

云防火墙

# 最佳实践

文档版本 08  
发布日期 2025-01-23



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI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。

# 目录

<b>1 CFW 最佳实践汇总</b> .....	<b>1</b>
<b>2 使用 API 购买并查询 CFW</b> .....	<b>2</b>
<b>3 批量迁移安全策略到 CFW</b> .....	<b>5</b>
<b>4 CFW 与 WAF、DDoS 高防、CDN 同时使用的配置建议</b> .....	<b>9</b>
<b>5 仅放行互联网对指定端口的访问流量</b> .....	<b>12</b>
<b>6 仅放行云内资源对指定域名的访问流量</b> .....	<b>15</b>
<b>7 使用 CFW 防御网络攻击</b> .....	<b>18</b>
7.1 使用 CFW 防御访问控制攻击.....	18
7.2 使用 CFW 防御黑客工具.....	19
7.3 使用 CFW 防御可疑 DNS 活动.....	21
7.4 使用 CFW 防御特洛伊木马.....	22
7.5 使用 CFW 防御漏洞攻击.....	23
7.6 使用 CFW 防御蠕虫病毒.....	25
<b>8 通过配置 CFW 防护规则实现两个 VPC 间流量防护</b> .....	<b>27</b>
<b>9 通过配置 CFW 防护规则实现 SNAT 流量防护</b> .....	<b>37</b>
9.1 SNAT 防护概述.....	37
9.2 资源和成本规划.....	40
9.3 将 VPC1 和 VPC-NAT 接入企业路由器中.....	41
9.4 配置 NAT 网关.....	45
9.5 配置 VPC1 路由表.....	47
9.6 配置 NAT 防护规则.....	47
<b>10 使用 CFW 防护企业资源</b> .....	<b>49</b>
<b>11 使用 CFW 跨账号防护 EIP 资源</b> .....	<b>53</b>
<b>12 使用 CFW 跨账号防护 VPC 资源</b> .....	<b>58</b>

# 1 CFW 最佳实践汇总

本文汇总了云防火墙（CFW）服务的常见应用场景，并提供详细的方案描述和操作指导，帮助您轻松防护云上业务。

## CFW 最佳实践

表 1-1 CFW 最佳实践一览表

分类	相关文档
使用API购买CFW	<a href="#">使用API购买并查询CFW</a>
批量迁移策略	<a href="#">批量迁移安全策略到CFW</a>
与WAF等云服务同时使用	<a href="#">CFW与WAF、DDoS高防、CDN同时使用的配置建议</a>
配置访问控制策略	<a href="#">仅放行互联网对指定端口的访问流量</a>
	<a href="#">仅放行云内资源对指定域名的访问流量</a>
	<a href="#">通过配置CFW防护规则实现两个VPC间流量防护</a>
	<a href="#">通过配置CFW防护规则实现SNAT流量防护</a>
配置入侵防御	<a href="#">使用CFW防御访问控制攻击</a>
	<a href="#">使用CFW防御黑客工具</a>
	<a href="#">使用CFW防御可疑DNS活动</a>
	<a href="#">使用CFW防御特洛伊木马</a>
	<a href="#">使用CFW防御漏洞攻击</a>
	<a href="#">使用CFW防御蠕虫病毒</a>
企业项目管理	<a href="#">使用CFW防护企业资源</a>
多账号管理	<a href="#">使用CFW跨账号防护EIP资源</a>
	<a href="#">使用CFW跨账号防护VPC资源</a>

# 2 使用 API 购买并查询 CFW

## 应用场景

对于专业人士而言，使用API的效率高于控制台操作，CFW提供多个功能的API接口，请参见[API接口](#)。

本文介绍如何通过API的方式快速购买和查询标准版防火墙实例。

## 前提条件

当前账号拥有BSS Administrator和CFW FullAccess权限。

## 购买并查询标准版防火墙

**步骤1** [登录管理控制台](#)。

**步骤2** 在右上角选择“工具 > API Explorer”。

**步骤3** 在左侧导航栏中，单击“所有产品”，选择“安全与合规 > 云防火墙”。

**步骤4** 购买标准版防火墙：选择“创建防火墙”接口，填写关键参数如下，其余参数按需填写：

- Region：选择云资产所在的区域。
- project\_id：项目ID，自动获取。
- flavor：填写规格信息。
  - version：防火墙版本，本文购买标准版，选择“Standard”，各版本之间的差异请参见[服务版本差异](#)。
- charge\_info：填写计费类型信息。
  - charge\_mode：计费模式，本文购买包年/包月，填写“prePaid”。
  - is\_auto\_renew：是否自动续订，本文以购买一个月为例，选择“false”。
  - is\_auto\_pay：支付方式是否选择自动支付，本文选择自动支付，选择“true”。

**步骤5** 查询购买的防火墙：选择“查询防火墙列表”接口，填写关键参数如下，其余参数按需填写：

- Region：选择防火墙所在的区域。

- project\_id: 项目ID, 自动获取。
- key\_word: 填写关键字, 例如防火墙的名称。
- limit: 每页显示的结果数量, 本文查询一个防火墙, 此处填“1”。
- offset: 偏移量, 指定返回记录的开始位置, 此处填0。

----结束

## 代码示例

请准备基础认证信息:

- ak: 华为账号Access Key, 获取方式请参见[获取AK/SK](#)。
- sk: 华为账号Secret Access Key, 获取方式请参见[获取AK/SK](#)。
- Region: 区域ID, 例如cn-east-3, 获取方式请参见[地区和终端节点](#)。

```
import com.huaweicloud.sdk.cfw.v1.CfwClient;
import com.huaweicloud.sdk.cfw.v1.model.*;
import com.huaweicloud.sdk.cfw.v1.region.CfwRegion;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;

import java.util.ArrayList;
import java.util.List;

public class CreateFirewallSolution {

    public static void main(String[] args) {
        String ak = "xxxx";
        String sk = "xxxx";

        BasicCredentials auth = new BasicCredentials().withAk(ak).withSk(sk);

        CfwClient client = CfwClient.newBuilder()
            .withCredential(auth)
            .withRegion(CfwRegion.valueOf("xxxx"))
            .build();

        //创建创建防火墙请求体
        CreateFirewallRequest request = new CreateFirewallRequest();
        CreateFirewallReq body = new CreateFirewallReq();
        body.setName("cfwtest");
        body.setEnterpriseProjectId("0");
        CreateFirewallReqTags createFirewallReqTags = new CreateFirewallReqTags();
        createFirewallReqTags.setKey("TagKey");
        createFirewallReqTags.setValue("TagValue");
        List<CreateFirewallReqTags> createFirewallReqTagsList = new ArrayList<>();
        createFirewallReqTagsList.add(createFirewallReqTags);
        body.setTags(createFirewallReqTagsList);
        CreateFirewallReqFlavor flavor = new CreateFirewallReqFlavor();
        flavor.setVersion(CreateFirewallReqFlavor.VersionEnum.STANDARD);
        body.setFlavor(flavor);
        CreateFirewallReqChargeInfo createFirewallReqChargeInfo = new CreateFirewallReqChargeInfo();
        createFirewallReqChargeInfo.setChargeMode("prePaid");
        createFirewallReqChargeInfo.setPeriodType("month");
        createFirewallReqChargeInfo.setPeriodNum(1);
        createFirewallReqChargeInfo.setIsAutoPay(true);
        createFirewallReqChargeInfo.setIsAutoRenew(true);
        body.setChargeInfo(createFirewallReqChargeInfo);
        request.setBody(body);

        //创建查询防火墙请求体
        ListFirewallListRequest listFirewallListRequest = new ListFirewallListRequest();
```

```
QueryFireWallInstanceDto queryFireWallInstanceDto = new QueryFireWallInstanceDto();
queryFireWallInstanceDto.setOffset(0);
queryFireWallInstanceDto.setLimit(1);
queryFireWallInstanceDto.setKeyWord("cfwtest");
listFirewallListRequest.setBody(queryFireWallInstanceDto);
try {
    //创建防火墙
    CreateFirewallResponse createFirewallResponse = client.createFirewall(request);
    System.out.println(createFirewallResponse.toString());

    //查询防火墙列表
    ListFirewallListResponse listFirewallListResponse = client.listFirewallList(listFirewallListRequest);
    System.out.println(listFirewallListResponse.toString());
} catch (ConnectionException e) {
    System.out.println(e.getMessage());
} catch (RequestTimeoutException e) {
    System.out.println(e.getMessage());
} catch (ServiceResponseException e) {
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

# 3 批量迁移安全策略到 CFW

## 应用场景

当业务需要从其他云迁移到华为云，或者安全策略需要从其他防火墙更换到云防火墙时，支持通过批量导入功能，快速添加安全策略。

## 注意事项

- 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。

## 批量迁移内到外的阻断规则



**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。

例如导出如下规则：

- 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

**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** 在左侧导航栏中, 单击左上方的, 选择“安全与合规 > 云防火墙”, 进入云防火墙的总览页面。
- 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** 在模板中填写参数,
- 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
- 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[开启EIP防护](#), 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。


----结束

## 批量迁移地址组成员和域名组成员

**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** 在左侧导航栏中, 单击左上方的, 选择“安全与合规 > 云防火墙”, 进入云防火墙的总览页面。

**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** 在模板中填写参数,

- 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防护
  - 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

**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[开启EIP防护](#)，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。

----结束

## 相关文档

- 导入安全策略参数说明请参见[导入规则模板参数](#)。
- 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](#)。

# 4 CFW 与 WAF、DDoS 高防、CDN 同时使用的配置建议

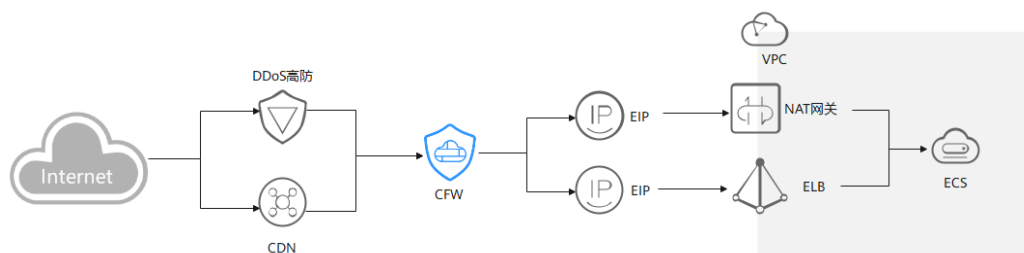
本文介绍入云流量防护时云防火墙在网络架构中的位置，以及与其他华为云服务一起使用时，云防火墙上的策略配置和注意事项。

## 概述

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。

当配置了华为云的其他产品后，业务流量会经过多道防护，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，避免误拦截，购买独享模式WAF或ELB模式WAF时，按业务需要配置即可。

