云防火墙

最佳实践

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。
您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

版权所有：腾讯云计算（北京）有限责任公司

最佳实践
云防火墙数据库防护最佳实践

最近更新时间：2024-03-15 15:54:31

数据库防护服务可通过云防火墙主动识别内网数据库资产，在 NAT 边界形成一道安全防护，并通过接入域名实现访问的管控，避免直接将 CVM 绑定的弹性公网 IP 暴露在公网。 域名接入方式可以实现在外网通过域名去访问内网的数据库，从而避免数据库端口暴露。
数据库防护服务主要分为接入域名和数据库白名单两大块。本文档还介绍了如何去查看数据库白名单的日志，并针对 MySQL 数据库进行测试举例，可供参考。

配置接入域名

步骤1：开启 NAT 边界防火墙，配置接入域名

1. 登录 云防火墙控制台，在左侧导航栏中，单击**防火墙开关** > **NAT 边界开关** > **防火墙实例**，进入防火墙实例页面。
2. 在防火墙实例页面，单击**创建实例**，选择所需地域，单击**下一步**。

3. 在新建 NAT 边界防火墙窗口中，配置相关参数后，单击**下一步**。

字段说明：

- **地域**：选择创建地域，支持国内所有地域，创建实例后不可更改。

> **说明：**
> 用户可在拥有 VPC 的所有国内地域（支持中国香港地域）中进行地域选择，同地域下可创建多个防火墙实例，但总带宽不能超过限定规格。

- **可选区**：根据需求选择合适的可用区。
- **实例名称**：输入实例名称。
- **带宽规格**：根据需求选择带宽规格，最小20Mbps，如需更多带宽请 升级扩容 。

> **说明：**
> 互联网带宽保持一致，如果分了多个 NAT 防火墙，那么多个 NAT 防火墙的带宽之和，要小于等于互联网边界的带宽。

- **模式**：分为新增模式和接入模式。
  - **新增模式**：若当前地域没有 NAT 网关，新增模式可以通过 NAT 边界防火墙内置的 NAT 功能，实现指定实例通过防火墙访问互联网。
  - **接入模式**：若当前地域已有 NAT 网关，或者希望公网对外的出口 IP 保持不变，接入模式可以将 NAT 边界防火墙平滑接入到 NAT 网关与 CVM 实例之间。
- **弹性 IP**：选择**新增模式**时，若选择新建弹性 IP，系统会自动为用户申请一个弹性 IP，用户也可从所有闲置的弹性 IP 中选择一个进行绑定。如需要更多带宽请 升级扩容 。

4. 选择要接入 NAT 防火墙的 VPC，单击**创建**。

5. 等待若干分钟后，即可在防火墙实例列表中，查看刚刚创建的实例。
6. 单击**防火墙开关**，根据实际需求选择数据库在所在的子网，单击 开启防火墙开关。

> **说明：**
> 若数据库所在地域已有 NAT 防火墙和域名，请检查数据库资产所在子网是否已开启防火墙开关。

7. 在 零信任防护页面，单击**接入域名管理 > 新增域名**。

8. 在新增域名窗口中，选择地域、域名和刚刚创建的实例，单击**确定**即可完成域名接入。

> **说明：**
> 若当前地域下已创建域名可忽略该步骤。

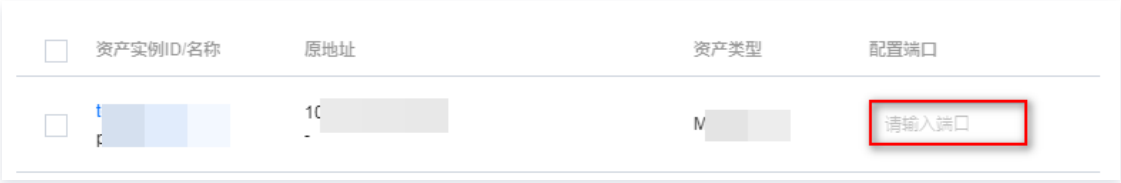
步骤2：数据库资产识别

将内网所有的数据库识别出来，并通过域名接入方式加入域名中。

1. 在 资产中心页面，选择**资产列表 > 数据库资产**，单击**资产更新**，完成后在数据库资产页面中可以查看当前的数据库资产。

2. 在数据库资产页面，选择所需实例，单击**查看防护**，跳转至零信任防护页面。

3. 在数据库资产页面，支持如下两种方式将数据库添加到域名：
   - 方式1：单击**一键接入**，选择所需资产实例 ID，输入配置端口后， 单击**确定**即可。



   - 方式2：选择所需资产实例 ID，单击操作列的**域名接入**，选择所需端口号，单击**确定**即可。

> **说明：**
> 创建域名是指针对不同的地域创建用于访问的域名，以上域名已创建好，端口号是访问时用到的端口，可以自行定义。

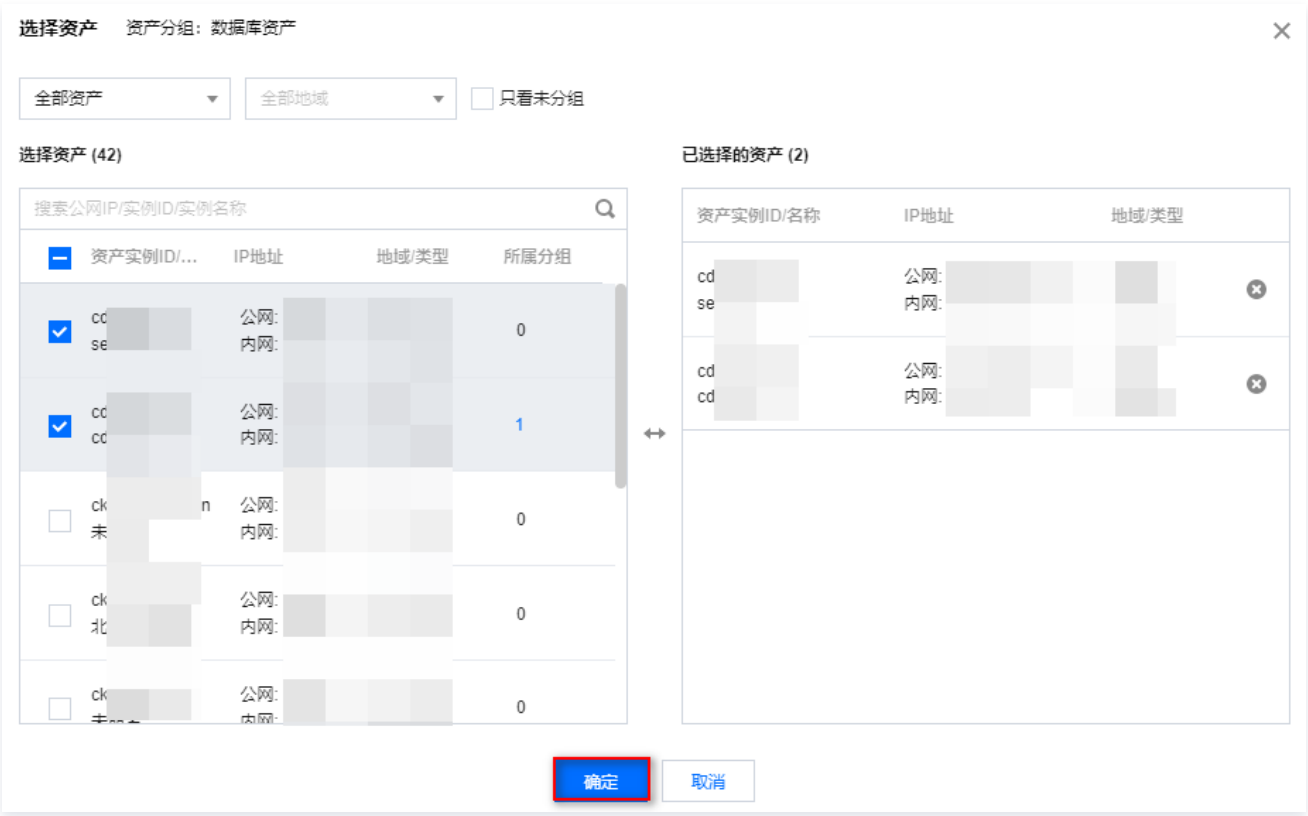
步骤3：配置资产分组

使用资产分组功能对资产进行统一管理和配置。

1. 在 资产中心页面，单击**资源分组** > **资产分组**，进入资产分组页面。
2. 在资产分组页面，单击**新建分组**，输入分组名称后，单击**确定**。

