ALIBABA CLOUD

Alibaba Cloud

云防火墙
最佳实践

文档版本：20220518

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.云防火墙最佳实践

本文从版本选择、开启资产保护、配置访问控制策略等方面提供指导。

- 开启公网资产保护
- 开启VPC资产保护
- 开启云防火墙保护和入侵防御拦截模式
- 云防火墙数据库防御最佳实践
- 云防火墙保护堡垒机最佳实践
- 防御挖矿程序最佳实践

如何选择适合我的云防火墙版本

云防火墙分为高级版、企业版和旗舰版三个版本，每个版本支持的功能和资产/带宽扩展规格不同，详细信息参见功能特性。

开启公网资产保护

互联网边界防火墙帮助您检测和防护云上公网IP资产间的通信流量。只有为资产开启互联网边界防火墙后，您才可以使用云防火墙分析和控制云上主机的互联网访问流量。

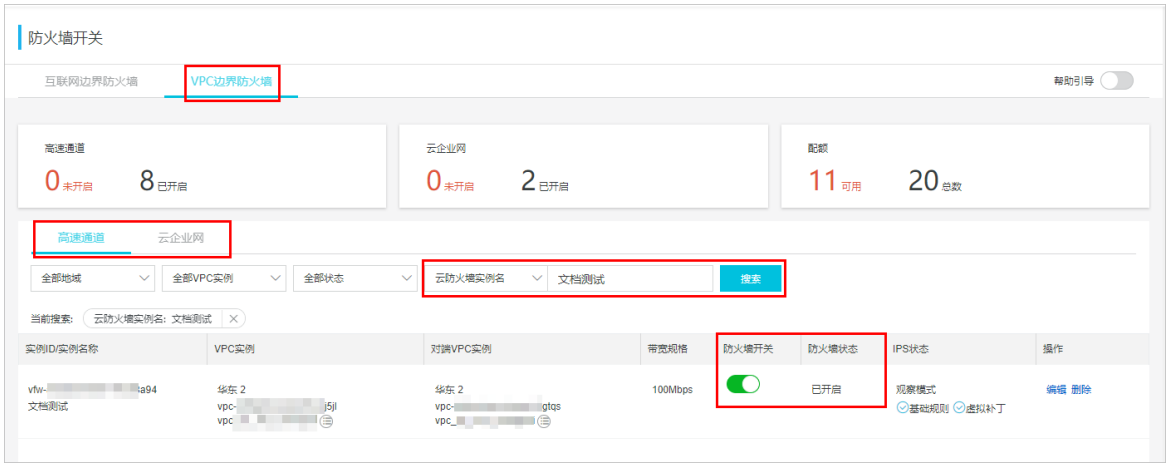
您可以在云防火墙控制台的**防火墙开关**页面的**互联网边界防火墙**页签，对指定的公网IP资产开启互联网边界防火墙。

开启VPC资产保护

VPC边界防火墙能够检测和统计已连通的VPC间的通信流量数据，帮助您发现和排查异常攻击。开启VPC边界防火墙之前，您需要先创建VPC边界防火墙。

步骤说明如下：

1. 在云防火墙控制台的**防火墙开关**页面的**VPC边界防火墙**页签，选择为云企业网实例或高速通道实例创建VPC边界防火墙。
2. 为云企业网实例或高速通道实例开启VPC边界防火墙。



开启云防火墙保护和入侵防御拦截模式

云防火墙服务开通后，您可在**防火墙开关**页面将资产全部开启保护，在**入侵防御**页面中开启**拦截模式**，即可全面保护您的资产安全。

配置外到内的访问策略

在外对内流量的访问策略中，不要对公网IP全部端口开放访问，对外仅开放必要的互联网IP和端口，其他端口请全部设置为**拒绝**。

1. 放行需要对外开放的应用或端口。

   在**访问控制**页面**外对内**流量列表中，依据业务需求，将源IP地址配置为`0.0.0.0/0`或特定源，也可选择地址簿中系统默认配置的地址簿**ANY**（`0.0.0.0/0`）或特定源，目的选择要放开的IP或地址簿中的特定目的，协议选择**ANY**或者依据业务需要选择对应协议，动作选择**放行**。

   例如，80端口为Web服务，对全网开放，因此访问源为0.0.0.0/0；1433、3389端口分别为SqlServer、RDP服务，对特定源开放，因此访问源为特定源。

2. 将除放行策略之外的流量设置为拒绝放行。

   在**访问控制**页面**外对内**流量列表中，将源IP地址配置为`0.0.0.0/0`或地址簿中系统默认配置的地址簿**ANY**（`0.0.0.0/0`），目的设置为**ANY**，协议设置为**ANY**，动作选择**拒绝**。

配置内到外的访问策略

内对外流量建议不要开放全部放行的策略，只对到必要的外部IP或域名的访问开启放行，其他访问全部设置为**拒绝**。

1. 放行需要对外访问的应用或端口。

   在**访问控制**页面**内对外**流量列表中，依据业务需求，将源IP地址配置为`0.0.0.0/0`或特定源，也可选择地址簿中系统默认配置的地址簿**ANY**（`0.0.0.0/0`）或特定源，目的选择要放开的域名或IP或地址簿中的特定目的，协议选择ANY或者依据业务需要选择对应协议，动作选择放行。

2. 将除放行策略之外的流量设置为**拒绝**放行。

   在访问控制页面内对外流量列表中，将源IP地址配置为`0.0.0.0/0`或选择地址簿中系统默认配置的地址簿**ANY**（`0.0.0.0/0`），目的设置为ANY，协议设置为ANY，动作选择**拒绝**。

2.云防火墙中控蠕虫防御最佳实践

蠕虫病毒是当前云上业务面临的主要威胁。它们利用服务器的漏洞在网络上扩散感染，执行各种恶意行为给用户资产和业务带来严重威胁。云防火墙针对蠕虫的攻击链路进行分层防御，可以检测和拦截多种蠕虫及其变种。同时可以基于云上风险态势，实时更新和扩展对最新蠕虫的检测和拦截能力。

蠕虫的威胁

蠕虫主要导致以下几种危害：

- 业务中断：蠕虫在感染主机后，可能会进行修改配置、停止服务等操作，导致主机宕机、业务中断等风险。
- 信息窃取：信息窃取类蠕虫，会将服务器上的数据打包回传，可能造成严重的信息泄漏、资源滥用。
- 监管封锁：蠕虫对外传播过程大量发包，可能导致IP被监管单位封禁，直接导致业务中断。
- 勒索：包含勒索功能的蠕虫通过对文件加密进行勒索，造成财产损失或导致数据丢失。

云防火墙解决方案

云防火墙针对蠕虫的攻击链路进行分层防御，可检测并拦截多种蠕虫及其变种。同时云防火墙也会基于云上风险态势，实时更新和扩展对最新蠕虫的检测和拦截能力。

典型的蠕虫类型如下：

- **DDG**：利用Redis漏洞及爆破进行传播，感染后利用计算资源挖矿。
- **WannaCry**：利用Windows漏洞进行传播，感染后主要进行勒索。
- **BillGates**：利用爆破及应用漏洞进行传播，感染后构建僵尸网络进行DDoS攻击。

代表案例-DDG蠕虫

DDG是一种主要利用Redis漏洞及爆破等方式进行传播的活跃蠕虫，被感染的主机被加入僵尸网络后受控进行虚拟货币挖矿。

DDG蠕虫影响范围

- 存在SSH弱口令的服务器。
- 存在漏洞的Redis或其他类型的数据库服务器。

DDG蠕虫的主要危害

- 业务中断：感染DDG蠕虫的主机主要被用来挖矿，挖矿会大量占用服务器计算资源，可能导致服务不可用或正常业务的中断。
- 监管封闭：DDG蠕虫感染后会进一步扩散传播，可能会导致IP被监管单位封禁。

针对DDG攻击链的防御

云防火墙可针对DDG的攻击链进行实时检测和防御，从而阻断整个蠕虫的攻击和传播链路。

下图为云防火墙针对DDG攻击链的防御架构图：

云防火墙可提供以下四种防御类型：

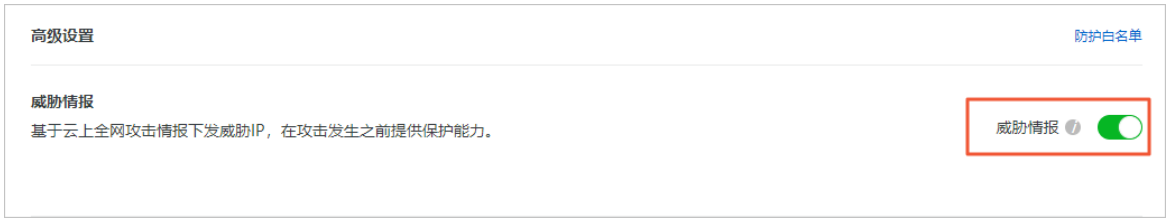
- **防护白名单**：云防火墙入侵防御模块不会对防护白名单中的流量进行拦截，加入到防护白名单的源/目的IP会被云防火墙视为可信流量并放行。
- **威胁情报**：云防火墙可扫描侦查威胁情报，并提供中控情报阻断。
- **基础规则**：支持恶意软件检测、中控通信拦截、后门通信拦截。
- **虚拟补丁**：针对漏洞利用的防护补丁，可实时防护热门的应用高危漏洞。

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 > 防护配置**。
3. 在**防护配置**页面**威胁引擎运行模式**模块选择**拦截模式-宽松**。

4. 在**高级设置**模块中单击**防护白名单**，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。