## DDoS 高防/CDN



建议您创建放行的防护规则或者添加回源IP至白名单。

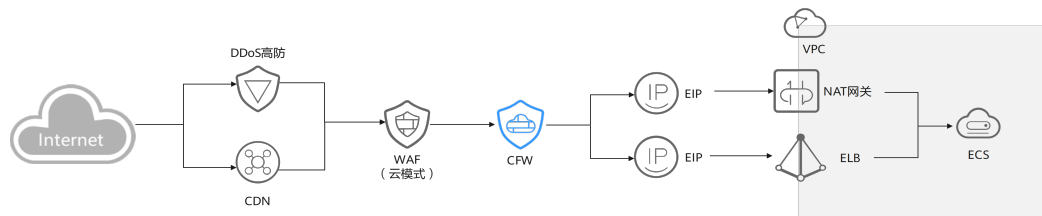
- 创建放行的防护规则：添加一条“优先级”“置顶”的“放行”策略，放行所有回源IP；配置后CFW仍会对流量进行检测，进一步保证您的流量安全。
- 添加回源IP至白名单：回源IP加入“白名单”后，这些流量将被直接放通，CFW不再进行任何防护。

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[如何获取攻击者的真实IP地址？](#)。

**⚠ 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。

## 云模式 WAF



建议您创建放行的防护规则或者添加回源IP至白名单。

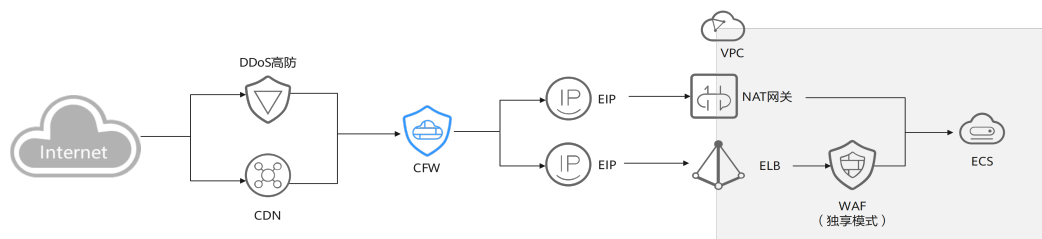
- 创建放行的防护规则：添加一条“优先级”“置顶”的“放行”策略，放行所有回源IP；配置后CFW仍会对流量进行检测，进一步保证您的流量安全。
- 添加回源IP至白名单：回源IP加入“白名单”后，这些流量将被直接放通，CFW不再进行任何防护。

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[如何获取攻击者的真实IP地址？](#)。

**⚠ 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。

## 独享模式 WAF

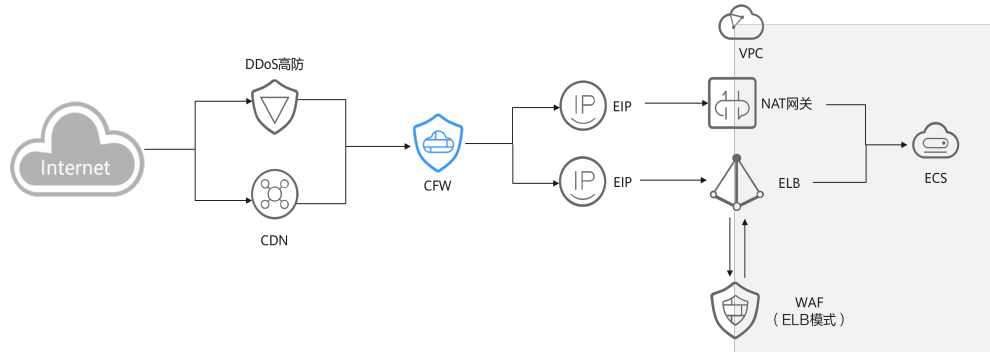


流量先经过CFW再经过WAF，正常配置即可，不同的防护场景，查看日志方式不同：

- 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。

## ELB 模式 WAF



流量先经过CFW再经过WAF，正常配置即可。

## 相关文档

- 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？](#)

# 5 仅放行互联网对指定端口的访问流量


## 应用场景

为了提升安全性，需要仅放行部分端口（例如80端口、443端口）的流量访问云内资源。

本文介绍如何通过CFW对云资源进行精细化管控，允许所有公网地址访问EIP（xx.xx.xx.1）的80端口。

## 通过 CFW 放行互联网对指定端口的访问流量

**步骤1** 购买云防火墙标准版或专业版，请参见[购买云防火墙](#)。

**步骤2** 在左侧导航栏中，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

**步骤3** （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4** 对需要防护的EIP（xx.xx.xx.1）开启防护。

1. 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，弹性公网IP信息将自动更新至列表中。
2. 在EIP（xx.xx.xx.1）所在行的“操作”列中，单击“开启防护”。

**步骤5** 配置防护规则。

1. 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。
2. 单击“添加”，在弹出的“添加防护规则”中，填写防护信息，其余参数可根据业务部署填写。

共配置两条防护规则：

- 一条拦截所有流量，如[图 拦截所有流量](#)所示，优先级置于最低。
  - 方向：外-内
  - 源：Any
  - 目的：Any

- 服务: Any
- 应用: Any
- 动作: 阻断

图 5-1 拦截所有流量

**匹配条件** [查看配置指导](#)

方向

外-内  内-外

源 [?](#)

IP地址  IP地址组  地域  Any [?](#)

目的 [?](#)

IP地址  IP地址组  Any [?](#)

服务 [?](#)

服务  服务组  Any [?](#)

应用 [?](#)

应用  Any

**防护配置**

防护动作

放行  阻断

- 一条放行EIP (xx.xx.xx.1) 80端口的流量, 如图 [放行域名的访问流量](#)所示, 优先级设置最高。
  - 方向: 外-内
  - 源: Any
  - 目的: 选择“IP地址”, 填写xx.xx.xx.1。
  - 服务: TCP/1-65535/80
  - 应用: Any



- 动作：放行

图 5-2 放行 xx.xx.xx.1 80 端口的访问流量

匹配条件 [查看配置指导](#)

方向

外-内  内-外

源

IP地址  IP地址组  地域  Any

目的

IP地址  IP地址组  Any

1

服务

服务  服务组  Any

协议	源端口	目的端口	操作
TCP	1-65535	80	删除

+ 添加 最少添加1个, 最多添加5个

应用

应用  Any

防护配置

防护动作

放行  阻断

**步骤6** 通过访问控制日志查看命中详情。

在左侧导航栏中，选择“日志审计 > 日志查询”。默认进入“攻击事件日志”页面，选择“访问控制日志”页签。

#### 说明

日志中“目的IP”列是xx.xx.xx.1时对应的“响应动作”是“阻断”。

----结束

## 相关文档

需要增加其他防护规则时，请参见防护规则的详细参数说明[添加防护规则](#)。

# 6 仅放行云内资源对指定域名的访问流量


## 应用场景

为了防止敏感数据泄露或受到外部恶意攻击，需要限制云内资源仅能访问特定公网域名。

本文介绍如何通过CFW对云资源进行精细化管控，实现放行所有EIP对指定域名（本文以泛域名\*.example.com为例）的访问流量。

## 通过 CFW 放行云内资源对指定域名的访问流量

**步骤1** 购买云防火墙标准版或专业版，请参见[购买云防火墙](#)。

**步骤2** 在左侧导航栏中，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

**步骤3** （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4** 对需要防护的EIP开启防护。

1. 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，弹性公网IP信息将自动更新至列表中。
2. 在EIP所在行的“操作”列中，单击“开启防护”。

**步骤5** 配置防护规则。

1. 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。
2. 单击“添加”，在弹出的“添加防护规则”中，填写防护信息，其余参数可根据业务部署填写。

共配置两条防护规则：

- 一条拦截所有流量，如[图 拦截所有流量](#)所示，优先级置于最低。
  - 方向：内-外
  - 源：Any
  - 目的：Any

- 服务：Any
- 应用：Any
- 动作：阻断

图 6-1 拦截所有流量

匹配条件 [查看配置指导](#)

方向

外-内  内-外

源 [?](#)

IP地址  IP地址组  Any [?](#)

目的 [?](#)

IP地址  IP地址组  地域  域名/域名组  Any [?](#)

服务 [?](#)

服务  服务组  Any [?](#)

应用 [?](#)

应用  Any

防护配置

防护动作

放行  阻断

- 一条放行EIP对\*.example.com的访问流量，如[图 放行域名的访问流量](#)所示，优先级设置最高。
  - 方向：内-外
  - 源：Any
  - 目的：选择“域名/域名组”、“应用型”、“域名”，填写\*.example.com。
  - 服务：TCP/1-65535/1-65535
  - 应用：HTTP、HTTPS
  - 动作：放行

图 6-2 放行域名的访问流量

匹配条件 [查看配置指导](#)

方向  
 外-内  内-外

源 <sup>①</sup>  
 IP地址  IP地址组  Any <sup>②</sup>

目的 <sup>①</sup>  
 IP地址  IP地址组  地域  域名/域名组  Any <sup>②</sup>

应用型  网络型  
通过HOST或SNI字段实现域名的访问控制，仅支持HTTP、HTTPS、TLS1、SMTPS、POP3S应用。  
域名

服务 <sup>①</sup>  
 服务  服务器组 <sup>②</sup>

协议	源端口 <sup>②</sup>	目的端口 <sup>②</sup>	操作
TCP	1-65535	1-65535	删除

+ 添加 最少添加1个，最多添加5个

应用 <sup>①</sup>  
 应用  
HTTP × HTTPS ×

防护配置  
防护动作

#### 步骤6 通过访问控制日志查看命中详情。

在左侧导航栏中，选择“日志审计 > 日志查询”。默认进入“攻击事件日志”页面，选择“访问控制日志”页签。

#### 说明

日志中“目的IP”列是任意example.com的域名时，对应的“响应动作”是“放行”，其他流量对应的“响应动作”是“阻断”。

----结束

#### 相关文档

- 域名组的配置示例请参见[放行业务访问某平台的流量](#)。
- 需要增加其他防护规则时，请参见防护规则的详细参数说明[添加防护规则](#)。
- 放行云内资源通过NAT网关对指定域名的访问流量请参见[通过配置CFW防护规则实现SNAT流量防护](#)。

# 7 使用 CFW 防御网络攻击

## 7.1 使用 CFW 防御访问控制攻击

本文介绍如何通过CFW防御访问控制攻击。

### 应用场景

访问控制是保护系统资源免受非法访问的关键手段，通过限制用户或进程对系统资源的访问权限来维护系统的安全性。攻击者可能利用各种手段来绕过或破坏这些控制，从而实现非法访问。

CFW的IPS规则库配置了针对访问控制攻击的防御规则，可有效识别和拦截该类绕过或破坏系统访问控制机制的行为，降低此类攻击的风险。

