Web Application Firewall

Guia de usuário

Edição 01

Data 2025-01-21

HUAWEI CLOUD COMPUTING 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, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem 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 ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

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 Cloud Computing Technologies Co., Ltd.

Endereço: Huawei Cloud Data Center, Rua Jiaoxinggong
Avenida Qianzhong
Novo Distrito de Gui'an
Guizhou 550029
República Popular da China

Site: https://www.huaweicloud.com/intl/pt-br/

Índice

1 Visão geral....1

2 Compra de WAF....3

2.1 Compra de uma instância do Cloud WAF....3
2.2 Compra de uma instância dedicada do WAF....9
2.3 Atualização de Cloud WAF edição e as especificações (console antigo)....13
2.4 Pacotes de expansão de largura de banda domodo de nuvem de WAF....17
2.5 Pacotes de expansão de domínio doModo de Nuvem WAF....19
2.6 Pacotes de expansão da regra do modo de nuvem do WAF....20

3 Ativação de proteção de WAF....21

3.1 Portas suportadas pelo WAF....21
3.2 Conexão de um site ao WAF (Modo Nuvem)....25
3.2.1 Processo de conexão (modo de nuvem)....25
3.2.2 Passo 1: Adicionando um nome de domínio ao WAF (Modo de Nuvem)....28
3.2.3 Passo 2: Coloque os endereços de IP de WAF na lista branca....45
3.2.4 Passo 3: Testando o WAF....48
3.2.5 Passo 4: Encaminhamento do tráfego do site para o WAF....52
3.3 Conexão de um site ao WAF (Modo Dedicado)....55
3.3.1 Processo de conexão (modo dedicado)....55
3.3.2 Passo 1: Adicionar um site ao WAF (Modo Dedicado)....56
3.3.3 Passo 2: Configurar um balanceador de carga....66
3.3.4 Passo 3: Vincular um EIP a um balanceador de carga....71
3.3.5 Passo 4: Colocando na lista branca o endereço de IP de recuperação da instância WAF dedicada....72

4 Gerenciamento de nomes de domínio do site....77

4.1 Exibição de informações básicas....77
4.2 Alternação de modo de trabalho do WAF....80
4.3 Configuração de verificação de certificação PCI DSS/3DS e a versão do TLS....82
4.4 Ativação de proteção WAF IPv6....90
4.5 Ativação de protocolo HTTP/2....91
4.6 Configuração de tempo limite de conexão....92
4.7 Configuração de proteção de conexão....94
4.8 Alternação de algoritmo de balanceamento de carga....96
4.9 Atualização de um certificado....97

4.10 Configuração de um identificador de tráfego para uma origem de ataque conhecida....101
4.11 Edição de informações do servidor....103
4.12 Modificação de página de alarme....104
4.13 Remoção de um site protegido do WAF....106
5 Gerenciamento de certificado....109
5.1 Carregamento de um certificado....109
5.2 Vinculação de um certificado a um site protegido....112
5.3 Apagar um certificado....114
5.4 Exibição de informações do certificado....116
6 Gerenciamento de grupos de lista negra e lista branca de endereço de IP....118
6.1 Adição de um grupo de endereços de IP....118
6.2 Modificação ou exclusão de um grupo de endereços IP da lista negra ou da lista branca....120
7 Configuração da regra....123
7.1 Guia de configuração....123
7.2 Configuração de regras básicas de proteção de Web....128
7.3 Configuração de controle de acesso inteligente....137
7.4 Configuração de uma regra de proteção contra ataques CC....139
7.5 Configuração de uma regra de proteção precisa....149
7.6 Adição de uma tabela de referência....161
7.7 Configuração de uma regra de lista negra ou de lista branca de endereços IP....164
7.8 Configuração de uma regra de origem de ataque conhecido....172
7.9 Configuração de uma regra de controle de acesso de geolocalização....177
7.10 Configuração de uma regra de proteção contra adulteração da Web....185
7.11 Configuring Anti-Crawler Rules....189
7.12 Configuração de uma regra de prevenção de vazamento de informações....197
7.13 Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule....202
7.14 Configuração de uma regra de mascaramento de dados....207
8 Painel de controle....212
9 Gerenciamento de eventos....217
9.1 Exibição de registros de eventos de proteção....217
9.2 Manipulação de alarmes falsos....219
9.3 Download de dados de eventos....226
10 Ativa LTS para registro em log do WAF....229
11 Ativação de notificações de alarme....244
12 Gerenciamento de políticas....247
12.1 Adição de uma política....247
12.2 Adição de regras a uma ou mais políticas....248
12.3 Aplicação de uma política ao seu site....250
13 Gerenciamento dedicado do motor WAF....252

14 Visualização de detalhes do produto....259

15 Gerenciamento de projetos e projetos corporativos....260

16 Gerenciamento de permissões....262

16.1 Criação de um grupo de usuários e concessão de permissões....262
16.2 Políticas personalizadas do WAF....263
16.3 Permissões do WAF e ações suportadas....265

17 Principais operações gravadas pelo CTS....273

17.1 Operações de WAF gravadas pelo CTS....273
17.2 Exibição de um rastreamento de auditoria....275

18 Monitoramento....277

18.1 Métricas monitoradas pelo WAF....277
18.2 Configuração de regras de monitoramento de alarmes....300
18.3 Exibição de métricas monitoradas....301

1 Visão geral

Depois de ativar o serviço WAF, conecte o nome de domínio do site ao WAF para que todas as solicitações de acesso sejam encaminhadas ao WAF para monitoramento e proteção.

Como usar o WAF

Tabela 1-1 descreve o procedimento para usar o WAF.

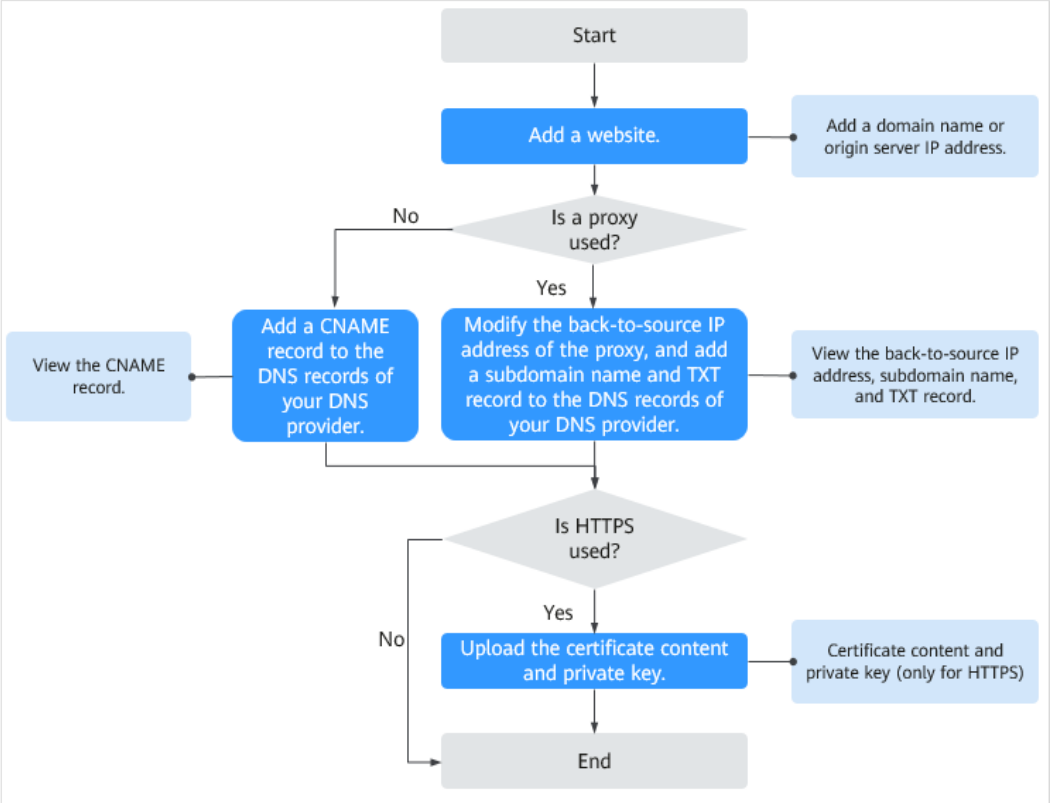
Tabela 1-1 Procedimento para usar o WAF

Etapa	Descrição
Comprando uma instância do WAF	Compre uma instância WAF na nuvem no modo de faturamento anual/mensal ou pay-per-use ou compre instâncias WAF dedicadas faturadas no modo pay-per-use. **AVISO** ● Para comprar instâncias WAF de pagamento por uso, **envie um tíquete de serviço** para ativar o serviço. ● As API do WAF são gratuitas. Para obter detalhes, consulte **Ativação do WAF**.
Adicionando um site ao WAF	Adicione o site que você deseja proteger ao WAF. ● Modo de Nuvem: Consulte **Passo 1: Adicionando um nome de domínio ao WAF (Modo de Nuvem)**. ● Modo Dedicado: Consulte **Passo 1: Adicionar um site ao WAF (Modo Dedicado)**.
Ativação da proteção WAF	Ative a proteção WAF para proteger o site adicionado. **NOTA** ● O uso do WAF não afeta o desempenho do servidor Web porque o mecanismo do WAF não está em execução no servidor Web. ● Depois que seu nome de domínio for conectado ao WAF, haverá uma latência de dezenas de milissegundos, que pode ser aumentada com base no tamanho da página solicitada ou no número de solicitações recebidas.

Etapa	Descrição
Configurando regras de proteção	Use as regras de proteção integradas do WAF e configure regras personalizadas para proteger seu site. Para mais detalhes, veja **Configuração da regra**.
Ativando a notificação de alarme	Habilite esta função para receber uma notificação de alarme no instante em que um ataque é detectado. Para obter detalhes, consulte **Ativação de Notificação de Alarme**.
Manipulação de alarmes falsos	Mascarar eventos bloqueados ou registrados que são tratados como alarmes falsos. Para mais detalhes, veja **Manipulação de alarmes falsos**.
Exibindo o **Dashboard**	Exibir dados de proteção de ontem, hoje, últimos 3 dias, últimos 7 dias ou últimos 30 dias. Para mais detalhes, veja **Painel de controle**.

Para obter detalhes sobre como conectar seu site ao WAF, consulte **Figura 1-1**.

Figura 1-1 Processo de conexão de um site ao WAF



2 Compra de WAF

2.1 Compra de uma instância do Cloud WAF

As instâncias do Cloud WAF são cobradas no modo de cobrança anual/mensal (pré-pago) ou de pagamento por uso (pós-pago). No modo de faturação anual/mensal, estão disponíveis as edições padrão (antiga edição profissional), profissional (antiga edição empresarial) e platina (antiga edição premium). Cada edição oferece pacotes de expansão de domínio, largura de banda e regras.

AVISO

- Para comprar instâncias WAF de pagamento por uso, **envie um tíquete de serviço** para ativar o serviço.
- As API do WAF são gratuitas.

Antes de começar

- Apenas um modo de cobrança pode ser selecionado para sua instância do WAF em uma conta.
- No modo de cobrança anual/mensal, você pode comprar apenas uma edição do WAF na mesma região geográfica.
- Alternar entre pagamentos anuais/mensais e pay-per-use é suportado.
- Para uma instância do WAF na nuvem faturada anualmente/mensalmente, após ela expirar ou você cancelar sua assinatura, você pode ativar outra instância do WAF faturada anualmente/mensalmente ou paga por uso. O serviço WAF pode salvar os dados de configuração da instância do WAF original para que você possa usar os dados de configuração sem precisar configurar a nova instância do WAF somente quando as seguintes condições forem atendidas:
  - Se você escolher o modo de faturamento de pagamento por uso, as instâncias WAF novas e originais deverão estar sob o mesmo projeto na mesma região.
  - Se você escolher o modo de cobrança anual/mensal, as instâncias WAF novas e originais deverão estar na mesma região.

- Para uma instância do WAF na nuvem faturada com base em pagamento por uso, você pode desativar o modo de cobrança anual/mensal e ativar a instância no modo de cobrança anual/mensal ou de pagamento por uso.

  AVISO

  Depois que o modo de cobrança de pagamento por uso é desativado, o faturamento do WAF é interrompido, os dados de configuração do WAF são salvos e o **Mode** WAF é alterado para **Suspended**. Nessa situação, o WAF encaminha o tráfego do seu site sem detectá-lo.

Pré-requisitos

Você obteve credenciais de login do console de gerenciamento para uma conta com as permissões **WAF Administrator** e **BSS Administrator**.

Restrições

- As especificações de uma instância do WAF não podem ser alteradas após a conclusão da compra. Para usar uma instância do WAF com especificações inferiores, cancele a assinatura da instância do WAF que você está usando e compre outra.
- O pacote de expansão só pode ser renovado ou cancelado junto com a instância do WAF que você está usando.

Limitações da especificação

- 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.

Cenários de aplicação

O Cloud WAF é uma boa opção se seus servidores de serviço forem implantados na nuvem ou no local e você planeja proteger seu site adicionando seus nomes de domínio ao WAF.

Os cenários de aplicação para diferentes edições são os seguintes:

- Padrão (antiga edição profissional)

  Esta edição é adequada para sites de pequeno e médio porte que não possuem requisitos especiais de segurança.

- Professional (anteriormente Enterprise Edition)

  Esta edição é adequada 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)

  Esta edição é adequada para sites de empresas de grande e médio porte que possuem serviços de grande escala ou têm requisitos especiais de segurança.

Comprando uma Instância do WAF Faturada Anual/Mensalmente

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 Se você for um usuário iniciante, clique em **Buy WAF Now**.

NOTA

Se você não for um usuário pela primeira vez, clique em **Buy/Upgrade WAF** no canto superior direito.

Passo 5 (Facultativo): Selecione um projeto corporativo na lista suspensa para **Enterprise Project**.

Essa opção só estará disponível se você estiver conectado usando uma conta corporativa ou se tiver habilitado projetos corporativos. Para saber mais, consulte **Ativando o Enterprise Center**. Você pode usar projetos corporativos para gerenciar com mais eficiência os recursos da nuvem e os membros do projeto.

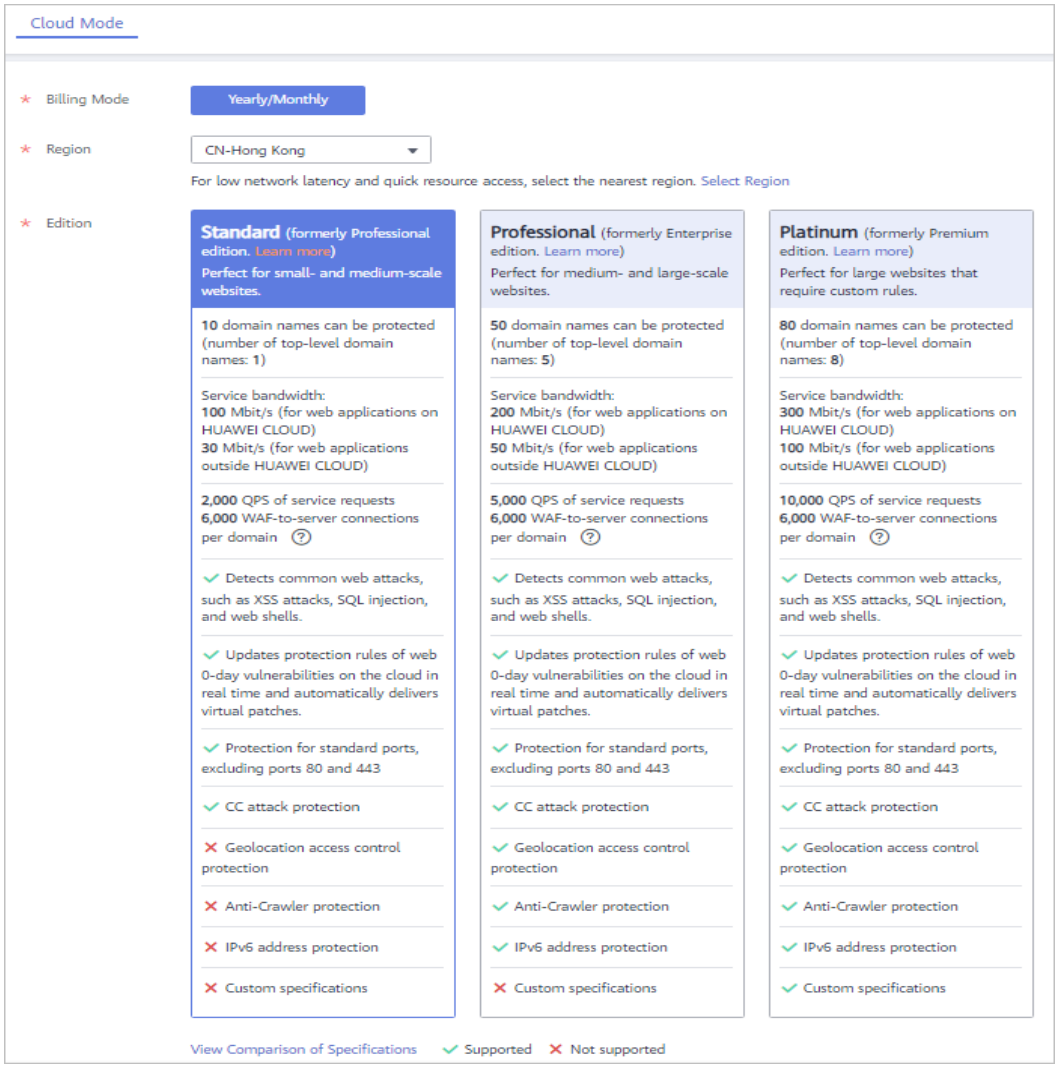
NOTA

- Valor **default** indica o projeto corporativo padrão. Os recursos que não são alocados a nenhum projeto da empresa na sua conta são listados no projeto da empresa padrão.
- A opção **default** está disponível na lista suspensa **Enterprise Project** quando você compra o WAF.

Passo 6 Na página **Buy Web Application Firewall**, selecione **Cloud Mode**.

Passo 7 Na página **Buy Web Application Firewall**, selecione uma região e uma edição. **Figura 2-1** mostra um exemplo.

Figura 2-1 Selecionando a edição do WAF



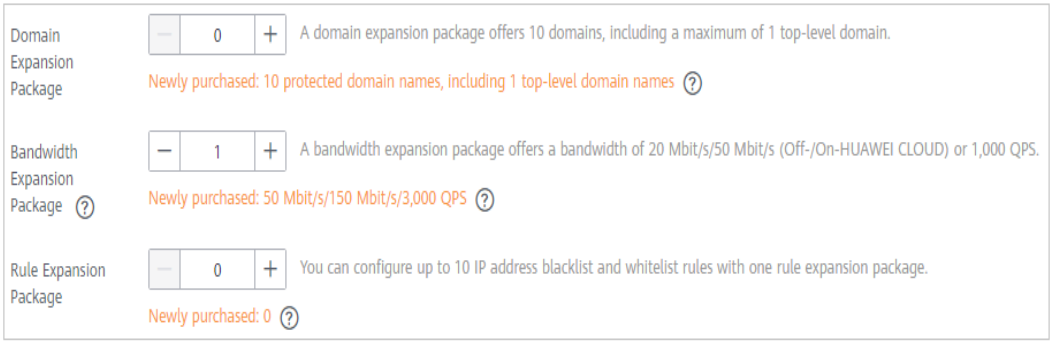
NOTA

Para alternar regiões, selecione uma região na lista suspensa. Apenas uma edição do WAF pode ser comprada em uma região.

Passo 8 Especifique o número de pacotes de expansão de nome de domínio, largura de banda ou regra. **Figura 2-2** mostra um exemplo.

Para mais detalhes, veja **Pacotes de expansão de domínio doModo de Nuvem WAF**, **Pacotes de expansão de largura de banda domodo de nuvem de WAF**, e **Pacotes de expansão da regra do modo de nuvem do WAF**.

Figura 2-2 Seleção de pacotes de expansão



Passo 9 Configure a **Required Duration**. Você pode selecionar a duração necessária de um mês a três anos.

NOTA

Selecione **Auto renew** para que o sistema possa renovar automaticamente sua assinatura de serviço com base na duração necessária especificada aqui após a expiração da assinatura.

Passo 10 No canto inferior direito da página, clique em **Next**.

Passo 11 Confirme os detalhes do pedido e clique em **Pay Now**.

Passo 12 Na página de pagamento, selecione um método de pagamento e pague seu pedido.

----Fim

Comprando uma Instância do WAF Faturada em uma Base de Pagamento por Uso

Para comprar instâncias WAF de pagamento por uso, **envie um tíquete de serviço** para ativar o serviço.

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

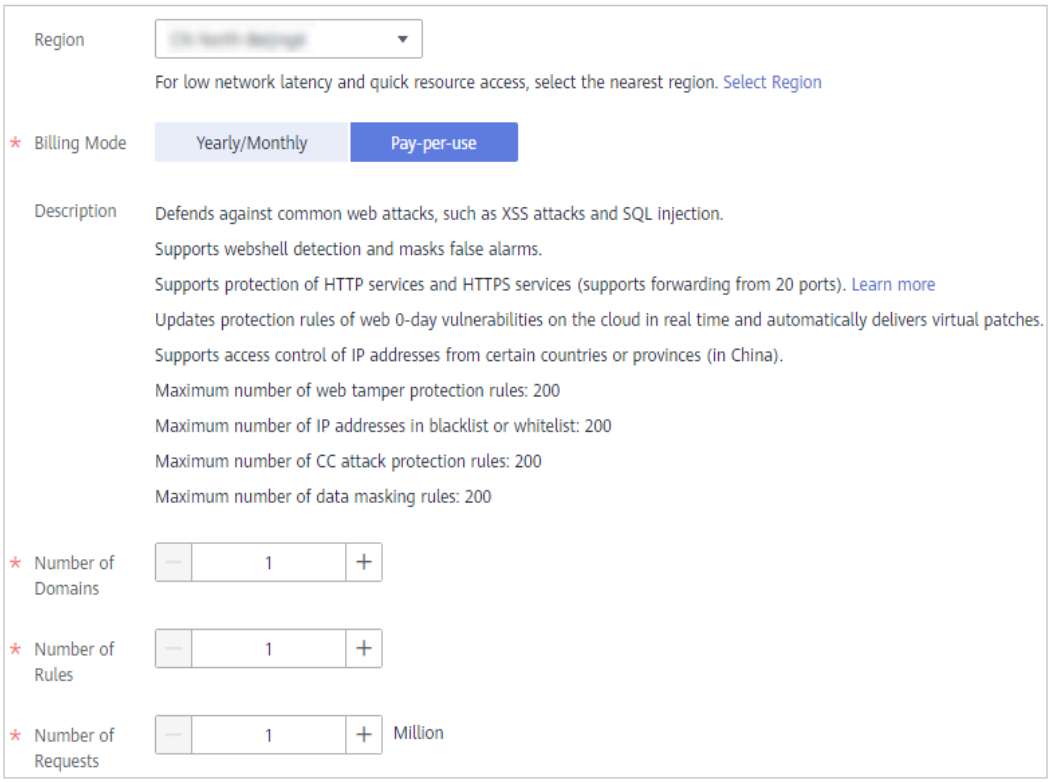
Passo 4 Se você for um usuário iniciante, clique em **Buy WAF Now**.

NOTA

Se você não for um usuário iniciante, clique em **Buy WAF** no canto superior direito da página.

Passo 5 Na página **Buy Web Application Firewall**, selecione **Pay-per-use**, selecione uma edição e configure o número de nomes de domínio, regras e solicitações. **Figura 2-3** mostra um exemplo.

Figura 2-3 Selecionando **pay-per-use**



NOTA

Para alternar regiões, selecione uma região na lista suspensa **Region**.

Passo 6 No canto inferior direito da página, clique em **Next**.

Passo 7 Clique em **Back to Website Settings** e adicione nomes de domínio de sites a serem protegidos.

NOTA

Para desativar o WAF, clique em **Disable Pay-per-Use Cloud WAF** no canto superior direito da página.

----Fim

Verificação

Sua instância do WAF é comprada quando sua edição de instância e seus dias de validade restantes são exibidos no canto superior direito do console de gerenciamento.

Outras operações

- **Atualização de Cloud WAF edição e as especificações (console antigo)**

  No modo de nuvem, para proteger mais nomes de domínio ou tráfego, atualize a edição de instância ou aumente o número de pacotes de expansão.

2.2 Compra de uma instância dedicada do WAF

Se seus servidores de serviço forem implantados na HUAWEI CLOUD, você poderá comprar uma instância WAF dedicada para proteger nomes de domínio importantes ou serviços da Web apenas com endereços IP. Para expandir as capacidades de proteção e eliminar pontos únicos de falha (os SPOF), compre um balanceador de carga Elastic Load Balance (ELB) para suas instâncias WAF dedicadas.

As instâncias dedicadas do WAF são cobradas com base em pagamento por uso. Você paga apenas pelo que usa.

Pré-requisitos

- Você obteve credenciais de login do console de gerenciamento para uma conta com **WAF Administrator**, **WAF FullAccess**, e **BSS Administrator**.
- Uma VPC foi criada.

Restrições

Se a instância WAF dedicada e o servidor de origem não estiverem na mesma VPC, ative a comunicação entre a instância e a sub-rede do servidor de origem no grupo de segurança. Você pode usar **Conexão de emparelhamento VPC** para habilitar a comunicação entre as VPC.

NOTA

Para obter detalhes sobre as regiões suportadas, consulte **Em que regiões o WAF está disponível?**

Limitações da especificação

As especificações de uma instância WAF dedicada não podem ser modificadas.

Cenários de aplicação

Instâncias WAF dedicadas são uma boa escolha se seus servidores de serviço estiverem implantados na HUAWEI CLOUD e você planeja proteger seu site adicionando seus nomes de domínio ou endereços IP ao WAF.

Sites corporativos de grande porte adequados que tenham uma grande escala de serviço e tenham requisitos de segurança personalizados.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em ☰ no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 3 Se você for um usuário iniciante, clique em **Buy WAF Now**.

NOTA

Se você não for um usuário pela primeira vez, clique em **Buy/Upgrade WAF** no canto superior direito.

Passo 4 (Facultativo): Selecione um projeto corporativo na lista suspensa para **Enterprise Project**.

Essa opção só estará disponível se você estiver conectado usando uma conta corporativa ou se tiver habilitado projetos corporativos. Para saber mais, consulte **Ativando o Enterprise Center**. Você pode usar projetos corporativos para gerenciar com mais eficiência os recursos da nuvem e os membros do projeto.

NOTA

- Valor **default** indica o projeto corporativo padrão. Os recursos que não são alocados a nenhum projeto da empresa na sua conta são listados no projeto da empresa padrão.
- A opção **default** está disponível na lista suspensa **Enterprise Project** quando você compra o WAF.

Passo 5 Na página **Buy Web Application Firewall**, selecione **Dedicated Mode**.

Passo 6 Configure os parâmetros da instância referindo-se a **Tabela 2-1**. **Figura 2-4** mostra um exemplo.

Figura 2-4 Configuração de uma instância dedicada do WAF

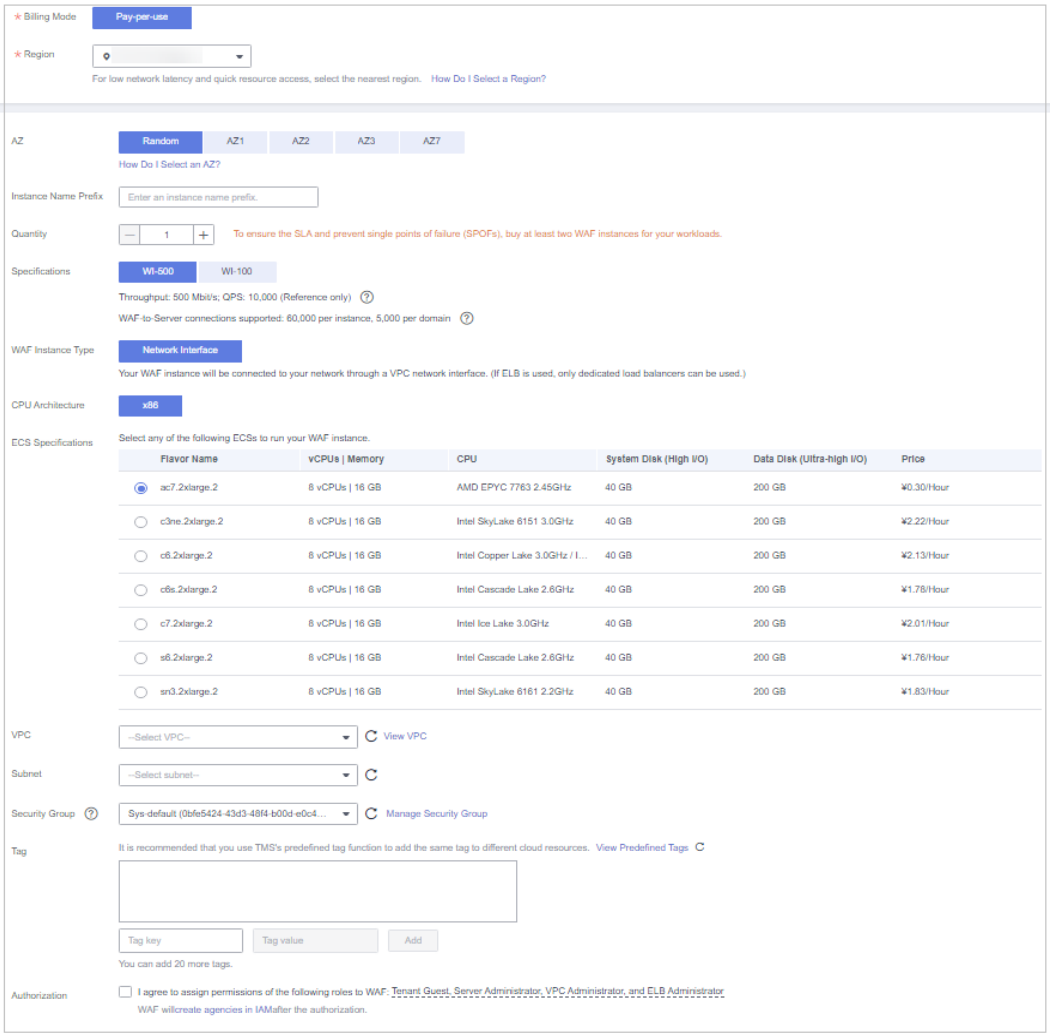


Tabela 2-1 Parâmetros de uma instância dedicada do WAF

Parâmetro	Descrição
Região	Para obter detalhes sobre as regiões suportadas, consulte **Em que regiões o WAF está disponível?** Geralmente, uma instância do WAF comprada em qualquer região pode proteger serviços da Web em todas as regiões. Para fazer com que uma instância do WAF encaminhe o tráfego do seu site mais rapidamente, selecione a região mais próxima dos seus serviços.
AZ	Selecione uma AZ na região selecionada.
Prefixo do Nome da Instância	Defina um prefixo do nome de instância do WAF dedicado. Se você comprar várias instâncias, o prefixo para cada nome de instância será o mesmo.
Quantidade	Defina o número de instâncias do WAF que você deseja comprar. Recomendamos que você compre pelo menos duas instâncias do WAF e use as duas para proteger seus serviços. Com várias instâncias do WAF sendo usadas para seus serviços, se uma delas apresentar defeito, o WAF alterna automaticamente o tráfego para outras instâncias do WAF em execução para garantir a proteção contínua.
Especificações	Especificações **WI-500** e **WI-100** estão disponíveis.
Tipo de instância do WAF	Selecione um tipo de instância do WAF. Apenas **Network interface** está disponível agora. A instância do WAF será conectada à sua rede por meio de uma interface de rede VPC. Se o ELB for usado, somente balanceadores de carga dedicados poderão ser usados.
Arquitetura da CPU	Selecione a arquitetura da CPU para sua instância.
Especificações da CPU	Selecione as especificações do ECS para sua instância.
VPC	Selecione a VPC à qual o servidor de origem pertence.
Sub-rede	Selecione uma sub-rede configurada na VPC.

Parâmetro	Descrição
Grupo de segurança	Selecione um grupo de segurança na região ou clique em **Manage Security Group** para acessar o console da VPC e criar um grupo de segurança. Depois de selecionar um grupo de segurança, a instância do WAF será protegida pelas regras de acesso do grupo de segurança. **AVISO** ● Você pode configurar seu grupo de segurança da seguinte maneira: – Regras de entrada Adicione uma regra de entrada para permitir que o tráfego de rede de entrada passe por uma porta especificada com base em seus requisitos de serviço. Por exemplo, se você quiser permitir o acesso da porta 80, você pode adicionar uma regra que permite **TCP** e porta **80**. – Regras de saída Todo o tráfego de rede de saída é permitido por padrão. Para obter mais detalhes, consulte **Adicionando uma regra de grupo de segurança**. ● Se a instância WAF dedicada e o servidor de origem não estiverem na mesma VPC, habilite a comunicação entre a instância e a sub-rede do servidor de origem no grupo de segurança.
Tag	A função de tag pré-definida do TMS é recomendada para adicionar a mesma tag a diferentes recursos de nuvem.
Autorização	Esse parâmetro está disponível na primeira vez que você compra uma instância do WAF. Depois de ativar a autorização, o WAF criará uma agência no IAM em nome de você para conceder permissões relacionadas a si mesmo.

Passo 7 No canto inferior direito da página, clique em **Next**.

Passo 8 Confirme os detalhes do pedido e clique em **Pay Now**.

Passo 9 Na página de pagamento, selecione um método de pagamento e pague pelo seu pedido.

Passo 10 Depois que o pagamento for bem-sucedido, clique em **Back to Dedicated Engine List**. Na página **Dedicated Engine**, visualize o status da instância.

----Fim

Verificação

Demora cerca de 5 minutos para criar uma instância dedicada do WAF. Se o status da instância estiver **Running**, a criação da instância estará concluída.

Outras operações

Gerenciamento dedicado do motor WAF

Este tópico descreve como gerenciar instâncias (ou mecanismos) dedicadas do WAF, incluindo a exibição de informações da instância, a exibição de configurações de monitoramento da instância, o upgrade da edição da instância ou a exclusão de uma instância.

Autorizando o WAF a acessar dados na VPC em que seu site reside

Se você espera usar uma instância dedicada do WAF, autorize o WAF a acessar diretamente os dados na VPC ativando determinadas regras de segurança.

Ao adquirir uma instância dedicada do WAF, você concorda em autorizar o WAF a ativar tais regras de segurança. Atualmente, as regras de grupo de segurança listadas em **Tabela 2-2** serão automaticamente ativadas para uma instância dedicada do WAF.

Tabela 2-2 Regras de grupo de segurança para o WAF acessar a VPC em que seu site reside

Protocolo & Porta	Tipo	Endereço de origem	Descrição
Regras de entrada			
TCP: 22	IPv4	100.64.0.0/10	O&M remoto WAF
Regras de saída			
TCP: 9011	IPv4	100.125.0.0/16	Relatórios de logs de eventos do WAF
TCP: 9012	IPv4	100.125.0.0/16	Relatórios de logs de eventos do WAF
TCP: 9013	IPv4	100.125.0.0/16	Relatórios de logs de eventos do WAF
TCP: 9018	IPv4	100.125.0.0/16	Sincronização da política WAF
TCP: 9019	IPv4	100.125.0.0/16	Relatórios de logs de heartbeat do WAF
TCP: 4505	IPv4	100.125.0.0/16	Sincronização da política WAF
TCP: 4506	IPv4	100.125.0.0/16	Sincronização da política WAF
TCP: 50051	IPv4	100.125.0.0/16	Relatórios de logs de desempenho do WAF
TCP: 443	IPv4	100.125.0.0/16	Sincronização da política WAF

2.3 Atualização de Cloud WAF edição e as especificações (console antigo)

Para instâncias do WAF na nuvem faturadas anualmente/mensalmente, você pode atualizar a edição do WAF que está usando para aumentar a cota. Você também pode comprar pacotes de expansão de domínio, largura de banda ou regra para aumentar a cota sem atualizar a edição

do WAF. Os pacotes de expansão de regras permitem que você configure mais regras de lista negra e lista branca.

Pré-requisitos

- Você obteve credenciais de login do console de gerenciamento para uma conta com as permissões **WAF Administrator** e **BSS Administrator**.
- Você comprou uma instância do WAF na nuvem.

Limitações da especificação

- 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.

Restrições

Uma instância WAF expirada não pode ser atualizada diretamente. Renove o WAF antes de atualizá-lo.

Cenários de aplicação

Você pode querer atualizar sua edição ou especificações do WAF quando:

- Sua instância do WAF na nuvem atual não pode oferecer suporte a determinadas funções disponíveis em outras edições do WAF.
- Você deseja proteger mais nomes de domínio ou maior largura de banda com a instância atual do WAF.
- Você deseja configurar mais regras de blacklist e whitelist de endereços IP com a instância atual do WAF.

  Para obter mais detalhes sobre cada edição, consulte **Diferenças da Edição**.

Impacto no sistema

A atualização de uma edição do WAF ou a compra de pacotes extras de domínio, largura de banda ou expansão de regras não afeta os serviços de sites protegidos.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No canto superior direito, clique em **Buy/Upgrade WAF**.

Passo 5 (Facultativo): Selecione um projeto corporativo na lista suspensa para **Enterprise Project**.

Essa opção só estará disponível se você estiver conectado usando uma conta corporativa ou se tiver habilitado projetos corporativos. Para saber mais, consulte **Ativando o Enterprise Center**. Você pode usar projetos corporativos para gerenciar com mais eficiência os recursos da nuvem e os membros do projeto.

NOTA

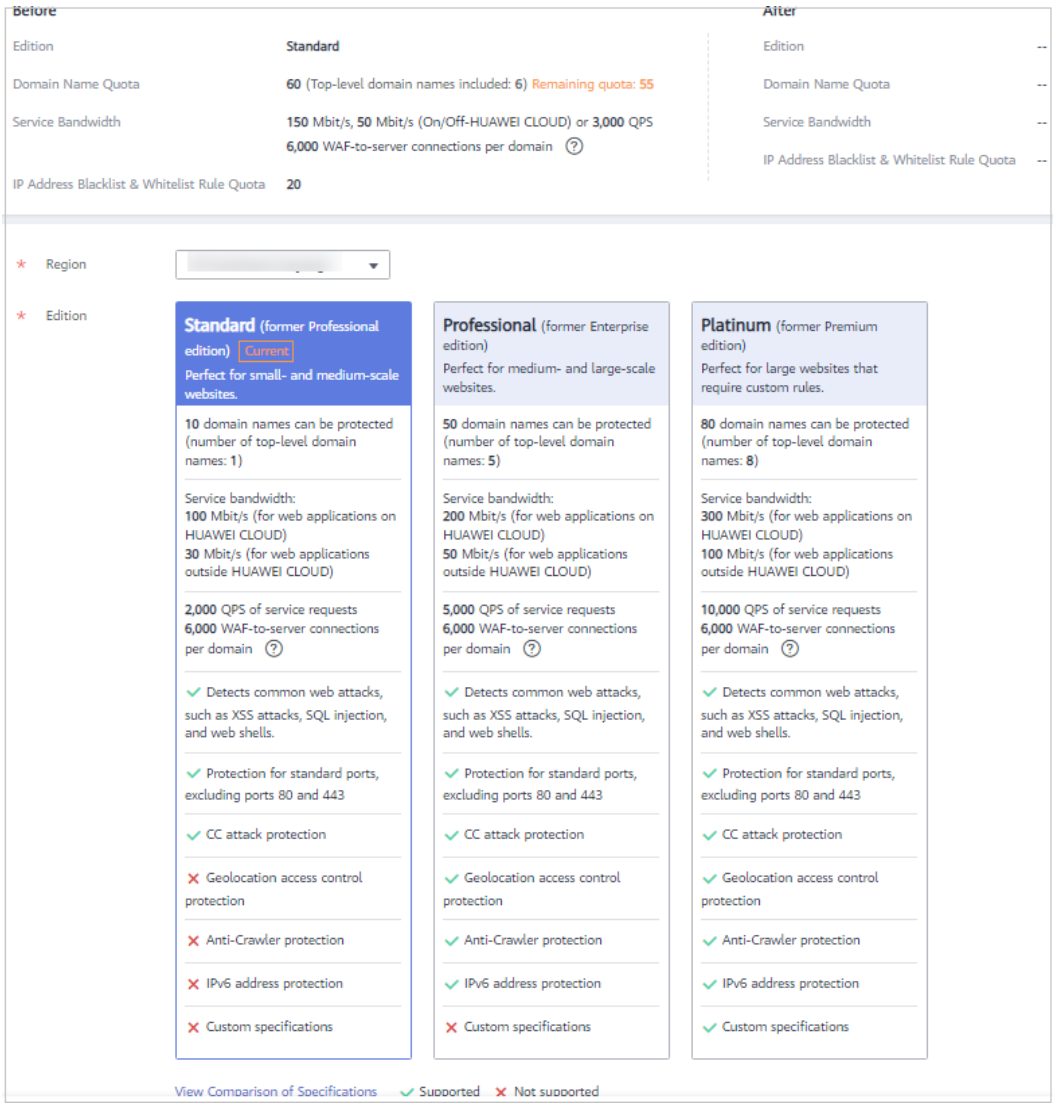
- Valor **default** indica o projeto corporativo padrão. Os recursos que não são alocados a nenhum projeto da empresa na sua conta são listados no projeto da empresa padrão.
- A opção **default** está disponível na lista suspensa **Enterprise Project** quando você compra o WAF.

Passo 6 Na página **Buy Web Application Firewall**, selecione **Cloud Mode**.

Passo 7 Na página de compra, selecione qualquer edição superior à atual. Por padrão, a edição atual é selecionada. **Figura 2-5** mostra um exemplo.

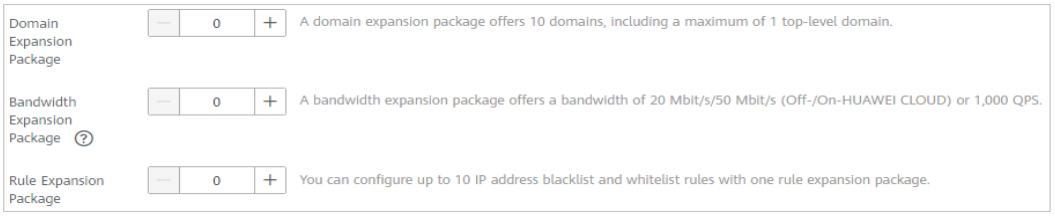
A edição listada no lado direito da atual é uma edição mais rica em recursos.

Figura 2-5 Selecionando a edição do WAF



Passo 8 Especifique o número de pacotes de expansão de domínio, largura de banda e regra que você deseja comprar.

Figura 2-6 Seleção de pacotes de expansão



Passo 9 No canto inferior direito da página, clique em **Next**.

Passo 10 Confirme os detalhes do pedido e clique em **Pay Now**.

Passo 11 Na página de pagamento, selecione um método de pagamento e pague seu pedido.

----Fim

Verificação

A instância e as especificações da nova edição entram em vigor após a conclusão do pagamento.

Outras operações

- **Pacotes de expansão de domínio doModo de Nuvem WAF**
- **Pacotes de expansão de largura de banda domodo de nuvem de WAF**
- **Pacotes de expansão da regra do modo de nuvem do WAF**

2.4 Pacotes de expansão de largura de banda domodo de nuvem de WAF

Uma certa quantidade de largura de banda é fornecida quando você compra uma instância do WAF padrão (antiga edição profissional), profissional (antiga edição empresarial) ou platina (antiga edição premium) faturada anualmente/mensalmente. Se você precisar de mais largura de banda, poderá comprar pacotes de expansão de largura de banda adicionais.

Os pacotes de expansão de largura de banda estão disponíveis quando você compra ou atualiza instâncias WAF em nuvem. Um pacote de expansão de largura de banda deve ser renovado ou cancelado junto com a instância WAF associada.

Qual é o limite de largura de banda do serviço?

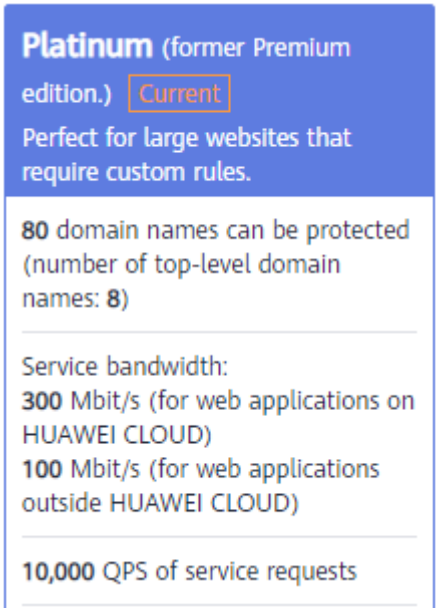
O limite de largura de banda do serviço é a quantidade de tráfego normal que uma instância do WAF pode proteger.

Um pacote de expansão de largura de banda pode proteger até 20 Mbit/s de tráfego para aplicativos no Huawei Cloud ou 50 Mbit/s para aplicativos não no Huawei Cloud; ou 1 000 Consultas por Segundo (QPS). Cada requisição HTTP Get é uma consulta.

> NOTA
>
> A largura de banda no WAF é calculada pelo próprio WAF e não está associada à largura de banda ou ao limite de tráfego de outros produtos Huawei Cloud (como CDN, ELB e ECS).

Por padrão, uma certa quantidade de largura de banda pode ser protegida pela instância do WAF padrão (antiga edição profissional), profissional (antiga edição empresarial) ou platina (antiga edição premium) faturada no modo anual/mensal. Se seus servidores de origem (como balanceadores de carga ECSs ou ELB) estiverem no Huawei Cloud, mais largura de banda poderá ser protegida. Por exemplo, se seus servidores de origem estiverem no Huawei Cloud, uma instância WAF platinum (antiga edição premium) pode proteger um máximo de 300 Mbit/s de largura de banda. Se seus servidores de origem estiverem fora do Huawei Cloud (como em salas de equipamentos da IDC), uma instância premium do WAF pode proteger até 100 Mbit/s de largura de banda. **Figura 2-7** mostra um exemplo.

Figura 2-7 Largura de banda do serviço



Quantos pacotes de expansão de largura de banda eu preciso?

Antes de comprar o WAF, confirme o pico total de tráfego de entrada e saída dos sites a serem protegidos pelo WAF. Certifique-se de que a largura de banda da edição do WAF selecionada seja maior que o tráfego de pico total de entrada ou o tráfego de pico total de saída, o que for maior.

NOTA

Geralmente, o tráfego de saída é maior que o tráfego de entrada.

Você pode estimar o tráfego consultando as estatísticas de tráfego no console do ECS ou usando outras ferramentas de monitoramento.

O tráfego de ataque deve ser removido em suas estimativas. Por exemplo, se seu site estiver sendo acessado normalmente, o WAF encaminhará o tráfego de volta para o ECS de origem, mas se seu site estiver sob ataque, o WAF bloqueará e filtrará o tráfego ilegítimo e roteará apenas o tráfego legítimo de volta para o ECS de origem. O tráfego de entrada e saída do ECS de origem exibido no console do ECS é o tráfego normal. Se houver vários ECSs, colete estatísticas sobre o tráfego normal de todos os ECSs. Por exemplo, se você tiver seis sites e a largura de banda de saída de pico de cada site não exceder 50 Mbit/s, a largura de banda de pico total não excederá 300 Mbit/s. Nesse caso, você pode comprar a edição WAF Platinum (antiga edição premium).

O que acontece se o tráfego do site exceder o limite de largura de banda do serviço?

Se o tráfego normal do seu site exceder o limite de largura de banda do serviço da edição selecionada, o tráfego pode ser limitado ou pode haver perda aleatória de pacotes. Como resultado, os serviços estão indisponíveis, congelados ou atrasados por um determinado período de tempo.

Nesse caso, atualize sua edição ou compre mais pacotes de expansão de largura de banda.

Pacote de expansão de largura de banda

Se a largura de banda exigida pelo seu site exceder o limite de largura de banda da edição do WAF selecionada, você poderá comprar pacotes de expansão de largura de banda para garantir que os serviços estejam protegidos.

Por exemplo, se você comprou a edição profissional do WAF (antiga edição corporativa), com um limite de largura de banda de 50 Mbit/s, e seus requisitos de largura de banda são de 70 Mbit/s para seus servidores fora do Huawei Cloud, Você pode comprar um pacote de expansão de largura de banda de 20 Mbit/s para compensar a diferença. Para mais detalhes, consulte **Atualização de Cloud WAF edição e as especificações (console antigo)**.

2.5 Pacotes de expansão de domínio doModo de Nuvem WAF

Um pacote de domínio pode proteger 10 nomes de domínio, incluindo um máximo de um nome de domínio de nível superior. Se a edição do WAF que você está usando não puder atender aos requisitos da sua empresa, você poderá comprar pacotes de expansão de domínio para aumentar a cota. Por exemplo, se você estiver usando o edição padrão (anteriormente edição profissional), 10 nomes de domínio podem ser protegidos, incluindo apenas um nome de domínio de nível superior. Se você quiser proteger três nomes de domínio de nível superior, você pode comprar dois pacotes de expansão de nome de domínio para aumentar a cota.

Vá para o console do WAF, clique em **Buy/Upgrade WAF** no canto superior direito. Em seguida, compre pacotes de expansão de domínio. Um pacote de expansão de domínio não pode ser cancelado. Um pacote de expansão de domínio só pode ser renovado junto com a edição do WAF que você usa.

Quota de nomes de domínio de diferentes edições no Modo Nuvem

As edições do Cloud WAF oferecem cotas de domínio diferentes.

- Edição standard (edição anterior profissional): 10 nomes de domínio podem ser protegidos, incluindo apenas um nome de domínio de nível superior
- Edição profissional (anteriormente Enterprise Edition): cinco pacotes de domínio que podem proteger cada um 10 nomes de domínio, incluindo até cinco nomes de domínio de nível superior.
- Edição Platinum (antiga edição premium): oito pacotes de domínio que podem proteger cada um 10 nomes de domínio, incluindo até oito nomes de domínio de nível superior.

NOTA

- Se apenas um domínio de nível superior puder ser adicionado a uma instância do WAF, você poderá adicionar um domínio de nível superior e nomes de domínio de subdomínio ou curinga relacionados ao domínio de nível superior. Por exemplo, você pode adicionar um nome de domínio de nível superior exemplo.com e um máximo de nove subdomínios ou domínios genéricos, por exemplo www.example.com, *.exemplo.com, mail.exemplo.com, user.pay.exemplo.com, e x.y.z.example.com. Cada um desses nomes de domínio (incluindo o nome de domínio de nível superior example.com) é contado para uma cota de nome de domínio no pacote de nomes de domínio.
- 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.

Você também pode atualizar sua edição do WAF de nuvem para aumentar a cota de nomes de domínio. Para mais detalhes, consulte **Atualização de Cloud WAF edição e as especificações (console antigo)**.

2.6 Pacotes de expansão da regra do modo de nuvem do WAF

Para instâncias do WAF faturadas anualmente/mensalmente, se a cota para as regras da lista negra de endereços IP e da lista branca da sua instância atual do WAF for insuficiente, você poderá comprar pacotes de expansão de regras para configurar mais regras desse tipo.

Um pacote de expansão de regras permite configurar até 10 regras de lista negra e lista branca de endereços de IP.

Os pacotes de expansão de regras estão disponíveis quando você compra ou atualiza uma instância de WAF na nuvem. Um pacote de expansão de regras deve ser renovado ou cancelado junto com a instância de WAF associada.

Para mais detalhes, consulte **Atualização de Cloud WAF edição e as especificações (console antigo)**.

3 Ativação de proteção de WAF

3.1 Portas suportadas pelo WAF

Além das portas padrão 80 e 443, o WAF suporta um grande número de portas não padrão. **Tabela 3-1** mostra quais portas não padrão são suportadas por diferentes edições do WAF.

Tabela 3-1 Supported ports

Edition	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
Standard edition (formerly professional edition) billed on a pay-per-use basis	Standard ports	80	443	Unlimited
	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

Edition	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
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**

3.2 Conexão de um site ao WAF (Modo Nuvem)

3.2.1 Processo de conexão (modo de nuvem)

Para permitir que a instância do WAF na nuvem proteja seu site, o nome de domínio do site deve estar conectado à instância do WAF para que o tráfego de entrada do site possa ir para o WAF primeiro.

Limitações

- Uma instância do WAF na nuvem pode proteger aplicativos da Web e sites acessíveis por meio de nomes de domínio. Para obter detalhes, consulte **Diferenças da edição**
- Depois que seu site é conectado ao WAF, o arquivo que os visitantes podem carregar a cada vez não pode exceder 512 MB.

Pré-requisitos

A seguir, descrevemos como o WAF funciona quando há um proxy usado ou nenhum proxy usado na frente do WAF:

- Proxy usado

  Se o seu site usou proxies, como anti-DDoS, Content Delivery Network (CDN) ou aceleração de nuvem, **Figura 3-1** mostra como o WAF funciona.

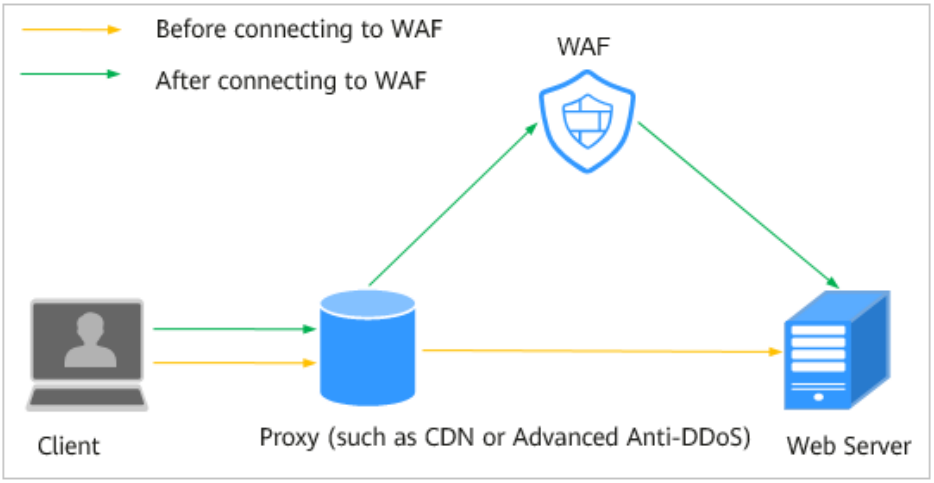
  – O DNS resolve o nome de domínio para o endereço IP do proxy antes que seu site seja conectado ao WAF. Neste caso, o tráfego passa através do proxy e, em seguida, o proxy encaminha o tráfego de volta para o servidor de origem.

  – Depois que seu site é conectado ao WAF, o DNS resolve seu nome de domínio para o endereço de acesso do WAF. Dessa forma, o proxy encaminha o tráfego para o WAF. O WAF, então, filtra o tráfego ilegítimo e apenas roteia o tráfego legítimo de volta ao servidor de origem.

    i. Altere o endereço IP de retorno à origem do proxy para o registro CNAME do WAF.

    ii. (Opcional) Adicione um nome de subdomínio do WAF e um registro TXT no seu provedor de DNS.

Figura 3-1 Configuração do WAF quando um proxy é usado



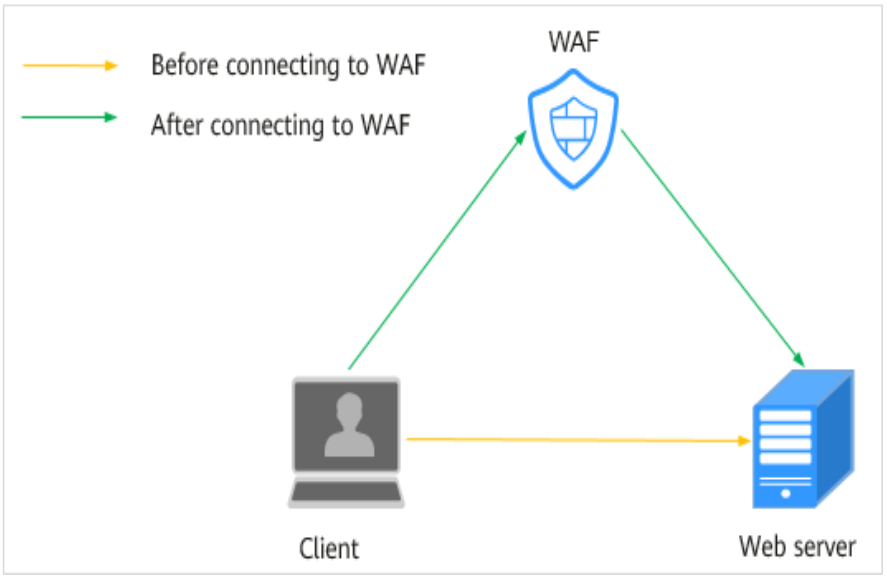
- Nenhum proxy usado

  Se nenhum proxy for usado antes que o site seja conectado ao WAF, **Figura 3-2** mostra como o WAF funciona.

  – O DNS resolve seu nome de domínio para o endereço IP do servidor de origem antes que seu site seja conectado ao WAF. Portanto, os visitantes da web podem acessar diretamente o servidor.

  – Depois que seu site é conectado ao WAF, o DNS resolve seu nome de domínio para o registro CNAME do WAF. Dessa forma, o tráfego passa pelo WAF. O WAF, então, filtra o tráfego ilegítimo e apenas roteia o tráfego legítimo de volta ao servidor de origem.

Figura 3-2 Nenhum proxy usado



Processos de conexão de um site ao WAF

Depois de comprar uma instância do WAF na nuvem, conclua as configurações necessárias seguindo o processo mostrado em **Figura 3-3**.

Figura 3-3 Processo de conexão de um site ao WAF

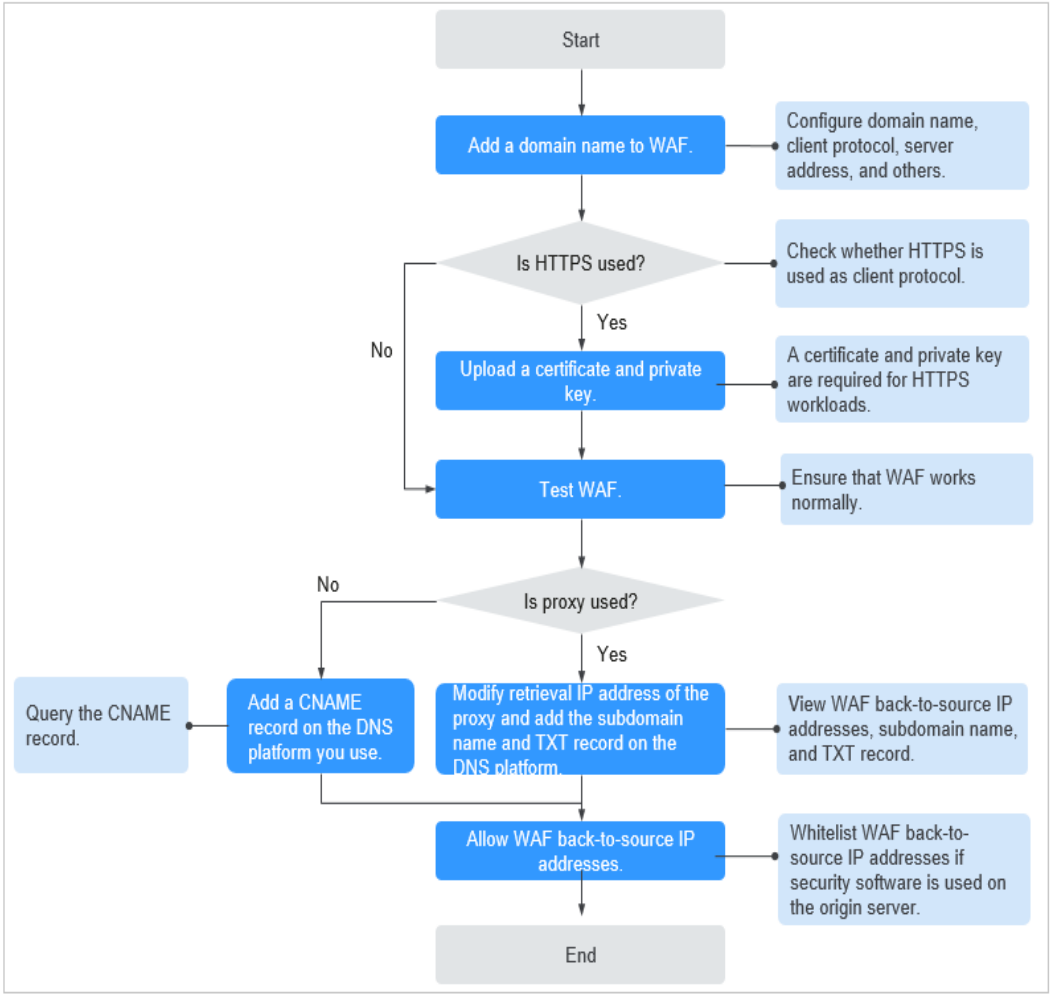


Tabela 3-2 Processo de conexão do nome de domínio do seu site ao WAF

Procedimento	Descrição
Passo 1: Adicionando um nome de domínio ao WAF (Modo de Nuvem)	Configure informações básicas, como o nome de domínio, o protocolo e o servidor de origem.
Passo 2: Coloque os endereços de IP de WAF na lista branca	Se outro software de segurança ou firewalls estiverem instalados em seu servidor de origem, a lista de permissões só solicita solicitações do WAF. Isso garante o acesso normal e protege o servidor de origem de hackers.
Passo 3: Testando o WAF	Para garantir que sua instância do WAF encaminhe o tráfego do site normalmente, teste a instância do WAF localmente e, em seguida, roteie o tráfego destinado ao nome de domínio do site para o WAF, modificando o registro DNS.

Procedimento	Descrição
Passo 4: Encaminhamento do tráfego do site para o WAF	● Nenhum proxy usado Configure um registro CNAME para o nome de domínio protegido na plataforma DNS que você usa. ● Proxy (como anti-DDoS avançado e CDN) usado Altere o endereço IP de origem do proxy usado, como anti-DDoS avançado e CDN, para o registro CNAME copiado.

Depois que você conecta um nome de domínio ao WAF, o WAF funciona como um proxy reverso entre o cliente e o servidor. O endereço IP real do servidor de origem é oculto e apenas o endereço IP do WAF é visível para os visitantes da web.

Corrigindo sites inacessíveis

Se um nome de domínio não estiver conectado ao WAF, seu status de acesso será **Inaccessible**. Para corrigir esse problema, consulte **Por que o status de acesso de um nome de domínio ou endereço IP está inacessível?**

3.2.2 Passo 1: Adicionando um nome de domínio ao WAF (Modo de Nuvem)

Este tópico descreve como adicionar um nome de domínio ao WAF para que o tráfego do site possa passar pelo WAF. Depois de conectar um nome de domínio de site à instância do WAF, o WAF funciona como um proxy reverso entre o cliente e o servidor. O endereço IP real do servidor é oculto e apenas o endereço IP do WAF é visível para os visitantes da web.

NOTA

Se você tiver ativado projetos da empresa, poderá selecionar seu projeto da empresa na lista suspensa **Enterprise Project** e adicionar nomes de domínio de sites a serem protegidos no projeto.

Pré-requisitos

- Você adquiriu uma instância do WAF.
- O nome de domínio foi registrado com a licença ICP e não foi adicionado ao WAF.

Restrições

- Os nomes de domínio adicionados por um usuário do IAM podem ser visualizados pela conta que cria o usuário do IAM, mas os nomes de domínio adicionados por uma conta não podem ser visualizados pelos usuários do IAM criados na conta.
- Um nome de domínio não pode ser adicionado ao WAF repetidamente.

  Cada combinação de um nome de domínio e uma porta não padrão é contada para a cota de nome de domínio da edição do WAF que você está usando. Por exemplo, o www.example.com:8080 e o www.example.com:8081 usam dois nomes de domínio da cota. Se você quiser proteger serviços da Web em várias portas com o mesmo nome de domínio, adicione o nome de domínio e cada porta ao WAF.

- Você pode inserir um nome de domínio único multinível (por exemplo, nome de domínio de nível superior exemplo.com e nome de domínio de nível 2 www.example.com) ou um nome de domínio curinga (*.exemplo.com).

  AVISO

  - Nomes de domínio curinga não podem conter sublinhados (_).
  - A seguir estão as regras para adicionar curingas a nomes de domínio:
    - Se o endereço IP do servidor de cada nome de subdomínio for o mesmo, digite um nome de domínio curinga a ser protegido. Por exemplo, se os nomes de subdomínio a.exemplo.com, b.exemplo.com e c.exemplo.com tiverem o mesmo endereço IP de servidor, você poderá adicionar o nome de domínio curinga *.exemplo.com ao WAF para proteger os três.
    - Se os endereços IP do servidor dos nomes de subdomínio forem diferentes, adicione nomes de subdomínio como nomes de domínio únicos, um por um.

- O WAF não oferece suporte a cabeçalhos HTTP definidos pelo usuário para nomes de domínio protegidos.
- Somente os nomes de domínio que foram registrados com licenças ICP podem ser adicionados ao WAF.
- Um registro CNAME é gerado com base em um nome de domínio. Para o mesmo nome de domínio, os registros CNAME são os mesmos.
- Somente certificados .pem podem ser usados no WAF.
- Atualmente, os certificados comprados no Huawei Cloud SCM podem ser enviados apenas para o projeto corporativo **default**. Para outros projetos corporativos, os certificados SSL enviados pelo SCM não podem ser usados.
- O WAF oferece suporte ao protocolo WebSocket, que é ativado por padrão.
  - WebSocket request inspection is enabled by default if **Client Protocol** is set to **HTTP**.
  - WebSockets request inspection is enabled by default if **Client Protocol** is set to **HTTPS**.
- Se você estiver usando o WAF standard edition (antiga edição profissional), somente **system-generated policy** poderá ser selecionada para **Configure Policy**.
- As políticas de segurança do WAF entram em vigor para endereços IP de clientes reais onde as solicitações são iniciadas. Para garantir que o WAF obtenha endereços IP de cliente reais, se seu site tiver servidores proxy de camada-7, como CDN e produtos de aceleração de nuvem implantados na frente do WAF, selecione **Yes** para **Proxy Configured**.

Limitações da especificação

Depois que seu site é conectado ao WAF, o arquivo que os visitantes podem carregar a cada vez não pode exceder 512 MB.

Impacto no sistema

Se uma porta não-padrão estiver configurada, os visitantes precisarão adicionar a porta não-padrão ao final do endereço do site quando acessarem o site. Caso contrário, ocorrerá um erro 404. Se ocorrer um erro 404, consulte **Como solucionar erros 404/502/504?**

Coletando informações de nome de domínio

Antes de adicionar um nome de domínio, obtenha as informações listadas em **Tabela 3-3**.

Tabela 3-3 Informações de nome de domínio necessárias

Informação	Parâmetro	Descrição	Valor de exemplo
Se um proxy é usado para o nome de domínio	Proxy configurado	Esse parâmetro deve ser definido como **Yes** se um proxy da Web de camada 7, como CDN e serviço de aceleração de nuvem, tiver sido implantado para seu site antes de você conectá-lo ao WAF.	N/D
gerais	Nome de domínio	O nome de domínio é usado pelos visitantes para acessar seu site. Um nome de domínio consiste em letras separadas por pontos (.). É um endereço legível por humanos que mapeia para o endereço IP legível por máquina do seu servidor.	www.example.com
	Porto padrão/não padronizado	A porta de serviço correspondente ao nome de domínio do site que você deseja proteger. ● Portas padrão – 80: porta padrão quando o protocolo do cliente é definido como HTTP – 443: porta padrão quando o protocolo do cliente é definido como HTTPS ● Portas não padronizadas Portos diferentes de 80 e 443 **AVISO** Se o seu site usa uma porta não padrão, verifique se a edição do WAF que você planeja comprar pode proteger a porta não padrão antes de fazer uma compra. Para mais detalhes, consulte **Portas suportadas pelo WAF**.	80
	HTTP/2 Usado	O protocolo HTTP/2 pode ser usado apenas para acesso entre o cliente e o WAF com a condição de que pelo menos um servidor de origem tenha **HTTPS** usado para o **Client Protocol**.	-
	Protocolo do cliente	Protocolo usado por um cliente (por exemplo, um navegador) para acessar um site. O WAF suporta HTTP e HTTPS.	HTTP

Informação	Parâmetro	Descrição	Valor de exemplo
	Protocolo do servidor	Protocolo usado pelo WAF para encaminhar solicitações ao cliente (como um navegador). As opções são **HTTP** e **HTTPS**.	HTTP
	Endereço do servidor	Endereço IP público ou nome de domínio do servidor de origem para um cliente (como um navegador) acessar. Geralmente, um endereço IP público mapeia para o registro A do nome de domínio configurado no DNS e um nome de domínio para o registro CNAME.	XXX.XXX.1.1
(Opcional) Certificado	-	Se você definir o **Client Protocol** como **HTTPS**, será necessário configurar um certificado no WAF e associá-lo ao nome de domínio. **AVISO** Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver no formato PEM, converta-o para o formato pem consultando **Como faço para converter um certificado em Formato PEM?**	Nenhum

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

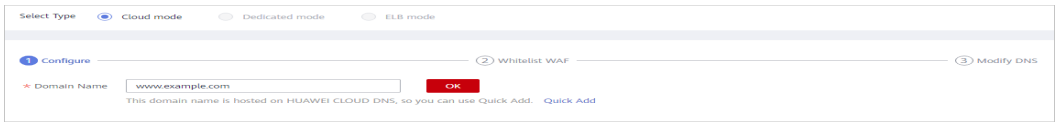
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 No canto superior esquerdo da lista de sites, clique em **Add Website**.

Passo 6 Selecionar **Modo de Nuvem**. Digite o nome de domínio na caixa de texto **Domain Name** e clique em **OK**.

Figura 3-4 Nome de domínio



Você pode inserir um nome de domínio único multinível . (por exemplo, nome de domínio de nível superior exemplo.com e nome de domínio de nível 2 www.example.com) ou um nome de domínio curinga (*.exemplo.com).

AVISO

- Nomes de domínio curinga não podem conter sublinhados (_).
- A seguir estão as regras para adicionar curingas a nomes de domínio:
  - Se o endereço IP do servidor de cada nome de subdomínio for o mesmo, digite um nome de domínio curinga a ser protegido. Por exemplo, se os nomes de subdomínio a.exemplo.com, b.exemplo.com e c.exemplo.com tiverem o mesmo endereço IP de servidor, você poderá adicionar o nome de domínio curinga *.exemplo.com ao WAF para proteger os três.
  - Se os endereços IP do servidor dos nomes de subdomínio forem diferentes, adicione nomes de subdomínio como nomes de domínio únicos, um por um.

Se o seu nome de domínio estiver hospedado no Huawei Cloud, você pode clicar em **Quick Add**. Na caixa de diálogo **Select Domain Name** exibida, selecione o nome de domínio que deseja proteger e clique em **OK**. O nome de domínio hospedado é adicionado automaticamente.

Passo 7 Configurar **Domain Name** e outros parâmetros, referindo-se a **Tabela 3-4**. **Figura 3-5** mostra um exemplo.

