# 云防火墙

# 最佳实践

**文档版本** 07

**发布日期** 2024-03-29

**华为云计算技术有限公司**

### 商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

### 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

## 华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

# 目 录



# 1 配置入方向和出方向的访问策略

## 选择云防火墙版本

云防火墙提供了“基础版”、“标准版”、“专业版”供您使用，包括访问控制、入侵防御、流量分析以及日志审计等功能。

详细的功能介绍请参见**功能特性**

服务版本差异说明请参见**服务版本差异**

## 开启弹性公网 IP 防护

**步骤1** **登录管理控制台**。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

**步骤4** （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

**步骤5** 在左侧导航栏中，选择“资产管理 > 弹性公网IP管理”，进入“弹性公网IP管理”页面。

**步骤6** 开启弹性公网IP。

- 开启单个弹性公网IP。在所在行的“操作”列中，单击“开启防护”。
- 开启多个弹性公网IP。勾选需要开启防护的弹性公网IP，单击表格上方的“开启防护”。

**须知**

- 一个EIP只能在一个防火墙上开启防护。
- 仅支持当前账号所属企业项目下的弹性公网IP。

**步骤7** 在弹出的界面确认信息无误后，单击“绑定并开启防护”，可查看操作行的“防护状态”列显示“防护中”。

**说明**

EIP开启防护后，访问控制策略默认动作为“放行”。

**----结束**

## 开启入侵防御拦截模式

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

**步骤4** 在左侧导航栏中，选择“攻击防御 > 入侵防御” 。

**步骤5** 在入侵防御界面，页面上方的“防护模式”中，选择防御模式。

- 观察模式：仅对攻击事件进行检测并记录到日志中。
- 拦截模式：在发生明确攻击类型的事件和检测到异常IP访问时，将实施自动拦截操作。
  - 拦截模式-宽松：防护粒度较粗。拦截可信度高且威胁程度高的攻击事件。
  - 拦截模式-中等：防护粒度中等。满足大多数场景下的防护需求。
  - 拦截模式-严格：防护粒度精细，全量拦截攻击请求。建议您等待业务运行一段时间后，根据防护效果配置误报屏蔽规则，再开启“严格”模式。

**----结束**

## 配置外到内的访问策略

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

**步骤4** 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

**步骤5** 单击“添加”，在弹出“添加防护规则”对话框，配置防护规则。

- 添加放行的防护规则。在“添加防护规则”对话框，配置源IP地址，“目的”和“服务”选为“Any”，“动作”选择“放行”。

**图 1-1** 放行指定 IP


- 添加全局阻断。在“添加防护规则”对话框，配置为“Any”，动作选择阻断，始终保持该条规则优先级最低。

**图 1-2** 拦截所有流量


**----结束**

## 配置内到外的访问策略

**步骤1** **登录管理控制台**。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

**步骤4** 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

**步骤5** 单击“添加”，在弹出“添加防护规则”对话框，配置防护规则。

- 添加放行的防护规则。在“添加防护规则”对话框，配置源IP地址，“目的”和“服务”为“Any”，“动作”选择“放行”。

**图 1-3** 放行指定 IP（内到外）


- 在“添加防护规则”对话框，配置“源”为“Any”，“目的”选择“域名”，“服务”为“Any”，“动作”选择“放行”。

**图 1-4** 内到外流量放行策略（域名）


- 添加全局阻断。在“添加防护规则”对话框，“源”、“目的”和“服务”配置为“Any”，“动作”选择“阻断”，始终保持该条规则优先级最低。

**图 1-5** 拦截所有流量（内到外）


**----结束**

## 查看防护效果

查看防护详情请参见**查看防护详情**。

# 2 配置 IP 地址组和服务组访问策略

当防护对象成功接入云防火墙后，您可以配置IP地址组和服务组的访问控制策略，以验证配置的组规则是否生效，即验证配置访问控制策略的访问控制效果。本实践以配置IP地址组和服务组为例，说明如何批量配置IP地址和服务访问控制策略。

## 应用示例

例如，您的业务部署在企业，由于IP地址和服务有多个，针对多个IP地址和服务在同一个企业的业务场景，为了确保业务正常运行，您需要对用户的IP地址组和服务组统一配置访问控制策略，以放行或阻断访问请求，提升云防火墙防护效果。

## 前提条件

- 防护网站已成功接入云防火墙。
- 已开启“入侵防御”，且防护模式为“拦截”。

## 配置访问控制策略

- 添加IP地址组请参见**添加IP地址组**。
- 添加服务组请参见**添加服务组**。
- 添加防护规则请参见**添加防护规则**。

## 查看防护效果

查看防护详情请参见**查看防护详情**。

# 3 配置 VPC 边界防火墙

## 应用场景

VPC边界防火墙能够检测和统计VPC间的通信流量数据，帮助您发现异常流量。

## 约束条件

- 仅“专业版”支持VPC边界防火墙。
- 依赖企业路由器（Enterprise Router, ER）服务引流。
- 仅支持防护当前账号所属企业项目下的VPC。
- 如果您存在私用公网(即使用10.0.0.0/8、 172.16.0.0/12、192.168.0.0/16 以及运营商级NAT保留网段100.64.0.0/10 以外的公网网段作为私网地址段)的情况，请您**提交工单**进行私网网段扩容，否则云防火墙可能无法正常转发您VPC间的流量。

## 适用版本

新版VPC边界防火墙

**说明**

判断方法：

通过创建VPC边界防火墙的界面区分，界面如**图 VPC边界防火墙（新版）**所示为新版VPC边界防火墙，界面如**图 创建VPC间防火墙（旧版）**所示为旧版VPC边界防火墙。

