ALIBABA CLOUD

阿里云

云防火墙

安全策略

文档版本：20200827

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.访问控制

1.1. 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。

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：

- 高级版： 内-外流量和外-内流量各可配置1000条。
- 企业版： 内-外流量和外-内流量各可配置2000条。
- 旗舰版 ： 内-外流量和外-内流量各可配置5000条。

> 说明 云防火墙支持对域名进行访问控制。对域名配置访问控制策略后，访问该域名的所有流量都将受到该条策略的控制（放行、拒绝或观察）。

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

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

1.2. 互联网边界防火墙（内外双向流量）

云防火墙支持对互联网边界防火墙进行访问控制。您可在云防火墙中配置访问控制策略，限制主机对内、外双向流量的未授权访问。

前提条件

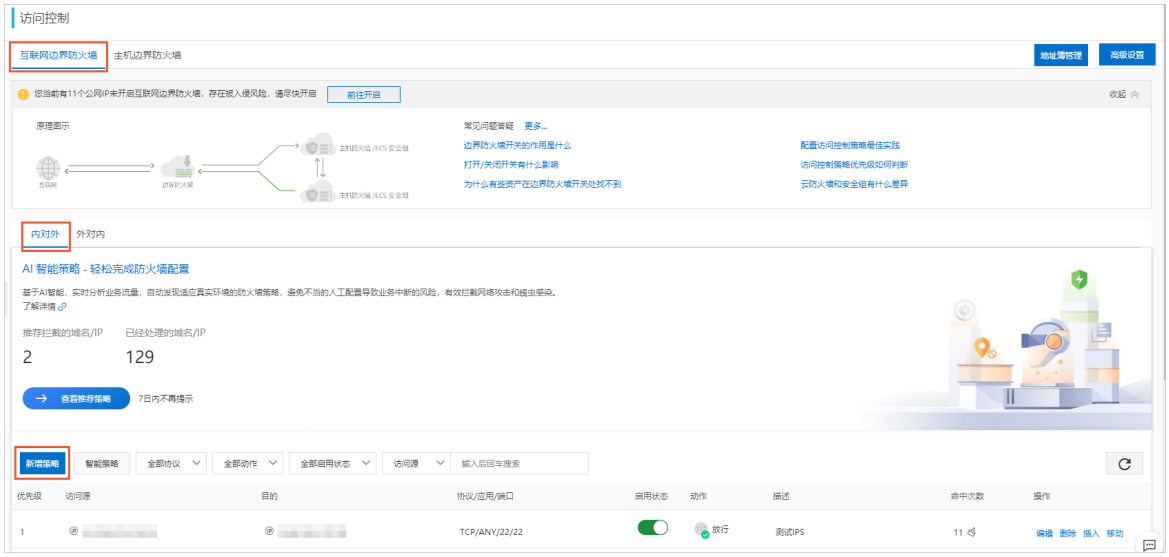
配置互联网边界防火墙策略前，请您确认需要进行访问控制实例的**互联网边界防火墙**开关已开启，否则策略将不会生效。

背景信息

互联网边界防火墙支持**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）流量的访问控制。

内对外流量访问控制

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**安全策略 > 访问控制**。
3. 在**互联网边界防火墙 > 内对外**页签下，单击**新增策略**。



4. 在**新增内-外策略**对话框中，按照以下步骤新增**内对外**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. **参考表格中的配置说明配置规则参数。**

参数名称	参数配置说明
源类型	可选择*IP*或*地址簿*。 ■ **IP**：仅支持单个IP地址段。 ■ **地址簿**：是您预先配置的IP地址簿，是多个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。

参数名称	参数配置说明
访问源	设置访问流量的来源地址（公网IP）。 ■ 选择**IP**作为源类型时，该访问源一定要设置成网段，例如：1.1.1.1/32。 ■ 选择**地址簿**作为源类型时，您可单击指定地址薄操作栏**选择**按钮，选择该IP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。
目的类型	可选择*IP*、*地址簿*、*域名*或*区域*。 **说明** 目的*区域*已支持中国全部区域（中国23个省、4个直辖市、5个自治区以及2个特别行政区），以及全部国际区域（全球7个洲）。
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，例如：1.1.1.1/32。 ■ 选择**地址簿**作为目的类型时，您可单击指定地址薄操作栏**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个地址薄，如果需要使用多个地址薄，您可以通过**新增策略**来添加。 ■ 选择**域名**作为目的类型时，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。 ■ 选择**区域**作为目的类型时，请您选择**目的**所在的区域。
协议类型	设置该内到外访问流量的协议类型，可选择*TCP*、*UDP*、*ICMP*或*ANY*。不确定具体协议类型时可选择*ANY*。
端口类型	可选择*端口*或*地址簿*。 ■ **端口**：仅支持一个端口范围。 ■ **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，手动输入单个端口号，或者单击**选择**，从地址薄中选择预先配置的**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
应用	设置该内到外访问流量的应用类型。 说明 目的类型选择*域名*时，应用可选择*HTTP*、*HTTPS*、*SMTP*或*SMTPS*。
动作	设置允许或拒绝该流量通过互联网边界防火墙。本操作步骤中选择*放行*。
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。

b. 单击**提交**完成访问控制策略的创建。

说明 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，拒绝其它所有访问源去访问外部互联网。

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。

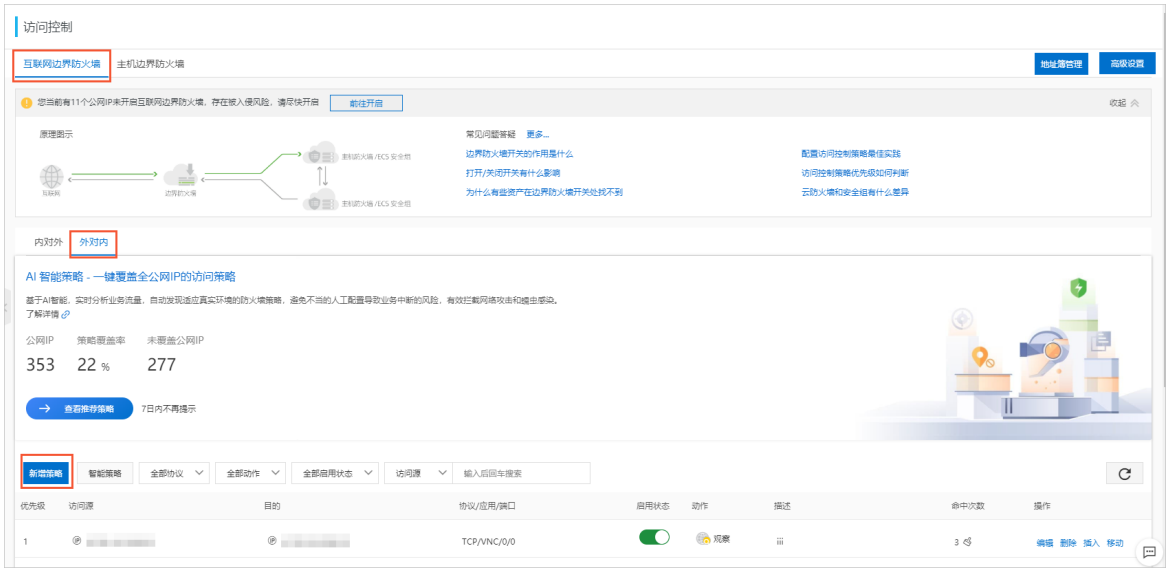
iii. 确定第一条可信源**放行**策略的优先级高于第二条所有访问源**拒绝**策略的优先级。

