Web Application Firewall

Guía del usuario

Edición 01

Fecha 2022-11-01

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y la divulgación del presente documento en todo o en parte, de cualquier forma y por cualquier medio, sin la autorización previa de Huawei Technologies Co., Ltd. otorgada por escrito.

Marcas y permisos

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

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Huawei Technologies Co., Ltd.

Dirección: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Sitio web: https://www.huawei.com

Email: support@huawei.com

Índice

1 Descripción general....1

2 Compra de WAF....3

2.1 Comprar una instancia de Cloud WAF....3
2.2 Compra de una instancia WAF dedicada....9
2.3 Actualización de edición y especificación de Cloud WAF....13
2.4 Paquetes de expansión de ancho de banda de WAF Cloud Mode....17
2.5 Paquetes de expansión de dominio en WAF Cloud Mode....19
2.6 Paquetes de expansión de reglas de WAF Cloud Mode....20

3 Habilitación de la protección WAF....21

3.1 Puertos soportados por WAF....21
3.2 Conexión de un sitio web a WAF (Cloud Mode)....26
3.2.1 Proceso de conexión (Cloud Mode)....26
3.2.2 Paso 1: Agregar un nombre de dominio a WAF....29
3.2.3 Paso 4: Lista blanca de direcciones IP WAF Back-to-Source....45
3.2.4 Paso 2: Prueba de WAF....51
3.2.5 Paso 3: Enrutación del tráfico del sitio web a WAF....54
3.3 Conexión de un sitio web a WAF (Modo dedicado)....57
3.3.1 Proceso de conexión (Modo dedicado)....57
3.3.2 Paso 1: Agregar un sitio web a WAF (modo dedicado)....59
3.3.3 Paso 2: Configurar un balanceador de carga....68
3.3.4 Paso 3: Enlazar un EIP a un balanceador de carga....72
3.3.5 Paso 4: Lista blanca de las direcciones IP de origen de sus instancias de WAF dedicadas....73

4 Gestión de nombres de dominio de sitios web....78

4.1 Consulta de información básica....78
4.2 Cambio de modo de trabajo WAF....81
4.3 Configuración de la comprobación de certificación PCI DSS/3DS y versión TLS....83
4.4 Habilitación de la protección IPv6 WAF....91
4.5 Habilitación del protocolo HTTP/2....93
4.6 Configuración del tiempo de espera de conexión....94
4.7 Configuración de la protección de la conexión....95
4.8 Cambio del algoritmo de equilibrio de carga....98
4.9 Actualización de un certificado....99

 Copyright © Huawei Technologies Co., Ltd.

4.10 Configuración de un identificador de tráfico para un Known Attack Source 103
4.11 Edición de información del servidor 105
4.12 Modificación de la página de alarma 106
4.13 Eliminación de un sitio web protegido de WAF 108
5 Gestión de certificados 111
5.1 Carga de un certificado 111
5.2 Vinculación de un certificado a un sitio web protegido 114
5.3 Eliminación de un certificado 116
5.4 Consulta de información de certificado 118
6 Gestión de grupos de listas negras y listas blancas de direcciones IP 120
6.1 Agregar un grupo de direcciones IP 120
6.2 Modificación o eliminación de un grupo de direcciones IP de lista negra o blanca 122
7 Configuración de regla 125
7.1 Guía de configuración 125
7.2 Configuración de reglas básicas de protección web 130
7.3 Configuración del control de acceso inteligente 135
7.4 Configuración de una regla de protección contra ataques de CC 137
7.5 Configuración de una regla de protección precisa 147
7.6 Adición de una tabla de referencia 159
7.7 Configuración de una lista negra o una regla de lista blanca de direcciones IP 162
7.8 Configuración de una regla de origen de ataque conocida 170
7.9 Configuración de una regla de control de acceso de geolocalización 175
7.10 Configuración de una Regla de protección contra manipulaciones de Web 184
7.11 Configuración de las reglas de anti-crawler 188
7.12 Configuración de una regla de prevención de fugas de información 197
7.13 Configuración de una regla de enmascaramiento de falsa alarma 203
7.14 Configuración de una regla de enmascaramiento de datos 208
8 Panel 213
9 Gestión de Eventos 218
9.1 Consulta de registros de eventos de protección 218
9.2 Manejo de falsas alarmas 220
9.3 Descarga de datos de eventos 226
10 Habilitación de LTS para el registro de WAF 229
11 Habilitación de notificaciones de alarma 245
12 Gestión de políticas 248
12.1 Agregar una política 248
12.2 Adición de reglas a una o más políticas 249
12.3 Aplicación de una política a su sitio web 251
13 Gestión del motor WAF dedicado 253

 Copyright © Huawei Technologies Co., Ltd.

14 Visualización de los detalles de productos..... 259

15 Gestión de Proyectos y Proyectos Empresariales..... 260

16 Gestión de permisos.....262

16.1 Creación de un grupo de usuarios y concesión de permisos..... 262
16.2 Políticas personalizadas de WAF.....263
16.3 Permisos y acciones admitidas de WAF.....265

17 Operaciones clave registradas por CTS.....273

17.1 Operaciones clave registradas por CTS.....273
17.2 Visualización de un rastro de auditoría.....275

18 Monitoreo.....277

18.1 Métricas monitorizadas de WAF..... 277
18.2 Configuración de reglas de monitoreo de alarmas..... 303
18.3 Consulta de métricas monitoreadas..... 304

 Copyright © Huawei Technologies Co., Ltd.

1 Descripción general

Después de habilitar el servicio WAF, conecte el nombre de dominio de su sitio web a WAF para que todas las solicitudes de acceso se reenvíen a WAF para su monitoreo y protección.

Cómo usar WAF

Tabla 1-1 describe el procedimiento para usar WAF.

Tabla 1-1 Procedimiento para usar WAF

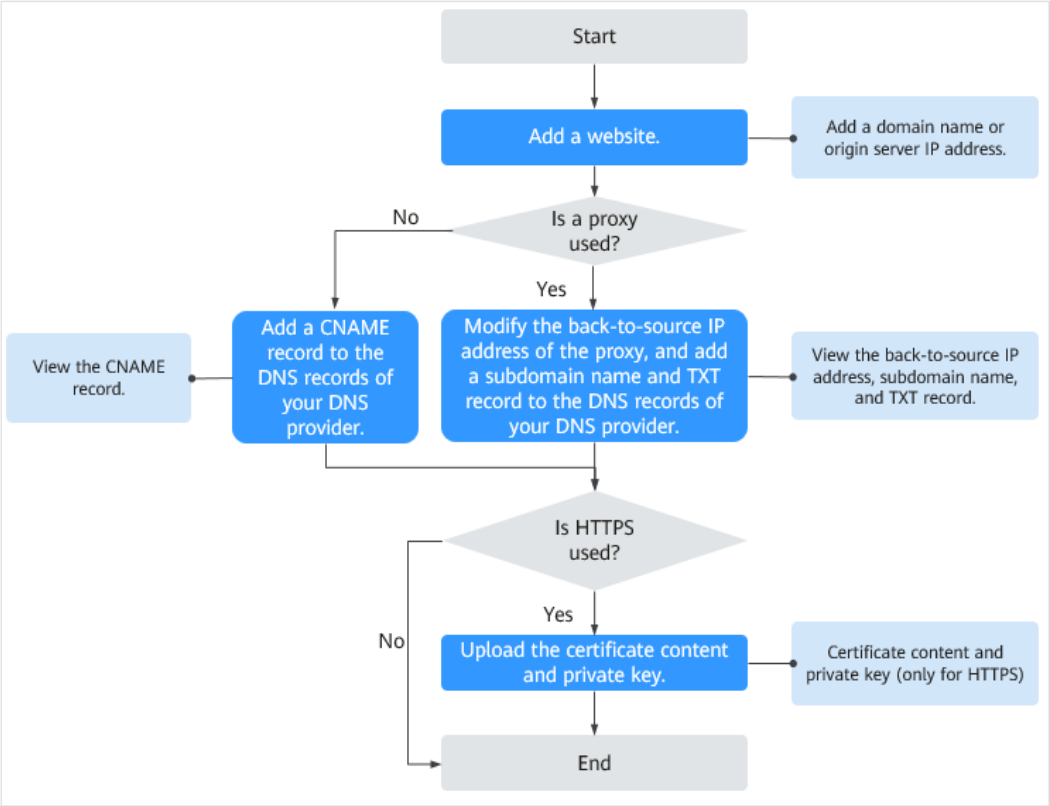
Paso	Descripción
Compra de una instancia WAF	Comprar una instancia WAF en la nube en el modo de facturación anual/mensual o de pago por uso o compre instancias WAF dedicadas facturadas en el modo de facturación de pago por uso. **AVISO** ● Para comprar instancias de WAF de pago por uso, **envíe un ticket de servicio** para habilitar el servicio. ● Las API de WAF son gratuitas. Para obtener más información, consulte **Habilitación de WAF**.
Adición de un sitio web a WAF	Agregar el sitio web que deseas proteger a WAF. ● Modo Cloud: Consulte **Paso 1: Agregar un nombre de dominio a WAF**. ● Modo dedicado: Consulte **Paso 1: Agregar un sitio web a WAF (modo dedicado)**.
Habilitación de la protección WAF	Habilitar la protección WAF para proteger el sitio web agregado. **NOTA** ● El uso de WAF no afecta el rendimiento de su servidor web porque el motor WAF no se está ejecutando en su servidor web. ● Después de que su nombre de dominio esté conectado a WAF, habrá una latencia de decenas de milisegundos, que podría aumentarse según el tamaño de la página solicitada o el número de solicitudes entrantes.

 Copyright © Huawei Technologies Co., Ltd.

Paso	Descripción
Configuración de reglas de protección	Utilizar las reglas de protección integradas WAF y configure reglas personalizadas para proteger su sitio web. Para más detalles, consulte **Configuración de regla**.
Habilitación de la notificación de alarma	Habilitar esta función para recibir una notificación de alarma en el instante en que se detecta un ataque. Para obtener más información, consulte **Habilitación de notificación de alarma**.
Manejo de falsas alarmas	Máscara de eventos bloqueados o registrados que se manejan como falsas alarmas. Para más detalles, consulte **Manejo de falsas alarmas**.
Consulta de **Dashboard**	Vea los datos de protección de ayer, hoy, últimos 3 días, últimos 7 días o últimos 30 días. Para más detalles, consulte **Panel**.

Para obtener más información sobre cómo conectar tu sitio web a WAF, consulta **Figura 1-1**.

Figura 1-1 Process of connecting a website to WAF



 Copyright © Huawei Technologies Co., Ltd.

2 Compra de WAF

2.1 Comprar una instancia de Cloud WAF

Las instancias de Cloud WAF en la nube se facturan en modo de facturación anual/mensual (prepago) o de pago por uso (postpago). En el modo de facturación anual/mensual, están disponibles las ediciones estándar (anteriormente edición profesional), profesional (anteriormente edición empresarial) y platino (anteriormente edición premium). Cada edición ofrece paquetes de expansión de dominio, ancho de banda y reglas.

AVISO

- Para comprar instancias de WAF de pago por uso, **envíe un ticket de servicio** para habilitar el servicio.
- Las API de WAF son gratuitas.

Antes de comenzar

- Solo se puede seleccionar un modo de facturación para su instancia WAF en una cuenta.
- En el modo de facturación anual/mensual, solo puede comprar una edición WAF en la misma región geográfica.
- Se admite el cambio entre pagos anuales/mensuales y de pago por uso.
- 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 anualmente/mensualmente o de pago por uso. El servicio WAF puede guardar los datos de configuración de la instancia WAF original para que pueda utilizar los datos de configuración sin tener que configurar la nueva instancia WAF solo cuando se cumplan las siguientes condiciones:
  - Si elige el modo de facturación de pago por uso, las instancias WAF nuevas y originales deben estar bajo el mismo proyecto en la misma región.
  - Si elige el modo de facturación anual/mensual, las instancias WAF nuevas y originales deben estar en la misma región.

 Copyright © Huawei Technologies Co., Ltd.

- 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 la instancia en el modo de facturación anual/mensual o de pago por uso.

AVISO

Después de deshabilitar el modo de facturación de pago por uso, la facturación de WAF se detiene, los datos de configuración de WAF se guardan y **Mode** de WAF cambia a **Suspended**. En esta situación, WAF reenvía el tráfico de tu sitio web sin detectarlo.

Prerrequisitos

Ha obtenido credenciales de inicio de sesión en la consola de gestión para una cuenta con los permisos de **WAF Administrator** y **BSS Administrator**.

Restricciones

- Las especificaciones de una instancia WAF no se pueden cambiar una vez que haya completado la compra. Para utilizar una instancia WAF con especificaciones más bajas, cancele la suscripción de la instancia WAF que está utilizando y compre otra.
- El paquete de expansión solo puede renovarse o darse de baja junto con la instancia WAF que está utilizando.

Limitaciones de la especificación

- Un paquete de dominio le permite agregar 10 nombres de dominio a WAF, incluyendo un dominio de nivel superior y nueve subdominios o dominios comodín relacionados con el dominio de nivel superior.
- Un paquete de expansión de ancho de banda puede proteger hasta 20 Mbit/s de tráfico para servicios 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.

  NOTA

  - Off Huawei Cloud: Los servidores de origen no se implementan en Huawei Cloud ni se implementan en las instalaciones.
  - On Huawei Cloud: los servidores de origen se implementan en Huawei Cloud.
- Un paquete de expansión de reglas le permite configurar hasta 10 reglas de listas negras y blancas de direcciones IP.

Escenarios de aplicación

Cloud WAF es una buena opción si sus servidores de servicio se implementan en la nube o en las instalaciones y planea proteger su sitio web agregando sus nombres de dominio a WAF.

Los escenarios de aplicación para diferentes ediciones son los siguientes:

- Standard (formerly professional edition)

  This edition is suitable for small- and medium-sized websites that do not have special security requirements.

 Copyright © Huawei Technologies Co., Ltd.

- Professional (formerly enterprise edition)

  This edition is suitable for medium-sized enterprise websites or services that are open to the Internet, focus on data security, and have high security requirements.
- Platinum (formerly premium edition)

  This edition is suitable for large- and medium-sized enterprise websites that have large-scale services or have special security requirements.

Compra de una instancia WAF facturada anualmente/mensualmente

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

NOTA

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

Paso 5 (Opcional): Seleccione un proyecto de empresa en la lista desplegable para **Enterprise Project**.

Esta opción sólo está disponible si ha iniciado sesión con una cuenta de empresa o si ha habilitado proyectos de empresa. Para obtener más información, consulte **Habilitación del centro de empresa**. Puede utilizar proyectos empresariales para gestionar de manera más eficiente los recursos de la nube y los miembros del proyecto.

NOTA

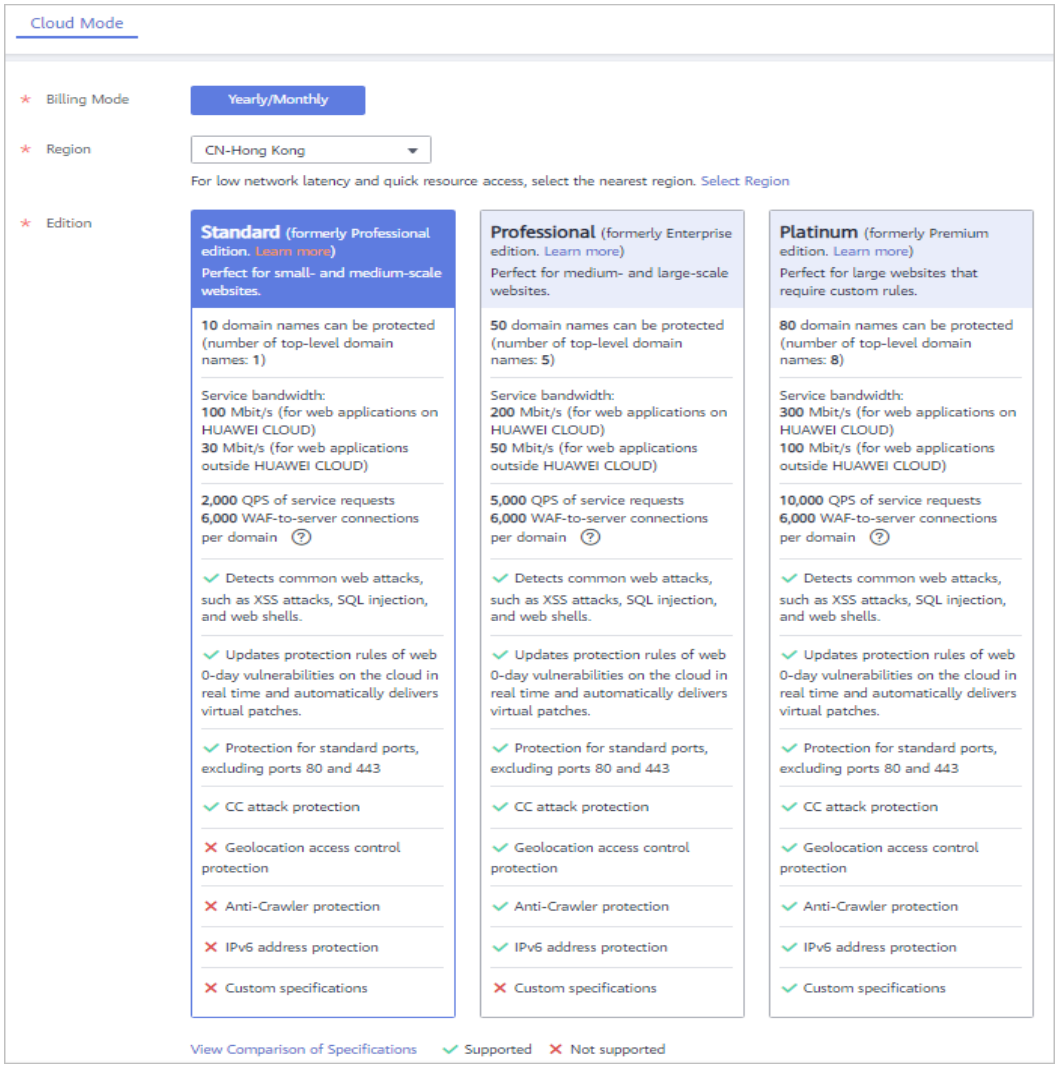
- Valor **default** indica el proyecto de empresa predeterminado. Los recursos que no están asignados a ningún proyecto de empresa bajo su cuenta se enumeran en el proyecto de empresa predeterminado.
- La opción **default** está disponible en la lista desplegable de **Enterprise Project** al comprar WAF.

Paso 6 En la página **Buy Web Application Firewall**, seleccione **Cloud Mode**.

Paso 7 En la página **Buy Web Application Firewall**, seleccione una región y una edición. **Figura 2-1** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 2-1 Selección de la edición WAF



NOTA

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.

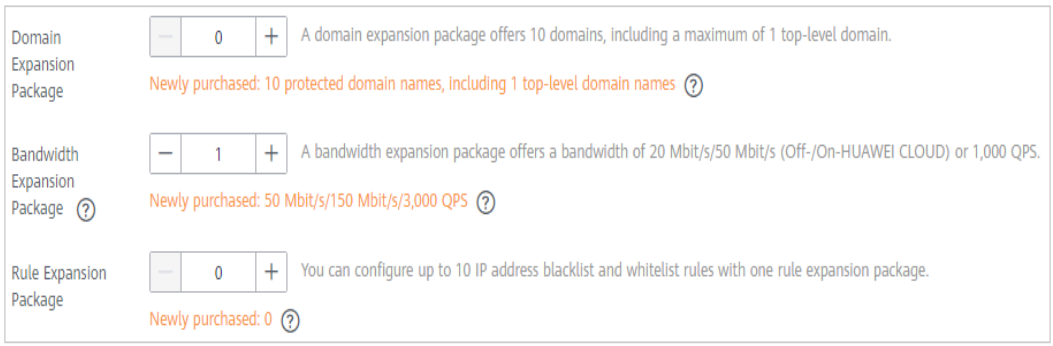
Para cambiar de región, seleccione una región en la lista desplegable. Solo se puede comprar una edición WAF en una región.

Paso 8 Especifique el número de nombres de dominio, ancho de banda o paquetes de expansión de reglas. **Figura 2-2** muestra un ejemplo.

Para obtener más información, consulte **Paquetes de expansión de dominio en WAF Cloud Mode** , **Paquetes de expansión de ancho de banda de WAF Cloud Mode**, y **Paquetes de expansión de reglas de WAF Cloud Mode** .

 Copyright © Huawei Technologies Co., Ltd.

Figura 2-2 Selección de paquetes de expansión



Paso 9 Configure la **Required Duration**. Puede seleccionar la duración requerida de un mes a tres años.

NOTA

Seleccione **Auto renew** para que el sistema pueda renovar automáticamente su suscripción de servicio según la duración requerida especificada aquí al expirar la suscripción.

Paso 10 En la esquina inferior derecha de la página, haz clic en **Next**.

Paso 11 Confirme los detalles del pedido y haga clic en **Pagar ahora**.

Paso 12 En la página de pago, seleccione un método de pago y paga su pedido.

----Fin

Compra de una instancia WAF facturada sobre una base de pago por uso

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

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

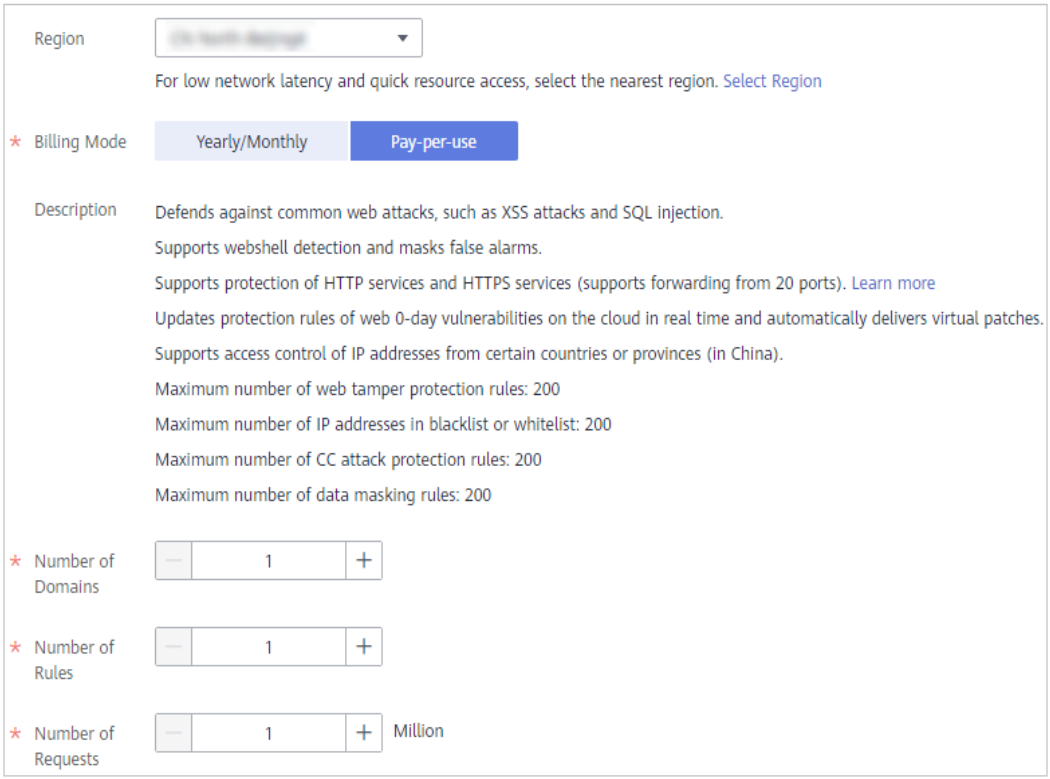
NOTA

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

Paso 5 En la página **Buy Web Application Firewall**, seleccione **Pay-per-use**, seleccione una edición y configure el número de nombres de dominio, reglas y solicitudes. **Figura 2-3** muestra un ejemplo.

Copyright © Huawei Technologies Co., Ltd.

Figura 2-3 Selección de **pay-per-use**



NOTA

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.

Para cambiar de región, seleccione una región en la lista desplegable de **Region**.

Paso 6 En la esquina inferior derecha de la página, haz clic en **Next**.

Paso 7 Haga clic en **Back to Website Settings** y agregue los nombres de dominio de los sitios web que desea proteger.

NOTA

Para desactivar WAF, puedes hacer clic en **Disable Pay-per-Use Cloud WAF** en la nube en la esquina superior derecha de la página.

----Fin

Verificación

La instancia WAF se compra cuando la edición de la instancia y los días de validez restantes se muestran en la esquina superior derecha de la consola de gestión.

Otras operaciones

En modo nube, para proteger más nombres de dominio o tráfico, actualice la edición de instancia o aumente el número de paquetes de expansión.

 Copyright © Huawei Technologies Co., Ltd.

2.2 Compra de una instancia WAF dedicada

Si sus servidores de servicio están implementados en Huawei Cloud, puede comprar una instancia WAF dedicada para proteger nombres de dominio o servicios web importantes con solo direcciones IP. Para ampliar las capacidades de protección y eliminar los puntos únicos de fallo (SPOF), compre un equilibrador de carga Elastic Load Balance (ELB) para sus instancias de WAF dedicadas.

Las instancias de WAF dedicadas se facturan sobre una base de pago por uso. Solo paga por lo que usa.

AVISO

Antes de comprar una instancia de WAF dedicada, **envíe un ticket de servicio** para habilitar la compra de instancias de WAF dedicadas. De lo contrario, no puede comprar instancias WAF dedicadas.

Prerrequisitos

- Ha obtenido credenciales de inicio de sesión en la consola de gestión para una cuenta con los permisos **WAF Administrator**, **WAF FullAccess**, y **BSS Administrator**.
- Se ha creado una VPC.

Restricciones

Si la instancia WAF dedicada y el servidor de origen no están en la misma VPC, habilite la comunicación entre la instancia y la subred del servidor de origen en el grupo de seguridad. Puede utilizar una **conexión de interconexión de VPC** para habilitar las comunicaciones entre VPC.

NOTA

Para obtener más información sobre las regiones admitidas, consulte **¿En qué regiones está disponible WAF?**

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.

Limitaciones de la especificación

Las especificaciones de una instancia WAF dedicada no se pueden modificar.

Escenarios de aplicación

Las instancias de WAF dedicadas son una buena opción si sus servidores de servicio se implementan en Huawei Cloud y planea proteger su sitio web agregando sus nombres de dominio o direcciones IP a WAF.

Sitios web adecuados para grandes empresas que tienen una gran escala de servicio y tienen requisitos de seguridad personalizados.

Copyright © Huawei Technologies Co., Ltd.

Procedimiento

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

Paso 2 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 3 Si es usuario por primera vez, haga clic en **Buy WAF Now**.

NOTA

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

Paso 4 (Opcional): Seleccione un proyecto de empresa en la lista desplegable para **Enterprise Project**.

Esta opción sólo está disponible si ha iniciado sesión con una cuenta de empresa o si ha habilitado proyectos de empresa. Para obtener más información, consulte **Habilitación del centro de empresa**. Puede utilizar proyectos empresariales para gestionar de manera más eficiente los recursos de la nube y los miembros del proyecto.

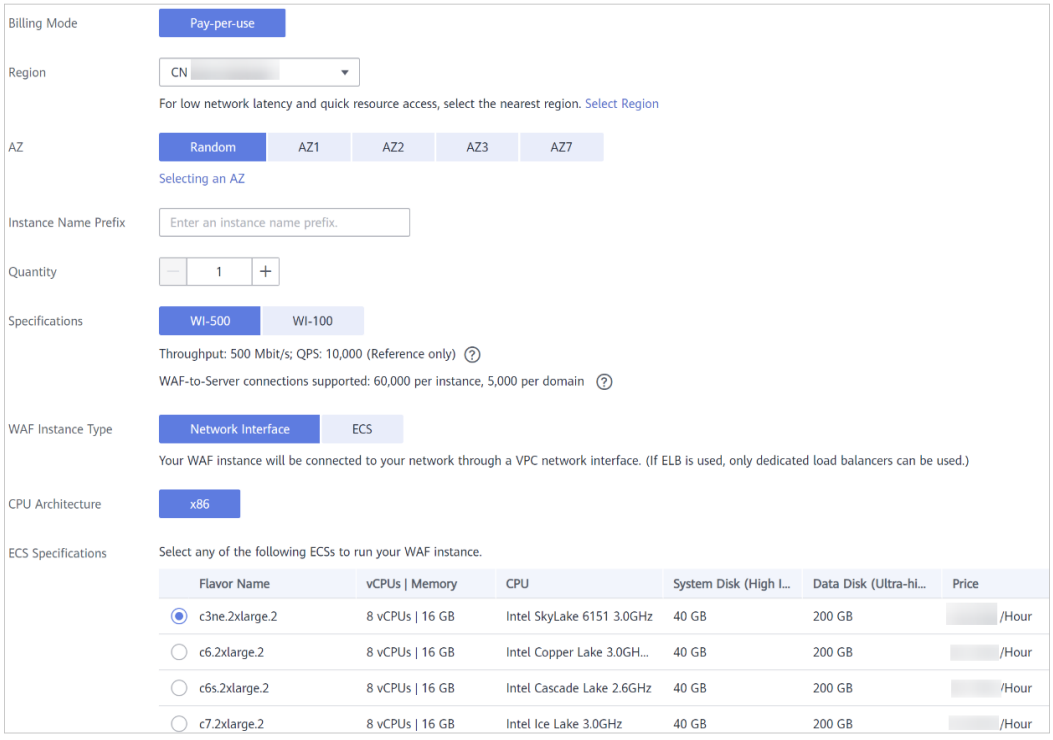
NOTA

- Valor **default** indica el proyecto de empresa predeterminado. Los recursos que no están asignados a ningún proyecto de empresa bajo su cuenta se enumeran en el proyecto de empresa predeterminado.
- La opción **default** está disponible en la lista desplegable de **Enterprise Project** al comprar WAF.

Paso 5 En la página **Buy Web Application Firewall**, seleccione **Dedicated Mode**.

Paso 6 Configure los parámetros de instancia haciendo referencia a **Tabla 2-1**. **Figura 2-4** muestra un ejemplo.

Figura 2-4 Configuración de una instancia WAF dedicada



 Copyright © Huawei Technologies Co., Ltd.

Tabla 2-1 Parámetros de una instancia WAF dedicada

Parámetro	Descripción
Region	Para obtener más información sobre las regiones admitidas, consulte **¿En qué regiones está disponible WAF?** 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.
AZ	Seleccione una AZ en la región seleccionada.
Instance Name Prefix	Establezca un prefijo del nombre de instancia WAF dedicado. Si compra varias instancias, el prefijo de cada nombre de instancia es el mismo.
Quantity	Establezca el número de instancias de WAF que desea comprar. Se recomienda comprar al menos dos instancias WAF y utilizar ambas para proteger sus servicios. Con múltiples instancias WAF que se utilizan para sus servicios, si una de ellas se vuelve defectuosa, WAF cambia automáticamente el tráfico a otras instancias WAF en ejecución para garantizar una protección continua.
Specifications	Las especificaciones **WI-500** y **WI-100** están disponibles.
WAF Instance Type	Este campo especifica el tipo de recurso de la instancia. Las opciones son las siguientes: ● **Network Interface** La instancia WAF se conectará a su red a través de una interfaz de red VPC. Si se usa ELB, solo se pueden usar balanceadores de carga dedicados. ● **ECS** La instancia WAF se creará en el ECS. Puede ver la instancia WAF creada en la consola de gestión de ECS.
CPU Architecture	Seleccione la arquitectura de CPU para su instancia.
CPU Specifications	Seleccione las especificaciones de ECS para su instancia.
VPC	Seleccione la VPC a la que pertenece el servidor de origen.
Subnet	Seleccione una subred configurada en la VPC.

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción
Security Group	Seleccione un grupo de seguridad en la región o haga clic en **Manage Security Group** para ir a la consola de VPC y crear un grupo de seguridad. Después de seleccionar un grupo de seguridad, la instancia WAF estará protegida por las reglas de acceso del grupo de seguridad. **AVISO** ● Puede configurar su grupo de seguridad de la siguiente manera: – Reglas de entrada Agregue una regla de entrada para permitir que el tráfico de red entrante pase a través de un puerto específico según sus requisitos de servicio. Por ejemplo, si desea permitir el acceso desde el puerto 80, puede agregar una regla que permita **TCP** y el puerto **80**. – Reglas de salida Todo el tráfico de red saliente está permitido de forma predeterminada. Para obtener más información, consulte **Adición de una regla de grupo de seguridad**. ● Si la instancia WAF dedicada y el servidor de origen no están en la misma VPC, habilite las comunicaciones entre la instancia y la subred del servidor de origen en el grupo de seguridad.

Paso 7 En la esquina inferior derecha de la página, haz clic en **Next**.

Paso 8 Confirme los detalles del pedido y haga clic en **Pay Now**.

Paso 9 En la página de pago, seleccione un método de pago y pague su pedido.

Paso 10 Después de que el pago se haya realizado correctamente, haga clic en **Back to Dedicated Engine List**. En la página **Dedicated Engine**, vea el estado de la instancia.

----Fin

Verificación

Se tarda unos 5 minutos en crear una instancia WAF dedicada. Si el estado de la instancia es **Running**, la creación de la instancia se ha completado.

Otras operaciones

Gestión del motor WAF dedicado

En este tema se describe cómo gestionar las instancias (o motores) de WAF dedicadas, incluida la visualización de información de instancia, visualización de configuraciones de monitoreo de instancia, la actualización de la edición de instancia o la eliminación de una instancia.

Autorización de WAF para acceder a los datos en la VPC que reside en su sitio web

Si espera utilizar una instancia de WAF dedicada, autorice a WAF a acceder directamente a los datos de la VPC habilitando ciertas reglas de seguridad.

 Copyright © Huawei Technologies Co., Ltd.

Al comprar una instancia dedicada de WAF, usted acepta autorizar a WAF a habilitar dichas reglas de seguridad. Actualmente, las reglas de grupo de seguridad enumeradas en **Tabla 2-2** se habilitarán automáticamente para una instancia WAF dedicada.

Tabla 2-2 Reglas de grupo de seguridad para que WAF acceda a la VPC que reside en su sitio web

Protocolo & Puerto	Tipo	Dirección de origen	Descripción
Reglas de entrada			
TCP: 22	IPv4	100.64.0.0/10	O&M remoto de WAF
Reglas de salida			
TCP: 9011	IPv4	100.125.0.0/16	Informe de registros de eventos de WAF
TCP: 9012	IPv4	100.125.0.0/16	Informe de registros de eventos de WAF
TCP: 9013	IPv4	100.125.0.0/16	Informe de registros de eventos de WAF
TCP: 9018	IPv4	100.125.0.0/16	Sincronización de políticas de WAF
TCP: 9019	IPv4	100.125.0.0/16	Informe de registros de latidos de WAF
TCP: 4505	IPv4	100.125.0.0/16	Sincronización de políticas de WAF
TCP: 4506	IPv4	100.125.0.0/16	Sincronización de políticas de WAF
TCP: 50051	IPv4	100.125.0.0/16	Informe de registros de rendimiento de WAF
TCP: 443	IPv4	100.125.0.0/16	Sincronización de políticas de WAF

2.3 Actualización de edición y especificación de Cloud WAF

Para las instancias de WAF en la nube que se facturan anualmente/mensualmente, puede actualizar la edición de WAF que está utilizando para aumentar la cuota. También puede comprar paquetes de expansión de dominios, ancho de banda o reglas para aumentar la cuota sin actualizar la edición WAF. Los paquetes de expansión de reglas le permiten configurar más reglas de listas negras y listas blancas.

 Copyright © Huawei Technologies Co., Ltd.

Prerrequisitos

- Ha obtenido credenciales de inicio de sesión en la consola de gestión para una cuenta con los permisos de **WAF Administrator** y **BSS Administrator**.
- Ha comprado una instancia WAF en la nube.

Limitaciones de la especificación

- Un paquete de dominio le permite agregar 10 nombres de dominio a WAF, incluyendo un dominio de nivel superior y nueve subdominios o dominios comodín relacionados con el dominio de nivel superior.
- Un paquete de expansión de ancho de banda puede proteger hasta 20 Mbit/s de tráfico para servicios 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.

  NOTA

  - Off Huawei Cloud: Los servidores de origen no se implementan en Huawei Cloud ni se implementan en las instalaciones.
  - On Huawei Cloud: los servidores de origen se implementan en Huawei Cloud.
- Un paquete de expansión de reglas le permite configurar hasta 10 reglas de listas negras y blancas de direcciones IP.

Restricciones

Una instancia WAF caducada no se puede actualizar directamente. Renueve WAF antes de actualizarlo.

Escenarios de aplicación

Es posible que desee actualizar su edición o especificaciones WAF cuando:

- Su instancia actual de WAF en la nube no puede admitir ciertas funciones disponibles en otras ediciones de WAF.
- Desea proteger más nombres de dominio o mayor ancho de banda con la instancia WAF actual.
- Desea configurar más reglas de listas negras y blancas de direcciones IP con la instancia WAF actual.

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

Impacto en el sistema

La actualización de una edición WAF o la compra de paquetes adicionales de expansión de dominios, ancho de banda o reglas no tiene ningún impacto en los servicios de sitios web protegidos.

Procedimiento

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.

 Copyright © Huawei Technologies Co., Ltd.

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

Paso 4 En la esquina superior derecha, haz clic en **Buy/Upgrade WAF**.

Paso 5 (Opcional): Seleccione un proyecto de empresa en la lista desplegable para **Enterprise Project**.

Esta opción sólo está disponible si ha iniciado sesión con una cuenta de empresa o si ha habilitado proyectos de empresa. Para obtener más información, consulte **Habilitación del centro de empresa**. Puede utilizar proyectos empresariales para gestionar de manera más eficiente los recursos de la nube y los miembros del proyecto.

NOTA

- Valor **default** indica el proyecto de empresa predeterminado. Los recursos que no están asignados a ningún proyecto de empresa bajo su cuenta se enumeran en el proyecto de empresa predeterminado.
- La opción **default** está disponible en la lista desplegable de **Enterprise Project** al comprar WAF.

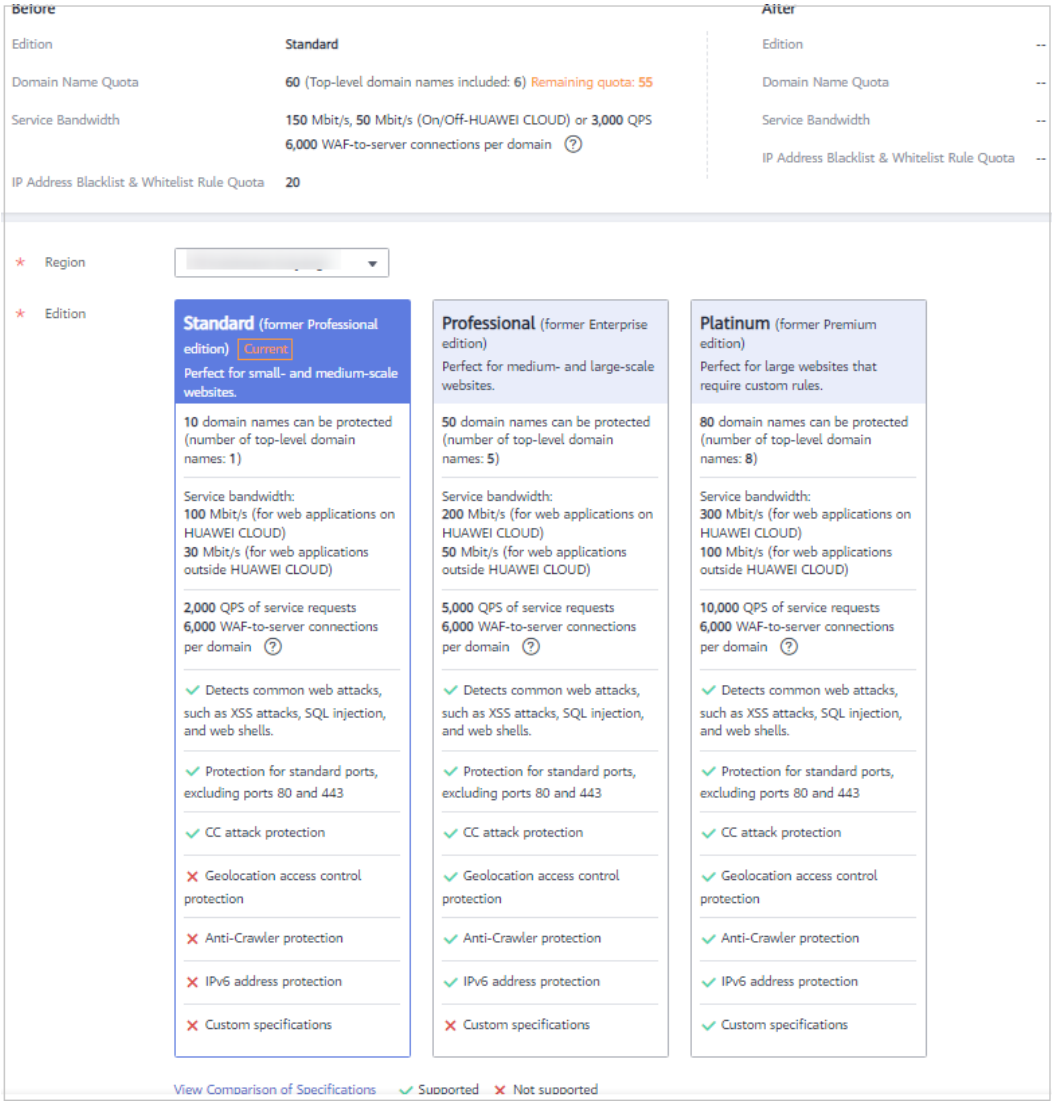
Paso 6 En la página **Buy Web Application Firewall**, seleccione **Cloud Mode**.

Paso 7 En la página de compra, seleccione cualquier edición superior a la actual. De forma predeterminada, se selecciona la edición actual. **Figura 2-5** muestra un ejemplo.

La edición listada en el lado derecho de la actual es una edición más rica en funciones.

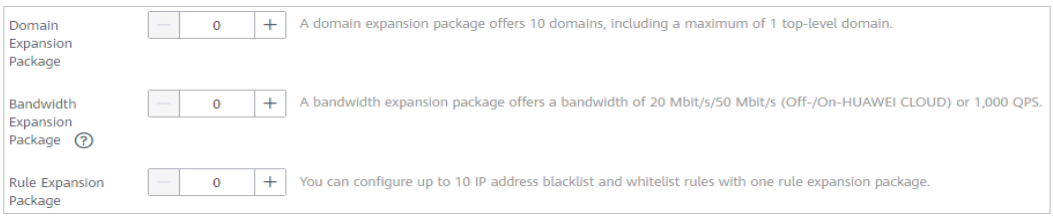
 Copyright © Huawei Technologies Co., Ltd.

Figura 2-5 Selección de la edición WAF



Paso 8 Especifique el número de paquetes de expansión de dominios, ancho de banda y reglas que desea comprar.

Figura 2-6 Selección de paquetes de expansión



Paso 9 En la esquina inferior derecha de la página, haz clic en **Next**.

Paso 10 Confirme los detalles del pedido y haga clic en **Pagar ahora**.

Paso 11 En la página de pago, seleccione un método de pago y paga su pedido.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

Verificación

La nueva instancia de edición y las especificaciones entran en vigor al finalizar el pago.

Otras operaciones

- **Paquetes de expansión de dominio en WAF Cloud Mode**
- **Paquetes de expansión de ancho de banda de WAF Cloud Mode**
- **Paquetes de expansión de reglas de WAF Cloud Mode**

2.4 Paquetes de expansión de ancho de banda de WAF Cloud Mode

Se proporciona una cierta cantidad de ancho de banda cuando compra una instancia WAF estándar (anteriormente edición profesional), profesional (anteriormente edición empresarial) o platino (anteriormente edición premium) que se factura anualmente/mensualmente. Si necesita más ancho de banda, puede comprar paquetes de expansión de ancho de banda adicionales.

Los paquetes de expansión de ancho de banda están disponibles al comprar o actualizar instancias WAF cloud. Un paquete de expansión de ancho de banda debe renovarse o darse de baja de junto con la instancia WAF asociada.

¿Cuál es el límite de ancho de banda del servicio?

El límite de ancho de banda de servicio es la cantidad de tráfico normal que una instancia WAF puede proteger.

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.

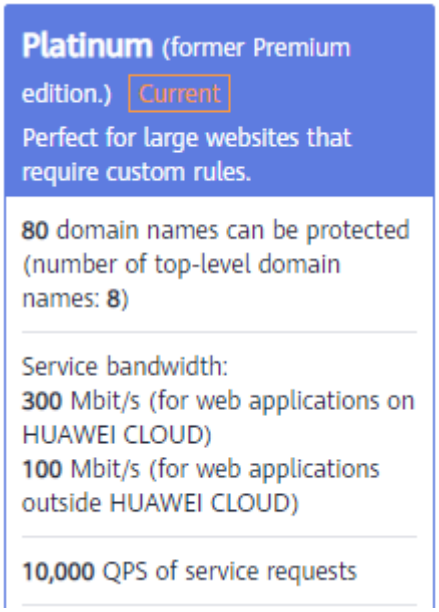
NOTA

El ancho de banda en WAF es calculado por el propio WAF y no está asociado con el ancho de banda o el límite de tráfico de otros productos de Huawei Cloud (como CDN, ELB y ECS).

De forma predeterminada, una cierta cantidad de ancho de banda puede ser protegida por la instancia WAF estándar (anteriormente edición profesional), profesional (anteriormente edición empresarial) o platino (anteriormente edición premium) facturada en modo anual/mensual. Si sus servidores de origen (como los balanceadores de carga ECS o ELB) están en Huawei Cloud, se puede proteger más ancho de banda. Por ejemplo, si sus servidores de origen están en Huawei Cloud, una instancia WAF platinum (anteriormente edición premium) puede proteger un máximo de 300 Mbit/s de ancho de banda. Si sus servidores de origen están fuera de Huawei Cloud (como en las salas de equipos IDC), una instancia premium WAF puede proteger hasta 100 Mbit/s de ancho de banda. **Figura 2-7** muestra un ejemplo.

Copyright © Huawei Technologies Co., Ltd.

Figura 2-7 Ancho de banda del servicio



¿Cuántos paquetes de expansión de ancho de banda necesito?

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.

NOTA

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

Puede estimar el tráfico haciendo referencia a las estadísticas de tráfico en la consola de ECS o utilizando otras herramientas de supervisión.

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).

¿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.

 Copyright © Huawei Technologies Co., Ltd.

Paquete de expansión de ancho de banda

Si el ancho de banda requerido por su sitio web excede el límite de ancho de banda de la edición WAF que ha seleccionado, puede comprar paquetes de expansión de ancho de banda para garantizar la protección de los servicios.

Por ejemplo, si compró la edición profesional WAF (anteriormente edición empresarial), con un límite de ancho de banda de 50 Mbit/s, y sus requisitos de ancho de banda son de 70 Mbit/s para sus servidores fuera de Huawei Cloud, puede comprar un paquete de expansión de ancho de banda de 20 Mbit/s para compensar la diferencia. Para más detalles, consulte **Actualización de edición y especificación de Cloud WAF**.

2.5 Paquetes de expansión de dominio en WAF Cloud Mode

Un paquete de dominio puede proteger 10 nombres de dominio, incluyendo un máximo de un nombre de dominio de nivel superior. Si la edición WAF que está utilizando no puede cumplir con los requisitos de su negocio, puede comprar paquetes de expansión de dominio para aumentar la cuota. Por ejemplo, si está utilizando la edición estándar (anteriormente edición profesional), se pueden proteger 10 nombres de dominio, incluido solo un nombre de dominio de nivel superior. Si desea proteger tres nombres de dominio de nivel superior, puede comprar dos paquetes de expansión de nombres de dominio para aumentar la cuota.

Vaya a la consola WAF, haga clic en **Buy/Upgrade WAF** en la esquina superior derecha. Luego, compre paquetes de expansión de dominios. No se puede cancelar la suscripción a un paquete de expansión de dominio. Un paquete de expansión de dominio solo puede renovarse junto con la edición WAF que utilice.

Cuota de nombres de dominio de diferentes ediciones in Cloud Mode

Las ediciones Cloud WAF ofrecen diferentes cuotas de dominio.

- Edición estándar (anteriormente edición profesional): 10 nombres de dominio pueden ser protegidos, incluyendo solo un nombre de dominio de nivel superior
- Edición profesional (anteriormente edición empresarial): cinco paquetes de dominio que pueden proteger 10 nombres de dominio, incluidos hasta cinco nombres de dominio de nivel superior.
- Edición Platinum (anteriormente edición premium): ocho paquetes de dominio que pueden proteger 10 nombres de dominio, incluyendo hasta ocho nombres de dominio de nivel superior.

NOTA

- Si solo se puede agregar un dominio de nivel superior a una instancia WAF, puede agregar un dominio de nivel superior y nombres de dominio de subdominio o comodín relacionados con el dominio de nivel superior. Por ejemplo, puede agregar un nombre de dominio de nivel superior example.com y un máximo de nueve subdominios o dominios genéricos, por ejemplo, www.example.com, *.ejemplo.com, mail.ejemplo.com, user.pay.example.com y x.y.z.example.com. Cada uno de estos nombres de dominio (incluido el nombre de dominio de nivel superior example.com) se cuenta para una cuota de nombres de dominio en el paquete de nombres de dominio.
- 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.

Copyright © Huawei Technologies Co., Ltd.

También puede actualizar su edición cloud WAF para aumentar la cuota de nombres de dominio. Para más detalles, consulte **Actualización de edición y especificación de Cloud WAF**.

2.6 Paquetes de expansión de reglas de WAF Cloud Mode

Para las instancias WAF facturadas anualmente/mensualmente, si la cuota para las reglas de la lista negra de direcciones IP y de la lista blanca de su instancia WAF actual es insuficiente, puede comprar paquetes de expansión de reglas para configurar más reglas de este tipo.

Un paquete de expansión de reglas le permite configurar hasta 10 reglas de listas negras y blancas de direcciones IP.

Los paquetes de expansión de reglas están disponibles al comprar o actualizar una instancia cloud WAF. Un paquete de expansión de reglas debe renovarse o darse de baja de junto con la instancia WAF asociada.

Para más detalles, consulte **Actualización de edición y especificación de Cloud WAF**.

 Copyright © Huawei Technologies Co., Ltd.

3 Habilitación de la protección WAF

3.1 Puertos soportados por WAF

Además de los puertos estándar 80 y 443, WAF soporta un gran número de puertos no estándar **Tabla 3-1**. muestra qué puertos no estándar son compatibles con diferentes ediciones WAF.

Tabla 3-1 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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

3.2 Conexión de un sitio web a WAF (Cloud Mode)

3.2.1 Proceso de conexión (Cloud Mode)

Para permitir que su instancia WAF en la nube proteja su sitio web, el nombre de dominio del sitio web debe estar conectado a su instancia WAF para que el tráfico entrante del sitio web pueda ir primero a WAF.

Restricciones

- Una instancia de WAF en la nube puede proteger aplicaciones web y sitios web a los que se puede acceder a través de nombres de dominio. Para obtener más información, consulte **Diferencias de ediciones**
- Después de que su sitio web esté conectado a WAF, el archivo que los visitantes pueden subir cada vez no puede exceder los 512 MB.

Prerrequisitos

A continuación se describe cómo funciona WAF cuando se usa un proxy o no se usa un proxy delante de WAF:

- Proxy used

  Si su sitio web ha utilizado proxies, como anti-DDoS, Content Delivery Network (CDN) o aceleración en la nube, **Figura 3-1** muestra cómo funciona WAF.

  – DNS resuelve el nombre de dominio a la dirección IP del proxy antes de que su sitio web esté conectado a WAF. En este caso, el tráfico pasa a través del proxy y luego el proxy enruta el tráfico de vuelta al servidor de origen.

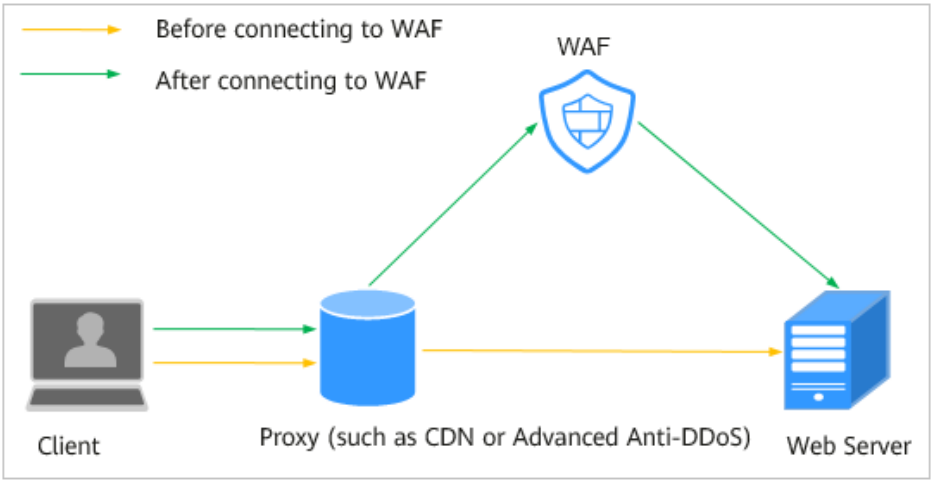
  – Después de que su sitio web esté conectado a WAF, DNS resuelve su nombre de dominio a la dirección de acceso de WAF. De esta manera, el proxy reenvía el tráfico a WAF. A continuación, WAF filtra el tráfico ilegítimo y solo enruta el tráfico legítimo de vuelta al servidor de origen.

    i. Cambie la dirección IP de origen del proxy al registro CNAME de WAF.

    ii. (Opcional) Agregue un nombre de subdominio WAF y un registro TXT en su proveedor DNS.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-1 Configuración WAF cuando se utiliza un proxy



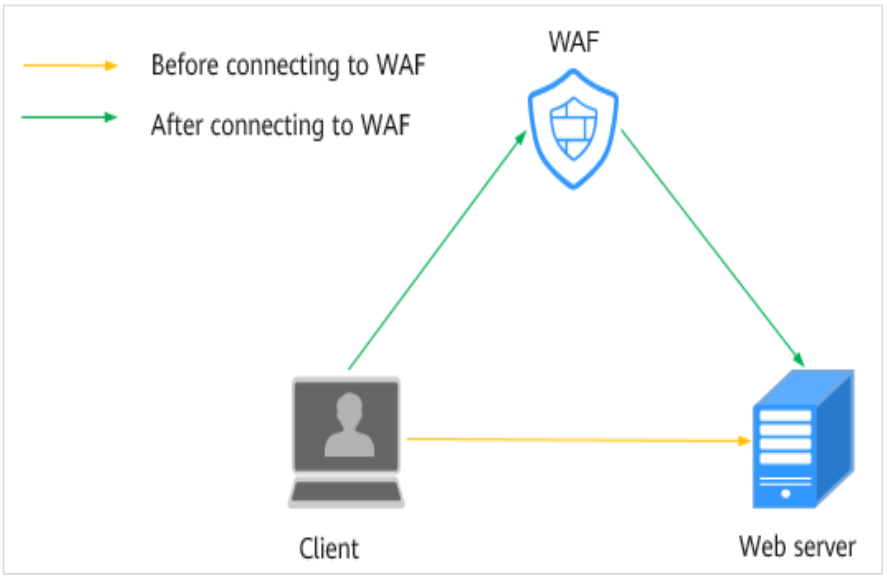
- No proxy used

  Si no se utiliza ningún proxy antes de que el sitio web esté conectado a WAF, **Figura 3-2** muestra cómo funciona WAF.

  – DNS resuelve su nombre de dominio a la dirección IP del servidor de origen antes de que su sitio web esté conectado a WAF. Por lo tanto, los visitantes de la web pueden acceder directamente al servidor.

  – Después de que su sitio web esté conectado a WAF, DNS resuelve su nombre de dominio en el registro CNAME de WAF. De esta manera, el tráfico pasa a través de WAF. A continuación, WAF filtra el tráfico ilegítimo y solo enruta el tráfico legítimo de vuelta al servidor de origen.

Figura 3-2 No proxy used



Procesos de conexión de un sitio web a WAF

Después de comprar una instancia WAF en la nube, complete las configuraciones requeridas siguiendo el proceso que se muestra en **Figura 3-3**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-3 Proceso de conexión de un sitio web a WAF

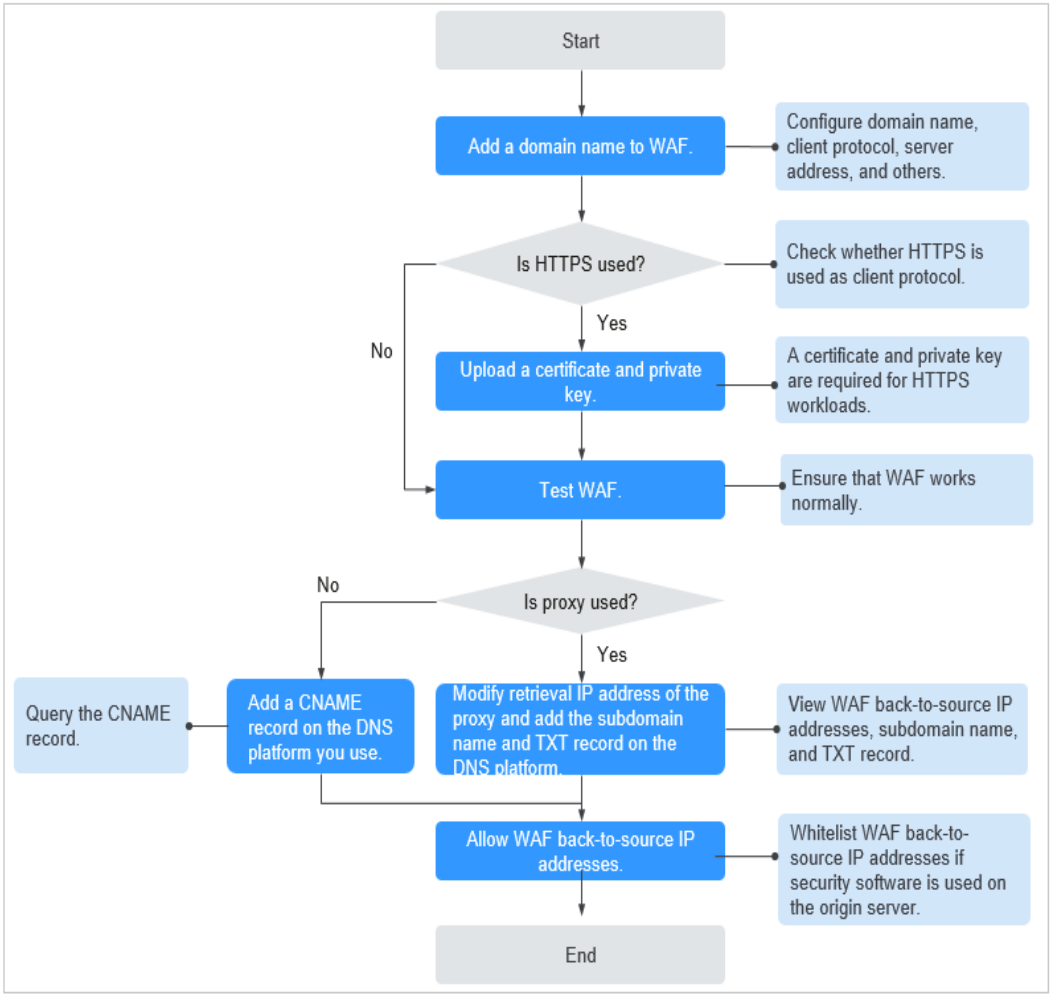


Tabla 3-2 Proceso de conectar el nombre de dominio de su sitio web a WAF

Procedimiento	Descripción
Paso 1: Agregar un nombre de dominio a WAF	Configure la información básica, como el nombre de dominio, el protocolo y el servidor de origen.
Paso 2: Prueba de WAF	Para asegurarse de que su instancia WAF reenvía el tráfico del sitio web normalmente, pruebe la instancia WAF localmente y, a continuación, enrute el tráfico destinado al nombre de dominio del sitio web a WAF modificando el registro DNS.
Paso 3: Enrutación del tráfico del sitio web a WAF	● No proxy used Configure un registro CNAME para el nombre de dominio protegido en la plataforma DNS que utilice. ● Proxy (como anti-DDoS avanzado y CDN) used Cambie la dirección IP de origen del proxy usado, como anti-DDoS avanzado y CDN, al registro CNAME copiado.

 Copyright © Huawei Technologies Co., Ltd.

Procedimiento	Descripción
Paso 4: Lista blanca de direcciones IP WAF Back-to-Source	Si hay otro software de seguridad o firewalls instalados en su servidor de origen, haga una lista blanca solo para las solicitudes de WAF. Esto garantiza un acceso normal y protege el servidor de origen de hacking.

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

Arreglar sitios web inaccesibles

Si un nombre de dominio no se conecta a WAF, su estado de acceso es **Inaccessible**. Para solucionar este problema, consulte **¿Por qué es inaccesible el estado de acceso de un nombre de dominio o una dirección IP?**

3.2.2 Paso 1: Agregar un nombre de dominio a WAF

Este tema describe cómo agregar un nombre de dominio a WAF para que el tráfico del sitio web pueda pasar a través de WAF. Después de conectar un nombre de dominio de 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.

NOTA

Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable de **Enterprise Project** y agregar nombres de dominio de sitios web que se protegerán en el proyecto.

Prerrequisitos

- Usted ha comprado una instancia WAF.
- El nombre de dominio se ha registrado con la licencia ICP y no se ha agregado a WAF.

Restricciones

- 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.
- No se puede agregar un nombre de dominio a WAF repetidamente.

  Cada combinación de un nombre de dominio 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, agregue el nombre de dominio y cada puerto a WAF.
- Puede introducir un nombre de dominio único de varios niveles , (por ejemplo, nombre de dominio de nivel superior ejemplo.com y nombre de dominio de nivel 2 www.example.com) o un nombre de dominio comodín (*.ejemplo.com).

Copyright © Huawei Technologies Co., Ltd.

AVISO

- Los nombres de dominio comodín no pueden contener guiones bajos (_).
- Las siguientes son las reglas para agregar comodines a los nombres de dominio:
  - 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.ejemplo.com, b.ejemplo.com y c.ejemplo.com tienen la misma dirección IP del servidor, puede agregar el nombre de dominio comodín *.ejemplo.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.

- WAF no admite encabezados HTTP definidos por el usuario para nombres de dominio protegidos.
- Solo los nombres de dominio que se han registrado con licencias ICP se pueden agregar a WAF.
- Se genera un registro CNAME basado en un nombre de dominio. Para el mismo nombre de dominio, los registros CNAME son los mismos.
- Solo se pueden utilizar certificados .pem en 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.
- WAF admite el protocolo WebSocket que está 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**.
- Si utiliza la edición estándar de WAF (anteriormente edición profesional), sólo se puede seleccionar **system-generated policy** para **Configure Policy**.
- Las políticas de seguridad WAF entran en vigor para las direcciones IP reales del cliente donde se inician las solicitudes. Para asegurarse de que WAF obtiene direcciones IP de cliente reales, si su sitio web tiene servidores proxy de capa 7 como CDN y productos de aceleración de nube implementados delante de WAF, seleccione **Yes** para **Proxy Configured**.

Limitaciones de la especificación

Después de que su sitio web esté conectado a WAF, el archivo que los visitantes pueden subir cada vez no puede exceder los 512 MB.

Impacto en el sistema

Si se configura un puerto no estándar, los visitantes deben agregar el puerto no estándar al final de la dirección del sitio web cuando acceden al sitio web. De lo contrario, se producirá un error 404. Si se produce un error 404, consulte **¿Cómo soluciono los errores 404/502/504?**

 Copyright © Huawei Technologies Co., Ltd.

Procedimiento

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.

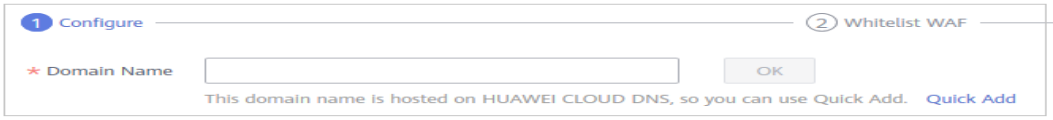
Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 In the navigation pane, choose **Website Settings**.

Paso 5 En la esquina superior izquierda de la lista de sitios web, haz clic en **Add Website**.

Paso 6 . Introduzca el **Domain Name** en el cuadro de texto Nombre de dominio y haga clic en **OK**.

Figura 3-4 Nombre de dominio



Puede introducir un nombre de dominio único de varios niveles (por ejemplo, nombre de dominio de nivel superior ejemplo.com y nombre de dominio de nivel 2 www.example.com) o un nombre de dominio comodín (*.ejemplo.com).

AVISO

- Los nombres de dominio de comodín no pueden contener guiones bajos (_).
- Las siguientes son las reglas para agregar comodines a los nombres de dominio:
  - 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.ejemplo.com, b.ejemplo.com y c.ejemplo.com tienen la misma dirección IP del servidor, puede agregar el nombre de dominio comodín *.ejemplo.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.

Si su nombre de dominio está alojado en Huawei Cloud, puede hacer clic en **Quick Add**. En el cuadro de diálogo **Select Domain Name** que se muestra, seleccione el nombre de dominio que desea proteger y haga clic en **OK**. El nombre de dominio alojado se agrega automáticamente.

Paso 7 Configura **Domain Name** y otros parámetros haciendo referencia a **Tabla 3-3**. **Figura 3-5** shows an example.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-5 Configuración de la configuración básica

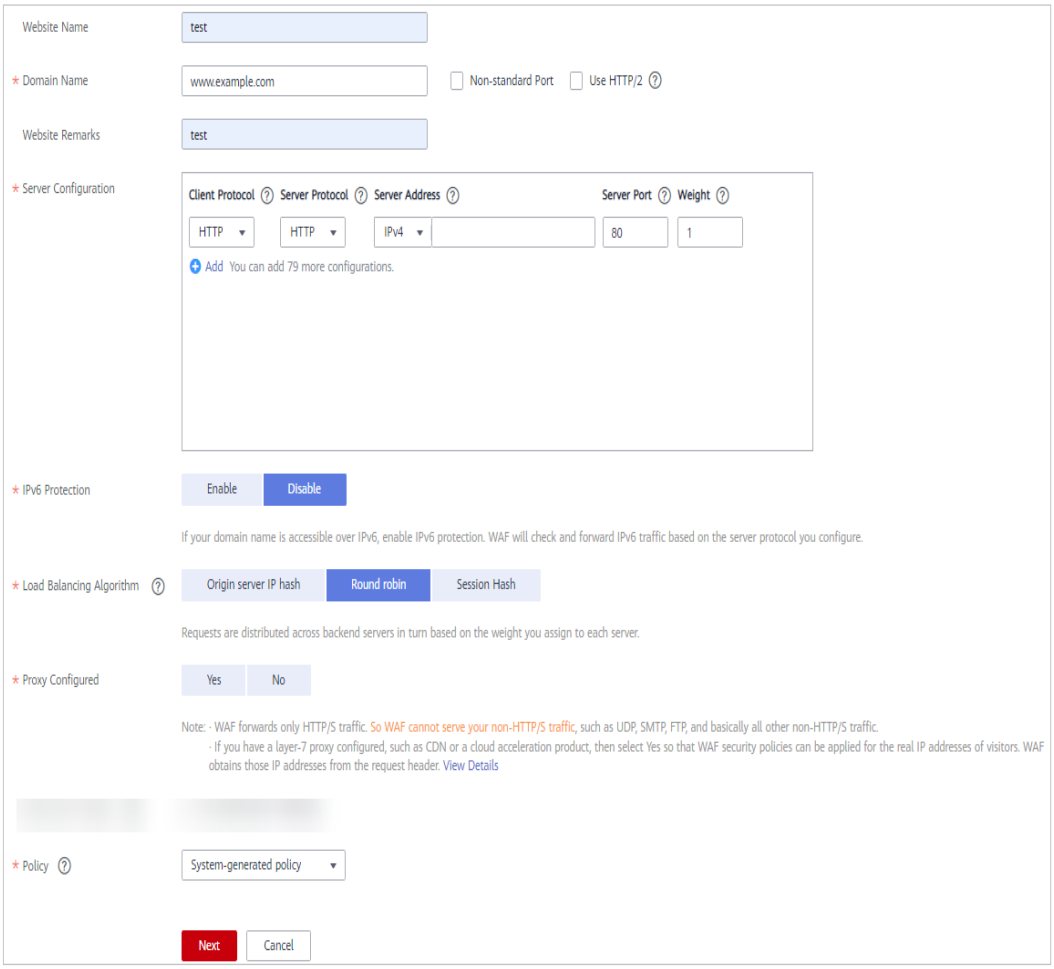


Tabla 3-3 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Website Name	Nombre del sitio web que desea proteger	N/A

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Domain Name	El nombre de dominio de un sitio web a ser protegido. Puede ser un solo nombre de dominio o un nombre de dominio comodín. ● Nombre de dominio único: Ingrese un nombre de dominio único. ● Nombre de dominio comodín: Ingrese un nombre de dominio comodín del sitio web que se va a proteger. Los nombres de dominio comodín no pueden contener guiones bajos (_). **NOTA** ● Si la dirección IP del servidor de cada nombre de subdominio es la misma, introduzca un nombre de dominio comodín. Por ejemplo, si los nombres de subdominio a.ejemplo.com, b.ejemplo.com y c.ejemplo.com tienen la misma dirección IP del servidor, puede agregar el nombre de dominio comodín *.ejemplo.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.	Nombre de dominio único **www.example.com** Nombre de dominio de nivel superior: example.com Nombre de dominio comodín: ***.example.com**
Website Remarks	(Opcional) Puede proporcionar comentarios sobre su sitio web si lo desea.	-
Non-standard Port	Establezca este parámetro sólo si se selecciona **Non-standard Port**. Para más detalles, consulte **Ejemplo de configuración 1: Protección del tráfico al mismo puerto estándar con diferentes direcciones IP del servidor de origen asignadas**. ● Si establece **Client Protocol** en **HTTP**, WAF protege los servicios en el puerto estándar 80 de forma predeterminada. Si establece **Client Protocol** en **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 **Non-standard Port** y seleccione un puerto no estándar de la lista desplegable de **Port**. Para obtener más información sobre los puertos no estándar soportados por WAF, consulte **¿Qué puertos no estándar soporta WAF?** **NOTA** Si se configura un puerto no estándar, los visitantes deben agregar el puerto no estándar al final de la dirección del sitio web cuando acceden al sitio web. De lo contrario, se producirá un error 404. Si se produce un error 404, consulte **¿Cómo soluciono los errores 404/502/504?**	81

Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Use HTTP/2	Si su sitio web necesita admitir el acceso HTTP/2, seleccione este parámetro. El protocolo 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**.	-
Website Remarks	Una breve descripción del sitio web	-
Server Configuration	Configuraciones de direcciones del servidor web, incluidos **Client Protocol**, **Server Protocol**, **Server Address**, y **Server Port**. ● **Client Protocol**: protocolo utilizado por un cliente para acceder a un servidor. Las opciones son **HTTP** y **HTTPS**. ● **Server Protocol**: protocolo utilizado por WAF para reenviar las solicitudes del cliente. Las opciones son **HTTP** y **HTTPS**. **NOTA** – Para obtener más información sobre cómo configurar **Client Protocol** y **Server Protocol**, consulte **Reglas para configurar el protocolo de cliente y el protocolo de servidor**. – WAF puede comprobar la solicitud WebSocket y WebSockets que está habilitada por defecto. ● **Server Address**: dirección IP pública (generalmente correspondiente al registro A del nombre de dominio configurado en el DNS) o nombre de dominio (generalmente correspondiente al CNAME del nombre de dominio configurado en el DNS) del servidor web al que accede un cliente. ● **Server Port**: puerto de servicio del servidor al que la instancia WAF reenvía las solicitudes del cliente.	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **Server Address**: XXX.XXX.1.1 **Server Port**: **80**

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Certificate Name	Si establece **Client Protocol** en **HTTPS**, se requiere un certificado SSL. Puede seleccionar un certificado creado o importar un certificado. Para obtener más información sobre cómo importar un certificado, consulte **Importación de un nuevo certificado**. Los certificados importados aparecen en la página **Certificates**. Para más detalles, consulte **Carga de un certificado**. Además, puede comprar un certificado en la consola SCM y enviarlo a WAF. Para obtener más información sobre cómo enviar un certificado SSL en SCM a WAF, consulte **Envío de un certificado SSL a otros servicios en la nube**. **AVISO** ● Solo se pueden utilizar certificados .pem en WAF. Si el certificado no está en formato in.pem, conviértelo en.pem haciendo referencia a **Tabla 3-5** antes de cargar el certificado. ● 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. ● Si su certificado de sitio web está a punto de caducar, compre un nuevo certificado antes de la fecha de caducidad y actualice el certificado asociado con el sitio web en WAF. ● Cada nombre de dominio debe tener un certificado asociado. Un nombre de dominio de carácter comodín solo puede usar un certificado de dominio de carácter comodín. Si solo tiene certificados de un solo dominio, agregue nombres de dominio uno por uno en WAF.	None
IPv6 Protection	● Si selecciona **IPv6** para **Server Address**, **IPv6 Protection** está habilitada de forma predeterminada. ● Si selecciona **IPv4** para **Server Address** y habilita **IPv6 Protection**, WAF asignará una dirección IPv6 al nombre de dominio para que el sitio web sea accesible a través de la dirección IPv6. De esta manera, las solicitudes a la dirección IPv6 son enrutadas por WAF a la dirección IPv4 del servidor de origen.	Enable

Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Load Balancing Algorithm	Seleccione un algoritmo de equilibrio de carga. ● **Origin server IP hash**: Las solicitudes de la misma dirección IP se enrutan al mismo servidor backend. ● **Weighted round robin**: Las solicitudes se distribuyen entre los servidores backend a su vez en función del peso que asigne a cada servidor. ● **Session hash**: Las solicitudes con la misma etiqueta de sesión se enrutan al mismo servidor de origen. Para habilitar este algoritmo, **configure identificadores de tráfico para fuentes de ataque conocidas**, o el algoritmo hash de sesión no puede tener efecto. Para más detalles, consulte **Cambio del algoritmo de equilibrio de carga**.	Weighted round robin

Paso 8 Configure **Proxy Configured**.

