

阿里云 云防火墙

网络流量分析

文档版本：20190911

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、特殊性或惩罚性的损害，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。未经阿里云和/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
	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。	禁止： 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定。
courier 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
##	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[]或者[a b]]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{}或者{a b} }	表示必选项，至多选择一个。	<code>switch {stand slave}</code>

目录

法律声明.....	I
通用约定.....	I
1 云防火墙网络流量活动概览.....	1
2 主动外联活动.....	2
3 互联网访问活动.....	8
4 VPC访问活动.....	11
5 入侵检测.....	12
6 IPS阻断分析.....	14
7 全量活动搜索.....	18
8 智能策略下发.....	21

1 云防火墙网络流量活动概览

通过网络流量分析，您可以实时查看主机上发生的入侵事件、网络活动、流量趋势、入侵防御阻断访问和主机主动外联活动等，实现全网流量的可视化。

云防火墙提供以下4种网络流量分析：

- [主动外联活动](#)
- [入侵检测](#)
- [IPS阻断分析](#)
- [全量活动搜索](#)

2 主动外联活动

主动外联活动页面为您实时展示主机主动外联的详细数据，帮助您及时发现可疑主机。

您可查看主机1小时、1天、7天、1个月内或自定义时间范围内的主动外联活动情况。可设置的自定义时间范围为6个月内。

主动外联活动显示资产的以下信息：

- 主动外联流量：显示进行主动外联活动的连接数量、峰值流量和选定时间范围内的均值流量等数据。
- 主动外联应用端口：显示进行主动外联活动的应用端口的流量占比数据等信息。
- 主动外联目的IP：显示主动外联次数排名前5的资产的目的IP地址。
- 主动外联未授权域名：显示主动外联活动中未授权的域名信息列表。您可对其执行关注/取消关注/忽略的操作。
- 主动外联风险事件：显示主动外联活动中被检测为风险的事件。危险等级分为：低危、中危和高危3个等级。