### 什么是访问控制攻击

访问控制攻击是指攻击者通过利用系统或应用中的访问控制漏洞，以非法方式获取或提升其在系统或应用中的访问权限，执行未授权的操作或访问敏感资源。

常见的访问控制攻击包括：

- **越权访问攻击**
  - 垂直越权：普通用户能够访问或执行只有管理员才具有权限的资源或功能。
  - 水平越权：某一用户可以访问或执行另一个用户才有权限访问或执行的资源或功能。
  - 多阶段越权：在需要多个步骤的操作中（如银行转账），攻击者可能跳过前面的步骤直接执行最后的步骤。
- **密码攻击**
  - 暴力破解：攻击者通过尝试所有可能的组合来破解用户的账户名和密码，包括纯粹式暴力破解（地毯式搜索）和字典式暴力破解（使用预设的单词字典）。
  - 彩虹表攻击：一种批处理字典攻击的实现方式，通过查找预生成的密码与哈希串对照表来破解密码。
- **会话劫持攻击**

攻击者通过获取用户的会话ID，使用该ID登录目标账号并执行未授权操作。这通常发生在用户会话标识被泄露或预测的情况下。

- **访问聚合攻击**

在深度测试中经常应用的一种方式，通过收集多个非敏感信息，结合来获得敏感信息，通过这些信息的组合，进行对比完成攻击。

## 访问控制攻击的危害


访问控制攻击对系统安全造成严重威胁，其主要危害表现为：


- **数据泄露**：攻击者可以通过绕过访问控制机制，获取系统中未授权的敏感数据，如用户个人信息、财务数据等，导致数据泄露。
- **数据篡改**：攻击者可以通过绕过访问控制机制，篡改系统数据，导致数据不真实和不可靠。
- **系统瘫痪**：攻击者可以通过绕过访问控制机制，获取系统中的管理员权限，导致系统被破坏和瘫痪，无法正常运行。
- **信息安全风险**：访问控制攻击会导致系统中的安全机制被破坏，增加系统面临的信息安全风险，如恶意软件、病毒、木马等的入侵。

## 如何防御访问控制攻击

为了防御访问控制攻击，除了从访问控制策略设计、身份验证、安全审计和监控、安全配置和补丁管理、访问控制漏洞防御、安全培训和意识提升以及使用安全技术和工具等方面入手外，您可以使用CFW入侵防御功能，拦截访问控制攻击。

**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，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

**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** 单击“基础防御”中的“查看生效中的规则”，进入“基础防御规则”页面。

**步骤6** 筛选出防护访问控制攻击的规则：在上方筛选框中，选择“攻击类型”是“访问控制”。

**步骤7** 批量开启防护：勾选对应规则，单击上方“拦截”。

### 说明

拦截：防火墙对匹配当前防御规则的流量，记录至攻击事件日志中并进行拦截。

----结束

## 7.2 使用 CFW 防御黑客工具

本文介绍如何通过CFW防御黑客工具攻击。

## 应用场景

攻击者恶意利用黑客工具非法入侵计算机系统或网络，可能会导致计算机系统或网络的损坏、数据泄露、网络瘫痪等严重后果，甚至会导致严重的法律后果和安全风险。

CFW提供了针对黑客工具的入侵防御规则，可以有效地识别和拦截端口扫描、远程控制、木马程序、网络监听等各类型的黑客工具攻击。

## 什么是黑客工具

黑客工具（Hack Tools）是一种用于实施网络攻击的恶意软件程序，它通常由黑客或者恶意程序安装到您的计算机中，用于窃取敏感信息、破坏系统或网络、远程控制计算机或网络等非法活动。在合法的情况下，黑客工具也可以被安全研究人员用于测试系统或网络的安全性。

黑客工具包括如下显著特点：

- 隐蔽性：黑客工具通常被设计得十分隐蔽，它们可能伪装成合法的软件或服务，或者以其他不易被察觉的形式存在，以便在不被发现的情况下进行攻击。
- 繁杂性：黑客工具种类繁多，包括但不限于端口扫描器、漏洞扫描器、密码破解器、远程控制软件、木马程序、网络监听工具等，可以用于不同场景的攻击。
- 低门槛：黑客工具通常可以通过简单的操作实现复杂的攻击或渗透。随着互联网信息的高度共享，网络上流传的黑客工具繁多，并且大部分工具教程详细、操作简便，使得使用黑客工具的技术门槛不断降低，攻击者无需精通专业技术即可利用这些工具进行攻击。
- 破坏性：黑客工具有极强的破坏性，可以进行各种攻击、渗透、破解等操作，并且可以快速地发现和利用目标系统的漏洞，从而实现高效的攻击。

## 黑客工具的危害


滥用黑客工具会给个人和社会带来巨大的安全风险和经济损失，包括但不限于以下几个方面：

- 盗取信息：黑客工具可以窃取个人隐私信息，如账号密码、银行账户信息、社交媒体账号等，导致财产损失和个人隐私泄露。
- 破坏系统：黑客工具可以攻击计算机系统，破坏系统文件和数据，导致系统崩溃或数据丢失等问题。
- 恶意攻击：黑客工具可以用于进行恶意攻击，如DDoS攻击、病毒攻击等，使网站无法正常访问或瘫痪。
- 网络犯罪：黑客工具可以被用于进行犯罪活动，如网络诈骗、网络敲诈等，导致社会安全问题。

## 如何防御黑客工具

**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，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

**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** 单击“基础防御”中的“查看生效中的规则”，进入“基础防御规则”页面。

**步骤6** 筛选出防护黑客工具的规则：在上方筛选框中，选择“攻击类型”是“黑客工具”。

**步骤7** 批量开启防护：勾选对应规则，单击上方“拦截”。

#### 说明

拦截：防火墙对匹配当前防御规则的流量，记录至攻击事件日志中并进行拦截。

----结束

## 7.3 使用 CFW 防御可疑 DNS 活动

本文介绍如何通过CFW防御可疑DNS活动。

### 应用场景

DNS是绝大部分互联网请求的组成部分，是互联网应用中非常基础和重要的一环，一旦DNS系统受到攻击将会对网络服务带来严重影响，因此保障DNS安全显得尤为重要。CFW提供了检测可疑DNS活动的入侵防御规则，当检测到可疑DNS活动入侵时，可以实时拦截入侵活动和攻击性网络流量。

### 什么是可疑 DNS 活动

DNS（Domain Name System，域名系统），是用于将域名转换成用于计算机连接的IP地址的一套查询和转换系统。当用户在浏览器中输入网站的域名时，浏览器会向域名解析服务器（DNS服务器）发送域名解析请求，DNS服务器返回域名对应的IP地址，最终，用户通过IP地址获取到相应的网站资源。

可疑DNS活动是指在网络中出现的异常DNS请求或响应行为。攻击者利用DNS缺陷或通过发送超量请求等各种方式攻击DNS，致使DNS出现异常请求或响应的行为，最终导致DNS解析域名错误、解析超时或DNS系统瘫痪等，这不仅会影响用户的上网体验，还可能带来经济损失甚至法律责任等严重后果。

### 常见的可疑 DNS 活动及其危害

常见的可疑DNS活动及其危害，包括但不限于以下几种：


- DNS缓存中毒：攻击者利用DNS服务器的漏洞来接管DNS，通过篡改DNS服务器的缓存记录，将用户访问重定向到恶意网站，从而实施钓鱼、恶意软件下载等攻击行为。
- DNS缓冲区溢出攻击：攻击者利用DNS服务器的漏洞，通过向DNS服务器的缓存区发送大量恶意数据，导致DNS服务器缓存区溢出，最终使得恶意数据覆盖了原有的合法数据，从而实现篡改DNS响应、重定向流量、中间人攻击等攻击行为。

### 如何防御可疑 DNS 活动

**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，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。
- 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** 单击“基础防御”中的“查看生效中的规则”，进入“基础防御规则”页面。
- 步骤6** 筛选出防护可疑DNS活动的规则：在上方筛选框中，选择“攻击类型”是“可疑DNS活动”。
- 步骤7** 批量开启防护：勾选对应规则，单击上方“拦截”。

#### 说明

拦截：防火墙对匹配当前防御规则的流量，记录至攻击事件日志中并进行拦截。

---结束

## 7.4 使用 CFW 防御特洛伊木马

本文介绍如何通过CFW防御特洛伊木马攻击。

### 应用场景

特洛伊木马是攻击者常用的网络攻击方式之一，通过植入木马程序以控制用户计算机，实现窃取用户信息、破坏用户计算机系统等目的，其极强的伪装性和潜伏性使其在计算机中不易被发现和查杀。

CFW提供了针对特洛伊木马的入侵防御规则，可以有效地帮您识别和抵御木马入侵。

### 什么是特洛伊木马

特洛伊木马（Trojan Horse）简称木马，是指寄宿在计算机中为实现非法意图的一种恶意软件程序。特洛伊木马通常伪装成正常的软件，通过诱导用户下载到用户计算机中，攻击者通过木马控制用户的计算机系统并实现窃取用户的个人信息、密码或其他敏感数据，或者破坏用户的计算机系统为目的。

木马与计算机病毒的区别在于木马不会自我复制，不具有传染性，也不会主动发起攻击。木马的主要特点如下：

- 伪装性强：木马通常会伪装成一些看似正常的程序或文件，以此欺骗用户主动安装或打开它们。木马伪装方式很多，例如修改木马程序的图标为常用的文本、图片或HTML等文件图标，或将木马的名称修改为系统文件的名称等。
- 潜伏性强：木马一旦被植入到目标计算机以后，能够长时间潜伏在用户计算机中不易被发现和查杀，等待攻击者的指令。木马藏匿于合法的程序中，运行时不会在“任务栏”中生成图标，不会在任务管理器中被轻易发现。
- 危害性大：当木马被植入到目标计算机以后，攻击者可以通过对客户端的远程控制进行一系列能造成严重后果的非法行为，例如窃取用户隐私信息、控制系统的运行、破坏系统的数据等。

### 特洛伊木马的类型及其危害

常见的特洛伊木马类型及其危害，包括但不限于以下几种：

- 远程控制型：远程控制是木马的基本功能，在用户不知情的情况下，攻击者通过下发命令实现对用户计算机的远程控制，并完成木马传播者下发的攻击指令，例如篡改文件和数据、下载恶意软件等。
