Web Application Firewall

Descripción general del servicio

Edición	01
Fecha	2022-11-01

HUAWEI TECHNOLOGIES CO., LTD.

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 ¿Qué es el Web Application Firewall?

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

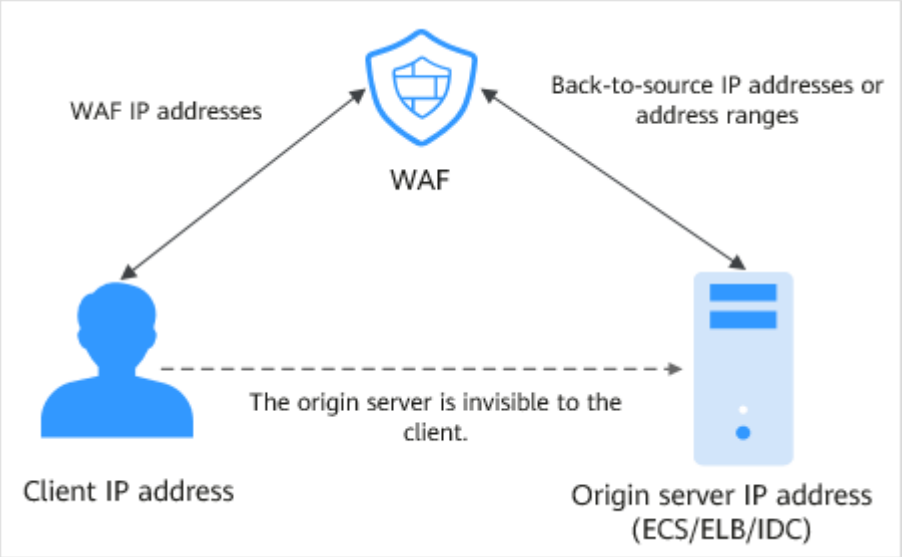
Cómo funciona WAF

Después de comprar WAF, agregue el sitio web a WAF en la consola WAF. Después de que un sitio web se conecta a WAF, todas las solicitudes de acceso al sitio web se reenvían a WAF primero. 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.

Figura 1-1 Cómo protege WAF un sitio web

El proceso de reenvío del tráfico de WAF a los servidores de origen se llama back-to-source. WAF inspecciona el tráfico que se origina en el cliente y utiliza direcciones IP de origen WAF para reenviar el tráfico normal al servidor de origen. Para el servidor de origen, las direcciones IP de origen de todas las solicitudes son las direcciones IP de origen WAF. De esta manera, la dirección IP del servidor de origen se oculta al cliente.

Figura 1-2 Dirección IP de retorno al origen



2 Diferencias de edición

WAF proporciona modos en la nube y dedicados para que pueda implementar instancias WAF. Para más detalles, consulte **Cloud e instancias de WAF dedicadas**.

Cloud e instancias de WAF dedicadas

Puede seleccionar las instancias WAF en la nube y/o WAF dedicadas para satisfacer las necesidades de su negocio. Para ver sus diferencias, consulte **Tabla 2-1**. **Figura 2-1** muestra arquitecturas de implementación.

AVISO

Antes de comprar una instancia de WAF dedicada o de equilibrio de carga, **envíe un ticket de servicio** para habilitar la compra de instancias WAF dedicadas .Otherwise, you cannot buy dedicated WAF instances.