3. 在左侧的树形结构中，选择刚刚创建的资源分组，单击 ••• 并选择**添加资产到分组**。

4. 在选择资产窗口中，选择所需资产后，单击**确定**即可。



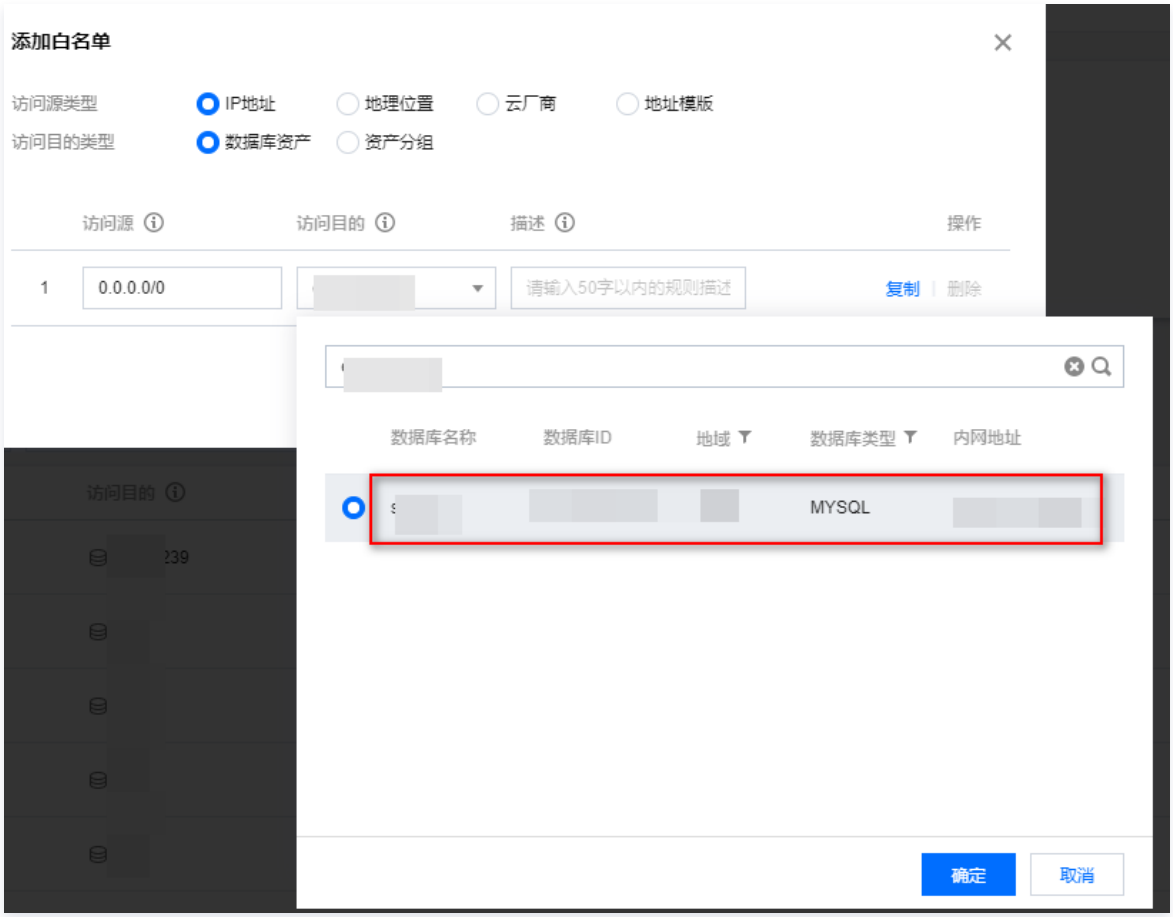
数据库白名单配置

数据库白名单是基于 NAT 防火墙针对数据库的访问控制表，可以根据 IP、地理位置等对流量进行过滤。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**零信任防护 > 数据库管理 >白名单管控**。

2. 在白名单管控页面，单击阻断白名单以外访问处的 经过确认后开启。否则默认是所有 IP 或者地域都能通过域名进行访问，开启之后需配置白名单规则，只有规则之内的源 IP 或者地域才能访问。

3. 在白名单管控页面，单击**添加规则**，访问目的选择 步骤2：数据库资产识别 所创建的数据库或资产分组，其他根据实际需求选择。

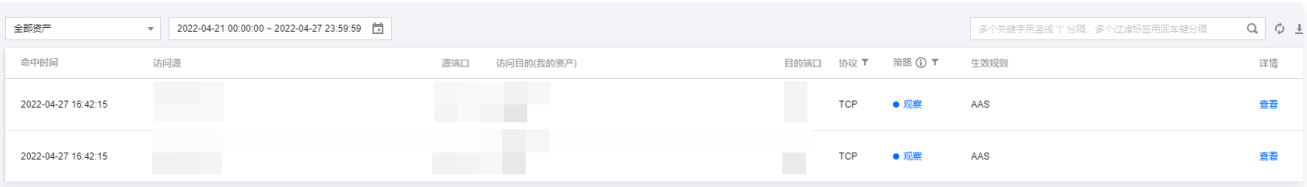


4. 配置完成后，单击**确定**即可。

查看数据库防护日志

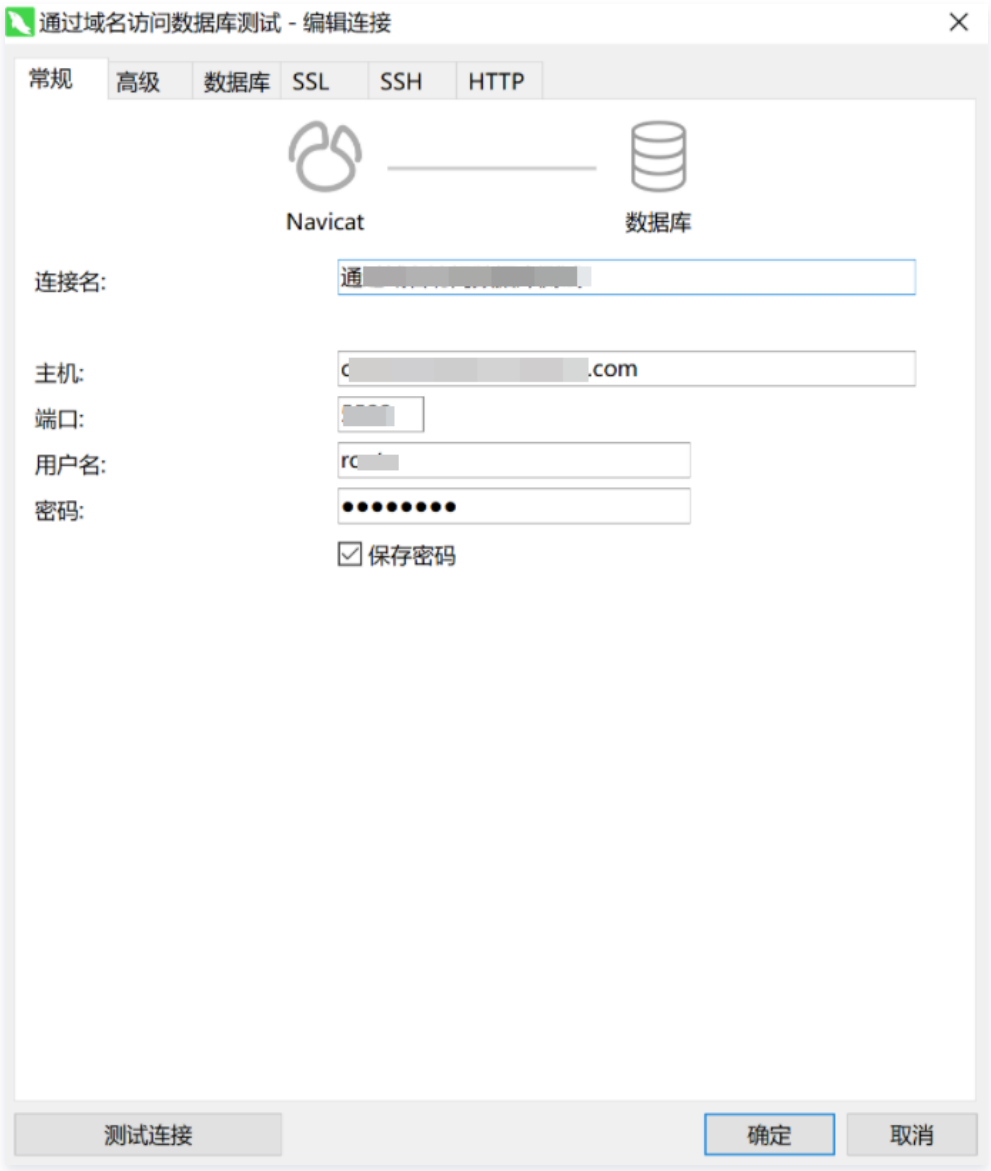
零信任防护日志的数据库防护日志记录了资产所有的放通和阻断记录。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**日志审计** > **零信任防护日志** > **数据库访问**。
2. 在数据库访问页面，可以查看数据库相关的访问控制日志。其中命中白名单策略的会被记录为观察类型，其他的则会被记录为阻断类型。