**图 3-1** VPC 边界防火墙（新版）

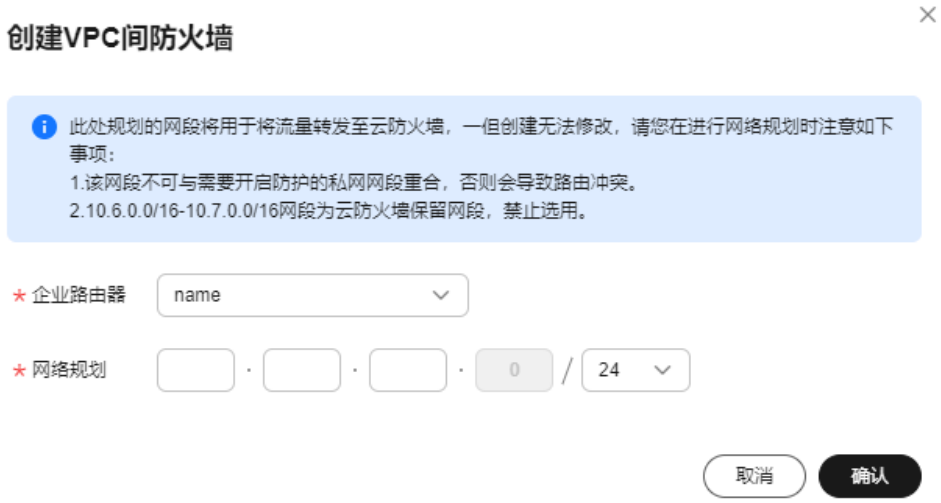
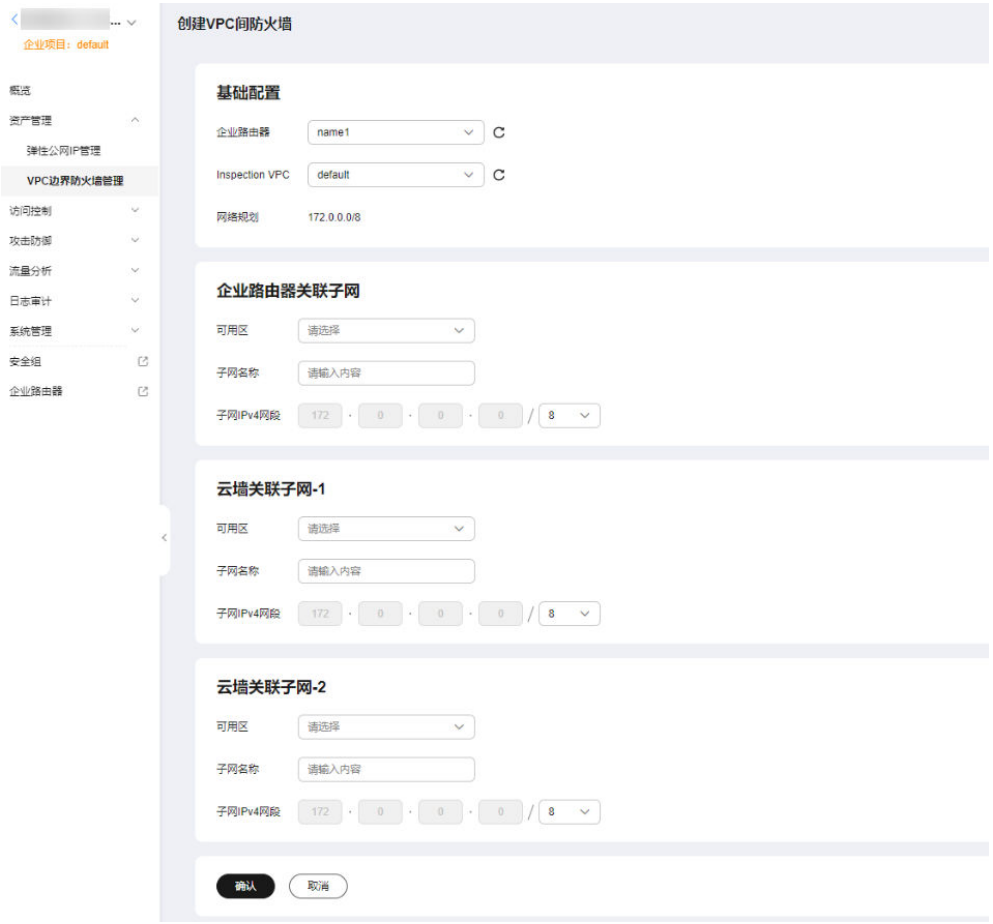



**图 3-2** 创建 VPC 边界防火墙（旧版）

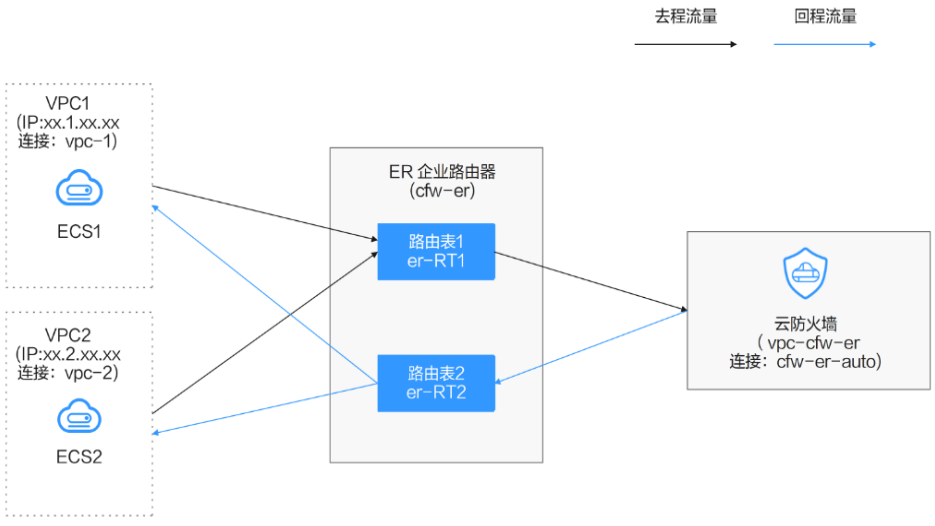


## 配置原理

您需要按以下步骤操作：

1. 创建防火墙（以命名vpc-cfw-er为例）并关联子网，请参见**创建防火墙**。
2. 如您新创建了企业路由器，请参见**配置企业路由器（新创建企业路由器）**，分解操作如下：
   a. 配置所有VPC（包括防火墙VPC和需要互联的VPC）的路由转向企业路由器，请参见**3 将路由转向企业路由器。**
   b. 创建所有VPC（包括防火墙VPC和需要互联的VPC）的连接，请参见**5 添加连接**。
   c. 创建两个路由表(以er-RT1和er-RT2为例)，请参见**6 创建两个路由表**。
   d. 配置关联路由表er-RT1将流量从VPC传输到云防火墙，请参见**7 配置路由表er-RT1**。
      配置传播路由表er-RT2将流量从云防火墙传输到VPC，请参见**8 配置路由表er-RT2**。
   e. 开启防护前，需验证流量只通过企业路由器时正常通信，请参见**配置验证方法**。
3. 如您企业路由器已产生流量，请参见**配置企业路由器（已有企业路由器）**，分解操作如下：
   a. 创建防火墙VPC(vpc-cfw-er)的连接，请参见**4. 添加防火墙连接**。
   b. 从默认路由表(er-RT1)中删除自动生成的防火墙VPC(vpc-cfw-er)的关联和传播功能，请参见**删除关联和传播**。
   c. 创建一个新的路由表(er-RT2)，并配置关联和传播功能，请参见**6. 创建路由表er-RT2**和**7 配置路由表er-RT2**。
   d. 配置默认路由表(er-RT1)的静态路由及删除表中所有的传播，请参见**8. 配置默认路由表er-RT1**。
   e. （可选）设置传播路由表为er-RT2后，添加新VPC只需添加连接，无需其他配置，设置传播路由表请参见**9 更改传播路由表**。

**图 3-3** 流量走势图



## 创建防火墙

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航树中，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

**步骤4** 在左侧导航栏中，选择“资产管理 > VPC边界防火墙管理”，进入“VPC边界防火墙管理”页面。

**步骤5** 单击“创建防火墙”，选择企业路由器并配置合适的网段。

- 企业路由器用于引流，选择时需满足以下限制：
  - 没有与其他防火墙实例关联。
  - 需归属本账号，非共享企业路由器。
  - 需关闭“默认路由表关联”、“默认路由表传播”和“自动接收共享连接”功能。
- 网段配置后默认创建InspectionVPC将流量转发至云防火墙，并自动分配云墙关联子网，将云防火墙流量转发到企业路由器，选择时需注意以下限制：
  - 创建防火墙后不支持修改网段。
  - 该网段需满足以下条件：
    - 仅支持私网地址段（即在10.0.0.0/8、172.16.0.0/12、192.168.0.0/16范围中），否则可能在SNAT等访问公网的场景下产生路由冲突，
    - 10.6.0.0/16-10.7.0.0/16网段为防火墙保留网段，不可使用。
    - 不可与需要开启防护的私网网段重合，否则会因路由冲突，导致该网段无法防护。

**步骤6** 单击“确认”，需等待3-5分钟，完成防火墙创建。

**----结束**

## 配置企业路由器（新创建企业路由器）

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 配置VPC（VPC1、VPC2、vpc-cfw-er）的路由表转向企业路由器。

