Web Application Firewall

Visão geral de serviço

Edição 01

Data 01-11-2022

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Huawei Technologies Co., Ltd.

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

Site: https://www.huawei.com

Email: support@huawei.com

Índice

1 O que é Web Application Firewall?

Web Application Firewall (WAF) mantém os serviços web estáveis e seguros. Ele examina todas as solicitações HTTP e HTTPS para detectar e bloquear os seguintes ataques: Injeção de linguagem de consulta estruturada (SQL), cross-site scripting (XSS), web shells, injeções de comando e código, inclusão de arquivos, acesso a arquivos sensíveis, explorações de vulnerabilidade de terceiros, ataques Challenge Collapsar (CC), rastreadores maliciosos, e falsificação de solicitação entre sites (CSRF).

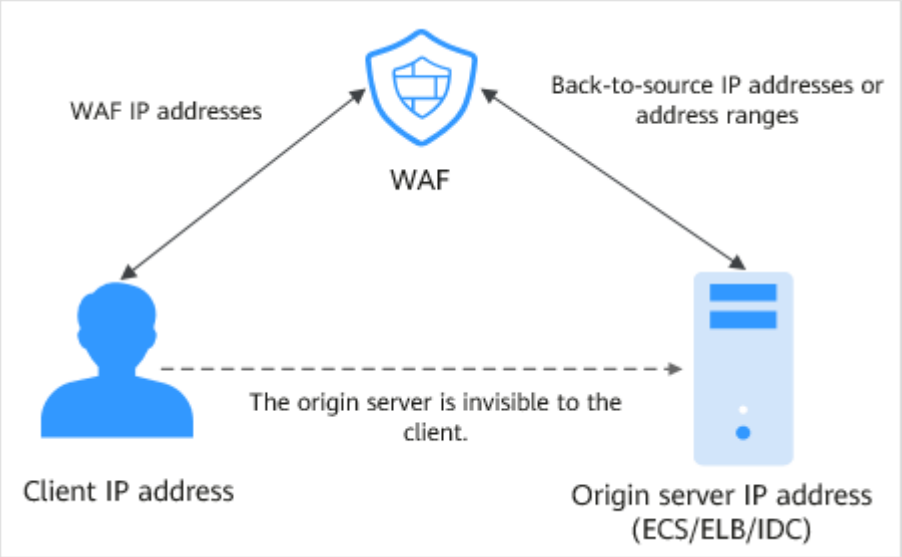
Como funciona o WAF

Depois de comprar o WAF, adicione o site ao WAF no console do WAF. Depois que um site é conectado ao WAF, todas as solicitações de acesso ao site são encaminhadas primeiro ao WAF. O WAF detecta e filtra o tráfego de ataque malicioso e retorna o tráfego normal para o servidor de origem para garantir que o servidor de origem esteja seguro, estável e disponível.

Figura 1-1 Como o WAF protege um site

O processo de encaminhamento de tráfego do WAF para os servidores de origem é chamado de back-to-source. O WAF inspeciona o tráfego proveniente do cliente e usa endereços IP back-to-source do WAF para encaminhar o tráfego normal para o servidor de origem. Para o servidor de origem, os endereços IP de origem de todas as solicitações são os endereços IP back-to-source do WAF. Desta forma, o endereço IP do servidor de origem fica oculto do cliente.

Figura 1-2 Back-to-source IP address



2 Diferenças de edição

O WAF fornece modos dedicados e de nuvem para você implantar instâncias do WAF. Para mais detalhes, veja **Nuvem e instâncias WAF dedicadas**.

Nuvem e instâncias WAF dedicadas

Você pode selecionar o WAF na nuvem e/ou instâncias WAF dedicadas para atender às suas necessidades de negócios. Para suas diferenças, veja **Tabela 2-1**. **Figura 2-1** mostra arquiteturas de implantação.

Figura 2-1 Arquiteturas de implantação WAF dedicadas e em nuvem

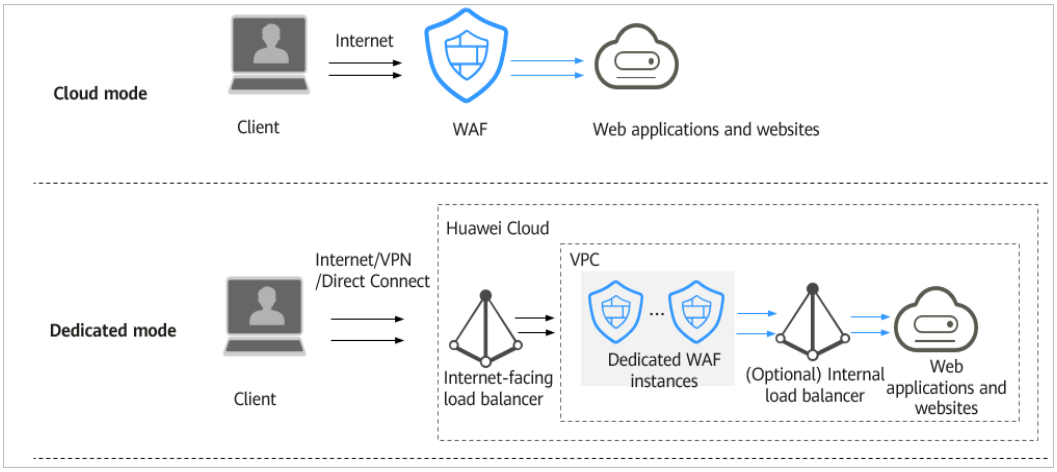


Tabela 2-1 Descrição de como usar diferentes modos de instâncias do WAF

Item	Modo nuvem	Modo Dedicado
Modo de cobrança	● Anual/Mensal ● Cobrança por uso **NOTA** Se você comprar uma instância WAF na nuvem, poderá alterar seu modo de cobrança sempre que desejar.	Cobrança por uso