测试连接

1. 在外网通过数据库连接工具进行连接测试，配置相关参数。



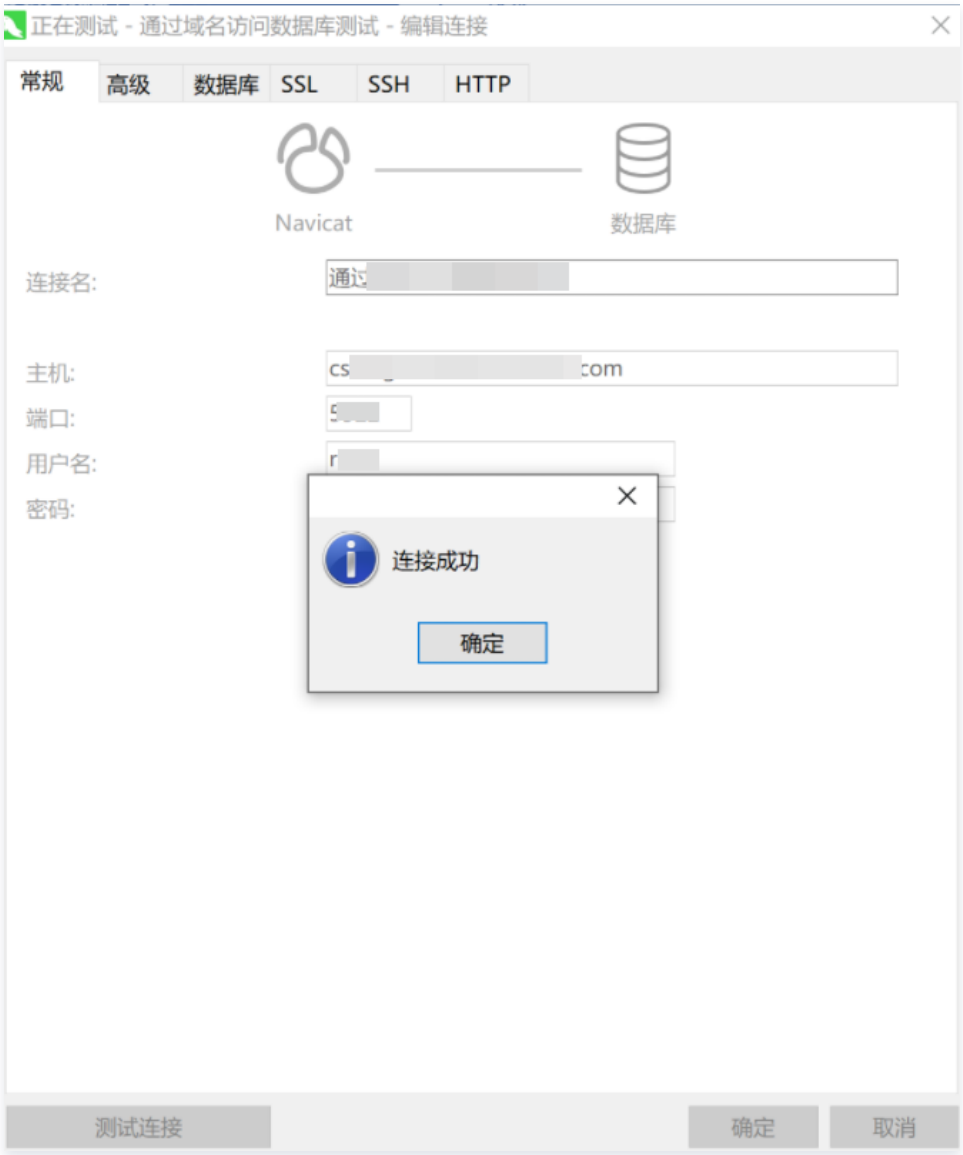
参数说明

- 连接名：可以任意设置的。
- 主机名：创建接入域名时所创建的用于访问的域名。
- 端口：创建接入域名时设置端口，该端口并非数据库真实端口，可以任意设置。
- 用户名：数据库的用户名。
- 密码：数据库的密码。

2. 搭建好测试环境后，通过控制数据库白名单的开关来验证。
   - **开关关闭状态**

     2.1.1 在 **零信任防护** > **数据库管理**页面，“阻断白名单以外访问”为关闭状态，也就是数据库白名单不生效这种情况。

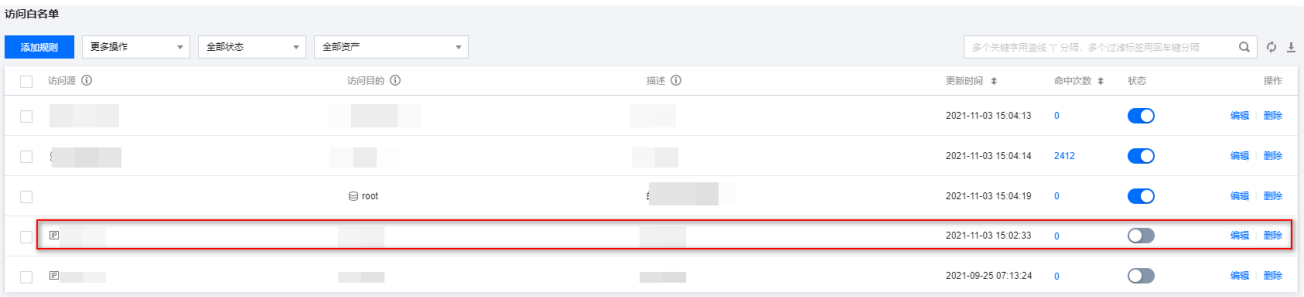
2.1.2 单击界面左下角的**测试连接**，数据库访问成功，如下所示。



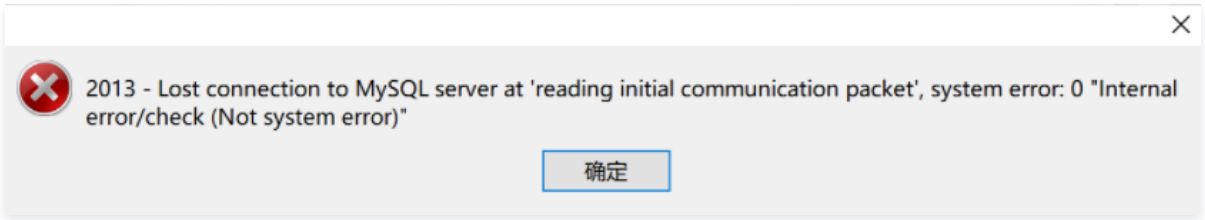
- **开关开启状态**

  2.1.1 在 **零信任防护** > **数据库管理**页面，“阻断白名单以外访问”为开启状态，即白名单生效。

2.1.2此时如果不配置规则来放通相应 IP，访问是不成功的，如将之前创建好的规则删除或者是将开关关闭，此时连接数据库是失败的。



2.1.3 如上，将规则开关关闭，单击界面左下角的**测试连接**，连接过程中报错。



3. 以上测试证明了数据库白名单的作用，可以有效降低数据库连接域名的暴露面，从而避免数据库被客户进行暴力破解等攻击，保障了数据库安全。

云防火墙等保测评解读

最近更新时间：2023-07-04 11:06:23

腾讯云防火墙符合等级保护2.0标准体系主要标准。根据《网络安全等级保护基本要求》（GB/T 22239-2019），腾讯云防火墙（仅限高级版及以上版本且已购买日志分析）满足第三级及以下安全要求。

序号	等保标准章节	等保标准序号	等保标准内容	对应功能	测评解读
1	安全区域边界-边界防护	8.1.3.1 a)	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信	防火墙开关、访问控制	云防火墙支持在南北向边界和东西向边界对流量进行管控；支持梳理互联网暴露面，封禁暴露端口
2	安全区域边界-边界防护	8.1.3.1 b)	应能够对非授权设备私自联到内部网络的行为进行检查或限制	防火墙开关、访问控制	云防火墙支持南北向和东西向的流量审计与分析，通过ACL和黑白名单对资产的网络访问进行实时管控；支持通过微信远程运维，阻断非授权人对资产的访问
3	安全区域边界-边界防护	8.1.3.1 c)	应能够对内部用户非授权联到外部网络的行为进行检查或限制	防火墙开关、访问控制	云防火墙支持南北向和东西向的流量审计与分析，对主动外联行为感知分析并阻断，同时支持配置访问控制规则对非授权访问进行限制
4	安全区域边界-访问控制	8.1.3.2 a)	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信	访问控制	云防火墙的互联网边界规则、NAT 边界规则、VPC 间规则实现业务流量的南北向和东西向隔离；配置规则后将按照指定执行顺序统一管控
5	安全区域边界-访问控制	8.1.3.2 b)	应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化	访问控制	您需要根据规则的执行顺序和命中次数，对无效规则或冗余规则进行删除或停用，从而优化访问控制规则列表
6	安全区域边界-访问控制	8.1.3.2 c)	应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许 / 拒绝数据包进出	访问控制	云防火墙访问控制规则支持按照指定访问源、源端口、访问目的、目的端口、协议进行配置，可选策略为放通或阻断
7	安全区域边界-访问控制	8.1.3.2 d)	应能根据会话状态信息为进出数据流提供明确的允许 / 拒绝访问的能力	访问控制	云防火墙支持以会话粒度为开启防护的资产对恶意流量进行实时检测和阻断拦截
8	安全区域边界-访问控制	8.1.3.2 e)	应对进出网络的数据流实现基于应用协议和应用内容的访问控制	访问控制	云防火墙访问控制规则支持按照协议配置；云防火墙支持对数据库、远程连接等应用的防护
9	安全区域边界-入侵防范	8.1.3.3 a)	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为	入侵防御	云防火墙支持为开启防护的资产进行恶意流量和常见攻击行为的实时检测和阻断拦截
10	安全区域边界-入侵防范	8.1.3.3 b)	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为	访问控制	云防火墙支持流量主动外联管控、主机失陷感知等出方向流量检测防护和 ACL 管控
11	安全区域边界-入侵防范	8.1.3.3 c)	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析	入侵防御	云防火墙结合腾讯安全威胁情报库对云上新型攻击行为、0day漏洞实时感知，并支持通过虚拟补丁进行拦截和防护
12	安全区域边界-入侵防范	8.1.3.3 d)	当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警	告警中心	云防火墙实时检测网络流量，对风险事件进行告警，对恶意行为实施阻断，并记录攻击事件类型、危险等级、访问源、源端口、访问目的、目的端口、协议、发生时间等信息
13	安全区域边界-恶意代码和垃圾邮件防范	8.1.3.4 a)	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新	入侵防御	云防火墙支持对网络恶意代码攻击进行实时检测和防护，并定期更新恶意代码检测规则
14	安全区域边	8.1.3	应在网络边界、重要网络节点进	日志审	云防火墙在开通日志分析功能后支持可存储6个月内的日志数