Figura 2-1 Arquitecturas de implementación WAF dedicadas y en la nube

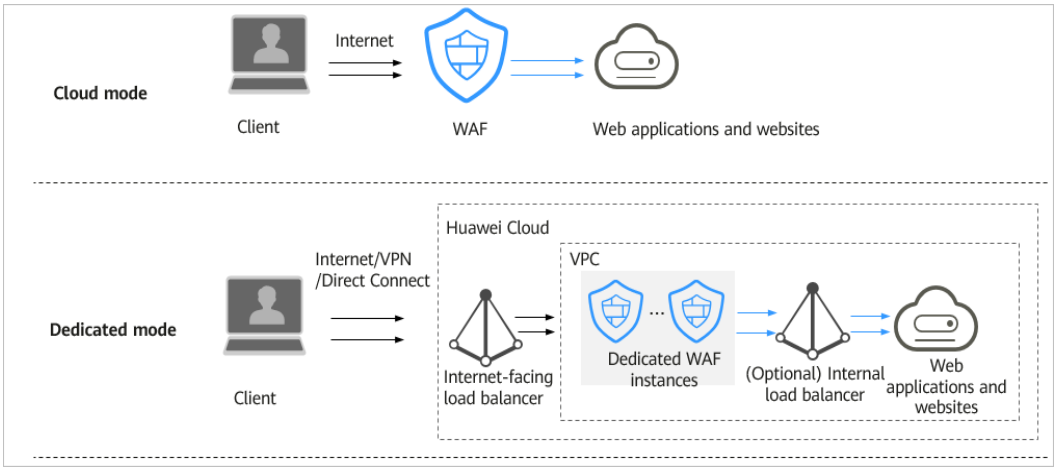


Tabla 2-1 Descripción de cómo utilizar diferentes modos de instancias WAF

Elemento	Modo de Cloud	Modo dedicado
Modo de facturación	● Anual/Mensual ● Pago por uso **NOTA** Si compra una instancia WAF en la nube, puede cambiar su modo de facturación cuando quiera.	Pago por uso
Edición	El modo de facturación anual/mensual es compatible con las siguientes ediciones de servicio: ● Estándar (anteriormente edición profesional) ● Profesional (anteriormente edición empresarial) ● Platino (anteriormente edición premium)	N/A
Escenarios de aplicación	Los servidores de servicio se implementan en una nube o en centros de datos locales. Los escenarios de aplicación para diferentes ediciones son los siguientes: ● Estándar (anteriormente edición profesional) Adecuado para sitios web pequeños y medianos que no tienen requisitos de seguridad especiales ● Profesional (anteriormente edición empresarial) Adecuado para sitios web o servicios de empresas medianas que están abiertos a Internet, se centran en la seguridad de los datos y tienen altos requisitos de seguridad ● Platino (anteriormente edición premium) Adecuado para sitios web de empresas grandes y medianas que tienen una gran escala de servicio o tienen requisitos de seguridad personalizados	Los servidores de servicio se implementan en la nube. Sitios web adecuados para grandes empresas que tienen una gran escala de servicio y tienen requisitos de seguridad personalizados.

Elemento	Modo de Cloud	Modo dedicado
Objeto de protección	Nombres de dominio	Nombres de dominio o direcciones IP
Ventajas	● Amplíe la capacidad de protección actualizando las especificaciones. ● Proteja los servicios web en la nube y en las instalaciones.	● Habilite la implementación en la nube y en las instalaciones. ● Habilite el uso exclusivo de la instancia WAF. ● Cumpla los requisitos de protección contra ataques de tráfico a gran escala. ● Implemente instancias WAF dedicadas en una VPC para reducir la latencia de la red.

Especificaciones compatibles con cada edición

Tabla 2-2 enumera las especificaciones de una instancia WAF en la nube y una instancia WAF dedicada. En el modo de nube, para proteger más nombres de dominio y tráfico, puede comprar paquetes de expansión de reglas, ancho de banda y nombres de dominio o **actualizar la edición de su instancia de WAF en la nube**.

Las restricciones y especificaciones del paquete de expansión son las siguientes:

- 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.

AVISO

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

Tabla 2-2 Escalamiento de servicio aplicable

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

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

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

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

Funciones compatibles con cada edición

Para las funciones de cada edición, consulte **Tabla 2-3**. Para satisfacer sus crecientes requisitos de protección, **actualice la edición WAF que está utilizando**.

Notas:

- √: La función se incluye en la edición actual.
- x: La función no está incluida en la edición actual.

Tabla 2-3 Funciones de seguridad

Función	Estándar (anteriormente edición profesional)	Profesional (anteriormente edición empresarial)	Platino (anteriormente edición premium)	WAF dedicado	Pago por uso
Nombre de dominio, ancho de banda y paquetes de expansión de reglas	√	Soportado	Soportado	No soportado	No soportado
Adición de nombres de dominio carácter comodín	√	Soportado	Soportado	Soportado	Soportado
Protección para puertos excepto 80 y 443	√	Soportado	Soportado	Soportado	Soportado
Personalización de puertos estándar distintos de los puertos 80 y 443	×	Soportado	Soportado	No soportado	×
Configuración por lotes de directivas de defensa	×	Soportado	Soportado	Soportado	Soportado
Lote que agrega nombres de dominio a una política	×	Soportado	Soportado	Soportado	√
Protección contra ataques web comunes, 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 comandos/códigos	√	Soportado	Soportado	Soportado	Soportado
Actualización de las reglas de protección contra vulnerabilidades de día cero a lo último en la nube y entrega de parches virtuales de manera oportuna	√	Soportado	Soportado	×	Soportado

