ALIBABA CLOUD

阿里云

云防火墙

云防火墙公共云合集

文档版本：20220425

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.攻击防护 05
1.1. 入侵防御 05
1.2. 漏洞防护 07
1.3. 失陷感知 09
1.4. 防护配置 10
2.访问控制 13
2.1. 访问控制策略总览 13
2.2. 互联网边界（内外双向流量） 13
2.3. 主机边界防火墙（ECS实例间） 18
2.4. VPC边界防火墙 25
2.5. DNS域名解析地址访问控制策略 29
2.6. 安全组默认放通 34
2.7. 安全组检查 37
2.8. 智能策略 40
2.9. 地址簿管理 41
2.10. 修改云防火墙访问控制策略的优先级 46
2.11. DNS域名访问控制策略 47

1.攻击防护

1.1. 入侵防御

入侵防御页面为您实时展示云防火墙拦截流量的源IP、目的IP、阻断应用、阻断来源和阻断事件详情等信息。本文介绍了入侵防御页面展示的信息和相关操作。

前提条件

您需要先在**防护配置**页面，开启**基础防御**功能，云防火墙才能拦截这些流量并展示在**入侵防御**页面的拦截记录中。

概述

入侵防御页面为您展示了云防火墙对互联网出方向、入方向的流量和VPC间流量进行防护的详细信息，您可切换到**互联网防护**或**VPC防护**页签查看对应事件详情。

> **注意** 云防火墙高级版不支持展示**VPC防护**页签。

限制说明

- 云防火墙高级版、企业版和旗舰版支持入侵防御功能，免费版不支持。
- 云防火墙攻击防护功能不支持解析TLS、SSL加密的流量，因此无法对此类流量进行检测和防护。

互联网防护

在**互联网防护**页签中，您可查看最近1小时、1天、7天、1个月和自定义时间范围内互联网出方向或入方向的阻断情况。可设置的自定义时间范围为距离当前时间6个月以内。

互联网防护页签包含以下模块：

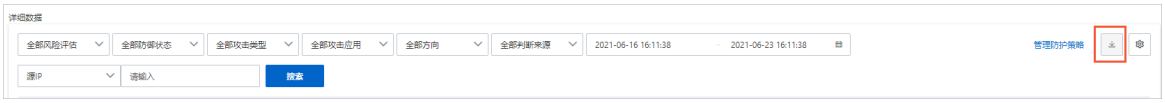
- **防护数据**：包含攻击总数、攻击类型分布、拦截数据。其中，拦截数据包含以下内容：
  - **阻断目的TOP**：展示了被云防火墙阻断的流量中，占比最大的前5个目的IP地址。

    单击阻断目的IP地址右侧的**查看日志**可跳转到云防火墙**日志审计**页面。您可在日志列表中查看该目的IP地址的目的端口、应用类型、动作等详细信息。
  - **阻断来源TOP**：展示了被云防火墙阻断的流量中，占比最大的前3个来源类型。
  - **阻断应用TOP**：展示了被云防火墙阻断的流量中，占比最大的前5个应用类型。
- **详细数据**：展示了所有阻断事件的详细信息，包括事件的风险级别、事件数量、源IP地址和目的IP地址等信息。

在**详细数据**模块，您可以执行以下操作：

- 在搜索栏通过筛选风险级别、判断来源、方向和时间范围等信息定位到具体事件。
- 单击**操作**栏的**详情**可打开阻断事件的详情页面，查看事件描述、攻击载荷等详细信息。

- 在搜索栏右侧，单击 图标，下载入侵防御策略。默认下载距离当前时间最近的1,000条入侵防御策略，超出部分不支持下载。



VPC防护

VPC防护页签展示了云防火墙拦截到的VPC网络之间的异常事件信息。您可以查看指定时间段内VPC拦截事件的名称、风险级别、攻击类型等详细信息。

在**VPC防护**页签，您可根据需要执行以下操作：

- 选择风险级别、防御状态、攻击类型和时间等条件后，单击**搜索**，查看符合设定条件的事件信息。
- 定位到目标事件，单击**详情**，查看当前事件的事件描述、规则ID、防御状态等详细信息。

相关文档

- 云防火墙支持防护的范围
- 防护配置

1.2. 漏洞防护

漏洞防护页面展示了可被网络侧攻击利用的漏洞（这类漏洞由云安全中心漏洞检测功能自动检测并同步到云防火墙），并提供针对此类漏洞的攻击防御能力。您可以通过手动开启云防火墙开关和IPS防御规则，防止这些漏洞被利用，从而避免您的资产遭受入侵。

前提条件

已在**防护配置**页面，将威胁引擎运行模式设置为**拦截模式-宽松**、**拦截模式-中等**或**拦截模式-严格**。

> **说明** 如果您未将威胁引擎设置为拦截模式，**漏洞防护**页面中，所有漏洞的防护状态将为**仅告警**，表示云防火墙仅对检测到的漏洞进行告警和记录，不会对其进行拦截。有关威胁引擎运行模式的详细介绍，请参见威胁引擎运行模式。

限制说明

- 云防火墙高级版、企业版和旗舰版支持漏洞防护功能，免费版不支持。
- 漏洞防护功能支持自动检测漏洞，不支持手动检测漏洞。

  > **说明** 如果您需要手动实时扫描漏洞威胁情况，请前往云安全中心控制台的**漏洞修复**页面进行操作。相关信息，请参见一键扫描漏洞。

- 云防火墙攻击防护模块不支持解析TLS、SSL加密的流量，因此无法对此类流量进行检测和防护。

可检测的漏洞类型

- **Web-CMS漏洞**：Web-CMS漏洞检测功能监控网站目录，识别通用建站软件，通过漏洞文件比对方式检测建站软件中的漏洞。详细内容，请参见Web-CMS漏洞。
- **应用漏洞**：应用漏洞检测功能提供系统服务弱口令、系统服务和应用服务的漏洞检测及修复服务。详细内容，请参见应用漏洞。
- **应急漏洞**：应急漏洞检测功能临时提供针对网络上突然出现的紧急漏洞的检测和修复服务。详细内容，请参见应急漏洞。

支持的漏洞防护状态

- **已拦截**：表示该攻击漏洞被云防火墙拦截。
- **仅告警**：表示云防火墙仅检测该漏洞并提供告警，不进行拦截处理。
- **部分防护**：表示部分ECS服务器已开启漏洞防护。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**攻击防护 > 漏洞防护**。
3. 在**漏洞防护**页面，查看云防火墙对资产进行漏洞攻击检测的结果。

   漏洞防护页面展示了最近1个月、1天和7天内的漏洞检测结果。

   - 鼠标移动到**存在漏洞资产数**列的

     图标上，会展示检测到存在该漏洞的服务器IP地址。

- **攻击次数**：表示您资产受到漏洞攻击的次数。
- **防护状态**：表示云防火墙对漏洞攻击进行的相应处置。支持的防护状态如下：
  - **已拦截**：表示该攻击漏洞被云防火墙拦截。
  - **仅告警**：表示云防火墙仅检测该漏洞并提供告警，不进行拦截处理。
  - **部分防护**：表示部分ECS服务器已开启漏洞防护。
- **详情**：单击**详情**，打开**漏洞实时防护详情**页面，查看漏洞的详细信息，包括漏洞名称、漏洞风险等级、CVE编号、受影响资产等。

4. 在**漏洞防护**页面，定位到状态为**仅告警**的漏洞，单击**操作**列的**开启防护**。
   提交一键开启防护后，云防火墙将自动开启该漏洞所在的服务器的防火墙开关，漏洞状态更新预计需要1~2分钟时间，请您耐心等待。

> **说明** 开启漏洞防护后，原有的访问控制策略在新开启防火墙开关的资产上会继续生效，您需要确保在云防火墙控制台的**互联网边界防火墙**页面**外对内**页签中已经放行这些资产对外的端口。

1.3. 失陷感知

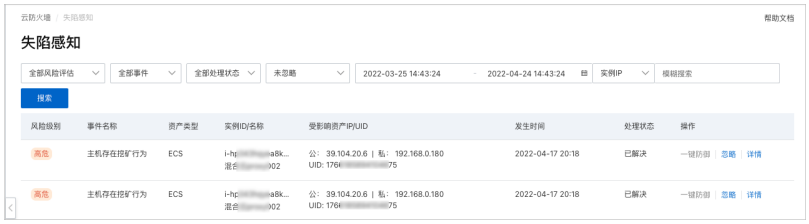
云防火墙失陷感知页面实时为您展示由威胁检测引擎检测到的入侵活动及其详细信息。

前提条件

您需要先开启互联网边界防火墙开关，**失陷感知**页面才会采集到相关入侵事件的信息。如何开启互联网边界防火墙开关，请参见开启防火墙。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**攻击防护 > 失陷感知**。
3. 在**失陷感知**页面，查看入侵事件详细信息。



在**失陷感知**页面，您可以根据需要执行以下操作。

- 查看事件列表

  在入侵事件列表，查看入侵事件的详细信息，包括风险级别、受影响资产IP和UID、处理状态等信息。

- 查找目标事件

  在上方菜单栏，筛选风险级别、时间类型、处理状态、检测时间范围，或输入实例IP、ID、名称或UID进行模糊搜索，然后单击**搜索**，查找目标入侵事件。

- 忽略入侵事件

  如果判断入侵事件为正常活动，可定位到需要忽略的事件，在**操作**列单击**忽略**。

  > **说明** 标记为**忽略**的入侵事件将从入侵事件列表中移除，云防火墙后续不会再对该事件进行告警。

- 查看事件详情

  定位到需要查看详情的事件，在**操作**列单击**详情**，查看入侵事件的详细信息和对应的安全建议。

  > **说明** **一键防御**开关不对单个事件进行控制。开启或关闭**一键防御**将会开启或关闭整个云防火墙的入侵防御功能。

1.4. 防护配置

云防火墙内置了威胁检测引擎，可对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截，并提供精准的威胁检测虚拟补丁，智能阻断入侵风险。