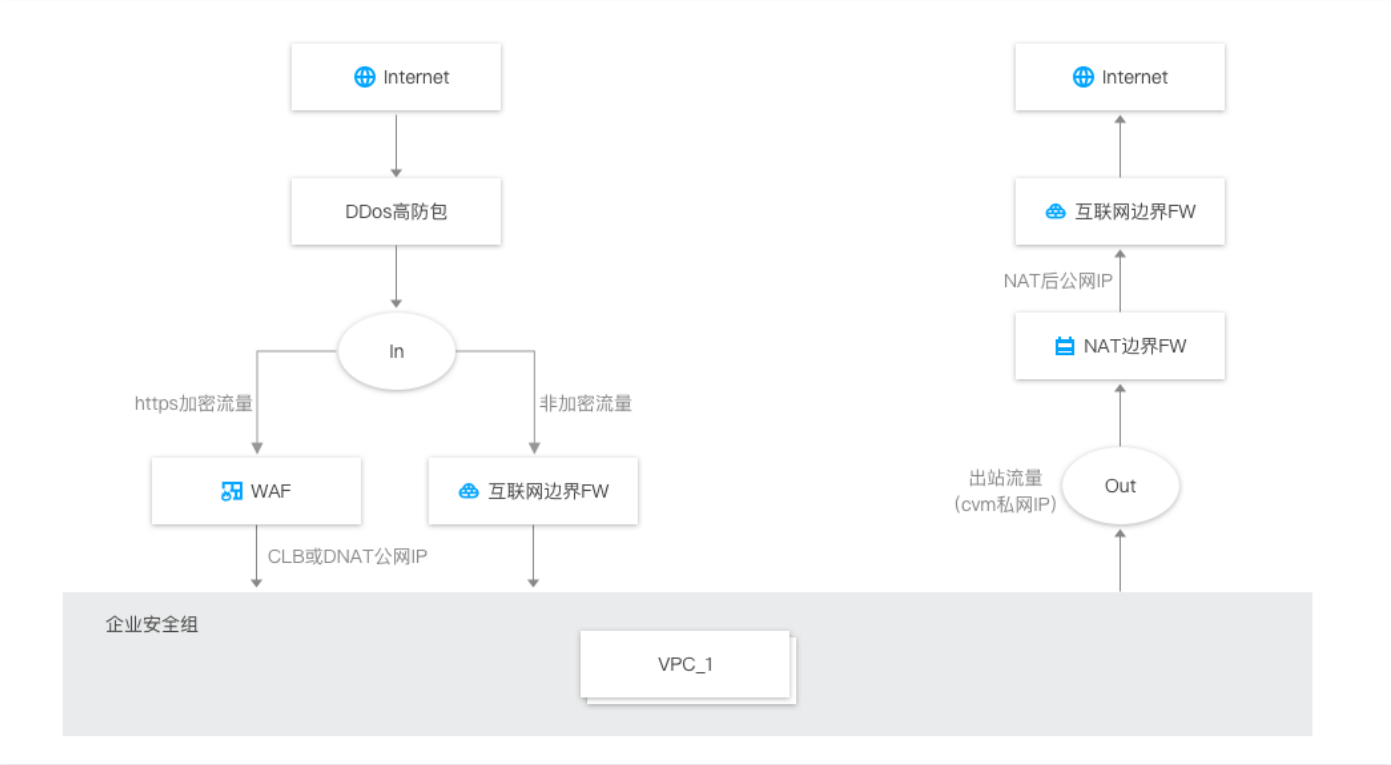
	界-安全审计	.5 a)	行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	计、流量中心	据，包含流量日志、入侵防御日志、访问控制日志和操作日志
15	安全区域边界-安全审计	8.1.3.5 b)	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	日志审计	云防火墙日志记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
16	安全区域边界-安全审计	8.1.3.5 c)	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	日志审计	云防火墙日志记录通过主备存储系统实时备份，保证用户日志在其存储周期内不丢失、可恢复
17	安全区域边界-安全审计	8.1.3.5 d)	应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析	日志分析	云防火墙微信远程运维功能可记录用户远程访问后的所有行为；结合南北向和东西向流量日志和云防火墙日志分析功能可以对用户行为做全方位审计和数据分析

版权所有：腾讯云计算（北京）有限责任公司

云防火墙与其他产品的联合防护

最近更新时间：2023-10-09 11:07:00

云防火墙可以与 DDoS 高防包 、Web 应用防火墙（WAF） 、安全组 进行联合防护，具体原理如下：



- 对于入方向流量
  - 云防火墙和 WAF 共同组成了云上网络安全的整体边界防护，WAF 更偏向于对加密的 HTTPS 流量进行防护，非加密流量通过云防火墙集成的威胁情报、 入侵防御系统（IPS）的基础规则和虚拟补丁等进行安全防护。
  - SaaS 化 WAF 和互联网边界防火墙是并行工作，流量经过 SaaS 化 WAF 后，不再经过互联网边界云防火墙，但流量可回源到 NAT 边界 FW 的 DNAT IP。
  - CLB 类型 WAF 和云防火墙是串联部署，流量先经过互联网边界防火墙，再经过 CLB WAF。
  - 使用腾讯云 CDN 回源到 CLB、CVM 的流量暂时无法被旁路部署的互联网边界防火墙防护。
- 对于出方向流量
  - 可以通过 NAT 边界 FW（防火墙），实现基于云服务器（CVM）颗粒度的主动外联控制，并且支持基于域名的访问控制，结合腾讯威胁情报，可对主动外联的恶意 IP 及域名进行自动拦截。
  - 如未开启 NAT 边界 FW，则只能在互联网边界 FW，对 NAT gateway 后的流量进行访问控制，此时云防火墙看到的是公网 IP。
- 云防火墙和安全组是两个独立的系统，策略同时放通，流量才放行。
- 在云防火墙企业版中，集成了企业级安全组功能，可以通过企业级安全组，灵活的实现 VPC 间、同 VPC 子网间及 IDC 专线间的访问控制和阻挡日志。

说明：

云防火墙产品支持基于公网 IP 地址颗粒度的防护，因此您可以根据企业自身的情况选择开启方式：

- 只开启部分资产的防护以节省费用。如果企业预算允许，我们仍然建议您开启云上全部资产的防护，以免黑客从非重要资产入侵。
- 如果您云上资产只对外暴露了 Web 类业务，且已经被 WAF 防护，可以只开启主动外联的防护，形成从外到内的 WAF 防护，从内到外的云防火墙防护的整体网络安全防护方案，以节省您的宝贵投资。
- 云防火墙产品具备几十 Gbps 大带宽流量的游戏、电商行业大型客户应用案例，当您的业务流量超过1Gbps时，您可以联系您的商务经理，沟通定制商务方案。

DNS 防火墙最佳实践

最近更新时间：2023-10-09 11:07:00

NAT 防火墙 DNS 开关开启后，系统会修改所接入 VPC 的 DNS 解析地址，将 DNS 流量牵引至 NAT 边界防火墙，从而获取全流量域名。

> **说明：**
> 腾讯云默认 DNS 为：183.60.83.19，183.60.82.98。

可以按照如下流程，配置 DNS 防护：

1. 创建相关地区 NAT 防火墙接入 VPC 网络。
2. 开启 NAT 防火墙开关，流量都从 NAT 防火墙经过。（涉及到路由变更网络会抖动1-2秒）
3. 开启 DNS 开关进行验证 DNS 地址。
4. 使用 NAT 防火墙访问控制限制 DNS 解析（验证）。

如下图示例：腾讯云 CVM 公网资源为默认的 DNS 服务器。

步骤1：创建 NAT 防火墙

1. 登录 云防火墙控制台，在左侧导航中，单击**防火墙开关** > **NAT 边界开关** > **网络拓扑**。
2. 在网络拓扑页面，单击**创建实例**，选择所需地域。
3. 在新建 NAT 边界防火墙弹窗中，配置相关参数，单击**下一步**。

字段说明：

- **地域**：选择创建地域，支持国内所有地域，创建实例后不可更改。

  > **说明：**
  > 用户可在拥有 VPC 的所有国内地域（支持中国香港地域）中进行地域选择，同地域下可创建多个防火墙实例，但总带宽不能超过限定规格。

- **可选区**：根据需求选择合适的可用区。
- **实例名称**：输入实例名称。
- **带宽规格**：根据需求选择带宽规格，最小20Mbps，如需更多带宽请 升级扩容 。