Función	Estándar (anteriormente edición profesional)	Profesional (anteriormente edición empresarial)	Platino (anteriormente edición premium)	WAF dedicado	Pago por uso
Detección de shell web	√	Soportado	Soportado	Soportado	√
Inspección antievasión profunda para identificar y bloquear ataques de evasión, como los que utilizan ofuscación de caracteres homomórficos, inyección de comandos con carácter comodín deformados, UTF7, esquema de URI de datos y otras técnicas	√	Soportado	Soportado	Soportado	√
Inspección de todos los campos de encabezado de las solicitudes	√	Soportado	Soportado	Soportado	Soportado
Prevención de ataques CC	√	Soportado	Soportado	Soportado	Soportado
Protección precisa	No todos son compatibles	Soportado	Soportado	Soportado	No todos son compatibles
Gestión de tablas de referencias	×	Soportado	Soportado	Soportado	×
Lista blanca de direcciones IP y lista negra e importación por lotes de direcciones IP/intervalos de direcciones IP)	√	Soportado	Soportado	Soportado	Soportado
Permitir o bloquear solicitudes web en función de los países de los que se originan las solicitudes.	No soportado	Soportado	Soportado	Soportado	Soportado
Protección contra manipulación de páginas web	√	Soportado	Soportado	Soportado	√

Función	Estándar (anteriormente edición profesional)	Profesional (anteriormente edición empresarial)	Platino (anteriormente edición premium)	WAF dedicado	Pago por uso
Identificación y bloqueo del comportamiento de los rastreadores, como motores de búsqueda, escáneres, herramientas de script y otros rastreadores	×	Soportado	Soportado	Soportado	√
Protección anti-explotación basada en JavaScript	×	Soportado	Soportado	Soportado	×
Prevención de fuga de información	×	Soportado	Soportado	Soportado	√
Enmascaramiento de falsas alarmas	Soportado	Soportado	Soportado	Soportado	Soportado
Enmascaramiento de datos	√	Soportado	Soportado	Soportado	Soportado

3 Funciones

WAF hace que sea más fácil para usted manejar los riesgos de seguridad web.

Protección de servicio HTTP/HTTPS

WAF mantiene las aplicaciones estables y seguras. Examina las solicitudes HTTP y HTTPS para detectar y bloquear ataques, tales como inyecciones de Lenguaje de consulta estructurado (SQL), secuencias de comandos entre sitios (XSS), carga de shell web, inyecciones de comandos o código, inclusión de archivos, acceso a archivos confidenciales, vulnerabilidades de terceros, Ataques de CC, rastreadores maliciosos y falsificación de solicitudes entre sitios (CSRF).

WebSocket/WebSockets

WAF admite el protocolo WebSocket/WebSockets, que está habilitado de forma predeterminada.

Protección web básica

Con una extensa base de datos de reputación preestablecida, WAF defiende contra Open Web Application Security Project (OWASP) las 10 principales amenazas, vulnerabilidades, web shells y otras amenazas.

- Protección integral

  WAF detecta y bloquea ataques variados, como inyección SQL, XSS, vulnerabilidades de desbordamiento remoto, inclusiones de archivos, vulnerabilidades Bash, ejecución de comandos remotos, ataques transversales de directorio (ruta), acceso no autorizado a archivos sensibles, inyecciones de comandos/código, y ataques de inyección XML o Xpath.
- Detección de shell web

  WAF protege contra shells web de la interfaz de carga.
- Identificación precisa
  - WAF utiliza un motor de análisis semántico y un motor de expresiones regulares incorporados y admite la configuración de reglas de lista negra/lista blanca, lo que reduce los falsos positivos.
  - WAF soporta anti-escape y restauración automática de códigos comunes, lo que mejora la capacidad de reconocer ataques web de deformación.

WAF puede descodificar los siguientes tipos de código: url_encode, Unicode, XML, OCT, hexadecimal, HTML escape, and base64 code, case confusion, JavaScript, shell, y PHP concatenation confusion

- Inspección profunda

  WAF 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.

- Detección de encabezado

  WAF detecta todos los campos de encabezado en las solicitudes.

Prevención de ataques 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. Las acciones de protección de las reglas de protección contra ataques CC incluyen **Verification code**, **Block**, **Dynamically block**, y **Log only**.

- Configuración flexible de políticas

  WAF le permite establecer de manera flexible las políticas de limitación de tarifas por dirección IP, cookie o campo de referencia.

- Personalización de página devuelta

  Puede personalizar el contenido devuelto y los tipos de página para satisfacer diversas necesidades de servicio.

Datos de seguridad basados en GUI

WAF proporciona una interfaz basada en GUI para que monitoree la información de ataques y los registros de eventos en tiempo real.