背景信息

您可以通过防护配置功能设置威胁引擎的运行模式，并根据业务需要对威胁情报、基础防御、智能防御和虚拟补丁进行自定义配置，更精准地识别和阻断入侵风险。

> **注意** 您需要先开启互联网边界防火墙开关，才能使入侵防御策略生效。相关内容，请参见互联网边界防火墙。

限制说明

云防火墙高级版、企业版和旗舰版支持防护配置功能，免费版不支持。

云防火墙高级版不支持自定义虚拟补丁和基础防御配置，云防火墙企业版和旗舰版无此限制。

威胁引擎运行模式

威胁引擎可选择以下两种模式：

- **观察模式**：开启观察模式后，可对恶意流量进行监控并告警。
- **拦截模式**：开启拦截模式后，可对恶意流量进行拦截，阻断入侵活动。您可以针对您的防护需求，选择不同严格程度的拦截模式：
  - 拦截模式-宽松：防护粒度较粗，主要覆盖低误报规则，适合业务对误报要求高的场景。
  - 拦截模式-中等：防护粒度较宽松，介于宽松和严格之间，精准度较高，适合日常运维的常规防护场景。
  - 拦截模式-严格：防护粒度精细，覆盖全量规则，相比中等规则组可能误报更高，适合对安全防护漏报要求高（例如：重保、护网）的场景。

以下NOTE被流量拓扑可视化复用。更新NOTE同时需要更新复用目标文档。

> **注意** 云防火墙服务开通后，威胁引擎默认启用**拦截模式**。具体开启哪种程度的拦截模式，云防火墙会根据您流量的实际情况进行判断和默认选择。只有开启**拦截模式**后，威胁情报、基础防御和虚拟补丁模块才会开启相应的威胁拦截。如未开启**拦截模式**，入侵防御模块将只会对各类威胁和恶意流量进行监控。

高级设置

高级设置模块支持您对入侵防御白名单、威胁情报、智能防御、基础防御和虚拟补丁进行自定义设置，为您提供更精准的入侵防御体系。

您可以在**高级设置**页面进行以下操作：

- 设置防护白名单

  在**高级设置**模块中单击**防护白名单**，将您确定为可信的IP添加到白名单中。设置防护白名单后，云防火墙攻击防护模块不会对防护白名单中的IP进行拦截，防护白名单中IP的流量默认被放行。

  > **注意** 自定义目的IP白名单或源IP白名单最多添加50个IP地址。

  您可将内外双向流量的可信源源IP地址、目的IP地址或地址簿配置到防护白名单中。

- 设置威胁情报

  威胁情报可将阿里云全网检测到的恶意IP同步到云防火墙，如：恶意访问源、扫描源、暴力破解的源IP等，并对其进行精准拦截。开启后可提前感知全网威胁源。

  打开**威胁情报**开关后，云防火墙可扫描侦查威胁情报，并提供中控情报阻断。建议您开启威胁情报。

- 设置基础防御

  基础防御可提供基础的入侵防御能力，包括暴力破解拦截、命令执行漏洞拦截、对被感染后连接C&C（命令控制）的行为进行管控。开启后可为您的资产提供基础的防护能力。建议您开启基础防御。

  打开**基础规则**开关后，云防火墙默认为您开启部分常见威胁相关的检测规则。如果默认规则无法满足您的需求，您可以在**基础防御**模块单击右侧的**自定义选择**，打开**基础防御-自定义选择**对话框，对单个或多个基础防御规则进行自定义设置。自定义设置仅支持修改该基础防御规则的放行状态，即观察、拦截、关闭。

  > **说明** 仅云防火墙企业版和旗舰版支持自定义设置基础防御规则。

- 设置智能防御

  智能防御可基于云上海量攻击数据、方式进行学习，对攻击行为进行智能识别和实时告警。

  打开**智能防御**开关后，云防火墙可以学习云上海量攻击数据，提高威胁和攻击的识别准确率。建议您开启智能防御。

  > **说明** 目前智能防御仅支持观察模式。

- 设置虚拟补丁

  针对可被远程利用的高危漏洞和应急漏洞，在网络层提供热补丁，实时拦截漏洞攻击行为，避免修复主机漏洞时对业务产生的中断影响。虚拟补丁无需在您的服务器上进行安装。开启后，云防火墙可为您实时防护热门的高危漏洞和应急漏洞。虚拟补丁关闭后将无法实时自动更新。建议开启所有的虚拟补丁。

> **说明** 仅云防火墙企业版和旗舰版支持自定义设置虚拟补丁规则。

在**虚拟补丁**设置中单击右侧的**自定义选择**，打开**虚拟补丁-自定义选择**对话框，可对单个或部分基础虚拟补丁规则进行自定义设置。

> **说明** **虚拟补丁-自定义选择**对话框中，部分规则会展示**重点关注**的标签，代表全网中检测到攻击非常频繁的威胁，需要您重点关注并及时排查。

2.访问控制

2.1. 访问控制策略总览

您可在云防火墙中配置访问控制策略，限制主机对内、外双向的访问控制，有效降低您资产被入侵的风险。

访问控制策略包含的元素

访问控制策略中支持对以下元素进行限制，实现对相关流量进行访问控制（放行、拒绝或观察）。

- IP地址段：针对来自某个IP地址段或去向某个IP地址段（单个地址段）的流量进行访问控制。
- IP地址簿：针对来自某些IP地址段或去向某些IP地址段（多个地址段）的流量进访问控制。
- 区域：针对来自某些地理区域或去向某些地理区域的流量进行访问控制。
- 网站域名：针对访问流量来源的域名地址进行访问控制。
- 协议类型：针对访问流量的协议类型进行访问控制。
- 端口：针对访问流量经过的端口进行访问控制。
- 应用类型：针对访问流量的应用类型进行访问控制。

不同版本可配置的访问控制策略数量限制说明

云防火墙不同版本可配置不同数量的访问控制策略。详细内容，请参见云防火墙功能与计费表。

主机边界防火墙（ECS实例间）策略数量限制说明

默认情况下，您最多可创建100个主机边界防火墙策略组和100条策略（也就是在ECS安全组创建并同步到云防火墙的策略数量，与在云防火墙主机边界防火墙侧创建的策略数加起来不超过100条）。

> **说明** 如果当前策略数量上限无法满足您的需求，建议您及时清理无需使用的策略或提交工单，申请阿里云技术支持。

访问控制策略相关操作参考文档

- 互联网边界（内外双向流量）
- 主机边界防火墙（ECS实例间）
- 修改云防火墙访问控制策略的优先级

2.2. 互联网边界（内外双向流量）

互联网边界防火墙支持对Web资产的出、入流量进行访问控制。您可在云防火墙中配置访问控制策略，限制Web资产和互联网之间的未授权访问。

前提条件

配置互联网边界防火墙策略前，请确认**互联网边界防火墙**开关已开启，否则策略将不生效。详细内容，请参见互联网边界防火墙。

背景信息

互联网边界防火墙支持对**内对外**（内网访问外部互联网）和**外对内**（外部互联网访问您的内部网络）流量进行访问控制，并提供策略导出功能。

互联网边界防火墙支持IPv4访问控制策略（表示策略中的访问源IP、目的IP使用IPv4格式）和IPv6访问控制策略，云防火墙各版本对该功能支持的情况不同。详细内容，请参见功能特性。

使用限制

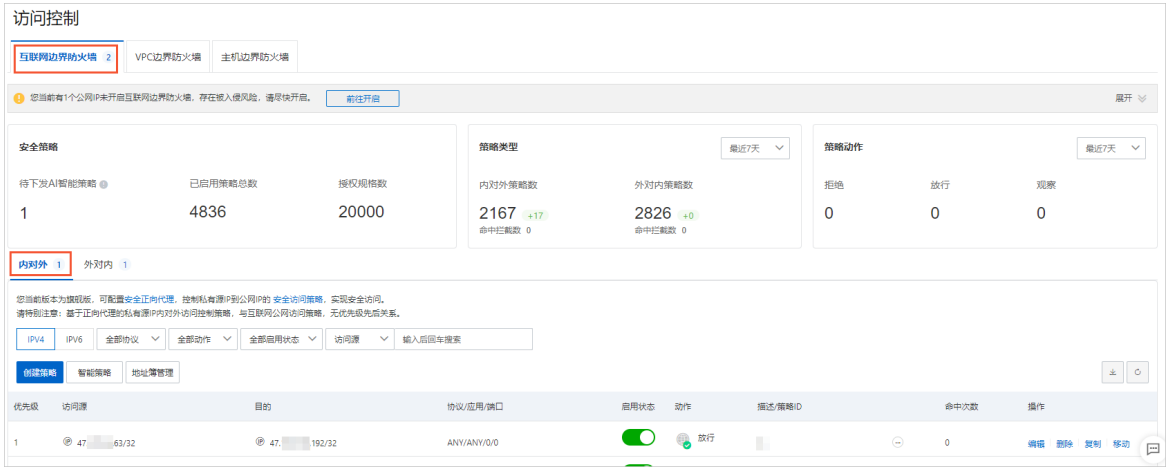
互联网边界防火墙访问控制策略数量存在以下限制：

- 高级版：不超过4,000条。
- 企业版：不超过10,000条。
- 旗舰版：不超过20,000条（可提交工单申请扩展）。
- 内对外**目的类型**为**域名**，且**应用**不为**HTTP**、**HTTPS**、**SMTP**、**SMTPS**、**SSL**的策略：不超过200条。

> **注意** 策略数计算公式为：**访问源**地址段个数*__目的__地址段个数或区域个数*__端口__个数。例如：某个策略中__源类型__、__目的类型__、__端口类型__分别选择了IP、IP、__端口__，表示该策略的__访问源__、__目的__和__端口__都是单个，则计算为1条策略；如果__源类型__、__目的类型__、__端口类型__选择了地址簿且地址簿中的IP或者端口存在多个时，该策略计算为多条策略。

内对外流量访问控制

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**访问控制**页面，单击**互联网边界防火墙**页签，然后在页面下方，单击**内对外**页签。
4. 在**内对外**页签，单击**创建策略**。



5. 在**创建内-外策略**对话框中，按照以下步骤新增访问控制策略。
   i. 创建第一条内对外策略，先对可信的源IP进行**放行**。
      a. 请参照下表，完成参数配置。

参数名称	参数配置说明
源类型	选择访问源的类型。可选项： ■ **IP**：仅支持单个IP地址段。 ■ **地址簿**：您预先配置的IP地址簿，是多个IP地址段的组合，便于您在配置策略时对多个IP地址进行管控。