在左侧导航栏中，选择“网络 > 虚拟私有云 > 路由表”，进入“路由表”页面，在“名称”列，单击对应VPC的路由表名称。

单击“添加路由”，参数详情见**表 添加路由参数说明**。

**表 3-1** 添加路由参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 目的地址 | 目的地址网段。<br>**须知**<br>不能与已有路由和VPC下子网网段冲突。 | xx.xx.xx.0/16 |
| 下一跳类型 | 在下拉列表中，选择类型“企业路由器”。 | 企业路由器 |
| 下一跳 | 选择下一跳资源。<br>下拉列表中将展示您创建的企业路由器名称。 | cfw-er |
| 描述 | 路由的描述信息，非必填项。<br>**说明**<br>描述信息内容不能超过255个字符，且不能包含“<”和“>”。 | - |

**步骤4** 选择“网络 > 企业路由器”，进入“企业路由器”页面。

在企业路由器中添加VPC连接，操作步骤请参见**企业路由器中添加VPC连接**。

**说明**

- 至少需要添加三条VPC连接（CFW及两个防护的VPC）；每增加一个防护的VPC，都需要增加一条连接。

  例如：对防火墙连接命名为cfw-er-auto（创建防火墙后自动生成）;对VPC1连接命名为vpc-1；对VPC2连接命名为vpc-2，需防护VPC3时，增加连接命名为vpc-3。
- 如需防护其他账号（如账号B）下的VPC，请将当前账号A的企业路由器共享至账号B，共享步骤请参见**创建共享**，共享成功后在账号B中添加连接，后续配置仍在账号A中进行。
- 后文示例：对防火墙连接命名为cfw-er-auto（创建防火墙后自动生成）;对VPC1连接命名为vpc-1；对VPC2连接命名为vpc-2。

**步骤5** 创建两个路由表er-RT1和er-RT2分别用于连接需防护的VPC和连接防火墙。

单击企业路由器名称，进入“基本信息”页面，“路由表”页签，进入路由表设置页面，单击“创建路由表”。

参数详情见**表 创建路由表参数说明**。

**表 3-2** 创建路由表参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 输入路由表的名称。要求如下：<br>• 长度范围为1~64位。<br>• 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。 | er-RT1/er-RT2 |
| 描述 | 您可以根据需要在文本框中输入对该路由表的描述信息。 | - |

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 标签 | 您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。<br>关于标签更详细的说明，请参见**标签概述**。 | “标签键”：test<br>“标签值”：01 |

**步骤6** 配置关联路由表er-RT1：设置关联和路由功能。

1. 在路由表设置页面，选择用于连接需防护VPC的路由表(er-RT1)，单击“关联”页签，单击“创建关联”。
   如**图 创建关联**，参数详情见**表 创建关联参数说明**。

**图 3-4** 创建关联


**表 3-3** 创建 VPC1 关联参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 | 虚拟私有云（VPC） |
| 连接 | 在连接下拉列表中，选择需防护的VPC连接。 | vpc-1 |

**表 3-4** 创建 VPC2 关联参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 | 虚拟私有云（VPC） |
| 连接 | 在连接下拉列表中，选择需防护的VPC连接。 | vpc-2 |

2. 创建同一路由表(er-RT1)的路由功能。单击“路由”页签，单击“创建路由”，根据实际数量创建路由功能。

   如图 创建路由，参数详情见表 创建路由参数说明。

**图 3-5** 创建路由


**表 3-5** 创建路由参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 目的地址 | 设置目的地址，设置为：0.0.0.0/0。 |
| 黑洞路由 | 建议您保持关闭状态；开启后如果路由匹配上黑洞路由的目的地址，则该路由的报文会被丢弃。 |
| 连接类型 | 选择连接类型“云防火墙（CFW）”。 |
| 下一跳 | 在下拉列表中，选择自动生成的防火墙连接（cfw-er-auto-attach）。 |

**步骤7** 配置传播路由表er-RT2：设置关联和传播功能。

1. 在路由表设置页面，单击“关联”页签，选择用于连接防火墙的路由表(er-RT2)，单击“创建关联”。

   如图 创建关联，参数详情见表 创建关联参数说明 。

**图 3-6** 创建关联


**表 3-6** 创建关联参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 连接类型 | 选择连接类型“云防火墙（CFW）”。 |
| 连接 | 在下拉列表中，选择自动生成的防火墙连接（cfw-er-auto-attach）。 |

2. 创建同一路由表(er-RT2)的传播功能。单击“传播”页签，单击“创建传播”.。如图 创建传播，参数详情见表 创建传播参数说明。

**图 3-7** 创建传播


**表 3-7** 创建传播参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 | 虚拟私有云（VPC） |

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 传播 | 在传播下拉列表中，选择需防护的VPC连接。 | vpc-1 |

**表 3-8** 创建传播参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 | 虚拟私有云（VPC） |
| 传播 | 在传播下拉列表中，选择需防护的VPC连接。 | vpc-2 |

**说明**

- 传播至少需要添加两条，每增加一个防护的VPC，都需增加一条传播。
  例如：选择VPC1的连接vpc-1以及VPC2的连接vpc-2，需防护VPC3时，增加一条传播，选择连接vpc-3。
- 创建传播后，会自动将连接的路由信息学习到ER路由表中，生成“传播路由”。同一个路由表中，不同传播路由的目的地址可能相同，连接配置不支持修改和删除。
- 您也可以手动在路由表中配置连接的静态路由，同一个路由表中，静态路由的目的地址不允许重复，连接配置支持修改和删除。
- 如果路由表中存在多条路由目的地址相同，则优先级：静态路由 > 传播路由。

**----结束**

## 配置验证方法

**前提条件**

- 已完成全部配置步骤。
- 两个VPC中各有一台ECS。

**验证方式**

VPC中的ECS互相*ping*，确定流量未经过防火墙时是否正常通信。

**故障定位**

**步骤1** 企业路由器的两个路由表配置是否正确。正确配置方式请参见**配置企业路由器操作步骤7**和**配置企业路由器操作步骤8**。

**步骤2** 检查VPC1和VPC2的默认路由表是否将路由转向企业路由器。配置方式请参见**配置企业路由器操作步骤3**。

**----结束**

## 配置企业路由器（已有企业路由器）

**适用场景**

用户当前已有企业路由器（例如vpc-cfw-er），产生流量并开启默认路由表(er-RT1)关联和传播功能，不适用标准方案时可执行此方案。

**操作步骤**

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航栏中，选择“网络 > 企业路由器”，进入“企业路由器”页面。

**步骤4** 添加防火墙连接。

单击企业路由器右上方“管理连接”，进入“连接”页面。单击“添加连接”,弹出“添加连接”对话框，填写参数如表 添加连接参数说明所示，添加后自动生成防火墙VPC的关联和传播功能。

**表 3-9** 添加连接参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 输入连接的名称。要求如下：<br>• 长度范围为1~64位。<br>• 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。 | cfw-er-auto |
| 连接类型 | • 连接类型：虚拟私有云（VPC）。<br>• 虚拟私有云：下拉列表中选择创建的防火墙。<br>• 子网：选择云防火墙关联的子网。 | • 连接类型：虚拟私有云（VPC）<br>• 虚拟私有云：vpc-cfw-er<br>• 子网：cfw-er-1（xx.xx.1.0/24） |
| 配置连接侧路由 | • 开启：在虚拟私有云的所有路由表中自动添加指向企业路由器的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。<br>• 关闭：如果虚拟私有云路由表中的路由与这三个网段冲突，则会添加失败。此时建议您不要开启该选项，并在企业路由器创建完成后，手动在VPC路由表配置路由。 | 开启 |
| 描述 | 您可以根据需要在文本框中输入对该路由表的描述信息。 | - |
| 标签 | 您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。<br>关于标签更详细的说明，请参见标签概述。 | “标签键”：test<br>“标签值”：01 |