- Configuración centralizada de políticas

  En la consola WAF, puede configurar las políticas aplicables a varios nombres de dominio protegidos de manera centralizada para que las directivas puedan entregarse y surtir efecto rápidamente.

- Estadísticas de tráfico y eventos

  WAF muestra el número de solicitudes, el número y los tipos de eventos de seguridad y la información de registro en tiempo real.

Puertos no estándar

Además de los puertos estándar 80 y 443, WAF también soporta puertos no estándar.

Tabla 3-1 Puertos soportados

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
Edición estándar (anterior mente	Puertos estándares	80	443	Sin límite

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
edición profesional) facturada sobre una base de pago por uso	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, 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, 28443	**10** ● Edición estándar (anteriormente edición profesional): protección hasta 10 puertos no estándar ● Modo de Cloud en modo de facturación de pago por uso: 20 puertos no estándar compatibles
Edición profesional (anteriormente edición empresarial)	Puertos estándares	80	443	Sin límite

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
	Non-standard ports (249 in 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, 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, 9021, 9023, 9027, 9037, 9050, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 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, 28080, 30002, 33332, 33334, 33702, 40010, 48299,	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, 8843, 9053, 9090, 9443, 9553, 9663, 9999, 11001, 11003, 13001, 13003, 13080, 14003, 14443, 18000, 18010, 18110, 18381, 18443, 18980, 19000, 20000, 28443, 60009	**18**

Edición	Categoría de Puertos	Protocolo HTTP	Protocolo HTTPS	Límite de puerto
		48800, 52725, 52726, 60008, 60010		
Edición Platinum (anteriormente edición premium)	Puertos estándares	80	443	Unlimited
	Puertos no estándar (236 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, 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, 9021, 9023, 9027, 9037, 9050, 9080, 9081, 9082, 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, 28080, 33702, 48299, 48800	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, 8843, 8848, 8910, 8920, 8950, 9053, 9090, 9182, 9184, 9190, 9443, 9553, 9663, 9999, 11001, 11003, 13001, 13003, 13080, 14003, 18000, 18010, 18110, 18381, 18443, 18980, 19000, 28443, 60009	**58**

Protección precisa

Admite políticas de control de acceso basadas en parámetros y lógicas precisas.

- Una variedad de condiciones de parámetros

  Establezca las condiciones con combinaciones de parámetros HTTP comunes, como **IP**, **URL**, **Referer**, **User Agent**, **Params**, y **Header**.
- Condiciones lógicas abundantes

  WAF bloquea o permite el tráfico basado en condiciones lógicas, como "Incluir", "Excluir", "Igual a", "No igual a", "Prefijo es" y "Prefijo no es".

Lista negra y lista blanca de direcciones IP

Esta función le permite poner en una lista negra o blanca direcciones IP o un rango de direcciones IP para mejorar la precisión de la defensa. WAF admite la importación por lotes de direcciones IP o intervalos de direcciones IP.

Fuente 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.
- Las reglas de origen de ataques conocidas se pueden establecer basándose en ataques bloqueados contra la protección web básica, la protección de acceso precisa y las reglas de listas negras y blancas.

Protección de 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.

Configuración del tiempo de espera de conexión

- 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.

  En el área **Basic Information** de la página de información del sitio web, habilite **Timeout Settings**. A continuación, haga clic en  junto a **WAF-to-Server Connection Timeout**, **Read Timeout**, y **Write Timeout**, modifique la configuración una por una y haga clic para guardar.

Control de acceso a la geolocalización

Puede permitir algunas solicitudes web y bloquear otras según las ubicaciones geográficas de las direcciones IP de las que se originan las solicitudes.

Prevención de manipulaciones de páginas web

Puede configurar la caché para páginas web estáticas. Cuando un usuario accede a una página web, el sistema devuelve una página almacenada en caché al usuario y comprueba aleatoriamente si la página está manipulada.

Protección Anti-Crawler

WAF analiza dinámicamente los modelos de servicios de su sitio web e identifica con precisión más de 700 tipos de comportamiento de rastreadores en función de los sistemas de control de riesgos de datos y de identificación de bots

- Biblioteca de funciones

  Bloquea el rastreo de páginas web con reglas de escáner y rastreador definidas por el usuario. Esta función mejora la precisión de la protección.

- JavaScript

  Identifica y bloquea el rastreo de JavaScript con reglas definidas por el usuario.

Enmascaramiento de falsas alarmas

Esta función le permite ignorar ciertas reglas de detección de ataques para solicitudes específicas.