操作步骤

1. 登录[云防火墙控制台](#)。
2. 单击导航栏网络流量分析，定位到主动外联活动页面。

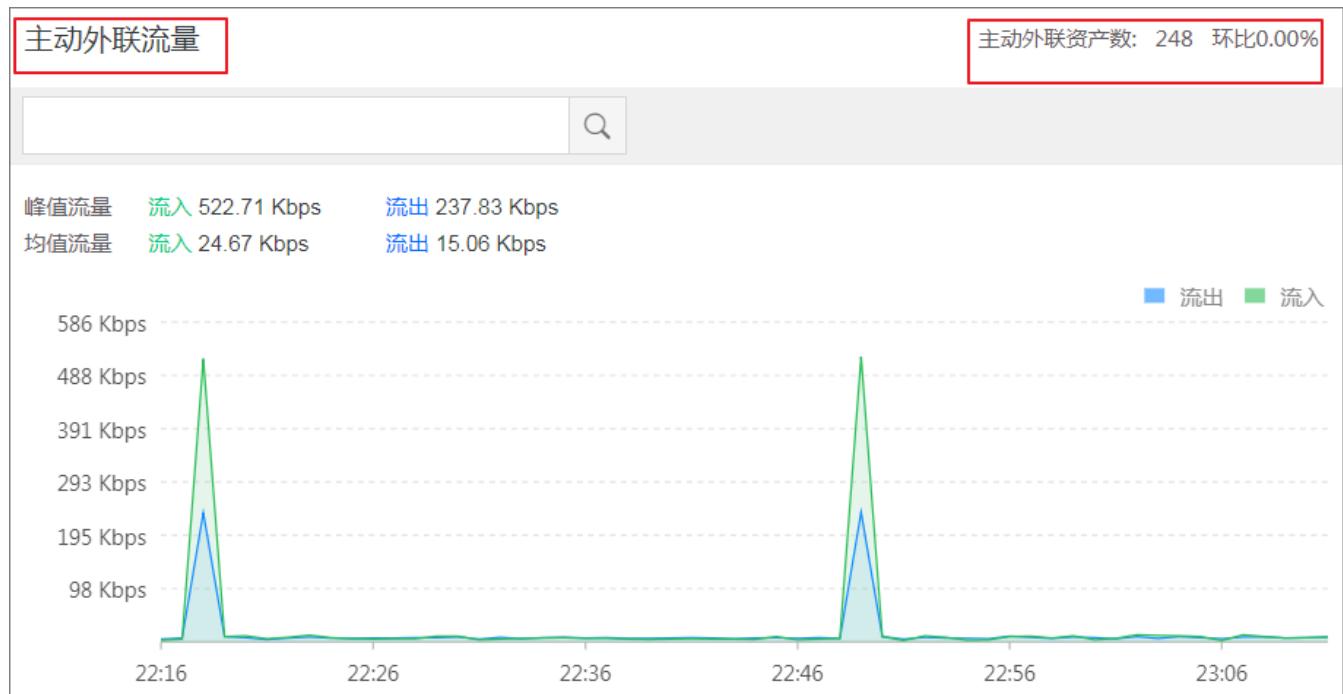


3. 在主动外联活动页面，查看1小时、1天、7天、1个月内或自定义时间范围内的主动外联活动情况和进行相应的处理。



查看主动外联流量数据

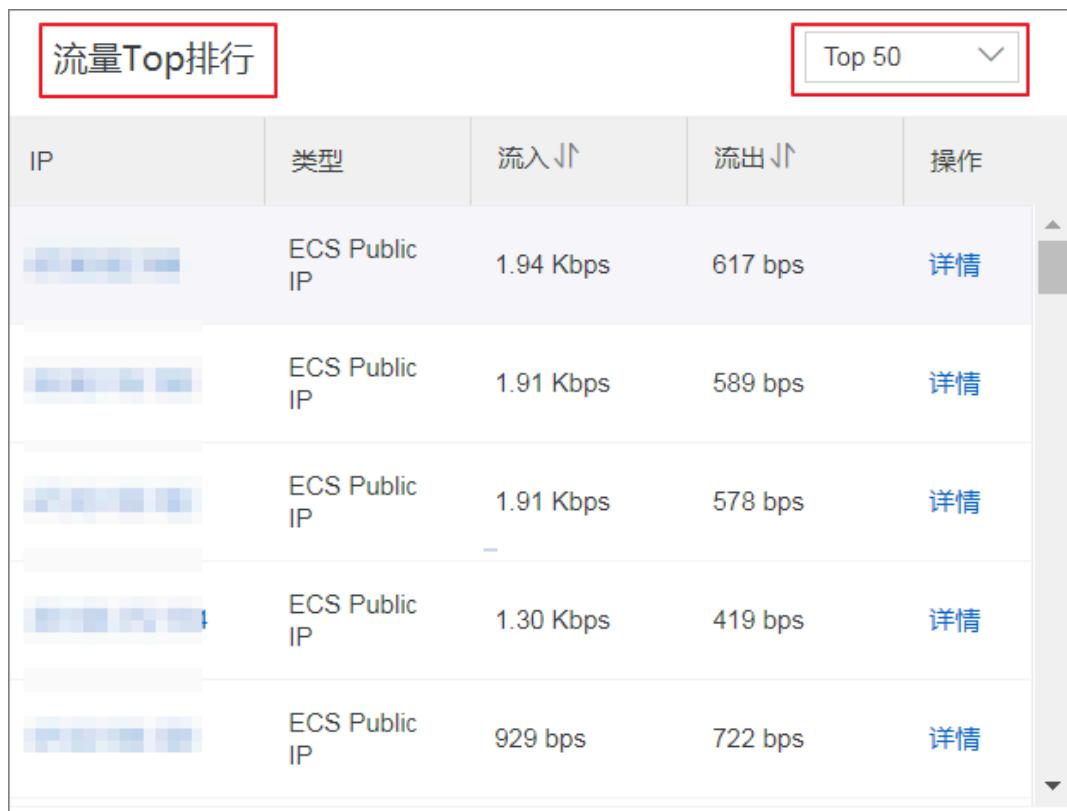
主动外联流量展示了1小时、1天、7天、1个月内或自定义时间范围内您资产中进行主动外联活动的流入和流出流量数据以及曲线图、主动外联资产总数、主动外联流量Top排行。



您可在主动外联流量区域查看以下信息：

- 主动外联资产总数和环比数据。
- 主动外联峰值流量（流入和流出）：鼠标悬浮在流量曲线图上看查看峰值流量发生的具体时间点。
- 主动外联均值流量（流入和流出）。

- 流量Top排行：展示主动外联流量排名前10、前20或前50的资产信息。



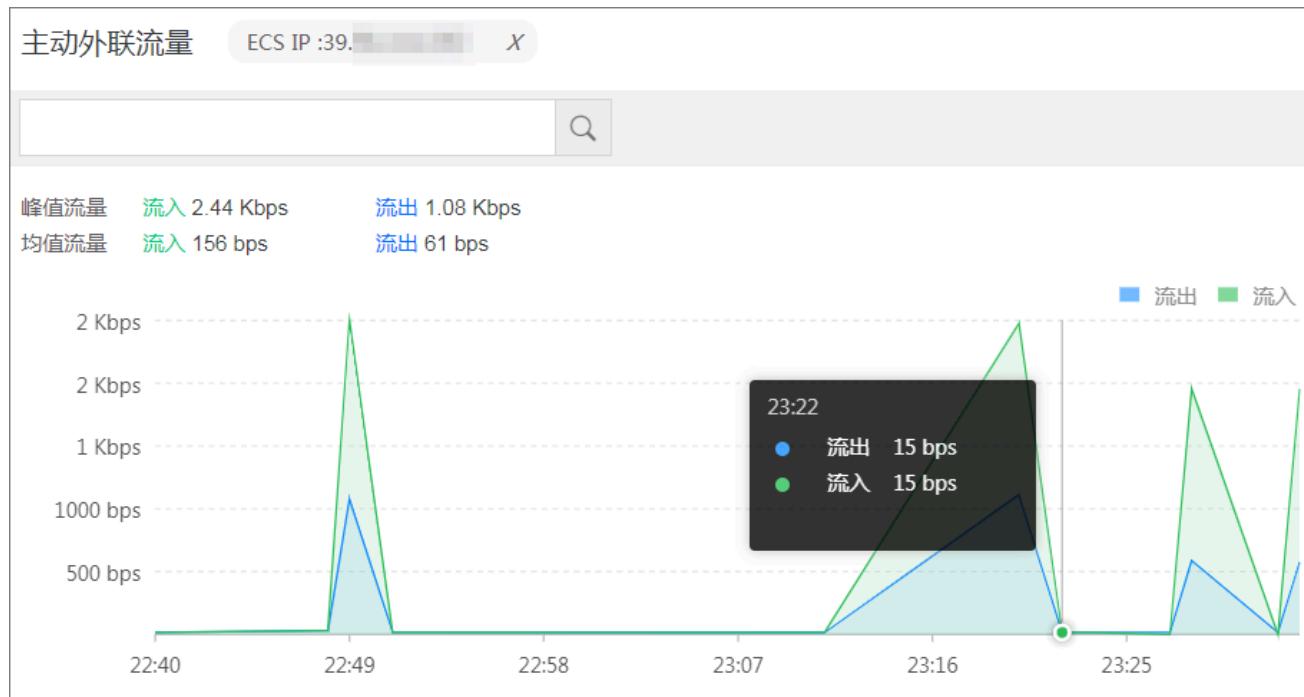
IP	类型	流入	流出	操作
██████████	ECS Public IP	1.94 Kbps	617 bps	详情
██████████	ECS Public IP	1.91 Kbps	589 bps	详情
██████████	ECS Public IP	1.91 Kbps	578 bps	详情
██████████	ECS Public IP	1.30 Kbps	419 bps	详情
██████████	ECS Public IP	929 bps	722 bps	详情