Si su sitio web tiene servidores proxy de capa 7, como CDN y productos de aceleración en la nube implementados delante de WAF, seleccione **Yes** para **Proxy Configured**. Esto asegura que WAF obtiene direcciones IP de cliente reales, ya que la protección WAF solo tiene efecto para direcciones IP de cliente reales donde se inician las solicitudes. Además, puede haber múltiples direcciones IP en el campo de dirección IP de origen. Para asegurarse de que WAF obtiene la dirección IP real del visitante que inicia la solicitud, agregue un identificador de tráfico IP para el sitio web protegido. (por ejemplo, se puede agregar **CDN-Src-IP** para un proxy CDN) Para más detalles, consulte **Configuración de un identificador de tráfico para un Known Attack Source**

AVISO

- Si se implementa un proxy antes de WAF en su sitio web, el modo de trabajo WAF no se puede cambiar a **Bypassed**. Para más detalles, consulte **Cambio de modo de trabajo WAF**.
- Si un sitio web no utiliza ningún proxy pero selecciona **Yes** para **Proxy Configured**, WAF confía en el campo **X-Forwarded-For** en el encabezado de solicitud HTTP al obtener la dirección IP de origen real. Por lo tanto, su negocio no se ve afectado.

Paso 9 Especifique **Configure Policy**. De forma predeterminada, se selecciona **system-generated policy**. Puede seleccionar reglas personalizadas. Para más detalles, consulte **Tabla 3-4**.

AVISO

Si utiliza la WAF o la edición estándar (anteriormente edición profesional), solo está disponible **System-generated policy**.

 Copyright © Huawei Technologies Co., Ltd.

Puede seleccionar una política que haya configurado. También puede personalizar las reglas después de que el nombre de dominio esté conectado a WAF.

Tabla 3-4 Políticas generadas por el sistema

Edición	Política	Descripción
Edición estándar (anteriormente edición profesional)	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.
Edición profesional (anteriormente edición empresarial) y edición platino (anteriormente premium)	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.

Paso 10 Haga clic en **Next**.

Se recomienda que omita este paso haciendo clic en **Next** y luego en **Finish**. Luego, conecte el nombre de dominio a WAF más tarde haciendo referencia a **Paso 2: Prueba de WAF** y **Paso 3: Enrutación del tráfico del sitio web a WAF**.

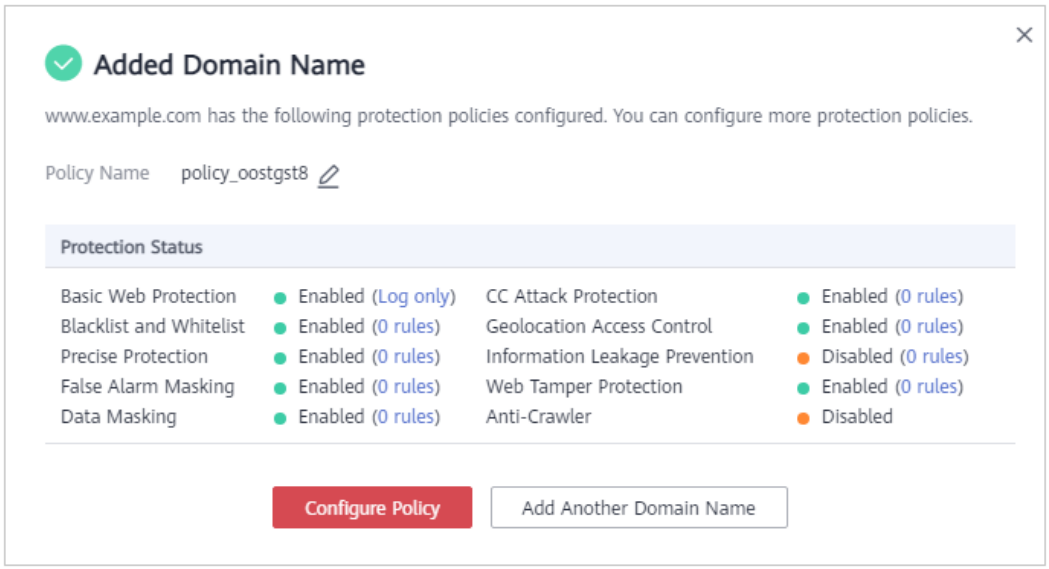
Se genera un registro CNAME basado en un nombre de dominio. Para el mismo nombre de dominio, los registros CNAME son los mismos.

 Copyright © Huawei Technologies Co., Ltd.

Paso 11 Haga clic en **Next** y, a continuación, **Finish**.

A continuación, puede ver el estado de acceso y el modo de trabajo para el nombre de dominio agregado en la página **Website Settings**.

Figura 3-6 Nombre de dominio agregado



- Para configurar una política de protección para el sitio Web, haga clic en **Configure Policy**.
- Para agregar más sitios web que proteger, haga clic en **Add Another Domain Name**.
- Para ver el sitio web agregado, cierre el cuadro de diálogo.

NOTA

- Si su servidor utiliza otros firewalls de red, deshabilite estos firewalls de red o agregue el intervalo de direcciones IP WAF a la lista blanca de direcciones IP de estos firewalls de red. De lo contrario, estos firewalls pueden considerar la dirección IP WAF como una dirección IP maliciosa. Para obtener más información, consulte **¿Cómo poner en lista blanca el intervalo de direcciones IP de origen WAF?**
- Si su servidor web utiliza software de seguridad personal, reemplácelo con software de seguridad empresarial y incluya en la lista blanca los intervalos de direcciones WAF IP.

----Fin

Verificación

- De forma predeterminada, WAF detecta **Access Status** de cada nombre de dominio protegido cada hora.
- Generalmente, si ha realizado la conexión de dominio y **Access Status** es **Accessible**, el nombre de dominio está conectado a WAF.

  Si un nombre de dominio se ha conectado a WAF pero **Access Status** es **Inaccessible**, haga clic para actualizar. Si **Access Status** sigue siendo **Inaccessible**, conecte el nombre de dominio a WAF de nuevo haciendo referencia a **Paso 3: Enrutación del tráfico del sitio web a WAF**.

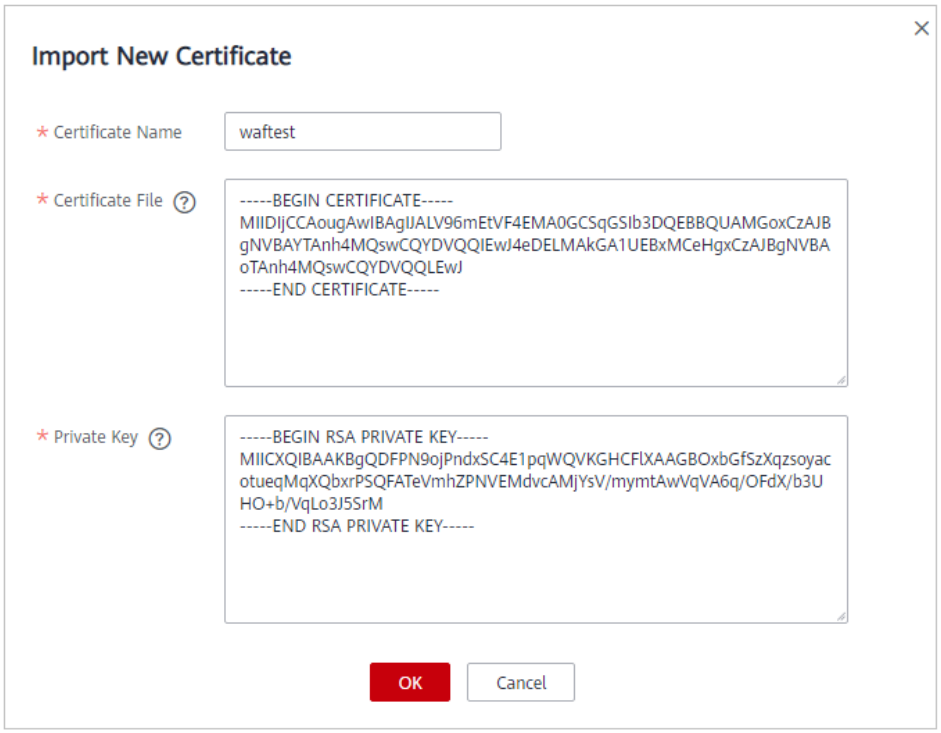
Copyright © Huawei Technologies Co., Ltd.

Importación de un nuevo certificado

Si establece **Client Protocol** en **HTTPS**, se requiere un certificado SSL. Puede realizar los siguientes pasos para importar un nuevo certificado.

1. Haga clic en **Import New Certificate**. En el cuadro de diálogo **Import New Certificate** que muestra, escriba el nombre del certificado y pegue el archivo de certificado y la clave privada en los cuadros de texto correspondientes. **Figura 3-7** shows an example.

Figura 3-7 Importar certificado nuevo



NOTA

WAF encripta y guarda la clave privada para mantenerla segura.

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 3-5** antes de cargarlo.

Tabla 3-5 Comandos de conversión de certificados

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

 Copyright © Huawei Technologies Co., Ltd.

Formato	Método de conversión
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

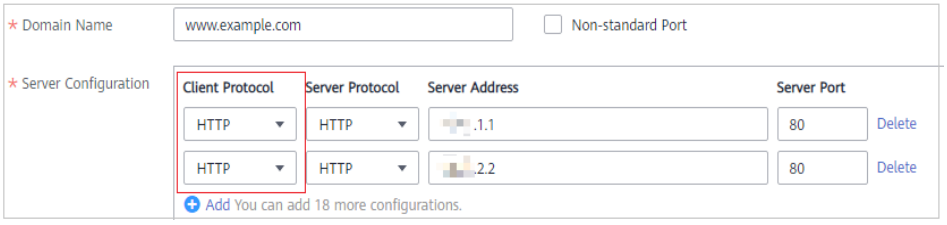
- Antes de ejecutar un comando OpenSSL, asegúrese de que la herramienta **OpenSSL** se haya instalado en el host local.
- Si su PC local ejecuta un sistema operativo Windows, vaya a la interfaz de línea de comandos (CLI) y, a continuación, ejecute el comando de conversión de certificados.

2. Haga clic en **OK**.

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

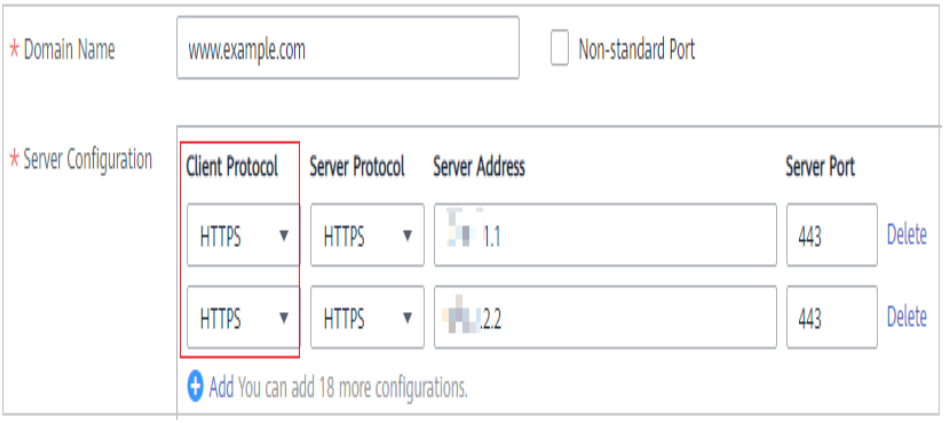
1. Anule la selección de **Non-standard Port**.
2. Seleccione **HTTP** o **HTTPS** para **Client Protocol**. **Figura 3-8** y **Figura 3-9** mostrar configuraciones de puerto estándar cuando el protocolo cliente es HTTP o HTTPS.

Figura 3-8 Puerto 80



 Copyright © Huawei Technologies Co., Ltd.

Figura 3-9 Puerto 443



NOTA

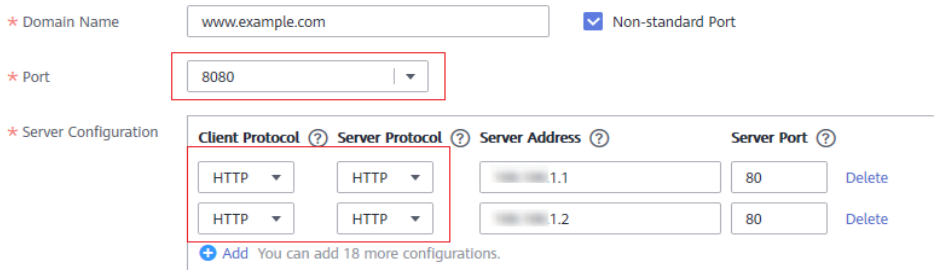
Si **Client Protocol** está establecido en **HTTPS**, se requiere un certificado.

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

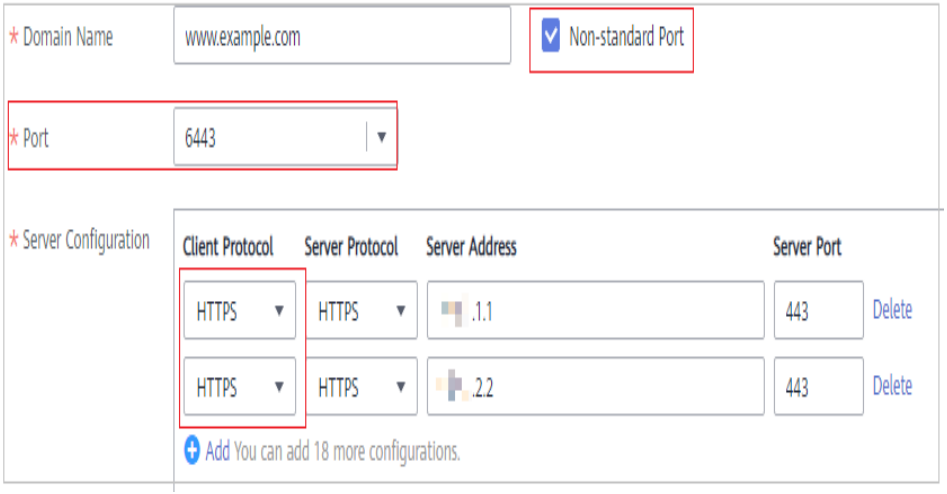
1. Seleccione **Non-standard Port** y seleccione un puerto no estándar que se va a proteger en la lista desplegable de **Port**. Para obtener más información sobre los puertos no estándar soportados por WAF, consulte **¿Qué puertos no estándar soporta WAF?**
2. Seleccione **HTTP** o **HTTPS** para **Client Protocol** para todos los puertos de servidor. **Figura 3-10** y **Figura 3-11** mostrar la configuración del puerto HTTP o HTTPS no estándar, respectivamente.

Figura 3-10 Otro puerto HTTP además del puerto 80



 Copyright © Huawei Technologies Co., Ltd.

Figura 3-11 Otro puerto HTTPS además del puerto 443



NOTA

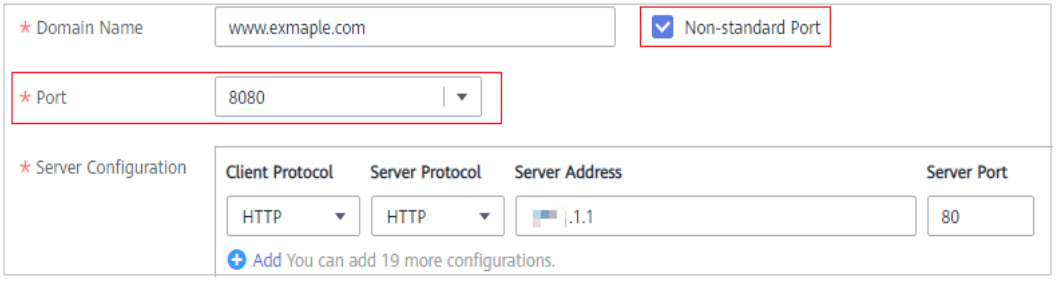
Si **Client Protocol** está establecido en **HTTPS**, se requiere un certificado.

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

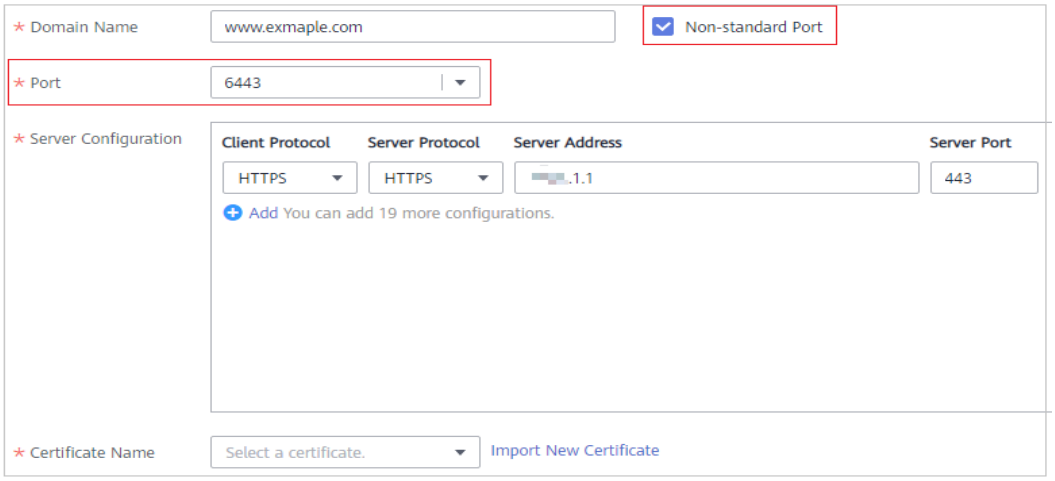
Si los puertos de servicio que se van a proteger son diferentes, configure los puertos por separado. Por ejemplo, para proteger los puertos 8080 y 6443 para su sitio **www.example.com**, agregue el dominio por separado para cada puerto, como se muestra en **Figura 3-12** y **Figura 3-13**.

Figura 3-12 Puerto de protección 8080



 Copyright © Huawei Technologies Co., Ltd.

Figura 3-13 Puerto de protección 6443

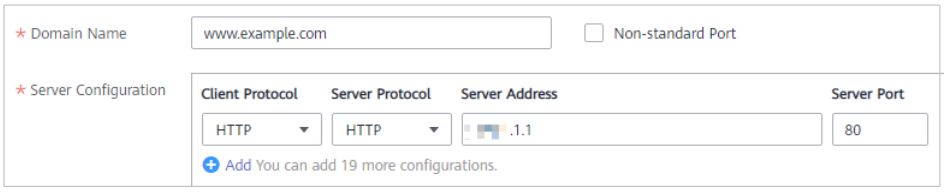


Reglas para configurar el protocolo de cliente y el protocolo de servidor

WAF proporciona varios tipos de protocolo. Si su sitio web es de www.example.com, WAF proporciona los siguientes cuatro modos de acceso:

- Método HTTP (**Figura 3-14**)

  Figura 3-14 Modo HTTP

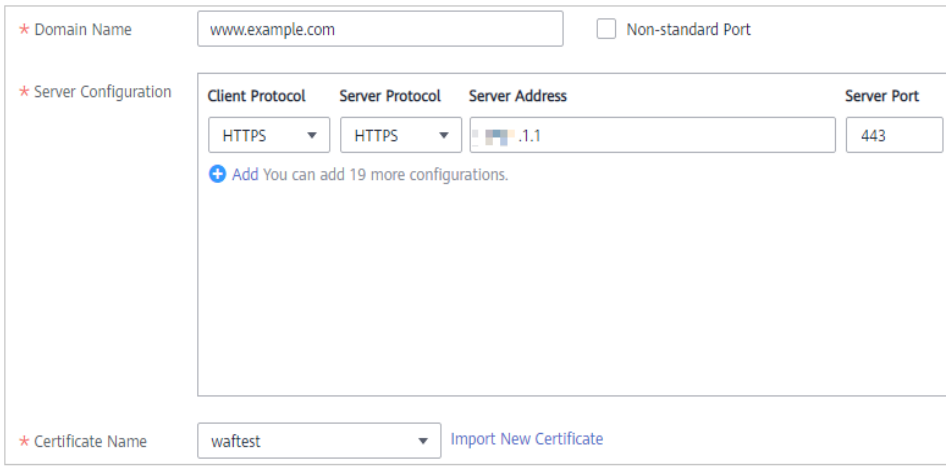
  AVISO

  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.

- Método HTTPS. Esta configuración permite que los visitantes de la web accedan a su sitio web a través de HTTPS solamente. Si acceden a él a través de HTTP, son redirigidos a la HTTPS URL. **Figura 3-15** shows an example.This configuration allows web visitors to access your website over HTTPS only. If they access it over HTTP, they are redirected to the HTTPS URL.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-15 Modo HTTPS

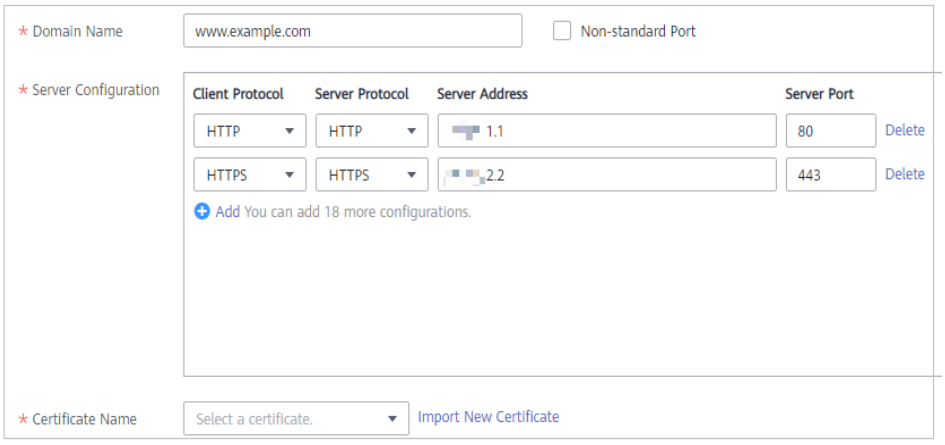


AVISO

- 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.

- Método de reenvío HTTP/HTTPS. **Figura 3-16** shows an example.

Figura 3-16 Modos HTTP y HTTPS



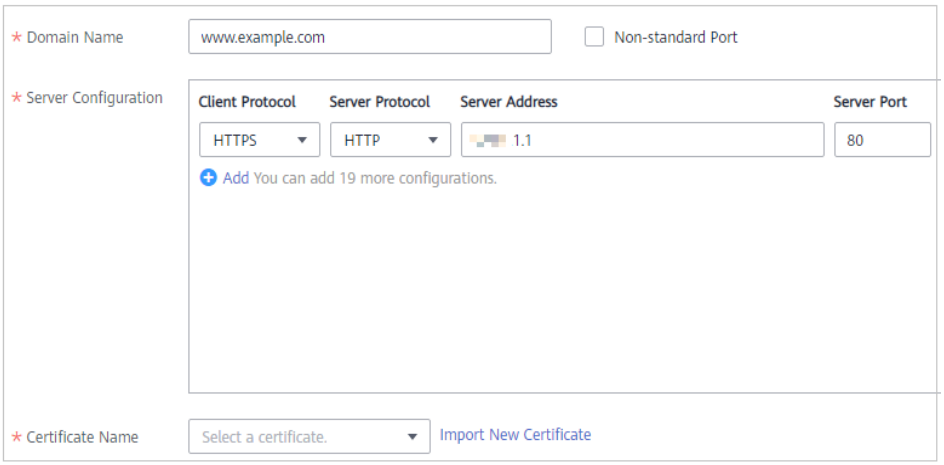
AVISO

- 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.

 Copyright © Huawei Technologies Co., Ltd.

- Descarga de HTTPS por WAF. **Figura 3-17** shows an example.

Figura 3-17 Descarga de HTTPS



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.

3.2.3 Paso 4: Lista blanca de direcciones IP WAF Back-to-Source

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?

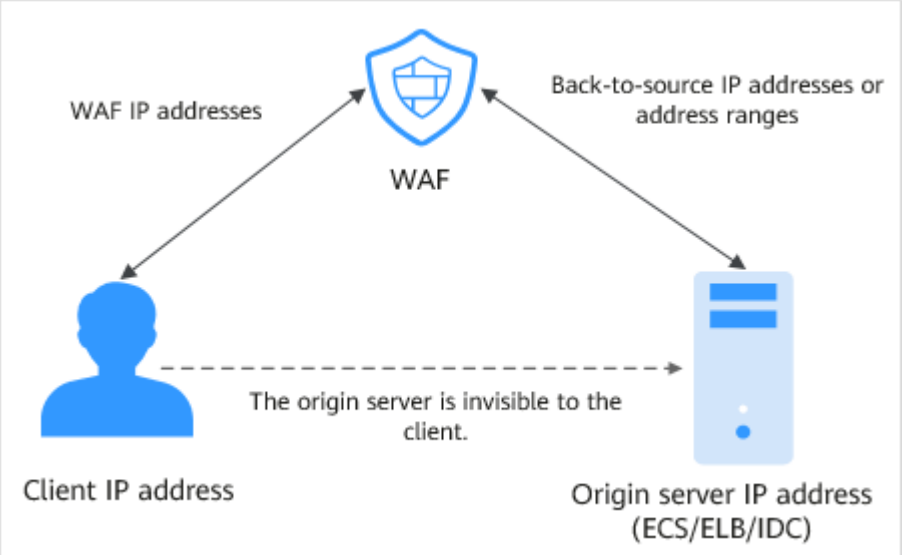
Desde la perspectiva de un servidor, todas las solicitudes web se originan en WAF. Las direcciones IP utilizadas por el reenvío WAF son direcciones IP de origen de WAF. La dirección IP real del cliente se escribe en el campo de encabezado HTTP X-Forwarded-For (XFF).

 Copyright © Huawei Technologies Co., Ltd.

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 3-18 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**.

 Copyright © Huawei Technologies Co., Ltd.

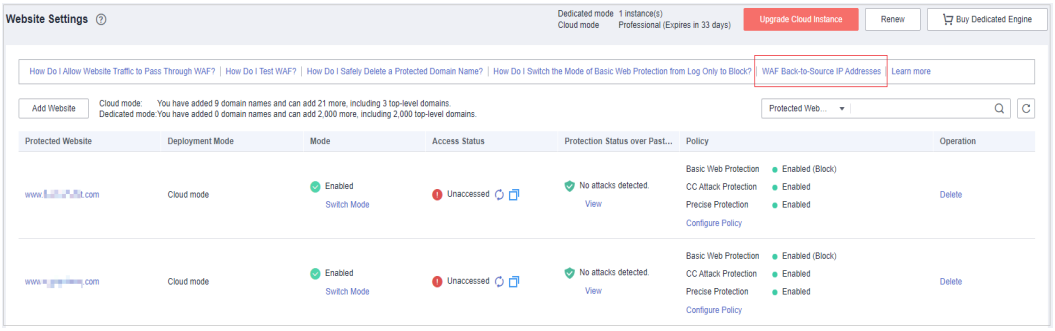
Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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**.

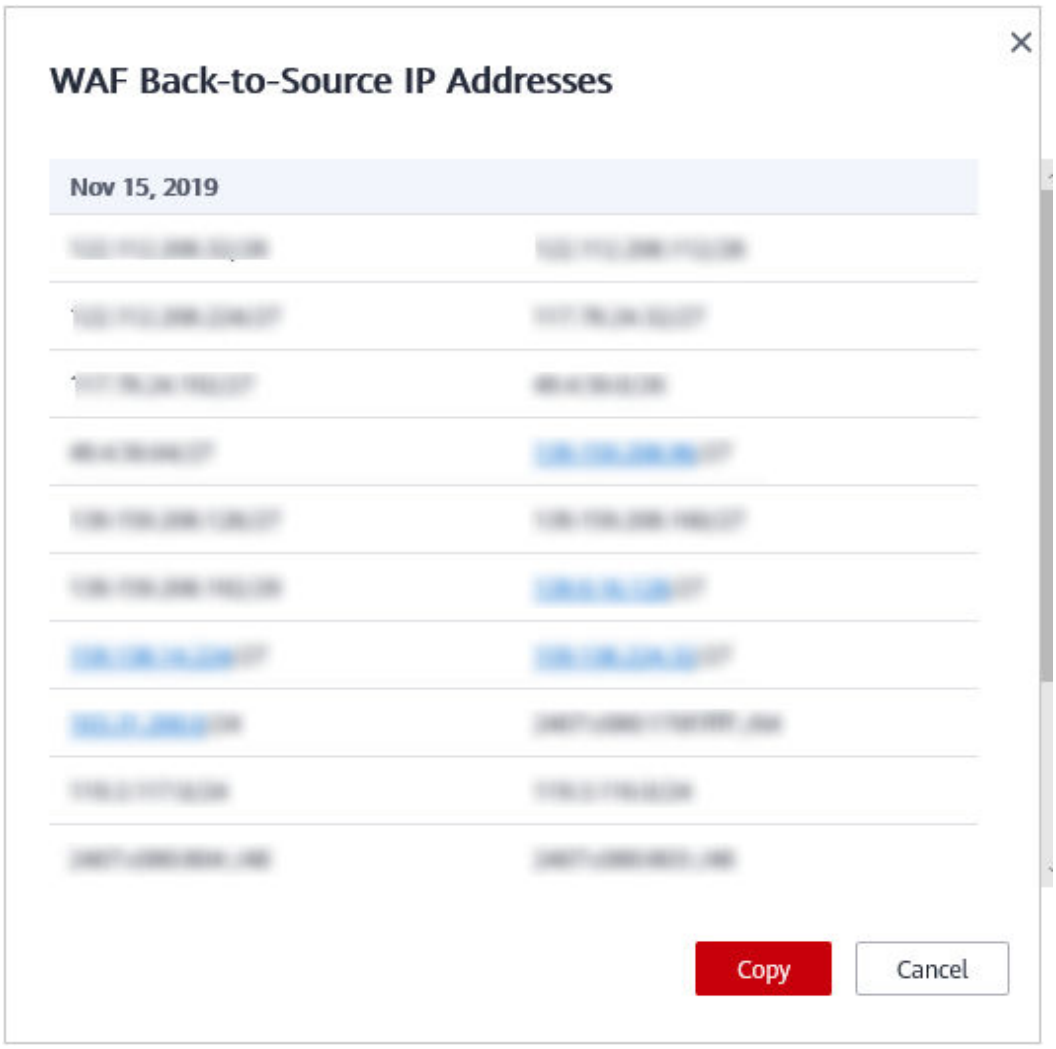
Figura 3-19 Direcciones IP de Back-to-Source de WAF



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

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-20 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

 Copyright © Huawei Technologies Co., Ltd.

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**.

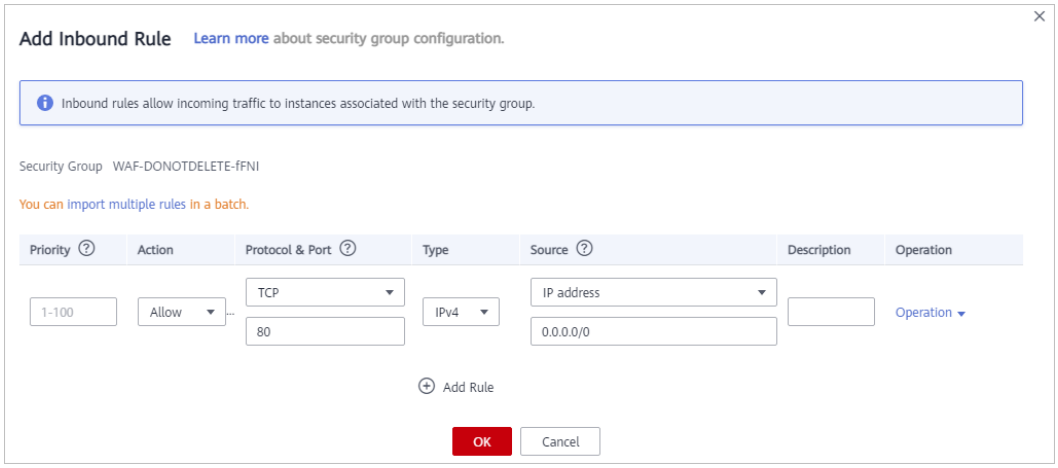
Paso 4 Localice la fila que contiene el ECS que aloja su sitio web. En la columna **Name/ID**, haga clic en el nombre de ECS para ir a la página de detalles de ECS.

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 3-6**. **Figura 3-21** muestra un ejemplo.

Figura 3-21 Agregar regla de entrada



 Copyright © Huawei Technologies Co., Ltd.

Tabla 3-6 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

 Copyright © Huawei Technologies Co., Ltd.

3.2.4 Paso 2: Prueba de WAF

Para asegurarse de que WAF puede reenviar sus solicitudes de sitio web normalmente, pruebe WAF localmente después de agregar el dominio a WAF.

Antes de probar WAF, asegúrese de que el protocolo, la dirección y el puerto utilizados por el servidor de origen (por ejemplo, **www.example5.com**) son correctos. Además, si **Client Protocol** está establecido en **HTTPS**, asegúrese de que el certificado cargado y la clave privada son correctos.

Prerrequisitos

Se ha agregado un nombre de dominio a WAF.

Restricciones

Se genera un registro CNAME basado en el nombre de dominio. Para el mismo nombre de dominio, los registros CNAME son los mismos.

Conexión de un nombre de dominio a WAF localmente

Paso 1 Obtener el registro CNAME.

- Si va a agregar un nombre de dominio, realice las siguientes operaciones para obtener el registro CNAME del nombre de dominio después de configurar la información básica sobre el nombre de dominio:

  Haga clic en **Copy** para obtener el registro CNAME del nombre de dominio. Vea **Figura 3-22** o **Figura 3-23**.

  Figura 3-22 Conexión de un nombre de dominio a WAF (proxy usado)

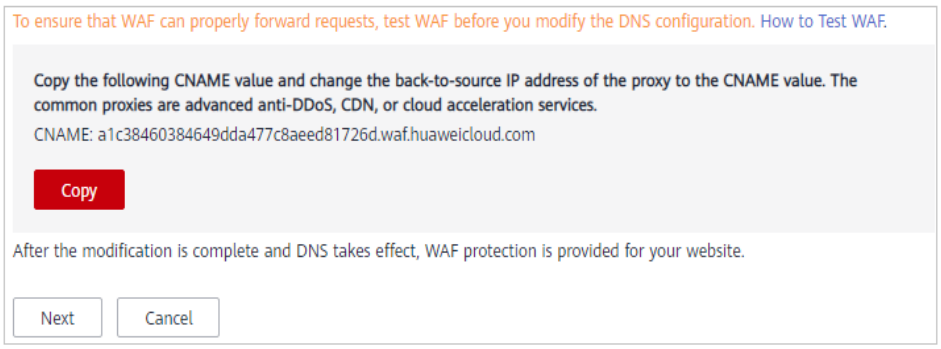
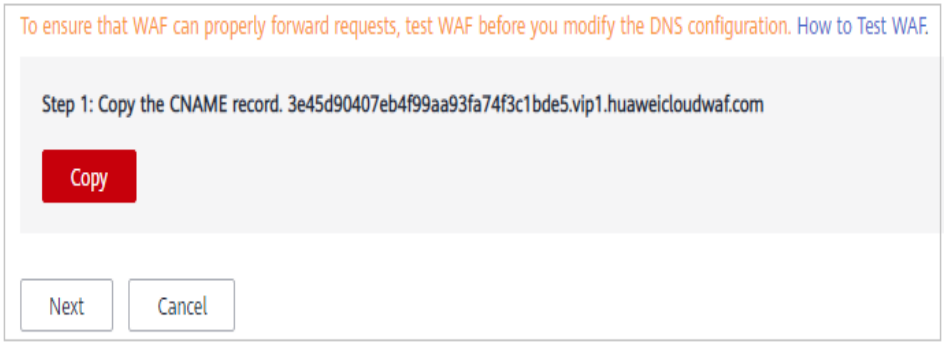
  

  Figura 3-23 Conexión de un nombre de dominio a WAF (no proxy used)

 Copyright © Huawei Technologies Co., Ltd.

- Si ha agregado un nombre de dominio, realice los siguientes pasos para obtener el registro CNAME del nombre de dominio:

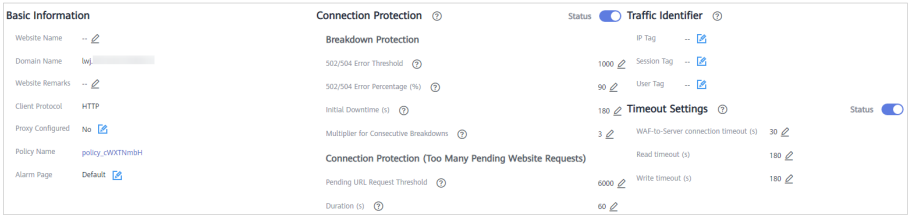
  a. Haga clic en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

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

  d. En la fila del nombre de dominio deseado, en la columna **Protected Website**, haga clic en el nombre de dominio que desea probar.

  Figura 3-24 Información básica

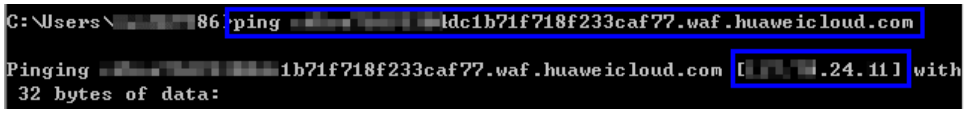
  e. En la fila **CNAME**, haga clic en p para copiar el registro CNAME.

Paso 2 Haga ping al registro CNAME y registre la dirección IP correspondiente.

Utilice **www.example5.com** como ejemplo y su registro CNAME es **xxxxxxxdc1b71f718f233caf77.waf.huaweicloud.com**.

Abra la CLI y ejecute el comando **ping xxxxxxxdc1b71f718f233caf77.waf.huaweicloud.com** para obtener la dirección IP de origen WAF. Como se muestra en **Figura 3-25**, se muestra la dirección IP de origen WAF.

Figura 3-25 Ping CNAME

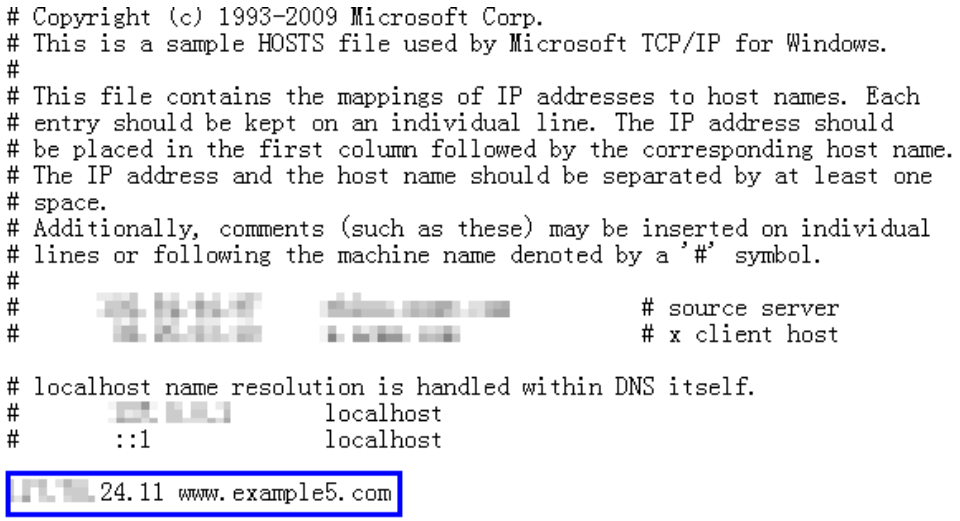


Paso 3 Agregue el nombre de dominio y la dirección IP de origen WAF al archivo **hosts**.

1. Utilice un editor de texto para abrir el archivo **hosts**. Generalmente, el archivo **hosts** se almacena en el directorio **C:\Windows\System32\drivers\etc**.
2. Agregue la dirección IP de origen WAF obtenida en **paso 2** y el nombre de dominio protegido al archivo **hosts**. **Adición de un registro** se muestra un ejemplo.

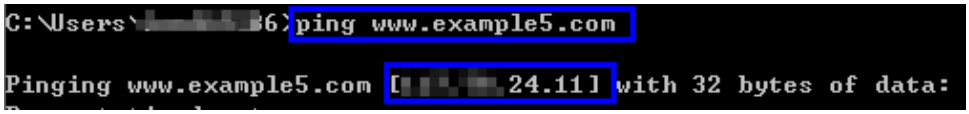
 Copyright © Huawei Technologies Co., Ltd.

Figura 3-26 Adición de un registro



3. Guarde el archivo **hosts** y haga ping al nombre de dominio protegido en el PC local.

Figura 3-27 Hacer ping al nombre de dominio



Se espera que la dirección IP resuelta sea la dirección IP de origen WAF obtenida en **paso 2**. Si la dirección IP resuelta es la dirección del servidor de origen, ejecute el comando **ipconfig/flushdns** en el sistema operativo Windows para vaciar la caché DNS.

----Fin

Comprobación de si el reenvío de WAF es normal

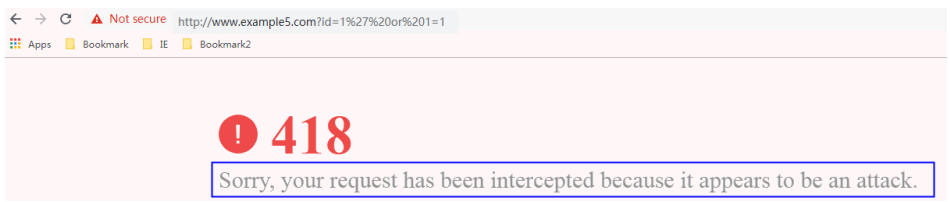
Paso 1 Borre la caché del navegador e introduzca el nombre de dominio en el cuadro de dirección de un navegador para comprobar si se puede acceder al sitio web.

Si el nombre de dominio se resuelve a la dirección IP de origen de las configuraciones WAF y WAF son correctas, se puede acceder al sitio web.

Paso 2 Simula comandos simples de ataque web.

1. Establezca el modo de **Basic Web Protection** en **Block**. Para obtener más información, consulte **Habilitación de la protección web básica**.
2. Borre la caché del navegador, introduzca el nombre de dominio de prueba en la barra de direcciones y compruebe si WAF bloquea el ataque de inyección SQL simulado en el nombre de dominio. **Figura 3-28** muestra un ejemplo.

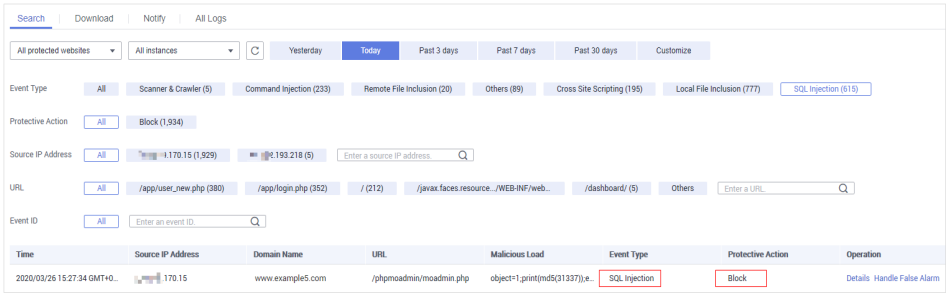
Figura 3-28 Solicitud bloqueada



 Copyright © Huawei Technologies Co., Ltd.

3. En el panel de navegación, elija **Events** para ver los datos de prueba. **Figura 3-29** muestra un ejemplo.

Figura 3-29 Consulta de datos de prueba



----Fin

3.2.5 Paso 3: Enrutación del tráfico del sitio web a WAF

Después de conectar un nombre de dominio 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.

Para asegurarse de que su instancia WAF funciona correctamente, pruébela de acuerdo con las instrucciones en **Paso 2: Prueba de WAF** antes de enrutar el tráfico de su empresa a WAF.

Prerrequisitos

Se ha agregado un nombre de dominio a WAF pero no está conectado a WAF.

Restricciones

La protección WAF solo tiene efecto para las direcciones IP reales de los clientes donde se originan las solicitudes. Para asegurarse de que WAF obtiene direcciones IP de cliente reales, si su sitio web tiene proxys de capa 7 como CDN y productos de aceleración de nube implementados delante de WAF, se debe seleccionar **Yes** para **Proxy Configured**.

Limitaciones de la especificación

Después de que su sitio web esté conectado a WAF, el archivo que los visitantes pueden subir cada vez no puede exceder los 512 MB.

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

 Copyright © Huawei Technologies Co., Ltd.

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 3-7**.

Tabla 3-7 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

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 In the navigation pane, choose **Website Settings**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 5 En la columna **Protected Website**, haga clic en el nombre de dominio para ir a la página **Basic Information**.

Paso 6 En la fila **CNAME**, haga clic en para copiar el registro CNAME. **Figura 3-30** muestra un ejemplo.

Figura 3-30 Copia del registro CNAME

Si se muestra el mensaje "CNAME copiado correctamente" en la esquina superior derecha de la página, el registro CNAME se copia correctamente.

Paso 7 Conecte el nombre de dominio a WAF.

- No proxy used

  Configure el registro CNAME en su proveedor DNS. Para obtener más información, póngase en contacto con su proveedor de DNS.

  A continuación, se utiliza Huawei Cloud DNS como ejemplo para mostrar cómo configurar un registro CNAME. Si la siguiente configuración no es coherente con la configuración, utilice la información proporcionada por los proveedores DNS.

- Proxy used

  AVISO

  Si su sitio web tiene proxies, como anti-DDoS avanzado, Red de entrega de contenido (CDN) y servicio de aceleración en la nube, establezca **Proxy configured** en **Yes** para asegurarse de que las políticas de seguridad WAF surtan efecto. Para más detalles, consulte **Consulta de información básica**.

  Cambie la dirección IP de origen del proxy usado, como los servicios anti-DDoS y CDN, al registro CNAME copiado.

  NOTA

  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.

  1. Obtener **Subdomain Name** y **TXT Record**: En la fila de **Access Status**, haga clic en **How to Access**. En el cuadro de diálogo **Access Guide**, copie **Subdomain Name** y **TXT Record**.
  2. Agregue **Subdomain Name** en el proveedor DNS y configure **TXT Record** para el nombre del subdominio. Para obtener más información sobre el método de configuración, consulte **¿Cuáles son los impactos si un nombre de subdominio y un registro TXT no están configurados?**

  WAF determina qué usuario posee el nombre de dominio basándose en **Subdomain Name** and **TXT Record** configurados.

Paso 8 Verifique que se haya configurado el CNAME del nombre de dominio.

 Copyright © Huawei Technologies Co., Ltd.

1. En Windows, elija **Start** > **Run**. A continuación, introduzca **cmd** y **Enter**.
2. Ejecute un comando **nslookup** para consultar el registro CNAME.

   Si se devuelve el CNAME configurado, la configuración se realiza correctamente. Se muestra una respuesta de comando de ejemplo en **Figura 3-31**.

   Comando de ejemplo:

   ```
   nslookup www.example.com
   ```

   Figura 3-31 Consulta del CNAME

----Fin

Procedimiento posterior

- Si su servidor utiliza otros firewalls de red, deshabilite estos firewalls de red o agregue el intervalo de direcciones IP WAF a la lista blanca de direcciones IP de estos firewalls de red. De lo contrario, estos firewalls pueden considerar la dirección IP WAF como una dirección IP maliciosa. Para obtener más información, consulte **¿Cómo poner en lista blanca el intervalo de direcciones IP de origen WAF?**
- Si su servidor web utiliza software de seguridad personal, reemplácelo con software de seguridad empresarial y incluya en la lista blanca los intervalos de direcciones WAF IP.

Verificación

- De forma predeterminada, WAF detecta **Access Status** de cada nombre de dominio protegido cada hora.
- Generalmente, si ha realizado la conexión de dominio y **Access Status** es **Accessible**, el nombre de dominio está conectado a WAF.

Otras operaciones

- **¿Por qué el sistema me indica que mi conjunto de registros está en conflicto con uno existente?**
- **¿Cuáles son los impactos si un nombre de subdominio y un registro TXT no están configurados?**

3.3 Conexión de un sitio web a WAF (Modo dedicado)

3.3.1 Proceso de conexión (Modo dedicado)

Para permitir que su instancia WAF dedicada proteja su sitio web, el nombre de dominio del sitio web debe estar conectado a la instancia WAF para que el tráfico entrante del sitio web pueda ir primero a WAF.

 Copyright © Huawei Technologies Co., Ltd.

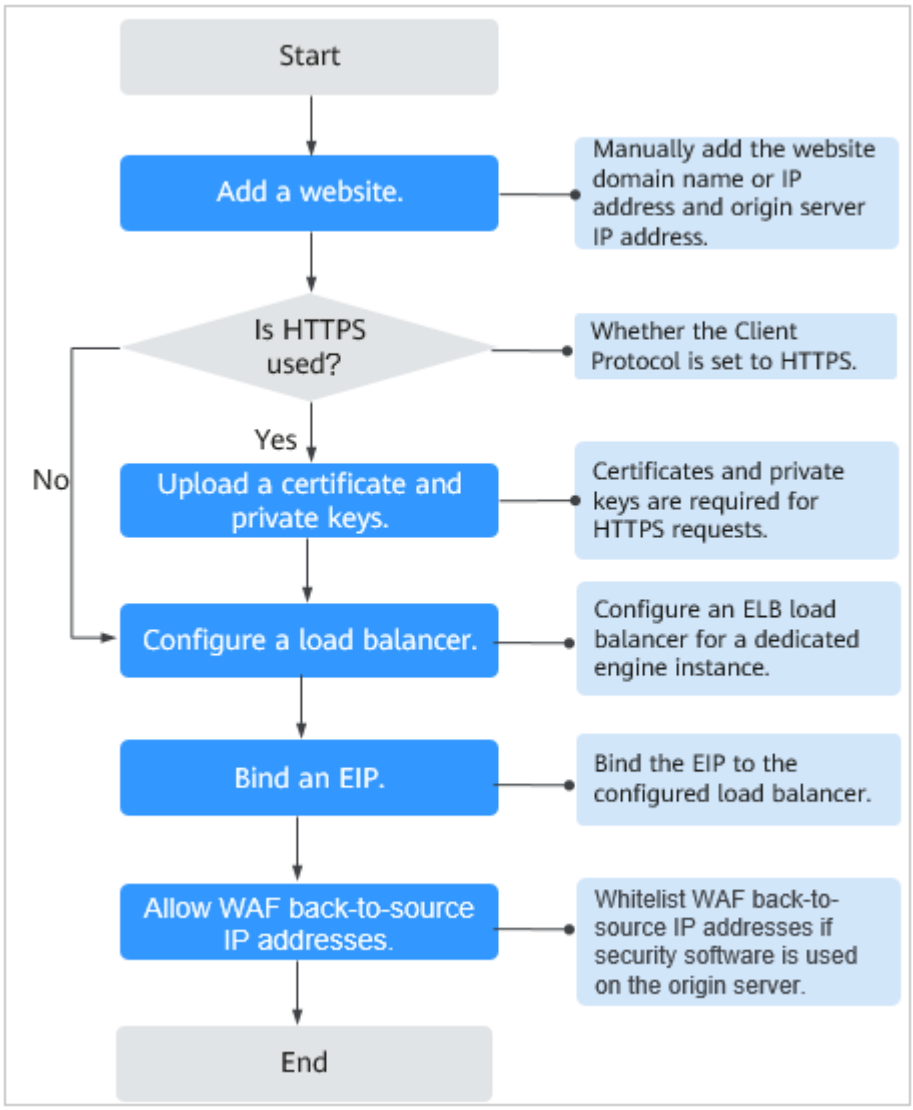
Restricciones

Las instancias WAF dedicadas solo pueden proteger las aplicaciones web y los sitios web que se implementan en Huawei Cloud y se pueden acceder a través de nombres de dominio o direcciones IP. Para obtener más información sobre las instancias dedicadas WAF, consulte **Diferencias de edición**.

Procesos de conexión de un sitio web a WAF

Después de comprar una instancia WAF dedicada, complete las configuraciones requeridas siguiendo el proceso que se muestra en **Figura 3-32**.

Figura 3-32 Proceso de conexión de un sitio web a una instancia WAF dedicada



Arreglar sitios web inaccesibles

Si un sitio web no se conecta a WAF, su estado de acceso es **Inaccessible**. Para solucionar este problema, consulte **¿Por qué es inaccesible el estado de acceso de un nombre de dominio o una dirección IP?**

Copyright © Huawei Technologies Co., Ltd.

3.3.2 Paso 1: Agregar un sitio web a WAF (modo dedicado)

Si sus servidores de servicio se implementan en Huawei Cloud, puede agregar el nombre de dominio o la dirección IP del sitio web a WAF para que el tráfico del sitio web se reenvíe a WAF para su inspección.

NOTA

Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable de **Enterprise Project** y agregar sitios web para protegerse en el proyecto.

Prerrequisitos

- Ha comprado una instancia de WAF dedicada.
- El nombre de dominio o la dirección IP se ha registrado con la licencia ICP pero no se ha agregado a WAF.

Restricciones

- Se ha implementado un balanceador de carga orientado a Internet en el sitio web que desea proteger con instancias de WAF dedicadas.
- Si su sitio web no tiene un servidor proxy de capa 7 como CDN y un servicio de aceleración en la nube desplegado frente a WAF y utiliza solo balanceadores de carga de capa 4 (o NAT), establezca **Proxy Configured** en **No**. De lo contrario, **Proxy Configured** debe estar establecido en **Yes**. Esto garantiza que WAF obtenga direcciones IP reales de los visitantes del sitio web y tome medidas de protección configuradas en las políticas de protección.
- Los nombres de dominio de los sitios web a proteger deben tener licencias ICP. De lo contrario, los nombres de dominio no se pueden agregar a WAF.

Recopilación de información de nombre de dominio/dirección IP

Antes de agregar un nombre de dominio o una dirección IP, obtenga la información que aparece en **Tabla 3-8**.

Tabla 3-8 Nombre de dominio o detalles de la dirección IP requeridos

Información	Parámetro	Descripción	Valor de ejemplo
Parámetros	Domain Name/IP Address	● 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

Copyright © Huawei Technologies Co., Ltd.

Información	Parámetro	Descripción	Valor de ejemplo
	Standard/ Non-standard Port	El puerto de servicio correspondiente al nombre de dominio del sitio web que desea proteger. ● Puertos estándares – 80: puerto predeterminado cuando el protocolo cliente se establece en HTTP – 443: puerto predeterminado cuando el protocolo cliente se establece en 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 obtener más información, consulte **¿Qué puertos no estándar pueden proteger WAF?**	80
	Client Protocol	Protocolo utilizado por un cliente (por ejemplo, un navegador) para acceder al sitio web. WAF soporta HTTP y HTTPS.	HTTP
	Server Protocol	Protocolo utilizado por WAF para reenviar solicitudes al cliente (como un navegador). Las opciones son **HTTP** y **HTTPS**.	HTTP
	VPC	Seleccione la VPC a la que pertenece la instancia WAF dedicada.	vpc-predeterminado
	Server Address	Dirección IP privada o nombre de dominio del servidor web al que accede un cliente (por ejemplo, un navegador)	192.168.1.1

Copyright © Huawei Technologies Co., Ltd.

Información	Parámetro	Descripción	Valor de ejemplo
(Opcional) Certificado	None	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 convierto un certificado en formato PEM?** ● Actualmente, los certificados adquiridos en Huawei Cloud SCM solo se pueden enviar al proyecto empresarial **default**. Para otros proyectos empresariales, los certificados SSL enviados por SCM no se pueden utilizar.	None

Procedimiento

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 la esquina superior izquierda de la lista de sitios web, haz clic en **Add Website**.

Paso 5 Configurar la información básica del nombre de dominio. **Figura 3-33** muestra uln ejemplo. **Tabla 3-9** lists parameters.lists parameters.lists parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-33 Configuración de la configuración básica de un sitio web

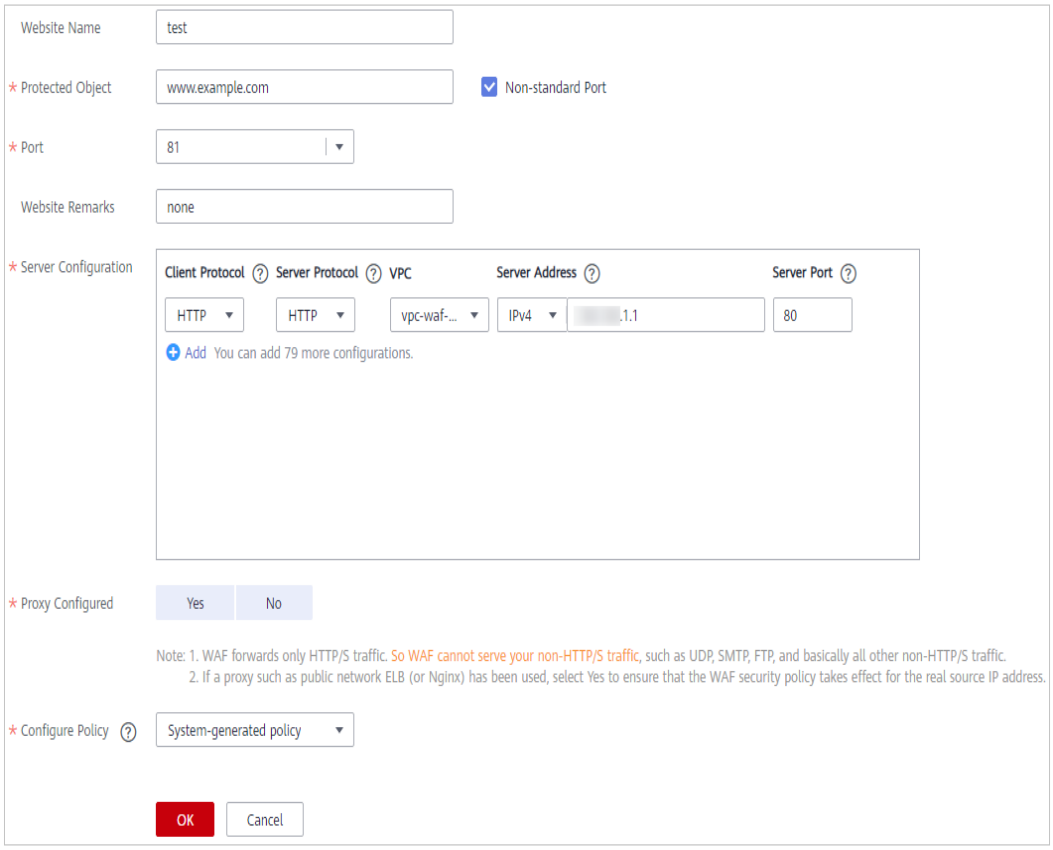


Tabla 3-9 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Website Name	Nombre del sitio web que desea proteger	None

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Protected Website	Un nombre de dominio o dirección IP del sitio web que se va a proteger. El nombre de dominio puede ser un nombre de dominio único o un nombre de dominio de carácter comodín. ● Nombre de dominio único: Ingrese un nombre de dominio único. Por ejemplo, el www.example.com. ● Nombre de dominio carácter comodín **NOTA** Los nombres de dominio de comodín no pueden contener guiones bajos (_). – 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*** 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.	Nombre de dominio único **www.example.com** Nombre de dominio comodín: ***.example.com** Formato de dirección IP: *XXX.XXX.1.1*
Port	Establezca este parámetro sólo si se selecciona **Non-standard Port**. **Ejemplo de configuración 1: Protección del tráfico al mismo puerto estándar con diferentes direcciones IP del servidor de origen asignadas** muestra un ejemplo de 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 **Non-standard Port** y seleccione un puerto no estándar de la lista desplegable de **Port**. Para obtener más información sobre los puertos no estándar soportados por WAF, consulte **¿Qué puertos no estándar soporta WAF?** **NOTA** Si se configura un puerto no estándar, los visitantes deben agregar el puerto no estándar al final de la dirección del sitio web cuando acceden al sitio web. De lo contrario, se producirá un error 404. Si se produce un error 404, consulte **¿Cómo soluciono los errores 404/502/504?**	81
Website Remarks	Una breve descripción del sitio web	-

Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Server Configuration	Dirección del servidor de web. La configuración contiene el **protocolo del cliente**, el **protocolo del servidor**, la VPC, la **dirección del servidor** y el **puerto del servidor**. ● **Protocolo de cliente**: Protocolo utilizado para reenviar solicitudes de cliente a la instancia WAF dedicada. Las opciones son **HTTP** y **HTTPS**. ● **Protocolo de servidor**: Protocolo utilizado para reenviar una solicitud de cliente al servidor de origen a través de la instancia WAF dedicada. Las opciones son **HTTP** y **HTTPS**. **NOTA** – Para obtener más información sobre cómo configurar el **Client Protocol** y el **Server Protocol**, consulte **Reglas para configurar el protocolo de cliente y el protocolo de servidor**. – WAF puede comprobar las solicitudes WebSocket y WebSockets que están habilitadas por defecto. ● **VPC**: Seleccione la VPC a la que pertenece la instancia WAF dedicada. ● **Dirección del servidor**: Dirección IP privada o nombre de dominio del servidor del sitio web al que accede un cliente (por ejemplo, un navegador). ● **Puerto del servidor**: puerto de servicio del servidor al que la instancia WAF dedicada reenvía las solicitudes del cliente.	**Protocolo de cliente**: **HTTP** **Protocolo de servidor**: **HTTP** **VPC**: vpc-default **Dirección del servidor**: *192.168.1.1* **Server Port**: **80**

Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Certificate Name	Si el **protocolo de cliente** está establecido en **HTTPS**, seleccione un certificado. Puede seleccionar un certificado existente o importar un certificado externo. Para obtener más información sobre cómo importar un certificado, consulte **Importación de un nuevo certificado**. Para obtener más información sobre cómo crear un certificado, consulte **Carga de un certificado**. Además, puede comprar un certificado en la consola SCM y enviarlo a WAF. Para obtener más información sobre cómo enviar un certificado SSL en SCM a WAF, consulte **Envío de un certificado SSL a otros servicios en la nube**. **AVISO** ● Solo se pueden utilizar certificados .pem en WAF. Si el certificado no está en formato.pem, conviértelo en un certificado.pem haciendo referencia a **Importación de un nuevo certificado** antes de cargar el certificado. ● Actualmente, los certificados adquiridos en Huawei Cloud SCM solo se pueden enviar al proyecto empresarial **default**. Para otros proyectos empresariales, los certificados SSL enviados por SCM no se pueden utilizar. ● Cada nombre de dominio debe tener un certificado asociado. Un nombre de dominio de carácter comodín solo puede usar un certificado de dominio de carácter comodín. Si solo tiene certificados de dominio único, agregue nombres de dominio a WAF uno por uno.	None

Paso 6 Configurar **Proxy Configured**.

Si su sitio web no tiene un servidor proxy de capa 7 como CDN y un servicio de aceleración en la nube desplegado frente a WAF y utiliza solo balanceadores de carga de capa 4 (o NAT), establezca **Proxy Configured** en **No**. De lo contrario, **Proxy Configured** debe estar establecido en **Yes**. Esto garantiza que WAF obtenga direcciones IP reales de los visitantes del sitio web y tome medidas de protección configuradas en las políticas de protección.

Paso 7 Seleccione una política. De forma predeterminada, se selecciona **system-generated policy**.

Puede seleccionar una política que haya configurado. También puede personalizar las reglas después de que el nombre de dominio esté conectado a WAF.

Políticas generadas por el sistema:

- 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**)

 Copyright © Huawei Technologies Co., Ltd.

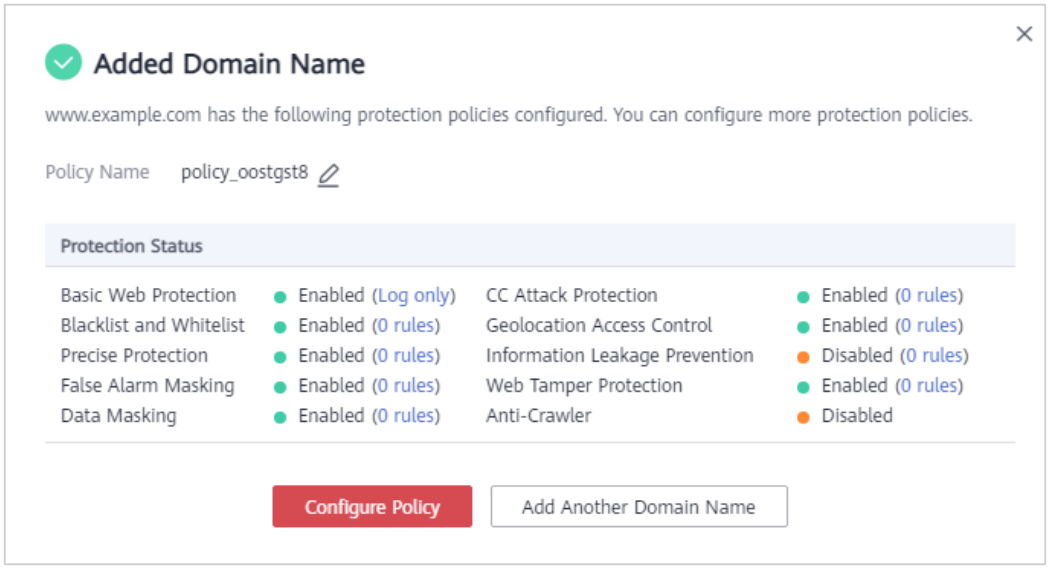
WAF solo registra tareas de análisis web, como análisis de vulnerabilidades y análisis de virus, como el comportamiento de rastreo de OpenVAS y Nmap.

NOTA

Log only: WAF solo registra los eventos de ataque detectados en lugar de bloquearlos.

Paso 8 Haga clic en **OK**.

Figura 3-34 Nombre de dominio agregado



- Haga clic en **Configure Policy** y configure una política de protección para el sitio web.
- Haga clic en **Add Another Domain Name** y agregue más sitios web para protegerse.
- Cierre el cuadro de diálogo y vea los sitios web agregados en la lista de sitios web protegidos.

----Fin

Verificación

El **estado de acceso** inicial de un sitio web es **Inaccesible**. Después de configurar un balanceador de carga y vincular un EIP al balanceador de carga de su sitio web, cuando una solicitud llega a la instancia dedicada WAF, el estado de acceso cambia automáticamente a **Accesible**.

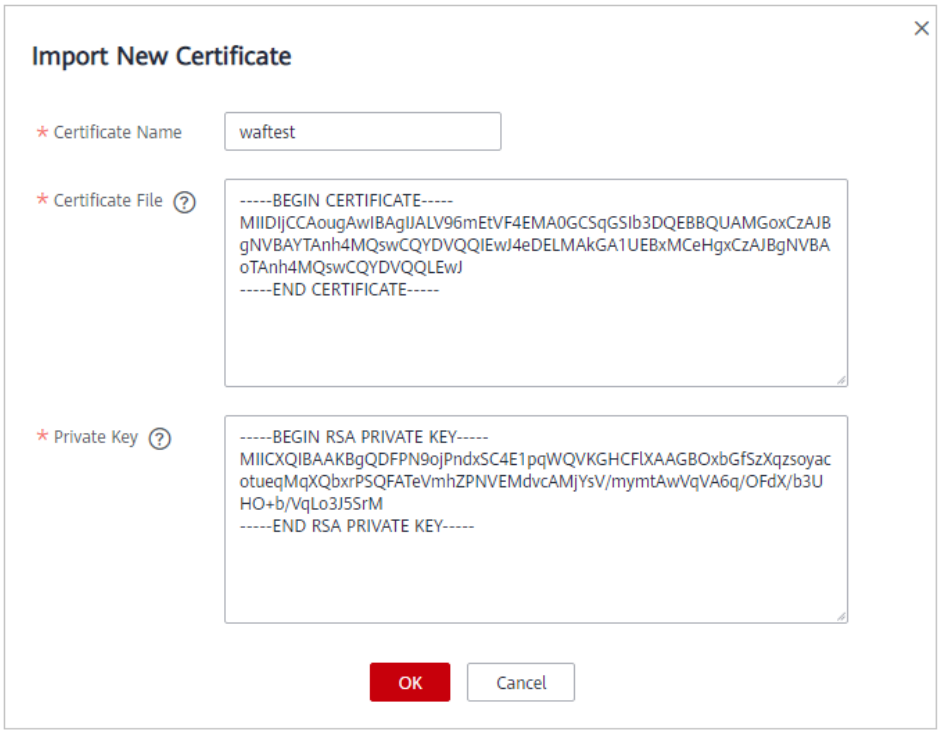
Importación de un nuevo certificado

Si establece **Client Protocol** en **HTTPS**, se requiere un certificado SSL. Puede realizar los siguientes pasos para importar un nuevo certificado.

1. Haga clic en **Import New Certificate**. En el cuadro de diálogo que aparece, escriba un nombre de certificado y copie el archivo de certificado y la clave privada en los cuadros de texto correspondiente.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-35 Importar certificado nuevo



NOTA

WAF encripta y guarda la clave privada para mantenerla segura.

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 3-10** antes de cargarlo.

Tabla 3-10 Comandos de conversión de certificados

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

 Copyright © Huawei Technologies Co., Ltd.

Formato	Método de conversión
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.

2. Haga clic en **OK**.

3.3.3 Paso 2: Configurar un balanceador de carga

Para garantizar la fiabilidad de su instancia WAF dedicada, después de agregarle un sitio web, use Huawei Cloud Elastic Load Balance (ELB) para configurar un balanceador de carga y una comprobación de estado para la instancia WAF dedicada.

AVISO

Huawei Cloud ELB se factura por el tráfico. Para obtener más información, consulte **Detalles de precios ELB**.

Prerrequisitos

- Ha agregado un sitio web a una instancia de WAF dedicada.
- Usted ha comprado un balanceador de carga. Para obtener más información sobre los balanceadores de carga, consulte **Diferencias entre los balanceadores de carga compartidos y dedicados**.
- Los puertos relacionados se han habilitado en el grupo de seguridad al que pertenece la instancia WAF dedicada.

  Puede configurar su grupo de seguridad de la siguiente manera:

  – Reglas de entrada

    Agregue una regla de entrada para permitir que el tráfico de red entrante pase a través de un puerto específico según sus requisitos de servicio. Por ejemplo, si desea permitir el acceso desde el puerto 80, puede agregar una regla que permita **TCP** y el puerto **80**.

  – Reglas de salida

    Todo el tráfico de red saliente está permitido de forma predeterminada.

  Para obtener más información, consulte **Adición de una regla de grupo de seguridad**.

Copyright © Huawei Technologies Co., Ltd.

Restricciones

El puerto de escucha de la instancia WAF dedicada debe ser el mismo que el configurado en **Paso 1: Agregar un sitio web a WAF (modo dedicado)**.

Procedimiento

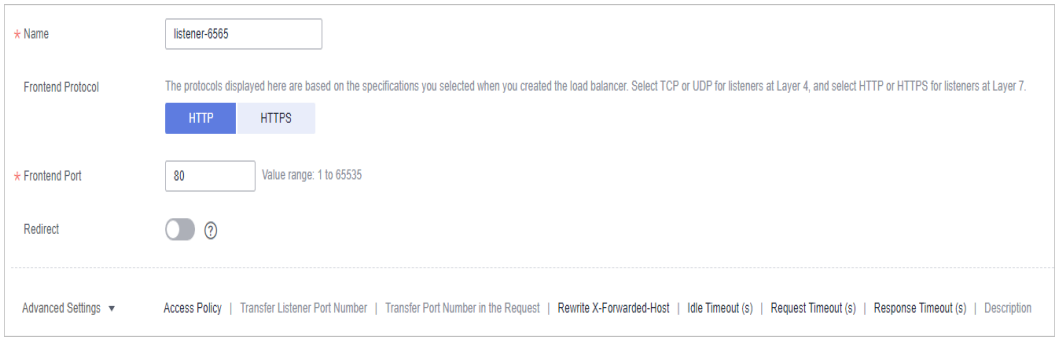
Paso 1 **Inicie sesión en la consola de gestión**.

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 el nombre del balanceador de carga en la columna **Name** para ir a la página **Basic Information**.

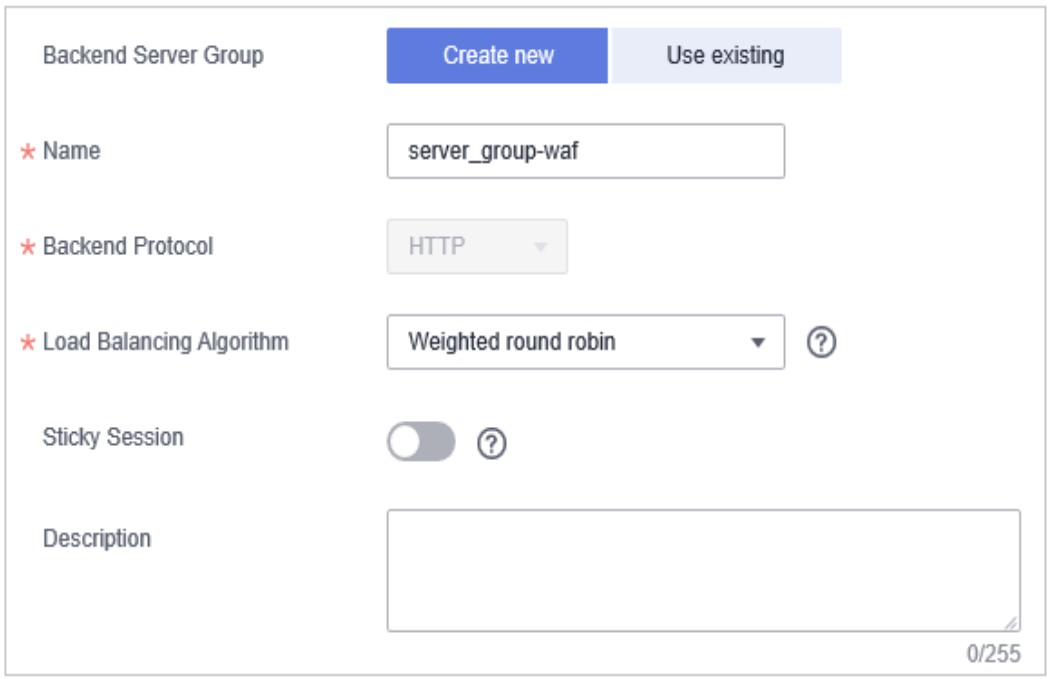
Paso 4 Haga clic en la pestaña **Listeners**, haga clic en **Add Listener** y configure la información del listener. **Figura 3-36** muestra un ejemplo.