Enmascaramiento de datos

WAF enmascara información confidencial, como nombres de usuario y contraseñas, en el registro de eventos.

Prevención de fuga de información

WAF evita que su información confidencial se divulgue en páginas web, como números de identificación, números de teléfono y direcciones de correo electrónico.

Confiable

WAF se puede implementar en múltiples clústeres en múltiples regiones basándose en el principio de equilibrio de carga. Esto puede evitar punto único de falla (SPOF) y garantizar una expansión de la capacidad en línea sin problemas, maximizando la estabilidad del servicio.

Notificación de alarmas

Puede habilitar la notificación de los registros de ataques. Una vez que esta función está habilitada, WAF te envía los registros de ataques mediante el método que configures.

Gestión de Eventos

- WAF le permite ver y manejar falsas alarmas para eventos bloqueados o registrados.
- Puede descargar datos de eventos en los últimos cinco días.
- Puede usar Log Tank Service (LTS) en Huawei Cloud para registrar todos los registros WAF, incluidos los registros de ataque y acceso.

4 Ventajas del producto

WAF examina el tráfico web desde múltiples dimensiones para identificar con precisión las solicitudes maliciosas y filtrar los ataques, reduciendo los riesgos de que los datos sean manipulados o robados.

Identificar amenazas de manera precisa y eficiente

- WAF utiliza motores duales de regla e IA e integra nuestras últimas reglas de seguridad y mejores prácticas.
- Puede configurar políticas de nivel empresarial para proteger su sitio web con mayor precisión, incluidas las páginas de alarma personalizadas, la combinación de varias condiciones en una regla de protección contra ataques de CC y la inclusión en listas negras o blancas de un gran número de direcciones IP.

Vulnerabilidades de día cero parcheadas rápidamente

Un equipo de seguridad especializado proporciona soporte de servicio 24/7 para corregir vulnerabilidades de día cero en 2 horas.

Protección fuerte para la privacidad de los datos del usuario

- La información confidencial, como cuentas y contraseñas, en los registros de ataques se puede anonimizar.
- Las comprobaciones PCI-DSS para el encriptación SSL están disponibles.
- Se puede configurar la versión mínima del protocolo TLS y el conjunto de cifrado.

Excelente ayuda en cumplimiento de seguridad

Facilitar el cumplimiento de los requisitos de cumplimiento para la certificación DJCP (o MLPS) y PCI DSS.

5 Escenarios de aplicación

Protección común

WAF le ayuda a defenderse de ataques web comunes, como la inyección de comandos y el acceso a archivos confidenciales.

Protección para actividades de promoción de centros comerciales en línea

Se pueden enviar innumerables solicitudes maliciosas a las interfaces de servicio durante las promociones en línea. WAF permite configurar políticas de limitación de velocidad para defenderse contra ataques de CC. Esto evita que los servicios se descompongan debido a muchas solicitudes simultáneas, lo que garantiza la respuesta a solicitudes legítimas.

Protección contra vulnerabilidades de día cero

Los servicios no pueden recuperarse rápidamente del impacto de las vulnerabilidades de día cero en los marcos web y complementos de terceros. WAF actualiza las reglas de protección preestablecidas inmediatamente para agregar una capa de protección adicional a dichos marcos web y complementos, y esta capa puede reaccionar más rápido que corregir las vulnerabilidades.

Prevención de fugas de datos

WAF evita que los actores maliciosos utilicen métodos como la inyección SQL y los shells web para evitar la seguridad de las aplicaciones y obtener acceso remoto a bases de datos web. Puede configurar reglas de fuga antidatos en WAF para proporcionar las siguientes funciones:

- Identificación precisa

  WAF utiliza el análisis semántico & regex para examinar el tráfico de diferentes dimensiones, detectando con precisión el tráfico malicioso.

- Detección de ataques de distorsión

  WAF detecta una amplia gama de patrones de ataque de distorsión con 7 métodos de decodificación para evitar intentos de derivación.

Prevención de manipulaciones de páginas web

WAF asegura que los atacantes no puedan dejar puertas traseras en sus servidores web o manipular el contenido de su página web, evitando daños a su credibilidad. Puede configurar

reglas de protección contra manipulaciones web en WAF para proporcionar las siguientes funciones:

- Detección de código malicioso en sitios web

  Puede configurar WAF para detectar código malicioso inyectado en los servidores web y garantizar visitas seguras a las páginas web.

- Prevención de manipulaciones de páginas web

  WAF evita que los atacantes alteren el contenido de la página web o publiquen información inapropiada que pueda dañar su reputación.

