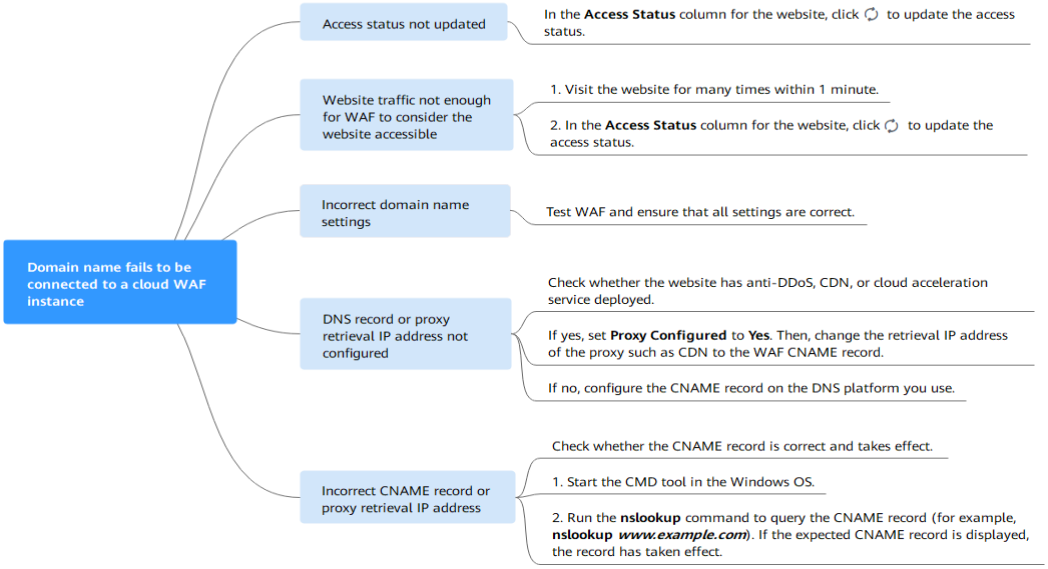


Tabla 6-2 Soluciones para fallas de instancias de WAF

Causa posible	Solución
Causa 1: **Access Status** de **Protected Website** no actualizado	En la columna **Access Status** del sitio web protegido, haga clic en para actualizar el estado.
Causa 2: El tráfico de acceso al sitio web no es suficiente para que WAF considere el sitio web accesible **AVISO** Después de conectar un sitio web a WAF, el sitio web se considera accesible solo cuando WAF detecta al menos 20 solicitudes al sitio web en 5 minutos.	1. Acceda al sitio web protegido muchas veces dentro de 1 minuto. 2. En la columna **Access Status** del sitio web, haga clic en para actualizar el estado.

Causa posible	Solución
Causa 3: Configuración del nombre de dominio incorrecta	**AVISO** WAF puede proteger el sitio web utilizando los siguientes tipos de nombres de dominio: ● Nombres de dominio de nivel superior, por ejemplo, example.com ● Nombres de dominio únicos/ Dominios de segundo nivel, por ejemplo www.example.com ● Nombres de dominio carácter comodín, por ejemplo, *.example.com Los nombres de dominio example.com y www.example.com son diferentes. Asegúrese de que los nombres de dominio correctos se agregan a WAF. Realice los siguientes pasos para asegurarse de que la configuración del nombre de dominio sea correcta. 1. En los sistemas operativos Windows, elija **Start** > **Run**. A continuación, introduzca **cmd** y **Enter**. 2. Haga ping al registro de CNAME (por ejemplo, hacer ping e59e684e2278043ae98a5423aef8ee329.vip.huaweicloudwaf.com) del nombre de dominio para obtener el WAF de vuelta dirección IP de origen. 3. Utilice un editor de texto para abrir el archivo **hosts**. Generalmente, el archivo **hosts** se almacena en el directorio **C:\Windows\System32\drivers\etc**. 4. Agregue un registro en el archivo **hosts** con el formato de ***DomainName WAF back-to-source IP address***. 5. Guarde el archivo **hosts** después de agregar el registro. En la CLI, ejecute el comando **ping** *Domain name added to WAF*, por ejemplo, ping www.example.com. Si la dirección IP de back-to-source de WAF en **2** se muestra en la salida del comando, la

Causa posible	Solución
	configuración del nombre de dominio es correcta. Para obtener más información, consulte **Pruebas de WAF**. Si hay una configuración incorrecta del nombre de dominio, quite el nombre de dominio de WAF y vuelva a agregarlo a WAF.
Causa 4: el registro DNS o las direcciones IP de origen de los proxies no configurados	Compruebe si el sitio web conectado a WAF utiliza proxies como anti-DDoS avanzado, CDN y servicio de aceleración en la nube. ● En caso afirmativo, asegúrese de que **Proxy Configured** esté configurado en **Yes** para el sitio web. – Cambie la dirección IP de retorno al origen del proxy, como CDN, al registro CNAME de WAF. – (Opcional) Agregue un nombre de subdominio WAF y un registro TXT en su proveedor DNS. ● Si no, póngase en contacto con su proveedor de servicios DNS para configurar un registro CNAME para el nombre de dominio. Para obtener más información, consulte **Conexión a un nombre de dominio a WAF**.

Causa posible	Solución
Causa 5: Registro DNS incorrecto o dirección de retorno de proxy	Realice los siguientes pasos para comprobar si el registro CNAME de nombre de dominio tiene efecto: 1. En los sistemas operativos Windows, elija **Start** > **Run**. A continuación, introduzca **cmd** y **Enter**. 2. Ejecute un comando **nslookup** para consultar el registro de CNAME. Si la salida del comando muestra el registro CNAME de WAF, el registro tiene efecto. Usando www.example.com como ejemplo, la salida es la siguiente: `nslookup www.example.com` Si el registro de CNAME no tiene efecto, modifique el registro de DNS o la dirección de origen. Para obtener más información, consulte **Conexión a un nombre de dominio a WAF**.

Solución de problemas y soluciones para instancias de WAF dedicadas

Consulte **Figura 6-10**y **Tabla 6-3** para corregir fallas de conexión.

Figura 6-10 Solución de problemas para el modo dedicado

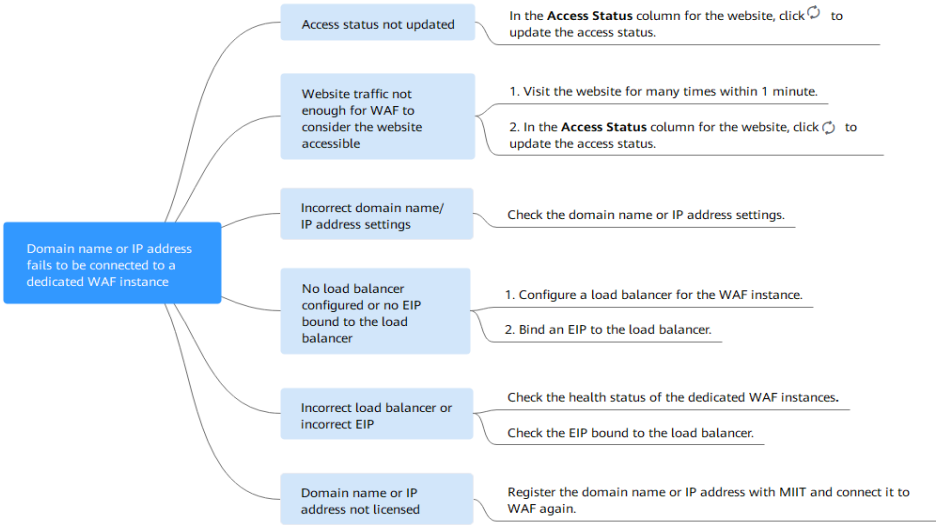


Tabla 6-3 Soluciones para el modo dedicado

Causa posible	Solución
Causa 1: **Access Status** para **Domain Name/IP Address** no actualizado	En la columna **Access Status** del sitio web, haga clic en para actualizar el estado.
Causa 2: El tráfico de acceso al sitio web no es suficiente para que WAF considere el sitio web accesible **AVISO** Después de conectar un sitio web a WAF, el sitio web se considera accesible solo cuando WAF detecta al menos 20 solicitudes al sitio web en 5 minutos.	1. Acceda al sitio web protegido muchas veces dentro de 1 minuto. 2. En la columna **Access Status** del sitio web, haga clic en para actualizar el estado.
Causa 3: Configuración incorrecta del nombre de dominio o de la dirección IP	Verifique la configuración de nombre de dominio o dirección IP haciendo referencia a **Ver la información básica sobre el nombre de dominio**. Si hay una configuración incorrecta para el nombre de dominio o la dirección IP, quite este nombre de dominio o la dirección IP de WAF y vuelva a agregarlo a WAF.
Causa 4: Ningún balanceador de carga configurado para la instancia de WAF dedicada o ningún EIP vinculado al equilibrador de carga configurado para la instancia de WAF dedicada	1. Configure un equilibrador de carga para instancias WAF dedicadas haciendo referencia a **Configuración de un balanceador de carga**. 2. **Vincule una EIP a un balanceador de carga**.
Causa 5: Balanceador de carga incorrecto configurado o EIP incorrecta vinculada al balanceador de carga	● Después de **configurar un balanceador de carga**, asegúrese de que **Health Check Result** para las instancias de WAF dedicadas agregadas al balanceador de carga es **Healthy**. ● Después de **vincular una EIP para balanceador de carga**, compruebe el estado de la EIP.

6.3 ¿Cómo manejo falsas alarmas cuando WAF bloquea las solicitudes normales a mi sitio web?

Una vez que un ataque alcanza una regla WAF, WAF responderá al ataque inmediatamente de acuerdo con la acción de protección (**Log only** o **Block**) que haya configurado para la regla y mostrará un evento en la página **Events**.

AVISO

Si ha habilitado proyectos de empresa, asegúrese de que tiene todos los permisos de operación para el proyecto en el que se encuentra la instancia WAF. A continuación, puede seleccionar el proyecto de la lista desplegable de **Enterprise Project** y manejar falsas alarmas en el proyecto. Para más detalles, consulte **Proyecto y Proyecto empresarial** .

En la fila que contiene el evento de falsa alarma, haga clic en **Details** en la columna **Operation** y vea los detalles del evento. Si está seguro de que el evento es un falso positivo, manténgalo como una falsa alarma haciendo referencia a **Tabla 6-4**. Después de que un evento es manejado como una falsa alarma, WAF deja de bloquear el tipo correspondiente de evento. No se mostrará este tipo de evento en la página **Events** y ya no recibirá notificaciones de alarma en consecuencia.

Tabla 6-4 Manejo de falsas alarmas

Tipo de regla de acierto	Regla de acierto	Método de gestión
Reglas de protección incorporadas WAF	• Reglas básicas de protección web La protección web básica protege contra ataques web comunes, como inyección SQL, ataques XSS, ataques remotos de desbordamiento de búfer, inclusión de archivos, vulnerabilidades Bash, ejecución remota de comandos, recorrido de directorios, acceso sensible a archivos e inyecciones de comandos y código. La protección web básica también detecta web shells y ataques de evasión. • Protección antirrastreador basada en características El antirrastreador basado en funciones identifica y bloquea el comportamiento del rastreador de motores de búsqueda, escáneres, herramientas de script y otros rastreadores.	En la fila que contiene el evento de ataque, haga clic en **Handle False Alarm** en la columna **Operation**. Para obtener más información, consulte **Manejo de alarmas falsas**.
Reglas de protección personalizadas	• Reglas de protección contra ataques CC • Reglas de protección precisas • Reglas de la lista negra y de la lista blanca • Reglas de control de acceso de geolocalización • Reglas de protección web contra manipulaciones • Protección antirrastreador de JavaScript • Normas de prevención de fugas de información • Reglas de enmascaramiento de datos	Vaya a la página que muestra la regla de acierto y elimínela.

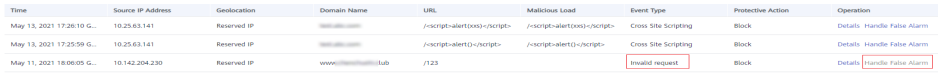
Tipo de regla de acierto	Regla de acierto	Método de gestión
Otros	Solicitudes de acceso no válidas **NOTA** Si cualquiera de los siguientes casos, WAF bloquea la solicitud de acceso como una solicitud no válida: ● Cuando se utiliza **form-data** para solicitudes POST o PUT, el número de parámetros en un formulario supera a 8,192. ● El URI contiene más de 2,048 parámetros. ● El número de encabezados es superior a 512.	Permitir las solicitudes bloqueadas haciendo referencia a **Configuración de una regla de protección precisa**. El botón **Handle False Alarm** para los eventos de acceso no válidos aparece atenuado, ya que dichos eventos se generan contra una regla de protección precisa.

6.4 ¿Por qué WAF bloquea las solicitudes normales como solicitudes no válidas?

Síntoma

Después de conectar un sitio web a WAF, WAF bloquea una solicitud de acceso normal. En la página **Events**, el **Event Type** correspondiente indica **Invalid request**, y el botón **Handle False Alarm** aparece atenuado, como se muestra en **Figura 6-11**.

Figura 6-11 Solicitudes normales bloqueadas por WAF como solicitudes no válidas



Causa posible

Si cualquiera de los siguientes casos, WAF bloquea la solicitud de acceso como una solicitud no válida:

- Cuando se utiliza **form-data** para solicitudes POST o PUT, el número de parámetros en un formulario supera a 8,192.
- El URI contiene más de 2,048 parámetros.
- El número de encabezados es superior a 512.

Solución

Si confirma que la solicitud bloqueada es una solicitud normal, permítela haciendo referencia a **Configuración de una regla de protección precisa**.

6.5 ¿Por qué está gris el botón de Handle False Alarm?

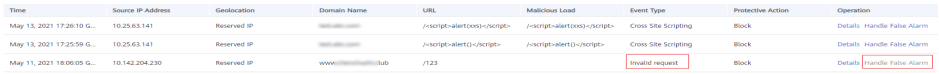
Compruebe que tiene los permisos para WAF. Para obtener más información, consulte **Gestión de permisos de WAF**.

AVISO

Si ha habilitado **Enterprise Project**, seleccione un proyecto de empresa y maneje falsas alarmas en el proyecto.

- Para eventos generados basados en reglas personalizadas (como una regla de protección contra ataques CC, una regla de protección precisa, una regla de lista negra, una regla de lista blanca o una regla de control de acceso de geolocalización) no pueden ser manejados como falsas alarmas. Para ignorar dicho evento, elimine o deshabilite la regla personalizada golpeada por el evento.
- Si cualquiera de los siguientes números en una solicitud de acceso excede de 512, WAF bloqueará la solicitud como una solicitud no válida y atenuará el botón **Handle False Alarm**.
  - Cuando se utiliza **form-data** para solicitudes POST o PUT, el número de parámetros en un formulario supera a 8,192.
  - El URI contiene más de 2,048 parámetros.
  - El número de encabezados es superior a 512.