说明 默认情况下，云防火墙按照访问控制策略创建的先后顺序为策略分配优先级，新创建策略的优先级低于已有策略的优先级。有关策略优先级的详细内容，请参见设置和修改访问控制策略的优先级。

有关策略配置参数的详细说明，参见访问控制策略参数表。

外对内流量访问控制

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**安全策略 > 访问控制**。
3. 在**互联网边界防火墙 > 外对内**页签中，单击**新增策略**。



4. 在**新增外-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**选择了*地址簿*，那么**访问源**可选择IP地址簿或云地址簿类型，目的地址簿仅可选择IP地址簿类型。

5. 创建第二条**外对内**访问控制策略，拒绝其它所有访问源去访问内部网络。

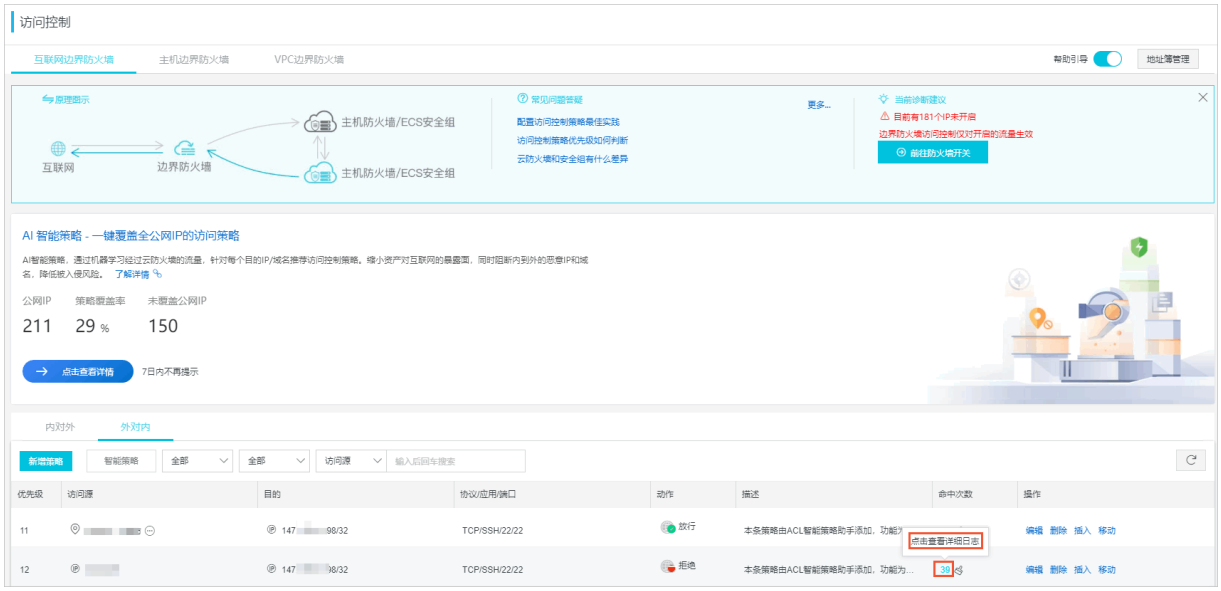
   将**访问源**地址设置为 `0.0.0.0/0` ，**动作**设置为**拒绝**，禁止所有未授权的访问。

6. 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。

查看访问控制策略是否已生效

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。

您可在访问控制策略列表中定位到该新增的策略，并单击命中次数，跳转到**流量日志**页面，查看策略是否生效。**流量日志**页面**规则名**一栏如果显示出该策略的名称，表示该策略已生效。



> **注意** 如果删除访问控制策略，之前配置的放行和拒绝策略会失效，请您谨慎删除。

访问控制策略参数表

参数名称	参数配置说明
源类型	访问源地址的类型。取值： • **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**：访问源设置需从您预先配置的地址簿中选择。 **说明** 您可以将多个IP地址设置成一个地址簿，方便您在配置访问控制规则时简化规则配置。

参数名称	参数配置说明
访问源	发送流量的IP/CIDR地址。 说明 访问源只支持配置一个网段，例如：1.1.1.1/32。 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 • 内对外流量：源类型只可选择IP地址簿类型，目的地址簿可选择IP地址簿、域名地址簿或云地址簿类型。 • 外对内流量：源类型可以选择IP地址簿或云地址簿类型，目的地址簿仅可选择IP地址簿类型。 • 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。
目的类型	您可以选择以下目的类型： • IP地址：访问目的设置为IP地址。 • 地址簿：访问目的从地址簿中选择IP地址簿、域名地址簿或云地址簿。 • 域名：策略目的设置为某一个域名。域名配置支持泛域名，如 *.aliyun.com 。 说明 对于HTTP Header中没有Host字段或HTTPS请求没有SNI的流量默认放行。 • 区域：访问目的从列表中选择一个区域。可选国内区域或国际区域。
目的	访问目的需要设置为网段；只可配置一个网段。 如果目的类型选择的是域名，可以配置为域名或泛域名。 说明 • 内对外流量：访问源如果选择地址簿，只可选择IP地址簿类型；目的地址簿可选择IP地址簿、域名地址簿或云地址簿类型。 • 外对内流量：源类型可选择IP地址簿或云地址簿类型，目的地址簿仅可选择IP地址簿类型。 • 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。
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

参数名称	参数配置说明
端口类型	您可以选择以下端口类型： • **端口**：仅支持一个端口范围。 • **地址簿**：是您预先配置的**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，手动输入单个端口号，或者单击选择，从地址薄中选择预先配置的**端口地址簿**。 **说明** • 您1次只能选择1个地址薄，如果需要使用多个地址薄，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有：ANY、HTTP、HTTPS、Mamcache、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	允许或拒绝该流量通过互联网边界防火墙。 取值： • **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。取值： • **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。 默认优先级为*最后*。

1.3. 主机边界防火墙（ECS实例间）

云防火墙支持对主机边界防火墙的访问控制，即控制ECS实例间的入流量和出流量。您可以在云防火墙配置访问控制策略，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经发布后，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。
- 提供初始的策略组模板，便于设置放行、拒绝所有流量。
- 同应用组配合，自动创建安全组。

关于主机边界防火墙和ECS安全组的区别，请参见云防火墙和安全组有什么差异？

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. 新建策略组策略
3. 发布策略组策略

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提交工单，申请阿里云技术支持。

策略组类型

策略组分为普通策略组和企业策略组。下表列举了两种策略组类型的差异。

策略组类型	策略组策略类型	策略组策略优先级	入方向访问策略	出方向访问策略	适用场景
普通策略组	默认策略组策略	由策略组模板决定	由策略组模板（放行或拒绝）决定	由策略组模板（放行或拒绝）决定	对网络精细化控制要求较高、网络连接数适中的用户场景
	手动添加的策略组策略	在1~100之间取值，数值越低，优先级越高	支持允许和拒绝策略，可按需添加	支持允许和拒绝策略，可按需添加	
企业策略组	默认策略组策略	取值范围：1，该值不支持修改	由策略组模板（仅放行）决定	由策略组模板（仅放行）决定	对运维效率有更高需求的用户场景
	手动添加的策略组策略		支持允许策略，可按需添加	支持允许策略，可按需添加	

新建策略组

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

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，便于后期管理。
所属VPC	从**所属VPC**列表选择应用该策略组的专有网络VPC。 **说明** 一个策略组只允许隶属于一个VPC。
实例ID	从**实例ID**列表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，方便后期管理。