6 Descripción de la facturación

WAF admite dos modos de facturación: anual/mensual (prepago) y pago por uso (postpago). Para las instancias en la nube de WAF, ambos modos de facturación son compatibles. Para instancias de WAF dedicadas, solo se admite el modo de facturación de pago por uso.

Para obtener más información, consulte **Detalles de Precios de producto**.

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.

Artículos de facturación

Se le facturan las instancias WAF que seleccione en función del modo de facturación especificado.

Figura 6-1 Modo de facturación WAF

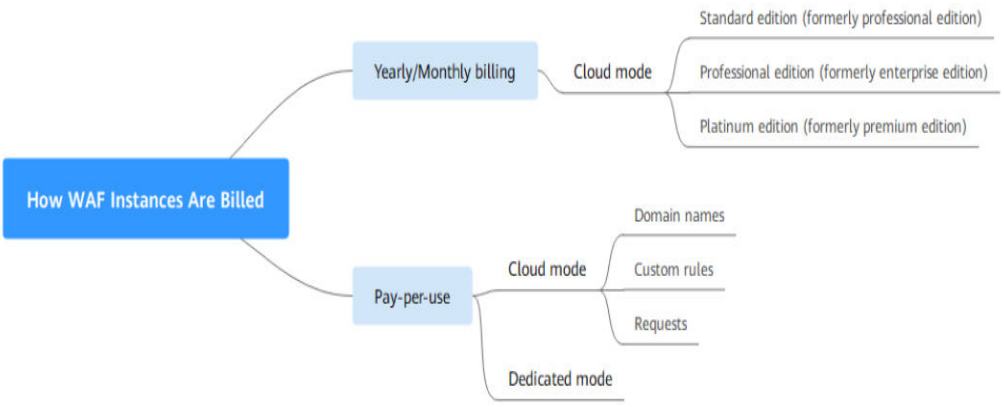


Tabla 6-1 Artículos de facturación

Modo de compra:	Modo de facturación	Concepto de facturación	Descripción de la facturación
Modo de Cloud	Anual/ Mensual	Edición (obligatorio)	Se le factura la edición que ha comprado. Las reglas de precios para las ediciones estándar (anteriormente edición profesional), profesional (anteriormente edición empresarial) y platino (anteriormente edición premium) son diferentes. Para obtener más información sobre las especificaciones y funciones de cada edición, consulte **Diferencias de edición**.
		Paquete de expansión de dominio (opcional)	Facturación basada en el número de paquetes de expansión de dominios comprados
		Paquete de expansión de ancho de banda (Opcional)	Facturación basada en el número de paquetes de expansión de ancho de banda comprados
		Paquete de expansión de reglas (opcional)	Se factura en función de cuántos paquetes compró.
		Duración requerida	Facturación anual o mensual
	Pago por uso	● Cantidad de dominios ● Número de reglas personalizadas ● Número de solicitudes	● Número de nombres de dominio: Facturación por hora. Una vez que se agrega un nombre de dominio durante el período de facturación, se facturará sin importar cuándo se elimine. ● Número de reglas personalizadas: Facturación diaria. La facturación se calcula a las 00:00 todos los días. ● Número de solicitudes: Facturación mensual.
Modo dedicado	Pago por uso	Cantidad de instancias	Facturación basada en lo que usa

NOTA

Las instancias de WAF en la nube admiten el cambio entre pagos anuales/mensuales y pagos por uso.

Opciones de facturación

- **Anual/Mensual**: soportado por las instancias de WAF en la nube. Cuanto más tiempo se suscriba, más ahorrará. Una instancia WAF en la nube anual/mensual se factura en función de la duración requerida que seleccione.
- **Pago por uso**: Este modo de facturación le permite realizar una suscripción o cancelar la suscripción en cualquier momento.
  - Para una instancia de WAF en la nube de pago por uso, se le factura el número de nombres de dominio agregados, el número de reglas personalizadas y el número de solicitudes utilizadas.
  - Para una instancia de WAF dedicada de pago por uso, se le factura la duración requerida (preciso a segundo), que comienza cuando se crea la instancia y finaliza cuando se elimina la instancia.

Cambio de las opciones de facturación

- En el modo de facturación anual/mensual, puede actualizar la edición de su instancia WAF o aumentar el número de nombres de dominio, ancho de banda y paquetes de expansión de reglas para satisfacer las necesidades de su empresa.
- Cancelación de suscripción: Si ya no necesita su instancia de WAF que se factura anualmente/mensualmente, **cancele su suscripción** en el Centro de facturación.