5. 在**威胁情报**模块中单击开启**威胁情报**。



6. 在**基础防御**模块中单击开启**基础规则**。

7. 在**虚拟补丁**模块中单击**开启补丁**。

云防火墙的入侵防御策略配置的更多详细内容，请参见防护配置。

3.云防火墙数据库防御最佳实践

阿里云云防火墙入侵防御功能可防御常见类型的数据库被入侵。

数据库安全防御需求

数据库是企业管理和存储数据资源的系统，数据库中存放大量有价值和敏感的信息，所以数据库也是黑客攻击的主要目标。数据库的安全对业务的正常运行和企业的发展有着重要的影响。

数据库面临的主要安全威胁有：

- 暴力破解

  可直接导致数据库被入侵。

- 数据库应用漏洞

  如数据库CVE漏洞，可导致数据库应用Dos、恶意命令执行、信息泄露等。

- 恶意文件读写、命令执行

  如高风险存储过程或函数调用，可导致恶意命令执行、文件读写等。

- 信息窃取、拖库

  攻击者对窃取的数据进行转售或用于诈骗，造成商业损失。

阿里云云防火墙解决方案

云防火墙入侵防御功能可针对以下数据库类型提供安全防御：

- MySQL
- MSSQL
- Redis
- PostgreSQL
- MemCache
- MongoDB
- Oracle

云防火墙如何防御数据库入侵

阿里云安全团队在数据库攻防实战中进行了长期的跟踪和研究，积累了大量的攻防经验，并转化为防御规则，有效提升了云防火墙对数据库安全的防御能力。

云防火墙对数据库面临的风险提供多点防御，保障数据库的正常运行。如：

- 暴力破解

  威胁情报：云防火墙威胁情报功能可感知全网攻击态势，提前阻断扫描、入侵行为。

- 数据库应用漏洞

  虚拟补丁：虚拟补丁功能可对数据库的高危漏洞进行重点防御。

- 恶意文件读写、命令执行

  基础规则：基础规则功能可对系统文件操作、写入webshell、存储过程/UDF等恶意操作进行实时阻断。

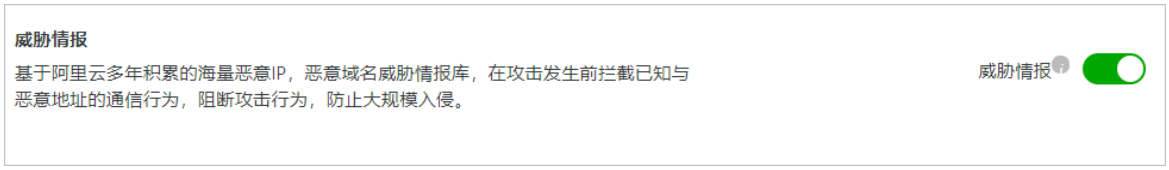
- 信息窃取、拖库

  高风险SQL阻断：由入侵防御基础规则功能提供，可对拖库操作进行实时阻断，防止信息被窃取。

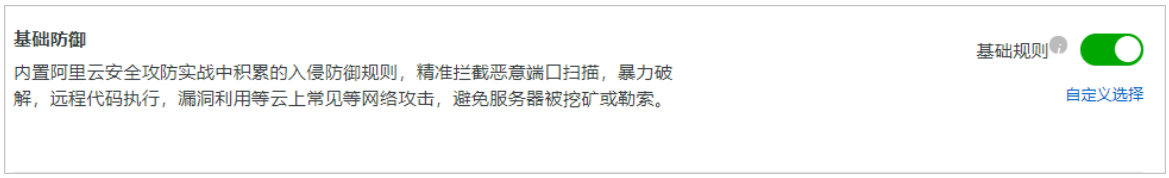
操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**攻击防护 > 防护配置**。
3. 在**防护配置**页面，定位到**威胁引擎运行模式**区域，选中**拦截模式-宽松**。

4. 在**威胁情报**区域，打开**威胁情报**开关。



5. 在**基础防御**区域，打开**基础规则**开关。



6. 在**虚拟补丁**区域，打开**开启补丁**开关。

4.系统安全防御最佳实践

系统安全是业务安全稳定运行的重要因素之一，随着网络安全对抗的愈演愈烈，规模化的自动化攻击、蠕虫、勒索、挖矿、APT等攻击形式逐渐增多，给系统的安全运行带来了很大的挑战。

默认安装的系统存在以下安全威胁，易导致系统被入侵：

- 系统配置不合理
  - 端口开放不当：开放不必要的服务和应用，增加攻击面。
  - 弱口令：易遭受暴力破解，造成系统被入侵。
  - 策略配置：系统安全策略弱或未配置安全策略。
- 系统漏洞或补丁缺失
  - 命令执行漏洞：任意命令执行，导致系统被入侵。
  - 拒绝服务漏洞：系统拒绝服务，造成业务中断。
  - 信息泄露漏洞：数据泄露。

代表案例-Samba远程代码执行

Samba是运行于Linux和Unix系统中实现SMB协议的软件，可以实现不同计算机之间提供文件及打印机等资源的共享服务。

Samba服务器软件存在远程执行代码漏洞。攻击者可以利用客户端将指定库文件上传到具有可写权限的共享目录，会导致服务器加载并执行指定的库文件。

CVE：CVE-2017-7494。

漏洞影响范围：

- 安装Samba软件的Linux或Unix系统。
- Samba版本：4.6.4、4.5.10、4.4.14。

漏洞主要危害：

- 命令执行：通过远程代码执行，造成服务器的沦陷和信息泄露。
- 业务中断：存在利用此漏洞进行传播的蠕虫SambaCry，成功感染后会进行挖矿，大量占用服务器计算资源，从而可能导致服务不可用或正常业务的中断。

典型案例：SMB远程代码执行

SMB Server是Windows操作系统中默认安装的一个服务器协议组件。Windows SMB中存在远程代码执行漏洞，远程攻击者可通过发送特制的数据包至SMBv1服务器利用该漏洞执行代码。

CVE：CVE-2017-0143。

漏洞影响范围：

- Microsoft Windows Server 2016。
- Microsoft Windows server 2012 Gold。
- Microsoft Windows Server 2012 R2。
- Microsoft Windows Server 2008 R2 SP1。
- Microsoft Windows Server 2008 SP2。

主要危害：

- 命令执行：通过远程代码执行，造成服务器的沦陷和信息泄露。

- 数据丢失：存在利用此漏洞进行传播的蠕虫，如WannaCry，成功感染后会加密文件并造成信息泄露。

阿里云云防火墙如何防御系统入侵

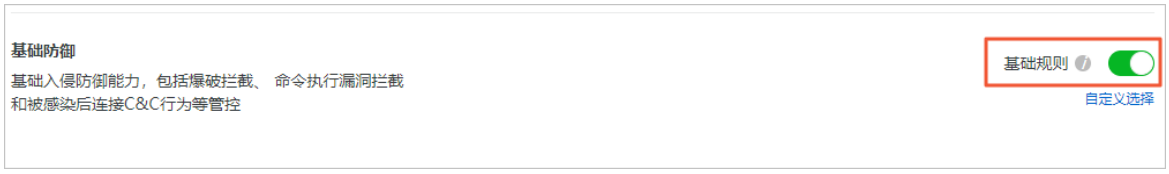
阿里云安全在系统漏洞攻防实战中进行了长期的跟踪和研究，积累了大量的攻防经验，并转化为防御规则，有力提升了云防火墙对系统安全的防御能力。

云防火墙对系统面临的所有风险进行多点防御，保障系统的正常运行。

- **暴力破解**：云防火墙提供威胁情报入侵防御，可感知全网攻击态势，提前阻断扫描和入侵行为。
- **系统漏洞**：云防火墙提供系统漏洞入侵防御，对操作系统的高危漏洞进行重点防御。
- **其他攻击**：云防火墙提供基础规则防御，对其他类型系统攻击，如Shell反弹和系统文件泄露等提供检测和实时阻断。

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 > 防护配置**。
3. 在**防护配置**页面的**威胁引擎运行模式**区域选择**拦截**模式。
4. 在**防护配置**页面的**基础防御**区域中单击开启**基础规则**。



5. 在**防护配置**页面的**虚拟补丁**区域中单击**开启补丁**。

5.配置访问控制策略最佳实践

本文档介绍了访问控制策略的推荐配置方法。

访问控制实现原理

- **互联网边界防火墙**：
  - 原理：在互联网到所有云上资产的公网出入路径进行统一访问控制。
  - 配置页面：访问控制-内对外流量，访问控制-外对内流量。
  - 默认策略：默认全部放行。
- **主机防火墙/安全组**：
  - 原理：在每个ECS上存在主机防火墙/安全组，进行主机粒度的访问控制。
  - 配置页面：访问控制-内对内流量（只在企业版提供，高级版用户可以在安全组控制台配置）。
  - 默认策略：默认出方向全部放行，入方向全部拒绝。

推荐配置步骤

1. 完善互联网策略（**外-内流量**）配置。

   请参考以下配置逻辑：

   - 先将所有必要在互联网开放的端口放行，比如http/80、https/443服务等。
   - 将一些运维或高安全风险的端口有限放行，比如ssh/22、mysql/3306等端口，只给必要的源开放，其它默认拒绝，可以配合地址簿简化配置。
   - 默认禁止互联网上一些高危服务端口，比如smb/445端口等。
   - 配置Any到Any的默认拒绝策略，可以先配置成观察模式，配合流量日志观察无误后在修改为拒绝模式。
2. 将ECS的主机防火墙入方向流量全部设置为**允许**。

   请参考以下配置逻辑：

   到访问控制-内对内流量页面，选择包含测试ECS的策略组，配置源0.0.0.0/0到目的ECS的放行策略（主机防火墙/安全组默认入方向禁止所有访问，必须显式配置放行策略）