**步骤5** 从默认路由表er-RT1中删除防火墙VPC(vpc-cfw-er)的关联和传播。

选择“路由表 > 关联”，在防火墙VPC行的“操作”列，单击“删除”，在删除确认框中，单击“是”。

选择“传播”，在防火墙VPC行的“操作”列，单击“删除”，在删除确认框中，单击“是”。

**步骤6** 创建路由表er-RT2。

单击页面左上角“创建路由表”。

参数详情见**表 创建路由表参数说明**。

**表 3-10** 创建路由表参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 输入路由表的名称。要求如下：<br>• 长度范围为1~64位。<br>• 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。 | er-RT2 |
| 描述 | 您可以根据需要在文本框中输入对该路由表的描述信息。 | - |
| 标签 | 您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。<br>关于标签更详细的说明，请参见**标签概述**。 | “标签键”：test<br>“标签值”：01 |

**步骤7** 配置路由表er-RT2：设置关联和传播功能。

1. 选择路由表er-RT2，单击“关联”页签，单击“创建关联”。
   如**图 创建关联**，参数详情见**表 创建关联参数说明** 。

**图 3-8** 创建关联

**表 3-11** 创建关联参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 连接类型 | 选择连接类型“云防火墙（CFW）”。 | 虚拟私有云（VPC） |
| 关联 | 在连接下拉列表中，选择防火墙VPC的连接。 | cfw-er-auto |

2. 创建同一路由表(er-RT2)的传播功能。单击“传播”页签，单击“创建传播”.。如**图 创建传播**，参数详情见**表 创建传播参数说明**。

**图 3-9** 创建传播


**表 3-12** 创建传播参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 | 虚拟私有云（VPC） |
| 传播 | 在传播下拉列表中，选择需防护的VPC连接。 | vpc-1 |

**表 3-13** 创建传播参数说明

| 参数名称 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 | 虚拟私有云（VPC） |
| 传播 | 在传播下拉列表中，选择需防护的VPC连接。 | vpc-2 |

**说明**

- 传播至少需要添加两条，每增加一个防护的VPC，都需增加一条传播。

  例如：选择VPC1的连接vpc-1以及VPC2的连接vpc-2，需防护VPC3时，增加一条传播，选择连接vpc-3。
- 创建传播后，会自动将连接的路由信息学习到ER路由表中，生成“传播路由”。同一个路由表中，不同传播路由的目的地址可能相同，连接配置不支持修改和删除。
- 您也可以手动在路由表中配置连接的静态路由，同一个路由表中，静态路由的目的地址不允许重复，连接配置支持修改和删除。
- 如果路由表中存在多条路由目的地址相同，则优先级：静态路由 > 传播路由。

**步骤8** 配置默认路由表er-RT1：

1. 添加静态路由。选择路由表er-RT1，单击“路由”页签，单击“创建路由”，填写信息如下：
   - 目的地址：0.0.0.0/0
   - 连接类型：“云防火墙（CFW）”
   - 下一跳：选择防火墙VPC的连接（cfw-er-auto）

   **图 3-10** 添加静态路由

2. 删除路由表er-RT1中的传播。

   单击“传播”页签，在“操作”列中，单击“删除”，在删除确认框中，单击“是”。

   **说明**

   需删除路由表er-RT1中所有传播。

**步骤9** 可选操作。建议您将当前企业路由器的传播路由表改为新创建的路由表（er-RT2），后续添加新VPC时，仅需添加连接，无需进行其他操作。

返回或进入“企业路由器”，单击“更多 > 修改配置”，选择传播路由表为er-RT2。如图3-11所示。

**图 3-11** 修改配置


**说明**

如需防护其他账号（如账号B）下的VPC，请将当前账号A的企业路由器共享至账号B，共享步骤请参见**创建共享**，共享成功后在账号B中添加连接即可完成配置。

**----结束**

# 4 如何使用 CFW 防护 SNAT 场景

## 4.1 SNAT 防护概述

### 背景信息

云防火墙标准版实现公网IP之间的防护，例如通过NAT网关实现多个VPC/子网使用公网IP对外发起访问的场景，云防火墙专业版提供更细粒度的访问控制，例如使用私网IP对公网发起访问的场景。

本文介绍如何配置云防火墙专业版实现SNAT场景下私网IP对公网发起访问的防护。

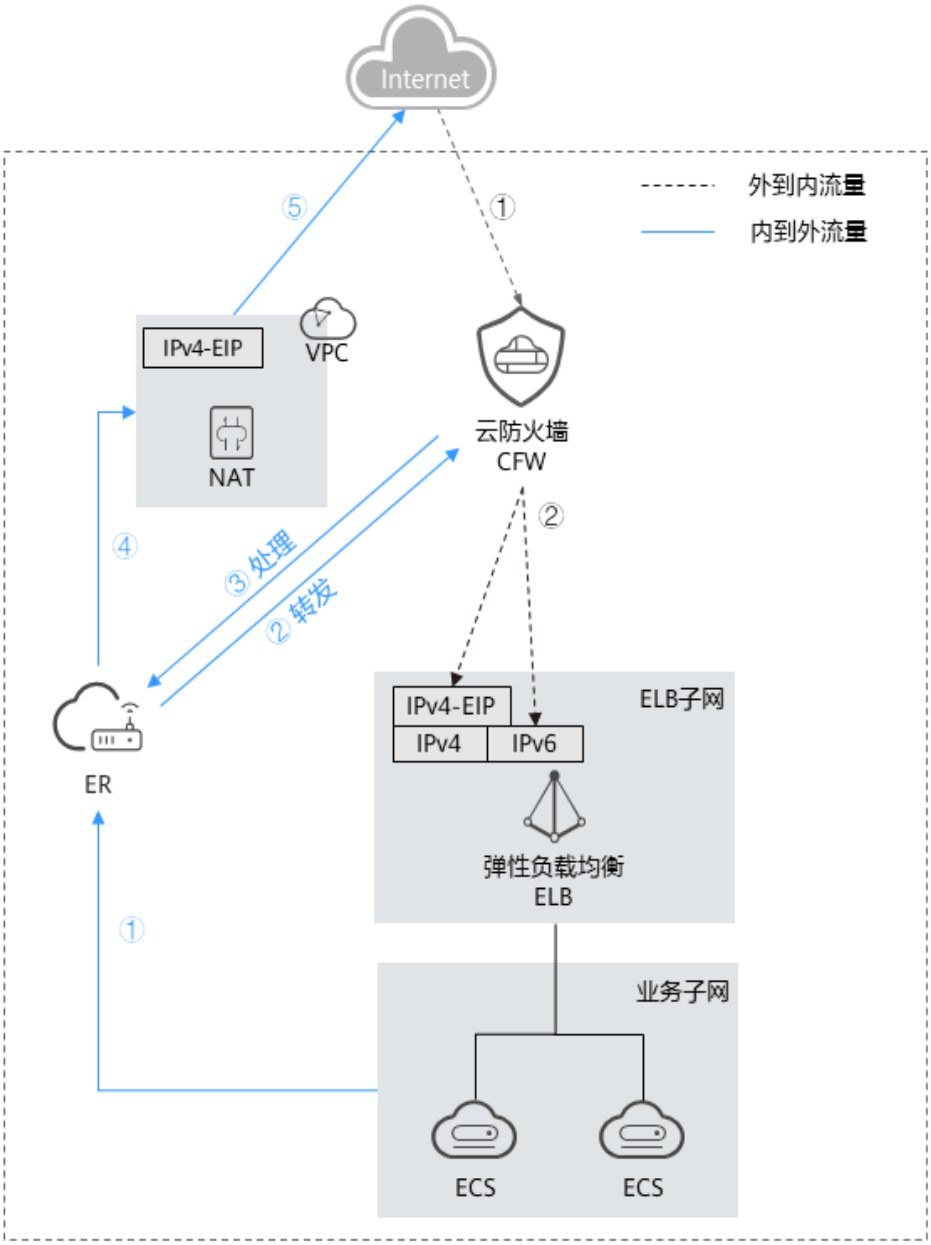
### 前提条件

- 配置中需要使用企业路由器（Enterprise Router, ER），关于企业路由器请参见**什么是企业路由器?**。
- 需完成创建防火墙，具体配置请参见**创建防火墙**。