Renovación

Si no renueva una instancia de WAF en la nube facturada anualmente/mensualmente al expirar, un período de retención está disponible para usted.

Para obtener más información, consulte **Período de retención**.

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

Para evitar pérdidas innecesarias causadas por problemas de seguridad, renueve su suscripción antes de que expire el período de retención. La expiración de WAF no afecta a sus otros servicios.

Puede renovar sus recursos en la consola de gestión. Para obtener más información, consulte **Reglas de renovación**.

Vencimiento y pago atrasado

- Caducidad

Si no renueva una instancia de WAF facturada anualmente/mensualmente al expirar, hay un período de retención disponible para usted. Para obtener más información, consulte **Período de retención**.

- Pago atrasado

  Si su cuenta de instancias de WAF facturadas anualmente/mensualmente está en mora, recargue su cuenta de manera oportuna para permitir que WAF proteja su sitio web continuamente. Para obtener más información, consulte **¿Cómo se repara un cliente común de Huawei Cloud?**

Preguntas Frecuentes

Para más preguntas frecuentes sobre facturación, consulta **Preguntas frecuentes sobre WAF**.

7 Mecanismo de protección de datos personales

Para garantizar que los datos personales de los visitantes del sitio web, como el nombre de usuario, la contraseña y el número de teléfono móvil, no sean obtenidos por entidades o personas no autorizadas o no autenticadas, y para evitar la fuga de datos, WAF encripta sus datos personales antes de almacenarlos para controlar el acceso a los datos y registros de registros para las operaciones realizadas con los datos.

Datos personales que se recopilarán

WAF registra las solicitudes que activan alarmas de ataque en los registros de eventos. **Tabla 7-1** proporciona los datos personales recopilados y generados por WAF.

Tabla 7-1 Datos personales

Tipo	Método de colección	Puede ser modificado	Obligatorio
Solicitar dirección IP de origen	Dirección IP del atacante que es bloqueada o registrada por WAF cuando el nombre de dominio es atacado.	No	Sí
URL	URL atacada del nombre de dominio protegido, o URL del nombre de dominio protegido que está bloqueado o registrado por WAF.	No	Sí

Tipo	Método de colección	Puede ser modificado	Obligatorio
Información del encabezado HTTP/ HTTPS (incluida la cookie)	El valor de la cookie y el valor del encabezado introducidos en la página de configuración al configurar un ataque de CC o una regla de protección precisa.	No	No Si los campos de cookies y encabezado configurados no contienen información personal de los usuarios, las solicitudes registradas por WAF no recopilarán ni generarán dichos datos personales.
Parámetros de solicitud (Obtener y publicar)	Solicitar los detalles registrados por WAF en los registros de protección.	No	No Si los parámetros de solicitud no contienen información personal de los usuarios, las solicitudes registradas por WAF no recopilarán ni generarán dichos datos personales.

Modo de almacenamiento

Los valores de los campos sensibles se guardan después de ser anonimizados, y los valores de otros campos se guardan en texto plano en los registros.

Control de acceso

Los usuarios solo pueden ver los registros relacionados con sus propios servicios.

8 Gestión de permisos WAF

Para asignar diferentes permisos a los empleados de su empresa para acceder a sus recursos WAF, IAM es una buena opción para la gestión de permisos detallada. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a proteger el acceso a sus recursos de Huawei Cloud.

Con IAM, puede usar su cuenta de Huawei Cloud para crear usuarios de IAM para sus empleados y asignar permisos a los usuarios para controlar su acceso a tipos de recursos específicos. Por ejemplo, algunos desarrolladores de software de su empresa necesitan usar recursos WAF pero no deben eliminarlos ni realizar operaciones de alto riesgo. Para lograr este resultado, puede crear usuarios de IAM para los desarrolladores de software y concederles solo los permisos necesarios para usar los recursos WAF.

Si su cuenta de Huawei Cloud no necesita usuarios individuales de IAM para la gestión de permisos, puede omitir este capítulo.

IAM se puede utilizar de forma gratuita. Solo paga por los recursos de tu cuenta. Para obtener más información, consulte **Descripción general del servicio IAM**.

Permisos WAF

De forma predeterminada, los nuevos usuarios de IAM no tienen ningún permiso asignado. Debe agregar un usuario a uno o más grupos y adjuntar políticas o roles 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.