Item	Modo nuvem	Modo Dedicado
Edição	O modo de cobrança anual/mensal é suportado para as seguintes edições de serviço: ● Standard (antiga edição profissional) ● Profissional (anteriormente Enterprise Edition) ● Platinum (antiga edição premium)	N/A
Cenários de aplicação	Os servidores de serviço são implantados em uma nuvem ou em data centers locais. Os cenários de aplicação para diferentes edições são os seguintes: ● Standard (antiga edição profissional) Adequado para sites de pequeno e médio porte que não têm requisitos especiais de segurança ● Professional (anteriormente Enterprise Edition) Adequado para sites ou serviços de empresas de médio porte que estão abertos à Internet, com foco na segurança de dados e com altos requisitos de segurança ● Platinum (antiga edição premium) Adequado para sites corporativos de grande e médio porte que têm uma grande escala de serviço ou têm requisitos de segurança personalizados	Os servidores de serviço são implantados na nuvem. Sites corporativos de grande porte adequados que tenham uma grande escala de serviço e tenham requisitos de segurança personalizados.
Objeto de proteção	Nomes de domínio	Nomes de domínio ou endereços de IP

Item	Modo nuvem	Modo Dedicado
Vantagens	● Expanda a capacidade de proteção atualizando as especificações. ● Proteja os serviços da Web na nuvem e no local.	● Habilite a implantação na nuvem e no local. ● Habilite o uso exclusivo da instância do WAF. ● Atenda aos requisitos de proteção contra ataques de tráfego em larga escala. ● Implante instâncias WAF dedicadas em uma VPC para reduzir a latência da rede.

Especificações suportadas por cada edição

Tabela 2-2 lista as especificações de uma instância do WAF na nuvem e de uma instância do WAF dedicada. No modo de nuvem, para proteger mais nomes de domínio e tráfego, você pode comprar pacotes de expansão de nome de domínio, largura de banda e regras ou **atualizar a edição de sua instância WAF na nuvem**.

As restrições e especificações do pacote de expansão são as seguintes:

- Um pacote de domínio permite adicionar 10 nomes de domínio ao WAF, incluindo um domínio de nível superior e nove subdomínios ou domínios curinga relacionados ao domínio de nível superior.
- Um pacote de expansão de largura de banda pode proteger até 20 Mbit/s de tráfego para serviços na HUAWEI CLOUD ou 50 Mbit/s para aplicativos não na HUAWEI CLOUD; ou Consultas 1 000 por Segundo (QPS). Cada solicitação HTTP Get é uma consulta.

  NOTA

  - Fora da HUAWEI CLOUD: Os servidores de origem não são implantados na HUAWEI CLOUD ou são implantados no local.
  - Em HUAWEI CLOUD: Os servidores de origem são implantados na HUAWEI CLOUD.
- Um pacote de expansão de regras permite configurar até 10 regras de lista negra e lista branca de endereços IP.

AVISO

- O número de domínios é o número total de nomes de domínio de nível superior (por exemplo, example.com), nomes de domínio único/domínios de segundo nível (por exemplo, nomes de domínio www.example.com), e curinga (por exemplo, *.exemplo.com). Por exemplo, uma instância WAF padrão (antiga edição profissional) pode proteger 10 nomes de domínio. Portanto, você pode adicionar 10 nomes de domínio únicos ou nomes de domínio curinga a ele ou adicionar um nome de domínio de nível superior e nove nomes de subdomínio ou nomes de domínio curinga relacionados ao nome de domínio de nível superior a ele.
- Se um nome de domínio mapear para portas diferentes, cada porta é considerada como representando um nome de domínio diferente. Por exemplo, **www.example.com:8080** e **www.example.com:8081** são contabilizados na sua cota como dois nomes de domínio distintos.

Tabela 2-2 Escala de serviço aplicável

Escala de serviço	Standard (antiga edição profissional)	Professional (anteriormente Enterprise Edition)	Platinum (antiga edição premium)	Cobrança por uso	Modo Dedicado
Taxa máxima de solicitações de serviço normais	● 2.000 QPS ● Conexões WAF-para-servidor: 6.000 por nome de domínio	● Solicitações de serviço: QPS do 5.000 ● Conexões WAF-para-servidor: 6.000 por nome de domínio	● Solicitações de serviço: 10.000 QPS ● Conexões WAF-para-servidor: 6.000 por nome de domínio	N/A	● Especificações: WI-500. Desempenho: – Rendimento: 500 Mbit/s; QPS: 10.000 – Conexões WAF-para-servidor suportadas: 60.000 por instância ou 5.000 por domínio ● Especificações: WI-100. Desempenho: – Rendimento: 100 Mbit/s; QPS: 2.000 – Conexões WAF-para-servidor suportadas: 60.000 por instância ou 5.000 por domínio

Escala de serviço	Standard (antiga edição profissional)	Professional (anteriormente Enterprise Edition)	Platinum (antiga edição premium)	Cobrança por uso	Modo Dedicado
Limite de largura de banda do serviço (O servidor de origem é implantado na nuvem.)	100 Mbit/s	200 Mbit/s	300 Mbit/s	N/A	• Especificações: WI-500. Desempenho: – Rendimento: 500 Mbit/s; QPS: 10.000 – Conexões WAF-para-servidor suportadas: 60.000 por instância ou 5.000 por domínio • Especificações: WI-100. Desempenho: – Rendimento: 100 Mbit/s; QPS: 2.000 – Conexões WAF-para-servidor suportadas: 60.000 por instância ou 5.000 por domínio
Limite de largura de banda do serviço (O servidor de origem não está implantado no Huawei Cloud.)	30 Mbit/s	50 Mbit/s	100 Mbit/s	N/A	N/A