- 盗取密码型：这类木马以找到所有的隐藏密码为主，如各种社交账号的账户和密码，网络游戏中游戏账号和密码，并在受害者不知情的情况下将密码信息发送出去。
- 记录键值型：这类木马可以记录用户每一次敲击键盘的操作，通过键盘操作记录，攻击者可以获取到用户的密码等有用信息。此类木马会随着操作系统的启动而自动加载，分为在线和离线两种，分别记录用户在在线和离线两种状态下敲击键盘的情况。记录键值型木马一般也有邮件发送功能，能通过邮件将记录的信息发送给控制者。

## 如何防御特洛伊木马


防御木马的关键在于预防，即在木马进入设备并造成实质性损失之前，拦截攻击。您除了需要提升网络安全意识外，还可以通过CFW的入侵防御规则抵御木马入侵。具体措施如下：


### 提升网络安全意识

- 安装正版操作系统和应用程序，不在非正规网站下载应用程序。
- 不打开或安装来历不明的邮件、软件等，一些看似正常的邮件和软件，实际可能包含恶意木马程序。
- 不查看网站上的弹出式广告，这类广告经过精美的包装，是木马程序常用的载体之一。

### CFW配置特洛伊木马入侵防御规则

**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，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

**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** 单击“基础防御”中的“查看生效中的规则”，进入“基础防御规则”页面。

**步骤6** 筛选出防护特洛伊木马的规则：在上方筛选框中，选择“攻击类型”是“特洛伊木马”。

**步骤7** 批量开启防护：勾选对应规则，单击上方“拦截”。

#### 说明

拦截：防火墙对匹配当前防御规则的流量，记录至攻击事件日志中并进行拦截。

----结束

## 7.5 使用 CFW 防御漏洞攻击

本文介绍如何通过CFW防御漏洞攻击。

## 应用场景

漏洞往往是攻击者入侵系统的突破口，为攻击者提供了绕过正常安全控制的机会，从而对系统构成威胁。

CFW的IPS规则库配置了针对漏洞攻击的防御规则，能够深入检测网络流量中的恶意行为，并自动阻断潜在的攻击，有效应对各种漏洞攻击。

## 什么是漏洞攻击

漏洞攻击是指攻击者利用系统、软件或硬件中存在的安全漏洞，通过精心构造的攻击手段，在未授权的情况下访问或破坏目标系统，以达到其恶意目的的行为。这些漏洞通常是由于设计、实现或配置过程中的缺陷所导致的，它们为攻击者提供了绕过正常安全防护机制的机会。

漏洞攻击可以涉及多种技术和方法，包括但不限于：

- **注入攻击**：如SQL注入、命令注入等，攻击者通过向应用程序的输入字段中插入恶意代码，以执行非预期的操作或访问敏感数据。
- **跨站脚本（XSS）**：攻击者利用网站的安全漏洞，在用户浏览器中注入恶意脚本，从而窃取用户信息、会话令牌或进行其他恶意活动。
- **跨站请求伪造（CSRF）**：攻击者诱使用户在已登录的Web应用程序上执行非预期的操作，如转账、更改密码等，而用户往往对此毫不知情。
- **缓冲区溢出**：攻击者通过向程序发送超出其处理能力的数据，导致程序崩溃或执行恶意代码。

## 漏洞攻击的危害


漏洞攻击的危害是多方面的，包括但不限于：


- **经济损失**：漏洞攻击可能导致受害者业务中断、数据泄露等，从而蒙受巨大的经济损失。
- **信息泄露**：攻击者可以通过漏洞获取用户的通讯录、聊天记录等敏感信息，侵犯个人隐私。
- **网络破坏**：当黑客成功攻击一台服务器后，可能会将其变成“傀儡机”，用于对其他主机发起攻击，扩大攻击范围。
- **恶意软件传播**：攻击者可能利用漏洞在受害者的系统中植入恶意软件，如病毒、木马等，进一步破坏系统安全。

## 如何防御漏洞攻击

为了防御漏洞攻击，除了及时更新和修补漏洞、使用强密码和多因素身份验证、定期备份数据、使用防火墙和防护软件、实施访问控制、定期进行安全审计和漏洞扫描外，您可以使用CFW入侵防御功能，拦截漏洞攻击。

**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，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

**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** 单击“基础防御”中的“查看生效中的规则”，进入“基础防御规则”页面。

**步骤6** 筛选出防护漏洞攻击的规则：在上方筛选框中，选择“攻击类型”是“漏洞攻击”。

**步骤7** 批量开启防护：勾选对应规则，单击上方“拦截”。

#### 📖 说明

拦截：防火墙对匹配当前防御规则的流量，记录至攻击事件日志中并进行拦截。

----结束

## 7.6 使用 CFW 防御蠕虫病毒

本文介绍如何通过CFW防御蠕虫病毒攻击。

### 应用场景

蠕虫病毒借用网络互联的优势，通过网络漏洞、弱口令等方式攻击服务器并快速传播，对用户资产和业务造成极大的安全威胁。

CFW IPS规则库配置了针对蠕虫病毒的防御规则，可有效拦截“JS.FortNight.E-2”、“Lovgate病毒netservices.exe”等蠕虫病毒的攻击。

### 什么是蠕虫病毒

蠕虫病毒（Computer Worm）是一种能够自我复制并通过网络进行传播的恶意软件，它通过扫描网络中的漏洞，利用这些漏洞感染其他服务器，从而在网络中迅速扩散。蠕虫病毒不需要依附于其他程序，就可以独立存在并自主运行。

蠕虫病毒具有如下显著特点：

- **利用漏洞**：蠕虫病毒通常利用操作系统或应用程序中的安全漏洞进行传播。当这些漏洞被发现时，如果系统没有及时安装补丁或更新，就可能成为蠕虫病毒的攻击目标。
- **自我复制**：蠕虫病毒能够复制自身的全部或部分代码，并将这些复制体传播到网络中的其他服务器上。这种自我复制的能力是蠕虫病毒能够迅速扩散的基础。
- **独立传播**：与需要用户交互（如打开附件）的传统病毒不同，蠕虫病毒能够自主地在网络中搜索并感染其他易受攻击的服务器，而无需用户的直接干预。这种独立传播性使得蠕虫病毒更加难以防范。

### 蠕虫病毒的危害

蠕虫病毒对网络业务安全构成严重威胁，具体表现如下：


- **破坏系统**：蠕虫病毒可以破坏系统文件和数据，导致系统崩溃或无法正常工作。
- **盗取信息**：蠕虫病毒可以窃取用户的敏感信息，如密码、银行账户信息等。
- **滥用网络资源**：蠕虫病毒可以利用被感染的计算机进行DDoS攻击、垃圾邮件发送等非法行为，造成网络拥塞和服务不可用。
- **传播其他恶意软件**：蠕虫病毒可以利用被感染的计算机传播其他恶意软件，如木马病毒、间谍软件等。

## 如何防御蠕虫病毒

为了防御蠕虫病毒，除了建立良好的安全习惯、关闭或删除不必要的服务、定期更新系统和应用程序、使用强密码和多重认证、定期备份数据等常规手段外，您可以使用 CFW 入侵防御功能，拦截蠕虫攻击。

**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，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

**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** 单击“基础防御”中的“查看生效中的规则”，进入“基础防御规则”页面。

**步骤6** 筛选出防护蠕虫病毒的规则：在上方筛选框中，选择“攻击类型”是“蠕虫攻击”。

**步骤7** 批量开启防护：勾选对应规则，单击上方“拦截”。

### 说明

拦截：防火墙对匹配当前防御规则的流量，记录至攻击事件日志中并进行拦截。

----结束

# 8 通过配置 CFW 防护规则实现两个 VPC 间流量防护

## 应用场景

VPC之间存在着大量的数据交换需求，CFW提供的VPC间流量防护能够检测和统计VPC间的通信流量数据，帮助您发现异常流量。

本文介绍如何配置云防火墙实现VPC1（172.16.0.0/16）和VPC2（172.18.0.0/16）之间的流量防护。

## 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，即配置界面如下：

图 8-1 VPC 边界防火墙（新版）



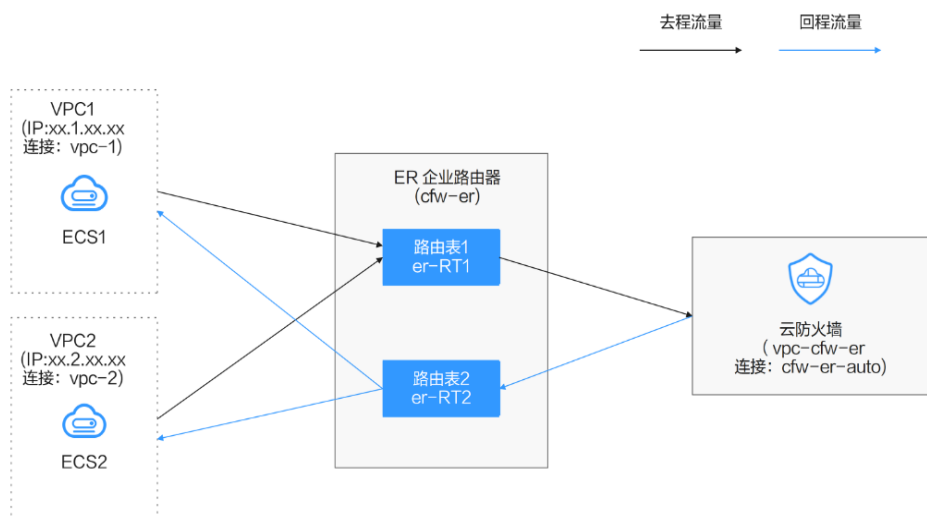
## 配置原理

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[步骤一：创建防火墙](#)。
2. 配置企业路由器。
  - 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[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[添加连接](#)。
  - c. 创建两个路由表(以er-RT1和er-RT2为例)，请参见[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[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[配置路由表er-RT2](#)。
  - e. 修改VPC的路由表，请参见[修改VPC的路由表](#)。
3. 开启VPC防护，并验证流量正常通信。
4. 配置防护规则，并查看防护效果。





图 8-2 流量走势图



## 步骤一：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** 在左侧导航栏中，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

**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：
  - 没有与其它防火墙实例关联。
  - 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 Inspection VPC 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