参数名称	参数配置说明
访问源	设置访问流量的来源地址： ■ 选择**IP**作为源类型时，该访问源一定要设置成网段。每条策略只支持配置一个网段。 ■ 选择**地址簿**作为源类型时，您可单击指定地址簿右侧的**选择**按钮，选择该IP地址簿作为**访问源**。 **说明** 每次只能选择1个地址簿，如果需要使用多个地址簿，您可以通过**新增策略**来添加。
目的类型	访问流量的目的地址类型。可选择**IP**、**地址簿**、**域名**或**区域**。 **说明** 目的**区域**已支持中国全部地域，以及全部国际区域。
目的	设置接收流量的目的地址。 ■ **目的类型**选择**IP**时，该目的地址一定要设置成网段。每条策略只支持配置一个网段。 ■ **目的类型**选择**地址簿**时，您可单击指定地址簿右侧的**选择**按钮，选择该地址簿作为**目的**。 **说明** 每次只能选择1个地址簿，如果需要使用多个地址簿，您可以通过**新增策略**来添加。 ■ **目的类型**选择**域名**时，云防火墙将自动为您解析该域名地址，并对该解析到的地址进行访问控制。详细介绍，请参见DNS域名解析地址访问控制策略。 ■ **目的类型**选择**区域**时，请您选择流量的目的地址所在的区域。可选中国区域或国际区域。
协议类型	设置该内到外访问流量的协议类型。当前支持配置的协议类型有：**TCP**、**UDP**、**ICMP**、**ANY**。不确定具体协议类型时可选择**ANY**。
端口类型	您可以选择以下端口地址类型： ■ **端口**：只支持设置单个端口范围。 ■ **地址簿**：是指您预先配置的**端口地址簿**，是多个端口的组合，便于您在策略配置时对多个端口进行限制。
端口	设置需要放开或限制的端口。可根据**端口类型**的配置项，手动输入单个端口范围，或者单击**选择**，从地址簿中选择预先配置的**端口地址簿**。 **说明** 每次只能选择1个地址簿，如果需要使用多个地址簿，您可以通过**新增策略**来添加。

参数名称	参数配置说明
应用	设置该内到外访问流量的应用类型。 支持多种应用类型，具体应用类型请参见云防火墙控制台的**互联网边界防火墙**页面。 **协议类型**选择TCP时，您可以选择任意应用类型；如选择其他类型协议，应用类型只能设置为**ANY**。 **目的**使用域名地址簿或泛域名时，您只能选择HTTP、HTTPS、SMTP、SMTPS或SSL。 **说明** 识别应用依赖应用报文特征（协议识别不依据端口），应用识别失败时，该会话流量会被放行。如果您想拦截未知应用类型的流量，建议您开启互联网边界防火墙严格模式。更多信息，请参见互联网边界防火墙-严格模式。
动作	设置允许或拒绝该流量通过互联网边界防火墙。本示例中选择**放行**。 ■ **放行**：允许访问。 ■ **拒绝**：禁止访问，并且不会提供任何形式的通知信息。 ■ **观察**：设置为观察模式后仍允许源到目的的访问。观察一段时间后，您可根据需要调整为**放行**或**拒绝**。
描述	输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。
优先级	选择该策略的优先级，默认为**最后**，表示优先级最低。 ■ **最后**：指访问控制策略生效的优先级最低，最后生效。 ■ **最前**：指访问控制策略生效的优先级最高，最先生效。

b. 单击**确认**，完成访问控制策略的创建。

注意 最新创建的策略会展示在访问控制策略列表最后一页的最后一行中。

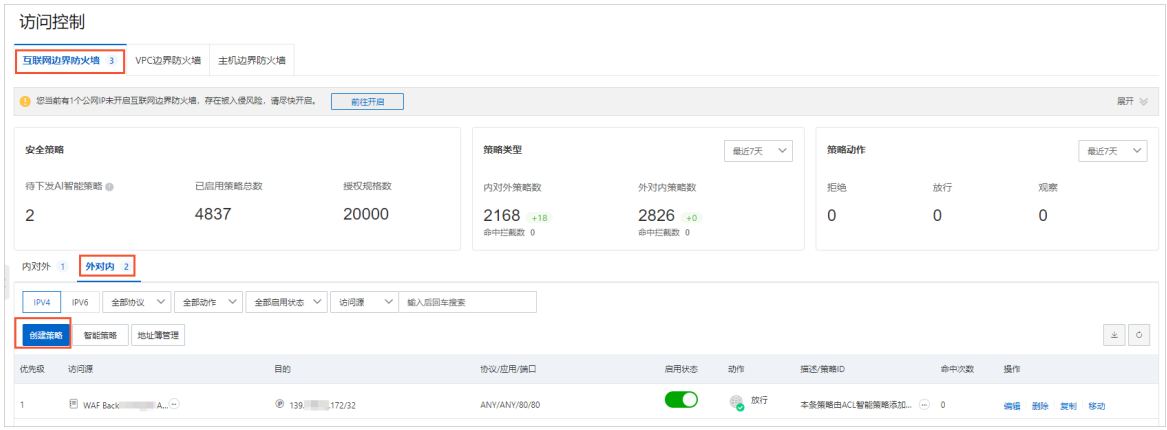
ii. 创建第二条**内对外**访问控制策略，拒绝所有访问源访问外部互联网。

将**访问源**地址设置为0.0.0.0/0，**动作**设置为**拒绝**，禁止所有未授权的访问。其他访问控制参数配置可参见上一步。

iii. 确定第一条可信源**放行**策略的优先级高于第二条**拒绝**策略的优先级。

外对内流量访问控制

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**访问控制**页面，单击**互联网边界防火墙**页签，然后在页面下方，单击**外对内**页签。
4. 在**外对内**页签，单击**创建策略**。



5. 在**创建外-内策略**对话框中，创建第一条**外对内**访问控制策略，先对可信的外部源IP进行**放行**。

   访问源设置为可信的IP地址段或选择预先配置的可信IP**地址簿**，**动作**设置为**放行**。其他访问控制参数配置，请参见内对外流量访问控制中的配置。

   > **说明** 外对内流量的访问控制策略中，如果**源类型**或**目的类型**选择了**地址簿**，那么**访问源**和**目的**可选择IPv4地址簿或云地址簿类型。

6. 创建第二条**外对内**访问控制策略，拒绝所有访问源访问内部网络。

   将**访问源**地址设置为0.0.0.0/0，**动作**设置为**拒绝**，禁止所有未授权的访问。

7. 确定第一条可信源**放行**策略的优先级高于第二条所有访问源**拒绝**策略的优先级。

互联网边界防火墙外对内访问控制策略配置视频教程

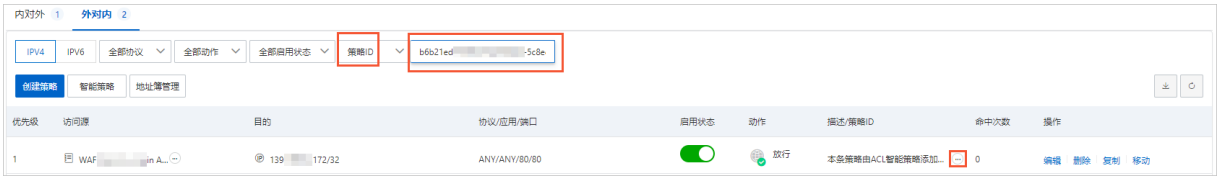
导出策略

互联网边界防火墙支持策略导出，您可以根据需要导出外对内策略或内对外策略。

根据策略ID搜索具体策略

互联网边界防火墙访问控制策略提供策略ID，您可以使用策略ID快速定位到具体的访问控制策略，及时了解策略状态和对策略进行调整。

您可以在互联网边界防火墙列表中，将鼠标移至**描述/策略ID**列的 ··· 图标上，查看该策略的ID。



查看是否有访问流量命中控制策略

访问控制策略配置完成后，默认情况下策略立即生效。但如果策略参数配置不正确，或者互联网边界防火墙未打开，可能会导致您的策略配置不生效。

您可以在访问控制策略列表中定位到该新增的策略，如果**命中次数**栏有显示对应的命中次数，表示已有访问流量命中该策略。**命中次数**是创建策略后，访问流量命中该策略的累计次数。

您还可以单击命中次数，跳转到**流量日志**页面。**流量日志**页面**规则名**一栏会显示出该流量命中的访问控制策略的名称。

> **说明** 流量日志仅展示最近7天内的流量信息。如果访问控制策略有命中次数，但命中策略是发生在7天前，流量日志列表中的数据将会为空。

相关操作

创建策略后，您可以在访问控制策略列表中，对该策略进行修改、删除、复制或移动（移动即修改策略的优先级）。

> **警告** 删除策略后，该策略管控的流量将不受云防火墙的访问控制。请谨慎删除。

2.3. 主机边界防火墙（ECS实例间）

主机边界防火墙可以对ECS实例间的入流量和出流量进行访问控制，限制ECS实例间的未授权访问。主机边界防火墙的访问控制策略发布后，会自动同步到ECS安全组并生效。

背景信息

相比于为ECS实例创建安全组规则，通过主机边界防火墙定义访问控制策略具有以下优势：

- 支持策略的批量发布。
- 策略支持观察模式。
- 同应用组配合，自动创建安全组。
- 在云防火墙控制台可实现策略的统一管控，并且无需切换ECS实例所在的地域。

默认情况下，您最多可以创建100个策略组和100条策略，即在ECS安全组创建并同步到云防火墙的策略数量和在云防火墙主机边界防火墙创建的策略数量加起来不超过100条。如果当前策略数量上限无法满足您的需求，建议您及时清理无需使用的策略，或者通过配置VPC边界访问控制策略，减少配置不必要的主机防火墙策略。

配置主机边界防火墙访问控制策略时，您必须先创建策略组（策略组中包含默认策略），然后在该策略组中配置精细的入方向或出方向访问控制策略。完成策略组和策略配置后，必须发布策略组，才能将策略组策略同步到ECS安全组并生效。完整的使用流程如下：

1. 新建策略组。
2. 配置策略。
3. 发布策略。

版本支持说明

仅企业版和旗舰版云防火墙支持主机边界防火墙功能。

策略组类型

策略组分为普通策略组和企业策略组。两种策略组的应用场景介绍如下：

- 普通策略组对应于ECS的普通安全组，是一种虚拟防火墙，具备状态检测和数据包过滤功能，用于在云端划分安全域。您可以通过配置策略组策略，允许或拒绝策略组内的ECS实例的入流量、出流量。
- 企业策略组对应于ECS的企业安全组，是一种全新的策略组类型，相比原有的普通策略组，大幅提升了组内容纳实例数量，不再限制组内私网IP数量，规则配置方式更加简洁便于维护，适用于对整体规模和运维效率有较高需求的企业级用户。

下表列举了两种策略组的差异：

功能	普通策略组	企业策略组
支持专有网络VPC	是	是
支持设置规则优先级	是	否
支持授权给其他策略组	是	否
支持手动设置允许访问的策略	是	是
支持手动设置拒绝访问的策略	是	否，企业策略组默认拒绝任何访问请求。
能容纳的私网IP地址数量	2000	65536
默认支持同一个策略组内ECS实例互通	否，需要在该策略组中创建**允许**的策略。	否，需要在该策略组中创建**允许**的策略。