参数	描述
模板	从模板列表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。

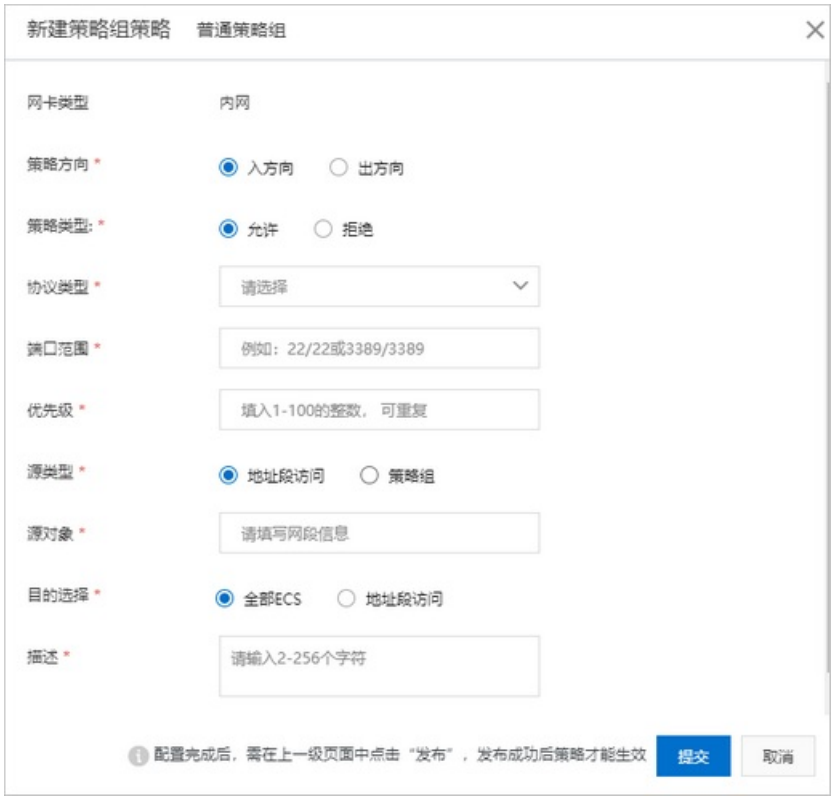
5. 单击**提交**。
   策略组创建完成后，您可以在主机边界防火墙的策略组列表中查看新建的策略组，并根据需要对策略组执行以下操作：
   - **配置策略**：为策略组配置精细的访问控制策略。
   - **发布**：将策略组的访问控制策略同步到ECS实例的安全组。
   - **编辑**：修改应用当前策略组的ECS实例和策略组的描述。
   - **删除**：删除策略组。

     警告 删除策略组后，策略组中的主机访问控制策略也将被自动删除并失效，请谨慎操作。

     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**，筛选出所有手动创建的策略组，再去判断策略组是否需要保留。

新建策略组策略

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**安全策略 > 访问控制**。
3. 在**访问控制**页面单击**主机边界防火墙**页签，定位到要设置的策略组，单击其操作列下的**配置策略**。
4. 在**策略配置**页面单击右上角的**新增策略**。
5. 在**新建策略组策略**对话框配置策略参数。



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。如果两个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。
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。

参数	描述
优先级	输入策略生效的优先级。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。 说明 企业策略组的策略优先级固定为1且不可修改，表示优先级最高。
源类型和源对象	针对入方向策略，选择访问源地址的类型，并根据选择的源类型设置源对象。 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，需要从策略组列表中选择一个策略组，表示设置策略组ECS实例作为源对象。 说明 企业策略组不支持策略组选项。
目的选择	针对入方向策略，选择访问流量的目的地址： ○ 全部ECS：表示阿里云账号下所有ECS实例。 ○ 地址段访问：选择该类型后，需要输入目的IP/CIDR地址段。
源选择	针对出方向策略，选择访问源： ○ 地址段访问：选择该类型后，需要输入访问源IP/CIDR地址。 ○ 全部ECS：表示阿里云账号下所有ECS实例。
目的类型和目的对象	针对出方向策略，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。 可选的目的类型： ○ 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，需要从策略组列表中选择一个策略组，表示设置策略组ECS实例作为目的对象。 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。

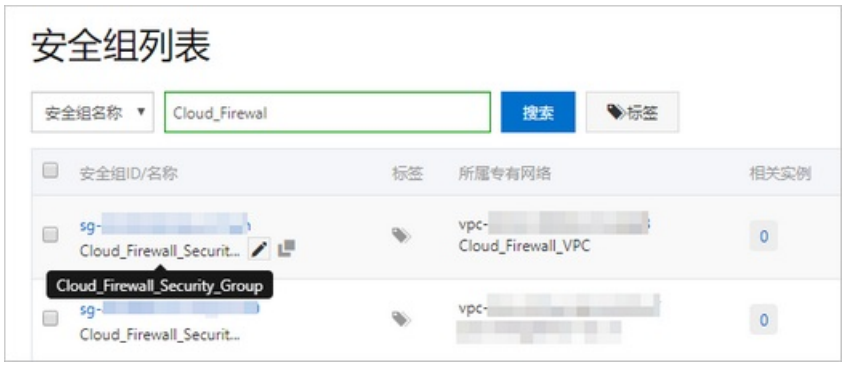
> 警告 删除策略后，策略中对应流量的访问控制将失效，请谨慎删除。删除策略后，策略记录仍会保留在策略列表中，但您无法再对其执行任何操作。

发布策略组策略

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**安全策略 > 访问控制**。
3. 在**访问控制**页面单击**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**对话框确认**变更策略**（即策略的变更内容），根据需要设置**变更备注**，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。策略的名称默认为Cloud_Firewall_Security_Group。



主机边界防火墙配置视频教程

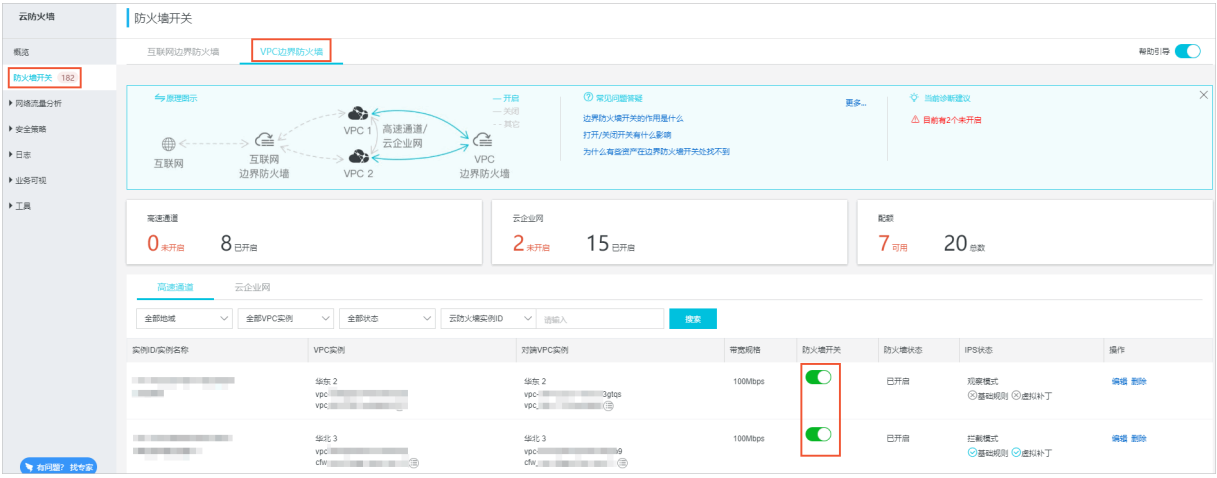
1.4. VPC边界防火墙

本文档介绍了VPC边界防火墙的访问控制操作。云防火墙支持对VPC边界防火墙的访问控制。VPC边界防火墙可用于检测和控制两个VPC间的通信流量。

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。



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，您需要对可疑流量或恶意流量进行拒绝；或者先对可信流量进行放行，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. 在左侧导航栏单击**安全策略 > 访问控制**。
3. 在**VPC边界防火墙**页签，单击**新增策略**。