## 步骤二：配置企业路由器

**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 8-1 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。 <b>须知</b> 不能与已有路由和VPC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。 下拉列表中将展示您创建的企业路由器名称。	cfw-er
描述	（可选）路由的描述信息。 <b>说明</b> 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 8-2 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： <ul style="list-style-type: none"> <li>长度范围为1~64位。</li> <li>名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。</li> </ul>	er-RT1/er-RT2
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。 关于标签更详细的说明，请参见 <a href="#">标签概述</a> 。	“标签键”：test “标签值”：01
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。	-

#### 步骤6 配置关联路由表er-RT1：设置关联和路由功能。

- 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 8-3 创建关联



表 8-3 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 8-4 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 8-4 创建路由

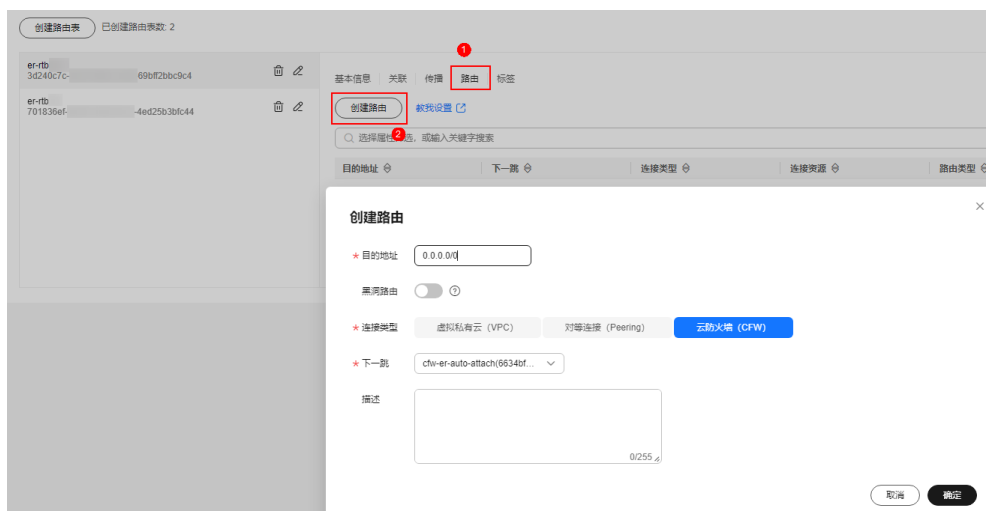


表 8-5 创建路由参数说明

参数名称	参数说明
目的地址	设置目的地址。 - 0.0.0.0/0: VPC的所有流量都会经过云防火墙防护 - 网段: 该网段的流量会经过云防火墙防护
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）。
描述	（可选）路由的描述信息。

**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 8-5** 创建关联**表 8-6** 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 8-6** 创建传播

表 8-7 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）
连接	在传播下拉列表中，选择需防护的VPC连接。	vpc-1

表 8-8 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）
连接	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 修改VPC的路由表，将VPC1的路由指向VPC2，VPC2的路由指向VPC1。

1. 返回至企业路由器服务页面，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。
2. 在“名称/ID”列，单击对应VPC的路由表名称，进入路由表“基本信息”页面。
3. 单击“添加路由”，主要参数填写如下：
  - VPC1（172.16.0.0/16）中添加路由：
    - 目的地址类型：选择“IP地址”。
    - 目的地址：172.18.0.0/16
    - 下一跳类型：企业路由器
  - VPC2（172.18.0.0/16）中添加路由：
    - 目的地址类型：选择“IP地址”。
    - 目的地址：172.16.0.0/16

- 下一跳类型：企业路由器

----结束

### 步骤三：开启 VPC 防护并验证流量正常通信

- 步骤1** 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2** 在“防火墙状态”侧，单击“开启防护”。
- 步骤3** 单击“确认”，完成开启VPC边界防火墙。
- 步骤4** 生成流量，请参见[验证网络互通情况](#)。
- 步骤5** 查看日志：在左侧导航栏中，选择“日志审计 > 日志查询”，选择“流量日志 > VPC边界防火墙”页签。
- 有日志记录：云防火墙已成功防护VPC间流量。
  - 无日志记录，排查企业路由器配置，请参见[步骤二：配置企业路由器](#)。

----结束

### 步骤四：配置防护规则并查看防护效果

- 步骤1** 在左侧导航栏中，选择“访问控制 > 访问策略管理”，选择“VPC边界”页签，进入VPC边界管理页面。
- 步骤2** 添加三条防护规则。
- 单击“添加”，在弹出的“添加防护规则”中，填写新的防护信息，其余参数可根据业务部署填写。

- 一条阻断所有流量。
  - 源：Any
  - 目的：Any
  - 服务：Any
  - 应用：Any
  - 动作：阻断
- 一条放行VPC1到VPC2的流量
  - 源：选择“IP地址”、填写172.16.0.0/16。
  - 目的：选择“IP地址”、填写172.18.0.0/16。
  - 服务：Any
  - 应用：Any
  - 动作：放行
- 一条放行VPC2到VPC1的流量
  - 源：选择“IP地址”、填写172.18.0.0/16。
  - 目的：选择“IP地址”、填写172.16.0.0/16。
  - 服务：Any
  - 应用：Any

- 动作：放行

**步骤3** 通过访问控制日志查看命中详情。

在左侧导航栏中，选择“日志审计 > 日志查询”。默认进入“攻击事件日志”页面，选择“访问控制日志”页签，切换至“VPC边界防火墙”页签。

----结束

## 相关文档

需要增加其他防护规则时，请参见防护规则的详细参数说明[添加防护规则](#)。

# 9 通过配置 CFW 防护规则实现 SNAT 流量防护

## 9.1 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

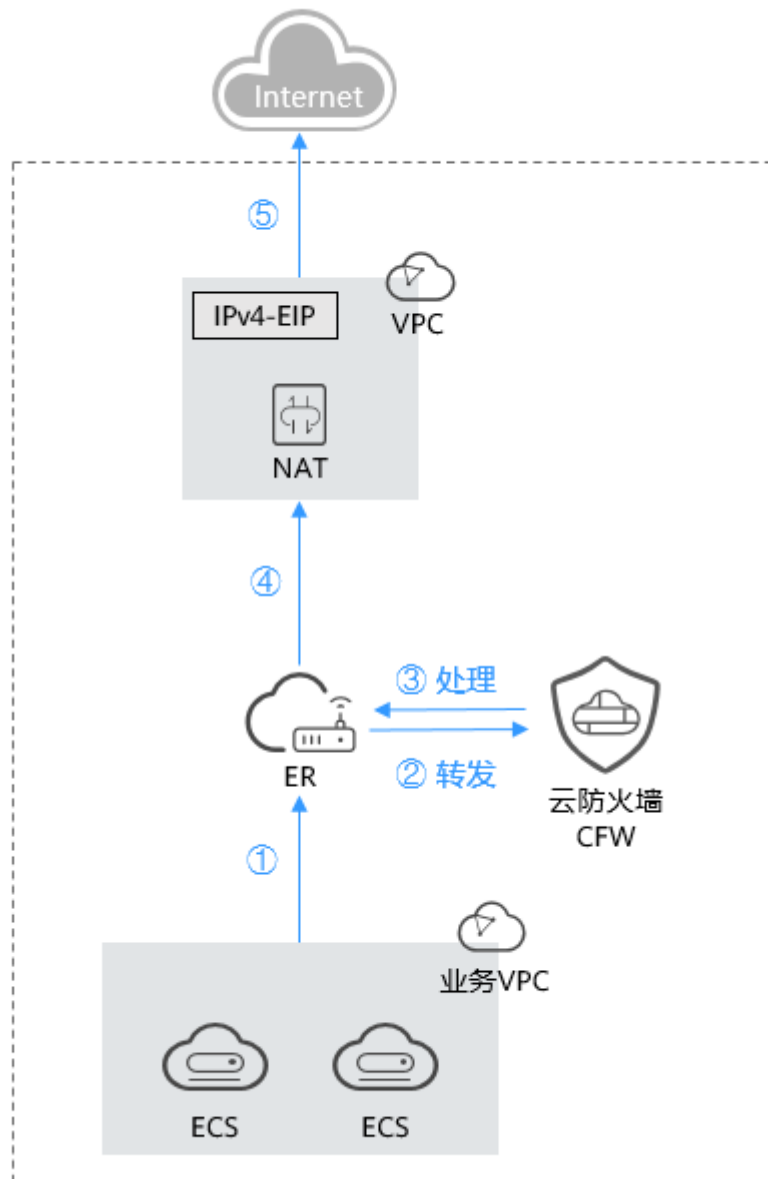
- 配置中需要使用企业路由器（Enterprise Router, ER），关于企业路由器请参见[什么是企业路由器？](#)。
- 需完成创建防火墙，具体配置请参见[创建防火墙](#)。

### 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

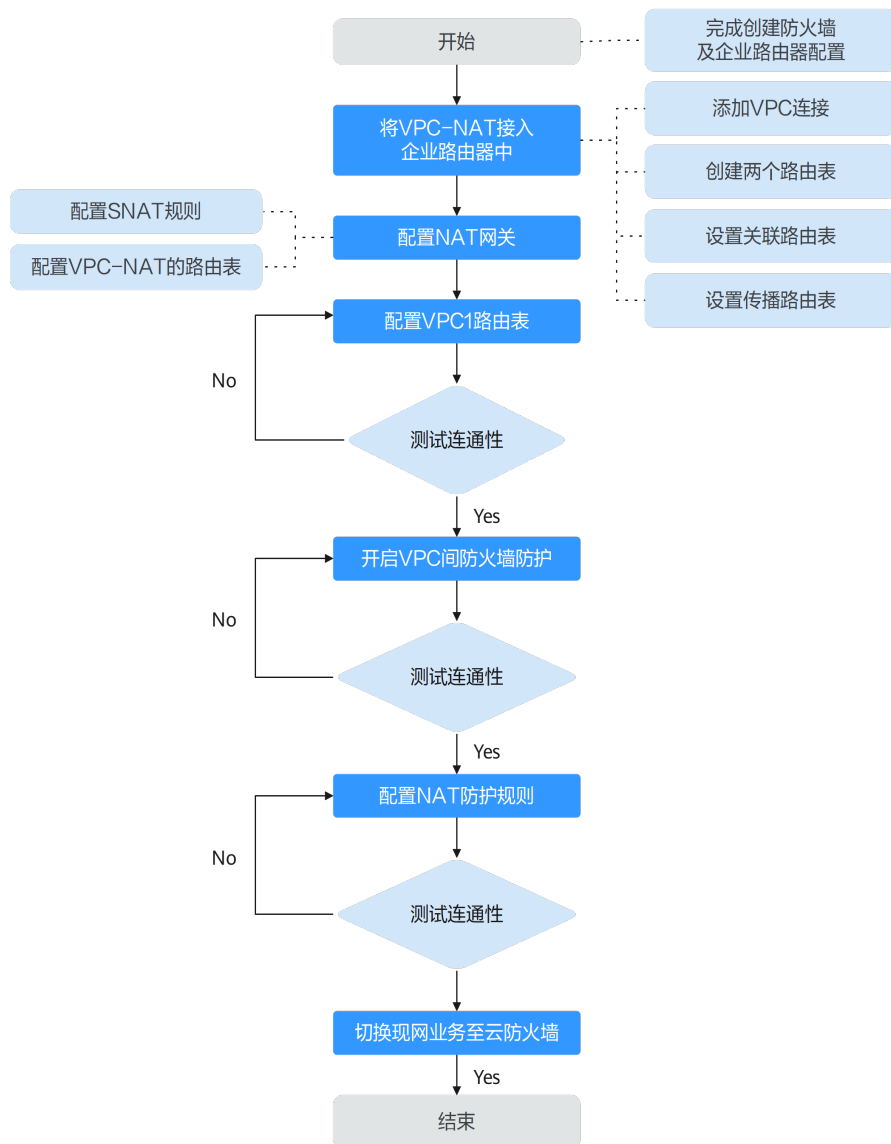
- 建议为NAT网关创建独立VPC不用于云服务器等实例网络配置，避免影响后续的访问控制。
- 在前期网络规划复杂甚至不合理的情况下（例如存在VPC网段重叠、NAT网关已有复杂配置、已通过VPC-Peering配置东西向通信等场景下），请充分评估网络互连、环路、路由冲突等风险。

- 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 9-1 SNAT 防护配置流程



## 9.2 资源和成本规划

本节介绍SNAT防护中的资源和成本规划。

表 9-1 资源说明

资源	资源说明	数量	成本说明
NAT网关 ( NAT Gateway )	被防护的资源。	1	具体的计费方式及标准请参考 <a href="#">NAT网关计费说明</a> 。

资源	资源说明	数量	成本说明
弹性公网IP (Elastic IP)	EIP, NAT网关绑定的EIP。	至少1个	具体的计费方式及标准请参考 <a href="#">EIP计费说明</a> 。
虚拟私有云 (Virtual Private Cloud)	NAT网关所在的VPC; CFW通过防护VPC实现NAT网关的流量防护。	1	具体的计费方式及标准请参考 <a href="#">VPC计费说明</a> 。
企业路由器 (Enterprise Router)	ER, 连接VPC到云防火墙的流量。	1	具体的计费方式及标准请参考 <a href="#">ER计费说明</a> 。
云防火墙 (Cloud Firewall)	CFW, 仅专业版提供SNAT防护。	1	具体的计费方式及标准请参考 <a href="#">CFW计费说明</a> 。

## 9.3 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。

### 将 VPC1 和 VPC-NAT 接入企业路由器中

**步骤1** 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2** 创建两个路由表。


1. 在左侧导航栏中，单击左上方的，选择“网络 > 企业路由器”，单击“管理路由表”，进入“路由表”页面。
2. 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 9-2 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。 命名规则如下： - 长度范围为1~64位。 - 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。 关于标签更详细的说明，请参见 <a href="#">标签概述</a> 。

**步骤3** 设置关联路由表。

1. 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](#)。

表 9-3 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。
2. 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 9-2 创建路由

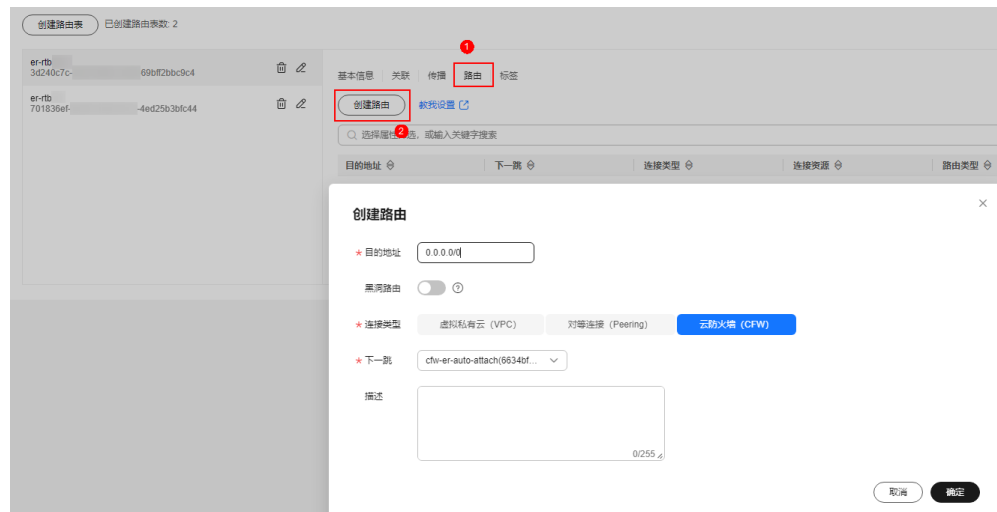


表 9-4 创建路由参数说明