### 约束条件

- 仅“专业版”支持私网IP的访问控制。
- 云防火墙当前默认支持标准私网网段，如需开通非标网段通信，请提交工单申请。

## SNAT 防护组网图




**说明**

请求流量和响应流量为同一个路径。

## 配置建议

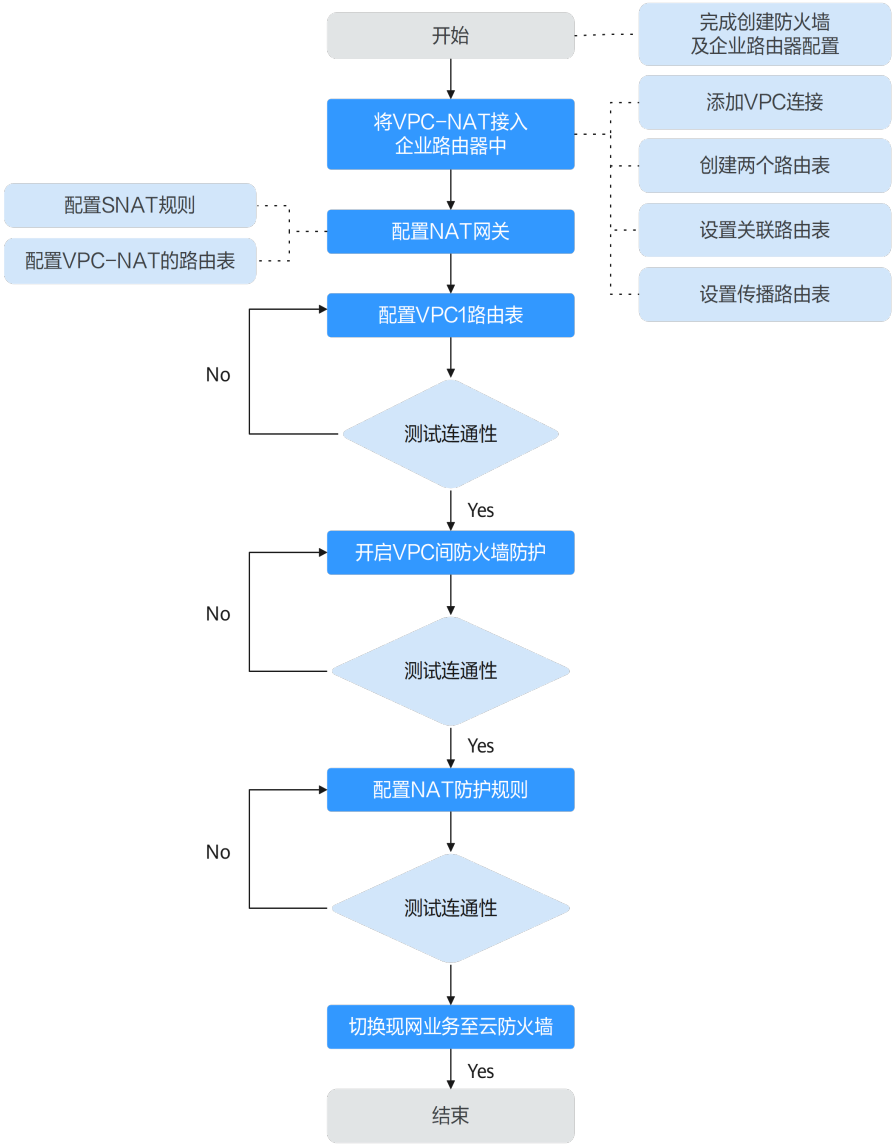
- 建议为NAT网关创建独立VPC不用于云服务器等实例网络配置，避免影响后续的访问控制。
- 在前期网络规划复杂甚至不合理的情况下（例如存在VPC网段重叠、NAT网关已有复杂配置、已通过VPC-Peering配置东西向通信等场景下），请充分评估网络互连、环路、路由冲突等风险。

- 因涉及组件多，不建议直接将现网业务导入，可先创建测试机，并在业务VPC路由表中配置目的地址路由，利用业务VPC中的测试机验证整个业务流是否走通及配置的规则是否有效，再对现网业务进行切流。
- 使用云防火墙后，避免第一时间配置拦截规则。建议首先验证流量接入防火墙后业务是否正常，逐步增加规则，并及时验证功能，一旦发现有问题，需及时关闭防护，避免现网业务受损。
- 对于SNAT EIP，外到内无法主动访问，内到外的访问控制规则使用的是互联网边界防护的能力，建议不在“弹性公网IP管理”页面中对SNAT所绑定的EIP开启防护，避免规则和日志混乱。

## 配置流程

1. **将VPC1和VPC-NAT接入企业路由器中**
2. **配置NAT网关**
3. **配置VPC1路由表**
4. （可选）使用业务VPC下的测试机访问外网测试网络连通性，正常访问则证明NAT配置成功。
5. 开启VPC间防火墙防护，请参见**开启VPC间防火墙**。
6. （可选）再次使用业务VPC下测试机进行网络连通性测试，查看防火墙流量日志中有响应记录，则证明防火墙引流成功。查询流量日志请参见**流量日志**。
7. 在防火墙上**配置NAT防护规则**。
8. （可选）使用测试机，访问IP或域名，查看访问控制日志是否有命中该条规则的日志，有则证明防护规则生效，查询访问控制日志请参见**访问控制日志**。
9. 在验证通过后，逐步切换类生产/现网业务到云防火墙。

**图 4-1** SNAT 防护配置流程




# 4.2 将 VPC1 和 VPC-NAT 接入企业路由器中

本节指导您如何将VPC1和VPC-NAT接入企业路由器。

## 步骤一：添加 VPC 连接

操作步骤请参见**企业路由器中添加VPC连接**。

**说明**

连接需要添加两条，“连接资源”分别选择VPC1和VPC-NAT。

## 步骤二：创建两个路由表

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航栏中，选择“网络 > 企业路由器”，单击“管理路由表”，进入“路由表”页面。

**步骤4** 创建两个路由表，作为**关联路由表**和**传播路由表**分别用于连接需防护的VPC和连接防火墙。

单击“路由表”页签，进入路由表设置页面，单击“创建路由表”，参数详情见**表 创建路由表参数说明**。

**表 4-1** 创建路由表参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 名称 | 输入路由表的名称。<br>命名规则如下：<br>● 长度范围为1~64位。<br>● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。 |
| 描述 | 您可以根据需要在文本框中输入对该路由表的描述信息。 |
| 标签 | 您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。<br>关于标签更详细的说明，请参见标签概述。 |