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**配置项说明表**。

您可根据实际业务的需要，选择合适的VPC边界防火墙策略配置：

- 对可疑流量或恶意流量**拒绝**放行。
- 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**设置和修改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。

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，可选择*IP*或*地址簿*类型。 • **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**地址类型为地址薄，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。
访问源	发送流量的IP/CIDR地址。 > 说明 访问源只支持配置一个网段，例如：1.1.1.1/32。 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个地址薄，如果需要使用多个地址薄，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薄。 • **域名**：目的地址设置为域名。支持设置为泛域名，例如：**.aliyun.com*。 > 说明 对于HTTP Header中没有Host字段或HTTPS请求没有SNI的流量默认放行。
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，例如：1.1.1.1/32。 • 选择**地址簿**作为目的类型时，您可单击指定地址薄操作栏的**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个地址薄，如果需要使用多个地址薄，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*。

规则参数	参数选项说明
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	可选择*端口*或*地址簿*。 • **端口**：仅支持一个端口范围。 • **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，手动输入单个端口号，或者单击选择，从地址薄中选择预先配置的**端口地址簿**。 **说明** • 您1次只能选择1个地址薄，如果需要使用多个地址薄，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。

1.5. DNS域名解析地址访问控制策略

云防火墙访问控制策略配置升级，访问控制策略目的地址选择域名类型时，支持对域名进行DNS解析，并提供可视化解析地址供您查看。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

访问控制功能上线以来，对于互联网内对外流量的访问控制，云防火墙支持配置目的类型为**域名**的规则。如果您在创建内对外访问控制策略时，目的地址类型选择**域名**，那么该规则只可管控访问流量协议为TCP 、应用类型为HTTP/HTTPS/SSL/SMTP/SMTPS的数据（协议默认为TCP，不支持自定义选择协议）。

现在，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。目前，已实现内对外策略配置时，目的地址类型选择**域名**，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。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。

> 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）。

防护原理

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。

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。

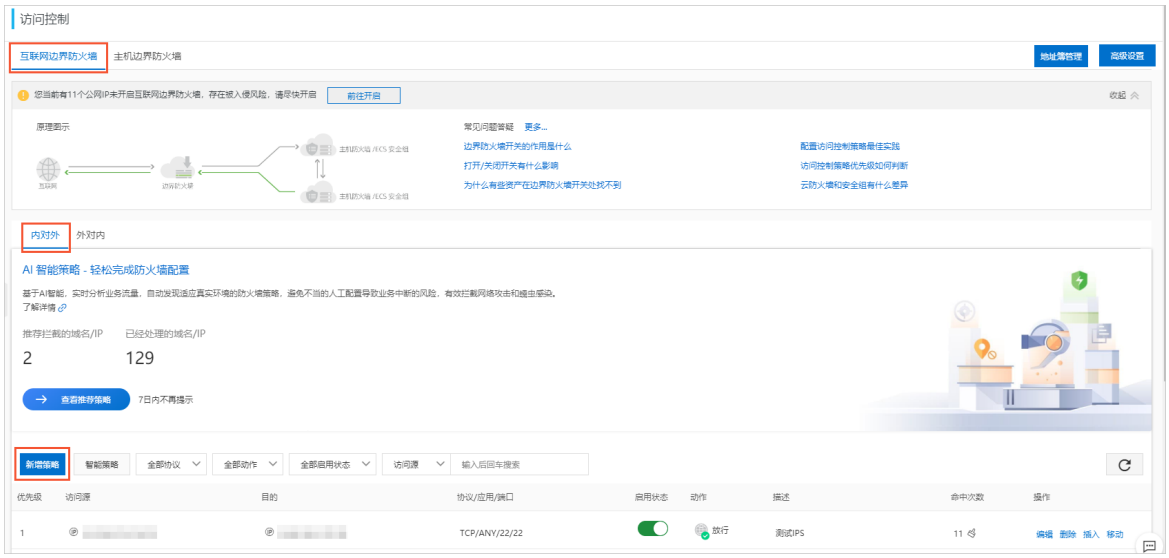
  目前，仅内对外流量的访问控制策略支持DNS域名解析。

- 目的地址域名为**通配符域名**（例如：*.aliyun.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*a.test.com*的ftp协议流量。假设*a.test.com*域名解析A记录为*1.1.1.1*，那么实际下发到引擎的规则为*1.1.1.1*的ftp协议允许。此时，如果*b.test.com*域名也解析A记录为*1.1.1.1*，那么访问*b.test.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*a.test.com*的解析结果由*1.1.1.1*变化为*2.2.2.2*，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. 在左侧导航栏单击**安全策略 > 访问控制**。
3. 在**互联网边界防火墙 > 内对外**页签下，单击**新增策略**。



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：1.1.1.1/32。
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**互联网边界防火墙 > 内对外**页面查看您配置的策略，对该策略进行编辑、删除、插入（即克隆已创建的策略）或移动该策略的优先级位置。

后续步骤

您可在**防火墙开关 > 互联网边界防火墙**查看您配置的访问控制策略是否已生效。

1.6. 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。

> **说明** 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。
- 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. 在左侧导航栏单击防火墙开关。
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。

后续步骤

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。

1.7. 智能策略

云防火墙智能策略使用了机器学习的技术，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

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。

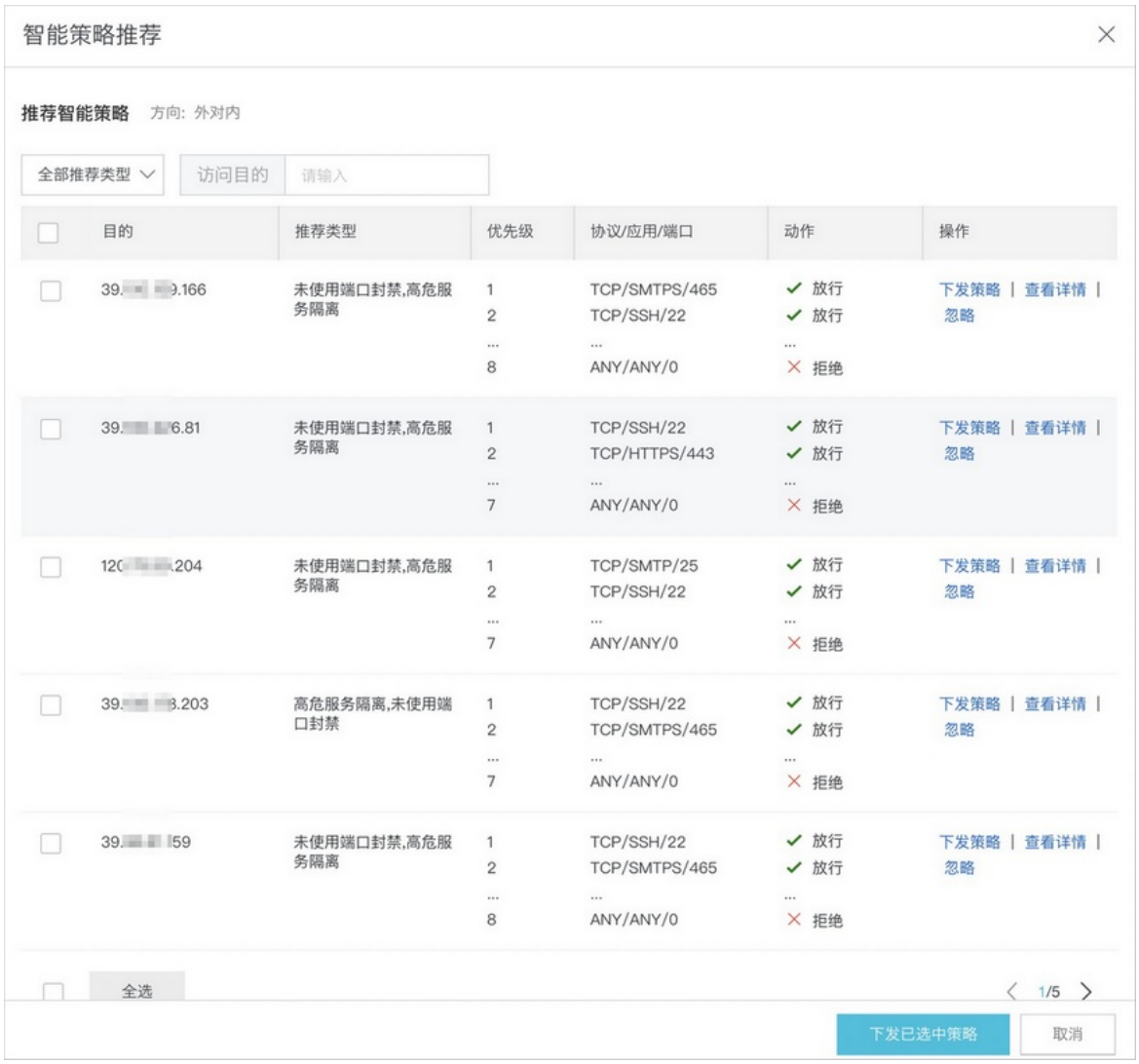
云防火墙为您推荐的智能策略包括以下三种类型：**高危服务隔离**、**未使用端口封禁**和**蠕虫防御**。