  > **说明：**
  > 互联网带宽保持一致，如果分了多个 NAT 防火墙，那么多个 NAT 防火墙的带宽之和，要小于等于互联网边界的带宽。

- **模式**：分为新增模式和接入模式。
  - **新增模式**：若当前地域没有 NAT 网关，新增模式可以通过 NAT 边界防火墙内置的 NAT 功能，实现指定实例通过防火墙访问互联网。
  - **接入模式**：若当前地域已有 NAT 网关，或者希望公网对外的出口 IP 保持不变，接入模式可以将 NAT 边界防火墙平滑接入到 NAT 网关与 CVM 实例之间。
- **弹性 IP**：若选择新建弹性 IP，系统会自动为用户申请一个弹性 IP，用户也可从所有闲置的弹性 IP 中选择一个进行绑定。

4. 选择需要接入的 VPC，单击**创建**，等待若干分钟后，即可在防火墙实例列表中，查看刚刚创建的实例。

步骤2：开启防火墙开关

在 NAT 边界开关页面，单击**防火墙开关**，根据实际需求选择数据库所在的子网，单击 开启防火墙开关。

步骤3：开启和验证 DNS

1. 在 NAT 边界开关页面，单击**防火墙实例**，选择 步骤1 创建的防火墙实例，单击**实例配置**。

2. 在接入 VPC 与公网 IP 页面，选择所需 ID，单击 开启 DNS 流量。

3. 通过 `ipconfig /release Ipconfig /renew` 刷新 DNS 获取地址。

步骤4：限制 DNS 解析

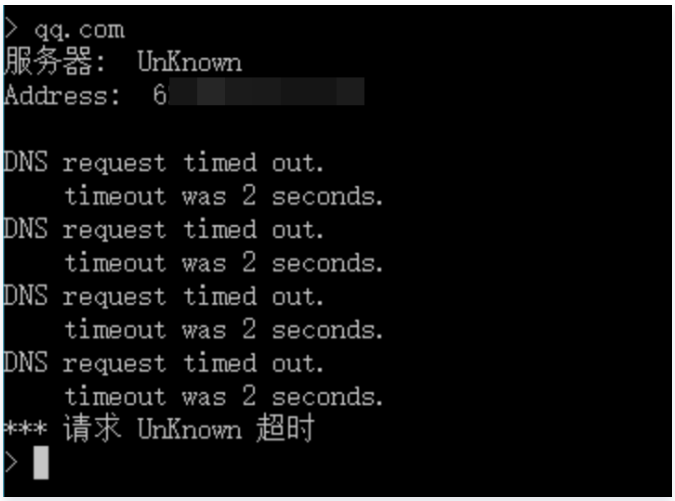
1. 在 NAT 边界规则页面，选择所需地域，单击**出向规则** > **添加规则**。

2. 在添加出向规则弹窗中，配置相关参数，单击**确定**。

字段说明：

- 执行顺序：访问控制规则的执行顺序，出站规则和入站规则的执行顺序互不影响，执行顺序较高的规则被优先匹配，命中某条规则后，不再匹配后序规则。当您修改某条规则的执行顺序时，原本该位置的规则的执行顺序+1，以此类推。当您删除某条规则时，后序所有规则的执行顺序-1。
- 访问源：出向规则访问源仅对当前地域内的所有内网资产生效，支持 IP 和 CIDR。
- 访问目的：出向规则访问目的对所有公网 IP/域名生效，支持 IP、CIDR、域名和地理位置。
- 目的端口：
- TCP/UDP/ANY 规则支持单端口号、基于'/'的端口段以及英文逗号分隔的离散端口值，例如“80”、“80/80”、“-1/-1”、“1/65535”或“80,443,3380/3389”。
- HTTP/HTTPS/SMTP/SMTPS/FTP 规则仅支持配置单端口值，且 SMTP/FTP 协议间端口不可重复。
- ICMP 规则不需要配置端口。
- 协议：当前版本的出向规则支持 ANY、TCP、UDP 和 ICMP 协议。
- 策略说明：
- 放行：放通命中规则的流量，记录命中次数但不记录访问控制日志，且记录流量日志。
- 观察：放通命中规则的流量，记录命中次数并记录访问控制日志与流量日志。
- 阻断：拦截命中规则的流量，记录命中次数并记录访问控制日志，流量日志记录流量的一个请求数据包信息。
- 描述：用于描述规则，最多支持50个字符。

3. 配置完成后验证 DNS 是否连通。



云防火墙防挖矿最佳实践

最近更新时间：2023-09-05 20:23:52

本文结合实际的云上环境，介绍云防火墙是如何防御常见的挖矿蠕虫攻击行为，主要从防御、检测以及入侵后如何快速止血三个方面来做介绍。

限制条件

挖矿蠕虫行为的防御是通过云防火墙的入侵防御模块来实现的，目前 IPS 版、高级版、企业版和旗舰版均支持入侵防御功能，可以防御挖矿攻击。但是常见挖矿攻击的方向是由内网主机感染了木马、僵尸网络等病毒后，再向互联网发起的，为了能够准确定位到内网风险主机，需要开启 NAT 边界防火墙功能，因此**建议云防火墙版本为高级版、企业版或旗舰版**。

挖矿蠕虫的传播原理

挖矿蠕虫主要是依靠网络的漏洞来进行传播的，漏洞一般分为通用型漏洞和 0 DAY/N DAY 漏洞。

通用漏洞利用

挖矿蠕虫通常会利用应用程序或者网站上广泛存在的通用漏洞（如代码缺陷、配置错误、业务系统弱密码等），在互联网上面发起持续的扫描和攻击行为，以达到感染主机的目的。利用通用型漏洞常见的攻击方式主要有：SSH/RDP 口令暴力破解、命令注入攻击、撞库攻击、Webshell 通信、外联黑主机等。常见通用漏洞入侵方式如下表所示：

入侵类型	代表家族	典型入侵方式
暴力破解类	MyKingsMrbMinerLoggerMinerGuardMinerDDG RDPMiner	MongoDB 爆破
		SSH 爆破
		Tomcat 爆破
		MySQL 爆破
		PostgreSQL爆破
		SQLServer 爆破
		FTP 爆破
		RDP 爆破
		SMB 爆破
		Telnet 爆破

0 DAY/N DAY漏洞利用

爆发 0 DAY或者 N DAY漏洞后，如果漏洞暂时处于没有修复的窗口期，极易导致大规模扩散感染，对程序或者业务的破坏性比较大。

- 常见的 0 DAY/N DAY 漏洞主要有：WebLogic 漏洞利用、反序列化漏洞利用、永恒之蓝、Tomcat 远程代码执行漏洞等。
- 常见的 0 DAY/N DAY 漏洞利用入侵方式如下表所示：

入侵类型	代表家族	典型入侵方式
系统漏洞	WannaMine	MS17-010永恒之蓝（CVE-2017-0143）
应用漏洞	8220MinerBashMinerkworkersMinerTraceMinerCarbonMiner	Confluence 远程代码执行漏洞（CVE-2021-26084）
		Confluence 远程命令执行（CVE-2019-3396）
		Gitlab exiftool 远程命令执行漏洞（CVE-2021-22205）
		Apache NIFI 远程代码执行漏洞（CVE-2020-9491）
		用友 NC 远程代码执行漏洞（CNVD-2021-30167）
		Docker Remote API 未授权访问漏洞（CVE-2019-17671）

版权所有：腾讯云计算（北京）有限责任公司

		YAPI 远程代码执行漏洞
组件漏洞	JumaMinerH2Minertellyouthepass	Log4j2 远程代码执行漏洞（CVE-2021-44228）
		Jenkins 未授权命令执行漏洞（CVE-2017-1000353）
		Weblogic 远程执行漏洞（CVE-2021-2109）
		Hadoop Yarn 未授权访问漏洞

云防火墙防御挖矿蠕虫的原理

云防火墙通过对流经的流量做实时的检测，如果发现流量中携带挖矿蠕虫等恶意特征，能够自动进行阻断，实现防御挖矿蠕虫病毒的目的，具体体现在这两个方面：

通用型漏洞的防御

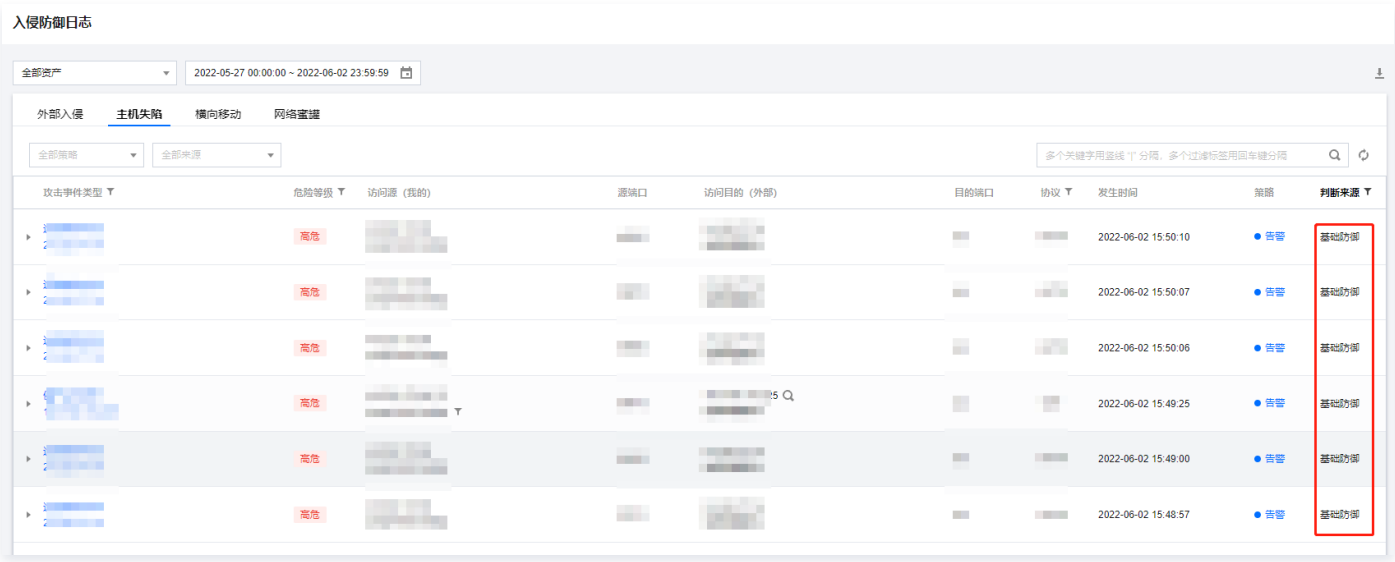
通用型漏洞攻击往往通过 RDP/SSH 暴力破解、系统命令注入等方式来进行的，对于这类攻击行为可通过云防火墙入侵防御中的基础防御模块来防护。基础防御内置了腾讯云平台长期攻防实战中积累的入侵检测规则，覆盖常见网络攻击类型和恶意代码。如下所示：