WAF es un servicio a nivel de proyecto implementado y accedido en regiones físicas específicas. Para asignar permisos WAF a un grupo de usuarios, especifique el ámbito como proyectos específicos de la región y seleccione proyectos para que los permisos surtan efecto. Si se selecciona **All projects**, los permisos surtirán efecto para el grupo de usuarios en todos los proyectos específicos de la región. Al acceder a WAF, los usuarios necesitan cambiar a una región en la que han sido autorizados para usar el servicio WAF.

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos relacionados con las responsabilidades de los usuarios. Solo hay disponible un número limitado de funciones de nivel de servicio para la autorización. También debe asignar otros roles dependientes para que el control de permisos surta efecto. Los roles no son ideales para la autorización detallada y el control de acceso seguro.

- Políticas: Un mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos específicos de la nube bajo ciertas condiciones. Este mecanismo permite una autorización basada en políticas más flexible y cumple con los requisitos de control de acceso seguro. Por ejemplo, puede conceder a los usuarios de WAF solo los permisos para administrar un determinado tipo de recursos. La mayoría de las políticas definen permisos basados en API. Para ver las acciones de API admitidas por WAF, consulta **Políticas de permisos y acciones admitidas**.

Tabla 8-1 lista todos los roles del sistema soportados por WAF.

Tabla 8-1 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	

Enlaces útiles

- **Descripción general del servicio de IAM**
- **Creación de un grupo de usuarios y usuarios y concesión de permisos WAF**
- **Políticas personalizadas de WAF**
- **Permisos y acciones admitidas de WAF**

Contenido de política de WAF FullAccess

```
{    "Version": "1.1",
     "Statement": [
          {
             "Action": [
               "waf:*:*",
               "lts:groups:get",
               "lts:groups:list",
               "lts:topics:get",
               "lts:topics:list",
               "smn:*:list*",
               "vpc:*:get*",
```



```
                "vpc:*:list*",
                "ecs:*:get*",
                "ecs:*:list*",
                "elb:*:get*",
                "elb:*:list*"
            ],
                "Effect": "Allow"
         }
                ]
}
```

Contenido de la política de WAF ReadOnlyAccess

```
{
    "Version": "1.1",
    "Statement": [
        {
           "Action": [
             "waf:*:get*",
             "waf:*:list*",
             "lts:groups:get",
             "lts:groups:list",
             "lts:topics:get",
             "lts:topics:list",
             "smn:*:list*",
             "vpc:*:get*",
             "vpc:*:list*",
             "ecs:*:get*",
             "ecs:*:list*",
             "elb:*:get*",
             "elb:*:list*"
         ],
             "Effect": "Allow"
        }
    ]
}
```


9 WAF y otros servicios

En este tema se describe WAF y otros servicios en la nube.

CTS

Cloud Trace Service (CTS) registra todas las operaciones WAF para que pueda consultar, auditar y retroceder.

AVISO

Actualmente, CTS está disponible en las siguientes regiones:

- CN-Hong Kong
- AP-Bangkok
- AP-Singapore
- AF-Johannesburg
- LA-Santiago

Tabla 9-1 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
Aplicación de una política de WAF	política	applyToHost

Operación	Tipo de recurso	Nombre del rastro
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

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

Cloud Eye

Cloud Eye monitrea los indicadores de WAF, para que pueda comprender el estado de protección de WAF de manera oportuna y establecer políticas de protección en consecuencia. Para obtener más información, consulte la *Guía del usuario de Cloud Eye*.

Para obtener más información sobre las métricas monitoreadas WAF, consulte **Métricas monitoreadas de WAF**

IAM

Identity and Access Management (IAM) proporciona la función de gestión de permisos para WAF. Solo los usuarios con permisos de administrador de WAF pueden usar WAF. Para obtener este permiso, póngase en contacto con los usuarios que tienen los permisos de administrador de seguridad.

LTS

Log Tank Service (LTS) recopila datos de registro de hosts y servicios en la nube. WAF le permite transferir registros de ataques WAF y registros de acceso a LTS para que pueda manejar con registros en tiempo real.

SMN

Simple Message Notification (SMN) proporciona la función de notificación. Después de habilitar la función de notificación en WAF, la información de alarma se le enviará como configurada una vez que su nombre de dominio sea atacado.

Gestión empresarial

Puede gestionar varios proyectos en una empresa, liquidar por separado sus costos y asignarles personal diferente. Un proyecto puede iniciarse o detenerse de forma independiente sin afectar a otros. Con **Enterprise Management**, puede gestionar fácilmente sus proyectos después de crear un proyecto empresarial para cada uno de ellos.

WAF se puede interconectar con Gestión empresarial. Puede gestionar los recursos WAF por proyecto empresarial y conceder diferentes permisos a los usuarios.