参数名称	参数说明
目的地址	设置目的地址。 - 0.0.0.0/0: VPC的所有流量都会经过云防火墙防护 - 网段: 该网段的流量会经过云防火墙防护
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)。
描述	(可选) 路由的描述信息。

**步骤4** 设置传播路由表。

1. 设置关联功能, 添加防火墙的关联: 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 9-3 创建关联



表 9-5 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. 设置传播功能，添加VPC1的传播：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 9-4 创建传播



表 9-6 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）”。

参数名称	参数说明
连接	在传播下拉列表中，选择VPC1的连接。

3. 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 9-7 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

## 9.4 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](#)。

#### 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 9-8 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 <ul style="list-style-type: none"><li>自定义：自定义一个网段或者填写某个VPC的地址。</li></ul> <b>说明</b> 支持配置0.0.0.0/0的地址段，在多段地址配置时更方便。 可以配置32位主机地址，NAT网关只针对此地址起作用。
公网IP类型	选择“弹性公网IP”，此处用来提供互联网访问的公网IP。 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。 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。 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 9-9 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，填写VPC1的IP地址。 <b>说明</b> 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”。

参数	说明
下一跳	选择下一跳资源。 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。 <b>说明</b> 描述信息内容不能超过255个字符，且不能包含“<”和“>”。

----结束

## 9.5 配置 VPC1 路由表

### 配置 VPC1 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 9-10 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。 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。 <b>说明</b> 描述信息内容不能超过255个字符，且不能包含“<”和“>”。


----结束


## 9.6 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。

### 配置 NAT 防护规则

**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，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。
- 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，关键参数填写如下：
- 规则类型：NAT规则
  - 方向：SNAT
  - 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”。
  - 应用：Any
- 步骤7** 单击“确认”，完成防护规则配置。
- 结束

# 10 使用 CFW 防护企业资源

## 背景信息

华为云提供了[企业项目管理](#)（Enterprise Project Management Service, EPS）服务，帮助企业管理云上的人、财、物、权、业务，规范企业在华为云上的操作，满足企业云上IT治理诉求。

用户可以根据组织架构规划企业项目，统一管理分布在不同区域的资源，还可以为每个企业项目设置拥有不同权限的“用户”和“用户组”。

## 应用场景

大企业按照分公司或部门的维度管理业务时，难以划分账单和分配资源，此时可以使用企业项目管理服务：

- 将不同的业务赋予不同的企业项目，按照企业项目的维度产生账单，方便预算管理和分账处理。
- 通过给用户和用户组授权不同的企业项目，实现更精细化的资源管理。

本文介绍企业通过EPS管理业务时如何规划云防火墙。

## 资源和成本规划

表 10-1 资源说明

资源	资源说明	数量	成本说明
企业项目（Enterprise Project Management Service）	EPS，管理企业资源。	至少2个	企业项目管理为免费服务。
云防火墙（Cloud Firewall）	CFW，提供云上资源防护。	至少2个	具体的计费方式及标准请参考 <a href="#">CFW 计费说明</a> 。

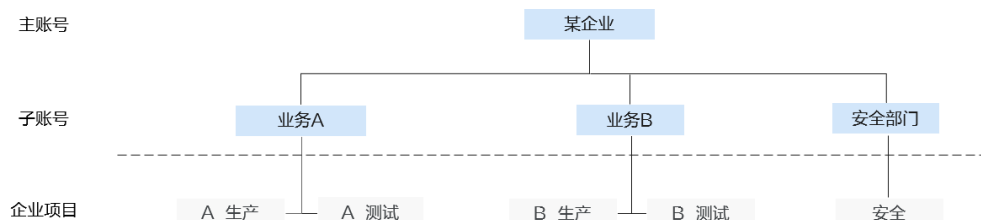
资源	资源说明	数量	成本说明
弹性公网IP (Elastic IP)	(可选) EIP, 云上资源。	按业务需求配置	具体的计费方式及标准请参考 <a href="#">EIP计费说明</a> 。
虚拟私有云 (Virtual Private Cloud)	(可选) VPC, 云上资源。	按业务需求配置	具体的计费方式及标准请参考 <a href="#">VPC计费说明</a> 。
企业路由器 (Enterprise Router)	(可选) ER, 连接VPC到云防火墙的流量。 云防火墙防护VPC时, 依赖ER服务引流。	至少1个	具体的计费方式及标准请参考 <a href="#">ER计费说明</a> 。

## 应用示例

某企业有A、B两个业务在云上, 每个业务分为生产和测试两个业务团队, 该企业按照以下维度创建企业项目:

- A、B两个业务需要分开管理, 则该企业为A业务创建了企业项目“A\_生产”、“A\_测试”, 为B业务创建了企业项目“B\_生产”、“B\_测试”; 在购买云上资源时, 将资源按业务团队绑定到对应的企业项目中。
- 该企业为安全部门创建了企业项目“安全”, 在购买安全产品时, 将产品绑定在“安全”下, 以便财务团队区分账单以及管理安全相关的预算使用情况。

图 10-1 账号及企业项目



该企业需要为子账号（业务A、业务B）提供隔离的生产环境和测试环境, 并使用CFW提供防护, 安全管理员为每个环境都独立购买一套云防火墙:

- 生产环境需要防护EIP和VPC, 安全管理员购买了专业版防火墙;
- 测试环境需要防护EIP, 安全管理员购买了标准版防火墙。

防火墙在每个环境中由AB两个业务共用, 账单由安全部门承担, 如图10-2所示。

图 10-2 资源划分及账单归属

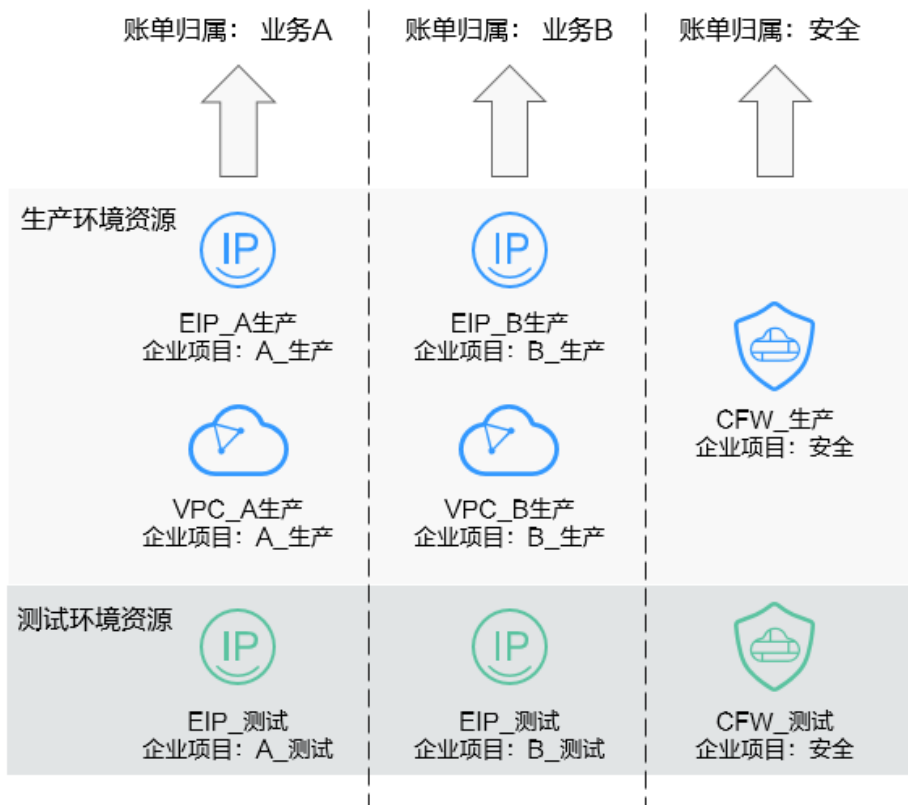


图 10-3 用户企业项目管理



企业可以在统一身份认证（Identity and Access Management, IAM）中对子账号进行企业项目级别的授权，达到隔离不同业务资源的效果，以安全管理员和测试环境管理员为例：

- 该企业授权安全管理员所有企业项目的权限，因此安全管理员可以在两个防火墙上看到资源，在两个防火墙上配置不同的防护策略以及安全防护模式，在不同环境上开启防护：

  - 在生产环境的云防火墙上，针对企业项目“A\_生产”、“B\_生产”下的弹性公网IP以及虚拟私有云都开启了防护。

- 在测试环境的云防火墙上，针对企业项目“A\_测试”、“B\_测试”下的弹性公网IP开启了防护。
- 该企业授权测试环境管理员“A\_测试”、“B\_测试”以及“安全”的企业项目，因此测试环境管理员可以操作账号中的两个防火墙，由于未获得生产环境资源的授权，测试管理员在防火墙的资源管理页，无法纳管生产环境的资源（EIP/VPC），只能看到测试环境上的资源信息。

## 相关操作

- 创建企业项目，请参见[创建企业项目](#)。
- 购买云防火墙请参见[购买云防火墙](#)。
- 通过IAM服务创建和授权用户组请参见[创建用户组并授权](#)，通过IAM服务授权用户请参见[给IAM用户授权](#)。

# 11 使用 CFW 跨账号防护 EIP 资源

## 应用场景

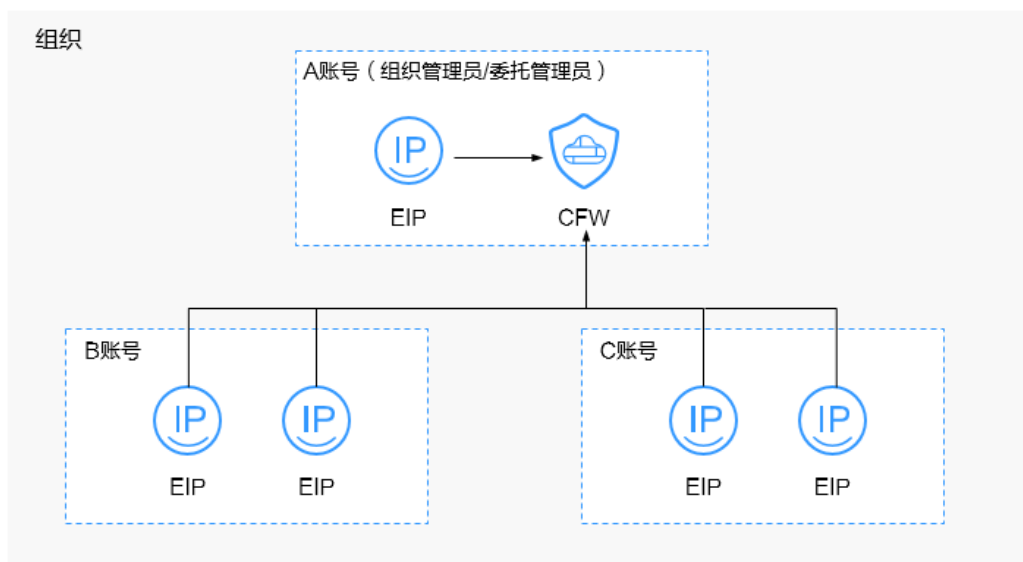
多个账号的资源防护，例如，企业中不同部门使用不同的账号，但多部门之间需要共用云防火墙的防护策略。

本文介绍如何通过CFW防护多个账号下的EIP资源。

## 方案介绍

跨账号防护EIP资源的方案为：A账号是组织管理员或委托管理员，将B账号、C账号添加到组织成员，A账号中购买云防火墙，在防火墙中将B账号、C账号添加到组织成员，开启对应EIP的防护及配置防护策略。

图 11-1 跨账号防护



## 约束限制

- 不支持跨区域防护EIP资源，如需在其它区域使用，请切换到对应区域购买防火墙，具体操作请参见[购买云防火墙](#)。



- 单个防火墙实例支持防护的账号个数如下：
  - 包年/包月防火墙：
    - 标准版：20个
    - 专业版：50个
  - 按需计费防火墙（专业版）：20个

## 资源和成本规划

表 11-1 资源说明

资源	资源说明	数量	成本说明