**----结束**

## 步骤三：设置关联路由表

**步骤1** 在左侧导航栏中，选择“网络 > 企业路由器”，单击“管理路由表”，进入“路由表”页面。

**步骤2** 设置关联功能，添加VPC1和VPC-NAT的连接：在路由表设置页面，选择关联路由表，单击“关联”页签，单击“创建关联”，参数详情见**表 创建关联参数说明**。

**图 4-2** 创建关联


**表 4-2** 创建关联参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 |
| 连接 | 在连接下拉列表中，选择VPC连接。 |

**说明**

关联需要增加两条，“连接”分别选择VPC1和VPC-NAT的连接。

**步骤3** 添加静态路由，指向防火墙：单击“路由”页签，单击“创建路由”，参数详情见**表创建路由参数说明**。

**图 4-3** 创建路由

**表 4-3** 创建路由参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 目的地址 | 设置目的地址，设置为：0.0.0.0/0。 |
| 黑洞路由 | 建议您保持关闭状态；开启后如果路由匹配上黑洞路由的目的地址，则该路由的报文会被丢弃。 |
| 连接类型 | 选择连接类型“云防火墙（CFW）”。 |
| 下一跳 | 在下拉列表中，选择自动生成的防火墙连接（cfw-er-auto-attach）。 |

**----结束**

## 步骤四：设置传播路由表

**步骤1** 在左侧导航栏中，选择“网络 > 企业路由器”，单击“管理路由表”，进入“路由表”页面。

**步骤2** 设置关联功能：在路由表设置页面，选择传播路由表，单击“关联”页签，单击“创建关联”，参数详情见**表 创建关联参数说明** 。

**图 4-4** 创建关联


**表 4-4** 创建关联参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 连接类型 | 选择连接类型“云防火墙（CFW）”。 |
| 连接 | 在下拉列表中，选择自动生成的防火墙连接（cfw-er-auto-attach）。 |

**步骤3** 设置传播功能，添加VPC1的传播：在路由表设置页面，选择传播路由表，单击“传播”页签，单击“创建传播”，参数详情见**表 创建传播参数说明**。

**图 4-5** 创建传播


**表 4-5** 创建传播参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 |
| 连接 | 在传播下拉列表中，选择VPC1的连接。 |

**步骤4** 添加静态路由，指向VPC-NAT：单击“路由”页签，单击“创建路由”，参数详情见**表 创建路由参数说明**。

**表 4-6** 创建路由参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 目的地址 | 设置目的地址，设置为：0.0.0.0/0。 |
| 黑洞路由 | 建议保持关闭状态；开启后如果路由匹配上黑洞路由的目的地址，则该路由的报文会被丢弃。 |
| 连接类型 | 选择连接类型“虚拟私有云（VPC）”。 |
| 下一跳 | 在下拉列表中，选择VPC-NAT的连接。 |

**----结束**

# 4.3 配置 NAT 网关

## 前提条件

- 已购买NAT网关：如果该网关对应的VPC未关联云资源（如云服务器），则可用于后续配置。
- 未购买NAT网关：需购买NAT网关，请参见**购买公网NAT网关**。关于NAT网关的收费，请参见**计费说明（公网NAT网关）**。

**⚠ 注意**

VPC-NAT关联NAT网关后，在默认路由表中默认添加一条路由（目的地址：0.0.0.0/0，“下一跳类型”为NAT网关），这个路由会将到达VPC-NAT的流量转向NAT网关，这条路由需注意不能删除。

## 步骤一：配置 SNAT 规则

**步骤1** 在左侧导航栏中，选择“网络 > NAT网关”，进入“公网NAT网关”页面。

**步骤2** 单击公网NAT网关的名称，进入“基本信息”页面，切换至“SNAT规则”页签。

**步骤3** 单击“添加SNAT规则”，参数详情如**表 添加SNAT规则**所示。

**表 4-7** 添加 SNAT 规则

| 参数名称 | 参数说明 |
| --- | --- |
| 使用场景 | SNAT规则使用的场景，选择“虚拟私有云”。 |
| 网段 | 选择“自定义”子网，使云服务器通过SNAT方式访问公网<br>• 自定义：自定义一个网段或者填写某个VPC的地址。<br>**说明**<br>支持配置0.0.0.0/0的地址段，在多段地址配置时更方便。<br>可以配置32位主机地址，NAT网关只针对此地址起作用。 |
| 弹性公网IP | 用来提供互联网访问的公网IP。<br>这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前公网NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性公网IP。<br>可选择多条EIP添加在SNAT规则中。一条SNAT规则最多添加20个EIP。SNAT规则使用多个EIP时，业务运行时会随机选取其中的一个。 |
| 监控 | 为SNAT连接数设置告警。<br>可通过设置告警及时了解SNAT连接数运行状况，从而起到预警作用。 |
| 描述 | SNAT规则信息描述。最大支持255个字符。 |

**----结束**

## 步骤二：配置 VPC-NAT 的路由表

**步骤1** 在左侧导航栏中，选择“网络 > 虚拟私有云 > 路由表”，进入“路由表”页面。

**步骤2** 在“名称”列，单击NAT网关对应VPC的路由表名称，进入路由表“基本信息”页面。

**步骤3** 单击“添加路由”，参数详情见**表 添加路由参数说明**。

**表 4-8** 添加路由参数说明

| 参数 | 说明 |
| --- | --- |
| 目的地址类型 | 选择“IP地址”。 |
| 目的地址 | 目的地址网段，填写VPC1的IP地址。<br>**说明**<br>不能与已有路由和VPC下子网网段冲突。 |
| 下一跳类型 | 在下拉列表中，选择类型“企业路由器”。 |
| 下一跳 | 选择下一跳资源。<br>下拉列表中将展示您创建的企业路由器名称。 |
| 描述 | 路由的描述信息，非必填项。<br>**说明**<br>描述信息内容不能超过255个字符，且不能包含“<”和“>”。 |

**----结束**

# 4.4 配置 VPC1 路由表

## 操作步骤

**步骤1** 在左侧导航栏中，选择“网络 > 虚拟私有云 > 路由表”，进入“路由表”页面。

**步骤2** 在“名称”列，单击VPC1的路由表名称，进入路由表“基本信息”页面。

**步骤3** 单击“添加路由”，参数详情见**表 添加路由参数说明**。

**表 4-9** 添加路由参数说明

| 参数 | 说明 |
| --- | --- |
| 目的地址类型 | 选择“IP地址”。 |
| 目的地址 | 目的地址网段，设置为：0.0.0.0/0。 |
| 下一跳类型 | 在下拉列表中，选择类型“企业路由器”。 |
| 下一跳 | 选择下一跳资源。<br>下拉列表中将展示您创建的企业路由器名称。 |
| 描述 | 路由的描述信息，非必填项。<br>**说明**<br>描述信息内容不能超过255个字符，且不能包含“<”和“>”。 |

**----结束**

# 4.5 配置 NAT 防护规则

验证流量流通后，需配置防护规则，云防火墙才会实施放行/拦截操作。

## 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

**步骤4** （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

**步骤5** 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

**步骤6** 在“互联网边界”页签中，单击“添加”按钮，在弹出的“添加防护规则”中，填写防护信息：

- 防护规则：NAT规则
- 源：选择“IP地址”，配置私网IP。
- 目的：选择“IP地址”（配置公网IP）或“域名/域名组”。

**图 4-6** 添加 NAT 防护规则


**步骤7** 单击“确认”，完成防护规则配置。

**----结束**

# 5 CFW 与 WAF、DDoS 高防、CDN 同时使用时的注意事项

本文介绍云防火墙在网络架构中的位置，以及与其他华为云服务一起使用时，云防火墙上的策略配置和注意事项。

## 应用场景

当购买了华为云的其他产品后，业务流量会经过多道防护，可能会存在开启反向代理导致IP地址发生转换的场景。

在对入云流量进行防护时，如果CFW前存在反向代理服务（即购买了CDN、DDoS高防或云模式WAF），需配置放行回源IP策略，请参见**配置策略**，购买独享模式WAF或ELB模式WAF时，按业务需要配置即可。