Figura 3-5 Configurando as configurações básicas

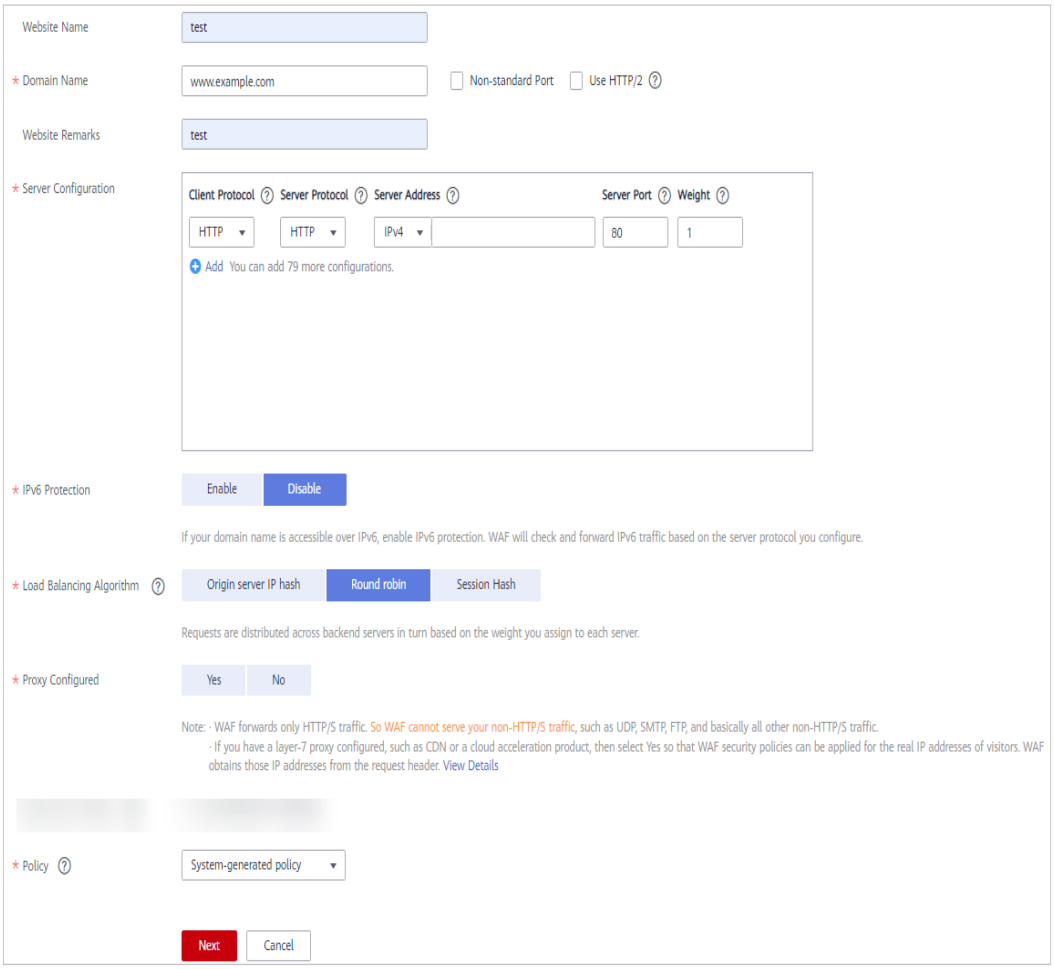


Tabela 3-4 Descrição do parâmetro

Parâmetro	Descrição	Valor de exemplo
Nome do site	Nome do site que você quer proteger	N/D

Parâmetro	Descrição	Valor de exemplo
Nome de domínio	O nome de domínio de um site a ser protegido. Pode ser um único nome de domínio ou um nome de domínio curinga. ● Nome de domínio único: Insira um único nome de domínio. ● Nome de domínio wildcard: Digite um nome de domínio curinga do site a ser protegido. Nomes de domínio curinga não podem conter sublinhados (_). **NOTA** ● Se o endereço IP do servidor de cada nome de subdomínio for o mesmo, insira um nome de domínio curinga. Por exemplo, se os nomes de subdomínio a.exemplo.com, b.exemplo.com e c.exemplo.com tiverem o mesmo endereço IP de servidor, você poderá adicionar o nome de domínio curinga *.exemplo.com ao WAF para proteger os três. ● Se os endereços IP do servidor dos nomes de subdomínio forem diferentes, adicione nomes de subdomínio como nomes de domínio únicos, um por um.	Nome de domínio único: **www.example.com** Nome de domínio de nível superior: example.com Nome de domínio Wildcard: ***.example.com**
Observações do site	(Opcional) Você pode fornecer comentários sobre seu site, se desejar.	-
Porto não padronizado	Defina este parâmetro somente se **Non-standard Port** estiver selecionada. Para mais detalhes, consulte **Exemplo de configuração 1: Protegendo o tráfego para a mesma porta padrão com diferentes endereços IP de servidor de origem atribuídos**. ● Se você definir o **Client Protocol** como **HTTP**, o WAF protegerá os serviços na porta padrão 80 por padrão. Se você definir o **Client Protocol** como **HTTPS**, o WAF protegerá os serviços na porta padrão 443 por padrão. ● Para configurar uma porta diferente das portas **80** e **443**, selecione **Non-standard Port** e selecione uma porta não padrão na lista suspensa **Port**. **NOTA** Se uma porta não-padrão estiver configurada, os visitantes precisarão adicionar a porta não-padrão ao final do endereço do site quando acessarem o site. Caso contrário, ocorrerá um erro 404. Se ocorrer um erro 404, consulte **Como solucionar erros 404/502/504?**	81
Usar HTTP/2	Se o seu site precisa oferecer suporte ao acesso HTTP/2, selecione esse parâmetro. O protocolo HTTP/2 pode ser usado apenas para acesso entre o cliente e o WAF com a condição de que pelo menos um servidor de origem tenha **HTTPS** usado para o **Client Protocol**.	-

Parâmetro	Descrição	Valor de exemplo
Observações do site	Uma breve descrição do site	-
Configuração do servidor	Configurações de endereço do servidor web, incluindo **Client Protocol**, **Server Protocol**, **Server Address**, e **Server Port**. ● **Client Protocol**: protocolo usado por um cliente para acessar um servidor. As opções são **HTTP** e **HTTPS**. ● **Server Protocol**: protocolo usado pelo WAF para encaminhar solicitações de clientes. As opções são **HTTP** e **HTTPS**. **NOTA** – Para obter detalhes sobre a configuração do **Client Protocol** e do **Server Protocol**, consulte **Regras para configurar o protocolo do cliente e o protocolo do servidor**. – O WAF pode verificar a solicitação WebSocket e WebSockets, que é ativada por padrão. ● **Server Address**: endereço IP público (geralmente correspondente ao registro A do nome de domínio configurado no DNS) ou nome de domínio (geralmente correspondendo ao CNAME do nome de domínio configurado no DNS) do servidor web que um cliente acessa. ● **Server Port**: porta de serviço do servidor para a qual a instância do WAF encaminha as solicitações do cliente.	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **Server Address**: XXX.XXX.1.1 **Server Port**: **80**

Parâmetro	Descrição	Valor de exemplo
Nome do certificado	Se você definir o **Client Protocol** como **HTTPS**, será necessário um certificado SSL. Você pode selecionar um certificado criado ou importar um certificado. Para obter detalhes sobre como importar um certificado, consulte **Importando um novo certificado**. Os certificados importados são listados na página **Certificates**. Para mais detalhes, veja **Carregamento de um certificado**. Além disso, você pode comprar um certificado no console do SCM e enviá-lo para o WAF. Para obter detalhes sobre como enviar um certificado SSL no SCM para o WAF, consulte **Enviando um certificado SSL para outros serviços em Nuvem**. **AVISO** ● Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver no formato.pem, converta-o em.pem consultando-o **Tabela 3-6** antes de carregar o certificado. ● Atualmente, os certificados comprados no Huawei Cloud SCM podem ser enviados apenas para o projeto corporativo **default**. Para outros projetos corporativos, os certificados SSL enviados pelo SCM não podem ser usados. ● Se o certificado do seu site estiver prestes a expirar, compre um novo certificado antes da data de expiração e atualize o certificado associado ao site no WAF. ● Cada nome de domínio deve ter um certificado associado. Um nome de domínio curinga só pode usar um certificado de domínio curinga. Se você tiver apenas certificados de domínio único, adicione nomes de domínio um a um no WAF.	Nenh
Proteção IPv6	● Se você selecionar **IPv6** para **Server Address**, **IPv6 Protection** será ativada por padrão. ● Se você selecionar **IPv4** para o **Server Address** e ativar a **IPv6 Protection**, o WAF atribuirá um endereço IPv6 ao nome de domínio para que o site seja acessível por meio do endereço IPv6. Desta forma, as solicitações para o endereço IPv6 são roteadas pelo WAF para o endereço IPv4 do servidor de origem. **NOTA** Se o servidor de origem usar endereços IPv6, a proteção IPv6 será ativada por padrão. Para evitar a interrupção do serviço IPv6, mantenha a proteção IPv6 ativada. Se a proteção IPv6 não for necessária, edite a configuração do servidor e exclua a configuração IPv6 do servidor de origem primeiro. Para obter detalhes, consulte **Editando Informações do Servidor**.	Ativar

Parâmetro	Descrição	Valor de exemplo
Algoritmo de balanceamento de carga	Selecione um algoritmo de balanceamento de carga. ● **Origin server IP hash**: As solicitações do mesmo endereço IP são roteadas para o mesmo servidor de back-end. ● **Weighted round robin**: As solicitações são distribuídas pelos servidores de back-end, por sua vez, com base no peso atribuído a cada servidor. ● **Session hash**: Solicitações com a mesma tag de sessão são roteadas para o mesmo servidor de origem. Para ativar esse algoritmo, **configure identificadores de tráfego para fontes de ataque conhecidas**, ou o algoritmo de hash de sessão não pode ter efeito. Para mais detalhes, consulte **Alternação de algoritmo de balanceamento de carga**.	Round Robin ponderado

Passo 8 Configurar **Proxy Configured**.

Se seu site tiver servidores proxy de camada-7, como CDN e produtos de aceleração de nuvem implantados na frente do WAF, selecione **Yes** para **Proxy Configured**. Isso garante que o WAF obtenha endereços IP reais do cliente, pois a proteção do WAF só entra em vigor para endereços IP reais do cliente onde as solicitações são iniciadas. Além disso, pode haver vários endereços IP no campo de endereço IP de origem.Para garantir que o WAF obtenha o endereço IP real do visitante que inicia a solicitação, adicione um identificador de tráfego IP para o site protegido . (por exemplo, **CDN-Src-IP** pode ser adicionado para um proxy CDN). Para mais detalhes, consulte **Configuração de um identificador de tráfego para uma origem de ataque conhecida**

AVISO

- If a proxy is deployed before WAF on your website, the WAF working mode cannot be switched to **Bypassed**. Para mais detalhes, veja **Alternação de modo de trabalho do WAF**.
- Se um site não usar nenhum proxy, mas você selecionar **Yes** para **Proxy Configured**, o WAF confiará no campo **X-Forwarded-For** no cabeçalho da solicitação HTTP ao obter o endereço IP de origem real. Portanto, seu negócio não é afetado.

Passo 9 Especifique **Configure Policy**. Por padrão, **system-generated policy** é selecionada. Você pode selecionar regras personalizadas. Para mais detalhes, consulte **Tabela 3-5**.

AVISO

Se você estiver usando o WAF standard edition (antiga edição profissional), somente **System-generated policy** estará disponível.

Você pode selecionar uma política configurada. Você também pode personalizar as regras depois que o nome de domínio for conectado ao WAF.

Tabela 3-5 Políticas geradas pelo sistema

Edição	Política	Descrição
Edição padrão (antiga edição profissional)	Proteção básica da Web (modo de **Log only** e verificações comuns)	The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections.
Edição Professional (anteriormente Enterprise Edition) e Platinum Edition (anteriormente Premium)	Proteção básica da Web (modo de **Log only** e verificações comuns)	The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections.
	Anti-crawler (modo de **Log only** e recurso **Scanner**)	WAF only logs web scanning tasks, such as vulnerability scanning and virus scanning, such as crawling behavior of OpenVAS and Nmap.

NOTA

Log only: WAF only logs detected attack events instead of blocking them.

Passo 10 Clique em **Next**.

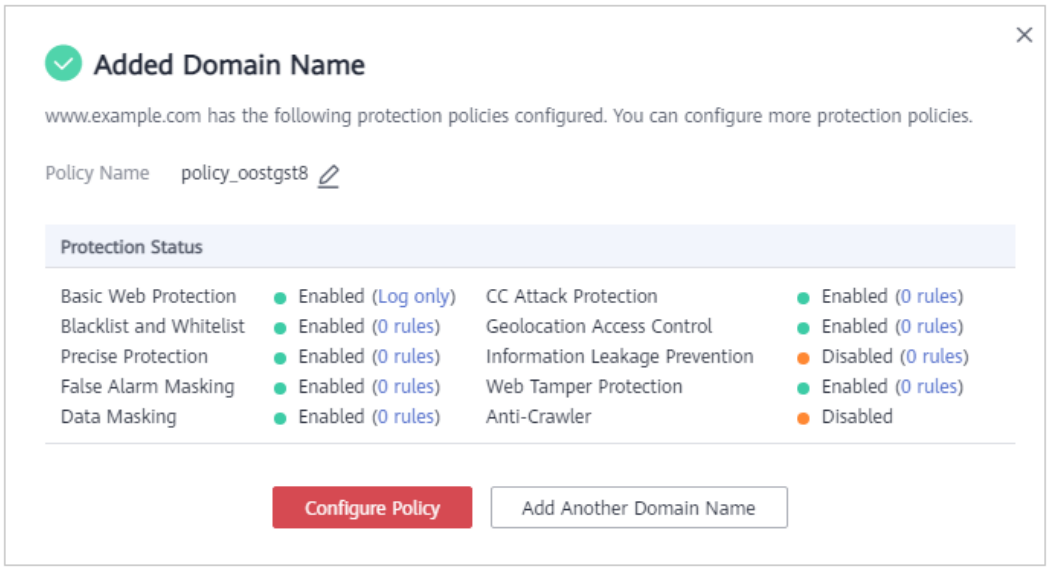
É aconselhável ignorar esta etapa clicando em **Next** e, em seguida, **Finish**. Em seguida, conecte o nome de domínio ao WAF posteriormente, referindo-se a **Passo 3: Testando o WAF** e **Passo 4: Encaminhamento do tráfego do site para o WAF**.

Um registro CNAME é gerado com base em um nome de domínio. Para o mesmo nome de domínio, os registros CNAME são os mesmos.

Passo 11 Clique em **Next** e, em seguida, em **Finish**.

Em seguida, você pode ver o status de acesso e o modo de trabalho para o nome de domínio adicionado na página **Website Settings**.

Figura 3-6 Nome de domínio adicionado



- Para configurar uma política de proteção para o site, clique em **Configure Policy**.
- Para adicionar mais sites a serem protegidos, clique em **Add Another Domain Name**.
- Para exibir o site adicionado, feche a caixa de diálogo.

NOTA

- Se o servidor usar outros firewalls de rede, desative esses firewalls de rede ou adicione o intervalo de endereços IP do WAF à lista de permissões de endereços IP desses firewalls de rede. Caso contrário, esses firewalls podem considerar o endereço IP do WAF como um endereço IP malicioso. Para obter detalhes, consulte **Como faço para colocar na lista branca o intervalo de endereços IP back-to-source do WAF?**
- Se o servidor da Web estiver usando software de segurança pessoal, substitua-o por software de segurança empresarial e coloque na lista de permissões os intervalos de endereços IP do WAF.

----Fim

Verificação

- Por padrão, o WAF detecta o **Access Status** de cada nome de domínio protegido a cada hora.
- Geralmente, se você executou uma conexão de domínio e **Access Status** é **Accessible**, o nome de domínio é conectado ao WAF.

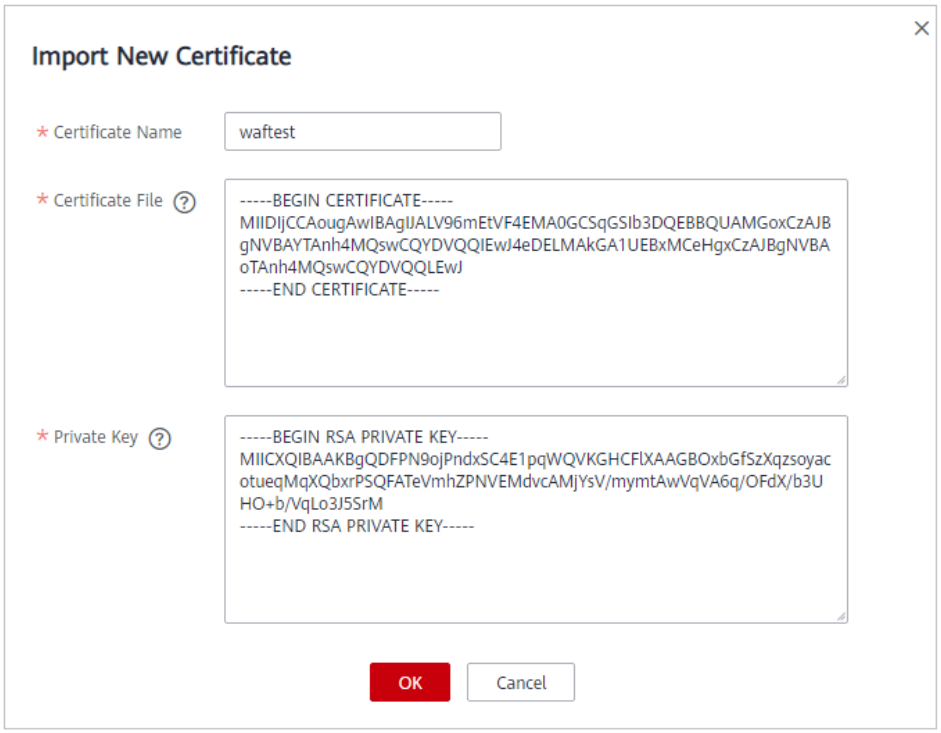
  Se um nome de domínio tiver sido conectado ao WAF, mas **Access Status** estiver **Inaccessible**, clique em para atualizar. Se o **Access Status** ainda estiver **Inaccessible**, conecte o nome de domínio ao WAF novamente, referindo-se a **Passo 4: Encaminhamento do tráfego do site para o WAF**.

Importando um novo certificado

Se você definir o **Client Protocol** como **HTTPS**, será necessário um certificado SSL. Você pode executar as etapas a seguir para importar um novo certificado.

1. Clique em **Import New Certificate**. Na caixa de diálogo **Import New Certificate** exibida, insira o nome do certificado e cole o arquivo do certificado e a chave privada nas caixas de texto correspondentes. **Figura 3-7** mostra um exemplo.

Figura 3-7 Importar Novo Certificado



NOTA

O WAF criptografa e salva a chave privada para mantê-la segura.

Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver no formato.pem, converta-o localmente para.pem consultando **Tabela 3-6** antes de carregá-lo.

Tabela 3-6 Comandos de conversão de certificados

Formato	Método de conversão
CER/CRT	Renomeie o arquivo de certificado **cert.crt** para **cert.pem**.
PFX (em inglês)	● Obtenha uma chave privada. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** ● Obter um certificado. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Converter um certificado. Por exemplo, execute o seguinte comando para converter **cert.p7b** em **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Renomeie o arquivo de certificado **cert.cer** para **cert.pem**.

Formato	Método de conversão
DER	● Obtenha uma chave privada. Por exemplo, execute o seguinte comando para converter **privatekey.der** em **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** ● Obter um certificado. Por exemplo, execute o seguinte comando para converter **cert.cer** em **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTA

- Antes de executar um comando OpenSSL, verifique se a ferramenta **OpenSSL** foi instalada no host local.
- Se seu PC local executa um sistema operacional Windows, vá para a interface de linha de comando (CLI) e execute o comando de conversão de certificados.

2. Clique em **OK**.

Exemplo de configuração 1: Protegendo o tráfego para a mesma porta padrão com diferentes endereços IP de servidor de origem atribuídos

1. Desmarque **Non-standard Port**.
2. Selecione **HTTP** ou **HTTPS** para **Client Protocol**. **Figura 3-8** e **Figura 3-9** mostrar configurações de porta padrão quando o protocolo do cliente é HTTP ou HTTPS.

Figura 3-8 Porto 80

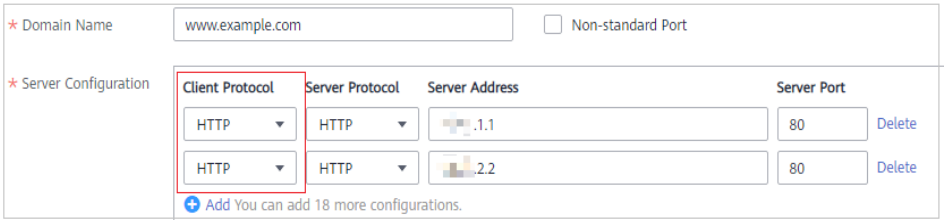
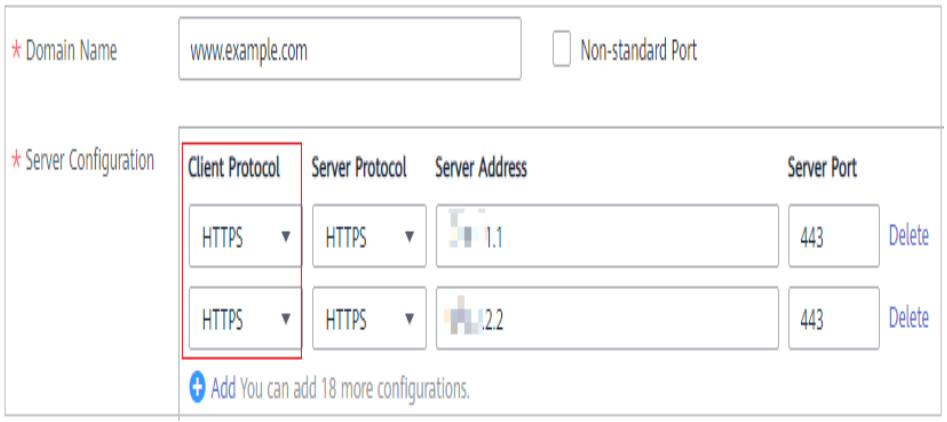


Figura 3-9 Porto 443



NOTA

Se o **Client Protocol** estiver definido como **HTTPS**, é necessário um certificado.

3. Os visitantes do seu site podem acessar o site sem adicionar uma porta ao final do nome de domínio. Por exemplo, digite **http://www.example.com** na caixa de endereço do navegador para acessar o site.

Exemplo de configuração 1: Protegendo o tráfego para uma porta não padrão com diferentes endereços IP do servidor de origem atribuídos

1. Selecione **Non-standard Port** e selecione uma porta não padrão a ser protegida na lista suspensa **Port**.
2. Selecione **HTTP** ou **HTTPS** para **Client Protocol** para todas as portas do servidor. **Figura 3-10** e **Figura 3-11** mostrar a configuração da porta HTTP ou HTTPS não padrão, respectivamente.

Figura 3-10 Outra porta HTTP além da porta 80

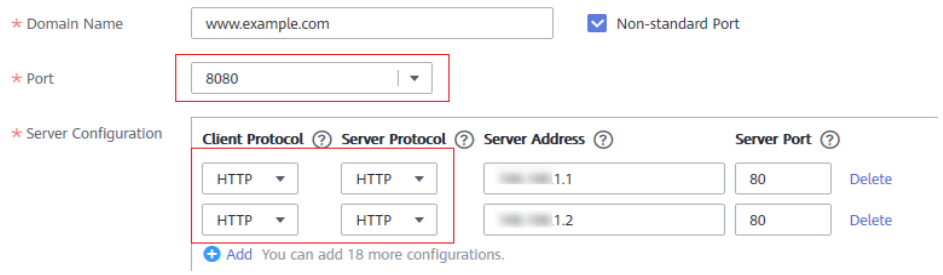
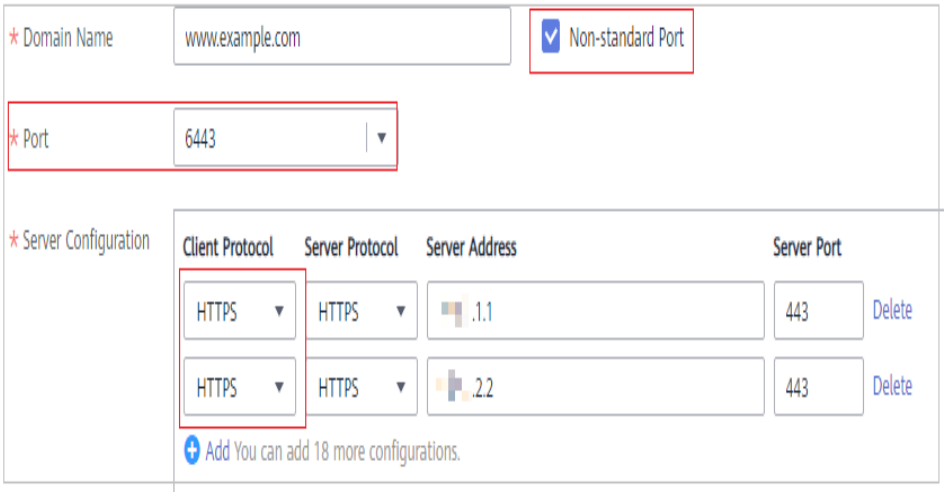


Figura 3-11 Outra porta HTTPS além da porta 443



NOTA

Se o **Client Protocol** estiver definido como **HTTPS**, é necessário um certificado.

3. Os visitantes devem adicionar a porta não padrão configurada ao nome de domínio quando acessam seu site. Caso contrário, o erro 404 é retornado. Se a porta não padrão for 8080, digite *http://www.example.com:8080* na caixa de endereço do navegador.

Exemplo de configuração 3: Protegendo diferentes portas de serviço

Se as portas de serviço a serem protegidas forem diferentes, configure-as separadamente. Por exemplo, para proteger as portas 8080 e 6443 para o site **www.example.com**, adicione o domínio separadamente para cada porta, como mostrado em **Figura 3-12** e **Figura 3-13**.

Figura 3-12 Protegendo o porto 8080

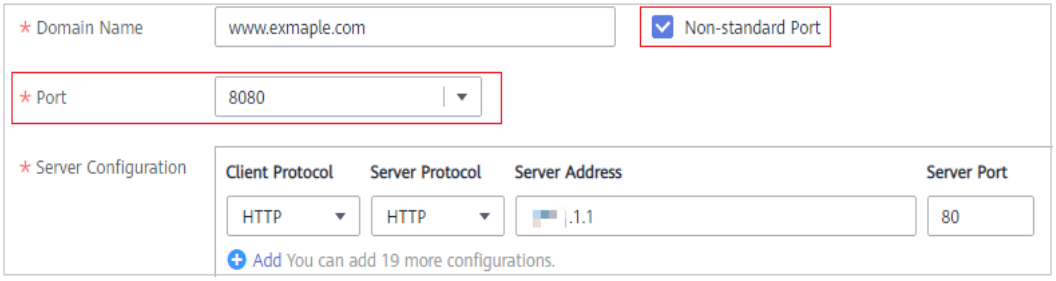
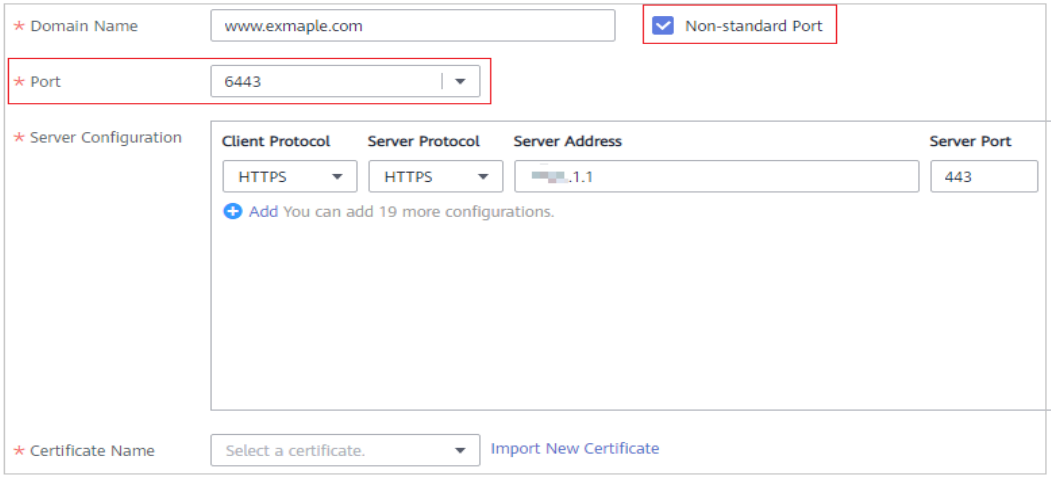


Figura 3-13 Protegendo a porta 6443

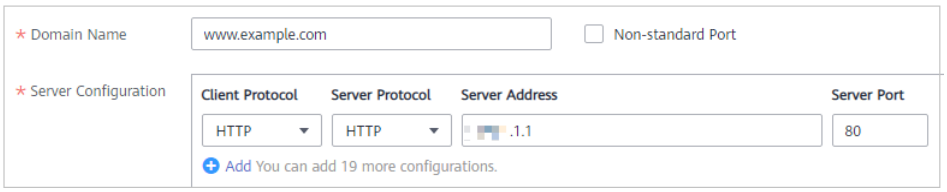


Regras para configurar o protocolo do cliente e o protocolo do servidor

O WAF fornece vários tipos de protocolo. Se o seu site for www.example.com, o WAF fornece os seguintes quatro modos de acesso:

- Método HTTP (**Figura 3-14**)

Figura 3-14 Modo HTTP

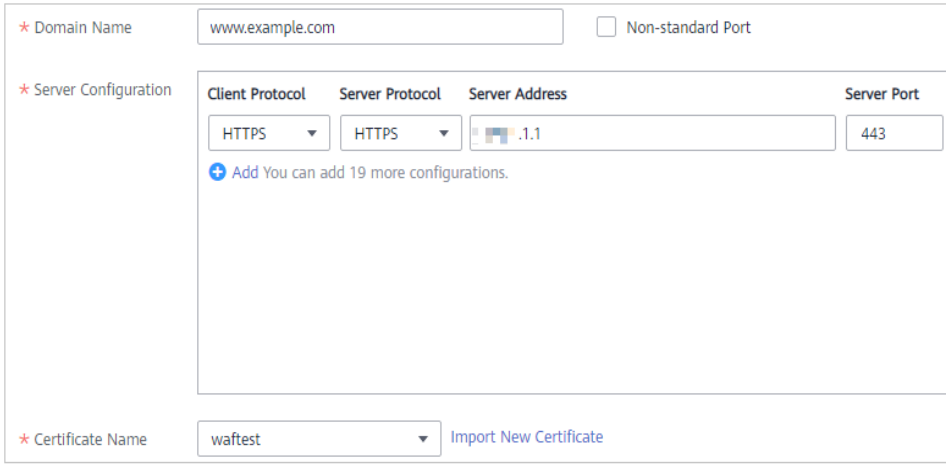


AVISO

Essa configuração permite que os visitantes da Web acessem o http://www.example.com apenas por HTTP. Se eles acessarem via HTTPS, eles receberão o código 302 Found e serão redirecionados para http://www.example.com.

- Método HTTPS. Essa configuração permite que os visitantes da Web acessem seu site apenas por HTTPS. Se eles acessarem via HTTP, eles serão redirecionados para a URL HTTPS. **Figura 3-15** mostra um exemplo.

Figura 3-15 Modo HTTPS

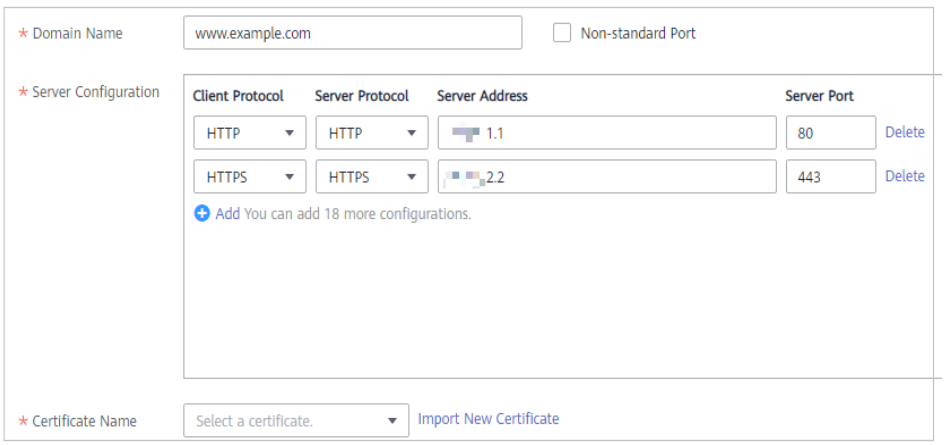


AVISO

- Se os visitantes da Web acessarem seu site por HTTPS, o site retornará uma resposta bem-sucedida.
- Se os visitantes da web acessarem o http://www.example.com por HTTP, eles receberão o código 302 Found e serão direcionados para https://www.example.com.

- Método de encaminhamento HTTP/HTTPS. **Figura 3-16** mostra um exemplo.

Figura 3-16 Modo HTTP e HTTPS

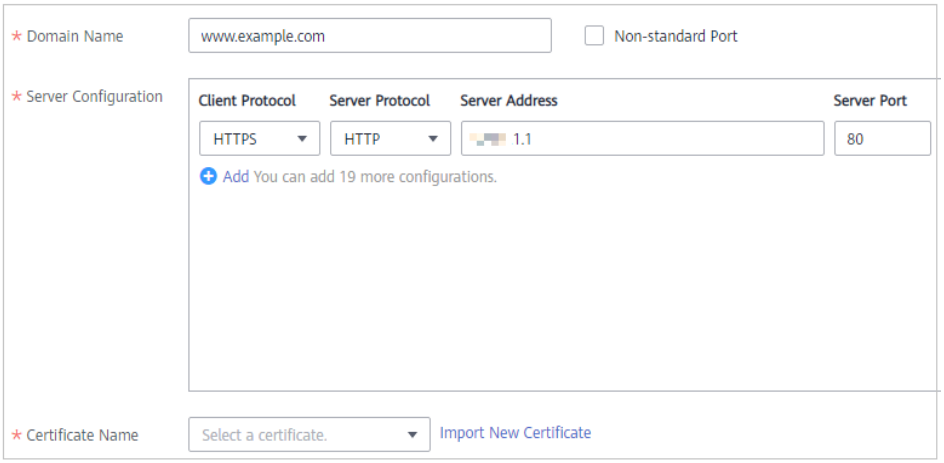


AVISO

- Se os visitantes da Web acessarem seu site por HTTP, o site retornará uma resposta bem-sucedida, mas nenhuma comunicação entre o navegador e o site será criptografada.
- Se os visitantes da Web acessarem seu site por HTTPS, o site retornará uma resposta bem-sucedida e todas as comunicações entre o navegador e o site serão criptografadas.

- Descarregamento HTTPS pelo WAF. **Figura 3-17** mostra um exemplo.

Figura 3-17 Descarregamento HTTPS



AVISO

Se os visitantes da Web acessarem seu site por HTTPS, o WAF encaminhará as solicitações para o servidor de origem por HTTP.

3.2.3 Passo 2: Coloque os endereços de IP de WAF na lista branca

To let your cloud WAF instances take effect, configure ACL rules on the origin server to trust only the back-to-source IP addresses of all your cloud WAF instances. This prevents hackers from attacking the origin server through the server IP addresses.

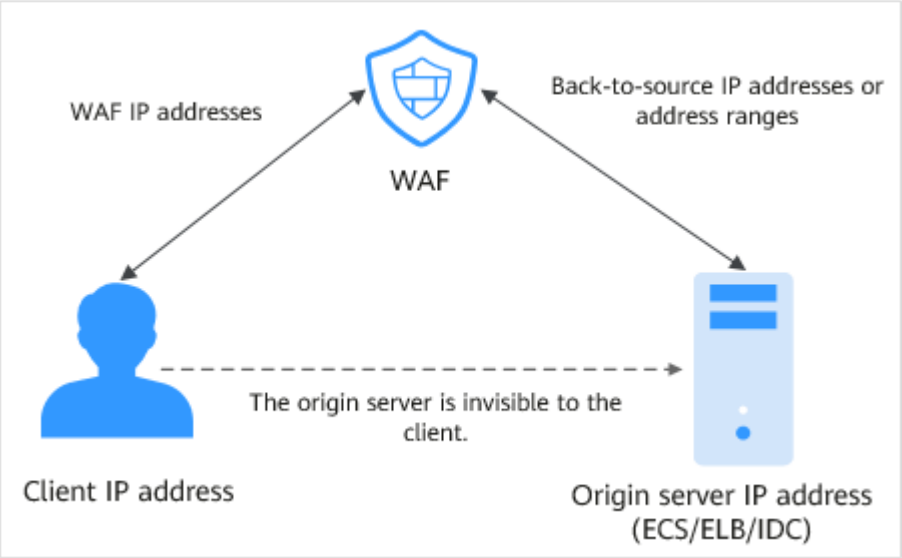
AVISO

ACL rules must be configured on the origin server to whitelist WAF back-to-source IP addresses. Otherwise, your website visitors will frequently receive 502 or 504 error code after your website is connected to WAF in cloud mode.

What Are Back-to-Source IP Addresses?

From the perspective of a server, all web requests originate from WAF. The IP addresses used by WAF forwarding are back-to-source IP addresses of WAF. The real client IP address is written into the X-Forwarded-For (XFF) HTTP header field.

Figura 3-18 Back-to-source IP address



WAF Back-to-Source IP Address Check Mechanism

A back-to-source IP address, or WAF IP address, is randomly allocated from the back-to-source IP address range. When WAF forwards requests to the origin server, WAF will check the IP address status. If the IP address is abnormal, WAF will remove it and randomly allocate a normal one to receive or send requests.

NOTA

WAF back-to-source IP addresses are periodically updated. Whitelist the new IP addresses in time to prevent these IP addresses from being blocked by origin servers.

Why Do I Need to Whitelist the WAF IP Address Ranges?

All web requests originate from a limited quantity of WAF IP addresses. The security software on the origin server may most likely regard these IP addresses as malicious and block them. Once WAF IP addresses are blocked, the website may fail to be accessed or it opens extremely slowly. To fix this, add the WAF IP addresses to the whitelist of the security software.

NOTA

After you connect your website to WAF, uninstall other security software from the origin server or allow only the requests from WAF to access your origin server. This ensures normal access and protects the origin server from hacking.

Procedure

Passo 1 **Efetue login no console de gerenciamento**.

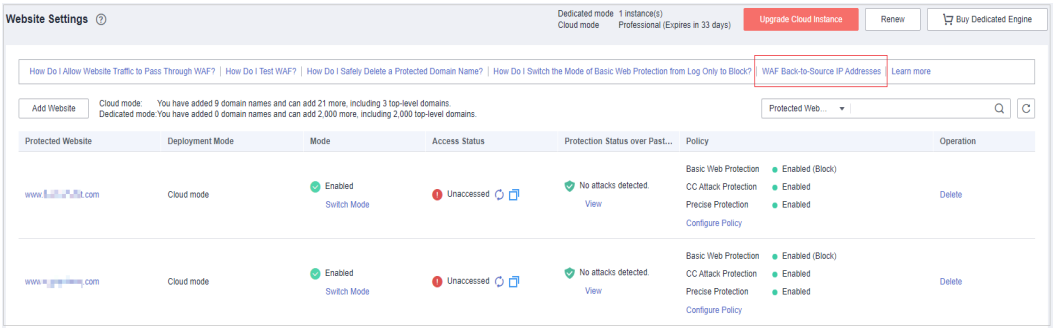
Passo 2 Click in the upper left corner of the management console and select a region or project.

Passo 3 Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

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

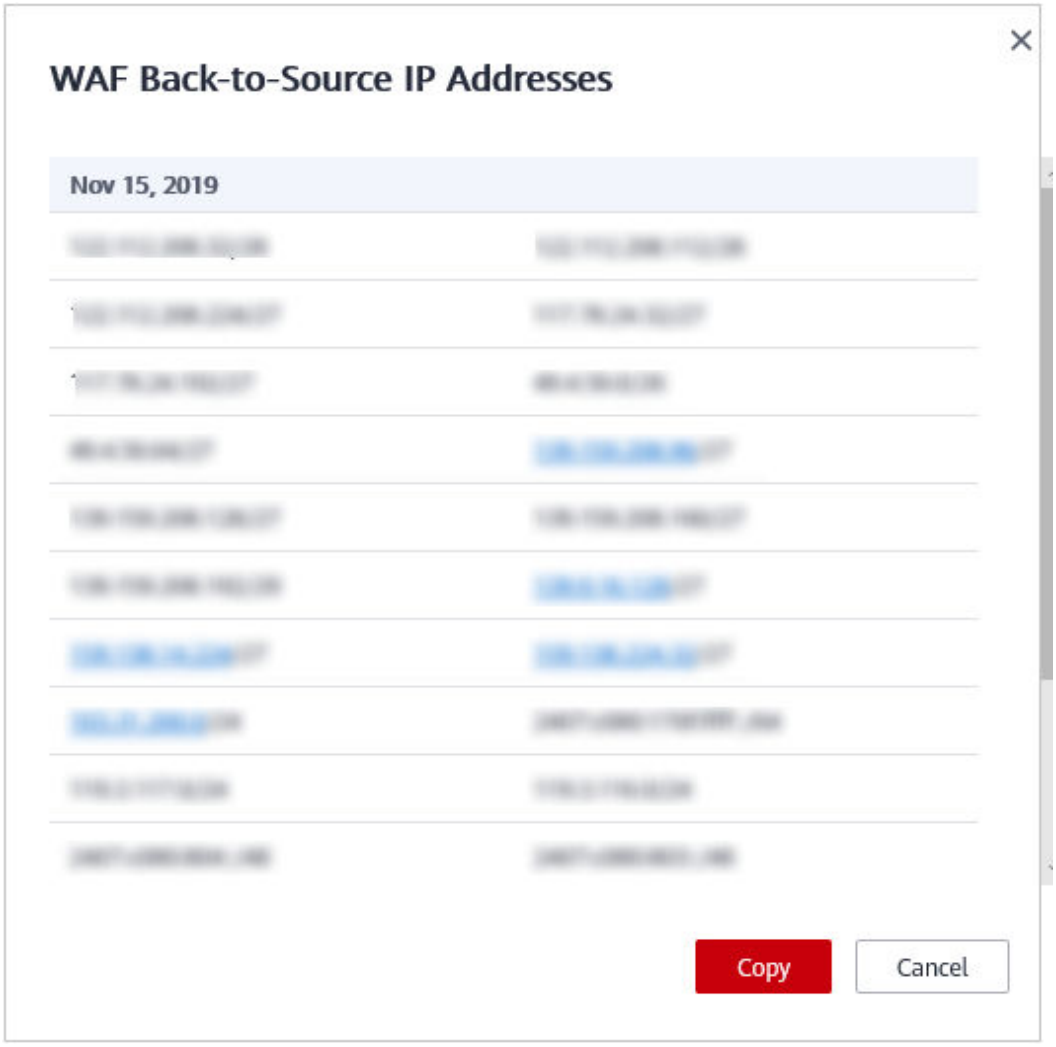
Passo 5 Above the website list, click **WAF Back-to-Source IP Addresses**.

Figura 3-19 WAF Back-to-Source IP Addresses



Passo 6 In the displayed dialog box, click **Copy** to copy all the addresses.

Figura 3-20 WAF Back-to-Source IP Addresses dialog box



Passo 7 Open the security software on the origin server and add the copied IP addresses to the whitelist.

----Fim

3.2.4 Passo 3: Testando o WAF

Para garantir que o WAF possa encaminhar suas solicitações de site normalmente, teste o WAF localmente depois de adicionar o domínio ao WAF.

Antes de testar o WAF, verifique se o protocolo, o endereço e a porta usados pelo servidor de origem (por exemplo, **www.example5.com**) estão corretos. Além disso, se o **Client Protocol** estiver definido como **HTTPS**, certifique-se de que o certificado e a chave privada carregados estejam corretos.

Pré-requisitos

Um nome de domínio foi adicionado ao WAF.

Restrições

Um registro CNAME é gerado com base no nome de domínio. Para o mesmo nome de domínio, os registros CNAME são os mesmos.

Conectando um nome de domínio ao WAF localmente

Passo 1 Obtenha o registro CNAME.

- Se você estiver adicionando um nome de domínio, execute as seguintes operações para obter o registro CNAME do nome de domínio depois de configurar as informações básicas sobre o nome de domínio:

  Clique em **Copy** para obter o registro CNAME do nome de domínio. Veja **Figura 3-21** ou **Figura 3-22**.

  Figura 3-21 Conectando um nome de domínio ao WAF (proxy usado)

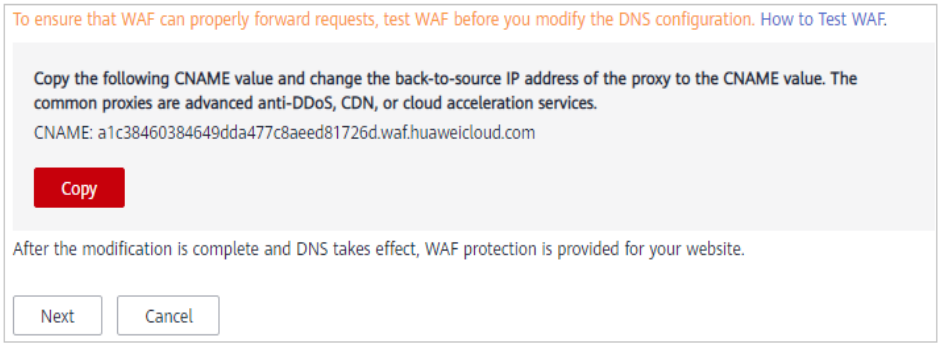
  

  Figura 3-22 Conectando um nome de domínio ao WAF (nenhum proxy usado)

- Se tiver adicionado um nome de domínio, execute os seguintes passos para obter o registo CNAME do nome de domínio:

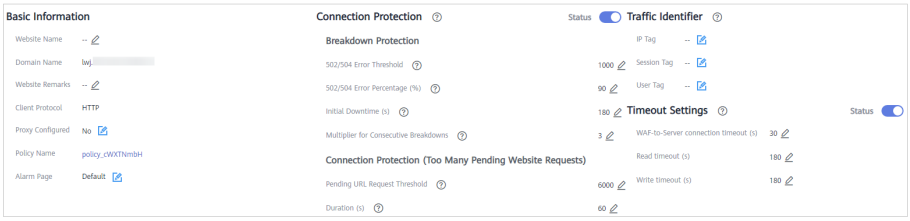
  a. Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

  b. Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

  c. No painel de navegação, escolha **Website Settings**.

  d. Na linha do nome de domínio desejado, clique no nome de domínio que deseja testar.

Figura 3-23 Informações básicas



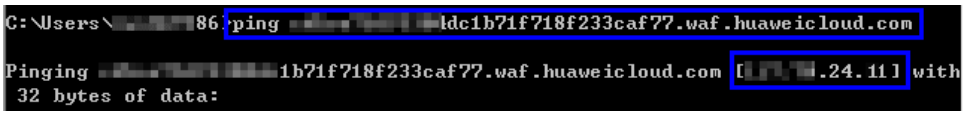
e. Na linha **CNAME**, clique em para copiar o registro CNAME.

Passo 2 Faça ping no registro CNAME e registre o endereço IP correspondente.

Use **www.example5.com** como um exemplo e seu registro CNAME é **xxxxxxxdc1b71f718f233caf77.waf.huaweicloud.com**.

Abra a CLI e execute o comando **ping xxxxxxxdc1b71f718f233caf77.waf.huaweicloud.com** para obter o endereço IP de retorno à origem do WAF. Como mostrado em **Figura 3-24**, o endereço IP de retorno à origem do WAF é exibido.

Figura 3-24 Ping CNAME



Passo 3 Adicione o nome de domínio e o endereço IP de retorno à origem do WAF ao arquivo **hosts**.

1. Use um editor de texto para abrir o arquivo **hosts**. Geralmente, o arquivo **hosts** é armazenado no diretório **C:\Windows\System32\drivers\etc**.
2. Adicione os endereços IP do WAF obtidos na **Etapa 2** e o nome de domínio protegido ao arquivo **hosts**. **Adicionar um registro** mostra um exemplo.

Figura 3-25 Adicionando um registro

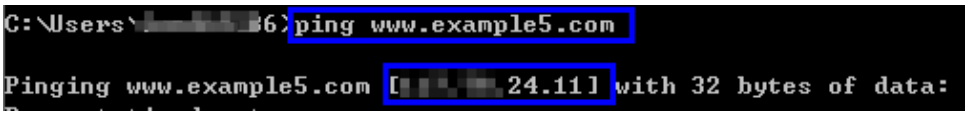
```
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
#                                         # source server
#                                         # x client host

# localhost name resolution is handled within DNS itself.
#       localhost
#       ::1             localhost

 24.11 www.example5.com
```

3. Salve o arquivo de **hosts** e sibile o nome de domínio protegido no PC local.

Figura 3-26 Pingando o nome de domínio



Espera-se que o endereço IP resolvido seja o endereço IP back-to-source do WAF obtido na **Etapa 2**. Se o endereço IP resolvido for o endereço do servidor de origem, execute o comando **ipconfig/flushdns** no sistema operacional Windows para limpar o cache DNS.

----Fim

Verificando se o encaminhamento WAF é normal

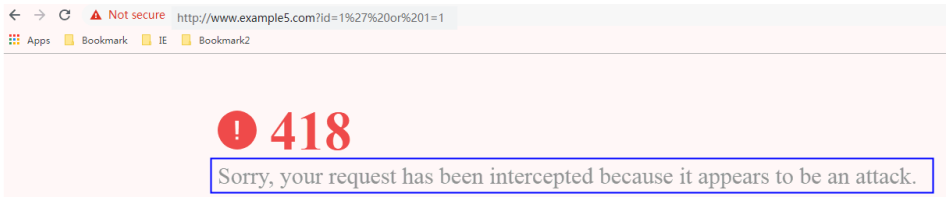
Passo 1 Limpe o cache do navegador e insira o nome do domínio na caixa de endereço de um navegador para verificar se o site pode ser acessado.

Se o nome de domínio resolver para o endereço IP back-to-source das configurações do WAF e do WAF estiver correto, o site poderá ser acessado.

Passo 2 Simula comandos simples de ataque na web.

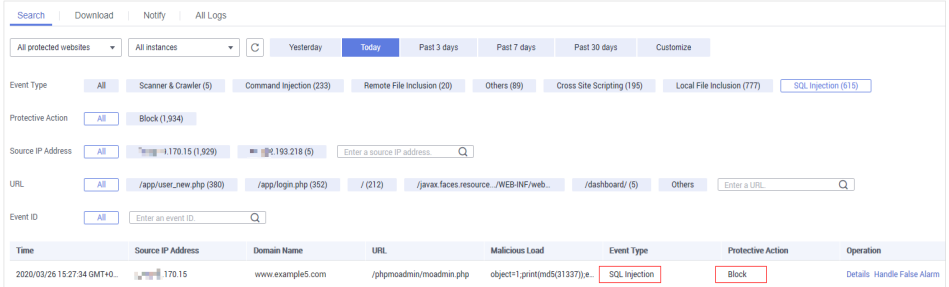
1. Defina o modo de **Basic Web Protection** para **Block**. Para obter detalhes, consulte **Ativar a Proteção Básica da Web**.
2. Limpe o cache do navegador, insira o nome de domínio de teste na barra de endereços e verifique se o WAF bloqueia o ataque de injeção SQL simulado no nome de domínio. **Figura 3-27** mostra um exemplo.

Figura 3-27 Solicitação bloqueada



3. No painel de navegação, escolha **Events** para exibir dados de teste. **Figura 3-28** mostra um exemplo.

Figura 3-28 Visualizando dados de teste



----Fim

3.2.5 Passo 4: Encaminhamento do tráfego do site para o WAF

Depois que você conecta um nome de domínio ao WAF, o WAF funciona como um proxy reverso entre o cliente e o servidor. O endereço IP real do servidor é oculto e apenas o endereço IP do WAF é visível para os visitantes da web.

Para garantir que sua instância do WAF funcione corretamente, teste-a de acordo com as instruções em **Passo 3: Testando o WAF** antes de rotear o tráfego de sua empresa para o WAF.

Pré-requisitos

Um nome de domínio foi adicionado, mas não conectado ao WAF.

Restrições

A proteção WAF entra em vigor apenas para endereços IP de clientes reais onde as solicitações se originam. Para garantir que o WAF obtenha endereços IP reais do cliente, se o seu site tiver proxies de camada-7, como CDN e produtos de aceleração de nuvem implantados na frente do WAF, **Yes** deve ser selecionado para **Proxy Configured**.

Limitações da especificação

Depois que seu site é conectado ao WAF, o arquivo que os visitantes podem carregar a cada vez não pode exceder 512 MB.

How WAF Works

- No proxy used

  DNS resolves your domain name to the origin server IP address before the site is connected to WAF. DNS resolves your domain name to the CNAME of WAF after the site is connected to WAF. Then WAF inspects the incoming traffic and filters out malicious traffic.

- A proxy (such as anti-DDoS service) used

  If a proxy such as anti-DDoS service is used on your site before it is connected to WAF, DNS resolves the domain name of your site to the anti-DDoS IP address. The traffic goes to the anti-DDoS service and the anti-DDoS service then routes the traffic back to the origin server. After you connect your website to WAF, change the back-to-source address of the proxy (such as anti-DDoS service) to the CNAME of WAF. In this way, the proxy forwards the traffic to WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

  NOTA

  - To ensure that WAF can properly forward requests, perform local verification by referring to **Testing WAF** before modifying the DNS configuration.
  - To prevent other users from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), add the subdomain name and TXT record on your DNS management platform. WAF can determine which user owns the domain name based on the subdomain name and TXT record.

Operation Guide

After a domain name is added, WAF generates a CNAME record, or CNAME, subdomain name, and TXT record for DNS to resolve the domain name to WAF so that website traffic can pass through WAF for detection. For details, see **Tabela 3-7**.

Tabela 3-7 Operation guide

Scenario	Generated Parameter Value	Operation Related to Domain Name Resolution
No proxy used	CNAME	The DNS obtains the CNAME of WAF.
Proxy used	CNAME, subdomain name, and TXT record	● Change the back-to-source IP address of the proxy, such as anti-DDoS service, to the CNAME of WAF. ● (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

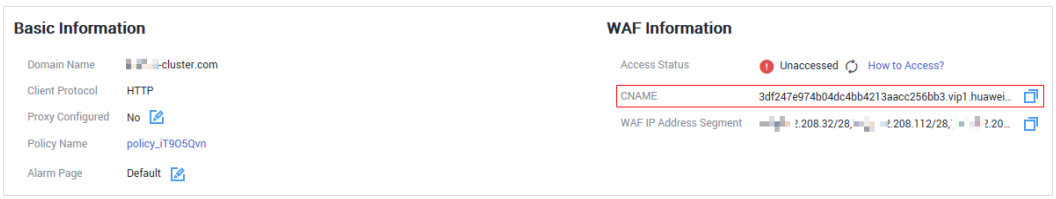
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na linha que contém o nome de domínio desejado, clique no nome de domínio para ir para a página **Basic Information**.

Passo 6 Na linha **CNAME**, clique em para copiar o registro CNAME. **Figura 3-29** mostra um exemplo.

Figura 3-29 Copiando o registro CNAME



Se a mensagem "CNAME copiado com êxito" for exibida no canto superior direito da página, o registro CNAME será copiado com êxito.

Passo 7 Conecte o nome de domínio ao WAF.

- Nenhum proxy usado

  Configure o registro CNAME no seu provedor de DNS. Para obter detalhes, entre em contato com seu provedor de DNS.

- Proxy usado

  AVISO

  Se seu site tiver implantado proxies de camada 7, como Rede de entrega de conteúdo (CDN) e serviço de aceleração de nuvem, defina **Proxy configured** como **Yes** para garantir que as políticas de segurança do WAF entrem em vigor. Para mais detalhes, consulte **Exibição de informações básicas**.

  Altere o endereço IP de origem do proxy usado, como serviços anti-DDoS e CDN, para o registro CNAME copiado.

  NOTA

  Para impedir que outros usuários configurem seus nomes de domínio no WAF com antecedência (isso causará interferência na proteção do nome de domínio), adicione o nome de subdomínio e o registro TXT em sua plataforma de gerenciamento de DNS.

  1. Obter **Subdomain Name** e **TXT Record**: Na linha **Access Status**, clique em **How to Access**. Na caixa de diálogo **Access Guide**, copie o **Subdomain Name** e o **TXT Record**.
  2. Adicione o **Subdomain Name** no provedor de DNS e configure o **TXT Record** para o nome do subdomínio. Para obter detalhes sobre o método de configuração, consulte **Quais são os impactos se um nome de subdomínio e registro TXT não forem configurados?**

  O WAF determina qual usuário é o proprietário do nome de domínio com base no **Subdomain Name** e no **TXT Record** configurados.

Passo 8 Verifique se o CNAME do nome de domínio foi configurado.

1. No Windows, escolha **Start** > **Run**. Em seguida, insira **cmd** e pressione **Enter**.
2. Execute um comando **nslookup** para consultar o registro CNAME.

   Se o CNAME configurado é retornado, a configuração é bem sucedida. Um exemplo de resposta de comando é exibido em **Figura 3-30**.

   Exemplo de comando:

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

Figura 3-30 Consultando o CNAME

----Fim

Procedimento de acompanhamento

- Se o servidor usar outros firewalls de rede, desative esses firewalls de rede ou adicione o intervalo de endereços IP do WAF à lista de permissões de endereços IP desses firewalls de rede. Caso contrário, esses firewalls podem considerar o endereço IP do WAF como um endereço IP malicioso. Para obter detalhes, consulte **Como faço para colocar na lista branca o intervalo de endereços IP back-to-source do WAF?**
- Se o servidor da Web estiver usando software de segurança pessoal, substitua-o por software de segurança empresarial e coloque na lista de permissões os intervalos de endereços IP do WAF.

Verificação

- Por padrão, o WAF detecta o **Access Status** de cada nome de domínio protegido a cada hora.
- Geralmente, se você efetuou uma conexão de domínio e o **Access Status** é **Accessible**, o nome de domínio é conectado ao WAF.

Outras operações

- **Por que o sistema me informa que meu conjunto de registros está em conflito com um existente?**
- **Quais são os impactos se um nome de subdomínio e um registro TXT não forem configurados?**

3.3 Conexão de um site ao WAF (Modo Dedicado)

3.3.1 Processo de conexão (modo dedicado)

Para permitir que sua instância dedicada do WAF proteja seu site, o nome de domínio do site deve estar conectado à instância do WAF para que o tráfego de entrada do site possa ir para o WAF primeiro.

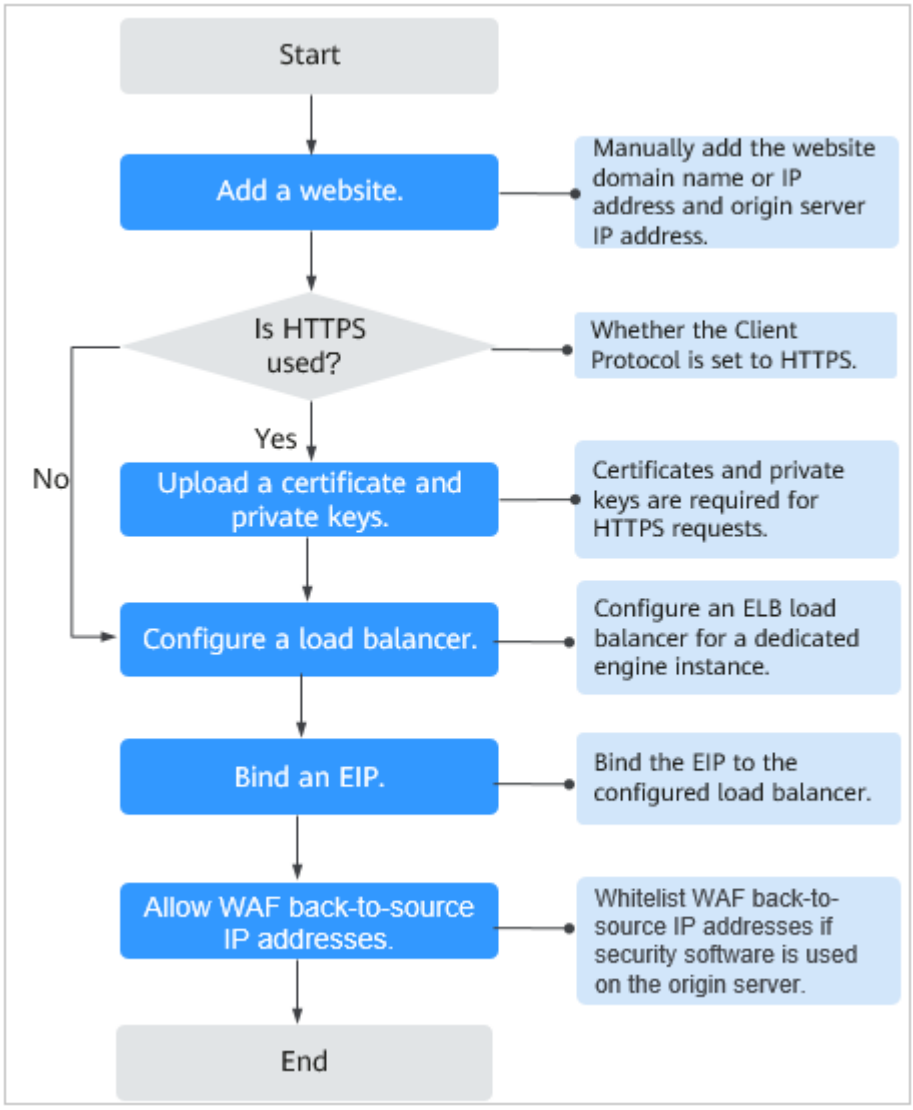
Limitações

As instâncias WAF dedicadas só podem proteger aplicativos da Web e sites implantados na HUAWEI CLOUD e acessíveis por meio de nomes de domínio ou endereços IP. Para obter detalhes sobre instâncias dedicadas do WAF, consulte **Diferenças de edição**.

Processos de conexão de um site ao WAF

Depois de adquirir uma instância dedicada do WAF, conclua as configurações necessárias seguindo o processo mostrado em **Figura 3-31**.

Figura 3-31 Processo de conexão de um site a uma instância dedicada do WAF



Corrigindo sites inacessíveis

Se um site não estiver conectado ao WAF, seu status de acesso será **Inaccessible**. Para corrigir esse problema, consulte **Por que o status de acesso de um nome de domínio ou endereço IP está inacessível?**

3.3.2 Passo 1: Adicionar um site ao WAF (Modo Dedicado)

Se seus servidores de serviço forem implantados no Huawei Cloud, você poderá adicionar o nome de domínio ou o endereço IP do site ao WAF para que o tráfego do site seja encaminhado ao WAF para inspeção.

NOTA

Se você tiver ativado projetos da empresa, poderá selecionar seu projeto da empresa na lista suspensa **Enterprise Project** e adicionar sites a serem protegidos no projeto.

Pré-requisitos

- Você adquiriu uma instância dedicada do WAF.
- O nome de domínio ou endereço IP foi registrado com a licença ICP, mas não foi adicionado ao WAF.

Restrições

- Um balanceador de carga voltado para a Internet foi implantado no site que você deseja proteger com instâncias WAF dedicadas.
- Se seu site não tiver um servidor proxy de camada-7, como CDN e serviço de aceleração de nuvem implantado na frente do WAF, e usar apenas balanceadores de carga de camada-4 (ou NAT), defina **Proxy Configured** como **No**. Caso contrário, **Proxy Configured** deve ser definido como **Yes**. Isso garante que o WAF obtenha endereços IP reais dos visitantes do site e tome ações de proteção configuradas nas políticas de proteção.
- Os nomes de domínio dos sites a serem protegidos devem ter licenças ICP. Caso contrário, os nomes de domínio não podem ser adicionados ao WAF.

Coletando Informações de Nome de Domínio/Endereço IP

Antes de adicionar um nome de domínio ou endereço IP, obtenha as informações listadas em **Tabela 3-8**.

Tabela 3-8 Nome de domínio ou detalhes de endereço IP necessários

Informação	Parâmetro	Descrição	Valor de exemplo
Parâmetros	Nome de domínio/ endereço IP	• Nome de domínio: usado pelos visitantes para acessar seu site. Um nome de domínio consiste em letras separadas por pontos (.). É um endereço legível por humanos que mapeia para o endereço IP legível por máquina do seu servidor. • IP: Endereço IP do site.	www.example.com

Informação	Parâmetro	Descrição	Valor de exemplo
	Porto padrão/não padronizado	A porta de serviço correspondente ao nome de domínio do site que você deseja proteger. ● Portas padrão – 80: porta padrão quando o protocolo do cliente é definido como HTTP – 443: porta padrão quando o protocolo do cliente é definido como HTTPS ● Portas não padronizadas Portas diferentes das portas 80 e 443 **AVISO** Se o seu site usa uma porta não padrão, verifique se a edição do WAF que você planeja comprar pode proteger a porta não padrão antes de fazer uma compra. Para mais detalhes, consulte **Portas suportadas pelo WAF**.	80
	Protocolo do cliente	Protocolo usado por um cliente (por exemplo, um navegador) para acessar o site. O WAF suporta HTTP e HTTPS.	HTTP
	Protocolo do servidor	Protocolo usado pelo WAF para encaminhar solicitações ao cliente (como um navegador). As opções são **HTTP** e **HTTPS**.	HTTP
	VPC	Selecione a VPC à qual a instância dedicada do WAF pertence.	vpc-default
	Endereço do servidor	Endereço IP privado ou nome de domínio do servidor do site que um cliente (por exemplo, um navegador) acessa	192.168.1.1

Informação	Parâmetro	Descrição	Valor de exemplo
(Opcional) Certificado	Nenhum	Se você definir o **Client Protocol** como **HTTPS**, será necessário configurar um certificado no WAF e associá-lo ao nome de domínio. **AVISO** ● Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver no formato PEM, converta-o para o formato pem consultando **Como faço para converter um certificado em formato PEM?** ● Atualmente, os certificados comprados no Huawei Cloud SCM podem ser enviados apenas para o projeto corporativo **default**. Para outros projetos corporativos, os certificados SSL enviados pelo SCM não podem ser usados.	Nenhum

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 No canto superior esquerdo da lista de sites, clique em **Add Website**.

Passo 6 Configure as informações básicas do nome de domínio. **Figura 3-32** mostra um exemplo. **Tabela 3-9** listas parâmetros.

Figura 3-32 Configurando as configurações básicas de um site

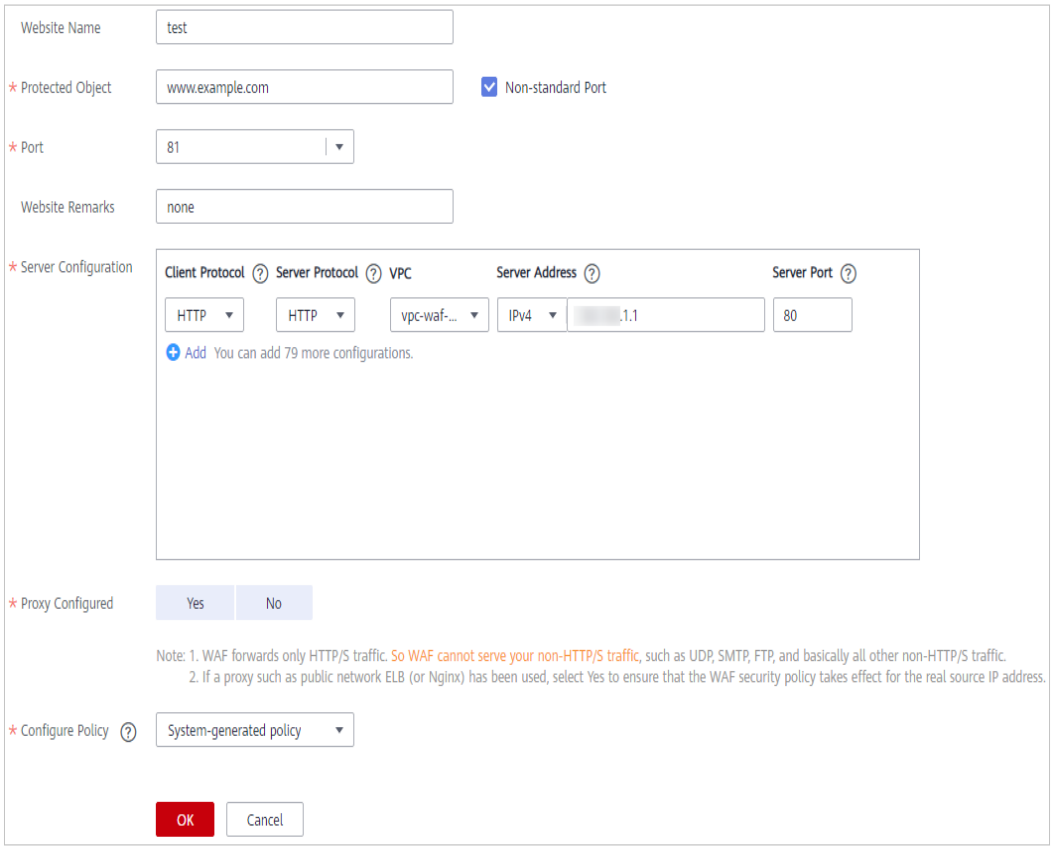


Tabela 3-9 Descrição do parâmetro

Parâmetro	Descrição	Valor de exemplo
Nome do site	Nome do site que você quer proteger	Nenh

Parâmetro	Descrição	Valor de exemplo
Site Protegido	Um nome de domínio ou endereço IP do site a ser protegido. O nome de domínio pode ser um único nome de domínio ou um nome de domínio curinga. ● Nome de domínio único: Insira um único nome de domínio. Por exemplo, o www.example.com. ● Nome de domínio Wildcard **NOTA** Nomes de domínio curinga não podem conter sublinhados (_). – Se o endereço IP do servidor de cada nome de subdomínio for o mesmo, digite um nome de domínio curinga a ser protegido. Por exemplo, se os nomes de subdomínio ***a.example.com***, ***b.example.com***, e ***c.example.com*** tiverem o mesmo endereço IP de servidor, você poderá adicionar o nome de domínio curinga ****.example.com*** ao WAF para proteger os três. – Se os endereços IP do servidor dos nomes de subdomínio forem diferentes, adicione nomes de subdomínio como nomes de domínio únicos, um por um.	Nome de domínio único: **www.example.com** Nome de domínio curinga: ***.example.com** Formato do endereço IP: *XXX.XXX.1.1*
Porta	Defina este parâmetro somente se **Non-standard Port** estiver selecionada. **Exemplo de configuração 1: Protegendo o tráfego para a mesma porta padrão com diferentes endereços IP de servidor de origem atribuídos** mostra um exemplo da configuração da porta. ● Se o **Client Protocol** for **HTTP**, o WAF protegerá os serviços na porta padrão 80 por padrão. Se o **Client Protocol** for **HTTPS**, o WAF protegerá os serviços na porta padrão 443 por padrão. ● Para configurar uma porta diferente das portas 80 e 443, selecione **Non-standard Port** e selecione uma porta não padrão na lista suspensa **Port**. **NOTA** Se uma porta não padrão estiver configurada, os visitantes precisarão adicionar a porta não padrão ao final do endereço do site quando acessarem o site. Caso contrário, ocorrerá um erro 404.	81
Observações do site	Uma breve descrição do site	-

Parâmetro	Descrição	Valor de exemplo
Configuração do servidor	Endereço do servidor web. A configuração contém o **Client Protocol**, **Server protocol**, a VPC, **Server Address,** e **Server Port**. ● **Client Protocol**: Protocolo usado para encaminhar solicitações de um cliente para a instância dedicada do WAF. As opções são **HTTP** e **HTTPS**. ● **Server Protocol**: Protocolo usado para encaminhar uma solicitação de cliente para o servidor de origem por meio da instância dedicada do WAF. As opções são **HTTP** e **HTTPS**. **NOTA** – Para obter detalhes sobre como configurar **Client Protocol** e **Server Protocol**, consulte **Regras para configurar o protocolo do cliente e o protocolo do servidor**. – O WAF pode verificar solicitações WebSocket e WebSockets, o que é ativado por padrão. ● **VPC**: Selecione a VPC à qual a instância dedicada do WAF pertence. ● **Server Address**: Endereço IP privado / interno ou nome de domínio do servidor do site que um cliente (por exemplo, um navegador) acessa. ● **Server Port**: porta de serviço do servidor para a qual a instância dedicada do WAF encaminha as solicitações do cliente.	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **VPC**: vpc-default **Server Address**: *192.168.1.1* **Server Port**: **80**

Parâmetro	Descrição	Valor de exemplo
Nome do certificado	Se **Client Protocol** estiver definido como **HTTPS**, selecione um certificado. Você pode selecionar um certificado existente ou importar um certificado externo. Para obter detalhes sobre como importar um certificado, consulte **Importando um Novo Certificado**. Para obter detalhes sobre como criar um certificado, consulte **Carregamento de um certificado**. Além disso, você pode comprar um certificado no console do SCM e enviá-lo para o WAF. Para obter detalhes sobre como enviar um certificado SSL no SCM para o WAF, consulte **Enviando um certificado SSL para outros serviços em Nuvem**. **AVISO** ● Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver no formato.pem, converta-o em certificado a.pem consultando **Importando um Novo Certificado** antes de carregar o certificado. ● Atualmente, os certificados comprados no Huawei Cloud SCM podem ser enviados apenas para o projeto corporativo **default**. Para outros projetos corporativos, os certificados SSL enviados pelo SCM não podem ser usados. ● Cada nome de domínio deve ter um certificado associado. Um nome de domínio curinga só pode usar um certificado de domínio curinga. Se você tiver apenas certificados de domínio único, adicione nomes de domínio ao WAF um por um.	Nenhum

Passo 7 Configurar **Proxy Configured** .

Se seu site não tiver um servidor proxy de camada-7, como CDN e serviço de aceleração de nuvem implantado na frente do WAF, e usar apenas balanceadores de carga de camada-4 (ou NAT), defina **Proxy Configured** como **No**. Caso contrário, **Proxy Configured** deve ser definido como **Yes**. Isso garante que o WAF obtenha endereços IP reais dos visitantes do site e tome ações de proteção configuradas nas políticas de proteção.

Passo 8 Selecione uma política. Por padrão, **system-generated policy** é selecionada.

Você pode selecionar uma política configurada. Você também pode personalizar as regras depois que o nome de domínio for conectado ao WAF.

Políticas geradas pelo sistema:

- Proteção básica da Web (modo **Log only** e verificações comuns)

  The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections.
- Anti-crawler (modo de **Log only** e recurso **Scanner**)

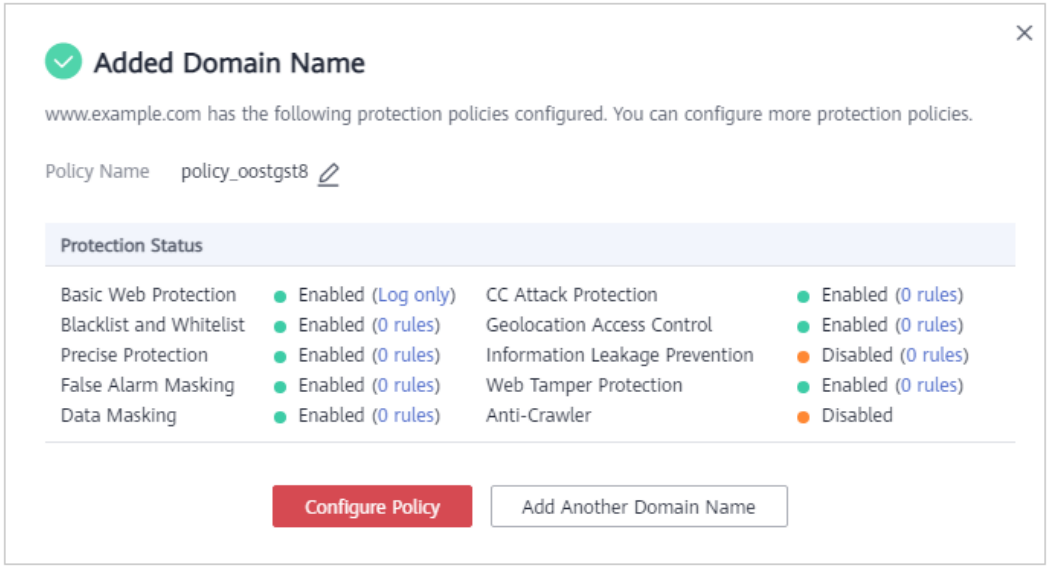
  WAF only logs web scanning tasks, such as vulnerability scanning and virus scanning, such as crawling behavior of OpenVAS and Nmap.

NOTA

Log only: WAF only logs detected attack events instead of blocking them.

Passo 9 Clique em **OK** .

Figura 3-33 Nome de domínio adicionado



- Clique em **Configure Policy** e configure uma política de proteção para o site.
- Clique em **Add Another Domain Name** e adicione mais sites a serem protegidos.
- Feche a caixa de diálogo e exiba os sites adicionados na lista de sites protegidos.

----Fim

Verificação

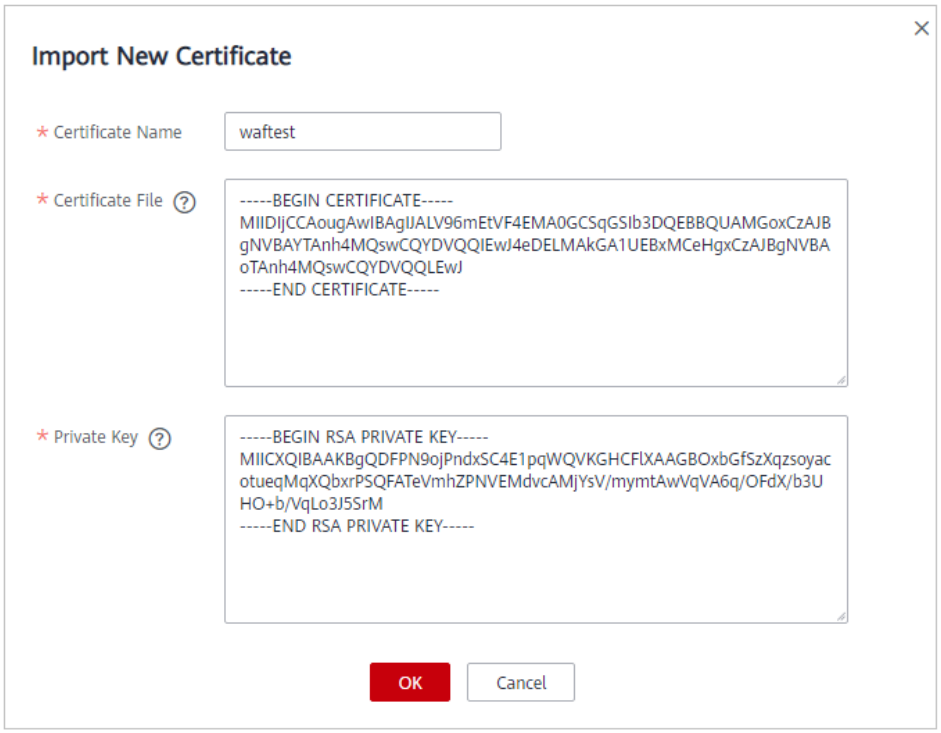
O **Access Status** inicial de um site é **Inaccessible**. Depois de configurar um balanceador de carga e vincular um EIP ao balanceador de carga do seu site, quando uma solicitação atinge a instância dedicada do WAF, o status de acesso muda automaticamente para **Accessible**.