Escala de serviço	Standard (antiga edição profissional)	Professional (anteriormente Enterprise Edition)	Platinum (antiga edição premium)	Cobrança por uso	Modo Dedicado
Número de domínios	10 (Suporta um nome de domínio de nível superior.)	50 (Suporta cinco nomes de domínio de nível superior.)	80 (Suporta oito nomes de domínio de nível superior.)	30 (Suporta três nomes de domínio de nível superior.)	2.000: (Suporta nomes de domínio de nível superior 2.000)
Quantidade de endereço IP de retorno à origem . (o número de endereços IP back-to-source do WAF que podem ser permitidos por um nome de domínio protegido)	20	50	80	20	N/A
Taxa máxima de defesa de ataque CC	QPS do 100.000	QPS do 300.000	QPS do 1.000.000	N/A	QPS do 500.000
Número de regras de defesa de ataque CC	20	50	100	200	100
Número de regras de proteção precisas	20	50	100	200	100
Número de regras da tabela de referência	N/A	50	100	200	100

Escala de serviço	Standard (antiga edição profissional)	Professional (anteriormente Enterprise Edition)	Platinum (antiga edição premium)	Cobrança por uso	Modo Dedicado
Número de regras de blacklist ou whitelist de endereços de IP	20	100	1.000	200	1.000
Número de regras de controle de acesso de geolocalização	20	50	100	200	100
Número de regras de proteção contra violações da Web	20	50	100	200	100
Número de regras de prevenção de fugas de informação	N/A	50	100	200	100
Número de regras de lista branca de proteção global (anteriormente mascaramento de alarme falso)	1.000	1.000	1.000	2.000	1.000
Número de regras de mascaramento de dados	20	50	100	200	100

Funções suportadas por cada edição

Para as funções de cada edição, ver **Tabela 2-3**. Para atender aos crescentes requisitos de proteção, **atualize a edição do WAF que você está usando**.

Notas:

- √: A função está incluída na edição atual.
- x: A função não está incluída na edição atual.

Tabela 2-3 Recursos de segurança

Função	Standard (antiga edição profissional)	Professional (anteriormente Enterprise Edition)	Platinum (antiga edição premium)	WAF dedicado	Cobrança por uso
Nome de domínio, largura de banda e pacotes de expansão de regras	√	Compatível	Compatível	Incompatível	Incompatível
Adicionando nomes de domínio curinga	√	Compatível	Compatível	Compatível	Compatível
Proteção para portas exceto 80 e 443	√	Compatível	Compatível	Compatível	Compatível
Personalização de portas padrão diferentes das portas 80 e 443	×	Compatível	Compatível	Incompatível	×
Lote configurando políticas de defesa	×	Compatível	Compatível	Compatível	Compatível
Lote adicionando nomes de domínio a uma política	×	Compatível	Compatível	Compatível	√
Proteção contra ataques comuns da Web, como injeções de SQL, XSS, vulnerabilidades de estouro remoto, inclusões de arquivos, vulnerabilidades Bash, execução de comandos remotos, passagem de diretório, acesso a arquivos confidenciais e injeções de comando/código	√	Compatível	Compatível	Compatível	Compatível

Função	Standard (antiga edição profissional)	Professional (anteriormente Enterprise Edition)	Platinum (antiga edição premium)	WAF dedicado	Cobrança por uso
Atualização das regras de proteção contra vulnerabilidades de dia zero para as mais recentes na nuvem e entrega de patches virtuais em tempo hábil	√	Compatível	Compatível	×	Compatível
Detecção de shell da Web	√	Compatível	Compatível	Compatível	√
Inspeção anti-evasão profunda para identificar e bloquear ataques de evasão, como os que usam ofuscação de caracteres homomórficos, injeção de comando com caracteres curinga deformados, UTF7, esquema de URI de dados e outras técnicas	√	Compatível	Compatível	Compatível	√
Inspeção de todos os campos de cabeçalho nas solicitações	√	Compatível	Compatível	Compatível	Compatível
Prevenção de ataques CC	√	Compatível	Compatível	Compatível	Compatível
Proteção precisa	Nem todos são suportados	Compatível	Compatível	Compatível	Nem todos são suportados
Gerenciamento de tabela de referência	×	Compatível	Compatível	Compatível	×
Lista branca de endereços IP e lista negra e importação em lote de endereços IP / intervalos de endereços IP)	√	Compatível	Compatível	Compatível	Compatível
Permitir ou bloquear solicitações da Web com base nos países de origem das solicitações.	Incompatível	Compatível	Compatível	Compatível	Compatível

Função	Standard (antiga edição profissional)	Professional (anteriormente Enterprise Edition)	Platinum (antiga edição premium)	WAF dedicado	Cobrança por uso
Proteção contra adulteração de páginas da Web	√	Compatível	Compatível	Compatível	√
Identificação e bloqueio do comportamento do rastreador, como mecanismos de pesquisa, scanners, ferramentas de script e outros rastreadores	×	Compatível	Compatível	Compatível	√
Proteção anti-crawler baseada em JavaScript	×	Compatível	Compatível	Compatível	×
Prevenção de vazamento de informações	×	Compatível	Compatível	Compatível	√
Lista branca de proteção global (anteriormente mascaramento de alarme falso)	Compatível	Compatível	Compatível	Compatível	Compatível
Mascaramento de dados	√	Compatível	Compatível	Compatível	Compatível

3 Funções

O WAF facilita o gerenciamento de riscos de segurança da Web.