**说明**

购买独享模式WAF时，有以下两种防护场景：

- 在CFW上对公网ELB绑定的EIP开启防护：
  此时受到来自客户端的攻击，CFW会将攻击事件打印在“攻击事件日志”的“互联网边界防火墙”页签中。
  事件的“目的IP”为公网ELB绑定的EIP地址，“源IP”为客户端的IP地址。
- 开启VPC边界防火墙，并关联了源站所在VPC，未对ELB的EIP开启防护：
  此时受到来自客户端的攻击，CFW会将攻击事件打印在“攻击事件日志”的“VPC边界防火墙”页签中。
  事件的“目的IP”为源站服务器的私网IP，“源IP”为流量入口（如Nginx服务器）的私网IP。

流量经过反向代理后，源IP被转换为回源IP，此时如果受到外部攻击，CFW无法获取到攻击者的真实IP地址，您可通过X-Forwarded-For字段获取真实IP地址，请参见**查看X-Forwarded-For**。

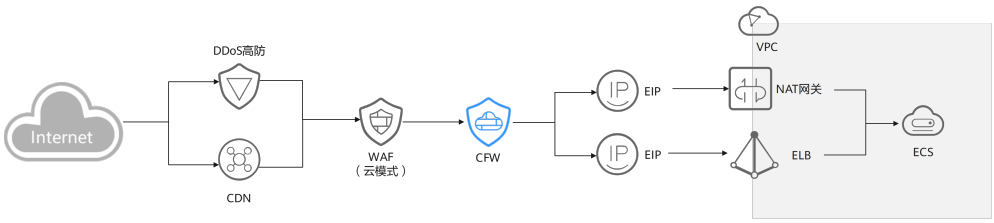
## 流量走势

Web应用防火墙（WAF）、DDoS高防（Advanced Anti-DDoS）、内容分发网络（CDN）会对用户的流量进行反向代理，部署后，CFW接收到的源IP为上述服务的回源IP。

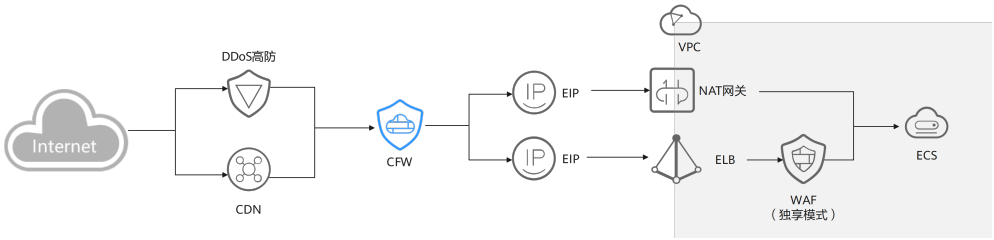
WAF分为三种模式：云模式、独享模式和ELB模式，不同的模式，架构位置不同；DDoS高防和CDN部署位置固定。

流量走势图如下：

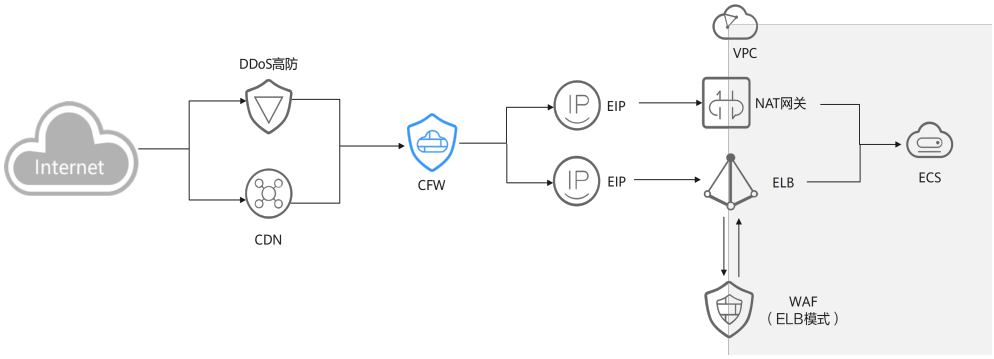
- 云模式WAF




- 独享模式WAF




- ELB模式WAF




## 配置策略

- 建议您创建一条“优先级”“置顶”的“放行”策略，放行所有回源IP；配置后CFW仍会对流量进行检测，进一步保证您的流量安全。
- 如果将回源IP加入“白名单”；配置后，这些流量将被直接放通，CFW不再进行任何防护。

**⚠ 注意**

请避免将回源IP加入黑名单或阻断的防护策略中，否则将会阻断来自这个IP的所有流量，影响您的业务。

- 添加防护规则请参见**添加防护规则**。
- 设置白名单请参见**管理黑/白名单**。
- CFW的防护顺序请参见**云防火墙的防护顺序是什么？**
- 获取Web应用防火墙的回源IP，请参见**步骤二：放行WAF回源IP**
- 获取DDoS高防的回源IP，请参见**如何查看高防回源IP段？**

## 查看 X-Forwarded-For

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的，选择区域。

**步骤3** 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

**步骤4** （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

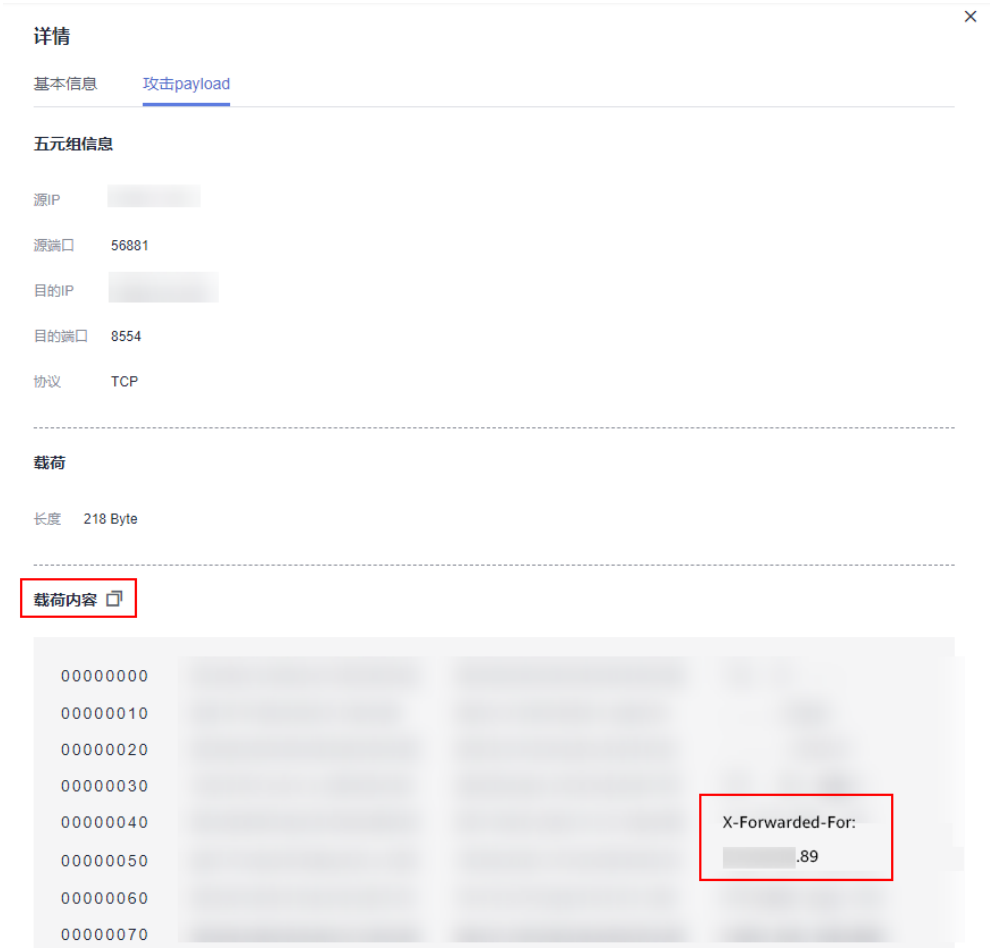
**步骤5** 在左侧导航树中，选择“日志审计 > 日志查询”。进入“攻击事件日志”页面，在对应事件的“操作”列，单击“查看”。