Importando um Novo Certificado

Se você definir o **Client Protocol** como **HTTPS**, será necessário um certificado SSL. Você pode executar as etapas a seguir para importar um novo certificado.

1. Clique em **Import New Certificate**. Na caixa de diálogo exibida, insira um nome de certificado e copie o arquivo de certificado e a chave privada para as caixas de texto correspondentes.

Figura 3-34 Importar Novo Certificado



NOTA

O WAF criptografa e salva a chave privada para mantê-la segura.

Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver no formato.pem, converta-o localmente para.pem consultando **Tabela 3-10** antes de carregá-lo.

Tabela 3-10 Comandos de conversão de certificados

Formato	Método de conversão
CER/CRT	Renomeie o arquivo de certificado **cert.crt** para **cert.pem**.
PFX (em inglês)	● Obtenha uma chave privada. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** ● Obter um certificado. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Converter um certificado. Por exemplo, execute o seguinte comando para converter **cert.p7b** em **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Renomeie o arquivo de certificado **cert.cer** para **cert.pem**.

Formato	Método de conversão
DER	• Obtenha uma chave privada. Por exemplo, execute o seguinte comando para converter **privatekey.der** em **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** • Obter um certificado. Por exemplo, execute o seguinte comando para converter **cert.cer** em **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTA

- Antes de executar um comando OpenSSL, verifique se a ferramenta **OpenSSL** foi instalada no host local.
- Se seu PC local executa um sistema operacional Windows, vá para a interface de linha de comando (CLI) e execute o comando de conversão de certificados.

2. Clique em **OK**.

3.3.3 Passo 2: Configurar um balanceador de carga

Para garantir a confiabilidade da sua instância dedicada do WAF, depois de adicionar um site a ela, use o Elastic Load Balance (ELB) da HUAWEI CLOUD para configurar um balanceador de carga e uma verificação de integridade para a instância dedicada do WAF.

AVISO

O ELB de HUAWEI CLOUD é cobrado por tráfego. Para obter detalhes, consulte **Detalhes de preços do ELB**.

Pré-requisitos

- Você adicionou um site a uma instância dedicada do WAF.
- Você comprou um balanceador de carga. Para obter detalhes sobre balanceadores de carga, consulte **Diferenças entre balanceadores de carga compartilhados e dedicados**.
- As portas relacionadas foram ativadas no grupo de segurança ao qual a instância dedicada do WAF pertence.

  Você pode configurar seu grupo de segurança da seguinte maneira:

  – Regras de entrada

    Adicione uma regra de entrada para permitir que o tráfego de rede de entrada passe por uma porta especificada com base em seus requisitos de serviço. Por exemplo, se você quiser permitir o acesso da porta 80, adicione uma regra que permita **TCP** e porta **80**.

  – Regras de saída

    Mantenha as configurações padrão. Todo o tráfego de rede de saída é permitido por padrão.

  Para obter mais detalhes, consulte **Adicionando uma regra de grupo de segurança**.

Restrições

A porta de escuta da instância WAF dedicada deve ser a mesma que a configurada no **Passo 1: Adicionar um site ao WAF (Modo Dedicado)**.

Impacto no sistema

Se você selecionar **Weighted round robin** para **Load Balancing Algorithm**, desative **Sticky Session**. Se você ativar **Sticky Session**, as mesmas solicitações serão encaminhadas para a mesma instância dedicada do WAF. Se essa instância se tornar defeituosa, ocorrerá um erro quando as solicitações chegarem a ela na próxima vez.

Adicionando um Listener

Passo 1 **Efetue login no console de gerenciamento**.

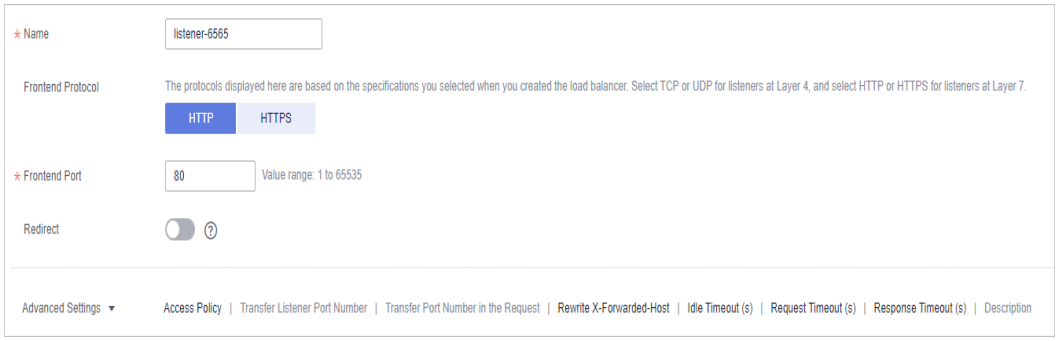
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo da página e escolha **Elastic Load Balance** em **Network** para acessar a página **Load Balancers**.

Passo 4 Clique no nome do balanceador de carga desejado na coluna **Name** para ir para a página **Basic Information**.

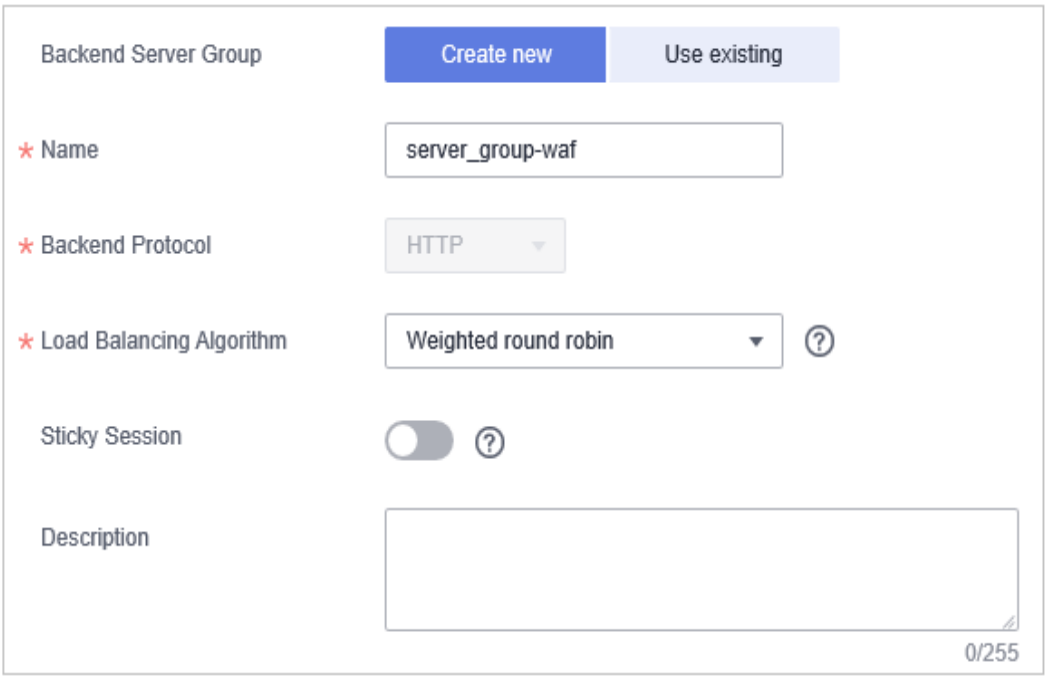
Passo 5 Clique na tab **Listeners**, clique em **Add Listener** e configure as informações do listener. **Figura 3-35** mostra um exemplo.

Figura 3-35 Configurando um ouvinte



Passo 6 Clique em **Next: Configure Request Routing Policy**. **Figura 3-36** mostra um exemplo.

Figura 3-36 Configurando um grupo de servidores de back-end

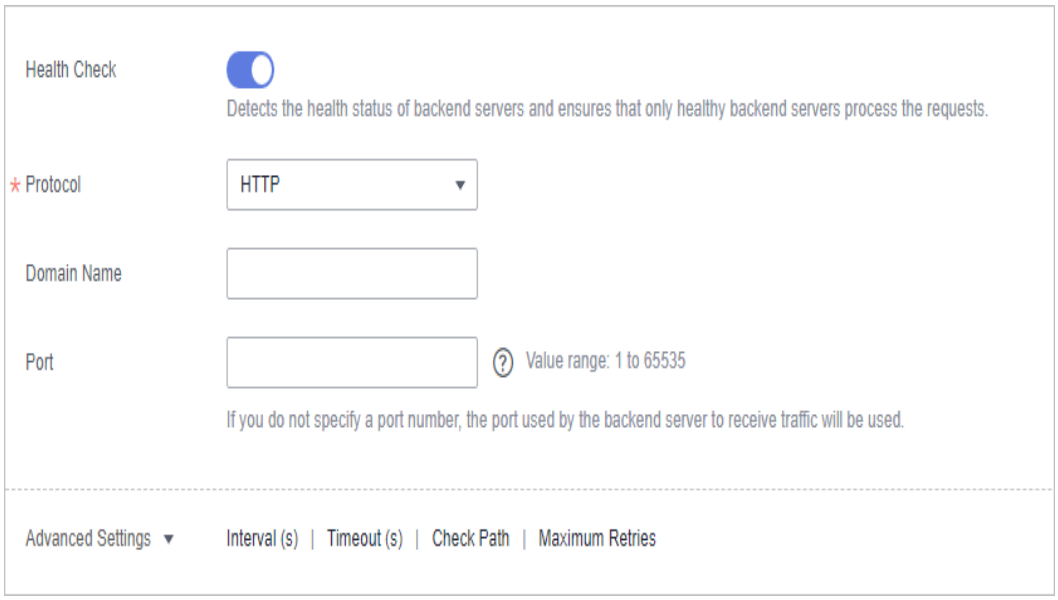


AVISO

- Se você selecionar **Weighted round robin** para **Load Balancing Algorithm**, desative **Sticky Session**. Se você ativar **Sticky Session**, as mesmas solicitações serão encaminhadas para a mesma instância dedicada do WAF. Se essa instância se tornar defeituosa, ocorrerá um erro quando as solicitações chegarem a ela na próxima vez.
- Para obter detalhes sobre as políticas de distribuição de tráfego do ELB, consulte **Algoritmos de balanceamento de carga**.

Passo 7 Clique em **Next: Add Backend Server** e configure uma verificação de integridade.

Figura 3-37 Configuração de verificação de saúde



AVISO

- Defina a **Port** como a porta do site configurado em **Passo 1: Adicionar um site ao WAF (Modo Dedicado)**, que é a porta de serviço escutada pela instância do WAF.
- Para obter detalhes sobre como configurar a verificação de integridade.

Passo 8 Clique em **Next: Confirm**.

Passo 9 Clique em **Submit**.

----Fim

Adicionando instâncias do WAF a um balanceador de carga do ELB

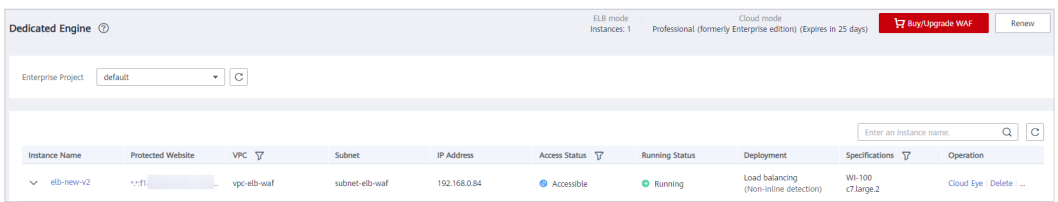
Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

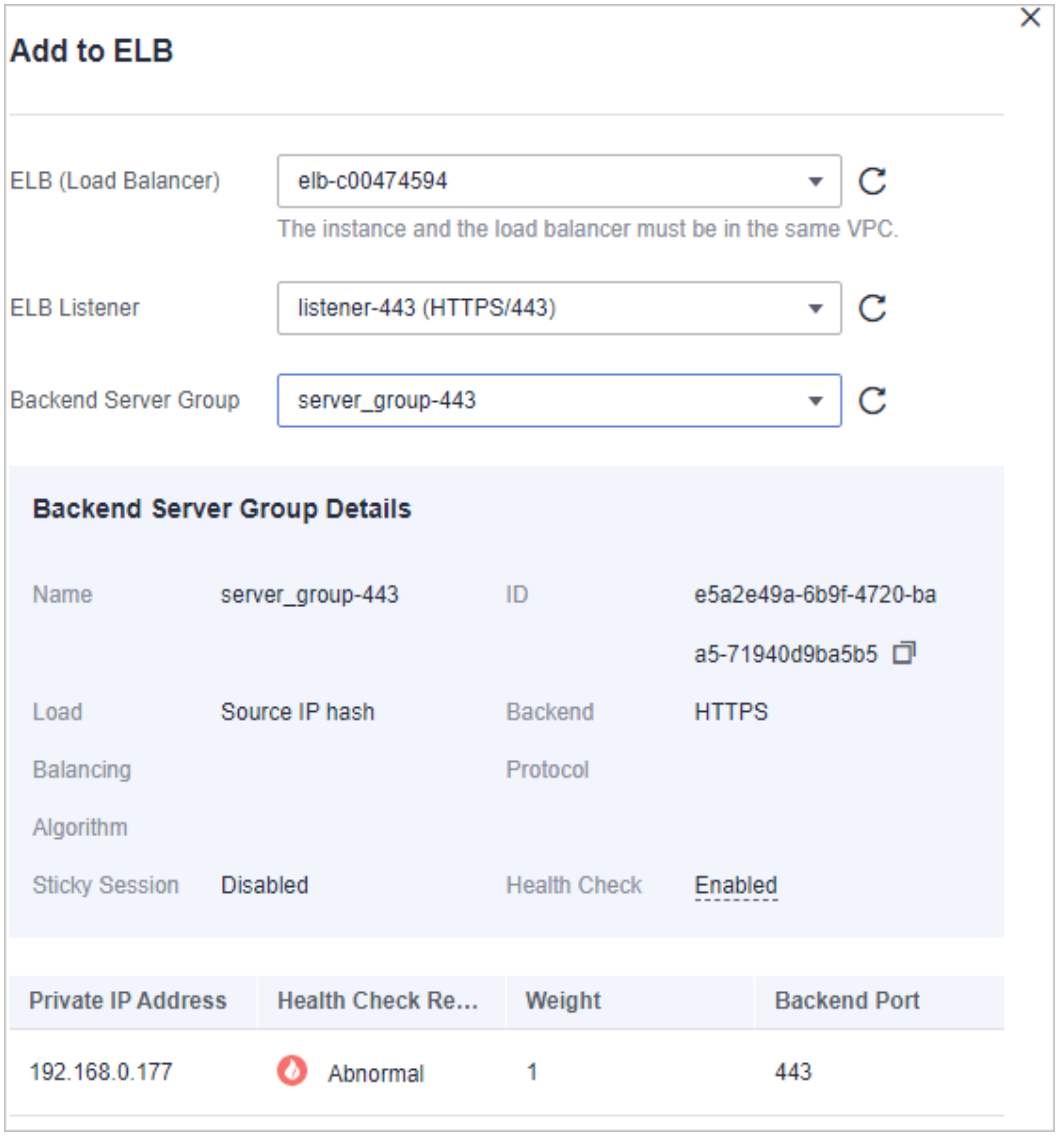
Figura 3-38 Lista de motores dedicada



Passo 5 Na linha que contém a instância que você deseja atualizar, clique em **More** > **Add to ELB** na coluna **Operation**.

Passo 6 Na caixa de diálogo **Add to ELB**, especifique **ELB (Load Balancer)**, **ELB Listener** e **Backend Server Group** com base em **Adicionando um Listener**.

Figura 3-39 Adicionar ao ELB



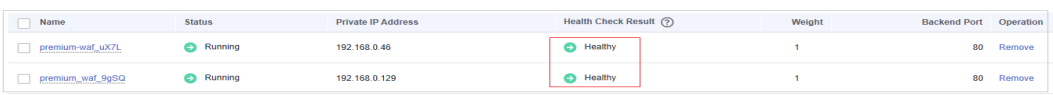
Passo 7 Clique em **OK**.

----Fim

Verificação

Se o **Health Check Result** for **Healthy**, o balanceador de carga será configurado.

Figura 3-40 Balanceador de carga ELB configurado



3.3.4 Passo 3: Vincular um EIP a um balanceador de carga

Depois de configurar um balanceador de carga para sua instância dedicada do WAF, você precisa desvincular o EIP do servidor de origem e, em seguida, vincular esse EIP ao balanceador de carga que você configurou. Para obter detalhes, consulte **Configuração de um Load Balancer**. O tráfego de solicitação, em seguida, vai para a instância dedicada do WAF para detecção de ataque primeiro e, em seguida, vai para o servidor de origem, garantindo a segurança, estabilidade e disponibilidade do servidor de origem.

Pré-requisitos

Você configurou um balanceador de carga para uma instância dedicada do WAF.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Na página **Elastic Load Balancers**, localize a linha que contém o load balancer configurado para o servidor de origem, clique em **More** na coluna **Operation** e selecione **Unbind IPv4 EIP**. **Figura 3-41** mostra um exemplo.

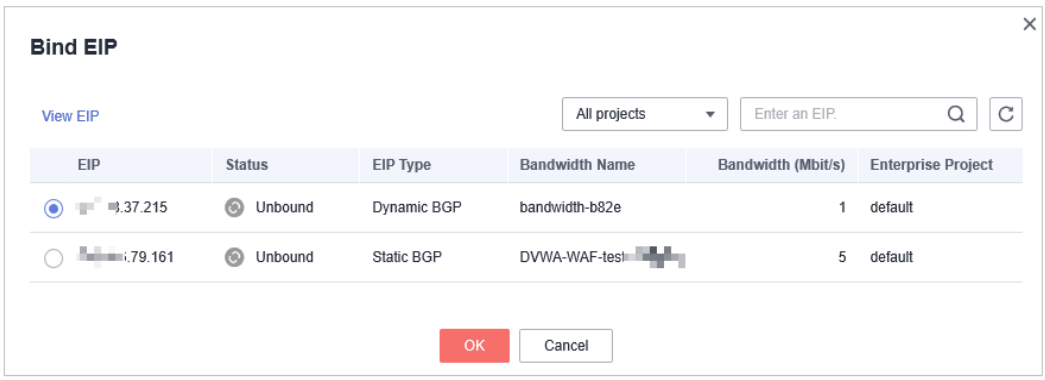
Figura 3-41 Desvinculação de um EIP

Passo 4 Na caixa de diálogo exibida, clique em **Yes**.

Passo 5 Na página **Load Balancers**, localize a linha que contém o balanceador de carga configurado para a instância dedicada do WAF, clique em **More** na coluna **Operation** e selecione **Bind EIP**.

Passo 6 Na caixa de diálogo **Bind EIP**, selecione o EIP não associado em **Passo 3** e clique em **OK**.

Figura 3-42 Vinculando um EIP



----Fim

3.3.5 Passo 4: Colocando na lista branca o endereço de IP de recuperação da instância WAF dedicada

Para permitir que as instâncias WAF dedicadas entrem em vigor, configure as regras de ACL no servidor de origem para confiar apenas nos endereços de IP de volta à origem de todas as instâncias WAF dedicadas. Isso impede que hackers ataquem o servidor de origem através dos endereços IP do servidor.

AVISO

As regras de ACL devem ser configuradas no servidor de origem para permitir endereços IP back-to-source do WAF. Caso contrário, os visitantes do seu site receberão frequentemente o código de erro 502 ou 504 depois que seu site for conectado ao WAF.

Por que eu preciso colocar os endereços IP back-to-source do WAF na lista de permissões?

No modo dedicado, o tráfego do site é direcionado para o balanceador de carga configurado para suas instâncias dedicadas do WAF e, em seguida, para instâncias dedicadas do WAF. Este último filtrará o tráfego malicioso e roteará apenas o tráfego normal para o servidor de origem. Dessa forma, o servidor de origem só se comunica com os endereços IP back-to-source do WAF. Ao fazer isso, o WAF protege o servidor de origem de ser atacado, mesmo que o endereço de IP do servidor seja exposto a hackers acidentalmente. No modo dedicado, os endereços de IP back-to-source do WAF são os endereços de IP de sub-rede das instâncias dedicadas do WAF.

O software de segurança no servidor de origem pode muito provavelmente considerar os endereços de IP do WAF back-to-source como maliciosos e bloqueá-los. Depois que eles forem bloqueados, o servidor de origem negará todas as solicitações do WAF. Como resultado, seu site pode ficar indisponível ou responder muito lentamente. Portanto, as regras de ACL devem ser configuradas no servidor de origem para confiar somente nos endereços de IP de sub-rede das instâncias dedicadas do WAF.

Pré-requisitos

Seu site foi conectado às instâncias dedicadas do WAF.

NOTA

Se você ativou projetos corporativos, pode selecionar seu projeto corporativo na lista suspensa **Enterprise Project** e colocar na lista de permissões os endereços IP back-to-source das instâncias WAF dedicadas no projeto.

Apontando tráfego para um ECS que hospeda seu site

Se o seu servidor de origem for implantado em um HUAWEI CLOUD ECS, execute as seguintes etapas para configurar uma regra de grupo de segurança para permitir que apenas o endereço de IP de retorno à origem da instância dedicada acesse o servidor de origem.

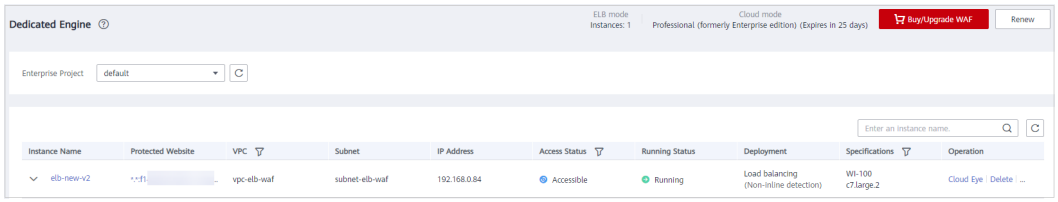
Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

Figura 3-43 Lista de motores dedicada



Passo 5 Na coluna **Subnet IP Address**, obtenha o endereço de IP de cada instância dedicada do WAF na sua conta. **Figura 3-44** mostra um exemplo.

Figura 3-44 Endereço de IP de sub-rede de uma instância WAF dedicada

Passo 6 Clique em no canto superior esquerdo da página e escolha **Compute** > **Elastic Cloud Server**.

Passo 7 Localize a linha que contém o ECS que hospeda seu site. Na coluna **Name/ID**, clique no nome do ECS para ir para a página de detalhes do ECS.

Passo 8 Clique na guia **Security Groups**. Em seguida, clique em **Change Security Group**.

Passo 9 Na caixa de diálogo **Change Security Group** exibida, selecione um grupo de segurança ou crie um grupo de segurança.

Passo 10 Clique no nome do grupo de segurança para exibir os detalhes.

Passo 11 Clique na guia **Inbound Rules** e clique em **Add Rule**. Em seguida, especifique os parâmetros na caixa de diálogo **Add Inbound Rule**. Para mais detalhes, consulte **Tabela 3-11**. **Figura 3-45** mostra um exemplo.

Figura 3-45 Adicionar regra de entrada

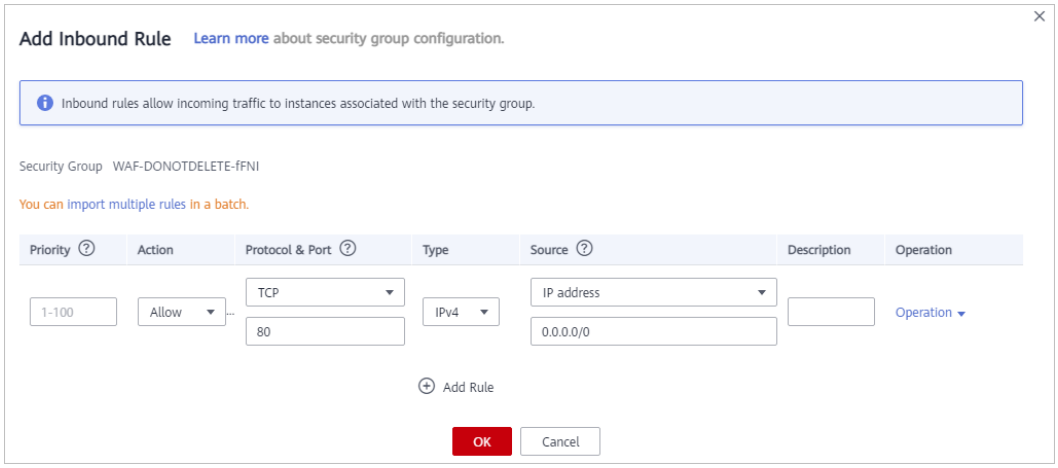


Tabela 3-11 Parâmetros da regra de entrada

Parâmetro	Descrição
Protocolo & Porta	Protocolo e porta para os quais a regra de grupo de segurança entra em vigor. Se você selecionar **TCP (Custom ports)**, insira o número da porta do servidor de origem na caixa de texto abaixo da caixa TCP.
Origem	Endereço IP de sub-rede de cada instância WAF dedicada que você obtém em **Passo 5**. Configure uma regra de entrada para cada endereço de IP. **NOTA** Uma regra de entrada pode conter apenas um endereço de IP. Para configurar uma regra de entrada para cada endereço de IP, clique em **Add Rule** para adicionar mais regras. Um máximo de 10 regras pode ser configurado.

Passo 12 Clique em **OK**.

Agora, o grupo de segurança permite todo o tráfego de entrada dos endereços de IP back-to-source de todas as instâncias dedicadas do WAF.

Para verificar se a configuração entra em vigor, use a ferramenta Telnet para verificar se uma conexão com a porta de serviço do servidor de origem vinculada ao endereço de IP protegido pelo WAF foi estabelecida.

Por exemplo, execute o comando a seguir para verificar se a conexão com a porta de serviço de servidor de origem 443 vinculada ao endereço de IP protegido pelo WAF foi estabelecida. Se a conexão não puder ser estabelecida pela porta de serviço, mas o site ainda estiver acessível, as regras de entrada do grupo de segurança entrarão em vigor.

*Endereço IP do servidor de origem***Telnet 443**

----Fim

Apontando tráfego para um balanceador de carga

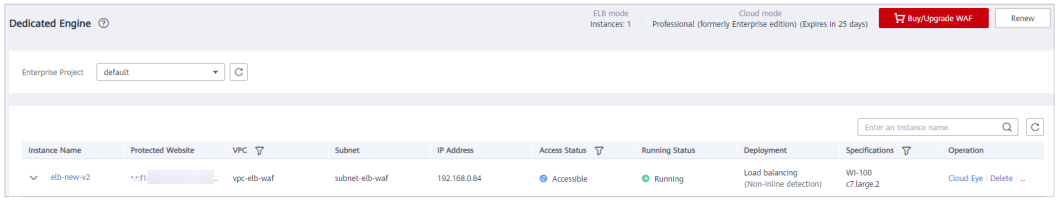
Se o seu servidor de origem usar o HUAWEI CLOUD ELB para distribuir o tráfego, execute as seguintes etapas para configurar uma política de controle de acesso para permitir que apenas os endereços de IP das instâncias WAF dedicadas acessem o servidor de origem:

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em ☰ no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 3 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

Figura 3-46 Lista de motores dedicada



Passo 4 Na coluna **Subnet IP Address**, obtenha o endereço de IP de cada instância dedicada do WAF na sua conta. **Figura 3-47** mostra um exemplo.

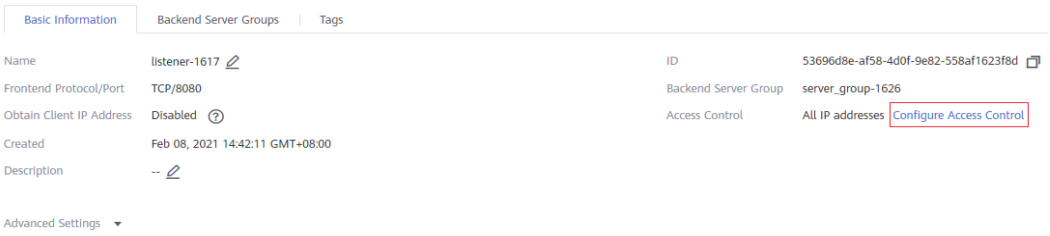
Figura 3-47 Endereço de IP de sub-rede de uma instância WAF dedicada

Passo 5 Clique em ☰ no canto superior esquerdo da página e escolha **Networking** > **Elastic Load Balance**.

Passo 6 Localize a linha que contém o balanceador de carga configurado para sua instância WAF dedicada e clique no nome do balanceador de carga na coluna **Name**.

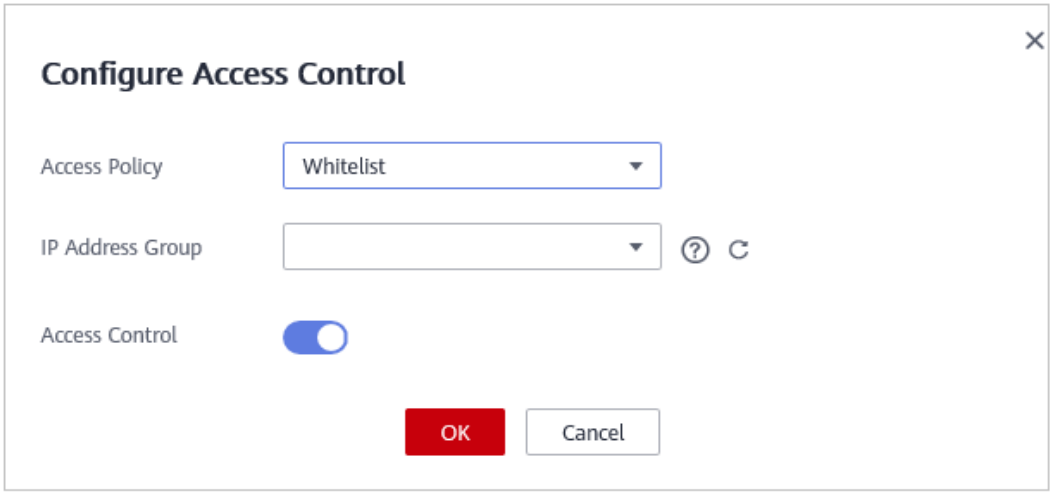
Passo 7 Na página de detalhes exibida, clique na guia **Listeners** e, em seguida, clique em **Configure Access Control**. **Figura 3-48** mostra um exemplo.

Figura 3-48 Configurando o Controle de Acesso



Passo 8 Na caixa de diálogo exibida, selecione **Whitelist** para **Access Policy**. Clique em **Create IP Address Group** e adicione os endereços de IP da instância de WAF obtidos no **Passo 4** a ele. Em seguida, selecione o grupo de endereços de IP criado para o **IP Address Group**. **Figura 3-49** mostra um exemplo.

Figura 3-49 Configurando o controle de acesso à lista branca



NOTA

Clique em **Create IP Address Group** e adicione os endereços de IP da instância dedicada do WAF ao grupo que está sendo criado.

Passo 9 Clique em **OK**.

Agora, a política de controle de acesso permite que todo o tráfego de entrada dos endereços de IP back-to-source de suas instâncias dedicadas do WAF.

Para verificar se a configuração entra em vigor, use a ferramenta Telnet para verificar se foi estabelecida uma conexão com a porta de serviço do servidor de origem vinculada ao endereço de IP protegido pelo WAF.

Por exemplo, execute o comando a seguir para verificar se a conexão com a porta de serviço de servidor de origem 443 vinculada ao endereço de IP protegido pelo WAF foi estabelecida. Se a conexão não puder ser estabelecida pela porta de serviço, mas o site ainda estiver acessível, as regras de entrada do grupo de segurança entrarão em vigor.

*Endereço IP do servidor de origem***Telnet 443**

----Fim

4 Gerenciamento de nomes de domínio do site

4.1 Exibição de informações básicas

Este tópico descreve como exibir o protocolo do cliente, o nome da política, a página de alarme, o registro CNAME e o endereço de IP CNAME configurado para um nome de domínio protegido.

NOTA

Se você tiver ativado projetos da empresa, poderá selecionar seu projeto da empresa na lista suspensa **Enterprise Project** e exibir os nomes de domínio no projeto.

Pré-requisitos

Um site foi conectado ao WAF.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Visualize as listas de sites protegidos. Para obter detalhes sobre os parâmetros, consulte **Tabela 4-1**.

NOTA

- Para alterar o modo de trabalho do WAF, na coluna **Mode**, clique em **Switch Mode** e selecione o modo de trabalho desejado.
- Para verificar o status da conexão de um site, na coluna **Access Status**, clique em  para atualizar o status.
- Para exibir os logs de proteção dos últimos três dias, na coluna **Protection Status over Past 3 Days**, clique em **View**.
- Para parar de proteger um site, na coluna **Operation**, clique em **Delete**.

Tabela 4-1 Descrição do parâmetro

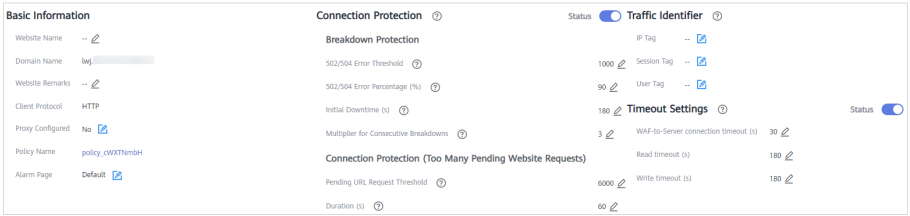
Parâmetro	Descrição
Site Protegido	O nome de domínio de um site a ser protegido.
Modo de implantação	Modo de implantação da instância do WAF configurada para seu site. As opções são **Cloud mode** e **Dedicated mode**.
modo	Modo WAF do nome de domínio protegido. Clique em **Switch** e selecione um dos seguintes modos de trabalho: ● **Enabled**: O WAF está habilitado. ● **Suspended**: O WAF está desativado. Se um grande número de solicitações normais for bloqueado, por exemplo, o código de status 418 for retornado com frequência, você poderá alternar o modo para **Suspended**. Nesse modo, seu site não está protegido porque o WAF apenas encaminha solicitações. Ele não faz varredura para ataques. Este modo é arriscado. É aconselhável usar regras lista branca de proteção global (anteriormente mascaramento de alarme falso) para reduzir alarmes falsos. ● **Contornado**: Nesse modo, as solicitações são enviadas diretamente aos servidores de back-end sem passar pelo WAF. **NOTA** O modo de trabalho pode ser alterado para **Bypassed** somente se o site protegido estiver implantado no **Cloud mode** e as seguintes condições forem atendidas: – Os serviços do site precisam ser restaurados para o status quando o domínio não está conectado ao WAF. – Você precisa investigar erros do site, como 502, 504 ou outros problemas de incompatibilidade. – Nenhum proxy é configurado entre o cliente e o WAF. Para mais detalhes, consulte **Alternação de modo de trabalho do WAF**.

Parâmetro	Descrição
Status de acesso	● **Inaccessible**: O site não está conectado ao WAF ou não pode se conectar ao WAF. ● **Accessible**: O site está conectado ao WAF. **AVISO** O **Access Status** inicial de um site implantado no **Dedicated Mode** é **Inaccessible**. Quando uma solicitação chega à sua instância do WAF para o site, o status de acesso muda automaticamente para **Accessible**.
Status de Proteção nos Últimos 3 Dias	Status de proteção do nome de domínio nos últimos 3 dias. Clique em **View** para exibir logs de proteção específicos.
Política	Configuração da política do nome de domínio. Clique em **Configure Policy** para configurar regras. Para mais detalhes, consulte **Configuração da regra**.
Operação	Para remover um site protegido do WAF, clique em **Delete**. **NOTA** ● Se você quiser remover um site protegido no **Cloud mode** da instância do WAF, acesse a plataforma DNS e traduza o nome de domínio para o endereço IP do servidor de origem antes de removê-lo. Caso contrário, o tráfego destinado ao nome de domínio não será direcionado para o servidor de origem. ● Demora cerca de um minuto para remover um site do WAF. Observe que a ação de exclusão não pode ser cancelada.

Passo 6 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Passo 7 Exiba as informações básicas sobre o nome de domínio do site protegido. **Figura 4-1** mostra um exemplo.

Figura 4-1 Informações básicas



- Obtenha informações sobre a instância do WAF: Clique em ao lado dos campos **CNAME** e **WAF IP Address Segment**.
- Obtenha **Subdomain Name** e **TXT Record**: Na linha **Access Status**, clique em **How to Access**. Na caixa de diálogo **Access Guide**, copie **Subdomain Name** e **TXT Record**.
- Atualize o certificado: Se você selecionar **HTTPS** para **Client Protocol**, será necessário um certificado SSL. Para atualizar o certificado, clique em ao lado do nome do

certificado na linha **Certificate Name**. Em seguida, na caixa de diálogo exibida, carregue um novo certificado ou selecione um certificado existente. Para mais detalhes, veja **Atualização de um certificado**.

- Atualize a versão TLS e o conjunto de cifras TLS para acessar o servidor de origem: Se você selecionar **HTTPS** para **Client Protocol**, poderá alterar a versão do TLS para uma mais segura. Para fazer isso, clique em ao lado do campo Configuração de TLS. Em seguida, na caixa de diálogo exibida, selecione a versão TLS desejada e o conjunto de cifras TLS. Para mais detalhes, veja **Configuração de verificação de certificação PCI DSS/3DS e a versão do TLS** .
- Modifique o campo de **Proxy Configured**: Clique em . Na caixa de diálogo exibida, selecione **Yes** se o servidor Web estiver usando um proxy.
- Personalizar a página de alarme: Clique em . Na caixa de diálogo exibida, selecione **Custom** ou **Redirection** e conclua as configurações necessárias. Por padrão, **Alarm Page** é **Default**.
- Se o seu site precisar de proteção IPv6, clique em . Na caixa de diálogo exibida, selecione **Enable**. Em seguida, o WAF atribui um endereço IPv6 ao nome de domínio. Para mais detalhes, consulte **Ativação de proteção WAF IPv6**.
- Se o seu site estiver acessível por HTTP/2, clique em na linha **HTTP/2 Used** e selecione **Yes**. Esse parâmetro é válido somente quando você seleciona **HTTPS** para **Client Protocol** para pelo menos um servidor de origem. Para mais detalhes, consulte **Ativação de protocolo HTTP/2**.
- Se você quiser definir uma duração de tempo limite para cada solicitação, ative **Timeout Settings** e clique em para especificar **WAF-to-Server Connection Timeout (s)**, **Read Timeout (s)**, e **Write Timeout (s)**. Esta função não pode ser desativada após ser ativada. Para mais detalhes, consulte **Configuração de tempo limite de conexão**.
- Para alterar o algoritmo de balanceamento de carga do site, clique em . Na caixa de diálogo exibida, selecione um algoritmo de balanceamento de carga e clique em **OK**. Para mais detalhes, consulte **Alternação de algoritmo de balanceamento de carga**.

----Fim

4.2 Alternação de modo de trabalho do WAF

Você pode alterar o modo de trabalho do WAF. O WAF pode funcionar no modo **Enabled**, **Suspended**, ou **Bypassed**.

NOTA

Se você tiver ativado projetos corporativos, certifique-se de ter todas as permissões de operação para o projeto em que a instância do WAF estiver localizada. Em seguida, você pode selecionar o projeto corporativo na lista suspensa **Enterprise Project** e alternar o modo de trabalho do WAF para um nome de domínio específico.

Pré-requisitos

O nome de domínio do site a ser protegido foi conectado ao WAF.

Cenários de aplicação

- **Enabled**: Nesse modo, o WAF defende seu site contra ataques com base em políticas configuradas.
- **Suspended**: Se um grande número de solicitações normais for bloqueado, por exemplo, o código de status 418 for retornado com frequência, você poderá alternar o modo para **Suspended**. Nesse modo, seu site não está protegido porque o WAF apenas encaminha solicitações. Ele não procura ou registra ataques. Esse modo é arriscado. É aconselhável usar lista branca de proteção global (anteriormente mascaramento de alarme falso) regras para reduzir alarmes falsos.
- **Bypassed**: As solicitações são enviadas diretamente aos servidores de origem de back-end sem passar pelo WAF. Antes de ativar esse modo, ative a porta de serviço dos servidores de origem para permitir que as solicitações sejam enviadas aos servidores de origem. Mude o modo para **Bypassed** somente se uma das seguintes condições for atendida:
  - Os serviços do site precisam ser restaurados para o status quando o site não está conectado ao WAF.
  - Você precisa investigar erros do site, como 502, 504 ou outros problemas de incompatibilidade.
  - Nenhum proxy é configurado entre o cliente e o WAF.

Impacto no sistema

No modo **Suspended**, seu site não está protegido porque o WAF encaminha apenas solicitações. Ele não faz varredura para ataques. Para evitar que solicitações normais sejam bloqueadas, configure lista branca de proteção global regras, em vez de usar o modo **Suspended**.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

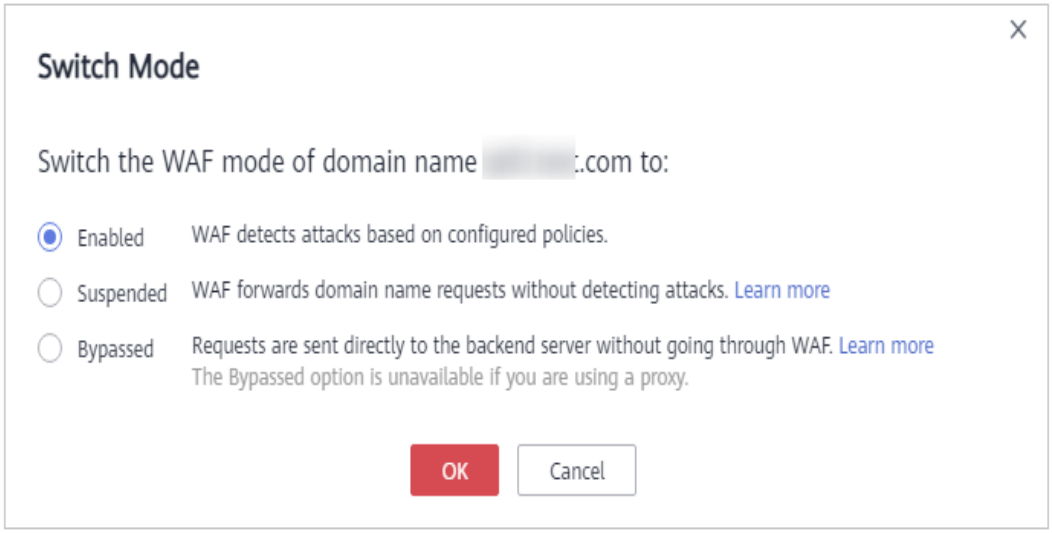
Passo 3 Clique em  no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na linha que contém o site de destino, clique em **Switch Mode** na coluna **Mode**.

Passo 6 Na caixa de diálogo **Switch Mode**, selecione um modo de trabalho e clique em **OK**.

Figura 4-2 Alternando o modo de trabalho do WAF



----Fim

4.3 Configuração de verificação de certificação PCI DSS/3DS e a versão do TLS

O TLS (Transport Layer Security) fornece confidencialidade e garante a integridade dos dados enviados entre aplicativos pela Internet. HTTPS é um protocolo de rede construído com base em TLS e HTTP e pode ser usado para transmissão criptografada e autenticação de identidade. Se você selecionar **Modo de Nuvem** ou **Modo dedicado** para implantação e definir **Client Protocol** como **HTTPS** , defina a versão mínima do TLS e o conjunto de cifras (um conjunto de vários algoritmos criptográficos) para o seu nome de domínio para bloquear solicitações que usam uma versão TLS anterior à configurada.

O TLS v1.0 e o conjunto de cifras 1 são configurados por padrão no WAF para segurança geral. Para proteger melhor seus sites, defina a versão mínima do TLS para uma versão posterior e selecione um conjunto de cifras mais seguro.

O WAF permite que você habilite as verificações de certificação PCI DSS e PCI 3DS. Depois que a verificação de certificação PCI DSS ou PCI 3DS é ativada, a versão mínima do TLS é definida automaticamente como TLS v1.2 para atender aos requisitos de certificação PCI DSS e PCI 3DS. O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) é um padrão de segurança da informação para organizações que lidam com cartões de crédito de marca dos principais esquemas de cartões. PCI 3-Domain Secure (PCI 3DS) é um padrão de segurança PCI Core.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto da empresa na lista suspensa **Enterprise Project** e configurar PCI DSS ou PCI 3DS e TLS para os nomes de domínio.

Pré-requisitos

- O modo de implantação da instância do WAF configurado para o seu site é **Cloud mode** ou **Dedicated mode**.

- Seu site usa HTTPS como o protocolo do cliente.

Restrições

- Se o **Client Protocol** para o site que você deseja proteger estiver definido como **HTTP**, o TLS não será necessário e você poderá ignorar este tópico.
- Atualmente, essa função não está disponível no CN North-Ulanqab1.

Cenários de aplicação

Por padrão, a versão mínima do TLS configurada para o WAF é o **TLS v1.0**. Para garantir a segurança do site, configure a versão TLS correta para seus requisitos de serviço. **Tabela 4-2** lista as versões mínimas recomendadas de TLS para diferentes cenários.

Tabela 4-2 Versões mínimas recomendadas de TLS

Cenário	Versão mínima do TLS (recomendado)	Efeito de proteção
Websites que lidam com dados críticos de negócios, como sites usados em bancos, finanças, valores mobiliários e comércio eletrônico.	TLS versão 1.2	O WAF bloqueia automaticamente as solicitações de acesso a sites que usam TLS v1.0 ou TLS v1.1.
Sites com requisitos básicos de segurança, por exemplo, sites de pequenas e médias empresas.	TLS v1.1	O WAF bloqueia automaticamente as solicitações de acesso a sites que usam o TLS v1.0.
Aplicações cliente sem requisitos especiais de segurança	TLS v1.0	Pedidos usando qualquer protocolo TLS podem acessar o site.

A suíte de cifras recomendada no WAF é **Cipher suite 1**. O Cipher Suite 1 oferece uma boa combinação de compatibilidade e segurança do navegador. Para obter detalhes sobre cada conjunto de cifras, consulte **Tabela 4-3**.

Tabela 4-3 Descrição de conjuntos de cifras

Nome da suíte de cifras	Algoritmos criptográficos suportados	Descrição
Conjunto de cifras padrão	● ECDHE-RSA-AES256-SHA384 ● AES256-SHA256 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !DH ● !EDH ● !AESGCM	● Compatibilidade: Boa. Uma ampla gama de navegadores são suportados. ● Segurança Média
Conjunto de cifras 1	● ECDHE-ECDSA-AES256-GCM-SHA384 ● HIGH ● !MEDIUM ● !LOW ● !aNULL ● !eNULL ● !DES ● !MD5 ● !PSK ● !kRSA ● !SRP ● !3DES ● !DSS ● !EXP ● !CAMELLIA ● @STRENGTH	Configuração recomendada. ● Compatibilidade: Boa. Uma ampla gama de navegadores são suportados. ● Segurança: Bom
Cipher suite 2	● EECDH+AESGCM ● EDH+AESGCM	● Compatibilidade: Média. Conformidade estrita com os requisitos de sigilo direto do PCI DSS e excelente proteção, mas os navegadores de versões anteriores podem não conseguir acessar o site. ● Segurança: Excelente

Nome da suíte de cifras	Algoritmos criptográficos suportados	Descrição
Cipher suite 3	● ECDHE-RSA-AES128-GCM-SHA256 ● ECDHE-RSA-AES256-GCM-SHA384 ● ECDHE-RSA-AES256-SHA384 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !DH ● !EDH	● Compatibilidade: Média. Versões anteriores de navegadores podem não conseguir acessar o site. ● Segurança: Excelente. Vários algoritmos, como ECDHE, DHE-GCM e RSA-AES-GCM, são suportados.
Cipher suite 4	● ECDHE-RSA-AES256-GCM-SHA384 ● ECDHE-RSA-AES128-GCM-SHA256 ● ECDHE-RSA-AES256-SHA384 ● AES256-SHA256 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !EDH	● Compatibilidade: Boa. Uma ampla gama de navegadores são suportados. ● Segurança: Média. O algoritmo GCM é suportado.

Os conjuntos de cifras TLS no WAF são compatíveis com todos os navegadores e clientes de versões posteriores, mas são incompatíveis com alguns navegadores de versões anteriores. **Tabela 4-4** lista os navegadores e clientes incompatíveis se o protocolo TLS v1.0 for usado.

AVISO

Recomenda-se que testes de compatibilidade sejam realizados no ambiente de serviço para garantir a estabilidade do serviço.

Tabela 4-4 Navegadores e clientes incompatíveis para conjuntos de cifras em TLS v1.0

Navegador/ Cliente	Padrão Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
Google Chrome 63 /macOS High Sierra 10.13.2	Não compatível	Compatível	Compatível	Compatível	Não compatível
Google Chrome 49/ Windows XP SP3	Não compatível	Não compatível	Não compatível	Não compatível	Não compatível
Internet Explorer 6 /Windows XP	Não compatível	Não compatível	Não compatível	Não compatível	Não compatível
Internet Explorer 8 /Windows XP	Não compatível	Não compatível	Não compatível	Não compatível	Não compatível
Safari 6/iOS 6.0.1	Compatível	Compatível	Não compatível	Compatível	Compatível
Safari 7/iOS 7.1	Compatível	Compatível	Não compatível	Compatível	Compatível
Safari 7/OS X 10.9	Compatível	Compatível	Não compatível	Compatível	Compatível
Safari 8/iOS 8.4	Compatível	Compatível	Não compatível	Compatível	Compatível
Safari 8/OS X 10.10	Compatível	Compatível	Não compatível	Compatível	Compatível
Internet Explorer 7/Windows Vista	Compatível	Compatível	Não compatível	Compatível	Compatível
Internet Explorer 8, 9 ou 10 /Windows 7	Compatível	Compatível	Não compatível	Compatível	Compatível
Internet Explorer 10 /Windows Phone 8.0	Compatível	Compatível	Não compatível	Compatível	Compatível
Java 7u25	Compatível	Compatível	Não compatível	Compatível	Compatível

Navegador/ Cliente	Padrão Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
OpenSSL 0.9.8y	Não compatível	Não compatível	Não compatível	Não compatível	Não compatível
Safari 5.1.9/OS X 10.6.8	Compatível	Compatível	Não compatível	Compatível	Compatível
Safari 6.0.4/OS X 10.8.4	Compatível	Compatível	Não compatível	Compatível	Compatível

Impacto no sistema

- Se você ativar a verificação de certificação PCI DSS:
  - A versão mínima do TLS e o conjunto de cifras são definidos automaticamente como **TLS v1.2** e **EECDH+AESGCM:EDH+AESGCM**, respectivamente, e não podem ser alterados.
  - Para alterar a versão mínima do TLS e o conjunto de cifras, desative a verificação.
- Se você ativar a verificação de certificação PCI 3DS:
  - A versão mínima do TLS é definida automaticamente como **TLS v1.2** e não pode ser alterada.
  - A verificação não pode ser desativada.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

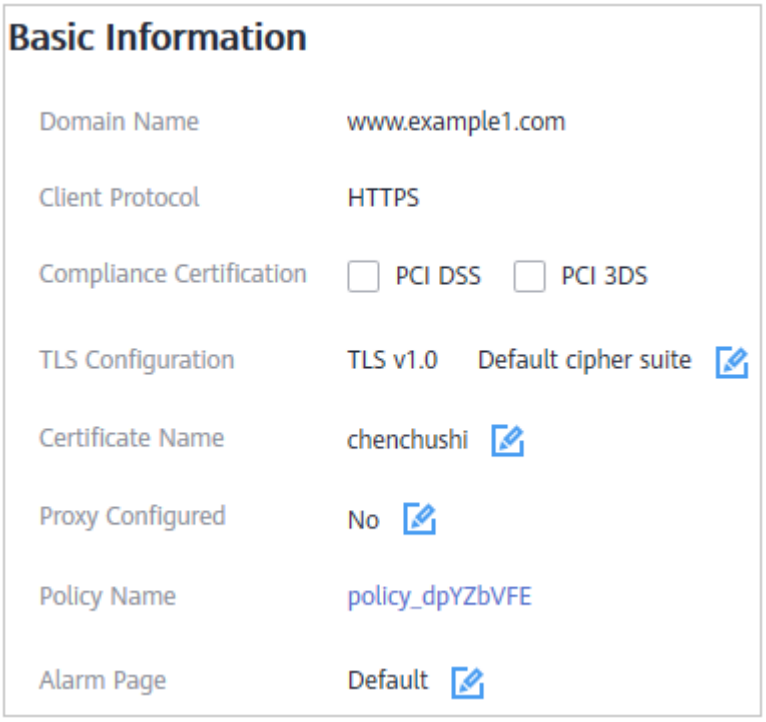
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

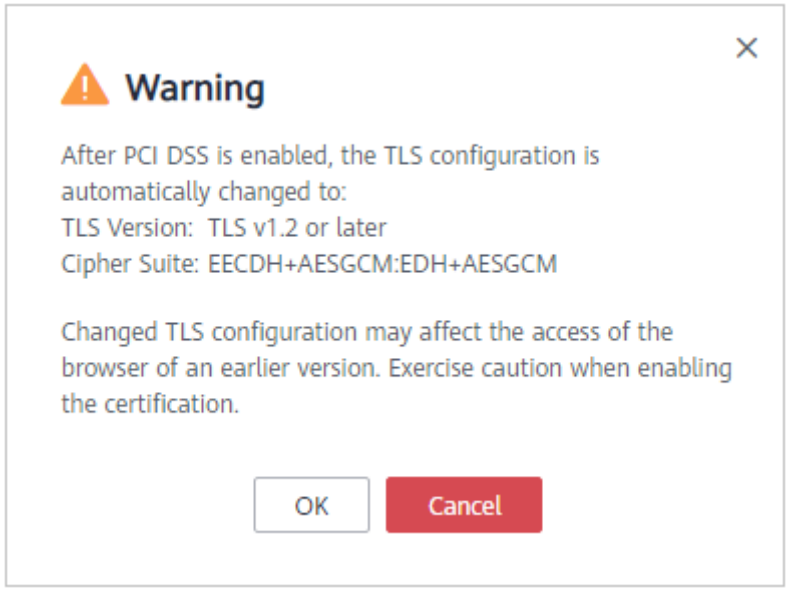
Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Passo 6 Na linha **Compliance Certification**, você pode selecionar **PCI DSS** e/ou **PCI 3DS** para permitir que o WAF verifique seu site quanto à conformidade de certificação PCI correspondente. Na linha **TLS Configuration**, clique em para concluir a configuração de TLS. **Figura 4-3** mostra um exemplo.

Figura 4-3 Modificação da configuração do TLS



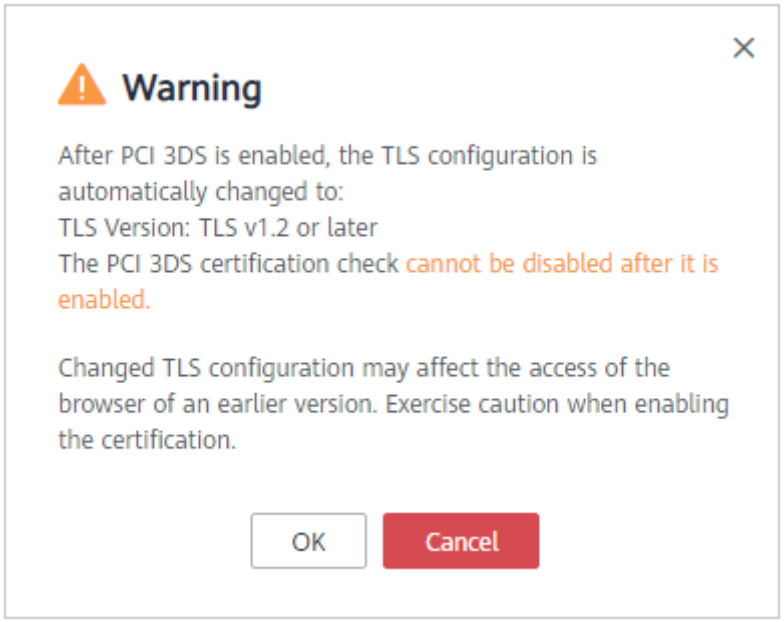
- Selecione **PCI DSS**. Na caixa de diálogo **Warning** exibida, clique em **OK** para habilitar a verificação de certificação PCI DSS.



AVISO

Se a verificação de certificação PCI DSS estiver ativada, a versão mínima do TLS e o conjunto de cifras não poderão ser alterados.

- Selecione **PCI 3DS**. Na caixa de diálogo **Warning** exibida, clique em **OK** para ativar a verificação de certificação PCI 3DS.

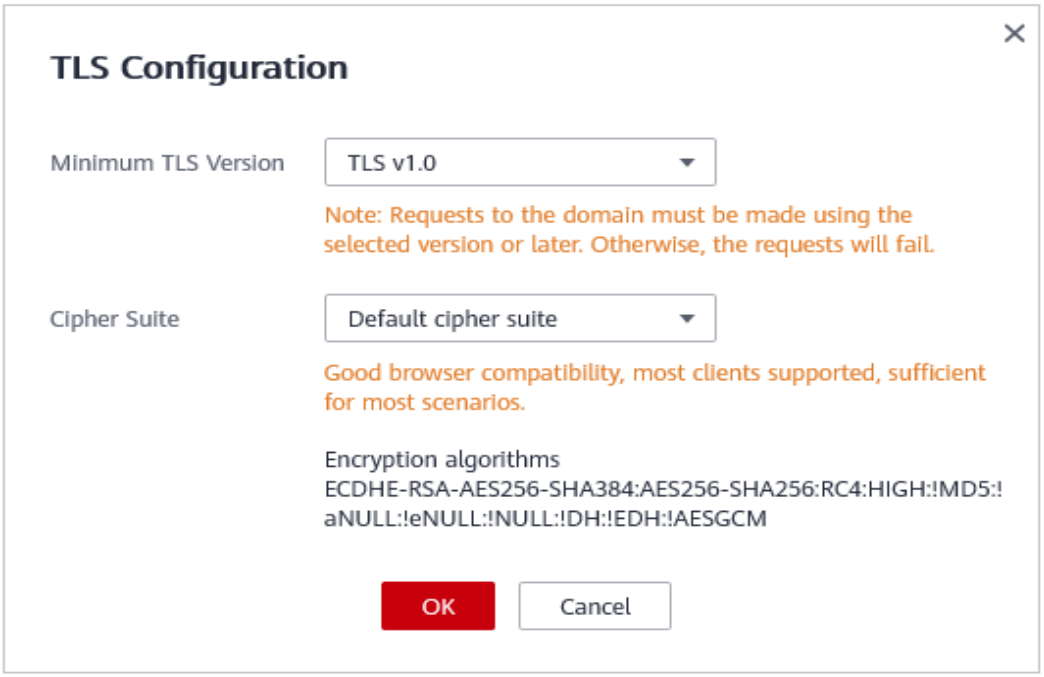


AVISO

- Se a verificação de certificação PCI 3DS estiver ativada, a versão mínima do TLS não poderá ser alterada.
- Uma vez ativada, a verificação de certificação PCI 3DS não pode ser desativada.

Passo 7 Na caixa de diálogo **Configuração de TLS** exibida, selecione a versão mínima de TLS e o conjunto de cifras. **Figura 4-4** mostra um exemplo.

Figura 4-4 Configuração de TLS



Selecione a versão mínima do TLS que você precisa. As opções são as seguintes:

- **TLS v1.0**: a versão padrão. As solicitações que usam o TLS v1.0 ou posterior podem acessar o nome de domínio.
- **TLS v1.1**: Somente solicitações usando TLS v1.1 ou posterior podem acessar o nome de domínio.
- **TLS v1.2**: Somente solicitações usando TLS v1.2 ou posterior podem acessar o nome de domínio.

Passo 8 Clique em **OK**.

----Fim

Verificação

Se **Minimum TLS Version** estiver definida como **TLS v1.2**, o site pode ser acessado por conexões protegidas pelo TLS v1.2 ou posterior, mas não pode ser acessado por conexões protegidas pelo TLS v1.1 ou anterior.

4.4 Ativação de proteção WAF IPv6

Se o seu site requer proteção IPv6, você pode ativar a proteção IPv6. Depois que a proteção IPv6 é ativada, o WAF atribui um endereço IPv6 ao nome de domínio e usa o endereço IPv6 para acessar o servidor de origem. O WAF adiciona a resolução de endereços IPv6 nos conjuntos de registros CNAME por padrão. As solicitações de acesso IPv6 são encaminhadas primeiro para o 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.

- Se o endereço do servidor de origem do site protegido for um endereço IPv6, a proteção IPv6 é ativada por padrão.
- Se o endereço do servidor de origem do site protegido estiver definido como um endereço IPv4, depois que você ativar manualmente a proteção IPv6, o WAF usará o mecanismo NAT64 para converter o site IPv4 em um site IPv6. Dessa forma, as solicitações para o endereço IPv6 são verificadas e roteadas pelo WAF para o servidor de origem. O NAT64 é um mecanismo de conversão de endereços de rede (NAT) que permite comunicações entre servidores IPv6 e IPv4.

Pré-requisitos

O site que você deseja proteger foi adicionado ao WAF.

Restrições

- Você selecionou **Cloud mode** para a implantação do seu site.
- Somente as edições Professional (antiga Enterprise Edition) e Platinum (antiga Premium Edition) podem proteger sites que usam endereços IPv6.
- A pilha dupla IPv4/IPv6 e o NAT64 são suportados apenas nas regiões da China Oriental e do Norte da China.
- Se o servidor de origem usar endereços IPv6, a proteção IPv6 será habilitada por padrão. Para evitar a interrupção do serviço IPv6, mantenha a proteção IPv6 ativada. Se a proteção IPv6 não for necessária, edite a configuração do servidor e exclua a

configuração IPv6 do servidor de origem primeiro. Para obter detalhes, consulte **Editando informações do servidor**.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

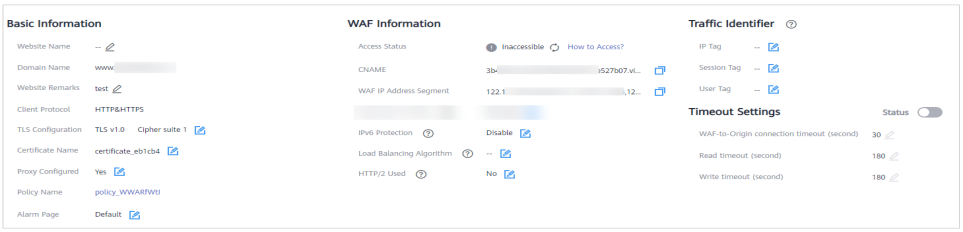
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Figura 4-5 Área de Informação Básica



Passo 6 Na linha **IPv6 Protection**, clique em . Na caixa de diálogo exibida, selecione **Enable** e clique em **OK**.

----Fim

4.5 Ativação de protocolo HTTP/2

Se seu site estiver acessível pelo protocolo HTTP/2, ative o HTTP/2 no WAF. O protocolo HTTP/2 pode ser usado apenas para acesso entre o cliente e o WAF com a condição de que pelo menos um servidor de origem tenha **HTTPS** usado para **Client Protocol**.

Pré-requisitos

- O site que você deseja proteger foi adicionado ao WAF.
- Você selecionou **HTTPS** para **Client Protocol** para pelo menos uma parte da configuração do servidor.

Restrições

- Você selecionou **Dedicated mode** para a implantação do seu site.
- Somente as edições Professional (antiga Enterprise Edition) e Platinum (antiga Premium Edition) podem proteger sites que são acessíveis através do protocolo HTTP/2.
- Atualmente, o HTTP/2 (HTTP2.0) pode ser ativado nas seguintes regiões:

- CN-Hong Kong
- AP-Bangkok

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

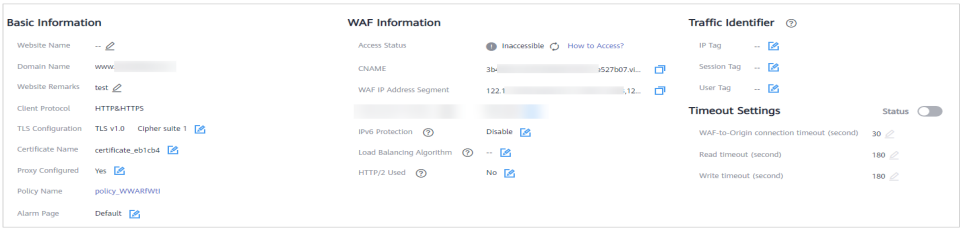
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Figura 4-6 Área de Informação Básica



Passo 6 Na linha **HTTP/2 Used**, clique em . Em seguida, selecione **Sim** e clique em **OK**.

----Fim

4.6 Configuração de tempo limite de conexão

Se você quiser definir uma duração de tempo limite para cada solicitação entre a instância do WAF e o servidor de origem, ative as **Timeout Settings** e especifique **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, e **Write timeout (s)**. Esta função não pode ser desativada depois de ativada.

NOTA

- 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.
- Para mais restrições, consulte **Restrições**.

Pré-requisitos

O site que você deseja proteger foi adicionado ao WAF.

Restrições

- O modo de implantação da instância do WAF configurado para o seu site é **Cloud mode** ou **Dedicated mode**.
- No **Cloud mode**, a duração do tempo limite da conexão pode ser modificada apenas na edição profissional (a antiga edição empresarial) e na edição platina (a antiga edição premium).
- A duração do tempo limite para conexões entre um navegador e o WAF não pode ser modificada. Somente a duração do tempo limite para conexões entre o WAF e o servidor de origem pode ser modificada.
- Esta função não pode ser desativada depois de ativada.
- Atualmente, o WAF suporta **Timeout Settings** nas seguintes regiões:
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapura

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

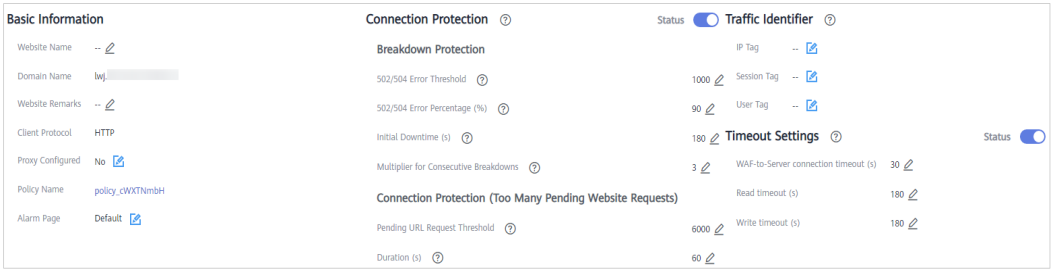
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para ir para a página de informações básicas.

Figura 4-7 Área de Informação Básica



Passo 6 Na linha **Timeout Settings**, clique na alternância **Status** e ative-a, se necessário.

Passo 7 Clique em , especifique **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, e **Write timeout (s)**, e clique em para salvar as configurações.

----Fim

4.7 Configuração de 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.

Pré-requisitos

- O site que você deseja proteger foi adicionado ao WAF.
- Você atualizou a instância dedicada do WAF para a versão mais recente. Para mais detalhes, consulte **Atualizando uma Instância Dedicada do WAF**.

Restrições

- Você selecionou **Dedicated mode** para a implantação do seu site.
- A **instância dedicada do WAF deve ser atualizada para a versão mais recente** antes de ativar a **Connection Protection**, ou as cargas de trabalho do site podem ser interrompidas.
- Atualmente, o WAF oferece suporte à **Connection Protection** de sites nas seguintes regiões:
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

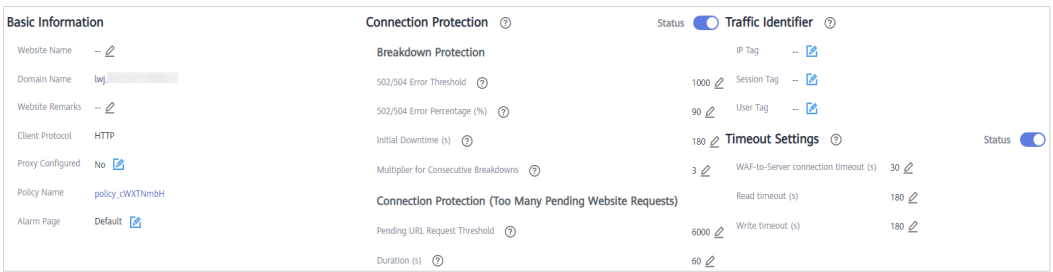
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para ir para a página de informações básicas.

Figura 4-8 Área de Informação Básica



Passo 6 Na área **Connection Protection**, clique na alternância de status para ativá-la.

Passo 7 Clique em ao lado de cada parâmetro, edite os parâmetros de **Breakdown Protection** e **Connection Protection** para atender aos seus requisitos e clique em para salvar as configurações. **Tabela 4-5** descreve os parâmetros.

Tabela 4-5 Parâmetros de proteção de conexão

Parâmetro		Descrição	Valor de exemplo
Proteção contra desagregação	Limite de erro 502/504	30s 502/504 Limiar de erro	1000
	Percentual de erro 502/504 (%)	Uma quebra é acionada quando o limite de erro 502/504 e o limite percentual são atingidos.	90
	Tempo de inatividade inicial (s)	Período de proteção após a primeira quebra. Durante esse período, o WAF deixa de encaminhar solicitações de clientes.	180
	Multiplicador para Repartições Consecutivas	O multiplicador máximo que você pode usar para quebras consecutivas. O número de avarias é contado a partir de 0 sempre que a duração da proteção contra avarias acumulada atinge 3.600s. Por exemplo, suponha que **Initial Downtime (s)** está definido como 180s e **Multiplier for Consecutive Breakdowns** está definido como 3. ● Se a avaria for acionada pela segunda vez, ou seja, menos de 3, a duração da proteção é de 360s (180s X 2). ● Se a avaria for acionada pelo terceiro ou quarto tempo, ou seja, igual ou superior a 3, a duração da proteção é de 540s (180s X 3). ● Quando a duração do tempo de inatividade acumulado excede 1 hora (3.600s), o número de avarias é contado a partir de 0.	3

Parâmetro		Descrição	Valor de exemplo
Proteção de conexão	Limite de solicitação de URL pendente	A Proteção de Conexão é acionada quando o número de solicitações de URL lidas atinge o limite que você configura.	6000
	Duração (s)	Duração da proteção. Durante esse período, o WAF deixa de encaminhar solicitações de clientes.	60

NOTA

O seguinte usa as configurações de **Connection Protection** em **Figura 4-8** como um exemplo para descrever como a proteção funciona.

- **Breakdown Protection**: Quando o número de erros 502/504 retornados pelo site protegido excede 1.000 e representa 90% ou mais do total de solicitações de acesso do site pela primeira vez, a primeira proteção é acionada. Durante a primeira proteção contra avarias, o WAF para de encaminhar solicitações de clientes para 180s . (ou seja, bloqueia o acesso dos visitantes ao site por 180s). Se uma segunda proteção contra avarias consecutiva for acionada, o WAF interrompe o encaminhamento de solicitações de clientes para 360s (180 X 2). Se uma terceira ou mais detalhamentos consecutivos forem acionados, o WAF interromperá o encaminhamento de solicitações de clientes para 540s (180s X 3). As quebras são contadas a partir de 0 quando a duração total do tempo de inatividade excede uma hora (3.600s).
- **Connection Protection**: Quando o número de solicitações de URL lidas na fila de espera excede 6.000, o WAF para de encaminhar solicitações do cliente por 60 segundos e retorna a página de manutenção do site aos visitantes.

----Fim

4.8 Alternação de algoritmo de balanceamento de carga

Se você configurar um ou mais endereços de servidor de origem, poderá usar um algoritmo de balanceamento de carga para distribuir o tráfego entre esses servidores de origem. O WAF suporta os seguintes algoritmos:

- **Origin server IP hash**: As solicitações do mesmo endereço IP são roteadas para o mesmo servidor de back-end.
- **Weighted round robin**: As solicitações são distribuídas pelos servidores de back-end, por sua vez, com base no peso atribuído a cada servidor.
- **Session hash**: Solicitações com a mesma tag de sessão são roteadas para o mesmo servidor de origem. Para ativar esse algoritmo, **configure identificadores de tráfego para fontes de ataque conhecidas**, ou o algoritmo de hash de sessão não pode ter efeito.

Pré-requisitos

O site que você deseja proteger foi adicionado ao WAF.

Restrições

- Você selecionou **Cloud mode** para a implantação do seu site.
- Somente as edições Professional (antiga Enterprise Edition) e Platinum (antiga Ultimate Edition) suportam algoritmos de balanceamento de carga.
- Atualmente, o WAF suporta algoritmos de balanceamento de carga nas seguintes regiões:
  - CN-Hong Kong
  - AP-Bangkok

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

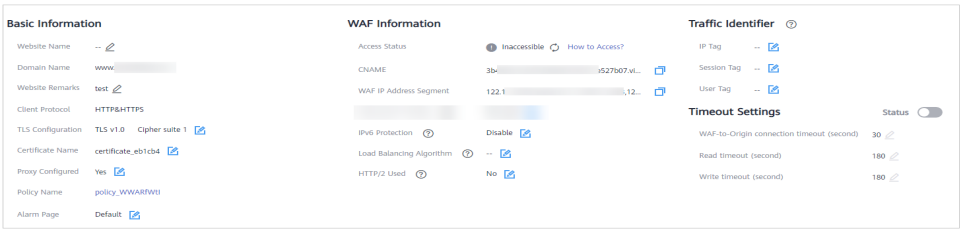
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Figura 4-9 Área de Informação Básica



Passo 6 No campo **Load Balancing Algorithm**, clique em . Na caixa de diálogo exibida, selecione um algoritmo de balanceamento de carga e clique em **OK**.

----Fim

4.9 Atualização de um certificado

Se você selecionar **Cloud mode** ou **Dedicated mode** para implantação de site e definir o **Client Protocol** como **HTTPS**, carregue um certificado para seu site nos seguintes cenários:

- Se o certificado do seu site estiver prestes a expirar, compre um novo certificado antes da data de expiração e atualize o certificado associado ao site no WAF.
- Se você planeja atualizar o certificado associado ao site, associe um novo certificado ao seu site no console do WAF.

NOTA

Se você ativou projetos corporativos, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto da empresa na lista suspensa **Enterprise Project** e atualizar certificados.

Pré-requisitos

- O modo de implantação da instância do WAF configurado para o seu site é **Cloud mode** ou **Dedicated mode**.
- Seu site usa HTTPS como o protocolo do cliente.