Figura 3-36 Configuración de un listener



Paso 5 Haga clic en **Next: Configure Request Routing Policy**. **Figura 3-37** muestra un ejemplo.

Figura 3-37 Configuración de un grupo de servidores backend



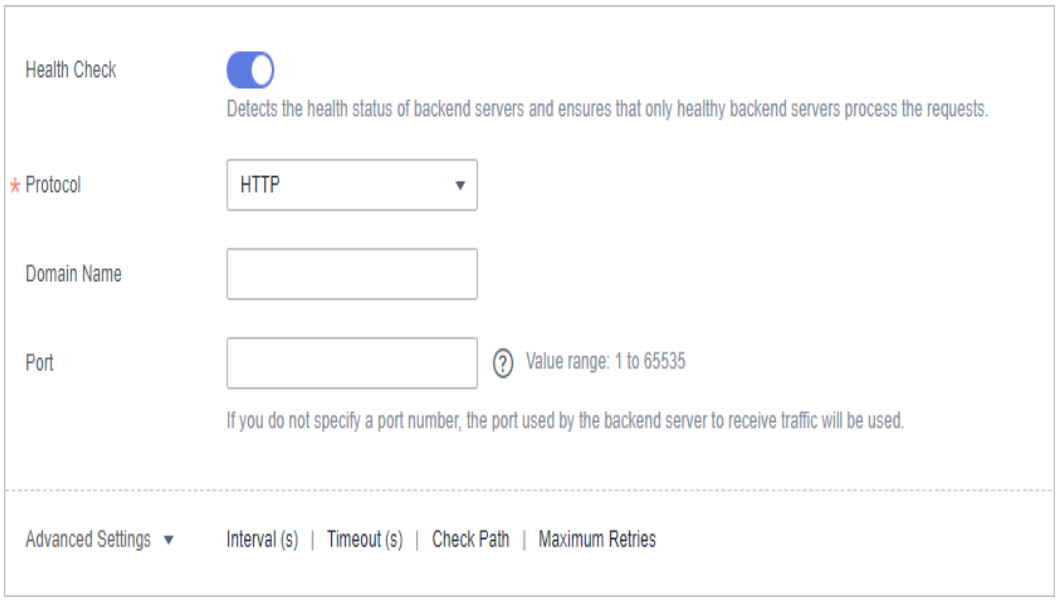
 Copyright © Huawei Technologies Co., Ltd.

AVISO

- Si selecciona **Weighted round robin** para **Load Balancing Algorithm**, desactive **Sticky Session**. Si habilita **Sticky Session**, las mismas solicitudes se reenviarán a la misma instancia WAF dedicada. Si esta instancia se vuelve defectuosa, se producirá un error cuando las solicitudes lleguen a ella la próxima vez.
- Para obtener más información sobre las directivas de distribución de tráfico ELB, consulte **Algoritmos de equilibrio de carga**.

Paso 6 Haga clic en **Next: Add Backend Server** y configure una comprobación de estado.

Figura 3-38 Configuración de control de buen funcionamiento



AVISO

- Establezca el **Port** en el puerto del sitio web configurado en **Paso 1: Agregar un sitio web a WAF (modo dedicado)**, que es el puerto de servicio escuchado por la instancia WAF.
- Para obtener más información acerca de cómo configurar la comprobación de estado, consulte **Configuración de una comprabación de estado**.

Paso 7 Haga clic en **Next: Confirm**.

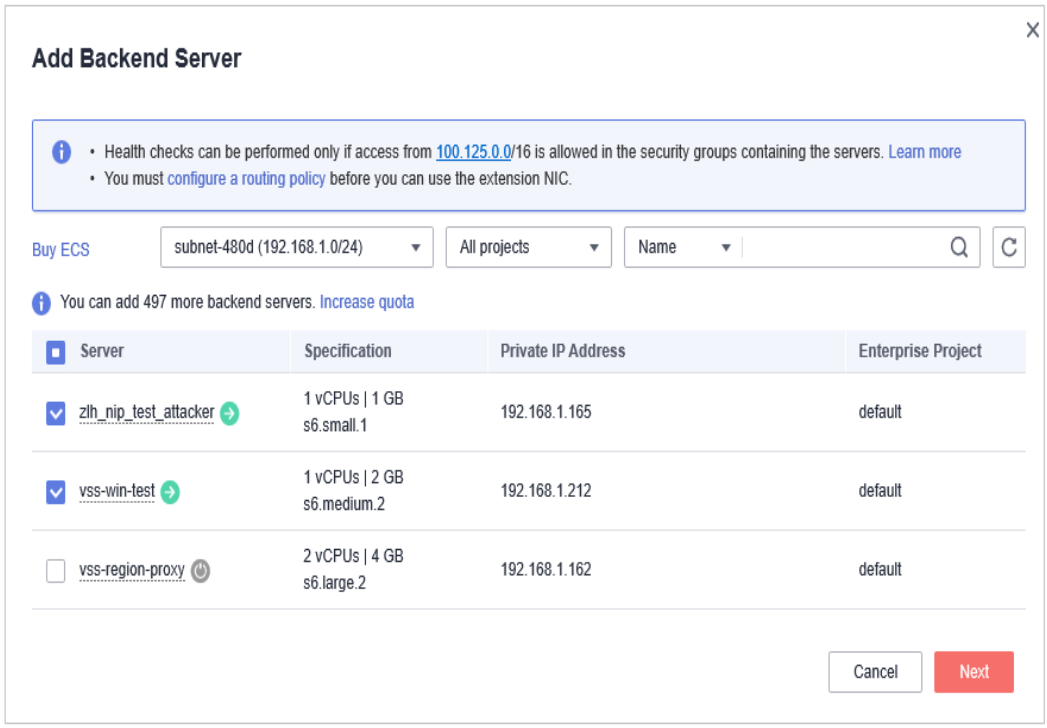
Paso 8 Haga clic en **Submit**.

Paso 9 Vaya a la página del agente de escucha agregado, seleccione la pestaña **Backend Server Groups** y haga clic en **Add**.

Paso 10 En el cuadro de diálogo **Add Backend Server** que se muestra, seleccione la instancia WAF dedicada creada en **Compra de una instancia WAF dedicada**. **Figura 3-39** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-39 Selección de la instancia WAF dedicada creada

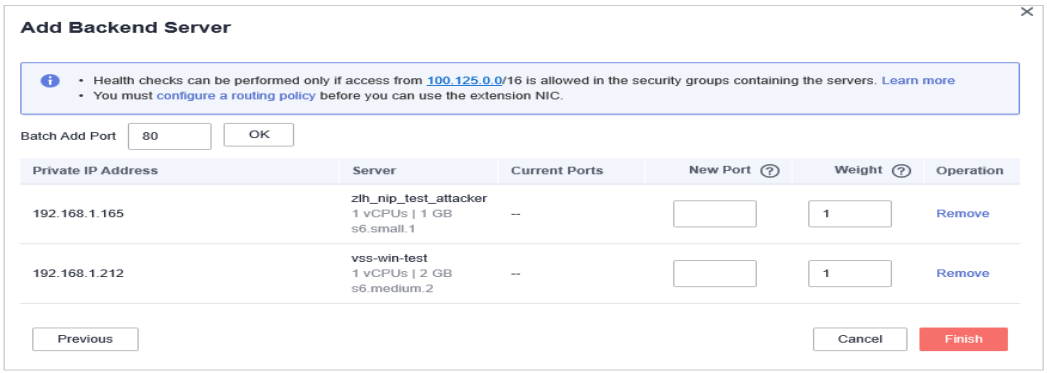


Paso 11 Haga clic en **Next** y configure un puerto para el motor dedicado. **Figura 3-40** muestra un ejemplo.

AVISO

El puerto de escucha de la instancia WAF dedicada debe ser el mismo que el configurado en **Paso 1: Agregar un sitio web a WAF (modo dedicado)**. Si configura un puerto estándar para el sitio web, establezca el puerto de escucha HTTP en **80** y el puerto de escucha HTTPS en **443**.

Figura 3-40 Configuración de un puerto para la instancia WAF dedicada



Paso 12 Haga clic en **Finish**.

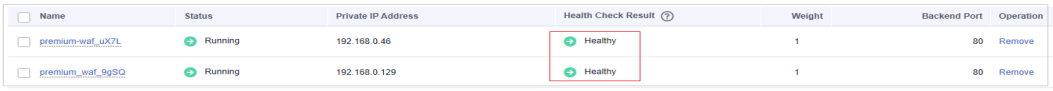
----Fin

 Copyright © Huawei Technologies Co., Ltd.

Verificación

Si **Health Check Result** es **Healthy**, se configura el balanceador de carga.

Figura 3-41 Blanaceador de carga ELB configurado



3.3.4 Paso 3: Enlazar un EIP a un balanceador de carga

Después de configurar un balanceador de carga para su instancia de WAF dedicada, debe desvincular el EIP del servidor de origen y luego vincular este EIP al balanceador de carga que configuró. Para obtener más información, consulte **Configuración de un balanceador de carga**. El tráfico de solicitud luego va a la instancia WAF dedicada para la detección de ataques primero y luego va al servidor de origen, asegurando la seguridad, estabilidad y disponibilidad del servidor de origen.

Prerrequisitos

Ha configurado un balanceador de carga para una instancia WAF dedicada.

Procedimiento

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 En la página **Elastic Load Balancers**, busque la fila que contiene el balanceador de carga configurado para el servidor de origen, haga clic en **More** en la columna **Operation** y seleccione **Unbind IPv4 EIP**. **Figura 3-42** muestra un ejemplo.

Figura 3-42 Desvincular una EIP

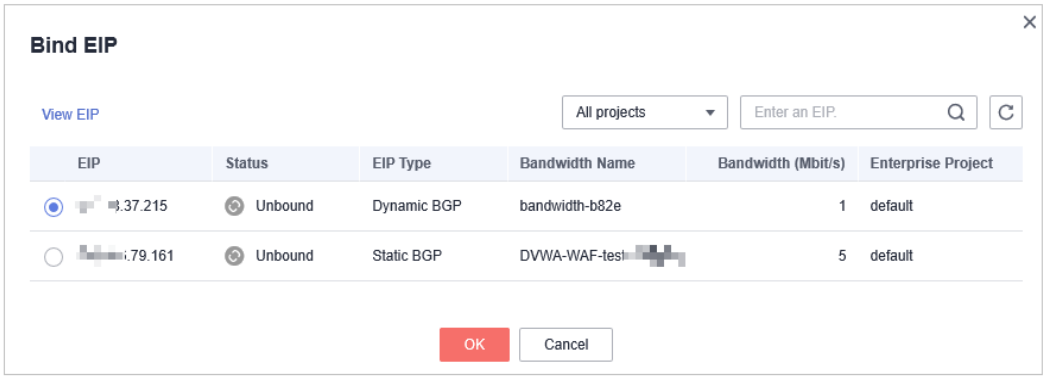
Paso 4 En la cuadro de diálogo que se muestra, haga clic en **Yes**.

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

Paso 6 En el cuadro de diálogo **Bind EIP**, seleccione EIP independiente en **Paso 3** y haga clic en **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-43 Vinculación de una EIP



----Fin

3.3.5 Paso 4: Lista blanca de las direcciones IP de origen de sus instancias de WAF dedicadas

Para que sus instancias de WAF dedicadas surtan efecto, configure las reglas de ACL en el servidor de origen para que confíen solo en las direcciones IP de origen de todas sus instancias de WAF dedicadas. 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 después de que su sitio web esté conectado a WAF.

¿Por qué necesito incluir en la lista blanca las direcciones IP de WAF back-to-source?

En modo dedicado, el tráfico del sitio web se dirige al equilibrador de carga configurado para sus instancias WAF dedicadas y luego a las instancias WAF dedicadas. Este último filtrará el tráfico malicioso y dirigirá solo el tráfico normal al servidor de origen. De esta manera, el servidor de origen solo se comunica con direcciones IP de WAF back-to-source. Al hacerlo, WAF protege el servidor de origen de ser atacado incluso si la dirección IP del servidor está expuesta a hackers informáticos accidentalmente. En el modo dedicado, las direcciones IP de origen WAF son las direcciones IP de subred de las instancias WAF dedicadas.

Lo más probable es que el software de seguridad en el servidor de origen considere las direcciones IP de origen WAF como maliciosas y las bloquee. Una vez que se bloquean, el servidor de origen denegará todas las solicitudes WAF. Como resultado, su sitio web puede no estar disponible o responder muy lentamente. Por lo tanto, las reglas de ACL deben configurarse en el servidor de origen para que confíen solo en las direcciones IP de subred de sus instancias WAF dedicadas.

Prerrequisitos

Su sitio web se ha conectado a sus instancias de WAF dedicadas.

 Copyright © Huawei Technologies Co., Ltd.

NOTA

Si ha habilitado proyectos empresariales, puede seleccionar su proyecto empresarial en la lista desplegable de **Enterprise Project** e incluir en la lista blanca las direcciones IP de back-to-source de sus instancias WAF dedicadas en el proyecto.

Apuntar el tráfico a un ECS de Alojamiento de su sitio web

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 la dirección IP de back-to-source de la instancia dedicada acceda al servidor de origen.

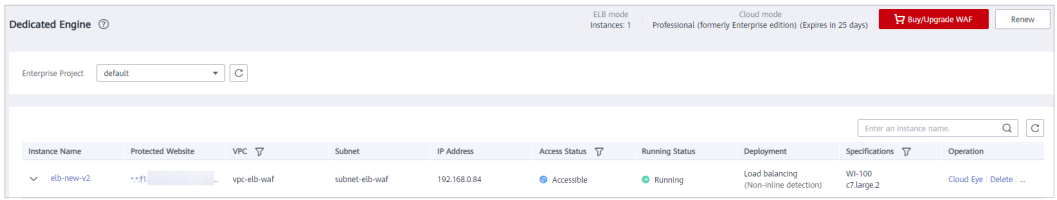
Paso 1 **Inicie sesión en la consola de gestión**

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, seleccione una región y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

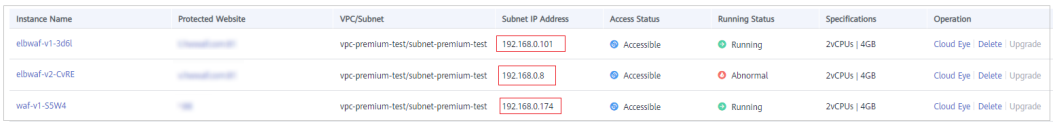
Paso 4 En el panel de navegación de la izquierda, seleccione **Instance Management** > **Dedicated Engine** para ir a la página de instancia de WAF dedicada.

Figura 3-44 Lista de motores dedicados



Paso 5 En la columna **Subnet IP Address**, obtenga la dirección IP de cada instancia WAF dedicada en su cuenta. **Figura 3-45** muestra un ejemplo.

Figura 3-45 Dirección IP de subred de una instancia WAF dedicada



Paso 6 Haga clic en la esquina superior izquierda de la página y elija **Compute** > **Elastic Cloud Server**.

Paso 7 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 8 Haga clic en la pestaña **Security Groups**. A continuación, haga clic en **Change Security Group**.

Paso 9 En el cuadro de diálogo **Change Security Group** que se muestra, seleccione un grupo de seguridad o cree un grupo de seguridad.

Paso 10 Haga clic en el nombre del grupo de seguridad para ver los detalles.

 Copyright © Huawei Technologies Co., Ltd.

Paso 11 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 3-11**. **Figura 3-46** muestra un ejemplo.

Figura 3-46 Agregar regla de entrada

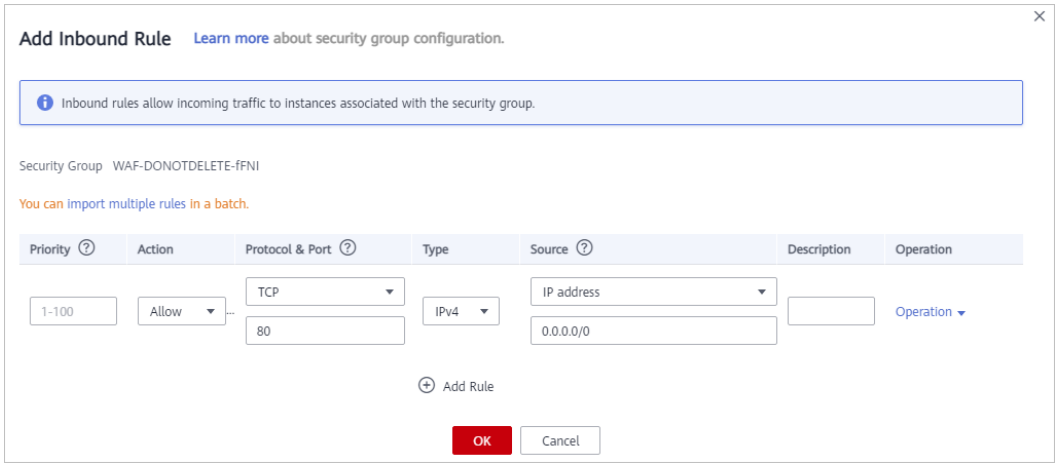


Tabla 3-11 Parámetros de regla de entrada

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	Dirección IP de subred de cada instancia de WAF dedicada que obtiene en **Paso 5**. Configure una regla de entrada para cada dirección IP. **NOTA** Una regla entrante 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 12 Haga clic en **OK**.

Ahora, el grupo de seguridad permite todo el tráfico entrante desde las direcciones IP de origen de todas sus instancias WAF dedicadas.

Para comprobar si la configuración tiene efecto, utilice la herramienta Telnet para comprobar si se establece una conexión al puerto de servicio del servidor de origen enlazado a la dirección IP protegida por WAF.

Por ejemplo, ejecute el siguiente comando para comprobar si se ha establecido la conexión al puerto de servicio del servidor de origen 443 enlazado a la dirección IP protegida por WAF. Si la conexión no se puede establecer a través del puerto de servicio pero el sitio web sigue siendo accesible, las reglas entrantes del grupo de seguridad entran en vigor.

Telnet *Origin server IP address***443**

----Fin

 Copyright © Huawei Technologies Co., Ltd.

Apuntar tráfico a un balanceador de carga

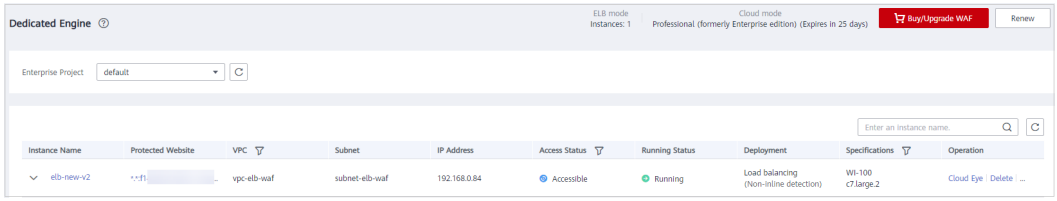
Si su servidor de origen utiliza Huawei Cloud ELB para distribuir el tráfico, realice los siguientes pasos para configurar una política de control de acceso para permitir que solo las direcciones IP de las instancias WAF dedicadas accedan al servidor de origen:

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

Paso 2 Haga clic ☰ en la esquina superior izquierda, seleccione una región y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

Paso 3 En el panel de navegación de la izquierda, seleccione **Instance Management** > **Dedicated Engine** para ir a la página de instancia de WAF dedicada.

Figura 3-47 Lista de motores dedicados



Paso 4 En la columna **Subnet IP Address**, obtenga la dirección IP de cada instancia WAF dedicada en su cuenta. **Figura 3-48** muestra un ejemplo.

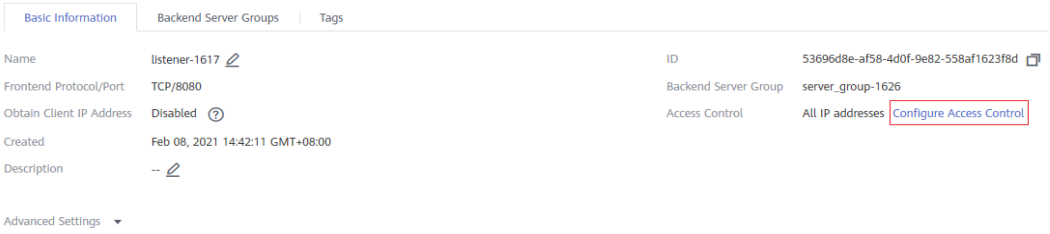
Figura 3-48 Dirección IP de subred de una instancia WAF dedicada

Paso 5 Haga clic ☰ en la esquina superior izquierda de la página y elija **Networking** > **Elastic Load Balance**.

Paso 6 Busque la fila que contiene el balanceador de carga configurado para su instancia de WAF dedicada y haga clic en el nombre del balanceador de carga en la columna **Name**.

Paso 7 En la página de detalles mostrada, haga clic en la pestaña **Listeners** y, a continuación, haga clic en **Configure Access Control**. **Figura 3-49** muestra un ejemplo.

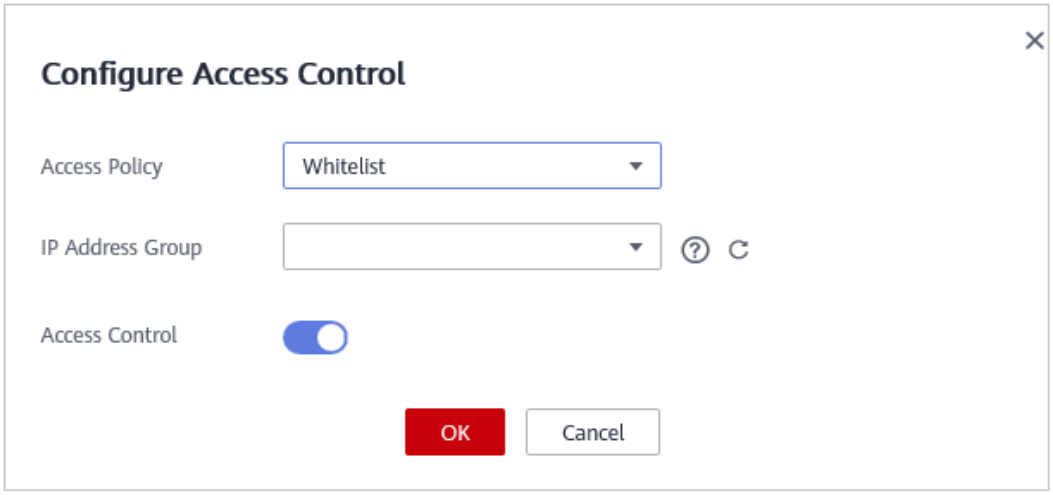
Figura 3-49 Configuración del control de acceso



Paso 8 En el cuadro de diálogo que se muestra, seleccione **Whitelist** para **Access Policy**. Haga clic en **Create IP Address Group** y agregue las direcciones IP de instancia WAF dedicadas obtenidas en **Paso 4** en él. A continuación, seleccione el grupo de direcciones IP creado para **IP Address Group**. **Figura 3-50** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 3-50 Configuración del control de acceso de lista blanca



NOTA

Haga clic en **Create IP Address Group** y agregue las direcciones IP de instancia WAF dedicadas al grupo que se está creando.

Paso 9 Haga clic en **OK**.

Ahora, la política de control de acceso permite todo el tráfico entrante desde las direcciones IP de origen de sus instancias WAF dedicadas.

Para comprobar si la configuración tiene efecto, utilice la herramienta Telnet para comprobar si se establece una conexión al puerto de servicio del servidor de origen enlazado a la dirección IP protegida por WAF.

Por ejemplo, ejecute el siguiente comando para comprobar si se ha establecido la conexión al puerto de servicio del servidor de origen 443 enlazado a la dirección IP protegida por WAF. Si la conexión no se puede establecer a través del puerto de servicio pero el sitio web sigue siendo accesible, las reglas entrantes del grupo de seguridad entran en vigor.

Telnet *Origin server IP address***443**

----Fin

 Copyright © Huawei Technologies Co., Ltd.

4 Gestión de nombres de dominio de sitios web

4.1 Consulta de información básica

En este tema se describe cómo ver el protocolo de cliente, el nombre de política, la página de alarma, el registro CNAME y la dirección IP CNAME configuradas para un nombre de dominio protegido.

NOTA

Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable de **Enterprise Project** y ver los nombres de dominio del proyecto.

Prerrequisitos

Un sitio web se ha conectado a WAF.

Procedimiento

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 In the navigation pane, choose **Website Settings**.

Paso 5 Ver la lista de sitios web protegidos. Para obtener más información sobre los parámetros, consulte **Tabla 4-1**.

 Copyright © Huawei Technologies Co., Ltd.

NOTA

- Para cambiar el modo de trabajo WAF, en la columna **Mode**, haga clic en **Switch Mode** y seleccione el modo de trabajo que desee.
- Para comprobar el estado de conexión de un sitio Web, en la columna **Access Status**, haga clic en para actualizar el estado.
- Para ver los registros de protección de los últimos tres días, en la columna **Protection Status over Past 3 Days**, haga clic en **View**.
- Para dejar de proteger un sitio Web, en la columna **Operation**, haga clic en **Delete**.

Tabla 4-1 Descripción del parámetro

Parámetro	Descripción
Protected Website	El nombre de dominio de un sitio web a proteger.
Deployment Mode	Modo de implementación de la instancia WAF configurada para su sitio web. Las opciones son **Cloud mode** y **Dedicated mode**.
Mode	Modo WAF del nombre de dominio protegido. Haga clic en **Switch** y seleccione uno de los siguientes modos de trabajo: ● **Enabled**: WAF está activado. ● **Suspended**: WAF está deshabilitado. Si se bloquea un gran número de solicitudes normales, por ejemplo, se devuelve con frecuencia el código de estado 418, entonces puede cambiar el modo a **Suspended**. En este modo, su sitio web no está protegido porque WAF solo reenvía solicitudes. No busca ataques. Para evitar que se bloqueen las solicitudes normales, en lugar de cambiar a **Suspended**, configure las reglas de enmascaramiento de falsas alarmas. ● **Bypassed**: En este modo, las solicitudes se envían directamente a los servidores backend sin pasar por WAF. **NOTA** El modo de trabajo se puede cambiar a **Bypassed** solo si el sitio web protegido se implementa en **Cloud mode** y se cumplen las siguientes condiciones: – Los servicios del sitio web deben restaurarse al estado cuando el dominio 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. Para más detalles, consulte **Cambio de modo de trabajo WAF**.

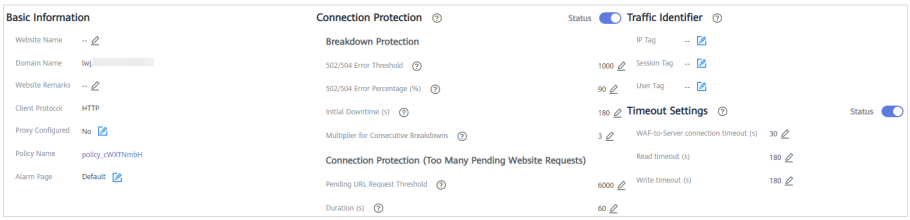
 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción
Access Status	● **Inaccessible**: El sitio web no está conectado a WAF o no puede conectarse a WAF. ● **Accessible**: El sitio web está conectado a WAF. **AVISO** El estado de **Access Status** de un sitio web implementado en **Dedicated Mode** es **Inaccessible**. Cuando una solicitud llega a su instancia de WAF para el sitio web, el estado de acceso cambia automáticamente a **Accessible**.
Protection Status over Past 3 Days	Estado de protección del nombre de dominio en los últimos 3 días. Haga clic en **View** para ver los registros de protección específicos.
Policy	Configuración de la política del nombre de dominio. Haga clic en **Configure Policy** para configurar reglas. Para más detalles, consulte **Configuración de regla**.
Operation	Para eliminar un sitio web protegido de WAF, haga clic en **Delete**. **NOTA** ● Si desea eliminar un sitio web protegido en **Cloud mode** de la instancia WAF, vaya a la plataforma DNS y traduzca el nombre de dominio a la dirección IP del servidor de origen antes de eliminarlo. De lo contrario, el tráfico destinado al nombre de dominio no se dirigirá al servidor de origen. ● Se tarda aproximadamente un minuto para eliminar un sitio web de WAF. Tenga en cuenta que la acción de eliminación no se puede cancelar.

Paso 6 En la columna **Protected Website**, haga clic en el nombre de dominio del sitio web para ir a la página de información básica.

Paso 7 Vea la información básica sobre el nombre de dominio del sitio web protegido. **Figura 4-1** muestra un ejemplo.

Figura 4-1 Información básica



- Obtener información sobre la instancia WAF: Haga clic en junto a campos de **CNAME** y **WAF IP Address Segment**.
- Obtener **Subdomain Name** y **TXT Record**: En la fila de **Access Status**, haga clic en **How to Access**. En el cuadro de diálogo **Access Guide**, copie **Subdomain Name** y **TXT Record**.

 Copyright © Huawei Technologies Co., Ltd.

- Actualizar el certificado: Si selecciona **HTTPS** para **Client Protocol**, se requiere un certificado SSL. Para actualizar el certificado, haga clic en junto al nombre del certificado en la fila **Certificate NameInternational Certificate** or **Chinese Certificate**. A continuación, en el cuadro de diálogo mostrado, cargue un nuevo certificado o seleccione un certificado existente. Para más detalles, consulte **Actualización de un certificado**.
- Actualice la versión TLS y el conjunto de cifrado TLS para acceder al servidor de origen: Si selecciona **HTTPS** para **Client Protocol**, puede cambiar la versión TLS a una más segura. Para ello, haga clic en junto al campo Configuración de TLS. A continuación, en el cuadro de diálogo que se muestra, seleccione la versión de TLS y el conjunto de cifrado TLS deseados. Para más detalles, consulte **Configuración de la comprobación de certificación PCI DSS/3DS y versión TLS**.
- Modificar el campo de **Proxy Configured**: Haga clic . En el cuadro de diálogo que se muestra, seleccione **Yes** si el servidor web utiliza un proxy.
- Personalizar la página de alarma: Haga clic en . En el cuadro de diálogo que se muestra, seleccione **Custom** o **Redirection** y complete las configuraciones requeridas. De forma predeterminada, **Alarm Page** es **Default**.
- Si su sitio web requiere protección IPv6, haga clic en . En el cuadro de diálogo que aparece, seleccione **Enable**. A continuación, WAF asigna una dirección IPv6 al nombre de dominio. Para más detalles, consulte **Habilitación de la protección IPv6 WAF**.
- Si su sitio web es accesible a través de HTTP/2, haga clic en en la fila **HTTP/2 Used** y seleccione **Yes**. Este parámetro sólo es válido cuando se selecciona **HTTPS** para **Client Protocol** para al menos un servidor de origen. Para más detalles, consulte **Habilitación del protocolo HTTP/2**.
- Si desea establecer una duración de tiempo de espera para cada solicitud, habilite **Timeout Settings** y haga clic en para especificar **WAF-to-Server Connection Timeout (s)**, **Read Timeout (s)**, and **Write Timeout (s)**. Esta función no se puede deshabilitar después de estar habilitada. Para más detalles, consulte **Configuración del tiempo de espera de conexión**.
- Para cambiar el algoritmo de equilibrio de carga del sitio web, haga clic . En el cuadro de diálogo que se muestra, seleccione un algoritmo de equilibrio de carga y haga clic en **OK**. Para más detalles, consulte **Cambio del algoritmo de equilibrio de carga**.

----Fin

4.2 Cambio de modo de trabajo WAF

Puede cambiar el modo de trabajo de WAF. WAF puede funcionar en modo **Enabled**, **Suspended**, or **Bypassed**.

NOTA

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 empresarial de la lista desplegable **Enterprise Project** y cambiar el modo de trabajo WAF por un nombre de dominio específico.

 Copyright © Huawei Technologies Co., Ltd.

Prerrequisitos

El nombre de dominio del sitio web a proteger ha sido vinculado a WAF.

Escenarios de aplicación

- **Enabled**: En este modo, WAF defiende su sitio web contra ataques basados en políticas configuradas.
- **Suspended**: si un gran número de solicitudes normales están bloqueadas, por ejemplo, el código de estado 418 se devuelve con frecuencia, entonces puede cambiar el modo a **Suspended**. En este modo, su sitio web no está protegido porque WAF solo reenvía solicitudes. No analiza ni registra ataques. Su sitio web no está protegido. Para evitar que se bloqueen las solicitudes normales, en lugar de cambiar a **Suspended**, configure las reglas de enmascaramiento de falsas alarmas.
- **Bypassed**: Las solicitudes se envían directamente a los servidores de origen backend sin pasar por WAF. Antes de habilitar este modo, habilite el puerto de servicio de los servidores de origen para permitir que las solicitudes vayan a los servidores de origen. Cambie el modo 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.

Impacto en el sistema

En el modo **Suspended**, su sitio web no está protegido porque WAF solo reenvía solicitudes. No analiza en busca de ataques. Para evitar que se bloqueen las solicitudes normales, configure las reglas de enmascaramiento de falsas alarmas en lugar de utilizar el modo **Suspended**.

Procedimiento

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**.

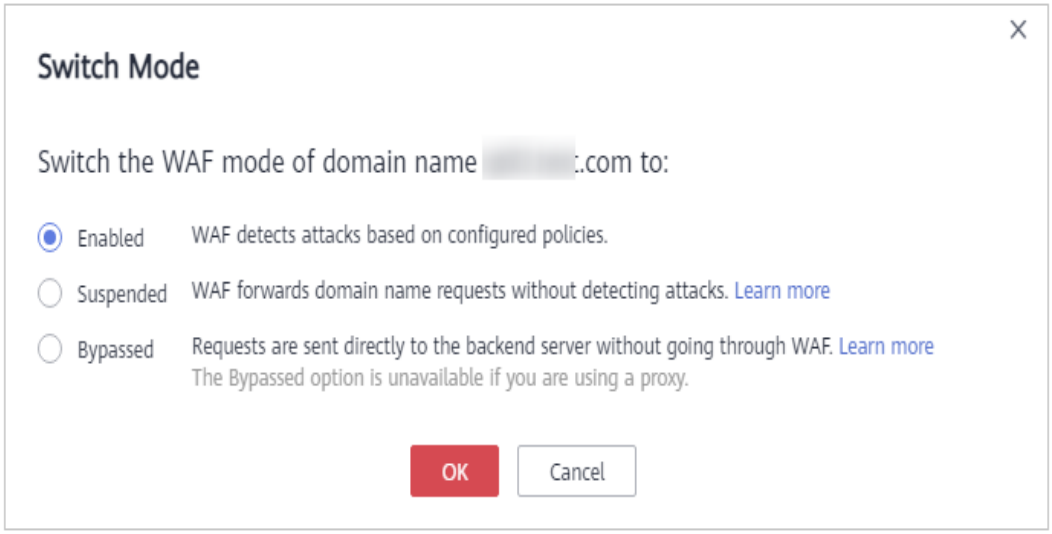
Paso 4 In the navigation pane, choose **Website Settings**.

Paso 5 En la columna **Mode** del sitio web de destino, haga clic en **Switch**.

Paso 6 En el cuadro de diálogo **Switch Mode**, seleccione un modo de trabajo y, a continuación, haga clic en **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 4-2 Cambio de modo de trabajo WAF



----Fin

Otras operaciones

- **Manejo de falsas alarmas**
- **¿Cómo soluciono los errores 404/502/504?**

4.3 Configuración de la comprobación de certificación PCI DSS/3DS y versión TLS

Transport Layer Security (TLS) proporciona confidencialidad y garantiza la integridad de los datos para los datos enviados entre aplicaciones a través de Internet. HTTPS es un protocolo de red construido basado en TLS y HTTP y se puede utilizar para la transmisión cifrada y la autenticación de identidad. Si selecciona **Cloud mode** o **Dedicated mode** para la implementación y establece **Client Protocol** en **HTTPS**, establecer la versión mínima de TLS y el conjunto de cifrado (un conjunto de múltiples algoritmos criptográficos) para su nombre de dominio para bloquear las solicitudes que utilizan una versión de TLS anterior a la configurada.

TLS v1.0 y el conjunto de cifrado 1 están configurados por defecto en WAF para la seguridad general. Para proteger mejor sus sitios web, establezca la versión mínima de TLS en una versión posterior y seleccione un conjunto de cifrado más segura.

WAF le permite habilitar las comprobaciones de certificación PCI DSS y PCI 3DS. Después de activar la comprobación de la certificación PCI DSS o PCI 3DS, la versión mínima de TLS se establece automáticamente en TLS v1.2 para cumplir con los requisitos de certificación PCI DSS y PCI 3DS. El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) es un estándar de seguridad de la información para organizaciones que manejan tarjetas de crédito de marca de los principales esquemas de tarjetas. PCI 3-Domain Secure (PCI 3DS) es un estándar de seguridad PCI Core.

 Copyright © Huawei Technologies Co., Ltd.

NOTA

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 empresarial en la lista desplegable de **Enterprise Project** y configurar PCI DSS o PCI 3DS y TLS para los nombres de dominio.

Prerrequisitos

- El modo de implementación de la instancia WAF configurada para su sitio web es **Cloud mode** o **Dedicated mode**.
- Su sitio web utiliza HTTPS como protocolo de cliente.

Restricciones

- Si **Client Protocol** para el sitio web que desea proteger está establecido en **HTTP**, TLS no es necesario y puede omitir este tema.
- Actualmente, esta función no está disponible en CN Norte-Ulanqab1.

Escenarios de aplicación

De forma predeterminada, la versión mínima de TLS configurada para WAF es **TLS v1.0**. Para garantizar la seguridad del sitio web, configure la versión TLS adecuada para sus requisitos de servicio. **Tabla 4-2** enumera las versiones mínimas recomendadas de TLS para diferentes escenarios.

Tabla 4-2 Versiones mínimas recomendadas de TLS

Escenario	Versión mínima de TLS (recomendada)	Efecto de protección
Sitios web que manejan datos empresariales críticos, como sitios utilizados en banca, finanzas, valores y comercio electrónico.	TLS v1.2	WAF bloquea automáticamente las solicitudes de acceso a sitios web que utilizan TLS v1.0 o TLS v1.1.
Sitios web con requisitos básicos de seguridad, por ejemplo, sitios web para pequeñas y medianas empresas.	TLS v1.1	WAF bloquea automáticamente las solicitudes de acceso a sitios web que utilizan TLS v1.0.
Aplicaciones de cliente sin requisitos de seguridad especiales	TLS v1.0	Las solicitudes que utilicen cualquier protocolo TLS pueden acceder al sitio web.

El conjunto de cifrado recomendada en WAF es **Cipher suite 1**. Cipher suite 1 ofrece una buena combinación de compatibilidad con navegador y seguridad. Para obtener más información sobre cada conjunto de cifrado, consulte **Tabla 4-3**.

 Copyright © Huawei Technologies Co., Ltd.

Tabla 4-3 Descripción del conjunto de cifrado

Nombre del conjunto de cifrado	Algoritmos criptográficos compatibles	Descripción
Conjunto de cifrado por defecto	● ECDHE-RSA-AES256-SHA384 ● AES256-SHA256 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !DH ● !EDH ● !AESGCM	● Compatibilidad: Bueno. Una amplia gama de navegadores son compatibles. ● Seguridad: Promedio
Conjunto de cifrado 1	● ECDHE-ECDSA-AES256-GCM-SHA384 ● HIGH ● !MEDIUM ● !LOW ● !aNULL ● !eNULL ● !DES ● !MD5 ● !PSK ● !kRSA ● !SRP ● !3DES ● !DSS ● !EXP ● !CAMELLIA ● @STRENGTH	Configuración recomendada. ● Compatibilidad: Bueno. Una amplia gama de navegadores son compatibles. ● Seguridad: Buena
Conjunto de cifrado 2	● EECDH+AESGCM ● EDH+AESGCM	● Compatibilidad: Promedio. Cumplimiento estricto de los requisitos de confidencialidad de PCI DSS y excelente protección, pero los navegadores de versiones anteriores pueden no ser capaces de acceder al sitio web. ● Seguridad: Excelente

 Copyright © Huawei Technologies Co., Ltd.

Nombre del conjunto de cifrado	Algoritmos criptográficos compatibles	Descripción
Conjunto de cifrado 3	● ECDHE-RSA-AES128-GCM-SHA256 ● ECDHE-RSA-AES256-GCM-SHA384 ● ECDHE-RSA-AES256-SHA384 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !DH ● !EDH	● Compatibilidad: Promedio. Es posible que las versiones anteriores de los navegadores no puedan acceder al sitio web. ● Seguridad: Excelente. Se admiten múltiples algoritmos, como ECDHE, DHE-GCM y RSA-AES-GCM.
Conjunto de cifrado 4	● ECDHE-RSA-AES256-GCM-SHA384 ● ECDHE-RSA-AES128-GCM-SHA256 ● ECDHE-RSA-AES256-SHA384 ● AES256-SHA256 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !EDH	● Compatibilidad: Bueno. Una amplia gama de navegadores son compatibles. ● Seguridad: Promedio. Se soporta el algoritmo GCM.

Las suites de cifrado TLS en WAF son compatibles con todos los navegadores y clientes de versiones posteriores, pero son incompatibles con algunos navegadores de versiones anteriores. **Tabla 4-4** enumera los navegadores y clientes incompatibles si se utiliza el protocolo TLS v1.0.

AVISO

Se recomienda que se realicen pruebas de compatibilidad en el entorno de servicio para garantizar la estabilidad del servicio.

Copyright © Huawei Technologies Co., Ltd.

Tabla 4-4 Navegadores y clientes incompatibles para conjuntos de cifrado bajo TLS v1.0

Navegador/ Cliente	Conjunto de cifrado predeterminado	Conjunto de cifrado 1	Conjunto de cifrado 2	Conjunto de cifrado 3	Cipher Suite 4
Google Chrome 63 /macOS High Sierra 10.13.2	No compatible	Compatible	Compatible	Compatible	Not compatible
Google Chrome 49/ Windows XP SP3	No compatible	No compatible	No compatible	No compatible	Not compatible
Internet Explorer 6 /Windows XP	No compatible	No compatible	No compatible	No compatible	Not compatible
Internet Explorer 8 /Windows XP	No compatible	No compatible	No compatible	No compatible	Not compatible
Safari 6/iOS 6.0.1	Compatible	Compatible	No compatible	Compatible	Compatible
Safari 7/iOS 7.1	Compatible	Compatible	No compatible	Compatible	Compatible
Safari 7/OS X 10.9	Compatible	Compatible	No compatible	Compatible	Compatible
Safari 8/iOS 8.4	Compatible	Compatible	No compatible	Compatible	Compatible
Safari 8/OS X 10.10	Compatible	Compatible	No compatible	Compatible	Compatible
Internet Explorer 7/Windows Vista	Compatible	Compatible	No compatible	Compatible	Compatible
Internet Explorer 8, 9, or 10 /Windows 7	Compatible	Compatible	No compatible	Compatible	Compatible
Internet Explorer 10 /Windows Phone 8.0	Compatible	Compatible	No compatible	Compatible	Compatible

 Copyright © Huawei Technologies Co., Ltd.

Navegador/ Cliente	Conjunto de cifrado predeterminado	Conjunto de cifrado 1	Conjunto de cifrado 2	Conjunto de cifrado 3	Cipher Suite 4
Java 7u25	Compatible	Compatible	No compatible	Compatible	Compatible
OpenSSL 0.9.8y	No compatible	No compatible	No compatible	No compatible	Not compatible
Safari 5.1.9/OS X 10.6.8	Compatible	Compatible	No compatible	Compatible	Compatible
Safari 6.0.4/OS X 10.8.4	Compatible	Compatible	No compatible	Compatible	Compatible

Impacto en el sistema

- Si habilita la certificación PCI DSS, compruebe:
  - La versión mínima de TLS y el conjunto de cifrado se establecen automáticamente en **TLS v1.2** y **EECDH+AESGCM:EDH+AESGCM**, respectivamente, y no se pueden cambiar.
  - Para cambiar la versión mínima de TLS y el conjunto de cifrado, desactive la comprobación.
- Si habilita la certificación PCI 3DS, compruebe:
  - La versión mínima de TLS se establece automáticamente en **TLS v1.2** y no se puede cambiar.
  - La comprobación no se puede deshabilitar.

Procedimiento

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 In the navigation pane, choose **Website Settings**.

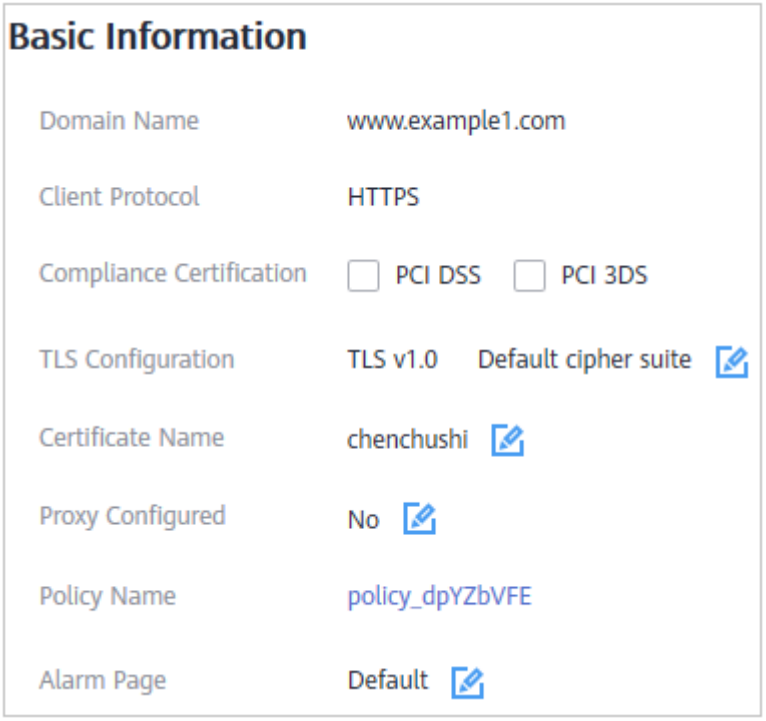
Paso 5 En la columna **Protected Website**, haga clic en el nombre de dominio del sitio web para ir a la página de información básica.

Paso 6 En la fila **Compliance Certification**, puede seleccionar **PCI DSS** y/o **PCI 3DS** para permitir que WAF revise su sitio web para el cumplimiento de la certificación PCI correspondiente. En

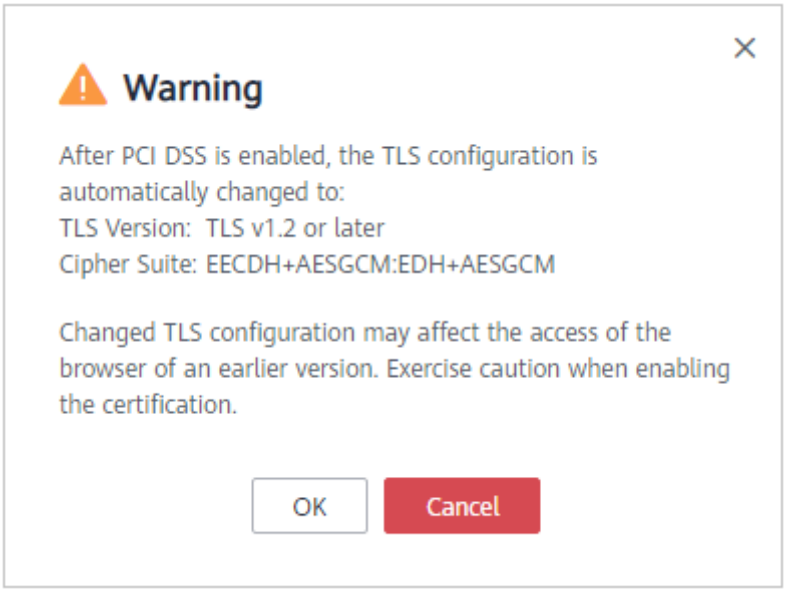
 Copyright © Huawei Technologies Co., Ltd.

la fila **TLS Configuration**, haga clic en para completar la configuración de TLS. **Figura 4-3** muestra un ejemplo.

Figura 4-3 Modificación de la configuración de TLS



- Seleccione **PCI DSS**. En el cuadro de diálogo **Warning** que se muestra, haga clic en **OK** para habilitar la comprobación de certificación PCI DSS.

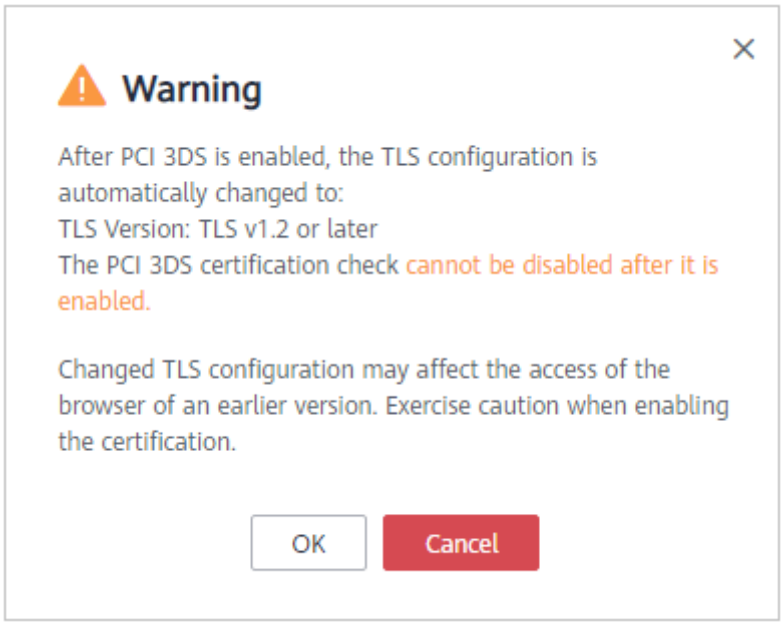


 Copyright © Huawei Technologies Co., Ltd.

AVISO

Si la comprobación de certificación PCI DSS está activada, no se puede cambiar la versión mínima de TLS y el conjunto de cifrado.

- Seleccione **PCI 3DS**. En el cuadro de diálogo **Warning** que se muestra, haga clic en **OK** para activar la comprobación de certificación PCI 3DS.



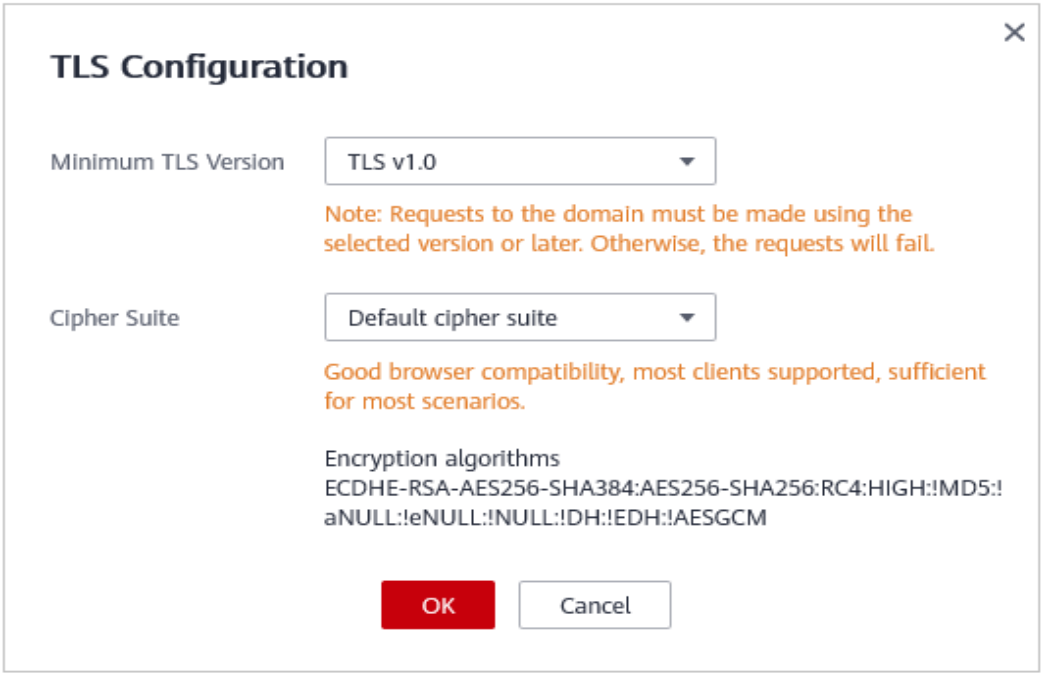
AVISO

- Si la comprobación de certificación PCI 3DS está activada, no se puede cambiar la versión mínima de TLS.
- Una vez habilitada, la comprobación de certificación PCI 3DS no se puede deshabilitar.

Paso 7 En el cuadro de diálogo de **TLS Configuration** que se muestra, seleccione la versión mínima de TLS y el conjunto de cifrado. **Figura 4-4** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 4-4 Configuración de TLS



Seleccione la versión mínima de TLS que necesita. Las opciones son las siguientes:

- **TLS v1.0**: la versión predeterminada. Las solicitudes que usan TLS v1.0 o posterior pueden acceder al nombre de dominio.
- **TLS v1.1**: Solo las solicitudes que usen TLS v1.1 o posterior pueden acceder al nombre de dominio.
- **TLS v1.2**: Solo las solicitudes que utilicen TLS v1.2 o posterior pueden acceder al nombre de dominio.

Paso 8 Click **OK**.

----Fin

Verificación

Si **Minimum TLS Version** está establecida en **TLS v1.2**, se puede acceder al sitio web a través de conexiones protegidas por TLS v1.2 o posterior, pero no se puede acceder a través de conexiones protegidas por TLS v1.1 o anterior.

4.4 Habilitación de la protección IPv6 WAF

Si su sitio web requiere protección IPv6, puede habilitar la protección IPv6. Después de habilitar la protección IPv6, WAF asigna una dirección IPv6 al nombre de dominio y utiliza la dirección IPv6 para acceder al servidor de origen. WAF agrega resolución de direcciones IPv6 en conjuntos de registros 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.

- Si la dirección del servidor de origen del sitio web protegido es una dirección IPv6, la protección IPv6 está habilitada de forma predeterminada.

 Copyright © Huawei Technologies Co., Ltd.

- Si la dirección del servidor de origen del sitio web protegido se establece en una dirección IPv4, después de habilitar manualmente la protección IPv6, WAF utiliza el mecanismo NAT64 para traducir el sitio web IPv4 en un sitio web IPv6. De esta manera, las solicitudes a la dirección IPv6 son verificadas y enrutadas por WAF al servidor de origen. NAT64 es un mecanismo de traducción de direcciones de red (NAT) que permite las comunicaciones entre servidores IPv6 e IPv4.

Prerrequisitos

El sitio web que desea proteger se ha añadido a WAF.

Restricciones

- Ha seleccionado **Cloud mode** para la implementación de su sitio web.
- Solo las ediciones profesional (anteriormente edición empresarial) y platino (anteriormente edición premium) pueden proteger los sitios web que usan direcciones IPv6.
- La pila dual IPv4/IPv6 y NAT64 solo se admiten en las regiones de China Este y China Norte.

Procedimiento

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

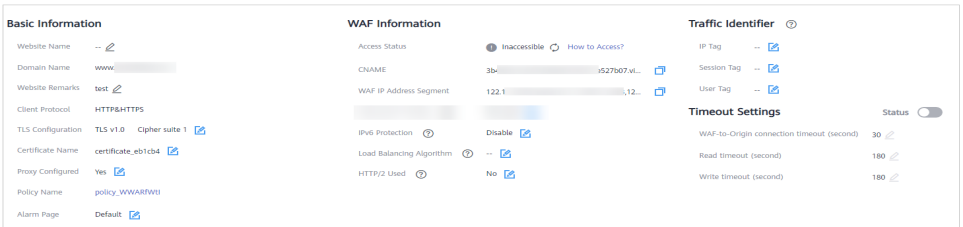
Paso 2 Haga clic en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 En el panel de navegación, 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.

Figura 4-5 Área de información básica



Paso 6 En la fila **IPv6 Protection**, haga clic en . En el cuadro de diálogo que aparece, seleccione **Enable** y haga clic en **OK**.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

4.5 Habilitación del protocolo HTTP/2

Si su sitio web es accesible a través del protocolo HTTP/2, habilite HTTP/2 en WAF. El protocolo 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**.

Prerrequisitos

- El sitio web que desea proteger se ha añadido a WAF.
- Ha seleccionado **HTTPS** para **Client Protocol** para al menos una pieza de configuración del servidor.

Restricciones

- Ha seleccionado **Dedicated mode** para la implementación de su sitio web.
- Solo las ediciones profesional (anteriormente edición empresarial) y platino (anteriormente edición premium) pueden proteger los sitios web a los que se puede acceder mediante el protocolo HTTP/2.
- Actualmente, HTTP/2 (HTTP2.0) se puede habilitar en las siguientes regiones:
  - CN-Hong Kong
  - AP-Bangkok

Procedimiento

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

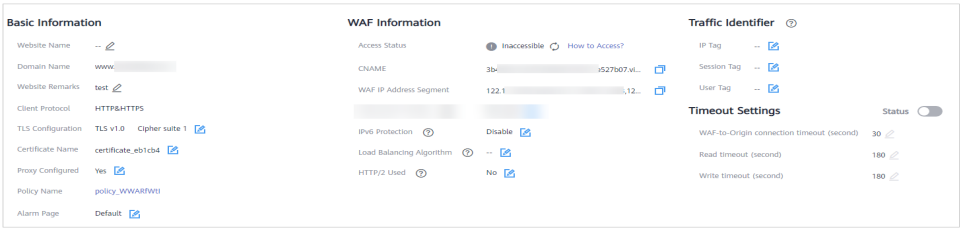
Paso 2 Haga clic en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 En el panel de navegación, 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.

Figura 4-6 Área de información básica



Paso 6 En la fila **HTTP/2 Used**, haga clic en . A continuación, seleccione **Yes** y haga clic en **OK**.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

4.6 Configuración del tiempo de espera de conexión

Si desea establecer una duración de tiempo de espera para cada solicitud entre la instancia WAF y el servidor de origen, habilite **Timeout Settings** de espera y especifique **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)**. Esta función no se puede deshabilitar una vez que está habilitada.

NOTA

- El tiempo de espera predeterminado para las conexiones entre un navegador y WAF es de 120 segundos, que no se puede ajustar manualmente.
- El tiempo de espera predeterminado para las conexiones entre WAF y el servidor de origen es de 60 segundos. Si utiliza una instancia de WAF dedicada o una instancia de WAF en la nube en la edición profesional (anteriormente Enterprise Edition) o en la edición platino (anteriormente última edición), puede personalizar la duración del tiempo de espera.
- Para más restricciones, consulte **Restricciones**.

Prerrequisitos

El sitio web que desea proteger se ha agregado a WAF.

Restricciones

- El modo de implementación de la instancia WAF configurada para su sitio web es **Cloud mode** o **Dedicated mode**.
- En **Cloud mode**, la duración del tiempo de espera de la conexión solo se puede modificar en la edición profesional (anteriormente Enterprise Edition) y en la edición platino (anteriormente Premium Edition).
- No se puede modificar el tiempo de espera de las conexiones entre un navegador y WAF. Solo se puede modificar la duración del tiempo de espera para las conexiones entre WAF y el servidor de origen.
- Esta función no se puede deshabilitar una vez que está habilitada.
- Actualmente, WAF admite **Timeout Settings** en las siguientes regiones:
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore

Procedimiento

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.

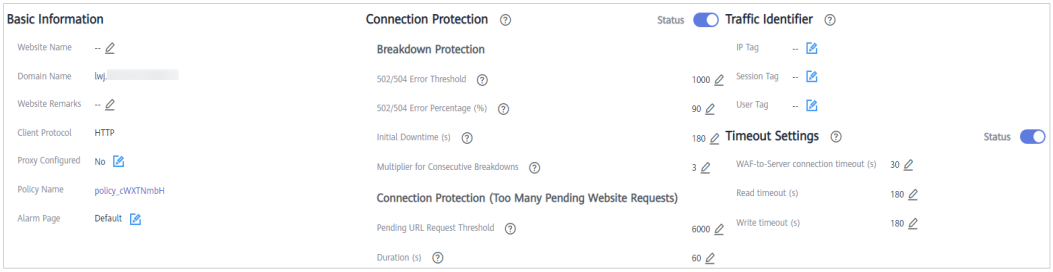
Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

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

 Copyright © Huawei Technologies Co., Ltd.

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.

Figura 4-7 Área de información básica



Paso 6 En la fila **Timeout Settings**, haga clic en la imagen **Status** si es necesario para habilitarla.

Paso 7 Haga clic en , especifique **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)**, y haga clic en para guardar la configuración.

----Fin

4.7 Configuración de la protección de la conexión

Si se detecta un gran número de errores de 502 Bad Gateway y 504 Gateway Timeout, puede activar la protección de averías WAF y la protección de conexión para permitir que WAF suspenda su sitio web y proteja sus servidores de origen de ser bloqueados. Cuando las solicitudes de error 502/504 y las solicitudes de URL pendientes alcanzan los umbrales que configura, WAF habilita la protección correspondiente para su sitio web.

Prerrequisitos

- El sitio web que desea proteger se ha agregado a WAF.
- Ha actualizado la instancia WAF dedicada a la última versión. Para más detalles, consulte **Actualización de una instancia WAF dedicada**.

Restricciones

- Ha seleccionado **Dedicated mode** para la implementación de su sitio web.
- La **instancia WAF dedicada debe actualizarse a la versión más reciente** antes de habilitar la **Connection Protection**, o es posible que se interrumpan las cargas de trabajo de su sitio web.
- Actualmente, WAF admite **Connection Protection** del sitio web en las siguientes regiones:
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore

Procedimiento

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

 Copyright © Huawei Technologies Co., Ltd.

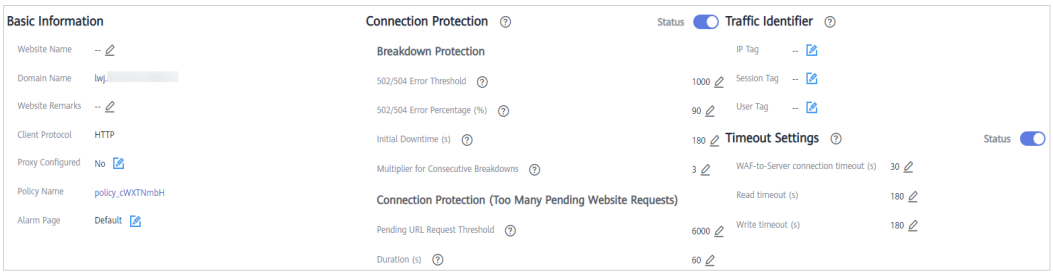
Paso 2 Haga clic en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 En el panel de navegación, 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.

Figura 4-8 Área de información básica



Paso 6 En el área **Connection Protection**, haga clic en el interruptor de estado para habilitarlo.

Paso 7 Haga clic junto a cada parámetro, edite los parámetros **Breakdown Protection** y **Connection Protection** para satisfacer sus requisitos y haga clic en para guardar la configuración. **Tabla 4-5** describe estos parámetros.

Tabla 4-5 Parámetros de protección de conexión

Parámetro		Descripción	Valor de ejemplo
Breakdown Protection	502/504 Error Threshold	30s 502/504 Umbral de error	1000
	502/504 Error Percentage (%)	Se activa una avería cuando se han alcanzado el umbral de error 502/504 y el umbral de porcentaje.	90
	Initial Downtime (s)	Periodo de protección en la primera avería. Durante este período, WAF deja de reenviar las solicitudes del cliente.	180

 Copyright © Huawei Technologies Co., Ltd.

Parámetro		Descripción	Valor de ejemplo
	Multiplier for Consecutive Breakdowns	El multiplicador máximo que puede usar para desgloses consecutivos. El número de averías se cuenta desde 0 cada vez que la duración acumulada de la protección contra averías alcanza los 3,600s. Por ejemplo, supongamos que **Initial Downtime (s)** se establece en 180s y **Multiplier for Consecutive Breakdowns** se establece en 3. ● Si la avería se activa por segunda vez, es decir, menos de 3, la duración de protección es de 360s (180s X 2). ● Si la avería se activa durante el tercer o cuarto tiempo, es decir, igual o mayor que 3, la duración de protección es de 540s (180s X 3). ● Cuando la duración del tiempo de inactividad acumulado supera 1 hora (3,600s), el número de averías se cuenta desde 0.	3
Connection Protection	Pending URL Request Threshold	La protección de conexión se activa cuando el número de solicitudes de URL de lectura alcanza el umbral que configura.	6000
	Duration (s)	Duración de la protección. Durante este período, WAF deja de reenviar las solicitudes del cliente.	60

 Copyright © Huawei Technologies Co., Ltd.

NOTA

A continuación se utiliza la configuración de **Connection Protection** en **Figura 4-8** como ejemplo para describir cómo funciona la protección.

- **Breakdown Protection**: Cuando el número de errores 502/504 devueltos por el sitio web protegido supera el 1,000 y representa el 90% o más del total de solicitudes de acceso del sitio web por primera vez, se activa la primera protección contra averías. Durante la primera protección contra averías, WAF deja de reenviar las solicitudes del cliente para 180s. (es decir, bloquea el acceso de los visitantes al sitio web durante 180 años). Si se activa una segunda protección de averías consecutiva, WAF detiene el reenvío de solicitudes de clientes para 360s (180 X 2). Si se activan una tercera o más averías consecutivas, WAF deja de reenviar solicitudes de clientes para 540s (180s X 3). Las averías se cuentan desde 0 cuando la duración total del tiempo de inactividad supera una hora (3,600s).
- **Connection Protection**: Cuando el número de solicitudes de URL leídas en la cola de espera supera los 6,000 el WAF deja de reenviar las solicitudes del cliente durante 60 segundos y devuelve la página de mantenimiento del sitio web a los visitantes.

----Fin

4.8 Cambio del algoritmo de equilibrio de carga

Si configura una o más direcciones de servidor de origen, puede utilizar un algoritmo de equilibrio de carga para distribuir el tráfico entre estos servidores de origen. WAF admite los siguientes algoritmos:

- **Origin server IP hash**: Las solicitudes de la misma dirección IP se enrutan al mismo servidor backend.
- **Weighted round robin**: Las solicitudes se distribuyen entre los servidores backend a su vez en función del peso que asigne a cada servidor.
- **Session hash**: Las solicitudes con la misma etiqueta de sesión se enrutan al mismo servidor de origen. Para habilitar este algoritmo, **configure identificadores de tráfico para fuentes de ataque conocidas**, o el algoritmo hash de sesión no puede tener efecto.

Prerrequisitos

El sitio web que desea proteger se ha agregado a WAF.

Restricciones

- Ha seleccionado **Cloud mode** para la implementación de su sitio web.
- Solo las ediciones profesional (anteriormente edición empresarial) y platino (anteriormente última edición) admiten algoritmos de equilibrio de carga.
- Actualmente, WAF admite algoritmos de equilibrio de carga en las siguientes regiones:
  - CN-Hong Kong
  - AP-Bangkok

Procedimiento

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.

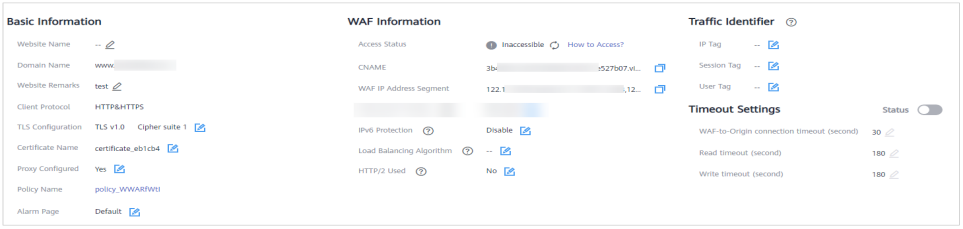
 Copyright © Huawei Technologies Co., Ltd.

Paso 3 Haga clic 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 **Protected Website**, haga clic en el nombre de dominio del sitio web para ir a la página de información básica.

Figura 4-9 Área de información básica



Paso 6 En el campo **Load Balancing Algorithm**, haga clic en . En el cuadro de diálogo que se muestra, seleccione un algoritmo de equilibrio de carga y haga clic en **OK**.

----Fin

4.9 Actualización de un certificado

Si selecciona **Cloud mode** o **Dedicated mode** para la implementación del sitio web y establece **Client Protocol** en **HTTPS**, carga un certificado para tu sitio web en los siguientes escenarios:

- Si su certificado de sitio web está a punto de caducar, compre un nuevo certificado antes de la fecha de caducidad y actualice el certificado asociado con el sitio web en WAF.
- Si tiene previsto actualizar el certificado asociado con el sitio web, asocie un nuevo certificado con su sitio web en la consola WAF.

NOTA

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 empresa en la lista desplegable de **Enterprise Project** y actualizar los certificados.

Prerrequisitos

- El modo de implementación de la instancia WAF configurada para su sitio web es **Cloud mode** o **Dedicated mode**.
- Su sitio web utiliza HTTPS como protocolo de cliente.

Restricciones

- Cada nombre de dominio debe tener un certificado asociado. Un nombre de dominio de carácter comodín solo puede usar un certificado de dominio de carácter comodín. Si solo tiene certificados de un solo dominio, agregue nombres de dominio uno por uno en WAF.
- Solo se pueden utilizar certificados .pem en WAF. Si el certificado no es in.pem, antes de subirlo, conviértelo a.pem haciendo referencia a **Paso 6**.

 Copyright © Huawei Technologies Co., Ltd.

- Antes de actualizar el certificado, asegúrese de que su instancia WAF y el certificado que desea cargar pertenecen a la misma cuenta.
- WAF no envía notificaciones si un certificado caduca, pero puede ver la hora de caducidad del certificado en la página **Certificates**.

Impacto en el sistema

- Se recomienda que actualice el certificado antes de que caduque. De lo contrario, todas las reglas de protección WAF no entrarán en vigor, y puede haber impactos masivos en el servidor de origen, incluso más graves que un host bloqueado o fallas de acceso al sitio web.
- La actualización de certificados no afecta a los servicios. El certificado antiguo todavía funciona durante la sustitución del certificado. El nuevo certificado se hará cargo del trabajo una vez que se haya subido y asociado correctamente con el nombre de dominio.
- El acceso a su sitio web puede verse afectado cuando actualiza las configuraciones de los certificados utilizados para servidores back-end o para nombres de dominio de sus sitios web protegidos por WAF. Para minimizar estos impactos, actualice los certificados durante las horas no pico.

Procedimiento

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 In the navigation pane, choose **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 al nombre del certificado. En el cuadro de diálogo **Update Certificate**, importe un nuevo certificado o seleccione un certificado existente.

- Si selecciona **Import new certificate** para **Update Method**, introduzca un nombre de certificado y copie y pegue el archivo de certificado y la clave privada en los cuadros de texto correspondientes. **Figura 4-10** muestra un ejemplo.

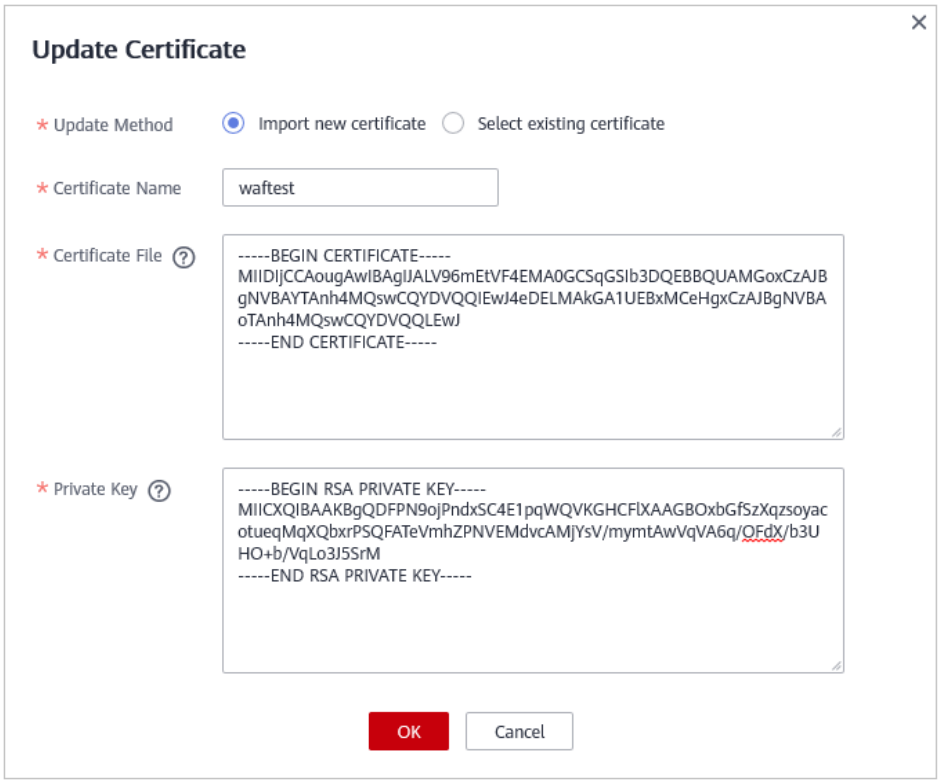
  Los certificados recién importados aparecerán en la página **Certificates**. Para más detalles, consulte **Carga de un certificado**.

  NOTA

  WAF encripta y guarda la clave privada para mantenerla segura.

 Copyright © Huawei Technologies Co., Ltd.

Figura 4-10 Actualizar certificado



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 4-6** antes de cargarlo.

Tabla 4-6 Comandos de conversión de certificados

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

 Copyright © Huawei Technologies Co., Ltd.

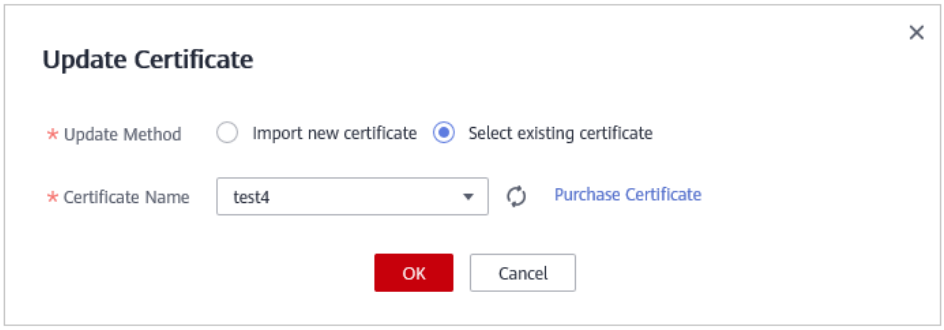
Formato	Método de conversión
DER	– Obtener una clave privada. Por ejemplo, ejecute el siguiente comando para convertir **privatekey.der** en **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** – Obtener un certificado. Por ejemplo, ejecute el siguiente 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.