您可以根据需要选择是否下发智能推荐策略。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**安全策略 > 访问控制**。
3. 在**互联网边界防火墙**页签下，选择要配置的策略类型：**内对外**或**外对内**。

4. **单击智能策略。**
   跳转到智能策略推荐页面，显示云防火墙为您推荐的当前公网IP入方向或出方向的访问控制策略。



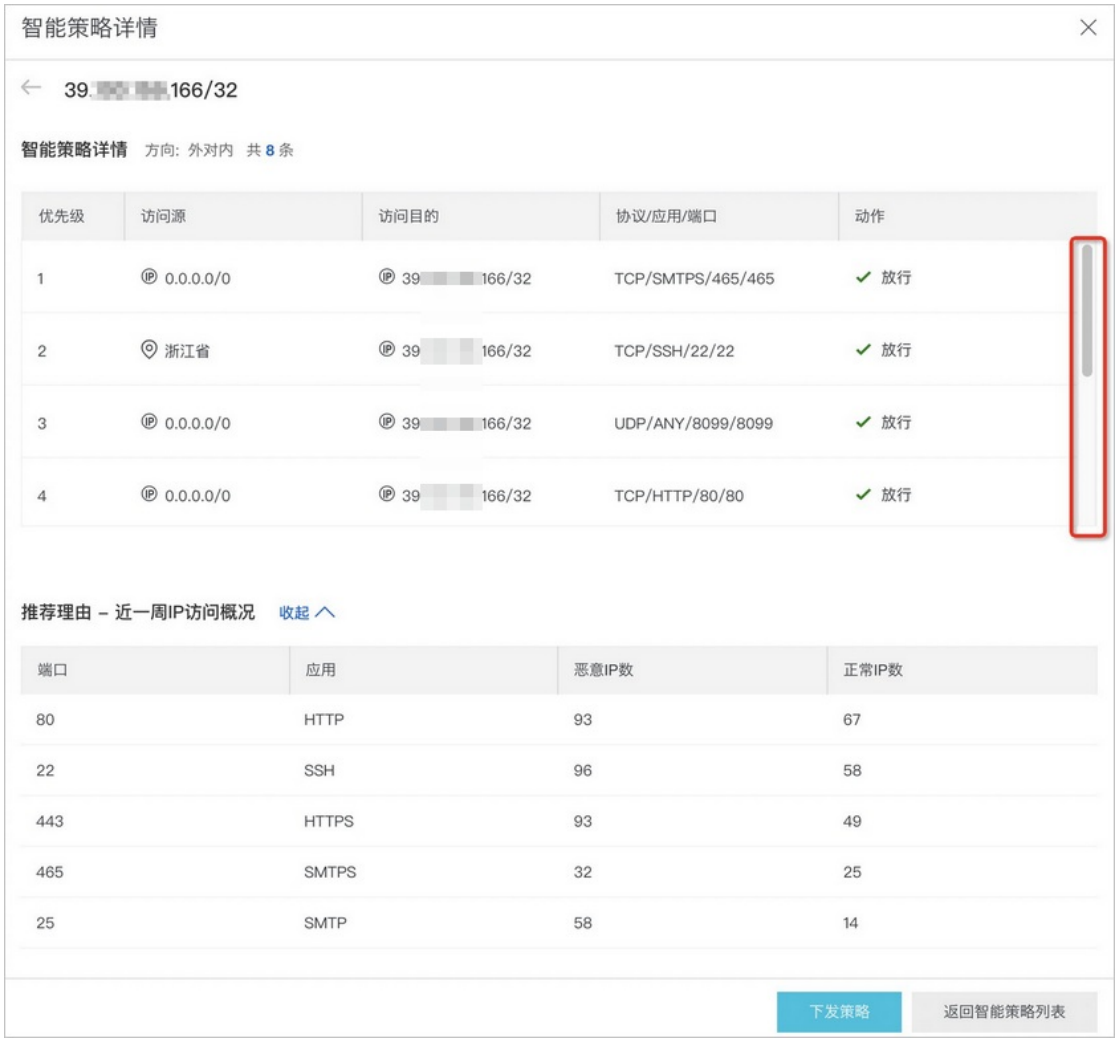
5. **（可选）查看策略详情。**

   i. **在智能策略推荐页面，定位到要查看的策略，单击其操作列下的查看详情。**

> **说明** 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。

ii. **在智能策略详情页面，查看云防火墙为当前公网IP智能推荐的所有策略和推荐理由。**

> **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。



6. **从以下方式中选择一种方式下发智能策略，使策略生效。**

> **注意** 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。

- **在推荐智能策略列表中，勾选要下发的策略，并单击下发已选中策略，批量下发策略。**
- **在推荐智能策略列表中，单击某个策略操作列下的下发策略，下发当前策略。**
- **进入某个策略的智能策略详情页面，单击下发策略，下发当前策略。**

执行结果

成功下发智能策略，已下发策略自动生效。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，请参见互联网边界防火墙（内外双向流量）。

1.8. 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灵活引用多个IP地址、端口或域名的信息。您可根据需要添加受信地址簿或威胁地址簿。本文介绍了地址簿的添加、查看和修改操作。