Restrições

- Cada nome de domínio deve ter um certificado associado. Um nome de domínio curinga só pode usar um certificado de domínio curinga. Se você tiver apenas certificados de domínio único, adicione nomes de domínio um a um no WAF.
- Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver em.pem, antes de carregá-lo, converta-o em.pem referindo-se a **Passo 6**.
- Antes de atualizar o certificado, verifique se a instância do WAF e o certificado que deseja carregar pertencem à mesma conta.
- O WAF não envia notificações se um certificado expirar, mas você pode exibir o tempo de expiração do certificado na página **Certificates**.

Impacto no sistema

- É recomendável que você atualize o certificado antes que ele expire. Caso contrário, todas as regras de proteção do WAF não entrarão em vigor, e pode haver impactos enormes no servidor de origem, ainda mais graves do que um host com falha ou falhas de acesso ao site.
- A atualização de certificados não afeta os serviços. O certificado antigo ainda funciona durante a substituição do certificado. O novo certificado assumirá o trabalho assim que tiver sido carregado e associado com sucesso ao nome de domínio.
- O acesso ao seu site pode ser afetado quando você atualizar as configurações de certificados usados para servidores de back-end ou para nomes de domínio de seus sites protegidos pelo WAF. Para minimizar esses impactos, atualize os certificados fora do horário de pico.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Passo 6 Clique em ao lado do nome do certificado. Na caixa de diálogo **Update Certificate**, importe um novo certificado ou selecione um certificado existente.

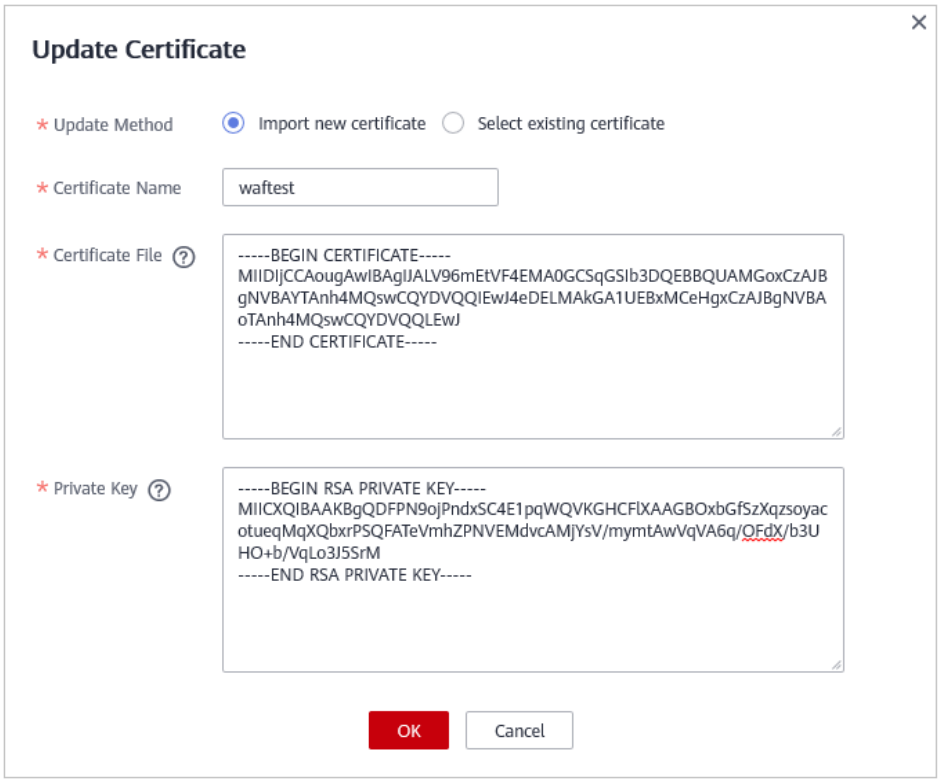
- Se você selecionar **Import new certificate** para **Update Method**, insira um nome de certificado e copie e cole o arquivo de certificado e a chave privada nas caixas de texto correspondentes. **Figura 4-10** mostra um exemplo.

  Os certificados recém-importados serão listados na página **Certificates**. Para mais detalhes, veja **Carregamento de um certificado**.

  NOTA

  O WAF criptografa e salva a chave privada para mantê-la segura.

Figura 4-10 Atualizando Certificado



Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver no formato.pem, converta-o localmente para.pem consultando **Tabela 4-6** antes de carregá-lo.

Tabela 4-6 Comandos de conversão de certificados

Formato	Método de conversão
CER/CRT	Renomeie o arquivo de certificado **cert.crt** para **cert.pem**.

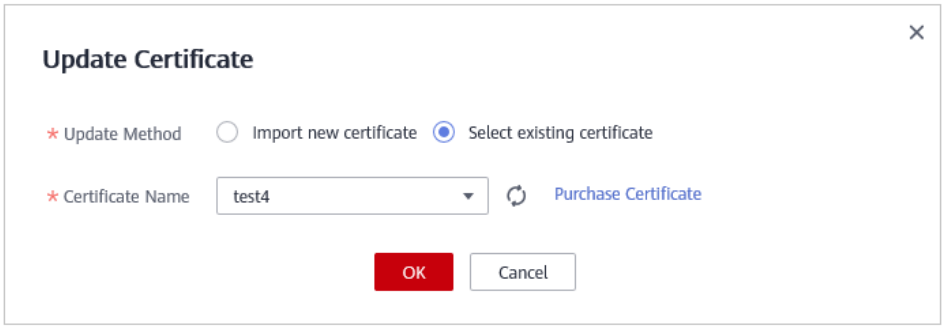
Formato	Método de conversão
PFX (em inglês)	– Obtenha uma chave privada. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** – Obter um certificado. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Converter um certificado. Por exemplo, execute o seguinte comando para converter **cert.p7b** em **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Renomeie o arquivo de certificado **cert.cer** para **cert.pem**.
DER	– Obtenha uma chave privada. Por exemplo, execute o seguinte comando para converter **privatekey.der** em **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** – Obter um certificado. Por exemplo, execute o seguinte comando para converter **cert.cer** em **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTA

- Antes de executar um comando OpenSSL, verifique se a ferramenta **OpenSSL** foi instalada no host local.
- Se seu PC local executa um sistema operacional Windows, vá para a interface de linha de comando (CLI) e execute o comando de conversão de certificados.

- Se você selecionar **Select existing certificate** para **Update Method**, selecione um certificado existente na lista suspensa **Certificate Name**.

Figura 4-11 Selecionando um certificado existente



NOTA

Se não houver certificados disponíveis, clique em **Purchase Certificate** e compre um certificado e envie-o para o WAF.

Passo 7 Clique em **OK**.

----Fim

Outras operações

Carregamento de um certificado

4.10 Configuração de um identificador de tráfego para uma origem de ataque conhecida

O WAF permite configurar identificadores de tráfego por endereço IP, sessão ou tag de usuário para bloquear solicitações possivelmente maliciosas de fontes de ataque conhecidas com base em **IP address**, **Cookie**, ou **Params**.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa de **Enterprise Project** e configurar identificadores de tráfego de origem de ataque conhecidos para os nomes de domínio.

Pré-requisitos

O site a ser protegido foi adicionado ao WAF.

Restrições

- Se a tag de endereço IP estiver configurada, certifique-se de que o site protegido tenha um proxy de camada 7 configurado na frente do WAF e que **Proxy Configured** esteja definido como **Yes** para o site protegido.

  Se a marca de endereço IP não estiver configurada, o WAF identificará o endereço IP do cliente por padrão.
- Antes de ativar as regras de origem de ataque conhecidas baseadas em cookies ou parâmetros, configure uma tag de sessão ou de usuário para o nome de domínio do site correspondente.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Passo 6 Na área **Traffic Identifier**, clique em ao lado de **IP Tag**, **Session Tag**, ou **User Tag** para configurar um identificador de tráfego referindo-se a **Tabela 4-7**. **Figura 4-12** mostra um exemplo.

Figura 4-12 Identificador de tráfego

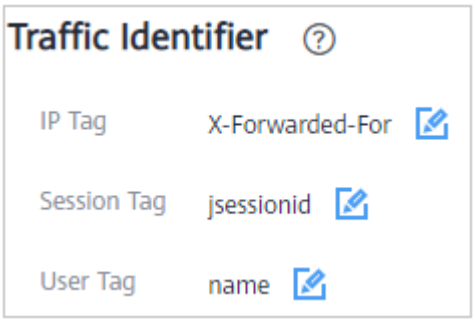


Tabela 4-7 Parâmetros do identificador de tráfego

Tag	Descrição	Valor de exemplo
Etiqueta IP	Campo do cabeçalho da solicitação HTTP do endereço IP original do cliente. Certifique-se de que o site protegido tenha um proxy de camada-7 configurado na frente do WAF e que o **Proxy Configured** nas configurações de informações básicas do site esteja definido como **Yes** para que esse parâmetro entre em vigor.	X-Encaminhado-Para
Tag da sessão	Essa tag é usada para bloquear solicitações possivelmente mal-intencionadas com base nos atributos de cookies de uma fonte de ataque. Configure esse parâmetro para bloquear solicitações com base em atributos de cookie.	jssessionid
Tag do usuário	Essa tag é usada para bloquear solicitações possivelmente mal-intencionadas com base no atributo Params de uma fonte de ataque. Configure esse parâmetro para bloquear solicitações com base nos atributos Params.	Nome

Passo 7 Clique em **OK** .

----Fim

Outras Operações

Configuração de uma regra de origem de ataque conhecido

4.11 Edição de informações do servidor

Depois de adicionar um site no **Cloud mode** ou no **dedicated mode**, você pode editar as informações do servidor do seu site.

Cenários aplicáveis:

- Edite as informações do servidor.
  - Modo de nuvem: Você pode modificar as configurações para **Client Protocol**, **Server Protocol**, **Server Address**, e **Server Port**.
  - Modo dedicado: Você pode modificar configurações para **Client Protocol**, **Server Protocol**, **Server Address**, **VPC**, e **Server Port**.
- Adicione configurações de servidor.
- Atualize um certificado referindo-se a **Atualização de um certificado**.

NOTA

Se você ativou projetos corporativos, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto da empresa na lista suspensa **Enterprise Project** e configurar as informações do servidor para os nomes de domínio.

Pré-requisitos

Um nome de domínio foi adicionado ao WAF. Você selecionou **Cloud mode** ou **Dedicated mode** para a implantação do site.

Impacto no sistema

Modificar a configuração do servidor não afeta os serviços.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Passo 6 Na área **Server Information**, clique em . **Figura 4-13** mostra um exemplo.

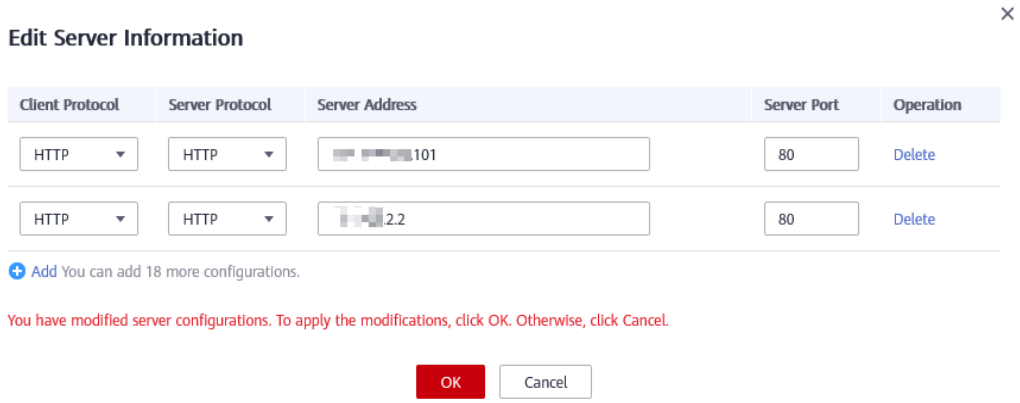
Figura 4-13 Informações do servidor

Passo 7 Na página **Edit Server Information**, edite as configurações do servidor (como o protocolo do cliente e o certificado associado). **Figura 4-14** mostra um exemplo.

NOTA

- Para obter detalhes sobre o certificado, consulte **Atualização de um certificado**.
- O WAF suporta a configuração de vários servidores de back-end. Para adicionar um servidor back-end, clique em **Add**.

Figura 4-14 Editar informações do servidor



Passo 8 Clique em **OK** .

----Fim

Verificação

Depois que as informações do servidor são modificadas, leva cerca de dois minutos para que a modificação entre em vigor.

4.12 Modificação de página de alarme

Se um visitante for bloqueado pelo WAF, a página de bloqueio **Default** do WAF será retornada por padrão. Você também pode configurar **Custom** ou **Redirection** para que a página de bloco seja retornada conforme necessário.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto da empresa na lista suspensa **Enterprise Project** e personalizar páginas de alarme para os nomes de domínio.

Pré-requisitos

Um site foi adicionado ao WAF.

Restrições

- O conteúdo das páginas text/html, text/xml e application/json pode ser configurado na página de bloco **Custom** a ser retornada.

- O nome de domínio raiz do endereço de redirecionamento deve ser o mesmo que o nome de domínio atualmente protegido (incluindo um nome de domínio curinga). Por exemplo, se o nome de domínio protegido for **www.example.com** e a porta for 8080, a URL de redirecionamento poderá ser definida como **http://www.example.com:8080/error.html**.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

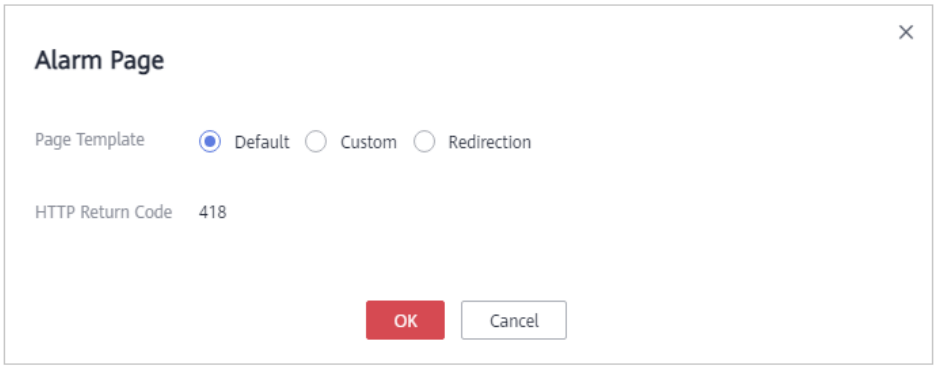
Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Protected Website**, clique no nome de domínio do site para acessar a página de informações básicas.

Passo 6 Clique em ao lado do nome do modelo de página na linha em que a **Alarm Page** está localizada. Na caixa de diálogo **Alarm Page** exibida, especifique **Page Template**.

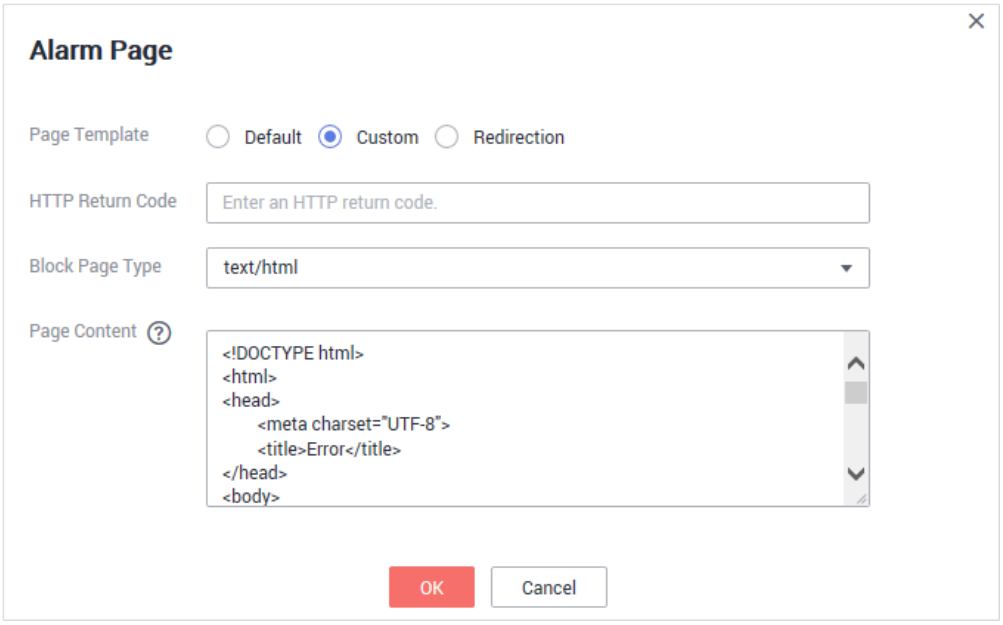
- Para usar a página interna, selecione **Default**. Um código HTTP 418 é retornado.

  Figura 4-15 Página de alarme padrão

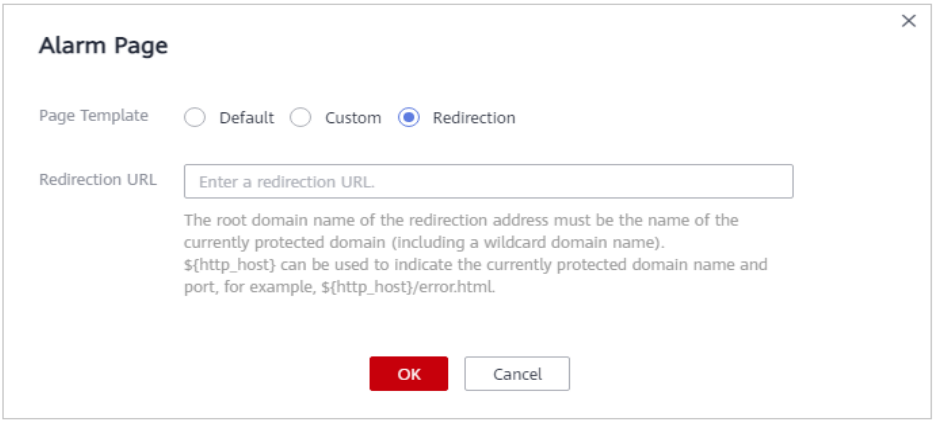
- Para personalizar a página de alarme, selecione **Custom** e configure os seguintes parâmetros. **Figura 4-16** mostra um exemplo.
  - **HTTP Return Code**: código de retorno configurado em uma página personalizada.
  - **Block Page Type**: As opções são **text/html**, **text/xml**, e **application/json**.
  - **Page Content**: Configure o conteúdo da página com base no valor selecionado para **Block Page Type**.

Figura 4-16 Página de alarme personalizada



- Para configurar um URL de redirecionamento, selecione **Redirection**.

Figura 4-17 Página de alarme de redirecionamento



O nome de domínio raiz do URL de redirecionamento deve ser o mesmo que o nome de domínio atualmente protegido (incluindo um nome de domínio curinga). Por exemplo, se o nome de domínio protegido for **www.example.com** e a porta for 8080, a URL de redirecionamento poderá ser definida como **http://www.example.com:8080/error.html**.

Passo 7 Clique em **OK**.

----Fim

4.13 Remoção de um site protegido do WAF

Este tópico descreve como remover um site do WAF se você não precisar mais protegê-lo.

NOTA

Se você ativou projetos corporativos, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar seu projeto corporativo na lista suspensa **Enterprise Project** e excluir nomes de domínio protegidos.

Pré-requisitos

Um nome de domínio de site foi adicionado ao WAF.

Impacto no sistema

- Se você quiser remover um site protegido no **Cloud mode** da instância do WAF, acesse a plataforma DNS e traduza o nome de domínio para o endereço IP do servidor de origem antes de removê-lo. Caso contrário, o tráfego destinado ao nome de domínio não será direcionado para o servidor de origem.
- Demora cerca de um minuto para remover um site do WAF. Observe que a ação de exclusão não pode ser cancelada.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

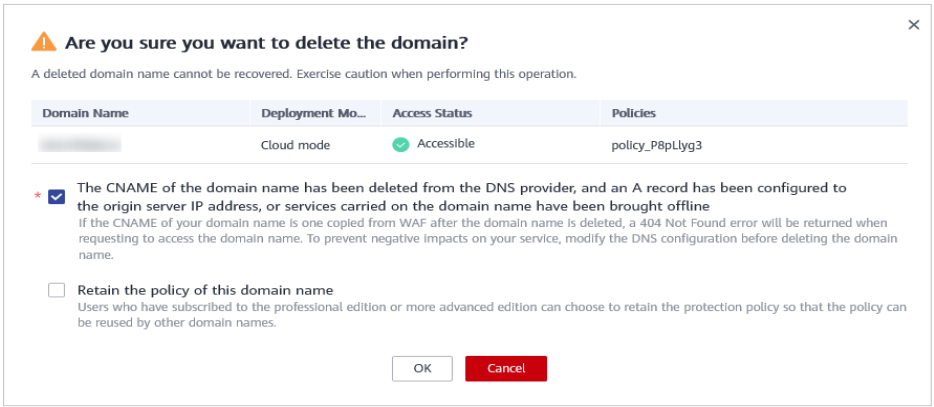
Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na linha que contém o nome de domínio do site que você deseja excluir, clique em **Delete** na coluna **Operation**.

Passo 6 Na caixa de diálogo de confirmação exibida, confirme a exclusão.

- Modo nuvem
  - Nenhum proxy usado

Figura 4-18 Excluindo um nome de domínio protegido (nenhum proxy usado)

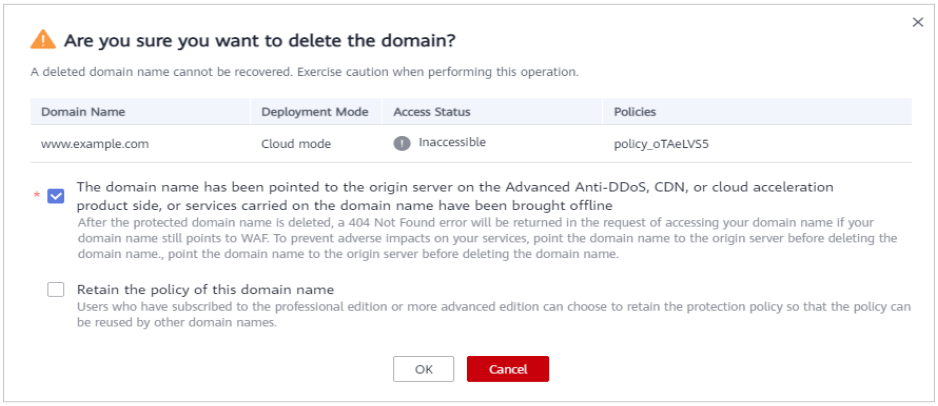


NOTA

- Verifique se as configurações relacionadas foram concluídas e selecione **The CNAME of the domain name has been deleted from the DNS provider, and an A record has been configured to the origin server IP address, or services carried on the domain name have been brought offline**.
- Se quiser manter a política vinculada ao nome de domínio, selecione **Retain the policy of this domain name**.

– Proxy usado

Figura 4-19 Exclusão de um nome de domínio protegido (proxy usado)



NOTA

- Certifique-se de que as configurações relacionadas sejam concluídas e selecione **The domain name has been pointed to the origin server on the Advanced Anti-DDoS, CDN, or cloud acceleration product side, or services carried on the domain name have been brought offline**.
- Se você quiser manter a política vinculada ao nome de domínio, selecione **Retain the policy of this domain name**.

- Modo dedicado

  Se quiser manter a política aplicada ao nome de domínio, selecione **Retain the policy of this domain name**.

Passo 7 Clique em **OK**.

Se **Nome de domínio excluído com sucesso** é exibido no canto superior direito, o nome de domínio do site foi excluído.

----Fim

5 Gerenciamento de certificado

5.1 Carregamento de um certificado

Se você selecionar **Cloud mode** ou **Dedicated mode** para implantação de site e definir **Client Protocol** como **HTTPS**, um certificado deverá ser associado ao site.

Você pode fazer upload de um certificado para o WAF. Em seguida, você pode selecionar diretamente o certificado carregado para o site protegido.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar seu projeto corporativo na lista suspensa **Enterprise Project** e carregar certificados no projeto.

Pré-requisitos

Você obteve o arquivo de certificado e a chave privada do certificado.

Limitações da especificação

Você pode carregar tantos certificados no WAF quanto o número de nomes de domínio que podem ser protegidos por suas instâncias do WAF na mesma conta. Por exemplo, se você comprar uma instância do WAF de edição padrão (antiga edição profissional), que pode proteger 10 nomes de domínio, e um pacote de expansão de nome de domínio, que pode proteger 20 nomes de domínio, sua instância do WAF pode proteger 30 nomes de domínio no total. Nesse caso, você pode fazer upload de 30 certificados.

Restrições

- Se você adquirir um certificado no console do SCM e enviá-lo por push para o WAF, o certificado será adicionado à lista de certificados na página **Certificates** no console do WAF. Este certificado também é contado para a sua quota total de certificados. Para obter detalhes sobre como enviar um certificado SSL no SCM para o WAF, consulte **Enviando um certificado SSL para outros serviços em nuvem**.

AVISO

Currently, certificates purchased in HUAWEI CLOUD SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used.

- Se você importar um novo certificado ao adicionar um site protegido ou atualizar um certificado, o certificado será adicionado à lista de certificados na página **Certificates** e o certificado importado também será contado na sua cota total de certificados.

Cenário de aplicação

Se você selecionar **HTTPS** para **Client Protocol**, será necessário um certificado.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

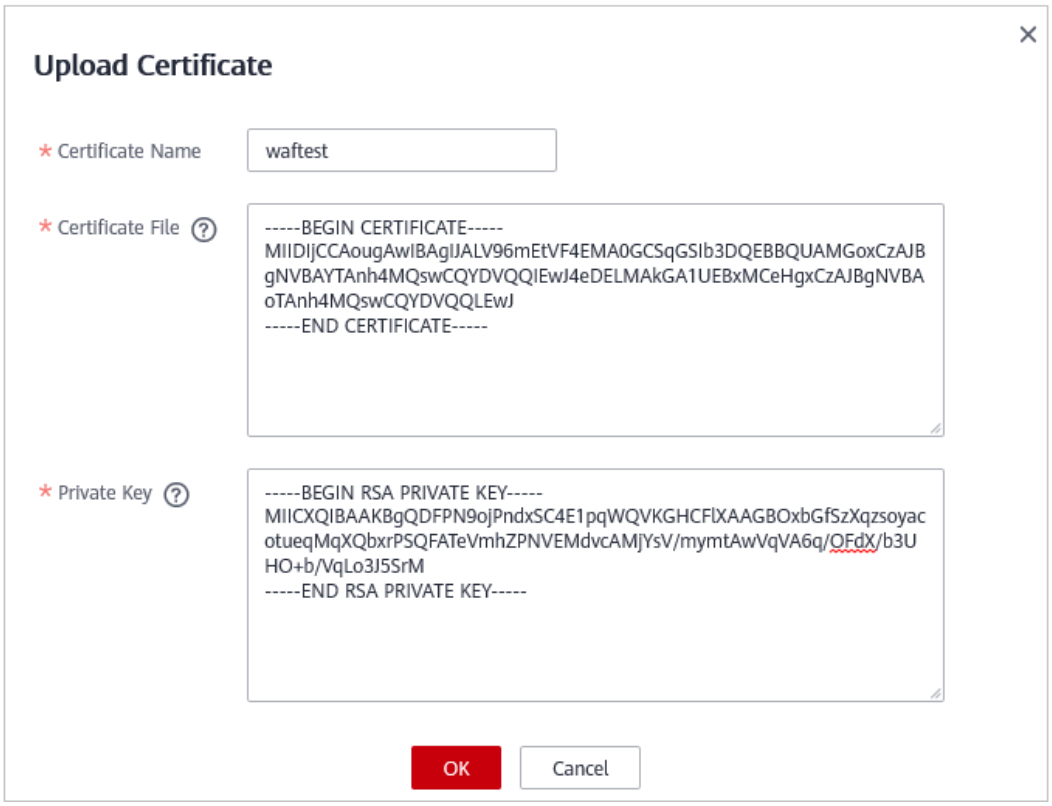
Passo 4 No painel de navegação, escolha **Objects** > **Certificates**.

Figura 5-1 Lista de certificados

Passo 5 Clique em **Upload Certificate**.

Passo 6 Na caixa de diálogo **Upload Certificate**, insira um nome de certificado e copie o arquivo de certificado e a chave privada nas caixas de texto correspondentes. **Figura 5-2** mostra um exemplo.

Figura 5-2 Carregar certificado



Somente certificados .pem podem ser usados no WAF. Se o certificado não estiver no formato.pem, converta-o localmente para.pem consultando **Tabela 5-1** antes de carregá-lo.

Tabela 5-1 Comandos de conversão de certificados

Formato	Método de conversão
CER/CRT	Renomeie o arquivo de certificado **cert.crt** para **cert.pem**.
PFX (em inglês)	● Obtenha uma chave privada. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** ● Obter um certificado. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Converter um certificado. Por exemplo, execute o seguinte comando para converter **cert.p7b** em **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Renomeie o arquivo de certificado **cert.cer** para **cert.pem**.

Formato	Método de conversão
DER	● Obtenha uma chave privada. Por exemplo, execute o seguinte comando para converter **privatekey.der** em **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** ● Obter um certificado. Por exemplo, execute o seguinte comando para converter **cert.cer** em **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTA

- Antes de executar um comando OpenSSL, verifique se a ferramenta **OpenSSL** foi instalada no host local.
- Se seu PC local executa um sistema operacional Windows, vá para a interface de linha de comando (CLI) e execute o comando de conversão de certificados.

Passo 7 Clique em **OK** .

----Fim

Verificação

O certificado criado é exibido na lista de certificados.

Outras Operações

- Para alterar o nome do certificado, mova o cursor sobre o nome do certificado, clique em , e digite um nome de certificado.

  AVISO

  Se o certificado estiver em uso, desvincule o certificado do nome de domínio primeiro. Caso contrário, o nome do certificado não pode ser alterado.

- Para exibir detalhes sobre um certificado, clique em **View** na coluna **Operation** do certificado.
- Na linha que contém o certificado desejado, clique em **Use** na coluna **Operation** para usar o certificado para o nome de domínio correspondente.
- Para excluir um certificado, localize a linha do certificado e clique em **Delete** na coluna **Operation**.

5.2 Vinculação de um certificado a um site protegido

Se você configurar o **Client Protocol** para **HTTPS** para o seu site, o site precisará de um certificado SSL. Este tópico descreve como vincular um certificado SSL que você carregou no WAF a um site.

> **NOTA**
>
> Se você tiver ativado projetos da empresa, poderá selecionar seu projeto da empresa na lista suspensa **Enterprise Project** e vincular certificados a sites no projeto.

Pré-requisitos

- Seu certificado ainda é válido.
- Seu site usa HTTPS como o protocolo do cliente.

Restrições

- Um certificado SSL pode ser usado para vários sites protegidos.
- Um site protegido pode usar apenas um certificado SSL.

Cenário de aplicação

Se você configurar o **Client Protocol** para **HTTPS**, será necessário um certificado.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

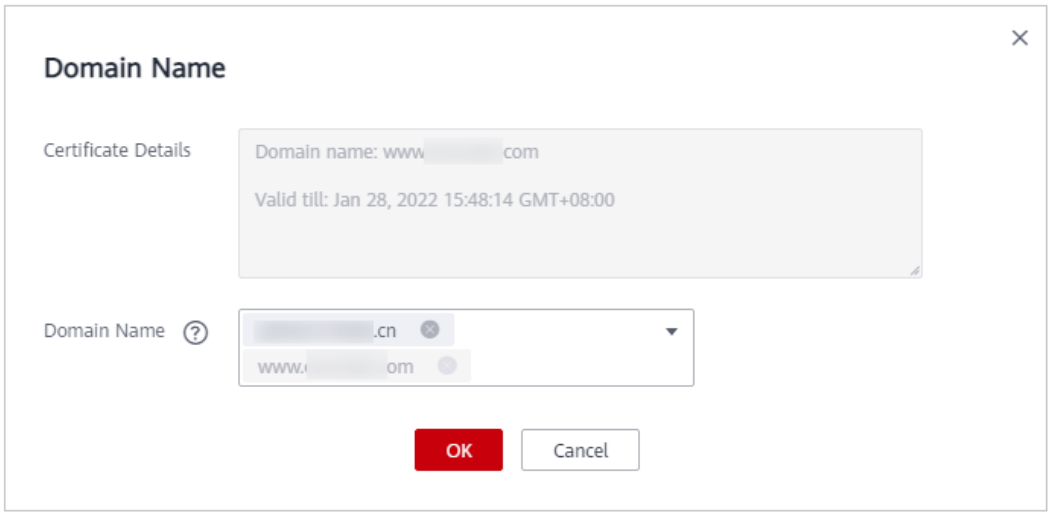
Passo 4 No painel de navegação, escolha **Objects** > **Certificates**.

Figura 5-3 Lista de certificados

Passo 5 Na linha que contém o certificado que você deseja usar, clique em **Use** na coluna **Operation**.

Passo 6 Na caixa de diálogo **Domain Name** exibida, selecione o site no qual deseja usar o certificado.

Figura 5-4 Caixa de diálogo Nome do Domínio



Passo 7 Clique em **OK**.

----Fim

Verificação

O site protegido é listado na coluna **Domain Name** do certificado.

Outras Operações

- Para alterar o nome do certificado, mova o cursor sobre o nome do certificado, clique em , e digite um nome de certificado.

  AVISO

  Se o certificado estiver em uso, desvincule o certificado do nome de domínio primeiro. Caso contrário, o nome do certificado não pode ser alterado.

- Para exibir detalhes sobre um certificado, clique em **View** na coluna **Operation** do certificado.
- Para excluir um certificado, localize a linha do certificado e clique em **Delete** na coluna **Operation**.

5.3 Apagar um certificado

Este tópico descreve como excluir um certificado expirado ou inválido.

NOTA

Se você ativou projetos corporativos, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e excluir um certificado.

Pré-requisitos

O certificado que você deseja excluir não está vinculado a um site protegido.

Restrições

Se um certificado a ser excluído estiver vinculado a um site, desvincule-o do site antes da exclusão.

Impacto no sistema

- A exclusão de certificados não afeta os serviços.
- Certificados excluídos não podem ser recuperados. Tenha cuidado ao realizar esta operação.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Objects** > **Certificates**.

Figura 5-5 Lista de certificados

Passo 5 Na linha que contém o certificado que você deseja excluir, clique em **Delete** na coluna **Operation**.

Passo 6 Na caixa de diálogo exibida, clique em **OK** .

----Fim

Outras Operações

Se um certificado a ser excluído estiver vinculado a um site, desvincule-o do site antes da exclusão.

Para desvincular um certificado de um nome de domínio de site, execute as seguintes etapas:

Passo 1 Na coluna **Domain Name** da linha que contém o certificado desejado, clique no nome do domínio para ir para a página de informações básicas.

Passo 2 Clique em ao lado do nome do certificado. Na caixa de diálogo exibida, carregue um novo certificado ou selecione um certificado existente.

----Fim

5.4 Exibição de informações do certificado

Este tópico descreve como exibir detalhes do certificado, incluindo o nome do certificado, o nome de domínio para o qual um certificado é usado e o tempo de expiração.

NOTA

Se você tiver ativado projetos da empresa, poderá selecionar seu projeto da empresa na lista suspensa **Enterprise Project** e exibir certificados no projeto.

Pré-requisitos

Você criou ou enviou um certificado para o WAF.

Restrições

- Para **certificados carregados no WAF**, o WAF não envia notificações de expiração para você.
- Para certificados enviados do CCM para o WAF, o período de validade do certificado pode ser exibido no WAF somente quando você ativa as notificações de expiração do certificado no CCM.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Objects** > **Certificates**.

Figura 5-6 Lista de certificados

Passo 5 Veja as informações do certificado. **Tabela 5-2** descreve os parâmetros.

Tabela 5-2 Descrição do parâmetro

Parâmetro	Descrição
Nome	Nome do certificado.
Nome do domínio	Os nomes de domínio protegidos pelo certificado Cada nome de domínio deve estar vinculado a um certificado. Um certificado pode ser usado para vários nomes de domínio.
Expirado	Tempo de expiração do certificado. Recomenda-se que você atualize o certificado antes que ele expire. Caso contrário, todas as regras de proteção do WAF não poderão entrar em vigor, e pode haver impactos maciços no servidor de origem, ainda mais graves do que um host com falha ou falhas de acesso ao site. Para mais detalhes, consulte **Atualização de um certificado**.

----Fim

Outras Operações

- Para alterar o nome do certificado, mova o cursor sobre o nome do certificado, clique em  , e digite um nome de certificado.

  AVISO

  Se o certificado estiver em uso, desvincule o certificado do nome de domínio primeiro. Caso contrário, o nome do certificado não pode ser alterado.

- Para exibir detalhes sobre um certificado, clique em **View** na coluna **Operation** do certificado.
- Na linha que contém o certificado desejado, clique em **Use** na coluna **Operation** para usar o certificado para o nome de domínio correspondente.
- Para excluir um certificado, localize a linha do certificado e clique em **Delete** na coluna **Operation**.

6 Gerenciamento de grupos de lista negra e lista branca de endereço de IP

6.1 Adição de um grupo de endereços de IP

Com grupos de endereços de IP, você pode adicionar rapidamente endereços de IP ou intervalos de endereços de IP a uma regra de lista negra ou de lista branca.

NOTA

Se você ativou projetos corporativos, poderá selecionar seu projeto corporativo na lista suspensa **Enterprise Project** e adicionar grupos de endereços de IP/intervalo no projeto.

Pré-requisitos

Você comprou o WAF.

Restrições

- Atualmente, o gerenciamento do grupo de endereços é suportado nas regiões CN-Hong Kong e AP-Bangkok.
- Não adicione o mesmo endereço de IP ou intervalo de endereços de IP a diferentes grupos de endereços de IP, ou os grupos de endereços de IP não serão criados.
- Se os balanceadores de carga ELB usados para as instâncias dedicadas ou de balanceamento de carga do WAF oferecerem suporte a endereços de IPv6, essas instâncias do WAF também poderão oferecer suporte a endereços de IPv6 ou intervalos de endereços de IPv6.

Limitações da especificação

- Um máximo de 50 grupos de endereços podem ser criados. Um máximo de 200 endereços IP ou intervalos de endereços de IP podem ser adicionados a um grupo de endereços. Use (,) de vírgulas para separar vários endereços de IP ou intervalos de endereços de IP. Não são permitidas quebras de linha.
- Antes de adicionar um grupo de endereços a uma regra de lista negra ou de lista branca, verifique se a cota de regra de lista negra e de lista branca de endereços de IP não foi usada.

NOTA

- Para mais detalhes, consulte **Configuração de uma regra de lista negra ou de lista branca de endereços IP**.

  Para obter detalhes sobre as especificações, consulte **Diferenças da edição**.
- Se a cota para as regras de lista branca e de lista negra de endereços de IP do seu WAF na nuvem não puder atender aos seus requisitos, você poderá comprar pacotes de expansão de regras na edição atual da instância do WAF ou atualizar sua edição da instância do WAF para aumentar essa cota. Um pacote de expansão de regras permite configurar até 10 regras de lista negra e lista branca de endereços de IP.

  Para obter detalhes, consulte **Atualizando a edição e especificações do Cloud WAF**

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

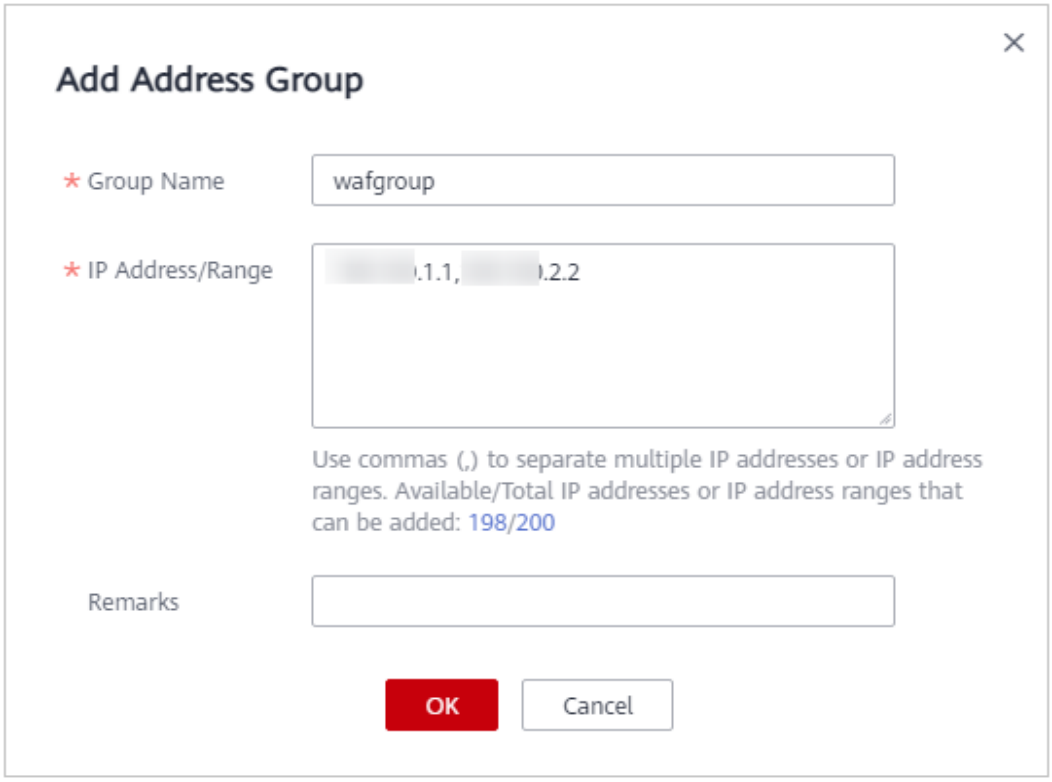
Passo 4 No painel de navegação à esquerda, escolha **Objects** > **Address Groups**.

Passo 5 Clique na guia **My Address Groups**.

Passo 6 No canto superior esquerdo da lista de grupos de endereços, clique em **Add Address Group**.

Passo 7 Na caixa de diálogo **Add Address Group** exibida, insira um nome de grupo de endereços e forneça intervalos de endereços de IP/IP. **Figura 6-1** mostra um exemplo.

Figura 6-1 Adicionar grupo de endereços



Passo 8 Clique em **OK**.

----Fim

6.2 Modificação ou exclusão de um grupo de endereços IP da lista negra ou da lista branca

Este tópico descreve como modificar ou excluir um grupo de endereços de IP.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e modificar ou excluir um grupo de endereços de IP.

Pré-requisitos

Você criou um grupo de endereços de IP.

Restrições

- Não adicione um endereço de IP ou intervalo de endereços de IP que tenha sido adicionado a um grupo de endereços de IP diferente ao grupo de endereços existente, ou o grupo de endereços de IP não será modificado.

- Somente grupos de endereços não usados por nenhuma regra podem ser excluídos. Antes de excluir um grupo de endereços que está sendo usado por uma regra de lista negra ou lista branca, remova o grupo de endereços da regra primeiro.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação à esquerda, escolha **Objects** > **Address Groups**.

Passo 5 Clique na guia **My Address Groups**.

Passo 6 Na lista de grupos de endereços, exiba as informações do grupo de endereços.

Tabela 6-1 Descrição do parâmetro

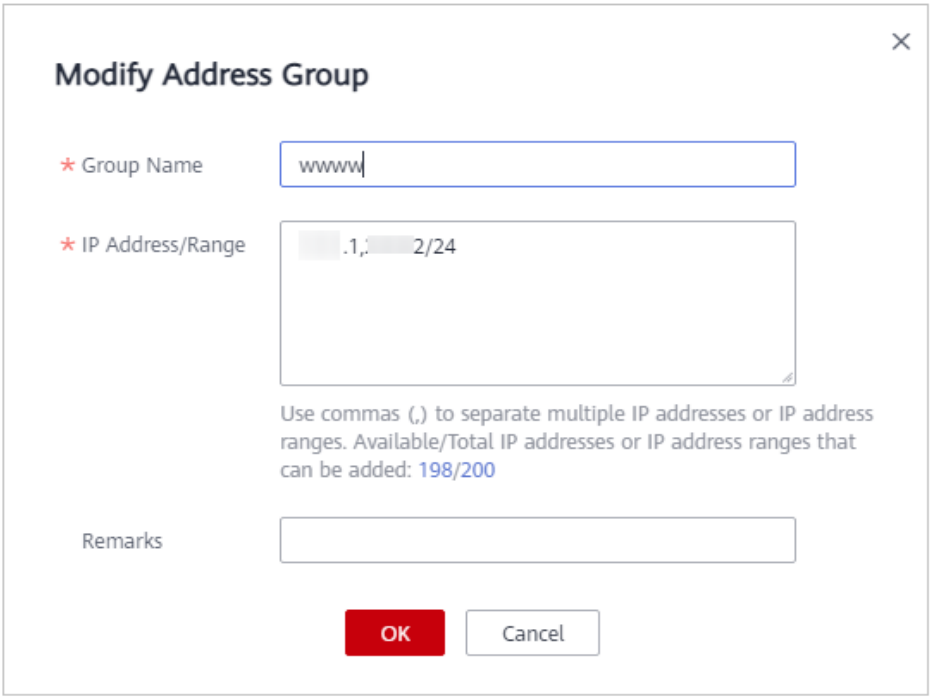
Parâmetro	Descrição
Nome de grupo	Nome do grupo de endereços que você configurou.
Endereço/ intervalo de IP	Endereços de IP ou intervalos de endereços de IP adicionados ao grupo de endereços.
Regra	Regras que estão usando o grupo de endereços.
Observações	Informações complementares sobre o grupo de endereços.

Passo 7 Modificar ou eliminar um grupo de endereços de IP.

- Modificar um grupo de endereços.

  Na linha que contém o grupo de endereços que você deseja modificar, clique em **Modify** na coluna **Operation**. Na caixa de diálogo **Modify Address Group**, altere o nome do grupo ou o intervalo de endereços de Ip/endereços de IP e clique em **OK**.

Figura 6-2 Modificar Grupo de Endereços



- Eliminar um grupo de endereços.

  Na linha que contém o grupo de endereços que você deseja excluir, clique em **Delete** na coluna **Operation**. Na caixa de diálogo exibida, clique em **OK**.

----Fim

7 Configuração da regra

7.1 Guia de configuração

Como funciona o motor WAF

As regras de proteção integradas do WAF ajudam você a se defender contra ataques comuns de aplicativos da Web, incluindo ataques XSS, injeção de SQL, rastreadores e web shells. Você pode personalizar as regras de proteção para permitir que o WAF proteja melhor seus serviços de site usando essas regras personalizadas. **Figura 7-1** mostra como funcionam as regras de proteção integradas do mecanismo WAF. **Figura 7-2** mostra a seqüência de detecção de regras definidas pelo usuário.

Figura 7-1 Processo de detecção de motor WAF

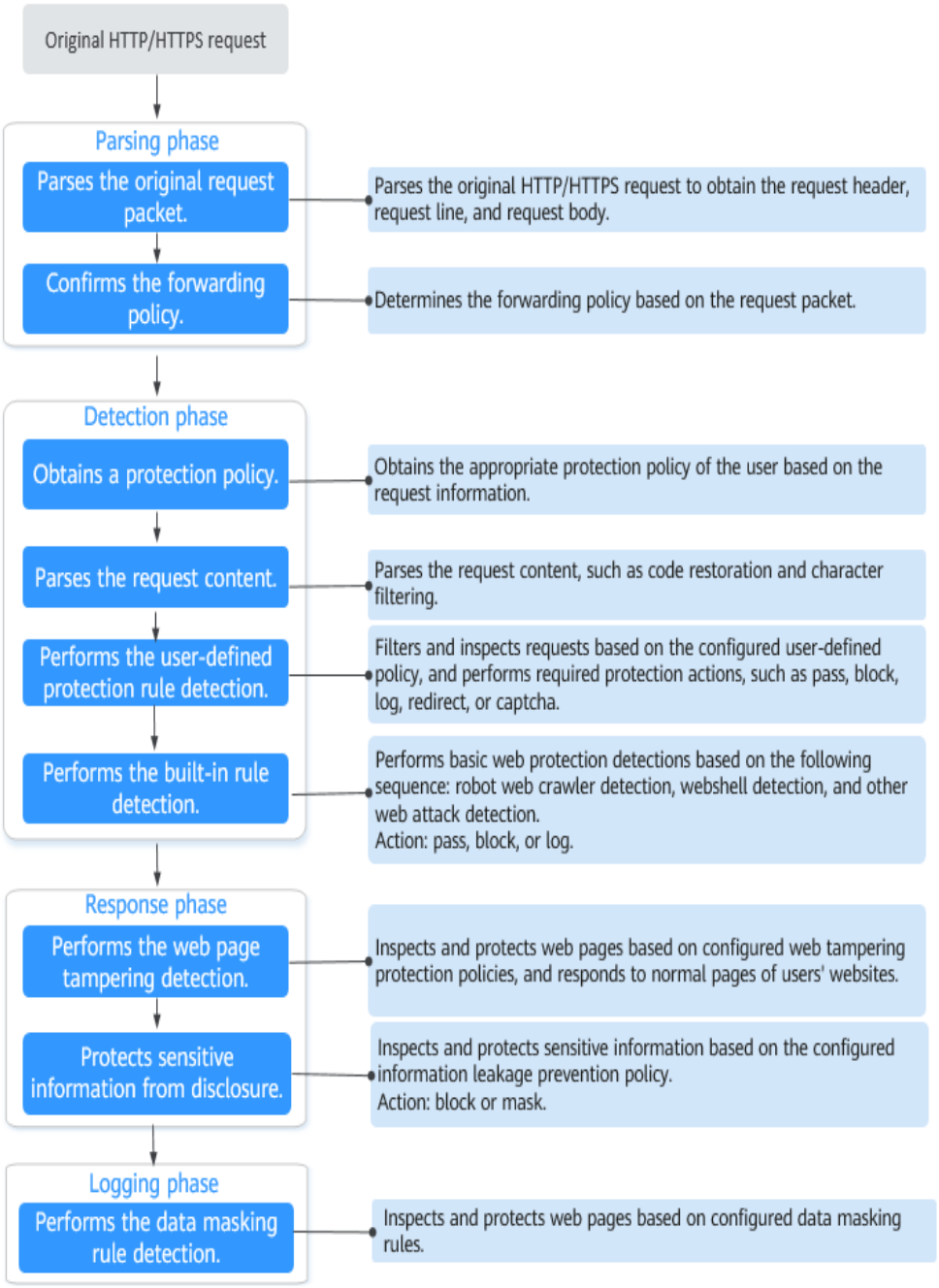
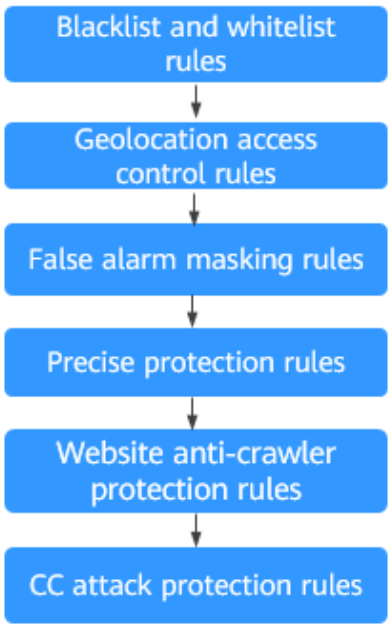


Figura 7-2 Prioridades das regras de proteção aduaneira



Ações de Resposta

- Pass: A solicitação atual é permitida incondicionalmente depois que uma regra de proteção é correspondida.
- Block: A solicitação atual é bloqueada após a correspondência de uma regra.
- CAPTCHA: O sistema realizará a verificação homem-máquina após a correspondência de uma regra.
- Redirect: O sistema notificará você para redirecionar a solicitação após a correspondência de uma regra.
- Log: Somente as informações de ataque são registradas após a correspondência de uma regra.
- Mask: O sistema anonimizará informações confidenciais após a correspondência de uma regra.

Métodos de configuração da regra de proteção

O WAF fornece os seguintes métodos de configuração personalizados para simplificar o processo de configuração. Selecione um método de configuração adequado para atender aos seus requisitos de serviço.

Método 1: Configurando regras de proteção para um único nome de domínio

Esse método é recomendado quando você tem poucos serviços de nome de domínio ou tem regras de configuração diferentes para serviços de nome de domínio.

NOTA

Depois que um nome de domínio é adicionado ao WAF, o WAF associa automaticamente uma política de proteção ao nome de domínio, e as regras de proteção configuradas para o nome de domínio também são adicionadas à política de proteção por padrão. Se houver nomes de domínio aplicáveis à política de proteção, você poderá adicioná-los diretamente à política. Para mais detalhes, consulte **Aplicação de uma política ao seu site**.

- Onde configurar
  a. No painel de navegação, escolha **Website Settings**.
  b. Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.
- Regras de proteção que você pode configurar na página de configuração de regras

Tabela 7-1 Regras de proteção configuráveis

Regra de proteção	Descrição	Referência
Regras básicas de proteção da Web	Com um extenso banco de dados de reputação, o WAF protege contra as 10 principais ameaças do Open Web Application Security Project (OWASP) e detecta e bloqueia ameaças, como scanners maliciosos, endereços de IP e web shells.	**Configuração de regras básicas de proteção de Web**
Regras de proteção contra ataque CC	As regras de proteção contra ataques da CC podem ser personalizadas para restringir o acesso a um URL específico em seu site com base em um endereço de IP exclusivo, cookie ou campo de referência, atenuando os ataques da CC.	**Configuração de uma regra de proteção contra ataques CC**
Regras de proteção precisa	Você pode personalizar regras de proteção combinando cabeçalhos HTTP, os URL, cookies, parâmetros de solicitação e endereços de IP do cliente.	**Configuração de uma regra de proteção precisa**
Regras da lista negra e da lista branca	Você pode configurar regras de lista negra e lista branca para bloquear, registrar somente ou permitir solicitações de acesso de endereços IP especificados.	**Configuração de uma regra de lista negra ou de lista branca de endereços IP**

Regra de proteção	Descrição	Referência
Regras de controle de acesso de geolocalização	Você pode personalizar essas regras para permitir ou bloquear solicitações de um país ou região específico.	**Configuração de uma regra de controle de acesso de geolocalização**
Regras de proteção contra adulteração da Web	Você pode configurar essas regras para evitar que uma página da Web estática seja adulterada.	**Configuração de uma regra de proteção contra adulteração da Web**
Proteção anti-crawler do Web site	Essa função analisa dinamicamente os modelos de serviços do site e identifica com precisão o comportamento do rastreador com base em sistemas de controle de risco de dados e identificação de bots, como o JS Challenge.	**Configuring Anti-Crawler Rules**
Regras de prevenção de fugas de informação	Você pode adicionar dois tipos de regras de prevenção de vazamento de informações. ● Filtragem de informações confidenciais: impede a divulgação de informações confidenciais (como números de identificação, números de telefone e endereços de e-mail). ● Interceptação de código de resposta: bloqueia os códigos de status HTTP especificados.	**Configuração de uma regra de prevenção de vazamento de informações**
Regras de lista branca de proteção global (anteriormente mascaramento de alarme falso)	Você pode configurar essas regras para permitir que o WAF ignore determinadas regras para solicitações específicas.	**Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule**
Regras de mascaramento de dados	Você pode configurar regras de mascaramento de dados para impedir que dados confidenciais, como senhas, sejam exibidos em logs de eventos.	**Configuração de uma regra de mascaramento de dados**

Método 2:Configurando regras de proteção para vários nomes de domínio

Esse método é recomendado se você tiver muitos serviços de nome de domínio e precisar da mesma política de proteção para vários nomes de domínio. Esse método reduz consideravelmente as cargas de trabalho de configuração repetidas e melhora a eficiência da proteção.

- Onde configurar

  No painel de navegação à esquerda, escolha **Policies**.

- Procedimento

  a. Adicione uma política. Para mais detalhes, consulte **Adição de uma política**.

  b. Configurar regras de proteção. Para mais detalhes, consulte **Adição de regras a uma ou mais políticas**.

  c. Lote adicionar vários nomes de domínio para a política. Para mais detalhes, consulte **Aplicação de uma política ao seu site**.

7.2 Configuração de regras básicas de proteção de Web

Depois que essa função é ativada, o WAF pode se defender contra ataques comuns da web, como injeções de SQL, XSS, vulnerabilidades de estouro remoto, inclusões de arquivos, vulnerabilidades de bash, execução de comandos remotos, passagem de diretório, acesso a arquivos sensíveis, e injeções de comando/código. Você também pode ativar outras verificações na proteção básica da Web, como detecção de shell da Web, inspeção profunda contra ataques de evasão e inspeção de cabeçalho.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

- A proteção básica da Web tem dois modos: **Block** e **Log only**.
- Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.
- Se você selecionar **Block** para o **Basic Web Protection**, poderá **configurar critérios de controle de acesso para uma fonte de ataque conhecida**. O WAF bloqueará solicitações correspondentes ao endereço IP configurado, cookie ou parâmetros por um período de tempo configurado como parte da regra.
- Atualmente, a inspeção profunda e a inspeção do encabeçamento são apoiadas em CN-Hong Kong e AP-Bangkok.
- Atualmente, a verificação de descriptografia Shiro é suportada em CN-Hong Kong.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração da **Basic Web Protection**, altere o **Status** e o **Mode** conforme necessário consultando a **Tabela 7-2**.

Figura 7-3 Área de configuração Basic Web Protection

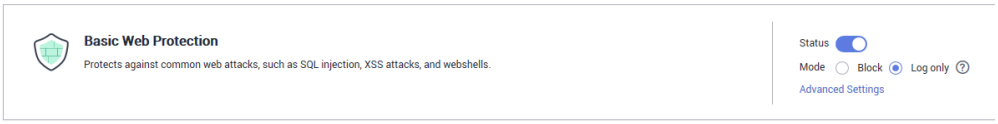


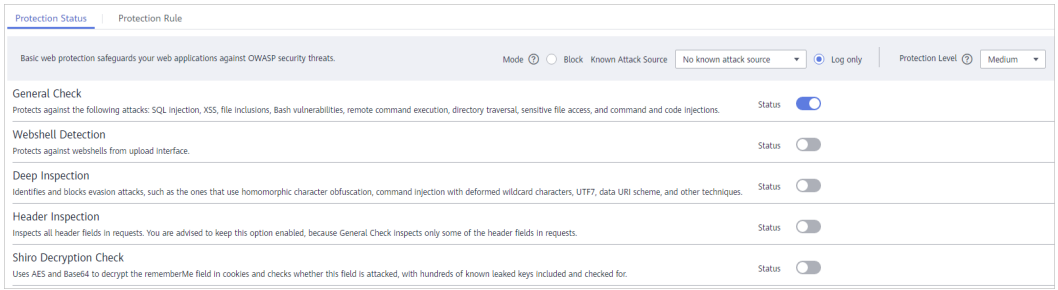
Tabela 7-2 Descrição do parâmetro

Parâmetro	Descrição
Status	Status da Proteção Básica da Web ● : ativado. ● : desativado.
modo	● **Block**: Bloqueios e logs do WAF detectaram ataques. ● **Log only**: O WAF registra apenas os ataques detectados.

Passo 7 Na área de configuração da **Basic Web Protection**, clique em **Advanced Settings**.

Passo 8 Clique na aba do **Protection Status**, e permita tipos da proteção um por um consultando **Tabela 7-4**. **Figura 7-4** mostra um exemplo.

Figura 7-4 Proteção Básica da Web



AVISO

Se você selecionar **Mode** para **Block** na guia **Protection Status**, poderá selecionar uma regra de origem de ataque conhecida para permitir que o WAF bloqueie solicitações de acordo. Para mais detalhes, consulte **Configuração de uma regra de origem de ataque conhecido**.

1. Defina o nível de proteção.

   Na parte superior da página, defina o **Protection Level** como **Low**, **Medium** ou **High**. O valor padrão é **Medium**.

   Tabela 7-3 Níveis de proteção

Nível de proteção	Descrição
Baixo	O WAF bloqueia apenas as solicitações com assinaturas de ataque óbvias. Se um grande número de alarmes falsos for relatado, recomenda-se **Low**.
Médio	O nível padrão é **Medium**, que atende à maioria dos requisitos de proteção da Web.
Alto	Nesse nível, o WAF oferece a melhor proteção granular e pode interceptar ataques com recursos complexos de desvio, como ataques cibernéticos Jolokia, detecção de vulnerabilidades de interface de gateway comum (CGI) e ataques de injeção Druid SQL. Recomendamos que você observe suas cargas de trabalho por um período de tempo antes de configurar uma regra de lista branca de proteção global e, em seguida, selecione **High** para que o WAF possa se defender contra mais ataques com efeito mínimo nas solicitações normais.

2. Defina o tipo de proteção.

   AVISO

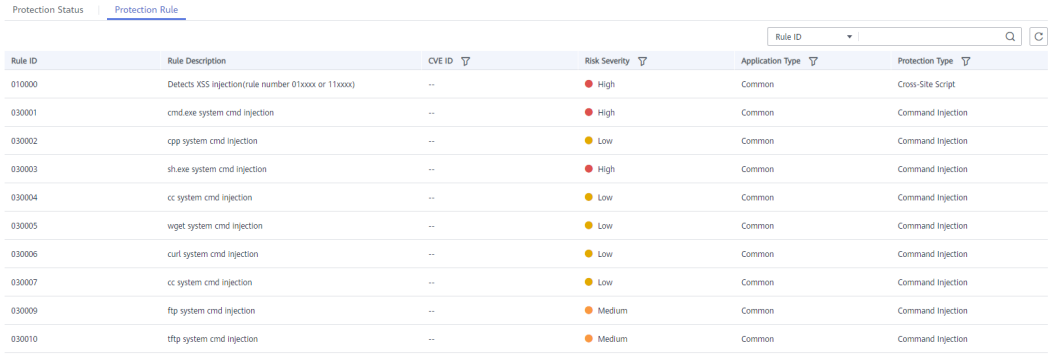
   Por predefinição, **General Check** está activada. Você pode ativar outros tipos de proteção referindo-se a **Tabela 7-4**.

Tabela 7-4 Tipos de proteção

Tipo	Descrição
Verificação geral	Defende contra ataques como injeções de SQL, XSS, vulnerabilidades de estouro remoto, inclusões de arquivos, vulnerabilidades Bash, execução de comandos remotos, passagem de diretórios, acesso a arquivos sensíveis e injeções de comando/código. Os ataques de injeção SQL são detectados principalmente com base na semântica. **NOTA** Se você ativar a **General Check**, o WAF verificará seus sites com base nas regras internas.
Detecção de Webshell	Protege contra shells da web da interface de upload. **NOTA** Se você ativar a **Webshell Detection**, o WAF detectará cavalos de Tróia de página da Web inseridos por meio da interface de upload.
Inspeção profunda	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. **NOTA** Se você ativar a **Deep Inspection**, o WAF detectará e defenderá ataques de evasão em profundidade.
Inspeção de cabeçalho	Esta função está desativada por padrão. Quando estiver desabilitado, a Verificação Geral verificará alguns dos campos de cabeçalho, como User-Agent, Content-type, Accept-Language e Cookie. **NOTA** Se você ativar essa função, o WAF verificará todos os campos de cabeçalho nas solicitações.
Verificação de descriptografia Shiro	Esta função está desativada por padrão. Depois que essa função é ativada, o WAF usa AES e Base64 para descriptografar o campo RememberMe no cookies e verifica se esse campo é atacado. Existem centenas de chaves vazadas conhecidas incluídas e verificadas.

Passo 9 Clique na guia **Protection Rules** para exibir os detalhes. **Figura 7-5** mostra um exemplo. Para obter mais detalhes sobre os parâmetros, consulte **Tabela 7-5**.

Figura 7-5 Exibindo regras de proteção



NOTA

Clique em para pesquisar uma regra por **CVE ID**, **Risk Severity**, **Application Type**, ou **Protection Type**.

Tabela 7-5 Regras de proteção

Parâmetro	Descrição
ID da regra	A ID da regra de proteção, que é gerada automaticamente.
Descrição da regra	Detalhes dos ataques para os quais a regra de proteção está configurada.
ID da CVE	ID CVE (Common Vulnerabilities & Exposures), que corresponde à regra de proteção. Para vulnerabilidades não-CVE, um traço duplo (--) é exibido.
Gravidade do risco	A gravidade da vulnerabilidade, incluindo: ● Alto ● Médio ● Baixo
Tipo de aplicativo	O tipo de aplicativo para o qual a regra de proteção é usada. Para obter detalhes sobre os tipos de aplicativos que o WAF pode proteger, consulte **Tabela 7-6**.
Tipo de proteção	O tipo da regra de proteção. O WAF pode descobrir injeção SQL, injeção de comandos, ataques XSS, injeção de entidade externa XML (XXE), injeção de linguagem de expressão (EL), CSRF, SSRF, inclusão de arquivos locais, inclusão de arquivos remotos, trojans de sites, rastreadores maliciosos, ataques de fixação de sessão, vulnerabilidades de desserialização, execução de comandos remotos, vazamento de informações, ataques DoS, vazamento de código-fonte / dados.

Tabela 7-6 Tipos de aplicativos que o WAF pode proteger

4images	Dragon-Fire IDS	Log4j2	ProjectButler
A1Stats	Drunken Golem GP	Loggix	Pulse Secure
Achievo	Drupal	lpswitch IMail	Quest CAPTCHA
Acidcat CMS	DS3	Lussumo Vanilla	QuickTime Streaming Server
Activist Mobilization Platform	Dubbo	MAGMI	R2 Newsletter
AdaptBB	DynPG CMS	ManageEngine ADSelfService Plus	Radware AppWall
Adobe	DZCP basePath	MassMirror Uploader	Rezervi root
Advanced Comment System	ea-gBook inc ordner	Mavili	Ruby
agendax	EasyBoard	MAXcms	RunCMS
Agora	EasySiteEdit	ME Download System	Sahana-Agasti
AIOCP	e-cology	Mevin	SaurusCMS CE
AjaxFile	E-Commerce	Microsoft Exchange Server	School Data Navigator
AJSquare	Elvin	Moa Gallery MOA	Seagull
Alabanza	Elxis-CMS	Mobius	SGI IRIX
Alfresco Community Edition	EmpireCMS	Moodle	SilverStripe
AllClubCMS	EmuMail	Movabletype	SiteEngine
Allwebmenus Wordpress	eoCMS	Multi-lingual E-Commerce	Sitepark
Apache	E-Office	Multiple PHP	Snipe Gallery
Apache APISIX Dashboard	EVA cms	mxCamArchive	SocialEngine
Apache Commons	eXtropia	Nakid CMS	SolarWinds
Apache Druid	EZPX Photoblog	NaviCOPA Web Server	SQuery

Apache Dubbo	F5 TMUI	NC	Squid
Apache Shiro	Faces	NDS iMonitor	StatCounteX
Apache Struts	FAQEngine	Neocrome Seditio	Subdreamer-CMS
Apache Tomcat	FASTJSON or JACKSON	NetIQ Access Manager	Sumsung IOT
Apache-HTTPD	FCKeditor	Netwin	Sun NetDynamics
Apple QuickTime	FileSeek	Nginx	SuSE Linux Sdbsearch
ardeaCore	fipsCMSLight	Nodesforum	SweetRice-2
AROUNDMe	fipsForum	Nucleus Plugin Gallery	Tatantella
Aurora Content Management	Free PHP VX Guestbook	Nucleus Plugin Twitter	Thecartpress Wordpress
AWCM final	FreeSchool	Nukebrowser	Thinkphp
AWStats	FreshScripts	NukeHall	ThinkPHP5 RCE
Baby Gekko	FSphp	Nullsoft	Tiki Wiki
BAROSmini Multiple	FusionAuth	Ocean12 FAQ Manager	Tomcat
Barracuda Spam	Gallo	OCPortal CMS	Trend Micro
BizDB	GetSimple	Open Education	Trend Micro Virus Buster
Blackboard	GetSimple CMS	OpenMairie openAnnuaire	Tribal Tribiq CMS
BLNews	GLPI	OpenPro	TYPO3 Extension
Caldera	GoAdmin	openUrgence Vaccin	Uebimiau
Cedric	Gossamer Threads DBMan	ORACLE Application Server	Uiga Proxy
Ciamos CMS	Grayscalecms	Oramon	Ultrize TimeSheet
ClearSite Beta	Hadoop	OSCommerce	VehicleManager
ClodFusion Tags	Haudenschilt Family	PALS	Visitor Logger
CMS S Builder	Havalite	Pecio CMS	VMware
ColdFusion	HIS Auktion	PeopleSoft	VoteBox

ColdFusion Tags	HP OpenView Network Node Manager	Persism Content Management	WayBoard
Commvault CommCell CVSearchService	HPInsightDiagnostics	PhotoGal	WebBBS
Concrete5	Huawei D100	PHP Ads	WebCalendar
Confluence Server and Data Center	HUBScript	PHP Classifieds	WEB-CGI
Coremail	IIS	PHP CMS	WebFileExplorer
Cosmicperl Directory Pro	iJoomla Magazine	PHP Paid 4 Mail Script	WebGlimpse
CPCommerce	ILIAS	PHPAddressBook	webLogic
DataLife Engine	Indexu	PHP-Calendar	WebLogic Server wls9-async
DCScripts	IRIX	phpCow	Webmin
DDL CMS	JasonHines PHPWebLog	PHPGenealogy	WEB-PHP Invision Board
DELL TrueMobile	JBOSS	PHPGroupWare	WebRCSdiff
Digitaldesign CMS	JBossSeam	phpMyAdmin	Websense
Dir2web	Joomla	phpMyAdmin Plugin	WebSphere
Direct News	JRE	PHPMyGallery	WikyBlog WBmap
Discourse	jsfuck	PHPNews	WordPress
Diskos CMS Manager	justVisual	Pie Web Masher	WORK system
DiY-CMS	Katalog Stron Hurricane	PlaySMS	Wpeasystats Wordpress
D-Link	KingCMS	Plogger	XOOPS
DMXReady Registration Manager	koesubmit	Plone	Xstream
DoceboLMS	Kontakt Formular	PointComma	YABB SE
Dokuwiki	KR-Web	Postgres	YP Portal MS-Pro Surumu
dompdf	Landray	PrestaShop	ZenTao

DotNetNuke	Livesig Wordpress	ProdLer	Zingiri Web Shop Wordpress
ZOHO ManageEngine	-	-	-

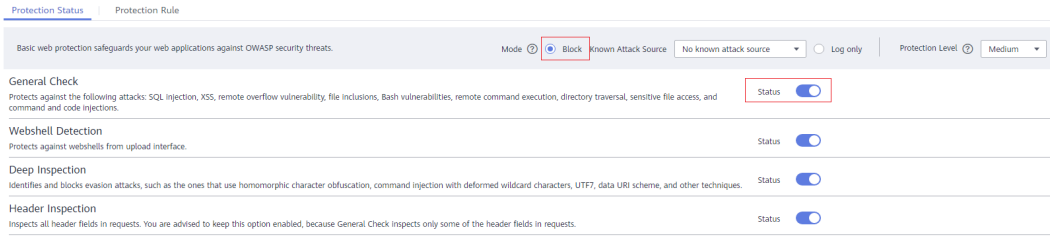
----Fim

Exemplo - Bloqueando ataques de injeção de SQL

Se o nome de domínio **www.example.com** tiver sido conectado ao WAF, execute as etapas a seguir para verificar se o WAF pode bloquear ataques de injeção SQL.

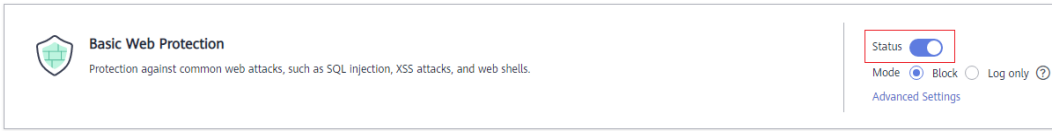
Passo 1 Ative a **General Check** na **Basic Web Protection** e defina o modo de proteção para **Block**.

Figura 7-6 Ativando Verificação Geral



Passo 2 Ative a proteção básica da Web do WAF.

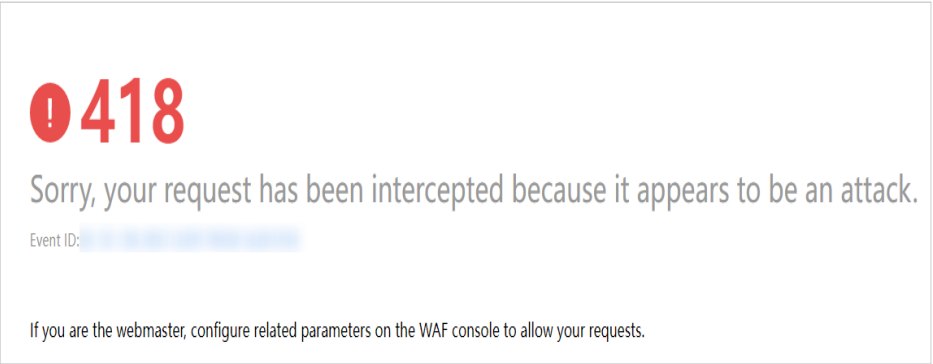
Figura 7-7 Ativando a proteção básica da Web do WAF



Passo 3 Limpe o cache do navegador e insira uma injeção SQL simulada (por exemplo, 1=1 ou http://www.example.com?id=') na caixa de endereço.

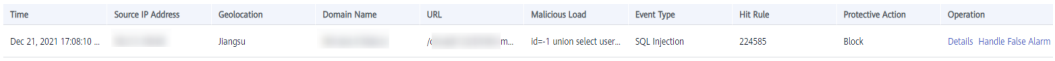
O WAF bloqueia a solicitação de acesso. **Figura 7-8** mostra uma página de bloco de exemplo.

Figura 7-8 Bloquear página



Passo 4 Acesse o console do WAF. No painel de navegação à esquerda, escolha **Events**. Veja o evento na página **Events**.

Figura 7-9 Evento de injeção SQL



----Fim

7.3 Configuração de controle de acesso inteligente

Se você ativar o controle de acesso inteligente, o WAF usará modelos integrados baseados em IA para analisar o tráfego do seu site, identificar ataques de CC e recursos anormais em solicitações HTTP no servidor de origem e gerar regras específicas de proteção e controle de acesso precisas para o seu site. Dessa forma, o WAF pode proteger automaticamente seu site contra ataques de CC.

AVISO

A proteção inteligente de controle de acesso agora está disponível para teste beta aberto (OBT). Para ativar, **enviar um ticket de serviço.**

Pré-requisitos

O site que você deseja proteger foi adicionado ao WAF.