新建策略组

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**访问控制**页面的**主机边界防火墙**页签，单击右上角的**新增策略组**。
4. 在**新建策略组**对话框中，配置策略组参数。

参数	描述
策略组类型	选择策略组的类型： ○ **普通策略组**：适用于对网络精细化控制要求较高、网络连接数适中的用户场景。 ○ **企业策略组**：适用于对运维效率有更高需求的用户场景。
策略组名称	按页面提示要求设置策略组的名称。 建议使用方便识别的名称，便于识别和管理。
所属VPC	在**所属VPC**下拉列表中，选择应用该策略组的专有网络VPC。 **说明** 每个策略组只能配置一个VPC。
实例ID	从**实例ID**下拉列表中，选择应用该策略组的一个或多个ECS实例。 **说明** 实例ID列表只包含**所属VPC**下的ECS实例。
描述	简短地描述策略组，方便后续对安全组进行管理。

参数	描述
模板	从**模板**下拉列表中，选择要应用的模板类型： ○ **default-accept-login**：默认放行TCP 22、TCP 3389协议入方向访问和所有出方向访问。 ○ **default-accept-all**：默认放行所有入方向和出方向访问。 ○ **default-drop-all**：默认拒绝所有入方向和出方向访问。 说明 企业策略组不支持**default-drop-all**选项。

5. 单击**确认**。
   策略组创建完成后，您可以在主机边界防火墙的策略组列表中查看新建的策略组，并根据需要对策略组执行以下操作：
   - **配置策略**：设置定制化的策略，实现更精细化的访问控制。
   - **发布**：将策略组的访问控制策略同步到ECS实例的安全组。
   - **编辑**：修改当前策略组包含的ECS实例和策略组的描述。
   - **删除**：删除策略组。

     警告 删除策略组后，策略组中的主机访问控制策略会失效，请谨慎操作。删除策略组后，策略记录仍会保留在策略组列表中，但您无法再对其执行任何操作。

     如果您希望清理不再需要的策略组，则可以将策略组来源设置为**自定义**，筛选出所有在云防火墙控制台手动创建的策略组，再去判断策略组是否需要保留。

配置策略

创建策略组之后，您还需要在该策略组中添加具体的访问控制策略。

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**访问控制**页面的**主机边界防火墙**页签，定位到要设置的策略组，单击**操作**列下的**配置策略**。
4. 在**策略配置**页面，单击右上角的**创建策略**。
5. 在**创建策略**对话框中，配置策略参数。

参数	描述
网卡类型	默认为**内网**且不可以修改，表示内网间的访问控制。
策略方向	选择策略方向： ○ **入方向**：指内网中的其他ECS实例访问策略组ECS实例。 ○ **出方向**：指策略组ECS实例访问内网中的其他ECS实例。
策略类型	选择策略类型： ○ **允许**：放行相应的访问流量。 ○ **拒绝**：直接丢弃数据包，不会返回任何回应信息。如果两条策略其他配置都相同，只有策略类型不同，则**拒绝**策略生效，**允许**策略不生效。 **说明** 企业策略组不支持**拒绝**选项。

参数	描述
协议类型	从**协议类型**列表选择访问流量的协议类型： ○ **TCP** ○ **UDP** ○ **ICMP** ○ **ANY**：表示任何协议类型。不确定访问流量的类型时可选择ANY。
端口范围	输入访问流量使用的端口地址范围。例如：22/22。
优先级	策略生效的优先级。使用整数表示，取值范围：1~100。优先级数值越小，优先级越高。 优先级数值可重复。策略优先级相同时，**拒绝**类型的策略优先生效。
源类型和**源对象**	选择访问流量的来源 。策略方向选择**入方向**时需要设置。您可以选择访问源地址的类型，并根据源类型设置源对象。 可选的源类型： ○ **地址段访问** 选择该类型后，需要在**源对象**中手动输入访问源地址段。仅支持设置单个地址段。 ○ **策略组** 选择该类型后，需要从**源对象**模块的策略组列表中，选择一个策略组作为源对象，表示对来自该策略组中所有ECS实例的流量进行管控。 **说明** 企业策略组不支持**策略组**选项。
目的选择	选择访问流量的目的地址。策略方向选择**入方向**时需要设置。可选择的目的地址类型： ○ **全部ECS**：表示当前策略组中的所有ECS实例。 ○ **地址段访问**：选择该类型后，需要输入目的IP或CIDR地址段，表示当前策略组中该地址段对应的ECS实例。
源选择	选择访问源的类型。策略方向选择**出方向**时需要设置。访问源包含以下类型： ○ **全部ECS**：表示当前策略组中的所有ECS实例。 ○ **地址段访问**：选择该类型后，需要输入目的IP或CIDR地址段，表示当前策略组中该地址段对应的ECS实例。

参数	描述
目的类型和目的对象	选择目的地址的类型并根据选择的目的类型设置目的对象。策略方向选择**出方向**时需要设置。 可选的目的类型如下： ○ **地址段访问** 选择该类型后，需要手动输入访问目的地址段。仅支持设置单个地址段。 ○ **策略组** 选择该类型后，从策略组列表中选择一个策略组，表示对本机访问该策略组中所有ECS实例的流量进行管控。 **说明** 企业策略组不支持**策略组**选项。
描述	简短地描述策略，方便后期管理。

6. 单击**提交**。
   策略组创建完成后，您可以在策略列表中查看新建的策略，并根据需要**编辑**或**删除**已创建的策略。

警告 删除策略后，策略中对应流量的访问控制将失效，请谨慎删除。删除策略后，策略记录仍会保留在策略列表中，但您无法再对其执行任何操作。

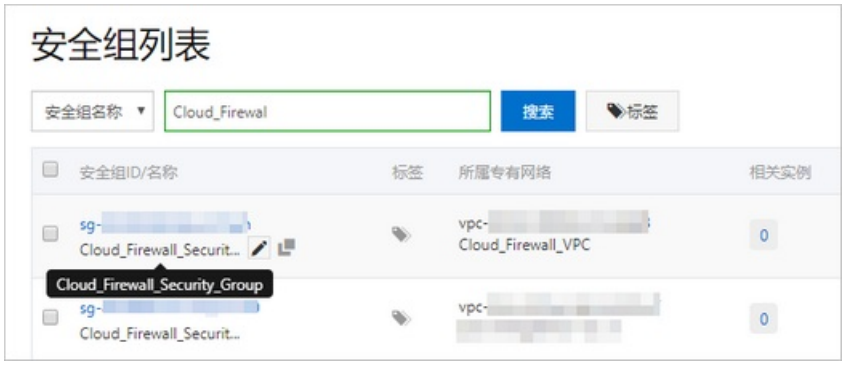
发布策略

创建策略后，您还需要发布该策略，策略才会生效，并开始对相应的内网流量进行访问控制。

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**访问控制**页面的**主机边界防火墙**页签，定位到需要发布的策略组，单击其**操作**列下的**发布**。

4. 在**策略发布**对话框，设置**变更备注**，确认**变更策略**（即策略的变更内容），并单击**确定**。

策略发布后才会同步到ECS安全组并生效。您可以在ECS控制台的**安全组 > 安全组列表**页面，查看云防火墙同步到安全组中的访问控制策略。云防火墙中创建的策略组策略名称默认为**Cloud_Firewall_Security_Group**。



主机边界防火墙配置视频教程

相关文档

- 为什么会有三种云防火墙?
- 普通策略组和企业策略组有什么区别?
- 主机边界防火墙策略组配置示例

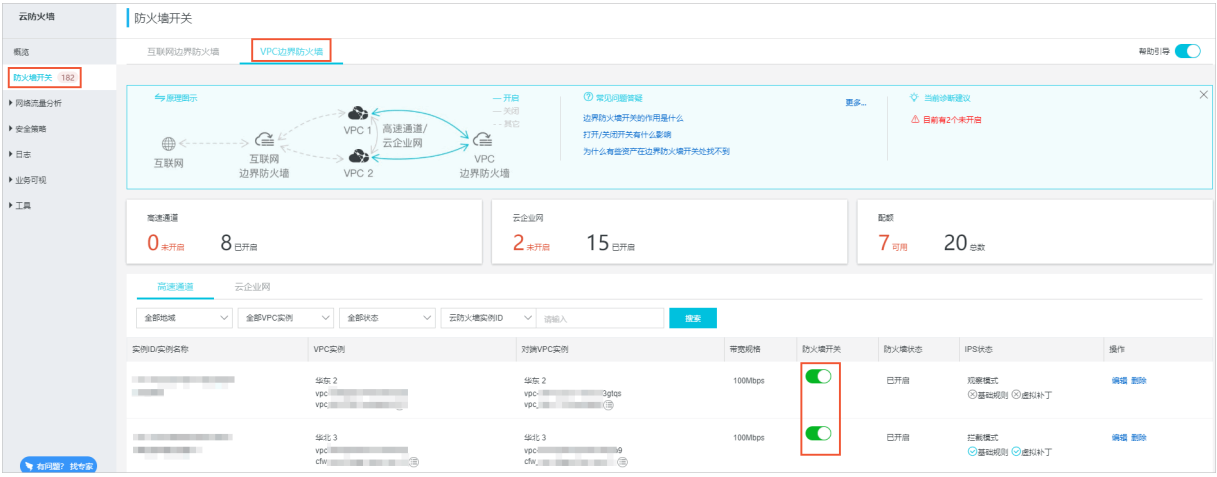
2.4. VPC边界防火墙

VPC边界防火墙可用于检测和控制两个VPC间的通信流量。您可在云防火墙中配置访问控制策略，限制两个VPC之间的未授权访问。

前提条件

VPC边界防火墙默认不存在。因此在创建VPC访问控制策略前，您需要先创建并开启相应的VPC边界防火墙。

VPC边界防火墙开关开启后，访问控制策略才能生效。



使用限制

云防火墙企业版和旗舰版支持VPC边界防火墙功能，高级版不支持。不同版本云防火墙实例支持配置的VPC边界防火墙访问控制策略数量有以下限制：

- 企业版：最多10,000条。
- 旗舰版：最多20,000条（可提交工单申请扩展）。

访问控制策略配置原理

VPC边界防火墙默认放行所有流量，在对两个VPC之间的流量进行管控时，您需要拒绝可疑流量或恶意流量；或者先放行可信流量，再拒绝其他任意地址的访问。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**
3. 在**访问控制**页面的**VPC边界防火墙**页签，单击**创建策略**。