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。

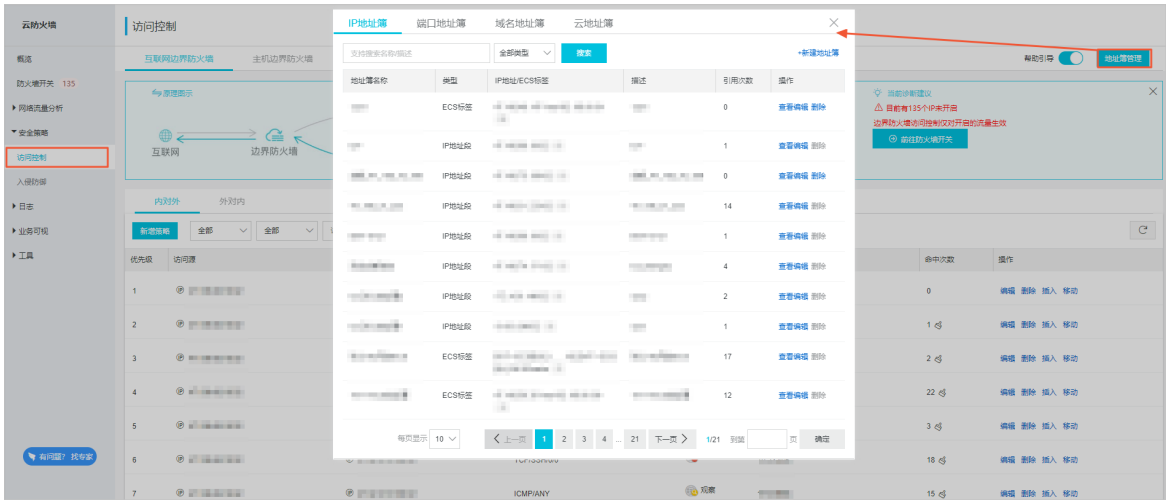
配置访问控制策略时，可灵活引用云防火墙地址簿。支持以下两种方式：

- 放行受信地址簿中的可信任IP和域名。
- 快速封禁威胁地址簿中的恶意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，且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。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**安全策略 > 访问控制**。
3. 在**互联网边界防火墙**页签，单击右上角的**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IP地址簿、端口地址簿、域名地址簿。具体请参见添加地址簿。

- **查看编辑地址簿**

  在IP地址簿/端口地址簿/域名地址簿页签，定位到目标地址簿。单击操作栏的查看编辑可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和地址簿名称。

- **查看云地址簿**

  在云地址簿页签可查看云地址簿的名称、类型、IP地址/域名及其数量、引用次数、描述等信息。

  单击操作栏的查看可查看云地址簿的配置项信息。

- **删除地址簿**

  在IP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。

添加地址簿

1. 在IP地址簿/端口地址簿/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/新建域名地址簿页面，配置地址簿的配置项（见下表）。
   - **IP地址簿**


IP地址簿
端口地址簿
域名地址簿
云地址簿
新建地址簿
地址簿类型
IP地址段
ECS标签
地址簿名称 *
地址簿名称会用于策略配置，请勿重复
ECS标签更新
有新匹配标签的ECS, 会自动加入到当前地址簿
ECS标签 *
全部VALUE
+ 新增一组ECS标签
VPC
ECS实例
ECS标签
IP
共 2 项
1/1
描述 *
请详细描述该地址簿内容和使用场景
提交
取消

- **端口地址簿**


IP地址簿
端口地址簿
域名地址簿
云地址簿
新建端口地址簿
地址簿名称 *
地址簿名称会用于策略配置，请勿重复
端口 *
端口范围 1-65535，多个端口间由英文逗号分割，形式如 22/22，80/88。最多只能添加50个端口。
描述 *
请详细描述该地址簿内容和使用场景
提交
取消

- **域名地址簿**

配置项类型	配置项	说明
IP地址簿	地址簿类型	选择IP地址簿类型。可选： ○ **IP地址段** ○ **ECS标签**
	IP地址	输入IP地址段。 说明 地址簿类型选择IP地址段时显示，多个地址段间用英文逗号隔开。
	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。
端口地址簿	端口	输入端口，多个端口间用英文逗号隔开。
域名地址簿	域名	输入域名，多个域名间用英文逗号隔开，不可重复。
通用配置项	地址簿名称	地址簿通用配置项。自定义地址簿名称，建议输入有实际意义的名称以便有效识别并应用该地址簿。
	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**提交**，完成地址簿添加。
   地址簿添加成功后，可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

互联网边界防火墙（内外双向流量）

VPC边界防火墙

入侵防御开关

1.9. 设置和修改访问控制策略的优先级

云防火墙中配置的每条访问控制策略都会自动分配一个默认的优先级。您可通过**移动**功能修改云防火墙访问控制策略的优先级。

背景信息

云防火墙的策略优先级是指访问控制策略生效的顺序。云防火墙每条访问控制策略拥有唯一优先级，1代表最高优先级。

优先级数字从1开始顺序递增，优先级数字越小，优先级越高。

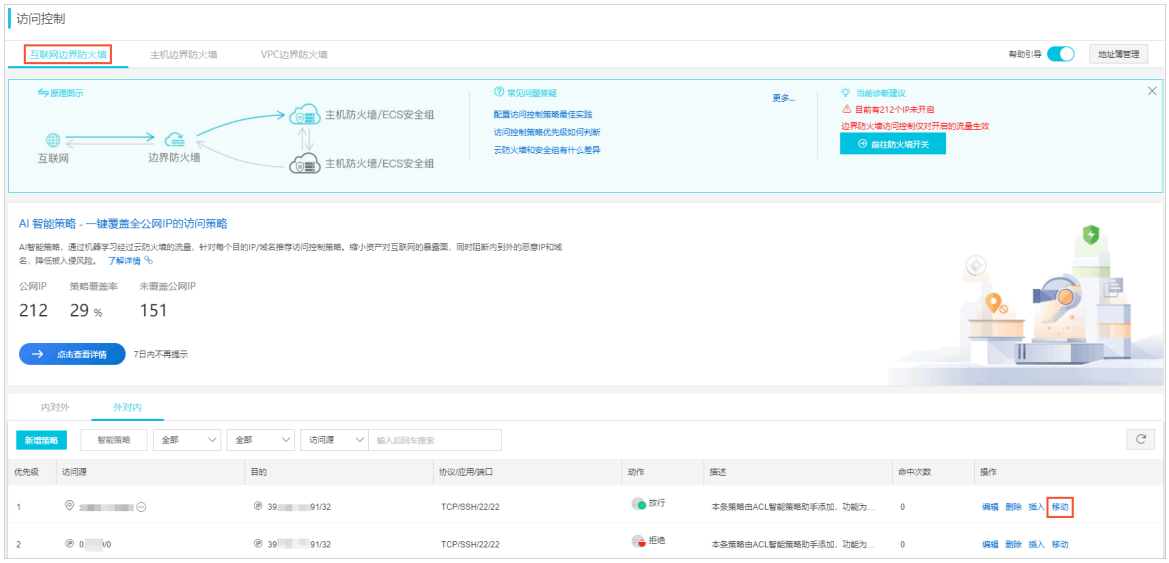
云防火墙不同版本可配置不同数量的访问策略，因此不同版本的优先级范围也不同。

- 高级版：可配置1000条访问控制策略。策略优先级范围为1~1000。
- 企业版：可配置2000条访问控制策略。策略优先级范围为1~2000。
- 旗舰版：可配置5000条访问控制策略。策略优先级范围为1~5000。

> **说明** 新增的策略默认为最低优先级（优先级最大数值）。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，单击**安全策略 > 访问控制**。
3. 在**互联网边界防火墙**页面的**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**栏中的**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.入侵防御开关

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

您可以通过入侵防御功能对威胁引擎的运行模式进行设置，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。

> 说明 您需要先开启互联网边界防火墙开关，您配置的入侵防御策略才会生效。相关内容请参见开启或关闭互联网边界防火墙。

限制说明

云防火墙高级版、企业版和旗舰版支持入侵防御功能，免费版不支持该功能。免费版需升级到高级版及以上版本，才能使用入侵防御功能。

对于入侵防御功能的子模块，云防火墙高级版不支持虚拟补丁自定义和基础防御自定义，云防火墙企业版和旗舰版无此限制。

入侵防御运行模式

入侵防御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。

  > 说明 云防火墙服务开通后，入侵防御功能默认开启为**观察模式**。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。