Restrições

- No **Cloud mode**, apenas a edição padrão (a antiga edição profissional), a edição profissional (a antiga edição empresarial) e a edição platina (a antiga edição final) incluem proteção de controle de acesso inteligente.
- A proteção inteligente de controle de acesso está disponível apenas nas regiões do norte da China.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

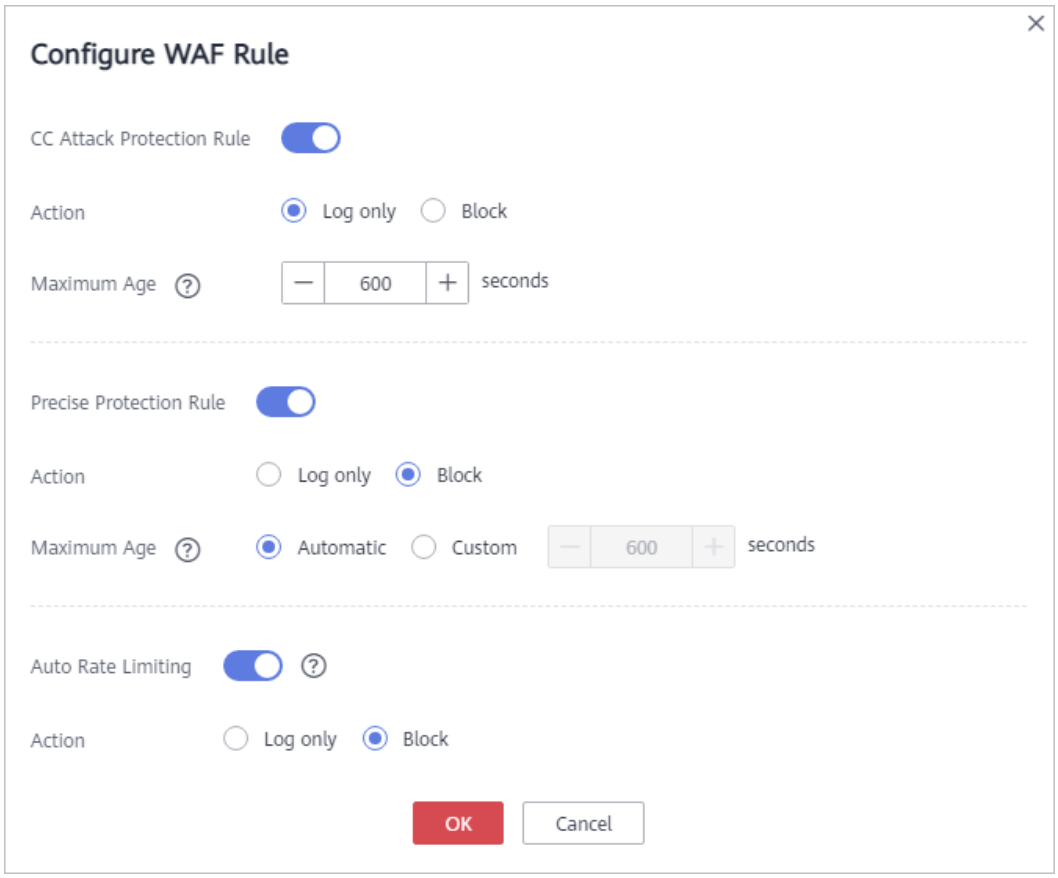
Passo 6 Na área de configuração do **Intelligent Access Control**, altere o **Status**, se necessário.

Figura 7-10 Controle de acesso inteligente

Passo 7 Clique em **Configure** para ir para a caixa de diálogo **Configure WAF Rule**.

- **CC Attack Protection Rule**/**Precise Protection Rule**: Configure **Action** e **Maximum Age** para eles depois de ativá-los.
  - **Action**: Selecione **Log only** ou **Block**.
  - **Maximum Age**: A regra torna-se inválida se o WAF não detectar nenhum tráfego de ataque CC dentro da idade máxima configurada.
- **Auto Rate Limiting**: Depois de ativar **Intelligent Access Control**, o WAF leva de 10 a 15 minutos para conhecer a linha de base do tráfego do seu site, determinar o volume máximo de tráfego que seu site pode processar e gerar uma regra para você. Portanto, você precisa ativar **Auto Rate Limiting** para limitar o tráfego que vai para o seu site durante esse tempo de janela. Dessa forma, o WAF pode proteger seus servidores de origem contra ataques DDoS antes que a proteção de controle de acesso inteligente entre em vigor. Depois que o WAF gera regras de controle de acesso inteligentes específicas para seu site, **Auto Rate Limiting Rate** se torna inválida automaticamente.

Figura 7-11 Configurar regra do WAF



Passo 8 Clique em **OK**.

Clique em **View WAF Rule** para exibir as políticas de proteção geradas automaticamente pelo WAF depois que ele detecta ataques de CC.

----Fim

7.4 Configuração de uma regra de proteção contra 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. Para fazer com que suas regras personalizadas de proteção contra ataques da CC entrem em vigor, certifique-se de que você habilitou a proteção contra ataques da CC (**Status** para **CC Attack Protection** deve ser ).

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

- Apenas uma regra de proteção contra ataques CC pode ser configurada para o mesmo caminho. Caso contrário, as regras de proteção contra ataques da CC podem entrar em conflito umas com as outras e não entrar em vigor. Se você tiver configurado várias regras de proteção CC para o mesmo caminho, exclua as desnecessárias.
- Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.
- Uma tabela de referência pode ser adicionada a uma regra de proteção contra ataques CC. A tabela de referência entra em vigor para todos os nomes de domínio protegidos.
- A proteção contra ataques da CC oferece diferentes ações de proteção para as regras de proteção contra ataques da CC, incluindo **Verification code**, **Block**. Por exemplo, você pode configurar uma regra de proteção contra ataque CC para bloquear solicitações de uma visita por 600 segundos, identificando o cookie (campo nome) se o visitante acessar um URL (por exemplo, /admin*) do seu site mais de 10 vezes em 60 segundos.
- O modo avançado não é suportado pela edição padrão (anteriormente edição profissional).
- O gerenciamento de tabelas de referência não é suportado pela edição padrão (anteriormente edição profissional).
- O caminho em uma regra de proteção contra ataques de CC deve ser definido como um URL (excluindo o nome de domínio). Este parâmetro permite correspondência de prefixo e correspondência exata.

  - Correspondência de prefixo: Um caminho terminado com * indica que o caminho é usado como um prefixo. O * pode ser usado como um valor curinga. Por exemplo, para proteger **/admin/test.php** ou **/adminabc**, você pode definir **Path** para /**admin***.
  - Correspondência exata: O caminho a ser inserido deve ser o mesmo que o caminho a ser protegido. Por exemplo, para proteger **/admin**Então o **Path** deve ser definido como **/admin**.
- Se seu site estiver conectado ao WAF e ao Content Delivery Network (CDN) e a **Protective Action** estiver definida como **Verification code** na regra de proteção contra ataques da CC, observe que:
  - **Path** deve ser definido para uma página dinâmica.
  - Se você configurar uma página estática para **Path**, a página estática será armazenada em cache pela CDN. Como resultado, a verificação falha. Lidar com o problema consultando **Por que o código de verificação falha ao ser atualizado após ativar o código de verificação em uma regra de proteção contra ataques da CC?**
- Se seu site usa proxies como anti-DDoS, Content Delivery Network (CDN) e serviços de aceleração de nuvem, selecione **Per user** para **Rate Limit Mode** e ative **All WAF instances**.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

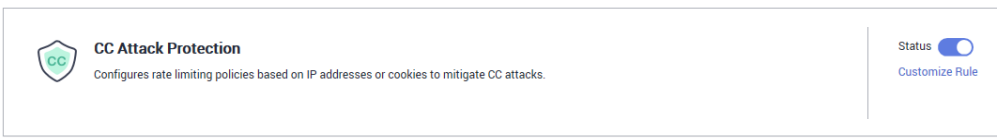
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração **CC Attack Protection**, altere **Status** se necessário e clique em **Customize Rule** para ir para a página **CC Attack Protection**.

Figura 7-12 Área de configuração CC Attack Protection



Passo 7 No canto superior esquerdo da página **CC Attack Protection**, clique em **Add Rule**.

Passo 8 Na caixa de diálogo exibida, configure uma regra de proteção contra ataques CC consultando **Tabela 7-7**.

Se um visitante cujo cookie é **name** acessar uma página em seu site onde o endereço inclui /**admin** no final (por exemplo, o https://www.example.com/adminlogic) mais de 10 vezes em 60 segundos, O WAF bloqueia as solicitações de visitantes com o mesmo **name** de cookie

para 600s e retorna a página configurada para **Page Content**. Figura 7-13 mostra as configurações.

Figura 7-13 Adicionando uma regra de proteção contra ataques CC

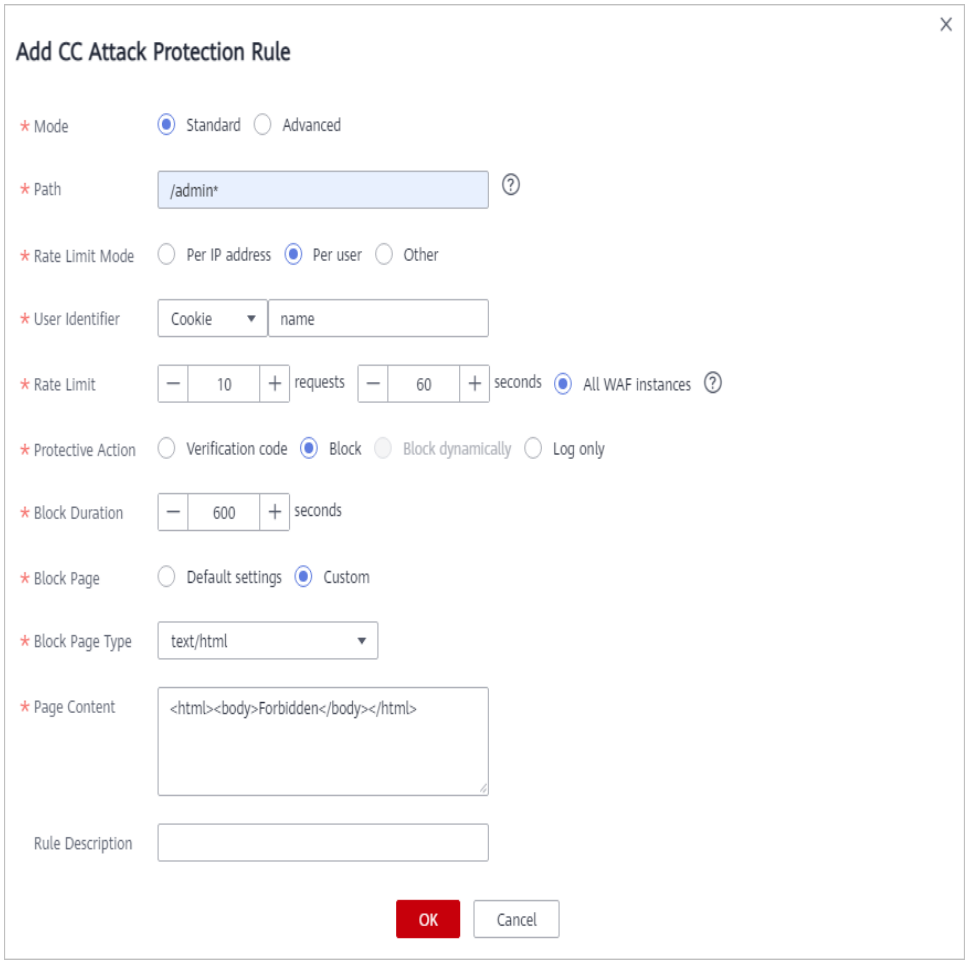


Tabela 7-7 Parâmetros de regra

Parâmetro	Descrição	Valor de exemplo
modo	• **Standard**: Somente o caminho de proteção de um nome de domínio pode ser restrito. • **Advanced**: Os campos caminho, endereço IP, cookie, cabeçalho e parâmetros podem ser restritos. Este parâmetro não está disponível na edição padrão (antiga edição profissional).	**Standard**

Parâmetro	Descrição	Valor de exemplo
Caminho	Defina este parâmetro somente quando **Standard** estiver selecionado para **Mode**. Parte da URL sem o nome de domínio. ● Correspondência de prefixo: Um caminho terminado com * indica que o caminho é usado como um prefixo. O * pode ser usado como um valor curinga. Por exemplo, para proteger **/admin/test.php** ou **/adminabc**, você pode definir **Path** para **/admin***. ● Correspondência exata: O caminho a ser inserido deve ser o mesmo que o caminho a ser protegido. Por exemplo, para proteger **/admin**Então o **Path** deve ser definido como **/admin**. **NOTA** ● O caminho suporta apenas correspondências de prefixo e exato, mas não suporta expressões regulares. ● O caminho não pode conter duas ou mais barras consecutivas. Por exemplo, ///**admin**. Se você digitar ///**admin**, o WAF converterá /// para /. ● O caminho é sensível a maiúsculas e minúsculas. ● Se **Path** estiver definido para /, todos os caminhos do site estão protegidos.	**/admin***

Parâmetro	Descrição	Valor de exemplo
Lista de Condição	Defina este parâmetro somente quando **Advanced** estiver selecionado para **Mode**. Clique em **Add** para adicionar condições. Pelo menos uma condição é necessária, mas até 30 condições são permitidas. Se você adicionar mais de uma condição, a regra só terá efeito se todas as condições forem atendidas. ● **Field**: As opções são **Path**, **IP**, **Cookie**, **Header**, e **Params**. ● **Subfield**: Configure este campo somente quando **Cookie**, **Header**, ou **Params** estiver selecionado para **Field**. **AVISO** O comprimento de um subcampo não pode exceder 2048 bytes. Apenas números, letras, sublinhados (_) e hifens (-) são permitidos. ● **Logic**: Selecione um relacionamento lógico na lista suspensa. **NOTA** Se você definir **Logic** para **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, ou **Suffix is not any of them**, selecione uma tabela de referência existente. Para mais detalhes, consulte **Adição de uma tabela de referência**. ● **Content**: Insira ou selecione o conteúdo que corresponde à condição.	**Path Include /admin**

Parâmetro	Descrição	Valor de exemplo
Modo de limitação de taxa	• **Per IP address**: Um visitante do site é identificado pelo endereço IP. • **Per user**: Um visitante do site é identificado pelo valor-chave de **Cookie** ou **Header**. • **Other**: Um visitante do site é identificado pelo campo Referer (fonte de solicitação definida pelo usuário). **NOTA** Se você definir **Rate Limit Mode** como **Other**, defina **Content** do **Referer** como um URL completo contendo o nome de domínio. O campo **Content** suporta apenas correspondência de prefixo e correspondência exata, mas não pode conter duas ou mais barras consecutivas, por exemplo, ///**admin**. Se você digitar ///**admin**, o WAF irá convertê-lo para /**admin**. Por exemplo, se **Path** for /**admin**, e você não quiser que os visitantes acessem a página a partir do **www.test.com**, defina **Content** de **Referer** como **http://www.test.com**.	**Per user**
Identificador do usuário	Esse parâmetro é obrigatório quando você seleciona **Per user** para **Rate Limit Mode**. • **Cookie**: Um nome de campo de cookie. Você precisa configurar um nome de variável de atributo no cookie que possa identificar exclusivamente um visitante da Web com base nos requisitos do seu site. Este campo não suporta expressões regulares. Apenas partidas completas são suportadas. Por exemplo, se um site usar o campo de **name** no cookie para identificar exclusivamente um visitante do site, selecione o **name**. • **Header**: Defina o cabeçalho HTTP definido pelo usuário que você deseja proteger. Você precisa configurar o cabeçalho HTTP que pode identificar visitantes da Web com base nos requisitos do seu site.	Nome

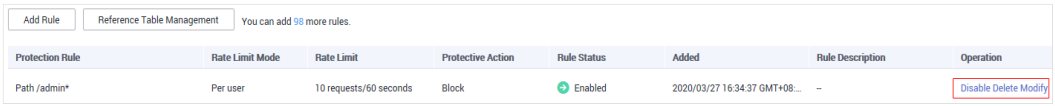
Parâmetro	Descrição	Valor de exemplo
Limite da taxa	O número de solicitações permitidas de um visitante do site no período de limite de taxa. Se o número de solicitações exceder o limite de taxa, o WAF executará a ação configurada para a **Protective Action**. **All WAF instances**: As solicitações para uma ou mais instâncias do WAF serão contadas juntas de acordo com o modo de limite de taxa selecionado. Por padrão, as solicitações para cada instância do WAF são contadas. Se você ativar isso, o WAF contará as solicitações para todas as suas instâncias do WAF para acionar essa regra. Para ativar o limite de taxa baseado no usuário, **Per user** ou **Other** (o **Referer** deve ser configurado) em vez de **Per IP address** deve ser selecionado para **Rate Limit Mode**. Isso ocorre porque a limitação de taxa baseada em endereço IP não pode limitar a taxa de acesso de um usuário específico. No entanto, na limitação de taxa baseada no usuário, as solicitações podem ser encaminhadas para uma ou mais instâncias do WAF. Portanto, **All WAF instances** devem estar habilitadas para acionar a regra com precisão.	**10** pedidos permitidos em **60** segundos
Ação Protetora	A ação que o WAF executará se o número de solicitações exceder o **Rate Limit** que você configurou. As opções são as seguintes: ● **Verification code**: O WAF permite solicitações que acionam a regra, desde que os visitantes do seu site completem a verificação necessária. ● **Block**: O WAF bloqueia solicitações que acionam a regra. ● **Block dynamically**: O WAF bloqueia solicitações que acionam a regra com base na **Allowable Frequency**, que você configura após o término do primeiro período de limite de taxa. A ação de proteção é suportada somente quando **Advanced** é selecionado para **Mode**. ● **Log only**: O WAF registra apenas solicitações que acionam a regra. Você pode **baixar dados de evento** e exibir os registros de proteção de um nome de domínio específico.	**Block**

Parâmetro	Descrição	Valor de exemplo
Frequência permissível	Esse parâmetro pode ser definido se você selecionar **Block dynamically** para **Protective Action**. O WAF bloqueia solicitações que acionam a regra com base no **Rate Limit** primeiro. Em seguida, no seguinte período de limite de taxa, o WAF bloqueia solicitações que acionam a regra com base na **Allowable Frequency** configurada por você. **Allowable Frequency** não pode ser maior que o **Rate Limit**. **NOTA** Se você definir **Allowable Frequency** como **0**, o WAF bloqueará todas as solicitações que acionarem a regra no próximo período de limite de taxa.	**8** pedidos permitidos em **60** segundos
Duração do bloqueio	Período de tempo para o qual bloquear o item quando você define **Protective Action** como **Block**.	**600** segundos
Bloquear página	A página exibida se o número máximo de solicitações foi atingido. Este parâmetro é configurado somente quando **Protective Action** é definida como **Block**. ● Se você selecionar **Default settings**, a página de bloco padrão será exibida. ● Se você selecionar **Custom**, uma mensagem de erro personalizada será exibida.	**Custom**
Tipo de página de bloco	Se você selecionar **Custom** para **Block Page**, selecione um tipo de página de bloco. As opções são: ● **application/jsontext/html** ● **text/htmltext/xml** ● **text/xml**	**text/html**

Parâmetro	Descrição	Valor de exemplo
Conteúdo da Página	Se você selecionar **Custom** para **Block Page**, configure o conteúdo a ser retornado.	Os estilos de conteúdo da página correspondentes a diferentes tipos de página são os seguintes: ● **text/html**: <html><body>Forbidden</body></html> ● **application/json**: {"msg": "Forbidden"} ● **text/xml**: <?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>
Descrição da regra	Uma descrição da regra. Este parâmetro é opcional.	Nenhum

Passo 9 Clique em **OK**. Em seguida, você pode exibir a regra de proteção contra ataques de CC adicionada na lista de regras de CC.

Figura 7-14 Lista de regras CC



- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.
- Para modificar uma regra, clique em **Modify** na linha que contém a regra.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

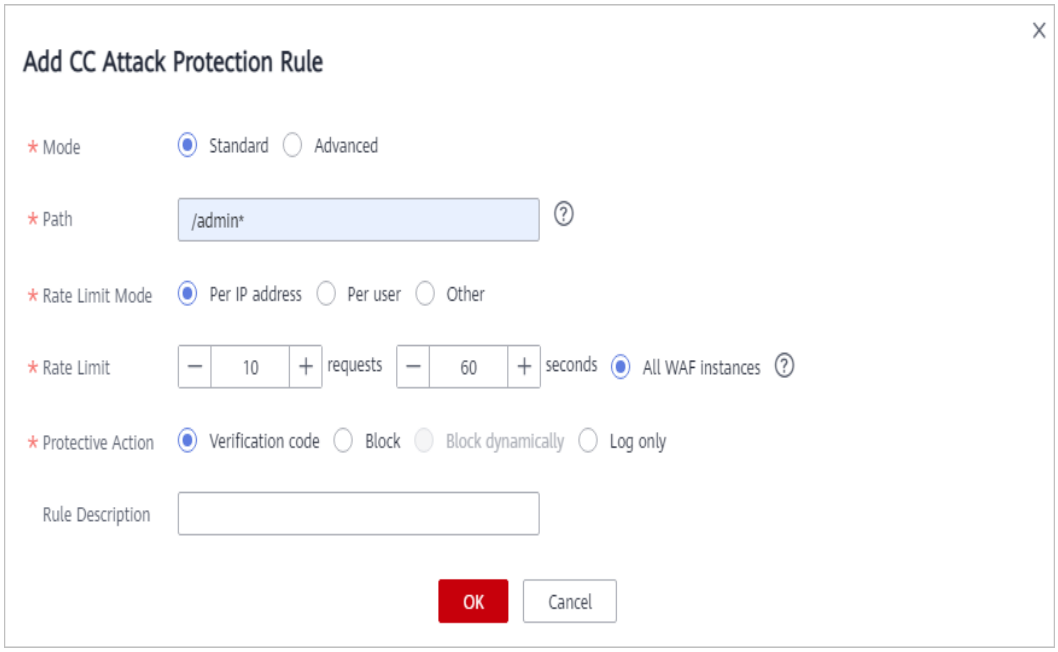
----Fim

Exemplo de Configuração - Código de Verificação

Se o nome de domínio **www.example.com** tiver sido conectado ao WAF, execute as etapas a seguir para verificar se a verificação WAF CAPTCHA está ativada.

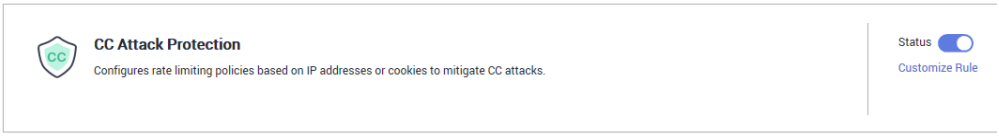
Passo 1 Adicione uma regra de proteção contra ataques CC com **Protection Action** definida como **Verification code**.

Figura 7-15 Código de verificação



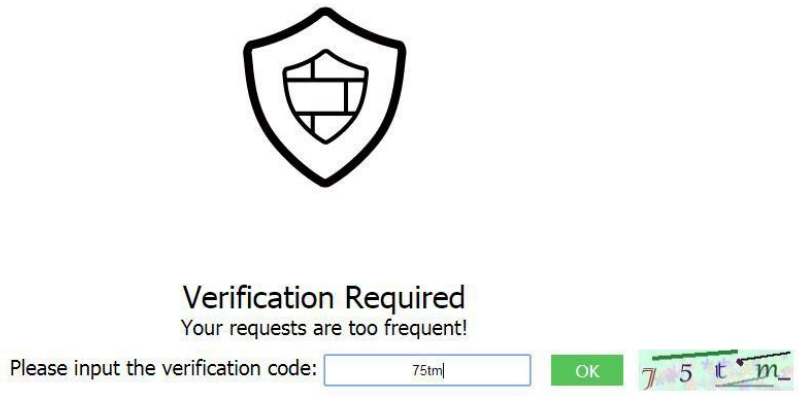
Passo 2 Ative a proteção contra ataques CC.

Figura 7-16 Área de configuração CC Attack Protection



Passo 3 Limpe o cache do navegador e acesse o http://www.example.com/admin/.

Se você acessar a página por 10 vezes dentro de 60 segundos, um código de verificação será necessário quando você tentar acessar a página pela décima primeira vez. Você precisa digitar o código de verificação para continuar o acesso.



Passo 4 Vá para o console do WAF. No painel de navegação à esquerda, escolha **Events**. Veja o evento na página **Events**.

Figura 7-17 Exibindo Eventos - Código de verificação

----Fim

7.5 Configuração de uma regra de proteção precisa

O WAF permite personalizar regras de proteção combinando cabeçalhos HTTP, URLs, cookies, parâmetros de solicitação e endereços IP do cliente.

Você pode combinar campos HTTP comuns, como **IP**, **Path**, **Referer**, **User Agent**, e **Params** em uma regra de proteção para permitir que o WAF permita, bloqueie ou registre apenas as solicitações que correspondam às condições combinadas.

Uma tabela de referência pode ser adicionada a uma regra de proteção precisa. A tabela de referência entra em vigor para todos os nomes de domínio protegidos.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

- O campo **Response** não pode ser configurado na edição padrão, antiga edição profissional.
- **Full Detection** não está disponível na edição padrão do WAF (antiga edição profissional) e para o WAF na nuvem faturado com base em pagamento por uso.
- A função de tabela de referência não está disponível na edição padrão do WAF (antiga edição profissional) e no WAF na nuvem faturado com base em pagamento por uso.
- Se quiser especificar o campo Resposta, selecione as seguintes regiões:
  - CN-Hong Kong
  - AP-Bangkok
- Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.
- Se configurar a **Protective Action** para **Block** para obter uma regra de protecção precisa, pode configurar uma regra de origem de ataque conhecida referindo-se a. O WAF bloqueará solicitações que correspondam ao endereço IP configurado, cookie ou parâmetros por um período de tempo configurado como parte da regra.

Cenários de aplicação

Regras de proteção precisas são usadas para proteção em segundo plano anti-leeching e gerenciamento de sites.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

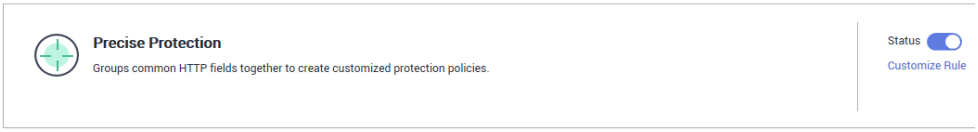
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração **Precise Protection**, altere o **Status** conforme necessário e clique em **Customize Rule** para acessar a página **Precise Protection**.

Figura 7-18 Área de configuração de proteção precisa

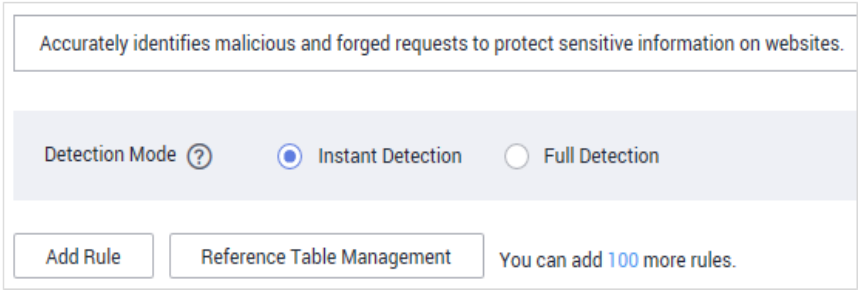


Passo 7 Na página **Precise Protection**, defina **Detection Mode**. **Figura 7-19** mostra um exemplo.

Dois modos de detecção estão disponíveis:

- **Instant Detection**: Se uma solicitação corresponder a uma regra de proteção precisa configurada, o WAF encerrará imediatamente a detecção de ameaças e bloqueará a solicitação.
- **Full Detection**: Se uma solicitação corresponder a uma regra de proteção precisa configurada, o WAF concluirá a verificação primeiro e, em seguida, bloqueará todas as solicitações que corresponderem à regra de proteção precisa configurada.

Figura 7-19 Configurando o modo de detecção



Passo 8 Clique em **Add Rule**.

Passo 9 Na caixa de diálogo exibida, adicione uma regra referindo-se a **Tabela 7-8** e **Exemplo de configuração - Bloqueando um determinado tipo de solicitações de ataque**.

As configurações mostradas em **Figura 7-20** são usadas como exemplo. Se um visitante tentar acessar um URL que contenha **/admin**O WAF bloqueará a solicitação.

AVISO

Para garantir que o WAF bloqueie apenas solicitações de ataque, configure a **Protective Action** para **Log only** primeiro e verifique se as solicitações normais estão bloqueadas na página **Events**. Se nenhuma solicitação normal for bloqueada, configure **Protective Action** para **Block**.

Figura 7-20 Adicionar regra de proteção precisa

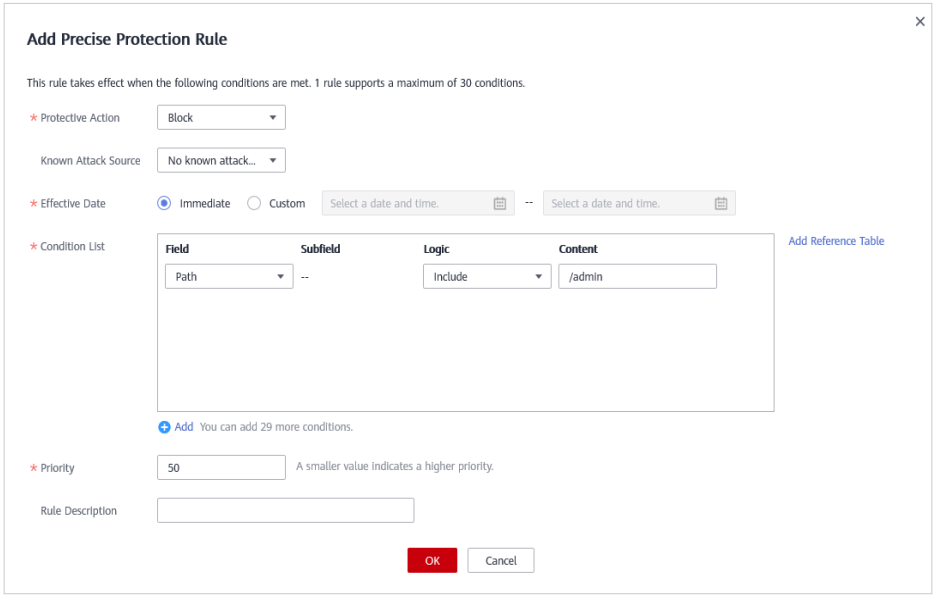


Tabela 7-8 Parâmetros de regra

Parâmetro	Descrição	Valor de exemplo
Ação Protetora	Você pode selecionar **Block**, **Allow**, ou **Log only**. Valor predefinido: **Block**	**Block**
Fonte de ataque conhecida	Se você definir **Protective Action** como **Block**, poderá selecionar um tipo de bloqueio para uma regra de origem de ataque conhecida. Em seguida, o WAF bloqueia solicitações correspondentes ao **IP**, **Cookie**, ou **Params** por um período de tempo que depende do tipo de bloqueio selecionado.	**Long-term IP address blocking**

Parâmetro	Descrição	Valor de exemplo
Data efetiva	Selecione **Immediate** para ativar a regra imediatamente ou selecione **Custom** para configurar quando você deseja que a regra seja ativada.	**Immediate**

Parâmetro	Descrição	Valor de exemplo
Lista de Condição	Clique em **Add** para adicionar condições. Pelo menos uma condição precisa ser adicionada. Você pode adicionar até 30 condições a uma regra de proteção. Se mais de uma condição for adicionada, todas as condições devem ser atendidas para que a regra seja aplicada. Uma condição inclui os seguintes parâmetros: Os parâmetros para configurar uma condição são descritos a seguir: ● **Field** ● **Subfield**: Configurar este campo somente quando **Parâmetros**, **Biscoito**, ou **Cabeçalho** é selecionado para **Field**. **AVISO** O comprimento de um subcampo não pode exceder bytes de 2 048. Apenas números, letras, sublinhados (_) e hifens (-) são permitidos. ● **Logic**: Selecione um relacionamento lógico na lista suspensa. **NOTA** – Se **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, ou **Suffix is not any of them** está selecionado, selecione uma tabela de referência existente na lista suspensa **Content**. Para mais detalhes, consulte **Adição de uma tabela de referência**. – **Exclude any value**, **Not equal to any value**, **Prefix is not any of them**, e **Suffix is not any of them** indica, respectivamente, que o WAF realiza a ação de proteção (bloquear, permitir, ou log only) quando o campo na solicitação de acesso não contém, não é igual a, ou o prefixo ou sufixo não é qualquer valor definido na tabela de referência. Por exemplo, suponha que o campo **Path** esteja definido como **Exclude any value** e a tabela de referência de **test** esteja selecionada. Se *test1*, *test2* e *test3* estiverem definidos na tabela de referência de **test**, o WAF executará a ação de proteção quando o caminho da solicitação de acesso não contiver *test1*, *test2*, ou *test3*. ● **Content**: Insira ou selecione o conteúdo da correspondência de condição.	● **Path Include /admin** ● **User Agent Prefix is not mozilla/5.0** ● **IP Equal to 192.168.2.3** ● **Cookie key1 Prefix is not jsessionid**

Parâmetro	Descrição	Valor de exemplo
	NOTA Para obter mais detalhes sobre as configurações em geral, consulte **Tabela 7-9**.	
Prioridade	Prioridade de regra. Se você tiver adicionado várias regras, as regras serão correspondidas por prioridade. Quanto menor o valor definido, maior a prioridade. **AVISO** Se várias regras precisas de controle de acesso tiverem a mesma prioridade, o WAF corresponderá às regras na seqüência de tempo em que as regras forem adicionadas.	**5**
Descrição da regra	Uma breve descrição da regra. Este parâmetro é opcional.	Nenhum

Tabela 7-9 Configurações da lista de condições

Campo	Exemplo de subcampo	lógico	Exemplo de Conteúdo
Path: Parte de um URL que não inclui um nome de domínio. Este valor suporta apenas correspondências exatas. Por exemplo, se o caminho a ser protegido é /**admin**, **Path** deve ser definido como /**admin**.	Nenhum	Selecione um relacionamento lógico na lista suspensa.	**/buy/phone/** **AVISO** Se **Path** estiver definido para /, todos os caminhos do site estão protegidos.
User Agent: Um agente de usuário do scanner a ser verificado.	Nenh		**Mozilla/5.0 (Windows NT 6.1)**
IP: Um endereço IP do visitante para a proteção.	Nenh		XXX.XXX.1.1

Campo	Exemplo de subcampo	lógico	Exemplo de Conteúdo
Params: Um parâmetro de solicitação.	**sttl**		**201901150929**
Referer: Um recurso de solicitação definido pelo usuário. Por exemplo, se o caminho protegido for **/admin/xxx** e você não quiser que os visitantes acessem a página do **www.test.com**, defina **Content** como **http://www.test.com**.	Nenhum		http://www.test.com
Cookie: Um pequeno pedaço de dados para identificar os visitantes da web.	**name**		JSESSIONID
Header: Um cabeçalho HTTP definido pelo usuário.	**Accept**		**text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8**
Method: o método de requisição definido pelo usuário.	Nenhum		**GET**, **POST**, **PUT**, **DELETE**, e **PATCH**
Request Line: Comprimento de uma linha de solicitação definida pelo usuário.	Nenhum		**50**

Campo	Exemplo de subcampo	lógico	Exemplo de Conteúdo
Request: Comprimento de uma solicitação definida pelo usuário. Ele inclui o cabeçalho da solicitação, a linha da solicitação e o corpo da solicitação.	Nenhum		Nenhum
Protocol: o protocolo da solicitação.	Nenhum		HTTP
Response Code: Código de status retornado à solicitação.	Nenhum	● Igual a ● Não é igual a ● Igual a qualquer valor ● Não é igual a nenhum valor	404
Response Length: o comprimento da resposta ao pedido.	Nenhum	● Comprimento do subcampo igual a ● Comprimento do subcampo não igual a ● Comprimento do subcampo maior que ● Comprimento do subcampo menor que	Nenhum
Response Time: tempo de resposta ao pedido.	Nenhum	● Comprimento do subcampo igual a ● Comprimento do subcampo diferente de ● Comprimento do subcampo maior que ● Comprimento do subcampo menor que	Nenhum

Campo	Exemplo de subcampo	lógico	Exemplo de Conteúdo
Response Header: cabeçalho da resposta.	Nenhum	● Incluir ● Excluir ● Igual a ● Não é igual a	Nenhum
Response Body: corpo da mensagem de resposta	Nenhum	● Incluir ● Excluir ● Inclua qualquer valor ● Excluir qualquer valor	Nenhum

AVISO

Os campos **Response Code**, **Response Length**, **Response Time**, **Response Header**, e **Response Body** são suportados apenas pela edição profissional (antiga edição empresarial), edição platinum (antiga edição final) e instância dedicada do WAF nas seguintes regiões:

- CN-Hong Kong
- AP-Bangkok

Passo 10 Clique em **OK**. Você pode então exibir a regra de proteção precisa adicionada na lista de regras de proteção.

Figura 7-21 Regras de proteção

- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.
- Para modificar uma regra, clique em **Modify** na linha que contém a regra.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

----Fim

Efeito de proteção

Se você configurou uma regra de proteção precisa como mostrada em **Figura 7-20** para seu nome de domínio, para verificar se o WAF está protegendo seu site (**www.example.com**) contra a regra:

Passo 1 Limpe o cache do navegador e digite o nome do domínio na barra de endereços para verificar se o site está acessível.

- Se o site estiver inacessível, conecte o nome de domínio do site ao WAF seguindo as instruções em **Passo 4: Encaminhamento do tráfego do site para o WAF**.

- Se o site estiver acessível, acesse **Passo 2**.

Passo 2 Limpe o cache do navegador e digite **http://www.example.com/admin** (ou qualquer página contendo **/admin**) na barra de endereços. Normalmente, o WAF bloqueia as solicitações que atendem às condições e retorna a página de bloqueio.

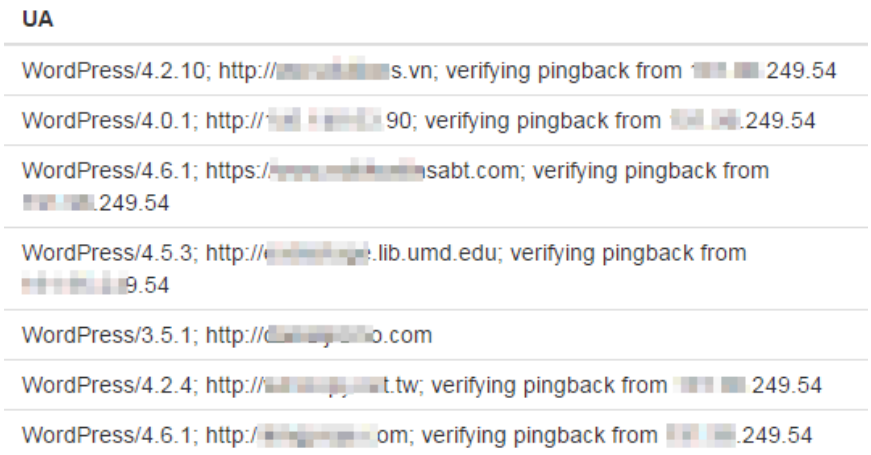
Passo 3 Retorne ao console do WAF. No painel de navegação, clique em **Events**. Na página exibida, visualize ou **baixe dados de eventos**.

----Fim

Exemplo de configuração - Bloqueando um determinado tipo de solicitações de ataque

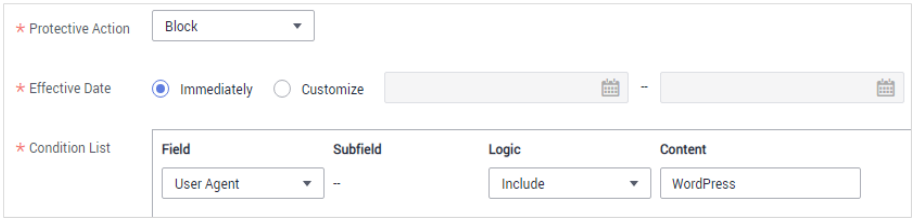
A análise de um tipo específico de ataque de pingback de WordPress mostra que o campo **User Agent** contém WordPress (Agente de Usuário). Consulte **Figura 7-22**.

Figura 7-22 WordPress ataque de pingback



Uma regra precisa, como mostrado na figura, pode bloquear esse tipo de ataque.

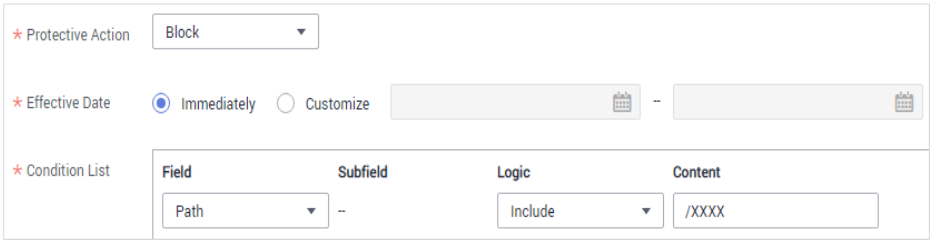
Figura 7-23 Configuração do User Agent



Exemplo de configuração - Bloqueando solicitações de ataque para um determinado URL

Se um grande número de endereços IP estiver acessando uma URL que não existe, configure a seguinte regra de proteção para bloquear tais solicitações para reduzir o uso de recursos no servidor de origem. **Figura 7-24** mostra a configuração da regra.

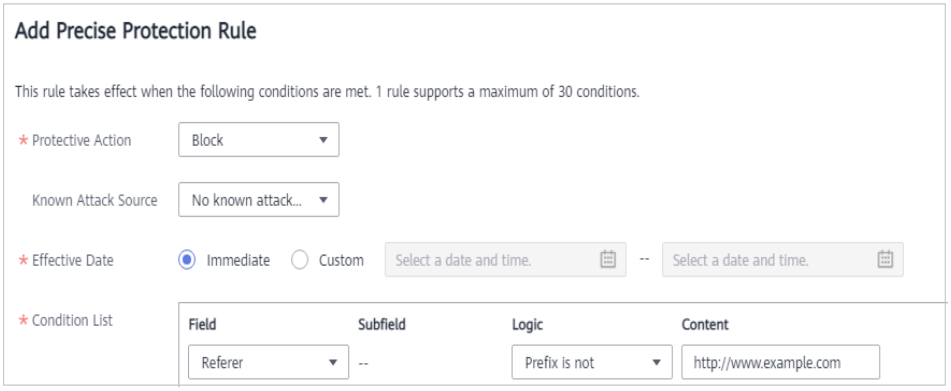
Figura 7-24 Bloqueio de solicitações para um URL específico



Exemplo de Configuração - Bloqueando Solicitações com Campos nulos

Você pode configurar regras de proteção precisas para bloquear um campo nulo. Por exemplo, para proteger o nome de domínio www.example.com de solicitações com Referer vazio, configure uma regra como mostrado em **Figura 7-25**.

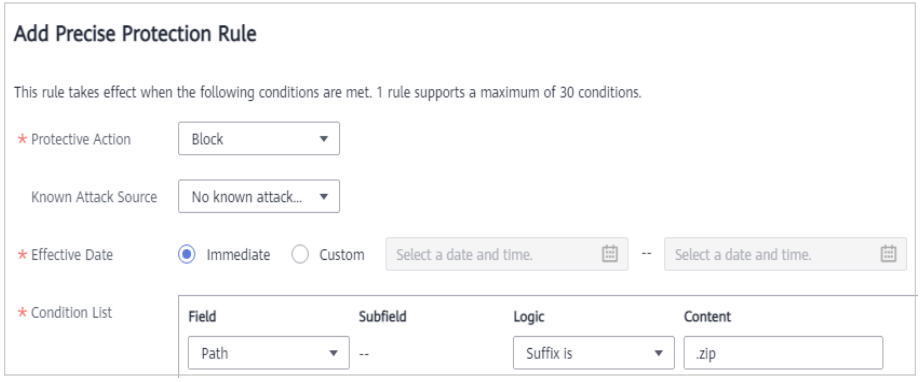
Figura 7-25 Bloqueando solicitações com Referer vazio



Exemplo de Configuração - Bloqueando Tipos de Arquivo Especificados (ZIP, TAR e DOCX)

Você pode configurar tipos de arquivo que correspondam ao campo de caminho para bloquear arquivos específicos de determinados tipos. Por exemplo, se você quiser block.zip arquivos, você pode configurar uma regra de proteção precisa como mostrado em **Figura 7-26** para bloquear solicitações de acesso de arquivos .zip.

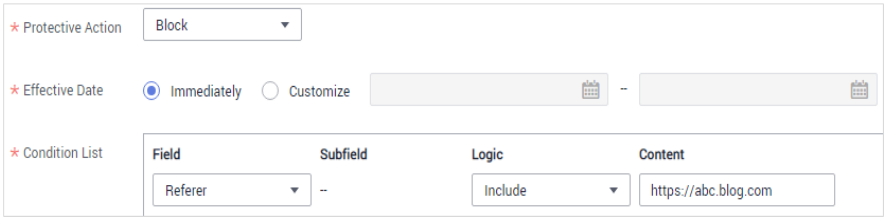
Figura 7-26 Bloqueio de solicitações de tipos de arquivos específicos



Exemplo de Configuração - Impedindo Hotlinking

Você pode configurar uma regra de proteção com base no campo Referer para permitir que o WAF bloqueie o hotlinking de um site específico. Se você descobrir que, por exemplo, solicitações do **https://abc.blog.com** estão roubando imagens do seu site, configure uma regra para bloquear essas solicitações.

Figura 7-27 Impedindo o hotlinking



Exemplo de configuração - Permitindo que um endereço IP especificado acesse seu site

Você pode configurar duas regras de proteção precisas, uma para bloquear todas as solicitações, como mostrado na **Figura 7-28**, mas outra para permitir o acesso de um endereço IP específico, como mostrado na **Figura 7-29**.

Figura 7-28 Bloqueando todas as solicitações

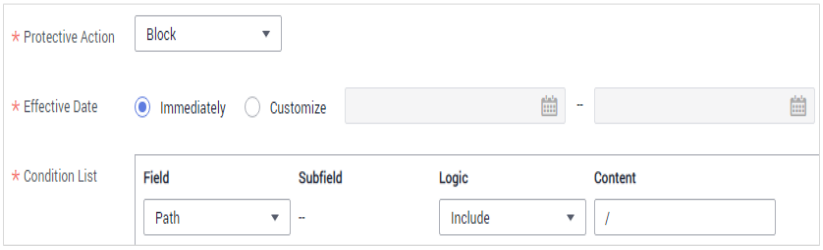
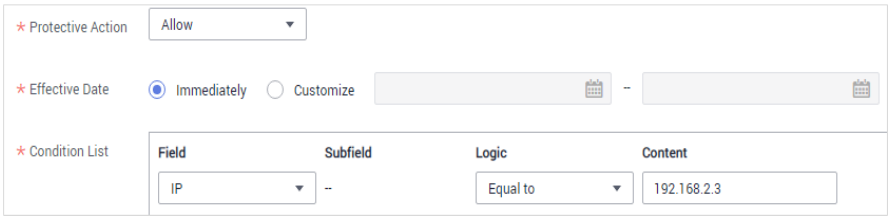


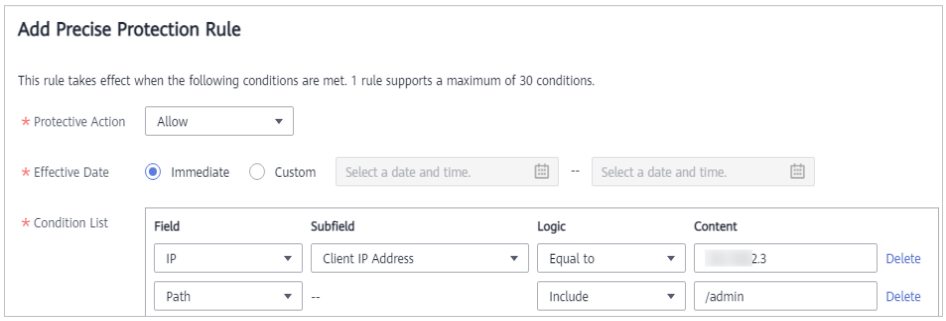
Figura 7-29 Permitir o acesso a um endereço IP especificado



Exemplo de configuração - Permitindo que um endereço IP específico acesse um determinado URL

Você pode configurar várias condições no campo **Condition List**. Se uma solicitação de acesso atender às condições da lista, o WAF permitirá que a solicitação de um endereço IP específico acesse um URL especificado. **Figura 7-30** mostra um exemplo.

Figura 7-30 Permitir que endereços IP específicos acessem URLs especificados



7.6 Adição de uma tabela de referência

Este tópico descreve como criar uma tabela de referência para configurar em lote métricas de proteção de um único tipo, como **Path**, **User Agent**, **IP**, **Params**, **Cookie**, **Referer**, e **Header**. Uma tabela de referência pode ser referenciada por regras de proteção contra ataques CC e regras de proteção precisas.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

Esta função não está disponível na Standard edition (antiga edição profissional) .

Cenários de aplicação

Você pode usar uma tabela de referência ao configurar campos de proteção em lotes para regras de proteção contra ataques CC e regras de proteção de acesso precisas.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área **CC Attack Protection** ou **Precise Protection**, clique em **Customize Rule**.

Passo 7 Clique em **Reference Table Management** no canto superior esquerdo da lista.

Passo 8 Na página **Reference Table Management**, clique em **Add Reference Table**.

Passo 9 Na caixa de diálogo **Add Reference Table**, especifique os parâmetros referindo-se a **Tabela 7-10**.

Figura 7-31 Adicionando uma tabela de referência

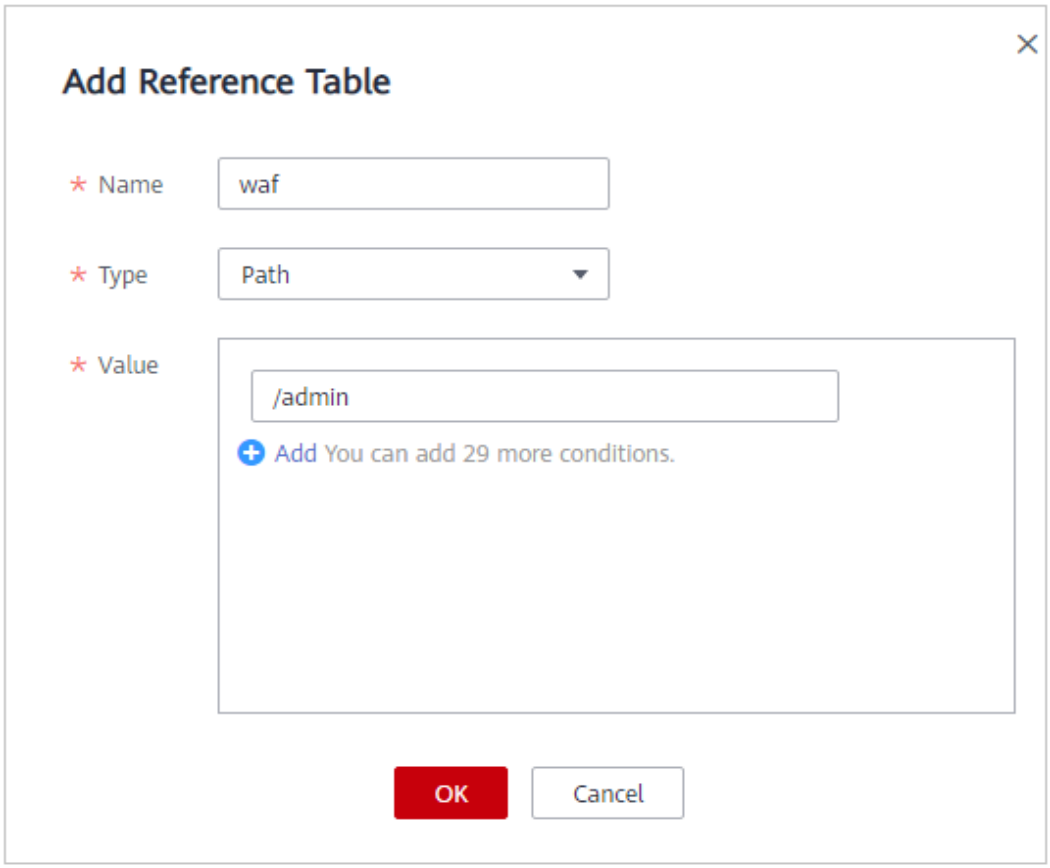


Tabela 7-10 Descrição do parâmetro

Parâmetro	Descrição	Valor de exemplo
Nome	Nome da tabela que você inseriu	Teste

Parâmetro	Descrição	Valor de exemplo
Tipo	● **Path**: Um URL a ser protegido, excluindo um nome de domínio ● **User Agent**: Um agente de usuário do scanner a ser protegido ● **IP**: Um endereço IP do visitante a ser protegido. ● **Params**: Um parâmetro de solicitação a ser protegido ● **Cookie**: Um pequeno pedaço de dados para identificar visitantes da web ● **Referer**: Um recurso de solicitação definido pelo usuário Por exemplo, se o caminho protegido for **/admin/xxx** e você não quiser que os visitantes possam acessá-lo a partir do *www.test.com*, defina **Value** como **http://www.test.com**. ● **Header**: Um cabeçalho HTTP definido pelo usuário	**Path**
Valor	Valor do **Type** correspondente. Wildcards não são permitidos. **NOTA** Clique em **Add** para adicionar mais de um valor.	**/buy/phone/**

Passo 10 Clique em **OK** . Em seguida, você pode exibir a tabela de referência adicionada na lista de tabela de referência.

----Fim

Outras operações

- Para modificar uma tabela de referência, clique em **Modify** na linha que contém a tabela de referência.
- Para excluir uma tabela de referência, clique em **Delete** na linha que contém a tabela de referência.

7.7 Configuração de uma regra de lista negra ou de lista branca de endereços IP

Por padrão, todos os endereços IP têm permissão para acessar seu site. Você pode configurar regras de lista negra e lista branca para bloquear, registrar apenas ou permitir solicitações de acesso de endereços IP ou intervalos de endereços IP específicos. Você pode adicionar um único endereço IP ou importar um grupo de endereços IP para a lista negra ou lista branca.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

- O WAF suporta a importação em lote de listas negras e listas brancas de endereços IP. Você pode usar grupos de endereços para adicionar vários endereços IP/intervalos rapidamente a uma regra de lista negra ou de lista branca. Para mais detalhes, consulte **Adição de um grupo de endereços de IP**.
- Se os balanceadores de carga ELB usados para as instâncias dedicadas ou de balanceamento de carga do WAF oferecerem suporte a endereços de IPv6, essas instâncias do WAF também poderão oferecer suporte a endereços de IPv6 ou intervalos de endereços de IPv6.
- Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.
- O endereço 0.0.0.0/0 não pode ser adicionado a uma lista negra ou lista branca de endereços IP do WAF e, se uma lista branca entrar em conflito com uma lista negra, a regra da lista branca terá prioridade. Se você quiser permitir apenas um endereço IP específico dentro de um intervalo de endereços bloqueados, adicione uma regra de lista negra para bloquear o intervalo e, em seguida, adicione uma regra de lista branca para permitir o endereço individual que você deseja permitir.

  AVISO

  Se você quiser permitir que apenas endereços IP especificados acessem o site protegido, consulte **Como faço para permitir que apenas endereços IP especificados acessem o site protegido?**

- Se você configurar **Protective Action** para **Block** para uma regra de lista negra ou lista branca, poderá configurar uma regra de origem de ataque conhecida fazendo referência a

Configuração de uma regra de origem de ataque conhecido. O WAF bloqueará solicitações que correspondam ao endereço IP configurado, cookie ou parâmetros por um período de tempo configurado como parte da regra.

Impacto no sistema

Se um endereço IP for adicionado a uma lista negra ou lista branca, o WAF bloqueia ou permite solicitações desse endereço IP sem verificar se as solicitações são maliciosas.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

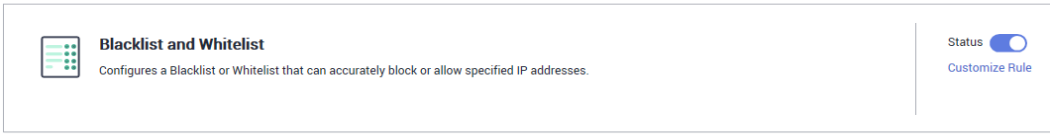
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração **Blacklist and Whitelist**, altere o **Status** conforme necessário e clique em **Customize Rule**.

Figura 7-32 Área de configuração Blacklist e Whitelist



Passo 7 No canto superior esquerdo da página **Blacklist and Whitelist**, clique em **Add Rule**.

Passo 8 Na caixa de diálogo exibida, especifique os parâmetros referindo-se a **Tabela 7-11**. **Figura 7-33** e **Figura 7-34** mostram dois exemplos.

NOTA

- Se você selecionar **Log only** para **Protective Action** para um endereço IP, o WAF identificará e registrará somente solicitações do endereço IP.
- Outros endereços IP são avaliados com base em outras regras de proteção WAF configuradas.

Figura 7-33 Adicionando um endereço IP/intervalo a uma regra de lista negra ou de lista branca

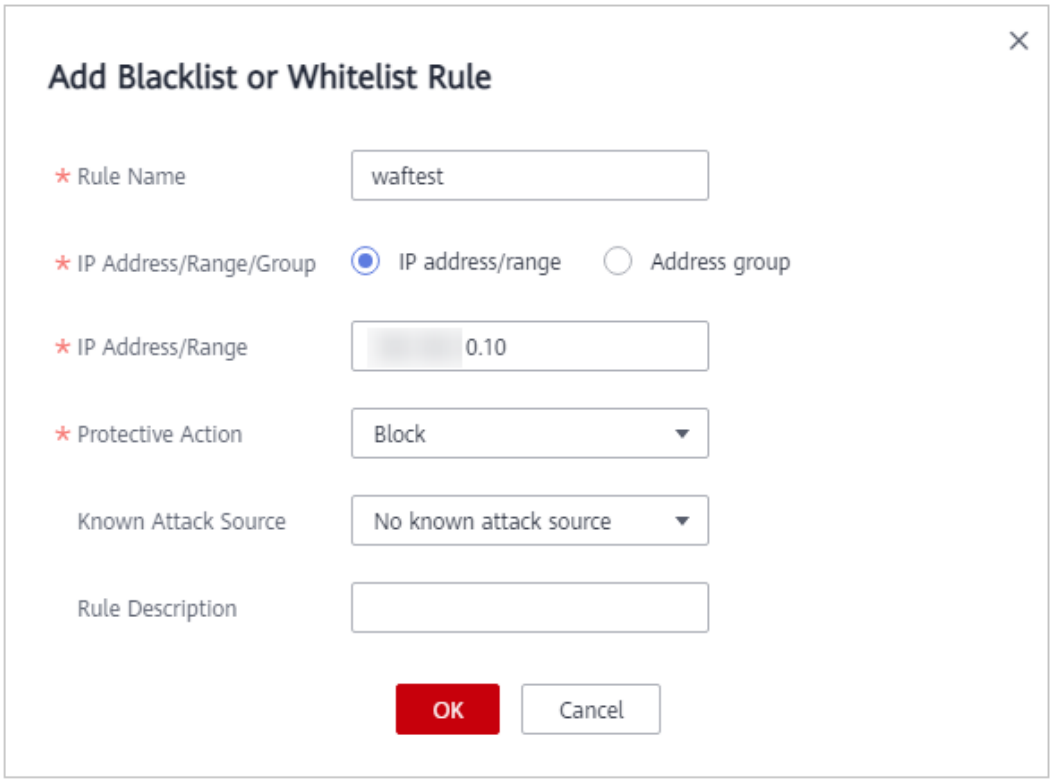


Figura 7-34 Adição em lote de endereços IP/intervalos a uma regra de lista negra ou de lista branca

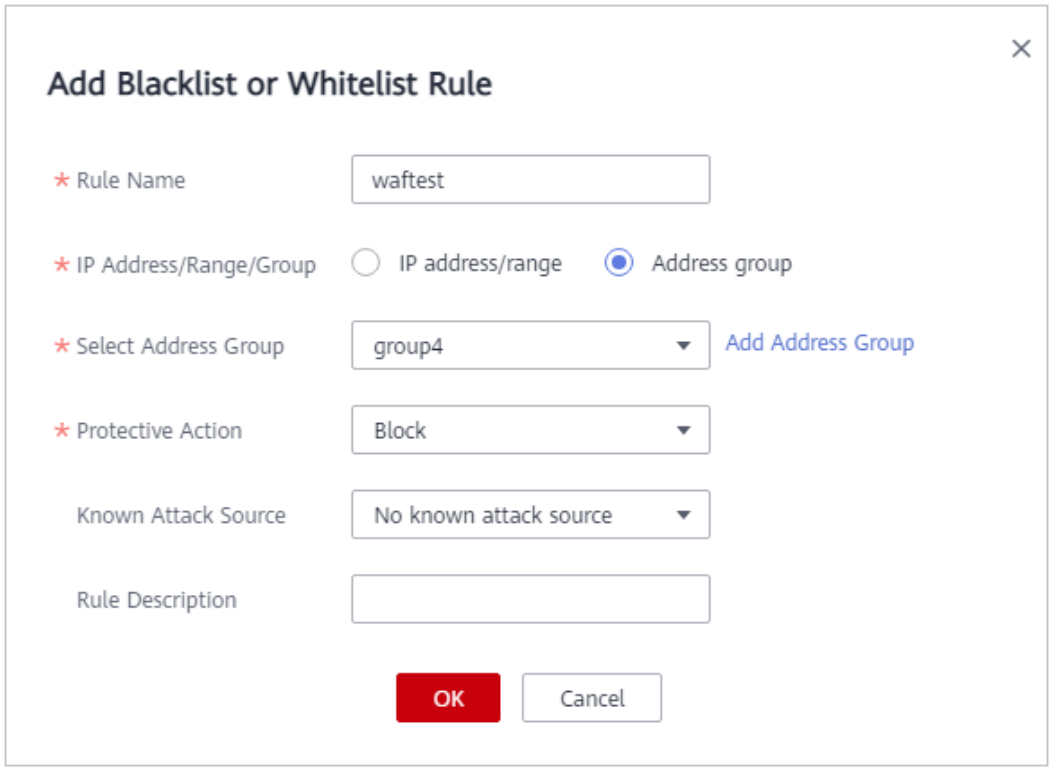


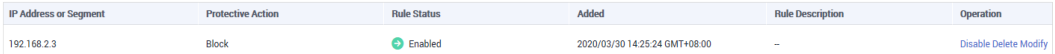
Tabela 7-11 Parâmetros de regra

Parâmetro	Descrição	Valor de exemplo
Nome da regra	Nome da regra que você inseriu.	waftest
Endereço IP/ Faixa/Grupo	Você pode selecionar **IP address/Range** ou **Address Group** para adicionar endereços IP a uma lista negra ou regra de lista branca.	Endereço/intervalo de IP
Endereço/ intervalo de IP	Esse parâmetro é obrigatório se você selecionar **IP address/ range** para **IP Address/Range/ Group**. Endereços IP ou intervalos de endereços IP são suportados. ● Endereço IP: Endereço IP a ser adicionado à lista negra ou lista branca ● Intervalo de endereços IP: Endereço IP e máscara de sub-rede definindo um segmento de rede	XXX.XXX.2.3
Selecionar Grupo de Endereços	Esse parâmetro é obrigatório se você selecionar **Address group** para IP **Address/Range/ Group**. Selecione um grupo de endereços IP na lista suspensa. Você também pode clicar em **Add Address Group** para criar um grupo de endereços. Para mais detalhes, consulte **Adição de um grupo de endereços de IP**.	groupwaf

Parâmetro	Descrição	Valor de exemplo
Ação Protetora	● **Block**: Selecione **Block** se quiser colocar na lista negra um endereço IP ou intervalo de endereços IP. ● **Allow**: Selecione **Allow** se quiser colocar na lista branca um endereço IP ou intervalo de endereços IP. ● **Log only**: Selecione **Log only** se quiser observar um endereço IP ou intervalo de endereços IP. Em seguida, o WAF determina se o endereço IP ou o intervalo de endereços IP estão na lista negra ou na lista branca com base nos **dados de eventos**.	Bloqueio
Fonte de ataque conhecida	Se você selecionar **Block** para **Protective Action**, poderá selecionar um tipo de bloqueio de uma regra de origem de ataque conhecida. O WAF bloqueará as solicitações que correspondam ao endereço IP configurado, cookie ou parâmetros por um período de tempo configurado como parte da regra.	Bloqueio de endereços IP a longo prazo
Descrição da regra	Uma breve descrição da regra. Este parâmetro é opcional.	Nenh

Passo 9 Clique em **OK**. Em seguida, você pode exibir a regra adicionada na lista de regras de lista negra e lista branca.

Figura 7-35 Regras de lista negra ou lista branca



- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.
- Para modificar uma regra, clique em **Modify** na linha que contém a regra.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

----Fim

Exemplo de configuração - Permitindo um endereço IP especificado

Se o nome de domínio *www.example.com* tiver sido conectado ao WAF, você poderá executar as seguintes etapas para verificar se a regra entra em vigor:

Passo 1 Adicione as duas regras de lista negra e lista branca a seguir para bloquear todos os endereços IP:

Figura 7-36 Bloqueando intervalo de endereços IP 1.0.0.0/1

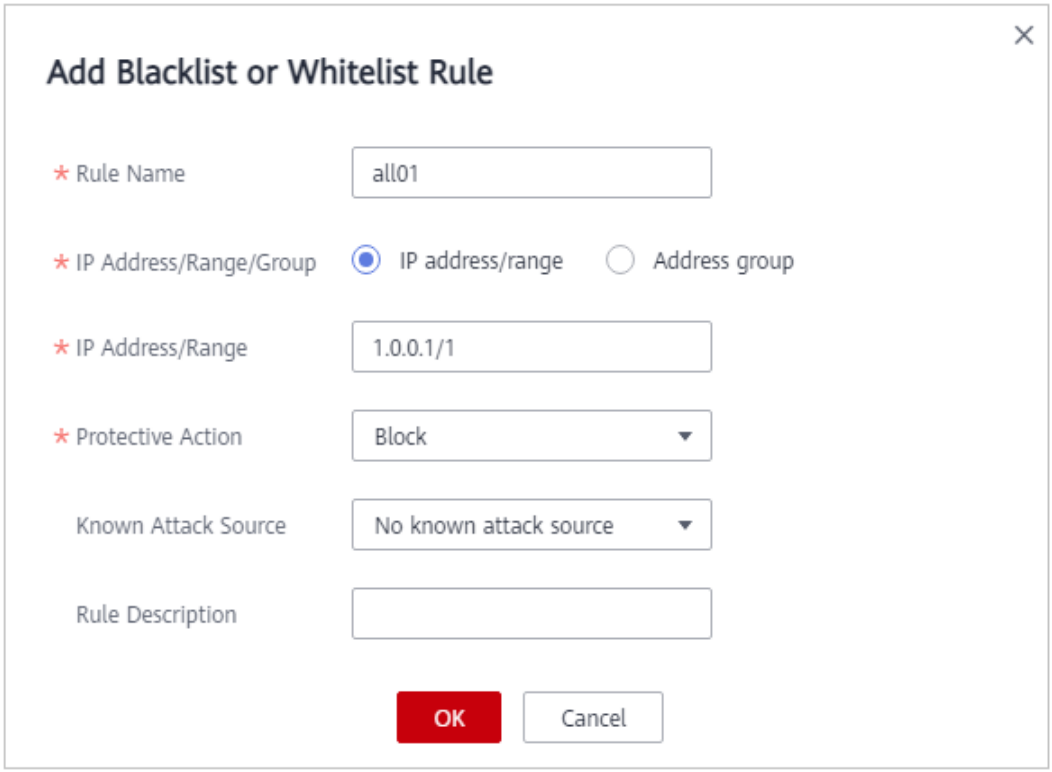
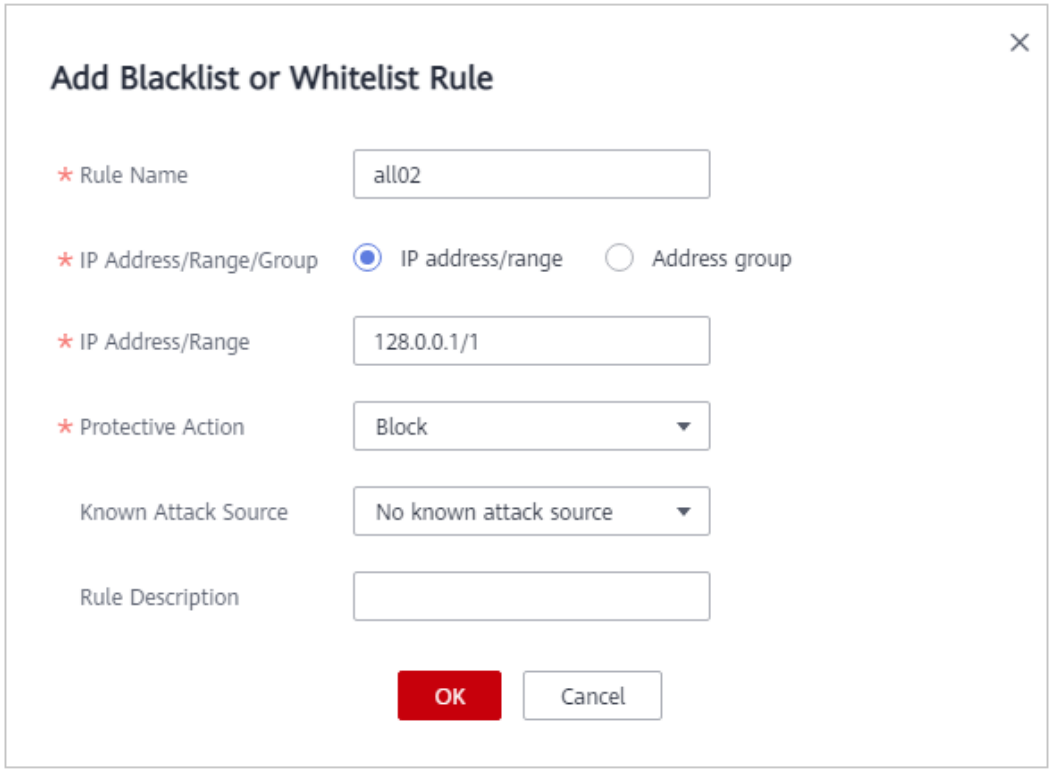
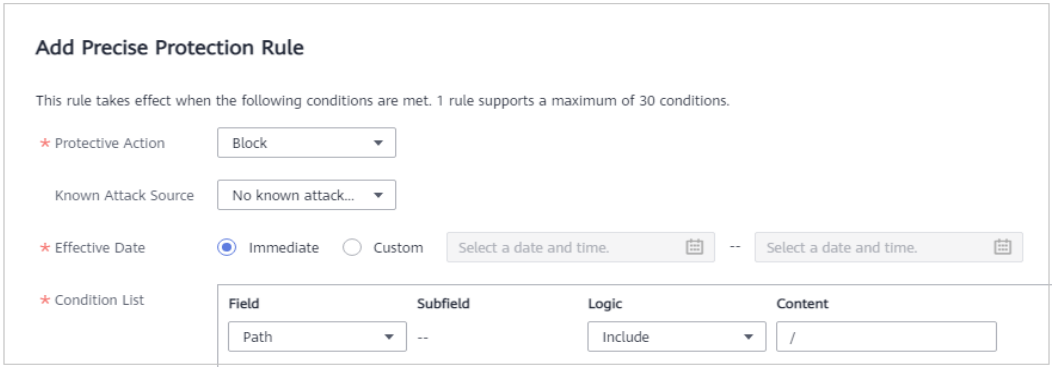


Figura 7-37 Intervalo de endereços IP de bloqueio 128.0.0.0/1



Você também pode adicionar uma regra de proteção precisa para bloquear todas as solicitações de acesso, conforme mostrado na **Figura 7-38**.

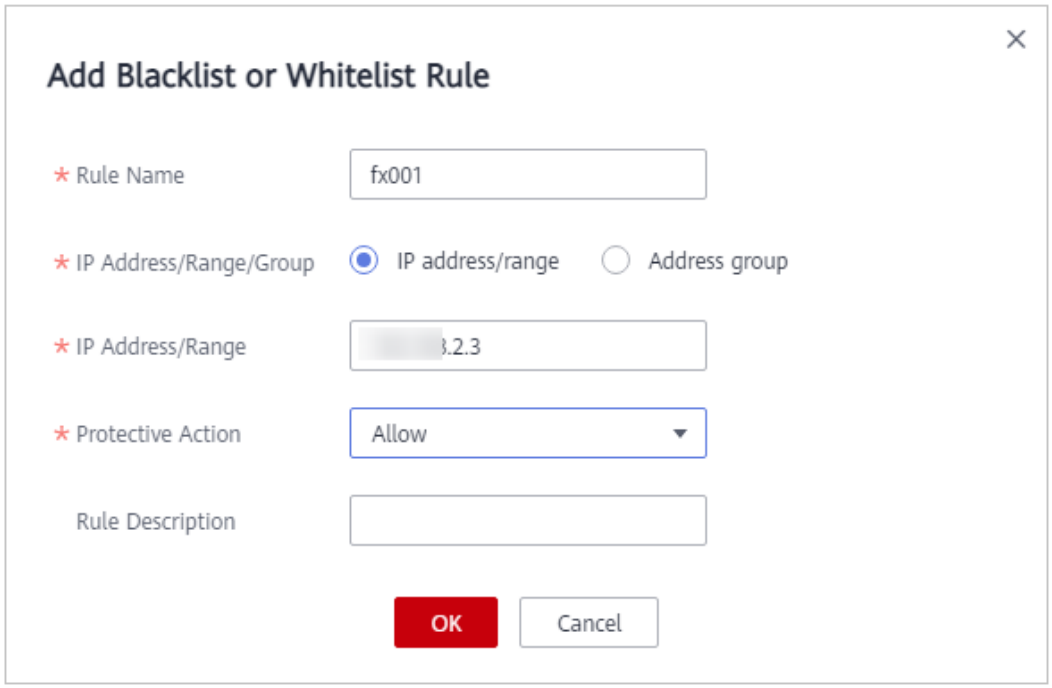
Figura 7-38 Bloquear todas as solicitações de acesso



Para mais detalhes, consulte **Configuração de uma regra de proteção precisa**.

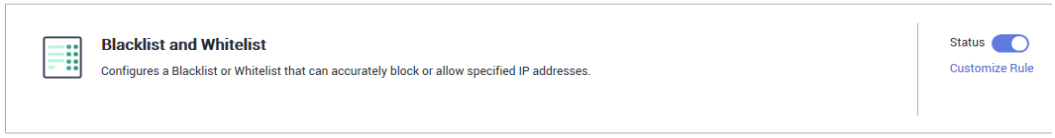
Passo 2 Consulte **Figura 7-39** e adicione uma regra de lista branca para permitir um endereço IP especificado, por exemplo, *XXX.XXX.2.3*.

Figura 7-39 Permitir o acesso a um endereço IP especificado



Passo 3 Ative a proteção branca e de lista negra.

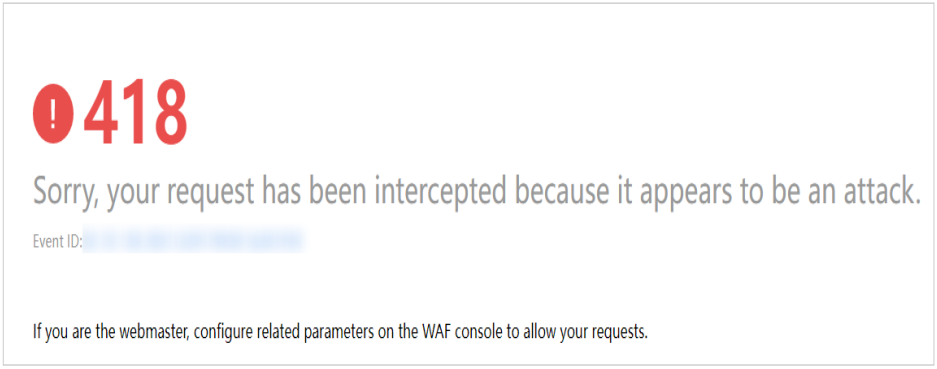
Figura 7-40 Área de configuração Blacklist e Whitelist



Passo 4 Limpe o cache do navegador e acesse o http://www.example.com.