4. 在**新增VPC边界防火墙策略**对话框中，配置访问控制策略。

访问控制策略配置项详细说明，请参见以下配置项说明表：

规则参数	参数选项说明
源类型	访问源地址的类型。可选值： ○ **IP地址**：**访问源**地址类型为IP地址，需手动输入IP地址段。 ○ **地址簿**：**访问源**地址类型为地址簿，需从预先设置的地址簿列表中选择一个地址簿。 **说明** 您可以将多个IP设置成一个地址簿，方便您在配置访问控制规则时简化规则。

规则参数	参数选项说明
访问源	发送流量的IP或CIDR地址。 **说明** 访问源只支持配置一个网段。 如果**源类型**选择的是**地址簿**，需要从地址簿列表中选择一个地址簿作为访问源。 **说明** 您1次只能选择1个地址簿，如果需要使用多个地址簿，您可以通过**新增策略**来添加。
目的类型	您可以选择以下目的地址类型： ○ **IP地址**：目的地址设置为IP地址。 ○ **地址簿**：目的地址设置为地址簿。 ○ **域名**：目的地址设置为域名。支持设置为泛域名，例如：*.aliyun.com。
目的	设置接收流量的目的地址。 ○ 选择IP作为目的类型时，该目的地址一定要设置成网段。 ○ 选择**地址簿**作为目的类型时，您可单击指定地址簿操作栏的**选择**按钮，选择该IP地址簿作为**目的**。 **说明** 您1次只能选择1个地址簿，如果需要使用多个地址簿，您可以通过**新增策略**来添加。 ○ 选择**域名**作为目的类型时，可以配置为域名或泛域名，例如：*.aliyun.com。
协议类型	您可选择以下协议： ○ **ANY**（任何协议） ○ **TCP**协议 ○ **UDP**协议 ○ **ICMP**协议
端口类型	您可以选择以下端口类型： ○ **端口**：只支持设置单个端口。 ○ **地址簿**：是指您预先配置的**端口地址簿**，是多个端口的组合，便于您在策略配置时对多个端口进行限制。

规则参数	参数选项说明
端口	设置需要放开或限制的端口。可根据**端口类型**的配置项，手动输入单个端口，或者单击**选择**，从地址簿中选择预先配置的**端口地址簿**。 **说明** ○ 您1次只能选择1个地址簿，如果需要使用多个地址簿，您可以通过**新增策略**来添加。 ○ 协议选择为ICMP，目的端口配置不生效。协议选择为**ANY**，对于ICMP流量做访问控制，目的端口配置不生效。
应用	当前支持配置的应用：ANY、HTTP、HTTPS、Memcache、MongoDB、MQTT、MySQL、RDP、Redis、SMTP、SMTPS、SSH和VNC。 **协议**选择**TCP**时，支持配置不同的应用类型；如选择其他类型协议，应用类型只能设置为**ANY**。 **说明** 识别应用依赖应用报文的特征（协议识别不依据端口）；应用识别失败时，该会话流量会被放行。
动作	允许或拒绝该流量通过VPC边界防火墙。 支持选择以下动作： ○ **放行**：允许访问。 ○ **拒绝**：禁止访问，并且不会提供任何形式的通知信息。 ○ **观察**：设置为观察模式后仍允许源到目的的访问。观察一段时间后可根据需要调整为*放行*或*拒绝*。
描述	对访问控制策略进行描述或备注。输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。
优先级	设置访问控制策略的优先级。默认优先级为**最后**。支持选择以下优先级： ○ **最后**：指访问控制策略生效的顺序最低，最后生效。 ○ **最前**：指访问控制策略生效的顺序最高，最先生效。

您可根据实际业务的需要，选择合适的VPC边界防火墙策略动作：

- **拒绝**：表示阻断可疑或恶意流量，拒绝其访问。
- **放行**：表示放行可信流量，允许其访问。选择放行策略动作时，您可以先创建可信流量的**放行**策略，再创建一条**拒绝**其他所有访问的策略。策略配置完成后，确认**放行**策略的优先级高于**拒绝**策略的优先级。有关优先级的详细内容，请参见修改云防火墙访问控制策略的优先级。

说明 VPC边界防火墙默认对所有地址放行。

2.5. DNS域名解析地址访问控制策略

云防火墙针对内网访问互联网（内对外）的场景下，支持访问控制策略中选择域名作为目的地址。云防火墙可以对域名进行DNS解析，提供可视化解析地址供您查看，并对该解析到的地址进行访问控制。本文档介绍了如何使用DNS域名解析地址配置内到外访问控制策略。

背景信息

云防火墙针对**内对外**访问控制策略进行了升级，通过采用动态DNS解析实现了域名访问控制策略功能的增强。您可实时查看目的域名解析地址，并在解析地址变更时手动更新该地址。

对于DNS域名解析地址的内对外访问控制规则（访问流量协议为TCP 、应用类型为HTTP/HTTPS/SSL/SMTP/SMTPS的数据除外），DNS解析域名地址后，该域名将被转化成IP地址。该内对外规则创建完成后，云防火墙将对域名解析出的IP地址进行防护，一个域名最多解析500个IP。

> **说明**
>
> - 流量的应用类型为HTTP、SMTP时，云防火墙优先通过host字段来实现域名的访问控制。
> - 流量的应用类型为HTTPS、SMTPS、SSL时，云防火墙优先通过SNI字段来实现域名的访问控制。
> - 除了应用类型为HTTP/HTTPS/SSL/SMTP/SMTPS以外的数据，才支持动态DNS解析的方式实现流量的访问控制（即才能查看到解析后的域名IP地址）。

限制条件

以下情况不支持DNS域名解析地址的访问控制策略：

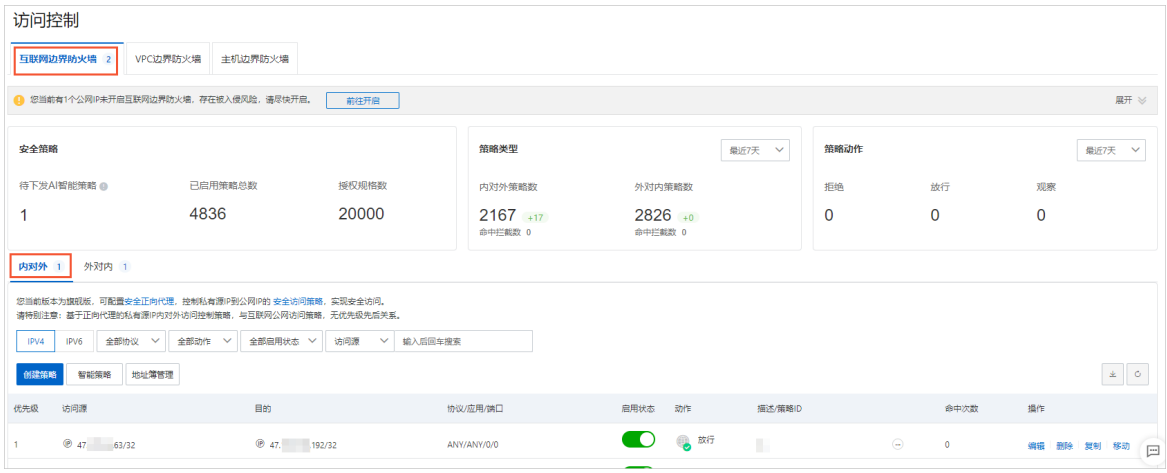
- 外对内流量。

  目前，仅内对外流量的访问控制策略支持DNS域名解析。
- 目的地址域名为**通配符域名**（例如：*.example.com）。
- 目的地址类型为**域名地址簿**。
- 金融云和政务云用户。

> **注意** 配置DNS域名解析访问控制策略时，需要关注以下问题：
>
> - 从ECS访问外部域名地址时，只支持ECS默认配置的DNS解析服务器（即ADNS），不支持用户指定特殊的DNS。也就是说，如果您修改了ECS的DNS服务器地址，则该域名解析访问控制规则将无法生效。
> - 多个域名解析到同一个IP地址，访问控制策略会受影响。
>
>   例如：配置一条放行*example1.aliyun.com*的FTP协议流量。假设*example1.aliyun.com*域名解析A记录为*1.*.*.1*，那么实际下发到引擎的规则为*1.*.*.1*的FTP协议允许。此时，如果域名*example2.aliyun.com*的A记录也解析为*1.*.*.1*，那么访问*example2.aliyun.com*的FTP协议也会被放行。
> - 域名的解析地址有变化时，云防火墙会使用最新的解析地址并自动更新对应的访问控制策略。
>
>   如果域名*example1.aliyun.com*的解析结果由*1.*.*.1*变化为*2.*.*.2*，云防火墙自动更新访问控制策略（即云防火墙会自动应用最新解析的IP地址，确保要拦截或放行的域名指向的实时IP地址都能包含在该访问控制策略内）。策略自动更新的周期为30分钟，也就是说，对于已配置的DNS策略，当解析地址变化时，该策略将于30分钟后生效。
>
>   如果您想根据实时变化的解析地址更新您的访问控制策略，可在该策略的编辑页面中单击**域名解析**，手动触发域名解析来获取最新的解析地址，并单击**确定**保存策略的更新。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**内对外**页签，单击**创建策略**。



4. 在**新增内-外策略**对话框中，创建**内对外**访问控制策略。

访问控制策略配置项说明和配置方法请参见下表。

配置项名称	配置项描述	配置方法
源类型	该访问控制策略要过滤的数据包的来源地址类型，包含以下2类： ○ **IP**：仅支持单个IP地址段。 ○ **地址簿**：是您预先配置的IP地址簿，为多个IP地址段的组合，便于您在策略配置时对多个IP地址进行限制，从而简化策略配置。	单击选择*IP*或*地址簿*。 **访问源**地址类型为IP地址，需手动输入IP地址段；**访问源**地址类型选择地址簿时，需从您预先配置的址簿中选择。