开启基础防御功能来防御通用漏洞挖矿蠕虫的攻击，具体的开启方式如下：

1. 登录 云防火墙控制台，在左侧导航中，单击**入侵防御**。
2. 在入侵防御页面，单击开启威胁情报和基础防御开关，并选择防护模式为拦截模式或者严格模式。

> **说明**
> - 观察模式检测到挖矿蠕虫行为不会自动拦截，会记录到告警中心。
> - 拦截模式中威胁情报模块支持自动拦截违规外联行为，基础防御模块支持自动拦截高置信度的告警。
> - 严格模式中威胁情报和基础防御模块检测到的任何告警均会自动拦截，或者是自动添加封禁列表。

3. 在 入侵防御日志页面，可以查看入侵日志详情。



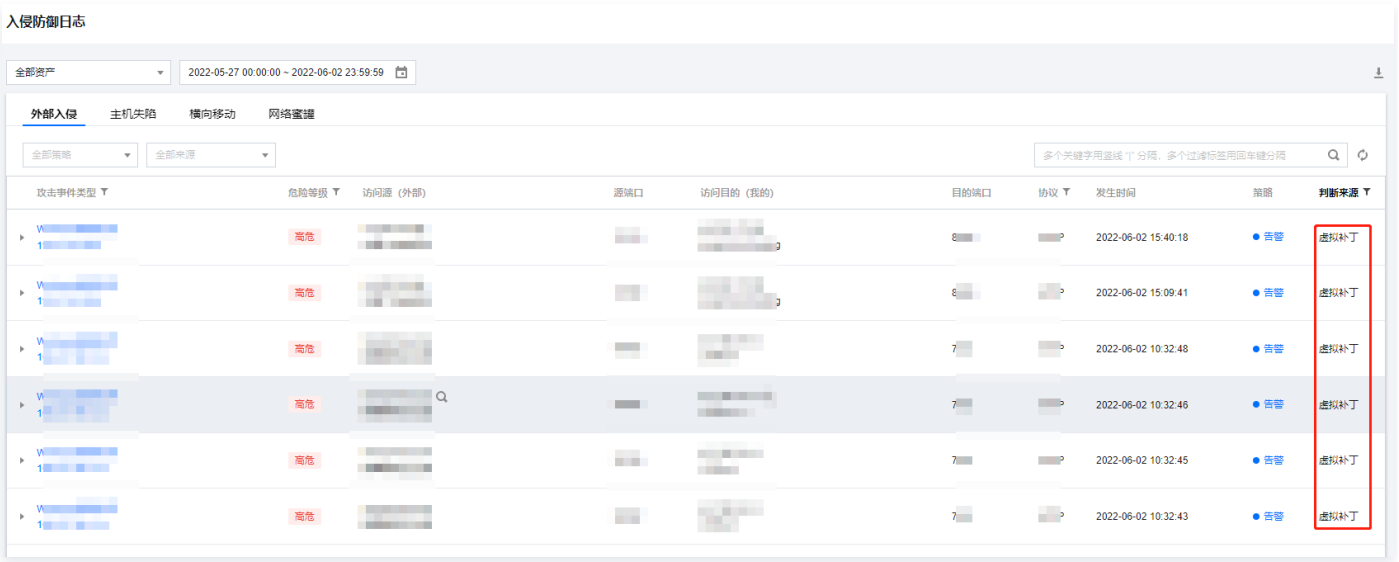
0 DAY/N DAY漏洞的防御

一些热门 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。云防火墙利用腾讯云情报中心实时获取漏洞情报，可及时发现关于 0 Day、N Day 的漏洞，并且能第一时间获取漏洞 POC，并落地形成虚拟补丁规则库，在与黑客的攻防对抗中占得时间先机。如下所示：

开启虚拟补丁开关来防御 0 DAY/N DAY 漏洞的挖矿蠕虫攻击，具体操作如下：

1. 登录 云防火墙控制台，在左侧导航中，单击**入侵防御**。
2. 在入侵防御页面，单击开启虚拟补丁开关，并选择防护模式为拦截模式或者严格模式。

3. 在 入侵防御日志页面，可以查看入侵日志详情。



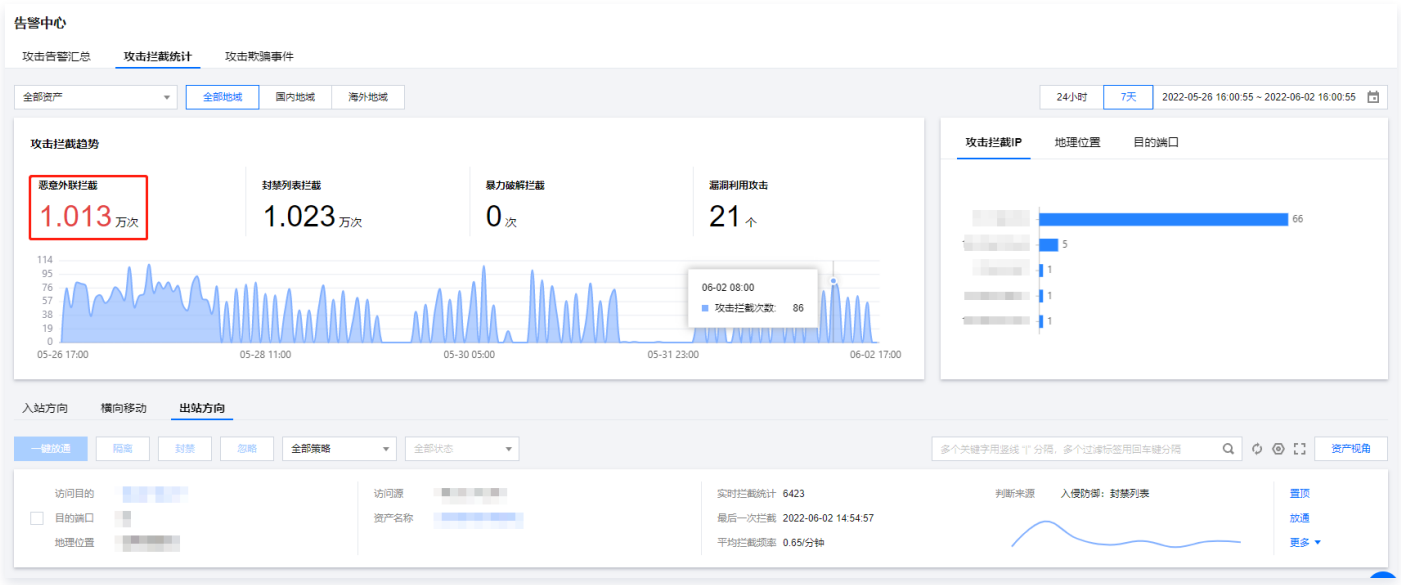
云防火墙检测挖矿蠕虫的原理

腾讯云威胁情报能够实时检测到恶意外联的流量，内置腾讯安全全网威胁情报检测，对于恶意源 IP、危险域名的访问流量，进行精准识别，秒级自动更新。不管是公网资产或者是内网资产，对于流经云防火墙的流量都会进行检测，如果检测到有挖矿蠕虫攻击流量，则会将主机标记为失陷主机，展示在 告警中心 。