Se o endereço IP de um visitante não for o especificado em **Passo 2**, o WAF bloqueará a solicitação de acesso. **Figura 7-41** mostra um exemplo da página do bloco.

Figura 7-41 Bloquear página



Passo 5 Vá para o console do WAF. No painel de navegação à esquerda, escolha **Events**. Veja o evento na página **Events**.

----Fim

7.8 Configuração de uma regra de origem de ataque conhecido

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. Por exemplo, se uma solicitação maliciosa bloqueada tiver origem em um endereço IP (192.168.1.1) e você definir a duração do bloqueio para 500 segundos, o WAF bloqueará o endereço IP por 500 segundos após a regra de origem de ataque conhecida entrar em vigor.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

- Para que uma regra de origem de ataque conhecida entre em vigor, ela deve ser ativada ao configurar regras básicas de proteção da Web, proteção precisa, lista negra ou lista branca.
- Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.
- Antes de adicionar uma regra de origem de ataque conhecida para solicitações mal-intencionadas bloqueadas por Cookie ou Params, um identificador de tráfego deve ser configurado para o nome de domínio correspondente. Para mais detalhes, veja **Configuração de um identificador de tráfego para uma origem de ataque conhecida**.

Limitações da especificação

- Você pode configurar até seis tipos de bloqueio. Cada tipo pode ter uma regra de origem de ataque conhecida configurada.
- O tempo máximo que um endereço IP pode ser bloqueado é de 30 minutos.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em ☰ no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração **Known Attack Source**, altere o **Status**, se necessário, e clique em **Customize Rule** para ir para a página **Known Attack Source**. Figura 7-42 mostra um exemplo.

Figura 7-42 Configuração de origem de ataque conhecida

Passo 7 No canto superior esquerdo das regras de origem de ataque conhecidas, clique em **Add Known Attack Source Rule**.

Passo 8 Na caixa de diálogo exibida, especifique os parâmetros fazendo referência a Tabela 7-12. Figura 7-43 mostra um exemplo.

Figura 7-43 Adicionar Regra de Origem de Ataque Conhecido

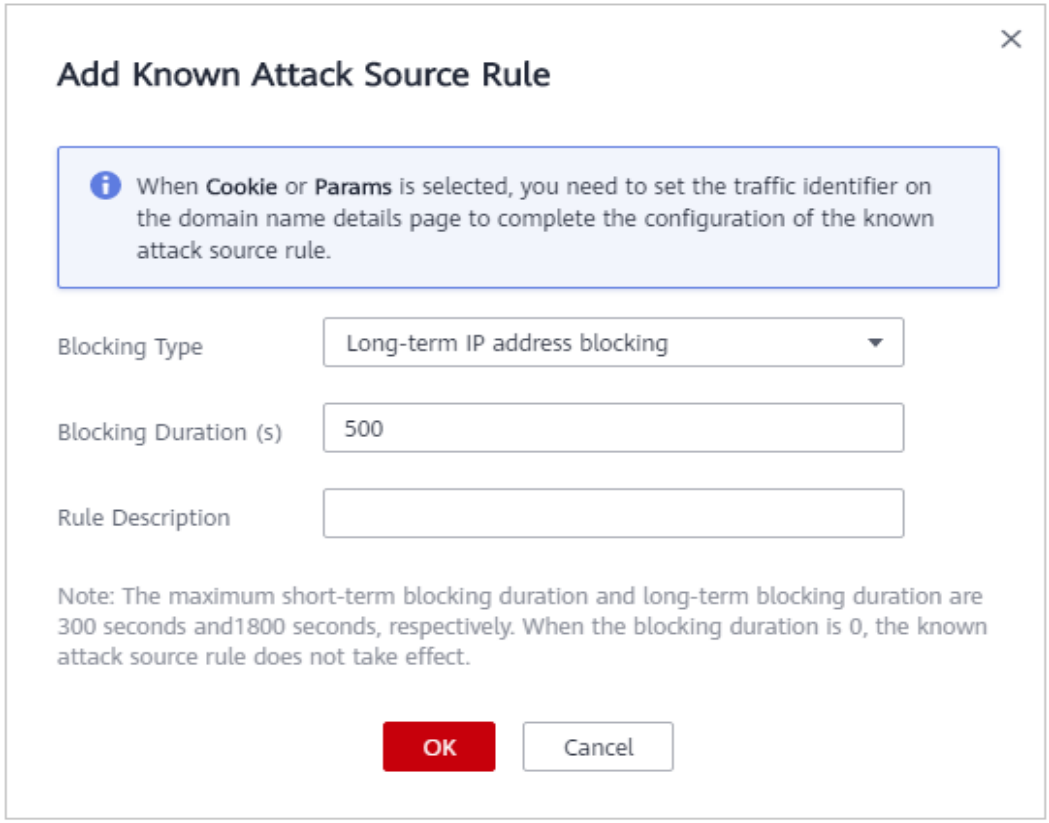
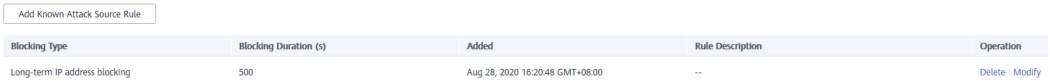


Tabela 7-12 Parâmetros de origem de ataque conhecidos

Parâmetro	Descrição	Valor de exemplo
Tipo de bloqueio	Especifica o tipo de bloqueio. As opções são: ● **Long-term IP address blocking** ● **Short-term IP address blocking** ● **Long-term Cookie blocking** ● **Short-term Cookie blocking** ● **Long-term Params blocking** ● **Short-term Params blocking**	**Long-term IP address blocking**
Duração do Bloqueio (s)	A duração do bloqueio deve ser um número inteiro e variar de: ● (300, 1800] para bloqueio a longo prazo ● (0, 300] para bloqueio de curto prazo	500
Descrição da regra	Uma breve descrição da regra. Este parâmetro é opcional.	Nenh

Passo 9 Clique em **OK** . Em seguida, você pode exibir a regra de origem de ataque conhecida adicionada na lista.

Figura 7-44 Regras de origem de ataque conhecidas



----Fim

Outras operações

- Para modificar uma regra, clique em **Modify** na linha que contém a regra.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

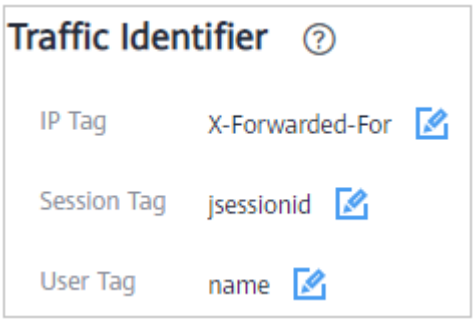
Exemplo de Configuração - Bloqueando Fonte de Ataque Conhecida Identificada por Cookie

Suponha que o nome de domínio *www.example.com* foi conectado ao WAF e um visitante enviou uma ou mais solicitações maliciosas por meio do endereço IP *XXX.XXX.248.195*. Você deseja bloquear solicitações de acesso a partir deste endereço IP e cujo cookie é **jsessionid** por 10 minutos. Consulte as etapas a seguir para configurar uma regra e verificar seu efeito.

Passo 1 Na página **Website Settings**, clique em *www.example.com* para ir para a página de informações básicas.

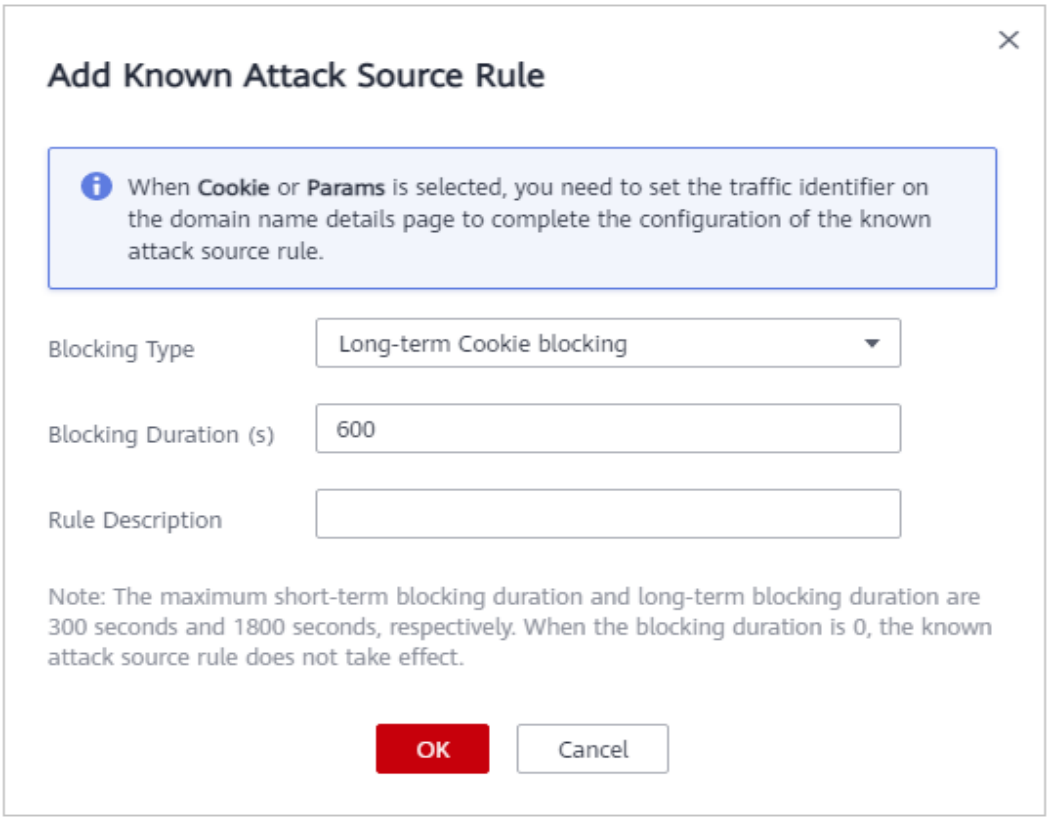
Passo 2 Na área **Traffic Identifier** configure o cookie no campo **Session Tag**.

Figura 7-45 Identificador de tráfego



Passo 3 Adicione uma fonte de ataque conhecida, selecione **Long-term Cookie blocking** para **Blocking Type**, e defina a duração do bloco para 600 segundos.

Figura 7-46 Adicionando uma regra de origem de ataque conhecida baseada em Cookie

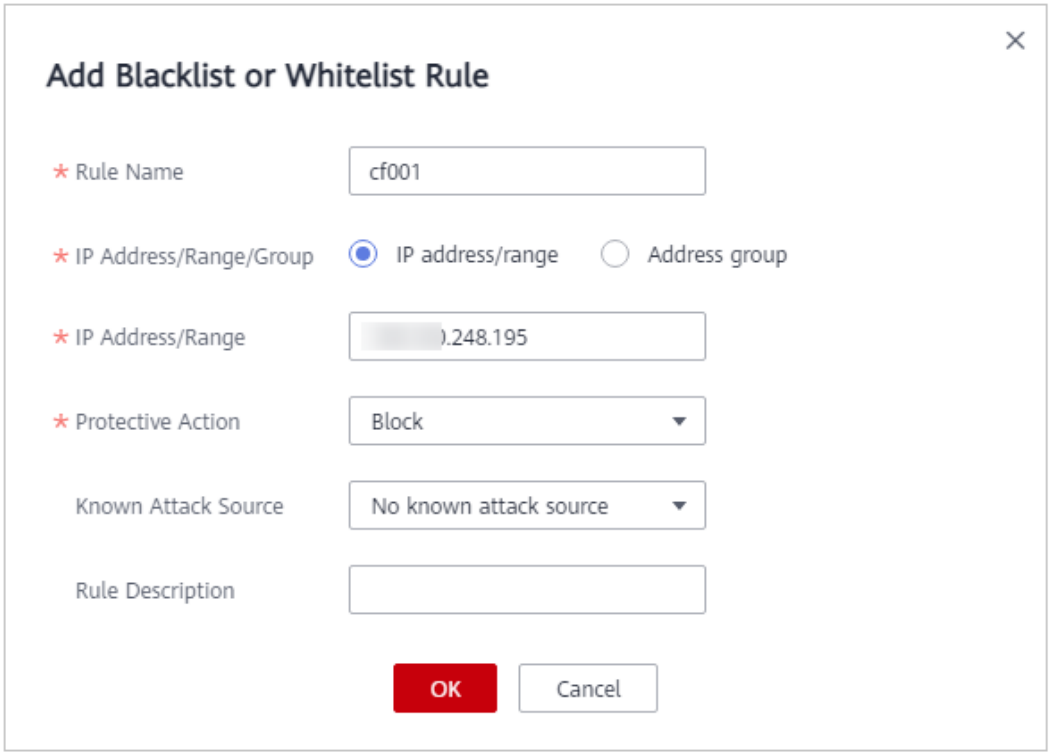


Passo 4 Habilitar a proteção de origem de ataque conhecida.

Figura 7-47 Configuração de origem de ataque conhecida

Passo 5 Adicione uma regra de lista negra e lista branca para bloquear *XXX.XXX.248.195*. Selecione **Long-term Cookie blocking** para **Known Attack Source**.

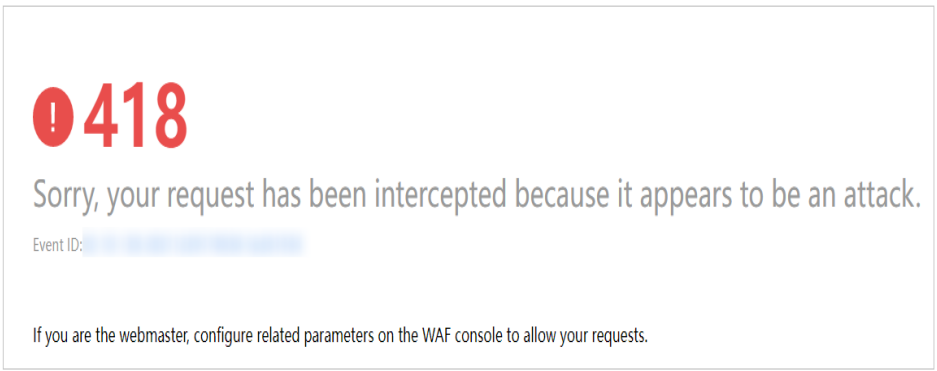
Figura 7-48 Especificando uma regra de origem de ataque conhecida



Passo 6 Limpe o cache do navegador e acesse o http://www.example.com.

Quando uma solicitação do endereço IP *XXX.XXX.248.195*, o WAF bloqueia o acesso. Quando o WAF detecta que o cookie da solicitação de acesso do endereço IP é **jsessionid**, o WAF bloqueia a solicitação de acesso por 10 minutos.

Figura 7-49 Página Bloquear



Passo 7 Acesse o console do WAF. No painel de navegação à esquerda, escolha **Events**. Veja o evento na página **Events**.

Figura 7-50 Exibindo Eventos - Eventos de Origem de Ataque Conhecidos

----Fim

7.9 Configuração de uma regra de controle de acesso de geolocalização

Este tópico descreve como configurar uma regra de controle de acesso de geolocalização. Uma regra de controle de acesso de geolocalização permite controlar endereços de IP encaminhados de ou para países e regiões especificados.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

- Uma região pode ser configurada em apenas uma regra de controle de acesso de geolocalização.
- Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

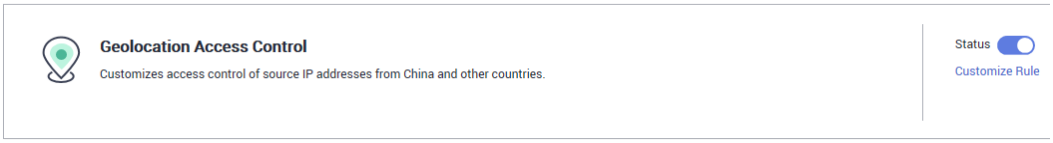
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração do **Geolocation Access Control**, altere o **Status**, se necessário, e clique em **Customize Rule**.

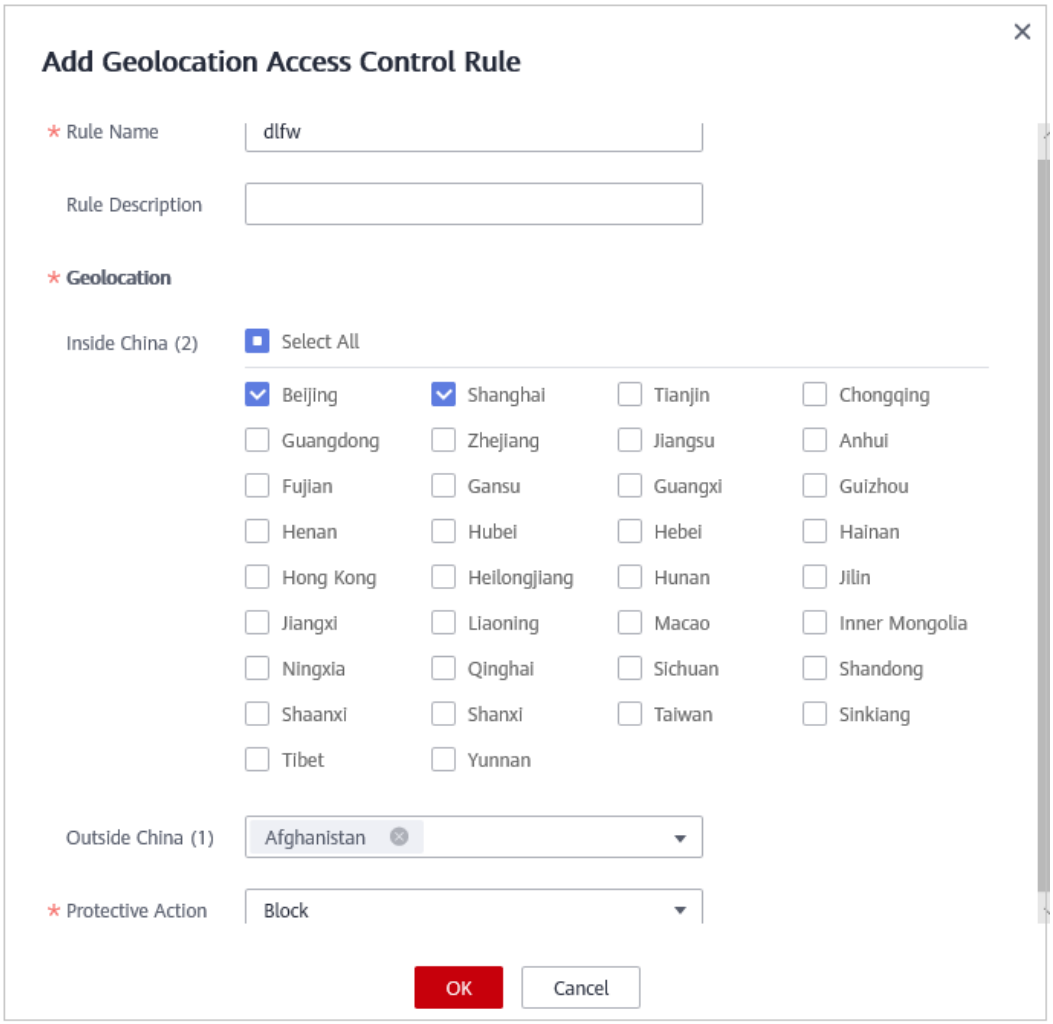
Figura 7-51 Área de configuração do Controle de Acesso de Geolocalização



Passo 7 No canto superior esquerdo da página **Geolocation Access Control**, clique em **Add Rule**.

Passo 8 Na caixa de diálogo exibida, adicione uma regra de controle de acesso de geolocalização fazendo referência a **Tabela 7-13** ou **Tabela 7-14**.

Figura 7-52 Adicionando uma regra de controle de acesso de geolocalização (nova versão)



AVISO

Atualmente, a nova versão da configuração de regra de controle de acesso de geolocalização é suportada apenas nas seguintes regiões:

- CN-Hong Kong
- AP-Bangkok

Figura 7-53 Adicionando uma regra de controle de acesso de geolocalização

Tabela 7-13 Parâmetros de regra (nova versão)

Parâmetro	Descrição	Valor de exemplo
Nome da regra	Nome da regra que você configurou	dlfw
Descrição da regra	Uma breve descrição da regra. Este parâmetro é opcional.	waf
Geolocalizaçã o	Âmbito geográfico do endereço de IP. Você pode selecionar uma região dentro da China ou fora da China.	-
Ação Protetora	Ação que o WAF tomará se a regra for atingida. Você pode selecionar **Block**, **Allow**, ou **Log only**.	**Block**

Tabela 7-14 Parâmetros de regra

Parâmetro	Descrição	Valor de exemplo
Geolocaliza ção	Localização geográfica a partir da qual um endereço IP é originado	Nenh
Ação Protetora	Ação que o WAF tomará se a regra for atingida. Você pode selecionar **Block**, **Allow**, ou **Log only**.	**Block**
Descrição da regra	Uma breve descrição da regra. Este parâmetro é opcional.	Nenhum

Passo 9 Clique em **OK**. Em seguida, você pode exibir a regra adicionada na lista de regras de controle de acesso de geolocalização.

Figura 7-54 Lista de regras de controle de acesso de geolocalização (novo console)

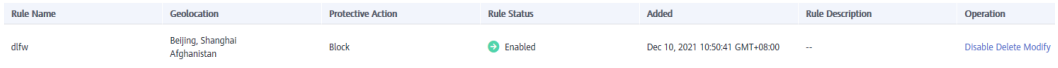
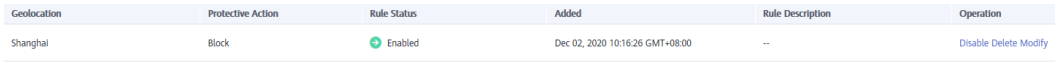


Figura 7-55 Lista de regras de controle de acesso de geolocalização



- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.
- Para modificar uma regra, clique em **Modify** na linha que contém a regra.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

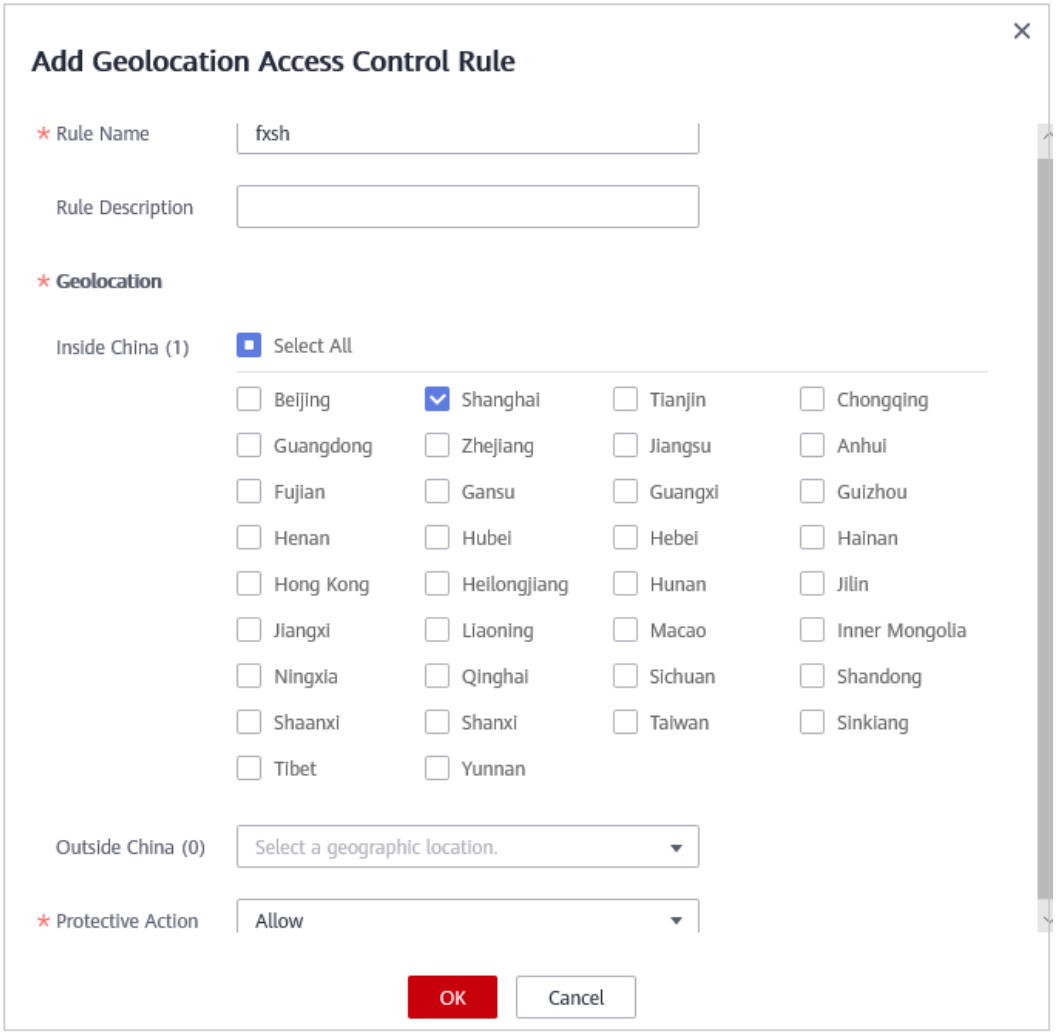
----Fim

Exemplo de configuração - Permitindo solicitações de acesso de endereços IP em uma região especificada

Suponha que o nome de domínio *www.example.com* tenha sido conectado ao WAF e você deseja permitir que apenas endereços IP em Xangai, China, acessem o nome de domínio. Execute as seguintes etapas:

Passo 1 Adicione uma regra de controle de acesso de geolocalização: Selecione **Shanghai** para **Geolocation** e selecione **Allow** para **Protective Action**.

Figura 7-56 Selecionando Permitir Ação Protetora (nova versão)

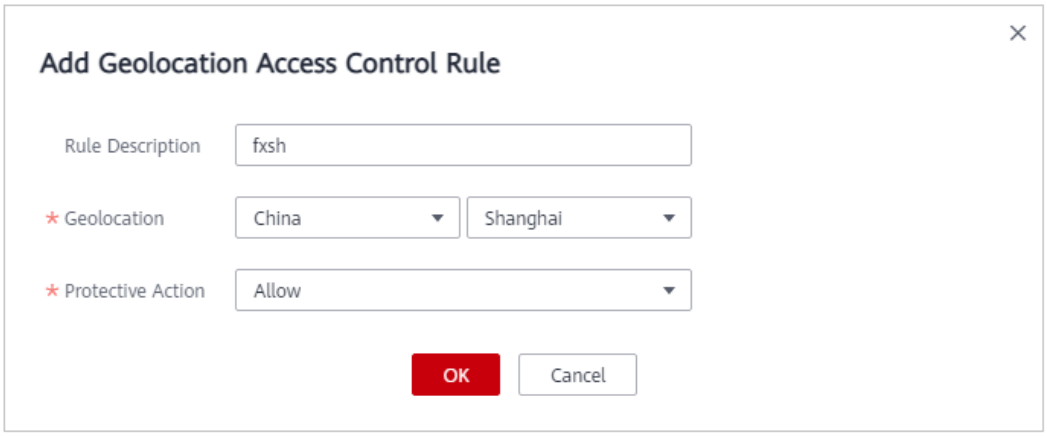


AVISO

Atualmente, a nova versão da configuração de regra de controle de acesso de geolocalização é suportada apenas nas seguintes regiões:

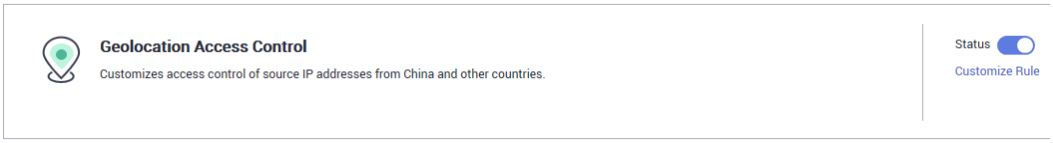
- CN-Hong Kong
- AP-Bangkok

Figura 7-57 Selecionando Permitir Ação Protetora



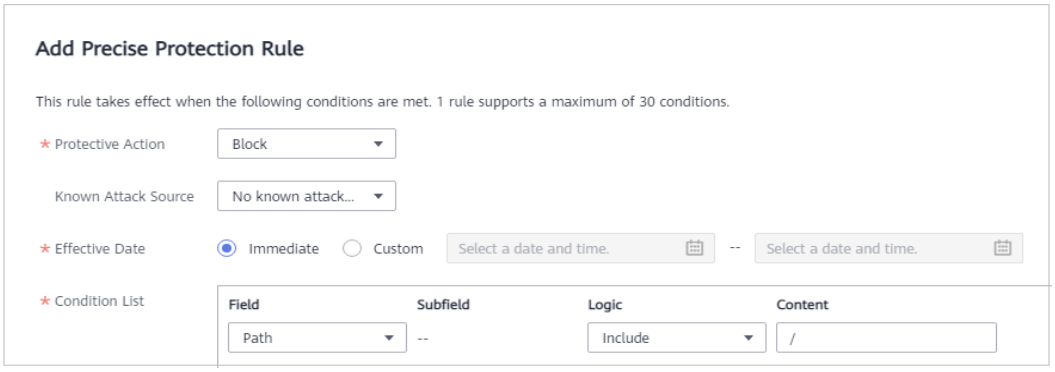
Passo 2 Habilite o controle de acesso de geolocalização.

Figura 7-58 Área de configuração do Controle de Acesso de Geolocalização



Passo 3 Configure uma regra de proteção precisa para bloquear todas as solicitações.

Figura 7-59 Bloquear todas as solicitações de acesso

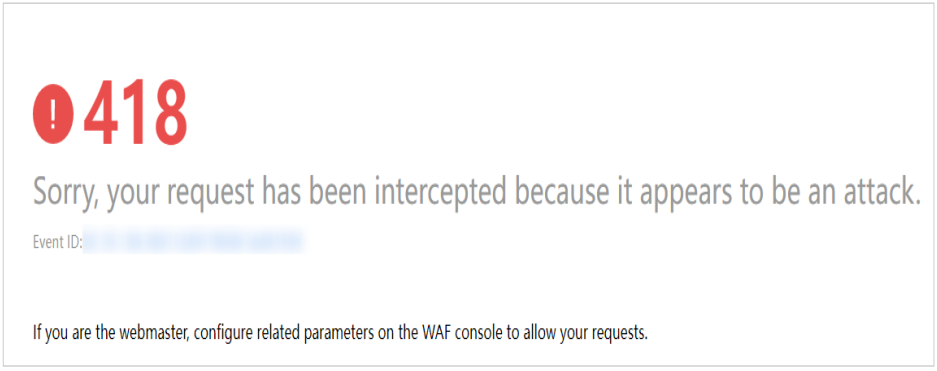


Para mais detalhes, consulte **Configuração de uma regra de proteção precisa**.

Passo 4 Limpe o cache do navegador e acesse o http://www.example.com.

Quando uma solicitação de acesso de endereços IP fora de Xangai acessa a página, o WAF bloqueia a solicitação de acesso. **Figura 7-60** mostra uma página de bloco de exemplo.

Figura 7-60 Bloquear página



Passo 5 Acesse o console do WAF. No painel de navegação à esquerda, escolha **Events**. Veja o evento na página **Events**. Verá que todos os pedidos não provenientes de Xangai foram bloqueados.

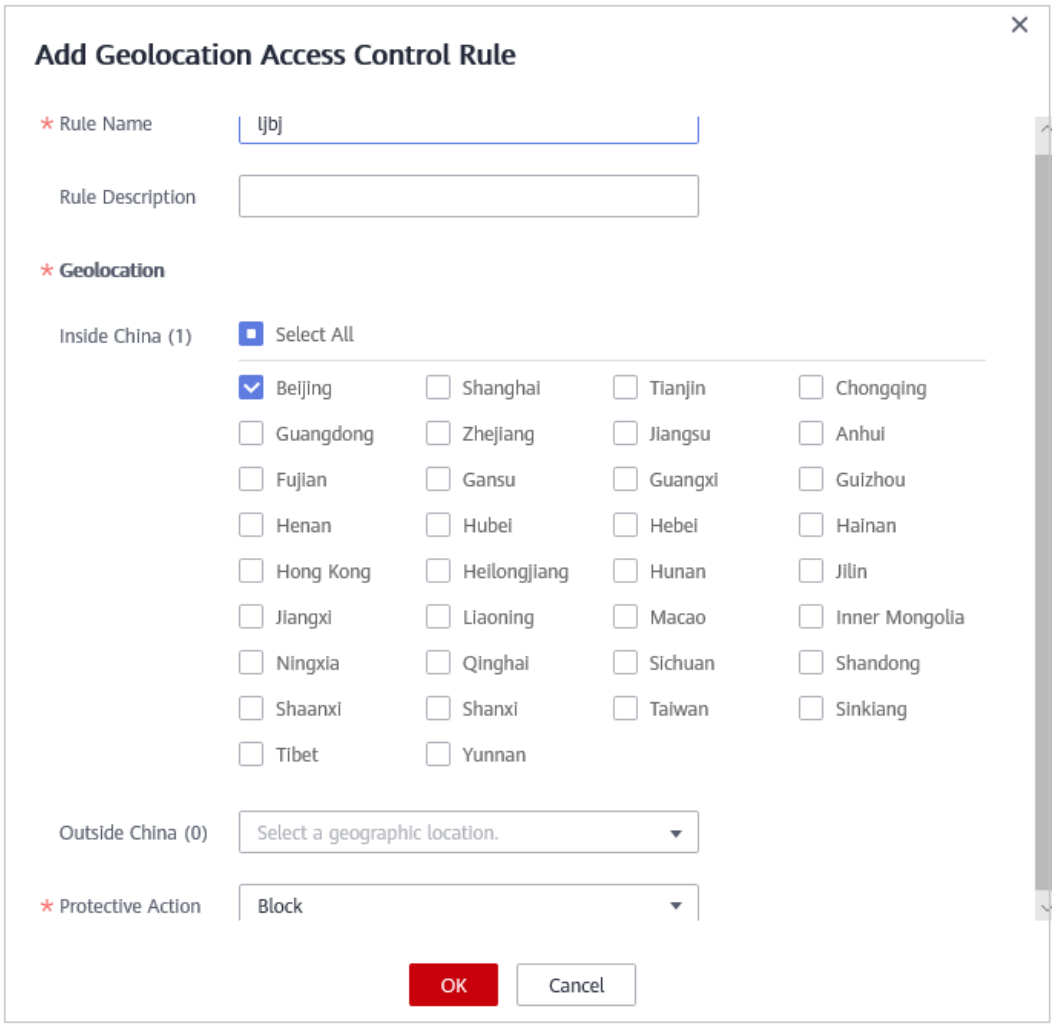
----Fim

Exemplo de configuração - Bloqueando solicitações de acesso de endereços IP em uma região especificada

Suponha que o nome de domínio *www.example.com* foi conectado ao WAF e você deseja bloquear todos os endereços de IP de Pequim para acessar o nome de domínio. A seguir, mostramos como configurar uma regra para esse fim:

Passo 1 Adicione uma regra de controle de acesso de geolocalização, selecione **Beijing** para **Geolocation** e **Block** para **Protective Action**.

Figura 7-61 Bloqueio de solicitações de acesso de uma região específica (nova versão)

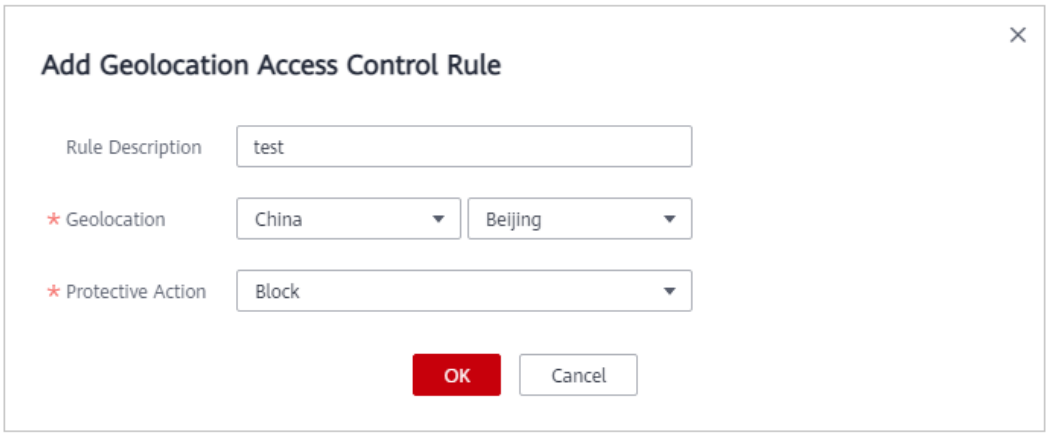


AVISO

Atualmente, a nova versão da configuração de regra de controle de acesso de geolocalização é suportada apenas nas seguintes regiões:

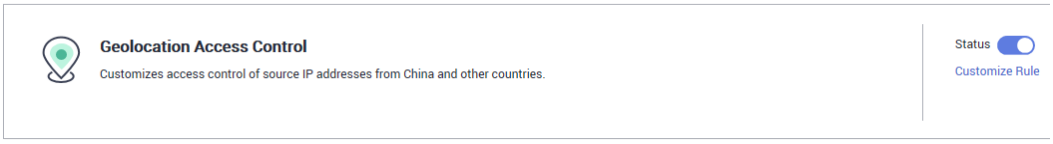
- CN-Hong Kong
- AP-Bangkok

Figura 7-62 Bloqueio de solicitações de acesso de uma região específica



Passo 2 Habilite o controle de acesso de geolocalização.

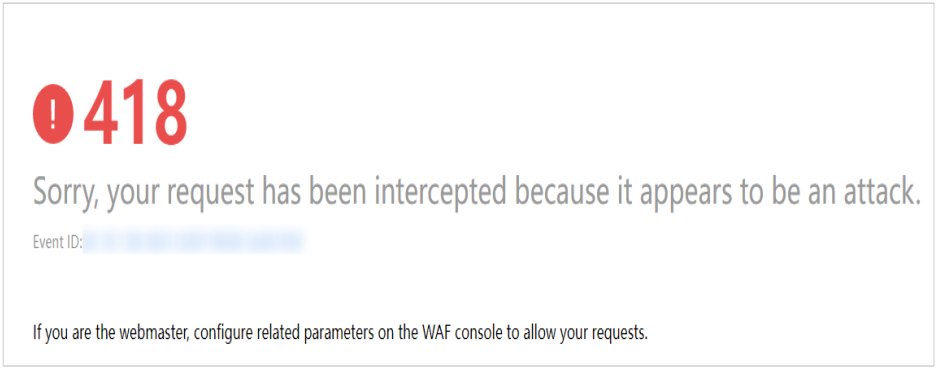
Figura 7-63 Área de configuração do Controle de Acesso de Geolocalização



Passo 3 Limpe o cache do navegador e acesse o http://www.example.com.

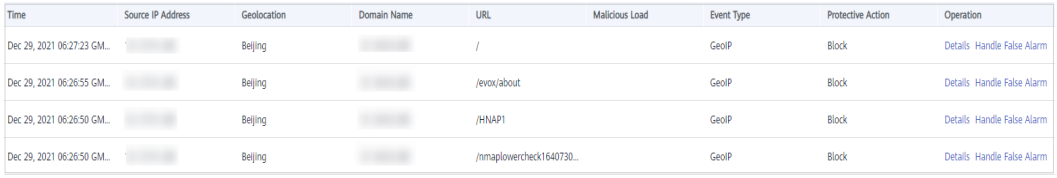
Quando uma solicitação de acesso de endereços de IP dentro de Pequim acessa a página, o WAF bloqueia a solicitação de acesso. **Figura 7-64** mostra uma página de bloco de exemplo.

Figura 7-64 Bloquear página



Passo 4 Acesse o console do WAF. No painel de navegação à esquerda, escolha **Events**. Veja o evento na página **Events**.

Figura 7-65 Exibição de eventos - bloqueando solicitações de acesso de endereços IP em uma região



----Fim

7.10 Configuração de uma regra de proteção contra adulteração da Web

O WAF pode armazenar em cache a configuração de páginas da Web estáticas de sites. Depois de configurar uma regra de proteção contra violação da Web, o WAF pode:

- Retornar diretamente a página da web em cache para o visitante normal da web para acelerar a resposta da solicitação.
- Devolva as páginas da Web originais em cache para os visitantes se um invasor adulterou as páginas da Web estáticas. Isso garante que os visitantes do seu site sempre obtenham as páginas da web certas.
- Proteja todos os recursos no caminho da página da Web. Por exemplo, se uma regra de proteção contra adulteração da Web estiver configurada para página estática **www.example.com/admin**, o WAF protegerá todos os recursos no diretório **/admin**.

  Portanto, se o URL no valor do cabeçalho da solicitação **Referer** for o mesmo que o caminho anti-tamper configurado, por exemplo, **/admin**, todos os recursos (recursos que terminam com png, jpg, jpeg, gif, bmp, css ou js) atingidos pela solicitação também são armazenados em cache.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.

AVISO

Verifique se a resposta do servidor de origem contém o cabeçalho de resposta **Content-Type** ou o WAF pode falhar ao armazenar em cache a resposta do servidor de origem.

Cenários de aplicação

- Resposta mais rápida aos pedidos

  Depois que uma regra de proteção contra violação da Web é configurada, o WAF armazena em cache páginas da Web estáticas no servidor. Ao receber uma solicitação de um visitante da Web, o WAF retorna diretamente a página da Web em cache para o visitante da Web.

- Proteção contra adulteração na Web

  Se um invasor modificar uma página da Web estática no servidor, o WAF ainda retornará a página da Web original em cache para os visitantes. Os visitantes nunca veem as páginas que foram adulteradas.

  O WAF extrai aleatoriamente solicitações de um visitante para comparar a página recebida com a página no servidor. Se o WAF detectar que a página foi adulterada, ele o notificará por SMS ou e-mail, dependendo do que você configurar. Para mais detalhes, veja **Ativação de notificações de alarme**.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

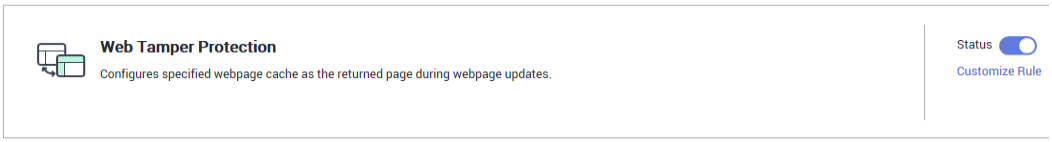
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração da **Web Tamper Protection**, altere o **Status**, se necessário, e clique em **Customize Rule** para acessar a página **Web Tamper Protection**.

Figura 7-66 Área de configuração Web Tamper Protection



Passo 7 No canto superior esquerdo da página **Web Tamper Protection**, clique em **Add Rule**.

Passo 8 Na caixa de diálogo exibida, especifique os parâmetros referindo-se a **Tabela 7-15**.

Figura 7-67 Adicionando uma regra de proteção contra adulteração da Web

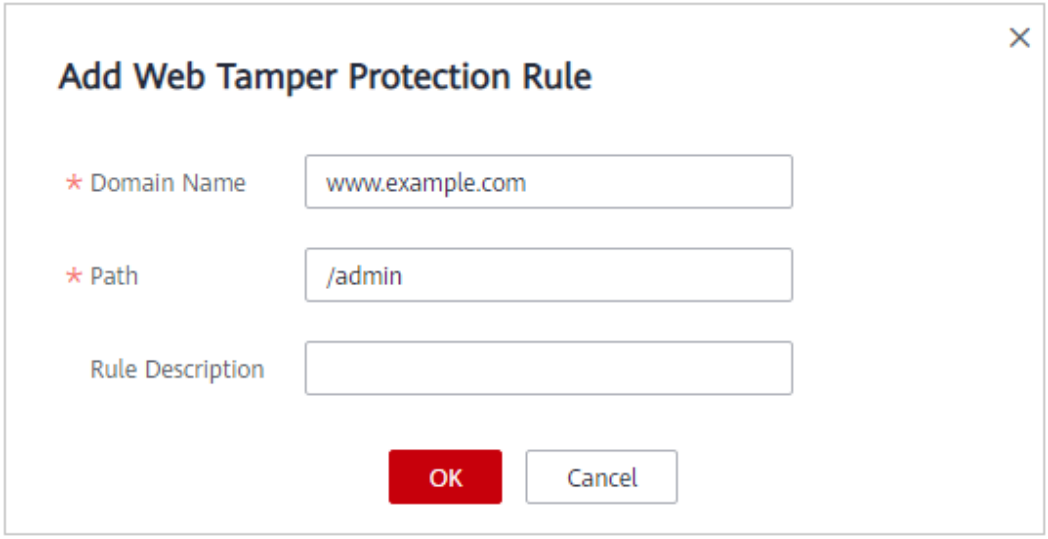


Tabela 7-15 Parâmetros de regra

Parâmetro	Descrição	Valor de exemplo
Nome de domínio	Nome de domínio do site a ser protegido	**www.example.com**
Caminho	Uma parte do URL, não incluindo o nome de domínio Um URL é usado para definir o endereço de uma página da web. O formato básico de URL é o seguinte: Nome do protocolo://nome do domínio ou endereço IP[:Porta]/[Caminho/.../Nome do arquivo]. Por exemplo, se o URL for **http://www.example.com/admin**, defina **Path** como **/admin**. **NOTA** ● O caminho não suporta expressões regulares. ● O caminho não pode conter duas ou mais barras consecutivas. Por exemplo, ///**admin**. Se você digitar ///**admin**, o WAF converterá ///para /.	**/admin**
Descrição da regra	Uma breve descrição da regra. Este parâmetro é opcional.	Nenh

Passo 9 Clique em **OK**. Você pode exibir a regra na lista de regras de proteção contra adulteração da Web.

Figura 7-68 Lista de regras de proteção contra violação da Web

----Fim

Outras Operações

- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.
- Para atualizar o cache de uma página da Web protegida, clique em **Update Cache** na linha que contém a regra de proteção contra adulteração da Web correspondente. Se a regra não for atualizada, o WAF retornará a página recentemente armazenada em cache, mas não a página mais recente.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

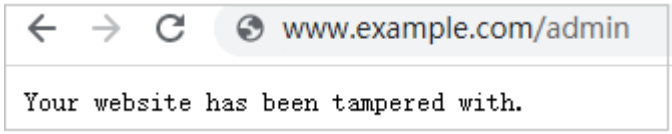
Exemplo de configuração - Prevenção de adulteração de página da Web estática

Para verificar se o WAF está protegendo uma página estática **/admin** no seu site **www.example.com** de ser adulterada:

Passo 1 Use um navegador para acessar o **http://www.example.com/admin**.

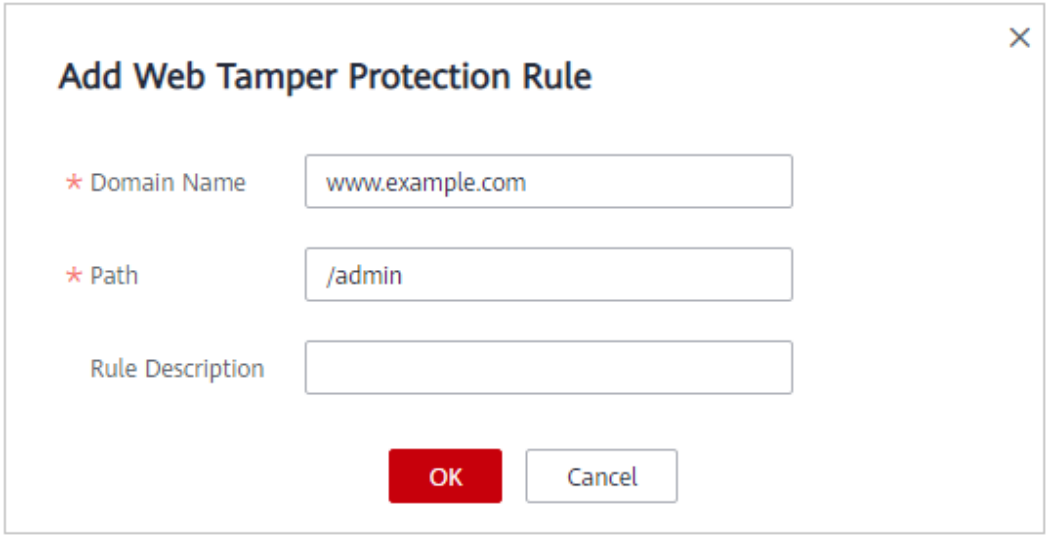
Uma página adulterada é retornada.

Figura 7-69 Uma página estática que foi adulterada



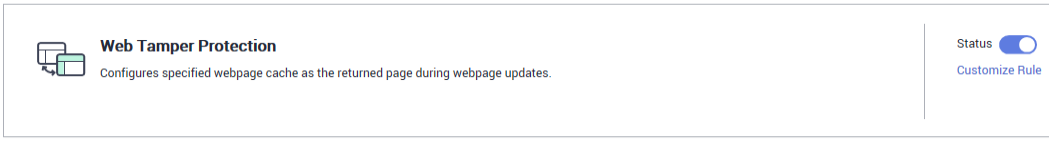
Passo 2 Adicione uma regra de prevenção contra adulteração da Web ao WAF.

Figura 7-70 Adicionando uma regra de proteção contra adulteração da Web



Passo 3 Habilitando o WTP

Figura 7-71 Área de configuração Web Tamper Protection



Passo 4 Use um navegador para acessar o **http://www.example.com/admin**. O WAF armazenará a página em cache.

Passo 5 Acesse o **http://www.example.com/admin** novamente.

A página intacta é retornada.

----Fim

7.11 Configuring Anti-Crawler Rules

You can configure website anti-crawler protection rules to protect against search engines, scanners, script tools, and other crawlers, and use JavaScript to create custom anti-crawler protection rules.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Constraints

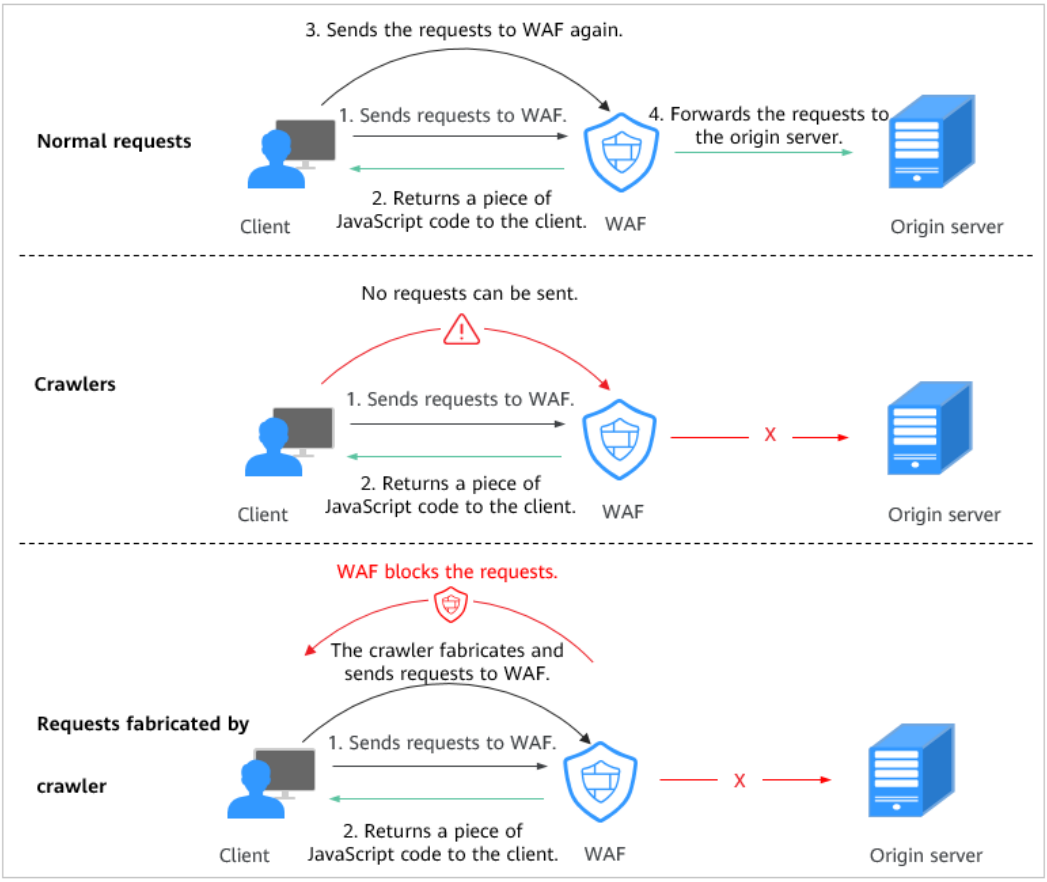
- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.

  CDN caching may impact JS anti-crawler performance and page accessibility.
- The JavaScript anti-crawler function is unavailable for pay-per-use WAF instances.
- This function is unavailable in the standard edition, formerly professional edition.
- Currently, the JavaScript anti-crawler is supported in CN-Hong Kong and AP-Bangkok regions.
- WAF only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.
- WAF JavaScript-based anti-crawler rules only check GET requests and do not check POST requests.

How JavaScript Anti-Crawler Protection Works

Figura 7-72 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figura 7-72 JavaScript Anti-Crawler protection process

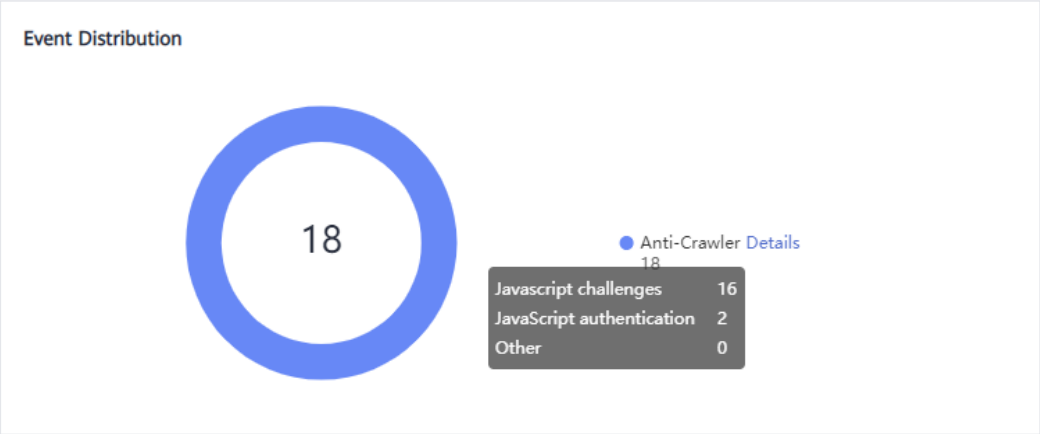


If JavaScript anti-crawler is enabled when a client sends a request, WAF returns a piece of JavaScript code to the client.

- If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification.
- If the client is a crawler, it cannot be triggered by the received JavaScript code and will not send a request to WAF again. The client fails JavaScript authentication.
- If a client crawler fabricates a WAF authentication request and sends the request to WAF, the WAF will block the request. The client fails JavaScript authentication.

By collecting statistics on the number of JavaScript challenges and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. In Figura 7-73, the JavaScript anti-crawler has logged 18 events, 16 of which are JavaScript challenge responses, and 2 of which are JavaScript authentication responses. **Others** is the number of WAF authentication requests fabricated by the crawler.

Figura 7-73 Parameters of a JavaScript anti-crawler protection rule



AVISO

WAF only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.

Procedure

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

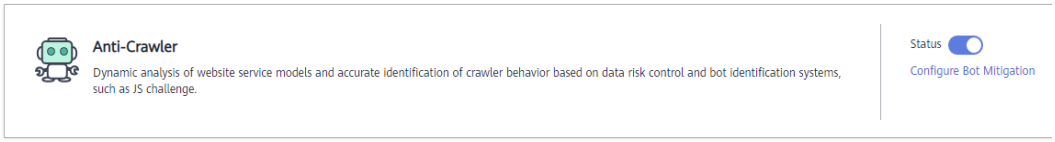
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 In the **Anti-Crawler** configuration area, enable anti-crawler using the toggle on the right, as shown in **Figura 7-74**. If you enable this function, click **Configure Bot Mitigation**.

Figura 7-74 Anti-Crawler configuration area



Passo 7 Select the **Feature Library** tab and enable the protection by referring to **Tabela 7-16**. **Figura 7-75** shows an example.

A feature-based anti-crawler rule has two protective actions:

- **Block**

  WAF blocks and logs detected attacks.

- **Log only**

  Detected attacks are logged only. This is the default protective action.

Scanner is enabled by default, but you can enable other protection types if needed.

Figura 7-75 Feature Library

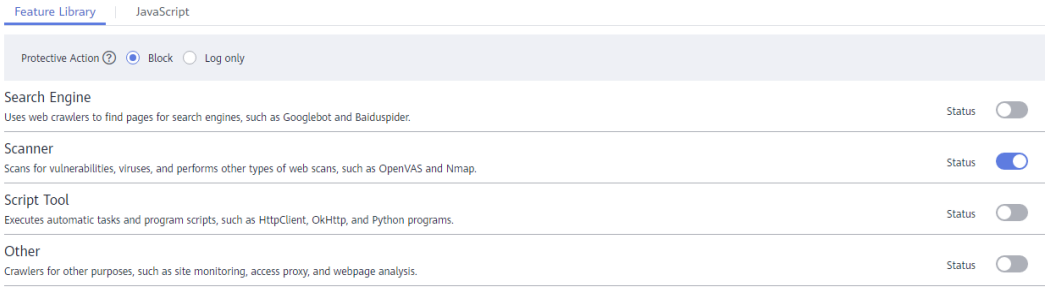


Tabela 7-16 Anti-crawler detection features

Type	Description	Remarks
Search Engine	This rule is used to block web crawlers, such as Googlebot and Baiduspider, from collecting content from your site.	If you enable this rule, WAF detects and blocks search engine crawlers. **NOTA** If **Search Engine** is not enabled, WAF does not block POST requests from Googlebot or Baiduspider. If you want to block POST requests from Baiduspider, use the configuration described in **Configuration Example - Search Engine**.
Scanner	This rule is used to block scanners, such as OpenVAS and Nmap. A scanner scans for vulnerabilities, viruses, and other jobs.	After you enable this rule, WAF detects and blocks scanner crawlers.
Script Tool	This rule is used to block script tools. A script tool is often used to execute automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs.	If you enable this rule, WAF detects and blocks the execution of automatic tasks and program scripts. **NOTA** If your application uses scripts such as HttpClient, OkHttp, and Python, disable **Script Tool**. Otherwise, WAF will identify such script tools as crawlers and block the application.

Type	Description	Remarks
Other	This rule is used to block crawlers used for other purposes, such as site monitoring, using access proxies, and web page analysis. **NOTA** To avoid being blocked by WAF, crawlers may use a large number of IP address proxies.	If you enable this rule, WAF detects and blocks crawlers that are used for various purposes.

Passo 8 Select the **JavaScript** tab and configure **Status** and **Protective Action**.

JavaScript anti-crawler is disabled by default. To enable it, click  and click **Confirm** in the displayed dialog box.  indicates that the JavaScript anti-crawler is enabled.

AVISO

- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.

  CDN caching may impact JS anti-crawler performance and page accessibility.

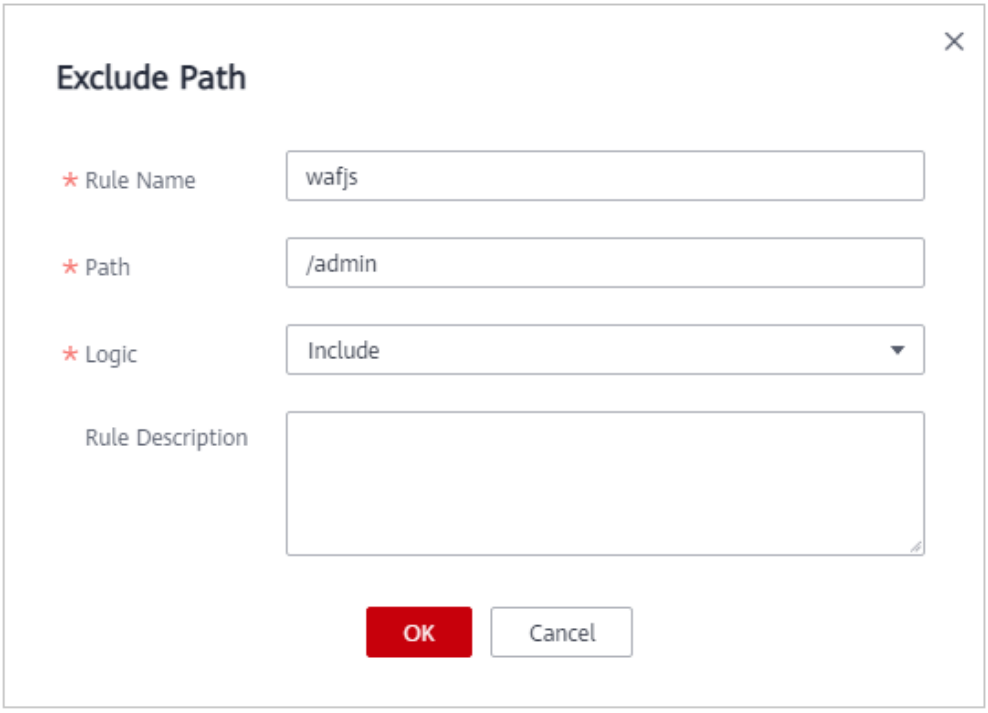
Passo 9 Configure a JavaScript-based anti-crawler rule by referring to **Tabela 7-17**.

Two protective actions are provided: **Protect all paths** and **Protect a specified path**.

- To protect all paths except a specified path

  Select **Protect all paths**, but then in the upper left corner of the page, click **Exclude Path**. Configure the required parameters in the displayed dialog box and click **OK**.

Figura 7-76 Exclude Path



- To protect a specified path only

  Select **Protect a specified path**. In the upper left corner of the page, click **Add Path**. In the displayed dialog box, configure required parameters and click **OK**.

Figura 7-77 Add Path

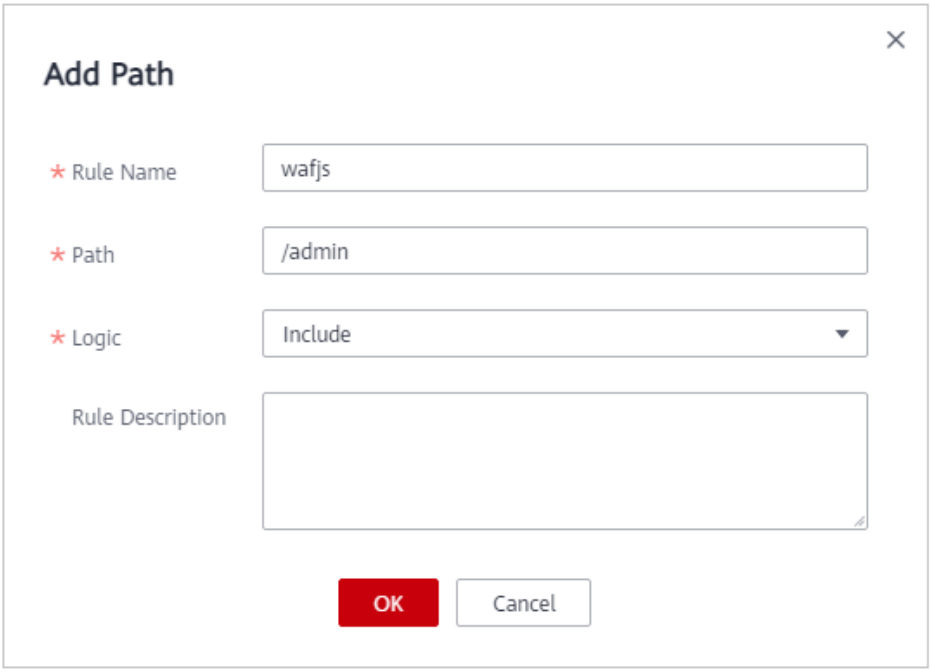


Tabela 7-17 Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule	wafjs
Path	A part of the URL, not including the domain name A URL is used to define the address of a web page. The basic URL format is as follows: Protocol name://Domain name or IP address[:Port]/[Path/.../File name]. For example, if the URL is **http://www.example.com/admin**, set **Path** to **/admin**. **NOTA** • The path does not support regular expressions. • The path cannot contain two or more consecutive slashes. For example, /// **admin**. If you enter /// **admin**, WAF converts /// to /.	/admin
Logic	Select a logical relationship from the drop-down list.	Include
Rule Description	A brief description of the rule.	None

----Fim

Other Operations

- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

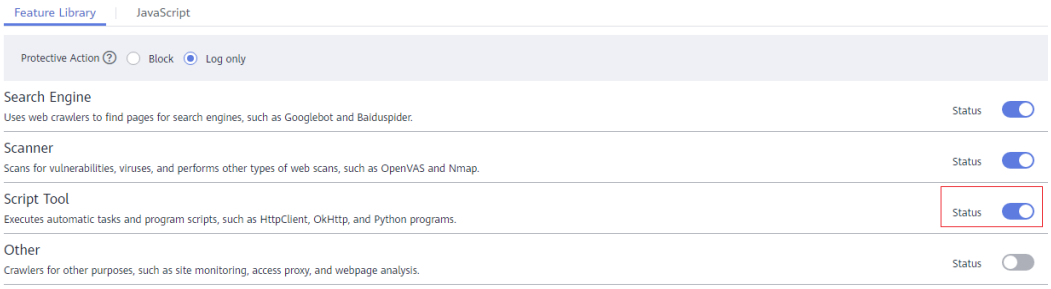
Configuration Example - Logging Script Crawlers Only

To verify that WAF is protecting domain name **www.example.com** against an anti-crawler rule:

Passo 1 Execute a JavaScript tool to crawl web page content.

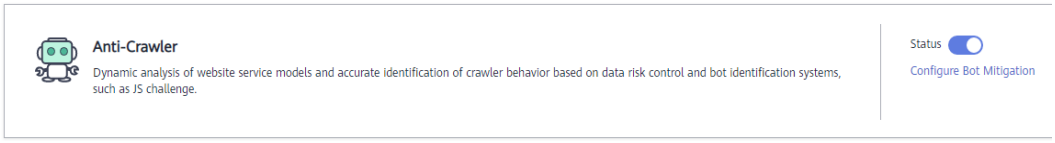
Passo 2 On the **Feature Library** tab, enable **Script Tool** and select **Log only** for **Protective Action**. (If WAF detects an attack, it logs the attack only.)

Figura 7-78 Enabling Script Tool



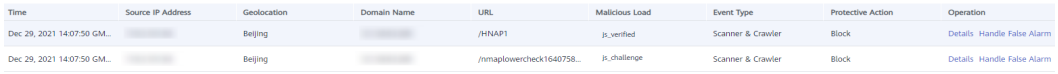
Passo 3 Enable anti-crawler protection.

Figura 7-79 Anti-Crawler configuration area



Passo 4 In the navigation pane on the left, choose **Events** to go to the **Events** page.

Figura 7-80 Viewing Events - Script crawlers



----Fim

Configuration Example - Search Engine

The following shows how to allow the search engine of Baidu or Google and block the POST request of Baidu.

Passo 1 Set **Status** of **Search Engine** to  by referring to the instructions in **Passo 6**.

Passo 2 Configure a precise protection rule by referring to **Configuração de uma regra de proteção precisa**, as shown in **Figura 7-81**.

Figura 7-81 Blocking POST requests

----Fim

7.12 Configuração de uma regra de prevenção de vazamento de informações

Você pode adicionar dois tipos de regras de prevenção de vazamento de informações.

- Filtragem de informações confidenciais: impede a divulgação de informações confidenciais (como números de identificação, números de telefone e endereços de e-mail).
- Interceptação de código de resposta: bloqueia os códigos de status HTTP especificados.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

Esta função não está incluída na standard edition, anteriormente edição profissional.

Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

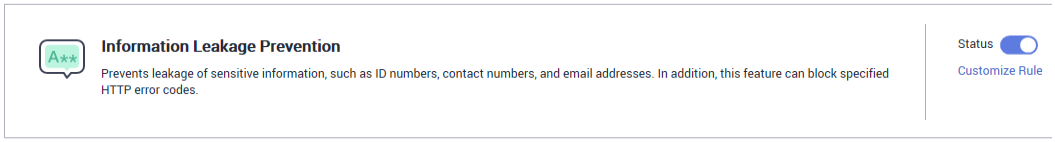
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração da **Information Leakage Prevention**, altere o **Status**, se necessário, e clique em **Customize Rule**.

Figura 7-82 Área de configuração da prevenção de vazamento de informações



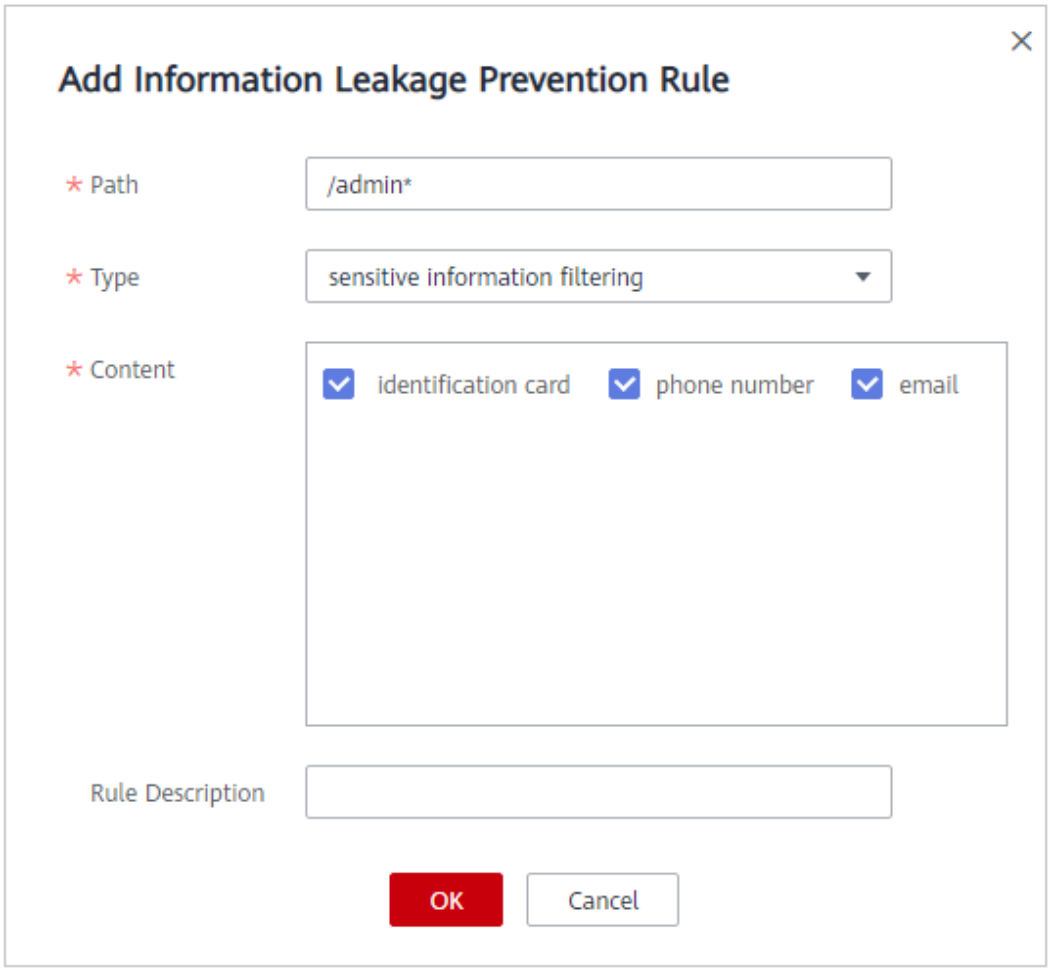
Passo 7 No canto superior esquerdo da página **Information Leakage Prevention**, clique em **Add Rule**.

Passo 8 Na caixa de diálogo exibida, adicione uma regra de prevenção de vazamento de informações consultando **Tabela 7-18**. **Figura 7-83** e **Figura 7-84** mostrar dois exemplos.

As regras de prevenção de vazamento de informações impedem que informações confidenciais (como números de identificação, números de telefone e endereços de e-mail) sejam divulgadas. Esse tipo de regra também pode bloquear códigos de status HTTP especificados.

sensitive information filtering: Configure regras para mascarar informações confidenciais, como números de telefone e números de identificação, de páginas da Web. Por exemplo, você pode definir as seguintes regras de proteção para mascarar informações confidenciais, como números de identificação, números de telefone e endereços de email:

Figura 7-83 Vazamento de informações sensíveis



response code interception: Uma página de erro de um código de resposta HTTP específico pode conter informações confidenciais. Você pode configurar regras para bloquear essas páginas de erro para evitar que essas informações sejam vazadas. Por exemplo, você pode definir a regra a seguir para bloquear páginas de erro dos códigos de resposta HTTP 404, 502 e 503 especificados.