   > **说明** 访问控制-内对内流量页面只提供给企业版、旗舰版用户，高级版用户可以到ECS安全组控制台操作。
3. 验证策略是否满足需求。

   在**日志审计 > 流量日志**处查询所有流量放行、拒绝、观察情况，可以结合实际测试结果验证策略是否满足要求。
4. 完善互联网边界防火墙策略。

   验证没有误拦截情况后，可以考虑将Any到Any的默认策略从观察修改为拒绝，注意此步骤需要评估风险后再操作。

5. 将所有ECS主机防火墙入方向全部放通。

   请参考以下配置逻辑：

   - 在访问控制-内对内流量中的每个策略组，都添加一条0.0.0.0/0的策略。
   - 后续新购ECS，加入到已有安全组时无需再额外配置，如果加入到新建立的安全组，需要在内对内流量页面配置默认放行策略。

6. 检查所有业务的可用性。

   在日志-流量日志处可以查询所有流量放行、拒绝、观察情况，可以结合实际测试结果验证策略是否满足要求。

7. 配置主动外联访问控制策略（内-外流量）。

   请参考以下配置逻辑：

   - 对主动外联有访问控制需求时，可以在**访问控制 > 互联网边界防火墙 > 内对外**处配置。
   - 推荐只放行到特定目的域名/IP的请求，如外部API域名等。
   - 只放行到特定目的域名/IP的请求，如外部API域名等。
   - 默认拦截其它所有主动外联流量（可以先观察一段时间确认所有外联需求）。

6.配置外到内流量只允许访问某个端口的访问控制策略

云防火墙的外对内和内对外流量是指面向互联网的流量，也就是南北向流量。您可以通过云防火墙访问控制功能对南北向的访问控制策略进行自定义配置，从而实现对访问流量的精准控制、保护您的网络安全。

外对内和内对外流量的访问控制支持自定义IP地址簿简化配置流程，可有效减少策略数量，提高配置效率。

背景信息

假如ECS（主机） IP地址是10.1.1.1， EIP是200.2.2.2，需要设置外到内流量只允许访问主机的TCP 80端口。

> **说明** EIP即弹性公网IP，是可以独立购买和持有的公网IP地址资源。EIP详细介绍参见什么是弹性公网IP。

实施步骤

1. 在阿里云云防火墙控制台定位到**访问控制**功能的**外对内**页签。
2. 配置允许外到内流量访问主机的TCP 80端口。
   - 新增外对内策略中**源类型**选择**IP**，**访问源**输入 `0.0.0.0/0` 。
   - **目的类型**选择**IP**，**目的**输入 `200.2.2.2/32` 。
   - **协议类型**选择**TCP**。
   - **端口类型**选择**端口**，**端口**输入 `80/80` 。
   - **应用**选择**ANY**。
   - **动作**选择**放行**。
   - 输入**描述信息**。建议输入策略及其目的的描述。
3. 配置拒绝所有外部流量访问主机的外-内访问控制策略。
   - 新增外-内策略中**源类型**选择**IP**，**访问源**输入 `0.0.0.0/0` 。
   - **目的类型**选择**IP**，**目的**输入 `0.0.0.0/0` 。
   - **协议类型**选择**ANY**。
   - **端口类型**选择**端口**，**端口**输入 `0/0` 表示所有端口。
   - **应用**选择**ANY**。
   - **动作**选择**拒绝**。
   - 输入**描述信息**。建议输入策略及其目的的描述。
4. 策略配置完成后，确认第一条**放行80端口**策略优先级是高于第二条配置的**拒绝所有流量**策略的。

   > **说明** 调整策略优先级操作详见修改云防火墙访问控制策略的优先级。

后续操作

访问控制策略配置完成后，可以通过**访问控制**页面中的命中次数观察策略的命中情况；通过**流量日志**页面查看该策略命中的流量。

7.配置内到外流量只允许访问某个域名的访问控制策略

云防火墙的外-内和内-外流量是指面向互联网的流量，也就是南北向流量。您可以通过云防火墙访问控制功能对南北向的访问控制策略进行自定义配置，从而实现对访问流量的精准控制、保护您的网络安全。

背景信息

假如ECS（主机）IP地址是10.1.X.X，EIP是47.100.X.X，需要设置内-外流量只允许主机访问www.aliyundoc.com这个域名。

> **说明** EIP即弹性公网IP，是可以独立购买和持有的公网IP地址资源。EIP详细介绍参见什么是弹性公网IP。

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**的**内对外**页签，配置内对外流量只允许主机访问*www.aliyundoc.com*。

   创建策略时的配置信息如下：

   - **源类型**选择**IP**，**访问源**输入`47.100.X.X/32`。
   - **目的类型**选择**域名**，**目的**输入*www.aliyundoc.com*。
   - **协议类型**选择**TCP**。
   - **端口类型**选择**端口**，**端口**输入`0/0`。
   - **应用**根据域名的类型选择**HTTP**或**HTTPS**。
   - **动作**选择**放行**。
   - 输入**描述信息**。建议输入策略及其目的的描述。
4. 配置内对外流量放行DNS解析。

   创建策略时的配置信息如下：

   - **源类型**选择**IP**，**访问源**输入`47.100.X.X/32`。
   - **目的类型**选择**IP**，**目的**输入*0.0.0.0/0*。
   - **协议类型**选择**UDP**。
   - **端口类型**选择**端口**，**端口**输入`53/53`。
   - **应用**选择**ANY**。
   - **动作**选择**放行**。
   - 输入**描述信息**。建议输入策略及其目的的描述。
5. 将除放行策略之外的流量设置为**拒绝**。

   创建策略时的配置信息如下：

   - **源类型**选择**IP**，**访问源**输入`0.0.0.0/0`。
   - **目的类型**选择**IP**，**目的**输入`0.0.0.0/0`。

- **协议类型**选择**ANY**。
- **端口类型**选择**端口**，**端口**输入 `0/0` 。
- **应用**选择**ANY**。
- **动作**选择**拒绝**。
- 输入**描述信息**。建议输入策略及其目的的描述。

6. 策略配置完成后，确认放行www.aliyundoc.com域名策略（步骤3）和第2条放行DNS（步骤4）策略优先级是高于配置拒绝所有流量策略（步骤5）。

> **说明** 调整策略优先级操作详见修改云防火墙访问控制策略的优先级。

后续操作

访问控制策略配置完成后，可以通过**访问控制**的**互联网边界防火墙**页签查看策略的命中情况；通过**流量日志**页面查看该策略命中的流量。

8.MongoDB数据库未授权访问漏洞防御最佳实践

MongoDB数据库未授权访问漏洞可以导致数据库数据泄露或被删除勒索。

背景信息

为保证您的业务和应用的安全，云防火墙提供以下漏洞修复指导方案。

MongoDB服务安装完成后，会默认存在一个admin数据库，该admin数据库内容为空，并且没有记录任何与权限相关的信息。

MongoDB默认设置为无权限访问限制，也就是说开启MongoDB服务时如果不添加任何参数，默认是不需要权限验证的。因此，用户无需密码即可通过默认端口对数据库任意操作（增、删、改、查等高危操作），并可远程访问数据库。

因此，加固的核心操作是实现在*admin.system.users*中添加用户，这样MongoDB的登录认证、授权服务才能生效。

修复方案

1. **配置云防火墙访问控制策略。**
   i. 限定MongoDB服务仅对内网服务器提供服务。

      在云防火墙控制台的左侧导航栏，选择**网络流量分析 > 互联网访问活动**，然后单击**开放应用**页签，查看公网中MongoDB服务所属的IP地址。如果该服务仅对内网服务器提供服务，建议禁止将MongoDB服务开放到互联网上。

      执行以下命令启动IP地址绑定、限定该MongoDB服务仅对内网服务器提供服务（本示例中MongoDB数据库实例将只监听192.168.XX.XX内网的请求）。

      ```
      mongod --bind_ip 192.168.XX.XX
      ```

   ii. 配置MongoDB云防火墙访问控制策略只对可信源放行。

   i. **配置MongoDB云防火墙访问控制策略只对可信源放行。**

      在云防火墙控制台的左侧导航栏，选择**访问控制 > 访问控制**，然后在**互联网边界防火墙**页签，单击**外对内**页签，配置访问控制策略，仅允许与MongoDB数据库依赖的服务器访问该MongoDB服务。

      a. 在**外对内**页签，单击**地址薄管理**，在**IPv4地址薄**页签将MongoDB所有可信源加入地址簿。
      b. 在**外对内**页签，单击**创建策略**，在**创建外-内策略**对话框对MongoDB可信源进行放行。 参数配置如下：
         - **访问源**：选择已配置好的MongoDB所有可信源地址簿。
         - **目的**：为MongoDB可信源地址。
         - **协议类型**：选择TCP协议，表示互联网访问流量。
         - **端口**： 设置为0/0，表示可信源的所有端口地址。
         - 其他参数按照页面提示完成配置。

ii. **拒绝所有其他非可信源访问MongoDB服务。**

在云防火墙控制台的左侧导航栏，选择 **访问控制 > 访问控制**，然后在**互联网边界防火墙**页签，单击**外对内**页签，配置访问控制策略，拒绝其他非可信源访问MongoDB服务。

在**外对内**页签，单击**创建策略**，在**创建外-内策略**对话框对MongoDB非可信源进行拒绝。 参数配置如下：

- **访问源**：设置为0.0.0.0/0，表示所有访问源。
- **目的**：为MongoDB 服务所属的公网IP地址。
- **协议类型**：选择TCP协议，表示互联网访问流量。
- **端口**： 设置为0/0，表示非可信源的所有端口地址。
- 其他参数按照页面提示完成配置。