- Si selecciona **Select existing certificate** para **Update Method**, seleccione un certificado existente en la lista desplegable de **Certificate Name**.

Figura 4-11 Selección de un certificado existente



NOTA

Si no hay certificados disponibles, haga clic en **Purchase Certificate** y compre un certificado y envíelo a WAF.

Paso 7 Haga clic en **OK**.

----Fin

Otras operaciones

Carga de un certificado

 Copyright © Huawei Technologies Co., Ltd.

4.10 Configuración de un identificador de tráfico para un Known Attack Source

WAF le permite configurar identificadores de tráfico por dirección IP, sesión o etiqueta de usuario para bloquear posibles solicitudes maliciosas de fuentes de ataque conocidas basadas en **IP address**, **Cookie**, o **Params**.

NOTA

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 **Enterprise Project** y configurar los identificadores de tráfico de origen de ataque conocidos para los nombres de dominio.

Prerrequisitos

El sitio web a proteger se ha agregado a WAF.

Restricciones

- Si la etiqueta de dirección IP está configurada, asegúrese de que el sitio web protegido tiene un proxy de capa 7 configurado delante de WAF y que **Proxy Configured** está configurado en **Yes** para el sitio web protegido.

  Si la etiqueta de dirección IP no está configurada, WAF identifica la dirección IP del cliente de forma predeterminada.
- Antes de habilitar las reglas de known attack source basadas en cookies o parámetros, configure una etiqueta de sesión o de usuario para el nombre de dominio del sitio web correspondiente.

Procedimiento

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 In the navigation pane, choose **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 En el área **Traffic Identifier**, haga clic en junto a **IP Tag**, **Session Tag**, o **User Tag** para configurar un identificador de tráfico mediante referencia **Tabla 4-7**. **Figura 4-12** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 4-12 Identificador de tráfico

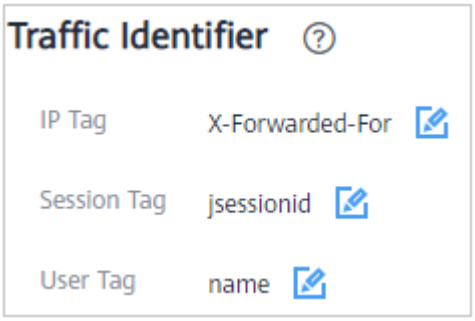


Tabla 4-7 Parámetros del identificador de tráfico

Etiqueta	Descripción	Valor de ejemplo
Etiqueta IP	Campo de encabezado de solicitud HTTP de la dirección IP original del cliente. Asegúrese de que el sitio web protegido tiene un proxy de capa 7 configurado delante de WAF y que el **Proxy Configured** bajo la configuración de información básica del sitio web está establecido en **Yes** para que este parámetro tenga efecto.	X-Forwarded-For
Etiqueta de sesión	Esta etiqueta se utiliza para bloquear solicitudes posiblemente maliciosas basadas en los atributos de cookies de una fuente de ataque. Configure este parámetro para bloquear solicitudes basadas en atributos de cookies.	jssessionid
Etiqueta de usuario	Esta etiqueta se utiliza para bloquear solicitudes posiblemente maliciosas basadas en el atributo Params de una fuente de ataque. Configure este parámetro para bloquear solicitudes basadas en los atributos Params.	name

Paso 7 Haga clic en **OK**.

----Fin

Otras operaciones

Configuración de una regla de origen de ataque conocida

 Copyright © Huawei Technologies Co., Ltd.

4.11 Edición de información del servidor

Después de agregar un sitio web en **Cloud mode** o **dedicated mode**, puede editar la información del servidor de su sitio web.

Casos de aplicación:

- Editar la información del servidor.
  - Modo Cloud: puede modificar las configuraciones para **Client Protocol**, **Server Protocol**, **Server Address**, y **Server Port**.
  - Modo dedicado: puede modificar las configuraciones para **Client Protocol**, **Server Protocol**, **Server Address**, **VPC**, y **Server Port**.
- Agregar configuraciones de servidor.
- Actualizar un certificado haciendo referencia a **Actualización de un certificado**.

NOTA

Si ha habilitado proyectos empresarial, 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 empresa en la lista desplegable **Enterprise Project** y configurar la información del servidor para los nombres de dominio.

Prerrequisitos

Se ha agregado un nombre de dominio a WAF. Ha seleccionado **Cloud mode** o **Dedicated mode** para la implementación del sitio web.

Impacto en el sistema

La modificación de la configuración del servidor no afecta a los servicios.

Procedimiento

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 In the navigation pane, choose **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 En el área **Server Information**, haga clic en . **Figura 4-13** muestra un ejemplo.

Figura 4-13 Información del servidor

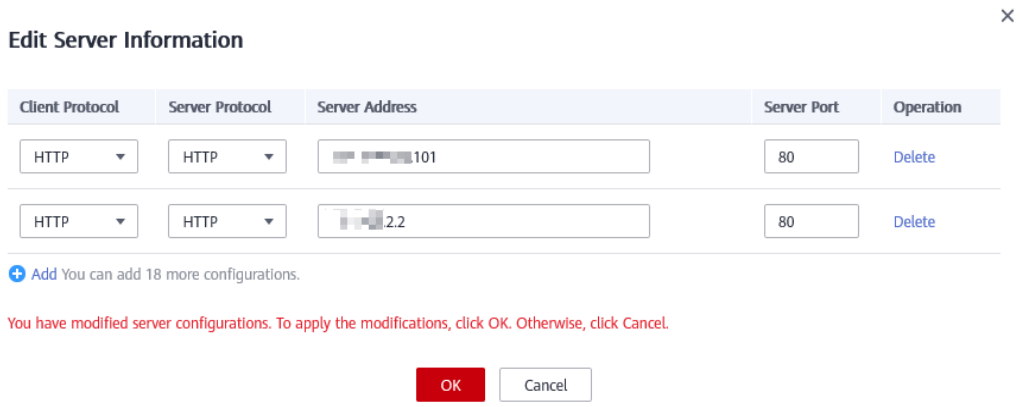
 Copyright © Huawei Technologies Co., Ltd.

Paso 7 En la página **Edit Server Information**, edite las configuraciones del servidor (como el protocolo de cliente y el certificado asociado). **Figura 4-14** muestra un ejemplo.

NOTA

- Para obtener más información sobre el certificado, consulte **Actualización de un certificado**.
- WAF admite la configuración de múltiples servidores back-end. Para agregar un servidor backend, haga clic en **Add**.

Figura 4-14 Editar información del servidor



Paso 8 Haga clic en**OK**.

----Fin

Verificación

Después de que se modifica la información del servidor, se tarda aproximadamente dos minutos para que la modificación surta efecto.

4.12 Modificación de la página de alarma

Si un visitante es bloqueado por WAF, la página de bloqueo **predeterminado** de WAF se devuelve por defecto. También puede configurar **Custom** o **Redirection** para que la página de bloque se devuelva según sea necesario.

NOTA

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 empresarial en la lista desplegable **Enterprise Project** y personalizar las páginas de alarma para los nombres de dominio.

Prerrequisitos

Se ha agregado un nombre de dominio a WAF.

Restricciones

- El contenido de las páginas text/html, text/xml y application/json se puede configurar en la página **Custom** que se va a devolver.

 Copyright © Huawei Technologies Co., Ltd.

- El nombre de dominio root de la dirección de redirección debe ser el mismo que el nombre de dominio actualmente protegido (incluido un nombre de dominio comodín). Por ejemplo, si el nombre de dominio protegido es **www.example.com** y el puerto es 8080, la URL de redirección se puede establecer en **http://www.example.com:8080/error.html**.

Procedimiento

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**.

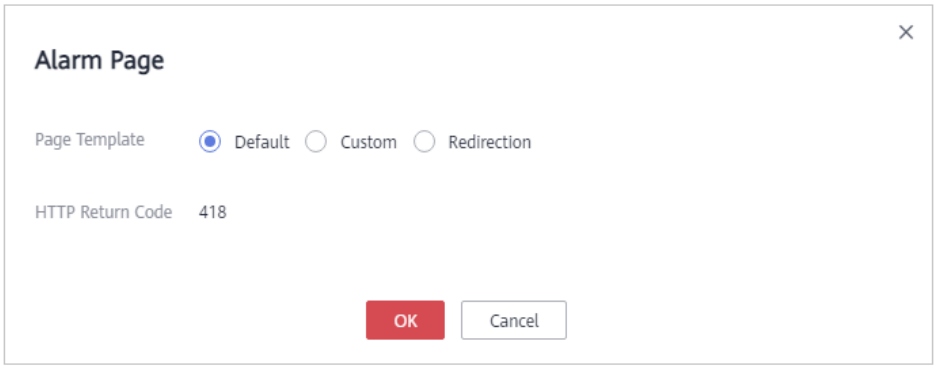
Paso 4 In the navigation pane, choose **Website Settings**.

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 junto al nombre de la plantilla de página en la fila donde se encuentra **Alarm Page**. En el cuadro de diálogo **Alarm Page** que se muestra, especifique **Page Template**.

- Para utilizar la página integrada, seleccione **Default**. Se devuelve un código HTTP 418.

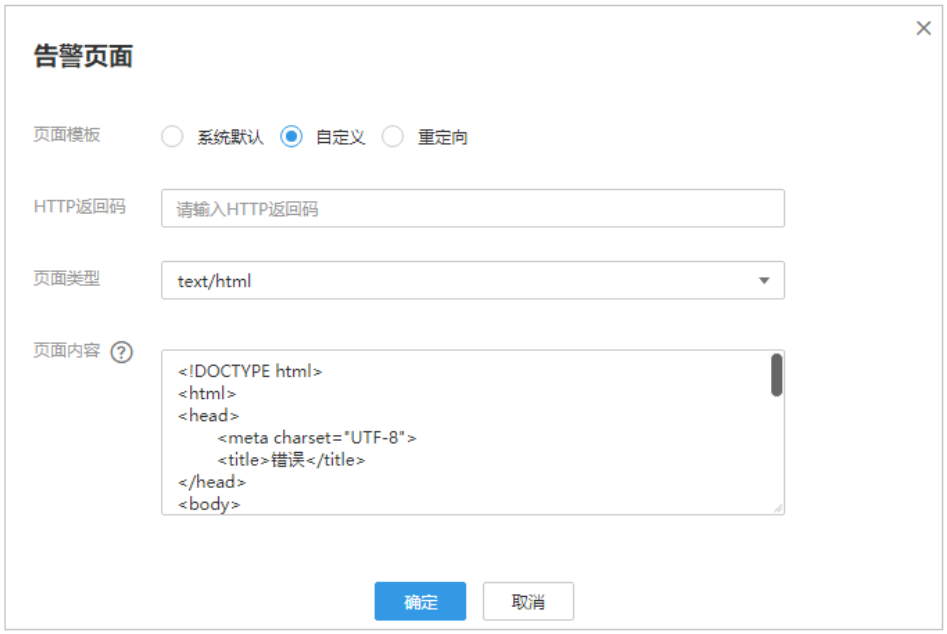
  Figura 4-15 Página de alarma predeterminada

- Para personalizar la página de alarma, seleccione **Custom** y configure los siguientes parámetros. **Figura 4-16** muestra un ejemplo.
  - **HTTP Return Code**: código de retorno configurado en una página personalizada.
  - **Block Page Tkype**: Las opciones son **text/html**, **text/xml**, y **application/json**.
  - **Page Content**: configure el contenido de la página en función del valor seleccionado para **Block Page Type**.

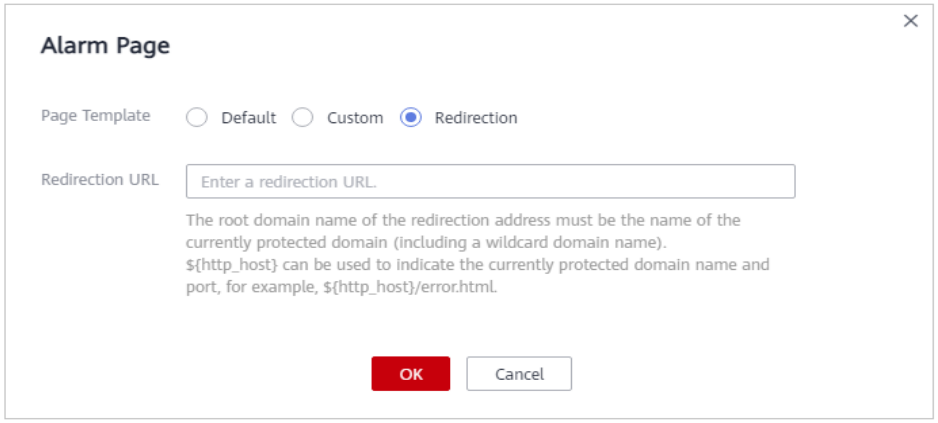
 Copyright © Huawei Technologies Co., Ltd.

Figura 4-16 Página de alarma personalizada



- Para configurar una URL de redirección, seleccione **Redirection**.

Figura 4-17 Página de alarma de redirección



El nombre de dominio de root de la URL de redirección debe ser el mismo que el nombre de dominio actualmente protegido (incluido un nombre de dominio de carácter comodín). Por ejemplo, si el nombre de dominio protegido es **www.example.com** y el puerto es 8080, la URL de redirección se puede establecer en **http://www.example.com:8080/error.html**.

Paso 7 Haga clic en **OK**.

----Fin

4.13 Eliminación de un sitio web protegido de WAF

En este tema se describe cómo eliminar un sitio web de WAF si ya no es necesario protegerlo.

 Copyright © Huawei Technologies Co., Ltd.

NOTA

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 su proyecto empresarial en la lista desplegable **Enterprise Project** y eliminar los nombres de dominio protegidos.

Prerrequisitos

Se ha agregado un nombre de dominio de sitio web a WAF.

Impacto en el sistema

- Si desea eliminar un sitio web protegido en **Cloud mode** de la instancia WAF, vaya a la plataforma DNS y traduzca el nombre de dominio a la dirección IP del servidor de origen antes de eliminarlo. De lo contrario, el tráfico destinado al nombre de dominio no se dirigirá al servidor de origen.
- Se tarda aproximadamente un minuto para eliminar un sitio web de WAF. Tenga en cuenta que la acción de eliminación no se puede cancelar.

Procedimiento

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**.

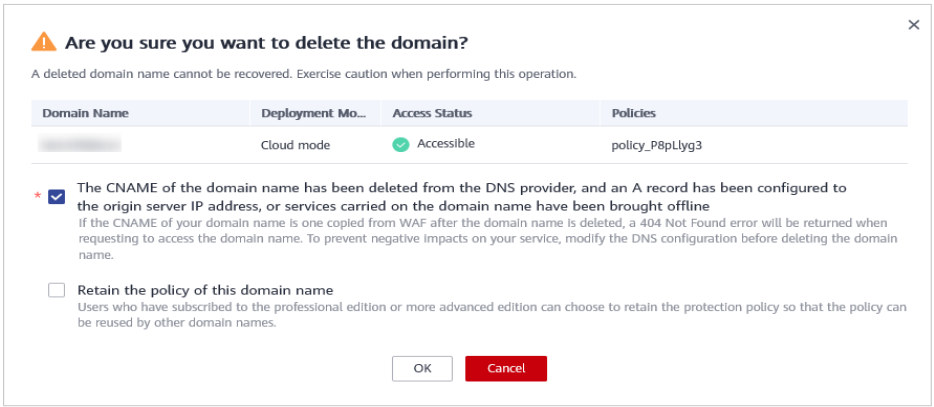
Paso 4 In the navigation pane, choose **Website Settings**.

Paso 5 En la fila que contiene el nombre de dominio del sitio web que desea eliminar, haga clic en **Delete** en la columna **Operation**.

Paso 6 En el cuadro de diálogo de confirmación que se muestra, confirme la eliminación.

- Modo de Cloud
  - No proxy utilizado

Figura 4-18 Eliminación de un nombre de dominio protegido (no se utiliza proxy)



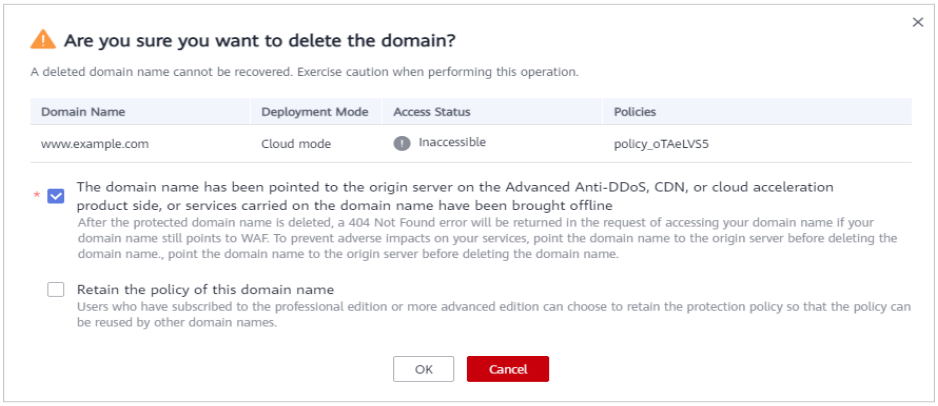
 Copyright © Huawei Technologies Co., Ltd.

NOTA

- Asegúrese de que se hayan completado las configuraciones relacionadas y seleccione **The CNAME of the domain name has been deleted from the DNS provider, and an A record has been configured to the origin server IP address, or services carried on the domain name have been brought offline**.
- Si desea conservar la política vinculada al nombre de dominio, seleccione **Retain the policy of this domain name**.

– Proxy utilizado

Figura 4-19 Eliminación de un nombre de dominio protegido (proxy usado)



NOTA

- Asegúrese de que se hayan completado las configuraciones relacionadas y seleccione **The domain name has been pointed to the origin server on the Advanced Anti-DDoS, CDN, or cloud acceleration product side, or services carried on the domain name have been brought offline**.
- Si desea conservar la política vinculada al nombre de dominio, seleccione **Retain the policy of this domain name**.

- Modo dedicado

  Si desea conservar la política aplicada al nombre de dominio, seleccione **Retain the policy of this domain name**.

Paso 7 Haga clic en **OK**.

Si **Domain name deleted successfully** se muestra en la esquina superior derecha, se eliminó el nombre de dominio del sitio web.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

5 Gestión de certificados

5.1 Carga de un certificado

Si seleccionas **Cloud mode** o **Dedicated mode** para la implementación del sitio web y estableces **Client Protocol** en **HTTPS**, se debe asociar un certificado al sitio web.

Puede cargar un certificado en WAF. A continuación, puede seleccionar directamente el certificado cargado para el sitio web protegido.

NOTA

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 su proyecto de empresa en la lista desplegable de **Enterprise Project** y cargar certificados en el proyecto.

Prerrequisitos

Ha obtenido el archivo de certificado y la clave privada del certificado.

Limitaciones de la especificación

Puede cargar tantos certificados en WAF como el número de nombres de dominio que pueden proteger sus instancias WAF en la misma cuenta. Por ejemplo, si compra una instancia WAF de edición estándar (anteriormente edición profesional), que puede proteger 10 nombres de dominio, y un paquete de expansión de nombres de dominio, que puede proteger 20 nombres de dominio, su instancia WAF puede proteger 30 nombres de dominio en total. En este caso, puede cargar 30 certificados.

Restricciones

- Si compra un certificado en la consola SCM y lo envía a WAF, el certificado se agrega a la lista de certificados en la página **Certificates** en la consola WAF. Este certificado también se cuenta para su cuota total de certificados. Para obtener más información sobre cómo enviar un certificado SSL en SCM a WAF, consulte **Envío de un certificado SSL a otros servicios en la nube**.

 Copyright © Huawei Technologies Co., Ltd.

AVISO

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.

- Si importa un certificado nuevo al agregar un sitio Web protegido o actualizar un certificado, el certificado se agrega a la lista de certificados de la página **Certificates** y el certificado importado también se cuenta para la cuota total de certificados.

Escenario de aplicación

Si selecciona **HTTPS** para **Client Protocol**, se requiere un certificado.

Procedimiento

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, elija **Objects** > **Certificates**.

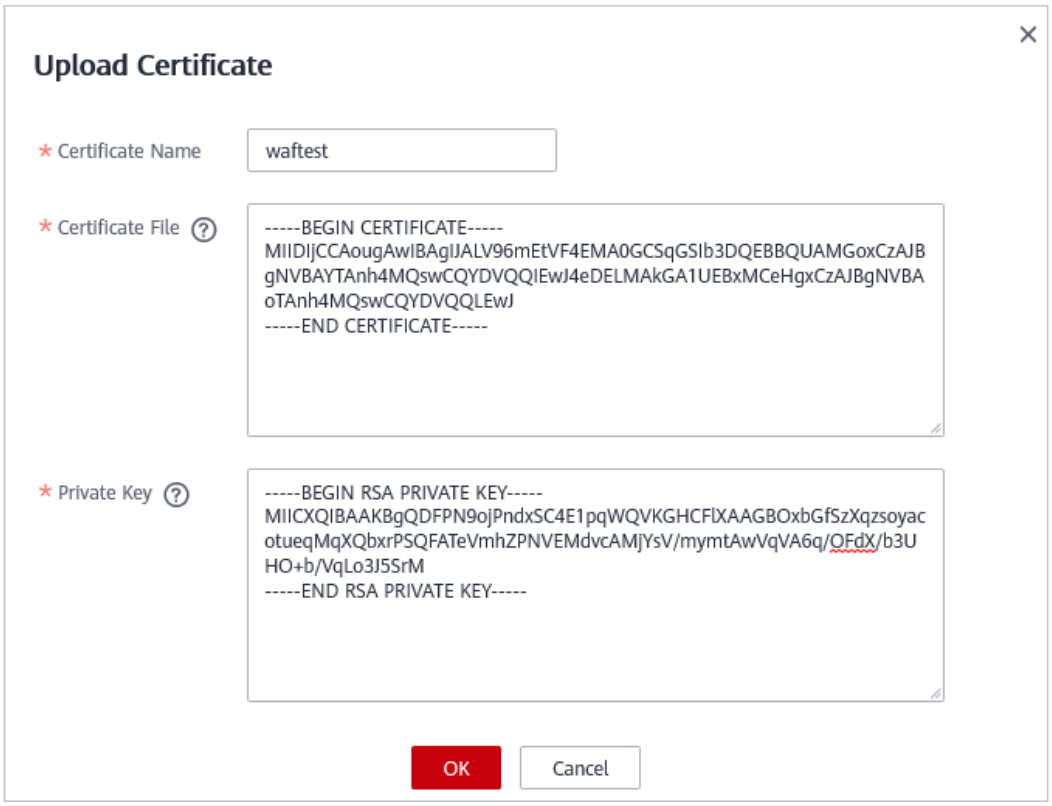
Figura 5-1 Lista de certificados

Paso 5 Haga clic en **Upload Certificate**.

Paso 6 En el cuadro de diálogo **Upload Certificate**, escriba un nombre de certificado y copie el archivo de certificado y la clave privada en los cuadros de texto correspondientes. **Figura 5-2** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 5-2 Upload Certificate



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 5-1** antes de cargarlo.

Tabla 5-1 Comandos de conversión de certificados

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

 Copyright © Huawei Technologies Co., Ltd.

Formato	Método de conversión
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.

Paso 7 Haga clic en **OK**.

----Fin

Verificación

El certificado que ha creado se muestra en la lista de certificados.

Otras operaciones

- Para cambiar el nombre del certificado, mueva el cursor sobre el nombre del certificado, haga clic y escriba un nombre de certificado.

  AVISO

  Si el certificado está en uso, desvincule primero el certificado del nombre de dominio. De lo contrario, el nombre del certificado no se puede cambiar.

- Para ver los detalles de un certificado, haga clic en **View** en la columna **Operation** del certificado.
- En la fila que contiene el certificado que desea, haga clic en **Use** en la columna **Operation** para usar el certificado con el nombre de dominio correspondiente.
- Para eliminar un certificado, busque la fila del certificado y haga clic en **Delete** en la columna **Operation**.

5.2 Vinculación de un certificado a un sitio web protegido

Si configura **Client Protocol** a **HTTPS** para su sitio web, el sitio web necesita un certificado SSL. En este tema se describe cómo vincular un certificado SSL que ha subido a WAF a un sitio web.

 Copyright © Huawei Technologies Co., Ltd.

NOTA

Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable **Enterprise Project** y vincular certificados a sitios web del proyecto.

Prerrequisitos

- Su certificado sigue siendo válido.
- Su sitio web utiliza HTTPS como protocolo de cliente.

Restricciones

- Un certificado SSL se puede utilizar para múltiples sitios web protegidos.
- Un sitio web protegido solo puede utilizar un certificado SSL.

Escenario de aplicación

Si configura **Client Protocol** a **HTTPS**, se requiere un certificado.

Procedimiento

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, elija **Objects** > **Certificates**.

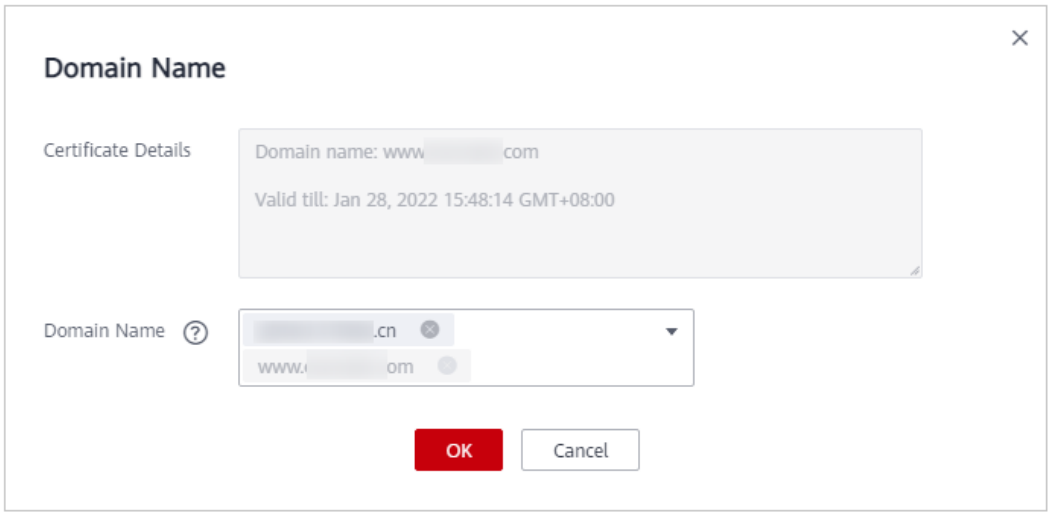
Figura 5-3 Lista de certificados

Paso 5 En la fila que contiene el certificado que desea utilizar, haga clic en **Use** en la columna **Operation**.

Paso 6 En el cuadro de diálogo **Domain Name** que se muestra, seleccione el sitio web en el que desea utilizar el certificado.

 Copyright © Huawei Technologies Co., Ltd.

Figura 5-4 Cuadro de diálogo Nombre de dominio



Paso 7 Haga clic en **OK**.

----Fin

Verificación

El sitio web protegido aparece en la columna **Domain Name** del certificado.

Otras operaciones

- Para cambiar el nombre del certificado, mueva el cursor sobre el nombre del certificado, haga clic y escriba un nombre de certificado.

  AVISO

  Si el certificado está en uso, desvincule primero el certificado del nombre de dominio. De lo contrario, el nombre del certificado no se puede cambiar.

- Para ver los detalles de un certificado, haga clic en **View** en la columna **Operation** del certificado.
- Para eliminar un certificado, busque la fila del certificado y haga clic en **Delete** en la columna **Operation**.

5.3 Eliminación de un certificado

En este tema se describe cómo eliminar un certificado caducado o no válido.

NOTA

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 **Enterprise Project** y eliminar un certificado.

 Copyright © Huawei Technologies Co., Ltd.

Prerrequisitos

El certificado que desea eliminar no está vinculado a un sitio web protegido.

Restricciones

Si un certificado que se va a eliminar está enlazado a un sitio web, desvinúelo del sitio web antes de eliminarlo.

Impacto en el sistema

- La eliminación de certificados no afecta a los servicios.
- Los certificados eliminados no se pueden recuperar. Tenga cuidado al realizar esta operación.

Procedimiento

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, elija **Objects** > **Certificates**.

Figura 5-5 Lista de certificados

Paso 5 En la fila que contiene el certificado que desea eliminar, haga clic en **Delete** en la columna **Operation**.

Paso 6 En el cuadro de diálogo mostrado, haga clic en **OK**.

----Fin

Otras operaciones

Si un certificado que se va a eliminar está enlazado a un sitio web, desvinúelo del sitio web antes de eliminarlo.

Para desvincular un certificado de un nombre de dominio de sitio web, realice los siguientes pasos:

Paso 1 En la columna **Domain Name** de la fila que contiene el certificado deseado, haga clic en el nombre de dominio para ir a la página de información básica.

 Copyright © Huawei Technologies Co., Ltd.

Paso 2 Haga clic en junto al nombre del certificado. En el cuadro de diálogo que se muestra, cargue un nuevo certificado o seleccione un certificado existente.

----Fin

5.4 Consulta de información de certificado

En este tema se describe cómo ver los detalles del certificado, incluido el nombre del certificado, el nombre de dominio para el que se utiliza un certificado y la hora de caducidad.

NOTA

Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable **Enterprise Project** y ver certificados en el proyecto.

Prerrequisitos

Ha creado o enviado un certificado a WAF.

Restricciones

- En el caso de los **certificados que cargue en WAF**, WAF no le envía notificaciones de caducidad.
- Para los certificados que envía de CCM a WAF, el período de validez del certificado se puede ver en WAF solo cuando se habilitan las notificaciones de caducidad del certificado en CCM.

Procedimiento

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, elija **Objects** > **Certificates**.

Figura 5-6 Lista de certificados

Paso 5 Ver la información del certificado. **Tabla 5-2** describe los parámetros.describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Tabla 5-2 Descripción del parámetro

Parámetro	Descripción
Name	Nombre del certificado.
Domain Name	Los nombres de dominio protegidos por el certificado Cada nombre de dominio debe estar enlazado a un certificado. Se puede utilizar un certificado para varios nombres de dominio.
Expired	Tiempo de caducidad del certificado. Se recomienda que actualice el certificado antes de que caduque. De lo contrario, todas las reglas de protección WAF no tendrán efecto, y puede haber impactos masivos en el servidor de origen, incluso más graves que un host bloqueado o fallas de acceso al sitio web. Para más detalles, consulte **Actualización de un certificado**.

----Fin

Otras operaciones

- Para cambiar el nombre del certificado, mueva el cursor sobre el nombre del certificado, haga clic y escriba un nombre de certificado.

  AVISO

  Si el certificado está en uso, desvincule primero el certificado del nombre de dominio. De lo contrario, el nombre del certificado no se puede cambiar.

- Para ver los detalles de un certificado, haga clic en **View** en la columna **Operation** del certificado.
- En la fila que contiene el certificado que desea, haga clic en **Use** en la columna **Operation** para usar el certificado con el nombre de dominio correspondiente.
- Para eliminar un certificado, busque la fila del certificado y haga clic en **Delete** en la columna **Operation**.

 Copyright © Huawei Technologies Co., Ltd.

6 Gestión de grupos de listas negras y listas blancas de direcciones IP

6.1 Agregar un grupo de direcciones IP

Con los grupos de direcciones IP, puede agregar rápidamente direcciones IP o intervalos de direcciones IP a una regla de lista negra o de lista blanca.

NOTA

Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable de **Enterprise Project** y agregar grupos de direcciones IP/rangos en el proyecto.

Prerrequisitos

Usted ha comprado WAF.

Restricciones

- Actualmente, la gestión de grupos de direcciones se apoya en las regiones de CN-Hong Kong, y AP-Bangkok.
- No agregue la misma dirección IP o rango de direcciones IP a diferentes grupos de direcciones IP, o los grupos de direcciones IP no se crearán.
- Si los balanceadores de carga ELB utilizados para las instancias de WAF dedicadas o de equilibrio de carga admiten direcciones IPv6, esas instancias de WAF también pueden admitir direcciones IPv6 o intervalos de direcciones IPv6.

Limitaciones de la especificación

- Se puede crear un máximo de 50 grupos de direcciones. Se puede agregar un máximo de 200 direcciones IP o intervalos de direcciones IP a un grupo de direcciones. Utilice comas (,) para separar varias direcciones IP o intervalos de direcciones IP. No se permiten saltos de línea.
- Antes de agregar un grupo de direcciones a una regla de lista negra o blanca, asegúrese de que la cuota de reglas de la lista negra y la lista blanca de direcciones IP no se haya agotado.

 Copyright © Huawei Technologies Co., Ltd.

NOTA

- Para más detalles, consulte **Configuración de una lista negra o una regla de lista blanca de direcciones IP**.

  Para obtener más información sobre las especificaciones, consulte **Diferencias de edición**.
- Si la cuota para las reglas de la lista blanca y la lista negra de direcciones IP de su WAF en la nube no puede cumplir con sus requisitos, puede comprar paquetes de expansión de reglas bajo la edición de instancia WAF actual o actualizar su edición de instancia WAF para aumentar dicha cuota. Un paquete de expansión de reglas le permite configurar hasta 10 reglas de listas negras y blancas de direcciones IP.

  Para obtener más información, consulte **Actualización de edición y especificación de Cloud WAF**.

Procedimiento

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, elija **Objects** > **Address Groups**.

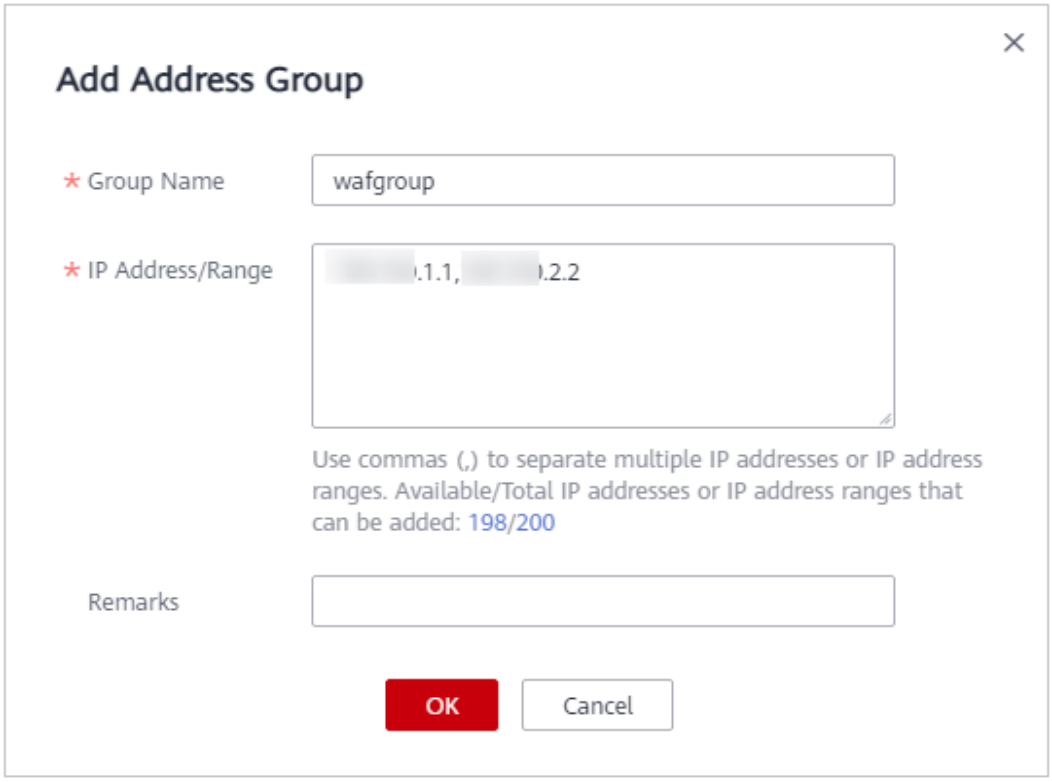
Paso 5 Haga clic en la pestaña **My Address Groups**.

Paso 6 En la parte superior izquierda de la lista de grupos de direcciones, haga clic en **Add Address Group**.

Paso 7 En el cuadro de diálogo **Add Address Group** que se muestra, introduzca un nombre de grupo de direcciones y proporcione rangos de direcciones IP. **Figura 6-1** muestra un ejemplo.

Copyright © Huawei Technologies Co., Ltd.

Figura 6-1 Agregar grupo de direcciones



Paso 8 Haga clic en **OK**.

----Fin

6.2 Modificación o eliminación de un grupo de direcciones IP de lista negra o blanca

En este tema se describe cómo modificar o eliminar un grupo de direcciones IP.

NOTA

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 **Enterprise Project** y modificar o eliminar un grupo de direcciones IP.

Prerrequisitos

Ha creado un grupo de direcciones IP.

Restricciones

- No agregue una dirección IP o un rango de direcciones IP que se haya agregado a un grupo de direcciones IP diferente al grupo de direcciones existente, o el grupo de direcciones IP no se modificará.

Copyright © Huawei Technologies Co., Ltd.

- Solo los grupos de direcciones no utilizados por ninguna regla pueden ser eliminados. Antes de eliminar un grupo de direcciones que está siendo utilizado por una regla de lista negra o de lista blanca, elimine primero el grupo de direcciones de la regla.

Procedimiento

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, elija **Objects** > **Address Groups**.

Paso 5 Haga clic en la pestaña **My Address Groups**.

Paso 6 En la lista de grupos de direcciones, vea la información del grupo de direcciones.

Tabla 6-1 Descripción del parámetro

Parámetro	Descripción
Group Name	Nombre del grupo de direcciones configurado.
IP Address/Range	Direcciones IP o intervalos de direcciones IP agregados al grupo de direcciones.
Rule	Reglas que utilizan el grupo de direcciones.
Remarks	Información adicional sobre el grupo de direcciones.

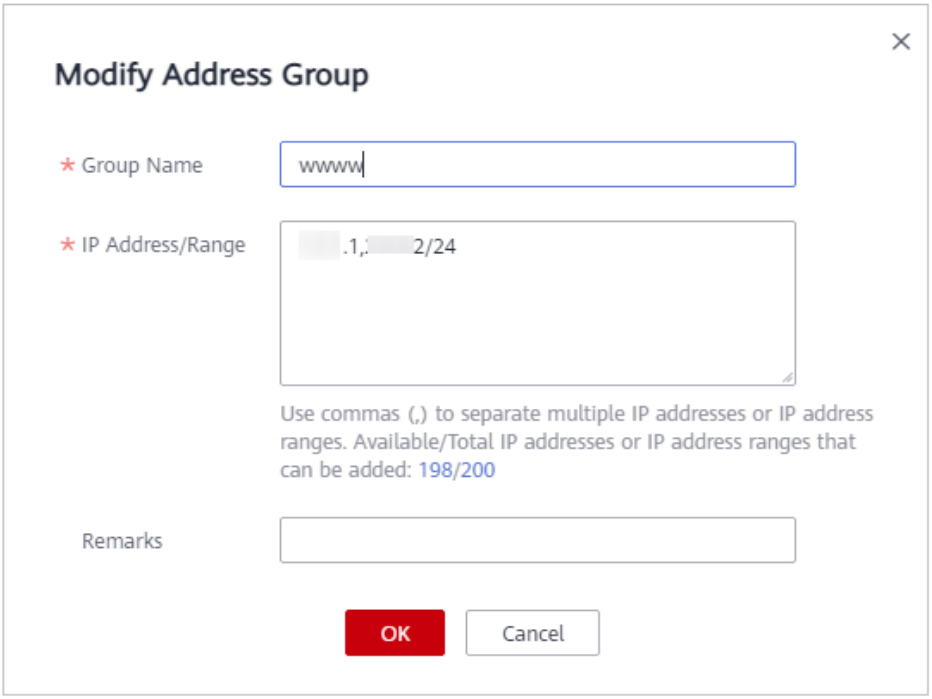
Paso 7 Modificar o eliminar un grupo de direcciones IP.

- Modificar un grupo de direcciones.

  En la fila que contiene el grupo de direcciones que desea modificar, haga clic en **Modify** en la columna **Operation**. En el cuadro de diálogo **Modify Address Group**, cambie el nombre del grupo o el intervalo de direcciones IP/dirección IP y haga clic en **OK**.

Copyright © Huawei Technologies Co., Ltd.

Figura 6-2 Modificar grupo de direcciones



- Eliminar un grupo de direcciones.

  En la fila que contiene el grupo de direcciones que desea eliminar, haga clic en **Delete** en la columna **Operation**. En el cuadro de diálogo mostrado, haga clic en **OK**.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

7 Configuración de regla

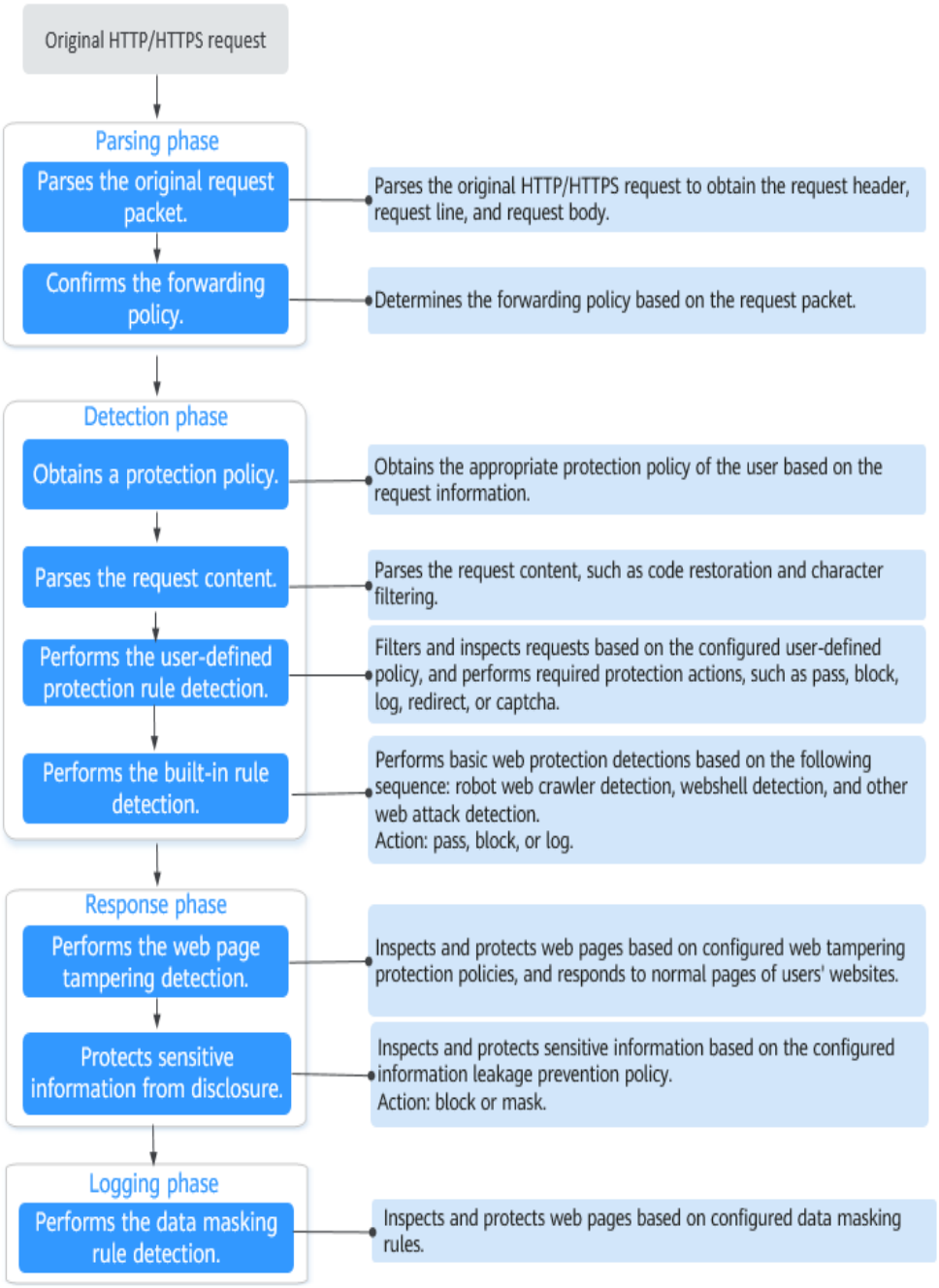
7.1 Guía de configuración

Cómo funciona el motor WAF

Las reglas de protección incorporadas de WAF le ayudan a defenderte contra ataques comunes de aplicaciones web, incluidos ataques XSS, inyección SQL, rastreadores y web shells. Puede personalizar las reglas de protección para que WAF proteja mejor los servicios de su sitio web utilizando estas reglas personalizadas. **Figura 7-1**. muestra cómo funcionan las reglas de protección incorporadas del motor WAF. **Figura 7-2** muestra la secuencia de detección de reglas definidas por el usuario.

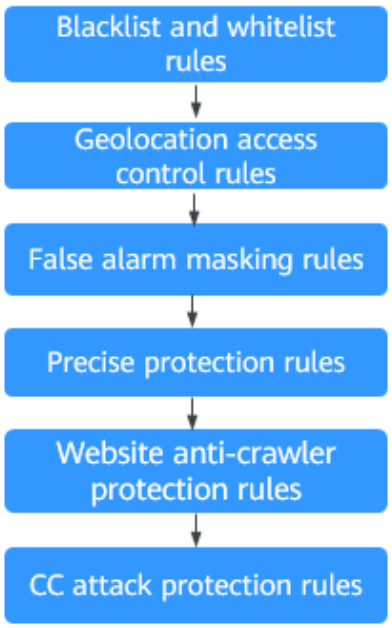
 Copyright © Huawei Technologies Co., Ltd.

Figura 7-1 Proceso de detección del motor WAF



 Copyright © Huawei Technologies Co., Ltd.

Figura 7-2 Prioridades de las reglas de protección personalizadas



Acciones de respuesta

- Pasar: La solicitud actual se permite incondicionalmente después de que se coincida con una regla de protección.
- Bloquear: La solicitud actual se bloquea después de que se coincide con una regla.
- CAPTCHA: El sistema realizará la verificación hombre-máquina después de que una regla sea coincidente.
- Redirigir: El sistema le notificará para redirigir la solicitud después de que una regla es coincidente.
- Registro: Solo se registra la información de ataque después de que se coincide con una regla.
- Máscara: El sistema anonimizará la información confidencial después de que se coincida con una regla.

Métodos de configuración de reglas de protección

WAF proporciona los siguientes métodos de configuración personalizados para simplificar el proceso de configuración. Seleccione un método de configuración adecuado para satisfacer sus requisitos de servicio.

Método 1: Configuración de reglas de protección para un solo nombre de dominio

Este método se recomienda cuando tiene pocos servicios de nombres de dominio o tiene reglas de configuración diferentes para los servicios de nombres de dominio.

 Copyright © Huawei Technologies Co., Ltd.

NOTA

Después de agregar un nombre de dominio a WAF, WAF asocia automáticamente una política de protección con el nombre de dominio y las reglas de protección configuradas para el nombre de dominio también se agregan a la política de protección de forma predeterminada. Si hay nombres de dominio aplicables a la política de protección, puede agregarlos directamente a la política. Para más detalles, consulte **Aplicación de una política a su sitio web**.

- Dónde configurar
  a. En el panel de navegación, seleccione **Website Settings**.
  b. En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.
- Reglas de protección que puede configurar en la página de configuración de reglas

Tabla 7-1 Reglas de protección configurables

Regla de protección	Descripción	Referencia
Reglas básicas de protección web	Con una extensa base de datos de reputación, WAF defiende contra las 10 principales amenazas del Open Web Application Security Project (OWASP), y detecta y bloquea amenazas, como escáneres maliciosos, direcciones IP y web shells.	**Configuración de reglas básicas de protección web**
Reglas de protección contra ataques CC	Las reglas de protección contra ataques de CC se pueden personalizar para restringir el acceso a una URL específica en su sitio web basándose en una dirección IP única, una cookie o un campo de referencia, lo que mitiga los ataques de CC.	**Configuración de una regla de protección contra ataques de CC**
Reglas de protección precisas	Puede personalizar las reglas de protección combinando encabezados HTTP, direcciones cookies URL, parámetros de solicitud y direcciones IP de cliente.	**Configuración de una regla de protección precisa**
Reglas de la lista negra y de la lista blanca	Puede configurar reglas de listas negras y blancas para bloquear, registrar únicamente o permitir solicitudes de acceso desde direcciones IP especificadas.	**Configuración de una lista negra o una regla de lista blanca de direcciones IP**

 Copyright © Huawei Technologies Co., Ltd.

Regla de protección	Descripción	Referencia
Reglas de control de acceso de geolocalización	Puede personalizar estas reglas para permitir o bloquear solicitudes de un país o región específico.	**Configuración de una regla de control de acceso de geolocalización**
Reglas de protección web contra manipulaciones	Puede configurar estas reglas para evitar que una página web estática sea manipulada.	**Configuración de una Regla de protección contra manipulaciones de Web**
Protección del sitio web anti-crawler	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.	**Configuración de las reglas de anti-crawler**
Normas de prevención de fugas de información	Puede agregar dos tipos de reglas de prevención de fugas de información. ● Filtrado de información confidencial: evita la divulgación de información confidencial (como números de identificación, números de teléfono y direcciones de correo electrónico). ● Intercepción de código de respuesta: bloquea los códigos de estado HTTP especificados.	**Configuración de una regla de prevención de fugas de información**
Reglas de enmascaramiento de falsas alarmas	Puede configurar estas reglas para permitir que WAF ignore ciertas reglas para solicitudes específicas.	**Configuración de una regla de enmascaramiento de falsa alarma**
Reglas de enmascaramiento de datos	Puede configurar reglas de enmascaramiento de datos para evitar que los datos confidenciales, como las contraseñas, se muestren en los registros de eventos.	**Configuración de una regla de enmascaramiento de datos**

Método 2: Configuración de reglas de protección para varios nombres de dominio

 Copyright © Huawei Technologies Co., Ltd.

Este método se recomienda si tiene muchos servicios de nombres de dominio y requiere la misma política de protección para varios nombres de dominio. Este método reduce en gran medida las cargas de trabajo de configuración repetidas y mejora la eficiencia de la protección.

- Dónde configurar

  En el panel de navegación de la izquierda, elija **Policies**.

- Procedimiento

  a. Agregue una política. Para más detalles, consulte **Agregar una política**.

  b. Configure reglas de protección. Para más detalles, consulte **Adición de reglas a una o más políticas**.

  c. Agregue por lotes varios nombres de dominio a la política. Para más detalles, consulte **Aplicación de una política a su sitio web**.

7.2 Configuración de reglas básicas de protección web

Una vez habilitada esta función, WAF puede defenderse contra ataques web comunes, como inyecciones SQL, XSS, vulnerabilidades de desbordamiento remoto, inclusiones de archivos, vulnerabilidades Bash, ejecución de comandos remotos, recorrido por directorios, acceso a archivos confidenciales e inyecciones de comandos/código. También puede habilitar otras comprobaciones en la protección web básica, como la detección de shell web, la inspección profunda contra ataques de evasión y la inspección de encabezados.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

- La protección web básica tiene dos modos: **Block** y **Log only**.
- Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.
- Si selecciona **Block** para **Basic Web Protection**, puede **configurar los criterios de control de acceso para un origen de ataque conocido**. WAF bloqueará las solicitudes que coincidan con la dirección IP, la cookie o los parámetros configurados durante un período de tiempo configurado como parte de la regla.
- Actualmente, la inspección profunda y la inspección del jefe se apoyan en CN-Hong Kong, y AP-Bangkok.
- Actualmente, la comprobación de descifrado de Shiro es compatible con China-Hong Kong.

 Copyright © Huawei Technologies Co., Ltd.

Procedimiento

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 In the navigation pane, choose **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**, cambie **Status** y **Mode** según sea necesario haciendo referencia a **Tabla 7-2**.

Figura 7-3 Área de configuración de Protección web básica

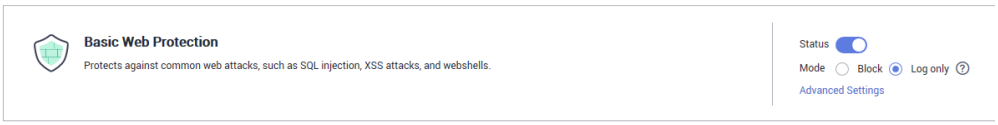


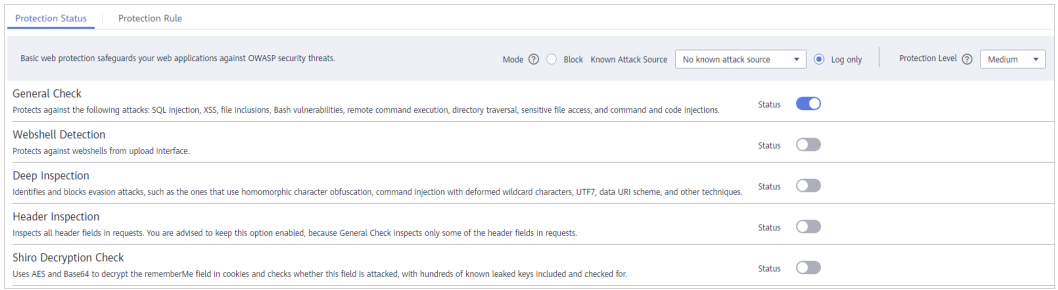
Tabla 7-2 Descripción del parámetro

Parámetro	Descripción
Status	Estado de la protección web básica ● : habilitado. ● : deshabilitado.
Mode	● **Block**: WAF bloquea y registra los ataques detectados. ● **Log only**: WAF solo registra los ataques detectados.

Paso 7 En el área de **Basic Web Protection**, haga clic en **Advanced Settings**.

Paso 8 Click the **Protection Status** tab, and enable protection types one by one by referring to **Tabla 7-4**. **Figura 7-4** shows an example.shows an example.

Figura 7-4 Protección web básica



 Copyright © Huawei Technologies Co., Ltd.

AVISO

Si selecciona **Mode** para **Block** en la pestaña **Protection Status**, puede seleccionar una regla de origen de ataque conocida para permitir que WAF bloquee las solicitudes en consecuencia. Para más detalles, consulte **Configuración de una regla de origen de ataque conocida**.

1. Establezca el nivel de protección.

   En la parte superior de la página, establezca **Protection Level** en **Low**, **Medium**, o **High**. El valor predeterminado es **Medium**.

   Tabla 7-3 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.

2. Establezca el tipo de protección.

   AVISO

   De forma predeterminada, **General Check** está habilitada. Puede habilitar otros tipos de protección haciendo referencia a **Tabla 7-4**.

 Copyright © Huawei Technologies Co., Ltd.

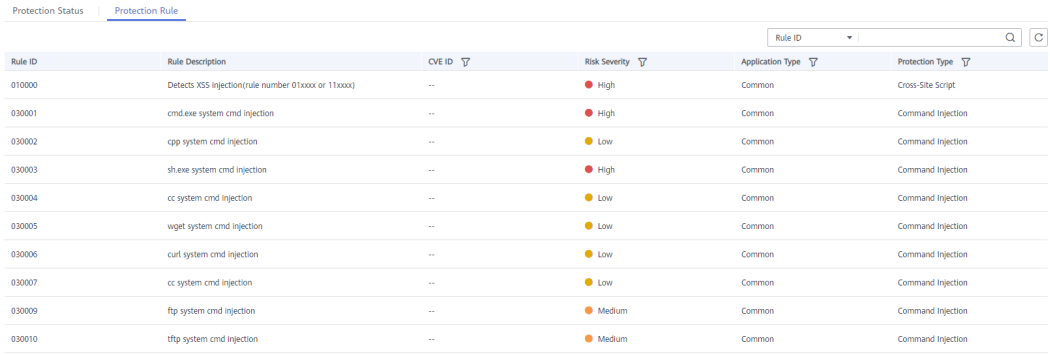
Tabla 7-4 Tipos de protección

Tipo	Descripción
Verificación general	Protege contra ataques como inyecciones SQL, XSS, vulnerabilidades de desbordamiento remoto, inclusiones de archivos, vulnerabilidades Bash, ejecución remota de comandos, recorrido de directorios, acceso a archivos confidenciales e inyecciones de código/comando. Los ataques de inyección de SQL se detectan principalmente en base a la semántica. **NOTA** Si habilita **General Check**, WAF comprueba sus sitios web basándose en las reglas incorporadas.
Detección de webshell	Protege contra shells web de la interfaz de carga. **NOTA** Si habilita la **Webshell Detection**, WAF detecta los caballos de Troya de la página web insertados a través de la interfaz de carga.
Inspección profunda	Identifica y bloquea los ataques de evasión, como los que usan ofuscación de caracteres homomórficos, inyección de comandos con caracteres comodín deformados, UTF7, esquema de URI de datos y otras técnicas. **NOTA** Si habilita **Deep Inspection**, WAF detecta y defiende contra ataques de evasión en profundidad.
Inspección de cabecera	Esta función está deshabilitada por defecto. Cuando está deshabilitada, General Check comprobará algunos de los campos de encabezado, como User-Agent, Content-type, Accept-Language y Cookie. **NOTA** Si habilita esta función, WAF comprueba todos los campos de encabezado de las solicitudes.
Comprobación de descifrado de Shiro	Esta función está deshabilitada por defecto. Después de activar esta función, WAF utiliza AES y Base64 para descifrar el campo de memoria de cookies y comprueba si este campo es atacado. Hay cientos de claves filtradas conocidas incluidas y comprobadas.

Paso 9 Haga clic en la pestaña **Protection Rules** para ver los detalles. **Figura 7-5** muestra un ejemplo. Para obtener más información sobre los parámetros, consulte **Tabla 7-5**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-5 Visualización de reglas de protección



NOTA

Haga clic para buscar una regla por **CVE ID**, **Risk Severity**, **Application Type**, o **Protection Type**.

Tabla 7-5 Reglas de protección

Parámetro	Descripción
Rule ID	El ID de regla de protección, que se genera automáticamente.
Rule Description	Detalles de los ataques para los que está configurada la regla de protección.
CVE ID	ID de vulnerabilidades y exposiciones comunes (CVE), que corresponde a la regla de protección. Para vulnerabilidades que no son CVE, se muestra un guion doble (--).
Risk Severity	La gravedad de la vulnerabilidad, incluyendo: ● High ● Medium ● Low
Application Type	El tipo de aplicaciones a las que se aplica la regla de protección, por ejemplo, WordPress.
Protection Type	El tipo de ataque que la regla de protección está configurada para, por ejemplo, inyecciones de comandos.

----Fin

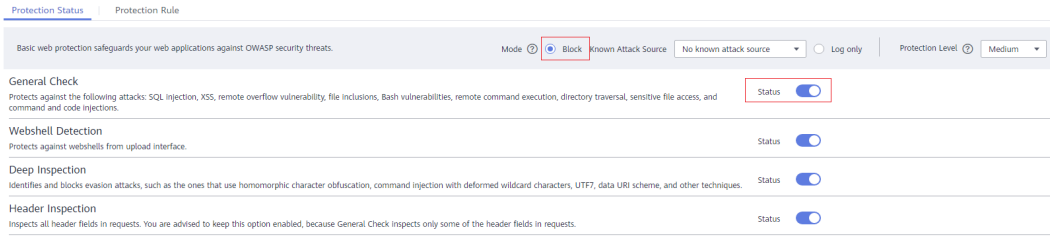
Ejemplo - Bloqueo de Ataques de Inyección SQL

Si el nombre de dominio **www.example.com** se ha conectado a WAF, realice los siguientes pasos para verificar que WAF pueda bloquear ataques de inyección SQL.

Paso 1 Habilite **General Check** en **Basic Web Protection** y establezca el modo de protección en **Block**.

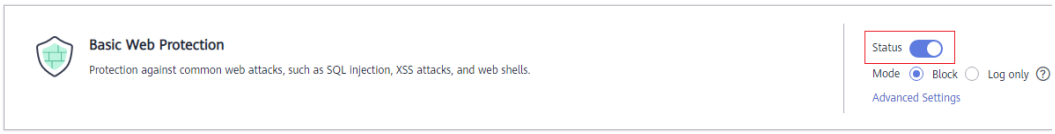
 Copyright © Huawei Technologies Co., Ltd.

Figura 7-6 Habilitación de la comprobación general



Paso 2 Habilite la protección web básica WAF.

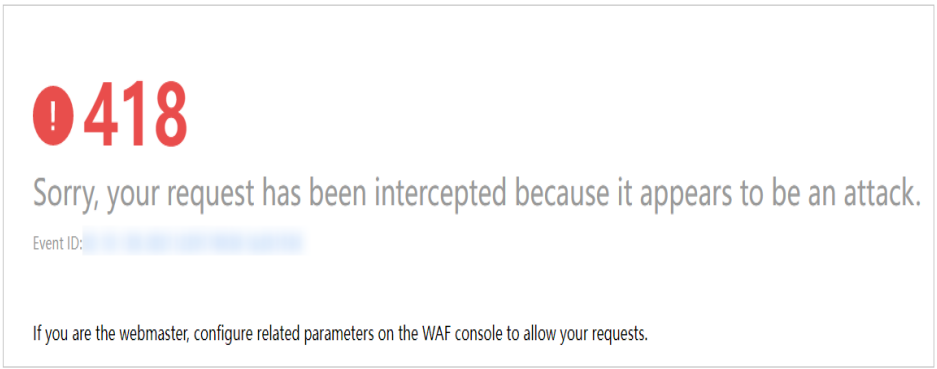
Figura 7-7 Habilitación de la protección web básica WAF



Paso 3 Borre la caché del navegador e introduzca una inyección SQL simulada (por ejemplo, http://www.example.com?id=' o 1=1) en el cuadro de dirección.

WAF bloquea la solicitud de acceso. **Figura 7-8** muestra una página de bloque de ejemplo.

Figura 7-8 Página de bloqueo



Paso 4 Vaya a la consola WAF. En el panel de navegación de la izquierda, seleccione **Events**. Vea el evento en la página **Events**.

Figura 7-9 Evento de inyección SQL

----Fin

7.3 Configuración del control de acceso inteligente

Si habilita el control de acceso inteligente, WAF utiliza modelos integrados impulsados por IA para analizar el tráfico a su sitio web, identificar ataques de CC y características anormales en las solicitudes HTTP en el servidor de origen, y generar reglas específicas de protección precisa y control de acceso para su sitio web. De esta manera, WAF puede proteger automáticamente su sitio web de ataques de CC.

 Copyright © Huawei Technologies Co., Ltd.

AVISO

La protección de control de acceso inteligente ya está disponible para open beta test (OBT). Para habilitarlo, **envíe un ticket de servicio.**

Prerrequisitos

El sitio web que desea proteger se ha agregado a WAF.

Restricciones

- En **Cloud mode**, solo la edición estándar (anteriormente la edición profesional), la edición profesional (anteriormente la edición empresarial) y la edición platino (anteriormente la edición definitiva) incluyen protección de control de acceso inteligente.
- La protección de control de acceso inteligente solo está disponible en las regiones de norte de China.

Procedimiento

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, seleccione **Website Settings**.

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

Paso 6 En el área de **Intelligent Access Control**, cambie el **Status** si es necesario.

Figura 7-10 Control de acceso inteligente

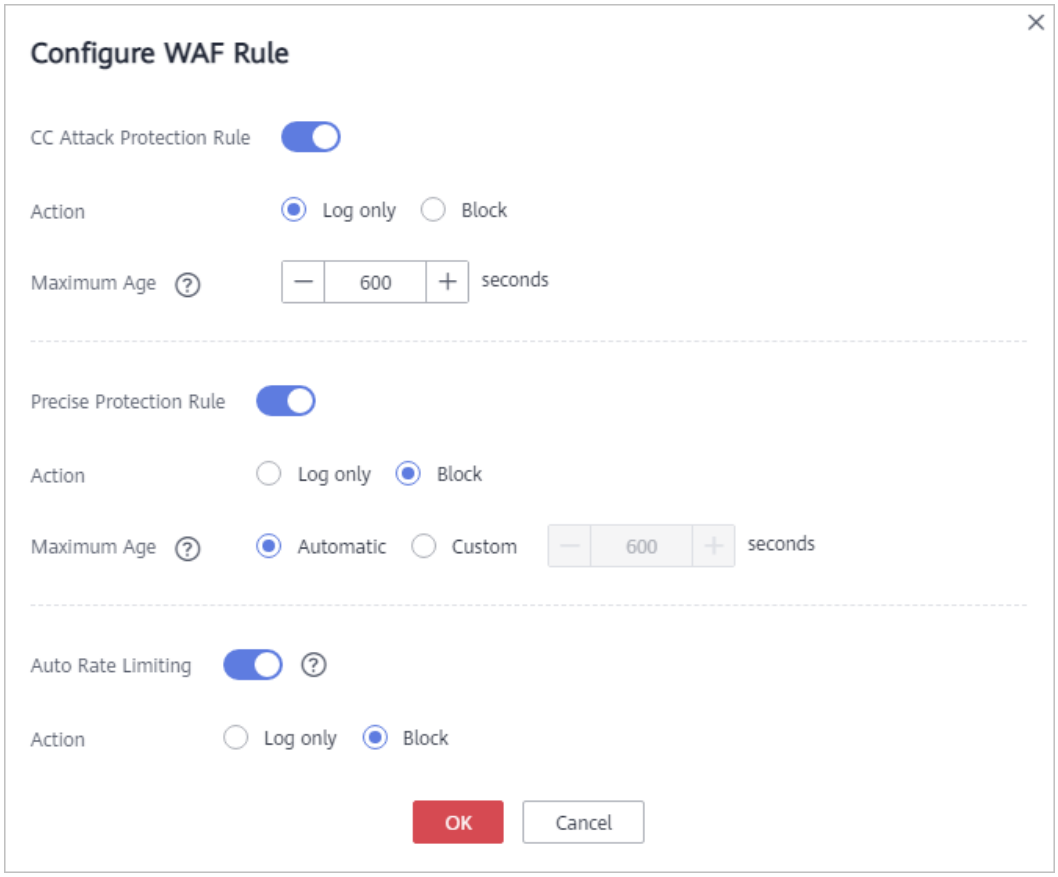
Paso 7 Haga clic en **Configure** para ir al cuadro de diálogo **Configure WAF Rule**.

- **CC Attack Protection Rule**/**Precise Protection Rule**: Configure **Action** and **Maximum Age** para ellos después de habilitarlos.
  - **Action**: Seleccione **Log only** o **Block**.
  - **Maximum Age**: La regla no es válida si WAF no detecta ningún tráfico de ataque de CC dentro de la edad máxima que configure.
- **Auto Rate Limiting**: Después de habilitar **Intelligent Access Control**, WAF tarda entre 10 y 15 minutos en conocer la línea base de tráfico de tu sitio web, determinar los volúmenes máximos de tráfico que puede manejar su sitio web y, a continuación, generar una regla para usted. Por lo tanto, debe habilitar **Auto Rate Limiting** para limitar el tráfico que va a su sitio web durante este tiempo de ventana. De esta manera, WAF puede proteger sus servidores de origen de ataques DDoS antes de que la protección de control

 Copyright © Huawei Technologies Co., Ltd.

de acceso inteligente entre en vigor. Después de que WAF genere reglas de control de acceso inteligente específicas para su sitio web, **Auto Rate Limiting Rate** no es válida automáticamente.

Figura 7-11 Configurar regla WAF



Paso 8 Haga clic en **OK**.

Haga clic en **View WAF Rule** para ver las políticas de protección generadas automáticamente por WAF después de detectar ataques de CC.

----Fin

7.4 Configuración de una regla de protección contra ataques de CC

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 que las reglas de protección contra ataques CC personalizadas entren en vigor, asegúrese de que ha habilitado la protección contra ataques CC (**Status** para **CC Attack Protection** debe ser).

 Copyright © Huawei Technologies Co., Ltd.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

- Solo se puede configurar una regla de protección contra ataques CC para la misma ruta. De lo contrario, las reglas de protección contra ataques de CC pueden entrar en conflicto entre sí y no surten efecto. Si ha configurado varias reglas de protección de CC para la misma ruta, elimine las innecesarias.
- Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.
- Se puede agregar una tabla de referencia a una regla de protección contra ataques de CC. La tabla de referencia tiene efecto para todos los nombres de dominio protegidos.
- La protección contra ataques CC ofrece diferentes acciones de protección para las reglas de protección contra ataques CC, incluyendo **Verification code**, **Block**. Por ejemplo, puede configurar una regla de protección contra ataques CC para bloquear las solicitudes de una visita durante 600 segundos identificando su cookie (campo de nombre) si el visitante accedió a una URL (por ejemplo, /admin*) de su sitio web más de 10 veces en 60 segundos.
- El modo avanzado no es compatible con Edición estándar (anteriormente edición profesional).
- La administración de tablas de referencia no es compatible con Edición estándar (anteriormente edición profesional)
- La ruta de acceso de una regla de protección contra ataques de CC debe establecerse en una URL (excluyendo el nombre de dominio). Este parámetro permite la coincidencia de prefijos y la coincidencia exacta.
  - Coincidencia de prefijo: Una ruta que termina con * indica que la ruta se utiliza como prefijo. El * se puede utilizar como un valor de carácter comodín. Por ejemplo, para proteger **/admin/test.php** or **/adminabc**, puede establecer **Path** en **/admin***.
  - Coincidencia exacta: la ruta que se va a introducir debe ser la misma que la ruta que se va a proteger. Por ejemplo, para proteger **/admin**, entonces **Path** debe establcerse en **/admin**.
- Si su sitio web está conectado tanto a WAF como a Content Delivery Network (CDN) y la **Protective Action** está establecida en **Verification code** en la regla de protección contra ataques CC, tenga en cuenta que:
  - **Path** debe establecerse en una página dinámica.
  - Si configura una página estática para **Path**, CDN almacenará en caché la página estática. Como resultado, la verificación falla. Manejar el problema refiriéndose a

 Copyright © Huawei Technologies Co., Ltd.

¿Por qué no se actualiza el código de verificación después de activar el código de verificación en una regla de protección contra ataques CC?

Procedimiento

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.

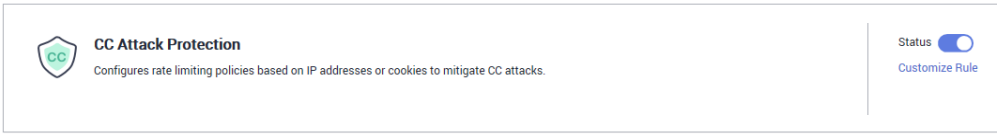
Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 In the navigation pane, choose **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 **CC Attack Protection**, cambie **Status** si es necesario y haga clic en **Customize Rule** para ir a la página **CC Attack Protection**.

Figura 7-12 Área de configuración de CC Attack Protection



Paso 7 En la esquina superior izquierda de la página **CC Attack Protection**, haga clic en **Add Rule**.

Paso 8 En el cuadro de diálogo que se muestra, configure una regla de protección contra ataques CC haciendo referencia a **Tabla 7-6**.