Proteção de serviço HTTP/HTTPS

O WAF mantém os aplicativos estáveis e seguros. Ele examina solicitações HTTP e HTTPS para detectar e bloquear ataques, como injeções de SQL (Structure Query Language), cross-site scripting (XSS), upload de shell da web, injeções de comando ou código, inclusão de arquivos, acesso a arquivos sensíveis, explorações de vulnerabilidade de terceiros, Ataques CC, rastreadores mal-intencionados e falsificação de solicitações entre sites (CSRF).

WebSocket/WebSockets

O WAF é compatível com o protocolo WebSocket/WebSockets, que é ativado por padrão.

Proteção Básica da Web

Com um extenso banco de dados de reputação predefinido, o WAF protege contra as 10 principais ameaças do Open Web Application Security Project (OWASP), exploits de vulnerabilidade, web shells e outras ameaças.

- Proteção completa

  O WAF detecta e bloqueia ataques variados, como injeção SQL, XSS, vulnerabilidades de estouro remoto, inclusões de arquivos, vulnerabilidades Bash, execução de comandos remotos, ataques de passagem de diretório (caminho), acesso não autorizado a arquivos confidenciais, injeções de comando/código e ataques de injeção XML ou Xpath.
- Detecção de shell da Web

  O WAF protege contra web shells da interface de upload.
- Identificação precisa
  - O WAF usa mecanismo de análise semântica integrado e mecanismo de regex e suporta a configuração de regras de lista negra/lista branca, o que reduz os falsos positivos.
  - O WAF suporta anti-escape e restauração automática de códigos comuns, o que melhora a capacidade de reconhecer ataques de deformação na web.

    O WAF pode decodificar os seguintes tipos de código: url_encode, Unicode, XML, OCT, hexadecimal, HTML escape e código base64, confusão de casos, concatenação JavaScript e shell PHP

- Inspeção profunda

  O WAF identifica e bloqueia ataques de evasão, como os que usam ofuscação de caracteres homomórficos, injeção de comando com caracteres curinga deformados, UTF7, esquema de URI de dados e outras técnicas.

- Detecção de cabeçalho

  O WAF detecta todos os campos de cabeçalho nas solicitações.

Prevenção de Ataques CC

Você pode personalizar uma regra de proteção contra ataques da CC para restringir o acesso a um URL específico em seu site com base em um endereço IP, cookie ou Referer, mitigando os ataques da CC. As ações de proteção das regras de proteção contra ataques CC incluem **Verification code**, **Block**, **Dynamically block**, e **Log only**.

- Configuração de política flexível

  O WAF permite que você defina de forma flexível políticas de limitação de taxa por endereço IP, cookie ou campo Referer.

- Personalização da página exibida

  Você pode personalizar o conteúdo retornado e os tipos de página para atender a diversas necessidades de serviço.

Dados de segurança baseados em GUI

O WAF fornece uma interface baseada em GUI para monitorar informações de ataques e registros de eventos em tempo real.

- Configuração centralizada de políticas

  No console do WAF, você pode configurar políticas aplicáveis a vários nomes de domínio protegidos de maneira centralizada para que as políticas possam ser entregues rapidamente e entrar em vigor.

- Estatísticas de tráfego e eventos

  O WAF exibe o número de solicitações, o número e os tipos de eventos de segurança e as informações de registro em tempo real.

Portas não padronizadas

Além das portas padrão 80 e 443, o WAF também suporta portas não padrão.

Tabela 3-1 Supported ports

Edition	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
Standard edition (formerly professional edition) billed on	Standard ports	80	443	Unlimited

Edition	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
a pay-per-use basis	Non-standard ports (89 in 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** ● Standard edition (formerly professional edition): protection up to 10 non-standard ports ● Cloud mode in pay-per-use billing mode: 20 non-standard ports supported
Professional edition (formerly enterprise edition)	Standard ports	80	443	Unlimited

Edition	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
	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**

Edition	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
		48800, 52725, 52726, 60008, 60010		
Platinum edition (formerly premium edition)	Standard ports	80	443	Unlimited
	Non-standard ports (236 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, 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**

Proteção precisa

Suporta políticas de controle de acesso com base em parâmetros e logic- precisas.

- Uma variedade de condições de parâmetros

  Defina condições com combinações de parâmetros HTTP comuns, como **IP**, **URL**, **Referer**, **User Agent**, **Params**, e **Header**.
- Condições lógicas abundantes

  O WAF bloqueia ou permite tráfego com base em condições lógicas, como "Incluir", "Excluir", "Igual a", "Não é igual a", "Prefixo é" e "Prefixo não é".

Lista negra e lista branca de endereços IP

Esta função permite que você coloque endereços IP na lista negra ou na lista branca ou um intervalo de endereços IP para melhorar a precisão da defesa. O WAF suporta a importação em lote de endereços IP ou intervalos de endereços IP.

Fonte de ataque conhecida

- Se o WAF bloquear uma solicitação mal-intencionada por endereço IP, cookie ou parâmetros, você poderá configurar uma regra de origem de ataque conhecida para permitir que o WAF bloqueie automaticamente todas as solicitações da origem de ataque por uma duração de bloqueio definida na regra de origem de ataque conhecida.
- As regras de origem de ataque conhecidas podem ser definidas com base em ataques bloqueados contra a proteção básica da Web, proteção de acesso precisa e regras de lista negra e lista branca.

Proteção de conexão

Se um grande número de erros 502 Bad Gateway e 504 Gateway Timeout forem detectados, você poderá ativar a proteção contra avarias do WAF e a proteção de conexão para permitir que o WAF suspenda seu site e proteja seus servidores de origem contra falhas. Quando as solicitações de erro 502/504 e as solicitações de URL pendentes atingem os limites configurados, o WAF ativa a proteção correspondente para seu site.