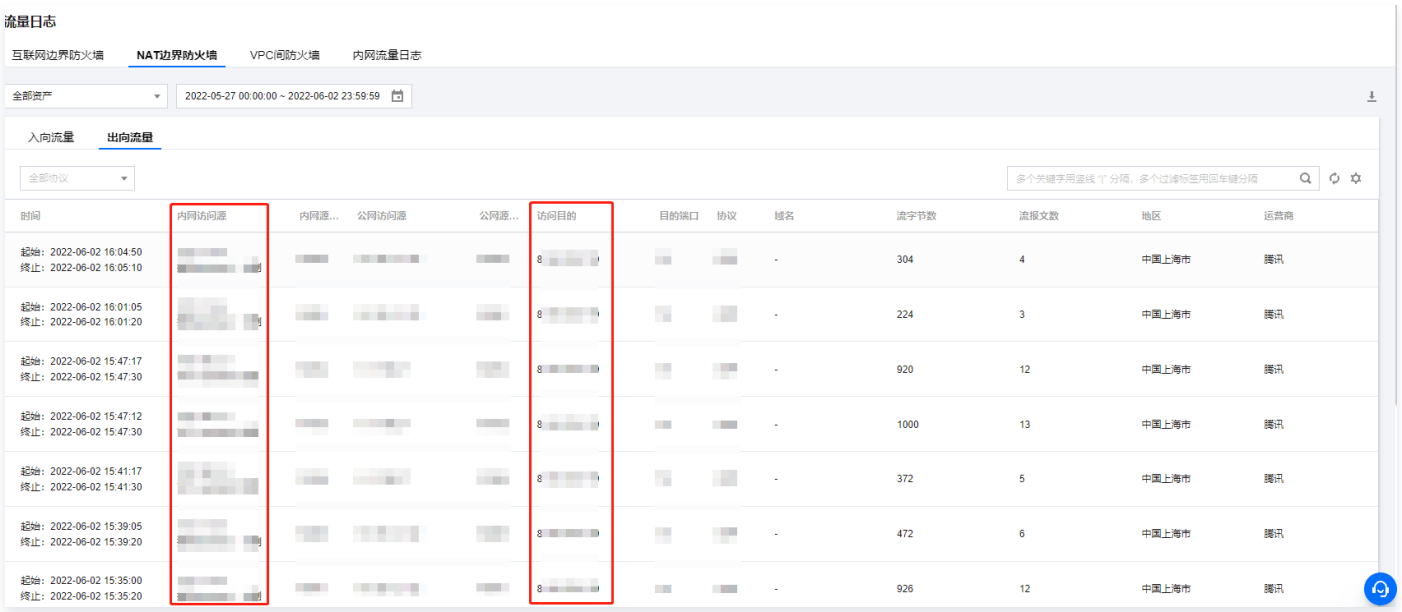
入侵后如何利用云防火墙快速止血

如果服务器已经被挖矿蠕虫成功入侵，可以利用云防火墙快速定位风险主机，再利用主机安全针对感染挖矿蠕虫的主机做查杀，从而避免被黑客恶意上传文件、造成信息泄露等风险。

- 对于公网资产，云防火墙的互联网边界能够识别，如果是公网资产中了挖矿蠕虫，威胁情报能够第一时间定位到是哪个资产，并能够自动拦截。



- **对于私网资产，这类资产需要经过地址转换才能访问互联网，云防火墙只能定位到转换后的公网地址，因此如果私网资产感染了挖矿蠕虫，需要将私网资产加入到 NAT 边界防火墙，告警中心会提示转换后的公网 IP 访问了矿池的 IP 或者域名，再根据矿池的 IP 或者域名到 NAT 边界防火墙的流量日志中，查询是哪台私网资产发生挖矿蠕虫行为，达到定位源主机的目的。**



- **主动配置访问控制规则拦截。当入侵防御检测到是哪台主机向互联网发起了挖矿行为，如果是公网资产，可以在 访问控制 > 互联网边界规则 > 出站规则中，配置拦截规则。**

- 如果是私有网络资产，可以在 访问控制 > **NAT 边界规则** > **出向规则**中，配置拦截规则。

云防火墙日志最佳实践

最近更新时间：2024-01-18 16:20:31

日志配置

使用云防火墙日志前，可在通用设置进行配置。

> **注意：**
> 仅支持企业版及以上用户可以修改日志存储类型和存储时长，每 2 个月仅可修改 1 次。您也可以 手动清空日志，但请注意每个用户每个自然月仅有 4 次机会。

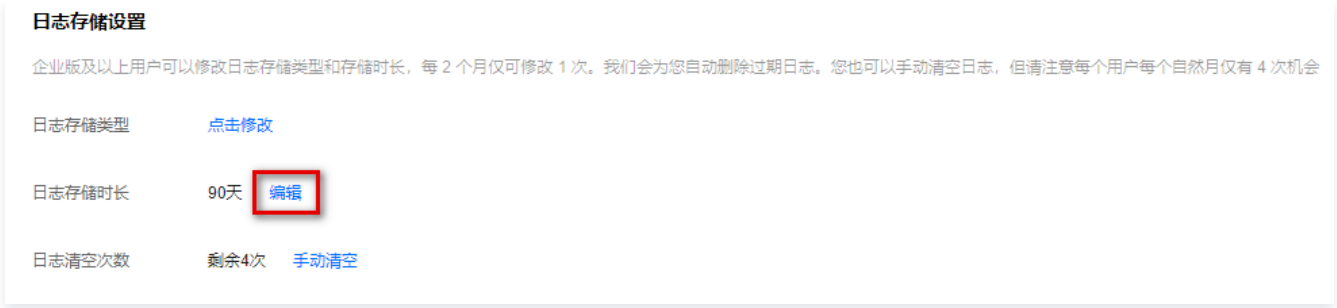
1. 登录 云防火墙控制台，在左侧导航中，单击**通用设置**。
2. 在通用设置页面，选择**日志存储设置**，支持设置如下内容：
   - 日志存储类型：单击**点击修改**，根据实际情况选择存储类型，单击**确定**保存。

     > **说明：**
     > 实际支持的存储类型以您在控制台的显示为准。

日志类型	日志详情
访问控制日志	• 互联网边界规则 • NAT 边界规则 • 内网间规则 • 企业安全组 • DNS 规则
零信任防护日志	• 远程运维登录 • Web 服务访问 • 数据库访问
入侵防御日志	• 威胁情报 • 基础防御 • 虚拟补丁 • 封禁列表 • 安全基线 • 网络蜜罐
流量日志	• 互联网边界防火墙 • NAT 边界防火墙 • VPC 间防火墙 • 内网流量日志 • DNS 防火墙

   - 日志存储时长：单击**编辑**，修改日志存储时长，单击**确认**。

     > **说明：**
     > • 云防火墙日志按照设置的存储时长滚动刷新，每天存储新产生的日志，并丢弃180天前的日志（以设置存储180天为例）。
     > • 按照等保合规要求，建议选择180天；如需180天以上，请 提交工单 联系我们。



- 日志清空次数：单击**手动清空**，经过二次确认后，即可清空日志。

> **注意：**
> 当前操作会删除所有日志，部分统计和报表数据将被丢弃，操作不可恢复，请谨慎操作；整个操作预计耗时10分钟左右，操作期间日志将停止写入。

查询日志

云防火墙的 日志审计功能 支持基于关键字的检索。同时，其 日志分析功能 不仅支持关键字搜索，还支持逻辑筛选（与、或、非、判断）。
在使用日志分析功能查询日志时，您可以进行以下操作：

- 查询原地址为114.67.120.184，端口为22的日志：`src_ip:114.67.120.184 AND src_port:22` 。
- 查询原地址为114.67.120.184，端口不为22的日志：`src_ip:114.67.120.184 NOT src_port:22` 。
- 查询时间在1月11日22点~13点之间，资产上的告警：dst_ip:112.56.189.6，左上角筛选时间为22点。

导出日志

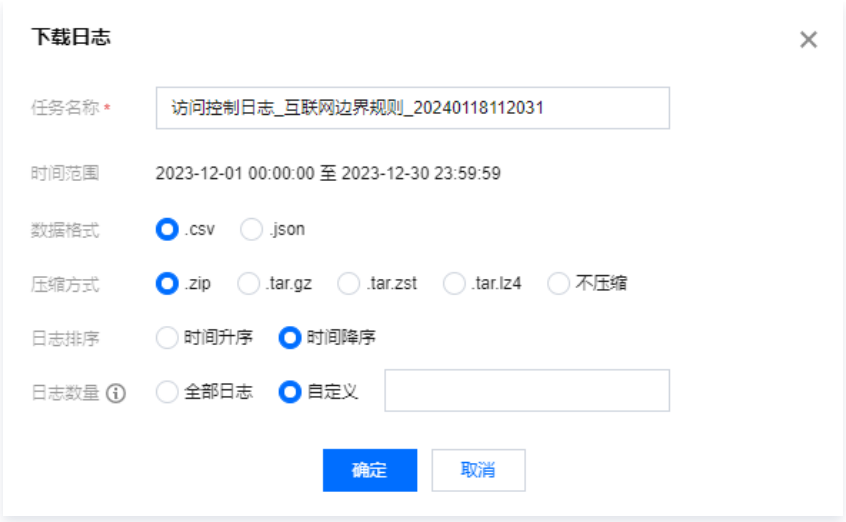
用户可根据自己需求选择对应的日志模块将日志下载导出，支持将日志导出并下载到本地，或者导出到用户自有的COS。

> **注意：**
> - 导出至 COS 可能会产生一定存储费用和下载费用，详情参考 费用说明 。
> - 零信任防护日志暂不支持导出远程运维登录日志和 Web 服务访问日志。
> - 不支持筛选结果后导出，云防火墙日志仅支持单次离线导出；如需导出筛选后的日志结果，请使用 云安全中心的日志分析功能 。
> - 同一时间仅能执行一个下载任务，多个下载任务将按照创建时间依次执行。

1. 登录 云防火墙控制台，在左侧导航中，单击**日志审计 > 访问控制日志**。
2. 在互联网边界规则页面，选择所需规则，单击 ，选择**下载日志/导出到 COS**。