Si un visitante cuya cookie es **name** accede a una página de su sitio web donde la dirección incluye **/admin** al final (por ejemplo, https://www.example.com/adminlogic) más de 10 veces en 60 segundos, WAF bloquea las solicitudes de los visitantes del mismo **name** de cookie durante 600s y devuelve la página configurada para el **Page Content**. **Figura 7-13** muestra las configuraciones.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-13 Adición de una regla de protección contra ataques de CC

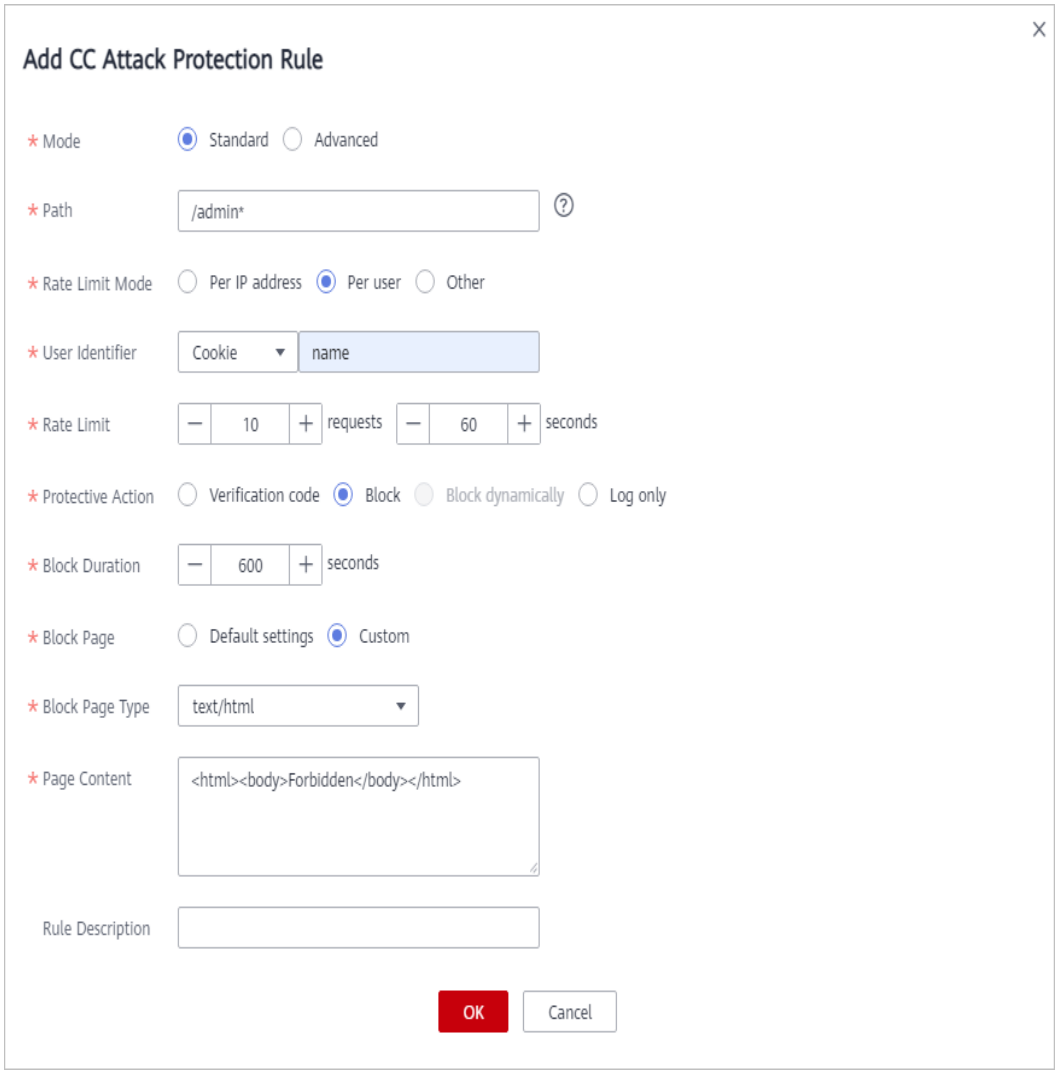


Tabla 7-6 Parámetros de regla

Parámetro	Descripción	Valor de ejemplo
Mode	● **Standard**: Solo se puede restringir la ruta de protección de un nombre de dominio. ● **Advanced**: La ruta, la dirección IP, la cookie, el encabezado y los campos de parámetros pueden restringirse. Este parámetro no está disponible en la edición estándar (anteriormente edición profesional).	**Standard**

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Path	Establezca este parámetro sólo cuando se seleccione **Standard** para **Mode**. Parte de la URL sin el nombre de dominio. ● Coincidencia de prefijo: Una ruta que termina con * indica que la ruta se utiliza como prefijo. El * se puede utilizar como un valor de carácter comodín. Por ejemplo, para proteger **/admin/test.php** or **/adminabc**, puede establecer **Path** en **/admin***. ● Coincidencia exacta: la ruta que se va a introducir debe ser la misma que la ruta que se va a proteger. Por ejemplo, para proteger **/admin**, entonces **Path** debe establcerse en **/admin**. **NOTA** ● La ruta solo admite coincidencias exactas y prefijos, pero no admite expresiones regulares. ● La ruta de acceso no puede contener dos o más barras diagonales consecutivas. Por ejemplo, ///**admin**. Si introduce ///**admin**, WAF convertirá /// en /. ● La ruta distingue entre mayúsculas y minúsculas. ● Si **Path** está establecido en /, todas las rutas del sitio web están protegidas.	**/admin***

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Condition List	Establezca este parámetro solo cuando esté seleccionado **Advanced** para **Mode**. Haga clic en **Add** para agregar condiciones. Se requiere al menos una condición, pero se permiten hasta 30 condiciones. Si agrega más de una condición, la regla sólo tendrá efecto si se cumplen todas las condiciones. ● **Field**: Las opciones son Path, **Path**, **IP**, **Cookie**, **Header**, y **Params** ● **Subfield**: configura este campo solo cuando se selecciona **Cookie**, **Header**, or **Params** para **Field**. **AVISO** La longitud de un subcampo no puede exceder de 2048 bytes. Solo se permiten dígitos, letras, guiones bajos (_) y guiones (-). ● **Lógica**: Seleccione una relación lógica de la lista desplegable. **NOTA** Si establece **Logic** en **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, o **Suffix is not any of them**, seleccione una tabla de referencia existente. Para más detalles, consulte **Adición de una tabla de referencia**. ● **Content**: Ingrese o seleccione el contenido que coincida con la condición.	**Path Include /admin**

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Rate Limit Mode	● **Per IP address**: Un visitante del sitio web es identificado por la dirección IP. ● **Per user**: Un visitante del sitio web se identifica por el valor clave de **Cookie** o **Header**. ● **Other**: Un visitante del sitio web se identifica mediante el campo Referer (fuente de solicitud definida por el usuario). **NOTA** Si establece el modo de **Rate Limit Mode** en **Other**, establezca **Content** del **Referer** en una dirección URL completa que contenga el nombre de dominio. El campo **Content** solo admite coincidencia de prefijo y coincidencia exacta, pero no puede contener dos o más barras diagonales consecutivas, por ejemplo, ///**admin**. Si escribe ///**admin**, WAF lo convertirá a /**admin**. Por ejemplo, si **Path** es /**admin**, y no desea que los visitantes accedan a la página desde **www.test.com**, establezca **Content** de **Referer** en **http://www.test.com**.	**Per user**
User Identifier	Este parámetro es obligatorio cuando selecciona **Per user** para **Rate Limit Mode**. ● **Cookie**: Un nombre de campo de cookie. Debe configurar un nombre de variable de atributo en la cookie que pueda identificar de manera única a un visitante web en función de los requisitos de su sitio web. Este campo no admite expresiones regulares. Solo se admiten las coincidencias completas. Por ejemplo, si un sitio web utiliza el campo de **name** en la cookie para identificar de manera única a un visitante del sitio web, seleccione **name**. ● **Header**: Establezca el encabezado HTTP definido por el usuario que desea proteger. Debe configurar el encabezado HTTP que pueda identificar a los visitantes de la web en función de los requisitos de su sitio web.	name
Rate Limit	El número de solicitudes permitidas de un visitante del sitio web en el período límite de tarifas. Si el número de solicitudes excede el límite de velocidad, WAF realiza la acción que configura para **Protective Action**.	**10** solicitudes permitidas en **60** segundos

 Copyright © Huawei Technologies Co., Ltd.

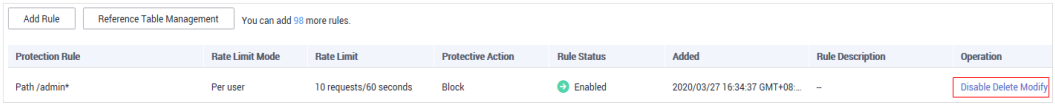
Parámetro	Descripción	Valor de ejemplo
Protective Action	La acción que WAF llevará a cabo si el número de solicitudes excede **Rate Limit** que configuró. Las opciones son las siguientes: ● **Verification code**: WAF permite solicitudes que desencadenan la regla siempre y cuando los visitantes de su sitio web completen la verificación requerida. ● **Block**: WAF bloquea las solicitudes que activan la regla. ● **Block dynamically**: WAF bloquea las solicitudes que activan la regla en función de **Allowable Frequency**, que configura después de que finalice el primer período de límite de velocidad. La acción de protección solo se admite cuando se selecciona **Advanced** para **Mode**. ● **Log only**: WAF solo registra las solicitudes que activan la regla. Puede **descargar datos de eventos** y ver los registros de protección de un nombre de dominio específico.	**Block**
Allowable Frequency	Este parámetro se puede establecer si selecciona **Block dynamically** para **Protective Action**. 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 configure. **Allowable Frequency** no puede ser mayor que **Rate Limit**. **NOTA** Si establece **Allowable Frequency** en **0**, WAF bloquea todas las solicitudes que desencadenan la regla en el siguiente período límite de tasa.	**8** solicitudes permitidas en **60** segundos
Block Duration	Período de tiempo para el que se debe bloquear el elemento cuando se establece **Protective Action** en **Block**.	**600** segundos

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Block Page	La página que se muestra si se ha alcanzado el número máximo de solicitudes. Este parámetro se configura solo cuando **Protective Action** se establece en **Block**. ● Si selecciona **Default settings**, se mostrará la página de bloqueo predeterminada. ● Si selecciona **Custom**, se mostrará un mensaje de error personalizado.	**Custom**
Block Page Type	Si selecciona **Custom** para **Block Page**, seleccione un tipo de página de bloque. Las opciones son: ● **application/jsontext/html** ● **text/htmltext/xml** ● **text/xml**	**text/html**
Page Content	Si selecciona **Custom** para **Block Page**, configure el contenido que se va a devolver.	Los estilos de contenido de página correspondientes a diferentes tipos de página son los siguientes: ● **text/html**: <html><body>Forbidden</body></html> ● **application/json**: {"msg": "Forbidden"} ● **text/xml**: <?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>
Rule Description	Una descripción de la regla. Este parámetro es opcional.	None

Paso 9 Haga clic en **OK**. A continuación, puede ver la regla de protección contra ataques de CC agregada en la lista de reglas de CC.

Figura 7-14 Lista de reglas de CC



- Para deshabilitar una regla, haga clic en **Disable** en la columna **Operation** de la regla. El **Rule Status** predeterminado es **Enabled**.

 Copyright © Huawei Technologies Co., Ltd.

- 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.

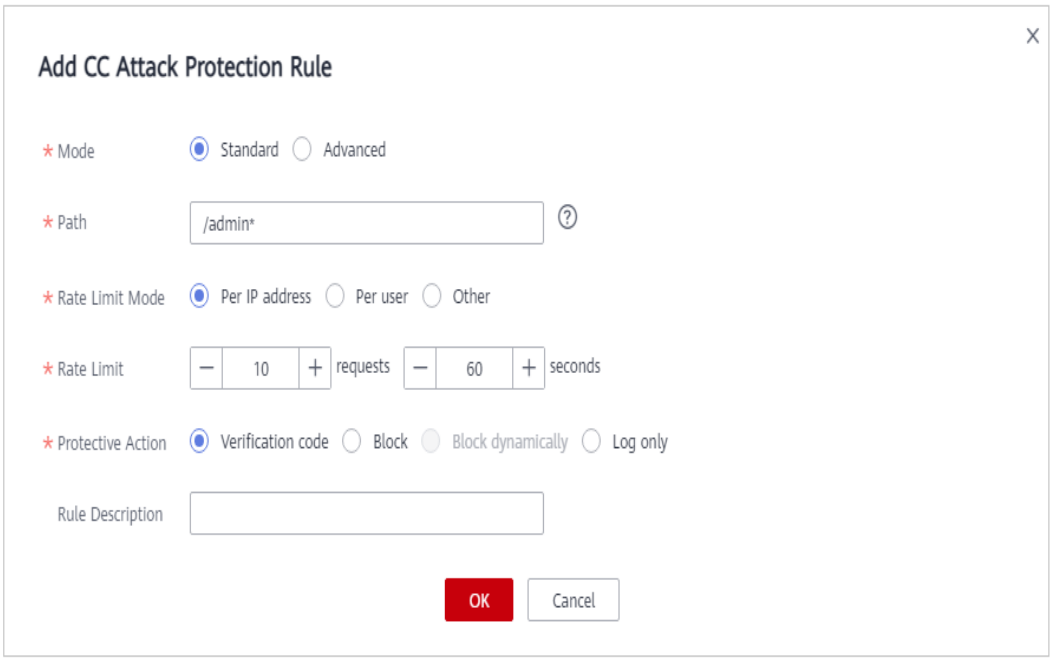
----Fin

Ejemplo de configuración - Código de verificación

Si el nombre de dominio **www.example.com** se ha conectado a WAF, realice los siguientes pasos para verificar que la verificación WAF CAPTCHA esté activada.

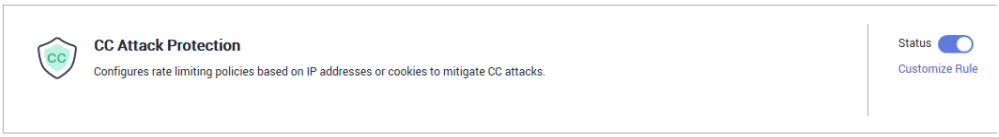
Paso 1 Agregue una regla de protección contra ataques CC con **Protection Action** establecida en **Verification code**.

Figura 7-15 Código de verificación



Paso 2 Habilite la protección contra ataques CC.

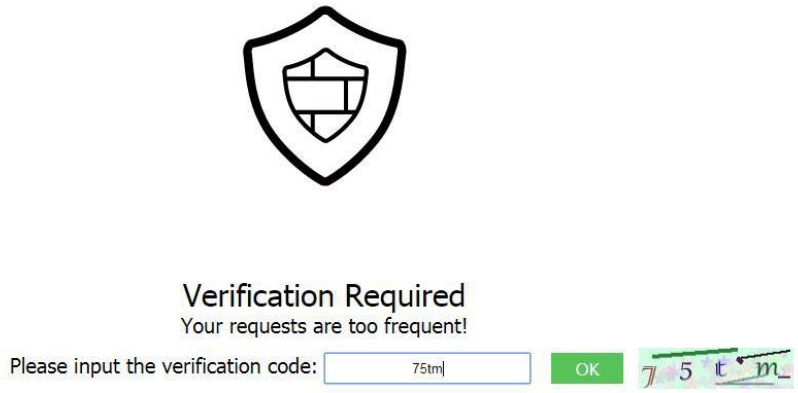
Figura 7-16 Área de configuración de CC Attack Protection



Paso 3 Borrar la caché del navegador y acceder a http://www.example.com/admin/.

Si accede a la página 10 veces en un plazo de 60 segundos, se requiere un código de verificación cuando intenta acceder a la página por undécima vez. Es necesario introducir el código de verificación para continuar con el acceso.

 Copyright © Huawei Technologies Co., Ltd.



Paso 4 Vaya a la consola WAF. En el panel de navegación de la izquierda, seleccione **Events**. Vea el evento en la página **Events**.

Figura 7-17 Consulta de eventos - Código de verificación

----Fin

7.5 Configuración de una regla de protección precisa

WAF le permite personalizar las reglas de protección combinando encabezados HTTP, URL, parámetros de solicitud y direcciones IP de cliente.

Puede combinar campos HTTP comunes, como **IP**, **Path**, **Referer**, **User Agent**, and **Params** en una regla de protección para permitir que WAF permita, bloquee o solo registre las solicitudes que coincidan con las condiciones combinadas.

Se puede añadir una tabla de referencia a una regla de protección precisa. La tabla de referencia tiene efecto para todos los nombres de dominio protegidos.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

- El campo **Response** no se puede configurar en la edición estándar, anteriormente edición profesional.

 Copyright © Huawei Technologies Co., Ltd.

- **Full Detection** no está disponible en la edición estándar WAF (anteriormente edición profesional) y para la nube WAF facturada sobre una base de pago por uso.
- La función de tabla de referencia no está disponible en la edición estándar WAF (anteriormente edición profesional) y en la nube WAF facturado sobre una base de pago por uso.
- Si desea especificar el campo Respuesta, seleccione las siguientes regiones:
  - CN-Hong Kong
  - AP-Bangkok
- Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.
- Si configura **Protective Action** para **Block** para una regla de protección precisa, puede configurar una regla de origen de ataque conocida haciendo referencia a **Configuración de una regla de origen de ataque conocida**. WAF bloqueará las solicitudes que coincidan con la dirección IP, la cookie o los parámetros configurados durante un período de tiempo configurado como parte de la regla.

Escenarios de aplicación

Se utilizan reglas de protección precisas para la protección de fondo anti-leching y gestión de sitios web.

Procedimiento

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.

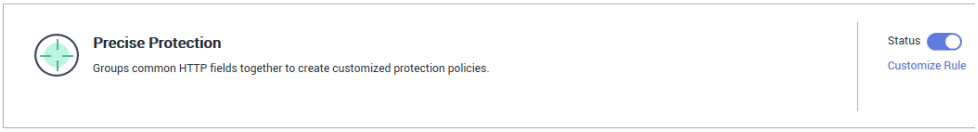
Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 In the navigation pane, choose **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**, cambie el **Status** según sea necesario y haga clic en **Customize Rule** para ir a la página **Precise Protection**.

Figura 7-18 Área de configuración de protección precisa



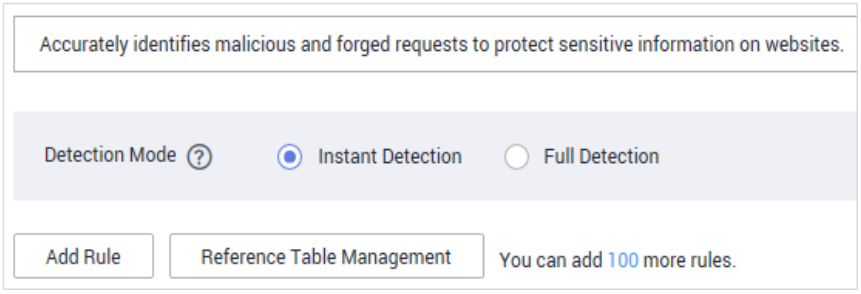
Paso 7 En la página **Precise Protection**, configure **Detection Mode**. **Figura 7-19** muestra un ejemplo.

Two detection modes are available:

 Copyright © Huawei Technologies Co., Ltd.

- **Instant Detection**: si una solicitud coincide con una regla de protección precisa configurada, WAF finaliza inmediatamente la detección de amenazas y bloquea la solicitud.
- **Full Detection**: Si una solicitud coincide con una regla de protección precisa configurada, WAF finaliza su análisis primero y luego bloquea todas las solicitudes que coinciden con la regla de protección precisa configurada.

Figura 7-19 Configuración del modo de detección



Paso 8 Haga clic en **Add Rule**.

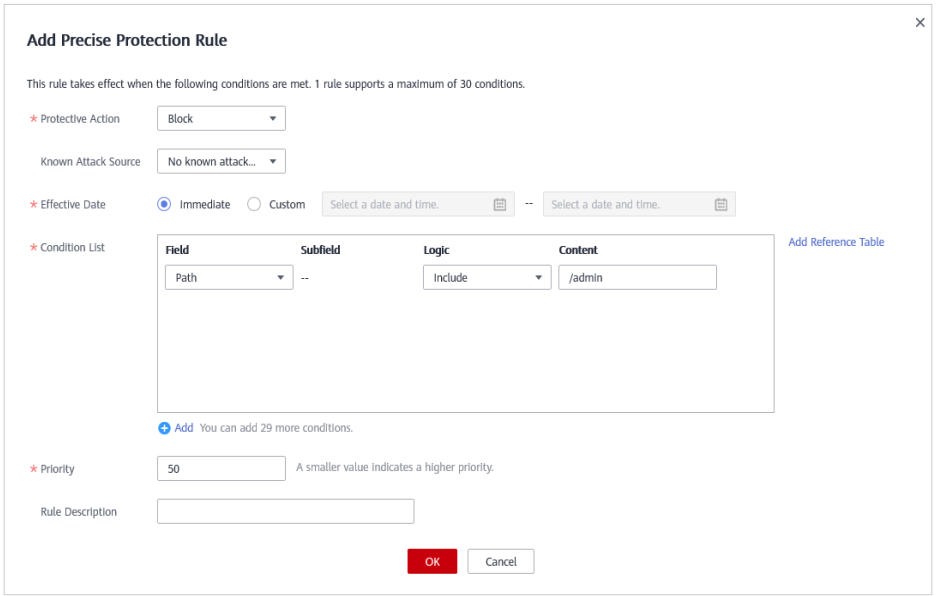
Paso 9 En el cuadro de diálogo que se muestra, agregue una regla haciendo referencia a **Tabla 7-7** y **Ejemplo de Configuración - Bloqueo de Cierto Tipo de Solicitudes de Ataque**.

Los ajustes mostrados en **Figura 7-20** se utilizan como ejemplo. Si un visitante intenta acceder a una URL que contiene **/admin**, WAF bloqueará la solicitud.

AVISO

Para asegurarse de que WAF bloquea solo las solicitudes de ataque, configure primero **Protective Action** a **Log only** para registrar solo y compruebe si las solicitudes normales están bloqueadas en la página **Events**. Si no se bloquean solicitudes normales, configure **Protective Action** para **Block**.

Figura 7-20 Agregar regla de protección precisa



 Copyright © Huawei Technologies Co., Ltd.

Tabla 7-7 Parámetros de regla

Parámetro	Descripción	Valor de ejemplo
Protective Action	Puede seleccionar **Block**, **Allow**, o **Log only**. Valor predeterminado: **Block**	**Block**
Known Attack Source	Si establece **Protective Action** en **Block**, puede seleccionar un tipo de bloqueo para una regla de origen de ataque conocida. A continuación, WAF bloquea las solicitudes que coinciden con la **IP**, **Cookie**, or **Params** configurados durante un período de tiempo que depende del tipo de bloqueo seleccionado.	**Long-term IP address blocking**
Effective Date	Seleccione **Immediate** para activar la regla inmediatamente, o seleccione **Custom** para configurar cuando desee activar la regla.	**Immediate**

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Condition List	Haga clic en **Add** para agregar condiciones. Es necesario añadir al menos una condición. Puede agregar hasta 30 condiciones a una regla de protección. Si se añade más de una condición, se deben cumplir todas las condiciones para que se aplique la regla. Una condición incluye los siguientes parámetros: Los parámetros para configurar una condición se describen de la siguiente manera: ● **Field** ● **Subfield**: configure este campo solo cuando se seleccione **Params**, **Cookie**, o **Header** para **Field**. **AVISO** La longitud de un subcampo no puede superar los 2,048 de bytes. Solo se permiten dígitos, letras, guiones bajos (_) y guiones (-). ● **Lógica**: Seleccione una relación lógica de la lista desplegable. **NOTA** – Si se selecciona **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, o **Suffix is not any of them**. seleccione una tabla de referencia existente en la lista desplegable de **Content**. Para más detalles, consulte **Adición de una tabla de referencia**. – **Exclude any value**, **Not equal to any value**, **Prefix is not any of them**, y **Suffix is not any of them** indica, respectivamente, que WAF realiza la acción de protección (bloquear, permitir o registrar solamente) cuando el campo en la solicitud de acceso no contiene, no es igual a, o el prefijo o sufijo no es ningún valor establecido en la tabla de referencia. Por ejemplo, supongamos que el campo **Path** está establecido en **Exclude any value** y que se selecciona la tabla de referencia de **test**. Si la *test1*, *test2*, and *test3* se establecen en la tabla de referencia de **test**, WAF realiza la acción de protección cuando la ruta de la solicitud de acceso no contiene la *test1*, *test2*, o *test3*.	● **Path Include /admin** ● **User Agent Prefix is not mozilla/5.0** ● **IP Equal to 192.168.2.3** ● **Cookie key1 Prefix is not jsessionid**

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
	● **Content**: Ingrese o seleccione el contenido de la coincidencia de condiciones. **NOTA** Para obtener más detalles sobre las configuraciones en general, consulte **Tabla 7-8**.	
Priority	Prioridad de la regla. Si ha agregado varias reglas, las reglas se comparan por prioridad. Cuanto menor sea el valor que establezca, mayor será la prioridad. **AVISO** Si varias reglas de control de acceso precisas tienen la misma prioridad, WAF coincide con las reglas en la secuencia de tiempo en que se añaden las reglas.	**5**
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	None

Tabla 7-8 Configuraciones de lista de condiciones

Campo	Ejemplo de subcampo	Lógica	Ejemplo de contenido
Path: Parte de una URL que no incluye un nombre de dominio. Este valor solo admite coincidencias exactas. Por ejemplo, si la ruta a proteger es **/admin**, **Path** debe establecerse en **/admin**.	None	Seleccione una relación lógica en la lista desplegable.	**/buy/phone/** **AVISO** Si **Path** está establecido en /, todas las rutas del sitio web están protegidas.
User Agent: Un agente de usuario del escáner que se va a comprobar.	None		**Mozilla/5.0 (Windows NT 6.1)**

 Copyright © Huawei Technologies Co., Ltd.

Campo	Ejemplo de subcampo	Lógica	Ejemplo de contenido
IP: Una dirección IP del visitante para la protección.	None		XXX.XXX.1.1
Params: Un parámetro de solicitud.	**sttl**		**201901150929**
Referer: A user-defined request resource. Por ejemplo, si la ruta protegida es **/admin/xxx** y no desea que los visitantes accedan a la página de **www.test.com**, establezca **Content** en **http://www.test.com**.	None		http://www.test.com
Cookie: Una pequeña porción de datos para identificar a los visitantes de la web.	**name**		jsessionid
Header: Un encabezado HTTP definido por el usuario.	**Accept**		**text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8**
Method: the user-defined request method.	None		**GET**, **POST**, **PUT**, **DELETE**, and **PATCH**
Request Line: Longitud de una línea de solicitud definida por el usuario.	None		**50**

 Copyright © Huawei Technologies Co., Ltd.

Campo	Ejemplo de subcampo	Lógica	Ejemplo de contenido
Request: Longitud de una solicitud definida por el usuario. Incluye el encabezado de la solicitud, la línea de solicitud y el cuerpo de la solicitud.	None		None
Protocol: el protocolo de la solicitud.	None		http
Response Code: Código de estado devuelto a la solicitud.	None	● Equivalente a ● Distinto a ● Igual a cualquier valor ● No igual a cualquier valor	404
Response Length: la duración de la respuesta a la solicitud.	None	● La longitud del subcampo es igual a ● La longitud del subcampo no es igual a ● La longitud del subcampo es superior a ● La longitud del subcampo es inferior a	None
Response Time: tiempo para responder a la solicitud.	None	● La longitud del subcampo es igual a ● La longitud del subcampo no es igual a ● La longitud del subcampo es superior a ● La longitud del subcampo es inferior a	None

 Copyright © Huawei Technologies Co., Ltd.

Campo	Ejemplo de subcampo	Lógica	Ejemplo de contenido
Response Header: encabezado de respuesta.	None	● Incluir ● Excluir ● Equivalente a ● Distinto a	None
Response Body: cuerpo del mensaje de respuesta	None	● Incluir ● Excluir ● Incluir cualquier valor ● Excluir cualquier valor	None

AVISO

Los campos **Response Code**, **Response Length**, **Response Time**, **Response Header**, and **Response Body** solo son compatibles con la edición profesional (anteriormente edición empresarial), edición platino (anteriormente última edición) e instancia WAF dedicada en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok

Paso 10 Haga clic en **OK**. A continuación, puede ver la regla de protección precisa agregada en la lista de reglas de protección.

Figura 7-21 Reglas de protección

- 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

Efecto de protección

Si ha configurado una regla de protección precisa como se muestra en **Figura 7-20** para su nombre de dominio, para verificar que WAF está protegiendo su sitio web (**www.example.com**) contra la regla:

Paso 1 Borre la caché del navegador e introduzca el nombre de dominio en la barra de direcciones para comprobar si el sitio web es accesible.

 Copyright © Huawei Technologies Co., Ltd.

- Si el sitio web es inaccesible, conecte el nombre de dominio del sitio web a WAF siguiendo las instrucciones en **Paso 3: Enrutación del tráfico del sitio web a WAF**.
- Si el sitio web es accesible, vaya a **Paso 2**.

Paso 2 Borre la caché del navegador e introduzca **http://www.example.com/admin** (o cualquier página que contenga **/admin**) en la barra de direcciones. Normalmente, WAF bloquea las solicitudes que cumplen con las condiciones y devuelve la página de bloqueo.

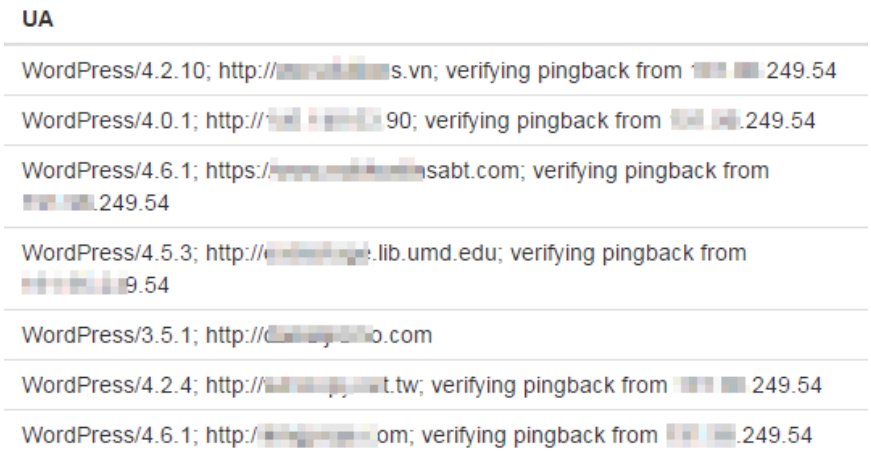
Paso 3 Vuelva a la consola WAF. En el panel de navegación, haga clic en **Events**. En la página mostrada, vea o **descargue datos de eventos**.

----Fin

Ejemplo de Configuración - Bloqueo de Cierto Tipo de Solicitudes de Ataque

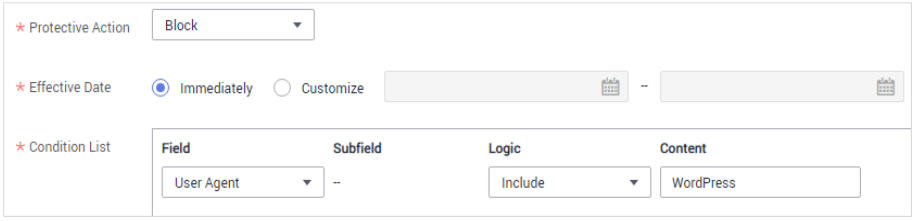
El análisis de un tipo específico de ataque pingback de WordPress muestra que el campo **User Agent** contiene WordPress. Vea **Figura 7-22**.

Figura 7-22 WordPress ataque de pingback



Una regla precisa como se muestra en la figura puede bloquear este tipo de ataque.

Figura 7-23 Configuración del agente de usuario

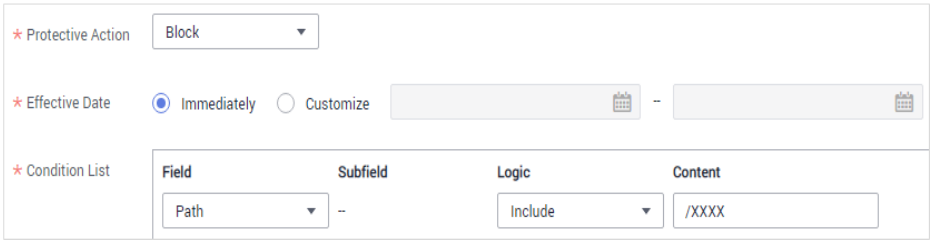


Ejemplo de Configuración - Bloqueo de Solicitudes de Ataque a Cierta URL

Si un gran número de direcciones IP está accediendo a una dirección URL que no existe, configure la siguiente regla de protección para bloquear dichas solicitudes y reducir el uso de recursos en el servidor de origen. **Figura 7-24** muestra la configuración de la regla.

 Copyright © Huawei Technologies Co., Ltd.

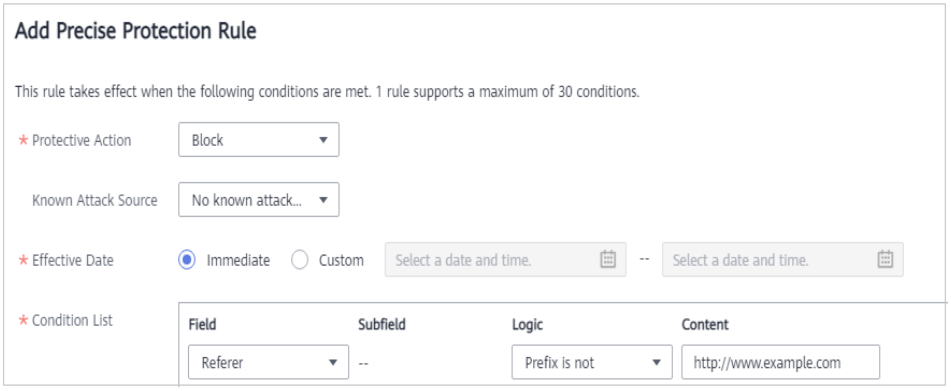
Figura 7-24 Bloquear solicitudes a una URL específica



Ejemplo de configuración: bloqueo de solicitudes con campos nulos

Puede configurar reglas de protección precisas para bloquear un campo nulo. Por ejemplo, para proteger el nombre de dominio www.example.com de solicitudes con Referer vacío, configure una regla como se muestra en **Figura 7-25**.

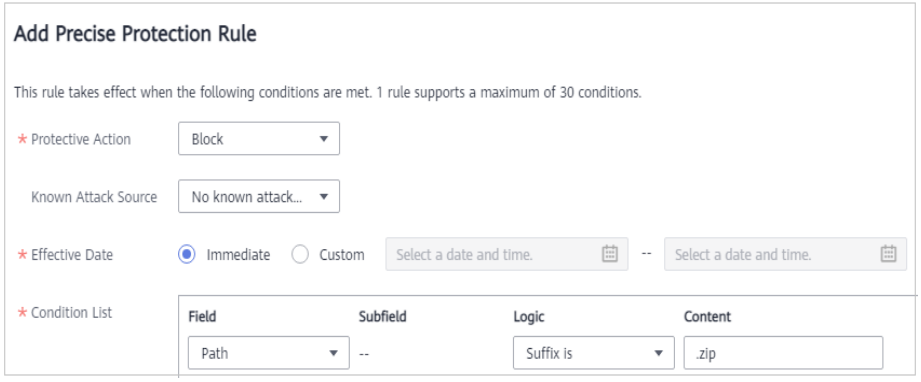
Figura 7-25 Bloquear solicitudes con Referer vacío



Ejemplo de configuración - Bloqueo de tipos de archivo especificados (ZIP, TAR y DOCX)

Puede configurar tipos de archivo que coincidan con el campo de ruta de acceso para bloquear archivos específicos de ciertos tipos. Por ejemplo, si desea bloquear archivos.zip, puede configurar una regla de protección precisa como se muestra en **Figura 7-26** para bloquear las solicitudes de acceso de archivos.zip.

Figura 7-26 Bloqueo de solicitudes de tipos de archivo específicos

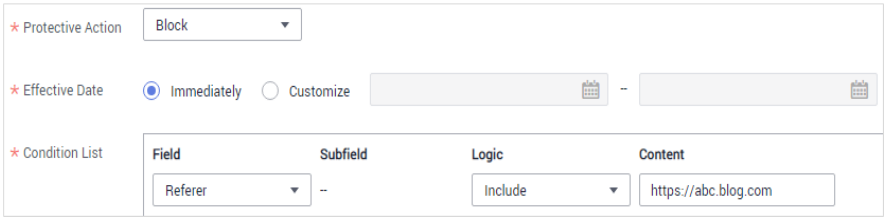


 Copyright © Huawei Technologies Co., Ltd.

Ejemplo de configuración: prevención de enlaces directos

Puede configurar una regla de protección basada en el campo Referente para permitir que WAF bloquee los vínculos directos desde un sitio web específico. Si descubre que, por ejemplo, las solicitudes de **https://abc.blog.com** están robando imágenes de su sitio, puede configurar una regla para bloquear dichas solicitudes.

Figura 7-27 Prevención de enlaces directos



Ejemplo de configuración: permitir que una dirección IP especificada acceda a su sitio web

Puede configurar dos reglas de protección precisas, una para bloquear todas las solicitudes, como se muestra en **Figura 7-28**, pero otra para permitir el acceso desde una dirección IP específica, como se muestra en **Figura 7-29**.

Figura 7-28 Bloqueo de todas las solicitudes

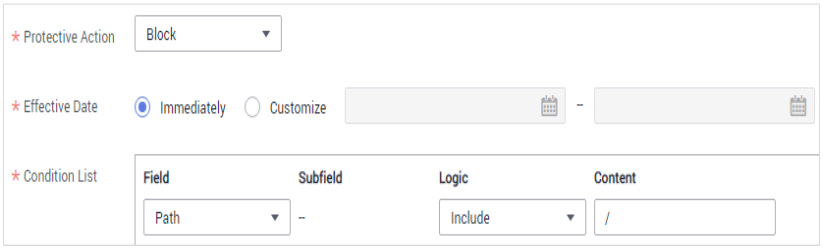
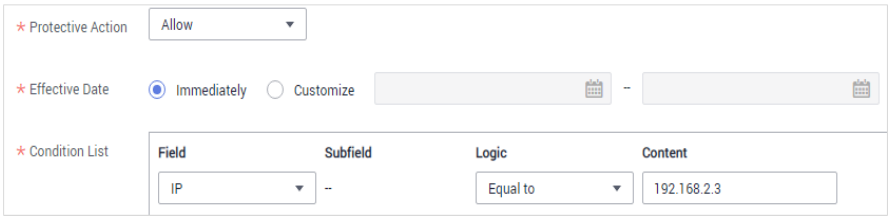


Figura 7-29 Permitir el acceso de una dirección IP especificada

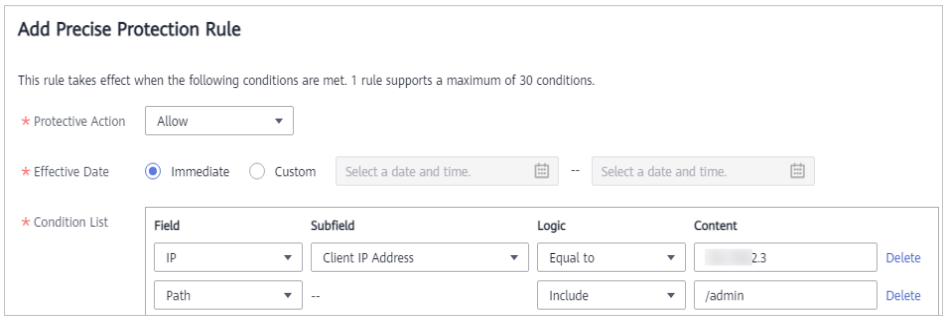


Ejemplo de configuración: permitir que una dirección IP específica acceda a una dirección URL determinada

Puede configurar varias condiciones en el campo **Condition List**. Si una solicitud de acceso cumple las condiciones de la lista, WAF permitirá que la solicitud desde una dirección IP específica acceda a una URL especificada. **Figura 7-30** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-30 Permitir que las direcciones IP específicas accedan a las URL especificadas



7.6 Adición de una tabla de referencia

En este tema se describe cómo crear una tabla de referencia para configurar por lotes métricas de protección de un solo tipo, como **Path**, **User Agent**, **IP**, **Params**, **Cookie**, **Referer**, y **Header**. Las reglas de protección contra ataques CC y las reglas de protección precisas pueden hacer referencia a una tabla de referencia.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

Esta función no está disponible en la edición profesionaledición estándar (anteriormente edición profesional)

Escenarios de aplicación

Puede utilizar una tabla de referencia cuando configure campos de protección en lotes para reglas de protección contra ataques de CC y reglas de protección de acceso precisas.

Procedimiento

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**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 4 In the navigation pane, choose **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 **CC Attack Protection** o **Precise Protection**, haga clic en **Customize Rule**.

Paso 7 Haga clic en **Reference Table Management** en la esquina superior izquierda de la lista.

Paso 8 En la página **Reference Table Management**, haga clic en **Add Reference Table**.

Paso 9 En el cuadro de diálogo **Add Reference Table**, especifique los parámetros haciendo referencia a **Tabla 7-9**.

Figura 7-31 Adición de una tabla de referencia

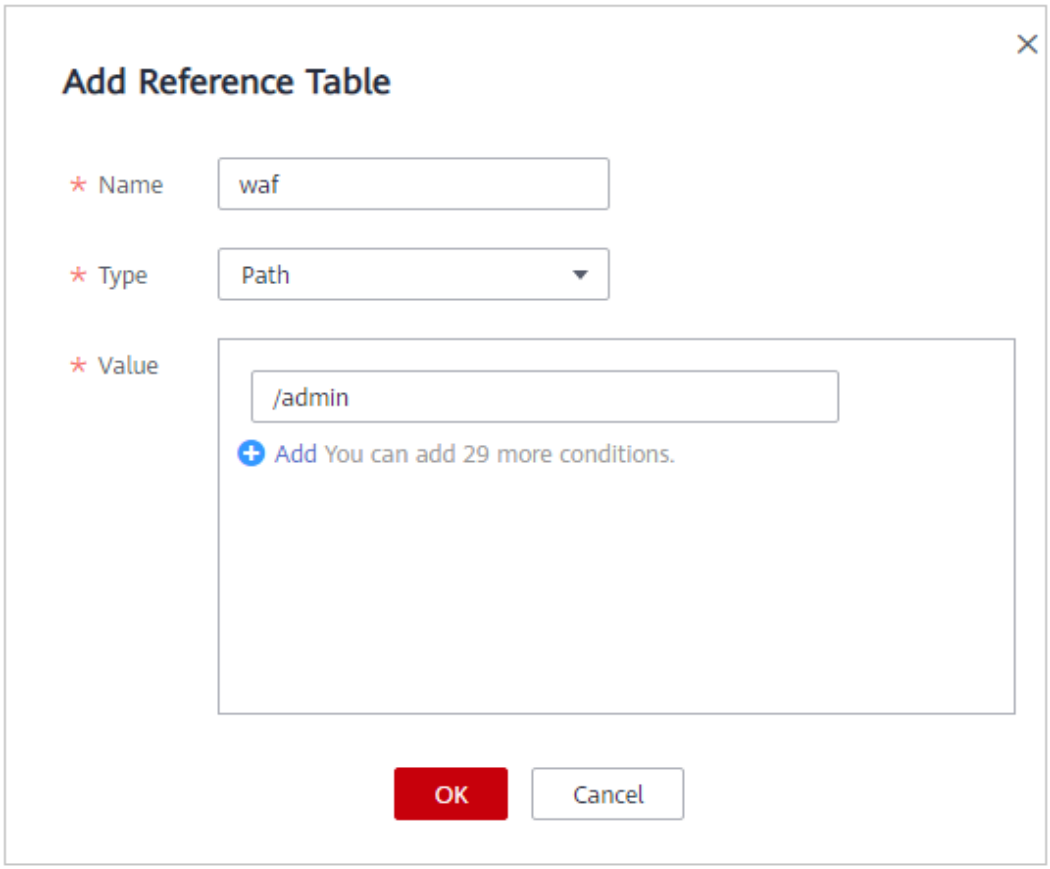


Tabla 7-9 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Name	Nombre de tabla que ha introducido	test

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Type	● **Path**: URL que se va a proteger, excluyendo un nombre de dominio ● **User Agent**: Un agente de usuario del escáner que se va a proteger ● **IP**: Una dirección IP del visitante a proteger. ● **Params**: Un parámetro de petición que se va a proteger ● **Cookie**: Una pequeña porción de datos para identificar a los visitantes de la web ● **Referer**: Un recurso de solicitud definido por el usuario Por ejemplo, si la ruta protegida es **/admin/xxx** y no desea que los visitantes puedan acceder a ella desde *www.test.com*, establezca **Value** en **http://www.test.com**. ● **Header**: Un encabezado HTTP definido por el usuario	**Path**
Value	Valor del tipo correspondiente.**Type**. No se permiten carácteres comodines. **NOTA** Haga clic en **Add** para agregar más de un valor.	**/buy/phone/**

Paso 10 Haga clic en **OK**. A continuación, puede ver la tabla de referencia agregada en la lista de tablas de referencia.

----Fin

Otras operaciones

- Para modificar una tabla de referencia, haga clic en **Modify** en la fila que contiene la tabla de referencia.
- Para eliminar una tabla de referencia, haga clic en **Delete** en la fila que contiene la tabla de referencia.

 Copyright © Huawei Technologies Co., Ltd.

7.7 Configuración de una lista negra o una regla de lista blanca de direcciones IP

De forma predeterminada, todas las direcciones IP pueden acceder a su sitio web. Puede configurar reglas de listas negras y blancas para bloquear, registrar únicamente o permitir solicitudes de acceso desde direcciones IP o intervalos de direcciones IP específicos. Puede agregar una sola dirección IP o importar un grupo de direcciones IP a la lista negra o blanca.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

- WAF admite la importación por lotes de listas negras y listas blancas de direcciones IP. Puede utilizar grupos de direcciones para agregar varias direcciones IP/intervalos rápidamente a una regla de lista negra o blanca. Para más detalles, consulte **Agregar un grupo de direcciones IP**.
- Si los balanceadores de carga ELB utilizados para las instancias de WAF dedicadas o de equilibrio de carga admiten direcciones IPv6, esas instancias de WAF también pueden admitir direcciones IPv6 o intervalos de direcciones IPv6.
- Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.
- La dirección 0.0.0.0/0 no se puede agregar a una lista negra o blanca de direcciones IP WAF, y si una lista blanca entra en conflicto con una lista negra, la regla de lista blanca tiene prioridad. Si desea permitir solo una dirección IP específica dentro de un rango de direcciones bloqueadas, agregue una regla de lista negra para bloquear el rango y luego agregue una regla de lista blanca para permitir la dirección individual que desea permitir.

  AVISO

  Si desea permitir que solo las direcciones IP especificadas accedan al sitio web protegido, consulte **¿Cómo permito que solo las direcciones IP especificadas accedan al sitio web protegido?**

- Si configura **Protective Action** para **Block** para una regla de lista negra o lista blanca, puede configurar una regla de origen de ataque conocida haciendo referencia a **Configuración de una regla de origen de ataque conocida**. WAF bloqueará las

 Copyright © Huawei Technologies Co., Ltd.

solicitudes que coincidan con la dirección IP, la cookie o los parámetros configurados durante un período de tiempo configurado como parte de la regla.

Impacto en el sistema

Si se agrega una dirección IP a una lista negra o blanca, WAF bloquea o permite solicitudes desde esa dirección IP sin verificar si las solicitudes son maliciosas.

Procedimiento

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.

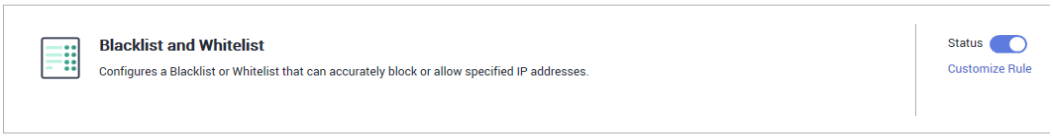
Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 In the navigation pane, choose **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 **Blacklist and Whitelist**, cambie **Status** según sea necesario y haga clic en **Customize Rule**.

Figura 7-32 Área de configuración de listas negras y blancas



Paso 7 En la esquina superior izquierda de la página **Blacklist and Whitelist**, haga clic en **Add Rule**.

Paso 8 En el cuadro de diálogo que se muestra, especifique los parámetros haciendo referencia a **Tabla 7-10**. **Figura 7-33** y **Figura 7-34** mostrar dos ejemplos.

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.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-33 Adición de una dirección IP/Rango a una regla de lista negra o blanca

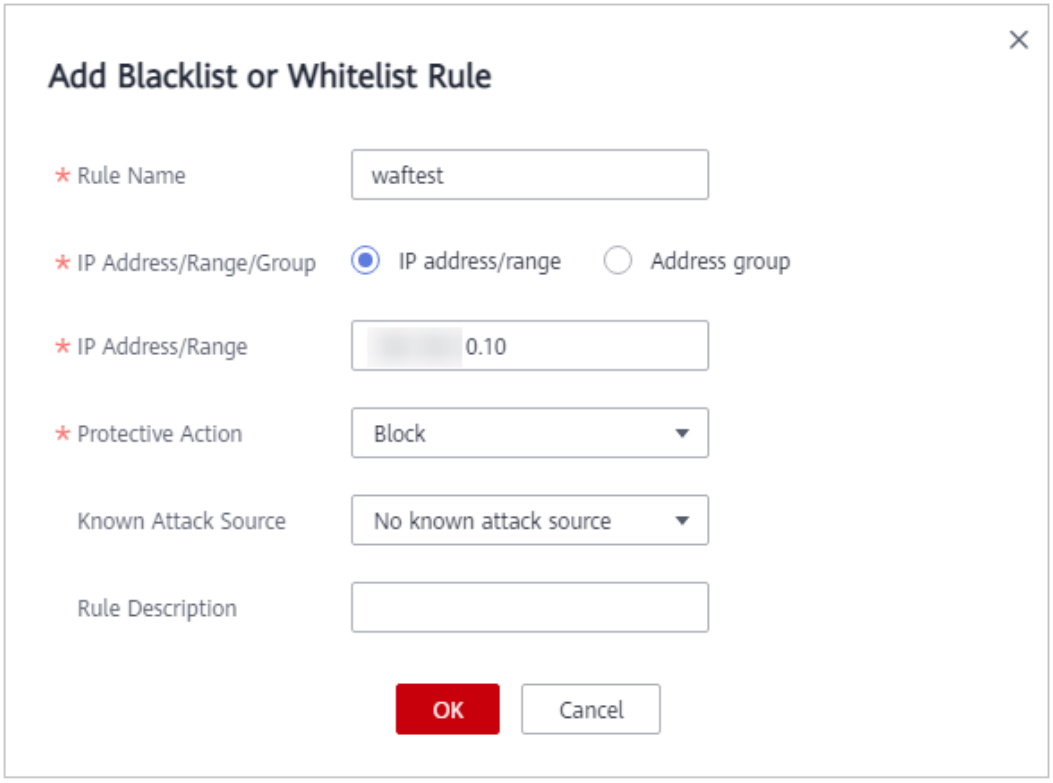
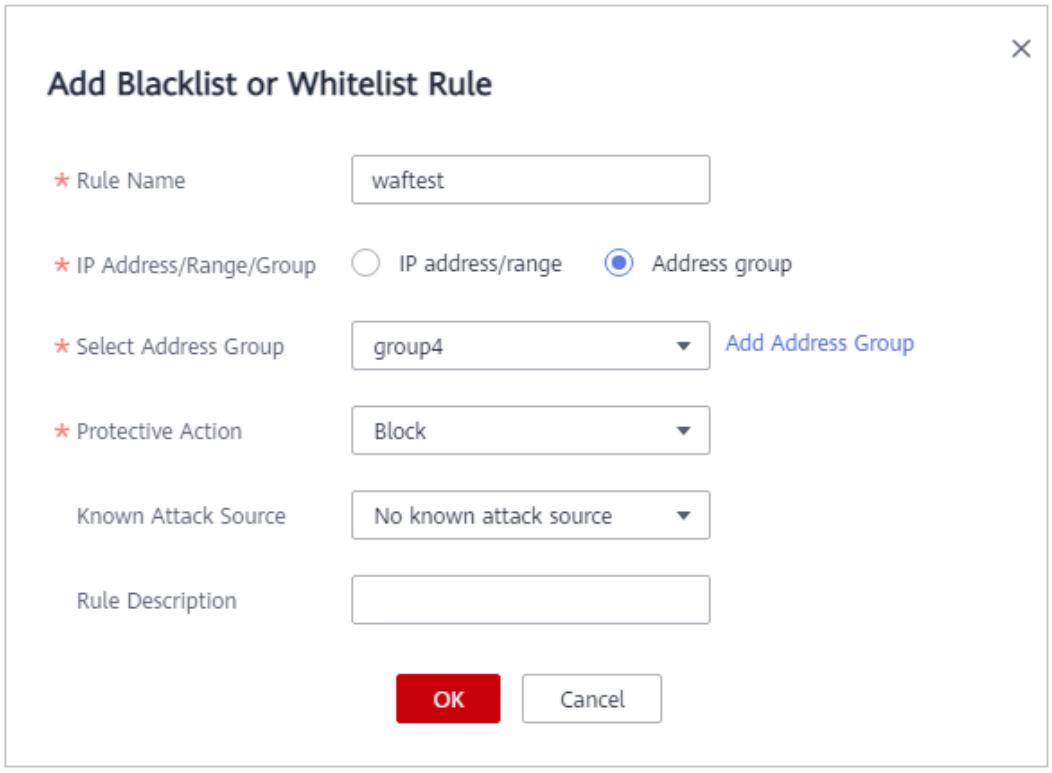


Figura 7-34 Adición de direcciones IP/Rangos a una regla de lista negra o blanca



 Copyright © Huawei Technologies Co., Ltd.

Tabla 7-10 Parámetros de regla

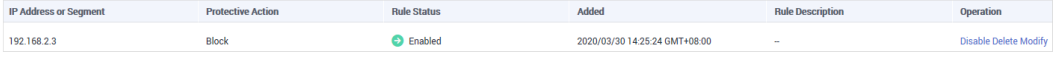
Parámetro	Descripción	Valor de ejemplo
Rule Name	Nombre de regla que ha introducido.	waftest
IP Address/ Range/Group	Puede seleccionar **IP address/ Range** o **Address Group** para agregar direcciones IP a una lista negra o una regla de lista blanca.	Dirección IP/Rango
IP Address/ Range	Este parámetro es obligatorio si selecciona **IP address/range** para **IP Address/Range/ Group**. IP addresses or IP address ranges are supported. ● Dirección IP: dirección IP que se agregará a la lista negra o blanca ● Rango de direcciones IP: dirección IP y máscara de subred que definen un segmento de red	XXX.XXX.2.3
Select Address Group	Este parámetro es obligatorio si selecciona **Address group** para IP **Address/Range/Group**. Seleccione un grupo de direcciones IP en la lista desplegable. También puede hacer clic en **Add Address Group** para crear un grupo de direcciones. Para más detalles, consulte **Agregar un grupo de direcciones IP**.	grupowaf

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Protective Action	● **Block**: seleccione **Block** si desea incluir en la lista negra una dirección IP o un rango de direcciones IP. ● **Allow**: seleccione **Allow** si desea incluir en la lista blanca una dirección IP o un rango de direcciones IP. ● **Log only**: seleccione **Log only** si desea observar una dirección IP o un rango de direcciones IP. A continuación, WAF determina si la dirección IP o el intervalo de direcciones IP están en la lista negra o en la lista blanca en función de **los datos de eventos**.	Block
Known Attack Source	Si selecciona **Block** para **Protective Action**, puede seleccionar un tipo de bloqueo de una regla de origen de ataque conocida. WAF bloqueará las solicitudes que coincidan con la dirección IP, la cookie o los parámetros configurados durante un período de tiempo configurado como parte de la regla.	Bloqueo de direcciones IP a largo plazo
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	None

Paso 9 Haga clic en **OK**. A continuación, puede ver la regla agregada en la lista de reglas de listas negras y listas blancas.

Figura 7-35 Reglas de la lista negra o de la lista blanca



- 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

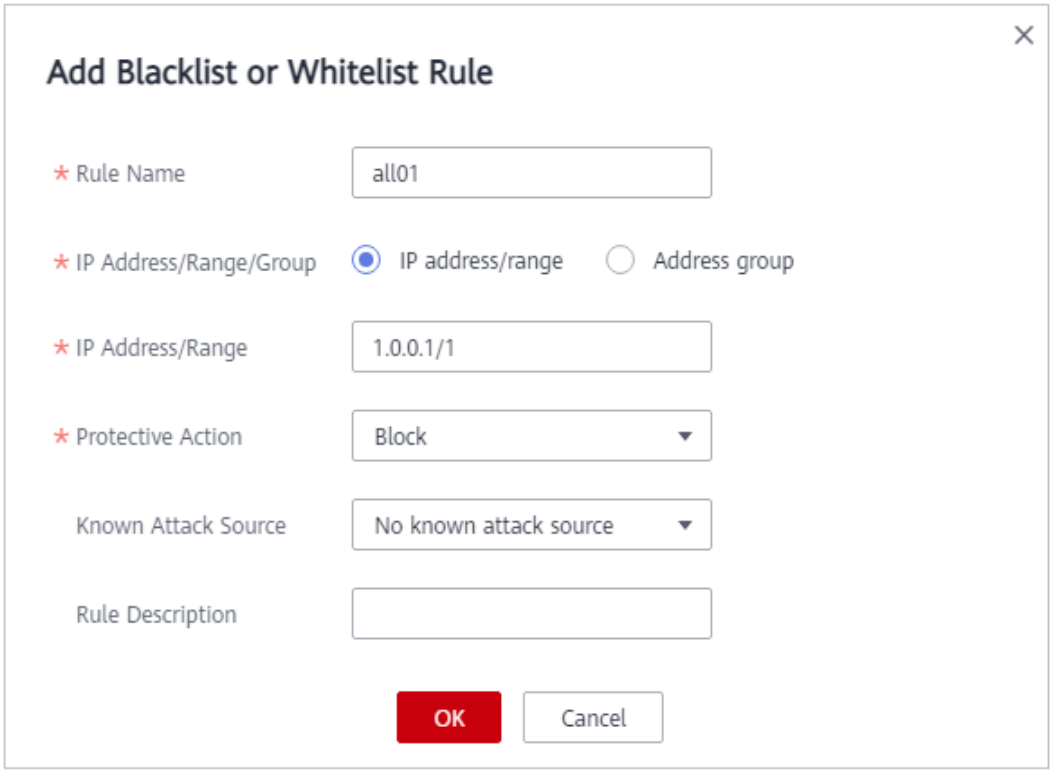
 Copyright © Huawei Technologies Co., Ltd.

Ejemplo de configuración: permitir direcciones IP especificadas

Si el nombre de dominio *www.example.com* se ha conectado a WAF, puede realizar los siguientes pasos para verificar que la regla entre en vigor:

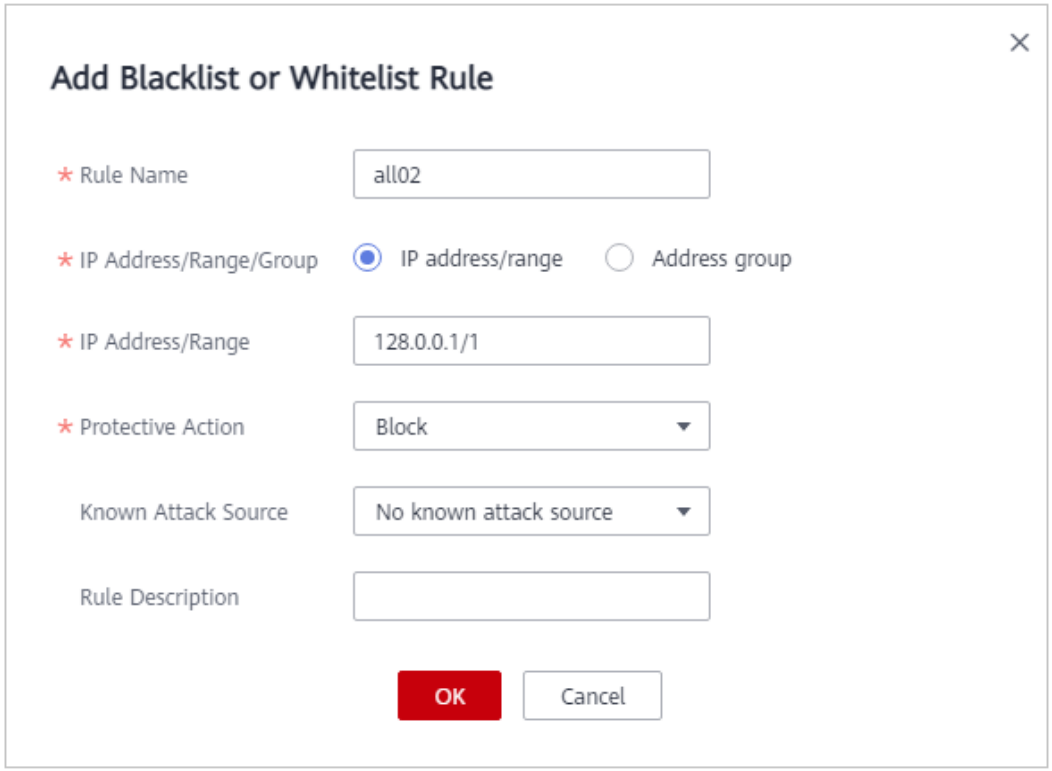
Paso 1 Agregue las siguientes dos reglas de listas negras y blancas para bloquear todas las direcciones IP:

Figura 7-36 Bloqueo de rango de direcciones IP 1.0.0.0/1



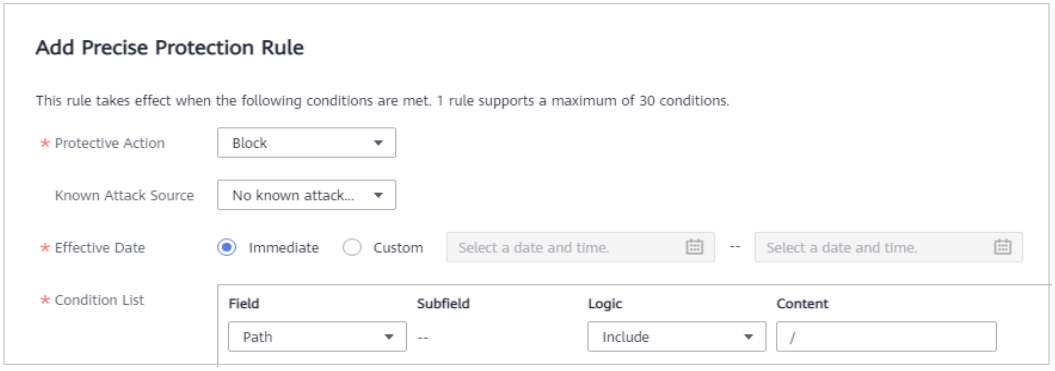
 Copyright © Huawei Technologies Co., Ltd.

Figura 7-37 Intervalo de direcciones IP de bloqueo 128.0.0.0/1



También puede agregar una regla de protección precisa para bloquear todas las solicitudes de acceso, como se muestra en **Figura 7-38**.

Figura 7-38 Bloqueo de todas las solicitudes de acceso

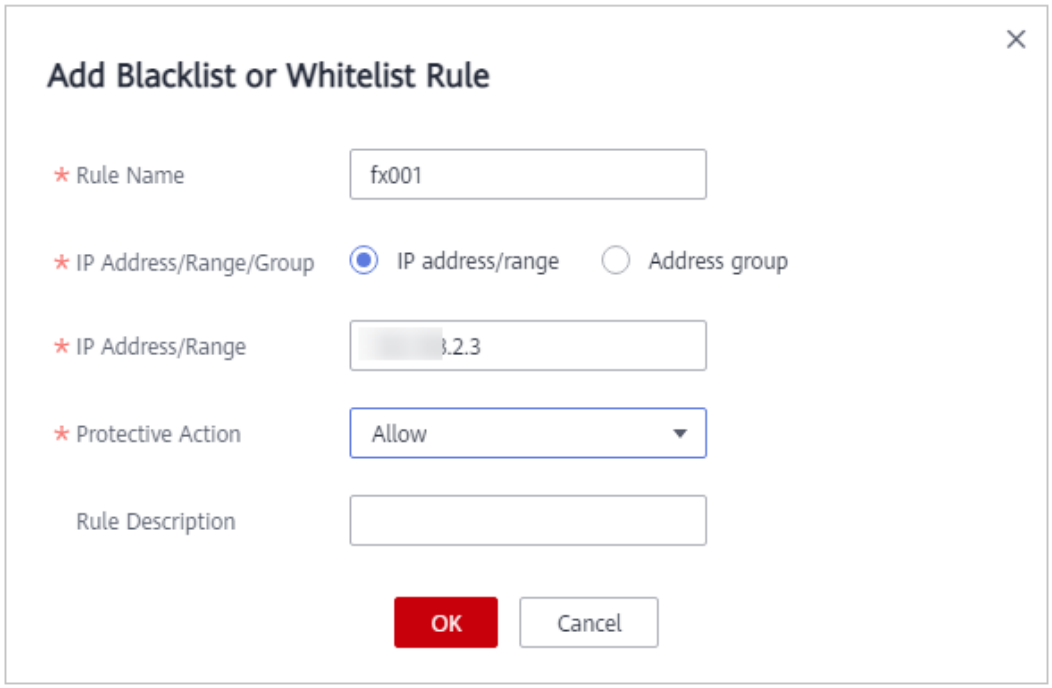


Para más detalles, consulte **Configuración de una regla de protección precisa**.

Paso 2 Consulte **Figura 7-39** y agregue una regla de lista blanca para permitir una dirección IP especificada, por ejemplo, *XXX.XXX.2.3*.

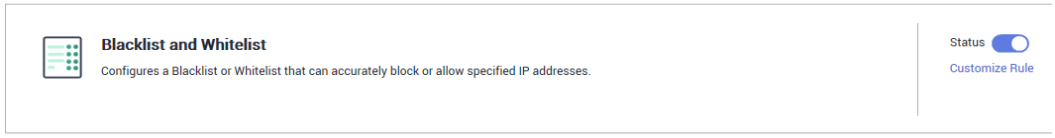
 Copyright © Huawei Technologies Co., Ltd.

Figura 7-39 Permitir el acceso de una dirección IP especificada



Paso 3 Habilite la protección de listas blancas y negras.

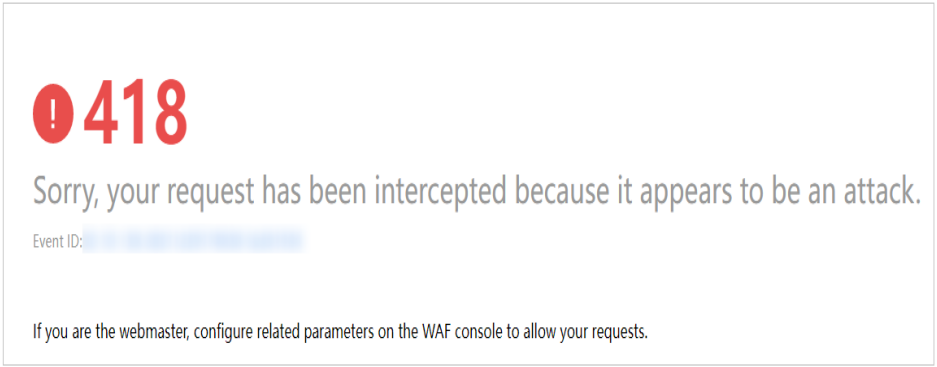
Figura 7-40 Área de configuración de listas negras y blancas



Paso 4 Borrar la caché del navegador y acceder a http://www.example.com.

Si la dirección IP de un visitante no es la especificada en **Paso 2**, WAF bloquea la solicitud de acceso. **Figura 7-41** muestra un ejemplo de la página de bloques.

Figura 7-41 Página de bloqueo



Paso 5 Vaya a la consola WAF. En el panel de navegación de la izquierda, seleccione **Events**. Vea el evento en la página **Events**.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

7.8 Configuración de una regla de origen de ataque conocida

Si WAF bloquea una solicitud maliciosa por dirección IP, Cookie o Params, puede configurar una regla de fuente de ataque conocida para permitir que WAF bloquee automáticamente todas las solicitudes de la fuente de ataque durante una duración de bloqueo establecida en la regla de fuente de ataque conocida. Por ejemplo, si una solicitud maliciosa bloqueada se origina desde una dirección IP (192.168.1.1) y establece la duración de bloqueo en 500 segundos, WAF bloqueará la dirección IP durante 500 segundos después de que la regla de origen de ataque conocida entre en vigor.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

- Para que una regla de origen de ataque conocida entre en vigor, debe habilitarse al configurar reglas de protección web básica, protección precisa, protección de listas negras o de listas blancas.
- Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.
- Antes de agregar una regla de origen de ataque conocida para solicitudes maliciosas bloqueadas por Cookie o Params, se debe configurar un identificador de tráfico para el nombre de dominio correspondiente. Para más detalles, consulte **Configuración de un identificador de tráfico para un Known Attack Source**.

Limitaciones de la especificación

- Puede configurar hasta seis tipos de bloqueo. Cada tipo puede tener una regla de origen de ataque conocida configurada.
- El tiempo máximo que se puede bloquear una dirección IP es de 30 minutos.

Procedimiento

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.

Copyright © Huawei Technologies Co., Ltd.

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

Paso 4 In the navigation pane, choose **Website Settings**.

Paso 5 En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.

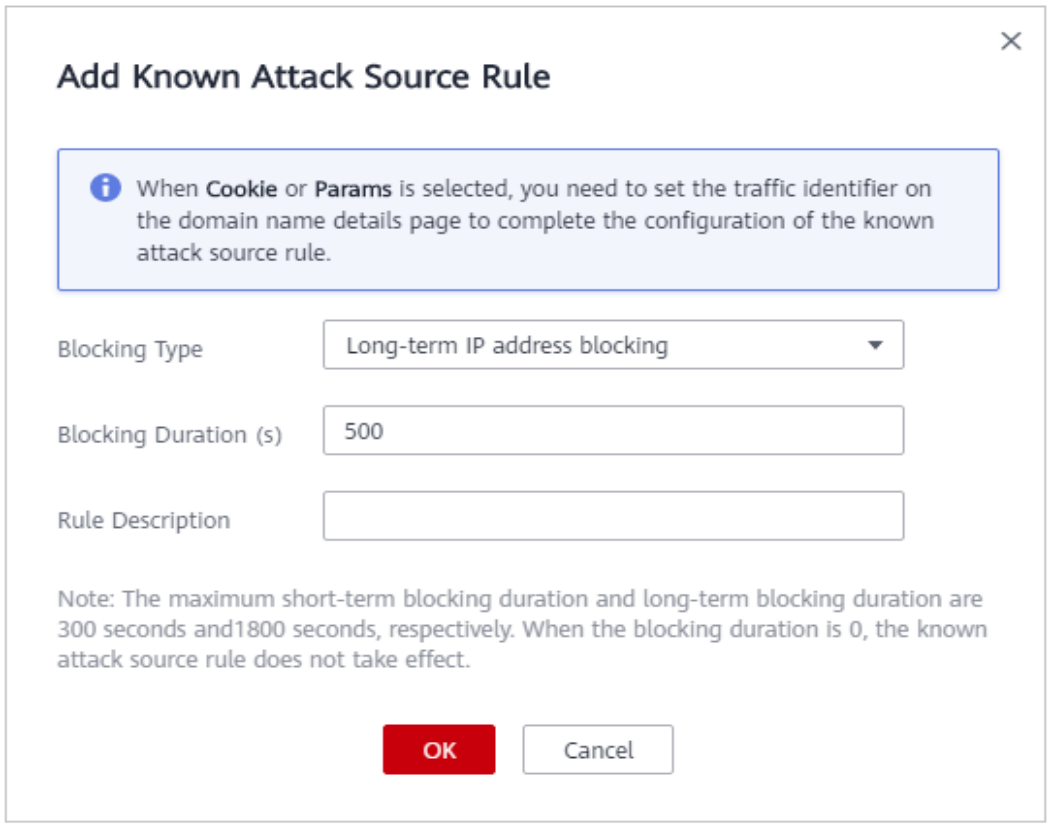
Paso 6 En el área de configuración **Known Attack Source**, cambie **Status** si es necesario y haga clic en **Customize Rule** para ir a la página **Known Attack Source**. Figura 7-42 muestra un ejemplo.

Figura 7-42 Configuración de Known Attack Source

Paso 7 En la esquina superior izquierda de las reglas de origen de ataque conocidas, haga clic en **Add Known Attack Source Rule**.

Paso 8 En el cuadro de diálogo que se muestra, especifique los parámetros haciendo referencia a Tabla 7-11. Figura 7-43 muestra un ejemplo.

Figura 7-43 Agregar regla de origen de ataque conocida



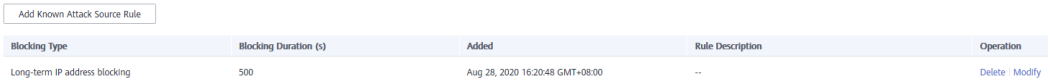
 Copyright © Huawei Technologies Co., Ltd.

Tabla 7-11 Parámetros de origen de ataque conocidos

Parámetro	Descripción	Valor de ejemplo
Blocking Type	Especifica el tipo de bloqueo. Las opciones son: ● **Long-term IP address blocking** ● **Short-term IP address blocking** ● **Long-term Cookie blocking** ● **Short-term Cookie blocking** ● **Long-term Params blocking** ● **Short-term Params blocking**	**Long-term IP address blocking**
Blocking Duration (s)	La duración del bloqueo debe ser un entero y variar desde: ● (300, 1800] para el bloqueo a largo plazo ● (0, 300] para el bloqueo a corto plazo	500
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	None

Paso 9 Haga clic en **OK**. A continuación, puede ver la regla de origen de ataque conocida agregada en la lista.

Figura 7-44 Reglas de Known attack source



----Fin

Otras operaciones

- 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.

Ejemplo de configuración: Bloqueo de Known Attack Source identificada por Cookie

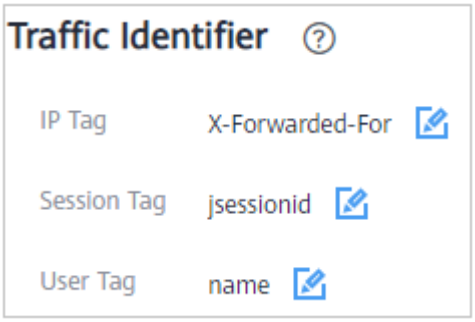
Supongamos que el nombre de dominio *www.example.com* se ha conectado a WAF y que un visitante ha enviado una o más solicitudes maliciosas a través de la dirección IP *XXX.XXX.248.195*. Desea bloquear las solicitudes de acceso desde esta dirección IP y cuya cookie es **jsessionid** durante 10 minutos. Consulte los siguientes pasos para configurar una regla y verificar su efecto.

Paso 1 En la página **Website Settings**, haga clic en *www.example.com* para ir a su página de información básica.

 Copyright © Huawei Technologies Co., Ltd.

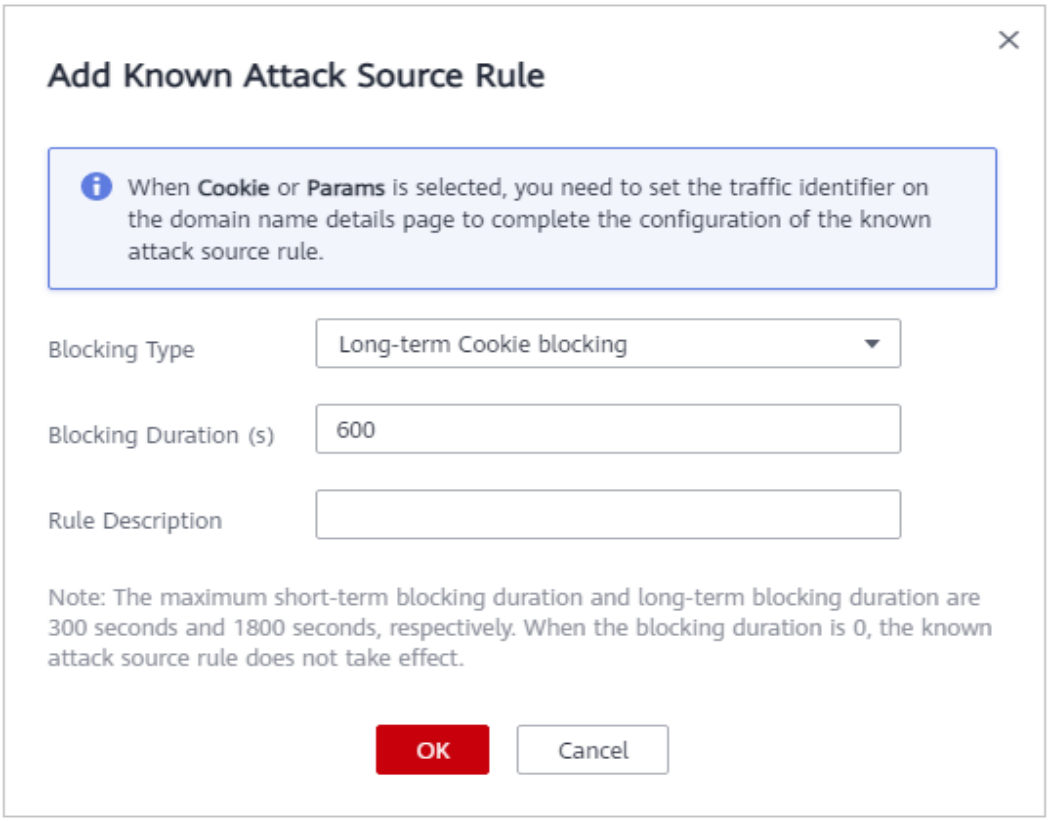
Paso 2 En el área **Traffic Identifier**, configure la cookie en el campo **Session Tag**.