**图 5-1** 查看攻击事件日志详情

**步骤6** 在“详情”中，切换至“攻击payload”页签，获取X-Forwarded-For字段。

- 方法一：在“载荷内容”中查看X-Forwarded-For（从客户端到最后一个代理服务器的所有地址IP）。

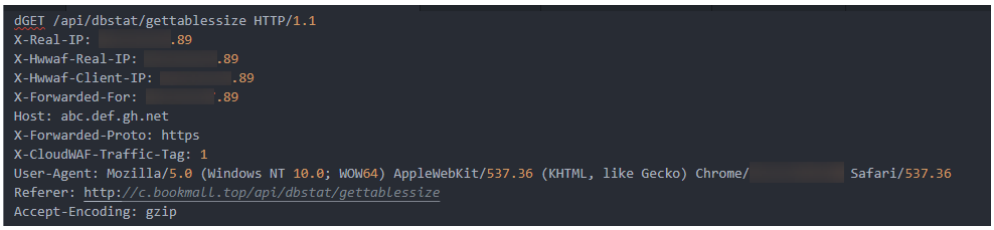
**图 5-2** 载荷内容中 X-Forwarded-For



- 方法二：复制“载荷内容”，通过Base64工具，获得解码结果：
  - X-Forwarded-For：从客户端到最后一个代理服务器的所有地址IP

  例如，通过**图 Base64解码结果**可得真实客户端的IP为xx.xx.xx.89，只经过云模式WAF的一层代理。

  **图 5-3** Base64 解码结果示例

**----结束**

# 6 迁移安全策略

云防火墙支持批量导入防护策略，帮助您更快速的迁移安全策略。

## 应用场景

当您需要从其他云迁移到华为云或者从其他防火墙更换安全策略到云防火墙时，支持通过批量导入功能，快速添加安全策略。

## 操作步骤

**步骤1** 通过API/策略备份功能从其他防火墙上导出策略配置文件。

**步骤2** **登录管理控制台**。

**步骤3** 单击管理控制台左上角的  ，选择区域。

**步骤4** 在左侧导航树中，单击左上方的  ，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

**步骤5** （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

**步骤6** 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

**步骤7** 单击页面右上方“下载中心”，右侧弹出“下载中心”页面。

**步骤8** 单击“下载模板”，下载导入规则模板到本地。

**步骤9** 填写参数，参数说明请参见**导入规则模板参数**。

- 内到外的阻断示例请参见**导入参数示例——内到外的阻断规则**。
- 地址组和域名组的防护示例请参见**导入参数示例——地址组成员对域名组成员的访问**。

**说明**

- 如果业务迁移时组网发生改变，则需要重新改写原有策略中的网络信息（如IP地址）。
- 为减小迁移对业务的影响，建议将所有规则的“启用状态”先设置为“禁用”（尤其是阻断类策略），待导入表格并检查策略配置正确后，再启用策略。
- 导入后的策略优先级低于已创建的策略。
- 云防火墙与网络ACL、安全组等防护检测服务的策略都设置为放行时，才能正常放行指定流量。
- 导入并引用对象组（如IP地址组）时，需要在对应的信息表（如地址信息表）中填写组的信息，再在防护策略表中引用。

**步骤10** 表格填写完成后，单击“导入规则”，导入防护规则表。

**步骤11** 开启策略的“启用状态”，建议优先开启不影响主要业务的策略。

**步骤12** 查看访问控制日志中是否有该策略的命中记录，查看访问控制日志请参见**访问控制日志**。

- 如果有命中记录，则表明策略已经生效。
- 如果没有命中记录，可按以下步骤排查：
  a. 策略对应的资源需在防火墙中开启防护，EIP资源请参见**查看弹性公网IP信息**，VPC资源请参见**添加防护VPC**。
  b. 查看策略优先级，是否有更高优先级的策略被命中，设置优先级请参见**设置优先级**。
  c. 在“访问策略管理”页面查看是否有下发失败的报错。

**步骤13** （可选）通过查看策略助手或定制安全报告定期查看策略的命中情况。

策略助手和安全报告中会展示策略被命中的趋势以及各类TOP N统计，便于您及时排查异常策略，助力您做好策略运营。

- 策略助手请参见：**策略助手**。
- 安全报告请参见：**安全报告**。

**----结束**

## 导入参数示例——内到外的阻断规则

**原规则**

- rule id：123
- src-zone：trust
- dst-zone：untrust
- src-addr：0.0.0.0/0
- dst-addr：xx.xx.xx.9
- service ： SSH
- action：deny
- name：example123

**转换后填写规则**

- 顺序：1

- 规则名称：example123
- 防护规则：EIP防护
- 方向：内到外
- 动作：阻断
- 规则地址类型：IPv4
- 启用状态：禁用
- 描述：一个样例
- 源地址类型：IP地址
- 源IP地址：0.0.0.0/0
- 目的地址类型：IP地址
- 目的IP地址：xx.xx.xx.9
- 服务类型：服务
- 协议/源端口/目的端口：TCP/1-65535/22

## 导入参数示例——地址组成员对域名组成员的访问

地址信息表：

- 地址组名称：地址组1
- 地址组描述：业务A
- 地址组地址类型：IPv4
- 地址组成员
  - IP地址：10.1.1.2；描述：ECS1
  - IP地址：10.1.1.3；描述：ECS2
  - IP地址：10.1.1.4；描述：ECS3

域名组信息表：

- 域名组名称：域名组1
- 域名组类型：URL过滤
- 域名组描述：业务A对外访问域名
- 域名组成员
  - 域名成员：www.example.test.api；域名描述：api
  - 域名成员：www.test.example.com；域名描述：一个域名
  - 域名成员：www.example.example.test；域名描述：XX系统

防护规则表

- 顺序：1
- 规则名称：业务A外联
- 防护规则：NAT规则
- 方向：内到外
- 动作：放行
- 规则地址类型：IPv4

- 启用状态：禁用
- 源地址类型：IP地址组
- 源地址组名称：地址组1
- 目的地址类型：域名组
- 目的域名组名称：域名组1
- 服务类型：服务
- 协议/源端口/目的端口：TCP/0-65535/8080

# A 修订记录

| 发布日期 | 修改说明 |
| --- | --- |
| 2024-03-29 | 第七次正式发布。<br>新增**迁移安全策略**章节。 |
| 2023-12-22 | 第六次正式发布。<br>新增**CFW与WAF、DDoS高防、CDN同时使用时的注意事项**章节。 |
| 2023-11-08 | 第五次正式发布。<br>优化：<br>**配置IP地址组和服务组访问策略**，查看防护详情内容。<br>**配置VPC边界防火墙**，版本约束。 |
| 2023-08-22 | 第四次正式发布。<br>新增**如何使用CFW防护SNAT场景**章节。 |
| 2022-07-28 | 第三次正式发布。<br>新增**配置VPC边界防火墙**章节。 |
| 2022-01-05 | 第二次正式发布。<br>新增**配置入方向和出方向的访问策略**章节。<br>新增**配置IP地址组和服务组访问策略**章节。 |
| 2021-12-10 | 第一次正式发布。 |