Figura 7-84 Bloqueio de códigos de resposta

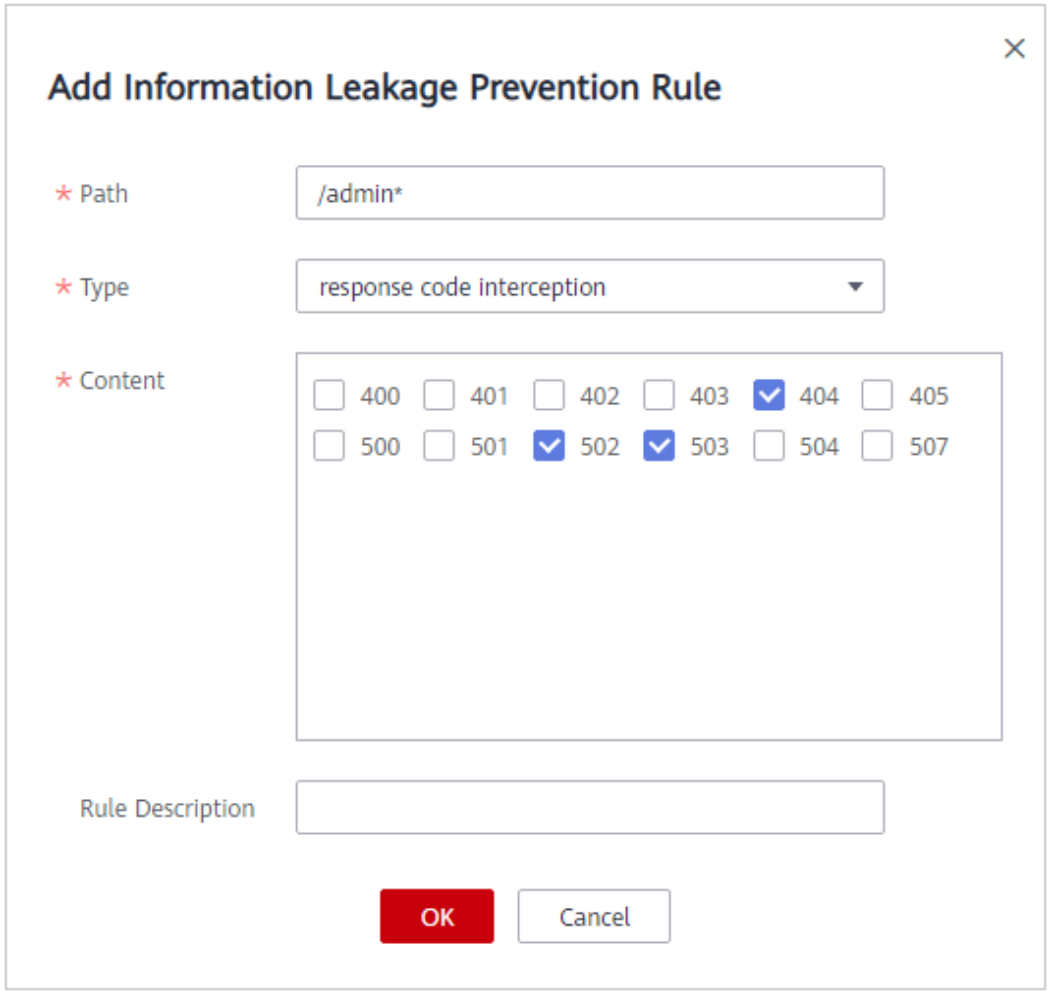
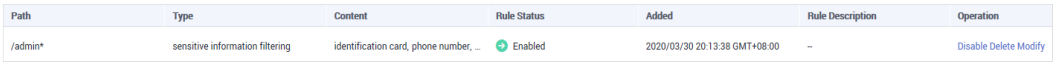


Tabela 7-18 Parâmetros de regra

Parâmetro	Descrição	Valor de exemplo
Caminho	Uma parte do URL que não inclui o nome de domínio. O URL pode conter informações confidenciais (como números de identificação, números de telefone e endereços de e-mail) ou um código de erro bloqueado. ● Correspondência de prefixo: Somente o prefixo do caminho a ser inserido deve corresponder ao do caminho a ser protegido. Se o caminho a ser protegido é **/admin**, Definir **Path** para **/admin***. ● Correspondência exata: O caminho a ser inserido deve corresponder ao caminho a ser protegido. Se o caminho a ser protegido é **/admin**, Definir **Path** para **/admin**. **NOTA** – O caminho suporta apenas correspondências de prefixo e exato. Expressões regulares não são suportadas. – O caminho não pode conter duas ou mais barras consecutivas. Por exemplo, ///**admin**. Se você digitar ///**admin**, o mecanismo WAF converterá /// para /.	**/admin***
Tipo	● **sensitive information filtering** ● **response code interception**: Ative o WAF para bloquear a página de código de resposta HTTP especificada.	**sensitive information filtering**
Conteúdo	Informação a ser protegida. As opções são **identification card**, **phone number**, e **email**.	**identification card**
Descrição da regra	Uma breve descrição da regra. Este parâmetro é opcional.	Nenh

Passo 9 Clique em **OK**. A regra de prevenção de vazamento de informações adicionadas é exibida na lista de regras de prevenção de vazamento de informações.

Figura 7-85 Lista de regras de prevenção de fugas de informação



----Fim

Outras Operações

- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.

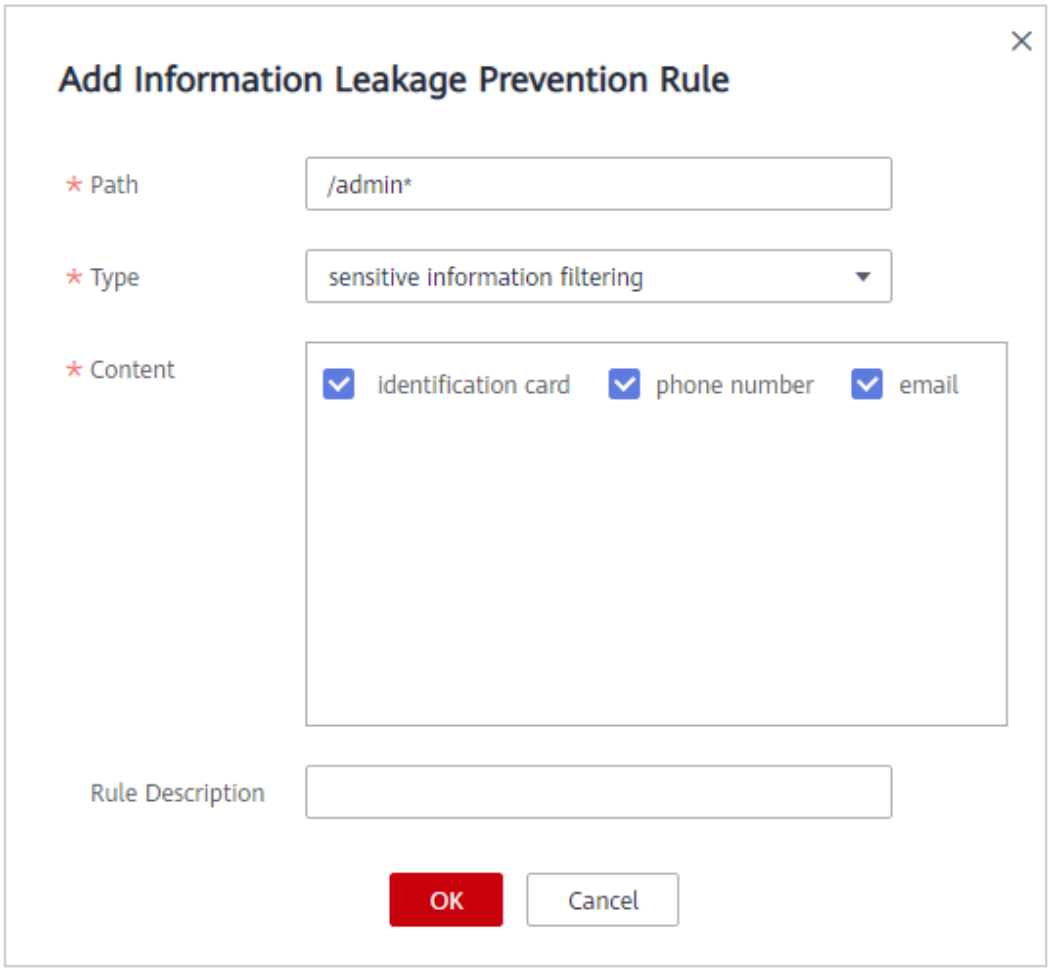
- Para modificar uma regra, clique em **Modify** na linha que contém a regra.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

Exemplo de Configuração - Mascarando Informações Sensíveis

Para verificar se o WAF está protegendo seu nome de domínio *www.example.com* contra uma regra de prevenção de vazamento de informações:

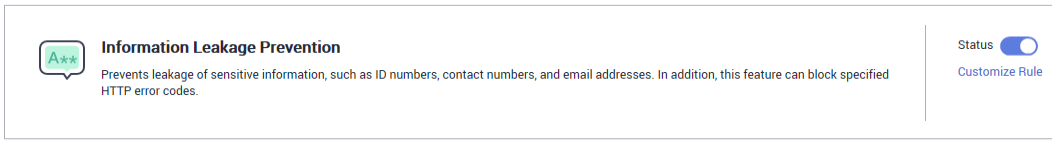
Passo 1 Adicione uma regra de prevenção de vazamento de informações.

Figura 7-86 Vazamento de informações sensíveis



Passo 2 Possibilitando a prevenção de vazamento de informações.

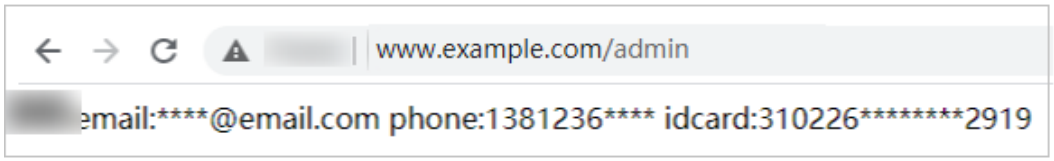
Figura 7-87 Área de configuração da prevenção de vazamento de informações



Passo 3 Limpe o cache do navegador e acesse o http://www.example.com/admin/.

O endereço de e-mail, número de telefone e número de identidade na página retornada são mascarados.

Figura 7-88 Informação sensível mascarada



----Fim

7.13 Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule

When WAF detects a malicious attack that matches the basic web protection rule or custom rules you configure, it processes the attack event based on the protective action in the hit rule.

You can add false alarm masking rules to let WAF ignore certain rule IDs or event types (for example, skip XSS checks for a specific URL).

- If you select **All protection** for **Ignore WAF Protection**, all WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.
- If you select **Basic Web Protection** for **Ignore WAF Protection**, you can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Prerequisites

A website has been added to WAF.

Constraints

- If you select **All protection** for **Ignore WAF Protection**, all WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.
- If you select **Basic web protection** for **Ignore WAF Protection**, global protection whitelist (formerly false alarm masking) rules take effect only for events triggered against WAF built-in rules in **Basic Web Protection** and anti-crawler rules under **Feature Library**.
  - Basic web protection rules

    Basic web protection defends against common web attacks, such as SQL injection, XSS attacks, remote buffer overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command and code injections. Basic web protection also detects web shells and evasion attacks.
  - Feature-based anti-crawler protection

    Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers.

- Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.
- You can configure a global whitelist (formerly false alarm masking) rule by referring to **Manipulação de alarmes falsos**. After handling a false alarm, you can view the rule in the global whitelist (formerly false alarm masking) rule list.
- Currently, the following regions support global protection whitelist (formerly false alarm masking) rules:
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - RU-Moscow201

Procedure

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

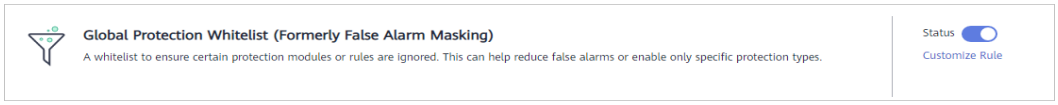
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 In the **Global Protection Whitelist (Formerly False Alarm Masking)** configuration area, click **Status** if needed. Then, click **Customize Rule**.

Figura 7-89 Global Protection Whitelist configuration area



Passo 7 In the upper left corner of the **Global Protection Whitelist** page, click **Add Rule**.

Passo 8 Add a global whitelist rule by referring to **Tabela 7-19**. **Figura 7-90** shows an example.

Figura 7-90 Add Global Protection Whitelist Rule

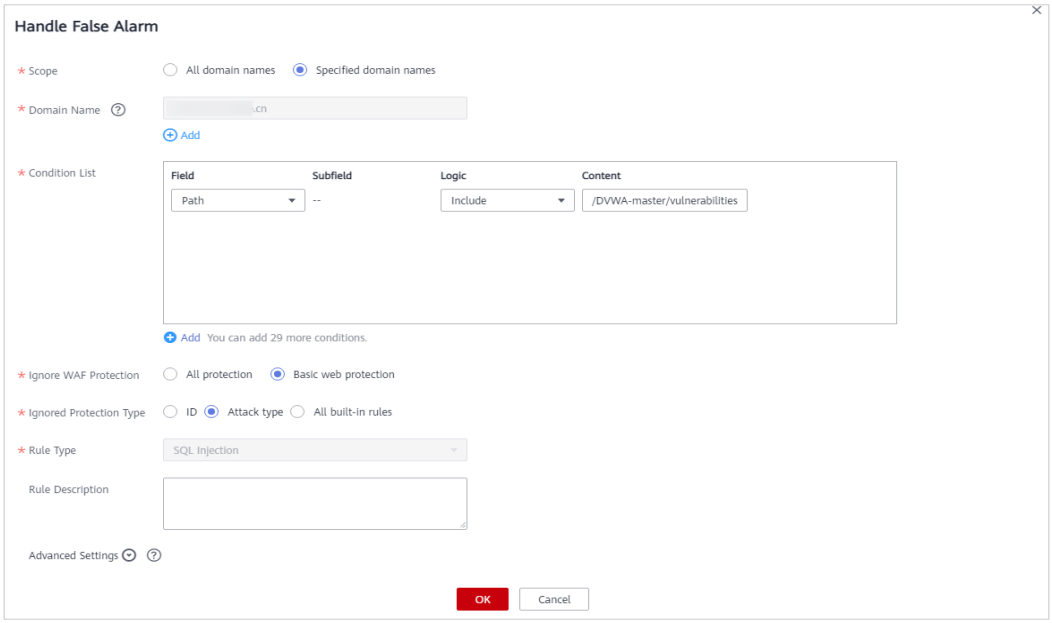


Tabela 7-19 Parameters

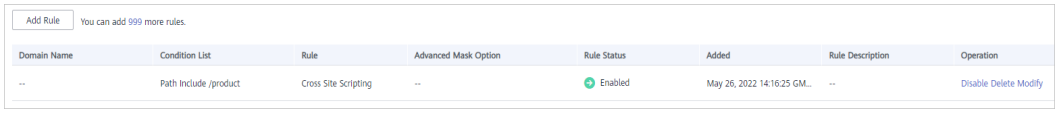
Parameter	Description	Example Value
Scope	• **All domain names**: By default, this rule will be used to all domain names that are protected by the current policy. • **Specified domain names**: This rule will be used to the specified domain names that match the wildcard domain name being protected by the current policy.	Specified domain names
Domain Name	This parameter is mandatory when you select **Specified domain names** for **Scope**. Enter a single domain name that matches the wildcard domain name being protected by the current policy.	www.example.com

Parameter	Description	Example Value
Condition List	Click **Add** to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters: Parameters for configuring a condition are described as follows: ● Field ● **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected for **Field**. **AVISO** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. ● **Logic**: Select a logical relationship from the drop-down list. ● **Content**: Enter or select the content that matches the condition.	Path, Include, /product
Ignore WAF Protection	● **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. ● **Basic Web Protection**: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.	Basic Web Protection
Ignored Protection Type	If you select **Basic web protection** for **Ignored Protection Type**, specify the following parameters: ● **ID**: Configure the rule by event ID. ● **Attack type**: Configure the rule by attack type, such as XSS and SQL injection. One type contains one or more rule IDs. ● **All built-in rules**: all checks enabled in **Basic Web Protection**.	Attack type

Parameter	Description	Example Value
ID	This parameter is mandatory when your select **ID** for **Ignored Protection Type**. ID of an attack event on the **Events** page. If the event type is **Custom**, it has no event ID. Click **Handle False Alarm** in the row containing the attack event to obtain the ID. You are advised to configure global protection whitelist (formerly false alarm masking) rules on the the **Events** page by referring to **Manipulação de alarmes falsos**.	041046
Attack type	This parameter is mandatory when your select **Attack type** for**Ignored Protection Type**. Select an attack type from the drop-down list box. WAF can defend against XSS attacks, web shells, SQL injection attacks, malicious crawlers, remote file inclusions, local file inclusions, command injection attacks, and other attacks.	SQL injection
Rule Description	A brief description of the rule. This parameter is optional.	SQL injection attacks are not intercepted.
Advanced Settings	To ignore attacks of a specific field, specify the field in the **Advanced Settings** area. After you add the rule, WAF will stop blocking attack events of the specified field. Select a target field from the first drop-down list box on the left. The following fields are supported: **Params**, **Cookie**, **Header**, **Body**, and **Multipart**. ● If you select **Params**, **Cookie**, or **Header**, you can select **All** or **Specified field** to configure a subfield. ● If you select **Body** or **Multipart**, you can select **All**. ● If you select **Cookie**, the **Domain Name** and **Path** can be empty. **NOTA** If **All** is selected, WAF will not block all attack events of the selected field.	Params All

Passo 9 Click **OK**.

Figura 7-91 Global protection whitelist (formerly false alarm masking) rules



----Fim

Other Operations

- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.
- To modify a global protection whitelist (formerly false alarm masking) rule, click **Modify** in the row containing the rule.
- To delete a global protection whitelist (formerly false alarm masking) rule, click **Delete** in the row containing the rule.

7.14 Configuração de uma regra de mascaramento de dados

Este tópico descreve como configurar regras de mascaramento de dados. Você pode configurar regras de mascaramento de dados para impedir que dados confidenciais, como senhas, sejam exibidos em logs de eventos.

NOTA

Se você ativou projetos corporativos, verifique se tem todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio no projeto.

Pré-requisitos

Um site foi adicionado ao WAF.

- Para o modo de nuvem, consulte **Conexão de um site ao WAF (Modo Nuvem)**.
- Para o modo dedicado, veja **Conexão de um site ao WAF (Modo Dedicado)**.

Restrições

- Leva vários minutos para que uma nova regra entre em vigor. Depois que a regra entrar em vigor, os eventos de proteção desencadeados pela regra serão exibidos na página **Events**.

Impacto no sistema

Dados sensíveis nos eventos serão mascarados para proteger a privacidade do visitante do seu site.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

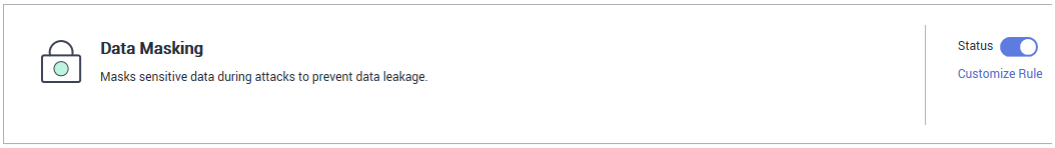
Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação, escolha **Website Settings**.

Passo 5 Na coluna **Policy** da linha que contém o nome de domínio, clique em **Configure Policy**.

Passo 6 Na área de configuração de **Data Masking**, altere o **Status**, se necessário, e clique em **Customize Rule**.

Figura 7-92 Área de configuração de mascaramento de dados



Passo 7 No canto superior esquerdo da página **Data Masking**, clique em **Add Rule**.

Passo 8 Na caixa de diálogo exibida, especifique os parâmetros descritos em **Tabela 7-20**.

Figura 7-93 Adicionando uma regra de mascaramento de dados

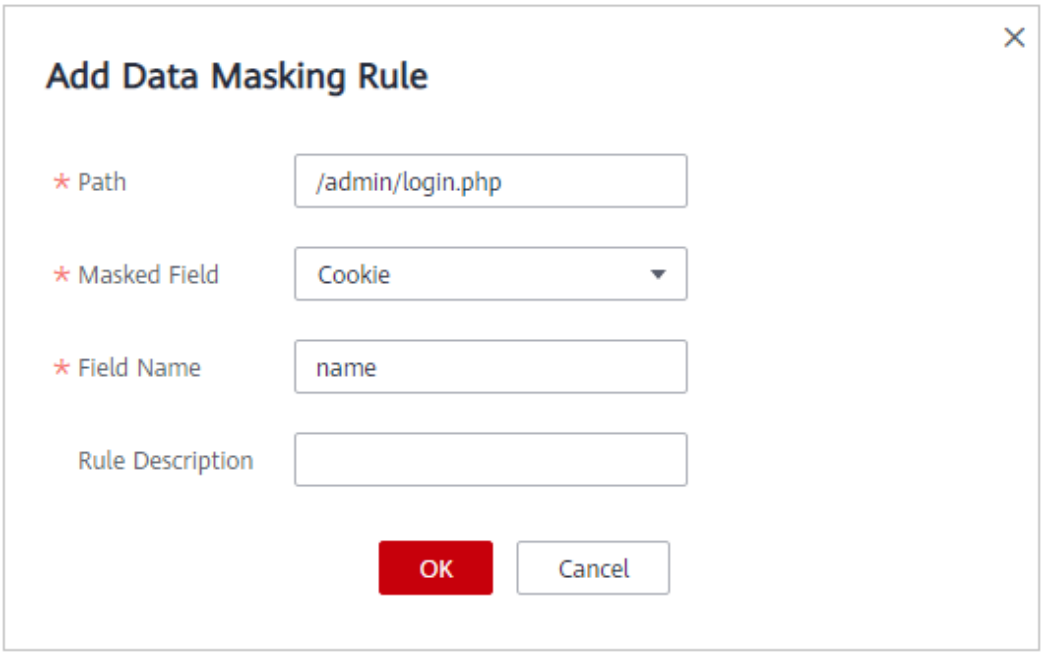
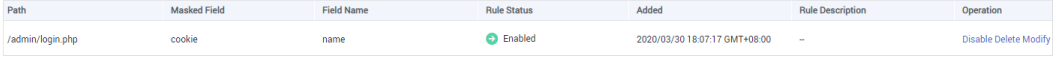


Tabela 7-20 Parâmetros de regra

Parâmetro	Descrição	Valor de exemplo
Caminho	Parte de URL que não inclui o nome de domínio. ● Correspondência de prefixo: O caminho que termina com * indica que o caminho é usado como um prefixo. Por exemplo, se o caminho a ser protegido for **/admin/test.php** ou **/adminabc**, defina **Path** como **/admin***. ● Correspondência exata: O caminho a ser inserido deve corresponder ao caminho a ser protegido. Se o caminho a ser protegido é **/admin**, Definir **Path** para **/admin**. **NOTA** ● O caminho suporta apenas correspondências de prefixo e exato e não suporta expressões regulares. ● O caminho não pode conter duas ou mais barras consecutivas. Por exemplo, ///**admin**. Se você digitar ///**admin**, o WAF converterá /// para /.	**/admin/login.php** Por exemplo, se a URL a ser protegida for **http://www.example.com/admin/login.php**, defina **Path** como **/admin/login.php**.
Campo mascarado	Um campo definido para ser mascarado ● **Params**: Um parâmetro de solicitação ● **Cookie**: Um pequeno pedaço de dados para identificar visitantes da web ● **Header**: Um cabeçalho HTTP definido pelo usuário ● **Form**: Um parâmetro de formulário	● Se **Masked Field** for **Params** e **Field Name** for **id**, Conteúdo relevante que corresponde **id** é mascarado. ● Se **Masked Field** for **Cookie** e **Field Name** for **Nome**Conteúdo relevante que corresponde **Nome** é mascarado.
Nome do Campo	Defina o parâmetro com base no **Masked Field**. O campo mascarado não será exibido nos logs. **AVISO** O comprimento de um subcampo não pode exceder bytes de 2 048. Apenas números, letras, sublinhados (_) e hifens (-) são permitidos.	
Descrição da regra	Uma breve descrição da regra. Este parâmetro é opcional.	Nenhum

Passo 9 Clique em **OK**. A regra de mascaramento de dados adicionada é exibida na lista de regras de mascaramento de dados.

Figura 7-94 Lista de regras de mascaramento de dados



----Fim

Outras Operações

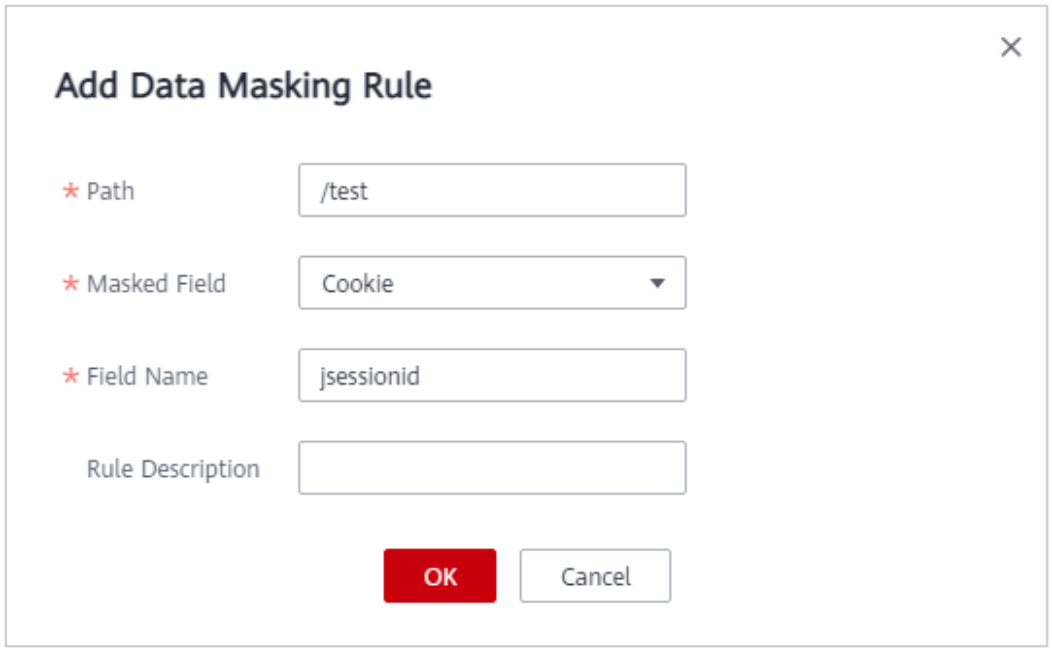
- Para desativar uma regra, clique em **Disable** na coluna **Operation** da regra. O **Rule Status** padrão é **Enabled**.
- Para modificar uma regra, clique em **Modify** na linha que contém a regra.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

Exemplo de configuração - Mascarando o campo Cookie

Para verificar se o WAF está protegendo seu nome de domínio *www.example.com* contra uma regra de mascaramento de dados (com **Cookie** selecionado para **Masked Field** e **jsessionid** inserido em **Field Name**):

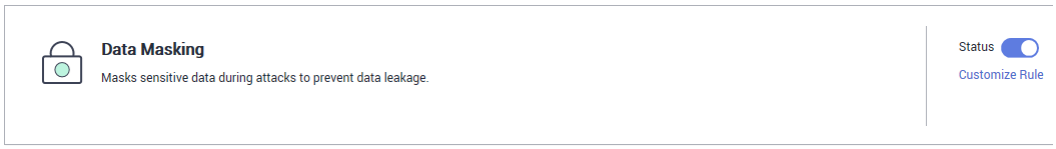
Passo 1 Adicione uma regra de mascaramento de dados.

Figura 7-95 Selecione **Cookie** para **Masked Field** e digite **jsessionid** em **Field Name**.



Passo 2 Ative o mascaramento de dados.

Figura 7-96 Área de configuração de mascaramento de dados

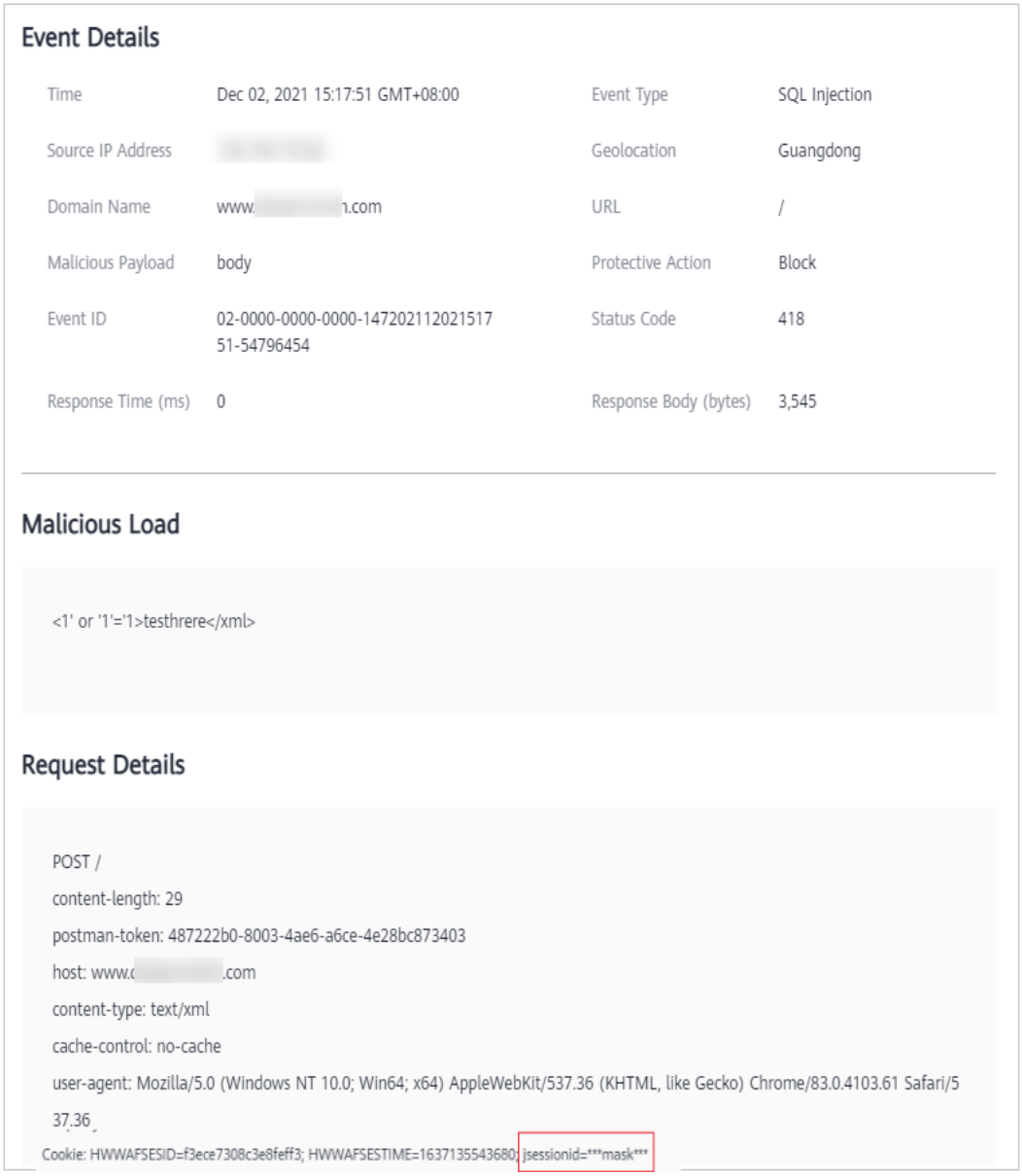


Passo 3 No painel de navegação à esquerda, escolha **Events**.

Passo 4 Na linha que contém o evento atingiu a regra, clique em **Details** na coluna **Operation** e exiba os detalhes do evento.

Os dados no campo cookie **jsessionid** são mascarados.

Figura 7-97 Visualização de eventos - mascaramento de dados de privacidade



----Fim

8 Painel de controle

Na página **Dashboard**, você pode exibir os logs de proteção de todos os sites ou instâncias protegidos para um intervalo de tempo especificado, incluindo ontem, hoje, últimos 3 dias, últimos 7 dias ou últimos 30 dias. Nesta página, os logs de eventos são exibidos por diferentes dimensões, incluindo o número de solicitações e tipos de ataque, QPS, largura de banda, código de resposta, distribuição de eventos, 10 principais nomes de domínio atacados, 10 principais endereços IP de origem de ataque, os 10 principais URL atacados, 10 principais locais de origem de ataque, e as 10 principais páginas de erro.

As estatísticas na página **Dashboard** são atualizadas a cada dois minutos.

NOTA

Se você tiver ativado projetos da empresa, poderá selecionar seu projeto da empresa na lista suspensa **Enterprise Project** e exibir os dados de estatísticas de segurança do projeto.

Pré-requisitos

- Um nome de domínio foi adicionado e conectado ao WAF.
- A proteção WAF está ativada.
- Pelo menos uma regra de proteção foi configurada para o nome de domínio.

Restrições

Atualmente, você pode exibir estatísticas de largura de banda nas seguintes regiões:

- CN-Hong Kong
- AP-Bangkok

Limitações da especificação

Na página **Dashboard**, os dados de proteção de no máximo 30 dias podem ser visualizados.

Como calcular o QPS

O método de cálculo do QPS varia de acordo com o intervalo de tempo. Para mais detalhes, consulte **Tabela 8-1**.

Tabela 8-1 Cálculo do QPS

Intervalo de tempo	Descrição média do QPS	Descrição do Peak QPS
Ontem ou **Hoje**	A curva QPS é feita com os QPS médios em cada minuto.	A curva QPS é feita com cada QPS de pico em cada minuto.
Últimos 3 dias	A curva QPS é feita com os QPS médios a cada cinco minutos.	A curva QPS é feita com cada QPS de pico a cada dois minutos.
Últimos 7 dias	A curva QPS é feita com o valor máximo entre os QPS médios a cada cinco minutos em um intervalo de 10 minutos.	A curva QPS é feita com cada QPS de pico a cada 10 minutos.
Últimos 30 dias	A curva QPS é feita com o valor máximo entre os QPS médios a cada cinco minutos em um intervalo de uma hora.	A curva QPS é feita com os QPS de pico a cada uma hora.

NOTA

Queries Per Second (QPS) indicates the number of requests per second. For example, an HTTP GET request is also called a query. The number of requests is the total number of requests in a specific time range.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Security & Compliance** > **Web Application Firewall** para ir para a página **Dashboard**.

Passo 4 Na parte superior da página, selecione um projeto na lista suspensa **Enterprise Project**. Em seguida, especifique o site, a instância e o período de tempo que você deseja consultar.

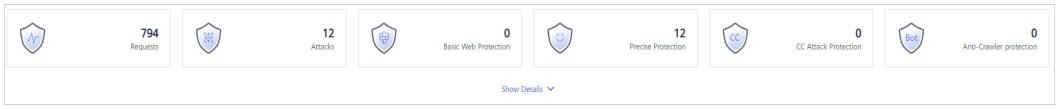
- Por padrão, as informações sobre todos os sites adicionados ao WAF em todos os projetos corporativos são exibidas.
- **Domain Names**: mostra informações sobre nomes de domínio de sites adicionados à instância do WAF no projeto corporativo selecionado. Clique em **View** para ir para a página **Website Settings** e exibir detalhes sobre nomes de domínio de sites protegidos.
- Tempo de consulta: Você pode selecionar **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, ou **Past 30 days**.

Figura 8-1 Definição de critérios de pesquisa

Passo 5 Veja quantas solicitações, ataques e páginas sob cada tipo de ataque.

- **Requests**: mostra as visualizações de página do site, facilitando a visualização do número total de páginas acessadas pelos visitantes em um determinado período de tempo.
- **Attacks**: mostra quantas vezes o site é atacado.
- Você pode ver quantas páginas são atacadas por um determinado tipo de ataque dentro de um determinado período de tempo.
- Você pode clicar em **Show Details** para exibir os detalhes dos 10 nomes de domínio com mais solicitações, ataques e proteção básica da Web, proteção precisa, proteção contra ataques CC e ações de proteção anticrawler.

Figura 8-2 Estatísticas de ação de proteção



Passo 6 Consulte dados de segurança na área **Security Event Statistics**.

By day: Você pode selecionar essa opção para exibir os dados coletados por dia. Se você deixar essa opção desmarcada, terá as seguintes opções:

- **Yesterday** and **Today**: Os dados de eventos de segurança são coletados a cada 2 minutos.
- **Past 3 days**: Os dados de eventos de segurança são coletados a cada 5 minutos.
- **Past 7 days**: Os dados de eventos de segurança são coletados a cada 10 minutos.
- **Past 30 days**: Os dados de eventos de segurança são coletados a cada hora.

Figura 8-3 Estatísticas de Eventos de Segurança

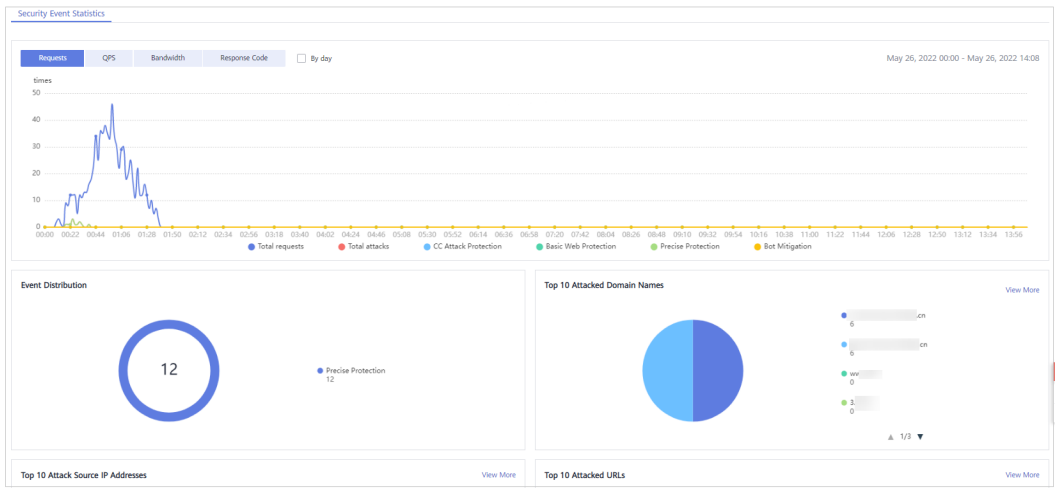


Tabela 8-2 Parâmetros em Estatísticas de Eventos de Segurança

Parâmetro	Descrição
Solicitações	Você pode visualizar quantas solicitações para o seu site, bem como o total de ataques e ataques de cada tipo de ataque.
QPS	Número médio de solicitações por segundo para o nome de domínio. Para obter detalhes sobre os valores do QPS, consulte **Como calcular o QPS**. Consultas por segundo (QPS) indica o número de solicitações por segundo. Por exemplo, uma solicitação HTTP GET também é chamada de consulta.
Largura de banda	Uso de largura de banda **AVISO** Atualmente, você pode exibir estatísticas de largura de banda nas seguintes regiões: ● CN-Hong Kong ● AP-Bangkok
Código de resposta	Códigos de resposta retornados pelo WAF ao cliente ou retornados pelo servidor de origem ao WAF juntamente com o número correspondente de respostas. Você pode clicar em **WAF to Client** ou **Origin Server to WAF** para visualizar as informações correspondentes. O número de códigos de resposta é acumulado com base na sequência de códigos de resposta (da esquerda para a direita) na parte inferior do gráfico. O número de códigos de resposta é a diferença entre duas linhas. Se o valor de um código de resposta for 0, a linha do código de resposta se sobrepõe à do código de resposta anterior.
Distribuição de eventos	Tipos de eventos de ataque Clique em uma área na área **Event Distribution** para exibir o tipo, o número e a proporção de um ataque.
Top 10 nomes de domínio atacados	Os dez nomes de domínio mais atacados e o número de ataques em cada nome de domínio. Clique em **View More** para ir para a página **Events** e exibir mais dados de proteção.
Os 10 principais endereços IP de origem de ataque	Os dez endereços IP de origem com mais ataques e o número de ataques de cada endereço IP de origem. Clique em **View More** para ir para a página **Events** e exibir mais dados de proteção.
Os 10 URL mais atacadas	Os dez URL mais atacados e o número de ataques em cada URL. Clique em **View More** para ir para a página **Events** e exibir mais dados de proteção.
Top 10 locais de origem de ataque	Os dez locais que geram mais ataques e o número de ataques de cada local.

Parâmetro	Descrição
Top 10 Páginas de Erro	Os dez sites com mais exceções de serviço. Sites com erros **404**, **500**, ou **502** podem ser visualizados. Clique em **Exception Check** e encontre as soluções correspondentes para corrigir as interrupções de serviço.

----Fim

9 Gerenciamento de eventos

9.1 Exibição de registros de eventos de proteção

Na página **Events**, você pode visualizar eventos gerados para ataques bloqueados e somente ataques registrados. Você pode exibir detalhes de eventos do WAF, incluindo a hora em que um evento ocorre, o endereço IP do servidor de origem, a localização geográfica do endereço IP do servidor de origem, a carga maliciosa e a regra de acerto.

AVISO

- No console do WAF, você pode exibir os dados de eventos de todos os nomes de domínio protegidos nos últimos 30 dias. Você pode ativar o Serviço de Tanque de Logs (LTS) no WAF para armazenamento de log de longo prazo. No LTS, você pode visualizar os detalhes do registro de ataque e acesso. Para mais detalhes, veja **Ativa LTS para registro em log do WAF**.
- Se você alternar o modo de trabalho do WAF de um site para **Suspended**, o WAF só encaminhará todas as solicitações para o site sem inspeção. Ele também não registra nenhum evento de ataque.
- Se você tiver ativado projetos da empresa, poderá selecionar seu projeto da empresa na lista suspensa **Enterprise Project** e exibir logs de eventos de proteção no projeto.

Pré-requisitos

O site a ser protegido foi conectado ao WAF.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em  no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação à esquerda, escolha **Events**.

Passo 5 Clique na guia **Search**. Na lista suspensa de site ou instância, selecione um site para exibir os logs de eventos correspondentes. O tempo de consulta pode ser **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, **Past 30 days**, ou um intervalo de tempo configurado por você. **Tabela 9-2** lista os parâmetros relacionados.

Figura 9-1 Exibindo eventos de proteção

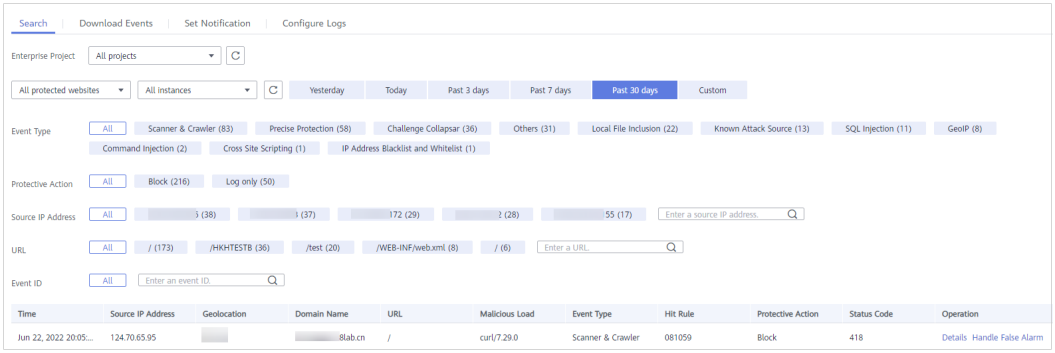


Tabela 9-1 Parâmetros do evento

Parâmetro	gerais
Tipo de evento	Tipo do ataque. Por padrão, **All** é selecionado. Você pode exibir logs de todos os tipos de ataque ou selecionar um tipo de ataque para exibir os logs de ataque correspondentes.
Ação Protetora	As opções são **Block**, **Log only**, e **Verification code**.
Endereço IP de origem	Endereço IP público do visitante / invasor da web Por padrão, **All** é selecionado. Você pode exibir logs de todos os endereços IP de origem de ataque, selecionar um endereço IP de origem de ataque ou inserir um endereço IP de origem de ataque para exibir os logs de ataque correspondentes.
URL	URL atacada.
ID do evento	ID do evento.

Tabela 9-2 Parâmetros na lista de eventos

Parâmetro	Descrição	Valor de exemplo
Horário	Quando o ataque ocorreu	2021/02/04 13:20:04
Endereço IP de origem	Endereço IP público do visitante / invasor da web	Nenh

Parâmetro	Descrição	Valor de exemplo
Geolocalização	Local de onde se origina o endereço IP do ataque	-
Nome de domínio	Nome de domínio atacado	www.example.com
URL	URL atacada	/admin
Carga maliciosa	O local ou parte do ataque que causa danos ou o número de vezes que a URL foi acessada. **NOTA** • Em um ataque CC, a carga maliciosa indica o número de vezes que a URL foi acessada. • Para eventos de proteção de lista negra, a carga maliciosa é deixada em branco.	id=1 e 1='1
Tipo de evento	Tipo de ataque	Injeção de SQL
Regra de Hit	ID da regra de proteção da Web básica interna atingida pelo evento de ataque. Esse campo é exibido se o evento de ataque corresponder a uma das regras básicas de proteção da Web. Por exemplo, injeção de SQL, XSS e ataques de inclusão de arquivos.	223633
Ação Protetora	Ações de proteção configuradas na regra. As opções são **Block**, **Log only**, e **Verification code**. **NOTA** Se uma solicitação de acesso corresponder a uma regra de proteção contra violação da Web, regra de prevenção contra vazamento de informações ou regra de mascaramento de dados, a ação de proteção será marcada como **Mismatch**.	Bloqueio
código de status	Código de status HTTP retornado na página de bloqueio.	418

NOTA

Para exibir detalhes do evento, clique em **Details** na coluna **Operation** da lista de eventos.

----Fim

9.2 Manipulação de alarmes falsos

Se confirmar que um evento de ataque na página **Events** é um alarme falso, você pode tratar o evento como alarme falso ignorando o URL e a ID da regra na proteção básica da Web ou

excluindo ou desativando a regra de proteção correspondente configurada. Depois que um evento de ataque é tratado como um alarme falso, o evento não será mais exibido na página **Events**. Você não receberá mais nenhuma notificação de alarme sobre o evento.

O WAF detecta ataques usando regras básicas de proteção da Web incorporadas, recursos integrados na proteção anticrawler e regras personalizadas configuradas por você. (como proteção contra ataques CC, proteção de acesso precisa, lista negra, lista branca e regras de controle de acesso de geolocalização). O WAF responderá aos ataques detectados com base nas ações de proteção (como somente **Block** e **Log only**) definidas nas regras e exibirá eventos de ataque na página **Events**.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e manipular alarmes falsos no projeto.

Pré-requisitos

Há pelo menos um evento de alarme falso na lista de eventos.

Restrições

- Somente eventos de ataque bloqueados ou gravados por regras básicas pré-configuradas de proteção da Web e recursos na proteção anti-crawler podem ser tratados como alarmes falsos.
- Para eventos gerados com base em regras personalizadas (como uma regra de proteção contra ataques CC, regra de proteção precisa, regra de lista negra, regra de lista branca ou regra de controle de acesso de geolocalização) não podem ser tratados como falsos alarmes. Para ignorar esse evento, exclua ou desabilite a regra personalizada atingida pelo evento.
- Um evento de ataque só pode ser tratado como um alarme falso uma vez.

Cenários de aplicação

Às vezes, solicitações de serviço normais podem ser bloqueadas pelo WAF. Por exemplo, suponha que você implante um aplicativo da Web em um HUAWEI CLOUD ECS e, em seguida, adicione o nome de domínio público associado a esse aplicativo ao WAF. Se você habilitar a proteção básica da Web para esse aplicativo, o WAF poderá bloquear as solicitações de acesso que correspondem às regras básicas de proteção da Web. Como resultado, o site não pode ser acessado através do seu nome de domínio. No entanto, o site ainda pode ser acessado através do endereço IP. Nesse caso, você pode manipular os alarmes falsos para permitir solicitações de acesso normais ao aplicativo.

Impacto no sistema

O evento de ataque não será exibido na página **Events**. Você não receberá mais nenhuma notificação de alarme sobre o evento.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação à esquerda, escolha **Events**.

Passo 5 Selecione a guia **Search**. Selecione um site na lista suspensa **All protected websites**. Em seguida, selecione **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, **Past 30 days**, ou um intervalo de tempo personalizado. **Figura 9-2** mostra um exemplo. **Tabela 9-3** e **Tabela 9-4** descrevem os parâmetros.

Figura 9-2 Exibindo eventos de proteção

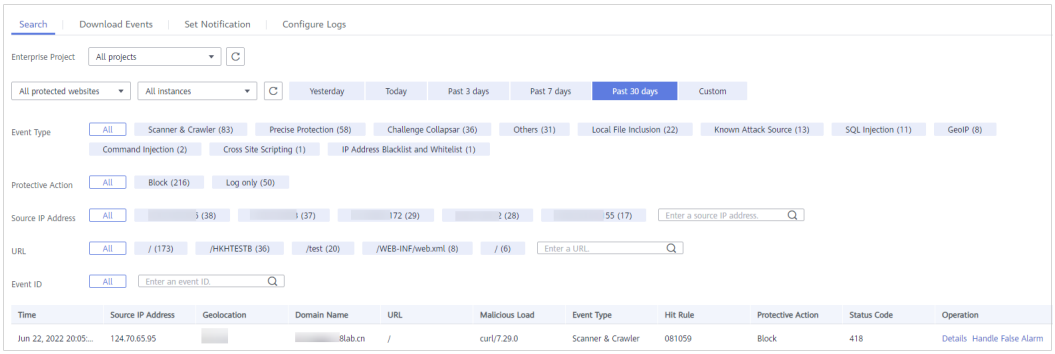


Tabela 9-3 Parâmetros do evento

Parâmetro	Descrição
Tipo de evento	Tipo de ataque. Por padrão, **All** está selecionado. Você pode exibir logs de todos os tipos de ataque ou selecionar um tipo de ataque para exibir os logs de ataque correspondentes.
Ação Protetora	As opções são **Block**, **Log only**, e **Verification code**.
Endereço IP de origem	Endereço IP público do visitante / atacante da web Por padrão, **All** é selecionado. Você pode exibir logs de todos os endereços IP de origem de ataque, selecionar um endereço IP de origem de ataque ou digitar um endereço IP de origem de ataque para exibir os logs de ataque correspondentes.
URL	URL atacada
ID do evento	ID do evento

Tabela 9-4 Parâmetros na lista de eventos

Parâmetro	Descrição	Valor de exemplo
Horário	Quando o ataque ocorreu	2021/02/04 13:20:04
Endereço IP de origem	Endereço IP público do visitante / invasor da web	Nenh
Geolocalização	Local de onde se origina o endereço IP do ataque	-
Nome de domínio	Nome de domínio atacado	www.example.com
URL	URL atacada	/admin
Carga maliciosa	O local ou parte do ataque que causa danos ou o número de vezes que a URL foi acessada. **NOTA** ● Em um ataque CC, a carga maliciosa indica o número de vezes que a URL foi acessada. ● Para eventos de proteção de lista negra, a carga maliciosa é deixada em branco.	id=1 e 1='1
Tipo de evento	Tipo de ataque	Injeção de SQL
Regra de Hit	ID da regra de proteção da Web básica interna atingida pelo evento de ataque. Esse campo é exibido se o evento de ataque corresponder a uma das regras básicas de proteção da Web. Por exemplo, injeção de SQL, XSS e ataques de inclusão de arquivos.	223633
Ação Protetora	Ações de proteção configuradas na regra. As opções são **Block**, **Log only**, e **Verification code**. **NOTA** Se uma solicitação de acesso corresponder a uma regra de proteção contra violação da Web, regra de prevenção contra vazamento de informações ou regra de mascaramento de dados, a ação de proteção será marcada como **Mismatch**.	Bloqueio
código de status	Código de status HTTP retornado na página de bloqueio.	418

NOTA

Para exibir detalhes do evento, clique em **Details** na coluna **Operation** da lista de eventos.

Passo 6 Depois de confirmar que um evento é um alarme falso, clique em **Handle False Alarm** na coluna **Operation** da linha e adicione uma regra de mascaramento de alarme falso. **Figura 9-3** mostra um exemplo. **Tabela 9-5** descreve os parâmetros.

Figura 9-3 Manipulação de um alarme falso

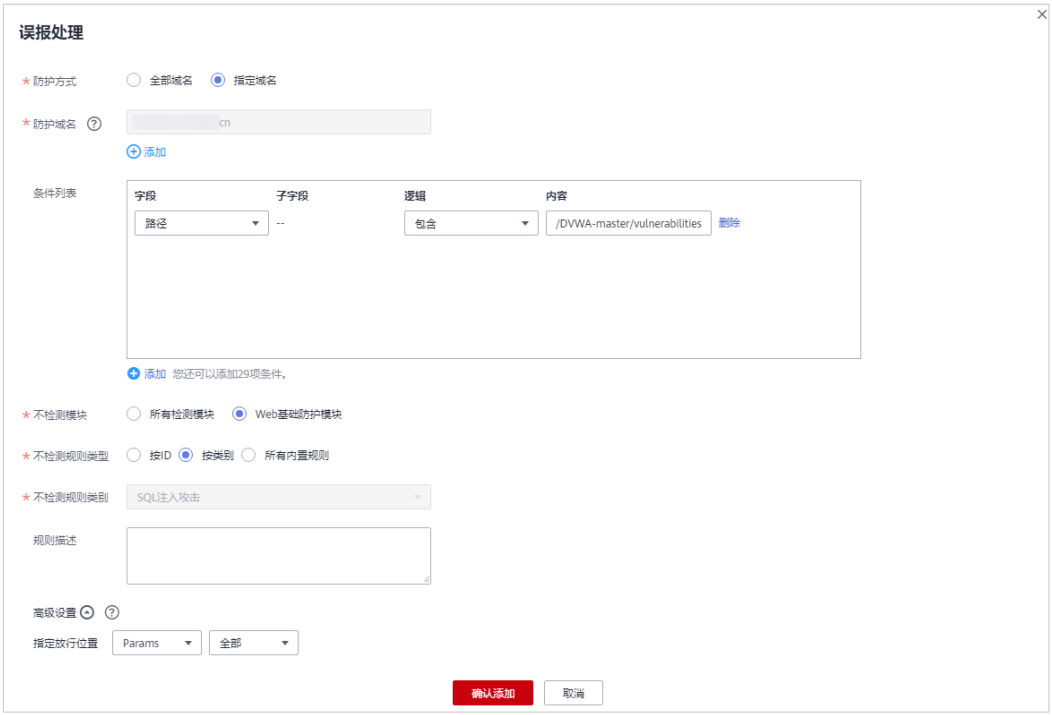


Tabela 9-5 Parameters

Parameter	Description	Example Value
Scope	• **All domain names**: By default, this rule will be used to all domain names that are protected by the current policy. • **Specified domain names**: This rule will be used to the specified domain names that match the wildcard domain name being protected by the current policy.	Specified domain names
Domain Name	This parameter is mandatory when you select **Specified domain names** for **Scope**. Enter a single domain name that matches the wildcard domain name being protected by the current policy.	www.example.com

Parameter	Description	Example Value
Condition List	Click **Add** to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters: Parameters for configuring a condition are described as follows: ● Field ● **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected for **Field**. **AVISO** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. ● **Logic**: Select a logical relationship from the drop-down list. ● **Content**: Enter or select the content that matches the condition.	Path, Include, /product
Ignore WAF Protection	● **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. ● **Basic Web Protection**: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.	Basic Web Protection
Ignored Protection Type	If you select **Basic web protection** for **Ignored Protection Type**, specify the following parameters: ● **ID**: Configure the rule by event ID. ● **Attack type**: Configure the rule by attack type, such as XSS and SQL injection. One type contains one or more rule IDs. ● **All built-in rules**: all checks enabled in **Basic Web Protection**.	Attack type

Parameter	Description	Example Value
ID	This parameter is mandatory when your select **ID** for **Ignored Protection Type**. ID of an attack event on the **Events** page. If the event type is **Custom**, it has no event ID. Click **Handle False Alarm** in the row containing the attack event to obtain the ID. You are advised to configure global protection whitelist (formerly false alarm masking) rules on the the **Events** page by referring to **Manipulação de alarmes falsos**.	041046
Attack type	This parameter is mandatory when your select **Attack type** for**Ignored Protection Type**. Select an attack type from the drop-down list box. WAF can defend against XSS attacks, web shells, SQL injection attacks, malicious crawlers, remote file inclusions, local file inclusions, command injection attacks, and other attacks.	SQL injection
Rule Description	A brief description of the rule. This parameter is optional.	SQL injection attacks are not intercepted.
Advanced Settings	To ignore attacks of a specific field, specify the field in the **Advanced Settings** area. After you add the rule, WAF will stop blocking attack events of the specified field. Select a target field from the first drop-down list box on the left. The following fields are supported: **Params**, **Cookie**, **Header**, **Body**, and **Multipart**. ● If you select **Params**, **Cookie**, or **Header**, you can select **All** or **Specified field** to configure a subfield. ● If you select **Body** or **Multipart**, you can select **All**. ● If you select **Cookie**, the **Domain Name** and **Path** can be empty. **NOTA** If **All** is selected, WAF will not block all attack events of the selected field.	Params All

Passo 7 Clique em **OK**.

----Fim

Verificação

Um alarme falso será excluído dentro de cerca de um minuto após a configuração de manuseio ser feita. Ele não será mais exibido na lista de detalhes do evento de ataque. Você pode atualizar o cache do navegador e solicitar a página para a qual a regra de lista branca de proteção global (anteriormente mascaramento de alarme falso) está configurada para verificar se a configuração tem efeito.

Outras Operações

Se um evento for tratado como um alarme falso, o hit de regra será adicionado à lista de regras de lista branca de proteção global (anteriormente mascaramento de alarme falso). Acesse a página **Policies** e alterne para a página Lista branca de Proteção Global (Anteriormente Mascaramento de Alarme Falso) para gerenciar a regra, incluindo consulta, desativação, exclusão e modificação da regra. Para mais detalhes, consulte **Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule**.

9.3 Download de dados de eventos

Este tópico descreve como fazer o download de dados de eventos (eventos registrados e bloqueados) dos últimos cinco dias. Um ou mais arquivos CSV contendo os dados do evento do dia atual serão gerados no início do dia seguinte.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e fazer o download dos logs de eventos de proteção no projeto.

Pré-requisitos

- O site a ser protegido foi adicionado ao WAF.
- Um arquivo de evento foi gerado.

Limitações da especificação

- Cada arquivo pode incluir um máximo de eventos 5 000. Se houver mais de eventos 5 000, outro arquivo será gerado.
- Somente os dados de eventos dos últimos cinco dias podem ser baixados por meio do console do WAF.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação à esquerda, escolha **Events**.

Passo 5 Clique na guia **Download Events** e baixe os dados de proteção desejados. **Tabela 9-6** descreve os parâmetros.

Tabela 9-6 Descrição do parâmetro

Parâmetro	Descrição
Nome do arquivo	O formato é *file-name*.**csv**.
Número de Eventos	Número total de eventos bloqueados e registrados **NOTA** O número máximo de eventos em um arquivo é 10.000. Se houver mais de eventos 10.000, outro arquivo será gerado.

Passo 6 Na coluna **Operation**, clique em **Download** para fazer download de dados para o PC local.

----Fim

Campos em um arquivo de dados de evento de proteção

Campo	Descrição	Valor de exemplo
action	Ação de proteção tomada em resposta ao evento	block
attack	Tipo de ataque	SQL Injection
body	Solicitar conteúdo do ataque	N/A
cookie	Biscoito do atacante	N/A
headers	Cabeçalho do atacante	N/A
host	Nome de domínio ou endereço IP do site protegido	www.example.com
id	ID do evento.	02-11-16-20201121060347-feb42002
payload	A parte do ataque que causa danos ao site protegido	python-requests/2.20.1
payload_location	A localização do ataque que causa danos ou o número de vezes que o URL é acedido pelo atacante	user-agent
policyid	ID da política.	d5580c8f6cd4403ebbf85892d4bbb8e4
request_line	Linha de pedido do ataque	GET /
rule	ID da regra contra a qual o evento é gerado.	81066
sip	Endereço IP público do visitante / invasor da web	N/A

Campo	Descrição	Valor de exemplo
time	Quando o evento ocorreu.	2020/11/21 0:20:44
url	URL do nome de domínio protegido	N/A

Outras Operações

Habilite o LTS no WAF para armazenamento de registros de longo prazo. No LTS, você pode exibir os detalhes do registro de ataque e acesso. Para mais detalhes, veja **Ativa LTS para registro em log do WAF**.

10 Ativa LTS para registro em log do WAF

Depois de autorizar o WAF a acessar o Serviço de Tanque de Registros (LTS), você poderá usar os registros do WAF registrados pelo LTS para análise rápida e eficiente em tempo real, gerenciamento de O&M de dispositivos e análise de tendências de serviço.

O LTS analisa e processa um grande número de logs. Ele permite que você processe logs em tempo real, de forma eficiente e segura. Os registros podem ser armazenados no LTS por sete dias por padrão, mas você pode configurar o LTS por até 30 dias, se necessário. Logs anteriores a 30 dias são excluídos automaticamente. No entanto, você pode configurar o LTS para despejar esses logs em um intervalo do Object Storage Service (OBS) ou habilitar o Data Ingesttion Service (DIS) para armazenamento de longo prazo.

AVISO

- No console do WAF, você pode ver os logs dos últimos 30 dias e baixar os logs de todos os sites protegidos dos últimos cinco dias.
- O LTS é faturado por tráfego e é cobrado separadamente do WAF. Para obter detalhes sobre preços LTS, consulte **Detalhes de preços LTS**.
- Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar o registro WAF.

Pré-requisitos

- Você adquiriu uma instância do WAF.
- O site a ser protegido foi adicionado ao WAF.

Restrições

Você pode habilitar o LTS para o registro em log do WAF nas seguintes regiões: CN-Hong Kong, AP-Bangkok, e AP-Singapura.

Impacto no sistema

Ativar o LTS para WAF não afeta o desempenho do WAF.

Ativando o LTS para registro de eventos de proteção WAF

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação à esquerda, escolha **Events**.

Passo 5 Clique na guia **Configure Logs**, ative o LTS ( ), e selecione um grupo de logs e um fluxo de logs. **Tabela 10-1** descreve os parâmetros.

Figura 10-1 Configurando logs

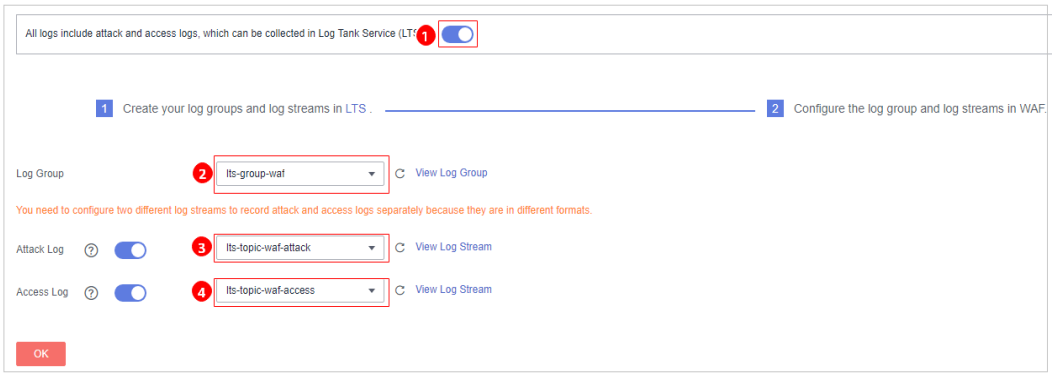


Tabela 10-1 Configuração do log

Parâmetro	Descrição	Valor de exemplo
Grupo de logs	Selecione um grupo de logs ou clique em **View Log Group** para acessar o console LTS e criar um grupo de logs.	lts-grupo-waf
Registro de Ataque	Selecione um fluxo de log ou clique em **View Log Stream** para ir para o console LTS e criar um fluxo de log. Um log de ataque inclui informações sobre o tipo de evento, ação de proteção e endereço IP de origem de ataque de cada ataque.	lts-topic-waf-ataque

Parâmetro	Descrição	Valor de exemplo
Log de acesso	Selecione um fluxo de log ou clique em **View Log Stream** para ir para o console LTS e criar um fluxo de log. Um log de acesso inclui informações importantes sobre o tempo de acesso, o endereço IP do cliente e a URL do recurso de cada solicitação de acesso HTTP.	lts-topic-waf-access

Passo 6 Clique em **OK**.

Você pode exibir logs de eventos de proteção WAF no console LTS.

----Fim

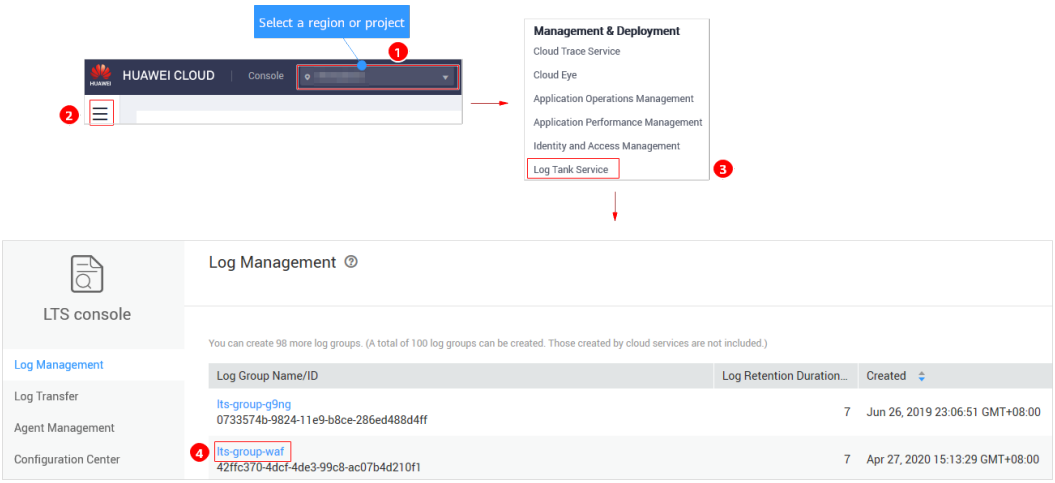
Visualizando logs de eventos de proteção WAF em LTS

Depois de ativar o LTS, execute as etapas a seguir para exibir e analisar os logs do WAF no console do LTS.

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Vá para a página de fluxo de log seguindo as etapas mostradas em **Figura 10-2**.

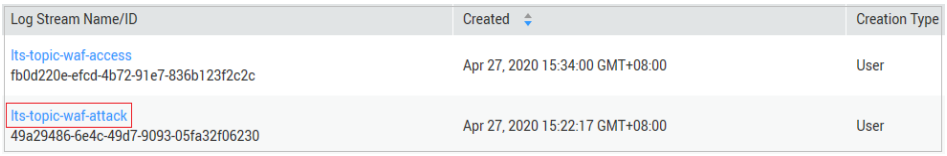
Figura 10-2 Acesso à página de gerenciamento de log



Passo 3 Exibir logs de eventos de proteção.

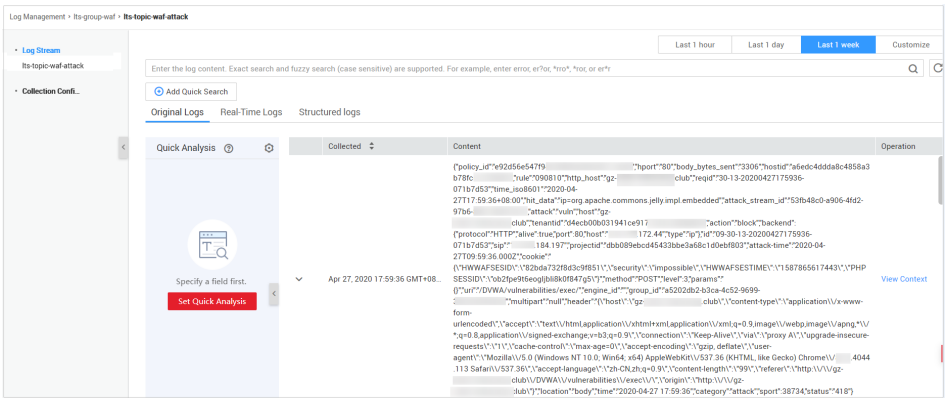
- Ver registos de ataque.
  a. Na lista de fluxo de log, clique no nome do fluxo de log (por exemplo, **lts-topic-waf-attack**) configurado para logs de ataque.

Figura 10-3 Nome do fluxo de log configurado para logs de ataque



b. Ver logs de ataque. **Figura 10-4** mostra um exemplo.

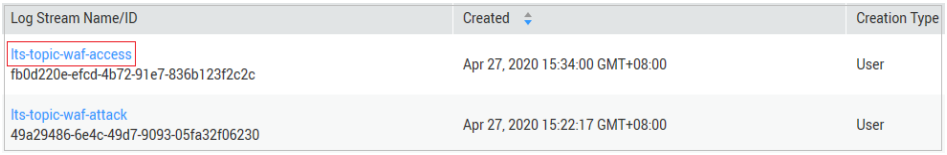
Figura 10-4 Visualizando logs de ataque



- Ver registos de acesso.

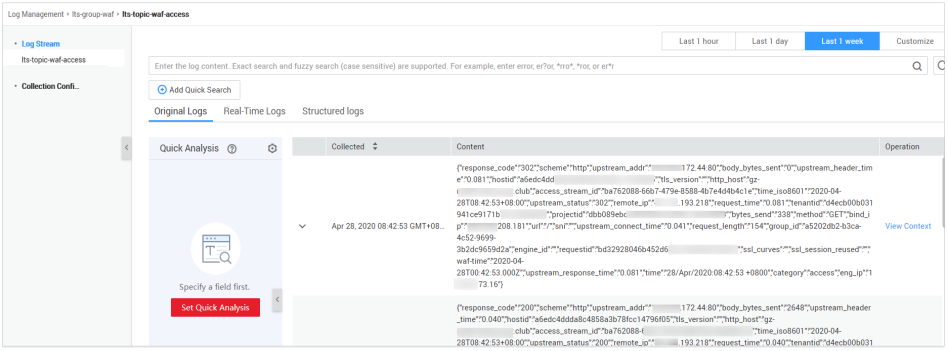
  a. Na lista de fluxo de log, clique no nome do fluxo de log (por exemplo, **lts-topic-waf-access**) configurado para logs de acesso.

Figura 10-5 Nome do fluxo de log configurado para logs de acesso



  b. Ver registos de acesso. **Figura 10-6** mostra um exemplo.

Figura 10-6 Exibindo logs de acesso



----Fim

Campo access_log do WAF

Campo	Tipo	Descrições do campo	Descrição
requestid	string	ID aleatório	O valor é o mesmo que os últimos oito caracteres do campo **req_id** no log de ataque.
time	string	Hora em que uma solicitação de acesso é recebida.	GMT hora em que um log é gerado.
eng_ip	string	Endereço IP do mecanismo WAF	-
hostid	string	Identificador do nome de domínio da solicitação de acesso.	ID de nome de domínio protegido (upstream_id).
tenantid	string	ID da conta	A sua conta
projectid	string	ID do projeto ao qual o nome de domínio protegido pertence	ID do projeto de um usuário em uma região específica.
remote_ip	string	Endereço IP a partir do qual uma solicitação de cliente se origina.	Endereço IP a partir do qual uma solicitação de cliente se origina. **AVISO** Se um proxy de camada 7 for implantado na frente do WAF, esse campo indicará o endereço IP do nó de proxy mais próximo do WAF. O endereço IP real do visitante é especificado pelos campos **x-forwarded-for** e **x_real_ip**.
x-forwarded-for	string	Uma seqüência de endereços IP para um proxy quando o proxy é implantado na frente do WAF.	A picada inclui um ou mais endereços IP. O endereço IP mais à esquerda é o endereço IP de origem do cliente. Cada vez que o servidor proxy recebe uma solicitação, ele adiciona o endereço IP de origem da solicitação à direita do endereço IP de origem.

Campo	Tipo	Descrições do campo	Descrição
x_real_ip	string	Endereço IP real do cliente quando um proxy é implantado na frente do WAF.	Endereço IP real do cliente, que é identificado pelo proxy.
cdn_src_ip	string	Endereço IP do cliente identificado pelo CDN quando o CDN é implantado na frente do WAF	Este campo especifica o endereço IP real do cliente se a CDN for implantada na frente do WAF. **AVISO** Alguns fornecedores de CDN podem usar outros campos. O WAF registra apenas os campos mais comuns.
scheme	string	Protocolo de solicitação	Protocolos que podem ser usados na requisição: ● HTTP ● HTTPS
response_code	string	Código de resposta	Código de status de resposta retornado pelo servidor de origem ao WAF.
method	string	Método de solicitação.	Tipo de solicitação em uma linha de solicitação. Geralmente, o valor é **GET** ou **POST**.
http_host	string	Nome de domínio do servidor solicitado.	Endereço, nome de domínio ou endereço IP inserido na caixa de endereço de um navegador.
url	string	URL da solicitação.	Caminho em um URL (excluindo o nome de domínio).
request_length	string	Comprimento do pedido.	O comprimento da solicitação inclui o endereço da solicitação de acesso, o cabeçalho da solicitação HTTP e o número de bytes no corpo da solicitação.
bytes_send	string	Número total de bytes enviados ao cliente.	Número de bytes enviados pelo WAF para o cliente.

Campo	Tipo	Descrições do campo	Descrição
body_bytes_sent	string	Número total de bytes do corpo de resposta enviado ao cliente	Número de bytes do corpo de resposta enviado pelo WAF ao cliente
upstream_addr	string	Endereço do servidor backend.	Endereço IP do servidor de origem para o qual uma solicitação é destinada. Por exemplo, se o WAF encaminhar solicitações para um ECS, o endereço IP do ECS será retornado para esse parâmetro.
request_time	string	Tempo de processamento da solicitação	O tempo de processamento começa quando o primeiro byte do cliente é lido.
upstream_response_time	string	Tempo de resposta do servidor back-end.	Hora em que o servidor de back-end responde à solicitação do WAF.
upstream_status	string	Código de resposta do servidor backend.	Código de status de resposta retornado pelo servidor de back-end ao WAF.
upstream_connect_time	string	Tempo decorrido para que os servidores de origem se conectem aos servidores de back-end	Tempo para o servidor de origem estabelecer uma conexão com seus servidores de back-end. Se o serviço de back-end utilizar um protocolo de encriptação, este parâmetro inclui o tempo de handshake.
upstream_header_time	string	Tempo usado pelo servidor de back-end para receber o primeiro byte do cabeçalho da resposta.	-
bind_ip	string	Endereço IP back-to-source do mecanismo WAF.	Endereço IP back-to-source usado pelo mecanismo WAF.

Campo	Tipo	Descrições do campo	Descrição
group_id	string	ID do grupo de registos LTS	ID do grupo de registros para interconexão do WAF com o LTS.
access_stream_id	string	ID do fluxo de log.	ID de **access_stream** do usuário no grupo de logs identificado pelo campo **group_id**.
engine_id	string	ID do mecanismo WAF	ID exclusivo do motor WAF.
time_iso8601	string	ISO 8601 formato de tempo de logs.	-
sni	string	Nome de domínio solicitado através do SNI.	-
tls_version	string	Versão do protocolo para estabelecer uma conexão SSL.	Versão TLS usada na solicitação.
ssl_curves	string	Lista de grupos de curvas suportadas pelo cliente.	-
ssl_session_reused	string	Reutilização de sessão SSL	Se a sessão SSL pode ser reutilizada **r**: Sim **.**: Não
process_time	string	Duração da detecção	-

Descrição do campo request_log do WAF

Campo	Tipo	Descrições do campo	Descrição
scheme	string	Protocolo de solicitação	Protocolos que podem ser usados na solicitação: ● HTTP ● HTTPS
hport	string	Porta de escuta para o motor	-
body_bytes_sent	string	Número total de bytes do corpo de resposta enviado ao cliente.	-
hostid	string	ID de nome de domínio protegido (upstream_id).	-
time_iso8601	string	Formato de tempo ISO 8601 dos logs.	-
host	string	Nome de domínio do servidor solicitado.	-
tenantid	string	ID da conta	-
inet_ip	string	Endereço IP do motor	-
backend.protocol	string	Protocolo de back-end atual	-
backend.alive	string	Status do back-end atual	-
backend.port	string	Porta de back-end atual	-
backend.host	string	Valor atual do host de back-end	-
backend.type	string	Tipo de host de back-end atual	Tipo do host de backend. Pode ser um nome de domínio ou um endereço IP.
id	string	ID de Solicitação	Os últimos oito caracteres são os mesmos que os primeiros oito caracteres do **requestid** no log de acesso.