- 单击右上角Top 10/20/50下拉列表选择您需要查看的排名数量。



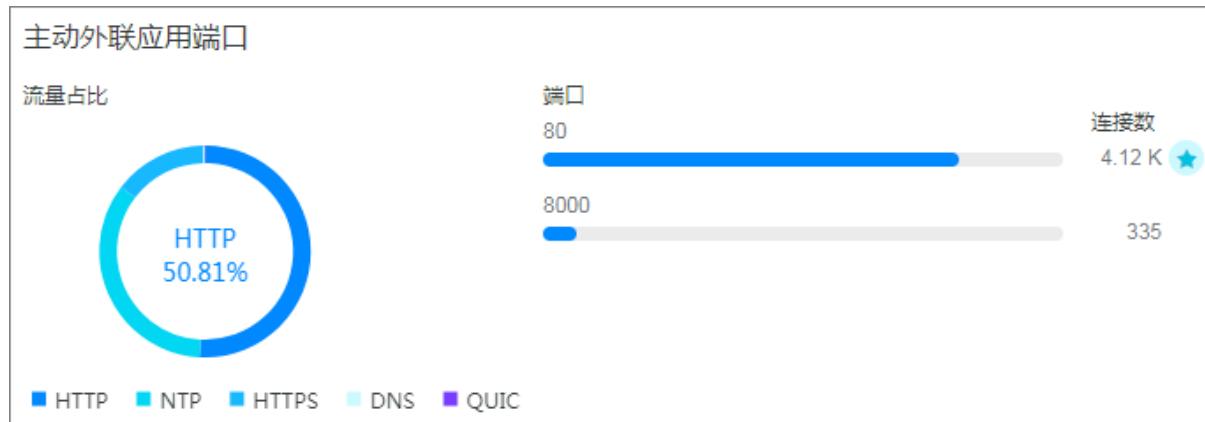
IP	类型	流入	流出	操作
██████████	ECS Public IP	1.94 Kbps	617 bps	Top 10

- 定位到单个Top资产并单击操作栏的详情可展示该资产的主动外联流量曲线图。

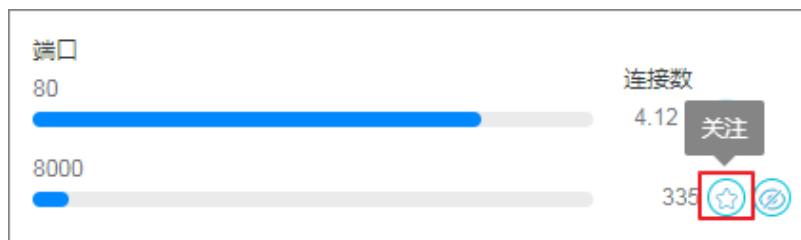


查看主动外联应用端口数据

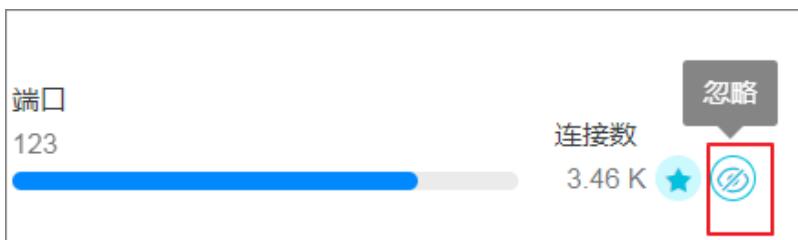
您可在主动外联应用端口区域查看主动外联应用端口数量和对应的连接数、应用类型和流量占比等数据。



- 单击端口连接数右侧的关注/取消关注按钮，被关注的端口信息将显示在主动外联资产对话框的已关注目的端口列表中。

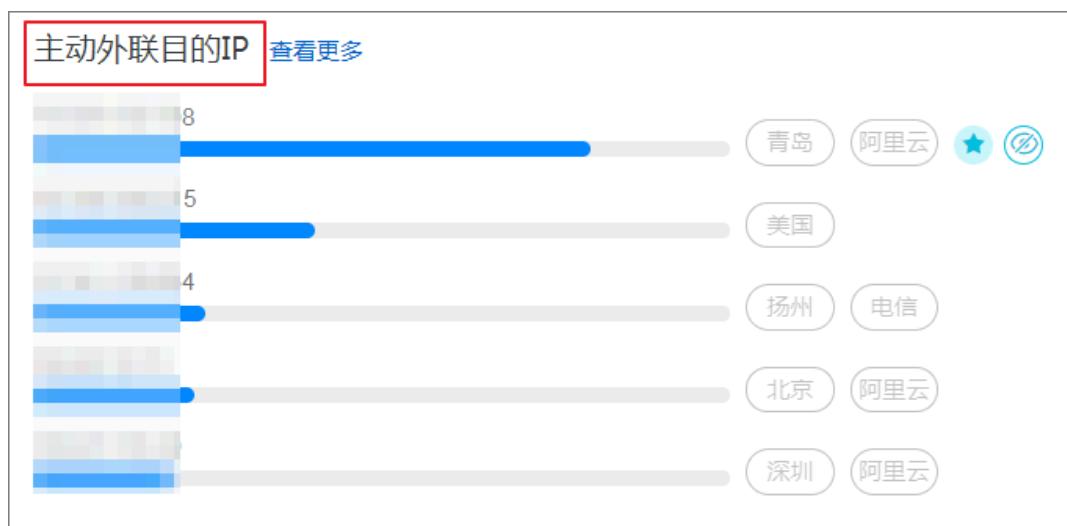


- 单击端口连接数右侧的忽略按钮，被关注的端口信息将从主动外联应用端口区域删除。



查看主动外联目的IP

在主动外联IP区域可查看主动外联流量访问的目的IP地址信息。



- 单击查看更多可跳转到主动外联资产列表页面，您可在该页面查看主动外联资产的IP地址信息、连接次数、已关注和已忽略的主动外联资产信息、或对单个资产进行搜索。

- 单击目的IP地址右侧的关注可将该资产添加到主动外联资产页面的已关注列表中。
- 单击目的IP地址右侧的取消关注，该资产信息将从已关注列表中删除。

- 单击目的IP地址右侧的忽略可将该资产添加到主动外联资产页面的已忽略列表中。



说明:

被忽略的IP地址将不再纳入主动外联资产检测范围内。

查看和处理主动外联未授权域名

您可在主动外联未授权域名区域查看主动外联未授权域名的总数量和恶意域名数量、域名信息、访问IP地址等资产信息。

主动外联未授权域名				恶意域名 0 / 6
域名 <input type="text"/> <input type="button" value=""/>	访问者IP <input type="text"/> <input type="button" value=""/>	恶意与否 <input type="button" value=""/>	操作	
upd. <input type="text"/>	3. <input type="text"/> , ...	非恶意	取消关注 忽略	
s3. <input type="text"/>	1. <input type="text"/>	非恶意	取消关注 忽略	
lab. <input type="text"/>	4. <input type="text"/>	非恶意	关注 忽略	

- 单击操作栏的关注，被关注的域名将显示在主动外联资产页面已关注的目的域名列表中。
- 单击操作栏的取消关注，该资产信息将从已关注列表中删除。
- 单击操作栏的忽略可将该资产添加到主动外联资产页面的已忽略列表中。



说明:

被忽略的域名将不再纳入主动外联资产检测范围内。

查看主动外联风险事件

您可在主动外联风险事件区域查看主动外联风险事件的事件名称、主机IP、事件数、危险等级和最近发现时间等信息。

主动外联风险事件					
事件名	主机IP <input type="text"/> <input type="button" value=""/>	事件数	危险等级 <input type="button" value=""/>	最近发现时间	动作 <input type="button" value=""/>
木马后门通信	<input type="text"/>	93	高危	2018-12-20 00:21	告警

3 互联网访问活动

云防火墙互联网入方向访问模块展示您资产入方向正常流量和异常流量的概览信息。

互联网入方向访问展示了入方向流量的开放应用、开放端口、开放公网IP地址和入方向流量访问的云产品信息。

操作步骤

1. 登录[云防火墙管理控制台](#)。

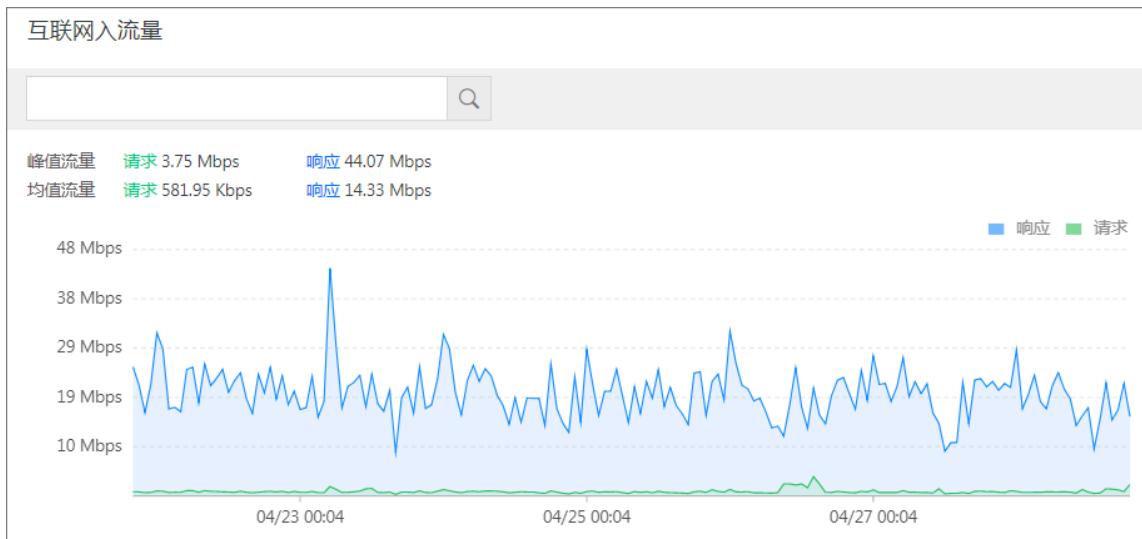
2. 定位到网络流量分析 > 互联网访问活动。

您在互联网访问活动页面可以进行以下操作：

- 查看互联网访问活动的概览信息，包括开放应用、开放端口、开放公网IP、入流量访问的云产品公网IP和开放端口总数量和对应的风险项数量。

开放应用	开放端口	开放公网IP	云产品
5 风险 11 全部	78 风险 189 全部	139 风险 267 全部	公网SLB 0 公网IP 0 开放端口

- 查看互联网入流量的峰值和均值流量数据，并查看选择时间范围内对应的入流量数据。



- 看到流量排名前10/20/50位的流量数据和相关信息，包括流量的IP地址、类型、请求和响应的流量大小。

流量Top排行		Top 50	2019-04-28 19:00		
IP		Top 50	请求 ↓	响应 ↓	操作
██████████	Top 50	548.29 Kbps	15.30 Mbps	查看日志	
██████████	Top 20	57.23 Kbps	68.09 Kbps	查看日志	
██████████	Top 10	ECS Public IP	28.48 Kbps	27.49 Kbps	查看日志
██████████		ECS Public IP	28.46 Kbps	27.49 Kbps	查看日志
██████████		ECS Public IP	28.39 Kbps	27.36 Kbps	查看日志
██████████		ECS Public IP	28.32 Kbps	27.37 Kbps	查看日志
██████████		ECS Public IP	28.24 Kbps	27.26 Kbps	查看日志