配置项名称	配置项描述	配置方法
访问源	该访问控制策略要过滤的数据包的来源地址。	手动输入访问源。 **说明** 访问源只支持配置一个公网IP网段，例如：1.*.*.1/32。
目的类型	该访问控制策略要过滤的数据包的目的地址类型，包含IP地址、地址簿、域名和区域4类。	此处单击选择**域名**。
目的	该访问控制策略要过滤的数据包的目的地址。	手动输入需要该访问控制策略管控的域名地址。 **说明** 非通配符域名才支持动态DNS解析功能，通配符域名无法使用该功能。
域名解析	云防火墙将自动为您解析目的域名地址，并对该解析到的地址进行访问控制。	单击**域名解析**，可查看该域名的实时解析地址。
协议类型	该访问控制策略要过滤的数据包的协议类型。包含以下类型： ○ ANY：任何协议。 ○ TCP协议。 ○ UDP协议。 ○ ICMP协议。	单击下拉框，选择需要访问控制策略管控的协议类型。
端口类型	可选单个端口或端口地址簿。	单击选择端口类型。
端口	允许或阻止该内对外流量数据包通过的端口号。	手动输入端口范围。0/0代表任意端口。
应用	当前支持配置的应用有：ANY、HTTP、HTTPS、Memcache、MongoDB、MQTT、MySQL、RDP、Redis、SMTP、SMTPS、SSH和VNC。 **协议**选择TCP时，支持配置不同的应用类型；如选择其他类型协议，应用类型只能设置为*ANY*。 **说明** 识别应用依赖应用报文特征（协议识别不依据端口）；应用识别失败时，该数据包会被**放行**。	单击下拉框选择需要访问控制策略管控的应用类型。

配置项名称	配置项描述	配置方法
动作	允许或拒绝该流量通过互联网边界防火墙。 ○ **放行**：允许访问。 ○ **拒绝**：禁止访问，并且不会提供任何形式的通知信息。 ○ **观察**：设置为观察模式后仍允许源到目的的访问。观察一段时间后可根据需要调整为**放行**或**拒绝**。	单击下拉框选择动作类型。
描述	对访问控制策略进行描述或备注。输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。	手动输入备注内容。
优先级	设置访问控制策略的优先级。默认优先级为*最后*。 ○ **最后**：指访问控制策略生效的顺序最低，最后生效。 ○ **最前**：指访问控制策略生效的顺序最高，最先生效。	单击选择**最前**或**最后**。

5. 单击**提交**，完成内对外策略的配置。
   策略提交后，您可在**内对外**页面中，查看您配置的策略，对该策略进行编辑、删除、复制或移动（即修改该策略的优先级）等操作。

2.6. 安全组默认放通

云防火墙支持安全组默认放通的功能，帮助您简化ECS安全组访问控制策略的配置。本文档介绍了如何执行安全组默认放通。

背景信息

ECS安全组的访问控制在互联网方向是默认拒绝的。云防火墙通过下发放通规则来将该默认拒绝的属性修改为默认放通，方便您在云防火墙的访问控制中统一管理规则，无需您前往ECS管理控制台的**安全组**页面修改安全组的配置。

防护原理

云防火墙通过给开放公网IP的ECS安全组下发4条优先级最低（优先级为100）的访问控制策略（即ECS安全组规则），实现该ECS的公网IP在互联网方向的默认放通。安全组放通功能无需您手动添加访问控制策略，只需在云防火墙自动新增策略后，确认这4条策略无误，并保存新增策略即可。

> **注意** 安全组放通的功能仅对ECS安全组规则设置为**放行**的流量生效，对于设置为**拒绝**的安全组规则无影响。

限制条件

- 企业安全组不支持安全组放通功能，并且您如果在同一个VPC网络中存在企业安全组，则该VPC所属的安全组也不支持默认放通功能。相关信息，请参见企业安全组。

- 目前，安全组放通只支持ECS Public IP和ECS EIP这两类资产的互联网方向（外到内）流量，公网SLB等不支持开启。
- 为更好地保护您的资产安全，对于未开启云防火墙开关的IP，不建议执行默认放通。对于已放通的IP，不建议关闭云防火墙的防护开关，否则会存在公网IP暴露的风险。

配置安全组放通

参考以下步骤配置安全组放通。

> **警告** 请您重点关注以下情况，以免为您的业务带来严重安全风险。
> - 对于未开启云防火墙开关的IP，不建议执行默认放通。
> - 如果ECS的公网IP不支持开启引流（例如：公网SLB），不建议执行默认放通。
> - 云防火墙服务到期后，如果您不再使用云防火墙服务，建议您前往ECS管理控制台的**网络与安全 > 安全组**页面，删除云防火墙之前自动添加的这4条放通策略。

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**防火墙开关 > 防火墙开关**。
3. 在**互联网边界防火墙**页面，定位到需要放通的安全组，并单击**下发**。

4. 在**安全组默认放通策略**对话框中，确认需要放通的关联安全组，并执行以下步骤。
   - 关联安全组不存在配置冲突的情况下：可直接单击**一键下发**，然后执行步骤5。

   - 关联安全组存在配置冲突的情况下：无法直接单击**一键下发**。

   您可参照以下方法进行处理：

配置冲突的场景	场景描述	操作方法
配置冲突可调整	该ECS实例IP所关联的安全组中，存在优先级大于等于100的规则（和待下发的默认规则优先级冲突）。 云防火墙会通过将原有安全组规则的优先级调高，解决冲突。	云防火墙会自动为您调整安全组优先级，无需您手动调整。您只需在**安全组默认放通策略**页面，单击**一键调整**，确认后云防火墙自动为您调整安全组优先级，**一键下发**按钮将会显示在**IP关联的安全组**列表的**操作**列中。
配置冲突不可调整	该ECS实例IP所关联的安全组中，存在优先级大于等于100的规则（和待下发的默认规则优先级冲突），但是无法通过调整冲突规则的优先级来解决。	配置冲突不可调整的情况下，**一键调整**按钮不可单击。建议您前往ECS管理控制台的**安全组**页面查看和调整冲突的规则优先级，或联系云防火墙钉钉技术支持。

5. 在**安全组默认放通策略 > 一键下发**对话框中，可查看到云防火墙自动为您新增的4条放通策略。确认无误后，单击**确定 > 提交**，默认放通该安全组互联网方向的访问。

   > **说明** 单击**提交**后，该安全组下所有ECS实例的互联网方向流量将会变为默认放开。建议您梳理一下该安全组ECS对外暴露的公网IP，确认这些公网IP都在云防火墙中配置了相应的访问控制策略。

   关联的安全组都执行了**一键下发**后，该目标IP地址所属的安全组放通策略状态将变为**已下发**，策略也将立即生效。单击**查看**可查看关联安全组的详细信息。

   > **注意** 由于安全组放通后，该安全组将默认放开互联网方向的访问流量，需要您关注以下几点：
   >
   > - 安全组放通后，需要确保在云防火墙上开启该IP的防火墙防护开关，并在**互联网边界防火墙**外对内方向中添加对应的访问控制策略。
   > - ECS公网IP所关联的安全组放通后，该安全组下所有ECS实例的互联网方向的访问都会变为默认放通。建议您合理配置安全组的实例，有效控制公网暴露范围和降低您ECS暴露的风险。
   > - 如果您的云防火墙服务过期并自动释放，已放通的安全组将不再受云防火墙的保护。建议您在收到云防火墙过期提醒消息时及时续费，或对已放通的安全组进行互联网方向的访问控制加固。放通安全组时，云防火墙为您自动新增的4条放通策略还会保留在ECS安全组中，并处于生效状态。如果您不再使用云防火墙服务，建议您前往ECS管理控制台的**网络与安全 > 安全组**页面，删除云防火墙之前自动添加的这4条放通策略。

相关操作

查看安全组默认放通策略下发状态

安全组放通配置完成后，您可前往**防火墙开关 > 互联网边界防火墙**页面，查看您ECS实例所在安全组默认放通策略的下发状态，确定策略是否已成功下发，及时排查未成功下发的问题。

下发状态包含以下几类：

- **已下发**：该IP所在的ECS实例关联的所有安全组都成功下发了放通规则（安全组中所有ECS实例在互联网入方向全部都已放通）；如果ECS实例对应多个安全组，需要所有关联的安全组状态都为**已下发**，该安全组放通规则才能生效。

- **未下发**：该IP所在的ECS实例关联的安全组中，有部分安全组存仍未成功下发放通规则（这种情况下，互联网入方向的流量仍然受安全组策略的控制）。关联安全组存在配置冲突或未执行**一键下发**都可能导致安全组放通规则未成功下发。
- **不支持**：该资产类型暂不支持一键下发默认放通安全组规则。目前，除了ECS EIP和ECS Public IP，其他资产类型的IP都不支持该功能，例如：SLB IP、ENI EIP、NAT EIP等不支持默认放通安全组规则。

2.7. 安全组检查

安全组规则设置不当可能会导致严重的安全问题。安全组检查功能为您检查ECS服务器安全组中存在高危风险的规则，并提供修复建议，帮助您更安全、更高效地使用安全组功能。本文介绍了如何在云防火墙控制台使用安全组检查功能。

背景信息

安全组是一种虚拟防火墙，仅适用于阿里云ECS服务器。安全组检查功能支持对普通安全组和企业级安全组进行安全检查。更多信息，请参见安全组概述。

关于安全组检查支持的检查项相关信息，请参见安全组配置检查项列表。

版本支持说明

云防火墙高级版、企业版和旗舰版均支持安全组检查功能。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 安全组检查**
3. （可选）在**安全组检查**页面，单击**获取最新检查结果**。

   安全组检查预计需要1~5分钟，请您耐心等待。

> **说明** 安全组检查根据安全规则的静态分析得出最新检查结果，可能无法覆盖全部的端口风险情况。您可以在互联网访问活动页面查看端口相关的全部检查结果，了解端口的实际暴露情况。

4. 在**检查结果详情**区域，查看检测出的安全组风险详细信息。

您可以查看安全组**风险等级**、**检查项**、**风险安全组/服务器数**和**检查项状态**信息。

> **说明** 您可以根据需要打开或关闭**检查项状态**。关闭表示不检查该项。

5. 修复高危安全组检查项。
   i. 定位到指定的检查项，单击其操作列下的**修复详情**。

      您也可以单击**风险安全组/服务器数**下的数字，跳转至**安全组修复详情**页面。

   ii. 在**安全组修复详情**页面，定位到需要修复的安全组，单击其操作列下的**去安全组修复**。

您也可以单击**风险安全组ID/名称**下的安全组ID链接跳转至ECS管理控制台的**安全组列表**页面，对有风险的安全组规则进行修复。

> **警告** 安全组规则设置不当可能会引起严重的安全事故。**安全组修复详情**页面针对风险安全组提供了**修复建议**，建议您根据**修复建议**尽快修改存在风险的安全组规则。

相关操作

如果您使用的是免费版云防火墙，您可以选择**立即升级**或**去安全组手动修复**。

立即升级和**去安全组手动修复**的详细信息如下：

- **立即升级**：购买云防火墙高级版及以上的版本，使用云防火墙提供的**安全组检查**功能修复安全组高危规则。云防火墙可统一管理安全组和公网IP访问控制策略，及时缩小安全风险暴露面，提高安全管理效率。推荐您使用该方式。
- **去安全组手动修复**：跳转至ECS管理控制台的**安全组**页面，手动修复高危安全组规则。更多信息，请参见修改安全组规则。