Configurando o tempo limite de conexão

- O tempo limite padrão para conexões entre um navegador e o WAF é de 120 segundos, o que não pode ser definido manualmente.
- A duração padrão do tempo limite para conexões entre o WAF e o servidor de origem é de 60 segundos. Se você usar uma instância dedicada do WAF ou uma instância do WAF na nuvem na edição profissional (anteriormente Enterprise Edition) ou na edição platinum (anteriormente Ultimate Edition), poderá personalizar uma duração de tempo limite.

  Na área **Basic Information** da página de informações do site, ative as **Timeout Settings**. Em seguida, clique em ao lado de **WAF-to-Server Connection Timeout**, **Read Timeout**, e **Write Timeout**, modifique as configurações uma a uma e clique em para salvar.

Controle de acesso por localização geográfica

Você pode permitir algumas solicitações da Web e bloquear outras com base nas localizações geográficas dos endereços IP dos quais as solicitações se originam.

Prevenção de adulteração de páginas da Web

Você pode configurar o cache para páginas da Web estáticas. Quando um usuário acessa uma página da Web, o sistema retorna uma página em cache para o usuário e verifica aleatoriamente se a página foi adulterada.

Proteção Anti-Crawler

O WAF analisa dinamicamente seus modelos de serviços de sites e identifica com precisão mais de 700 tipos de comportamento de rastreadores com base em sistemas de controle de risco de dados e identificação de bots

- Biblioteca de funcionalidades

  Bloqueia o rastreamento de páginas da Web com regras de scanner e rastreador definidas pelo usuário. Esse recurso melhora a precisão da proteção.

- JavaScript

  Identifica e bloqueia o rastreamento do JavaScript com regras definidas pelo usuário.

Lista branca de Proteção Global (Anteriormente Mascaramento de Alarme Falso)

Essa função permite ignorar certas regras de detecção de ataques para solicitações específicas.

Mascaramento de dados

O WAF mascara informações confidenciais, como nomes de usuários e senhas, no registro de eventos.

Prevenção contra vazamento de informações

O WAF impede que suas informações confidenciais sejam divulgadas em páginas da Web, como números de identificação, números de telefone e endereços de e-mail.

Confiável

O WAF pode ser implantado em vários clusters em várias regiões com base no princípio do balanceamento de carga. Isso pode evitar pontos únicos de falhas (os SPOF) e garantir a expansão suave da capacidade online, maximizando a estabilidade do serviço.

Notificação de alarme

Você pode habilitar a notificação para logs de ataque. Depois que essa função estiver ativada, o WAF enviará registros de ataque para você pelo método configurado.

Gerenciamento de eventos

- O WAF permite visualizar e manipular alarmes falsos para eventos bloqueados ou registrados.

- Você pode baixar dados de eventos dos últimos cinco dias.
- Você pode usar o Serviço de Tanque de Registros (LTS) na HUAWEI CLOUD para registrar todos os registros do WAF, incluindo registros de ataque e acesso.

4 Vantagens do produto

O WAF examina o tráfego da Web de várias dimensões para identificar com precisão solicitações maliciosas e ataques de filtro, reduzindo os riscos de adulteração ou roubo de dados.

Identificar ameaças com precisão e eficiência

- O WAF usa mecanismos duplos de regras e IA e integra nossas regras de segurança e práticas recomendadas mais recentes.
- Você pode configurar políticas de nível empresarial para proteger seu site com mais precisão, incluindo páginas de alarme personalizadas, combinando várias condições em uma regra de proteção contra ataques CC e colocando na lista negra ou na lista branca um grande número de endereços IP.

Vulnerabilidades de dia zero corrigidas rapidamente

Uma equipe de segurança especializada fornece suporte de serviço 24 horas por dia, 7 dias por semana, para corrigir vulnerabilidades de dia zero em até 2 horas.

Proteção Forte para Privacidade de Dados do Usuário

- Informações confidenciais, como contas e senhas, em registros de ataque podem ser anonimizadas.
- Verificações PCI-DSS para criptografia SSL estão disponíveis.
- A versão mínima do protocolo TLS e o conjunto de cifras podem ser configurados.

Excelente ajuda na Certificação de Segurança

Facilite o cumprimento dos requisitos de conformidade para a certificação DJCP (ou MLPS) e PCI DSS.

5 Cenários de aplicação

Proteção comum

O WAF ajuda a se defender contra ataques comuns da Web, como injeção de comandos e acesso a arquivos confidenciais.

Proteção para atividades de promoção de shopping center online

Inúmeras solicitações maliciosas podem ser enviadas para interfaces de serviço durante promoções online. O WAF permite políticas de limitação de taxa configuráveis para se defender contra ataques CC. Isso evita que os serviços quebrem devido a muitas solicitações simultâneas, garantindo a resposta a solicitações legítimas.

Proteção contra vulnerabilidades de dia zero

Os serviços não podem se recuperar rapidamente do impacto de vulnerabilidades de dia zero em estruturas e plug-ins da Web de terceiros. O WAF atualiza as regras de proteção predefinidas imediatamente para adicionar uma camada de proteção adicional a essas estruturas e plug-ins da Web, e essa camada pode reagir mais rapidamente do que corrigir as vulnerabilidades.

Prevenção de vazamento de dados

O WAF impede que agentes mal-intencionados usem métodos como injeção de SQL e shells da Web para ignorar a segurança do aplicativo e obter acesso remoto a bancos de dados da Web. Você pode configurar regras anti-vazamento de dados no WAF para fornecer as seguintes funções:

- Identificação precisa

  O WAF usa análise semântica e regex para examinar o tráfego de diferentes dimensões, detectando com precisão o tráfego malicioso.