单击查看日志可跳转到流量日志页面，您可在流量日志中查看到所有互联网入方向流量的详细信息。

- 查看互联网流量日志详情列表，包括入流量开放应用、开放端口、开放公网IP、流量的基础信息、以及入流量访问的云产品的基本信息。

开放应用									
应用		协议		端口		公网IP数		端口总明细数	
全部风险评估		全部安全建议		全部应用		端口:请输入		7日流量占比	
应用	协议	端口	公网IP数	端口总明细数	7日流量占比	风险评估	安全隐患	安全建议	操作
FTP_DATA	tcp	9024,9046 	2	2	<0.1% 	高危 	暴力破解, 僵尸, 溢出, 后门	 检查	访问详情
Unknown	tcp	80,443  123个 	157	5079	99.9% 	低危 	-	 未知	访问详情
HTTP	tcp	80,90  89个 	156	1807	<0.1% 	低危 	-	 检查	访问详情
RDP	tcp	1001,8092  91个 	139	2596	<0.1% 	低危 	暴力破解	 检查	访问详情

4 VPC访问活动

云防火墙VPC访问活动模块展示您VPC专有网络之间的流量信息，帮助您实时获取VPC网络流量信息，及时发现和排查异常流量，从而更快地发现和检测出攻击。VPC访问活动页面中展示的信息包括VPC间流量访问TOP排行、VPC间会话TOP排行、流量访问的开放端口和资产信息等。

背景信息

云防火墙提供的VPC防火墙可以有效防御异常流量，VPC防火墙捕获到的所有VPC间流量信息都会展示在VPC访问活动页面。

操作步骤

1. 登录[云防火墙管理控制台](#)。
2. 定位到[网络流量分析 > VPC访问活动](#)。
3. 选择待查看的目标VPC网络区域，展示VPC网络间的流量信息。

The screenshot shows the 'VPC traffic analysis' page. The top navigation bar includes 'Cloud Firewall', 'Network Traffic Analysis', 'Active External Traffic', 'Internet Traffic Analysis', 'VPC Traffic Analysis' (which is highlighted in blue), 'Inbound Inspection', 'IPS Scan Analysis', and 'Full Activity Search'. Below the navigation is a search bar with dropdowns for 'VPC' and 'All VPC Edge Firewalls'. A note below the search bar says '提示：下方以 % 为 % 为代理网段及会话'. The main content area shows a list of VPC peers with their names and status. On the right, there is a 'Traffic Top Ranking' section with dropdowns for 'IP', 'Inbound', 'Outbound', and 'Operation', and a note 'No data'.

您在VPC访问活动页面，可以进行以下操作：

- 查看VPC专有网路入方向、出方向流量的峰值和均值流量数据，并查看选择时间范围内对应的入方向、出方向流量数据。
- 查看流量排名前10/20/50位的流量数据和相关信息，包括流量的IP地址，流入和流出数据。
- 查看VPC间会话的流量排行数据和相关信息，包括流量排行、IP会话、IP会话数、流量和端口数据。

在VPC间会话TOP排行列表中，单击查看占比栏的查看，可展示该会话中端口占比的详细数据。

- 查看所有开放端口占比信息。
- 查看VPC间流量日志详情列表，包括VPC间流量访问的开放端口和资产的基本信息。

The screenshot shows the 'Open Port Analysis' page. The top navigation bar includes 'Cloud Firewall', 'Network Traffic Analysis', 'Active External Traffic', 'Internet Traffic Analysis', 'VPC Traffic Analysis', 'Inbound Inspection', 'IPS Scan Analysis', and 'Full Activity Search'. Below the navigation is a search bar with dropdowns for 'VPC', 'All VPC Edge Firewalls', 'Protocol', 'Application', 'Risk Assessment', and a search input field. The main content area shows a table with columns for 'Local Open Port', 'Protocol', 'Application', 'Traffic', 'Request Count', 'Local Asset IP', 'Risk Assessment', and 'Operation'. A note at the bottom of the table says 'No data'.

5 入侵检测

云防火墙入侵检测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。

操作步骤

1. 登录[云防火墙控制台](#)。
2. 单击导航栏网络流量分析打开网络流量分析页面。
3. 单击入侵检测打开入侵事件列表。

风险级别	事件名称	资产类型	实例ID/名称	受影响资产IP	发生时间	处理状态	操作
高危	Mining behavior ...	ECS	12345678901234567890	192.168.1.100	2019-04-28 19:15	已止血	一键防御 忽略 详情
高危	Mining behavior ...	ECS	12345678901234567890	192.168.1.100	2019-04-28 16:03	已止血	一键防御 忽略 详情
高危	Mining behavior ...	ECS	12345678901234567890	192.168.1.100	2019-04-28 16:02	已止血	一键防御 忽略 详情

- 您可在入侵检测列表中查看入侵事件的详细信息，如风险级别、受影响资产IP和事件处理状态等信息。
- 可通过筛选风险级别、处理状态、检测时间范围或输入实例IP搜索单个相关入侵事件。



- 如果您判断入侵事件为正常活动，可单击该事件操作栏的忽略。



说明:

标记为忽略的入侵事件将从入侵事件列表中移除，云防火墙后续也将不会再对该事件进行告警。

- 单击操作栏详情打开该事件的详情页面，查看入侵事件的详细信息和对应的安全建议。您还可以在事件详情页面开启/关闭入侵防御功能。



说明:

一键防御开关不对单个事件进行控制。开启/关闭一键防御将会开启/关闭整个云防火墙的入侵防御功能。

6 IPS阻断分析

云防火墙IPS阻断分析页面为您实时展示云防火墙阻断流量的源区域、目的IP、阻断应用、阻断来源和阻断事件详情等信息。

您可查看主机1小时、1天、7天、1个月内和自定义时间范围内的阻断活动情况。可设置的自定义时间范围为6个月内。

IPS阻断分析页面包含以下数据：

- 方向：被阻断流量的方向，云防火墙支持出/入方向流量检测。
- 时间范围：可筛选不同的时间段，定位到特定时间段内的IPS阻断流量数据。
- 被阻断的源区域TOP：显示被阻断流量的源区域地理位置分布图、阻断数量最高的前9名地区的地区名称和百分比。
- 阻断目的IP：显示阻断数量排名前5名的阻断流量的目的IP址。
- 被阻断的应用TOP：显示阻断数量排名前5名的阻断应用名称及其占比数。
- 阻断来源TOP：显示阻断数量排名前5名的阻断来源名称及其占比数。
- 阻断事件列表：显示阻断事件的详细信息。您可通过来源、出入方向、防御状态和自定义时间范围来搜索阻断事件。

操作步骤

1. 登录[云防火墙控制台](#)。
2. 单击导航栏网络流量分析打开网络流量分析页面。
3. 单击IPS阻断分析打开IPS阻断分析页面，查看1小时、1天、7天、1个月内或自定义时间范围内的出/入方向阻断活动情况。

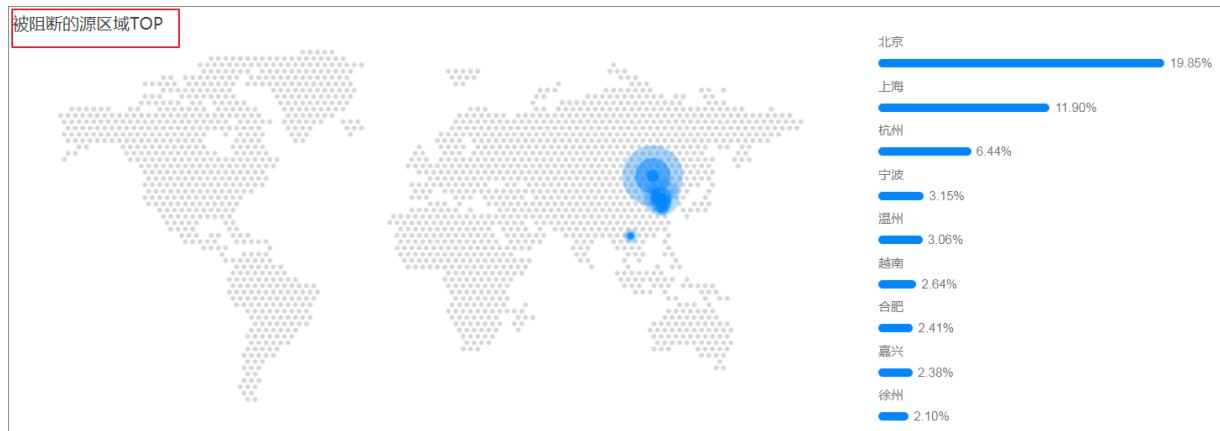


在方向模块中单击入方向或出方向，显示对应时间范围内入方向/出方向被阻断流量相关的数据。

4. 在阻断活动页面查看排名前九的阻断源区域信息及占比、阻断目的IP地址、占比排名前四的被阻断应用和阻断来源类型。

查看被阻断的源区域TOP

您可在被阻断的源区域TOP区域查看被云防火墙IPS功能阻断的出/入方向流量排名前9的来源区域及其占比。



查看阻断目的IP

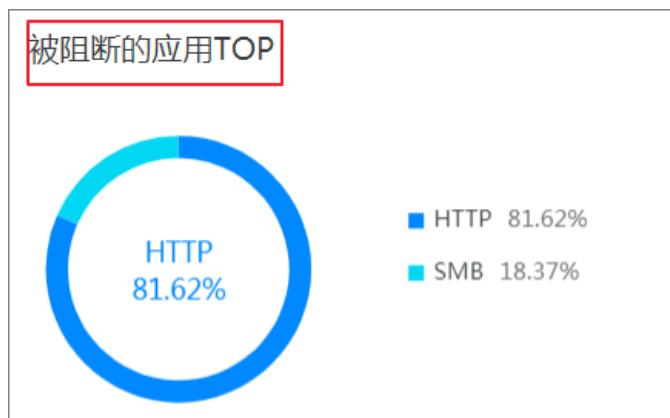
您可在阻断目的IP区域查看被云防火墙IPS功能阻断的出/入方向流量的目的IP地址信息。



单击阻断目的IP地址栏右侧的查看日志可跳转到云防火墙日志页面。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、动作类型等详细信息。

查看被阻断的应用TOP

您可在被阻断的应用TOP区域查看被云防火墙IPS功能阻断的出/入方向流量占比最高的应用类型。



查看阻断来源TOP

您可在被阻断的应用TOP区域查看云防火墙各个IPS功能模块阻断的流量占比。



查看阻断事件详情列表

您可在IPS阻断分析页面的阻断事件列表中查看所有阻断事件的详细信息，包括事件的风险级别、事件数量、防御状态、源/目的IP地址等信息。

风险级别	事件名称	事件数	防御状态	操作
高危	木马后门通信	17113	观察	查看详情
高危	ThinkPHP V5...	1	观察	查看详情
高危	Struts2远程命...	2	观察	查看详情

- 您可在搜索栏通过筛选风险级别、来源、方向和时间范围等定位到单个事件。

全部风险级别

全部判断来源

全部方向

- 单击动作栏的详情可打开阻断事件的详情页面，查看事件描述等详细信息。

事件详情	
事件名称	木马后门通信
防御状态	告警
首次发现时间	2018-12-12 15:02
最近发现时间	2018-12-20 00:00
事件数	18009
源IP	██████████
目的IP	██████████:28
方向	出方向
判断来源	基础防御
事件描述	检测到Typhoon中控木马的通信，可能系统已被入侵。Typhoon为一种DDos木马，常被用来进行DDos攻击