Figura 6-12 Solicitudes normales bloqueadas por WAF como solicitudes no válidas



Para gestionar una solicitud no válida, consulte **¿Por qué WAF bloquea las solicitudes normales como solicitudes no válidas?**

6.6 ¿Cómo incluyo rangos de direcciones IP en la lista blanca de WAF en la nube?

Para permitir que el WAF en la nube surta efecto, configure las reglas de ACL en el servidor de origen para que confíen solo en las direcciones IP de back-to-source de WAF. Esto evita que los piratas informáticos ataquen el servidor de origen a través de las direcciones IP del servidor.

AVISO

Las reglas de ACL deben configurarse en el servidor de origen para incluir en la lista blanca direcciones IP de WAF back-to-source. De lo contrario, los visitantes de su sitio web recibirán con frecuencia el código de error 502 o 504 cuando su sitio web está conectado a WAF en modo de la nube.

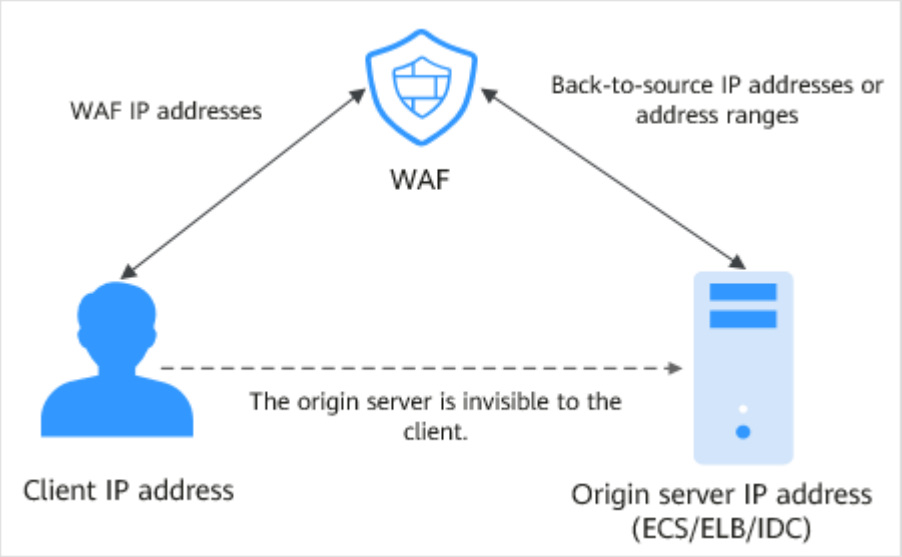
¿Qué son las direcciones IP de Back-to-Source?

Desde la perspectiva de un servidor, todas las solicitudes web se originan en WAF. Las direcciones IP utilizadas por el reenvío WAF son direcciones IP de origen de WAF. La dirección IP real del cliente se escribe en el campo de encabezado HTTP X-Forwarded-For (XFF).

NOTA

- Habrá más direcciones IP WAF debido a la escalabilidad horizontal o a los nuevos clústeres. Para sus nombres de dominio heredados, las direcciones IP de WAF suelen estar en varias direcciones IP de clase C (192.0.0.0 a 223.255.255.255) de dos a cuatro clústeres.
- Generalmente, estas direcciones IP no cambian a menos que los clústeres en uso se cambien debido a las conmutaciones de DR u otras conmutaciones de planificación. Incluso cuando el clúster WAF se conmuta en el fondo WAF, WAF comprobará la configuración del grupo de seguridad en el servidor de origen para evitar interrupciones del servicio.

Figura 6-13 Dirección IP de back-to-source



WAF Mecanismo de Comprobación de Dirección IP de Back-to-Source

Una dirección IP de Back-to-Source, o dirección IP de WAF, se asigna aleatoriamente desde el intervalo de direcciones IP de Back-to-Source. Cuando WAF reenvía solicitudes al servidor de origen, WAF comprobará el estado de la dirección IP. Si la dirección IP es anormal, WAF la eliminará y asignará aleatoriamente una normal para recibir o enviar solicitudes.

¿Por qué necesito incluir en la lista blanca los rangos de direcciones IP de WAF?

Todas las solicitudes web se originan a partir de una cantidad limitada de direcciones IP de WAF. Lo más probable es que el software de seguridad en el servidor de origen considere estas direcciones IP como maliciosas y las bloquee. Una vez que se bloquean las direcciones IP de WAF, es posible que no se acceda al sitio web o que se abra muy lentamente. Para solucionar esto, agregue las direcciones IP WAF a la lista blanca del software de seguridad.

> **NOTA**
>
> Después de conectar su sitio web a WAF, desinstale otro software de seguridad del servidor de origen o permita que solo las solicitudes de WAF accedan a su servidor de origen. Esto garantiza un acceso normal y protege el servidor de origen de hacking.

Procedimiento

Paso 1 **Inicie sesión en la consola de gestión**.

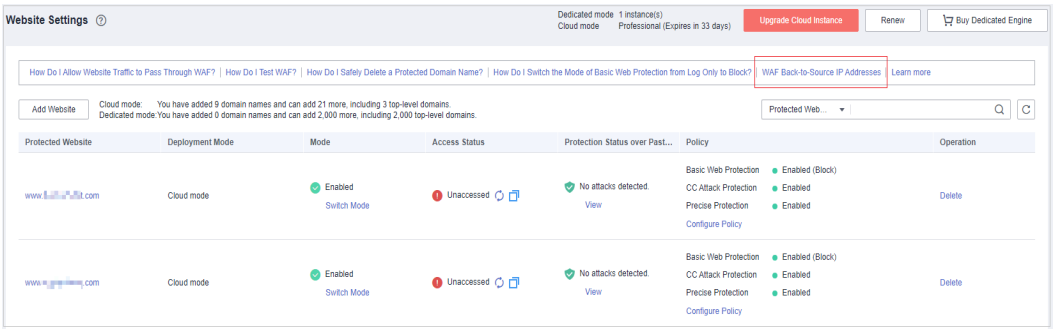
Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 En el panel de navegación, seleccione **Website Settings**.

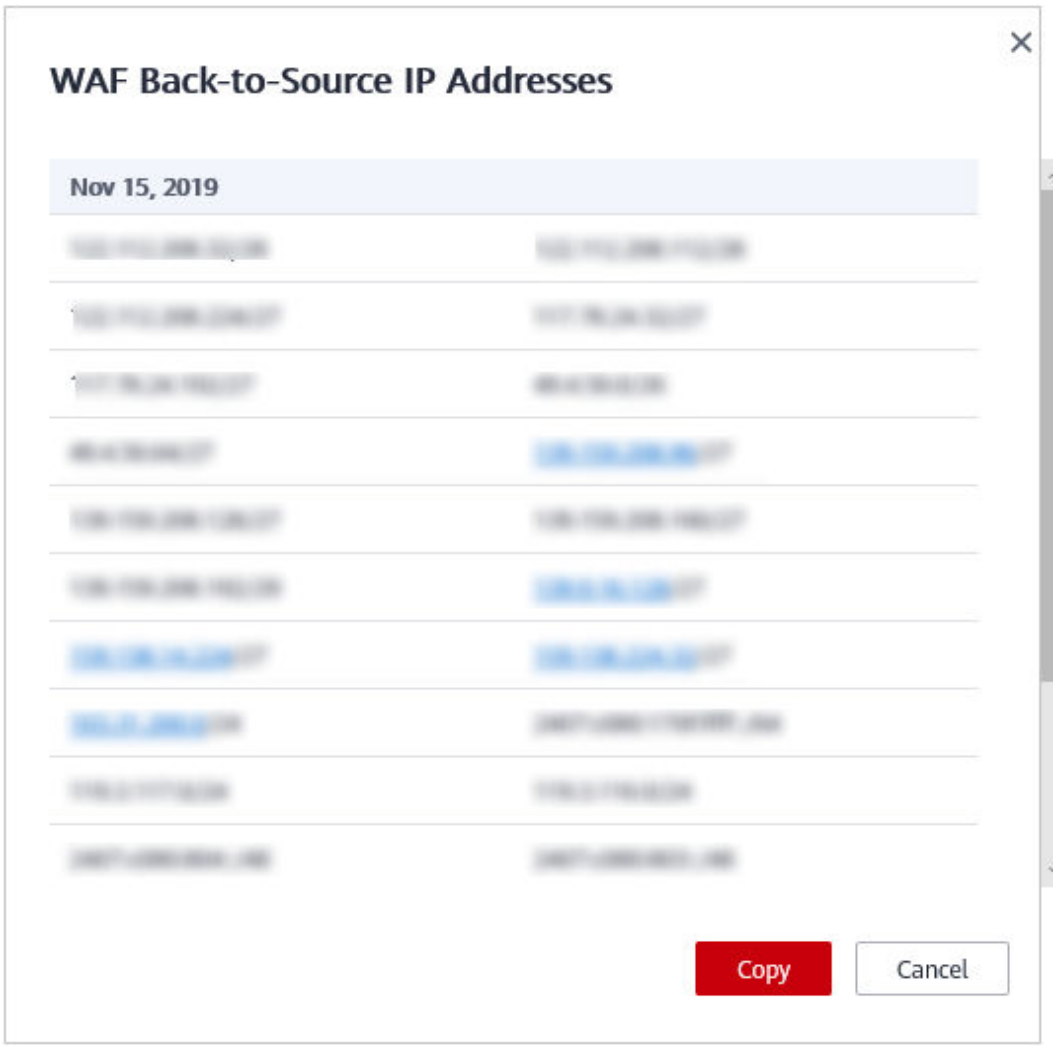
Paso 5 Encima de la lista de sitios web, haga clic en **WAF Back-to-Source IP Addresses**.

Figura 6-14 Direcciones IP de Back-to-Source de WAF



Paso 6 En el cuadro de diálogo mostrado, haga clic en **Copy** para copiar todas las direcciones.

Figura 6-15 Cuadro de diálogo de Direcciones IP de Back-to-Source de WAF



Paso 7 Abra el software de seguridad en el servidor de origen y agregue las direcciones IP copiadas a la lista blanca.

- Si sus servidores de origen se despliega en los ECS de Huawei Cloud, consulte **Incluir direcciones IP de WAF a la lista blanca en servidores de origen que se implementan en ECS de Huawei Cloud**.
- Si sus servidores de origen utilizan Huawei Cloud ELB, consulte **Incluir direcciones IP de WAF a la lista blanca en servidores de origen que utilizan Huawei Cloud ELB**.
- Si también usas la edición fuera de ruta Cloud Firewall (CFW) en Huawei Cloud, consulte **Adición de una regla de protección**.
- Si su sitio web se despliega en servidores de otros proveedores en la nube, incluya en la lista blanca las direcciones IP WAF en el grupo de seguridad correspondiente y las reglas de control de acceso.
- Si solo el software antivirus personal está instalado en el servidor de origen, el software no tiene la interfaz para incluir direcciones IP en la lista blanca. Si el servidor de origen proporciona servicios web externos, instale el software de seguridad empresarial o utilice el servicio de seguridad de Host Security Service (HSS) de Huawei Cloud para el servidor. Estos productos identifican los sockets de algunas direcciones IP con un gran

número de solicitudes y ocasionalmente desconectan las conexiones. Generalmente, las direcciones IP de WAF no están bloqueadas.

----Fin

Incluir direcciones IP de WAF a la lista blanca en servidores de origen que se implementan en ECS de Huawei Cloud

Si su servidor de origen se implementa en un ECS de Huawei Cloud, realice los siguientes pasos para configurar una regla de grupo de seguridad para permitir que solo las direcciones IP de origen WAF accedan al servidor de origen.

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda de la página y elija **Compute** > **Elastic Cloud Server**.

Paso 4 Localice la fila que contiene el ECS que aloja su sitio web. En la columna **Name/ID**, haga clic en el nombre de ECS para ir a la página de detalles de ECS.

Paso 5 Haga clic en la pestaña **Security Groups**. A continuación, haga clic en **Change Security Group**.

Paso 6 Haga clic en el nombre del grupo de seguridad para ver los detalles.

Paso 7 Haga clic en la pestaña **Inbound Rules** y haga clic en **Add Rule**. A continuación, especifique los parámetros en el cuadro de diálogo **Add Inbound Rule**. Para más detalles, consulte **Tabla 6-5**. **Figura 6-16** muestra un ejemplo.

Figura 6-16 Agregar regla de entrada

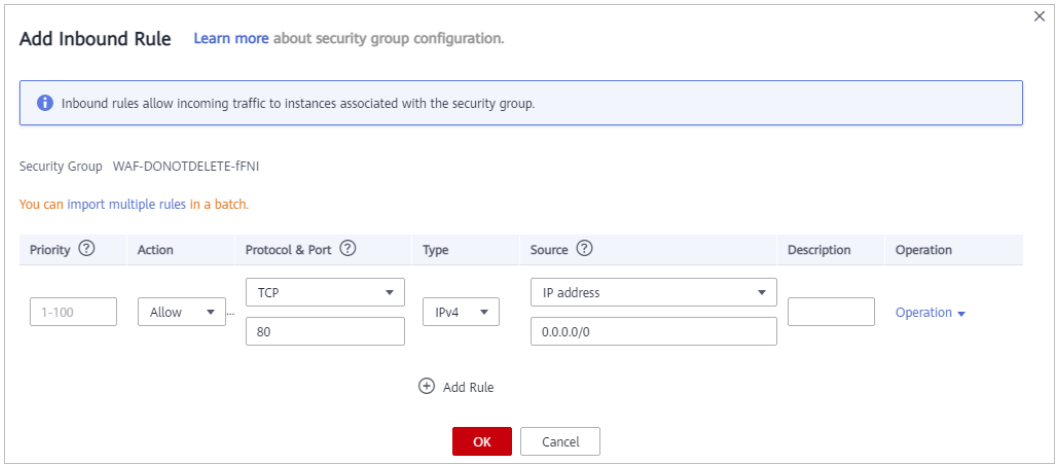


Tabla 6-5 Parámetros de regla de entrada

Parámetro	Descripción
Protocol & Port	Protocolo y puerto para los que la regla de grupo de seguridad tiene efecto. Si selecciona **TCP (Custom ports)**, introduzca el número de puerto del servidor de origen en el cuadro de texto situado debajo del cuadro TCP.
Source	Agregue todas las direcciones IP de origen WAF copiadas en **Paso 6** una por una. **NOTA** Una regla de entrada solo puede contener una dirección IP. Para configurar una regla de entrada para cada dirección IP, haga clic en **Add Rule** para agregar más reglas. Se puede configurar un máximo de 10 reglas.

Paso 8 Haga clic en **OK**.

A continuación, las reglas del grupo de seguridad permiten todo el tráfico entrante de las direcciones IP de back-to-source de WAF.

----Fin

Incluir direcciones IP de WAF a la lista blanca en servidores de origen que utilizan Huawei Cloud ELB

Si su servidor de origen se implementa en servidores de backend de un balanceador de carga de ELB de Huawei Cloud, realice los siguientes pasos para configurar una lista de control de acceso para permitir que solo las direcciones IP de WAF de origen accedan al servidor de origen.