2. **开启基于权限角色的登录认证功能。**

i. 执行以下命令，在未开启认证的环境下登录到数据库。

```
./mongo 127.0.0.1:27028 （此处修改了默认端口）
```

ii. 执行以下命令切换到admin数据库。

```
use admin
switched to db admin
```

> **说明** 只有切换到admin数据库后添加的账号才是管理员账号。

iii. 执行以下命令创建为admin数据库创建管理员用户。 本示例中用户名为*supper*，密码*supWDxsf67%H*。

> **说明** MongoDB从V3版本开始取消使用addUser方法、采用db.createUser命令创建用户。

```
db.addUser("supper", "supWDxsf67%H") 或
{ "n" : 0, "connectionId" : 4, "err" : null, "ok" : 1 }
db.createUser({user:"****",pwd:"***********",roles:["root"]})
{
"user" : "****",
"readOnly" : false,
"pwd" : "**************","_id"
ObjectId("4f2bc0d357a309043c6947a4")
}
#管理员账号在system.users中。
db.getCollectionNames()
[ "system.indexes", "system.users", "system.version" ]
```

创建的用户账号保存在*system.users*中。

> **说明** 管理员账号不要设置为常见账号；密码需要满足一定的复杂度：长度至少八位以上并包括大小写字母、数字、特殊字符混合体，不要使用生日、姓名、身份证编号等常见密码。

iv. 验证之前添加的用户是否创建成功。

执行命令后，返回1，表示用户已创建成功。

```
db.auth("supper","supWDxsf67%H")
1
```

v. 结束Mongodb进程并重启Mongodb服务。

```
db.auth("supper","supWDxsf67%H")
exit
bye
```

vi. 执行以下命令，启动用户权限认证。

开启用户权限认证后，未登录的客户端没有权限做任何操作。

```
mongod --dbpath=/path/mongodb --bind_ip=10.0.0.1 --port=27028 --fork=true logpath=/
path/mongod.log --auth&
```

> 说明
>
> - admin.system.users中将会保存比在其它数据库中设置的用户权限更大的用户信息，拥有超级权限，也就是说在admin中创建的用户可以对MongoDB中的其他数据库数据进行操作。
> - MongoDB系统中，数据库是由超级用户来创建的，一个数据库可以包含多个用户，一个用户只能在一个数据库下，不同数据库中的用户可以同名。
> - 特定数据库（例如：DB1）的用户User1不能够访问其他数据库DB2，但是可以访问本数据库下其他用户创建的数据。
> - 不同数据库中同名的用户不能够登录其他数据库，例如：DB1、DB2都有user1，以user1登录DB1后，不能登录到DB2进行数据库操作。
> - 在admin数据库创建的用户具有超级权限，可以对MongoDB系统内的任何数据库的数据对象进行操作。
> - 使用db.auth()可以对数据库中的用户进行验证，如果验证成功则返回1，否则返回0。db.auth()只能针对登录用户所属的数据库的用户信息进行验证，不能验证其他数据库的用户信息。

检测是否存在入侵风险

如果您是MongoDB数据库管理员，可使用以下方式确认是否有进一步的入侵行为：

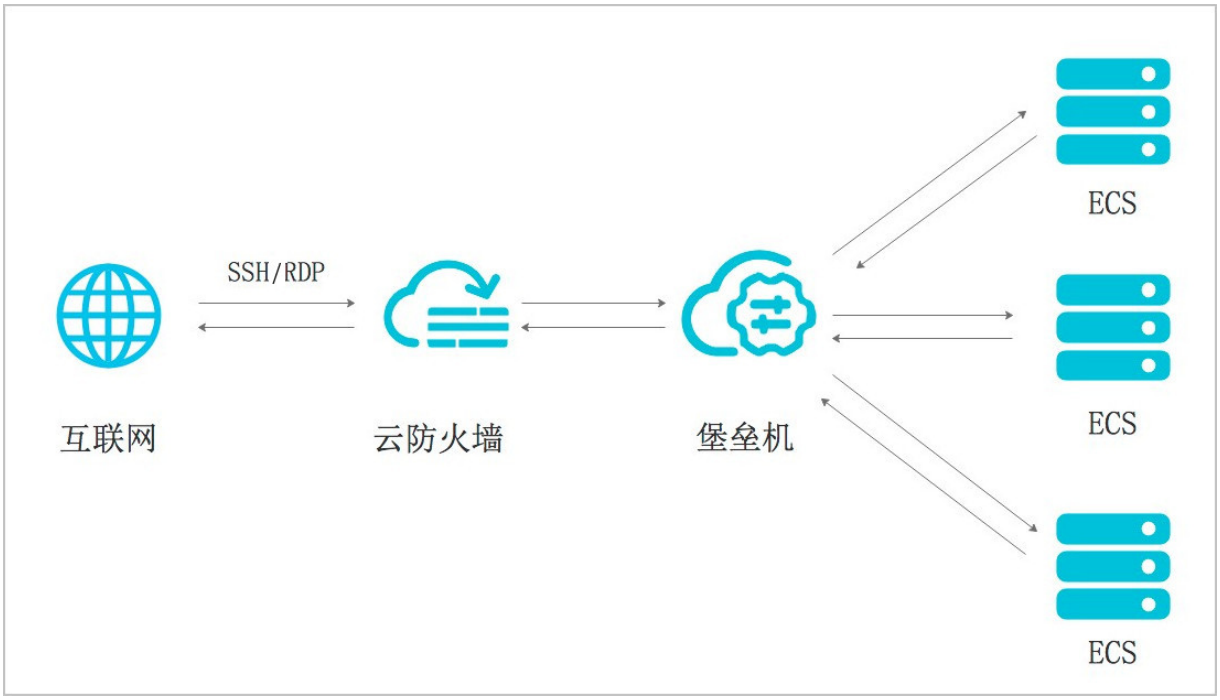
- 查看MongoDB的日志是否完整，并确认执行删除数据库的源IP地址和时间、行为。
- 使用db.system.users.find()命令检查MongoDB帐户是否存在未添加密码的账户。
- 使用db.fs.files.find()命令检查GridFS是否有其他用户存储了任何文件。
- 使用show log global命令查看日志文件，确认是否有其他用户访问了MongoDB。

9.云防火墙保护堡垒机最佳实践

云防火墙支持对堡垒机提供访问控制、IPS、网络流量分析等功能，实现对堡垒机公网IP进行统一管理和保护。

防护原理

以下是云防火墙为堡垒机提供安全防护的原理图。



推荐配置

云防火墙防护堡垒机公网IP的推荐配置如下：

1. 配置互联网边界防火墙**外到内**策略，允许互联网或指定区域的互联网访问堡垒机的开放端口。
2. 配置互联网边界防火墙**内到外**策略，允许堡垒机访问公网IP。
3. 在防火墙开关处打开堡垒机的保护，使进入、流出堡垒机的流量都经过云防火墙的保护。

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**互联网边界防火墙**页签，新建**外对内**访问控制策略，允许互联网或指定区域的互联网访问堡垒机的开放端口。
   i. 单击**外对内**页签。
   ii. （可选）单击**地址簿管理**，在**端口地址簿**页签单击**新建地址簿**。

   > **说明** 地址簿用于添加多个IP地址或端口进行批量配置，可简化您的配置流程。如果您只需要开放一个堡垒机端口，无需创建地址簿。

iii. 在**编辑地址簿**对话框中添加堡垒机对互联网要开放的端口。

堡垒机需要对互联网开放的端口：60022（SSH）、63389（RDP）、443（堡垒机BS运维）端口，请根据您的实际访问需要将要对互联网开放的端口加入到**端口地址簿**。多个端口用英文逗号分隔。最多可添加50个端口。

iv. 新建第一条**外对内**访问控制策略，允许互联网访问堡垒机指定端口。

参数	描述
源类型	选择*IP*类型。
访问源	如果是允许互联网所有地址访问堡垒机端口，填写*0.0.0.0/0*，表示互联网所有地址的访问；如果只允许部分区域的互联网访问堡垒机开放端口，请填写对应的IP地址段信息。
目的类型	选择*IP*类型。
目的	填写堡垒机的IP地址。 **说明** 您可以在云防火墙控制台**防火墙开关** > **防火墙开关**页面的**互联网边界防火墙**页签，通过筛选**资产类型**查看您的堡垒机IP地址，而无需切换到堡垒机控制台去查看IP信息。
协议类型	选择*TCP*。
端口类型	如果您需要开放多个堡垒机端口，**端口**类型需要选择**地址簿**并在**端口**配置项中选择之前已创建好的堡垒机开放端口地址簿。
应用	选择**ANY**。
动作	选择*放行*，表示允许互联网地址访问堡垒机对外开放的端口。
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**。可设置以下优先级： ■ **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。
启用状态	设置策略的启用状态，设置为启用状态。