- Detecção de ataques de distorção

  O WAF detecta uma ampla gama de padrões de ataques de distorção com 7 métodos de decodificação para evitar tentativas de desvio.

Prevenção de adulteração de páginas da Web

O WAF garante que os invasores não possam deixar backdoors em seus servidores da Web ou adulterar o conteúdo da página da Web, evitando danos à sua credibilidade. Você pode

configurar regras de proteção contra violações da Web no WAF para fornecer as seguintes funções:

- Detecção de código malicioso no site

  Você pode configurar o WAF para detectar código malicioso injetado em servidores da Web e garantir visitas seguras a páginas da Web.

- Prevenção de adulteração de páginas da Web

  O WAF impede que invasores adulterem o conteúdo de páginas da Web ou publiquem informações inadequadas que podem prejudicar sua reputação.

6 Descrição do Faturamento

O WAF suporta faturamento anual/mensal (pré-pago) e cobrança por uso (pós-pago). Para a nuvem WAF cloud, ambos os modos de cobrança são suportados. Para instâncias dedicadas do WAF, apenas o faturamento pay-per-use é suportado.

Para obter detalhes, consulte **Detalhes de Preço do Produto**.

AVISO

As API do WAF são gratuitas.

Item cobrado

Você será cobrado pelas instâncias do WAF selecionadas com base no modo de cobrança especificado.

Figura 6-1 Modo de cobrança do WAF

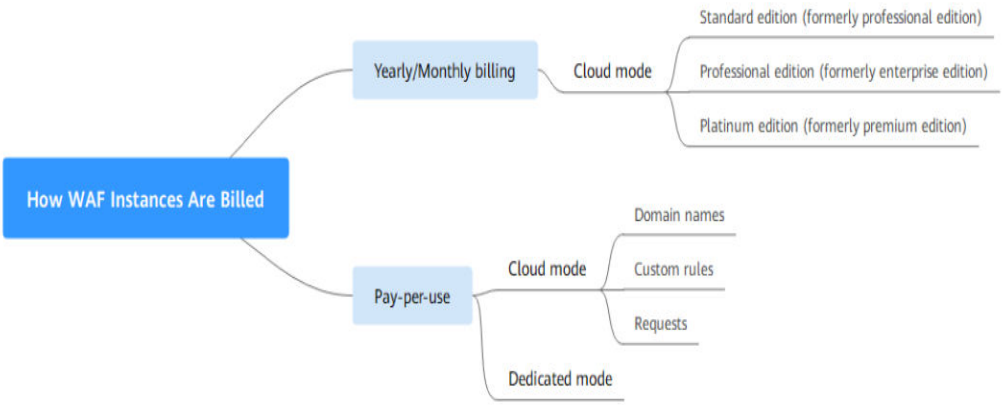


Tabela 6-1 Item cobrado

Modo de compra:	Modo de cobrança	Item cobrado	Descrição do Faturamento
Modo de nuvem	Anual/ Mensal	Edição (obrigatório)	Você será cobrado pela edição que comprou. As regras de preços das edições padrão (anteriormente Professional Edition), Professional (anteriormente Enterprise Edition) e Platinum (anteriormente Premium Edition) são diferentes. Para obter detalhes sobre as especificações e funções de cada edição, consulte **Diferenças de edição**.
		Pacote de expansão de domínio (Opcional)	Faturado com base no número de pacotes de expansão de domínio comprados
		Pacote de expansão de largura de banda (Opcional)	Faturado com base no número de pacotes de expansão de largura de banda comprados
		Pacote de expansão de regras (Opcional)	Faturado com base em quantos pacotes você comprou.
		Duração solicitada	Faturado em uma base anual ou mensal
	Cobrança por uso	● Número de domínios ● Número de regras personalizadas ● Número de solicitações	● Número de nomes de domínio: Cobrado em uma base horária. Depois que um nome de domínio for adicionado durante o período de cobrança, ele será cobrado, independentemente de quando for excluído. ● Número de regras personalizadas: Faturado diariamente. A faturação é calculada às 00:00 todos os dias. ● Número de solicitações: Faturado mensalmente.
Modo Dedicado	Cobrança por uso	Número de instâncias	Faturamento com base no que você usa

NOTA

A alternância entre pagamentos anuais/mensais e pagamentos por uso é suportada por instâncias WAF na nuvem.

Opções de Faturamento

- **Yearly/Monthly**: compatível com as instâncias WAF na nuvem. Quanto mais tempo você se inscrever, mais você economiza. Uma instância WAF de nuvem anual/mensal é cobrada com base na duração exigida selecionada.
- **Pay-per-use**: Este modo de cobrança permite que você faça uma assinatura ou cancelamento a qualquer momento.
  - Para uma instância WAF de nuvem paga por uso, você é cobrado pelo número de nomes de domínio adicionados, número de regras personalizadas e número de solicitações usadas.
  - Para uma instância WAF dedicada de pagamento por uso, você é cobrado pela duração necessária (precisa até a segunda), que começa quando a instância é criada e termina quando a instância é excluída.

Alteração das Opções de Faturamento

- No modo de cobrança anual/mensal, você pode atualizar a edição da instância do WAF ou aumentar o número de pacotes de expansão de nome de domínio, largura de banda e regras para atender às necessidades da sua empresa.
- Cancelamento de assinatura: Se você não precisar mais da instância do WAF que é cobrada anualmente/mensalmente, **cancele a assinatura** dela no Centro de cobrança.

Renovação

Se você não renovar uma instância WAF faturada anualmente/mensalmente após sua expiração, um período de retenção estará disponível para você.

Para obter detalhes, consulte **Período de Retenção**.