企业中心	提供给企业客户的云上组织管理、财务管理的企业上云综合管理服务。 使用组织服务依赖开通企业中心。	1个	企业中心为免费服务。
组织	Organizations，为企业用户提供多账号关系的管理能力。	1个	组织为免费服务。
云防火墙（Cloud Firewall）	CFW，提供云上资源防护。	1个	具体的计费方式及标准请参考 <a href="#">CFW计费说明</a> 。
弹性公网IP（Elastic IP）	EIP，被防护的资源。	按业务需求配置	具体的计费方式及标准请参考 <a href="#">EIP计费说明</a> 。

## 如何实现跨账号防护 EIP 资源

**步骤1** 准备账号和权限，本文以A账号是组织管理员为例。

### 📖 说明

如果A账号不是组织管理员，则由组织管理员将A账号添加为委托管理员，相关操作请参见[添加委托管理员](#)。

1. 使用A账号操作如下。
  - a. 购买云防火墙标准版或专业版，请参见[购买云防火墙](#)。
  - b. （可选）开通企业中心，详情请参见：[开通企业中心功能](#)。  
如果已开通企业中心，请跳过此步骤。
  - c. （可选）开通组织服务并创建组织。  
如果已开通组织服务，请跳过此步骤。

### 📖 说明

如果已经加入组织，请退出已加入的组织后再进行创建组织操作，退出组织操作步骤请参见[成员账号退出组织](#)。


- i. [登录管理控制台](#)。
- ii. 单击左上方的 ，选择“管理与监督 > 组织 Organizations”。
- iii. 开通Organizations云服务。进入开通页，单击“立即开通”。

图 11-2 开通 Organizations 云服务



开通Organizations云服务后，系统会自动创建组织和根组织单元，并将开通服务的账号设置为管理账号。

- d. 邀请B账号、C账号加入组织，相关操作请参见[邀请账号加入组织](#)。
  - e. 设置CFW为可信服务，操作详情请参考[启用、禁用可信服务](#)。
2. 使用B账号、C账号加入A账号的组织，具体操作请参见[接受或拒绝来自组织的邀请](#)。

**步骤2** 使用A账号在防火墙中添加B账号、C账号。


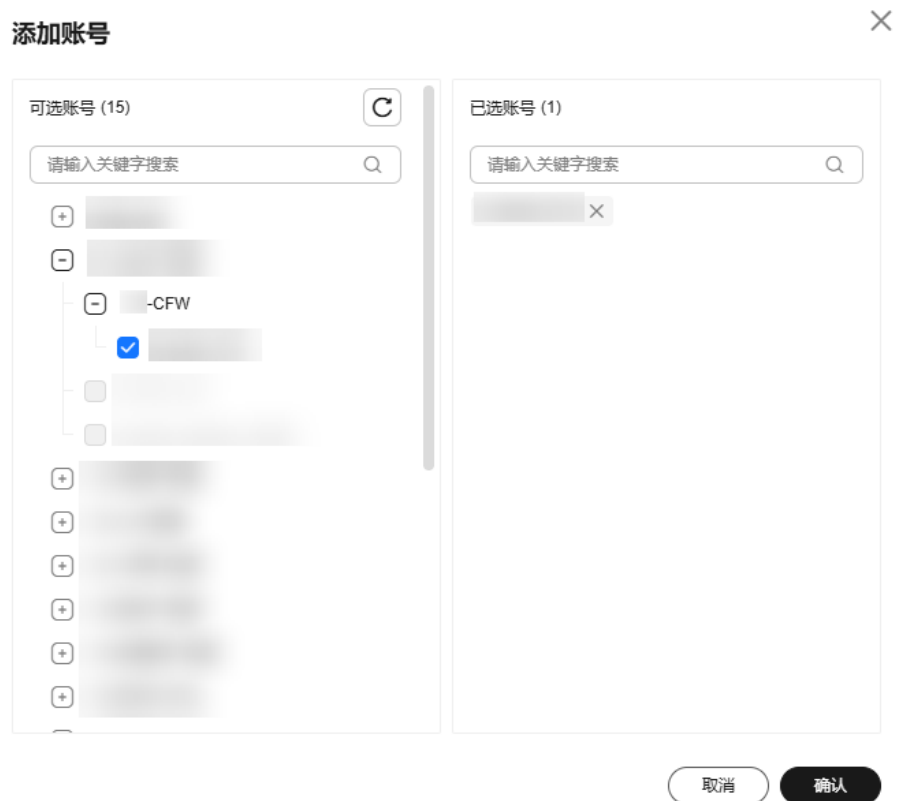
1. 在左侧导航栏中，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。
2. （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。
3. 在左侧导航栏中，选择“系统管理 > 多账号管理”，进入“多账号管理”页面。
4. 单击“添加账号”，弹出页面通过树状展开勾选B账号和C账号，自动添加至右侧“已选账号”，单击“确认”。

图 11-3 添加组织成员账号



### 说明

- 添加的账号需为同一个组织内的账号，有关组织账号的详细说明请参见《[组织账号概述](#)》。
- 该账号未被其它防火墙防护中。

### 步骤3 开启EIP防护。

1. 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。
2. 搜索B账号、C账号下的EIP：搜索框中选择“所有者”，选择B账号和C账号。

### 说明

如果无法搜索到B账号、C账号下的EIP，需单击页面右上角“资产同步”，将EIP资源信息同步至列表中。

3. 勾选需要开启防护的弹性公网IP，单击列表上方的“开启防护”。

### 说明

列表中的“所有者”列展示该EIP归属的账号。

### 步骤4 配置防护策略。

- 配置“防护规则”/“黑白名单”管控流量，详细介绍请参见[访问控制策略概述](#)。
- 配置“攻击防御”检测和防护流量，详细介绍请参见[攻击防御功能概述](#)。

**步骤5** 查看日志信息，详细介绍请参见[防护日志概述](#)。

----结束

## 相关文档

如果您需要跨账号防护VPC资源，请参见[使用CFW跨账号防护VPC资源](#)。

# 12 使用 CFW 跨账号防护 VPC 资源

## 应用场景

多个账号的资源防护，例如，企业中不同部门使用不同的账号，但多部门之间需要共用云防火墙的防护策略。

本文介绍使用CFW防护A账号的VPC后，如何将其它账号的VPC资源加入防护。

## 方案介绍

A账号已配置VPC边界防护并运行一段时间，此时需要将B账号、C账号的VPC资源加入防护的方案为：

A账号将企业路由器共享至B账号、C账号，使用B账号、C账号在企业路由器中添加连接，在A账号的企业路由器中接受连接，并添加关联和传播，在B账号、C账号的VPC中添加路由，则完成防护接入，此时云防火墙中的防护策略将同步防护B账号、C账号下的VPC资源。

图 12-1 跨账号防护方案

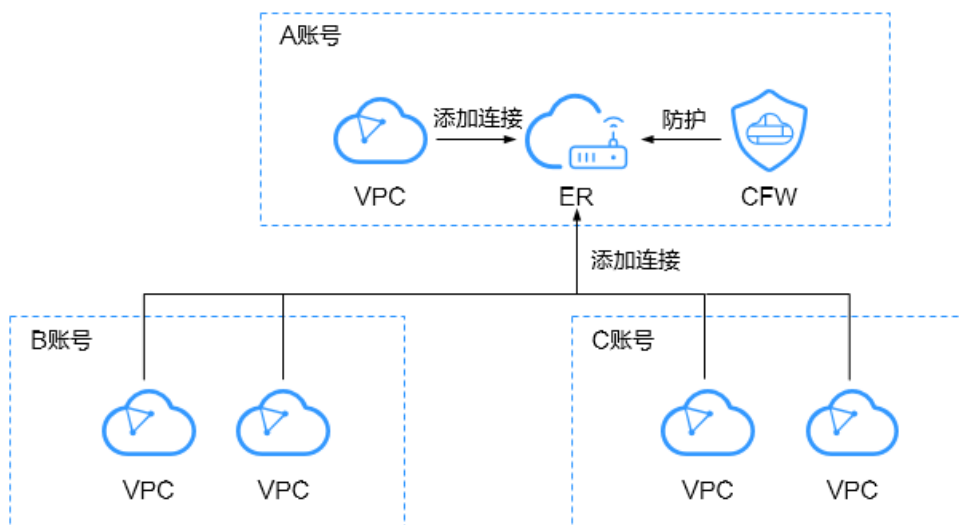


图 12-2 操作步骤



## 资源和成本规划

表 12-1 资源说明

资源	资源说明	数量	成本说明
企业路由器 (Enterprise Router)	ER, 连接VPC到云防火墙的流量。	1 (当前已有)	具体的计费方式及标准请参考 <a href="#">ER计费说明</a> 。
云防火墙 (Cloud Firewall)	CFW, 仅专业版提供VPC边界防护。	1 (当前已有)	具体的计费方式及标准请参考 <a href="#">CFW计费说明</a> 。
虚拟私有云 (Virtual Private Cloud)	VPC, 被防护的资源。	1	具体的计费方式及标准请参考 <a href="#">VPC计费说明</a> 。

## 如何将其它账号下的 VPC 资源加入防护

A账号中已经开启VPC边界防护（操作方式请参见[通过配置CFW防护规则实现两个VPC间流量防护](#)），并运行一段时间，此时将B账号、C账号的VPC资源加入防护的操作如下：

**步骤1** 在A账号中将企业路由器共享至B账号、C账号，共享步骤请参见[创建共享](#)。

**步骤2** 使用B账号、C账号在企业路由器中添加连接，具体操作请参见[企业路由器中添加VPC连接](#)。

### 说明

- 每个VPC需要添加1个连接。
- 下文资源举例：B账号下的1个VPC资源名为VPC1，连接为VPC\_B；C账号下的1个VPC资源名为VPC2，连接为VPC\_C。

**步骤3** 使用A账号配置路由表。

1. 接受B账号、C账号的连接申请，具体操作请参见[接受连接创建申请](#)。
2. 添加关联。

单击企业路由器名称，并选择“路由表”页签，在路由表设置页面，选择关联路由表(er-RT1)，单击“关联”页签，单击“创建关联”。

### 📖 说明

如何识别关联路由表：关联路由表用于将流量从VPC传输到云防火墙，即当前配置如下：

- 关联页签（多条关联的连接）：
  - 连接类型：虚拟私有云（VPC）
  - 连接：A账号下多个VPC的连接。
- 路由页签的关键参数：
  - 连接类型：云防火墙（CFW）
  - 下一跳：防火墙连接（cfw-er-auto-attach）

此处以添加B账号的VPC资源为例，如需添加多个（例如3个）VPC资源，需要添加对应个数（例如3个）的关联。

- 连接类型：选择“虚拟私有云（VPC）”。
- 连接：选择B账号下的VPC连接，即VPC\_B。

### 📖 说明

此时关联路由表配置如下：

- 关联页签（多条关联的连接+VPC\_B）：
  - 连接类型：虚拟私有云（VPC）
  - 连接：A账号下多个VPC的连接、B账号下VPC的连接。
- 路由页签的关键参数：
  - 连接类型：云防火墙（CFW）
  - 下一跳：防火墙连接（cfw-er-auto-attach）

### 3. 添加传播。

选择传播路由表（er-RT2），单击“传播”页签，单击“创建传播”。

### 📖 说明

如何识别传播路由表：传播路由表用于将流量从云防火墙传输到VPC，即当前配置如下：

- 关联页签的关键参数：
  - 连接类型：云防火墙（CFW）
  - 连接：防火墙连接（cfw-er-auto-attach）
- 传播页签（多条传播的连接）：
  - 连接类型：虚拟私有云（VPC）
  - 连接：A账号下多个VPC的连接。

此处以添加B账号的VPC资源为例，如需添加多个（例如3个）VPC资源，需要添加对应个数（例如3个）的传播。

- 连接类型：选择“虚拟私有云（VPC）”。
- 连接：选择B账号下的VPC连接，即VPC\_B。

### 📖 说明

此时传播路由表配置如下：

- 关联页签的关键参数：
  - 连接类型：云防火墙（CFW）
  - 连接：防火墙连接（cfw-er-auto-attach）
- 传播页签（多条传播的连接+VPC\_B）：
  - 连接类型：虚拟私有云（VPC）
  - 连接：A账号下多个VPC的连接、B账号下VPC的连接。

#### 步骤4 使用B账号、C账号，配置VPC的路由表。

例如需要防护VPC1和VPC2之间的流量，则此处将VPC1的路由指向VPC2，VPC2的路由指向VPC1。

1. 返回至企业路由器服务页面，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。
2. 在“名称/ID”列，单击对应VPC的路由表名称，进入路由表“基本信息”页面。
3. 单击“添加路由”，主要参数填写如下：
  - B账号的VPC1中添加路由：
    - 目的地址类型：选择“IP地址”。
    - 目的地址：填写VPC2的网段
    - 下一跳类型：企业路由器
  - C账号的VPC2中添加路由：
    - 目的地址类型：选择“IP地址”。
    - 目的地址：填写VPC1的网段
    - 下一跳类型：企业路由器

#### 步骤5 配置防护策略。

- 配置“防护规则”/“黑白名单”管控流量，详细介绍请参见[访问控制策略概述](#)。
- 配置“攻击防御”检测和防护流量，详细介绍请参见[攻击防御功能概述](#)。

### 📖 说明

接入同一个企业路由器的VPC资源，默认使用该企业路由器绑定的云防火墙下的防护策略。

#### 步骤6 查看日志信息，详细介绍请参见[防护日志概述](#)。

----结束

## 相关文档

如果您需要跨账号防护EIP资源，请参见[使用CFW跨账号防护EIP资源](#)。