安全组配置检查项列表

检查项名称	安全风险	修复建议
Linux远程运维端口暴露	22端口允许任意IP访问，关联的Linux服务器可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器22端口的访问。如果业务需要访问服务器22端口，建议您限制可访问该端口的公网IP，或使用堡垒机进行远程运维。更多信息，请参见什么是堡垒机。
Windows远程运维端口暴露	3389端口允许任意IP访问，关联的Windows服务器可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器3389端口的访问。如果业务需要访问服务器3389端口，建议您限制可访问该端口的公网IP，或使用堡垒机进行远程运维。更多信息，请参见什么是堡垒机。
DB2远程运维端口暴露	50000端口允许任意IP访问，关联的DB2数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器50000端口的访问。
ECS加入的安全组数量过多	ECS实例加入了3个及以上安全组，会增加运维难度，提高错误配置风险。	建议一台ECS实例加入的安全组数量小于等于2个。更多信息，请参见安全组概述。
Elasticsearch远程运维端口暴露	9200、9300端口允许任意IP访问，关联的Elasticsearch可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器9200、9300端口的访问。
Hadoop YARN远程运维端口暴露	8088端口允许任意IP访问，关联的Hadoop YRAN可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器8088端口的访问。
Hadoop远程运维端口暴露	50070、50030端口允许任意IP访问，关联的Hadoop可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器50070、50030端口的访问。
MongoDB远程运维端口暴露	27017端口允许任意IP访问，关联的Mongo DB数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器27017端口的访问。
MySQL远程运维端口暴露	3306端口允许任意IP访问，关联的MySQL数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器3306端口的访问。
Oracle远程运维端口暴露	1521端口允许任意IP访问，关联的Oracle数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器1521端口的访问。
PostgreSQL远程运维端口暴露	5432端口允许任意IP访问，关联的PostgreSQL数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器5432端口的访问。
Redis远程运维端口暴露	6379端口允许任意IP访问，关联的Redis数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器6379端口的访问。
SQL Server远程运维端口暴露	1433端口允许任意IP访问，关联的SQL Sever数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器1433端口的访问。
Spark远程运维端口暴露	6066端口允许任意IP访问，关联的Spark可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器6066端口的访问。

检查项名称	安全风险	修复建议
Splunk远程运维端口暴露	8089、8090端口允许任意IP访问，关联的Splunk可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器8089、8090端口的访问。
访问源过度开放	检查到安全组配置为入方向允许任意IP访问任意端口，关联服务器被入侵风险极大。	建议仅开放业务所需端口，并限制访问源IP范围。

2.8. 智能策略

云防火墙智能策略使用机器学习技术，基于您的IP资产、服务被访问和主动外联的情况，为每个目的IP或域名自动推荐合适的互联网边界防火墙访问控制策略，帮助您缩小资产在互联网中的暴露面，同时阻断内到外的恶意IP和域名，降低业务被入侵风险。

背景信息

云防火墙可以自动学习您近30日的流量情况，并结合发现的流量风险，为您推荐多条智能策略，您需要及时在云防火墙控制台查看详细推荐策略，并根据需要选择是否下发智能推荐策略（使策略生效）。

使用限制

智能策略目前仅支持对**互联网边界防火墙**自动生成智能推荐的访问控制策略。

对于**主机边界防火墙**、**VPC边界防火墙**，目前您只能手动创建对应的访问控制策略。具体操作，请参见主机边界防火墙（ECS实例间）、互联网边界（内外双向流量）。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**互联网边界防火墙**页签，根据要配置的策略类型，单击对应的页签（**内对外**、**外对内**）。
4. 单击**智能策略**，在**智能策略推荐**面板，根据需要选择和下发智能策略。

   智能策略推荐面板罗列了云防火墙为您推荐的入方向或出方向的访问控制策略。您可以单击某个策略后的**查看详情**，查看与该目的IP相关的所有推荐策略和**推荐理由**。如果推荐策略数量过多，您可以使用**推荐类型**和**访问目的**筛选策略。

   > **说明** 对于已开放的公网IP，我们会推荐您在云防火墙上放行已开放且有流量的端口，并拒绝所有到其他端口的访问，从而减小资产对互联网的暴露面。

   对于您认为需要应用的策略，您可以从以下方式中选择一种方式下发智能策略，使该策略生效：

   > **警告** 下发策略操作涉及一定风险，请确保您已完整知悉即将下发的策略内容，再执行下发策略操作。

   - 在智能策略列表中，选中要下发的策略，单击**下发已选中策略**，批量下发策略。
   - 在智能策略列表中，单击某个策略**操作**列下的**下发策略**，下发该策略。

执行结果

成功下发智能策略后，已下发的智能策略自动生效。

您可以在**访问控制**页面查看已下发生效的互联网边界防火墙策略，并根据需要**编辑**、**删除**策略。更多信息，请参见互联网边界（内外双向流量）。

2.9. 地址簿管理

云防火墙支持将多个IP地址、端口或域名指定成一个地址簿，便于在配置云防火墙访问控制策略时添加多个IP地址、端口或域名的信息。您可根据实际需求，添加受信地址簿或威胁地址簿。本文介绍了地址簿的添加、查看、修改和导出操作。

背景信息

云防火墙的威胁情报功能可将阿里云全网检测到的恶意IP或域名同步到云地址簿，且云防火墙会自动添加您云账号下的DDoS防护实例和WAF实例的回源地址到云地址簿。您在配置云防火墙访问控制策略时，可针对DDoS防护和WAF回源的云地址簿，制定精细化的访问控制策略。

配置访问控制策略时，可灵活引用云防火墙地址簿。支持以下两种方式：

- 放行受信地址簿中的可信任IP和域名。
- 快速封禁地址簿中的恶意IP和域名。

> **说明**
> - 多个地址簿可以包含同一个IP地址或端口。
> - 云防火墙会内置一些全局地址簿，不支持修改和删除内置的全局地址簿。
> - 云防火墙不支持修改和删除云地址簿。
> - 地址簿内IP、域名或端口变动，会自动生效于引用了该地址簿的访问控制策略。

使用限制

地址簿总数量最多为5,000个。不同地址簿支持添加数据的数量如下：

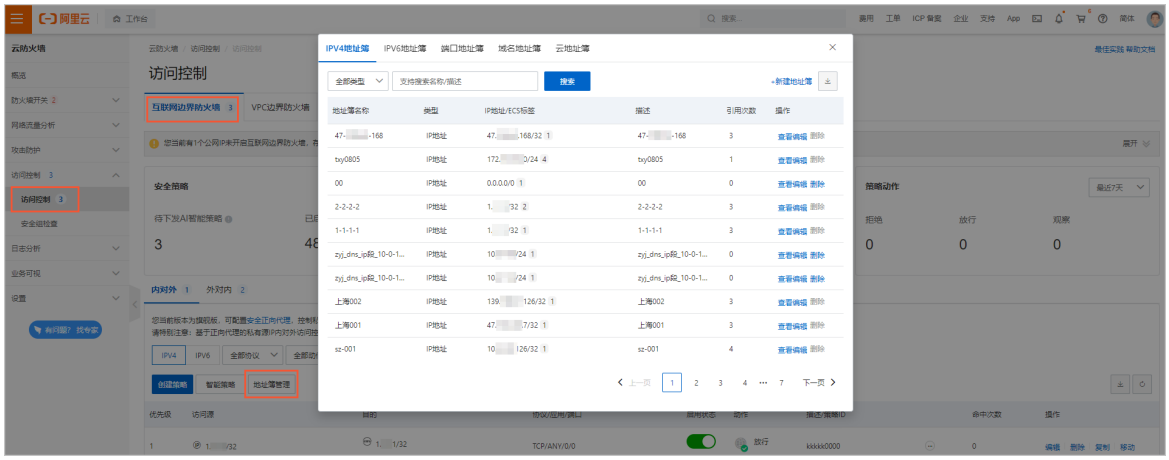
- **IPv4地址簿**：**地址簿类型**为**IP地址**时，单个地址簿最多只能添加2,000个格式为IPv4的IP地址；**地址簿类型**为**ECS标签**时，单个地址簿最多只能添加500个ECS标签。
- **IPv6地址簿**：单个地址簿最多只能添加2,000个格式为IPv6的IP地址。

  > **说明** 云防火墙高级版实例不支持IPv6地址簿功能。

- **端口地址簿**：单个地址簿最多只能添加50个端口。
- **域名地址簿**：单个地址簿最多只能添加2,000个域名。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**访问控制**页面的**互联网边界防火墙**页签，单击策略列表上方的**地址簿管理**。



4. 在地址簿对话框中，管理地址簿。

   支持以下操作：

   - **添加地址簿**

     您可根据云防火墙访问控制策略的配置需求，添加受信或威胁地址簿。云防火墙支持添加**IPv4地址簿**、**IPv6地址簿**、**端口地址簿**、**域名地址簿**。详细信息，请参见添加地址簿。

   - **查看编辑地址簿**

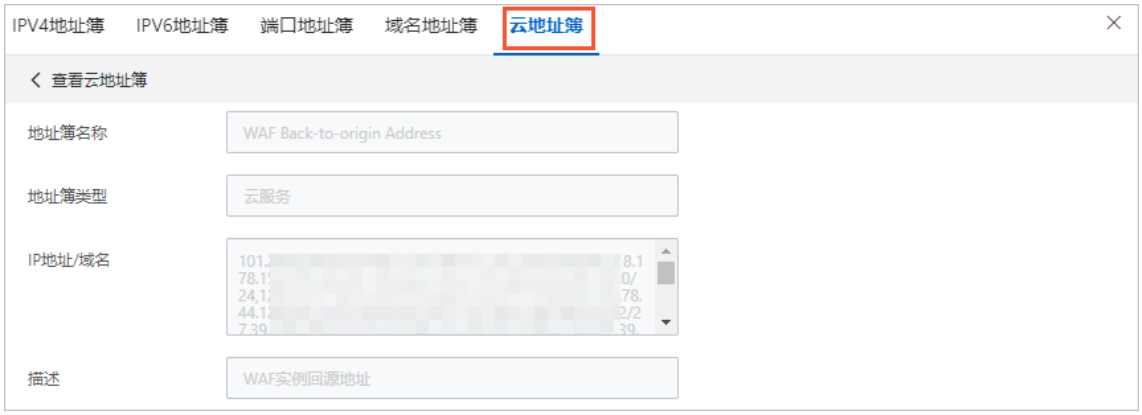
     在**IPv4地址簿**、**IPv6地址簿**、**端口地址簿**、**域名地址簿**页签，定位到目标地址簿。单击**操作**列的**查看编辑**，查看并修改地址簿配置项。