Figura 7-45 Identificador de tráfico



Paso 3 Agrega una fuente de ataque conocida, selecciona **Long-term Cookie blocking** en **Blocking Type** y establece la duración del bloqueo en 600 segundos.

Figura 7-46 Adición de una regla de origen de ataque conocido basada en cookies



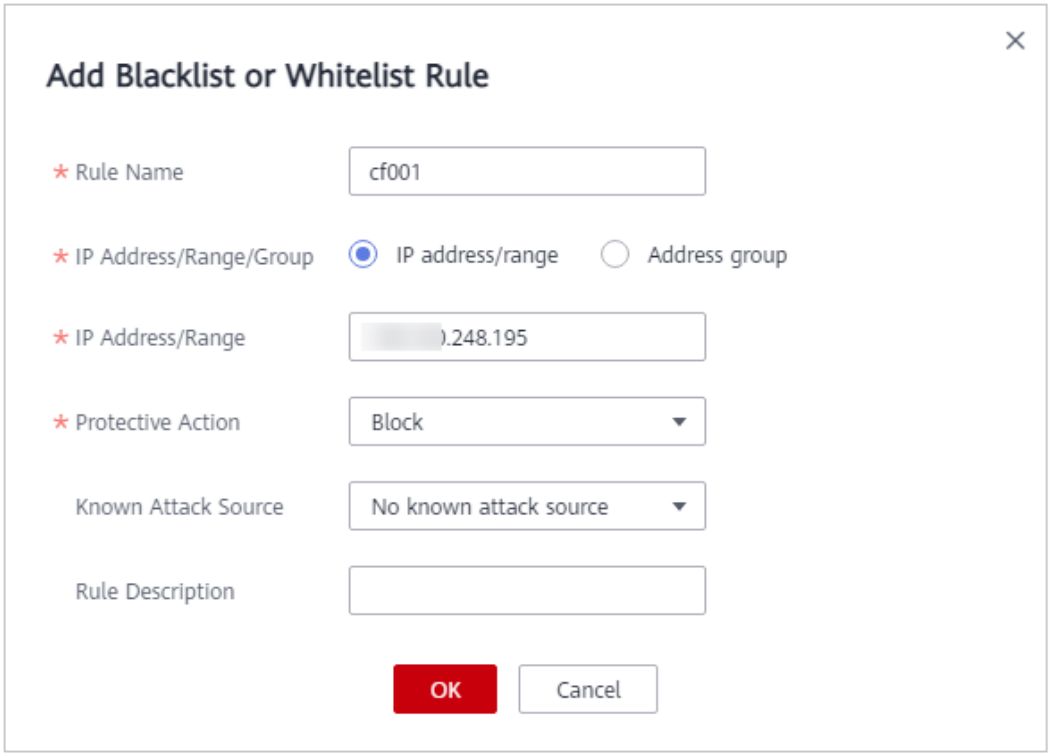
Paso 4 Habilite la protección conocida de la fuente de ataque.

Figura 7-47 Configuración de Known Attack Source

 Copyright © Huawei Technologies Co., Ltd.

Paso 5 Agregue una regla de lista negra y lista blanca para bloquear *XXX.XXX.248.195*. Selecciona **Long-term Cookie blocking** para **Known Attack Source**.

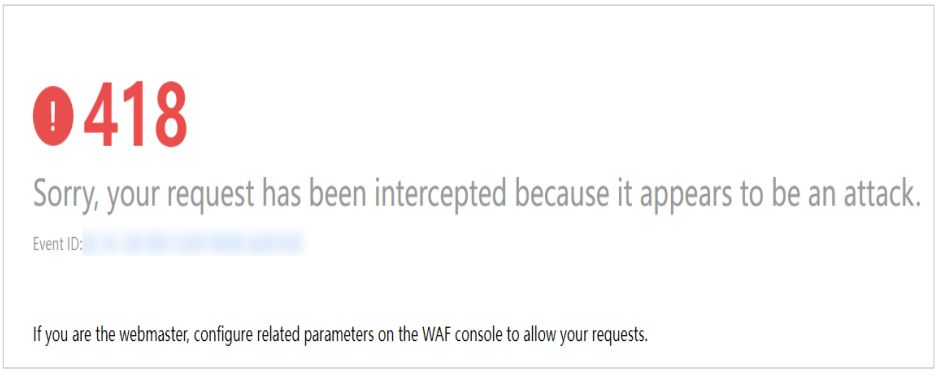
Figura 7-48 Especificación de una regla de origen de ataque conocida



Paso 6 Borrar la caché del navegador y acceder a http://www.example.com.

Cuando una solicitud de la dirección IP *XXX.XXX.248.195*, WAF bloquea el acceso. Cuando WAF detecta que la cookie de la solicitud de acceso desde la dirección IP es **jsessionid**, WAF bloquea la solicitud de acceso durante 10 minutos.

Figura 7-49 Página de bloqueo



Paso 7 Vaya a la consola WAF. En el panel de navegación de la izquierda, seleccione **Events**. Vea el evento en la página **Events**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-50 Consulta de eventos - Eventos de Known Attack Source

----Fin

7.9 Configuración de una regla de control de acceso de geolocalización

En este tema se describe cómo configurar una regla de control de acceso de geolocalización. Una regla de control de acceso de geolocalización le permite controlar las direcciones IP reenviadas desde o hacia países y regiones específicos.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

- Una región se puede configurar en una sola regla de control de acceso de geolocalización. Por ejemplo, si ha bloqueado solicitudes de Shanghái con una regla de control de acceso de geolocalización, Shanghái no se puede agregar a otras reglas de control de acceso de geolocalización.
- Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.

Procedimiento

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**.

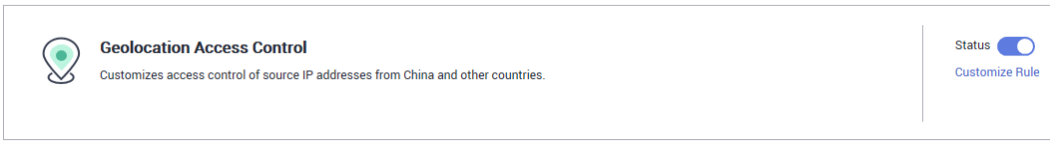
Paso 4 In the navigation pane, choose **Website Settings**.

Paso 5 En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 6 En el área de configuración de **Geolocation Access Control**, cambie **Status** si es necesario y haga clic en **Customize Rule**.

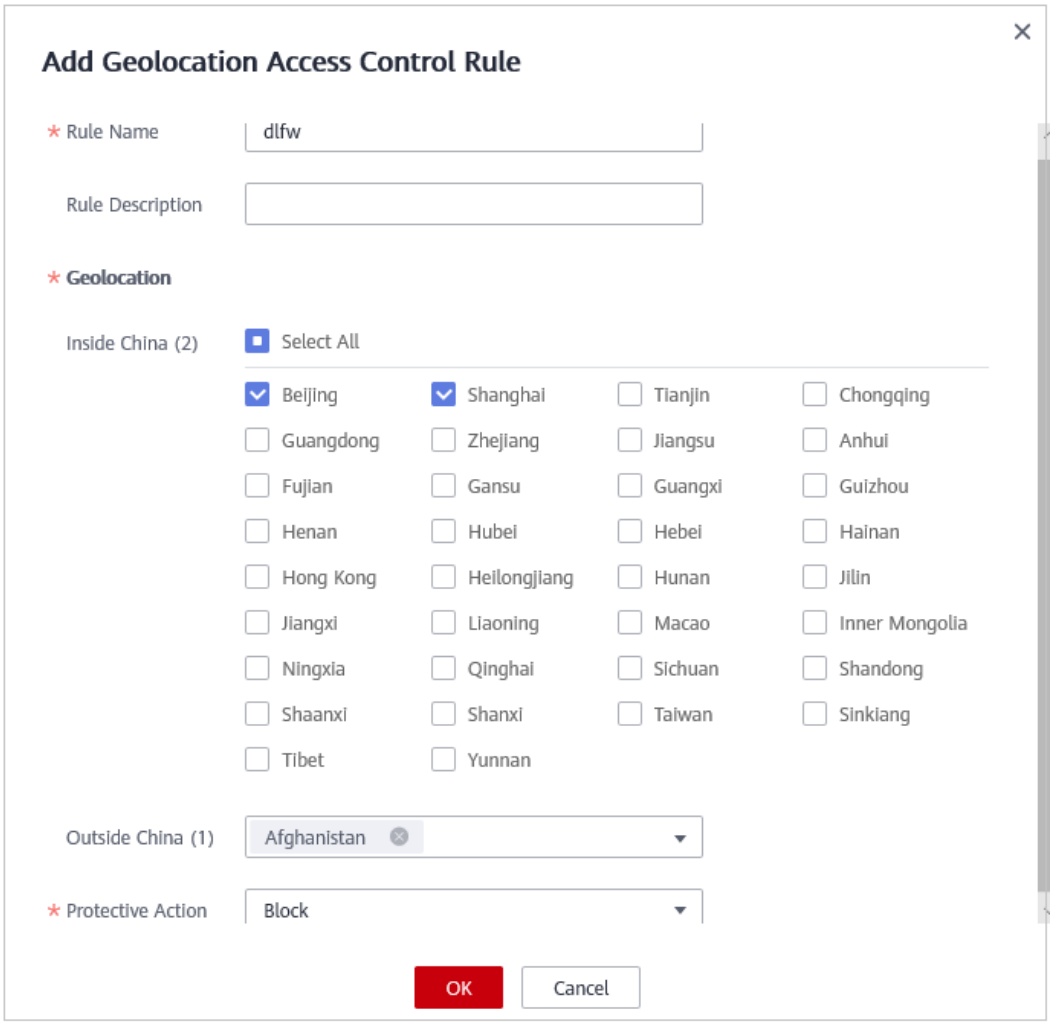
Figura 7-51 Área de configuración de control de acceso de geolocalización



Paso 7 En la esquina superior izquierda de la página **Geolocation Access Control**, haga clic en **Add Rule**.

Paso 8 En el cuadro de diálogo mostrado, agregue una regla de control de acceso de geolocalización. Tabla 7-12 o Tabla 7-13 describe parámetros.describes parameters.describes parameters.describes parameters.

Figura 7-52 Adición de una regla de control de acceso de geolocalización (nueva versión)



 Copyright © Huawei Technologies Co., Ltd.

AVISO

Actualmente, la nueva versión de la configuración de reglas de control de acceso de geolocalización solo se admite en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok

Figura 7-53 Adición de una regla de control de acceso de geolocalización

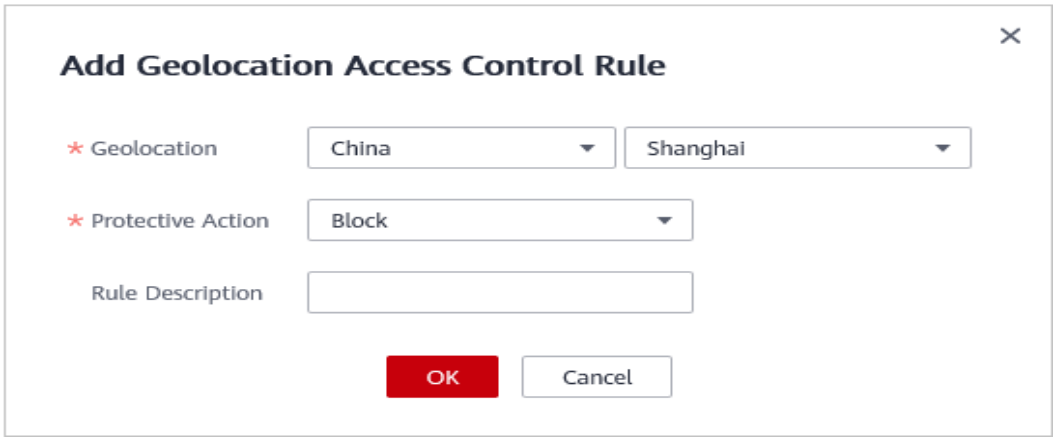


Tabla 7-12 Parámetros de regla (nueva versión)

Parámetro	Descripción	Valor de ejemplo
Rule Name	Nombre de regla configurado	dlfw
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	-
Geolocation	Ámbito geográfico de la dirección IP. Puede seleccionar una región dentro de China o fuera de la misma.	-
Protective Action	Acción WAF tomará si se cumple la regla. Puede seleccionar **Block**, **Allow**, o **Log only**.	**Block**

Tabla 7-13 Parámetros de regla

Parámetro	Descripción	Valor de ejemplo
Geolocation	Ubicación geográfica desde la que se origina una dirección IP	None
Protective Action	Acción WAF tomará si se cumple la regla. Puede seleccionar **Block**, **Allow**, o **Log only**.	**Block**

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	None

Paso 9 Haga clic en **OK**. A continuación, puede ver la regla agregada en la lista de las reglas de control de acceso de geolocalización.

Figura 7-54 Lista de reglas de control de acceso de geolocalización (nueva versión)

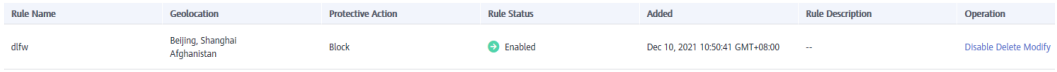
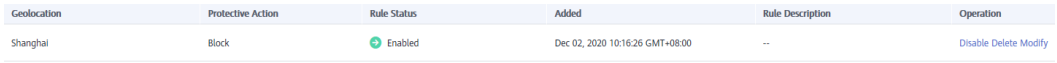


Figura 7-55 Lista de reglas de control de acceso de geolocalización



- 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

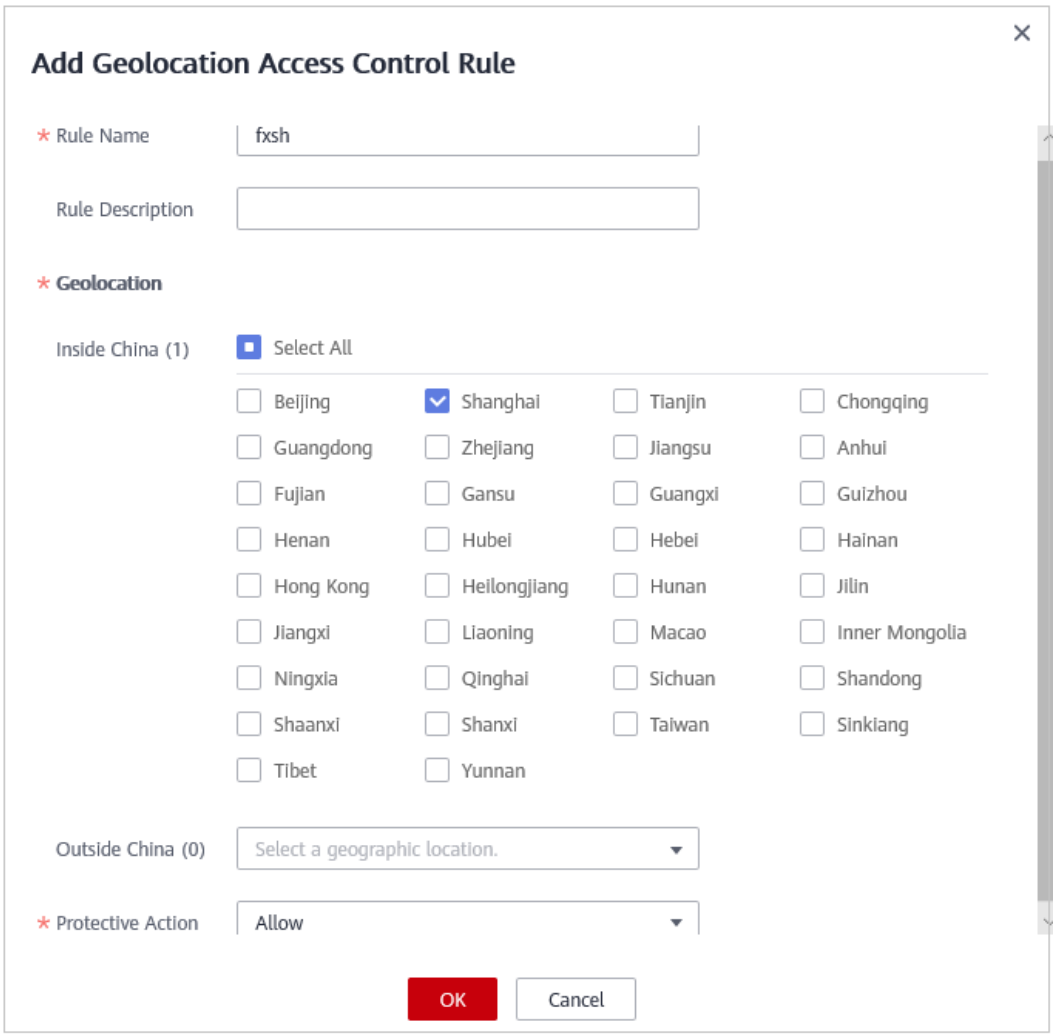
Ejemplo de configuración - Permitir solicitudes de acceso desde direcciones IP en una región especificada

Supongamos que el nombre de dominio *www.example.com* se ha conectado a WAF y que desea permitir que solo las direcciones IP de China accedan al nombre de dominio. Realice los siguientes pasos:

Paso 1 Añadir una regla de control de acceso de geolocalización: Seleccione **Shanghai** para **Geolocation** y seleccione **Allow** para **Protective Action**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-56 Seleccionar Allow para acción protectora (nueva versión)



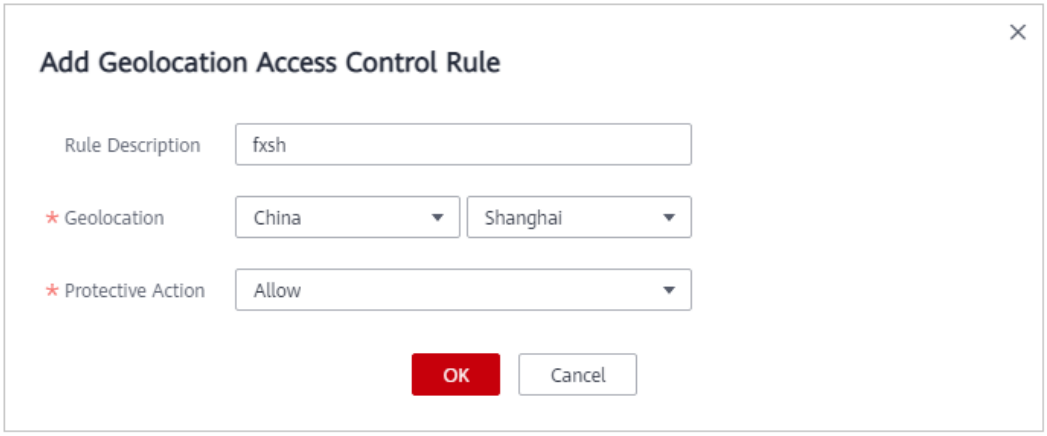
AVISO

Actualmente, la nueva versión de la configuración de reglas de control de acceso de geolocalización solo se admite en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok

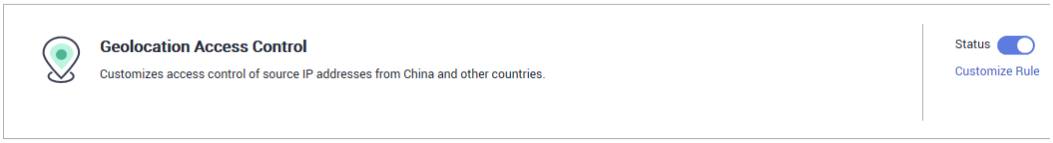
 Copyright © Huawei Technologies Co., Ltd.

Figura 7-57 Seleccionar Allow para acción protectora



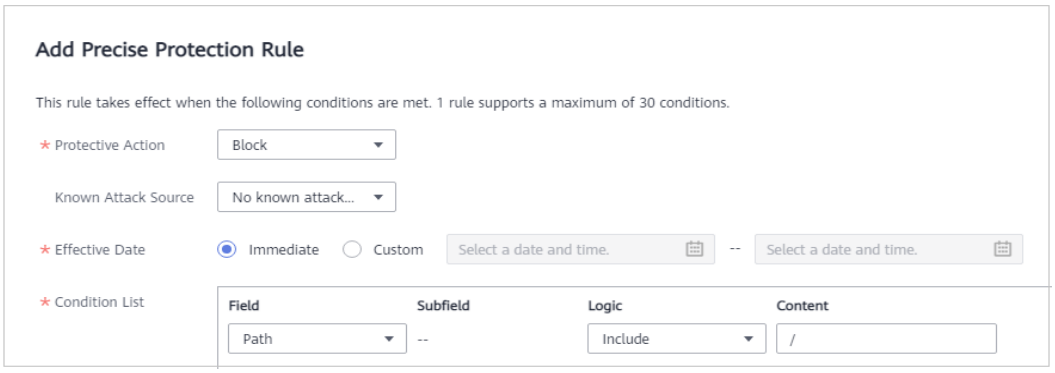
Paso 2 Habilitar el control de acceso de geolocalización.

Figura 7-58 Área de configuración de control de acceso de geolocalización



Paso 3 Configure una regla de protección precisa para bloquear todas las solicitudes.

Figura 7-59 Bloqueo de todas las solicitudes de acceso



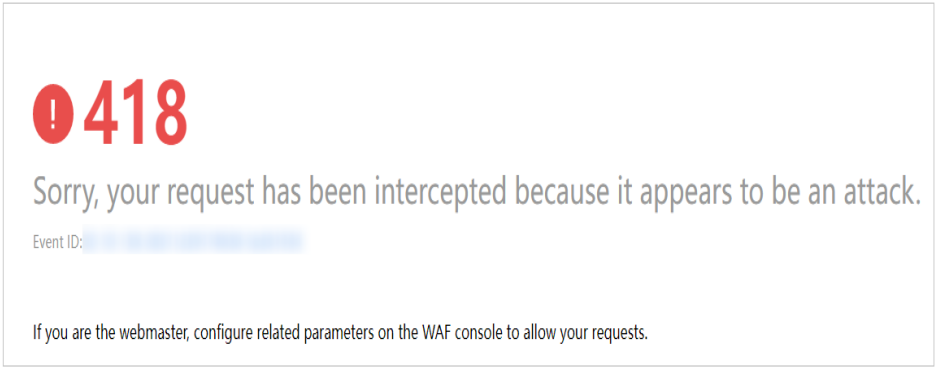
Para más detalles, consulte **Configuración de una regla de protección precisa**.

Paso 4 Borrar la caché del navegador y acceder a http://www.example.com.

Cuando una solicitud de acceso desde direcciones IP fuera de Shanghai accede a la página, WAF bloquea la solicitud de acceso. **Figura 7-60** muestra una página de bloque de ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-60 Página de bloqueo



Paso 5 Vaya a la consola WAF. En el panel de navegación de la izquierda, seleccione **Events**. Vea el evento en la página **Events**. Verá que todas las solicitudes que no provienen de Shanghai han sido bloqueadas.

----Fin

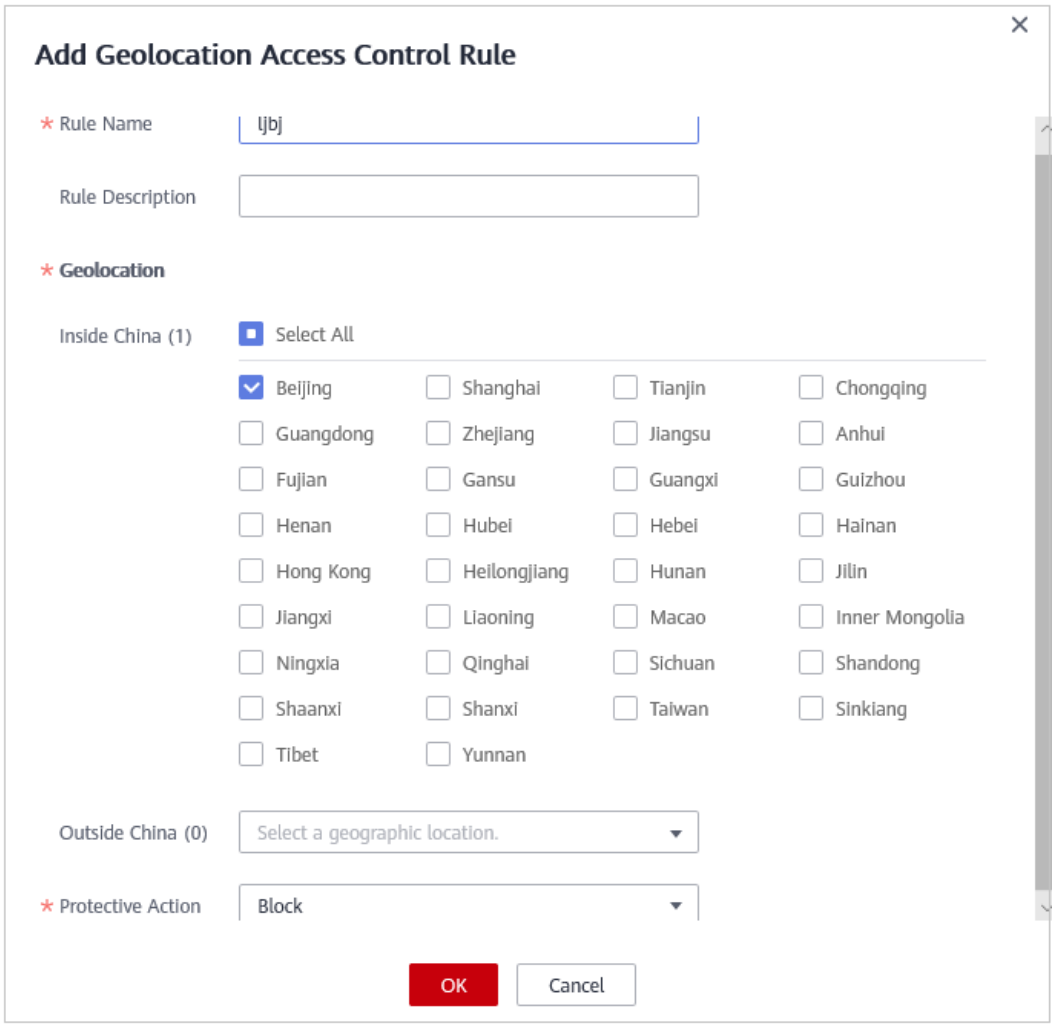
Ejemplo de configuración: Bloqueo de solicitudes de acceso desde direcciones IP en una región especificada

Supongamos que el nombre de dominio *www.example.com* se ha conectado a WAF y que desea bloquear todas las direcciones IP de Beijing para acceder al nombre de dominio. A continuación se muestra cómo configurar una regla para este fin:

Paso 1 Añada una regla de control de acceso de geolocalización, seleccione **Beijing** para **Geolocation** y **Block** pata **Protective Action**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-61 Bloqueo de solicitudes de acceso desde una región específica (nueva versión)



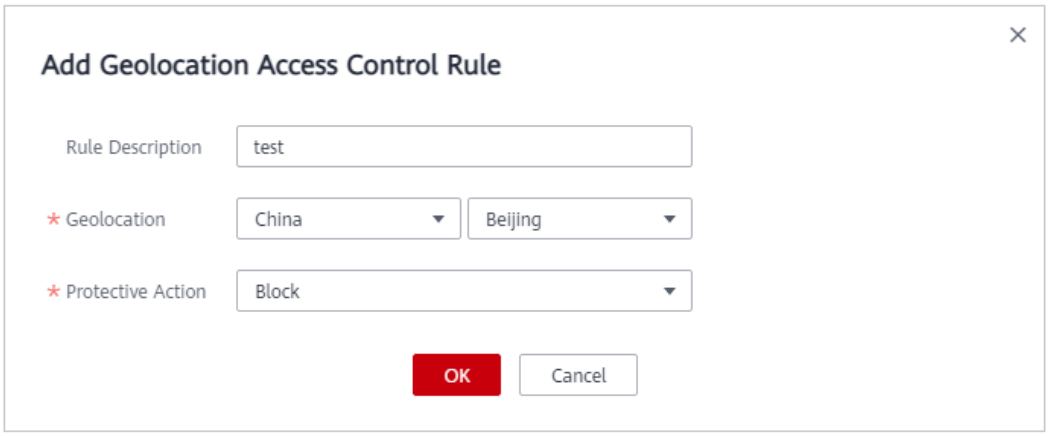
AVISO

Actualmente, la nueva versión de la configuración de reglas de control de acceso de geolocalización solo se admite en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok

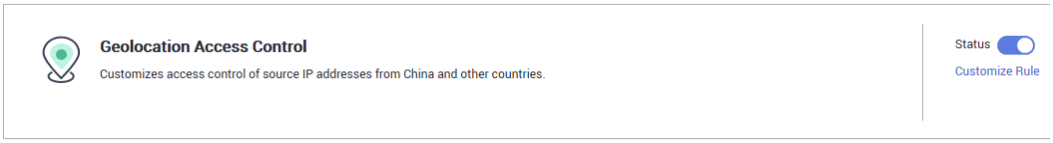
 Copyright © Huawei Technologies Co., Ltd.

Figura 7-62 Bloqueo de solicitudes de acceso desde una región específica



Paso 2 Habilitar el control de acceso de geolocalización.

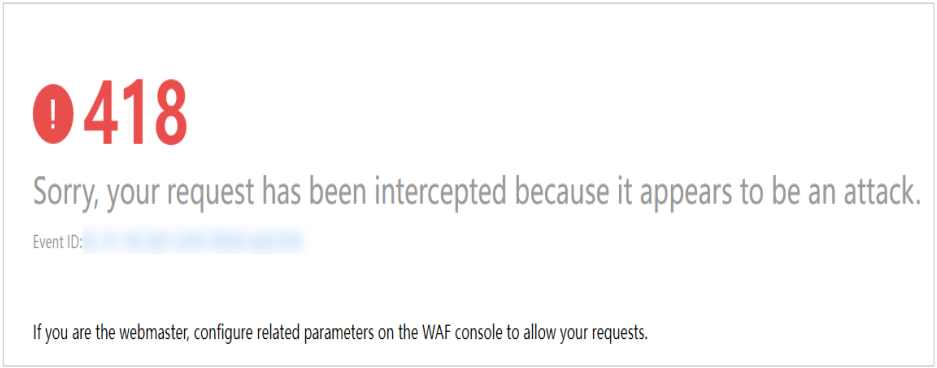
Figura 7-63 Área de configuración de control de acceso de geolocalización



Paso 3 Borrar la caché del navegador y acceder a http://www.example.com.

Cuando una solicitud de acceso desde direcciones IP dentro de Beijing accede a la página, WAF bloquea la solicitud de acceso. **Figura 7-64** muestra una página de bloque de ejemplo.

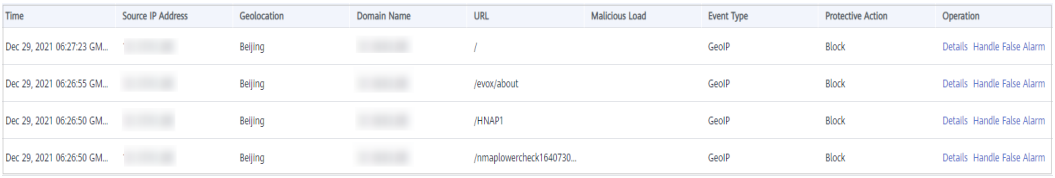
Figura 7-64 Página de bloqueo



Paso 4 Vaya a la consola WAF. En el panel de navegación de la izquierda, seleccione **Events**. Vea el evento en la página **Events**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-65 Consulta de eventos: bloqueo de solicitudes de acceso desde direcciones IP de una región



Time	Source IP Address	Geolocation	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
Dec 29, 2021 06:27:23 GM...	[redacted]	Beijing	[redacted]	/		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:55 GM...	[redacted]	Beijing	[redacted]	/evox/about		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:50 GM...	[redacted]	Beijing	[redacted]	/HNAP1		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:50 GM...	[redacted]	Beijing	[redacted]	/nmaplowercheck1640730...		GeoIP	Block	Details Handle False Alarm

----Fin

7.10 Configuración de una Regla de protección contra manipulaciones de Web

WAF puede almacenar en caché la configuración de las páginas web estáticas de los sitios web. Después de configurar una regla de protección contra manipulaciones web, WAF puede:

- Devolver directamente la página web almacenada en caché al visitante web normal para acelerar la respuesta a la solicitud.
- Devolver las páginas web originales almacenadas en caché a los visitantes si un atacante ha alterado las páginas web estáticas. Esto asegura que los visitantes de su sitio web siempre obtengan las páginas web correctas.
- Proteger todos los recursos de la ruta de la página Web. Por ejemplo, si se configura una regla de protección de manipulación web para la página estática **www.example.com/admin**, el WAF protege todos los recursos del directorio **/admin**.

  Por lo tanto, si la URL en el valor del encabezado de la solicitud **Referer** es la misma que la ruta de acceso antimanipulación configurada, por ejemplo, **/admin**, todos los recursos (recursos que terminan con png, jpg, jpeg, gif, bmp, css o js) también se almacenan en caché.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.

 Copyright © Huawei Technologies Co., Ltd.

AVISO

Asegúrese de que la respuesta del servidor de origen contiene el encabezado de respuesta **Content-Type**, o WAF puede no almacenar en caché la respuesta del servidor de origen.

Escenarios de aplicación

- Respuesta más rápida a las solicitudes

  Después de configurar una regla de protección de manipulación web, WAF almacena en caché las páginas web estáticas en el servidor. Cuando recibe una solicitud de un visitante web, WAF devuelve directamente la página web almacenada en caché al visitante web.

- Protección contra manipulación de la web

  Si un atacante modifica una página web estática en el servidor, WAF aún devuelve la página web original almacenada en caché a los visitantes. Los visitantes nunca ven las páginas que fueron manipuladas.

  WAF extrae aleatoriamente solicitudes de un visitante para comparar la página que recibió con la página en el servidor. Si WAF detecta que la página ha sido manipulada, se lo notifica por SMS o correo electrónico, dependiendo de lo que configure. Para más detalles, consulte **Habilitación de notificaciones de alarma**.

Procedimiento

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.

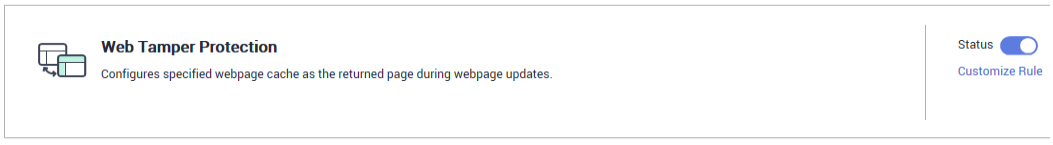
Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 In the navigation pane, choose **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**, cambie **Status** si es necesario y haga clic en **Customize Rule** para ir a la página **Web Tamper Protection**.

Figura 7-66 Área de configuración de Web Tamper Protection



Paso 7 En la esquina superior izquierda de la página **Web Tamper Protection**, haga clic en **Add Rule**.

Paso 8 En el cuadro de diálogo que se muestra, especifique los parámetros haciendo referencia a **Tabla 7-14**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-67 Adición de una regla de protección contra manipulaciones web

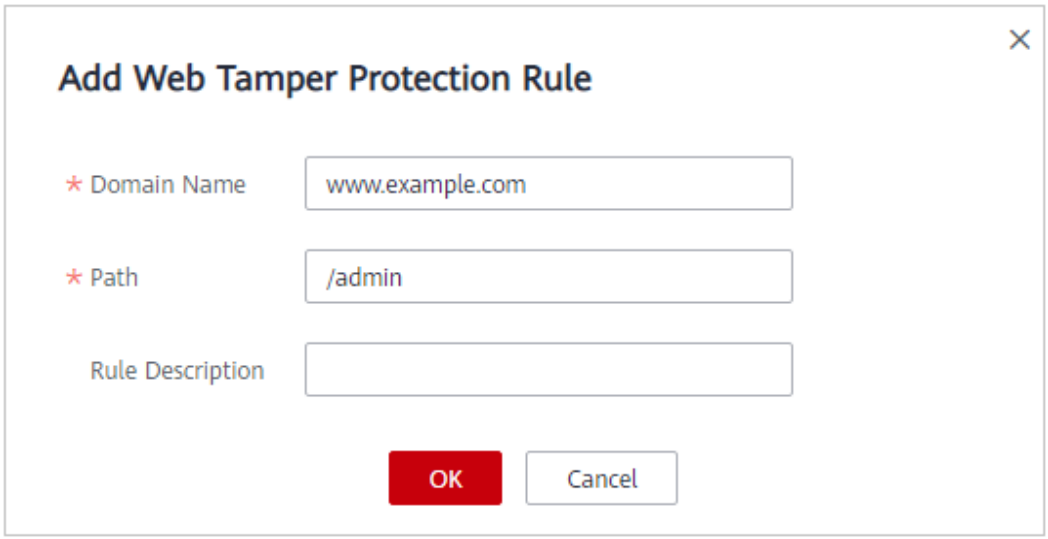


Tabla 7-14 Parámetros de regla

Parámetro	Descripción	Valor de ejemplo
Domain Name	Nombre de dominio del sitio web a proteger	**www.example.com**
Path	Una parte de la URL, sin incluir el nombre de dominio Una URL se utiliza para definir la dirección de una página web. El formato básico de URL es el siguiente: Nombre de protocolo://Domain name or IP address[:Port]/[Path/.../File name]. Por ejemplo, si la URL es **http://www.example.com/admin**, establezca **Path** en **/admin**. **NOTA** ● La ruta de acceso no admite expresiones regulares. ● La ruta de acceso no puede contener dos o más barras diagonales consecutivas. Por ejemplo, ///**admin**. Si introduce///**admin**, WAF converts /// to /.	**/admin**
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	None

 Copyright © Huawei Technologies Co., Ltd.

Paso 9 Haga clic en **OK**. Puede ver la regla en la lista de reglas de protección contra manipulaciones web.

Figura 7-68 Lista de reglas de protección web contra manipulaciones

----Fin

Otras operaciones

- Para deshabilitar una regla, haga clic en **Disable** en la columna **Operation** de la regla. El **Rule Status** predeterminado es **Enabled**.
- Para actualizar la caché de una página web protegida, haga clic en **Update Cache** en la fila que contiene la regla de protección de manipulación web correspondiente. Si la regla no se actualiza, WAF devolverá la página recientemente almacenada en caché, pero no la última página.
- Para eliminar una regla, haga clic en **Delete** en la fila que contiene la regla.

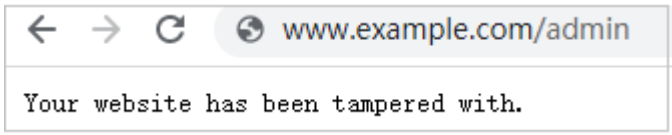
Ejemplo de configuración - Prevención de manipulaciones de Páginas Web estáticas

Para verificar que WAF está protegiendo una página **/admin** estático en su sitio web **www.example.com** de ser manipulado:

Paso 1 Utilice un navegador para acceder a **http://www.example.com/admin**.

Se devuelve una página manipulada.

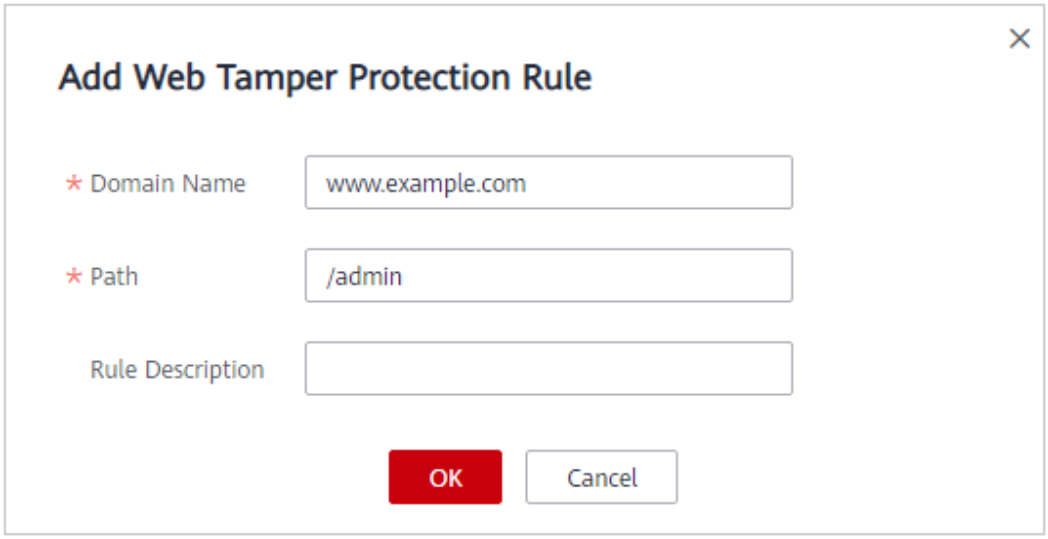
Figura 7-69 Una página estática que ha sido manipulada



Paso 2 Agregue una regla de prevención de manipulaciones web a WAF.

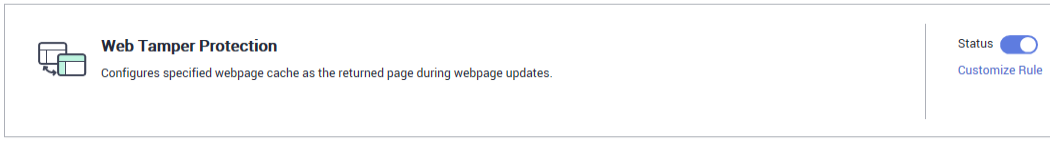
 Copyright © Huawei Technologies Co., Ltd.

Figura 7-70 Adición de una regla de protección contra manipulaciones web



Paso 3 Habilitación de WTP

Figura 7-71 Área de configuración de Web Tamper Protection



Paso 4 Utilice un navegador para acceder a **http://www.example.com/admin**. WAF almacenará en caché la página.

Paso 5 Acceda a **http://www.example.com/admin** de nuevo.

Se devuelve la página intacta.

----Fin

7.11 Configuración de las reglas de anti-crawler

Puede configurar reglas de protección contra anti-crawler de sitios web para protegerse contra motores de búsqueda, escáneres, herramientas de script y otros rastreadores, y usar JavaScript para crear reglas de protección contra rastreadores personalizadas.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.

 Copyright © Huawei Technologies Co., Ltd.

- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

- Las cookies deben estar habilitadas y JavaScript es compatible con cualquier navegador utilizado para acceder a un sitio web protegido por reglas de protección contra rastreadores.
- Si su servicio está conectado a CDN, tenga cuidado al usar la función anti-crawler de JS.

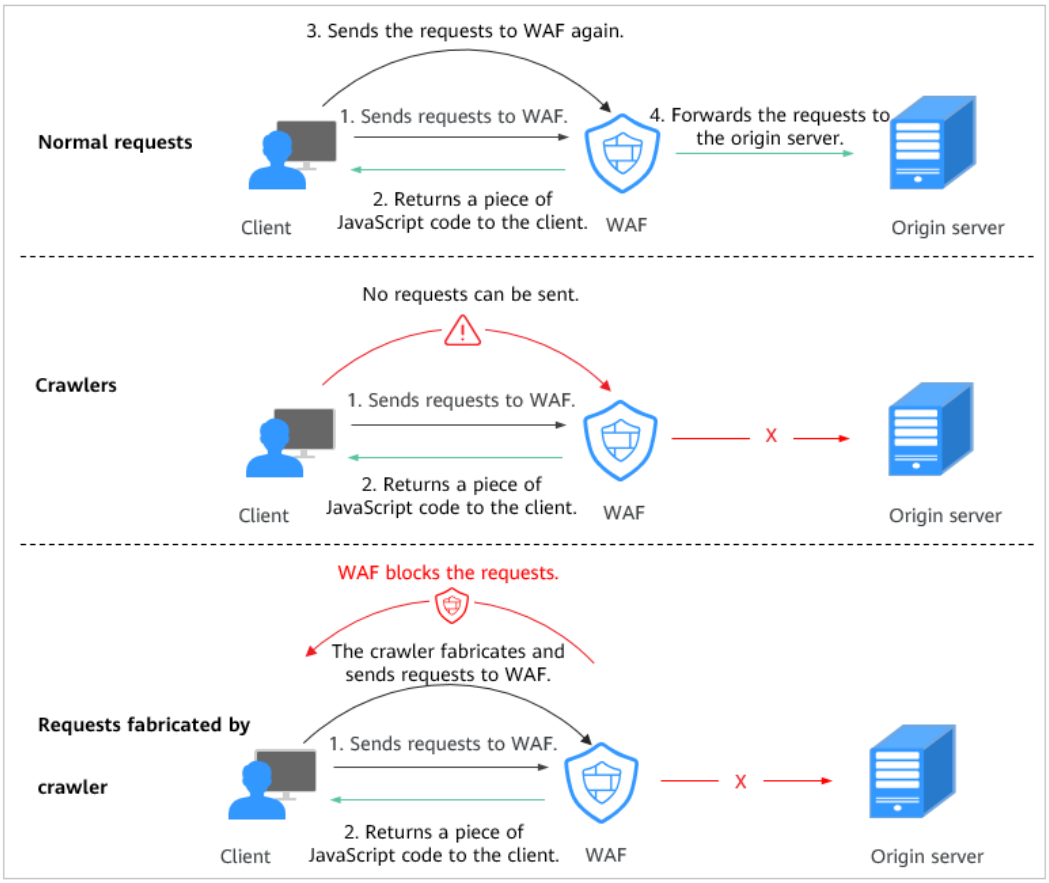
  El almacenamiento en caché de CDN puede afectar el rendimiento anti-crawler de JS y la accesibilidad de la página.
- La función anti-crawler de JavaScript no está disponible para instancias WAF de pago por uso.
- Esta función no está disponible en la edición estándar, anteriormente edición profesional.
- Actualmente, el JavaScript anti-rawler es apoyado en CN-Hong Kong and AP-Bangkok regions.
- Si no hay registros de bloqueo disponibles después de habilitar las reglas anti-crawler basadas en JavaScript, maneje el problema consultando **¿Por qué no se encuentran registros para algunas solicitudes bloqueadas por WAF después de activar el anti-Crawler?**
- 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.
- WAF Las reglas anti-crawler basadas en JavaScript solo verifican las solicitudes GET y no verifican las solicitudes POST.

Cómo Funciona la Protección Anti-Crawler JavaScript

Figura 7-72 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).

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-72 Proceso de protección Anti-Crawler de JavaScript



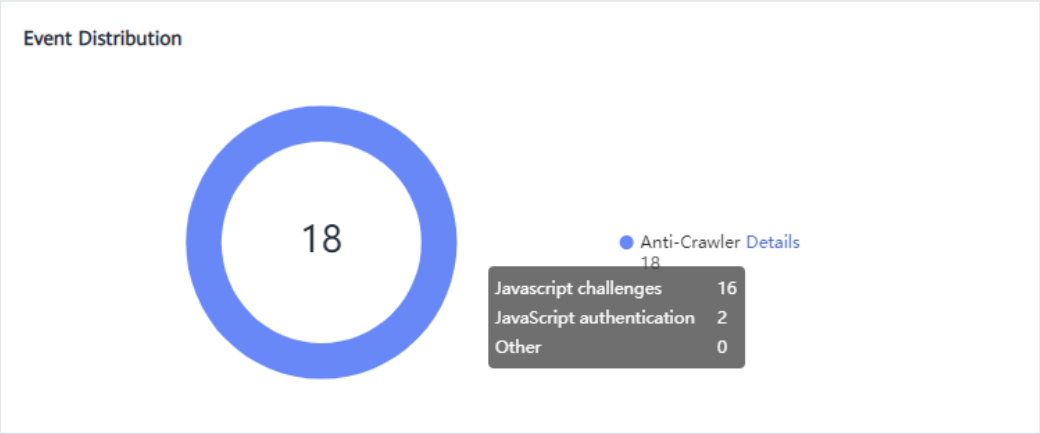
Si el anti-crawler JavaScript está habilitado cuando un cliente envía una solicitud, WAF devuelve un fragmento de código JavaScript al cliente.

- 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 desafíos de JavaScript y respuestas de autenticación, el sistema calcula cuántas solicitudes defiende el anti-crawler JavaScript. En **Figura 7-73**, el anti-crawler de JavaScript ha registrado 18 eventos, 16 de los cuales son respuestas de desafío de JavaScript, y 2 de los cuales son respuestas de autenticación de JavaScript. **Others** es el número de solicitudes de autenticación WAF fabricadas por el rastreador.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-73 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.

Procedimiento

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.

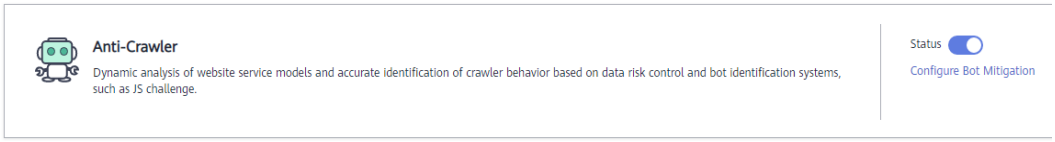
Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 In the navigation pane, choose **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 **Anti-Crawler**, habilite anti-Crawler usando el interruptor de la derecha, como se muestra en **Figura 7-74**. Si habilita esta función, haga clic en **Configure Bot Mitigation**.

Figura 7-74 Área de configuración Anti-Crawler



Paso 7 Seleccione la pestaña **Feature Library** y habilite la protección haciendo referencia a **Tabla 7-15**. **Figura 7-75** muestra un ejemplo.

Una regla anti-explotación basada en características tiene dos acciones de protección:

 Copyright © Huawei Technologies Co., Ltd.

- **Block**

  WAF bloquea y registra los ataques detectados.

- **Log only**

  Los ataques detectados solo se registran. Esta es la acción de protección predeterminada.

Scanner está habilitado de forma predeterminada, pero puede habilitar otros tipos de protección si es necesario.

Figura 7-75 Biblioteca de funciones

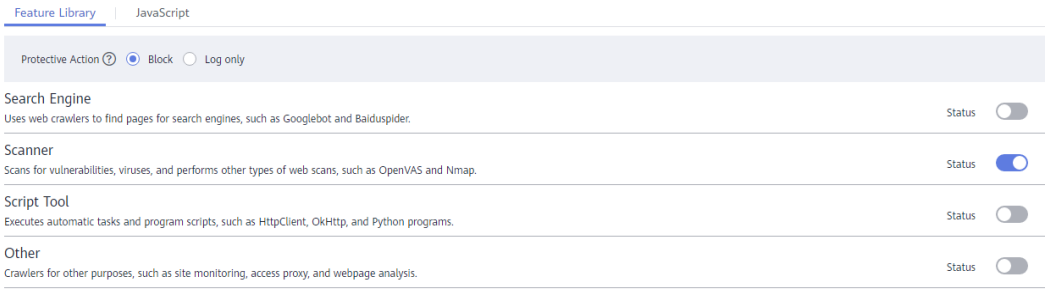


Tabla 7-15 Características de detección anti-crawler

Tipo	Descripción	Comentarios
Motor de búsqueda	Esta regla se utiliza para impedir que los rastreadores web, como Googlebot y Baiduspider, recopilen contenido de su sitio.	Si habilita esta regla, WAF detecta y bloquea los rastreadores de motores de búsqueda. **NOTA** Si **Search Engine** no está habilitado, WAF no bloquea las solicitudes POST de Googlebot o Baiduspider. Si desea bloquear las solicitudes POST de Baiduspider, utilice la configuración descrita en **Ejemplo de configuración - Motor de búsqueda**.
Escáner	Esta regla se utiliza para bloquear analizadores, como OpenVAS y Nmap. Un escáner analiza vulnerabilidades, virus y otros trabajos.	Después de activar esta regla, WAF detecta y bloquea los rastreadores del escáner.
Herramienta de script	Esta regla se utiliza para bloquear herramientas de script. Una herramienta de script se utiliza a menudo para ejecutar tareas automáticas y scripts de programa, como los programas HttpClient y Python.	Si habilita esta regla, WAF detecta y bloquea la ejecución de tareas automáticas y scripts de programa. **NOTA** Si su aplicación utiliza scripts como HttpClient y Python, deshabilite **Script Tool**. De lo contrario, WAF identificará tales herramientas de script como rastreadores y bloqueará la aplicación.

 Copyright © Huawei Technologies Co., Ltd.

Tipo	Descripción	Comentarios
Otro	Esta regla se utiliza para bloquear los rastreadores utilizados para otros fines, como el monitoreo de sitios, el uso de proxys de acceso y el análisis de páginas web. **NOTA** Para evitar ser bloqueados por WAF, los rastreadores pueden usar un gran número de proxies de direcciones IP.	Si habilita esta regla, WAF detecta y bloquea los rastreadores que se utilizan para diversos fines.

Paso 8 Seleccione la pestaña **JavaScript** y configure **Status** y **Protective Action**.

El anti-crawler de **JavaScript** está deshabilitado por defecto. Para habilitarlo, haga clic en y **Confirm** en el cuadro de diálogo mostrado. indica que el anti-crawler JavaScript está activado.

AVISO

- Las cookies deben estar habilitadas y JavaScript es compatible con cualquier navegador utilizado para acceder a un sitio web protegido por reglas de protección contra rastreadores.
- Si su servicio está conectado a CDN, tenga cuidado al usar la función anti-crawler de JS.

  El almacenamiento en caché de CDN puede afectar el rendimiento anti-crawler de JS y la accesibilidad de la página.

Paso 9 Configure una regla anti-crawler basada en JavaScript haciendo referencia a **Tabla 7-16**.

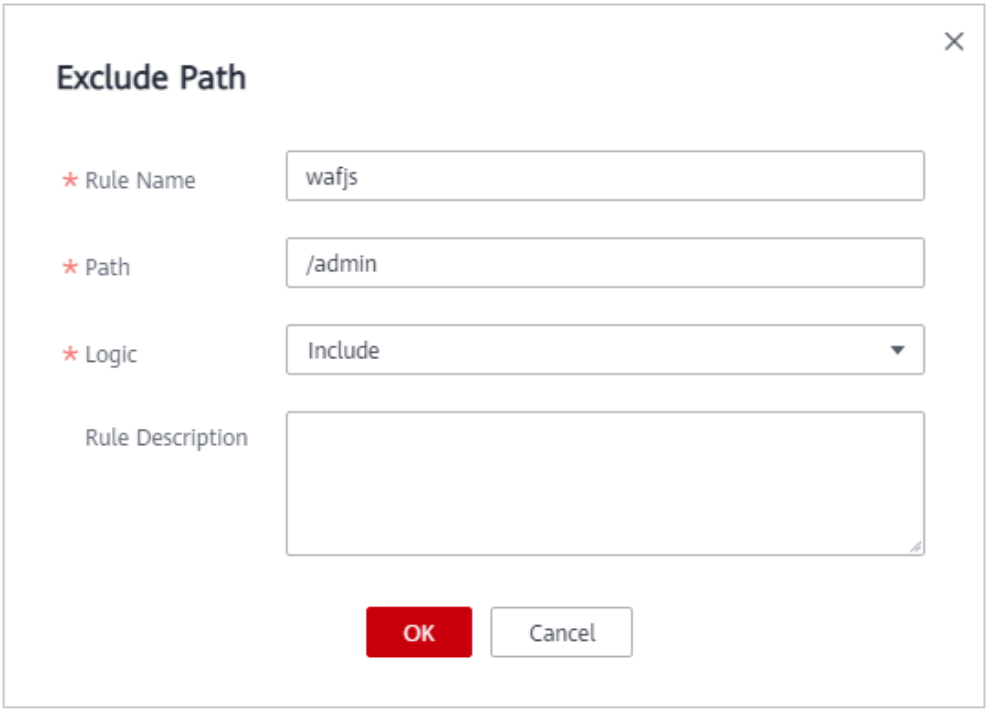
Se proporcionan dos acciones de protección: **Protect all paths** y **Protect a specified path**.

- Para proteger todas las rutas excepto una ruta especificada

  Seleccione **Protect all paths**, pero en la esquina superior izquierda de la página, haga clic en **Exclude Path**. Configure los parámetros necesarios en el cuadro de diálogo mostrado y haga clic en **OK**.

 Copyright © Huawei Technologies Co., Ltd.

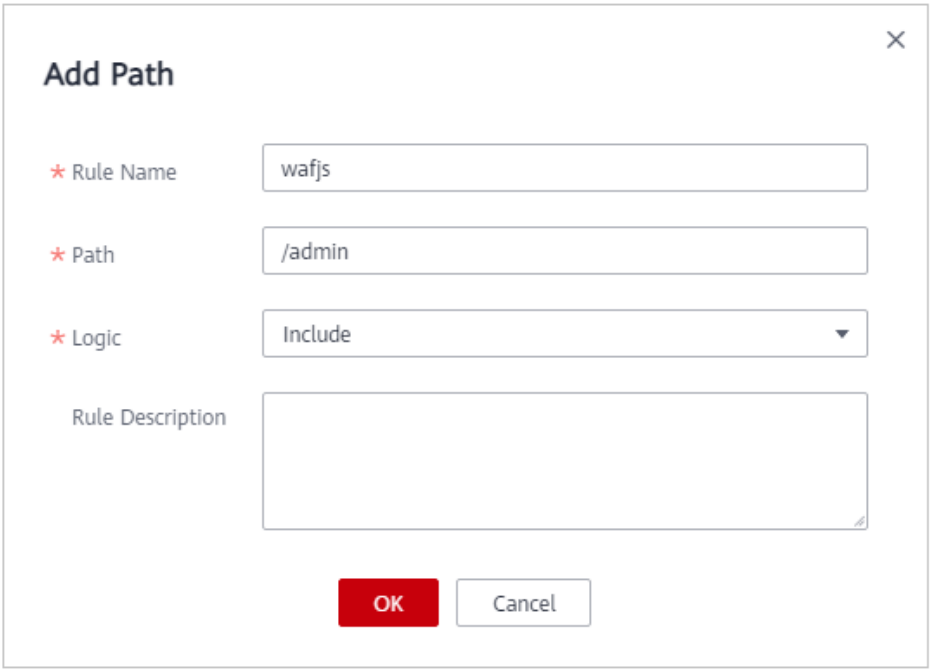
Figura 7-76 Excluir ruta



- Para proteger sólo una ruta de acceso especificada

  Seleccione **Protect a specified path**. En la esquina superior izquierda de la página, haga clic en **Add Path**. En el cuadro de diálogo que aparece, configure los parámetros necesarios y haga clic en **OK**.

Figura 7-77 Agregar ruta



 Copyright © Huawei Technologies Co., Ltd.

Tabla 7-16 Parámetros de una regla de protección anti-crawler basada en JavaScript

Parámetro	Descripción	Valor de ejemplo
Rule Name	Nombre de la regla	wafjs
Path	Una parte de la URL, sin incluir el nombre de dominio Una URL se utiliza para definir la dirección de una página web. El formato básico de URL es el siguiente: Nombre de protocolo:// Domain name or IP address[:Port]/[Path/.../File name]. Por ejemplo, si la URL es **http://www.example.com/admin**, establezca **Path** en **/admin**. **NOTA** ● La ruta de acceso no admite expresiones regulares. ● La ruta de acceso no puede contener dos o más barras diagonales consecutivas. Por ejemplo, ///**admin**. Si introduce///**admin**, WAF converts /// to /.	/admin
Logic	Seleccione una relación lógica en la lista desplegable.	Include
Rule Description	Una breve descripción de la regla.	None

----Fin

Otras operaciones

- 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.

 Copyright © Huawei Technologies Co., Ltd.

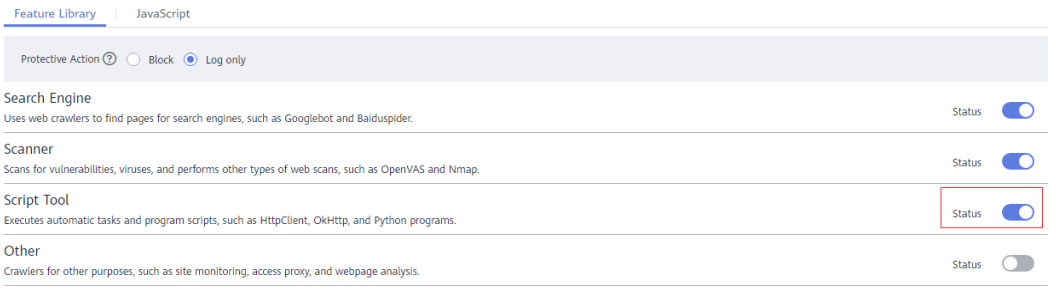
Ejemplo de configuración - sólo rastreadores de secuencias de comandos de registro

Para verificar que WAF está protegiendo el nombre de dominio **www.example.com** contra una regla anti-crawler:

Paso 1 Ejecute una herramienta de JavaScript para rastrear el contenido de la página web.

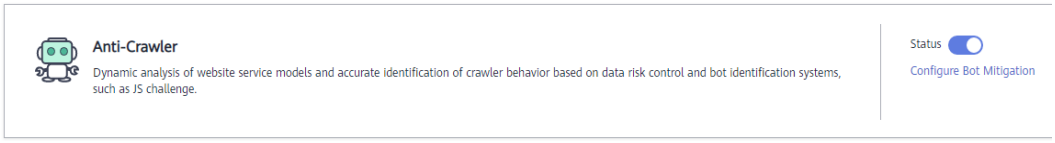
Paso 2 En la pestaña **Feature Library**, habilite la **Script Tool** y seleccione **Log only** para **Protective Action**. (Si WAF detecta un ataque, solo registra el ataque.)

Figura 7-78 Habilitación de la herramienta de script



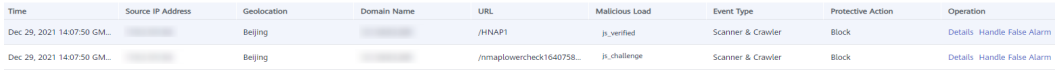
Paso 3 Habilite la protección de anti-crawler.

Figura 7-79 Área de configuración Anti-Crawler



Paso 4 En el panel de navegación de la izquierda, seleccione **Events** para ir a la página **Events**.

Figura 7-80 Consulta de eventos - Rastreadores de scripts



----Fin

Ejemplo de configuración - Motor de búsqueda

A continuación se muestra cómo permitir el motor de búsqueda de Baidu o Google y bloquear la solicitud POST de Baidu.

Paso 1 Establezca **Status** de **Search Engine** en haciendo referencia a las instrucciones en **Paso 6**.

Paso 2 Configure una regla de protección precisa haciendo referencia a **Configuración de una regla de protección precisa**, como se muestra en **Figura 7-81**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-81 Bloqueo de solicitudes POST

----Fin

7.12 Configuración de una regla de prevención de fugas de información

Puede agregar dos tipos de reglas de prevención de fugas de información.

- Filtrado de información confidencial: evita la divulgación de información confidencial (como números de identificación, números de teléfono y direcciones de correo electrónico).
- Intercepción de código de respuesta: bloquea los códigos de estado HTTP especificados.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

Esta función no está incluida en la edición estándar, anteriormente edición profesional.

Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.

Procedimiento

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.

 Copyright © Huawei Technologies Co., Ltd.

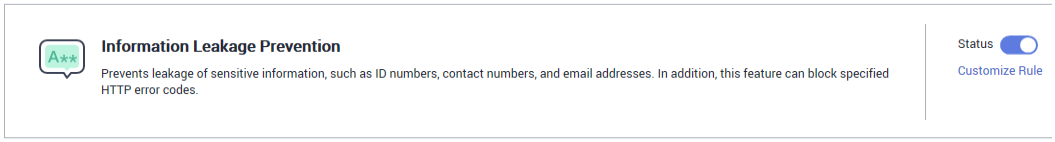
Paso 3 Haga clic ☰ en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 In the navigation pane, choose **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 **Information Leakage Prevention**, cambie **Status** si es necesario y haga clic en **Customize Rule**.

Figura 7-82 Área de configuración de Prevención de fugas de información



Paso 7 En la esquina superior izquierda de la página **Information Leakage Prevention**, haga clic en **Add Rule**.

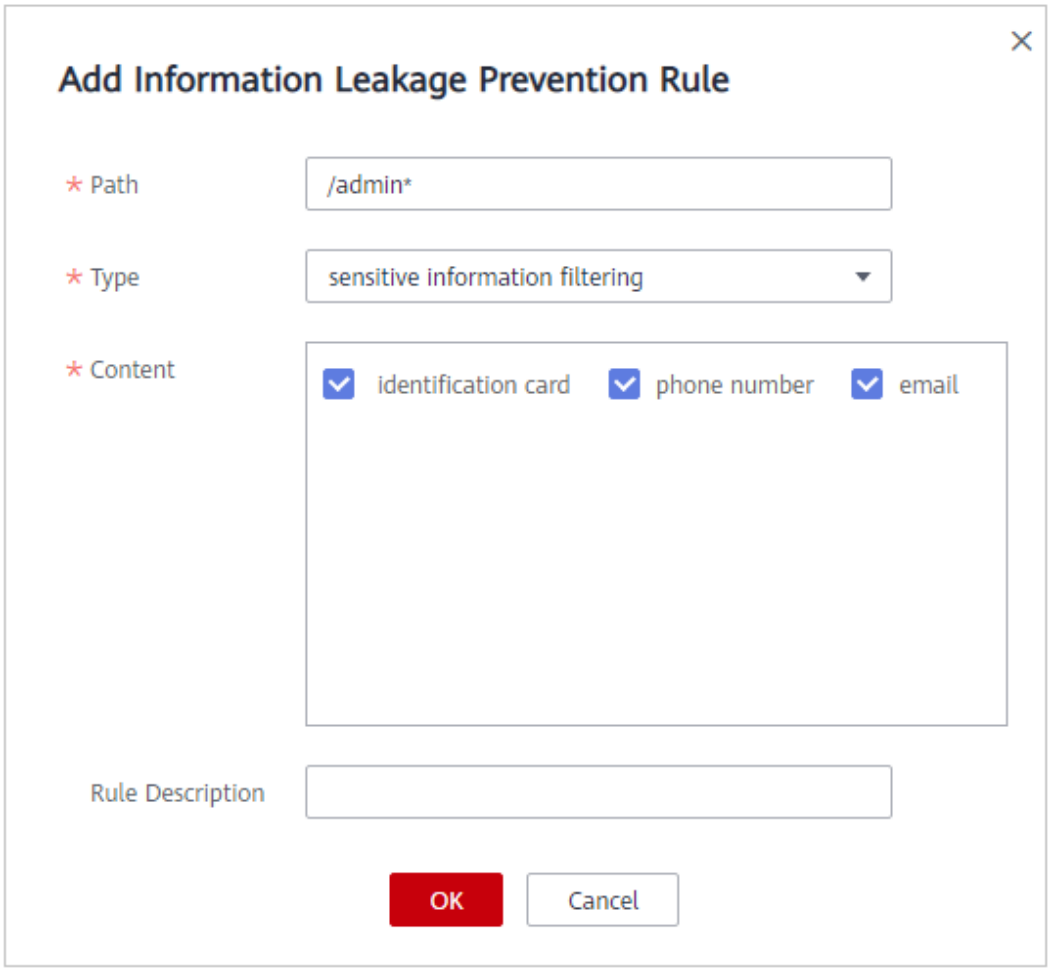
Paso 8 En el cuadro de diálogo que se muestra, agregue una regla de prevención de fugas de información haciendo referencia a **Tabla 7-17**. **Figura 7-83** y **Figura 7-84** muestran dos ejemplos.

Las reglas de prevención de fugas de información evitan que se divulgue información confidencial (como números de identificación, números de teléfono y direcciones de correo electrónico). Este tipo de regla también puede bloquear códigos de estado HTTP especificados.

sensitive information filtering: Configure reglas para enmascarar información sensible, como números de teléfono y números de identificación, de páginas web. Por ejemplo, puede establecer las siguientes reglas de protección para enmascarar información confidencial, como números de identificación, números de teléfono y direcciones de correo electrónico:

 Copyright © Huawei Technologies Co., Ltd.

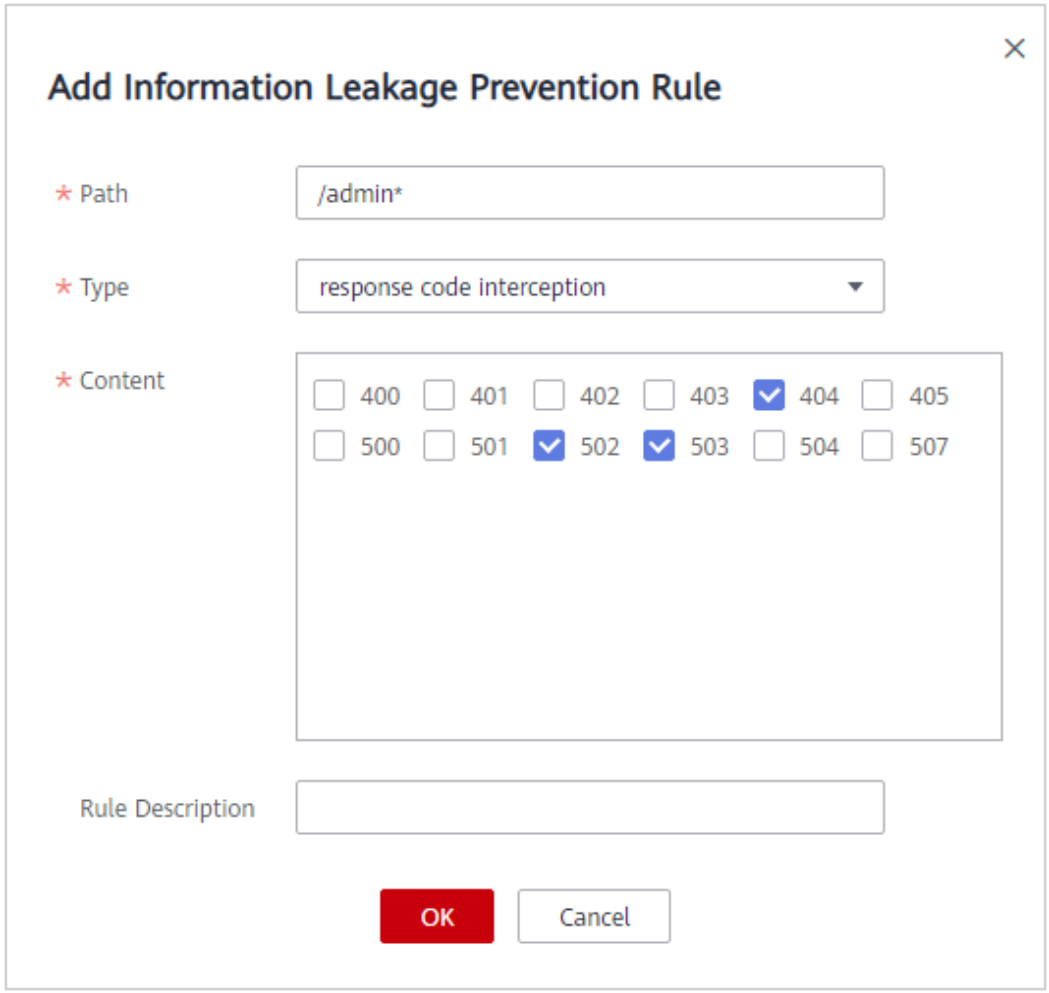
Figura 7-83 Fuga de información sensible



response code interception: Una página de error de un código de respuesta HTTP específico puede contener información sensible. Puede configurar reglas para bloquear dichas páginas de error para evitar que dicha información se filtre. Por ejemplo, puede establecer la siguiente regla para bloquear páginas de error de los códigos de respuesta HTTP 404, 502 y 503.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-84 Bloqueo de códigos de respuesta



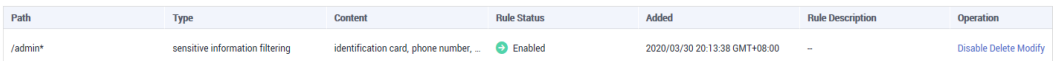
 Copyright © Huawei Technologies Co., Ltd.

Tabla 7-17 Parámetros de regla

Parámetro	Descripción	Valor de ejemplo
Path	Parte de la URL que no incluye el nombre de dominio. La URL puede contener información confidencial (como números de identificación, números de teléfono y direcciones de correo electrónico) o un código de error bloqueado. ● Coincidencia de prefijo: Solo el prefijo de la ruta a introducir debe coincidir con el de la ruta a proteger. Si la ruta de acceso que se va a proteger es /**admin**, establezca **Path** en **/admin***. ● Coincidencia exacta: La ruta que se va a introducir debe coincidir con la ruta que se va a proteger. Si la ruta de acceso que se va a proteger es /**admin**, establezca **Path** en **/admin**. **NOTA** – La ruta solo admite prefijo y coincidencias exactas. No se admiten expresiones regulares. – La ruta de acceso no puede contener dos o más barras diagonales consecutivas. Por ejemplo, ///**admin**. Si ingresa ///**admin**, el motor WAF convierte /// en /.	**/admin***
Type	● **sensitive information filtering** ● **response code interception**: Habilite WAF para bloquear la página de código de respuesta HTTP especificada.	**sensitive information filtering**
Content	Información a proteger. Las opciones son **identification card**, **phone number**, y **email**.	**identification card**
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	None

Paso 9 Haga clic en **OK**. La regla de prevención de fugas de información agregada se muestra en la lista de reglas de prevención de fugas de información.