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda de la página y elija **Networking** > **Elastic Load Balance**.

Paso 4 Localice el balanceador de carga que desee. En la columna **Listener**, haga clic en el nombre del agente de escucha para ir a la página de detalles.

Paso 5 En el cuadro de diálogo que aparece, seleccione **Whitelist** para **Access Control**.

1. Haga clic en **Create IP Address Group** y agregue las direcciones IP de instancia WAF dedicadas obtenidas en **Paso 6** al grupo que se está creando.
2. Seleccione el grupo de direcciones IP creado en **Paso 5.1** de la lista desplegable **IP Address Group**.

Paso 6 Haga clic en **OK**.

----Fin

6.7 ¿Cuál es la duración del tiempo de espera de la conexión de WAF? ¿Puedo establecer manualmente la duración del tiempo de espera?

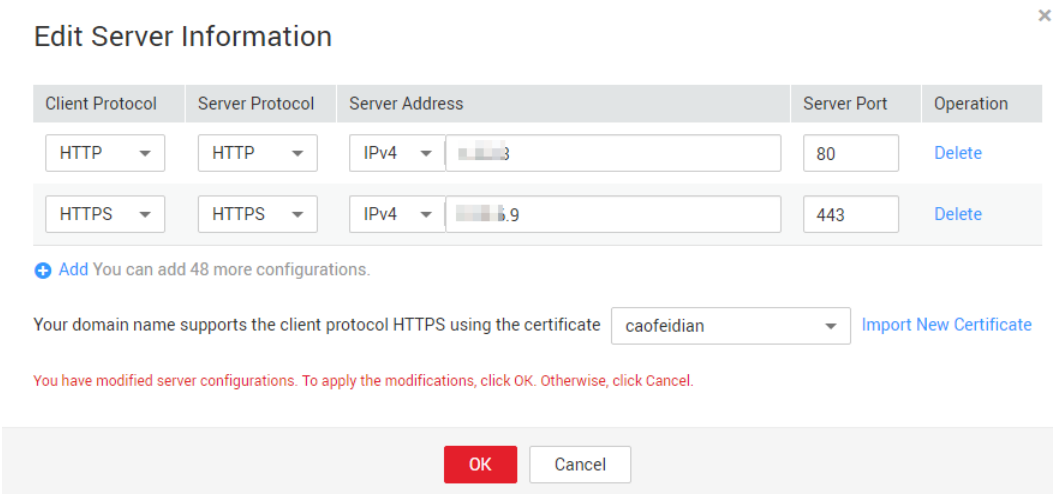
- El tiempo de espera predeterminado para las conexiones desde un navegador a WAF es de 120 segundos. El valor varía dependiendo de la configuración de su navegador y no se puede cambiar en la página de la consola WAF.
- El tiempo de espera predeterminado para las conexiones entre WAF y el servidor de origen es de 60 segundos. Puede personalizar un tiempo de espera en la consola WAF siempre que utilice una instancia WAF dedicada o WAF en la nube profesional o platino.

  En la página **Basic Information**, habilite **Timeout Settings** y haga clic en . A continuación, especifique **WAF-to-Server connection timeout (s)**, **Read timeout (s)** y **Write timeout (s)** y haga clic en para guardar la configuración.

6.8 ¿Cómo resuelvo el problema de los tiempos de redirección excesivos?

Después de conectar un nombre de dominio a WAF, si el sistema muestra un mensaje que indica que hay tiempos de redirección excesivos cuando un usuario solicita acceder al nombre de dominio de destino, la posible causa es que ha configurado la redirección forzada de HTTP a HTTPS en el servidor backend y el reenvío de HTTPS (protocolo de cliente) a HTTP (protocolo de servidor) se configura en WAF, WAF se ve obligado a redirigir las solicitudes de los usuarios, causando un bucle infinito. Puede configurar dos piezas de información del servidor acerca de HTTP (protocolo de cliente) a HTTP (protocolo de servidor) y HTTPS (protocolo de cliente) a HTTPS (protocolo de servidor). Para obtener más información, consulte **Edición de información de servidor**. **Figura 6-17** muestra las configuraciones de servidor completadas.

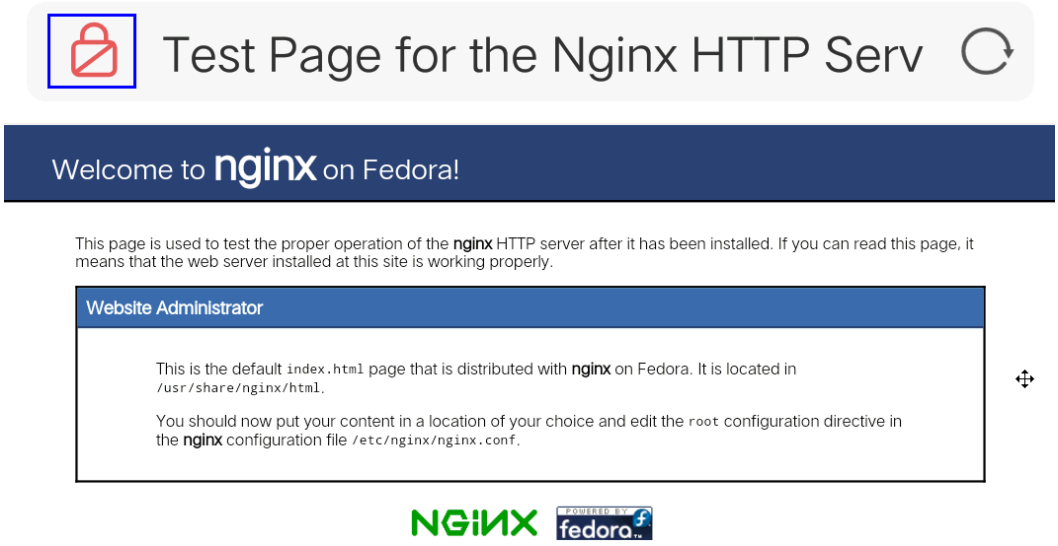
Figura 6-17 Ejemplo de configuración



6.9 ¿Por qué se rechazan las solicitudes HTTPS en algunos teléfonos móviles?

Si sus visitantes reciben una página similar a la de **Figura 6-18** cuando intentan acceder a su sitio web a través de un teléfono móvil, se carga una cadena de certificados incompleta cuando conecta el sitio web a WAF. Rectificar la falta haciendo referencia a **¿Cómo soluciono una cadena de certificados incompleta?**

Figura 6-18 Error en el acceso



6.10 ¿Cómo soluciono una cadena de certificados incompleta?

Si el certificado proporcionado por la entidad emisora de certificados no se encuentra en el almacén de confianza integrado de la plataforma y la cadena de certificados no tiene una entidad emisora de certificados, el certificado está incompleto. Si utiliza el certificado incompleto para acceder al sitio web correspondiente al nombre de dominio protegido, el acceso fallará.

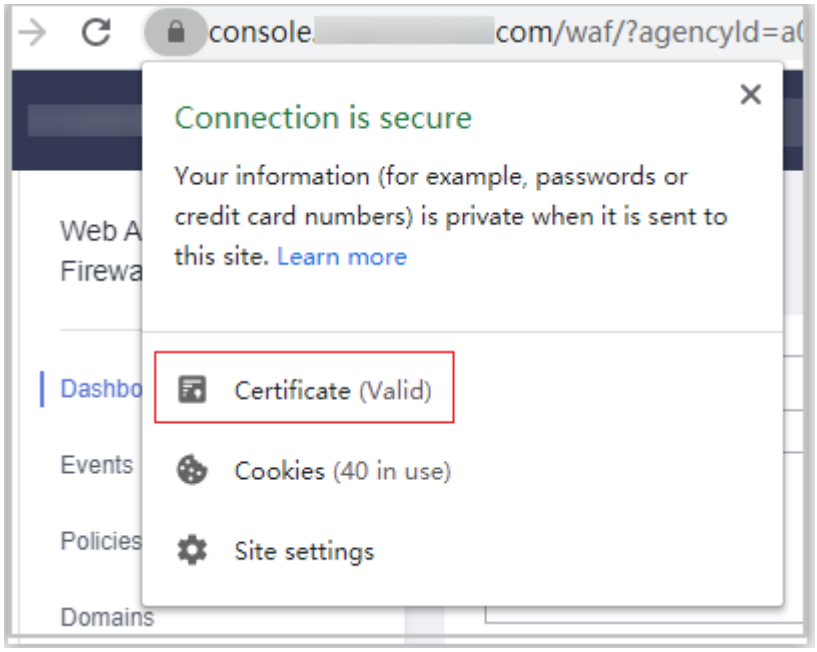
Utilice cualquiera de los siguientes métodos para solucionarlo:

- Construya manualmente una cadena de certificados completa y cargue el certificado. (Esta función estará disponible próximamente.)
- Suba el certificado correcto.

La última versión de Google Chrome admite la verificación automática de la cadena de confianza. A continuación se describe cómo crear manualmente una cadena de certificados completa (usando un certificado de Huawei Cloud como ejemplo):

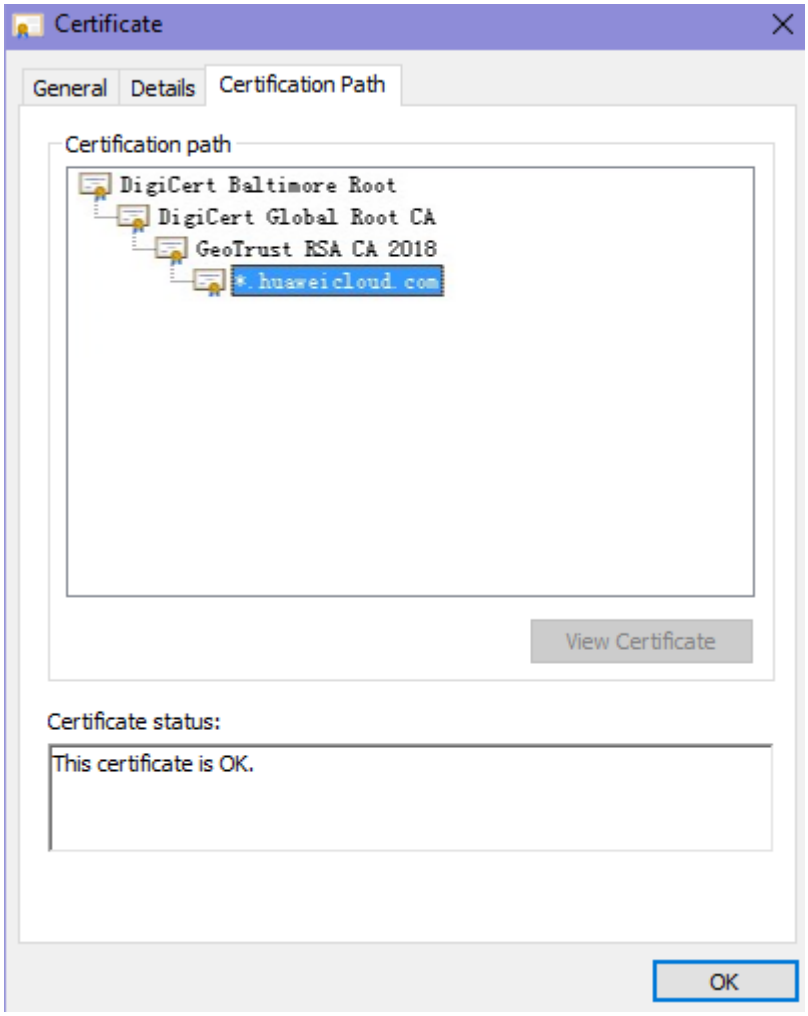
Paso 1 Compruebe el certificado. Haga clic en padlock en la barra de direcciones para ver el estado del certificado.

Figura 6-19 Visualización del certificado



Paso 2 Compruebe la cadena de certificados. Haga clic en **Certificate**. Seleccione la pestaña **Certificate Path** y, a continuación, haga clic en el nombre del certificado para ver el estado del certificado. **Figura 6-20** muestra un ejemplo.

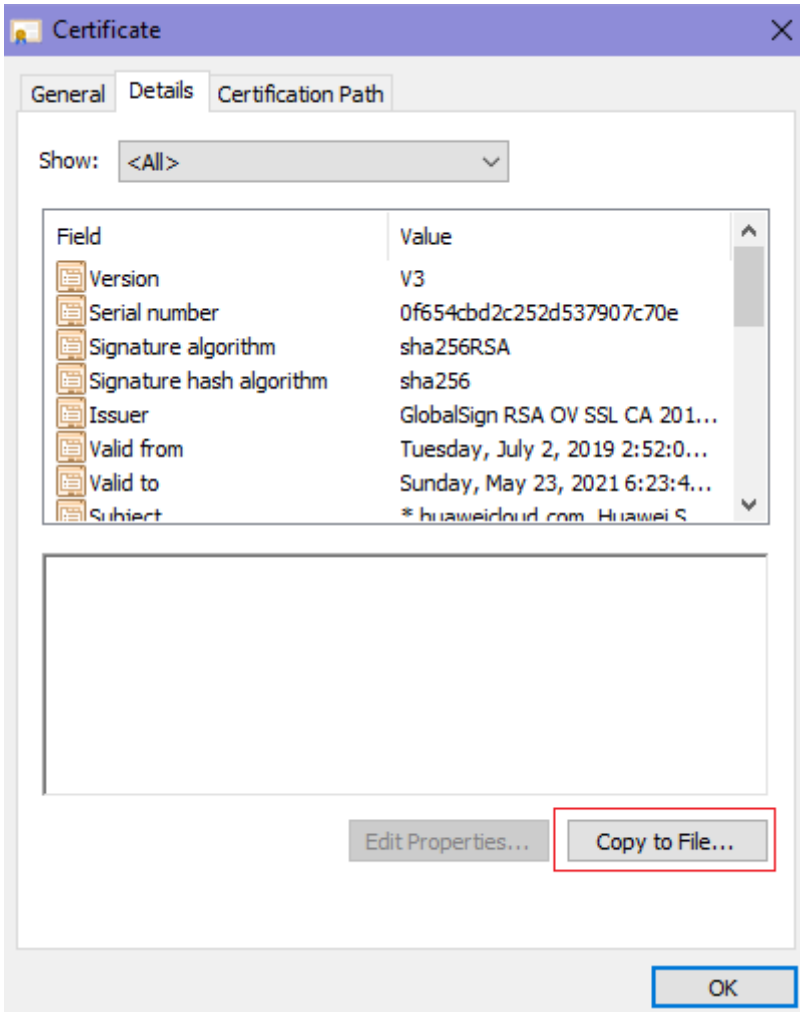
Figura 6-20 Visualización de la cadena de certificados



Paso 3 Guarde los certificados en el PC local uno por uno.