- **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。

高级设置

云防火墙入侵防御功能提供**高级设置**功能，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**

  云防火墙入侵防御模块不会对防护白名单中的流量进行拦截，加入到防护白名单的源和目的IP会被云防火墙视为可信流量并放行。

  在高级设置模块中单击防护白名单，将您确定为可信的流量添加到白名单中。设置防护白名单后，云防火墙入侵防御功能将对白名单中的流量地址放行。

  > **说明** 仅云防火墙企业版和旗舰版支持设置防护白名单。

  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

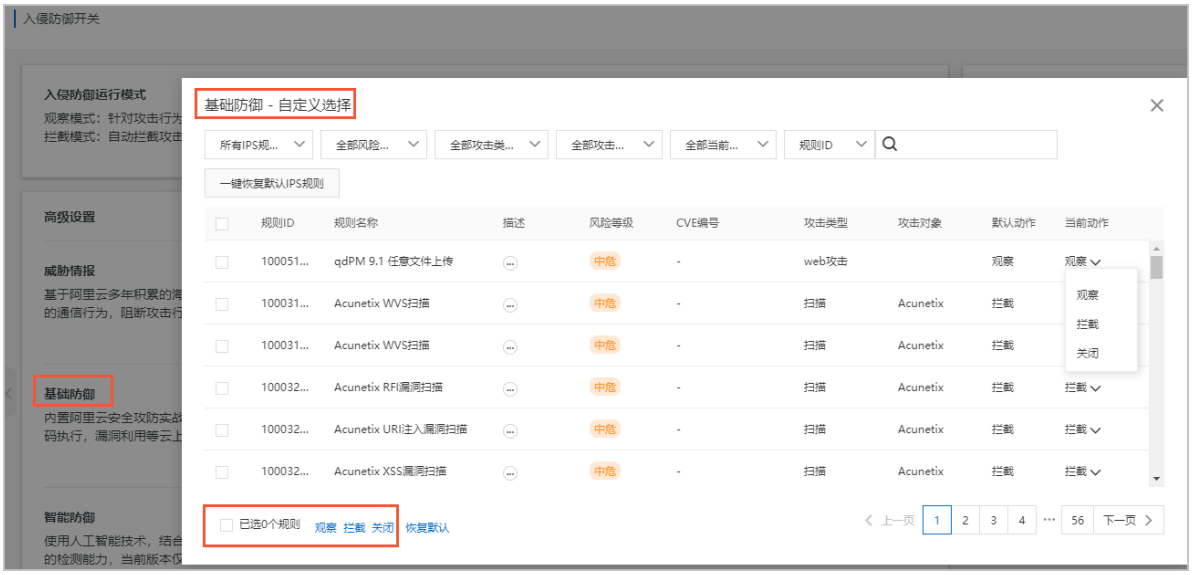
  威胁情报可将阿里云全网检测到的恶意IP同步到云防火墙，如：恶意访问源、扫描源、爆破源等，并对其进行精准拦截。开启后可提前感知全网威胁源。

  开启**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，包括爆破拦截、命令执行漏洞拦截、以及对被感染后连接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。

  开启**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才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。

  开启**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。

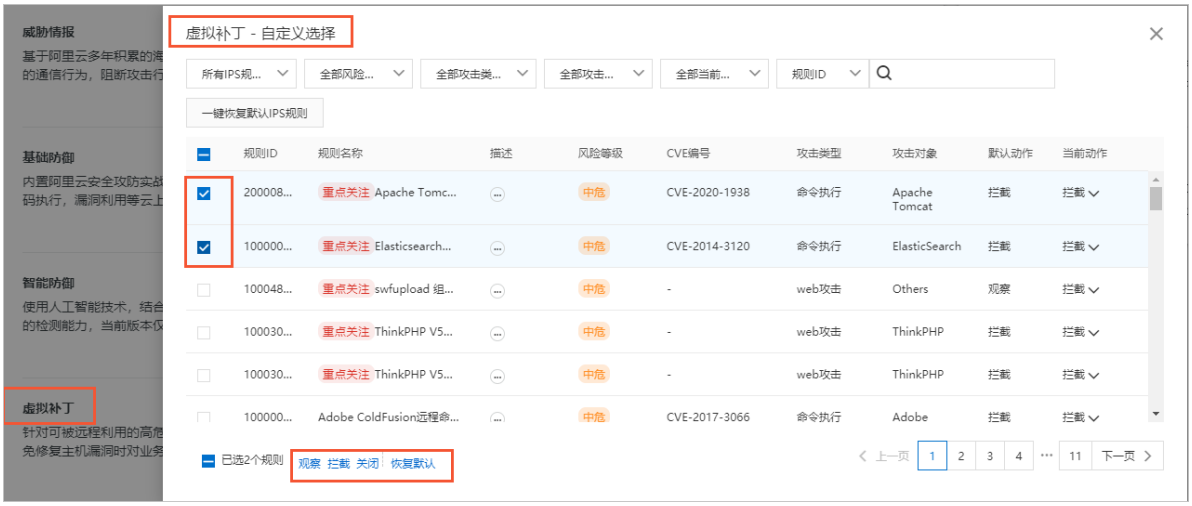
> **说明** 目前智能防御仅支持观察模式。

- 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才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。

规则库更新

云防火墙入侵防御页面的规则库更新 模块展示了云防火墙安全情报更新、虚拟补丁和IPS规则更新等产品快讯。

在规则库更新 模块右上角单击查看更多查看云防火墙推送的所有快讯。

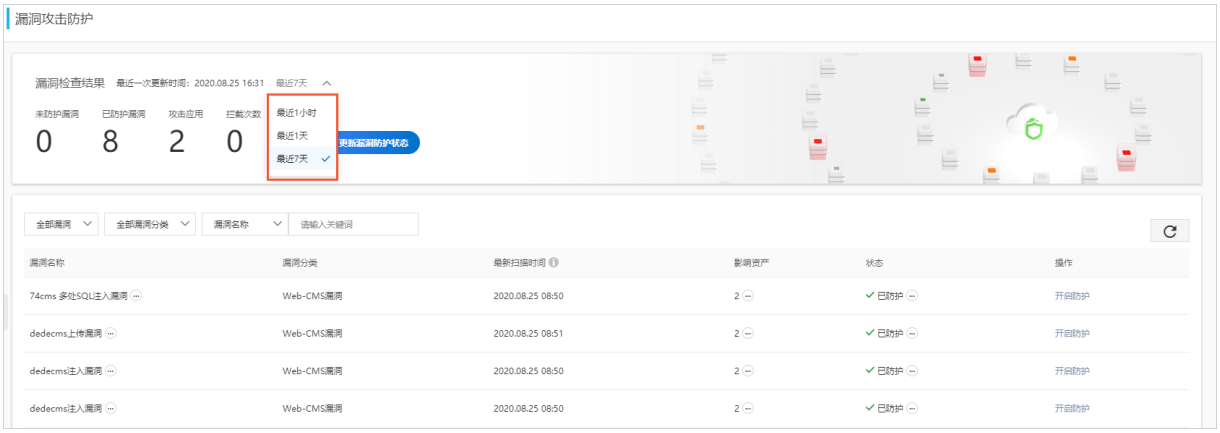
3.入侵防御

3.1. 漏洞攻击防护

漏洞攻击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到入侵。

背景信息

漏洞攻击防护页面可以展示最近1小时、1天和7天内的漏洞检查结果。



限制说明

云防火墙企业版和旗舰版支持漏洞攻击防护，免费版和高级版不支持漏洞攻击防护。

漏洞攻击防护功能支持自动检测漏洞，不支持手动检测。

> 说明 单击**更新漏洞防护状态**，表示仅同步云安全中心的最新漏洞扫描结果。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**漏洞修复页面进行操作。具体请参见**一键扫描漏洞**。