说明:

云防火墙检测到高危等级的告警事件后，请及时确认您已开启[入侵防御策略](#)。

7 全量活动搜索

全量活动为您实时展示云防火墙保护范围内所有主机的全部流量访问趋势数据、入方向/出方向TOP应用访问的来源地区及其占比数据、TOP会话地址及其占比数据等。

操作步骤

1. 登录云防火墙控制台。
2. 单击导航栏网络流量分析打开网络流量展示页面。

3. 单击全量活动搜索页面，查看15分钟、1小时、4小时、1天、7天内或自定义时间范围内的全部威胁活动情况和趋势图。

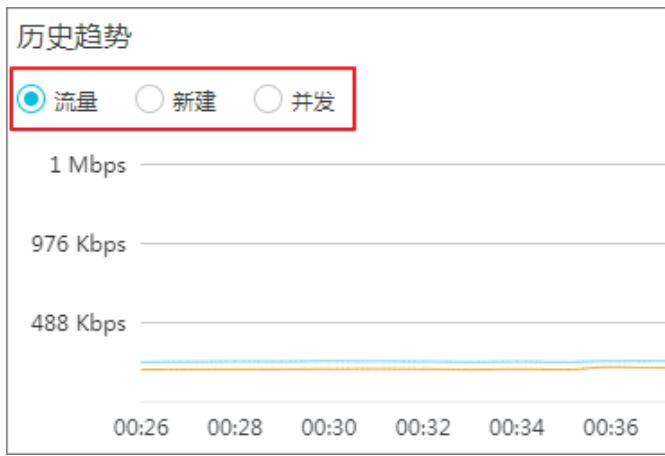
说明:

自定义时间范围不限。

- 单击条件下拉框选择对应的查询条件并输入/选择该条件的详细信息，查询对应的流量访问活动的历史趋势。单击重置清除设置的搜索条件。



- 在历史趋势模块，您可查看选定时间范围内公网流入/流出流量趋势图、新建连接数趋势图以及并发连接数趋势图。



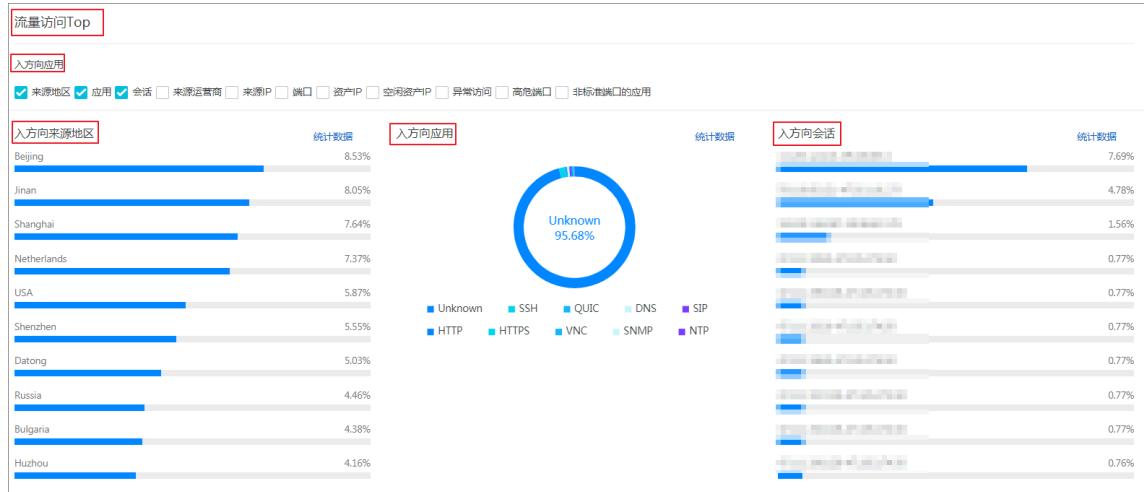
单击流量、新建或并发可对应切换到流量趋势/新建连接数趋势/出入方向并发流量趋势。



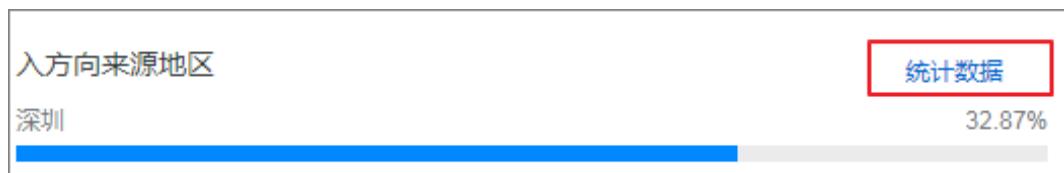
说明:

趋势图显示15分钟、1小时、4小时、1天、7天内或自定义时间范围内的流量数据。自定义时间范围不限。

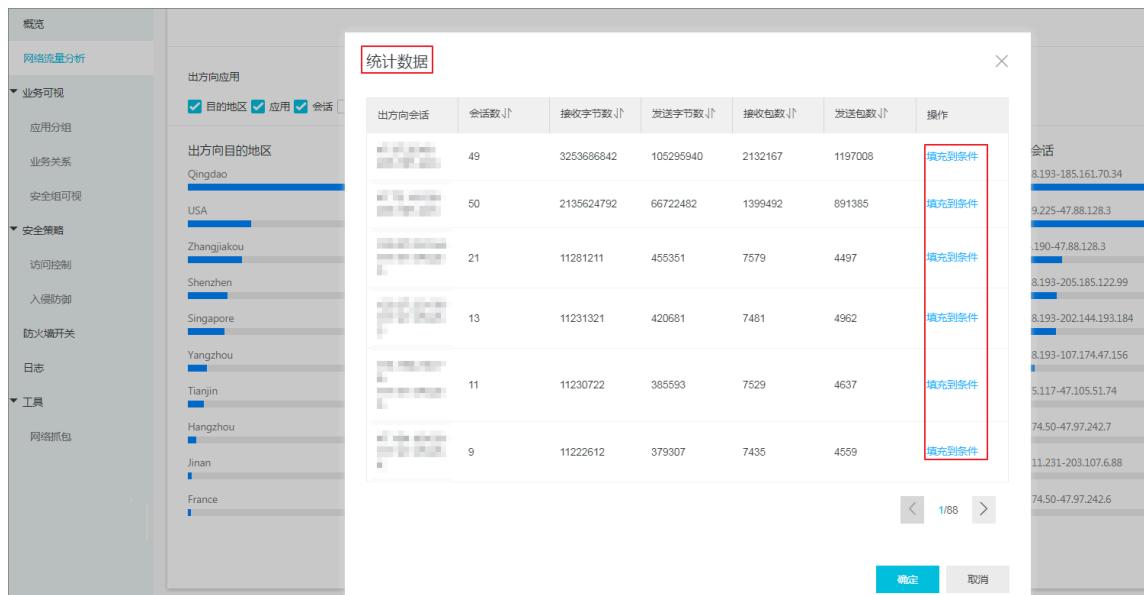
- 在流量访问TOP模块，您可查看出/入方向流量访问排名前十的区域、应用类型及其占比数。



- 在流量访问TOP模块单击统计数据打开对应的出/入方向、出/入来源或出/入应用统计数量列表，查看详细统计数据。



- 单击填充到条件可将对应条件自动填充到全量活动搜索条件栏。历史趋势和流量访问TOP模块将显示填充条件的相关趋势图。



8 智能策略下发

云防火墙基于互联网访问和主动外联的智能策略功能，为您提供高危服务隔离（外对内）和蠕虫防御（内对外）模式的安全策略配置，为您推荐更加安全的ACL策略，帮助您防御网络和主机的安全威胁。

高危服务隔离

云防火墙的智能策略功能会根据互联网访问检测的安全威胁，为您提供最佳的ACL策略。例如，如果互联网暴露的IP资产开启了危险性较高的服务（SSH, RDP等），且服务存在被爆破、入侵的风险，智能策略会推荐您配置策略，仅放行来自常用登录地区且登录状态正常的互联网请求，拒绝其他登录地区的互联网请求，从而降低网络被攻击的风险。

1. 登录[云防火墙管理控制台](#)。
2. 定位到[网络流量分析 > 互联网访问活动 > 开放公网IP列表](#)。

3. 定位到目标公网IP，单击最右侧操作栏下的智能策略。

在智能策略页面，会展示推荐智能策略，包括对于用户IP及端口的放行和拒绝策略。

4. 在智能策略页面，选择执行以下操作。

- 单击展开，可查看推荐智能策略的理由。

您可查看到曾有大量恶意IP尝试访问用户IP的SSH服务。

智能策略

推荐智能策略 方向: 外到内

优先级	访问源	访问目的	协议/应用/端口	动作
1	① [REDACTED]	② [REDACTED]	TCP/SSH/22/22	✓ 放行
2	① [REDACTED]	② [REDACTED]	TCP/SSH/22/22	✗ 拒绝

推荐理由 - 近一周IP外联概况 收起 ^

开放公网IP: [REDACTED]

端口	应用	恶意IP数	正常IP数
445	SMB	218	266
3389	Unknown,RDP	131	180
22	SSH	233	124
80	HTTP	171	105
3306	Unknown,HTTP	8	83

下发现策略 取消

- 单击下发现策略，即可在安全策略 > 访问控制 > 互联网边界防火墙 > 外对内页面，查看到配置的防御策略。



说明:

执行下发现策略前，请确保您已知悉推荐策略的含义，及该策略对业务可能造成的影响。

您可对下发现的策略进行编辑、删除、插入和移动。

蠕虫防御

当用户的主机遭受蠕虫攻击时，会受蠕虫恶意代码的控制，对恶意网站的域名发出请求。若云防火墙检测到您的主机发起了外联请求，会为您推荐配置策略，禁止主机对恶意域名的外联访问，防止主机下载恶意程序和遭受控制或恶意挖矿的风险。

1. 登录[云防火墙管理控制台](#)。
2. 定位到[网络流量分析 > 主动外联活动 > 外联域名列表](#)。

3. 定位到目标外联域名，单击最右侧建议操作栏下的智能策略。

在智能策略页面，会展示推荐智能策略：对于主机外联的拒绝策略。

4. 在智能策略页面，选择执行以下操作。

- 单击展开，可查看推荐智能策略的理由。

您可查看到用户主机曾对恶意源发起过很多次的恶意请求。

The screenshot shows the 'Smart Strategy' interface. At the top, it says '推荐智能策略 方向: 内到外'. Below is a table with columns: 优先级 (Priority), 访问源 (Access Source), 访问目的 (Access Destination), 协议/应用/端口 (Protocol/Application/Port), and 动作 (Action). One row is shown with Priority 1, Source IP [REDACTED], Destination IP [REDACTED] (www), Protocol TCP/HTTP/ANY, and Action 拒绝 (Reject). Below the table, it says '推荐理由 - 近一周IP外联概况 收起 ^'. It shows a table with columns: 资产私网IP (Asset Private IP), 资产公网IP (Asset Public IP), 资产类型 (Asset Type), 实例ID/名称 (Instance ID/Name), and 请求次数 (Request Count). The last column shows a value of 26, which is highlighted with a red box. At the bottom are buttons for '下发策略' (Deploy Strategy) and '取消' (Cancel).

- 单击下发策略，即可在安全策略 > 访问控制 > 互联网边界防火墙 > 内对外页面，查看到配置的防御策略。



说明:

执行下发策略前，请确保您已知悉推荐策略的含义，及该策略对业务可能造成的影响。

您可对下发的策略进行编辑、删除、插入和移动。