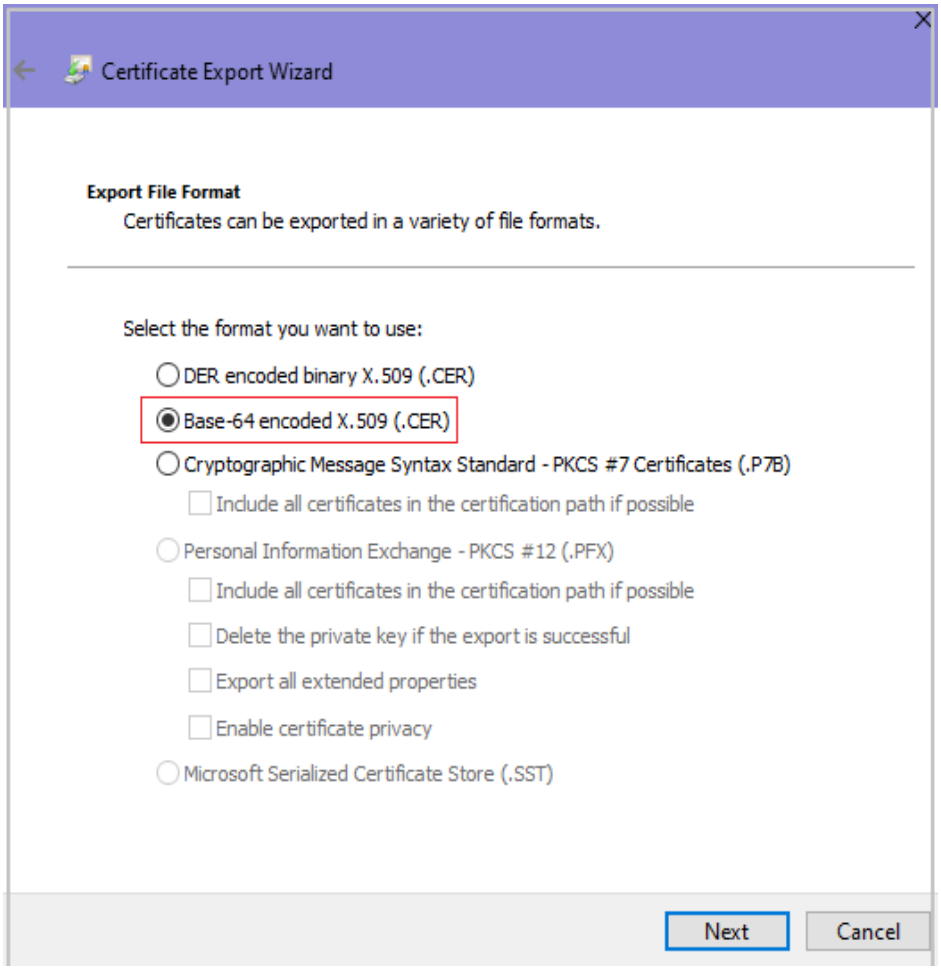
1. Seleccione el nombre del certificado y haga clic en la pestaña **Details**. **Figura 6-21** muestra un ejemplo.

Figura 6-21 Detalles



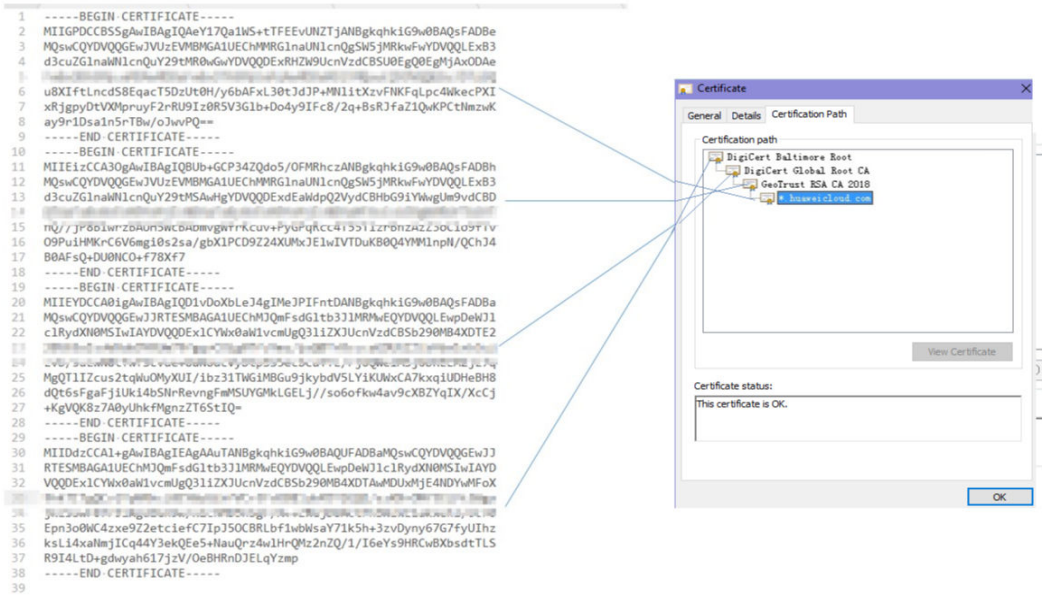
2. Haga clic en **Copy to File** y, a continuación, haga clic en **Next** según se le indique.
3. Seleccione **Base-64 encoded X.509 (.CER)** y haga clic en **Next**. Figura 6-22 muestra un ejemplo.

Figura 6-22 Asistente para exportación de certificados



Paso 4 Reconstruir el certificado. Después de exportar todos los certificados al PC local, abra el archivo de certificado en el Bloc de notas y vuelva a crear el certificado de acuerdo con la secuencia mostrada en **Figura 6-23**.

Figura 6-23 Reconstrucción de certificados



Paso 5 Vuelva a cargar el certificado.

----Fin

6.11 ¿Por qué mi certificado no coincide con la clave?

Después de cargar un certificado HTTPS en la consola AAD o WAF, se muestra un mensaje que indica que el certificado y la clave no coinciden.

Solución

Causa posible	Cómo arreglar
El certificado cargado no coincide con la clave privada cargada.	1. Ejecute los siguientes comandos para comprobar los valores hash MD5 del archivo de certificado y clave privada: **openssl x509 -noout -modulus -in** *<certificate file>*|**openssl md5** **openssl rsa -noout -modulus -in** *<private key file>*|**openssl md5** 2. Compruebe si los valores MD5 del certificado y del archivo de clave privada son los mismos. Si son diferentes, el archivo de certificado y el archivo de clave privada están asociados con nombres de dominio diferentes y el contenido del certificado no coincide con el del archivo de clave privada. 3. Si el certificado no coincide con el archivo de clave privada, cargue el certificado y el archivo de clave privada correctos.

Causa posible	Cómo arreglar
Formato de clave privada RSA incorrecto	1. Ejecute el siguiente comando para generar una nueva clave privada: `openssl rsa -in <private key file> -out <New private key file>` 2. Suba la clave privada de nuevo.

Otras operaciones

- **¿Cómo soluciono una cadena de certificados incompleta?**
- **¿Por qué se rechazan las solicitudes HTTPS en algunos teléfonos móviles?**

6.12 ¿Por qué estoy viendo el código de error 418?

Si la solicitud contiene carga maliciosa y es interceptada por WAF, el error 418 se notifica cuando se accede al nombre de dominio protegido por WAF. Puede ver los registros de protección WAF para ver la causa. Para obtener más información acerca de los registros de eventos, consulte **Consulta de registros de eventos de protección**.

- Si confirma que la solicitud es una solicitud de servicio normal, puede manejar la falsa alarma para evitar la repetición del evento de protección.

  Para obtener más información, consulte **Manejo de alarmas falsas**.
- Si confirma que el evento de protección no es una falsa alarma, su sitio web es atacado y la solicitud maliciosa es bloqueada por WAF.

6.13 ¿Por qué estoy viendo el código de error 523?

Si una solicitud ha pasado a través de WAF cuatro veces, WAF bloquea la solicitud para evitar un bucle infinito. En este caso, se devuelve el código de error 523.

Utilice los métodos siguientes para resolver el problema:

- Dirija la solicitud al servidor DNS interno para que la solicitud pueda omitir la red pública.

  Utilice Huawei Cloud DNS como ejemplo. Para obtener más información, consulte **Zonas privadas**.
- Configure el archivo hosts del servidor de origen.

  A continuación se utiliza el sistema operativo Windows como ejemplo.

  a. Utilice un editor de texto para abrir el archivo **hosts**. Generalmente, el archivo **hosts** se almacena en el directorio **C:\Windows\System32\drivers\etc**.

  b. Agregue un registro sobre la dirección IP del servidor de origen al archivo hosts.

  c. Guarde la modificación y salga.

6.14 ¿Por qué la página de inicio de sesión del sitio web se actualiza continuamente después de que un nombre de dominio se conecta a WAF?

Después de conectar el nombre de dominio de su sitio web a WAF, todas las solicitudes de sitio web se reenvían a WAF primero. A continuación, WAF reenvía solo el tráfico normal al servidor de origen. Para cada solicitud del cliente, WAF genera un identificador basado en la dirección IP de acceso y el agente de usuario. WAF tiene múltiples direcciones IP de back-to-source que se asignarán aleatoriamente. Cuando la dirección IP de retorno a origen cambia, el identificador de la solicitud cambia en consecuencia. Como resultado, la sesión es eliminada directamente por WAF, y la página de inicio de sesión se sigue actualizando. Para evitar este problema, se recomienda utilizar cookies de sesión para mantener la sesión persistente.

6.15 ¿Por qué la página solicitada responde lentamente después de configurar la política de reenvío de HTTP?

En este caso, agregue dos políticas de reenvío. Uno es el reenvío HTTP a HTTP, y el otro es el reenvío HTTPS a HTTPS.

Para obtener más información sobre cómo configurar una regla de reenvío, consulte **¿Cómo resuelvo el problema de los tiempos de redirección excesivos?**

6.16 ¿Cómo puedo cargar archivos después de que el sitio web esté conectado a WAF?

Después de que su sitio web esté conectado a WAF, puede cargar un archivo de no más de 10 GB cada vez.

Para cargar un archivo de más de 10 GB, cargue el archivo a través de cualquiera de las siguientes opciones:

- Dirección IP
- Servidor web separado que no está protegido por WAF
- Servidor FTP

6.17 ¿Qué hago si el protocolo no es compatible y el cliente y el servidor no son compatibles con las versiones comunes de protocolo SSL o conjuntos de cifrado?

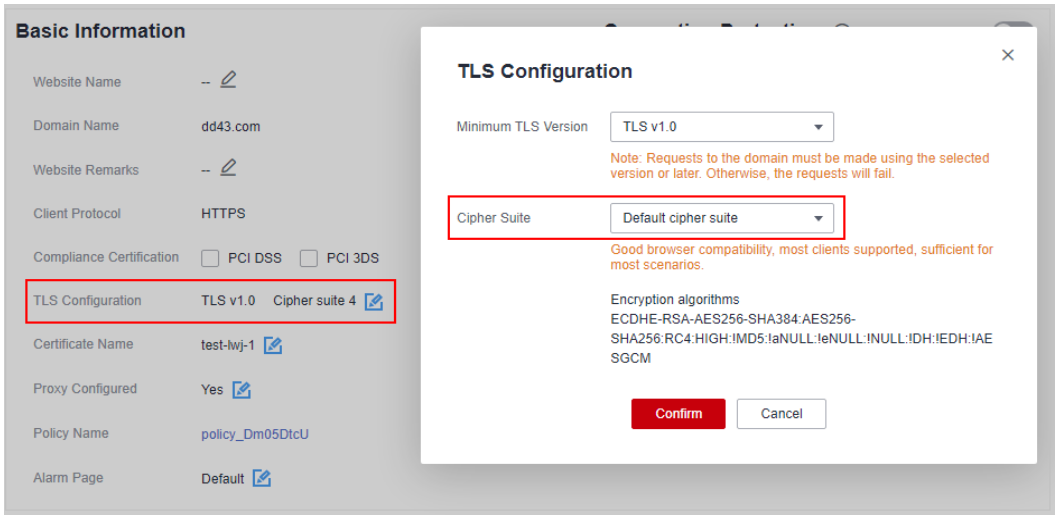
Síntoma

Después de conectar un nombre de dominio a WAF, no se puede acceder al sitio web. Se muestra un mensaje que indica que el protocolo no es compatible. El cliente y el servidor no son compatibles con las versiones comunes de protocolo SSL o conjuntos de cifrado.

Solución

Seleccione el conjunto de cifrado predeterminado para **Cipher Suite** en el cuadro de diálogo **TLS Configuration**. Para obtener más información, consulte **Configuración de comprobación de certificación PCI DSS/3DS y versión TLS**.

Figura 6-24 Configuración de TLS



6.18 ¿Por qué no puedo acceder a la página del motor dedicado?

Síntoma

Mensaje de error "Failed to request IAM. Please check the current user's IAM permissions." se muestra cuando un usuario intentó acceder a la página **Dedicate Engine** en la sección **Instance Management**.

Causa posible

El permiso **IAM ReadOnly** no se concede a la cuenta de inicio de sesión.

Solución

Asigne el permiso **IAM ReadOnly** a su cuenta. Para obtener más información, consulte **Asignar permisos a un usuario de IAM**.

7 Configuración de la regla de protección

7.1 Protección básica de Web

7.1.1 ¿Cómo cambio el modo de protección de web básica de solo registro a bloqueo?

Esta sección de preguntas frecuentes le guía para cambiar el modo de protección de web básica a **Block**.

Realice las siguientes operaciones:

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Click  in the upper left corner of the management console and select a region or project.

Paso 3 Haga clic en  en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 En el panel de navegación, seleccione **Website Settings**.

Paso 5 En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.

Paso 6 En el área de configuración de **Basic Web Protection**, establezca **Mode** en **Block**.

AVISO

Log only y **Block** son meramente modos de protección de web básica. La protección contra ataques CC y la protección precisa tienen sus propias acciones de protección.

----Fin

7.1.2 ¿Qué niveles de protección se pueden establecer para la protección web básica?

WAF proporciona tres niveles básicos de protección web: **Low**, **Medium**, y **High**. La opción predeterminada es **Medium**. Para obtener más información, consulte **Tabla 7-1**.

Tabla 7-1 Niveles de protección

Nivel de protección	Descripción
Low	WAF solo bloquea las solicitudes con firmas de ataque obvias. Si se reporta un gran número de falsas alarmas, se recomienda **Low**.
Medium	El nivel predeterminado es **Medium**, que cumple con la mayoría de los requisitos de protección web.
High	En este nivel, WAF proporciona la mejor protección granular y puede interceptar ataques con características complejas de bypass, como ciberataques Jolokia, detección de vulnerabilidades de interfaz de puerta de enlace común (CGI) y ataques de inyección de Druid SQL. Se recomienda observar sus cargas de trabajo durante un período de tiempo antes de configurar una regla de enmascaramiento de falsas alarmas y luego seleccionar **High** para que WAF pueda defenderse contra más ataques con un efecto mínimo en las solicitudes normales.