Figura 7-85 Lista de normas de prevención de fugas de información



----Fin

Otras operaciones

- Para deshabilitar una regla, haga clic en **Disable** en la columna **Operation** de la regla. El **Rule Status** predeterminado es **Enabled**.

 Copyright © Huawei Technologies Co., Ltd.

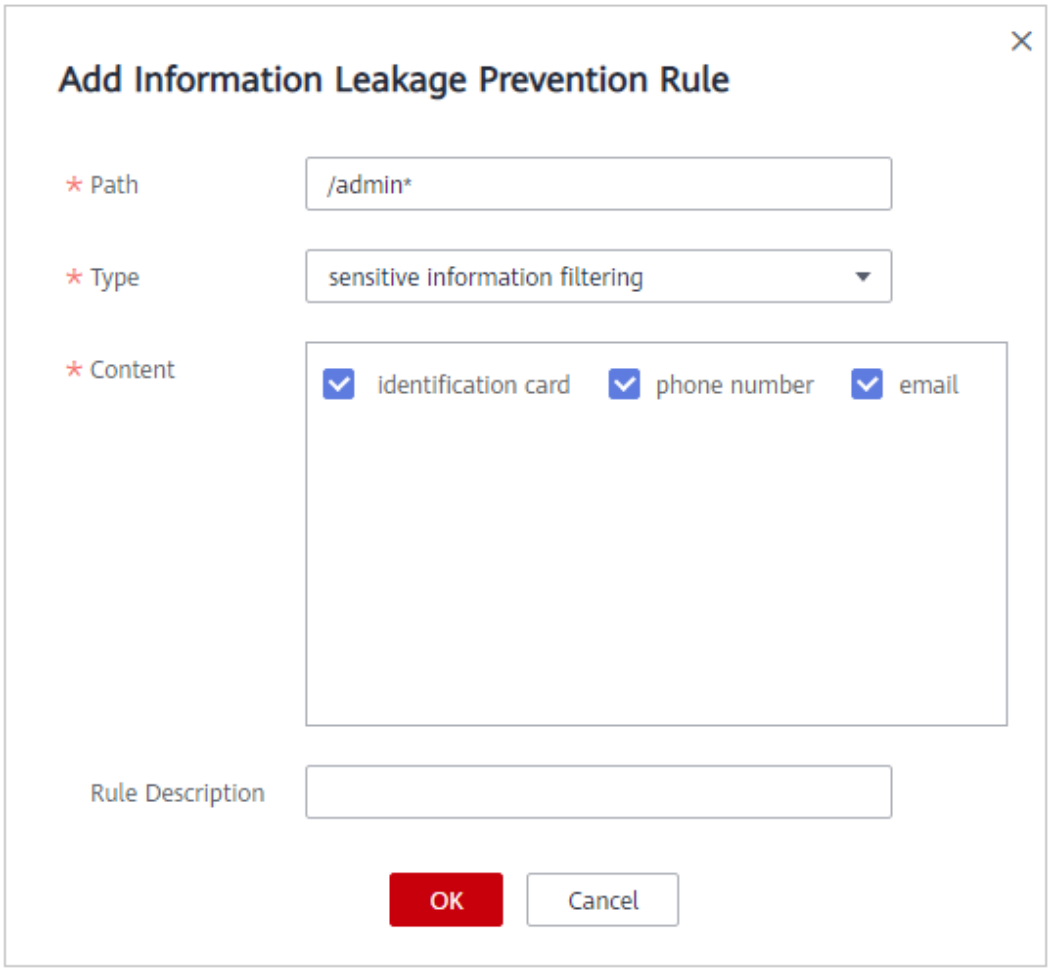
- Para modificar una regla, haga clic en **Modify** en la fila que contiene la regla.
- Para eliminar una regla, haga clic en **Delete** en la fila que contiene la regla.

Ejemplo de configuración - Enmascarar información confidencial

Para verificar que WAF está protegiendo su nombre de dominio *www.example.com* contra una regla de prevención de fugas de información:

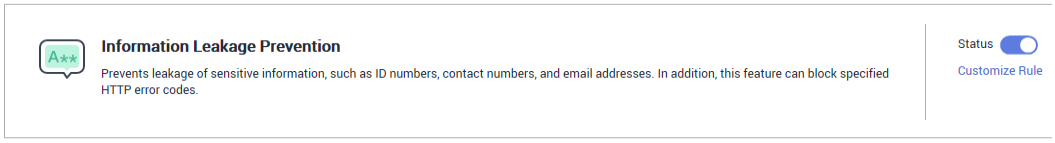
Paso 1 Agregue una regla de prevención de fugas de información.

Figura 7-86 Fuga de información sensible



Paso 2 Habilitación de la prevención de fugas de información.

Figura 7-87 Área de configuración de Prevención de fugas de información

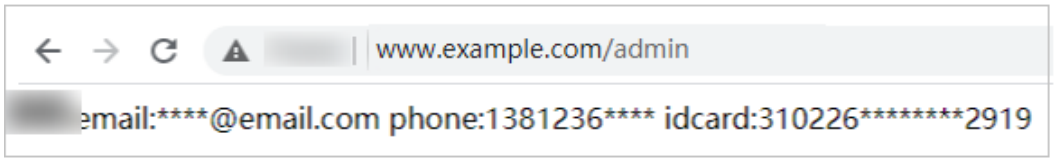


Paso 3 Borrar la caché del navegador y acceder a http://www.example.com/admin/.

La dirección de correo electrónico, el número de teléfono y el número de identidad de la página devuelta están enmascarados.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-88 Información sensible enmascarada



----Fin

7.13 Configuración de una regla de enmascaramiento de falsa alarma

Una vez que un ataque golpea una regla de protección web básica de WAF o una regla anti-crawler de la biblioteca de características, 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**.

Puede agregar reglas de enmascaramiento de falsas alarmas para permitir que WAF ignore ciertos ID de regla o tipos de eventos (por ejemplo, omita las comprobaciones XSS para una URL específica).

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

Restricciones

- Puede configurar reglas de enmascaramiento de falsas alarmas solo para eventos generados para reglas de protección web básicas preestablecidas y reglas anti-explotación de la biblioteca de características. A continuación se proporciona más detalles sobre las reglas:
  - 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.
- Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.

 Copyright © Huawei Technologies Co., Ltd.

- Puede configurar una regla de enmascaramiento de falsa alarma haciendo referencia a **Manejo de falsas alarmas**. Después de manejar una falsa alarma, puede ver la regla de enmascaramiento de falsa alarma activada en la lista de reglas de enmascaramiento de falsa alarma.

Procedimiento

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.

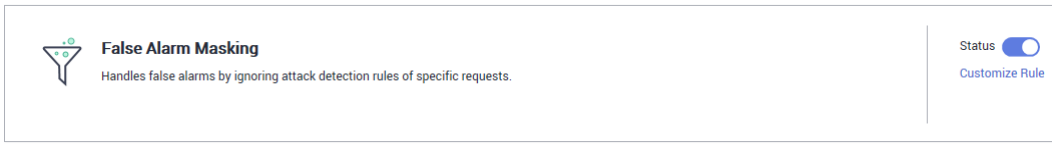
Paso 3 Haga clic en la esquina superior izquierda y elija **Web Application Firewall** en **Security & Compliance**.

Paso 4 In the navigation pane, choose **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 **False Alarm Masking**, cambie **Status** si es necesario y haga clic en **Customize Rule**.

Figura 7-89 Área de configuración de enmascaramiento de falsa alarma



Paso 7 En la esquina superior izquierda de la página **False Alarm Masking**, haga clic en **Add Rule**.

Paso 8 Agregue una regla de enmascaramiento de falsa alarma haciendo referencia a **Tabla 7-18**. **Figura 7-90** muestra un ejemplo.shows an example.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-90 Adición de una regla de enmascaramiento de falsa alarma

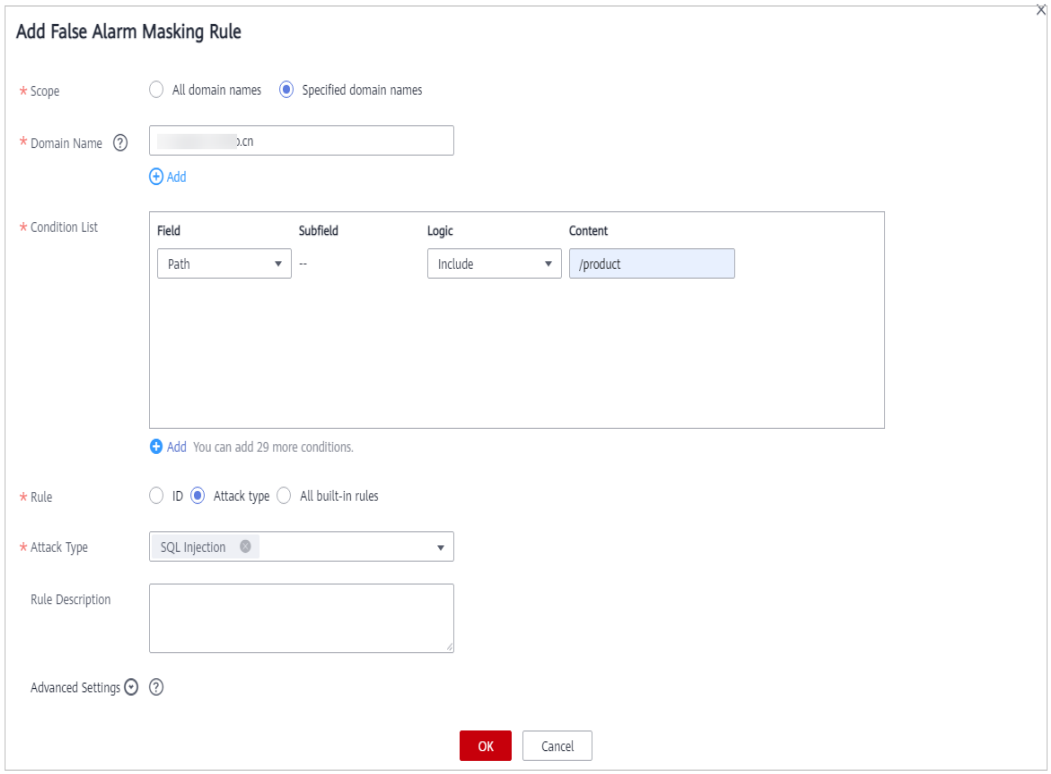


Tabla 7-18 Parámetros para agregar una regla de enmascaramiento de falsa alarma

Parámetro	Descripción	Valor de ejemplo
Scope	● **All domain names**: De forma predeterminada, esta regla se utilizará para todos los nombres de dominio que estén protegidos por la política actual. ● **Specified domain names**: Esta regla se utilizará para los nombres de dominio especificados que coincidan con el nombre de dominio comodín que está protegido por la política actual.	Nombres de dominio especificados
Domain Name	Este parámetro es obligatorio cuando selecciona **Specified domain names** para **Scope**. Introduzca un nombre de dominio único que coincida con el nombre de dominio comodín que está protegido por la política actual.	www.example.com

 Copyright © Huawei Technologies Co., Ltd.

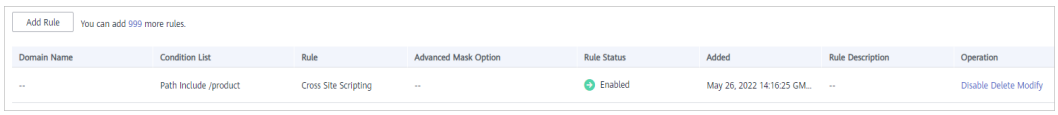
Parámetro	Descripción	Valor de ejemplo
Condition List	Haga clic en **Add** para agregar condiciones. Es necesario agregar al menos una condición. Puede agregar hasta 30 condiciones a una regla de protección. Si se agrega más de una condición, se deben cumplir todas las condiciones para que se aplique la regla. Una condición incluye los siguientes parámetros: Los parámetros para configurar una condición se describen de la siguiente manera: ● Campo ● **Subfield**: configure este campo solo cuando se seleccione **Params**, **Cookie**, o **Header** para **Field**. **AVISO** La longitud de un subcampo no puede superar los 2,048 de bytes. Solo se permiten dígitos, letras, guiones bajos (_) y guiones (-). ● **Lógica**: Seleccione una relación lógica de la lista desplegable. ● **Content**: Ingrese o seleccione el contenido que coincida con la condición.	Path, Include, /product
Rule	El elemento para el que tiene efecto la regla de enmascaramiento de falsa alarma. Las opciones son: ● **ID**: Configure la regla por ID de evento. ● **Attack type**: Configure la regla por tipo de evento. ● **All built-in rules**: todas las comprobaciones habilitadas en **Protección web básica**.	Attack type
ID	Este parámetro es obligatorio cuando **Rule** se establece en **ID**. ID de un evento de ataque en la página **Events**. Si el tipo de evento es **Custom**, no tiene ID de evento. Haga clic en **Handle False Alarm** en la fila que contiene el evento de ataque para obtener el ID. Para configurar el enmascaramiento de falsa alarma en la página **Events**, consulte **Manejo de falsas alarmas**.	041046

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Attack Type	Este parámetro es obligatorio cuando **Rule** se establece en **Attack type**. Seleccione un tipo de ataque en el cuadro de lista desplegable. WAF puede defenderse contra ataques XSS, shells web, ataques de inyección SQL, rastreadores maliciosos, inclusiones de archivos remotos, inclusiones de archivos locales, ataques de inyección de comandos y otros ataques.	Inyección de SQL
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	SQL injection attacks are not intercepted.
Advanced Settings	Para ignorar los ataques de un campo específico, especifique el campo en el área **Advanced Settings**. Después de agregar la regla, WAF dejará de bloquear los eventos de ataque del campo especificado. Seleccione un campo de destino en el primer cuadro de lista desplegable de la izquierda. Se admiten los siguientes campos: **Params**, **Cookie**, **Header**, **Body**, y **Multipart**. ● Si selecciona **Params**, **Cookie**, o **Header**, puede seleccionar **All** o **Specified field** para configurar un subcampo. ● Si selecciona **Body** o **Multipart**, puede seleccionar **All**. ● Si selecciona **Cookie**, el **Domain Name** y **Path** pueden estar vacíos. **NOTA** Si se selecciona **All**, WAF no bloqueará todos los eventos de ataque del campo seleccionado.	Params All

Paso 9 Haga clic en **OK**. Puede ver la regla en la lista de reglas de enmascaramiento de falsas alarmas.

Figura 7-91 Lista de reglas de enmascaramiento de falsas alarmas



----Fin

 Copyright © Huawei Technologies Co., Ltd.

Otras operaciones

- 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.

7.14 Configuración de una regla de enmascaramiento de datos

En este tema se describe cómo configurar reglas de enmascaramiento de datos. Puede configurar reglas de enmascaramiento de datos para evitar que los datos confidenciales, como las contraseñas, se muestren en los registros de eventos.

NOTA

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 **Enterprise Project** y configurar políticas de protección para los nombres de dominio del proyecto.

Prerrequisitos

Se ha agregado un sitio web a WAF.

- Para ver el modo en la nube, consulte **Conexión de un sitio web a WAF (Cloud Mode)**.
- Para el modo dedicado, consulte **Conexión de un sitio web a WAF (Modo dedicado)**.

Restricciones

- Se necesitan varios minutos para que una nueva regla entre en vigor. Una vez que la regla surta efecto, los eventos de protección activados por la regla se mostrarán en la página **Events**.

Impacto en el sistema

Los datos confidenciales de los eventos serán enmascarados para proteger la privacidad de los visitantes de su sitio web.

Procedimiento

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**.

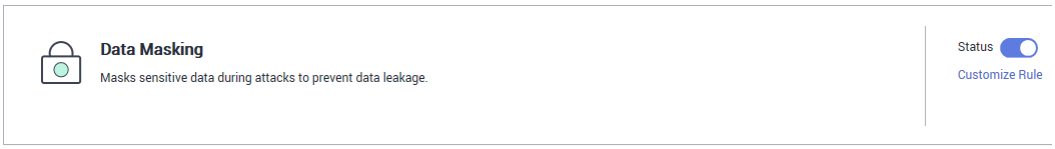
Paso 4 In the navigation pane, choose **Website Settings**.

Paso 5 En la columna **Policy** de la fila que contiene el nombre de dominio, haga clic en **Configure Policy**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 6 En el área de configuración de **Data Masking**, cambie **Status** si es necesario y haga clic en **Customize Rule**.

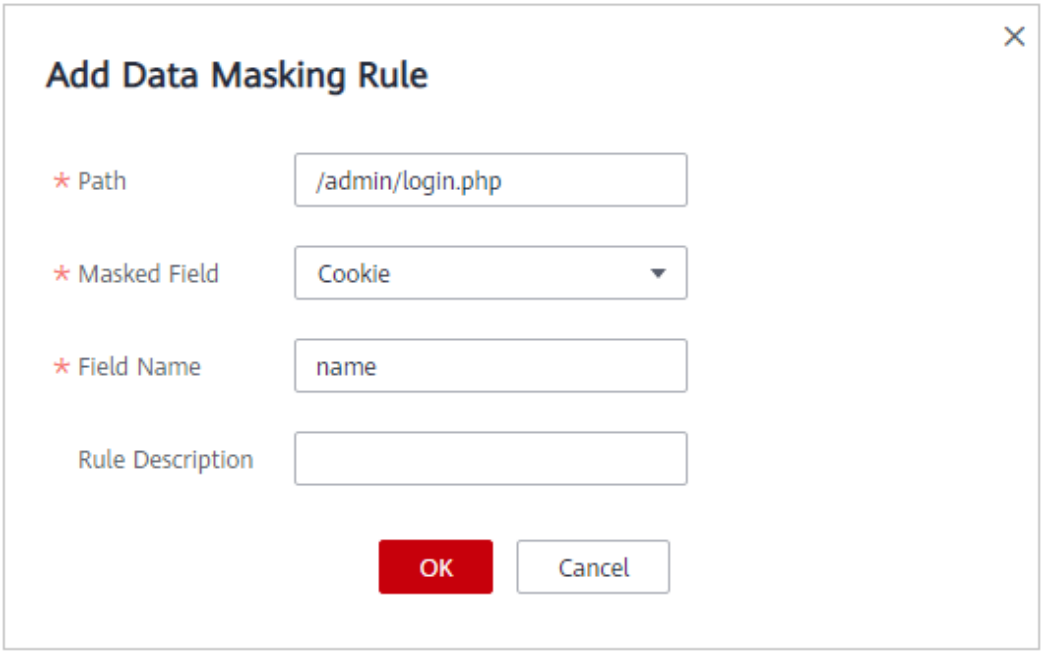
Figura 7-92 Área de configuración de enmascaramiento de datos



Paso 7 En la esquina superior izquierda de la página **Data Masking**, haga clic en **Add Rule**.

Paso 8 En el cuadro de diálogo que se muestra, especifique los parámetros descritos en **Tabla 7-19**.

Figura 7-93 Adición de una regla de enmascaramiento de datos



 Copyright © Huawei Technologies Co., Ltd.

Tabla 7-19 Parámetros de regla

Parámetro	Descripción	Valor de ejemplo
Path	Parte de la URL que no incluye el nombre de dominio. ● Coincidencia de prefijo: La ruta que termina con * indica que la ruta se utiliza como prefijo. Por ejemplo, si la ruta a proteger es **/admin/test.php** o **/adminabc**, establezca **Path** en **/admin***. ● Coincidencia exacta: la ruta que se va a introducir debe coincidir con la ruta que se va a proteger. Si la ruta de acceso que se va a proteger es **/admin**, establezca **Path** en **/admin**. **NOTA** ● La ruta solo admite coincidencias exactas y prefijos y no admite expresiones regulares. ● La ruta de acceso no puede contener dos o más barras diagonales consecutivas. Por ejemplo, ///**admin**. Si introduce///**admin**, WAF converts /// to /.	**/admin/login.php** Por ejemplo, si la URL que se va a proteger es **http://www.example.com/admin/login.php**, establezca **Path** en **/admin/login.php**.
Masked Field	Un conjunto de campos que se va a enmascarar ● **Params**: Un parámetro de solicitud ● **Cookie**: Una pequeña porción de datos para identificar a los visitantes de la web ● **Header**: Un encabezado HTTP definido por el usuario ● **Form**: Un parámetro de formulario	● Si **Masked Field** es **Params** y **Field Name** es **id**, el contenido que coincide con **id** se enmascara. ● Si **Masked Field** es **Cookie** y **Field Name** es **name**, el contenido que coincida con **name** se enmascara.
Field Name	Establezca el parámetro basado en **Masked Field**. El campo enmascarado no se mostrará en los registros. **AVISO** La longitud de un subcampo no puede superar los 2,048 de bytes. Solo se permiten dígitos, letras, guiones bajos (_) y guiones (-).	
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	None

Paso 9 Haga clic en **OK**. La regla de enmascaramiento de datos agregada se muestra en la lista de reglas de enmascaramiento de datos.

Figura 7-94 Lista de reglas de enmascaramiento de datos

Path	Masked Field	Field Name	Rule Status	Added	Rule Description	Operation
/admin/login.php	cookie	name	Enabled	2020/03/30 18:07:17 GMT+08:00	--	Disable Delete Modify

----Fin

 Copyright © Huawei Technologies Co., Ltd.

Otras operaciones

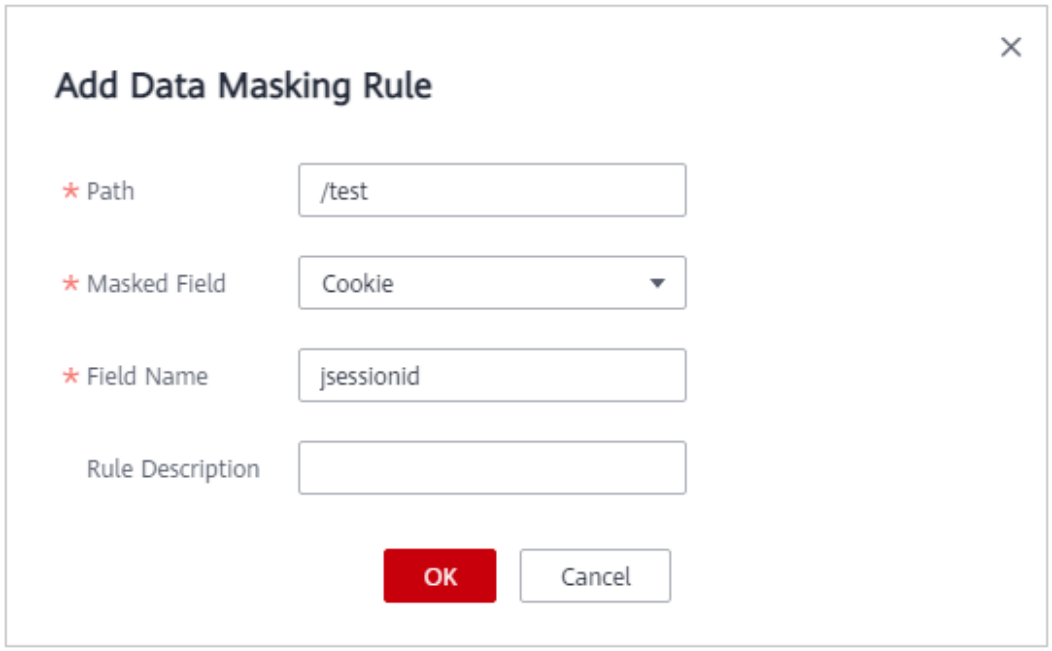
- Para deshabilitar una regla, haga clic en **Disable** en la columna **Operation** de la regla. El **Rule Status** predeterminado es **Enabled**.
- Para modificar una regla, haga clic en **Modify** en la fila que contiene la regla.
- Para eliminar una regla, haga clic en **Delete** en la fila que contiene la regla.

Ejemplo de Configuración - Enmascarar el Campo de Cookie

Para verificar que WAF está protegiendo su nombre de dominio *www.example.com* contra una regla de enmascaramiento de datos (con **Cookie** seleccionada para **Masked Field** y **jsessionid** introducida en **Field Name**):

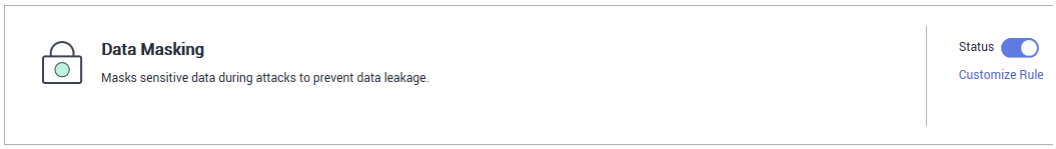
Paso 1 Agregar una regla de enmascaramiento de datos.

Figura 7-95 Seleccione **Cookie** para **Masked Field** e introduzca **jsessionid** en **Field Name**.



Paso 2 Habilitar el enmascaramiento de datos.

Figura 7-96 Área de configuración de enmascaramiento de datos



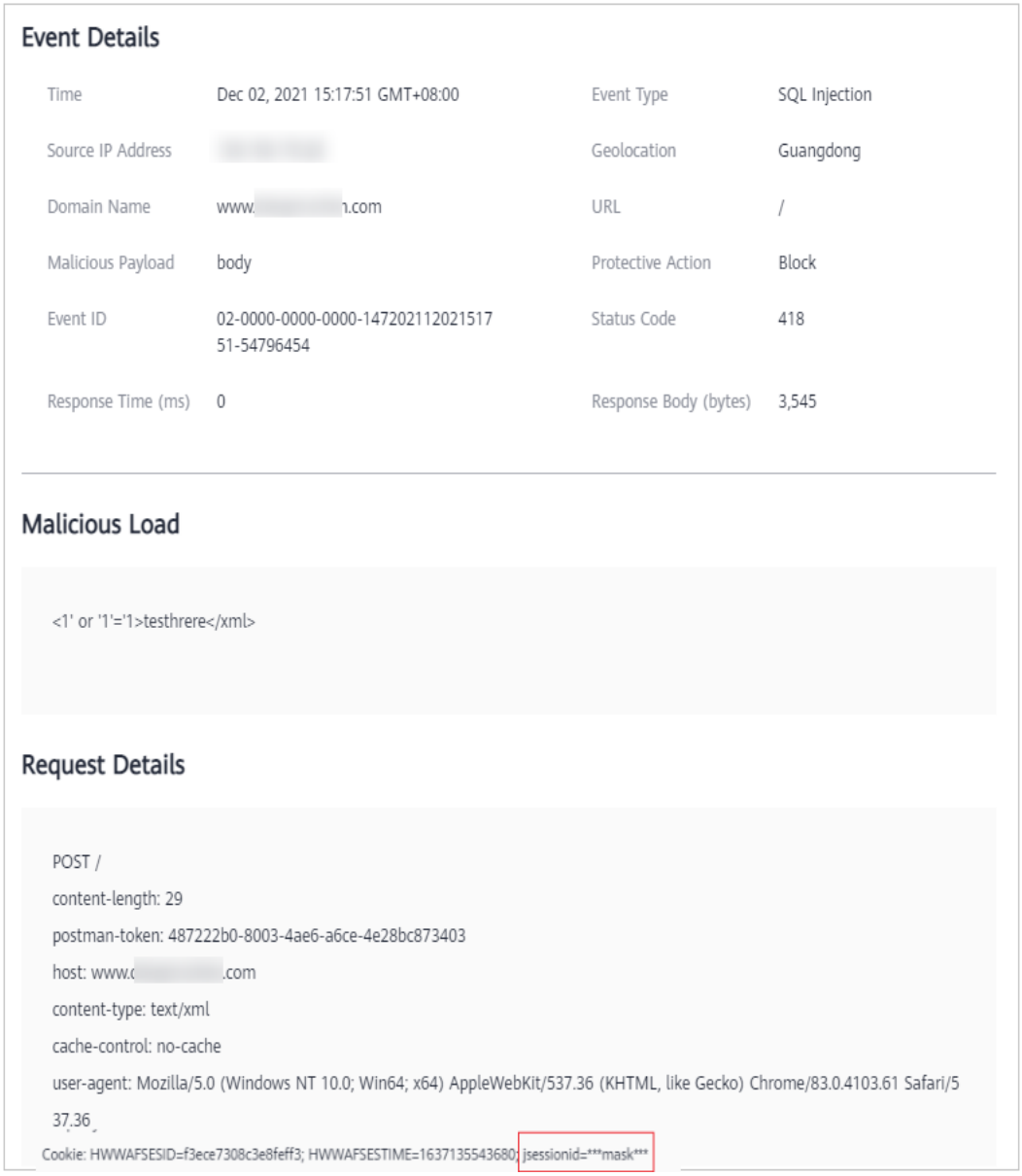
Paso 3 En el panel de navegación de la izquierda, seleccione **Events**.

Paso 4 En la fila que contiene el evento, haga clic en la regla, haga clic en **Details** en la columna **Operation** y vea los detalles del evento.

Los datos en el campo de la cookie **jsessionid** están enmascarados.

 Copyright © Huawei Technologies Co., Ltd.

Figura 7-97 Consulta de eventos - enmascaramiento de datos de privacidad



----Fin

 Copyright © Huawei Technologies Co., Ltd.

8 Panel

En la página **Dashboard**, puede ver los registros de protección de todos los sitios web o instancias protegidos para un intervalo de tiempo específico, incluidos ayer, hoy, pasados 3 días, pasados 7 días o pasados 30 días. En esta página, los registros de eventos se muestran por diferentes dimensiones, incluyendo el número de solicitudes y tipos de ataque, QPS, ancho de banda, código de respuesta, distribución de eventos, top 10 nombres de dominio atacados, top 10 direcciones IP de origen de ataque, top 10 URL atacadas, top 10 ubicaciones de origen de ataque, y las 10 mejores páginas de error.

Las estadísticas de la página **Dashboard** se actualizan cada dos minutos.

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.

Prerrequisitos

- Se ha agregado un nombre de dominio y se ha conectado a WAF.
- La protección WAF está activada.
- Se ha configurado al menos una regla de protección para el nombre de dominio.

Restricciones

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

- CN-Hong Kong
- AP-Bangkok

Limitaciones de la especificación

En la página **Dashboard**, se pueden ver los datos de protección de un máximo de 30 días.

Cómo calcular el QPS

El método de cálculo QPS varía dependiendo del intervalo de tiempo. Para más detalles, consulte **Tabla 8-1**.

 Copyright © Huawei Technologies Co., Ltd.

Tabla 8-1 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.

NOTA

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.

Procedimiento

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 **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

Paso 4 En la parte superior de la página, seleccione un proyecto de la lista desplegable de **Enterprise Project**. A continuación, especifique el sitio web, la instancia y el período de tiempo que desea consultar.

- De forma predeterminada, se muestra la información sobre todos los sitios web que agrega a WAF en todos los proyectos de empresa.
- **Nombres de dominio**: muestra información sobre los nombres de dominio de sitios web agregados a la instancia WAF en el proyecto de empresa seleccionado. Haga clic en **View** para ir a la página **Website Settings** y ver detalles sobre los nombres de dominio de sitios web protegidos.
- Tiempo de consulta: Puede seleccionar **Ayer**, **Hoy**, **Últimos 3 días**, **Últimos 7 días** o **Últimos 30 días**.

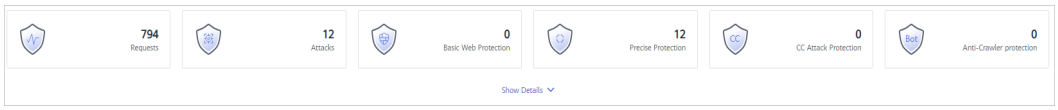
 Copyright © Huawei Technologies Co., Ltd.

Figura 8-1 Proyecto empresarial

Paso 5 Vea el número de solicitudes, ataques y páginas bajo cada tipo de ataque.

- **Requests**: muestra las páginas vistas del sitio web, lo que facilita la visualización del número total de páginas a las que acceden los visitantes en un determinado período de tiempo.
- **Ataques**: muestra cuántas veces se ataca el sitio web.
- Puede ver cuántas páginas son atacadas por un cierto tipo de ataques dentro de un período de tiempo determinado.
- Puede hacer clic en **Show Details** para ver los detalles de los 10 nombres de dominio con la mayor cantidad de solicitudes, ataques y protección web básica, protección precisa, protección contra ataques CC y acciones de protección antocrawler.

Figura 8-2 Estadísticas de acciones de protección

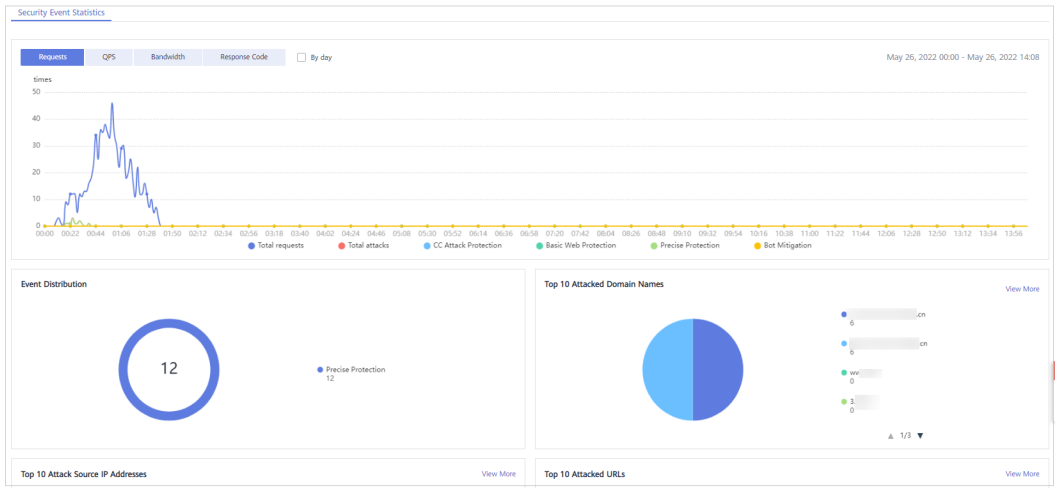


Paso 6 Consulte datos de seguridad en el área **Security Event Statistics**.

Por día: Puede seleccionar esta opción para ver los datos recopilados por día. Si deja esta opción sin seleccionar, tiene las siguientes opciones:

- **Ayer** y **hoy**: Los datos de eventos de seguridad se recopilan cada 2 minutos.
- **Últimos 3 días**: Los datos de eventos de seguridad se recopilan cada 5 minutos.
- **Últimos 7 días**: Los datos de eventos de seguridad se recopilan cada 10 minutos.
- **Últimos 30 días**: los datos de eventos de seguridad se recopilan cada hora.

Figura 8-3 Estadísticas de eventos de seguridad



 Copyright © Huawei Technologies Co., Ltd.

Tabla 8-2 Parámetros en Estadísticas de Eventos de Seguridad

Parámetro	Descripción
Requests	Puede ver cuántas solicitudes de su sitio web, así como el total de ataques y ataques de cada tipo de ataque.
QPS	Número promedio de solicitudes por segundo para el nombre de dominio. Para obtener más información sobre los valores de QPS, consulte **Cómo calcular el QPS**. Consultas por segundo (QPS) indica el número de solicitudes por segundo. Por ejemplo, una solicitud HTTP GET también se denomina consulta.
Bandwidth	Uso de ancho de banda **AVISO** Actualmente, puede ver estadísticas de ancho de banda en las siguientes regiones: ● CN-Hong Kong ● AP-Bangkok
Response Code	Códigos de respuesta devueltos por WAF al cliente o devueltos por el servidor de origen a WAF junto con el número correspondiente de respuestas. Puede hacer clic en **WAF to Client** o **Origin Server to WAF** para ver la información correspondiente. El número de códigos de respuesta se acumula en función de la secuencia de códigos de respuesta (de izquierda a derecha) en la parte inferior del gráfico. El número de códigos de respuesta es la diferencia entre dos líneas. Si el valor de un código de respuesta es 0, la línea del código de respuesta se superpone a la del código de respuesta anterior.
Event Distribution	Tipos de eventos de ataque Haga clic en un área del área **Event Distribution** para ver el tipo, el número y la proporción de un ataque.
Top 10 Attacked Domain Names	Los diez nombres de dominio más atacados y el número de ataques en cada nombre de dominio. Haga clic en **View More** para ir a la página **Events** y ver más datos de protección.
Top 10 Attack Source IP Addresses	Las diez direcciones IP de origen con más ataques y el número de ataques de cada dirección IP de origen. Haga clic en **View More** para ir a la página **Events** y ver más datos de protección.
Top 10 Attacked URLs	Las diez URL más atacadas y el número de ataques en cada URL. Haga clic en **View More** para ir a la página **Events** y ver más datos de protección.

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción
Top 10 Attack Source Locations	Las diez ubicaciones que generan la mayor cantidad de ataques y el número de ataques desde cada ubicación.
Top 10 Error Pages	Los diez sitios web con más excepciones de servicio. Los sitios web con errores **404**, **500**, o **502** pueden ser vistos. Haga clic en **Exception Check** y busque las soluciones correspondientes para rectificar las interrupciones del servicio.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

9 Gestión de Eventos

9.1 Consulta de registros de eventos de protección

En la página **Events**, puede ver los eventos generados por ataques bloqueados y solo ataques registrados. Puede ver los detalles de los eventos WAF, incluida la hora en que se produce un evento, la dirección IP del servidor de origen, la ubicación geográfica de la dirección IP del servidor de origen, la carga maliciosa y la regla de aciertos.

AVISO

- En la consola WAF, puede ver los datos de eventos de todos los nombres de dominio protegidos durante los últimos 30 días. Puede habilitar Log Tank Service (LTS) en WAF para el almacenamiento de registros a largo plazo. En LTS, puede ver los detalles del registro de ataques y acceso. Para más detalles, consulte **Habilitación de LTS para el registro de WAF**.
- Si cambia el modo de trabajo WAF de un sitio web a **Suspended**, WAF solo reenvía todas las solicitudes al sitio web sin inspección. Tampoco registra ningún evento de ataque.
- Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable **Enterprise Project** y ver los registros de eventos de protección en el proyecto.

Prerrequisitos

El sitio web a proteger se ha conectado a WAF.

Procedimiento

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**.

 Copyright © Huawei Technologies Co., Ltd.

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

Paso 5 Haga clic en la pestaña **Search**. En la lista desplegable del sitio web o de la instancia, seleccione un sitio web para ver los registros de eventos correspondientes. El tiempo de consulta puede ser **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, **Past 30 days**, o un rango de tiempo que configure. **Tabla 9-1** enumera los parámetros relacionados.

Figura 9-1 Consulta de eventos de protección

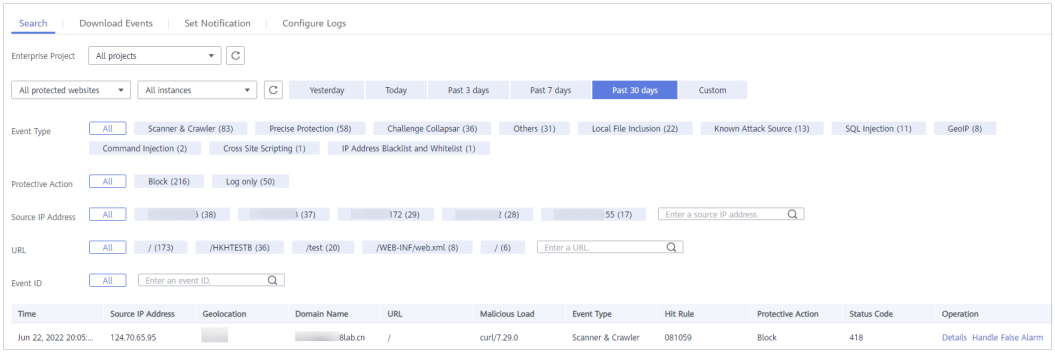


Tabla 9-1 Parámetros de registro

Parámetro	Descripción	Valor de ejemplo
Time	Cuando se produjo el ataque	2021/02/04 13:20:04
Source IP Address	Dirección IP pública del visitante/ ataque de la web	None
Geolocation	Ubicación desde la que se origina la dirección IP del ataque	Shanghai
Domain Name	Nombre de dominio atacado	www.example.com
URL	URL atacada	/admin
Malicious Load	La ubicación o parte del ataque que causa daño o el número de veces que se accedió a la URL. **NOTA** ● En un ataque de CC, la carga maliciosa indica el número de veces que se accedió a la URL. ● Para los eventos de protección de la lista negra, la carga maliciosa se deja en blanco.	id=1 and 1='1
Event Type	Tipo de ataque	SQL injection

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Hit Rule	ID de la regla de protección web básica incorporada afectada por el evento de ataque. Este campo se muestra si el evento de ataque coincide con una de las reglas básicas de protección web. Por ejemplo, ataques de inyección SQL, XSS e inclusión de archivos.	223633
Protective Action	Acciones de protección configuradas en la regla. Las opciones son **Block**, **Log only**, y **Verification code**. **NOTA** 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**.	Block
Status Code	Código de estado HTTP devuelto en la página de bloque.	418

NOTA

Para ver los detalles del evento, haga clic en **Details** en la columna **Operation** de la lista de eventos.

----Fin

9.2 Manejo de falsas alarmas

Si confirma que un evento de ataque en la página **Events** es una falsa alarma, puede manejar el evento como falsa alarma ignorando la URL y el ID de regla en la protección web básica, o eliminando o deshabilitando la regla de protección correspondiente que configuró. Después de que un evento de ataque se maneje como una falsa alarma, el evento ya no se mostrará en la página **Events**. Ya no recibirá ninguna notificación de alarma sobre el evento.

WAF detecta ataques mediante el uso de reglas de protección web básicas integradas, funciones integradas en la protección anti-explotación y reglas personalizadas que ha configurado (como la protección contra ataques CC, la protección de acceso precisa, la lista negra, la lista blanca y las reglas de control de acceso de geolocalización). WAF responderá a los ataques detectados basándose en las acciones de protección (como **Block** y **Log only**) definidas en las reglas y mostrará los eventos de ataque en la página **Events**.

NOTA

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.

 Copyright © Huawei Technologies Co., Ltd.

Prerrequisitos

Hay al menos un evento de falsa alarma en la lista de eventos.

Restricciones

- Solo los eventos de ataque bloqueados o registrados por las reglas básicas de protección web preconfiguradas y las funciones de protección anti-explotación pueden manejarse como falsas alarmas.
- 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.
- Un evento de ataque solo puede ser manejado como una falsa alarma una vez.

Escenarios de aplicación

A veces, las solicitudes de servicio normales pueden ser bloqueadas por WAF. Por ejemplo, supongamos que implementa una aplicación web en un ECS de Huawei Cloud y luego agrega el nombre de dominio público asociado a esa aplicación a WAF. Si habilita la protección web básica para esa aplicación, WAF puede bloquear las solicitudes de acceso que coincidan con las reglas básicas de protección web. Por lo tanto, no se puede acceder al sitio web a través de su nombre de dominio. Sin embargo, todavía se puede acceder al sitio web a través de la dirección IP. En este caso, puede manejar las falsas alarmas para permitir solicitudes de acceso normales a la aplicación.

Impacto en el sistema

El evento de ataque no se mostrará en la página**Events**. Ya no recibirá ninguna notificación de alarma sobre el evento.

Procedimiento

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 **Events**.

Paso 5 Seleccione la pestaña **Search**. Seleccione un sitio web en la lista desplegable **All protected websites**. A continuación, seleccione **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, **Past 30 days** o un intervalo de tiempo personalizado. **Figura 9-2** muestra un ejemplo. **Tabla 9-2** y **Tabla 9-3** describir parámetros.

 Copyright © Huawei Technologies Co., Ltd.

Figura 9-2 Consulta de eventos de protección

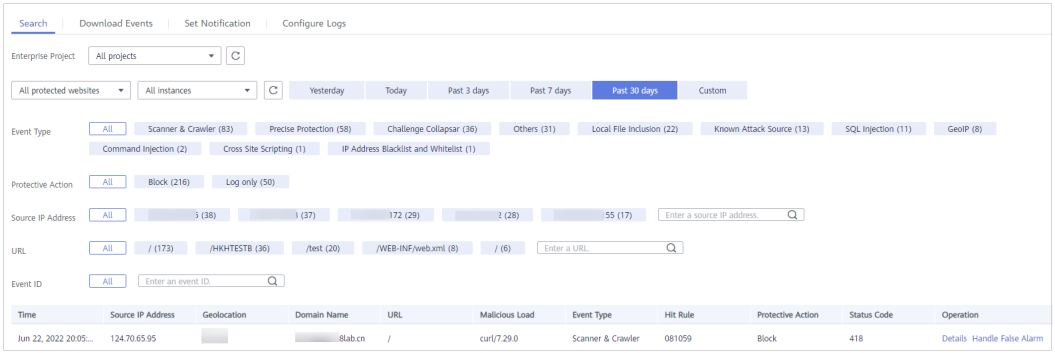


Tabla 9-2 Parámetros del evento

Parámetro	Descripción
Event Type	Tipo de ataque. De forma predeterminada, se selecciona **All**. Puede ver los registros de todos los tipos de ataque o seleccionar un tipo de ataque para ver los registros de ataque correspondientes.
Protective Action	Las opciones son **Block**, **Log only**, y **Verification code**.
Source IP Address	Dirección IP pública del visitante/ataque de la web De forma predeterminada, se selecciona **All**. Puede ver los registros de todas las direcciones IP de origen de ataque, seleccionar una dirección IP de origen de ataque o introducir una dirección IP de origen de ataque para ver los registros de ataque correspondientes.
URL	URL atacada
Event ID	ID del evento

Tabla 9-3 Parámetros de registro

Parámetro	Descripción	Valor de ejemplo
Time	Cuando se produjo el ataque	2021/02/04 13:20:04
Source IP Address	Dirección IP pública del visitante/ ataque de la web	None
Geolocation	Ubicación desde la que se origina la dirección IP del ataque	Shanghai
Domain Name	Nombre de dominio atacado	www.example.com
URL	URL atacada	/admin

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Malicious Load	La ubicación o parte del ataque que causa daño o el número de veces que se accedió a la URL. **NOTA** ● En un ataque de CC, la carga maliciosa indica el número de veces que se accedió a la URL. ● Para los eventos de protección de la lista negra, la carga maliciosa se deja en blanco.	id=1 and 1='1
Event Type	Tipo de ataque	SQL injection
Hit Rule	ID de la regla de protección web básica incorporada afectada por el evento de ataque. Este campo se muestra si el evento de ataque coincide con una de las reglas básicas de protección web. Por ejemplo, ataques de inyección SQL, XSS e inclusión de archivos.	223633
Protective Action	Acciones de protección configuradas en la regla. Las opciones son **Block**, **Log only**, y **Verification code**. **NOTA** 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**.	Block
Status Code	Código de estado HTTP devuelto en la página de bloque.	418

NOTA

Para ver los detalles del evento, haga clic en **Details** en la columna **Operation** de la lista de eventos.

Paso 6 Después de confirmar que un evento es una falsa alarma, haga clic en **Handle False Alarm** en la columna **Operation** de la fila y agregue una regla de enmascaramiento de falsa alarma haciendo referencia a **Tabla 9-4**. **Figura 9-3** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 9-3 Manejo de una falsa alarma

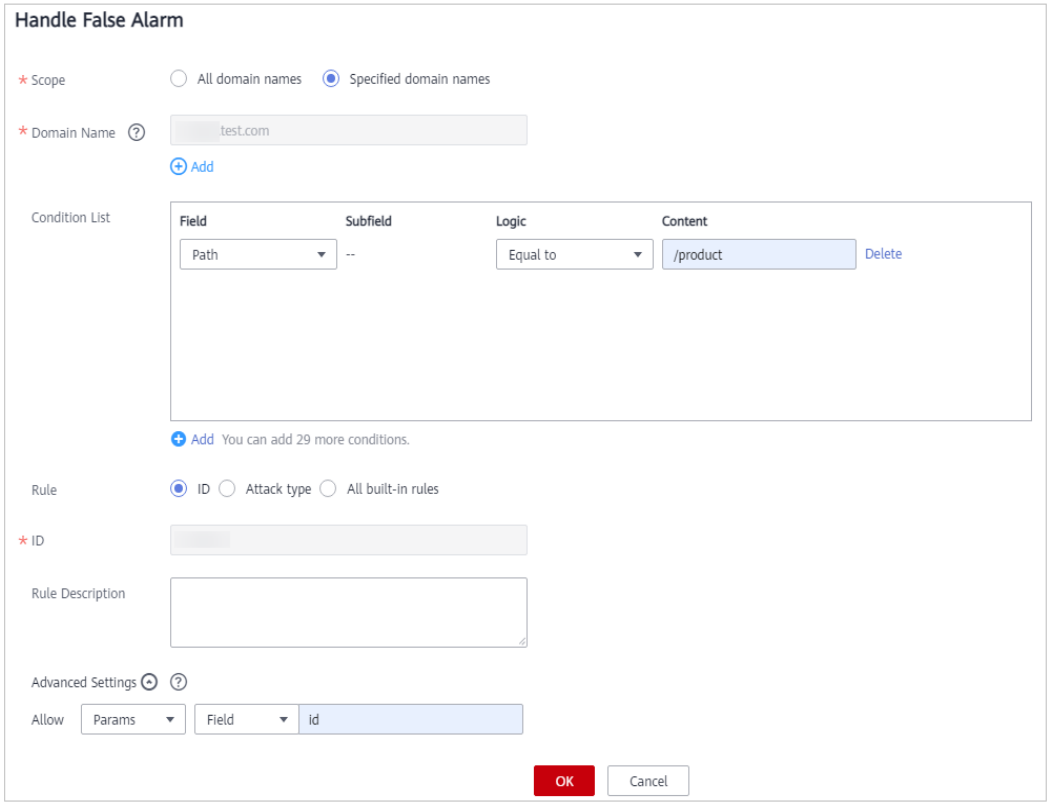


Tabla 9-4 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Domain Name	Nombre de dominio donde se produjo un ataque. WAF llena automáticamente el campo.	None
Path	Parte de la URL (excluyendo el nombre de dominio) para la que se reporta una falsa alarma. El valor predeterminado es la ruta de origen del evento. ● Coincidencia de prefijo: Si selecciona **Prefix is**, la ruta de acceso introducida se utiliza como prefijo. Por ejemplo, si la ruta a proteger es **/admin/test.php** or **/adminabc**, set **Path** to **/admin**. ● Coincidencia exacta: la ruta que se va a introducir debe ser i**gual a** la ruta que se va a proteger. Por ejemplo, si la ruta a proteger es /**admin/test.php**, set **Path** to **/admin/test.php**. **NOTA** ● La ruta soporta prefijo y coincidencias exactas. No se admiten expresiones regulares. ● La ruta de acceso no puede contener dos o más barras diagonales consecutivas. Por ejemplo, /// **admin**. Si introduce///**admin**, WAF converts /// to /.	None

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Rule	El elemento para el que tiene efecto la regla de enmascaramiento de falsa alarma. Las opciones son: ● **ID**: Configure las reglas por ID de la regla de hit. ● **Attack type**: Configure la regla por tipo de ataque. ● **All built-in rules**: todas las comprobaciones habilitadas en **Protección web básica**.	Attack type
ID	ID de una regla integrada, que se lee automáticamente. Este parámetro es obligatorio cuando **Rule** se establece en **ID**.	060015
Attack Type	Tipo de ataque obtenido automáticamente. Este parámetro es obligatorio cuando **Rule** se establece en **Attack type**.	Remote File Inclusion
Rule Description	Una breve descripción de la regla. Este parámetro es opcional.	SQL injection attacks are not intercepted.
Advanced Settings	Para ignorar los ataques de un campo específico, especifique el campo en el área **Advanced Settings**. Después de agregar la regla, WAF dejará de bloquear los eventos de ataque del campo especificado. Seleccione un campo de destino en el primer cuadro de lista desplegable de la izquierda. Se admiten los siguientes campos: **Params**, **Cookie**, **Header**, **Body**, y **Multipart**. ● Si selecciona **Params**, **Cookie**, o **Header**, configure los subcampos según sea necesario. ● Si selecciona **Cookie**, el **Domain Name** y **Path** pueden estar vacíos. **NOTA** Si se selecciona **All**, WAF no bloqueará todos los eventos de ataque del campo seleccionado.	Params All

Paso 7 Haga clic en **OK**.

----Fin

Verificación

Una falsa alarma se eliminará en aproximadamente un minuto después de que se haya realizado la configuración de manejo. Ya no se mostrará en la lista de detalles de eventos de ataque. Puede borrar la caché, actualizar el navegador y acceder de nuevo a la página para verificar si la alarma se ha manejado correctamente.

 Copyright © Huawei Technologies Co., Ltd.

Otras operaciones

Si un evento se maneja como una falsa alarma, la regla correspondiente se agregará a la lista de reglas de enmascaramiento de falsas alarmas. Puede ver, deshabilitar, eliminar o modificar la regla en la página **False Alarm Masking** en **Policies**. Para más detalles, consulte **Configuración de una regla de enmascaramiento de falsa alarma**.

9.3 Descarga de datos de eventos

En este tema se describe cómo descargar datos de eventos (eventos registrados y bloqueados) durante los últimos cinco días. Uno o más archivos CSV que contienen los datos de eventos del día actual se generarán al comienzo del día siguiente.

NOTA

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 **Enterprise Project** y descargar los registros de eventos de protección en el proyecto.

Prerrequisitos

- El sitio web a proteger se ha agregado a WAF.
- Se ha generado un archivo de evento.

Limitaciones de la especificación

- El número máximo de eventos en un archivo es de 10,000. Si hay más de eventos de 10,000 se genera otro archivo.
- Solo los datos de eventos de los últimos cinco días se pueden descargar a través de la consola WAF.

Procedimiento

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 **Events**.

Paso 5 Haga clic en la pestaña **Download Events** y descargue los datos de protección deseados. **Tabla 9-5** describe los parámetros.

Tabla 9-5 Descripción del parámetro

Parámetro	Descripción
File Name	El formato es *file-name*.**csv**.

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción
Number of Events	Número total de eventos bloqueados y registrados **NOTA** El número máximo de eventos en un archivo es de 10,000. Si hay más de eventos de 10,000 se genera otro archivo.

Paso 6 En la columna **Operation**, haga clic en **Download** para descargar datos al PC local.

----Fin

Campos en un archivo de datos de eventos de protección

Campo	Descripción	Valor de ejemplo
action	Medidas de protección adoptadas en respuesta al evento	block
attack	Tipo de ataque	SQL Injection
body	Solicitar contenido del ataque	N/A
cookie	Cookie del atacante	N/A
headers	Encabezado del atacante	N/A
host	Nombre de dominio o dirección IP del sitio web protegido	www.example.com
id	ID del evento.	02-11-16-20201121060347-feb42002
payload	La parte del ataque que causa daños al sitio web protegido	python-requests/2.20.1
payload_location	La ubicación del ataque que causa daño o el número de veces que el atacante accede a la URL	user-agent
policyid	ID de política.	d5580c8f6cd4403ebbf85892d4bbb8e4
request_line	Línea de solicitud del ataque	GET /
rule	ID de la regla contra la que se genera el evento.	81066
sip	Dirección IP pública del visitante/ataque de la web	N/A
time	Cuando se produjo el evento.	2020/11/21 0:20:44
url	URL del nombre de dominio protegido	N/A

 Copyright © Huawei Technologies Co., Ltd.

Otras operaciones

Habilite LTS en WAF para el almacenamiento de registros a largo plazo. En LTS, puede ver los detalles del registro de ataques y acceso. Para más detalles, consulte **Habilitación de LTS para el registro de WAF**.

 Copyright © Huawei Technologies Co., Ltd.

10 Habilitación de LTS para el registro de WAF

Después de autorizar a WAF a acceder a Log Tank Service (LTS), puede utilizar los registros WAF registrados por LTS para un análisis rápido y eficiente en tiempo real, la gestión de la operación del dispositivo y el análisis de las tendencias del servicio.

LTS analiza y procesa un gran número de registros. Le permite procesar registros en tiempo real, de manera eficiente y segura. 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.

AVISO

- 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.
- LTS se factura por el tráfico y se factura por separado de WAF. Para obtener más información sobre los precios de LTS, consulte **Detalles de precios de LTS**.
- 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 **Enterprise Project** y configurar el registro WAF.

Prerrequisitos

- Usted ha comprado una instancia WAF.
- El sitio web a proteger se ha agregado a WAF.

Restricciones

Puede habilitar LTS para el registro WAF en las siguientes regiones: CN-Hong Kong, AP-Bangkok,, y AP-Singapur.

 Copyright © Huawei Technologies Co., Ltd.

Impacto en el sistema

Habilitación de LTS para WAF no afecta al rendimiento de WAF.

Habilitación de LTS para registro de eventos de protección WAF

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 **Events**.

Paso 5 Haga clic en la pestaña **Configure Logs**, habilite el ( ), LTS y seleccione un grupo de registro y un flujo de registro. **Tabla 10-1** describe los parámetros.

Figura 10-1 Configuración de registros

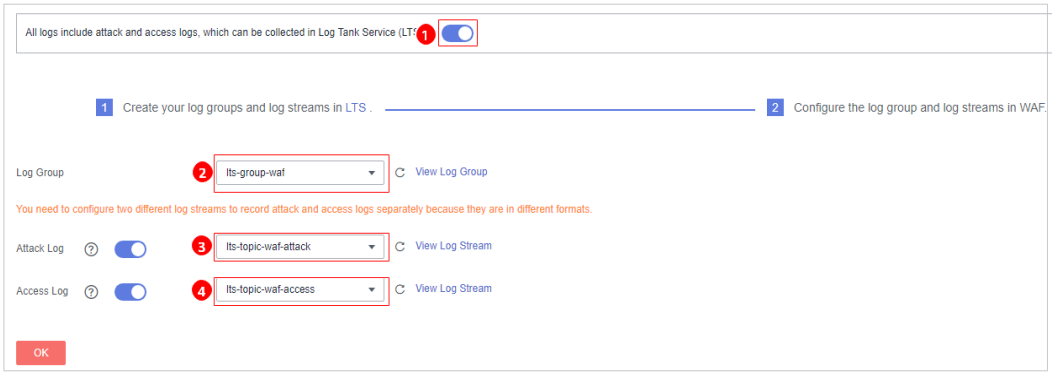


Tabla 10-1 Configuración de registros

Parámetro	Descripción	Valor de ejemplo
Log Group	Seleccione un grupo de registros o haga clic en **View Log Group** para ir a la consola LTS y crear un grupo de registros.	lts-grupo-waf
Attack Log	Seleccione un flujo de registro o haga clic en **View Log Stream** para ir a la consola LTS y crear un flujo de registro. Un registro de ataque incluye información sobre el tipo de evento, la acción de protección y la dirección IP de origen de ataque de cada ataque.	lts-topic-waf-attack

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción	Valor de ejemplo
Access Log	Seleccione un flujo de registro o haga clic en **View Log Stream** para ir a la consola LTS y crear un flujo de registro. Un registro de acceso incluye información clave sobre el tiempo de acceso, la dirección IP del cliente y la URL de recursos de cada solicitud de acceso HTTP.	lts-topic-waf-access

Paso 6 Haga clic en **OK**.

Puede ver los registros de eventos de protección WAF en la consola LTS.

----Fin

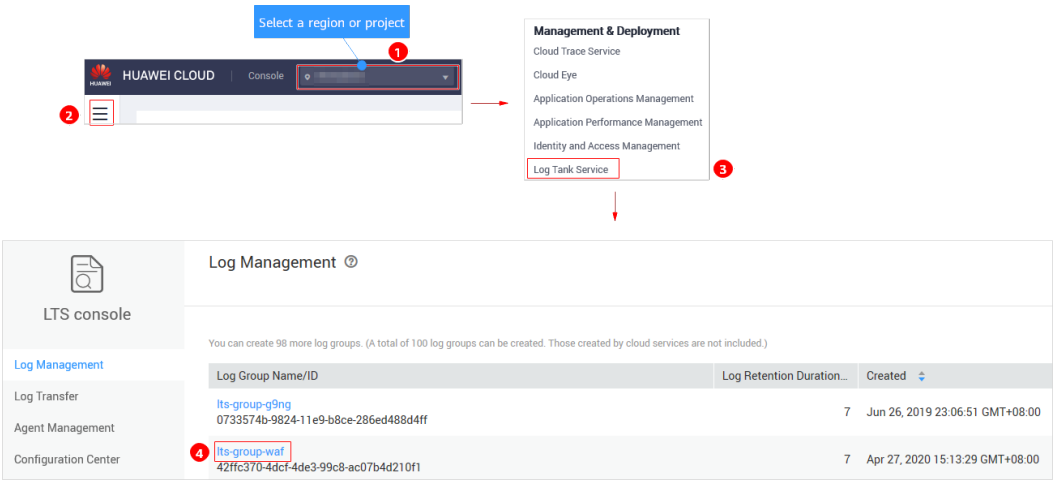
Consulta de registros de eventos de protección WAF en LTS

Después de habilitar LTS, realice los siguientes pasos para ver y analizar los registros WAF en la consola LTS.

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

Paso 2 Vaya a la página de flujo de registro siguiendo los pasos que se muestran en **Figura 10-2**.

Figura 10-2 Acceso a la página de gestión de registros

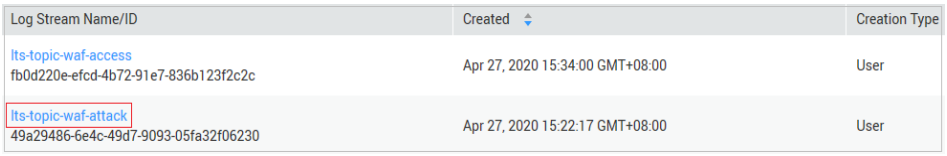


Paso 3 Vea los registros de eventos de protección.

- Vea los registros de ataques.
  a. En la lista de flujos de registro, haga clic en el nombre del flujo de registro (por ejemplo, **lts-topic-waf-attack**) configurado para los registros de ataques.

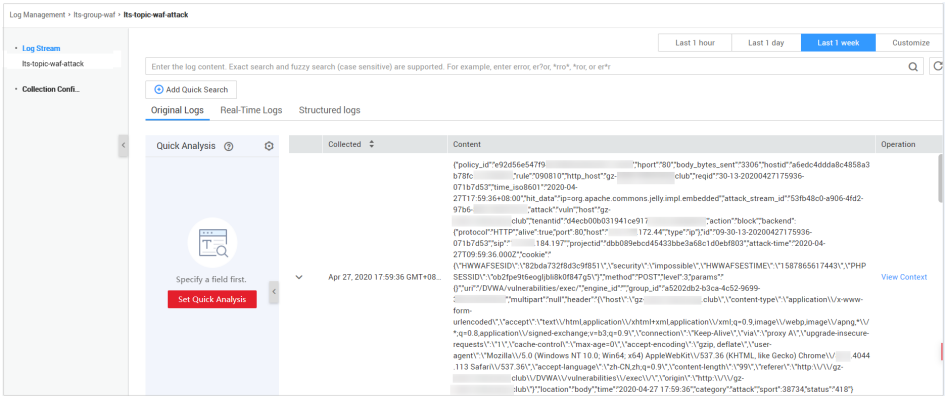
 Copyright © Huawei Technologies Co., Ltd.

Figura 10-3 Nombre del flujo de registro configurado para los registros de ataques



b. Vea los registros de ataques. **Figura 10-4** muestra un ejemplo.

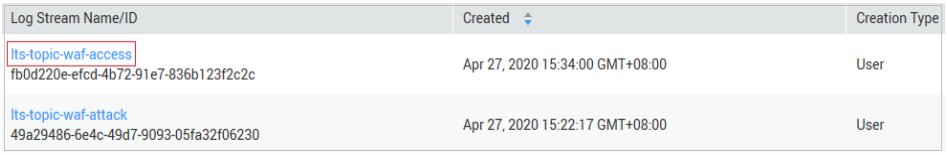
Figura 10-4 Consulta de registros de ataques



- Ver registros de acceso.

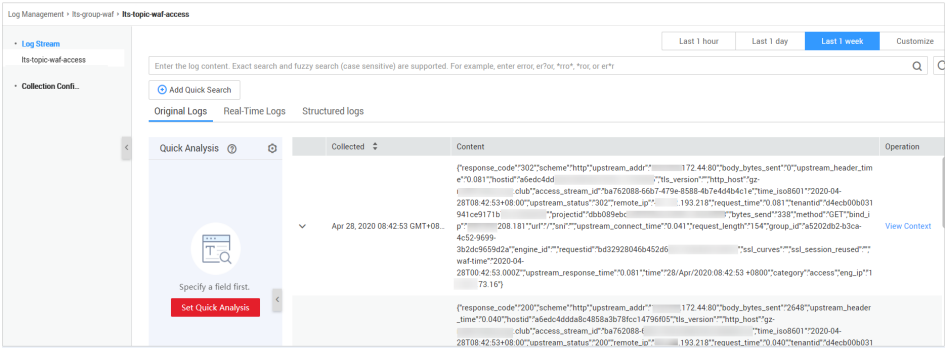
a. En la lista de flujos de registro, haga clic en el nombre del flujo de registro (por ejemplo, **lts-topic-waf-access**) configurado para los registros de acceso.

Figura 10-5 Nombre del flujo de registro configurado para los registros de acceso



b. Ver registros de acceso. **Figura 10-6** muestra un ejemplo.

Figura 10-6 Consulta de registros de acceso



----Fin

 Copyright © Huawei Technologies Co., Ltd.

Campo de WAF access_log

Campo	Tipo	Descripción de campo	Descripción
requestid	string	ID aleatorio	El valor es el mismo que los últimos ocho caracteres del campo **req_id** en el registro de ataques.
time	string	Tiempo en que se recibe una solicitud de acceso.	GMT hora en que se genera un registro.
eng_ip	string	Dirección IP del motor WAF	-
hostid	string	Identificador de nombre de dominio de la solicitud de acceso.	ID de nombre de dominio protegido (upstream_id).
tenantid	string	ID de cuenta	Su cuenta
projectid	string	ID del proyecto al que pertenece el nombre de dominio protegido	ID de proyecto de un usuario en una región específica.
remote_ip	string	Dirección IP desde la que se origina una solicitud de cliente.	Dirección IP desde la que se origina una solicitud de cliente. **AVISO** Si se implementa un proxy de capa 7 delante de WAF, este campo indica la dirección IP del nodo proxy más cercano a WAF. La dirección IP real del visitante se especifica mediante los campos **x-forwarded-for** y **x_real_ip**.
x-forwarded-for	string	Una cadena de direcciones IP para un proxy cuando el proxy se implementa delante de WAF.	El sting incluye una o más direcciones IP. La dirección IP más a la izquierda es la dirección IP de origen del cliente. Cada vez que el servidor proxy recibe una solicitud, añade la dirección IP de origen de la solicitud a la derecha de la dirección IP de origen.

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
x_real_ip	string	Dirección IP real del cliente cuando se implementa un proxy delante de WAF.	Dirección IP real del cliente, que es identificada por el proxy.
cdn_src_ip	string	Dirección IP del cliente identificada por CDN cuando CDN se implementa delante de WAF	Este campo especifica la dirección IP real del cliente si CDN se implementa delante de WAF. **AVISO** Algunos proveedores de CDN pueden usar otros campos. WAF registra solo los campos más comunes.
scheme	string	Solicitud de protocolo	Protocolos que se pueden utilizar en la solicitud: ● HTTP ● HTTPS
response_code	string	Código de respuesta	Código de estado de respuesta devuelto por el servidor de origen a WAF.
method	string	Método de solicitud.	Tipo de solicitud en una línea de solicitud. Generalmente, el valor es **GET** o **POST**.
http_host	string	Nombre de dominio del servidor solicitado.	Dirección, nombre de dominio o dirección IP introducida en el cuadro de direcciones de un navegador.
url	string	URL de solicitud.	Ruta de acceso en una URL (excluyendo el nombre de dominio).
request_length	string	Longitud de solicitud.	La longitud de la solicitud incluye la dirección de la solicitud de acceso, el encabezado de la solicitud HTTP y el número de bytes en el cuerpo de la solicitud.
bytes_send	string	Número total de bytes enviados al cliente.	Número de bytes enviados por WAF al cliente.

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
body_bytes_sent	string	Número total de bytes del cuerpo de respuesta enviado al cliente	Número de bytes del cuerpo de respuesta enviado por WAF al cliente
upstream_addr	string	Dirección del servidor backend.	Dirección IP del servidor de origen para el que está destinada una solicitud. Por ejemplo, si WAF reenvía solicitudes a un ECS, la dirección IP del ECS se devuelve a este parámetro.
request_time	string	Solicitar tiempo de procesamiento	El tiempo de procesamiento comienza cuando se lee el primer byte del cliente.
upstream_response_time	string	Tiempo de respuesta del servidor backend.	Hora en que el servidor backend responde a la solicitud WAF.
upstream_status	string	Código de respuesta del servidor backend.	Código de estado de respuesta devuelto por el servidor backend a WAF.
upstream_connect_time	string	Tiempo transcurrido para que los servidores de origen se conecten a los servidores backend	Tiempo para que el servidor de origen establezca una conexión con sus servidores backend. Si el servicio backend utiliza un protocolo de encriptación, este parámetro incluye el tiempo de establecimiento de enlace.
upstream_header_time	string	Tiempo utilizado por el servidor backend para recibir el primer byte del encabezado de respuesta.	-
bind_ip	string	Dirección IP de origen del motor WAF.	Dirección IP de Back-to-source utilizada por el motor WAF.

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
group_id	string	ID de grupo de registro LTS	ID del grupo de registro para interconectar WAF con LTS.
access_stream_id	string	ID de flujo de registro.	ID del **access_stream** del usuario en el grupo de registro identificado por el campo **group_id**.
engine_id	string	ID del motor WAF	Identificación única del motor WAF.
time_iso8601	string	Formato de tiempo ISO 8601 de los registros.	-
sni	string	Nombre de dominio solicitado a través del SNI.	-
tls_version	string	Versión del protocolo para establecer una conexión SSL.	Versión TLS utilizada en la solicitud.
ssl_curves	string	Lista de grupos de curvas admitida por el cliente.	-
ssl_session_reused	string	Reutilización de sesión SSL	Si se puede reutilizar la sesión SSL **r**: Sí **.**: No
process_time	string	Duración de la detección	-

 Copyright © Huawei Technologies Co., Ltd.

Descripción del campo de registro de solicitud WAF

Campo	Tipo	Descripción de campo	Descripción
scheme	string	Solicitud de protocolo	Protocolos que se pueden utilizar en la solicitud: ● HTTP ● https
hport	string	Puerto de escucha para el motor	-
body_bytes_sent	string	Número total de bytes del cuerpo de respuesta enviado al cliente.	-
hostid	string	ID de nombre de dominio protegido (upstream_id).	-
time_iso8601	string	Formato de tiempo ISO 8601 de los registros.	-
host	string	Nombre de dominio del servidor solicitado.	-
tenantid	string	ID de cuenta	-
inet_ip	string	Dirección IP del motor	-
backend.protocol	string	Protocolo de back-end actual	-
backend.alive	string	Estado actual del backend	-
backend.port	string	Puerto de back-end actual	-
backend.host	string	Valor actual del host backend	-
backend.type	string	Tipo de host de backend actual	Tipo del host de backend. Puede ser un nombre de dominio o una dirección IP.
id	string	ID de solicitud	Los últimos ocho caracteres son los mismos que los primeros ocho caracteres de **requestid** el registro de acceso.

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
sip	string	Dirección IP desde la que se origina una solicitud de cliente.	-
sport	string	Puerto utilizado por la dirección IP desde la que se origina una solicitud de cliente.	-
projectid	string	ID del proyecto al que pertenece el nombre de dominio protegido	-
cookie	string	Cookie	-
method	string	Método de solicitud.	-
uri	string	Solicitud de URI	-
request_stream_id	string	ID de flujo de registro	ID de **request_stream** del usuario en el grupo de registro identificado por el campo **group_id**.
group_id	string	ID del grupo de registros	ID de grupo de registro LTS
engine_id	string	Identificación única del motor	-
header	string	Contenido del encabezado	-
time	string	Fecha y hora del registro	-
category	string	Categoría del registro	El valor es **request**.
status	string	Código de respuesta	-

 Copyright © Huawei Technologies Co., Ltd.

Descripción del campo de WAF attack_log

Campo	Tipo	Descripción de campo	Descripción
category	string	Categoría del registro	El valor es **attack**.
time	string	Fecha y hora del registro	-
time_iso8601	string	Formato de tiempo ISO 8601 de los registros.	-
policy_id	string	ID de política	-
level	string	Nivel de protección	Nivel de protección de una regla integrada en la protección web básica ● **1**: Bajo ● **2**: Medio ● **3**: Alto

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
attack	string	Tipo de ataque	Tipo de ataque. Este parámetro solo se muestra en los registros de ataques. ● **default**: ataques predeterminados ● **sqli**: Inyecciones SQL ● **xss**: ataques de secuencias de comandos entre sitios (XSS) ● **webshell**l: shells web ● **robot**: rastreadores maliciosos ● **cmdi**: inyecciones de comando ● **rfi**: ataques de inclusión de archivos remotos ● **lfi**: ataques de inclusión de archivos locales ● **ilegal**: solicitudes no autorizadas ● **vuln**: vulnerabilidades ● **cc**: ataques que golpean las reglas de protección CC ● **custom_custom**: ataques que alcanzan una regla de protección precisa ● **custom_whiteip**: ataques que golpean una regla de lista negra o blanca de direcciones IP ● **custom_geoip**: ataques que golpean una regla de control de acceso de geolocalización ● **antitamper**: ataques que golpean una regla de protección contra manipulaciones web ● **anticrawler**: ataques que golpean el JS desafían la regla anti-crawler ● **leakage**: vulnerabilidades que afectan a una regla de prevención de fugas de información ● **followed_action**: ataques que golpean una regla de origen de ataque conocida
action	string	Acción protectora	Acción de defensa WAF. ● **block**: WAF bloquea los ataques. ● **log**: WAF solo registra los ataques detectados. ● **captcha**: Código de verificación

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
sub_type	string	Tipos de crawlers	Cuando **attack** se establece en **robot**, este parámetro no se puede dejar en blanco. ● **script_tool**: Herramientas de script ● **search_engine**: Motores de búsqueda ● **scanner:** Herramientas de escaneo ● **uncategorized**: Otros rastreadores
rule	string	ID de la regla activada o la descripción del tipo de política personalizada.	-
location	string	Ubicación que desencadena la carga maliciosa	-
hit_data	string	Cadena que desencadena la carga maliciosa	-
resp_headers	string	Encabezado de respuesta	-
resp_body	string	Cuerpo de respuesta	-
backend	string	Dirección del servidor backend al que se reenvía la solicitud.	-
status	string	Código de estado de respuesta	-
reqid	string	ID aleatorio	-
id	string	ID de ataque	ID del ataque
method	string	Método de solicitud	-
sip	string	Dirección IP de solicitud del cliente	-
sport	string	Puerto de solicitud del cliente	-

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
host	string	Nombre de dominio solicitado	-
http_host	string	Nombre de dominio del servidor solicitado.	-
hport	string	Puerto del servidor solicitado.	-
uri	string	URL de solicitud.	El dominio está excluido.
header	A JSON string. A JSON table is obtained after the string is decoded.	Encabezado de la solicitud	-
mutipart	A JSON string. A JSON table is obtained after the string is decoded.	Solicitar encabezado multiparte	Este parámetro se utiliza para cargar archivos.