- During this period, WAF only forwards traffic but does not check it against your protection policies.
- When this period ends, resources will be cleared, that is, all configurations of your domain names will be deleted. During the clearing period, domain names are pointed back to origin severs by default. However, services on your domain names may not run properly because there may be inconsistencies between your configured protocols and ports.

Para evitar perdas desnecessárias causadas por problemas de segurança, renove sua assinatura antes que o período de retenção expire. A expiração do WAF não afeta seus outros serviços.

Você pode renovar seus recursos no console de gerenciamento. Para obter detalhes, consulte **Regras de renovação**.

Expiração e pagamento em atraso

- Vencimento

  Se você não renovar uma instância do WAF faturada anualmente/mensalmente após sua expiração, um período de retenção estará disponível para você. Para obter detalhes, consulte **Período de retenção**.

- Pagamento em atraso

  Se sua conta de instâncias do WAF cobradas anualmente/mensalmente estiver em atraso, recarregue sua conta em tempo hábil para permitir que o WAF proteja seu site continuamente. Para obter detalhes, consulte **Como um cliente comum da HUAWEI CLOUD responde?**

7 Mecanismo de Proteção de Dados Pessoais

Para garantir que os dados pessoais dos visitantes do site, como nome de usuário, senha e número de telefone celular, não sejam obtidos por entidades ou pessoas não autorizadas ou não autenticadas e para evitar vazamento de dados, O WAF criptografa seus dados pessoais antes de armazená-los para controlar o acesso aos dados e registra logs para operações realizadas nos dados.

Dados Pessoais a Recolher

O WAF registra solicitações que acionam alarmes de ataque em registros de eventos. **Tabela 7-1** fornece os dados pessoais coletados e gerados pela WAF.

Tabela 7-1 Dados pessoais

Tipo	Método de recolha	Pode ser modificado	Obrigatório
Solicitar endereço de IP de origem	Endereço de IP do atacante bloqueado ou registrado pelo WAF quando o nome de domínio é atacado.	Não	Sim
URL	URL atacado do nome de domínio protegido ou URL do nome de domínio protegido bloqueado ou registrado pelo WAF.	Não	Sim

Tipo	Método de recolha	Pode ser modificado	Obrigatório
Informações de cabeçalho HTTP/ HTTPS (incluindo o cookie)	Valor do cookie e valor do cabeçalho inseridos na página de configuração quando você configura um ataque de CC ou uma regra de proteção precisa.	Não	Não Se os campos de cookie e cabeçalho configurados não contiverem informações pessoais dos usuários, as solicitações registradas pelo WAF não coletarão nem gerarão tais dados pessoais.
Parâmetros de solicitação (Get e Post)	Solicitar detalhes registrados pelo WAF nos registros de proteção.	Não	Não Se os parâmetros de solicitação não contiverem informações pessoais dos usuários, as solicitações registradas pela WAF não coletarão nem gerarão tais dados pessoais.

Modo de armazenamento

Os valores de campos sensíveis são salvos após serem anonimizados e os valores de outros campos são salvos em texto simples em logs.

Controle de acesso

Os usuários podem visualizar apenas logs relacionados aos seus próprios serviços.

8 Gerenciamento de permissões do WAF

Para atribuir permissões diferentes aos funcionários de sua empresa para acessar seus recursos do WAF, o IAM é uma boa opção para o gerenciamento de permissões refinado. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos da HUAWEI CLOUD.

Com o IAM, você pode usar sua conta da HUAWEI CLOUD para criar usuários do IAM para seus funcionários e atribuir permissões aos usuários para controlar seu acesso a tipos de recursos específicos. Por exemplo, alguns desenvolvedores de software em sua empresa precisam usar recursos do WAF, mas não devem excluí-los ou executar operações de alto risco. Para alcançar esse resultado, você pode criar usuários do IAM para os desenvolvedores de software e conceder a eles apenas as permissões necessárias para usar os recursos do WAF.

Se sua conta da HUAWEI CLOUD não precisar de usuários individuais do IAM para gerenciamento de permissões, você poderá pular este capítulo.

IAM pode ser usado gratuitamente. Você paga apenas pelos recursos em sua conta. Para obter mais detalhes, consulte **Visão geral do IAM**.

Permissões do WAF

Por padrão, os novos usuários de IAM não têm nenhuma permissão atribuída. Você precisa adicionar um usuário a um ou mais grupos e anexar políticas de permissões ou funções a esses grupos. Os usuários herdam permissões dos grupos aos quais são adicionados e podem executar operações especificadas em serviços de nuvem com base nas permissões.

O WAF é um serviço de nível de projeto implantado e acessado em regiões físicas específicas. Para atribuir permissões do WAF a um grupo de usuários, especifique o escopo como projetos específicos da região e selecione os projetos para que as permissões entrem em vigor. Se **All projects** estiver selecionado, as permissões entrarão em vigor para o grupo de usuários em todos os projetos específicos da região. Ao acessar o WAF, os usuários precisam mudar para uma região onde foram autorizados a usar o serviço WAF.

Você pode conceder permissões aos usuários usando funções e políticas.

- Funções: Um tipo de mecanismo de autorização grosseira que define permissões relacionadas às responsabilidades dos usuários. Apenas um número limitado de funções de nível de serviço para autorização está disponível. Você também precisa atribuir outras funções dependentes para que o controle de permissão entre em vigor. As funções não são ideais para autorização refinada e controle de acesso seguro.

- Políticas: Um mecanismo de autorização refinado que define as permissões necessárias para executar operações em recursos de nuvem específicos sob certas condições. Esse mecanismo permite uma autorização baseada em políticas mais flexível e atende aos requisitos de controle de acesso seguro. Por exemplo, você pode conceder aos usuários do WAF somente as permissões para gerenciar um determinado tipo de recursos. A maioria das políticas define permissões com base nas API. Para as ações de API suportadas pelo WAF, consulte **Políticas de permissões e ações suportadas** .