Para obtener más información acerca de la protección web básica, consulte **Configuración de reglas básicas de protección web**.

7.2 Reglas de protección contra ataques CC

7.2.1 ¿Cuál es la tasa máxima de protección contra ataques CC?

Depende de la edición WAF que esté usando. Para obtener más información, consulte **Tabla 7-2**.

Tabla 7-2 Velocidad máxima de protección contra ataques CC

Edición	Tasa máxima de solicitudes de servicio normales	Velocidad máxima de protección contra ataques CC
Estándar	● 2,000 QPS ● Conexiones WAF a servidor: 6,000 por nombre de dominio	100,000QPS

Edición	Tasa máxima de solicitudes de servicio normales	Velocidad máxima de protección contra ataques CC
Profesional	● Solicitudes de servicio: 5,000 QPS ● Conexiones WAF a servidor: 6,000 por nombre de dominio	300,000QPS
Platino	● Solicitudes de servicio: 10,000 QPS ● Conexiones WAF a servidor: 6,000 por nombre de dominio	1,000,000QPS
WAF dedicado	● Especificaciones: WI-500. Rendimiento referenciado: – Rendimiento: 500 Mbit/s; QPS: 10,000 – Conexiones WAF-a-servidor soportadas: 60,000 por instancia o 5,000 por dominio ● Especificaciones: WI-100. Rendimiento referenciado: – Rendimiento: 100 Mbit/s; QPS: 2,000 – Conexiones WAF-a-servidor soportadas: 60,000 por instancia o 5,000 por dominio	500,000QPS

7.2.2 ¿Cómo configuro una regla de protección contra ataques CC?

Cuando una interfaz de servicio está bajo un ataque de HTTP flood, puede establecer una regla de protección contra ataques CC en la consola WAF para aliviar la presión del servicio.

WAF proporciona la siguiente configuración para una regla de protección contra ataques CC:

- Número de solicitudes permitidas de un visitante web en un período especificado
- Identificación de los visitantes de la web basada en la dirección IP, la cookie o el campo de referencia.
- Acción cuando se alcanza el límite máximo, como el código de **Block** o **Verification code**

Para obtener más información, consulte **Configuración de reglas de protección contra ataques de CC**.

7.2.3 ¿Cuándo se utiliza la cookie para identificar a los usuarios?

Durante la configuración de una regla de protección contra ataques CC, si las direcciones IP no pueden identificar a los usuarios con precisión, por ejemplo, cuando muchos usuarios comparten una dirección IP de salida, utilice Cookie para identificar a los usuarios.

Si la cookie contiene valores clave, como el valor de sesión, de los usuarios, el valor clave puede utilizarse como base para identificar a los usuarios.

AVISO

Es posible que no se admita la identificación basada en cookies si la solicitud de URL configurada en una política de protección contra ataques de CC es una API invocada por otro servicio.

7.2.4 ¿Cuáles son las diferencias entre Rate Limit y Allowable Frequency en una regla CC?

En una regla de protección contra ataques de CC, **Rate Limit** especifica las solicitudes máximas que un visitante del sitio web puede iniciar dentro del período configurado. Si se ha alcanzado el límite de velocidad configurado, WAF responderá de acuerdo con la acción de protección configurada. Por ejemplo, si configura **Rate Limit** en **10 requests** en un plazo de **60 seconds** y **Protective Action** para **Block**, se permite un máximo de 10 solicitudes en un plazo de 60 segundos. Una vez que el visitante del sitio web inicia más de 10 solicitudes en 60 segundos, WAF bloquea directamente al visitante para que no acceda a la URL solicitada.

Si selecciona **Advanced** para **Mode** y **Block dynamically** para **Protective Action**, configure **Rate Limit** y **Allowable Frequency**.

WAF bloquea las solicitudes que activan la regla basándose en **Rate Limit** primero. A continuación, en el siguiente período de límite de velocidad, WAF bloquea las solicitudes que activan la regla en función de **Allowable Frequency** que haya configurado. Si se activa el bloqueo y **Allowable Frequency** es **0**, se bloquean todas las solicitudes que cumplan las condiciones de la regla en el siguiente período.

Diferencias

- El período límite de tasa de **Allowable Frequency** es el mismo que el del **Rate Limit**.
- **Allowable Frequency** es menor o igual que **Rate Limit**, y **Allowable Frequency** puede ser **0**.

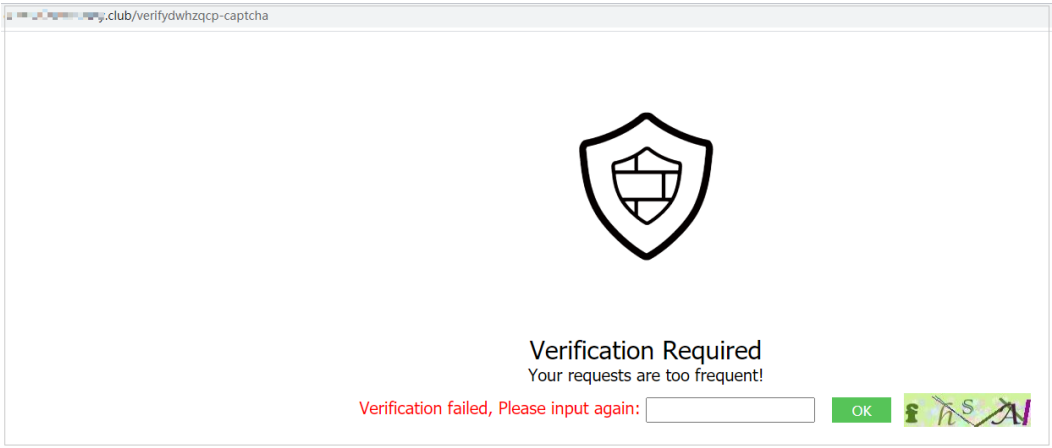
Para obtener más información, consulte **Configuración de una regla de protección contra ataque CC**.

7.2.5 ¿Por qué no se puede actualizar el código de verificación cuando el código de verificación está configurado en una regla de protección contra ataques CC?

Síntoma

Después de agregar una regla de ataque CC con **Protective Action** establecida en **Verification code** en WAF, el código de verificación no se puede actualizar y la verificación falla cuando se solicita el sitio web. **Figura 7-1** muestra un ejemplo.

Figura 7-1 Error de verificación



Después de configurar **Verification code**, se requiere un código de verificación cuando el número de solicitudes excede el límite máximo dentro de un período especificado. Al completar la verificación, se elimina el límite de acceso.

Para obtener más información, consulte **Configuración de reglas de protección contra ataques de CC**.

Causas posibles

Cuando un nombre de dominio está conectado tanto a WAF como a Content Delivery Network (CDN), y el valor para **Path** de la regla de protección contra ataques CC contiene una página estática, la página estática se almacena en caché por CDN. Como resultado, el código de verificación no se puede actualizar y la verificación falla.

Sugerencias sobre el manejo

En CDN, configure las políticas de caché para omitir la caché de direcciones URL estáticas.

AVISO

Una vez completada la configuración, las poilíticas de caché configuradas tardan de 3 a 5 minutos en aplicarse.

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en en la esquina superior izquierda de la página, en **Storage** y seleccione **CDN**.

Paso 4 En el panel de navegación, seleccione **Domains**.

Paso 5 En la columna **Domain Name**, haga clic en el nombre del dominio de destino.

Paso 6 Haga clic en la pestaña **Cache Settings** y haga clic en **Edit**.

Paso 7 En el cuadro de diálogo **Configure Cache Policy** que se muestra, haga clic en **Add** debajo de la lista de directivas y agregue dos reglas de política de caché haciendo referencia a **Tabla 7-3**. **Figura 7-2** muestra un ejemplo.

Figura 7-2 Configurar política de caché

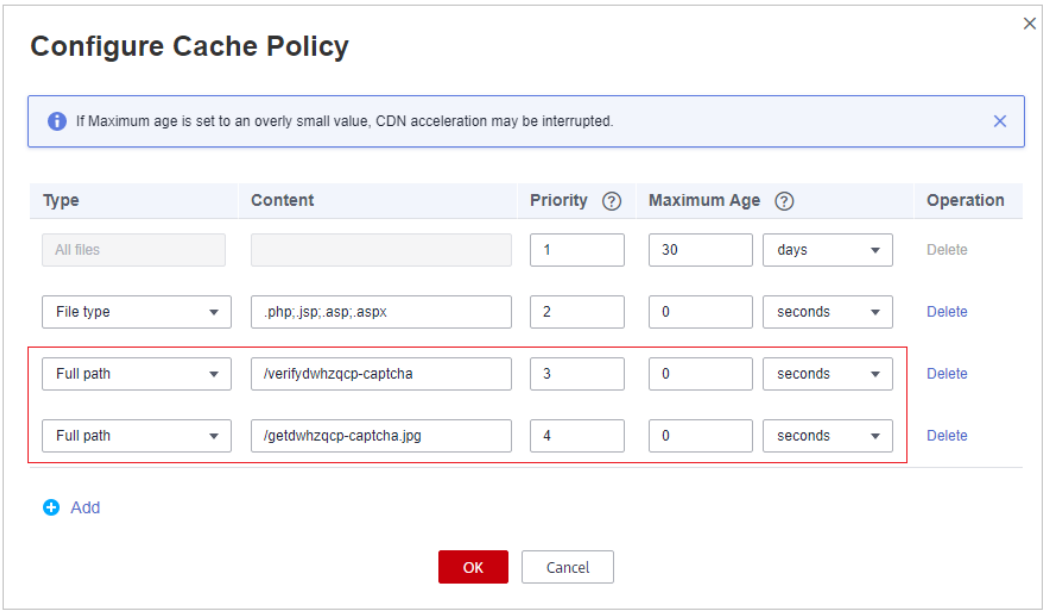
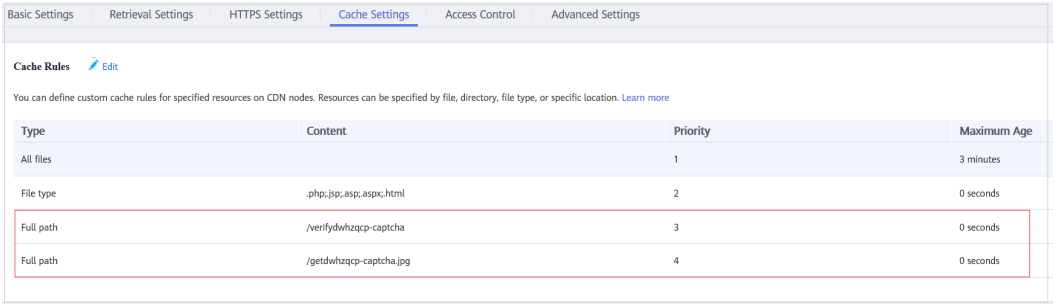


Tabla 7-3 Parámetros para configurar la política de caché de URL estática

Parámetro	Descripción de configuración
Type	Seleccione **Full path**.
Content	El contenido de las dos políticas que se agregarán es el siguiente: ● **/verifydwhzqcp-captcha** ● **/getdwhzqcp-captcha.jpg**
Priority	Establezca las dos políticas con la prioridad más alta.
Maximum Age	Establezca este parámetro en **0 seconds**, lo que indica que las URL estáticas no están almacenadas en caché.

Paso 8 Haga clic en **OK**. **Figura 7-3** muestra un ejemplo.

Figura 7-3 Políticas de caché configuradas



Una vez completada la configuración, las poilíticas de caché configuradas tardan de 3 a 5 minutos en aplicarse.

----Fin

7.3 Reglas de protección precisas

7.3.1 ¿Puede una regla de protección precisa entrar en vigor en un período especificado?

WAF no permite que las reglas de acceso de protección precisas entren en vigor en un período especificado.

Puede establecer reglas de protección precisas para filtrar las solicitudes de acceso basadas en una combinación de campos HTTP comunes (como dirección IP, ruta, referente, agente de usuario y parámetros) para permitir o bloquear las solicitudes que coincidan con las condiciones.

Para obtener más información acerca de cómo configurar, consulte **Configuración de reglas de protección precisas**.

7.4 Lista negra y lista blanca de direcciones IP

7.4.1 ¿Puedo agregar direcciones IP por lotes a una lista negra o una regla de lista blanca?

Sí. Puede seleccionar un grupo de direcciones al configurar una regla de lista blanca o lista negra. De esta manera, las solicitudes de esas direcciones IP incluidas en el grupo de direcciones serán bloqueadas, permitidas o registradas solamente. También puede configurar una regla de lista negra o blanca para cada dirección IP o intervalo de direcciones IP.

Para obtener más información, consulte **Configuración de una regla de lista negra o de lista blanca**.

7.4.2 ¿Puedo importar o exportar una lista negra o una lista blanca en o desde WAF?

WAF admite la importación de listas negras o blancas de direcciones IP. Para ello, seleccione **Address group** para **IP Address/Range/Group** cuando agregue una regla de lista negra o lista blanca. WAF no admite la exportación de listas negras y listas blancas de direcciones IP.

Para obtener más información, consulte **Configuración de reglas de listas negras y listas blancas**.

7.4.3 ¿Cómo puedo bloquear direcciones IP anormales?

Puede incluir en la lista negra una dirección IP anormal. WAF bloquea directamente todas las solicitudes de la dirección IP en la lista negra.

Para incluir una dirección IP en la lista negra, realice los siguientes pasos:

Paso 1 **Inicie sesión en la consola de gestión**.

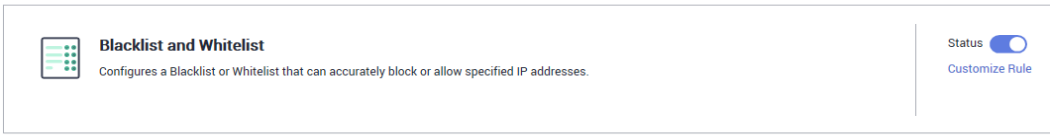
Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.

Paso 5 En el área de configuración de **Blacklist and Whitelist**, cambie **Status** según sea necesario y haga clic en **Customize Rule**.