v. 新建第二条**外对内**访问控制策略，拒绝互联网任意地址对堡垒机非开放端口的访问。

端口：输入*0/0*表示堡垒机的所有端口。

动作：选择**拒绝**，表示不允许互联网任意地址访问堡垒机非对外开放的端口。

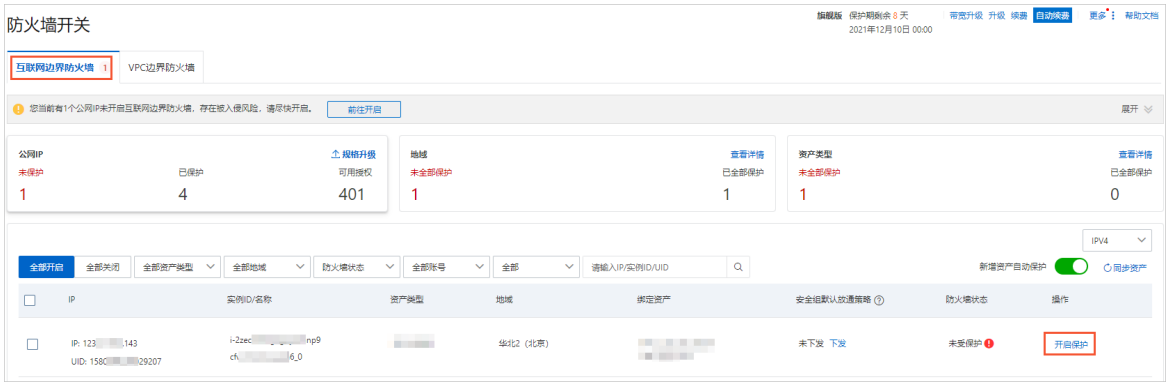
4. 允许堡垒机访问互联网。

堡垒机需要通过公网访问阿里云，或存在跨VPC访问ECS或者访问云外主机的情况，因此需要允许堡垒机对公网的访问。

i. 定位到**访问控制 > 访问控制**页面**互联网边界防火墙**页签中的**内对外**页签。

ii. 单击**创建策略**，并完成允许堡垒机访问互联网的策略配置。

5. 在**防火墙开关 > 防火墙开关**页面的**互联网边界防火墙**页签，定位到对应的堡垒机，单击**开启保护**，开启云防火墙对堡垒机的防护。



> **说明** 新购买的堡垒机在完成购买15~30分钟后同步到云防火墙。

相关文档

- 云防火墙帮助文档
- 访问控制策略配置帮助
- 防火墙开关使用帮助

10.防御挖矿程序最佳实践

本文以云上环境为例，从挖矿蠕虫的防御、检测和入侵后如何迅速止血三方面来介绍如何结合阿里云云防火墙和云安全中心全方位抵御挖矿蠕虫。

限制条件

- 云防火墙版本限制：

  请确保您使用的是云防火墙高级版、企业版或旗舰版。高级版、企业版或旗舰版才支持检测或防御挖矿蠕虫，免费版不支持。您可以通过购买云防火墙高级版、企业版或旗舰版来检测或防御挖矿蠕虫。更多信息，请参见购买云防火墙服务。

- 云安全中心版本限制：

  云安全中心不同版本支持的功能有差异，详细介绍，请参见功能特性。

> **说明** 云防火墙为免费版用户提供7天免费试用高级版的活动。详细内容，请参见云防火墙免费试用。

挖矿程序的特征

- 挖矿程序会占用CPU进行超频运算，导致CPU严重损耗，并且影响服务器上的其他应用。
- 挖矿程序还具备蠕虫化特点，当安全边界被突破时，挖矿病毒会向内网渗透，并在被入侵的服务器上持久化驻留以获取最大收益。
- 挖矿程序具有联动作用，在清理过程中会存在处理不及时或清理不干净导致挖矿病毒反复发生、出现恶意脚本替换系统命令的现象，从而导致执行系统命令时触发恶意脚本执行（例如：xorddos）。因此，需要在挖矿程序的一个执行周期内，尽快将被入侵服务器上的木马程序和持续化后门清理干净，否则容易导致挖矿病毒频繁复发。

挖矿蠕虫是如何传播的

根据阿里云安全团队发布的《2018年云上挖矿分析报告》显示，过去一年中，每一波热门0 Day漏洞出现都伴随着挖矿蠕虫的爆发性传播。挖矿蠕虫可能因为占用系统资源导致业务中断，甚至还有部分挖矿蠕虫同时会捆绑勒索病毒（如XBash等），给企业带来资金与数据的损失。

阿里云安全团队分析发现，云上挖矿蠕虫主要利用网络上普遍存在的以下漏洞进行传播：

- 通用漏洞利用

  过去一年挖矿蠕虫普遍会利用网络应用上广泛存在的通用漏洞（如配置错误、弱密码、SSH、RDP、Telnet爆破等），对互联网持续扫描和攻击，以对主机进行感染。

- 0 Day、N Day漏洞利用

  0 Day、N Day在网络上未被修复的窗口期也会被挖矿蠕虫利用，迅速进行大规模的感染。

挖矿蠕虫防御方案

防护阶段	防护方案	相关操作
	通过云防火墙的访问控制功能，设置访问控制策略，仅放行可信流量。	您可通过**互联网边界防火墙**页签下的**内对外**页签，创建内对外访问控制策略，对可信的外网IP进行放行，而对其他IP访问全部拒绝。相关内容，请参见访问控制策略。

防护阶段	防护方案	相关操作
事前阶段	通过在云防火墙中开启威胁引擎开关，及时阻断挖矿行为。	相关操作，请参见使用云防火墙防御挖矿蠕虫。
	通过云防火墙的入侵防御功能，有效检测并拦截攻击流量。	相关操作，请参见入侵防御。
	通过云安全中心的主动防御功能，自动拦截常见病毒、恶意网络连接和网站后门连接，抑制云服务器上挖矿事件的发生。	相关操作，请参见病毒防御概述。
	通过云安全中心的安全告警处理功能，检测云服务器中是否有运行挖矿程序、矿池通信行为。	相关操作，请参见查看和处理告警事件。
事中阶段	通过云防火墙的失陷感知功能快速检出挖矿蠕虫。	在**失陷感知**页面，可以定位到列表中具体事件和外联地址。详细内容，请参见使用云防火墙检测挖矿蠕虫。
	通过云防火墙入侵防御功能快速止血。	您可通过开启云防火墙的**基础防御**开关，对恶意文件下载进行阻断。详细内容，请参见入侵后如何使用云防火墙快速止血。
	通过云防火墙访问控制策略阻断挖矿连接。	创建内对外访问控制策略，对可信的外网IP进行放行，将对矿池地址的访问设置为**拒绝**。
	云防火墙ATT&CK最佳实践。	云防火墙提供的基础规则、虚拟补丁、威胁情报等功能覆盖ATT&CK各类风险，建议参考云防火墙基于Att&CK的最佳实践，对您的网络安全进行加固。
事后阶段	使云安全中心对挖矿病毒进行攻击溯源。	详细介绍，请参见攻击溯源。

使用云防火墙防御挖矿蠕虫

云防火墙通过对云上进出网络的恶意流量进行实时检测与阻断，实现防御挖矿蠕虫的目的，具体体现在以下方面：

- 通用漏洞的防御

  针对挖矿蠕虫对SSH、RDP等进行暴力破解的攻击方式，云防火墙的**基础防御**支持常规的暴力破解检测方式，如通过登录或试错频次阈值计算，对超过试错阈值的行为进行IP限制，在您的访问习惯、访问频率的基础上，结合行为模型，保证您正常访问不被拦截的同时对异常登录进行限制。

  针对一些通用的漏洞利用方式（如利用Redis写Crontab执行命令、数据库UDF进行命令执行等），云防火墙的基础防御基于阿里云的大数据优势，利用阿里云安全在云上攻防对抗中积累大量恶意攻击样本，形成精准防御规则。

  您可通过开启云防火墙的基础防御来防御通用漏洞。

  开启云防火墙的基础防御功能步骤如下：

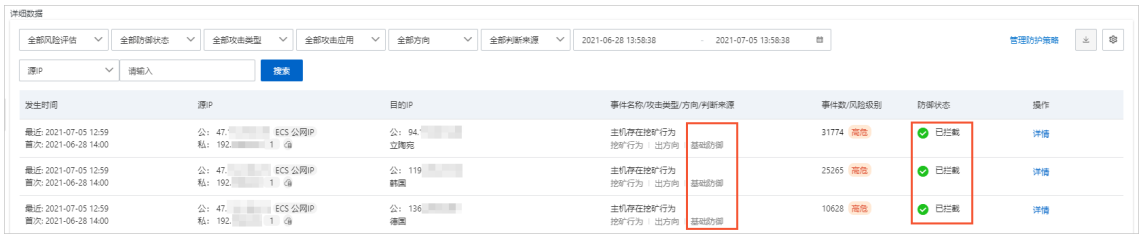
  i. 登录云防火墙控制台。

ii. 在左侧导航栏，选择**攻击防护 > 防护配置**。

iii. 在**防护配置**页面，定位到**威胁情报**区域，打开**威胁情报**开关。

iv. 在**防护配置**页面，定位到**基础防御**区域，打开**基础规则**开关。

v. 在左侧导航栏，选择**攻击防护 > 入侵防御**，在**入侵防御**页面的详细数据列表中查看详细的拦截日志。



- 0 Day、N Day漏洞防御

  热门0 Day、N Day漏洞修复不及时，被挖矿蠕虫利用感染的风险较大。云防火墙利用全网部署的蜜罐分析异常攻击流量或利用阿里云先知平台获取漏洞情报，可及时发现针对0 Day、N Day的漏洞，第一时间获取漏洞PoC或Exp，并落地形成虚拟补丁，在与黑客的攻防对抗中占得时间先机。