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
cookie	A JSON string. A JSON table is obtained after the string is decoded.	Cookie de la solicitud	-
params	A JSON string. A JSON table is obtained after the string is decoded.	Valor de los parámetros que sigue al URI de solicitud.	-
body_bytes_sent	string	Número total de bytes del cuerpo de respuesta enviado al cliente.	Número total de bytes del cuerpo de respuesta enviado por WAF al cliente.
upstream_response_time	string	Tiempo de respuesta del servidor backend.	-
process_time	string	Duración de la detección	-
engine_id	string	Identificación única del motor	-
group_id	string	ID del grupo de registros	ID de grupo de registro LTS
attack_stream_id	string	ID de flujo de registro	ID del **access_stream** del usuario en el grupo de registro identificado por el campo **group_id**.
hostid	string	ID de nombre de dominio protegido (upstream_id).	-

 Copyright © Huawei Technologies Co., Ltd.

Campo	Tipo	Descripción de campo	Descripción
tenantid	string	ID de cuenta	-
projectid	string	ID del proyecto al que pertenece el nombre de dominio protegido	-

 Copyright © Huawei Technologies Co., Ltd.

11 Habilitación de notificaciones de alarma

En este tema se describe cómo habilitar las notificaciones para los registros de ataques. Una vez habilitada esta función, WAF le envía notificaciones por SMS o correo electrónico si se detecta un ataque.

NOTA

- Simple Message Notification (SMN) es un servicio de pago. Para obtener más información, consulte **Detalles de Precios del producto**.
- Antes de configurar la notificación de alarma, cree un tema de mensaje en el servicio SMN como administrador. Para obtener más información, consulte **Antes de publicación de un mensaje**.
- 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 **Enterprise Project** y activar las notificaciones de alarma.

Prerrequisitos

Se ha habilitado el SMN.

Restricciones

Las notificaciones de alarma se envían si el número de ataques es al menos igual al umbral configurado para un período determinado.

Procedimiento

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 **Events**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 5 Haga clic en la pestaña **Set Notification** y configure los parámetros de notificación de alarma haciendo referencia a **Tabla 11-1**. **Figura 11-1** muestra un ejemplo.

Figura 11-1 Configuración de notificaciones de alarma

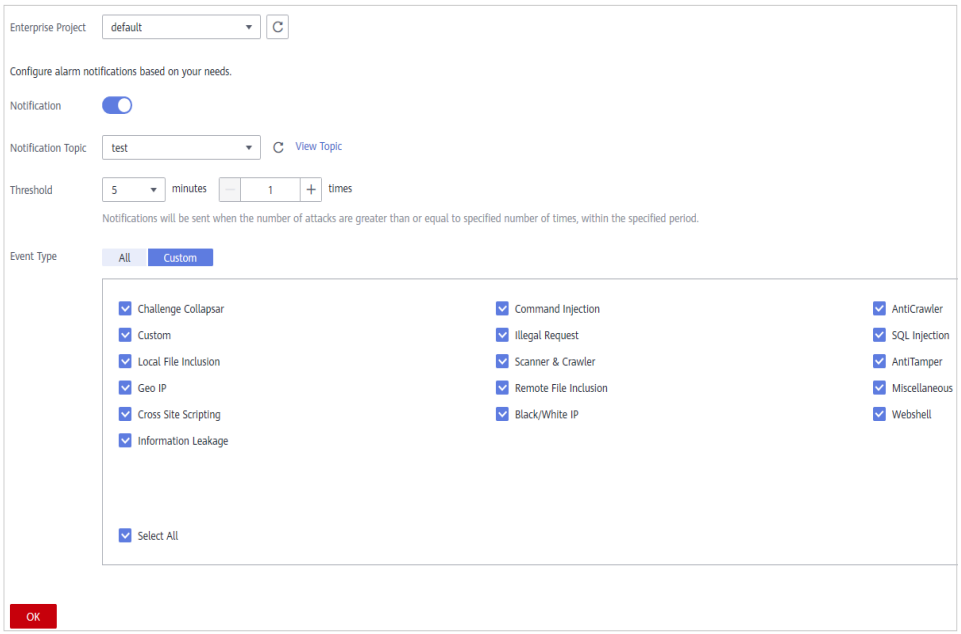


Tabla 11-1 Descripción de los parámetros de configuración de notificación

Parámetro	Descripción
Notification	Si la notificación de alarma está activada. ● : habilitado. ● : deshabilitado.
Notification Topic	Seleccione un tema de la lista desplegable. Si no hay temas, haga clic en **View Topic** y siga los pasos siguientes para crear un tema: 1. Crear un tema. Para obtener más información, consulte **Creación de un tema**. 2. Agregue una o más suscripciones al tema. Deberá proporcionar un número de teléfono, dirección de correo electrónico, función, punto final de aplicación de plataforma, punto final DMS o punto final HTTP/HTTPS para recibir notificaciones de alarma. Para obtener más información, consulte **Adición de una suscripción**. 3. Confirme la suscripción. Después de agregar la suscripción, confirme la suscripción. Para obtener más información sobre temas y suscripciones, consulte la *Guía de usuario de Simple Message Notification*.

 Copyright © Huawei Technologies Co., Ltd.

Parámetro	Descripción
Threshold	Umbral de alarma. **NOTA** Las notificaciones de alarma se envían cuando el número de ataques es mayor o igual al umbral dentro del período configurado.
Event Type	De forma predeterminada, se selecciona **All**. Para especificar los tipos de eventos, haga clic en **Custom**.

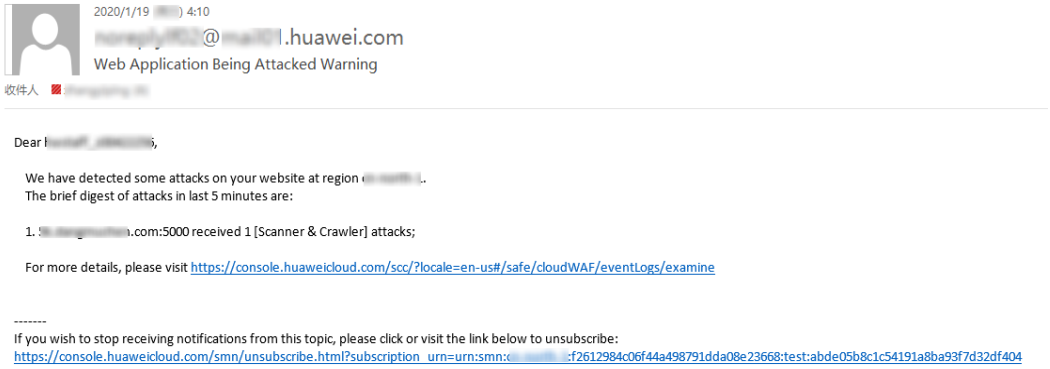
Paso 6 Haga clic en **OK**.

----Fin

Ejemplo de correo electrónico de notificación de alarma

Si ha habilitado las notificaciones de alarma y configurado las notificaciones de alarma por correo electrónico, WAF le informa por correo electrónico de cualquier ataque que ocurra. **Figura 11-2** muestra un ejemplo de un correo electrónico de notificación de alarma.

Figura 11-2 Correo electrónico de notificación de alarma



 Copyright © Huawei Technologies Co., Ltd.

12 Gestión de políticas

12.1 Agregar una política

Una política es una combinación de reglas, como la protección web básica, la lista negra, la lista blanca y las reglas de protección precisas. Una política se puede aplicar a varios nombres de dominio, pero solo se puede utilizar una política para un nombre de dominio. En este tema se describe cómo agregar una política a la instancia WAF.

NOTA

Si ha habilitado proyectos de empresa, puede seleccionar su proyecto de empresa en la lista desplegable **Enterprise Project** y agregar políticas de protección en el proyecto.

Prerrequisitos

Se ha agregado un nombre de dominio a WAF. Ha seleccionado **Cloud mode** o **Dedicated mode** para la implementación del sitio web.

Restricciones

Esta función no está disponible en la edición estándar (anteriormente edición profesional).

Un nombre de dominio de un sitio web protegido solo puede usar una política.

Procedimiento

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, elija **Policies**.

Paso 5 En la esquina superior izquierda, haz clic en **Add Policy**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 6 En el cuadro de diálogo que se muestra, escriba el nombre de la política y haga clic en **Confirm**. La política agregada se mostrará en la lista de políticas.

Paso 7 En la columna **Policy Name**, haga clic en el nombre de la política. En la página mostrada, agregue reglas a la política haciendo referencia a **Configuraciones de reglas**.

----Fin

Otras operaciones

- Para modificar un nombre de política, haga clic en junto al nombre de política. En el cuadro de diálogo que se muestra, escriba un nuevo nombre de política.
- Para eliminar una regla, haga clic en **Delete** en la fila que contiene la regla.

12.2 Adición de reglas a una o más políticas

En este tema se describe cómo agregar reglas a una o más políticas.

NOTA

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 **Enterprise Project** y configurar las políticas de protección para los nombres de dominio en lotes.

Prerrequisitos

Se ha agregado un nombre de dominio a WAF. Ha seleccionado **Cloud mode** o **Dedicated mode** para la implementación del sitio web.

Procedimiento

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, elija **Policies**.

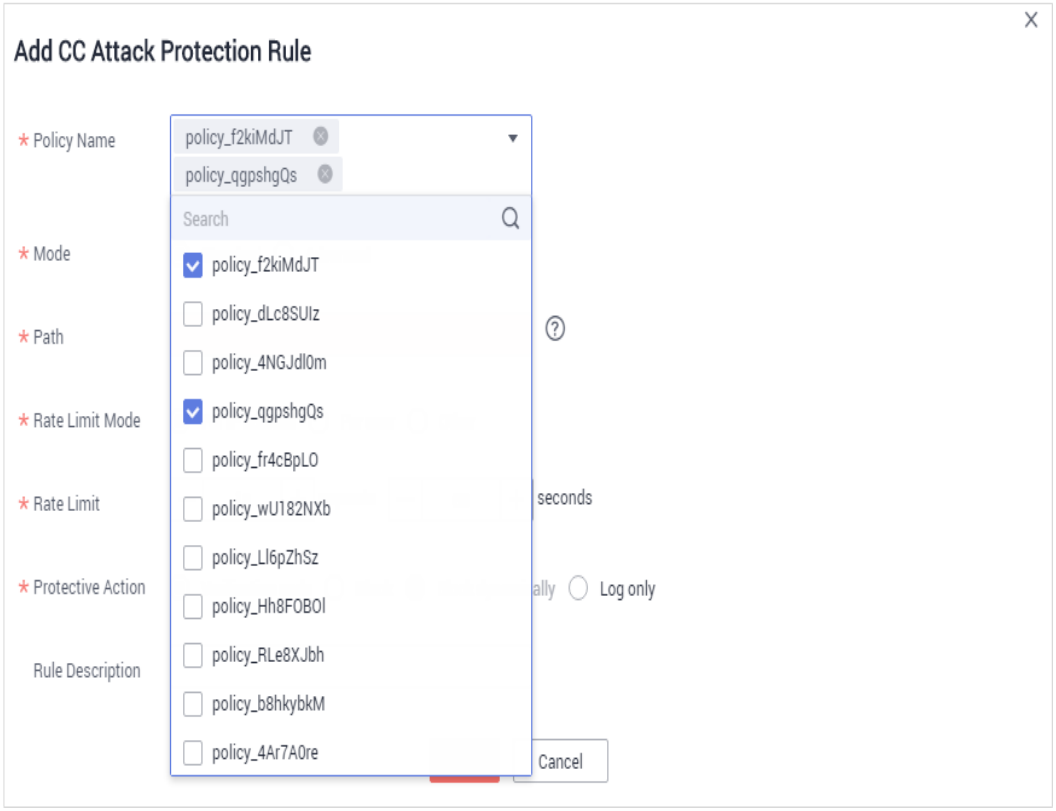
Paso 5 En la esquina superior izquierda de la página, haga clic en **View Rules**.

Paso 6 En la esquina superior izquierda, encima de una regla que se va a agregar, haga clic en **Add Rule**.

Paso 7 Seleccione una o más directivas en la lista desplegable **Policy Name**. **Figura 12-1** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 12-1 Adición de una regla a una o más políticas



Paso 8 Establezca otros parámetros.

- Para agregar una regla de protección contra ataques de CC, consulte **Tabla 7-6**.
- Para agregar una regla de protección precisa, consulte **Tabla 7-7**.
- Para agregar una regla de lista negra o blanca, consulte **Tabla 7-10**.
- Para agregar una regla de control de acceso de geolocalización, consulte **Tabla 7-12** o **Tabla 7-13**.
- Para agregar una regla WTP, consulte **Tabla 7-14**.
- Para agregar una regla de prevención de fugas de información, consulte **Tabla 7-17**.
- Para agregar una regla de enmascaramiento de falsa alarma, consulte **Tabla 7-18**.
- Para agregar una regla de enmascaramiento de datos, consulte **Tabla 7-19**.

Paso 9 Haga clic en **OK**.

----Fin

Otras operaciones

- Después de agregar una regla, la regla está **Enabled** de forma predeterminada. Para desactivarlo, haga clic en **Disable** en la columna **Operation** de la regla de destino. También puede seleccionar varias reglas y hacer clic en **Disable** encima de la lista de reglas para deshabilitarlas todas juntas.
- Para modificar una regla, busque la fila que contiene la regla y haga clic en **Modify** en la columna **Operation**. También puede seleccionar varias reglas y hacer clic en **Modify** encima de la lista para modificarlas todas juntas.

 Copyright © Huawei Technologies Co., Ltd.

- Para eliminar una regla, busque la fila que contiene la regla y haga clic en **Delete** en la columna **Operation**. También puede seleccionar varias reglas y hacer clic en **Delete** encima de la lista para eliminarlas todas juntas.

12.3 Aplicación de una política a su sitio web

En este tema se describe cómo aplicar una política a su sitio web protegido.

NOTA

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 **Enterprise Project** y configurar las políticas de protección para los nombres de dominio en lotes.

Prerrequisitos

Se ha agregado un nombre de dominio a WAF. Ha seleccionado **Cloud mode** o **Dedicated mode** para la implementación del sitio web.

Restricciones

Esta función no está disponible en la edición estándar (anteriormente edición profesional).

Procedimiento

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, elija **Policies**.

Paso 5 En la fila que contiene la política que desea aplicar a un sitio Web, haga clic en **Add Domain Name** en la columna **Operation**.

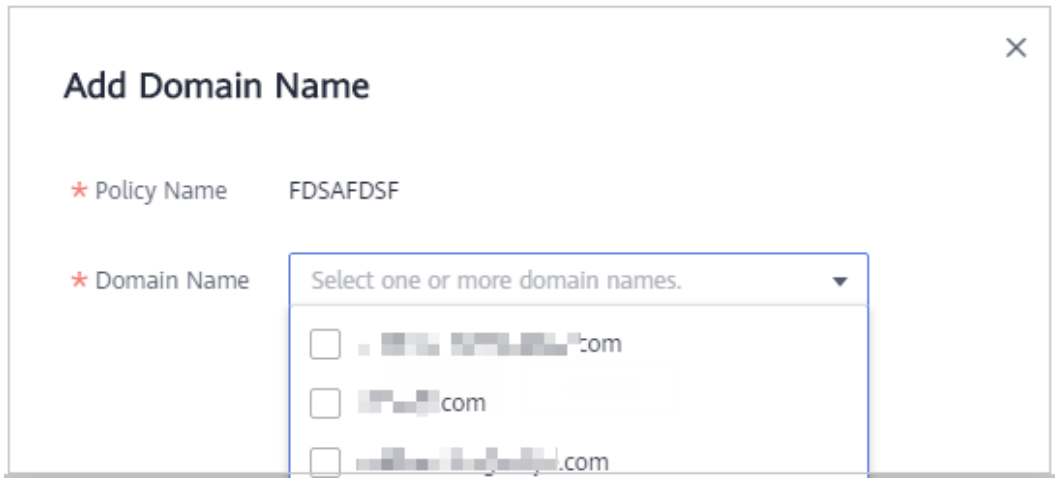
Paso 6 Seleccione uno o más nombres de dominio en la lista desplegable **Domain Name**. **Figura 12-2** muestra un ejemplo.

AVISO

- Un nombre de dominio protegido sólo puede utilizar una política, pero una política se puede aplicar a varios nombres de dominio.
- Para eliminar una política que se ha aplicado a los nombres de dominio, agregue primero estos nombres de dominio a otras políticas. A continuación, haga clic en **Delete** en la columna **Operation** de la política que desea eliminar.

 Copyright © Huawei Technologies Co., Ltd.

Figura 12-2 Selección de uno o más nombres de dominio



Paso 7 Haga clic en **OK**.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

13 Gestión del motor WAF dedicado

En este tema se describe cómo gestionar las instancias (o motores) de WAF dedicadas, incluida la visualización de información de instancia, visualización de configuraciones de monitoreo de instancia, la actualización de la edición de instancia o la eliminación de una instancia.

NOTA

Si ha habilitado proyectos de empresa, asegúrese de que tiene todos los permisos de operación para el proyecto en el que se encuentran las instancias WAF. A continuación, puede seleccionar el proyecto de la lista desplegable **Enterprise Project** y gestionar instancias de WAF dedicadas en el proyecto.

Prerrequisitos

Ha adquirido una instancia WAF dedicada

Consulta de información sobre una instancia WAF dedicada

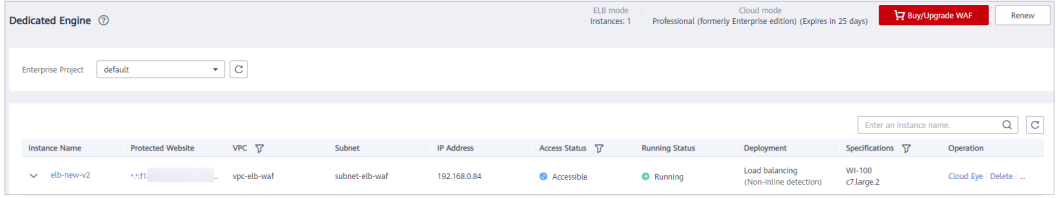
Paso 1 Inicie sesión en la consola de gestión.

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, seleccione una región y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Instance Management** > **Dedicated Engine** para ir a la página de instancia de WAF dedicada.

Figura 13-1 Lista de motores dedicados



Paso 5 Vea información sobre una instancia de WAF dedicada. Tabla 13-1 describe parámetros. describe parámetros.

 Copyright © Huawei Technologies Co., Ltd.

Tabla 13-1 Parámetros de una instancia dedicada

Parámetro	Descripción	Valor de ejemplo
Instance Name	Nombre generado automáticamente cuando se crea una instancia.	None
Protected Website	Nombre de dominio del sitio web protegido por la instancia.	www.example.com
VPC	VPC donde reside la instancia	vpc-waf
Subnet	Subred donde reside una instancia	subnet-62bb
IP Addresses	Dirección IP de la subred en la VPC donde se implementa la instancia WAF.	192.168.0.186
Access Status	Estado de la conexión de la instancia.	Accessible
Running Status	Estado de la instancia.	Running
Deployment	Cómo se implementa la instancia.	Standard mode (reverse proxy)
Specifications	Especificaciones de los recursos que alojan la instancia.	8 vCPUs | 16 GB

----Fin

Consulta de métricas de una instancia WAF dedicada

Cuando una instancia WAF está en el estado **Running**, puede ver las métricas supervisadas sobre la instancia.

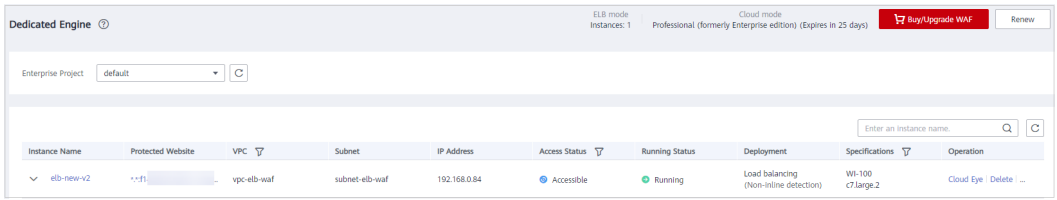
Paso 1 **Inicie sesión en la consola de gestión**.

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, seleccione una región y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Instance Management** > **Dedicated Engine** para ir a la página de instancia de WAF dedicada.

Figura 13-2 Lista de motores dedicados



 Copyright © Huawei Technologies Co., Ltd.

Paso 5 En la fila de la instancia, haga clic en **Cloud Eye** en la columna **Operation** para ir a la consola de Cloud Eye y ver la información de supervisión, como CPU, memoria y ancho de banda.

----Fin

Actualización de una instancia WAF dedicada

Solo se pueden actualizar a la última versión las instancias de WAF dedicadas en el estado de **Running**.

AVISO

- Se tarda unos 5 minutos para la actualización. Antes de la actualización, familiarícese con las siguientes condiciones:
  - Si implementa varias instancias WAF dedicadas y configura la política de comprobación de estado en el equilibrador de carga ELB, WAF reenvía automáticamente el tráfico del sitio web a otras instancias WAF dedicadas en ejecución. Casi no hay impacto en los servicios de su sitio web, excepto las desconexiones intermitentes de solicitud durante unos segundos.
  - Si implementa una instancia de WAF dedicada, configure el balanceador de carga para permitir que el tráfico omita WAF. Esto puede evitar la interrupción del servicio causada por la actualización. Una vez completada la actualización, configure el balanceador de carga para distribuir el tráfico a WAF.
- Si la instancia es de la versión más reciente, el botón **Upgrade** aparece atenuado.

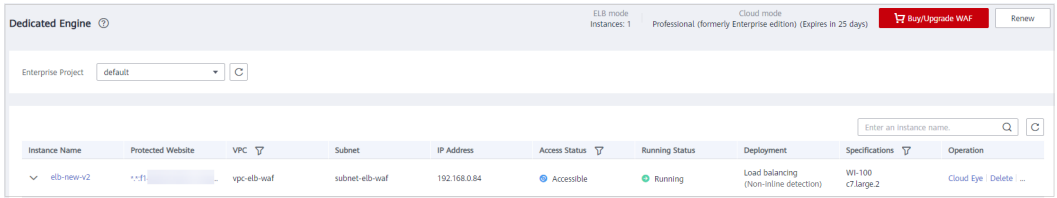
Paso 1 **Inicie sesión en la consola de gestión**.

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, seleccione una región y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Instance Management** > **Dedicated Engine** para ir a la página de instancia de WAF dedicada.

Figura 13-3 Lista de motores dedicados

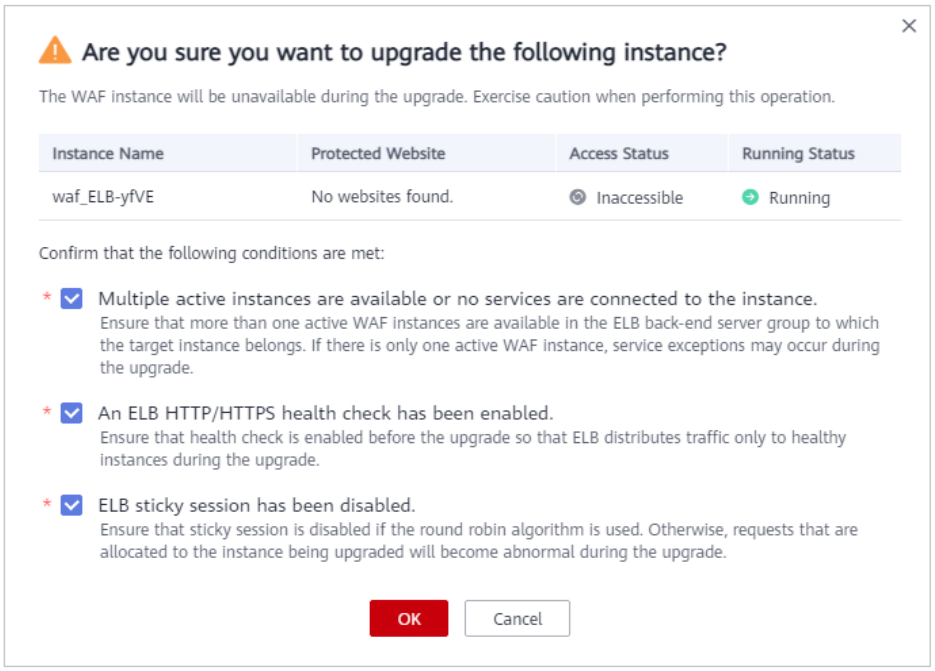


Paso 5 En la fila que contiene la instancia que desea actualizar, haga clic en **More** > **Upgrade** en la columna **Operation**.

Paso 6 Confirme las condiciones de actualización y haga clic en **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 13-4 Actualización de una instancia WAF dedicada



----Fin

Cambiar grupo de seguridad para una instancia WAF dedicada

Si selecciona **Network Interface** para **Instance Type**, puede cambiar el grupo de seguridad al que pertenece la instancia dedicada. Después de seleccionar un grupo de seguridad, la instancia WAF estará protegida por las reglas de acceso del grupo de seguridad.

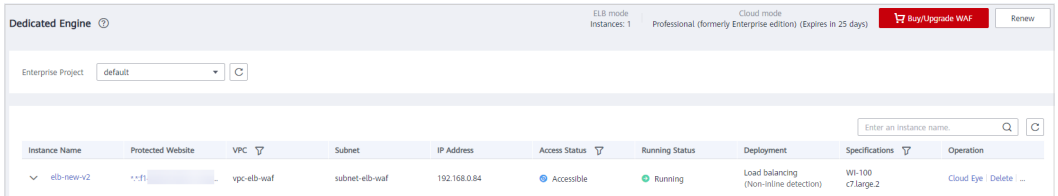
Paso 1 **Inicie sesión en la consola de gestión**.

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, seleccione una región y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Instance Management** > **Dedicated Engine** para ir a la página de instancia de WAF dedicada.

Figura 13-5 Lista de motores dedicados

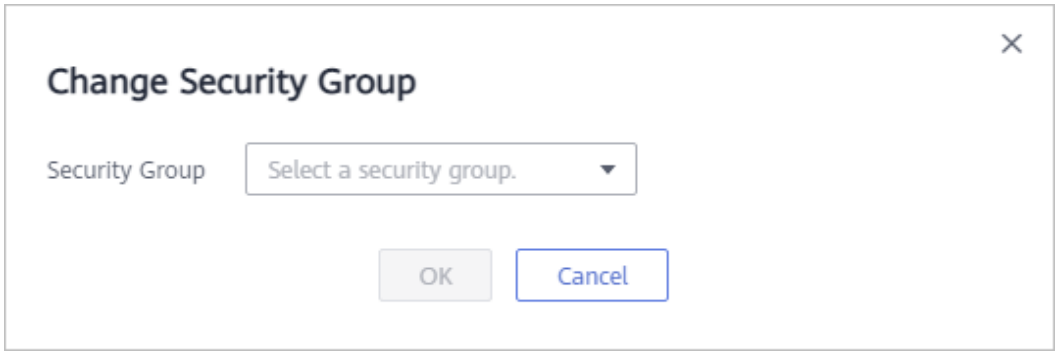


Paso 5 En la fila que contiene la instancia, elija **More** > **Change Security Group** en la columna **Operation**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 6 En el cuadro de diálogo que aparece, seleccione el nuevo grupo de seguridad y haga clic en **OK**.

Figura 13-6 Cambiar grupo de seguridad para una instancia WAF dedicada



----Fin

Eliminación de una instancia WAF dedicada

Puede eliminar una instancia WAF dedicada en cualquier momento. Después de que se elimina, la facturación finaliza.

AVISO

Los recursos de la instancia eliminada se liberan y no se pueden restaurar. Tenga cuidado al realizar esta operación.

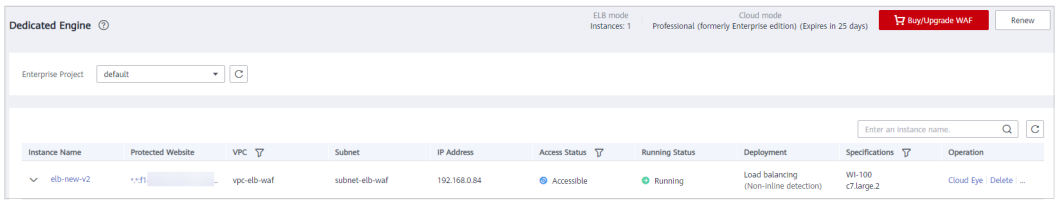
Paso 1 **Inicie sesión en la consola de gestión**.

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, seleccione una región y elija **Security & Compliance** > **Web Application Firewall** para ir a la página **Dashboard**.

Paso 4 En el panel de navegación de la izquierda, seleccione **Instance Management** > **Dedicated Engine** para ir a la página de instancia de WAF dedicada.

Figura 13-7 Lista de motores dedicados



Paso 5 En la fila de la instancia, haga clic en **Delete** en la columna **Operation**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 6 Haga clic en **OK**.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

14 Visualización de los detalles de productos

En la página **Product Details**, puede ver información sobre todas las instancias de WAF, incluidas la edición, las cuotas de dominio y las especificaciones.

NOTA

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

Prerrequisitos

Usted ha comprado una instancia WAF.

Procedimiento

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 en la esquina superior izquierda y elija **Web Application Firewall** en **Security**.

Paso 4 En el panel de navegación de la izquierda, elija **Instance Management** > **Product Details**.

Paso 5 En la página **Product Details**, consulte la edición WAF, las especificaciones y el tiempo de caducidad.

- Haga clic en **Details** para ver las especificaciones detalladas de la edición actual de WAF.
- Al mover el cursor a la edición WAF que se muestra en la esquina superior derecha de la página, se muestran las especificaciones.

----Fin

 Copyright © Huawei Technologies Co., Ltd.

15 Gestión de Proyectos y Proyectos Empresariales

Creación de un proyecto y asignación de permisos

- Creación de un proyecto

  Inicie sesión en la consola de gestión, haga clic en el nombre de usuario en la esquina superior derecha y seleccione **Identity and Access Management**. En el panel de navegación de la izquierda, elija **Projects**. En el panel derecho, haga clic en **Create Project**. En la página **Create Project** mostrada, seleccione una región e introduzca un nombre de proyecto.

- Autorización

  Puede asignar permisos (de recursos y operaciones) a grupos de usuarios para asociar proyectos a grupos de usuarios. Puede agregar usuarios a un grupo de usuarios para controlar a qué proyectos pueden acceder y a qué recursos pueden realizar operaciones. Para ello, siga estos pasos:

  a. En la página **User Groups** , busque el grupo de usuarios de destino y haga clic en **Configure Permission** en la columna **Operation** para ir a la página **User Group Permissions**. Busque la fila que contiene el proyecto de destino, haga clic en **Configure Policy** y seleccione las políticas necesarias para el proyecto.

  b. En la página **Users**, busque el usuario de destino y haga clic en **Modify** en la columna **Operation**. En el área **User Groups**, agregue un grupo de usuarios para el usuario.

Creación de un proyecto empresarial y asignación de permisos

- Creación de un proyecto de empresa

  En la consola de gestión, haga clic en **Enterprise** en la esquina superior derecha para ir a la página **Enterprise Management**. En el panel de navegación de la izquierda, elija **Enterprise Project Management**. En el panel derecho, haga clic en **Create Enterprise Project** e introduzca un nombre.

  NOTA

  Enterprise sólo está disponible en la consola de gestión si ha habilitado el proyecto de empresa o si tiene una cuenta de empresa. Para utilizar esta función, habilítela haciendo referencia a **Habilitación del centro de empresa**.

 Copyright © Huawei Technologies Co., Ltd.

- Autorización

  Puede agregar un grupo de usuarios a un proyecto de empresa y configurar una política para asociar el proyecto de empresa con el grupo de usuarios. Puede agregar usuarios a un grupo de usuarios para controlar a qué proyectos pueden acceder y a qué recursos pueden realizar operaciones. Para ello, siga estos pasos:

  a. Busque la fila que contiene el proyecto de empresa de destino, haga clic en **More** en la columna **Operation** y seleccione **View User Group**. En la página **User Groups** que se muestra, haga clic en **Add User Group**. En el cuadro de diálogo **Add User Group** que se muestra, seleccione los grupos de usuarios que desea agregar y muévalos al panel derecho. Haga clic en **Next** y seleccione las políticas.

  b. En el panel de navegación de la izquierda, elija **Personnel Management** > **User Management**. Busque la fila que contiene el usuario de destino, haga clic en **More** en la columna **Operation** y seleccione **Add to User Group**. En el cuadro de diálogo **Add to User Group** que se muestra, seleccione los grupos de usuarios para los que se han configurado las directivas y haga clic en **OK**.

- Asociar el recurso con proyectos de empresa

  Para utilizar un proyecto de empresa para gestionar recursos en la nube, asocie recursos con el proyecto de empresa.

  – Asociar una instancia WAF con un proyecto de empresa durante la compra.

    En la página de compra de WAF, seleccione un proyecto empresarial de la lista desplegable **Enterprise Project**.

  – Agregue instancias WAF a un proyecto de empresa después de comprar una instancia WAF.

    En la página **Enterprise Project Management**, agregue instancias WAF existentes adquiridas bajo su cuenta a un proyecto empresarial.

    Valor **default** indica el proyecto de empresa predeterminado. Los recursos que no están asignados a ningún proyecto de empresa bajo su cuenta se enumeran en el proyecto de empresa predeterminado.

    AVISO

    Las instancias de WAF facturadas en función de pago por uso no se pueden agregar a los proyectos de empresa.

Para obtener más información acerca de los proyectos de empresa, consulte **Guía del usuario de gestión de empresa**.

 Copyright © Huawei Technologies Co., Ltd.

16 Gestión de permisos

16.1 Creación de un grupo de usuarios y concesión de permisos

En este tema se describe cómo utilizar **IAM** para implementar un control de permisos detallado para los recursos WAF. 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.

Si su cuenta de Huawei Cloud no requiere usuarios individuales de IAM, omita este capítulo.

Prerrequisitos

Obtenga información sobre los permisos admitidos por WAF en **Tabla 16-1** y elija políticas o roles en función de sus requisitos.

 Copyright © Huawei Technologies Co., Ltd.

Tabla 16-1 Políticas de sistema soportadas por WAF

Nombre de rol/ política	Descripción	Categoría	Dependencias
WAF Administrator	Permisos de administrador para WAF	Rol definido por el sistema	Depende de los roles de **Tenant Guest** y **Server Administrator**. ● **Tenant Guest**: Un rol global, que debe asignarse en el proyecto global. ● **Server Administrator**: Rol de nivel de proyecto, que debe asignarse en el mismo proyecto.
WAF FullAccess	Todos los permisos para WAF	Política definida por el sistema	Ninguna.
WAF ReadOnlyAccess	Permisos de sólo lectura para WAF.	Política definida por el sistema	

Flujo del proceso

1. **Crear un grupo de usuarios y asignarle permisos**.

   Cree un grupo de usuarios en la consola de IAM y adjunte el permiso **WAF Administrator** al grupo.

2. **Crear un usuario de IAM**

   Cree un usuario en la consola de IAM y agregue el usuario al grupo creado en **1**.

3. **Iniciar sesión** y verificar los permisos.

   Inicie sesión en la consola WAF mediante el usuario recién creado y compruebe que el usuario solo tiene permisos de **WAF Administrator** para WAF.

   Elija cualquier otro servicio en Lista de servicios. Si aparece un mensaje que indica que no tiene permisos suficientes para acceder al servicio, la política **WAF Administrator** ya ha entrado en vigor.

16.2 Políticas personalizadas de WAF

Se pueden crear políticas personalizadas para complementar las políticas definidas por el sistema de WAF. Para obtener más información sobre las acciones admitidas por las directivas personalizadas, consulte **Permisos y acciones admitidas de WAF**.

Puede crear políticas personalizadas de cualquiera de las siguientes maneras:

- Editor visual: Seleccione servicios en la nube, acciones, recursos y condiciones de solicitud. Esto no requiere conocimiento de la sintaxis de políticas.
- JSON: Edite las políticas JSON desde cero o basándose en una política existente.

 Copyright © Huawei Technologies Co., Ltd.

Para obtener más información, consulte **Creación de una política personalizada**. La siguiente sección contiene ejemplos de políticas personalizadas comunes de WAF.

Ejemplo de políticas personalizadas

- Ejemplo 1: Permitir a los usuarios consultar la lista de dominios protegidos

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "waf:instance:list"
                                                        ]
                }
        ]
}
```

- Ejemplo 2: Denegación de la solicitud del usuario de eliminar las reglas de protección contra manipulaciones web

  Una política de denegación debe usarse junto con otras políticas. Si los permisos asignados a un usuario contienen tanto "Permitir" como "Denegar", los permisos "Denegar" tienen prioridad sobre los permisos "Permitir".

  El siguiente método se puede utilizar si necesita asignar permisos de la política **WAF FullAccess** a un usuario, pero también prohibir que el usuario elimine las reglas de protección contra manipulaciones web (**waf:antiTamperRule:delete**). Cree una política personalizada con la acción de eliminar las reglas de protección de manipulaciones web, establezca su **Effect** en **Deny** y asigne esta política y la política **WAF FullAccess** al grupo al que pertenece el usuario. A continuación, el usuario puede realizar todas las operaciones en WAF excepto eliminar las reglas de protección contra manipulaciones web. La siguiente es una política para denegar la eliminación de reglas de protección de manipulaciones web.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Deny",
                        "Action": [

"waf:antiTamperRule:delete"
                        ]
                },
        ]
}
```

- Política de acción múltiple

  Una política personalizada puede contener las acciones de varios servicios que son del tipo de proyecto. A continuación se muestra una política de ejemplo que contiene acciones de varios servicios:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "waf:instance:get",
                                "waf:certificate:get"
                        ]
                },
               {
                        "Effect": "Allow",
                        "Action": [
```

 Copyright © Huawei Technologies Co., Ltd.

```
                                "hss:hosts:switchVersion",
                                "hss:hosts:manualDetect",
                                "hss:manualDetectStatus:get"
                            ]
                        }
                ]
}
```

16.3 Permisos y acciones admitidas de WAF

En este tema se describe la gestión detallada de permisos para las instancias WAF. Si su cuenta de Huawei Cloud no necesita usuarios individuales de IAM, puede omitir esta sección.

De forma predeterminada, los nuevos usuarios de IAM no tienen ningún permiso asignado. Debe agregar un usuario a uno o más grupos y asignar directivas de permisos a estos grupos. Los usuarios heredan permisos de los grupos a los que se agregan y pueden realizar operaciones específicas a servicios en la nube según los permisos.

Puede conceder permisos a los usuarios mediante **roles** y **políticas**. Los roles son proporcionados por IAM para definir permisos basados en servicios dependiendo de las responsabilidades del trabajo del usuario. Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones.

Acciones soportadas

WAF proporciona políticas definidas por el sistema que se pueden usar directamente en IAM. También puede crear directivas personalizadas y utilizarlas para complementar las directivas definidas por el sistema, implementando un control de acceso más refinado.

- Permiso: Instrucción de una política que permite o niega ciertas operaciones.
- Acción: Operaciones específicas que están permitidas o denegadas.

Permiso	Acción	Proyectos IAM	Proyecto empresarial
Consulta de una regla de prevención de fugas de información	waf:antiLeakageRule:get	√	√
Consulta de una regla de protección contra manipulaciones web	waf:antiTamperRule:get	√	√
Consulta de una regla de protección contra ataques de CC	waf:ccRule:get	√	√
Consulta de una regla de protección precisa	waf:preciseProtectionRule:get	√	√

 Copyright © Huawei Technologies Co., Ltd.

Permiso	Acción	Proyectos IAM	Proyecto empresarial
Consulta de una regla de enmascaramiento de falsa alarma	waf:falseAlarmMaskRule:get	√	√
Consulta de una regla de enmascaramiento de datos	waf:privacyRule:get	√	√
Consulta de una regla de lista negra o de lista blanca	waf:whiteBlackIpRule:get	√	√
Consulta de una regla de control de acceso de geolocalización	waf:geoIpRule:get	√	√
Consulta de un certificado	waf:certificate:get	√	√
Modificación de certificados WAF	waf:certificate:put	√	√
Applying a certificate to a domain name	waf:certificate:apply	√	√
Consulta de un evento de protección	waf:event:get	√	√
Consulta de un dominio protegido	waf:instance:get	√	√
Consulta de una política de protección	waf:policy:get	√	√
Consulta de información del paquete de cuota	waf:bundle:get	√	√
Consulta del enlace de descarga del evento de protección	waf:dumpEventLink:get	√	√
Consulta de configuraciones	waf:consoleConfig:get	√	√

 Copyright © Huawei Technologies Co., Ltd.

Permiso	Acción	Proyectos IAM	Proyecto empresarial
Consulta del segmento de dirección IP de back-to-source	waf:sourceIp:get	√	√
Actualización de una regla de prevención de fugas de información	waf:antiLeakageRule:put	√	√
Actualización de una regla de protección contra manipulaciones web	waf:antiTamperRule:put	√	√
Actualización de una regla de protección contra ataques CC	waf:ccRuleRule:put	√	√
Actualización de una regla de protección precisa	waf:preciseProtectionRule:put	√	√
Actualización de una regla de enmascaramiento de falsa alarma	waf:falseAlarmMaskRule:put	√	√
Actualización de una regla de enmascaramiento de datos	waf:privacyRule:put	√	√
Actualización de una regla de lista negra o lista blanca de direcciones IP	waf:whiteBlackIpRule:put	√	√
Actualización de una regla de control de acceso de geolocalización	waf:geoIpRule:put	√	√
Actualización de un dominio protegido	waf:instance:put	√	√
Actualización de una política de protección	waf:policy:put	√	√

 Copyright © Huawei Technologies Co., Ltd.

Permiso	Acción	Proyectos IAM	Proyecto empresarial
Eliminación de una regla de prevención de fugas de información	waf:antiLeakageRule:delete	√	√
Eliminación de una regla de protección contra manipulaciones web	waf:antiTamperRule:delete	√	√
Eliminación de una regla de protección contra ataques de CC	waf:ccRule:delete	√	√
Configuración de una regla de protección precisa	waf:preciseProtection-Rule:delete	√	√
Eliminación de una regla de enmascaramiento de falsa alarma	waf:falseAlarmMaskRule:delete	√	√
Eliminación de una regla de enmascaramiento de datos	waf:privacyRule:delete	√	√
Eliminación de una regla de lista negra o de lista blanca	waf:whiteBlackIpRule:delete	√	√
Eliminación de una regla de control de acceso de geolocalización	waf:geoIpRule:delete	√	√
Eliminación de un dominio protegido	waf:instance:delete	√	√
Eliminación de una política de protección	waf:policy:delete	√	√
Adición de una regla de prevención de fugas de información	waf:antiLeakageRule:create	√	√

 Copyright © Huawei Technologies Co., Ltd.

Permiso	Acción	Proyectos IAM	Proyecto empresarial
Adición de una regla de protección contra manipulaciones web	waf:antiTamperRule:create	√	√
Adición de reglas de protección contra ataques de CC	waf:ccRule:create	√	√
Adición de una regla de protección precisa	waf:preciseProtection-Rule:create	√	√
Adición de una regla de enmascaramiento de falsa alarma	waf:falseAlarmMaskRule:create	√	√
Adición de una regla de enmascaramiento de datos	waf:privacyRule:create	√	√
Adición de una regla de lista negra o lista blanca	waf:whiteBlackIpRule:create	√	√
Adición de una regla de control de acceso de geolocalización	waf:geoIpRule:create	√	√
Adición de un certificado	waf:certificate:create	√	√
Adición de un dominio	waf:instance:create	√	√
Agregar una política	waf:policy:create	√	√
Consulta de reglas de prevención de fugas de información	waf:antiLeakageRule:list	√	√
Consulta de reglas de protección contra manipulaciones web	waf:antiTamperRule:list	√	√
Consulta de reglas de protección contra ataques de CC	waf:ccRuleRule:list	√	√

 Copyright © Huawei Technologies Co., Ltd.

Permiso	Acción	Proyectos IAM	Proyecto empresarial
Consulta de reglas de protección precisas	waf:preciseProtectionRule:list	√	√
Consulta de reglas de enmascaramiento de falsas alarmas	waf:falseAlarmMaskRule:list	√	√
Consulta de reglas de enmascaramiento de datos	waf:privacyRule:list	√	√
Consulta de reglas de listas negras y listas blancas	waf:whiteBlackIpRule:list	√	√
Consulta de reglas de control de acceso de geolocalización	waf:geoIpRule:list	√	√
Consulta de los dominios de protección	waf:instance:list	√	√
Consulta de políticas de protección	waf:policy:list	√	√
Consulta de elementos de facturación en modo nube	waf:subscription:get	√	√
Consulta de la configuración de notificación de alarma	waf:alert:get	√	√
Actualización de la configuración de notificación de alarma	waf:alert:put	√	√
Consulta de cuotas de registro	waf:ltsConfig:get	√	√
Actualización de cuotas de registro	waf:ltsConfig:put	√	√

 Copyright © Huawei Technologies Co., Ltd.

Permiso	Acción	Proyectos IAM	Proyecto empresarial
Creación de un pedido anual/ mensual para una instancia en modo cloud	waf:prepaid:create	√	√
Habilitación de la facturación de pago por uso para una instancia WAF en modo cloud	waf:postpaid:create	√	√
Deshabilitar la facturación de pago por uso para una instancia de WAF en modo cloud	waf:postpaid:delete	√	√
Visualización de detalles de un grupo de instancias WAF	waf:pool:get	√	√
Modificación de la configuración del grupo de instancias WAF	waf:pool:put	√	√
Creación de un grupo de instancias WAF	waf:pool:create	√	√
Eliminación de un grupo de instancias WAF	waf:pool:delete	√	√
Visualización de la lista de grupos de instancias WAF	waf:pool:list	√	√
Consulta de detalles de enlace de un grupo de instancias WAF	waf:poolBinding:get	√	√
Vinculación de un grupo de instancias WAF	waf:poolBinding:create	√	√
Desvinculación de un grupo de instancias WAF	waf:poolBinding:delete	√	√

 Copyright © Huawei Technologies Co., Ltd.

Permiso	Acción	Proyectos IAM	Proyecto empresarial
Consulta de detalles de enlace de un grupo de instancias WAF	waf:poolBinding:list	√	√
Consulta de configuraciones de comprobación de estado de un grupo de instancias WAF	waf:poolHealthMonitor:get	√	√
Modificación de la configuración de comprobación de estado de un grupo de instancias WAF	waf:poolHealthMonitor:put	√	√
Configuración de la comprobación de estado para un grupo de instancias WAF	waf:poolHealthMonitor:create	√	√
Eliminación de la configuración de comprobación de estado para un grupo de instancias WAF	waf:poolHealthMonitor:delete	√	√
Consulta de configuraciones de comprobación de estado para grupos de instancias WAF	waf:poolHealthMonitor:list	√	√

 Copyright © Huawei Technologies Co., Ltd.

17 Operaciones clave registradas por CTS

17.1 Operaciones clave registradas por CTS

CTS proporciona registros de operaciones en WAF. Con CTS, puede consultar, auditar y realizar un seguimiento posterior de estas operaciones. Para obtener más información, consulte la *Guía del usuario de Cloud Trace Service*.

Tabla 17-1 lista las operaciones de WAF registradas por CTS.

AVISO

Actualmente, CTS está disponible en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok
- AP-Singapore
- AF-Johannesburg
- LA-Santiago

Tabla 17-1 Operaciones WAF que pueden ser grabadas por CTS

Operación	Tipo de recurso	Nombre del rastro
Creación de una instancia WAF	Instancia	createInstance
Eliminación de una instancia WAF	Instancia	deleteInstance
Modificación de una instancia WAF	instancia	modifyInstance
Modificación del estado de protección de una instancia WAF	instancia	modifyProtectStatus
Modificación del estado de conexión de una instancia WAF	instancia	modifyAccessStatus
Creación de una política WAF	política	createPolicy

 Copyright © Huawei Technologies Co., Ltd.

Operación	Tipo de recurso	Nombre del rastro
Aplicación de una política de WAF	política	applyToHost
Modificación de una política	política	modifyPolicy
Eliminación de una política WAF	política	deletePolicy
Modificación de la configuración de notificación de alarma	alertNoticeConfig	modifyAlertNoticeConfig
Carga de un certificado	certificado	createCertificate
Cambio del nombre de un certificado	certificado	modifyCertificate
Eliminación de un certificado	certificado	deleteCertificate
Adición de una regla de protección contra ataques de CC	política	createCc
Modificación de una regla de protección contra ataques de CC	política	modifyCc
Eliminación de una regla de protección contra ataques de CC	política	deleteCc
Adición de una regla de protección precisa	política	createCustom
Modificación de una regla de protección precisa	política	modifyCustom
Eliminación de una regla de protección precisa	política	deleteCustom
Adición de una regla de lista negra o lista blanca de direcciones IP	política	createWhiteblackip
Modificación de una regla de lista negra o de lista blanca de direcciones IP	política	modifyWhiteblackip
Eliminación de una regla de lista negra o lista blanca de direcciones IP	política	deleteWhiteblackip
Adición de una regla de protección contra manipulaciones web	política	createAntitamper
Actualización de una regla de protección contra manipulaciones web	política	refreshAntitamper
Eliminación de una regla de protección contra manipulaciones web	política	deleteAntitamper
Adición de una regla de enmascaramiento de falsa alarma	política	createIgnore

 Copyright © Huawei Technologies Co., Ltd.

Operación	Tipo de recurso	Nombre del rastro
Eliminación de una regla de enmascaramiento de falsa alarma	política	deleteIgnore
Adición de una regla de enmascaramiento de datos	política	createPrivacy
Modificación de una regla de enmascaramiento de datos	política	modifyPrivacy
Eliminación de una regla de enmascaramiento de datos	política	deletePrivacy

17.2 Visualización de un rastro de auditoría

Después de habilitar CTS, el sistema inicia las operaciones de grabación en WAF. Los registros de operación de los últimos siete días se pueden ver en la consola CTS.

Visualización de los registros WAF en la consola CTS

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 en la esquina superior izquierda de la consola de gestión y seleccione **Cloud Trace Service** en **Management & Governance**.

Paso 4 Elija **Trace List** en el panel de navegación.

Paso 5 Haga clic en **Region** en la esquina superior derecha para establecer las condiciones correspondientes.

Los cuatro filtros siguientes están disponibles:

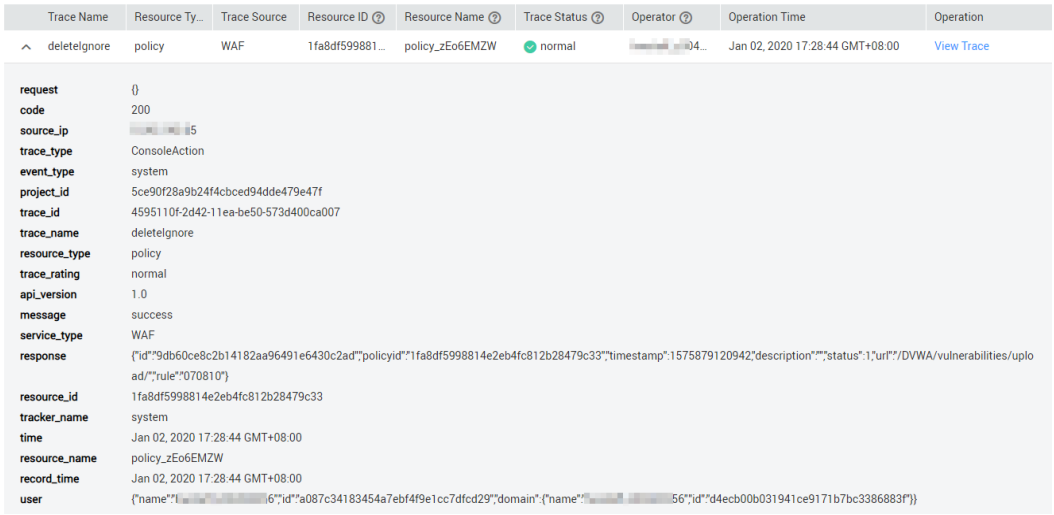
- **Trace Type**, **Trace Source**, **Resource Type**, y **Search By**.
  - Establezca **Trace Type** en **Management**.
  - Establezca **Trace Source** en **WAF**.
  - Cuando selecciona **Resource ID** para **Search By**, también debe introducir un Id. de recurso.
- **Operator**: Seleccione un operador específico (un usuario que no sea inquilino).
- **Trace Status**: las opciones disponibles incluyen **All trace statuses**, **normal**, **warning**, y **incident**. Solo se puede habilitar una de ellas.
- **Time Range**: En la esquina superior derecha de la página, puede consultar trazas en la última hora, el último día, la última semana o dentro de un período personalizado.

Paso 6 Haga clic en **Query**.

Paso 7 Haga clic en en la izquierda de una traza para ampliar sus detalles, como se muestra en **Figura 17-1**.

 Copyright © Huawei Technologies Co., Ltd.

Figura 17-1 Ampliación de los detalles de rastro



Paso 8 Haga clic en **View Trace** en la columna **Operation**. En el cuadro de diálogo **View Trace** que se muestra en **Figura 17-2**, se muestran los detalles de la estructura de rastro.

Figura 17-2 Visuzalización de rastro

----Fin

 Copyright © Huawei Technologies Co., Ltd.

18 Monitoreo

18.1 Métricas monitorizadas de WAF

Descripción de funciones

En este tema se describen las métricas reportadas por WAF a Cloud Eye, así como sus espacios de nombres y dimensiones. Puedes usar las API proporcionadas por Cloud Eye para consultar las métricas del objeto supervisado y las alarmas generadas para WAF. También puede consultarlos en la consola de Cloud Eye.

espacios de nombres

SYS.WAF

NOTA

Un espacio de nombres es una colección abstracta de recursos y objetos. Se pueden crear varios espacios de nombres en un solo clúster con los datos aislados entre sí. Esto permite que los espacios de nombres compartan los mismos servicios de clúster sin afectarse entre sí.

 Copyright © Huawei Technologies Co., Ltd.

Métricas para instancias de WAF dedicadas

Tabla 18-1 Métricas para instancias de WAF dedicadas

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
cpu_util	Uso de CPU	Consumo de CPU del objeto monitoreado Unidad: porcentaje (%) Método de recopilación: 100% menos porcentaje de uso de CPU inactivo	0% a 100% Tipo de valor: Float	Instancias de WAF dedicadas	1
mem_util	Uso de la memoria	Uso de memoria del objeto monitoreado Unidad: porcentaje (%) Método de recolección: 100% menos porcentaje de memoria inactiva	0% a 100% Tipo de valor: Float	Instancias de WAF dedicadas	1
disk_util	Utilización del disco	Uso del disco del objeto monitoreado Unidad: porcentaje (%) Método de recopilación: 100% menos porcentaje de espacio en disco inactivo	0% a 100% Tipo de valor: Float	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
disk_avail_size	Espacio de disco disponible	Espacio en disco disponible del objeto monitoreado Unidad: byte, KB, MB, GB, TB o PB Modo de recopilación: tamaño del espacio libre en disco	≥ 0 bytes Tipo de valor: Float	Instancias de WAF dedicadas	1
disk_read_bytes_rate	Velocidad de lectura de los discos	Número de bytes que el objeto supervisado lee del disco por segundo Unidad: byte/s, KB/s, MB/s o GB/s Modo de recopilación: número de bytes leídos del disco por segundo	≥0 byte/s Tipo de valor: Float	Instancias de WAF dedicadas	1
disk_write_bytes_rate	Velocidad de escritura del disco	Número de bytes que el objeto monitoreado escribe en el disco por segundo Unidad: byte/s, KB/s, MB/s o GB/s Modo de recopilación: número de bytes escritos en el disco por segundo	≥0 byte/s Tipo de valor: Float	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
disk_read_requests_rate	Solicitudes de lectura de disco	Número de solicitudes que el objeto supervisado lee del disco por segundo Unidad: Solicitudes/s Modo de recopilación: número de solicitudes de lectura procesadas por el disco por segundo	≥0 solicitud/s Tipo de valor: Float	Instancias de WAF dedicadas	1
disk_write_requests_rate	Solicitudes de escritura en disco	Número de solicitudes que el objeto monitoreado escribe en el disco por segundo Unidad: Solicitudes/s Método de recopilación: Número de solicitudes de escritura procesadas por el disco por segundo	≥0 solicitud/s Tipo de valor: Float	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
network_incoming_bytes_rate	Tráfico entrante	Tráfico entrante por segundo en el objeto monitorizado Unidad: byte/s, KB/s, MB/s o GB/s Método de recopilación: tráfico entrante a través de la NIC por segundo	≥0 byte/s Tipo de valor: Float	Instancias de WAF dedicadas	1
network_outgoing_bytes_rate	tráfico saliente	Tráfico saliente por segundo en el objeto monitoreado Unidad: byte/s, KB/s, MB/s o GB/s Método de recopilación: tráfico saliente a través de la NIC por segundo	≥0 byte/s Tipo de valor: Float	Instancias de WAF dedicadas	1
network_incoming_packets_rate	Tasa de paquetes entrantes	Paquetes entrantes por segundo en el objeto monitorizado Unidad: paquete/s Método de recopilación: paquetes entrantes a través de la NIC por segundo	≥0 paquete/s Tipo de valor: Int	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
network_outgoing_packets_rate	Tasa de paquete saliente	Paquetes salientes por segundo en el objeto monitoreado Unidad: paquete/s Método de recopilación: paquetes salientes a través de la NIC por segundo	≥0 paquete/s Tipo de valor: Int	Instancias de WAF dedicadas	1
concurrent_connections	Conexiones simultáneas	Número de conexiones simultáneas que se están procesando Unidad: cuenta Método de recopilación: Número de conexiones simultáneas en el sistema	≥0 cuenta Tipo de valor: Int	Instancias de WAF dedicadas	1
active_connections	Conexiones activas	Número de conexiones activas Unidad: cuenta Método de recogida: Número de conexiones activas en el sistema	≥0 cuenta Tipo de valor: Int	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
latest_policy_sync_time	Última sincronización de reglas	Tiempo transcurrido para que el WAF sincronice las últimas reglas personalizadas Unidad: ms Método de recopilación: tiempo transcurrido para la sincronización con las últimas políticas	≥0 ms Tipo de valor: Int	Instancias de WAF dedicadas	1
query_per_second	Tasa de consulta de capa 7	Número de solicitudes procesadas por segundo Unidad: cuenta/s Método de recogida: Velocidad de procesamiento de solicitudes del motor WAF	≥0 count/s Tipo de valor: Float	Instancias de WAF dedicadas	1
http_2xx	Códigos de estado 2xx	Número de códigos de estado 2xx Unidad: cuenta Método de recopilación: Número de códigos de estado 2XX devueltos por el motor WAF	≥0 cuenta Tipo de valor: Float	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
http_3xx	3xx Códigos de Estado	Número de códigos de estado 3xx Unidad: cuenta Método de recopilación: Número de códigos de estado 3XX devueltos por el motor WAF	≥0 cuenta Tipo de valor: Float	Instancias de WAF dedicadas	1
http_4xx	4xx Códigos de Estado	Número de códigos de estado 4xx Unidad: cuenta Método de recopilación: Número de códigos de estado 4XX devueltos por el motor WAF	≥0 cuenta Tipo de valor: Float	Instancias de WAF dedicadas	1
http_5xx	5xx Códigos de Estado	Número de códigos de estado 5xx Unidad: cuenta Método de recopilación: Número de códigos de estado 5XX devueltos por el motor WAF	≥0 cuenta Tipo de valor: Float	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
http_response_time	Tiempo promedio de respuesta	Tiempo promedio de respuesta para procesar todas las solicitudes recibidas durante el período estadístico Unidad: ms Método de recopilación: Tiempo medio de respuesta de todas las solicitudes procesadas por el motor WAF	≥0 ms Tipo de valor: Float	Instancias de WAF dedicadas	1
waf_attack_counts	Ataques bloqueados	Número de ataques bloqueados durante el período estadístico Unidad: cuenta Modo de recolección: Número de ataques bloqueados por el motor WAF por minuto	≥0 cuenta Tipo de valor: Float	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
waf_attack_percentage	Ataques bloqueados a partir de solicitudes recibidas	Relación entre el número de ataques bloqueados y el número total de solicitudes recibidas durante el período estadístico Unidad: porcentaje (%) Método de recopilación: Relación entre el número de ataques bloqueados por el motor WAF y el número total de solicitudes por minuto	0% a 100% Tipo de valor: Float	Instancias de WAF dedicadas	1

 Copyright © Huawei Technologies Co., Ltd.

Métricas de monitoreo WAF Cloud

Tabla 18-2 Métricas para cloud WAF

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
solicitudes	Número de solicitudes	Número de solicitudes devueltas por WAF en los últimos 5 minutos Unidad: Cuenta Método de recopilación: se recopila el número total de solicitudes para el nombre de dominio.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos
waf_http_2xx	Código de estado WAF (2XX)	Número de códigos de estado 2XX devueltos por WAF en los últimos 5 minutos Unidad: Cuenta Método de recopilación: Número de códigos de estado 2XX devueltos	≥ 0 Tipo de valor: Float	Protected domain dame	5

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
waf_http_3xx	Código de estado WAF (3XX)	Número de códigos de estado 3XX devueltos por WAF en los últimos 5 minutos Unidad: Cuenta Método de recopilación: Número de códigos de estado 3XX devueltos	≥ 0 Tipo de valor: Float	Protected domain dame	5
waf_http_4xx	Código de estado WAF (4XX)	Número de códigos de estado 4XX devueltos por WAF en los últimos 5 minutos Unidad: Cuenta Método de recopilación: Número de códigos de estado 4XX devueltos	≥ 0 Tipo de valor: Float	Protected domain dame	5
waf_http_5xx	Código de estado WAF (5XX)	Número de códigos de estado 5XX devueltos por WAF en los últimos 5 minutos Unidad: Cuenta Método de recopilación: Número de códigos de estado 5XX devueltos	≥ 0 Tipo de valor: Float	Protected domain dame	5

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
waf_fused_counts	Interrupciones del sitio web	Número de solicitudes destinadas al sitio web en los últimos 5 minutos durante la duración de la protección contra averías Unidad: Cuenta Método de recopilación: Número de solicitudes al nombre de dominio protegido mientras el sitio web estaba inactivo	≥ 0 Tipo de valor: Float	Protected domain dame	5
inbound_traffic	Total de tráfico entrante	Tráfico entrante total en los últimos 5 minutos Unidad: Mbit/s Método de recopilación: tráfico entrante total en los últimos 5 minutos	≥0 Mbit Tipo de valor: Float	Protected domain dame	5
outbound_traffic	Total de tráfico de saliente	Tráfico saliente total en los últimos 5 minutos Unidad: Mbit/s Método de recopilación: tráfico saliente total en los últimos 5 minutos	≥0 Mbit Tipo de valor: Float	Protected domain dame	5

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
waf_process_time_0	Latencia WAF [0-10) ms	Esta métrica se utiliza para recopilar cuántas solicitudes son procesadas por WAF en latencias en el rango de 0 ms a 10 ms en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes procesadas por WAF a latencias en el intervalo de 0 ms a menos de 10 ms en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
waf_process_time_10	Latencia WAF [10-20) ms	Esta métrica se utiliza para recopilar cuántas solicitudes son procesadas por WAF en latencias en el rango de 10 ms a menos de 20 ms en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes procesadas por WAF en latencias en el intervalo de 10 ms a menos de 20 ms en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
waf_process_time_20	Latencia WAF [20-50) ms	Esta métrica se utiliza para recopilar cuántas solicitudes son procesadas por WAF en latencias en el rango de 20 ms a menos de 50 ms en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes procesadas por WAF en latencias en el intervalo de 20 ms a menos de 50 ms en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
waf_process_time_50	Latencia WAF [50-100) ms	Esta métrica se utiliza para recopilar cuántas solicitudes son procesadas por WAF en latencias en el intervalo de 50 ms a menos de 100 ms en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes procesadas por WAF a latencias en el intervalo de 50 ms a menos de 100 ms en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
waf_process_time_100	Latencia WAF [100 y 1,000] ms	Esta métrica se utiliza para recopilar cuántas solicitudes son procesadas por WAF en latencias en el intervalo de 100 ms a menos de 1000 ms en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: Se recopila el número de solicitudes procesadas por WAF a latencias en el intervalo de 100 ms a menos de 1000 ms en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos
waf_process_time_1000	Latencia WAF [1,000, superior) ms	Esta métrica se utiliza para recopilar cuántas solicitudes son procesadas por WAF a latencias superiores a 1000 ms en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes procesadas por WAF a latencias superiores a 1000 ms en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
qps_peak	Picos de QPS	Esta métrica se utiliza para recopilar el pico de QPS del nombre de dominio en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el QPS máximo del nombre de dominio en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos
qps_mean	QPS promedio	Esta métrica se utiliza para recopilar el QPS promedio del nombre de dominio en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: Se recopila el QPS promedio del nombre de dominio en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
waf_http_0	Sin código de estado WAF	Esta métrica se utiliza para recopilar cuántas solicitudes sin código de estado devuelto por WAF en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes sin código de estado WAF devuelto en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos
upstream_code_2xx	Código de estado devuelto al cliente (2XX)	Esta métrica se utiliza para recopilar cuántas solicitudes con código de estado *2XX* son devueltas por el servidor de origen en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes con código de estado *2XX* devuelto por el servidor de origen en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
upstream_code_3xx	Código de estado devuelto por el servidor de origen (3XX)	Esta métrica se utiliza para recopilar cuántas solicitudes con código de estado *3XX* son devueltas por el servidor de origen en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes con código de estado *3XX* devuelto por el servidor de origen en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
upstream_code_4xx	Código de estado devuelto por el servidor de origen (4XX)	Esta métrica se utiliza para recopilar cuántas solicitudes con código de estado *4XX* son devueltas por el servidor de origen en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes con código de estado *4XX* devuelto por el servidor de origen en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
upstream_code_5xx	Código de estado devuelto por el servidor de origen (5XX)	Esta métrica se utiliza para recopilar cuántas solicitudes con código de estado *5XX* son devueltas por el servidor de origen en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes con código de estado *5XX* devuelto por el servidor de origen en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
upstream_code_0	No hay código de estado del servidor de origen	Esta métrica se utiliza para recopilar cuántas solicitudes sin código de estado devueltas por el servidor de origen en los últimos 5 minutos. Unidad: Cuenta Método de recopilación: se recopila el número de solicitudes sin código de estado devuelto por el servidor de origen en los últimos 5 minutos.	≥ 0 Tipo de valor: Float	Protected domain dame	5 minutos
inbound_traffic_peak	Pico de tráfico entrante	Esta métrica se utiliza para recopilar el tráfico entrante máximo al nombre de dominio en los últimos 5 minutos. Unidad: Mbit/s Método de recopilación: se recopila el tráfico entrante máximo al nombre de dominio en los últimos 5 minutos.	≥0 Mbit/s Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
inbound_traffic_mean	Tráfico entrante promedio	Esta métrica se utiliza para recopilar el tráfico entrante promedio al nombre de dominio en los últimos 5 minutos. Unidad: Mbit/s Método de recopilación: se recopila el tráfico entrante promedio al nombre de dominio en los últimos 5 minutos.	≥0 Mbit/s Tipo de valor: Float	Protected domain dame	5 minutos
outbound_traffic_peak	Pico de tráfico saliente	Esta métrica se utiliza para recopilar el tráfico saliente máximo del nombre de dominio en los últimos 5 minutos. Unidad: Mbit/s Método de recopilación: se recopila el tráfico saliente máximo del nombre de dominio en los últimos 5 minutos.	≥0 Mbit/s Tipo de valor: Float	Protected domain dame	5 minutos

 Copyright © Huawei Technologies Co., Ltd.

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
outbound_traffic_mean	Tráfico saliente promedio	Esta métrica se utiliza para recopilar el tráfico saliente promedio del nombre de dominio en los últimos 5 minutos. Unidad: Mbit/s Método de recopilación: se recopila el tráfico saliente promedio del nombre de dominio en los últimos 5 minutos.	≥0 Mbit/s Tipo de valor: Float	Protected domain dame	5

Dimensiones

Clave	Valor
instance_id	ID de la instancia WAF dedicada
waf_instance_id	ID del sitio web protegido con WAF

Ejemplo de formato de datos sin procesar de métricas monitorizadas

```
[
    {
        "metric": {
             // Namespace
            "namespace": "SYS.WAF",
            "dimensions": [
                {
                    // Dimension name, for example, protected website
                    "name": "waf_instance_id",
                    // ID of the monitored object in this dimension, for example,
ID of the protected website
                    "value": "082db2f542e0438aa520035b3e99cd99"
                }
            ],
           //Metric ID
            "metric_name": "waf_http_2xx"
        },
// Time to live, which is predefined for the metric
```

 Copyright © Huawei Technologies Co., Ltd.

```
        "ttl": 172800,
         // Metric value
        "value": 0.0,
       // Metric unit
        "unit": "Count",
         // Metric value type
        "type": "float",
        // Collection time for the metric
        "collect_time": 1637677359778
    }
]
```

18.2 Configuración de reglas de monitoreo de alarmas

Puede establecer reglas de alarma WAF para personalizar los objetos monitoreados y las políticas de notificación, y establecer parámetros como el nombre de la regla de alarma, el objeto monitoreado, la métrica, el umbral, el alcance de monitoreo y si se deben enviar notificaciones. Esto le ayuda a conocer el estado de protección de WAF de manera oportuna.

Prerrequisitos

Ha conectado un nombre de dominio a WAF o ha comprado una instancia de WAF dedicada.

Procedimiento

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 de la página y elija **Management & Governance** > **Cloud Eye**.

Paso 4 En el panel de navegación de la izquierda, elija **Alarm Management** > **Alarm Rules**.

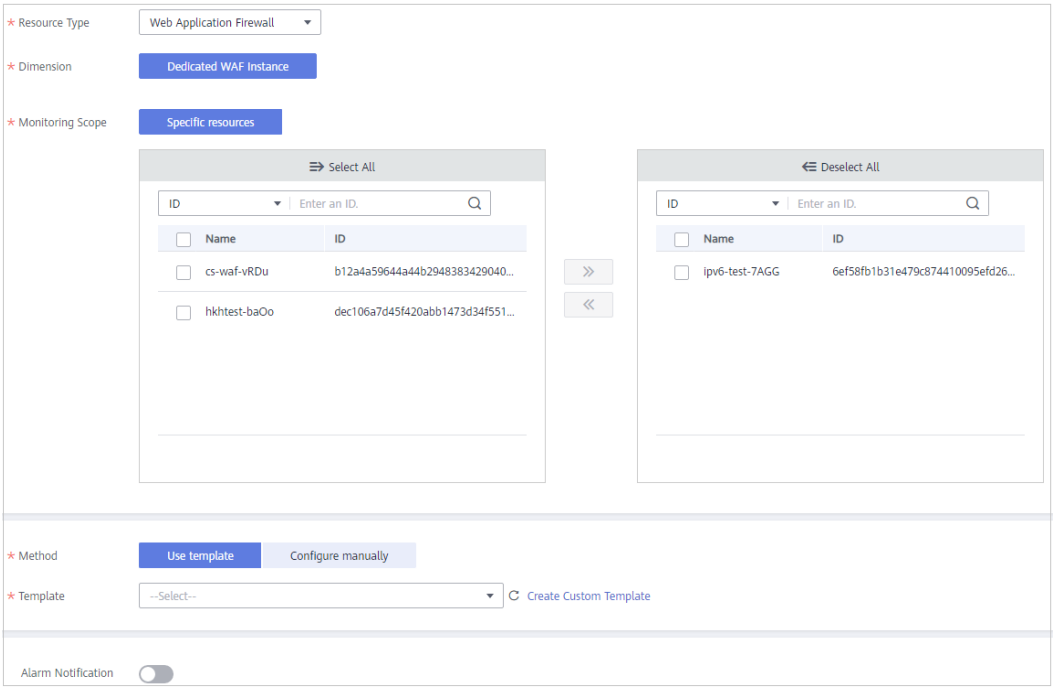
Paso 5 En la esquina superior derecha de la página, haga clic en **Create Alarm Rule**.

Paso 6 Establezca el nombre de la regla de alarma y seleccione un proyecto de empresa al que pertenece la regla de alarma.

Paso 7 Seleccione **Web Application Firewall** en la lista desplegable **Resource Type** y seleccione una dimensión, ámbito de supervisión, plantilla de alarma y si desea enviar una notificación. **Figura 18-1** muestra un ejemplo.

 Copyright © Huawei Technologies Co., Ltd.

Figura 18-1 Configuración de reglas de monitoreo de alarma WAF



Paso 8 Haga clic en **Create**. En el cuadro de diálogo mostrado, haga clic en **OK**.

----Fin

18.3 Consulta de métricas monitoreadas

Puede ver las métricas de WAF en la consola de gestión para obtener información sobre el estado de protección de WAF de manera oportuna y establecer políticas de protección basadas en las métricas.

Prerrequisitos

Las reglas de alarma WAF se han configurado en Cloud Eye. Para más detalles, consulte **Configuración de reglas de monitoreo de alarmas**.

Procedimiento

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 de la página y elija **Management & Governance** > **Cloud Eye**.

Paso 4 En el panel de navegación de la izquierda, elija **Cloud Service Monitoring** > **Web Application Firewall**.

 Copyright © Huawei Technologies Co., Ltd.

Paso 5 En la fila que contiene la instancia dedicada o el nombre de dominio protegido, haga clic en **View Metric** en la columna **Operation**.

----Fin

 Copyright © Huawei Technologies Co., Ltd.