漏洞统计数据介绍

- **未防护漏洞**：表示您存在漏洞的资产没有开启云防火墙开关，导致访问流量未经过云防火墙，或者未开启IPS拦截开关。
- **已防护漏洞**：表示您存在漏洞的资产已开启了云防火墙开关和IPS防御规则，云防火墙已开启了对该漏洞的网络侧攻击利用。
- **攻击应用**：表示您存在漏洞的资产数量。
- **拦截次数**：表示您存在漏洞的资产开启了云防火墙开关和IPS防御规则后，云防火墙拦截网络侧攻击的次数。

可检测的漏洞分类

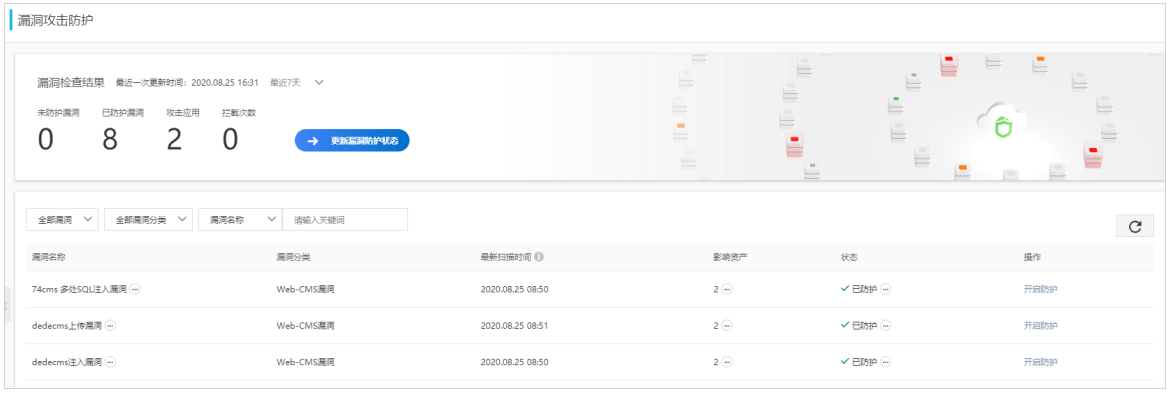
- **Web-CMS漏洞**：Web-CMS漏洞检测功能监控网站目录，识别通用建站软件，通过漏洞文件比对方式检测建站软件中的漏洞。详细内容请参见Web-CMS漏洞。
- **应用漏洞**：应用漏洞检测功能提供系统服务弱口令、系统服务和应用服务的漏洞检测及修复服务。详细内容请参见应用漏洞。
- **应急漏洞**：应急漏洞检测功能临时提供针对网络上突然出现的紧急漏洞的检测和修复服务。详细内容请参见应急漏洞。

漏洞的状态分类

- **已防护**：表示漏洞已在云防火墙的保护中。
- **未防护**：表示漏洞未受到云防火墙的保护。
- **部分防护**：表示部分ECS服务器已开启漏洞攻击防护。

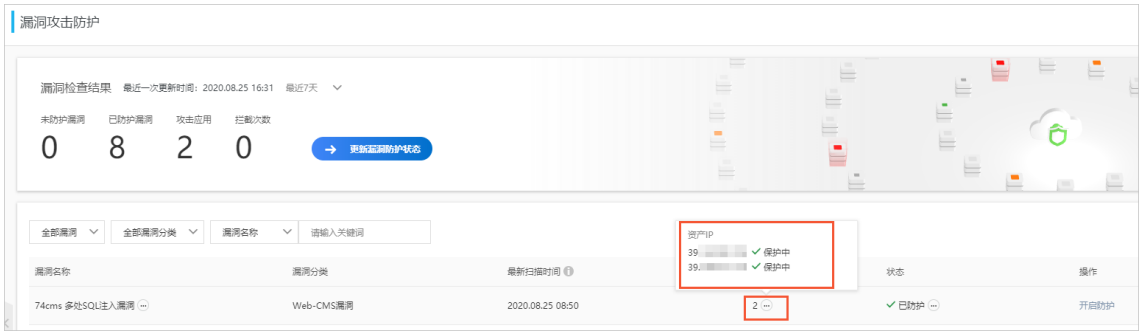
操作步骤

1. 登录云防火墙控制台。
2. 左侧导航栏单击**入侵防御 > 漏洞攻击防护**。
3. 在**漏洞攻击防护**页面，查看云防火墙的漏洞检查结果。



- 鼠标移动到**影响资产**列的

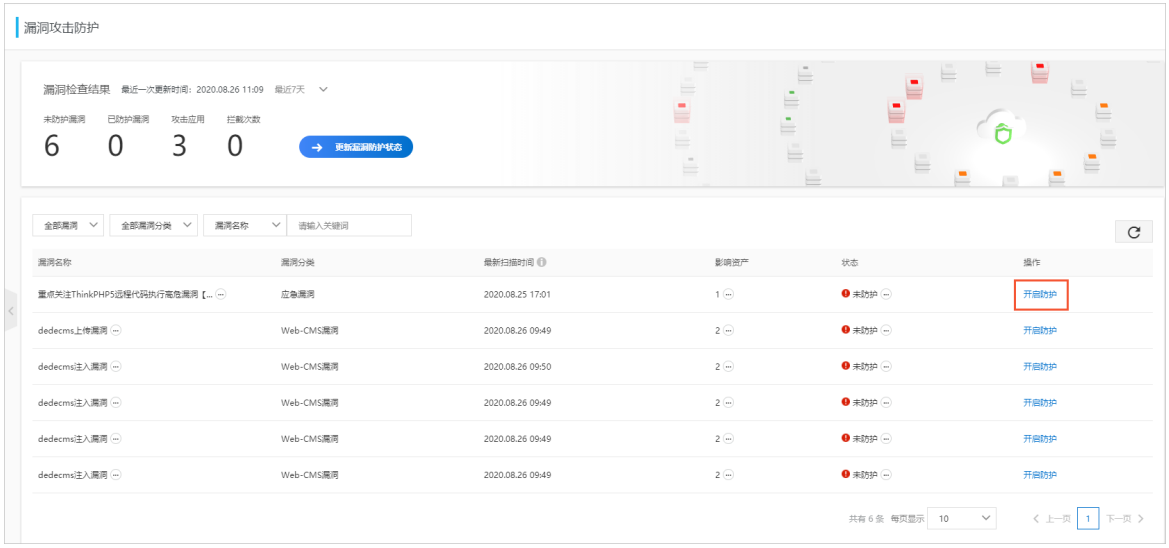
  上，会展示检测到存在该漏洞的服务器IP地址。



- 鼠标移动到**状态**列的

  上，会展示该漏洞的IPS防御规则ID。云防火墙内置的IPS防御规则都有对应的规则ID，您可以通过该规则ID在**入侵防御开关**页面的**高级设置**区域对应功能的自定义设置中查询该规则的详情。

4. 在**漏洞攻击防护**页面，定位到状态为**未防护**的漏洞，单击操作列的**开启防护**。



5. 在**一键开启防护**对话框中，单击**提交**，确认后开启漏洞攻击防护。

提交一键开启防护后，您的云防火墙将自动开启该漏洞对应服务器IP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** 开启漏洞攻击防护后，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 > 外对内**页签中已经放行这些资产对外的端口。