  您可通过开启云防火墙的虚拟补丁来防御0 Day、N Day漏洞。

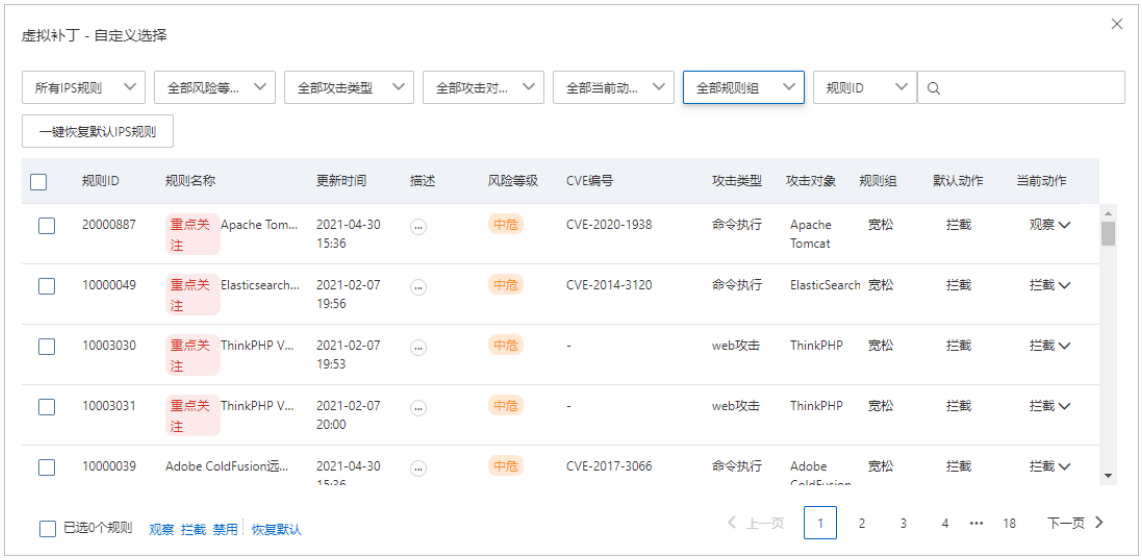
  开启云防火墙的虚拟补丁功能步骤如下：

  i. 登录云防火墙控制台。

  ii. 在左侧导航栏，选择**攻击防护 > 防护配置**。

  iii. 在**防护配置**页面，定位到**虚拟补丁**区域，打开**开启补丁**开关。

  iv. 单击**开启补丁**右下方的**自定义选择**，打开**虚拟补丁管理**对话框，查看或管理已开启的虚拟补丁信息。



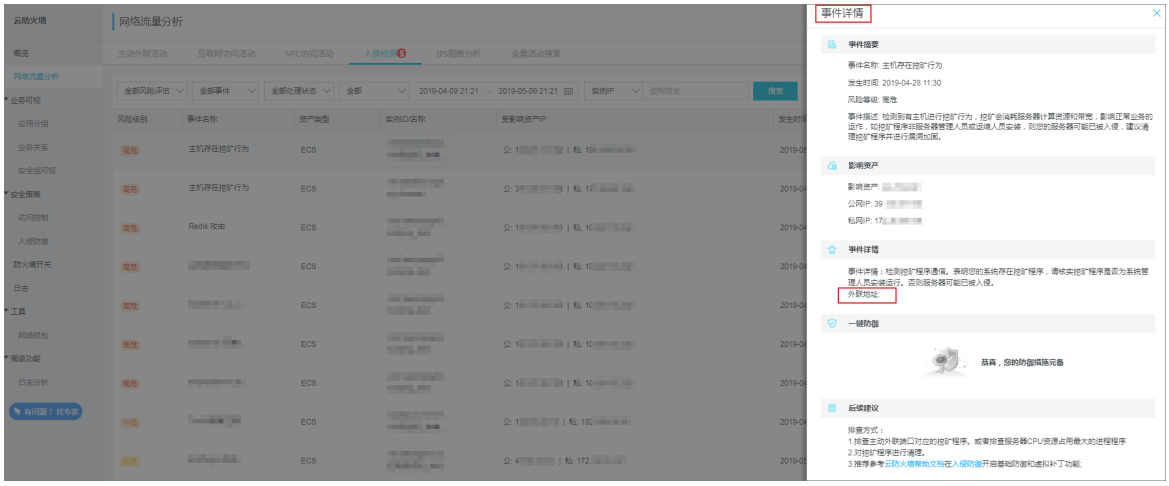
使用云防火墙检测挖矿蠕虫

在与蠕虫攻防对抗中，即使在公网边界做好入侵防御措施，仍有可能感染挖矿蠕虫。例如挖矿蠕虫可以通过VPN直接由开发机传播到生产网；用于运维的系统镜像、Docker镜像已经被植入挖矿病毒，从而导致大规模感染爆发。

云防火墙通过NTA（Network Traffic Analysis）能力提供**失陷感知**功能，能够及时并有效发现挖矿蠕虫感染事件。利用云上强大的威胁情报网，云防火墙可以及时发现常见货币的矿池地址、检测挖矿木马下载行为和常见矿池通信协议，实时识别主机挖矿行为，并及时告警。

您可通过开启云防火墙**失陷感知**功能的**一键防御**来检测挖矿蠕虫，并在网络端阻断挖矿木马与矿池通信。开启云防火墙入侵检测一键防御步骤如下：

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，定位到列表中具体事件，单击**操作**列**详情**。



您可以在**基本信息**面板中查看该挖矿程序的外联地址。

4. 登录检测到挖矿程序的服务器，定位到挖矿进程并进行快速清理。

入侵后如何使用云防火墙快速止血

如果服务器已感染挖矿蠕虫，云防火墙可以从恶意文件下载阻断、中控通信拦截、重点业务区加强访问控制三方面控制蠕虫进一步传播、减少业务和数据的损失。

- 恶意文件下载阻断

  服务器在感染挖矿蠕虫后通常会进行恶意文件下载。云防火墙**基础防御**功能集成恶意文件检测能力，实时更新常见挖矿蠕虫的各类恶意文件唯一性特征码和文件模糊hash，在挖矿蠕虫入侵成功、进一步下载更新的攻击载荷时，会对下载至服务器的文件在流量中进行文件还原及特征匹配等安全检测，在检测到尝试下载恶意文件时进行告警并阻断。

  您可通过开启云防火墙的**防护配置 > 基础防御**对恶意文件下载进行阻断。

- 中控通信拦截

  在感染挖矿蠕虫后，针对挖矿蠕虫可能和C&C控制端进行通信，接收进一步的恶意行为指令或者向外泄漏敏感数据等，云防火墙的基础防御功能通过以下方面对该行为进行实时拦截：

  - 通过分析和监控全网蠕虫数据和中控服务器通讯流量，可以对异常通讯流量特征化，落地形成中控通信检测特征，通过实时监控中控通信变化，不断地提取攻击特征，确保及时检测到攻击行为。
  - 通过自动学习历史流量访问信息，建立异常流量检测模型，挖掘潜在的未知挖矿蠕虫信息。

- 利用大数据可视化技术对全网IP访问行为关系进行画像，利用机器学习发现异常IP及访问域，并联动全网攻击数据，最终落地形成中控威胁情报库，从而可以对服务器流量通信进行情报匹配，实时阻断恶意的中控连接通信。

通过基础防御和威胁情报对中控通信拦截的记录如下。

您可通过开启云防火墙的**防护配置 > 基础防御**，对中控通信进行拦截。

- 为重点业务区开启强访问控制

重点业务通常需要对整个互联网开放服务或端口，而来自互联网的扫描、攻击会对企业的资产形成威胁，对外部的访问控制很难做到细粒度管控。而对某一台ECS、某一个EIP或内部网络主动外联场景下，域名或IP数量其实都是可控的，因为该类外联通常都是进行合法的外联访问。因此通过内对外的域名或IP访问控制，可有效防止ECS主机被入侵之后，利用恶意域名植入挖矿木马或木马与C&C进行通信等行为。

云防火墙支持对访问来源域名（含泛域名）、IP地址设置访问控制规则。针对重点业务的安全问题，可以通过配置一个强粒度的**内到外**访问控制策略，即重要业务端口只允许特定域名或者特定的IP进行访问，其他一律禁止。通过该操作可以有效地杜绝挖矿蠕虫下载、对外传播，防止入侵后阶段的维持与获利。

例如以下场景中，内网对外访问的总IP数为6个，其中NTP全部标识为阿里云产品，而DNS为我们所熟知的8.8.8.8，通过云防火墙的安全建议，我们可以将上述6个IP进行放行，而对其他IP访问进行全部拒绝。通过如上的配置，在不影响正常业务访问的情况下，防止其他对外连接行为，如恶意下载、C&C通信等。

您可通过云防火墙的**访问控制 > 访问控制**页面中的**互联网边界防火墙**页签下的**内对外**页签，创建内对外访问控制策略，对可信的外网IP进行放行，而对其他IP访问全部拒绝。

由于互联网上持续存在的通用应用漏洞、0 Day漏洞的频发，以及挖矿变现的高效率，挖矿蠕虫大规模蔓延。云上客户可以透明接入云防火墙，保护自身应用不受互联网上各种恶意攻击的威胁。同时依托云上海量的计算能力，能够更快地感知最新的攻击威胁、并且联动全网的威胁情报给用户最佳的安全防护，使用户免于挖矿蠕虫威胁。云防火墙可以伴随业务水平弹性扩容，让您更多地关注业务的扩展，无需花费更多精力投入在安全上。

11.将云防火墙流量日志导入第三方系统

云防火墙服务高级版、企业版和旗舰版支持通过阿里云日志服务（SLS）实时获取已接入云防火墙的流量日志。您可通过云防火墙的日志分析功能导出流量日志并对接到第三方系统中。

目前云防火墙已支持**互联网流量日志**和**VPC流量日志**，您可以通过云防火墙日志分析功能导出日志，并将导出的日志文件接入到您的业务系统中，如您的安全运维中心等。

> **说明** 互联网流量日志包括漏洞风险等级和访问控制规则命中结果等数据。

前提条件

已购买和开通日志分析服务。相关内容请参见开通日志分析服务和云防火墙日志存储规格和计费方式。

导出方法

您可通过云防火墙日志分析功能和阿里云日志服务两种方式导出日志。

- 日志数据量小的场景

  可登录云防火墙控制台，在左侧导航栏选择**日志分析 > 日志分析**，在**日志分析**页面**日志查询**页签单击 图标下载日志文件，然后上传到您的第三方系统中。