Figura 7-4 Área de configuración de listas negras y blancas



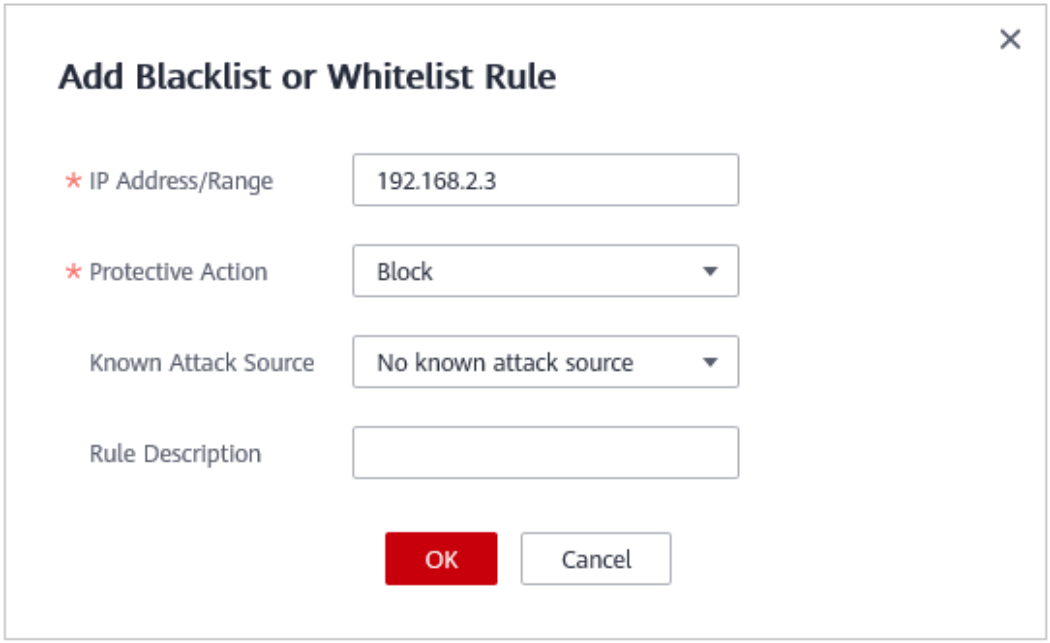
Paso 6 En la esquina superior izquierda de la página **Blacklist and Whitelist**, haga clic en **Add Rule**.

Paso 7 En el cuadro de diálogo que se muestra, agregue una regla de lista negra o lista blanca. **Figura 7-5** muestra un ejemplo.

NOTA

- Si selecciona **Log only** para **Protective Action** para una dirección IP, WAF solo identifica y registra las solicitudes de la dirección IP.
- Otras direcciones IP se evalúan basándose en otras reglas de protección WAF configuradas.

Figura 7-5 Adición de una regla de lista negra o lista blanca



Paso 8 Haga clic en **OK**. A continuación, puede ver la regla agregada en la lista de reglas de listas negras y listas blancas.

Figura 7-6 Reglas de la lista negra o de la lista blanca

IP Address or Segment	Protective Action	Rule Status	Added	Rule Description	Operation
192.168.2.3	Block	Enabled	2020/03/30 14:25:24 GMT+08:00	--	Disable Delete Modify

- Para deshabilitar una regla, haga clic en **Disable** en la columna **Operation** de la regla. El **Rule Status** predeterminado es **Enabled**.
- Para modificar una regla, haga clic en **Modify** en la fila que contiene la regla.
- Para eliminar una regla, haga clic en **Delete** en la fila que contiene la regla.

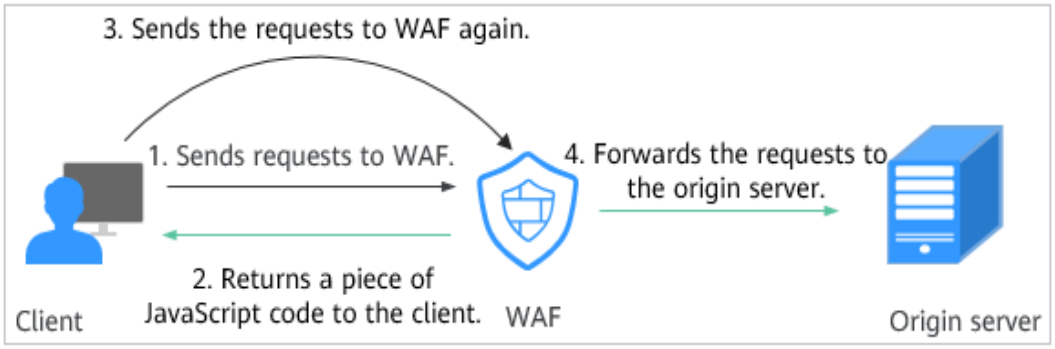
----Fin

7.5 Protección Anti-Crawler

7.5.1 ¿Por qué no se puede cargar la página solicitada después de activar el Anti-Crawler de JavaScript?

Después de activar el JavaScript anti-crawler, WAF devuelve un fragmento de código JavaScript al cliente cuando el cliente envía una solicitud. Si el cliente envía una solicitud normal al sitio web, activada por el código JavaScript recibido, el cliente enviará automáticamente la solicitud a WAF de nuevo. A continuación, WAF reenvía la solicitud al servidor de origen. Este proceso se llama verificación de JavaScript. **Figura 7-7** muestra cómo funciona la verificación de JavaScript.

Figura 7-7 Proceso de detección de anticrawler de JavaScript



- Si el cliente es un rastreador, no puede ser activado por el código JavaScript recibido y no enviará una solicitud a WAF de nuevo. El cliente falla la autenticación de JavaScript.
- Si un rastreador de cliente fabrica una solicitud de autenticación WAF y envía la solicitud a WAF, WAF bloqueará la solicitud. El cliente falla la autenticación de JavaScript.

AVISO

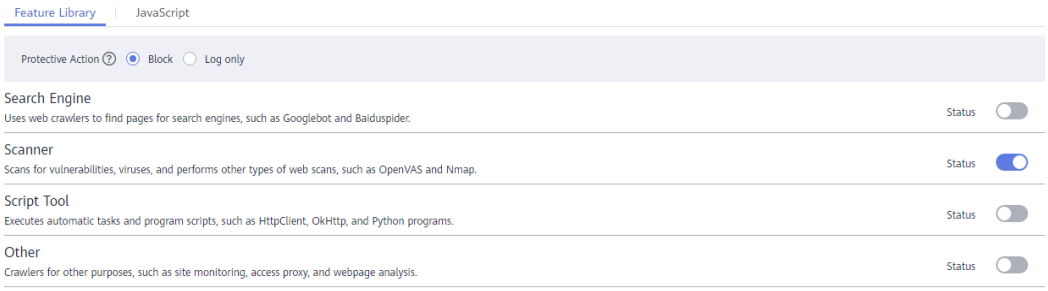
- Para habilitar la protección anti-exploración JavaScript el navegador del cliente debe tener JavaScript y cookies habilitados.
- Si el cliente no cumple con los requisitos anteriores, sólo se pueden realizar las etapas 1 y 2. En este caso, la solicitud del cliente no puede obtener la página.

Compruebe sus servicios. Si se puede acceder a su sitio web por otros medios, excepto por un navegador, desactive la protección anti-explotación de JavaScript.

7.5.2 ¿Hay algún impacto en la velocidad de carga del sitio web si se habilita la verificación de otros rastreadores en Anti-Crawler?

Si ha habilitado **Other** al configurar el **Feature Library** de protección de anti-crawler, WAF detecta los rastreadores para diversos fines, como la supervisión de sitios web, el proxy de acceso y el análisis de páginas web. La habilitación de esta opción no afecta a las visitas a la página web ni a la velocidad de navegación de la página web.

Figura 7-8 Habilitación de **Other**.

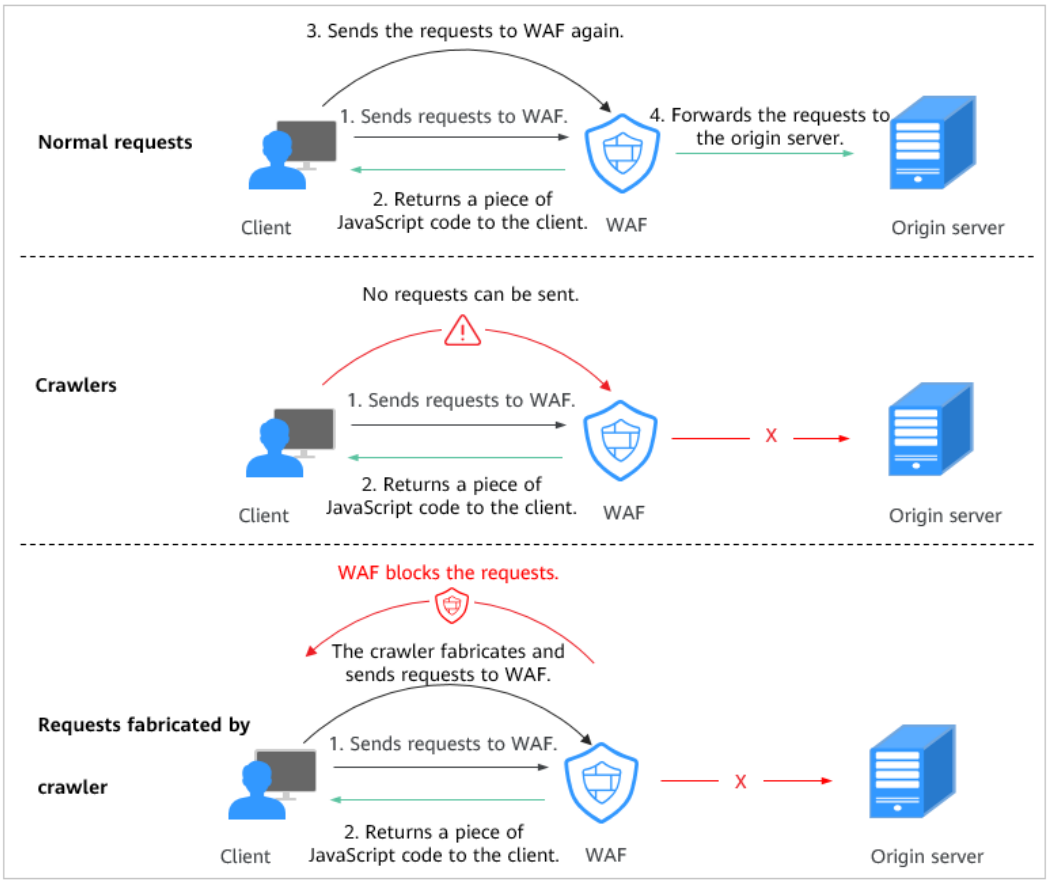


Para obtener más información, consulte **Configuración de reglas de anticrawler**.

7.5.3 ¿Cómo funciona la Detección Anti-Crawler JavaScript?

Figura 7-9 muestra cómo funciona la detección anti-crawler de JavaScript, que incluye desafíos de JavaScript (paso 1 y paso 2) y autenticación de JavaScript (paso 3).

Figura 7-9 Proceso de protección Anti-Crawler de JavaScript

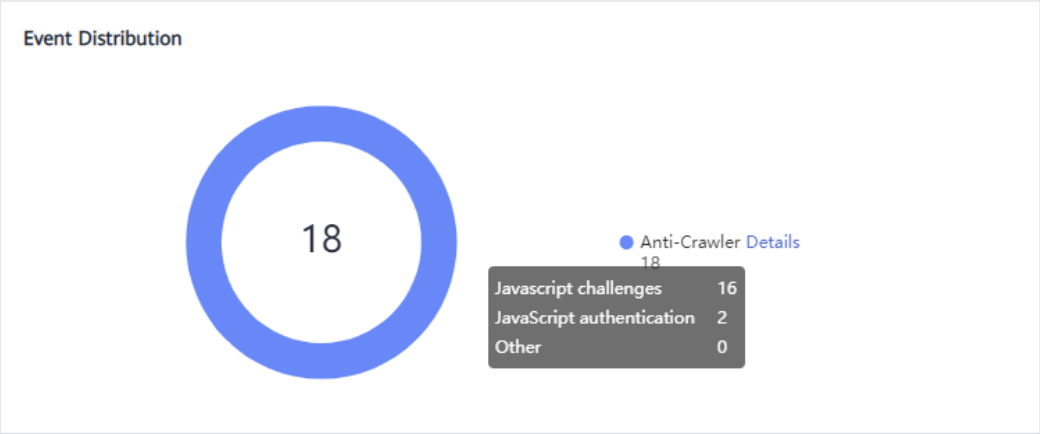


Después de activar el JavaScript anti-crawler, WAF devuelve un fragmento de código JavaScript al cliente cuando el cliente envía una solicitud.

- Si el cliente envía una solicitud normal al sitio web, activada por el código JavaScript recibido, el cliente enviará automáticamente la solicitud a WAF de nuevo. A continuación, WAF reenvía la solicitud al servidor de origen. Este proceso se llama verificación de JavaScript.
- Si el cliente es un rastreador, no puede ser activado por el código JavaScript recibido y no enviará una solicitud a WAF de nuevo. El cliente falla la autenticación de JavaScript.
- Si un rastreador de cliente fabrica una solicitud de autenticación WAF y envía la solicitud a WAF, WAF bloqueará la solicitud. El cliente falla la autenticación de JavaScript.

Mediante la recopilación de estadísticas sobre el número de respuestas de desafío y autenticación de JavaScript el sistema calcula cuántas solicitudes defiende el anti-explotación JavaScript. Como se muestra en **Figura 7-10**, el anti-crawler de JavaScript registra 18 eventos, 16 de los cuales son respuestas de desafío de JavaScript, 2 de los cuales son respuestas de autenticación de JavaScript. El número de **Other** son las solicitudes de autenticación WAF fabricadas por el rastreador.

Figura 7-10 Parámetros de una regla de protección contra anti-crawler JavaScript



AVISO

WAF solo registra el desafío de JavaScript y los eventos de autenticación de JavaScript. No se pueden configurar otras acciones de protección para el desafío y la autenticación de JavaScript.

7.6 Otros

7.6.1 ¿En qué situaciones fracasarán las políticas de la WAF?

Normalmente, todas las solicitudes destinadas a su sitio pasarán a través de WAF. Sin embargo, si su sitio utiliza CDN y WAF, la política WAF dirigida a las solicitudes de almacenamiento en caché de contenido estático no tendrá efecto porque CDN devuelve directamente estas solicitudes al cliente.

7.6.2 ¿Es la ruta de una regla de protección WAF sensible a mayúsculas y minúsculas?

Todos los paths configurados para las reglas de protección de WAF distinguen entre mayúsculas y minúsculas.

7.6.3 ¿Puedo exportar o hacer una copia de respaldo de la configuración WAF?

No se puede exportar ni realizar copias de seguridad de la configuración WAF actual.

7.6.4 ¿Qué modos de trabajo y mecanismos de protección tiene WAF?

Después de conectar un nombre de dominio a su instancia WAF, WAF funciona como un proxy inverso entre el cliente y el servidor. La dirección IP real del servidor está oculta y solo la dirección IP de WAF es visible para los visitantes de la web.

WAF admite los siguientes modos de trabajo:

- Habilitada
- Suspendida
- Omitido

AVISO

- Si se utiliza un proxy para el sitio web que se implementa en **Cloud mode** antes de conectarse a WAF, la instancia WAF no se puede cambiar al modo **Bypassed**.
- El modo **Bypassed** no está disponible para los sitios web implementados en **Dedicated mode**.

Para obtener más detalles, consulte **Conmutación de modo de trabajo de WAF**.

Tabla 7-4 describe el mecanismo de protección.