     > 说明 云防火墙不支持修改**地址簿类型**。

   - **查看云地址簿**

     在**云地址簿**页签，查看云地址簿的名称、类型、IP地址/域名、引用次数、描述等信息。

   单击**操作**列的**查看**，查看云地址簿的配置项信息。



- **删除地址簿**

  在**IPv4地址簿**、**IPv6地址簿**、**端口地址簿**或**域名地址簿**页签，定位到目标地址簿。单击**操作**栏的**删除**，并单击**确定**，可删除您不再需要的地址簿。

  > **说明** 云防火墙不支持删除已被引用的地址簿。

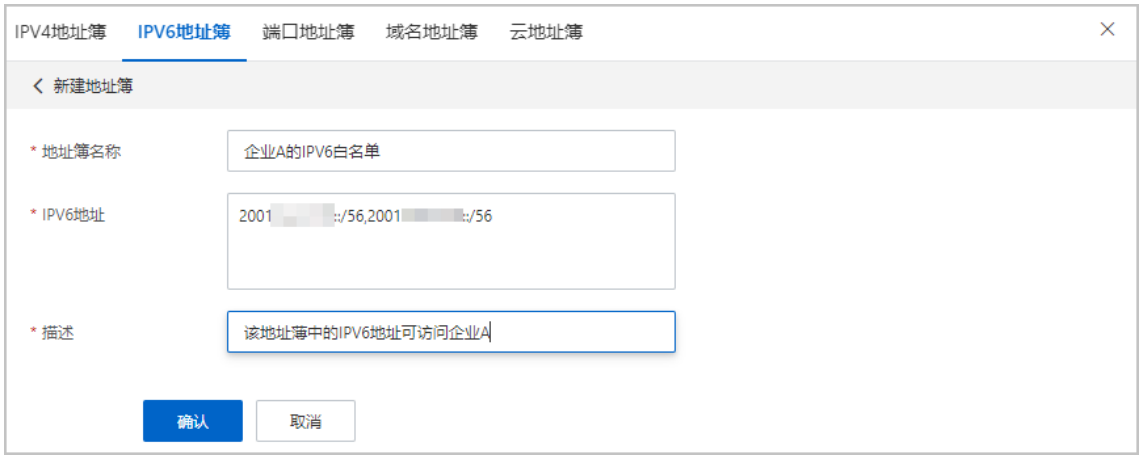
- **导出地址簿**

  在**地址簿管理**对话框右上角，单击 图标，导出地址簿。

添加地址簿

1. 在**IPv4地址簿**、**IPv6地址簿**、**端口地址簿**或**域名地址簿**页签，单击右上角的**新建地址簿**。
2. 在**新建地址簿**、**新建端口地址簿**或**新建域名地址簿**页面，配置地址簿的配置项。相关参数说明，请参见下表。
   - **IPv4地址簿**

- **IPv6地址簿**



- **端口地址簿**

- **域名地址簿**

配置项类型	配置项	说明
IPv4地址簿	**地址簿类型**	选择IP地址簿类型。可选： ○ **IP地址** ○ **ECS标签**
	IP地址	输入IP地址段。 **说明** **地址簿类型**选择**IP地址**时显示，多个地址段用半角逗号（,）隔开。
	ECS标签更新	有新匹配标签的ECS时，是否开启自动添加到当前地址簿。默认开启该功能，且不支持修改。 **说明** **地址簿类型**选择**ECS标签**时显示。
	ECS标签	选择当前阿里云账号下已创建的ECS标签及对应标签值。云防火墙自动将具有这些标签的ECS公网IP放到一个地址簿中。 单击**新增一组ECS标签**，可添加多个ECS标签。 添加ECS标签后，会在**ECS标签**下方显示对应的ECS信息，例如VPC名称、IP地址等。 **说明** **地址簿类型**选择**ECS标签**时显示。
IPv6地址簿	**IPv6地址**	输入IPv6地址段。多个IPv6地址段用半角逗号（,）隔开。
端口地址簿	**端口**	输入端口。多个端口间用半角逗号（,）隔开。
域名地址簿	**域名**	输入域名。多个域名间用半角逗号（,）隔开。
通用配置项	**地址簿名称**	自定义地址簿名称。建议输入有实际意义的名称，方便您有效识别并应用该地址簿。

配置项类型	配置项	说明
	描述	输入当前地址簿内容和使用场景。便于您识别并应用地址簿。

3. 单击**确认**，完成地址簿添加。
   地址簿添加成功后，您可以在地址簿对话框的对应地址簿页签，查看该地址簿的名称、引用次数、描述等信息，或修改、删除该地址簿。

相关文档

- 互联网边界（内外双向流量）
- VPC边界防火墙
- 防护配置

2.10. 修改云防火墙访问控制策略的优先级

云防火墙支持修改访问控制策略的优先级。本文介绍了如何修改互联网边界防火墙访问控制策略的优先级。

背景信息

云防火墙的访问控制策略优先级是指访问控制策略生效的顺序，1代表最高优先级，数字越大优先级越低。

互联网边界防火墙不同版本可配置的访问策略数量和优先级范围如下所示：

- 高级版：可配置4,000条访问控制策略。策略优先级范围为1~4,000。
- 企业版：可配置10,000条访问控制策略。策略优先级范围为1~10,000。
- 旗舰版：可配置20,000条访问控制策略。策略优先级范围为1~20,000。

VPC边界防火墙不同版本可配置的访问策略数量和优先级范围如下所示：

- 企业版：可配置10,000条访问控制策略。策略优先级范围为1~10,000。
- 旗舰版：可配置20,000条访问控制策略。策略优先级范围为1~20,000。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > 访问控制**。
3. 在**互联网边界防火墙**页签的**内对外**或**外对内**流量列表中，定位到需要修改优先级的访问控制策略，并单击最右侧**操作**列中的**移动**按钮。

4. 在移动优先级对话框中修改优先级参数。

5. 单击**确定**完成优先级修改。

> **说明** 云防火墙策略优先级修改后，该策略原优先级之后的策略优先级都将相应依次递减。

2.11. DNS域名访问控制策略

开启DNS防火墙后，您可以设置DNS域名访问控制策略，限制VPC资产对指定域名的访问。

前提条件

已开启DNS防火墙。相关操作，请参见DNS防火墙。

背景信息

VPC要访问指定域名，必须先通过DNS服务器解析域名对应的IP地址。开启DNS防火墙后，VPC访问互联网域名时会先经过DNS防火墙，您可以通过配置DNS域名访问控制策略对VPC访问互联网域名进行访问控制和防护。

版本限制

只有企业版和旗舰版云防火墙支持配置DNS域名访问控制策略。其中企业版最多支持配置10,000条策略，旗舰版最多支持配置20,000条策略。如果您需要配置更多策略，请提交工单申请扩展。

创建放行指定域名的访问控制策略

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**访问控制 > DNS域名**。
3. 在**DNS域名**页面，单击**创建策略**。
4. 在**创建策略**对话框，以创建一条放行指定域名的访问控制策略为例，按照以下步骤新增访问控制策略。
   i. 创建第一条策略，先对可信的源IP进行**放行**。

   请参照下表，完成参数配置。

参数名称	参数配置说明
源类型	访问源的类型。可选值： ■ **IP**：仅支持单个IP地址段。 ■ **地址簿**：您预先配置的IP地址簿，是多个IP地址段的组合，便于您在配置策略时对多个IP地址进行管控。
访问源	设置访问流量的来源地址。 不同源类型设置的访问源如下： ■ 选择**IP**作为源类型时，该访问源一定要设置成网段。每条策略只支持配置一个网段。 ■ 选择**地址簿**作为源类型时，您可单击指定地址薄右侧的**选择**按钮，选择某个域名地址簿作为**访问源**。 > **说明** 您1次只能选择1个地址薄，如果需要使用多个地址薄，您可以通过**新增策略**来添加。

参数名称	参数配置说明
目的类型	可选择**地址薄**、**域名**。
目的	设置接收流量的目的地址。 选择**地址簿**作为目的类型时，您可单击指定地址薄右侧的**选择**按钮，选择某个域名地址簿作为**目的**。 **说明** 您1次只能选择1个地址薄，如果需要使用多个地址薄，您可以通过**新增策略**来添加。
动作	访问控制策略执行的动作。可选值： ■ **放行**：访问源允许访问目的地址。 ■ **拒绝**：访问源禁止访问目的地址。 ■ **观察**：设置为观察模式后，允许访问源到目的地址的访问。观察一段时间后，您可根据实际需求调整为**放行**或**拒绝**。
描述	对该策略进行描述或备注，便于您后续查看时，能快速区分每条策略的目的。
优先级	选择该策略的优先级。1为最高优先级，数字越大，优先级越低。优先级相同的策略，动作为**拒绝**的策略优先生效。 **说明** DNS域名访问控制策略的优先级是静态的，可创建多条优先级相同的策略。请您在创建访问控制策略之前先做好策略优先级的规划。

ii. 创建第二条访问控制策略，拒绝所有访问流量的来源地址去访问指定的域名。

将**访问源**地址设置为 `0.0.0.0/0` ，**动作**设置为**拒绝**，禁止所有未授权的访问。其他访问控制参数配置，请参见参数配置表。

iii. 确定第一条可信源**放行**策略的优先级高于第二条所有访问流量的来源地址**拒绝**策略的优先级。

按照以上步骤配置完成访问控制策略后，云防火墙只允许指定的源IP地址访问策略中配置的域名。

导出策略

DNS域名访问控制策略支持导出功能。

查看是否有访问流量命中访问控制策略

访问控制策略配置完成后，默认情况下策略立即生效。但如果策略参数配置不正确，或者DNS防火墙未打开，可能会导致您的策略配置不生效。

您可以在访问控制策略列表中定位到该新增的策略，如果**命中次数**栏有显示对应的命中次数，表示已有访问流量命中该策略。**命中次数**是创建策略后，访问流量命中该策略的累计次数。

您还可以单击**命中次数**下的数字，跳转到**流量日志**页面。在**流量日志**页面**规则名**一栏会显示出该流量命中的访问控制策略的名称。

> **说明** 流量日志仅展示最近7天内的流量信息。某条访问控制策略有对应的命中次数，但如果命中策略是发生在距离当前时间的7天前，那么，流量日志列表中的数据将会为空。

相关操作

创建策略后，您可以在访问控制策略列表中，对该策略进行修改、删除、复制。

> **警告** 删除策略后，该策略管控的流量将不受云防火墙的访问控制。请谨慎删除。