- 日志数据量大的场景

  可登录日志服务控制台，通过程序组编程等方式导出日志数据。

  有关日志服务的操作详情，请参见通过消费组消费日志数据。

  > **说明** 如果您未开通阿里云日志服务（SLS），开通云防火墙日志分析功能时将会同时为您开通日志服务（SLS）功能。

云防火墙日志存储规格和计费方式

云防火墙日志分析功能为您提供弹性的日志存储空间。日志存储规格收费如下。

日志存储容量	适用带宽	推荐使用的版本	中国内地地域实例	
			包月费用	包年费用8.5折
1 TB	适用月带宽不高于10 Mbps的业务场景	高级版	80 USD	861 USD
5 TB	适用月带宽不高于50 Mbps的业务场景	企业版	400 USD	4,080 USD
20 TB	适用月带宽不高于200 Mbps的业务场景	旗舰版	1,600 USD	16,320 USD

有关日志存储空间的详情信息，请参见日志存储空间管理。

12.关闭境外所有访问

如果您的资产需要关闭所有来自境外的访问，您可以在云防火墙控制台创建一条访问控制策略，拒绝所有来自境外的流量。本文介绍如何通过云防火墙关闭境外所有访问。

前提条件

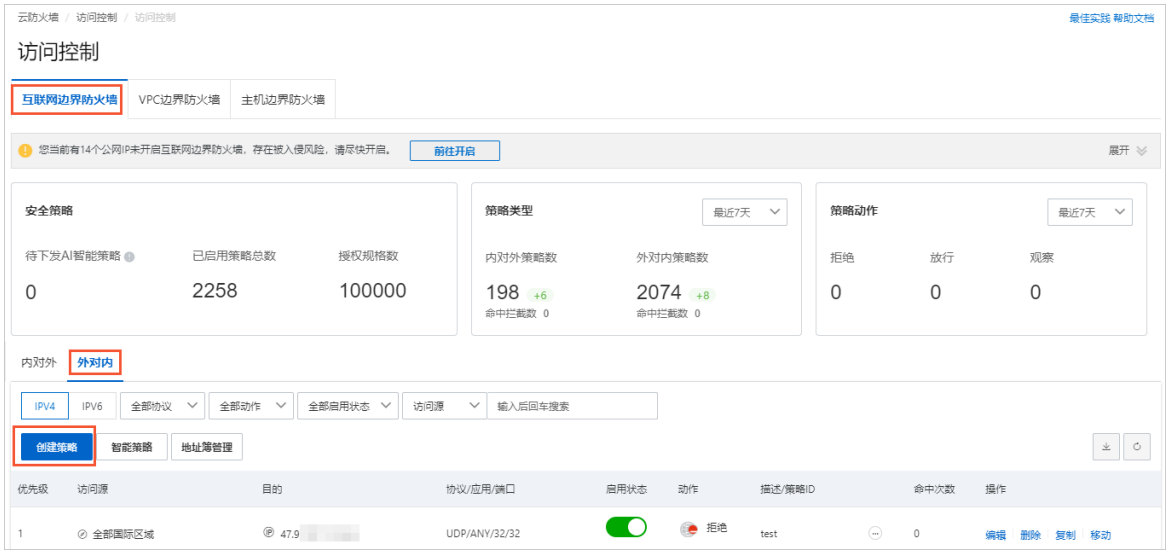
配置互联网边界防火墙策略前，请确认**互联网边界防火墙**开关已开启，否则策略将不生效。详细内容，请参见互联网边界防火墙。

背景信息

您需要在**互联网边界防火墙**页签中创建**外对内**（外部互联网访问您的内部网络）的策略，将访问流量的来源地址设置为**全部国际区域**，并将策略动作设置为**拒绝**。

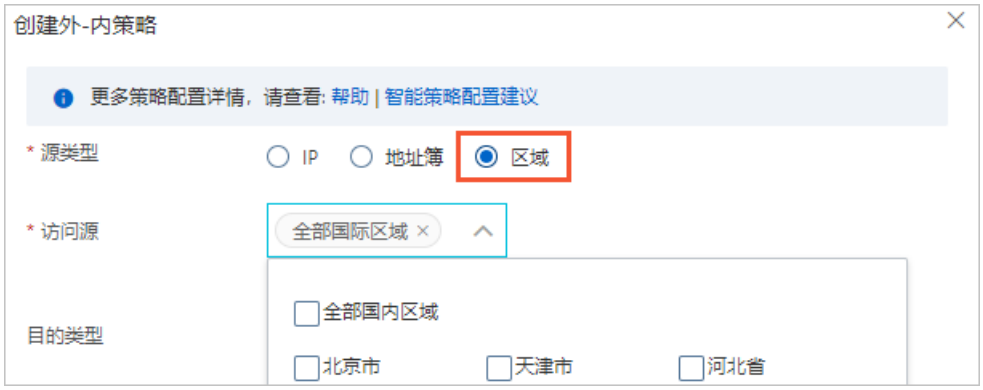
创建访问控制策略

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**互联网边界防火墙**页面，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**对话框中完成参数配置，单击**确认**。

   源类型选择**区域**、**访问源**选择所有需要禁止访问的境外区域、**动作**选择**拒绝**。详细的参数说明，请参见下表：



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**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。

修改访问控制策略

访问控制策略配置完成后，您可以根据实际需求修改该条策略的访问控制区域或其他访问控制参数。

您可以在访问控制策略列表中定位到该新增的策略，单击**操作**列**编辑**，在**编辑**对话框修改访问控制参数。

13.云防火墙基于Att&CK的最佳实践

13.1. 免责声明

云防火墙基于Att&CK的最佳实践目录下的文档中所述规则，在不同场景中可能属于人为正常操作，但也可能用于非法操作，故云防火墙默认处于禁止或观察模式，避免因为客户云上不同使用场景而导致误报误拦截行为。您可以通过改变规则模式来解决所列举诸多场景，但云防火墙不保障覆盖所列举的场景中所有子项功能，例如**禁止非法工具安装**不等同**禁止所有非法工具安装**，**仅支持防护配置中所列举项目**，如您需要对子项功能进行扩充，请您通过工单、钉群等方式进行反馈，云防火墙工程师进行评估后，将通过规则等方式发布。

13.2. 概述

当前云防火墙提供了基础规则、虚拟补丁、威胁情报等覆盖ATT&CK各类功能，包括漏洞防护、暴力破解、挖矿检测、信息泄露等十余个大类，但是各个客户业务、场景、内部合规有所不同，不同场景下直接封禁相关功能有所不当，针对这一场景，云防火墙将该类型统一置为观察或默认禁用模式，用户可以依据自身业务场景、企业安全规则通过基础规则、虚拟补丁的自定义规则进行观察/拦截切换，以实现网络防御、业务监控、企业内部安全合规的最佳实践。以下是云防火墙梳理的企业常用场景。

初始访问	执行	持久化	防御规避	发现	命令与控制
供应链攻击（开启供应链下载或安装监控）	计划任务或作业（禁止下载脚本执行主机相关操作）	计划任务或作业（禁止下载脚本执行主机相关操作）	文件或目录权限变更（禁止下载脚本执行主机相关操作）	网络服务扫描（禁止非法工具安装）	非应用层协议（禁止云上远程调试）
无	无	无	隐藏文件（禁止下载脚本执行主机相关操作）	安全软件发现（禁止安骑士等云上安全服务恶意卸载）	代理（禁止代理行为）
无	无	无	清除历史（禁止下载脚本执行主机相关操作）	系统信息发现（禁止系统关键信息泄露）	远程访问软件（禁止使用远控软件）
无	无	无	文件删除（禁止下载脚本执行主机相关操作）	无	协议隧道（禁止使用DNS over HTTPS）
无	无	无	无	无	Web服务（禁止访问公共服务）

相关文档

- 使用云防火墙阻止安装非法工具
- 使用云防火墙禁止恶意卸载云安全中心（安骑士）等云上安全服务
- 使用云防火墙禁用远程控制软件
- 使用云防火墙禁止下载脚本执行主机相关操作
- 使用云防火墙禁止代理行为
- 使用云防火墙禁止系统关键信息泄露

- 使用云防火墙禁止云上远程调试
- 使用云防火墙禁止信息探测行为
- 使用云防火墙禁用DNS over HTTPS
- 使用云防火墙禁止访问Onion代理域名
- 免责声明

13.3. 使用云防火墙阻止安装非法工具

Nmap、Masscan、Pnscan通常用于对互联网进行大规模扫描，Netcat通常用于端口监听、后门连接等。云防火墙可针对此类工具的非法安装情况进行识别和管控。

安装非法工具的危害

安装非法工具有可能导致以下问题：

- 内部员工执行违规操作

  企业内部员工下载并安装非法工具后，可通过该工具对企业的内部资产或外部资产进行绘制，将内部网络拓扑透露给外部人员或进行其他违规操作。

- 黑客攻击

  黑客入侵到内部网络后，可以通过`yum`、`apt-get`安装上非法工具，绘制内部网络拓扑进而横向移动、安装后门、窃取数据。

- 蠕虫、木马传播

  蠕虫等病毒入侵主机后，通过脚本下载并安装非法工具，对外部互联网进行扫描，进而批量传播感染大批主机。

防护说明

如果您需要对云服务器禁用上述非法工具，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义**页面中，将与非法工具相关的规则部分或全部开启为**拦截模式**，有效阻止或缓解非法工具带来的安全风险。

13.4. 使用云防火墙禁止恶意卸载云安全中心（安骑士）等云上安全服务

云安全中心、安骑士等主机侧安全服务软件通常用于监控主机侧安全情况，用于病毒查杀、脚本查杀、恶意命令执行等检测，这些安全服务软件可能被恶意卸载，导致安全服务无法对资产提供防护。