Tabla 7-4 Mecanismo de protección compatible

Regla de protección	Acción protectora
Reglas básicas de protección web	• Block • Log only
Reglas de protección contra ataques CC	• Verification code • Block • Block dynamically • Log only
Reglas de protección precisas	• Block • Allow • Log only
Reglas de la lista negra y de la lista blanca	• Block • Allow • Log only
Reglas de control de acceso de geolocalización	• Block • Allow • Log only **AVISO** Este tipo de reglas son compatibles con instancias profesionales, platino y dedicadas WAF.

Regla de protección	Acción protectora
Habilitación de la protección anti-Crawler	Acciones de protección para las reglas anti-crawler basadas en características: ● Block ● Log only **AVISO** Este tipo de reglas son compatibles con instancias profesionales, platino y dedicadas WAF.

NOTA

- **Block**: WAF bloquea y registra los ataques detectados.
- **Log only**: WAF solo registra los ataques detectados.

7.6.5 ¿Qué reglas de protección admite WAF?

Las reglas de protección soportadas por WAF se describen a continuación.

- Protección básica de Web

  WAF puede defenderse contra ataques web comunes, como inyección SQL, XSS, shells web y troyanos en canales de carga HTTP. Una vez habilitadas estas funciones, la protección entra en vigor inmediatamente.

- Protección contra ataques CC

  Las políticas de limitación de velocidad flexibles se pueden establecer en función de las direcciones IP, el campo cookies o el campo Referer, que mitigan los ataques de CC.

- Protección precisa

  Los campos HTTP comunes se pueden combinar para personalizar las políticas de protección, como la protección CSRF. Con reglas definidas por el usuario, WAF puede detectar con precisión solicitudes maliciosas y proteger la información confidencial en sitios web.

- Listas negras y blancas

  Las reglas de listas negras o blancas le permiten bloquear o permitir direcciones IP específicas o rangos de direcciones, mejorando la precisión de la defensa.

- Control de acceso a la geolocalización

  Las reglas de control de acceso de geolocalización le permiten personalizar el control de acceso basado en las direcciones IP de origen.

- Protección contra manipulación de la web

  La configuración de caché se realiza en páginas web estáticas. Cuando un usuario accede a una página web, el sistema devuelve una página almacenada en caché al usuario y comprueba aleatoriamente si la página está manipulada.

- Protección antirrastreador

  Esta función analiza dinámicamente los modelos de servicios del sitio web e identifica con precisión el comportamiento de los rastreadores en función de los sistemas de control de riesgos de datos y de identificación de bots, como JS Challenge.

- Lista blanca de protección global (anteriormente enmascaramiento de alarma falsa)

  Esta función ignora ciertas reglas de detección de ataques para solicitudes específicas.
- Enmascaramiento de datos

  El enmascaramiento de datos impide que datos como contraseñas se muestren en los registros de eventos.
- Prevención de fuga de información

  WAF evita que se divulgue información confidencial del usuario en las páginas web, como números de identificación, números de teléfono y direcciones de correo electrónico.

7.6.6 ¿Cuál de las reglas de protección de la WAF es compatible con la acción de protección de solo registro?

En WAF, **Log only** está disponible para **Protective Action** en las reglas básicas de protección web.

Log only está disponible para **Protective Action** en las reglas de protección contra ataques CC, reglas de protección precisas, reglas de listas negras y blancas, reglas de control de acceso de geolocalización y reglas anti-crawler.

7.6.7 ¿Cómo puedo permitir que solo las direcciones IP especificadas accedan a sitios web protegidos?

Después de agregar el sitio web a WAF, configure las reglas de listas negras y blancas o las reglas de protección precisas para permitir que solo las direcciones IP especificadas accedan al sitio web. A continuación, WAF bloquea todas las direcciones IP de origen excepto las especificadas.

Configuración de las reglas de listas negras y blancas de direcciones IP para bloquear todas las direcciones IP de origen excepto las especificadas

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

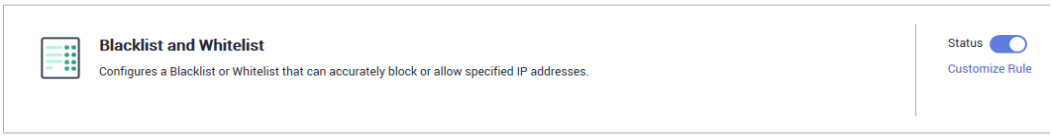
Paso 3 Haga clic en en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Website Settings**.

Paso 5 En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.

Paso 6 En el área de configuración **Blacklist and Whitelist**, active la protección. **Figura 7-11** muestra un ejemplo.

Figura 7-11 Área de configuración de listas negras y blancas



Paso 7 Haga clic en **Customize Rule**. En la página mostrada, haga clic en **Add Rule** en la esquina superior izquierda.

Paso 8 En el cuadro de diálogo **Add Blacklist or Whitelist Rule**, agregue dos reglas de lista negra para bloquear todas las direcciones IP de origen. **Figura 7-12** y **Figura 7-13** muestran ejemplos.

Figura 7-12 Bloqueo de rango de direcciones IP 1.0.0.0/1

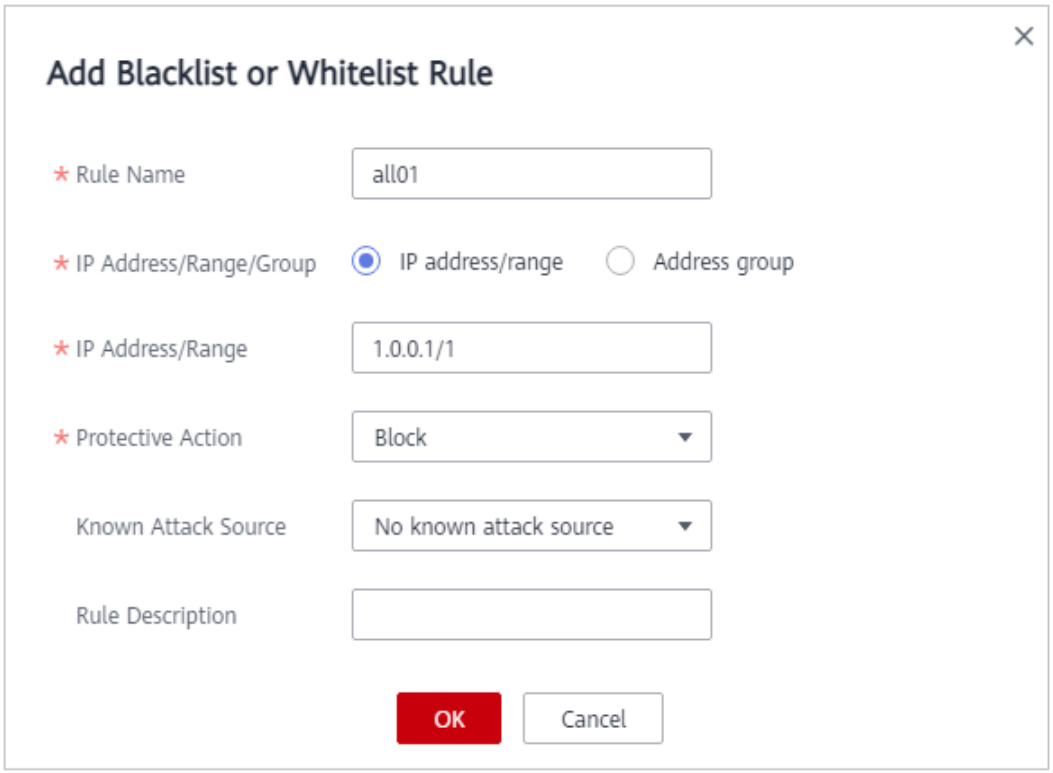
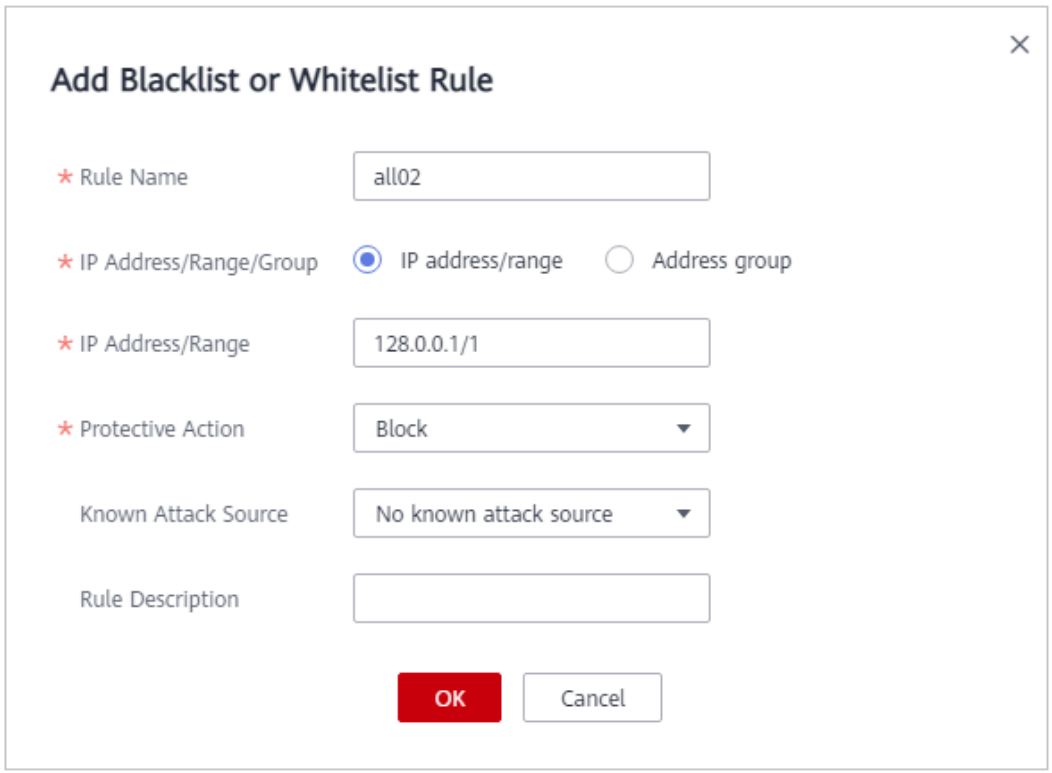


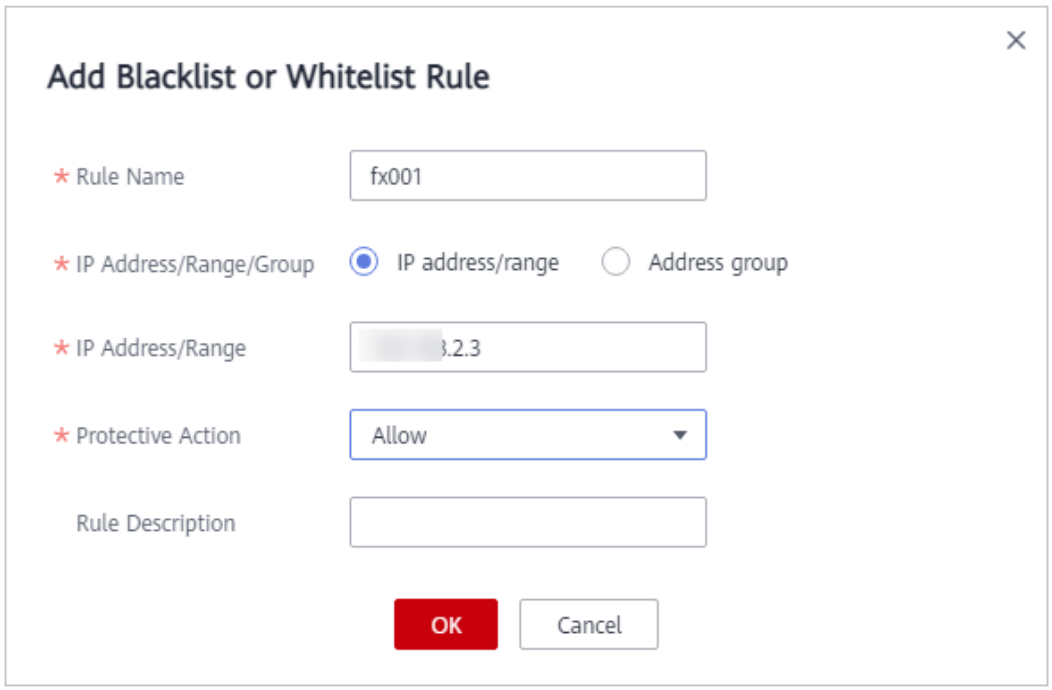
Figura 7-13 Intervalo de direcciones IP de bloqueo 128.0.0.0/1



Paso 9 Haga clic en **Add Rule**. En el cuadro de diálogo **Add Blacklist or Whitelist Rule** que se muestra, agregue una regla para la dirección IP o el intervalo de direcciones IP especificados.

Por ejemplo, si desea permitir que *XXX.XX.2.3* acceda a su sitio web, agregue una regla de protección como se muestra en **Figura 7-14**.

Figura 7-14 Permitir el acceso de una dirección IP especificada



----Fin

Configuración de una regla de protección precisa para bloquear todas las direcciones IP de origen excepto las especificadas

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

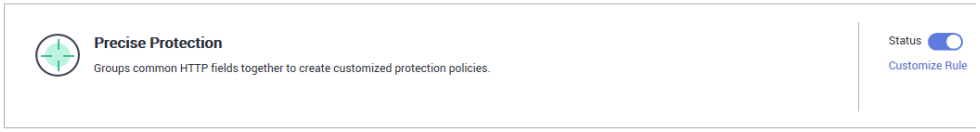
Paso 3 Haga clic en en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Website Settings**.

Paso 5 En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.

Paso 6 En el área de configuración de **Precise Protection**, active la protección. **Figura 7-15** muestra un ejemplo.

Figura 7-15 Área de configuración de protección precisa



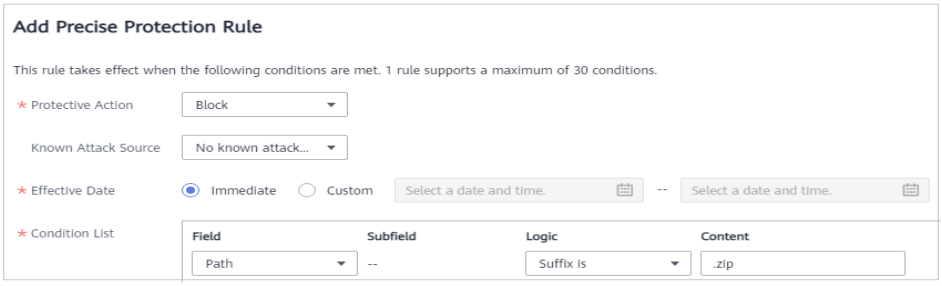
Paso 7 Haga clic en **Customize Rule**. En la esquina superior izquierda de la página mostrada, haga clic en **Add Rule**.