Campo	Tipo	Descrições do campo	Descrição
sip	string	Endereço IP a partir do qual uma solicitação de cliente se origina.	-
sport	string	Porta usada pelo endereço IP a partir do qual uma solicitação de cliente se origina.	-
projectid	string	ID do projeto ao qual o nome de domínio protegido pertence	-
cookie	string	Biscoito	-
method	string	Método de solicitação.	-
uri	string	Solicitar URI	-
request_stream_id	string	ID do fluxo de log	ID do **request_stream** do usuário no grupo de logs identificado pelo campo **group_id**.
group_id	string	ID do grupo de log	ID do grupo de registos LTS
engine_id	string	ID exclusivo do motor	-
header	string	Conteúdo do cabeçalho	-
time	string	Tempo de registro	-
category	string	Categoria de log	O valor é **request**.
status	string	Código de resposta	-

Descrição do campo attack_log do WAF

Campo	Tipo	Descrições do campo	Descrição
category	string	Categoria de log	O valor é o **attack**.
time	string	Tempo de registro	-

Campo	Tipo	Descrições do campo	Descrição
time_iso8601	string	Formato de tempo ISO 8601 dos logs.	-
policy_id	string	ID da política	-
level	string	Nível de proteção	Nível de proteção de uma regra incorporada na proteção básica da Web ● **1**: Baixo ● **2**: Médio ● **3**: Alto

Campo	Tipo	Descrições do campo	Descrição
attack	string	Tipo de ataque	Tipo de ataque. Esse parâmetro é listado somente nos logs de ataque. ● **default**: ataques padrão ● **sqli**: Injeções de SQL ● **xss**: ataques de cross-site scripting (XSS) ● **webshell**: shells da web ● **robot**: rastreadores maliciosos ● **cmdi**: injeções de comando ● **rfi**: ataques de inclusão de arquivos remotos ● **lfi**: ataques de inclusão de arquivo local ● **illegal**: solicitações não autorizadas ● **vuln**: façanhas ● **cc**: ataques que atingiram as regras de proteção da CC ● **custom_custom**: ataques que atingem uma regra de proteção precisa ● **custom_whiteip**: ataques que atingem uma regra de lista negra ou de lista branca de endereços IP ● **custom_geoip**: ataques que atingem uma regra de controle de acesso de geolocalização ● **antitamper**: ataques que atingem uma regra de proteção contra adulteração da Web ● **anticrawler**: ataques que atingiram a regra anticrawler do desafio JS ● **leakage**: vulnerabilidades que atingem uma regra de prevenção de vazamento de informações ● **followed_action**: a fonte é marcada como uma fonte de ataque conhecida. Para mais detalhes, consulte **Configuração de uma regra de origem de ataque conhecido** .
action	string	Ação Protetora	Ação de defesa da WAF. ● **Bloqueio**: O WAF bloqueia ataques. ● **log**: O WAF registra apenas os ataques detectados. ● **captcha**: Código de verificação

Campo	Tipo	Descrições do campo	Descrição
sub_type	string	Tipos de esteira rolante	Quando o **attack** é definido como **robot**, este parâmetro não pode ser deixado em branco. ● **script_tool**: Ferramentas de script ● **search_engine**: Motores de busca ● **scanner:** Ferramentas de digitalização ● **uncategorized**: Outros crawlers
rule	string	ID da regra acionada ou a descrição do tipo de política personalizada.	-
location	string	Localização que aciona a carga maliciosa	-
hit_data	string	String acionando a carga maliciosa	-
resp_headers	string	Cabeçalho de resposta	-
resp_body	string	Corpo da resposta	-
backend	string	Endereço do servidor de back-end para o qual a solicitação é encaminhada.	-
status	string	Código do estado da resposta	-
reqid	string	ID aleatório	-
id	string	ID do ataque	Identificação do ataque
method	string	Método de solicitação	-
sip	string	Endereço IP de solicitação do cliente	-
sport	string	Porta de solicitação do cliente	-
host	string	Nome de domínio solicitado	-

Campo	Tipo	Descrições do campo	Descrição
http_host	string	Nome de domínio do servidor solicitado.	-
hport	string	Porta do servidor solicitado.	-
uri	string	URL da solicitação.	O domínio é excluído.
header	Uma string JSON. Uma tabela JSON é obtida depois que a string é decodificada.	Cabeçalho da solicitação	-
mutipart	Uma string JSON. Uma tabela JSON é obtida depois que a string é decodificada.	Solicitar cabeçalho de várias partes	Este parâmetro é usado para fazer upload de arquivos.
cookie	Uma string JSON. Uma tabela JSON é obtida depois que a string é decodificada.	Cookie do pedido	-

Campo	Tipo	Descrições do campo	Descrição
params	Uma string JSON. Uma tabela JSON é obtida depois que a string é decodificada.	Valor dos parâmetros após o URI da solicitação.	-
body_bytes_sent	string	Número total de bytes do corpo de resposta enviado ao cliente.	Número total de bytes do corpo de resposta enviado pelo WAF ao cliente.
upstream_response_time	string	Tempo de resposta do servidor back-end.	-
process_time	string	Duração da detecção	-
engine_id	string	ID exclusivo do motor	-
group_id	string	ID do grupo de log	ID do grupo de logs LTS
attack_stream_id	string	ID do fluxo de log	ID de **access_stream** do usuário no grupo de logs identificado pelo campo **group_id**.
hostid	string	ID de nome de domínio protegido (upstream_id).	-
tenantid	string	ID da conta	-
projectid	string	ID do projeto ao qual o nome de domínio protegido pertence	-

11 Ativação de notificações de alarme

Este tópico descreve como ativar notificações para logs de ataque. Quando essa função estiver ativada, o WAF enviará notificações por SMS ou e-mail se um ataque for detectado.

NOTA

- Simple Message Notification (SMN) é um serviço pago.
- Antes que você ajuste a notificação do alarme, crie um tópico da mensagem no serviço SMN. Para obter detalhes, consulte **Antes de publicar uma mensagem**.
- Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e ativar as notificações de alarme.

Pré-requisitos

O SMN foi habilitado.

Restrições

As notificações de alarme são enviadas se o número de ataques for pelo menos igual ao limite configurado para um determinado período.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação à esquerda, escolha **Events**.

Passo 5 Clique na guia **Set Notification** e configure os parâmetros de notificação de alarme referindo-se a **Tabela 11-1**. **Figura 11-1** mostra um exemplo.

Figura 11-1 Configurando notificações de alarme

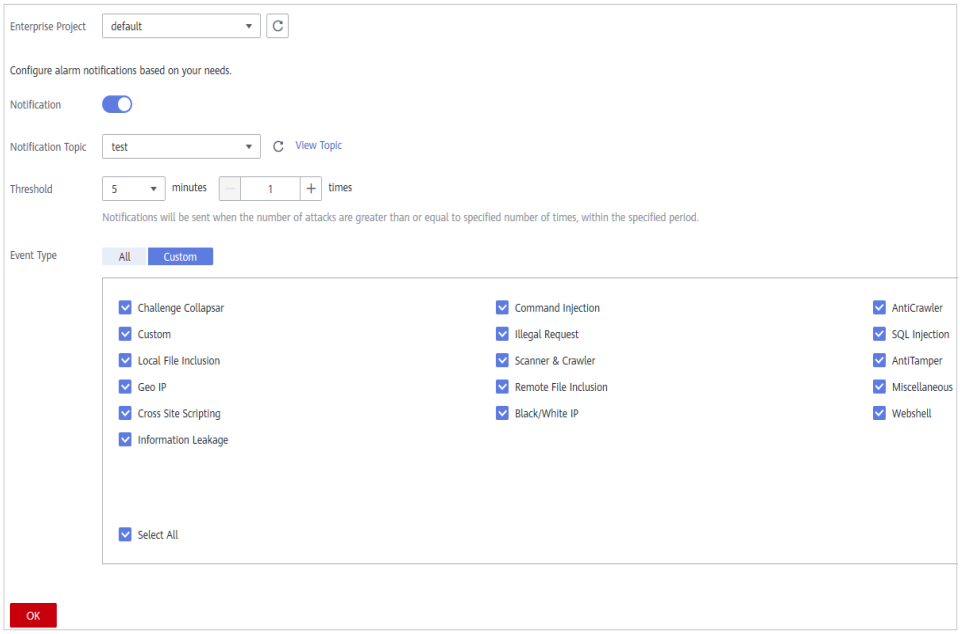


Tabela 11-1 Descrição dos parâmetros de configuração de notificação

Parâmetro	Descrição
Notificação	Se a notificação de alarme está ativada. ● : ativado. ● : desativado.
Tópico de notificação	Selecione uma chave na lista suspensa. Se não houver tópicos, clique em **View Topic** e execute as seguintes etapas para criar um tópico: 1. Crie um tópico. Para obter detalhes, consulte **Criando um Tópico**. 2. Adicione uma ou mais assinaturas ao tópico. Você precisará fornecer um número de telefone, endereço de e-mail, função, ponto de extremidade do aplicativo da plataforma, ponto de extremidade do DMS ou ponto de extremidade HTTP/HTTPS para receber notificações de alarme. Para obter detalhes, consulte **Adicionando uma assinatura**. 3. Confirme a subscrição. Depois que a assinatura for adicionada, confirme a assinatura. Para obter detalhes sobre tópicos e assinaturas, consulte o *Guia do usuário de Simple Message Notification*.
Limiar	Limite do alarme. **NOTA** As notificações de alarme são enviadas quando o número de ataques é maior ou igual ao limite dentro do período configurado.

Parâmetro	Descrição
Tipo de evento	Por padrão, **All** é selecionado. Para especificar tipos de evento, clique em **Custom**.

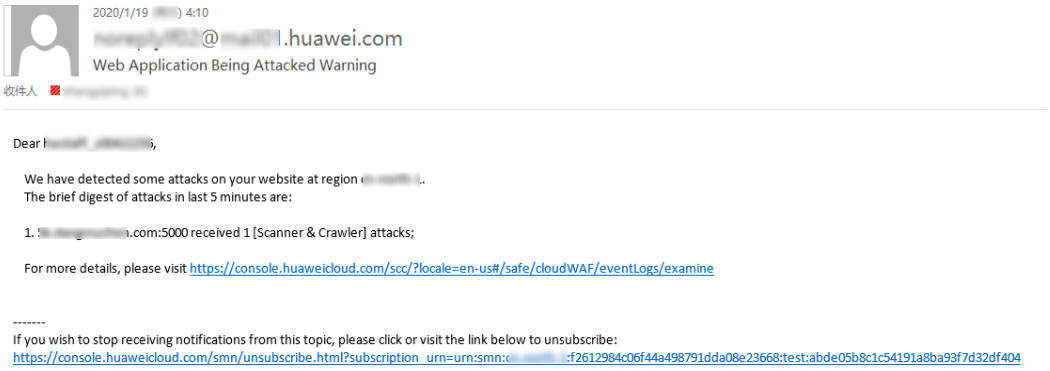
Passo 6 Clique em **OK**.

----Fim

Exemplo de e-mail de notificação de alarme

Se você ativou notificações de alarme e configurou notificações de alarme por e-mail, o WAF enviará e-mails para você relatando quaisquer ataques que ocorram. **Figura 11-2** mostra um exemplo de um e-mail de notificação de alarme.

Figura 11-2 E-mail de notificação de alarme



12 Gerenciamento de políticas

12.1 Adição de uma política

Uma política é uma combinação de regras, como proteção básica da Web, lista negra, lista branca e regras de proteção precisas. Uma política pode ser aplicada a vários nomes de domínio, mas apenas uma política pode ser usada para um nome de domínio. Este tópico descreve como adicionar uma política à sua instância do WAF.

NOTA

Se você habilitou projetos da empresa, poderá selecionar seu projeto da empresa na lista suspensa **Enterprise Project** e adicionar políticas de proteção no projeto.

Pré-requisitos

Um nome de domínio foi adicionado ao WAF. Você selecionou **Cloud mode** ou **Dedicated mode** para a implantação do site.

Restrições

Esta função não está disponível na edição padrão (anteriormente edição profissional).

Um nome de domínio de site protegido pode usar apenas uma política.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação à esquerda, escolha **Policies**.

Passo 5 No canto superior esquerdo, clique em **Add Policy**.

Passo 6 Na caixa de diálogo exibida, insira o nome da política e clique em **Confirm**. A política adicionada será exibida na lista de políticas.

Passo 7 Na coluna **Policy Name**, clique no nome da política. Na página exibida, adicione regras à política consultando **Configurações de regra**.

----Fim

Outras Operações

- Para modificar um nome de política, clique em ao lado do nome da política. Na caixa de diálogo exibida, insira um novo nome de política.
- Para excluir uma regra, clique em **Delete** na linha que contém a regra.

12.2 Adição de regras a uma ou mais políticas

Este tópico descreve como adicionar regras a uma ou mais políticas.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio em lotes.

Pré-requisitos

Um nome de domínio foi adicionado ao WAF. Você selecionou **Cloud mode** ou **Dedicated mode** para a implantação do site.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

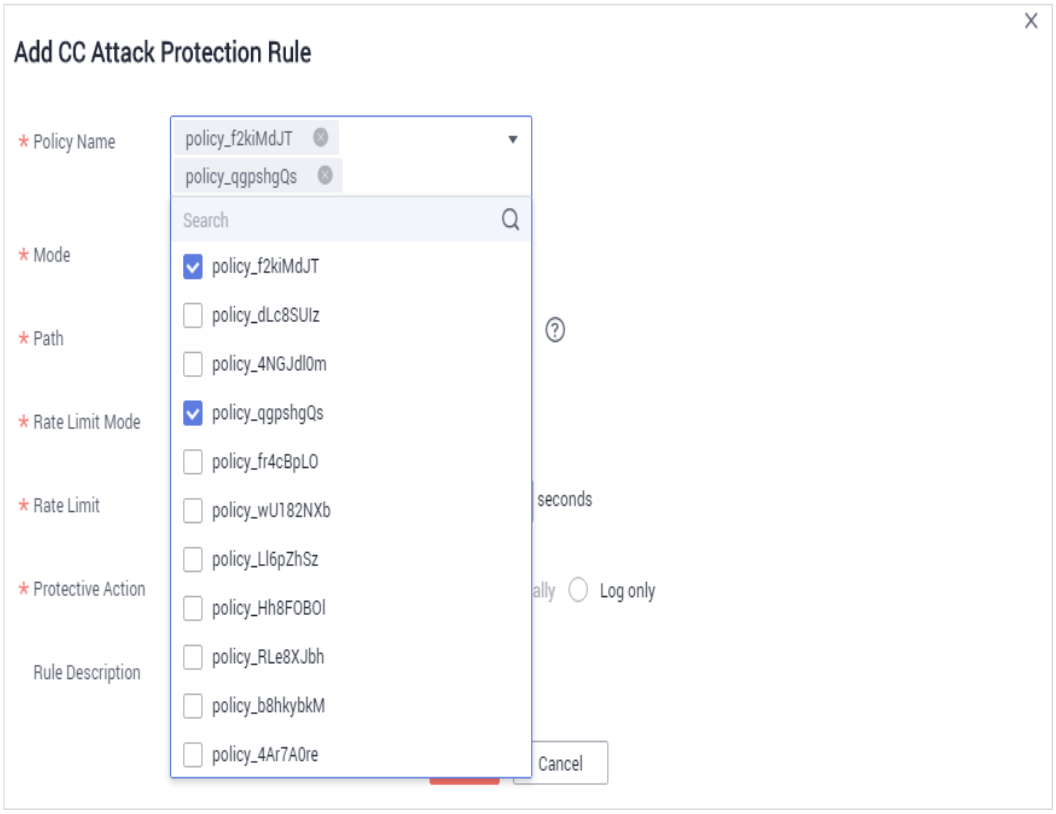
Passo 4 No painel de navegação à esquerda, escolha **Policies**.

Passo 5 No canto superior esquerdo da página, clique em **All Rules**.

Passo 6 No canto superior esquerdo acima de uma regra a ser adicionada, clique em **Add Rule**.

Passo 7 Selecione uma ou mais políticas na lista suspensa **Policy Name**. **Figura 12-1** mostra um exemplo.

Figura 12-1 Adicionar uma regra a uma ou mais políticas



Passo 8 Defina outros parâmetros.

- Para adicionar uma regra de proteção contra ataque CC, consulte **Tabela 7-7**.
- Para adicionar uma regra de proteção precisa, consulte **Tabela 7-8**.
- Para adicionar uma regra de lista negra ou de lista branca, consulte **Tabela 7-11**.
- Para adicionar uma regra de controle de acesso de geolocalização, consulte **Tabela 7-13** ou **Tabela 7-14**.
- Para adicionar uma regra WTP, consulte **Tabela 7-15**.
- Para adicionar uma regra de prevenção contra vazamento de informações, consulte **Tabela 7-18**.
- Para adicionar uma regra de lista branca de proteção global, consulte **Tabela 7-19**.
- Para adicionar uma regra de mascaramento de dados, consulte **Tabela 7-20**.

Passo 9 Clique em **OK**.

----Fim

Outras Operações

- Depois que uma regra é adicionada, a regra é **Enabled** por padrão. Para desativá-lo, clique em **Disable** na coluna **Operation** da regra de destino. Você também pode selecionar várias regras e clicar em **Disable** acima da lista de regras para desativá-las todas juntas.
- Para modificar uma regra, localize a linha que contém a regra e clique em **Modify** na coluna **Operation**. Você também pode selecionar várias regras e clicar em **Modify** acima da lista para modificá-las todas juntas.

- Para excluir uma regra, localize a linha que contém a regra e clique em **Delete** na coluna **Operation**. Você também pode selecionar várias regras e clicar em **Delete** acima da lista para excluí-las todas juntas.

12.3 Aplicação de uma política ao seu site

Este tópico descreve como aplicar uma política ao seu site protegido.

NOTA

Se você ativou projetos empresariais, certifique-se de ter todas as permissões de operação para o projeto em que sua instância do WAF está localizada. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e configurar políticas de proteção para os nomes de domínio em lotes.

Pré-requisitos

Um nome de domínio foi adicionado ao WAF. Você selecionou **Cloud mode** ou **Dedicated mode** para a implantação do site.

Restrições

Esta função não está incluída na edição padrão (anteriormente edição profissional).

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security & Compliance**.

Passo 4 No painel de navegação à esquerda, escolha **Policies**.

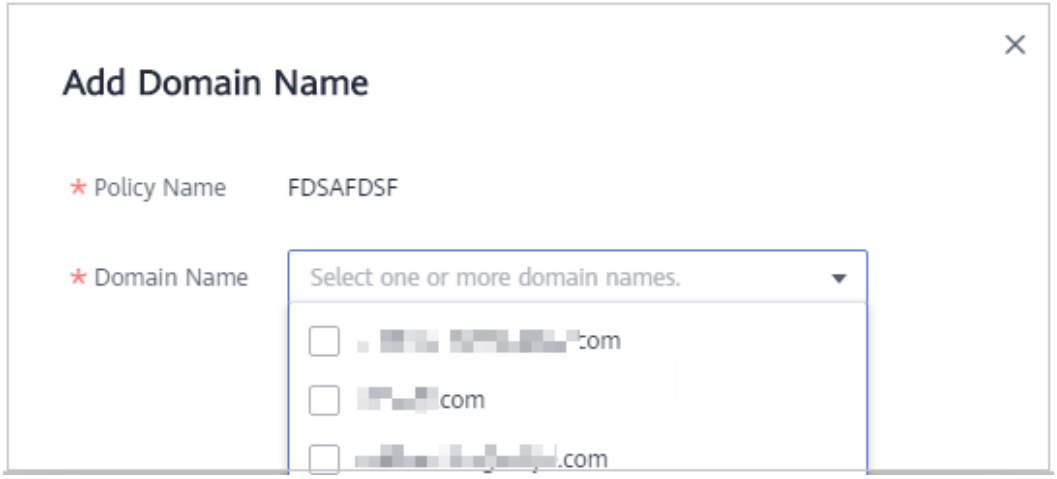
Passo 5 Na linha que contém a política que você deseja aplicar a um site, clique em **Add Domain Name** na coluna **Operation**.

Passo 6 Selecione um ou mais nomes de domínio na lista suspensa **Domain Name**. **Figura 12-2** mostra um exemplo.

AVISO

- Um nome de domínio protegido pode usar apenas uma política, mas uma política pode ser aplicada a vários nomes de domínio.
- Para eliminar uma política que tenha sido aplicada a nomes de domínio, adicione estes nomes de domínio a outras políticas primeiro. Em seguida, clique em **Delete** na coluna **Operation** da política que você deseja excluir.

Figura 12-2 Selecionar um ou mais nomes de domínio



Passo 7 Clique em **OK** .

----Fim

13 Gerenciamento dedicado do motor WAF

Este tópico descreve como gerenciar instâncias (ou mecanismos) dedicadas do WAF, incluindo a exibição de informações da instância, a exibição de configurações de monitoramento da instância, o upgrade da edição da instância ou a exclusão de uma instância.

NOTA

Se você ativou projetos corporativos, certifique-se de ter todas as permissões de operação para o projeto em que as instâncias do WAF estão localizadas. Em seguida, você pode selecionar o projeto na lista suspensa **Enterprise Project** e gerenciar instâncias WAF dedicadas no projeto.

Pré-requisitos

Você adquiriu uma instância dedicada do WAF.

Adicionando instâncias do WAF a um balanceador de carga do ELB

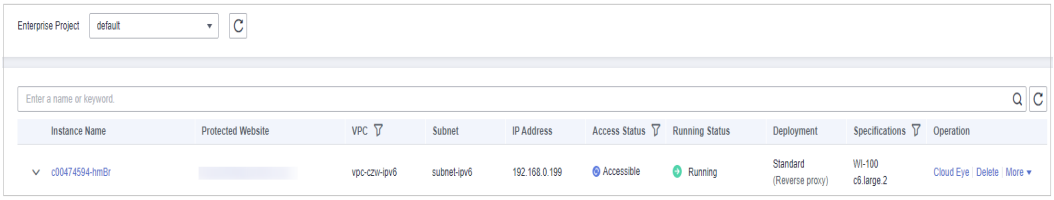
Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

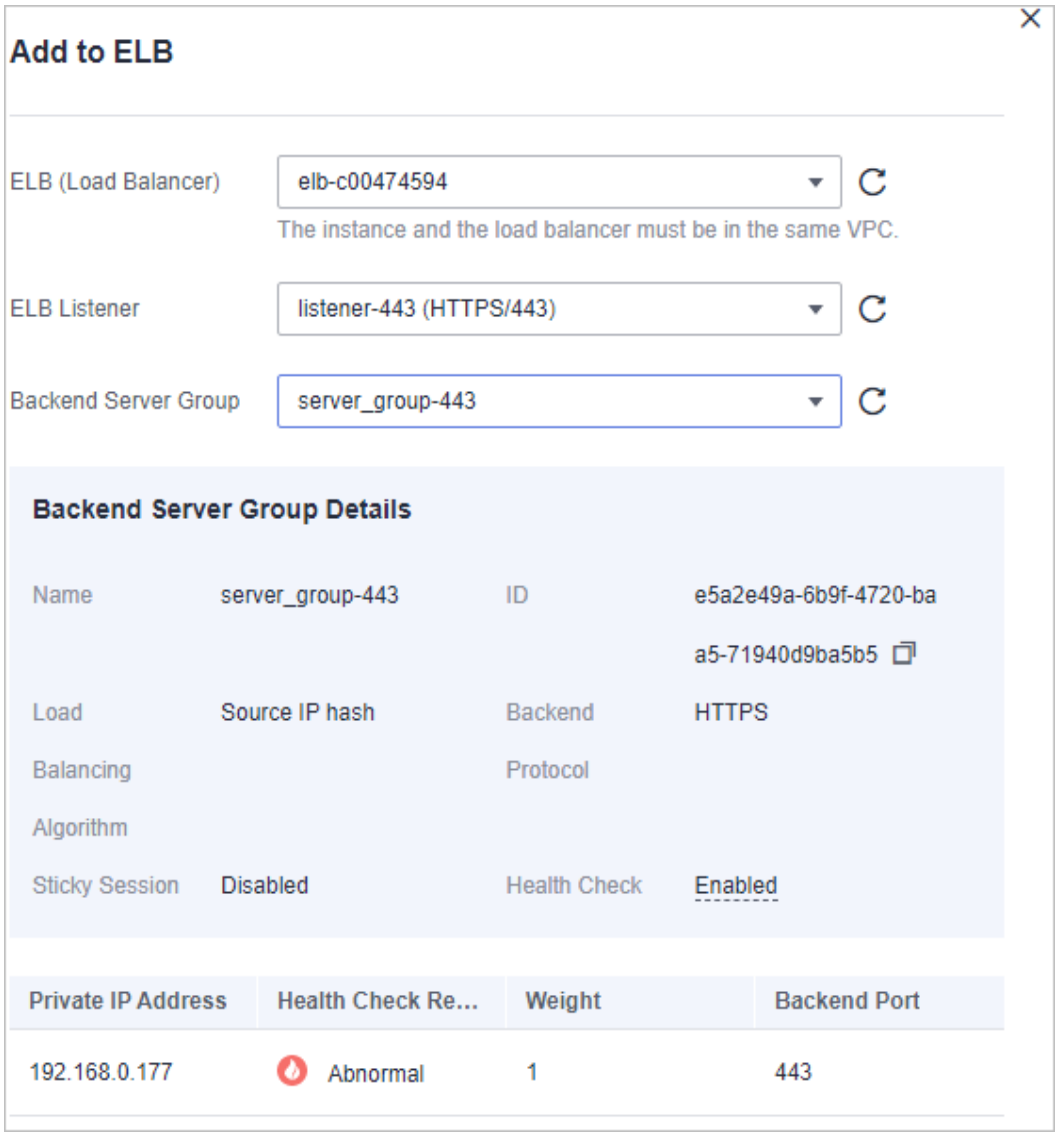
Figura 13-1 Lista de motores dedicada



Passo 5 Na linha que contém a instância que você deseja atualizar, clique em **More** > **Add to ELB** na coluna **Operation**.

Passo 6 Na caixa de diálogo **Add to ELB**, especifique **ELB (Load Balancer)**, **ELB Listener** e **Backend Server Group**. Em seguida, clique em **OK**.

Figura 13-2 Adicionar ao ELB



----Fim

Exibindo Informações Sobre uma Instância WAF Dedicada

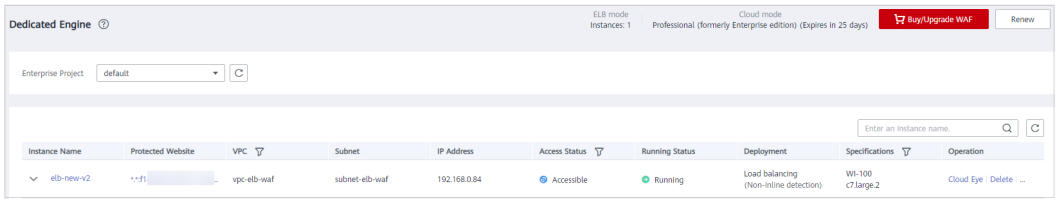
Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

Figura 13-3 Lista de motores dedicada



Passo 5 Exibir informações sobre uma instância dedicada do WAF. **Tabela 13-1** descreve os parâmetros.

Tabela 13-1 Parâmetros de uma instância dedicada

Parâmetro	Descrição	Valor de exemplo
Nome da instância	Nome gerado automaticamente quando uma instância é criada.	None
Sítio Web Protegido	Nome de domínio do site protegido pela instância.	www.example.com
VPC	VPC em que a instância reside	vpc-waf
Subnet	Subnet onde uma instância reside	subnet-62bb
Endereços de IP	Endereço de IP da sub-rede na VPC em que a instância do WAF está implantada.	192.168.0.186
Status de acesso	Status da conexão da instância.	Accessible
Estado de funcionamento	Status da instância.	Running
Implementação	Como a instância é implantada.	Standard mode (reverse proxy)
Especificações	Especificações dos recursos que hospedam a instância.	8 vCPUs | 16 GB

----Fim

Exibindo Métricas de uma Instância WAF Dedicada

Quando uma instância do WAF está no status **Running**, você pode exibir as métricas monitoradas sobre a instância.

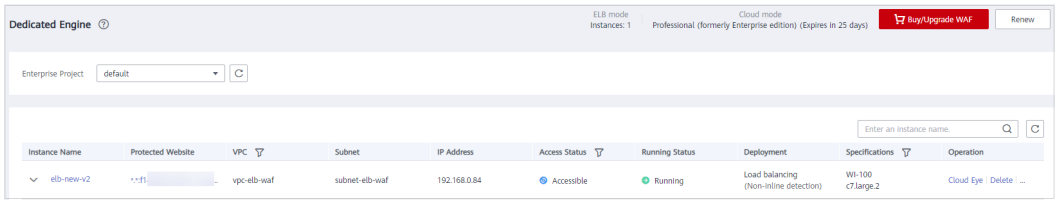
Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em ☰ no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

Figura 13-4 Lista de motores dedicada



Passo 5 Na linha da instância, clique em **Cloud Eye** na coluna **Operation** para ir até o console do Cloud Eye e exibir as informações de monitoramento, como CPU, memória e largura de banda.

----Fim

Atualizando uma Instância Dedicada do WAF

Somente instâncias dedicadas do WAF no status **Running** podem ser atualizadas para a versão mais recente.

AVISO

- Demora cerca de 5 minutos para a atualização. Antes da atualização, esteja familiarizado com as seguintes condições:
  - Se você implantar várias instâncias WAF dedicadas e configurar a política de verificação de integridade no balanceador de carga do ELB, o WAF encaminhará automaticamente o tráfego do site para outras instâncias WAF dedicadas em execução. Quase não há impacto nos serviços do seu site, exceto desconexões de solicitação intermitentes por alguns segundos.
  - Se você implantar uma instância dedicada do WAF, configure o balanceador de carga para permitir que o tráfego ignore o WAF. Isso pode evitar a interrupção do serviço causada pela atualização. Após a conclusão da atualização, configure o balanceador de carga para distribuir o tráfego para o WAF.
- Se a instância for da versão mais recente, o botão **Upgrade** ficará esmaecido.

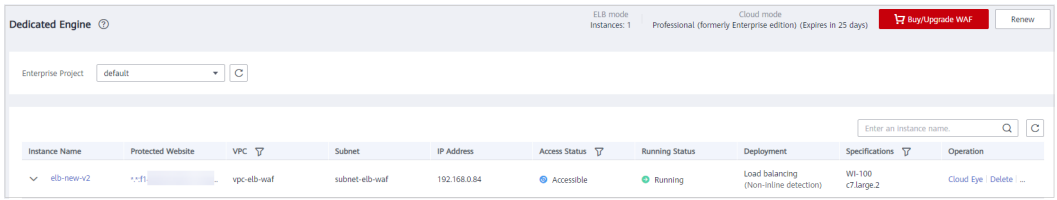
Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em ⌖ no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em ☰ no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

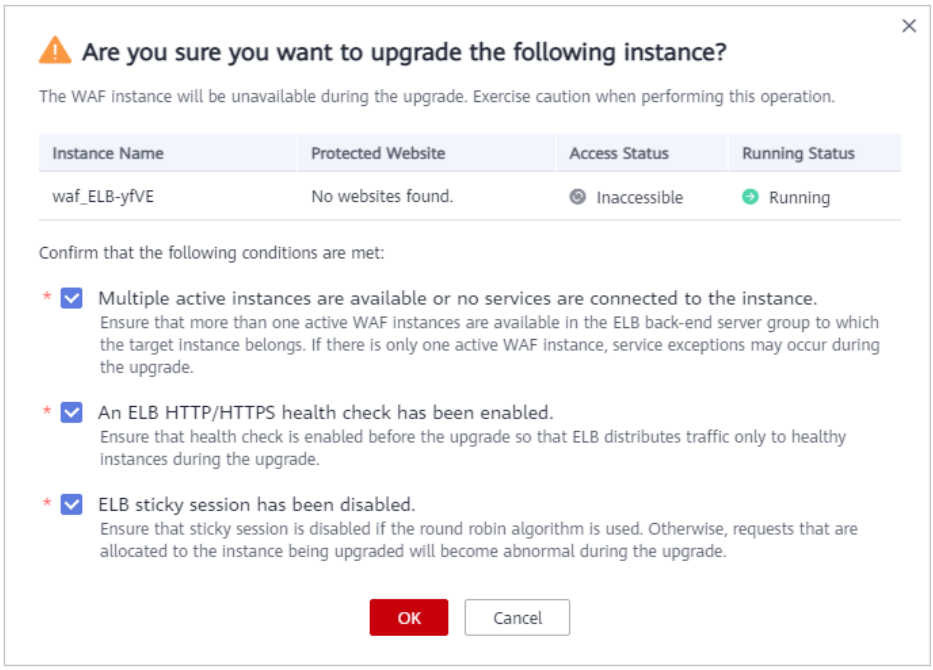
Figura 13-5 Lista de motores dedicada



Passo 5 Na linha que contém a instância que você deseja atualizar, clique em **More** > **Upgrade** na coluna **Operation**.

Passo 6 Confirme as condições de atualização e clique em **OK** .

Figura 13-6 Atualizando uma Instância Dedicada do WAF



----Fim

Alterar o grupo de segurança para uma instância dedicada do WAF

Se você selecionar **Network Interface** para **Instance Type**, poderá alterar o grupo de segurança ao qual sua instância dedicada pertence. Depois de selecionar um grupo de segurança, a instância do WAF será protegida pelas regras de acesso do grupo de segurança.

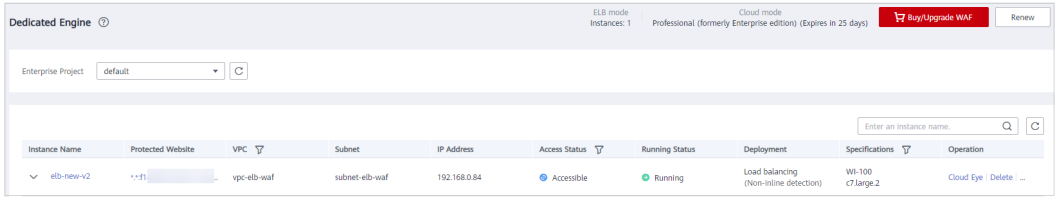
Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

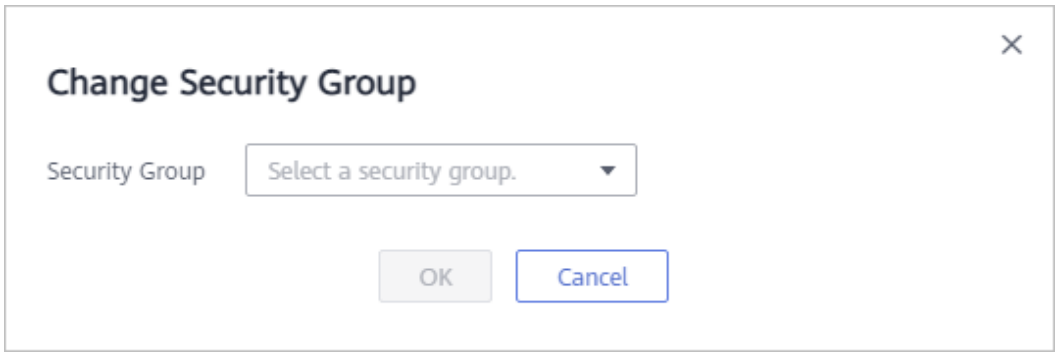
Figura 13-7 Lista de motores dedicada



Passo 5 Na linha que contém a instância, escolha **More** > **Change Security Group** na coluna **Operation**.

Passo 6 Na caixa de diálogo exibida, selecione o novo grupo de segurança e clique em **OK** .

Figura 13-8 Alterar grupo de segurança para uma instância dedicada do WAF



----Fim

Deletando uma Instância WAF Dedicada

Você pode excluir uma instância dedicada do WAF a qualquer momento. Depois que ele é excluído, a cobrança termina.

AVISO

Os recursos na instância excluída são liberados e não podem ser restaurados. Tenha cuidado ao realizar esta operação.

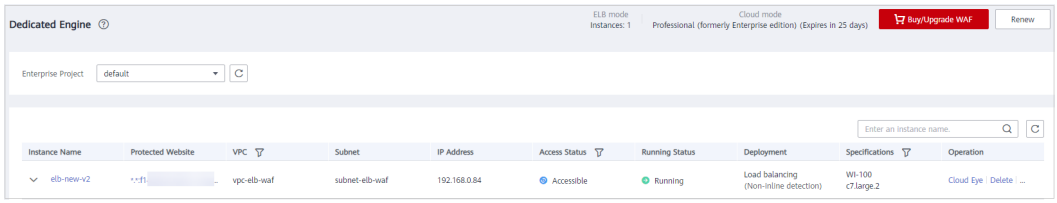
Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo, selecione uma região e escolha **Security & Compliance** > **Web Application Firewall** para acessar a página **Dashboard**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Dedicated Engine** para acessar a página dedicada da instância do WAF.

Figura 13-9 Lista de motores dedicada



Passo 5 Na linha da instância, clique em **More** > **Delete** na coluna **Operation**.

Passo 6 Clique em **OK** .

----Fim

14 Visualização de detalhes do produto

Na página **Product Details**, você pode visualizar informações sobre todas as instâncias do WAF, incluindo a edição, as cotas de domínio e as especificações.

NOTA

Se você ativou projetos corporativos, poderá selecionar seu projeto corporativo na lista suspensa **Enterprise Project** e exibir os produtos no projeto.

Pré-requisitos

Você adquiriu uma instância do WAF.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo e escolha **Web Application Firewall** em **Security**.

Passo 4 No painel de navegação à esquerda, escolha **Instance Management** > **Product Details**.

Passo 5 Na página **Product Details**, veja a edição, as especificações e o tempo de expiração do WAF.

- Clique em **Details** para visualizar as especificações detalhadas da edição atual do WAF.
- Quando você move o cursor para a edição do WAF mostrada no canto superior direito da página, as especificações são exibidas.

----Fim

15 Gerenciamento de projetos e projetos corporativos

Criando um projeto e atribuindo permissões

- Criar um projeto

  Faça login no console de gerenciamento, clique no nome de usuário no canto superior direito e selecione **Identity and Access Management**. No painel de navegação à esquerda, escolha **Projects**. No painel direito, clique em **Create Project**. Na página **Create Project** exibida, selecione uma região e insira um nome de projeto.

- Autorização

  Você pode atribuir permissões (de recursos e operações) a grupos de usuários para associar projetos a grupos de usuários. Você pode adicionar usuários a um grupo de usuários para controlar quais projetos eles podem acessar e quais recursos eles podem executar operações. Para fazer isso, realize as seguintes operações:

  a. Na página **User Groups**, localize o grupo de usuários de destino e clique em **Configure Permission** na coluna **Operation** para ir para a página **User Group Permissions**. Localize a linha que contém o projeto de destino, clique em **Configure Policy**, e selecione as políticas necessárias para o projeto.

  b. Na página **Users**, localize o usuário de destino e clique em **Modify** na coluna **Operation**. Na área **User Groups**, adicione um grupo de usuários para o usuário.

Criando um Projeto da Empresa e Atribuindo Permissões

- Criando um projeto empresarial

  No console de gerenciamento, clique em **Enterprise** no canto superior direito para ir para a página **Enterprise Management**. No painel de navegação à esquerda, escolha **Enterprise Project Management**. No painel direito, clique em **Create Enterprise Project** e insira um nome.

  NOTA

  Enterprise estará disponível no console de gerenciamento somente se você tiver ativado o projeto corporativo ou se tiver uma conta corporativa. Para usar essa função, habilite-a consultando **Ativando o Enterprise Center**.

- Autorização

  Você pode adicionar um grupo de usuários a um projeto da empresa e configurar uma política para associar o projeto da empresa ao grupo de usuários. Você pode adicionar

usuários a um grupo de usuários para controlar quais projetos eles podem acessar e quais recursos eles podem executar operações. Para fazer isso, realize as seguintes operações:

a. Localize a linha que contém o projeto empresarial de destino, clique em **More** na coluna **Operation** e selecione **View User Group**. Na página **User Groups** exibida, clique em **Add User Group**. Na caixa de diálogo **Add User Group** exibida, selecione os grupos de usuários que você deseja adicionar e mova-os para o painel direito. Clique em **Next** e selecione as políticas.

b. No painel de navegação à esquerda, escolha **Personnel Management** > **User Management**. Localize a linha que contém o usuário de destino, clique em **More** na coluna **Operation** e selecione **Add to User Group**. Na caixa de diálogo **Add to User Group** exibida, selecione os grupos de usuários para os quais as políticas foram configuradas e clique em **OK**.

- Associando o recurso a projetos corporativos

  Para usar um projeto corporativo para gerenciar recursos de nuvem, associe recursos ao projeto corporativo.

  – Associe uma instância do WAF a um projeto empresarial durante a compra.

    Na página de compra de WAF, selecione um projeto corporativo na lista suspensa **Enterprise Project**.

  – Adicione instâncias do WAF a um projeto empresarial após a compra de uma instância do WAF.

    Na página **Enterprise Project Management**, adicione instâncias WAF existentes compradas em sua conta a um projeto corporativo.

    Valor **default** indica o projeto corporativo padrão. Os recursos que não são alocados a nenhum projeto da empresa na sua conta são listados no projeto da empresa padrão.

    AVISO

    As instâncias WAF faturadas com base em pagamento por uso não podem ser adicionadas a projetos corporativos.

Para obter mais informações sobre o projeto corporativo, consulte **Guia do Usuário do Enterprise Management**.

16 Gerenciamento de permissões

16.1 Criação de um grupo de usuários e concessão de permissões

Este tópico descreve como usar o **IAM** para implementar o controle de permissões refinado para seus recursos do WAF. Com o IAM, você pode:

- Crie usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM tem suas próprias credenciais de segurança, fornecendo acesso aos recursos do WAF.
- Conceda somente as permissões necessárias para que os usuários executem uma tarefa.
- Confie uma conta da HUAWEI CLOUD ou um serviço de nuvem para realizar O&M profissional e eficiente em seus recursos WAF.

Se sua conta da HUAWEI CLOUD não exigir usuários individuais do IAM, pule este capítulo.

Pré-requisitos

Saiba mais sobre as permissões suportadas pelo WAF em **Tabela 16-1** e escolha políticas ou funções com base nas suas necessidades.

Tabela 16-1 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	

Fluxo do Processo

1. **Criar um grupo de usuários e atribuir permissões** a ele.

   Crie um grupo de usuários no console do IAM e anexe a permissão **WAF Administrator** ao grupo.

2. **Criar um usuário do IAM**.

   Crie um usuário no console do IAM e adicione o usuário ao grupo criado em **1**.

3. **Efetue login em** e verifique as permissões.

   Efetue login no console do WAF usando o usuário recém-criado e verifique se o usuário só tem permissões de **WAF Administrator** para o WAF.

   Escolha qualquer outro serviço na Lista de serviços. Se for exibida uma mensagem indicando que você não tem permissões suficientes para acessar o serviço, a política do **WAF Administrator** já entrou em vigor.

16.2 Políticas personalizadas do WAF

Políticas personalizadas podem ser criadas para complementar as políticas definidas pelo sistema do WAF. Para obter detalhes sobre as ações suportadas por políticas personalizadas, consulte **Permissões do WAF e ações suportadas**.

Você pode criar políticas personalizadas de uma das seguintes maneiras:

- Editor visual: Selecione serviços de nuvem, ações, recursos e condições de solicitação. Isso não requer conhecimento de sintaxe política.

- JSON: Edite políticas JSON do zero ou com base em uma política existente.

Para obter detalhes, consulte **Criando uma política personalizada**. A seção a seguir contém exemplos de políticas personalizadas comuns do WAF.

Exemplo de Políticas Personalizadas

- Exemplo 1: Permitindo que os usuários consultem a lista de domínios protegidos

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "waf:instance:list"
                                                        ]
                }
        ]
}
```

- Exemplo 2: Negando a solicitação do usuário de excluir regras de proteção contra violação da Web

  Uma política de negação deve ser usada em conjunto com outras políticas. Se as permissões atribuídas a um usuário contiverem "Permitir" e "Negar", as permissões "Negar" terão precedência sobre as permissões "Permitir".

  O método a seguir pode ser usado se você precisar atribuir permissões da política de **WAF FullAccess** a um usuário, mas também proibir o usuário de excluir regras de proteção contra adulteração da Web (**waf:antiTamperRule:delete**). Crie uma política personalizada com a ação de excluir regras de proteção contra adulteração da Web, defina seu **Effect** como **Deny**, e atribua essa política e a política de **WAF FullAccess** ao grupo ao qual o usuário pertence. Em seguida, o usuário pode executar todas as operações no WAF, exceto excluir as regras de proteção contra adulteração da Web. A seguir está uma política para negar a exclusão da regra de proteção contra adulteração da Web.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Deny",
                        "Action": [

"waf:antiTamperRule:delete"
                        ]
                },
        ]
}
```

- Política de multi-ação

  Uma política personalizada pode conter as ações de vários serviços que são do tipo de nível de projeto. Veja a seguir um exemplo de política que contém ações de vários serviços:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "waf:instance:get",
                                "waf:certificate:get"
                        ]
                },
               {
```



```
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:switchVersion",
                                "hss:hosts:manualDetect",
                                "hss:manualDetectStatus:get"
                        ]
                }
        ]
}
```

16.3 Permissões do WAF e ações suportadas

Este tópico descreve o gerenciamento de permissões refinado para suas instâncias do WAF. Se sua conta da HUAWEI CLOUD não precisar de usuários individuais do IAM, você pode pular esta seção.

Por padrão, os novos usuários de IAM não têm nenhuma permissão atribuída. Você precisa adicionar um usuário a um ou mais grupos e atribuir políticas de permissões 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.

Você pode conceder permissões aos usuários usando **funções** e **políticas**. As funções são fornecidas pelo IAM para definir permissões baseadas em serviço, dependendo das responsabilidades de trabalho do usuário. Políticas Um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos de nuvem específicos sob determinadas condições.

Ações Apoiadas

O WAF fornece políticas definidas pelo sistema que podem ser usadas diretamente no IAM. Você também pode criar políticas personalizadas e usá-las para complementar políticas definidas pelo sistema, implementando um controle de acesso mais refinado.

- Permissão: Uma declaração em uma política que permite ou nega determinadas operações.
- Ação: Operações específicas que são permitidas ou negadas.

Permissão	Ação	Projeto de IAM	Projeto corporativo
Consultando uma regra de prevenção contra vazamento de informações	waf:antiLeakageRule:get	√	√
Consultando uma regra de proteção contra adulteração da Web	waf:antiTamperRule:get	√	√
Consultando uma regra de proteção contra ataques CC	waf:ccRule:get	√	√
Consultar uma regra de proteção precisa	waf:preciseProtectionRule:get	√	√

Permissão	Ação	Projeto de IAM	Projeto corporativo
Consultando uma regra de lista branca de proteção global (anteriormente mascaramento de alarme falso)	waf:falseAlarmMaskRule:get	√	√
Consultando uma regra de mascaramento de dados	waf:privacyRule:get	√	√
Consultando uma regra de lista negra ou de lista branca	waf:whiteBlackIpRule:get	√	√
Consultando uma regra de controle de acesso de geolocalização	waf:geoIpRule:get	√	√
Consultando um certificado	waf:certificate:get	√	√
Modificando certificados WAF	waf:certificate:put	√	√
Aplicar um certificado a um nome de domínio	waf:certificate:apply	√	√
Consultando um evento de proteção	waf:event:get	√	√
Consultar um domínio protegido	waf:instance:get	√	√
Consultando uma política de proteção	waf:policy:get	√	√
Consultando informações do pacote de cotas	waf:bundle:get	√	√
Consultando o link de download do evento de proteção	waf:dumpEventLink:get	√	√
Consultando configurações	waf:consoleConfig:get	√	√

Permissão	Ação	Projeto de IAM	Projeto corporativo
Consultando o segmento de endereço IP de volta à origem	waf:sourceIp:get	√	√
Atualização de uma regra de prevenção de vazamento de informações	waf:antiLeakageRule:put	√	√
Atualização de uma regra de proteção contra adulteração da Web	waf:antiTamperRule:put	√	√
Atualização de uma regra de proteção contra ataques CC	waf:ccRuleRule:put	√	√
Atualização de uma regra de proteção precisa	waf:preciseProtectionRule:put	√	√
Atualizando uma regra de lista branca de proteção global (anteriormente mascaramento de alarme falso)	waf:falseAlarmMaskRule:put	√	√
Atualizando uma regra de mascaramento de dados	waf:privacyRule:put	√	√
Atualização de uma regra de lista negra ou de lista branca de endereços IP	waf:whiteBlackIpRule:put	√	√
Atualizando uma regra de controle de acesso de geolocalização	waf:geoIpRule:put	√	√
Atualizando um domínio protegido	waf:instance:put	√	√
Atualização de uma política de proteção	waf:policy:put	√	√

Permissão	Ação	Projeto de IAM	Projeto corporativo
Exclusão de uma regra de prevenção contra vazamento de informações	waf:antiLeakageRule:delete	√	√
Excluindo uma regra de proteção contra violação da Web	waf:antiTamperRule:delete	√	√
Excluindo uma regra de proteção contra ataques CC	waf:ccRule:delete	√	√
Configurando uma regra de proteção precisa	waf:preciseProtection-Rule:delete	√	√
Excluindo uma regra de lista branca de proteção global (anteriormente mascaramento de alarme falso)	waf:falseAlarmMaskRule:delete	√	√
Exclusão de uma regra de mascaramento de dados	waf:privacyRule:delete	√	√
Exclusão de uma regra de lista negra ou de lista branca	waf:whiteBlackIpRule:delete	√	√
Exclusão de uma regra de controle de acesso de geolocalização	waf:geoIpRule:delete	√	√
Excluindo um domínio protegido	waf:instance:delete	√	√
Exclusão de uma política de proteção	waf:policy:delete	√	√
Adicionando uma regra de prevenção de vazamento de informações	waf:antiLeakageRule:create	√	√

Permissão	Ação	Projeto de IAM	Projeto corporativo
Adicionando uma regra de proteção contra adulteração da Web	waf:antiTamperRule:create	√	√
Adicionando regras de proteção contra ataques CC	waf:ccRule:create	√	√
Adicionando uma regra de proteção precisa	waf:preciseProtection-Rule:create	√	√
Criando uma regra lista branca de proteção global (anteriormente mascaramento de alarme falso)	waf:falseAlarmMaskRule:create	√	√
Adicionando uma regra de mascaramento de dados	waf:privacyRule:create	√	√
Adicionando uma regra de lista negra ou de lista branca	waf:whiteBlackIpRule:create	√	√
Adicionando uma regra de controle de acesso de geolocalização	waf:geoIpRule:create	√	√
Adicionando um certificado	waf:certificate:create	√	√
Adicionando um domínio	waf:instance:create	√	√
Adicionando uma política	waf:policy:create	√	√
Consultando regras de prevenção de vazamento de informações	waf:antiLeakageRule:list	√	√
Consultando regras de proteção contra adulteração da Web	waf:antiTamperRule:list	√	√

Permissão	Ação	Projeto de IAM	Projeto corporativo
Consultando regras de proteção contra ataques da CC	waf:ccRuleRule:list	√	√
Consultar regras de proteção precisas	waf:preciseProtectionRule:list	√	√
Consultando o lista branca de proteção global (anteriormente mascaramento de alarme falso) lista de regras	waf:falseAlarmMaskRule:list	√	√
Consultando regras de mascaramento de dados	waf:privacyRule:list	√	√
Consultando regras de blacklist e whitelist	waf:whiteBlackIpRule:list	√	√
Consultando regras de controle de acesso de geolocalização	waf:geoIpRule:list	√	√
Consultando os domínios de proteção	waf:instance:list	√	√
Consultando políticas de proteção	waf:policy:list	√	√
Consultando itens de faturamento no modo nuvem	waf:subscription:get	√	√
Consultando configuração de notificação de alarme	waf:alert:get	√	√
Atualizando a configuração de notificação de alarme	waf:alert:put	√	√
Consultando cotas de log	waf:ltsConfig:get	√	√

Permissão	Ação	Projeto de IAM	Projeto corporativo
Atualizando cotas de registro	waf:ltsConfig:put	√	√
Criação de um pedido anual/mensal para uma instância no modo nuvem	waf:prepaid:create	√	√
Ativação do faturamento pay-per-use para uma instância no modo de nuvem do WAF	waf:postpaid:create	√	√
Desativar o faturamento de pagamento por uso para uma instância de modo de nuvem do WAF	waf:postpaid:delete	√	√
Exibindo detalhes de um grupo de instâncias do WAF	waf:pool:get	√	√
Modificando a configuração do grupo de instâncias do WAF	waf:pool:put	√	√
Criando um grupo de instâncias do WAF	waf:pool:create	√	√
Deletando um grupo de instâncias do WAF	waf:pool:delete	√	√
Exibindo a lista de grupos de instâncias do WAF	waf:pool:list	√	√
Consultando detalhes de vinculação de um grupo de instâncias do WAF	waf:poolBinding:get	√	√
Vinculando um grupo de instâncias do WAF	waf:poolBinding:create	√	√

Permissão	Ação	Projeto de IAM	Projeto corporativo
Desvinculação de um grupo de instâncias do WAF	waf:poolBinding:delete	√	√
Consultando detalhes de vinculação de um grupo de instâncias do WAF	waf:poolBinding:list	√	√
Consultando configurações de verificação de integridade de um grupo de instâncias do WAF	waf:poolHealthMonitor:get	√	√
Modificando a configuração de verificação de integridade de um grupo de instâncias do WAF	waf:poolHealthMonitor:put	√	√
Configurando a verificação de integridade para um grupo de instâncias do WAF	waf:poolHealthMonitor:create	√	√
Excluindo a configuração de verificação de integridade de um grupo de instâncias do WAF	waf:poolHealthMonitor:delete	√	√
Consultando configurações de verificação de integridade para grupos de instâncias do WAF	waf:poolHealthMonitor:list	√	√

17 Principais operações gravadas pelo CTS

17.1 Operações de WAF gravadas pelo CTS

O CTS fornece registros de operações no WAF. Com o CTS, você pode consultar, auditar e retroceder essas operações. Para obter detalhes, consulte o *Guia do Usuário do Cloud Trace Service*.

Tabela 17-1 lista as operações WAF registradas pelo CTS.

AVISO

Atualmente, o CTS está disponível nas seguintes regiões:

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

Tabela 17-1 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

Operação	Tipo de recurso	Nome do Rastreamento
Criando uma política WAF	política	createPolicy
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

17.2 Exibição de um rastreamento de auditoria

Depois que você habilita o CTS, o sistema inicia a gravação das operações no WAF. Os registros da operação para os últimos sete dias podem ser vistos no console CTS.

Visualizando logs do WAF no console CTS

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em no canto superior esquerdo do console de gerenciamento e selecione **Cloud Trace Service** em **Management & Governance**.

Passo 4 Escolha **Trace List** no painel de navegação.

Passo 5 Clique em **Region** no canto superior direito para definir as condições correspondentes.

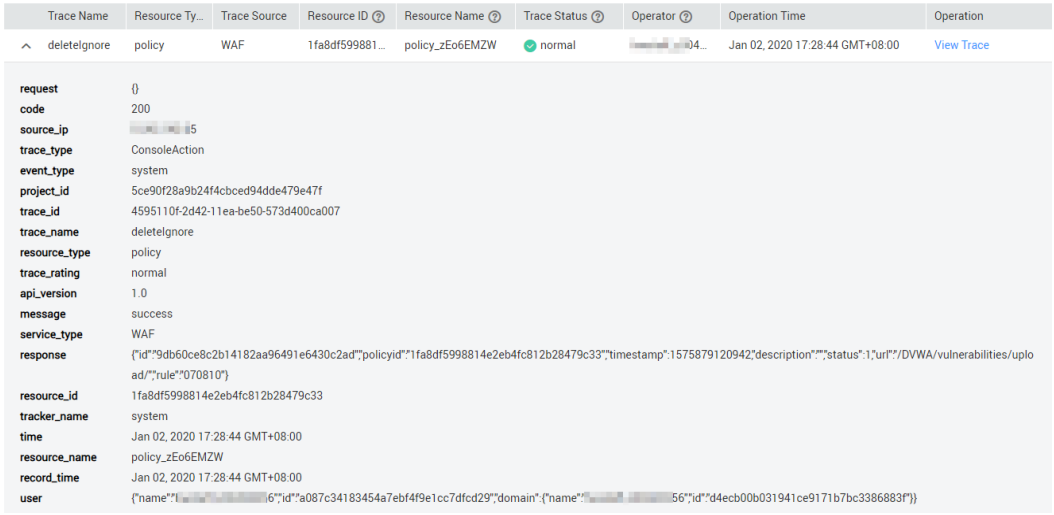
Os seguintes quatro filtros estão disponíveis:

- **Trace Type**, **Trace Source**, **Resource Type**, e **Search By**.
  - Defina **Trace Type** como **Management**.
  - Defina **Trace Source** como **WAF**.
  - Se você selecionar **Resource ID** para **Search By**, você também precisa inserir um ID de recurso.
- **Operator**: Selecione um operador específico (um usuário que não seja locatário).
- **Trace Status**: Os valores disponíveis são **All trace statuses**, **normal**, **warning**, e **incident**. Você só pode selecionar um deles.
- **Time Range**: No canto superior direito da página, você pode consultar rastreamentos na última 1 hora, no último 1 dia, na última 1 semana ou dentro de um período personalizado.

Passo 6 Clique em **Query**.

Passo 7 Clique em ⌄ à esquerda de um traço para expandir seus detalhes, como mostrado na **Figura 17-1**.

Figura 17-1 Expandindo detalhes do rastreamento



Passo 8 Clique em **View Trace** na coluna **Operation**. Na caixa de diálogo **View Trace** exibida em **Figura 17-2**, os detalhes da estrutura de rastreamento são exibidos.

Figura 17-2 Visualizando o rastreamento

----Fim

18 Monitoramento

18.1 Métricas monitoradas pelo WAF

Descrição da Função

Este tópico descreve as métricas relatadas pelo WAF para o Cloud Eye, bem como seus namespaces e dimensões. Você pode usar as API fornecidas pelo Cloud Eye para consultar as métricas do objeto monitorado e os alarmes gerados para o WAF. Você também pode consultá-los no console do Cloud Eye.

namespaces

SYS.WAF

NOTA

Um namespace é uma coleção abstrata de recursos e objetos. Vários namespaces podem ser criados em um único cluster com os dados isolados uns dos outros. Isso permite que os namespaces compartilhem os mesmos serviços de cluster sem afetar uns aos outros.

Métricas para instâncias dedicadas do WAF

Tabela 18-1 Métricas para instâncias dedicadas do WAF

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
cpu_util	CPU Usage	CPU consumida pelo objeto monitorado Unidade: percentagem (%) Método de recolha: 100% menos a porcentagem de uso da CPU ociosa	0% até 100% Tipo de valor: Flutuação	Instâncias de WAF dedicadas	1
mem_util	Memory Usage	Uso da memória do objeto monitorado Unidade: percentagem (%) Método de recolha: 100% menos porcentagem de memória ociosa	0% até 100% Tipo do valor: Flutuação	Instâncias de WAF dedicadas	1
disk_util	Disk Usage	Uso do disco do objeto monitorado Unidade: percentagem (%) Método de recolha: 100% menos porcentagem de espaço em disco ocioso	0% até 100% Tipo do valor: Flutuação	Instâncias de WAF dedicadas	1

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
disk_avail_size	Available Disk Space	Espaço em disco disponível do objeto monitorado Unidade: byte, KB, MB, GB, TB ou PB Modo de coleção: tamanho do espaço livre em disco	erro 0 bytes Tipo do valor: Flutuação	Instâncias de WAF dedicadas	1
disk_read_bytes_rate	Disk Read Rate	Número de bytes que o objeto monitorado lê do disco por segundo Unidade: byte/s, KB/s, MB/s ou GB/s Modo de coleta: número de bytes lidos do disco por segundo	≥0 byte/s Tipo do valor: Flutuação	Instâncias de WAF dedicadas	1
disk_write_bytes_rate	Disk Write Rate	Número de bytes que o objeto monitorado grava no disco por segundo Unidade: byte/s, KB/s, MB/s ou GB/s Modo de coleta: número de bytes escritos no disco por segundo	≥0 byte/s Tipo do valor: Flutuação	Instâncias de WAF dedicadas	1

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
disk_read_requests_rate	Disk Read Requests	Número de solicitações que o objeto monitorado lê do disco por segundo Unidade: Solicitações/s Modo de coleta: número de solicitações de leitura processadas pelo disco por segundo	≥0 solicitação/s Tipo do valor: Flutuação	Instâncias de WAF dedicadas	1
disk_write_requests_rate	Disk Write Requests	Número de solicitações que o objeto monitorado grava no disco por segundo Unidade: Solicitações/s Método de recolha: Número de solicitações de gravação processadas pelo disco por segundo	≥0 solicitação/s Tipo do valor: Flutuação	Instâncias de WAF dedicadas	1
network_incoming_bytes_rate	Incoming Traffic	Tráfego de entrada por segundo no objeto monitorado Unidade: byte/s, KB/s, MB/s ou GB/s Método de recolha: Tráfego de entrada pela NIC por segundo	≥0 byte/s Tipo de valor: Flutuação	Instâncias de WAF dedicadas	1

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
network_outgoing_bytes_rate	Outgoing Traffic	Tráfego de saída por segundo no objeto monitorado Unidade: byte/s, KB/s, MB/s ou GB/s Método de recolha: Tráfego de saída pela NIC por segundo	≥0 byte/s Tipo do valor: Flutuação	Instâncias de WAF dedicadas	1
network_incoming_packets_rate	Incoming Packet Rate	Pacotes recebidos por segundo no objeto monitorado Unidade: pacote/s Método de recolha: Pacotes recebidos pela NIC por segundo	≥0 pacote/s Tipo do valor: Int	Instâncias de WAF dedicadas	1
network_outgoing_packets_rate	Outgoing Packet Rate	Pacotes de saída por segundo no objeto monitorado Unidade: pacote/s Método de recolha: Pacotes de saída pela NIC por segundo	≥0 pacote/s Tipo do valor: Int	Instâncias de WAF dedicadas	1

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
concurrent_connections	Concurrent Connections	Número de conexões simultâneas sendo processadas Unidade: contagem Método de recolha: Número de conexões simultâneas no sistema	contagem ≥0 Tipo do valor: Int	Instâncias de WAF dedicadas	1
active_connections	Active Connections	Número de conexões ativas Unidade: contagem Método de recolha: Número de conexões ativas no sistema	contagem ≥0 Tipo do valor: INT	Instâncias de WAF dedicadas	1
latest_policy_sync_time	Latest Rule Synchronization	Tempo decorrido para o WAF sincronizar as regras personalizadas mais recentes Unidade: ms Método de recolha: Tempo decorrido para sincronizar com as últimas políticas	≥0 ms Tipo do valor: Int	Instâncias de WAF dedicadas	1

Métricas de monitoramento do Cloud WAF

Tabela 18-2 Métricas para WAF na nuvem

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
requests	Number of Requests	Número de solicitações retornadas pelo WAF nos últimos 5 minutos Unidade: Contagem Método de recolha: O número total de solicitações para o nome de domínio é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos
waf_http_2xx	WAF Status Code (2XX)	Número de códigos de status 2XX retornados pelo WAF nos últimos 5 minutos Unidade: Contagem Método de recolha: Número de códigos de status 2XX retornados	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
waf_http_3xx	WAF Status Code (3XX)	Número de códigos de status 3XX retornados pelo WAF nos últimos 5 minutos Unidade: Contagem Método de recolha: Número de códigos de status 3XX retornados	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5
waf_http_4xx	WAF Status Code (4XX)	Número de códigos de status 4XX retornados pelo WAF nos últimos 5 minutos Unidade: Contagem Método de recolha: Número de códigos de status 4XX retornados	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5
waf_http_5xx	WAF Status Code (5XX)	Número de códigos de status 5XX retornados pelo WAF nos últimos 5 minutos Unidade: Contagem Método de recolha: Número de códigos de status 5XX retornados	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
waf_fused_counts	WAF Traffic Threshold	Número de solicitações destinadas ao site nos últimos 5 minutos durante a duração da proteção contra avarias Unidade: Contagem Método de recolha: Número de solicitações para o nome de domínio protegido enquanto o site estava inativo	≥ 0 Tipo de valor: Flutuação	Domínio protegido dame	5
inbound_traffic	Total Inbound Traffic	Tráfego total de entrada nos últimos 5 minutos Unidade: Mbit/s Método de recolha: Tráfego total de entrada nos últimos 5 minutos	≥0 Mbit Tipo do valor: Flutuação	Domínio protegido dame	5
outbound_traffic	Total Outbound Traffic	Tráfego total de saída nos últimos 5 minutos Unidade: Mbit/s Método de recolha: Tráfego total de saída nos últimos 5 minutos	≥0 Mbit Tipo do valor: Flutuação	Domínio protegido dame	5

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
waf_process_time_0	WAF Latency [0-10) ms	Essa métrica é usada para coletar quantas solicitações são processadas pelo WAF em latências no intervalo de 0 ms a 10 ms nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações processadas pelo WAF em latências no intervalo de 0 ms a menos de 10 ms nos últimos 5 minutos é coletado.	≥ 0 Tipo de valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
waf_process_time_10	WAF Latency [10-20) ms	Essa métrica é usada para coletar quantas solicitações são processadas pelo WAF em latências no intervalo de 10 ms a menos de 20 ms nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações processadas pelo WAF em latências no intervalo de 10 ms a menos de 20 ms nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
waf_process_time_20	WAF Latency [20-50) ms	Essa métrica é usada para coletar quantas solicitações são processadas pelo WAF em latências no intervalo de 20 ms a menos de 50 ms nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações processadas pelo WAF em latências no intervalo de 20 ms a menos de 50 ms nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
waf_process_time_50	WAF Latency [50-100) ms	Essa métrica é usada para coletar quantas solicitações são processadas pelo WAF em latências no intervalo de 50 ms a menos de 100 ms nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações processadas pelo WAF em latências no intervalo de 50 ms a menos de 100 ms nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
waf_process_time_100	WAF Latency [100, 1,000) ms	Essa métrica é usada para coletar quantas solicitações são processadas pelo WAF em latências no intervalo de 100 ms a menos de 1000 ms nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações processadas pelo WAF em latências no intervalo de 100 ms a menos de 1000 ms nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
waf_process_time_1000	WAF Latency [1,000, above) ms	Essa métrica é usada para coletar quantas solicitações são processadas pelo WAF em latências acima de 1000 ms nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações processadas pelo WAF em latências acima de 1000 ms nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos
qps_peak	Peak QPS	Essa métrica é usada para coletar o pico de QPS do nome de domínio nos últimos 5 minutos. Unidade: Contagem Método de recolha: O pico de QPS do nome de domínio nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
qps_mean	Average QPS	Essa métrica é usada para coletar o QPS médio do nome de domínio nos últimos 5 minutos. Unidade: Contagem Método de recolha: O QPS médio do nome de domínio nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos
waf_http_0	No WAF Status Code	Essa métrica é usada para coletar quantas solicitações sem código de status retornadas pelo WAF nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações sem código de status WAF retornado nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
upstream_code_2xx	Status Code Returned to the Client (2XX)	Essa métrica é usada para coletar quantas solicitações com código de status *2XX* são retornadas pelo servidor de origem nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações com código de status *2XX* retornado pelo servidor de origem nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
upstream_code_3xx	Status Code Returned by the Origin Server (3XX)	Essa métrica é usada para coletar quantas solicitações com código de status *3XX* são retornadas pelo servidor de origem nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações com código de status *3XX* retornadas pelo servidor de origem nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
upstream_code_4xx	Status Code Returned by the Origin Server (4XX)	Essa métrica é usada para coletar quantas solicitações com código de status *4XX* são retornadas pelo servidor de origem nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações com código de status *4XX* retornadas pelo servidor de origem nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
upstream_code_5xx	Status Code Returned by the Origin Server (5XX)	Essa métrica é usada para coletar quantas solicitações com código de status *5XX* são retornadas pelo servidor de origem nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações com código de status *5XX* retornado pelo servidor de origem nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
upstream_code_0	No Origin Server Status Code	Essa métrica é usada para coletar quantas solicitações sem código de status retornadas pelo servidor de origem nos últimos 5 minutos. Unidade: Contagem Método de recolha: O número de solicitações sem código de status retornadas pelo servidor de origem nos últimos 5 minutos é coletado.	≥ 0 Tipo do valor: Flutuação	Domínio protegido dame	5 minutos
inbound_traffic_peak	Peak Inbound Traffic	Essa métrica é usada para coletar o pico de tráfego de entrada para o nome de domínio nos últimos 5 minutos. Unidade: Mbit/s Método de recolha: O pico de tráfego de entrada para o nome de domínio nos últimos 5 minutos é coletado.	≥0 Mbit/s Tipo de valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
inbound_traffic_mean	Average Inbound Traffic	Essa métrica é usada para coletar o tráfego médio de entrada para o nome de domínio nos últimos 5 minutos. Unidade: Mbit/s Método de recolha: O tráfego médio de entrada para o nome de domínio nos últimos 5 minutos é coletado.	≥0 Mbit/s Tipo do valor: Flutuação	Domínio protegido dame	5 minutos
outbound_traffic_peak	Peak Outbound Traffic	Essa métrica é usada para coletar o pico de tráfego de saída do nome de domínio nos últimos 5 minutos. Unidade: Mbit/s Método de recolha: O pico de tráfego de saída do nome de domínio nos últimos 5 minutos é coletado.	≥0 Mbit/s Tipo do valor: Flutuação	Domínio protegido dame	5 minutos

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
outbound_traffic_mean	Average Outbound Traffic	Essa métrica é usada para coletar o tráfego médio de saída do nome de domínio nos últimos 5 minutos. Unidade: Mbit/s Método de recolha: O tráfego médio de saída do nome de domínio nos últimos 5 minutos é coletado.	≥0 Mbit/s Tipo do valor: Flutuação	Domínio protegido dame	5

Dimensões

Chave	Valor
id_da_instância	ID da instância dedicada do WAF
waf_instance_id	ID do site protegido com WAF

Exemplo de Formato de Dados Brutos de Métricas Monitoradas

```
[
    {
        "metric": {
             // Namespace
            "namespace": "SYS.WAF",
            "dimensions": [
                {
                    // Dimension name, for example, protected website
                    "name": "waf_instance_id",
                    // ID of the monitored object in this dimension, for example,
ID of the protected website
                    "value": "082db2f542e0438aa520035b3e99cd99"
                }
            ],
           //Metric ID
            "metric_name": "waf_http_2xx"
        },
// Time to live, which is predefined for the metric
        "ttl": 172800,
         // Metric value
```



```
        "value": 0.0,
       // Metric unit
        "unit": "Count",
         // Metric value type
        "type": "float",
        // Collection time for the metric
        "collect_time": 1637677359778
    }
]
```

18.2 Configuração de regras de monitoramento de alarmes

Você pode definir regras de alarme do WAF para personalizar os objetos monitorados e as políticas de notificação e definir parâmetros como o nome da regra de alarme, o objeto monitorado, a métrica, o limite, o escopo de monitoramento e se deseja enviar notificações. Isso ajuda você a aprender o status de proteção do WAF em tempo hábil.

Pré-requisitos

Você conectou um nome de domínio ao WAF ou adquiriu uma instância dedicada do WAF.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo da página e escolha **Management & Governance** > **Cloud Eye**.

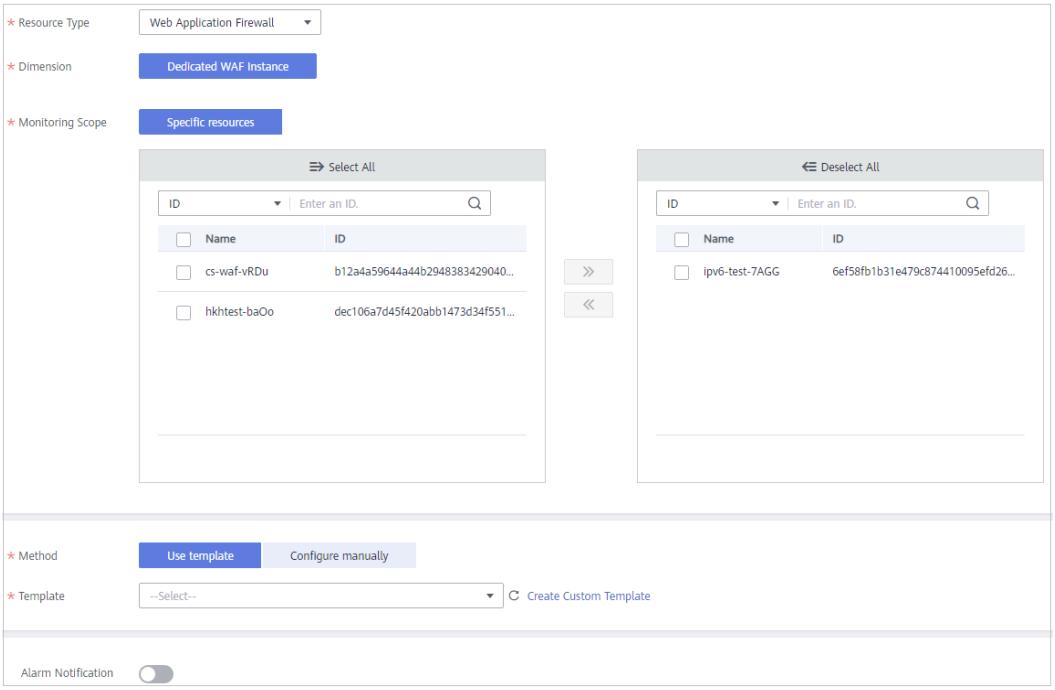
Passo 4 No painel de navegação à esquerda, escolha **Alarm Management** > **Alarm Rules**.

Passo 5 No canto superior direito da página, clique em **Create Alarm Rule**.

Passo 6 Defina o nome da regra de alarme e selecione um projeto empresarial ao qual a regra de alarme pertence.

Passo 7 Selecione **Web Application Firewall** na lista suspensa **Resource Type** e selecione uma dimensão, escopo de monitoramento, modelo de alarme e se deseja enviar uma notificação. **Figura 18-1** mostra um exemplo.

Figura 18-1 Configurando regras de monitoramento de alarmes do WAF



Passo 8 Clique em **Create**. Na caixa de diálogo exibida, clique em **OK**.

----Fim

18.3 Exibição de métricas monitoradas

Você pode visualizar as métricas do WAF no console de gerenciamento para obter informações sobre o status de proteção do WAF em tempo hábil e definir políticas de proteção com base nas métricas.

Pré-requisitos

As regras de alarme do WAF foram configuradas no Cloud Eye. Para mais detalhes, veja **Configuração de regras de monitoramento de alarmes**.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em no canto superior esquerdo da página e escolha **Management & Governance** > **Cloud Eye**.

Passo 4 No painel de navegação à esquerda, escolha **Cloud Service Monitoring** > **Web Application Firewall**.

Passo 5 Na linha que contém a instância dedicada ou o nome de domínio protegido, clique em **View Metric** na coluna **Operation**.

----Fim