恶意卸载场景

- 内部员工违规操作

  内部员工如果想进行违规操作，通常会选择先将主机侧安全软件卸载，避免违规操作被主机侧安全服务软件检测到而告警。

- 黑客攻击

  黑客入侵云上系统后，为了更好的在主机上实施攻击行为而不引起企业安全工程师注意，卸载安全服务软件可以避免安全工程师接到失陷感知告警。

- 蠕虫、木马传播

  蠕虫、木马通过下载恶意软件达到后门维持或数据窃取目的，卸载安全服务软件可以避免失陷感知告警。

云防火墙操作

当前云防火墙对安骑士卸载设置了**观察模式**，如您需要对云上环境禁止网络侧卸载，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
100000...	卸载安骑士	2021-09-07 16:21	...	低危	-	其他		宽松	观察	观察
100000...	卸载安骑士	2021-09-07 16:20	...	低危	-	其他		宽松	观察	观察
100000...	疑似执行卸载安骑士...	2021-09-03 00:35	...	中危	-	其他	HTTP	宽松	禁用	禁用

13.5. 使用云防火墙禁用远程控制软件

日常运维工作中，运维人员经常会使用远程控制软件，用于远程控制主机、远程桌面连接、远程开机、远程管理、内网穿透等操作。

远程控制的危害

- 内部员工违规操作

  通过部署远程控制软件，内部员工可以绕过设置的登录用户名、密码控制，对远端主机具有完全控制权，便于进行数据窃取、数据删除等操作。

- 黑客攻击

  通过集成远控软件，黑客可以部署后门进而远程实施可视化操作，完全控制主机，从而进行数据窃取、后门部署等操作。

- 蠕虫、木马传播

  蠕虫、木马通过远控软件在主机中部署后门，实现对主机的完全控制。

云防火墙操作

当前云防火墙对于应用范围较广的TeamViewer、向日葵等远程控制软件默认支持**观察模式**。

如果您需要对云服务器禁用上述远程控制软件，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将相关的规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
100000...	向日葵远控通信	2021-09-07 15:05	...	低危	-	其他		宽松	观察	观察

13.6. 使用云防火墙禁止下载脚本执行主机相关操作

脚本可以携带丰富的信息用于操作主机日常工作，其类型也非常丰富，有Bash Shell、Python、Perl、PowerShell等。

危害

- 内部员工违规操作

  通过远程下载带有恶意命令的脚本，可以执行预先编写的命令。

- 黑客攻击

  通过远程下载带有恶意命令的脚本用于实施各类攻击。

- 蠕虫、木马传播

  蠕虫、木马通过脚本进行维持，通常写入Crontab用于周期性执行，用于对抗主机侧的文件清理操作等。

云防火墙操作

当前云防火墙对下载的脚本中携带的疑似Bash History操作、疑似执行User Add增加账户等操作处于**观察模式**，如您需要对云上环境禁止通过下载脚本执行上述操作，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将相关的规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
100000...	疑似执行UserAdd增...	2021-09-03 01:04	...	中危	-	其他	HTTP	宽松	禁用	禁用
100000...	疑似执行UserAdd增...	2021-09-03 01:05	...	中危	-	其他	HTTP	宽松	禁用	禁用
100000...	疑似执行UserAdd增...	2021-09-03 01:06	...	中危	-	其他	HTTP	宽松	禁用	禁用

13.7. 使用云防火墙禁止代理行为

代理是一种特殊的网络服务，允许一个终端通过这个服务与另一个终端进行非直接的连接，通过代理可以绕过现有的网络检测。

危害

- 内部员工违规操作

  通过代理将内部数据转发出去，规避当前网络入侵防御、访问控制策略的管控、威胁情报等检测。

- 黑客攻击

  通过代理进行内部网络流量转发，用于对内部网络的探测、入侵等行为。

- 蠕虫、木马传播

  蠕虫、木马通过代理规避当前网络入侵防御、访问控制策略管控、威胁情报等检测。

云防火墙操作

当前云防火墙对SOCKS5代理等操作处于**观察模式**，如您需要对云上环境禁止SOCKS5通信等，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将相关的规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
100000...	Socks5代理协议	2021-09-03 00:16	...	低危	-	异常连接		宽松	禁用	禁用

13.8. 使用云防火墙禁止系统关键信息泄露

系统内部文件如/etc/passwd、/etc/shadow存放着主机用户的关键信息，通过系统命令`cat`、`head`、`tail`可以轻松读取此类关键信息。

危害

- 黑客攻击

  通过远程命令执行等Web攻击操作获取系统关键信息，进而实施远程登录、远程控制等攻击行为。

- 蠕虫、木马传播

  蠕虫、木马通过获取系统关键信息，用于内部网络横向传播。

云防火墙操作

当前云防火墙对系统关键信息泄露等操作处于**观察模式**，如您需要对云上环境禁止/etc/passwd等系统关键信息泄露，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将相关的规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
200000...	系统关键文件信息泄露	2021-02-08 13:57	...	高危	-	信息泄漏	Linux	宽松	拦截	拦截
200000...	系统关键文件信息泄露	2021-02-08 14:05	...	高危	-	信息泄漏	Linux	宽松	拦截	拦截
100000...	系统关键信息泄露	2021-09-07 16:46	...	中危	-	信息泄漏	Windows	中等	观察	观察
100000...	系统关键信息泄露	2021-09-07 16:46	...	中危	-	信息泄漏	Windows	中等	观察	观察

13.9. 使用云防火墙禁止云上远程调试

远程调试是指通过云上软件和服务进行断点、单步、查看堆栈等调试操作，通过gdbserver、JDWP 、Xdebug、ADB等网络协议可以调试C、C++、Java、PHP、Andorid等编写的脚本、二进制、系统文件。

危害

远程调试协议拥有对远程软件、服务具有的权利，可以导致远程命令执行。

- 内部员工违规操作

通过开放的远程调试服务，可以远程执行命令，进而完全控制主机。

- 黑客攻击

  通过扫描云上对外开放的远程服务调试端口，可以进行远程命令执行，进而完全控制主机，进行木马种植、数据窃取等操作。

- 蠕虫、木马传播

  蠕虫、木马通过远程调试协议进行传播，进而导致挖矿、勒索等行为。

云防火墙操作

当前云防火墙对云上远程调试等操作处于**观察模式**，如您需要对云上环境禁止远程调试，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将相关的规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

☐	规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
☐	200012...	JDWP Java 调试接口...	2021-04-30 15:34	...	中危	-	命令执行	Web Application Java	中等	观察	观察

13.10. 使用云防火墙禁止信息探测行为

网络扫描工具用于对网络开放服务、端口进行探测，可以实现对外暴露端口、服务资产绘制，通过Nmap、Masscan、Pnscan等软件实现。

危害

- 暴露对外端口和服务

  对外暴露端口和服务，该部分采集的信息将直接指导后续攻击阶段。

- 黑客攻击

  通过网络扫描工具可以探测到服务自身或配置等信息，该部分采集的信息可用于攻击阶段。

云防火墙操作

当前云防火墙对信息探测行为部分操作处于**观察模式**，如您需要对云上环境禁止诸如Nmap的信息探测，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将相关的规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

☐	规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
☐	200012...	检测到信息探测行为	2021-04-30 15:34	...	低危	-	扫描	Nmap	宽松	观察	观察
☐	200012...	检测到信息探测行为	2021-04-30 15:34	...	低危	-	扫描	Nmap	宽松	观察	观察
☐	200012...	检测到信息探测行为	2021-04-30 15:34	...	低危	-	扫描	Nmap	宽松	观察	观察
☐	200012...	检测到信息探测行为	2021-04-30 15:34	...	低危	-	扫描	Nmap	宽松	观察	观察
☐	200012...	检测到信息探测行为	2021-04-30 15:34	...	低危	-	扫描	Nmap	宽松	观察	观察

13.11. 使用云防火墙禁用DNS over HTTPS

DNS over HTTPS是一种安全化的域名解析方案，用于以加密的HTTPS协议进行DNS解析请求，避免原始DNS协议中用户的DNS解析请求被监听或修改。

危害

- 内部员工违规操作

  通过DoH访问非法域名，从而绕过访问控制策略或威胁情报的检测。

- 蠕虫、木马传播

  蠕虫、木马通过DoH查询域名真实IP，绕过入侵防御、访问控制策略、威胁情报的检测。

云防火墙操作

当前云防火墙对DoH等操作处于**观察模式**，如您需要对DoH禁用，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将相关的规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
100000...	通过DoH节点进行DN...	2021-09-07 17:39	...	低危	-	其他		宽松	禁用	禁用
100000...	通过DoH节点进行DN...	2021-09-07 17:38	...	低危	-	其他		宽松	禁用	禁用

13.12. 使用云防火墙禁止访问Onion代理域名

Onion用于在Tor网络上寻址特殊用途的顶级域后缀，只要安装了正确的代理软件，即可通过Tor服务器发送特定的请求访问.onion地址，可以避免追踪。

危害

- 内部员工违规操作

  内部员工可能会通过访问Onion代理域名访问Tor服务器，进行恶意操作，可避免被安全工程师追踪。

- 蠕虫、木马传播

  蠕虫、木马通过DoH查询域名真实IP，绕过入侵防御、访问控制策略管控、威胁情报的检测。

云防火墙操作

当前云防火墙对Tor网络监控等操作处于**观察模式**，如您需要对云上环境禁止Tor网络，您可以登录云防火墙控制台，打开**攻击防护 > 防护配置**页面，在**基础防御-自定义选择**页面中，将相关的规则部分或全部开启为**拦截模式**，能有效阻止或缓解上述危害。

规则ID	规则名称	更新时间	描述	风险等级	CVE编号	攻击类型	攻击对象	规则组	默认动作	当前动作
100000...	访问onion代理域名	2021-09-07 17:38	...	低危	-	其他		宽松	禁用	禁用