Paso 8 En el cuadro de diálogo **Add Precise Protection Rule** que se muestra, agregue una regla de protección como se muestra en **Figura 7-16** para bloquear todas las solicitudes.

ATENCIÓN

El valor de prioridad aquí debe ser mayor que el configurado en **Paso 9** porque permitir el acceso tiene una prioridad más alta que bloquear el acceso y un valor de prioridad más pequeño indica una prioridad más alta.

Figura 7-16 Bloqueo de todas las solicitudes



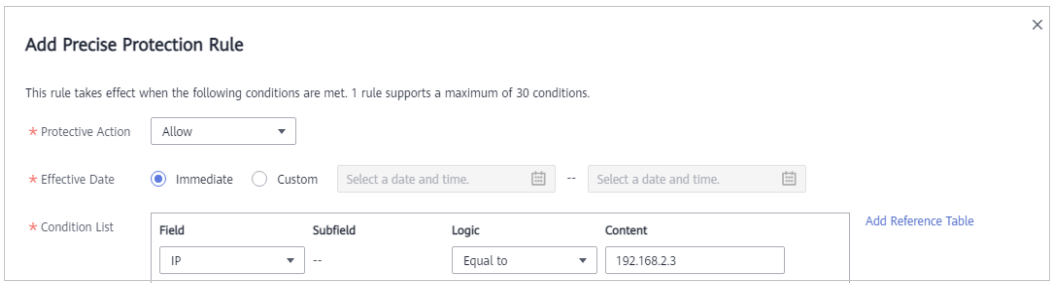
Paso 9 Haga clic en **Add Rule**. En el cuadro de diálogo **Add Precise Protection Rule** que se muestra, agregue una regla para la dirección IP especificada.

Por ejemplo, si desea permitir que 192.168.2.3 acceda al sitio web, agregue una regla de protección como se muestra en **Figura 7-17**.

ATENCIÓN

El valor de prioridad aquí debe ser más pequeño que el configurado en **Paso 8** porque permitir el acceso tiene una prioridad más alta que bloquear el acceso y un valor de prioridad más pequeño indica una prioridad más alta.

Figura 7-17 Permitir el acceso de una dirección IP especificada



También puede agregar una regla de lista blanca para las direcciones IP o el intervalo de direcciones IP especificados haciendo referencia a **Paso 9**.

----Fin

7.6.8 ¿Qué reglas de protección están incluidas en la política generada por el sistema?

Cuando agrega un sitio web a WAF, puede seleccionar una política existente que haya creado o la política generada por el sistema. Para obtener más información, consulte **Tabla 7-5**.

AVISO

Si utiliza la edición estándar de WAF, solo se puede seleccionar **System-generated policy**.

También puede adaptar sus reglas de protección después de que el nombre de dominio esté conectado a WAF.

Tabla 7-5 Políticas generadas por el sistema

Edición	Política	Descripción
Edición estándar	Protección web básica (modo **Log only** y comprobaciones comunes)	La protección web básica protege contra ataques como inyecciones SQL, XSS, vulnerabilidades de desbordamiento remoto, inclusiones de archivos, vulnerabilidades Bash, ejecución remota de comandos, recorrido de directorios, acceso sensible a archivos e inyecciones de comandos/código.
Ediciones profesionales y platino/Modo dedicado	Protección web básica (modo **Log only** y comprobaciones comunes)	La protección web básica protege contra ataques como inyecciones SQL, XSS, vulnerabilidades de desbordamiento remoto, inclusiones de archivos, vulnerabilidades Bash, ejecución remota de comandos, recorrido de directorios, acceso sensible a archivos e inyecciones de comandos/código.
	Anti-crawler (modo de **Log only** y función de **Scanner**)	WAF solo registra tareas de análisis web, como análisis de vulnerabilidades y análisis de virus, como el comportamiento de rastreo de OpenVAS y Nmap.

NOTA

Log only: WAF solo registra los eventos de ataque detectados en lugar de bloquearlos.

7.6.9 ¿Por qué no se actualiza la página después de activar WTP?

La protección contra manipulaciones web (WTP) solo admite el almacenamiento en caché de páginas web estáticas. Realice los siguientes pasos para solucionar este problema:

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 Haga clic en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Website Settings**.

Paso 5 En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.

Paso 6 En el área de configuración de **Web Tamper Protection**, compruebe si esta función está habilitada.

- Si esta función está activada (), vaya a **Paso 7**.
- Si esta función está desactivada (), haga clic en  para activar la función. Refresque la página unos minutos más tarde.

Paso 7 Haga clic en **Customize Rule**. En la página mostrada, compruebe si el nombre de dominio y la ruta son correctos.

- Si son correctos, vaya a **Paso 8**.
- Si no son correctos, haga clic en **Delete** en la columna **Operation** para eliminar la regla. A continuación, haga clic en **Add Rule** encima de la lista de reglas y configure otra regla. Para obtener más información, consulte **Configuración de una regla de protección contra manipulaciones web**.

  Una vez que la regla se haya agregado correctamente, actualice la página unos minutos más tarde. A continuación, vuelva a acceder a la página.

Paso 8 En la fila que contiene la regla de protección contra manipulaciones web, haga clic en **Update Cache** en la columna **Operation**.

Si se modifica el contenido de una página protegida, debe actualizar la caché. De lo contrario, WAF siempre devuelve el contenido en caché más reciente.

Después de actualizar la caché, actualice la página y acceda de nuevo a la página. Si la página sigue sin actualizarse, póngase en contacto con el soporte técnico.

----Fin

7.6.10 ¿Cuáles son las diferencias entre las reglas de lista negra/lista blanca y las reglas de protección precisas en el bloqueo de solicitudes de acceso desde direcciones IP especificadas?

Ambos pueden bloquear solicitudes de acceso desde direcciones IP especificadas. **Tabla 7-6** describe las diferencias entre los dos tipos de reglas.

Tabla 7-6 Diferencias entre las reglas de la lista negra y la lista blanca y las reglas de protección precisas

Reglas de protección	Protección	Secuencia de inspección de WAF
Reglas de la lista negra y de la lista blanca	Este tipo o reglas pueden bloquear, registrar únicamente o permitir solicitudes de acceso desde una dirección IP o intervalo de direcciones IP especificados.	Las reglas de la lista negra y la lista blanca tienen la prioridad más alta. WAF filtra las solicitudes de acceso basadas en las reglas de protección y la secuencia de activación. Para obtener más información, consulte **Guía de configuración**.
Reglas de protección precisas	Puede combinar campos HTTP comunes, como **IP**, **Path**, **Referer**, **User Agent**, y **Params** en una regla de protección para permitir que WAF permita o bloquee las solicitudes que coincidan con las condiciones combinadas.	Las reglas de protección precisas tienen menor prioridad en comparación con las reglas de lista negra y de lista blanca.

7.6.11 ¿Qué hago si un escáner, como AppScan detecta que falta la cookie segura o HttpOnly?

Las cookies son insertadas por servidores de web de back-end y se pueden desplegar a través de la configuración del marco o set-cookie. Secure y HttpOnly de cookies ayudan a defenderse de ataques, como los ataques XSS para obtener cookies y ayudan a defenderse del secuestro de cookies.

Si el analizador AppScan detecta que el sitio del cliente no inserta campos de configuración de seguridad, como HttpOnly y Secure, en la cookie de la solicitud de análisis después de analizar el sitio web, los registra como amenazas de seguridad.

WAF no proporciona tales funciones de cumplimiento. El administrador del sitio web debe realizar la configuración de seguridad relacionada en el backend.

8 Registros de eventos de protección

8.1 ¿Puede WAF registrar eventos de protección?

En la consola WAF, puede ver los registros de los últimos 30 días y descargar los registros de todos los sitios web protegidos durante los últimos cinco días de forma gratuita.

Si desea almacenar registros de protección WAF durante mucho tiempo, habilite Log Tank Service (LTS) con costos adicionales y autorice el registro WAF. Los registros se pueden almacenar en LTS durante siete días de forma predeterminada, pero puede configurar LTS durante hasta 30 días si es necesario. Los registros anteriores a 30 días se eliminan automáticamente. Sin embargo, puede configurar LTS para volcar esos registros en un bucket de Object Storage Service (OBS) o habilitar Data Ingestion Service (DIS) para el almacenamiento a largo plazo.

- Para obtener más información acerca de los registros de eventos, consulte **Visualización de los registros de eventos de protección**.
- Para obtener más información sobre la descarga de registros, consulte **Descarga de datos de eventos**.
- Para obtener más información acerca de cómo configurar LTS para WAF, consulte **Habilitación de LTS para el registro de WAF**.

8.2 ¿Puedo obtener registros de WAF usando las API?

Puede invocar a una API para ver los registros de protección WAF.

También puede descargar eventos de protección en la consola de WAF. Para obtener más información, consulte **Descarga de datos de eventos**.

8.3 ¿Cómo obtengo datos sobre acciones de bloqueo?

WAF le permite descargar los datos de eventos de ataque (solo registro y eventos de bloqueo) de todos los nombres de dominio protegidos durante los últimos cinco días. Al comienzo del día siguiente se generará un archivo CSV de los datos de eventos de protección para el día actual.

Para obtener más información sobre cómo obtener datos de eventos, consulte **Descarga de datos de eventos**.

8.4 ¿Qué significa "falta de coincidencia" para "acción protectora" en la lista de eventos?

Si una solicitud de acceso coincide con una regla de protección contra manipulaciones web, una regla de prevención de fugas de información o una regla de enmascaramiento de datos, la acción de protección se marca como **Mismatch**.

8.5 ¿Cómo obtiene WAF la dirección IP del cliente real para una solicitud?

WAF reenvía las solicitudes al backend según las reglas de protección. Si las reglas basadas en direcciones IP (como la lista negra y la lista blanca, la ubicación geográfica y las reglas de acceso precisas basadas en direcciones IP) se configuran para WAF, WAF comprueba primero las direcciones IP reales y luego permite o bloquea la solicitud de acuerdo con las reglas configuradas. WAF obtiene direcciones IP reales de acuerdo con los siguientes principios:

- Si selecciona **Yes** para **Proxy Configured** cuando agrega un nombre de dominio a WAF, WAF obtiene la dirección IP de origen en la siguiente secuencia:
  a. La lista de encabezados IP de origen configurada en el **upstream** se usa preferentemente, es decir, la etiqueta de dirección IP configurada en la página de información básica del nombre de dominio. Para obtener más información, consulte **Configuración de un identificador de tráfico para un ataque conocido**. Si no hay una dirección IP disponible, vaya a **b**.
  b. Obtenga el valor del campo **cdn-src-ip** en la lista de encabezados IP de origen configurada en el archivo de configuración. Si no se obtiene ningún valor, vaya a **c**.
  c. Obtenga el valor del campo **x-real-ip**. Si no se obtiene ningún valor, vaya a **d**.
  d. Obtenga la primera dirección IP pública desde la izquierda del campo **x-forwarded-for**. Si no se obtiene una dirección IP pública, vaya a **e**.
  e. Obtenga el valor del campo **remote_addr**, que incluye la dirección IP utilizada para establecer la conexión TCP.
- Si selecciona **No** para **Proxy Configured** cuando agrega un nombre de dominio a WAF, WAF obtiene la dirección IP de origen del campo **remote_ip**.

8.6 ¿Se pueden transferir los registros WAF a OBS?

Sí. Puede autorizar WAF para acceder a LTS y habilitar la función de transferencia de registros LTS para volcar los registros WAF a los buckets de OBS.

- Para habilitar LTS en WAF, consulte **Habilitación de LTS para registros WAF**.
- Para transferir registros LTS a OBS, **Transferir registros a OBS**.

8.7 ¿Cuánto tiempo pueden almacenarse los registros de protección WAF?

En la consola WAF, puede ver los registros de los últimos 30 días y descargar los registros de todos los sitios web protegidos durante los últimos cinco días de forma gratuita.

La duración del almacenamiento depende de sus opciones. Puede almacenar los registros WAF en Log Tank Service (LTS) durante siete días de forma predeterminada y hasta 30 días mediante una configuración personalizada adicional. Los registros anteriores a los 30 días serán eliminados automáticamente por LTS. LTS se factura adicionalmente. Si busca almacenamiento a largo plazo, habilite la función de transferencia de registros en LTS para volcar esos registros en los buckets de Object Storage Service (OBS) o habilite Data Ingestion Service (DIS).

- Para habilitar LTS en WAF, consulte **Habilitación de LTS para registros WAF**.
- Para transferir registros LTS a OBS, **Transferir registros a OBS**.

8.8 ¿Puedo consultar eventos de protección de un lote de direcciones IP especificadas a la vez?

WAF no admite consultas por lotes de eventos de protección de un lote de direcciones IP especificadas a la vez. En la página **Events**, puede ver los eventos mediante una combinación determinada de **Event Type**, **Protective Action**, **Source IP Address**, **URL** y **Event ID**.

Para obtener más información acerca de los eventos de protección, consulte **Consulta de registros de eventos de protección**.

8.9 ¿La WAF grabará los eventos desbloqueados?

No. WAF bloquea los eventos de ataque basándose en las reglas de protección configuradas y solo registra los eventos de ataque bloqueados en los registros de eventos de protección.

Para obtener más información acerca de los registros de eventos, consulte **Consulta de registros de evento de protección**.

8.10 ¿Por qué las estadísticas de tráfico en WAF son incompatibles con las del servidor de origen?

En cualquiera de los siguientes escenarios, las estadísticas de tráfico mostradas en la página **Dashboard** de WAF pueden ser incompatibles con las mostradas en el servidor de origen:

- Compresión de páginas web

  WAF habilita la compresión de forma predeterminada. Las páginas web entre el cliente (como un navegador) y WAF pueden comprimirse (dependiendo de la opción de compresión del navegador), pero el servidor de origen puede no admitir compresión.
- Reutilización de la conexión

WAF reutiliza las conexiones de socket con el servidor de origen, lo que reduce el uso de ancho de banda entre el servidor de origen y WAF.

- Solicitudes de ataque

  Las solicitudes de ataque bloqueadas por WAF no consumen el ancho de banda del servidor de origen.

- Otras solicitudes anormales

  Si el servidor de origen expira o no se puede conectar, el ancho de banda del servidor de origen no se consume.

- Retransmisión TCP

  WAF recopila estadísticas de ancho de banda en la capa 7, pero el adaptador de red del servidor de origen recopila estadísticas de ancho de banda en la capa 4. Si la conexión de red es deficiente, se produce la retransmisión TCP. El ancho de banda medido por el adaptador de red se calcula repetidamente, pero los datos transmitidos en la capa 7 no se calculan repetidamente. En este caso, el ancho de banda mostrado en WAF es menor que el mostrado en el servidor de origen.

8.11 ¿Por qué el número de registros en la página del panel es incompatible con el de la ficha Configurar registros?

Si el origen del ataque, la regla de aciertos, la ubicación de carga y la URL son coherentes para varios ataques, solo se muestra un registro en la pestaña **Configure Logs**. Por lo tanto, la página **Dashboard** muestra más registros.