Tabela 8-1 lista todas as funções do sistema suportadas pelo WAF.

Tabela 8-1 Políticas do sistema suportadas pelo WAF

Nome da Função/ Política	Descrição	Categoria	Dependências
Administrador do WAF	Permissões de administrador para WAF	Função definida pelo sistema	Depende das funções **Tenant Guest** e **Server Administrator**. ● **Tenant Guest**: Um papel global, que deve ser atribuído no projeto global. ● **Server Administrator**: Uma função no nível do projeto, que deve ser atribuída no mesmo projeto.
FullAccess do WAF	Todas as permissões para WAF	Política definida pelo sistema	Nenhuma
ReadOnlyAccess do WAF	Permissões somente leitura para WAF.	Política definida pelo sistema	

Links úteis

- **Visão geral do IAM**
- **Criando um Grupo de Usuários e Usuários e Concedendo Permissões WAF**
- **Políticas personalizadas do WAF**
- **Permissões do WAF e ações suportadas**

Conteúdo da Política de FullAccess do WAF

```
{    "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"
        }
               ]
}
```

Conteúdo da Política de ReadOnlyAccess do WAF

```
{
    "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 e outros serviços

Este tópico descreve o WAF e outros serviços de nuvem.

CTS

Cloud Trace Service (CTS) registra todas as operações do WAF para você consultar, auditar e rastrear.

AVISO

Atualmente, o CTS está disponível nas seguintes regiões:

- CN-Hong Kong
- AP-Bangkok
- AP-Singapura
- AF-Joanesburgo
- AL-Santiago

Tabela 9-1 Operações WAF que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Nome do Rastreamento
Criando uma instância do WAF	instância	createInstance
Deletando uma instância do WAF	instância	deleteInstance
Modificando uma instância do WAF	instância	alterInstanceName
Modificando o status de proteção de uma instância do WAF	instância	modifyProtectStatus
Modificando o status de conexão de uma instância do WAF	instância	modifyAccessStatus
Criando uma política WAF	política	createPolicy

Operação	Tipo de recurso	Nome do Rastreamento
Aplicação de uma política WAF	política	applyToHost
Modificando uma política	política	modifyPolicy
Exclusão de uma política do WAF	política	deletePolicy
Modificando configurações de notificação de alarme	alertNoticeConfig	modifyAlertNoticeConfig
Carregando um certificado	certificado	createCertificate
Alteração de nome de um certificado	certificado	modifyCertificate
Exclusão de um certificado	certificado	deleteCertificate
Adicionando uma regra de proteção contra ataques CC	política	createCc
Modificando uma regra de proteção contra ataques CC	política	modifyCc
Excluindo uma regra de proteção contra ataques CC	política	deleteCc
Adicionando uma regra de proteção precisa	política	createCustom
Modificando uma regra de proteção precisa	política	modifyCustom
Exclusão de uma regra de proteção precisa	política	deleteCustom
Adicionando uma regra de lista negra ou de lista branca de endereços IP	política	createWhiteblackip
Modificando uma regra de lista negra ou de lista branca de endereços IP	política	modifyWhiteblackip
Excluindo uma regra de lista negra ou de lista branca de endereços IP	política	deleteWhiteblackip
Adicionando uma regra de proteção contra adulteração da Web	política	createAntitamper
Atualização de uma regra de proteção contra adulteração da Web	política	refreshAntitamper
Excluindo uma regra de proteção contra violação da Web	política	deleteAntitamper
Criando uma regra lista branca de proteção global (anteriormente mascaramento de alarme falso)	política	createIgnore

Operação	Tipo de recurso	Nome do Rastreamento
Excluindo uma regra lista branca de proteção global (anteriormente mascaramento de alarme falso)	política	deleteIgnore
Adicionando uma regra de mascaramento de dados	política	createPrivacy
Modificando uma regra de mascaramento de dados	política	modifyPrivacy
Exclusão de uma regra de mascaramento de dados	política	deletePrivacy

Cloud Eye

O Cloud Eye monitora os indicadores do WAF, para que você possa entender o status de proteção do WAF em tempo hábil e definir as políticas de proteção de acordo. Para obter detalhes, consulte o *Guia do usuário do Cloud Eye* .

Para obter detalhes sobre as métricas monitoradas do WAF, consulte **Métricas monitoradas pelo WAF**

IAM

Identity and Access Management (IAM) fornece a função de gerenciamento de permissões para o WAF. Somente os usuários com permissões de Administrador do WAF podem usar o WAF. Para obter essa permissão, entre em contato com os usuários que têm as permissões de administrador de segurança.

LTS

Log Tank Service (LTS) coleta dados de log de hosts e serviços em nuvem. O WAF permite que você transfira logs de ataque do WAF e logs de acesso ao LTS para que você possa lidar com logs em tempo real.

SMN

Simple Message Notification (SMN) serviço fornece a função de notificação. Depois de ativar a função de notificação no WAF, as informações de alarme serão enviadas para você conforme configuradas assim que seu nome de domínio for atacado.

Gerenciamento corporativo

Você pode gerenciar vários projetos em uma empresa, liquidar separadamente seus custos e atribuir pessoal diferente para eles. Um projeto pode ser iniciado ou interrompido de forma independente, sem afetar os outros. Com **Gestão Empresarial** , pode gerir facilmente os seus projetos depois de criar um projeto empresarial para cada um deles.

O WAF pode ser interconectado com o Gerenciamento Empresarial. Você pode gerenciar recursos do WAF por projeto empresarial e conceder permissões diferentes aos usuários.