- 下载日志：选择数据格式、压缩方法等参数，单击**确定**。

> **说明：**
> 当前每月日志导出下载至本地的日志免费配额为1GB，单次导出做多支持100w条，日志下载文件有效期为3天。



- 导出到 COS：选择存储桶，保存时间等参数，单击**确定**。

> **说明：**
> - 导出至自有 COS 额度不受限制，默认单次导出日志数量为100w条，可 提交工单 联系我们后端开白至5kw。
> - 若需按条件筛选导出至自有 COS，可提供筛选条件后 提交工单 联系我们协助处理。

日志投递

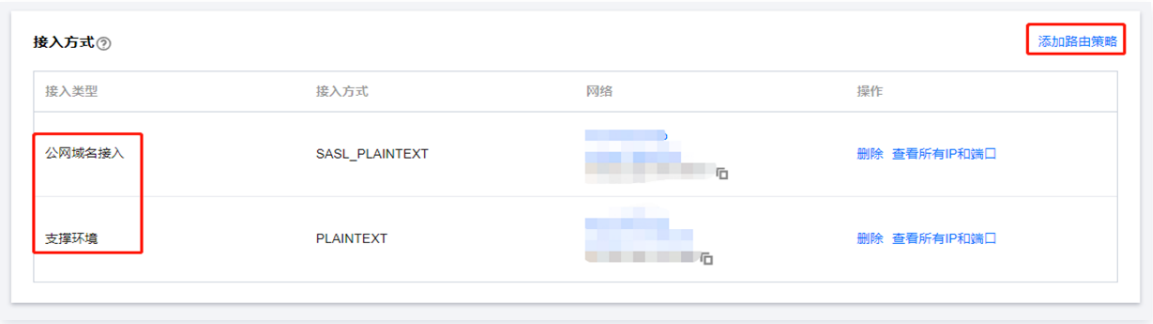
前提条件

- 需已购买 腾讯云消息队列 Ckafka 实例 和 云防火墙日志分析，按照云防火墙带宽来配置Ckafka 实例的带宽规格。
- 根据 消息队列 Ckafka 文档 指引，联系腾讯云客服开通**公网域名接入**或**支撑环境接入**白名单。
- 根据 创建实例文档 指引，创建一个 Ckafka 实例。
- 仅支持使用一个消息队列 Ckafka 账号进行日志投递。

操作步骤

1. 登录 消息队列 CKafka 版控制台，在左侧导航中，单击**实例列表**。
2. 在实例列表页面，单击所需 **Ckafka 实例名**。
3. 在实例详情页面，单击 **topic 管理 > 新建**。
4. 在新建 Topic 窗口中，配置相关参数，单击**提交**。更多详情请参见 创建 Topic 。
5. 在基本信息页面的接入方式中，单击**添加路由策略**，添加公网域名接入或支撑环境接入。更多详情请参见 添加路由策略 。

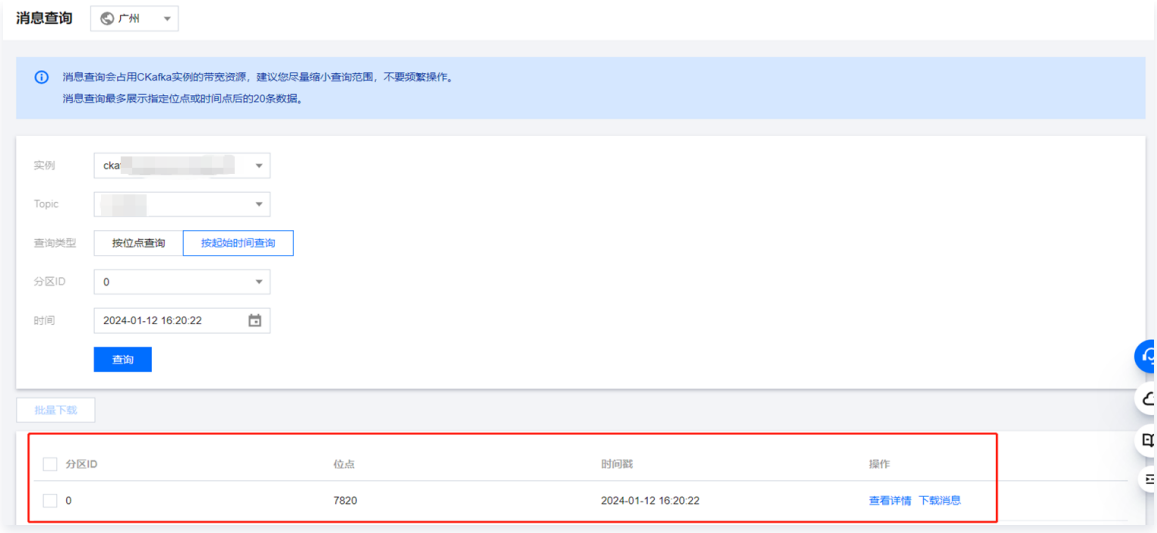
> **说明：**
> 支撑环境接入 CKafka 时需 提交工单，转 Ckafka 消息队列小助手加白名单才可以使用。



6. 在 ACL 策略管理页面，单击**用户管理 > 新建**，填写用户名和密码信息，单击**提交**。更多详情请参见 配置 ACL 策略 。
7. 在 日志分析页面，单击**日志投递**，选择**网络接入方式**、**Topic ID/名称**，单击**确定**。

> **说明：**
> 日志投递功能支持多种云防火墙日志类型的投递，不同类型的日志需要投递到不同的 Ckafka topic 中。每个 Ckafka topic 只能被一个云防火墙日志类型所绑定。

8. 投递完成后，可前往 消息队列 Ckafka-消息查询 查看日志是否投递成功。



日志规格与超量

日志存储空间容量占满后将无法写入日志，当您的日志存储容量达到上限后将不再进行写入，请您提前升级扩容或备份日志数据后清空日志，避免新的日志数据无法写入。

如需升级扩容日志容量，可以选择按量计费和包年包月两种模式：

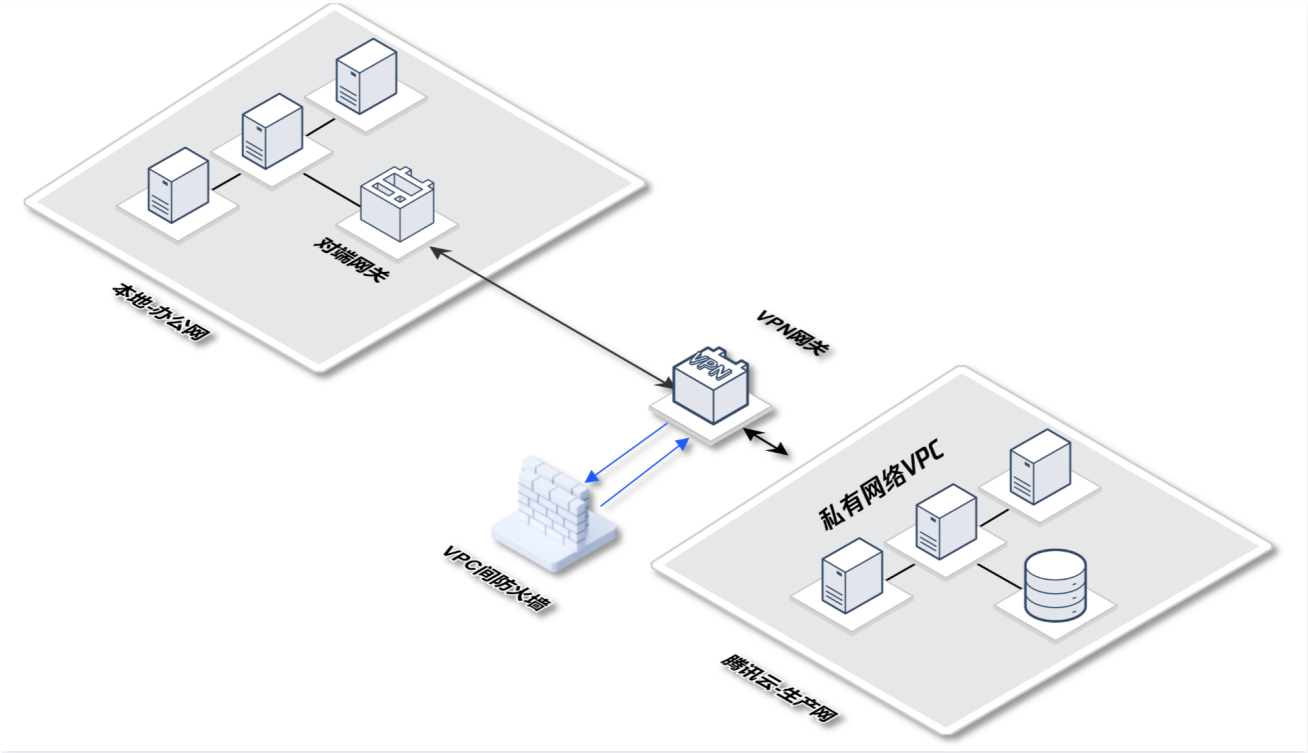
包年包月	按量计费
0.5元/GB/月，存储时间与版本购买时间相同。	1000GB至6120GB区间0.036元/GB/天，超过6120GB以上部分0.025元/GB/天。

VPC 间防火墙最佳实践

最近更新时间：2024-02-20 10:59:11

VPN 上云场景

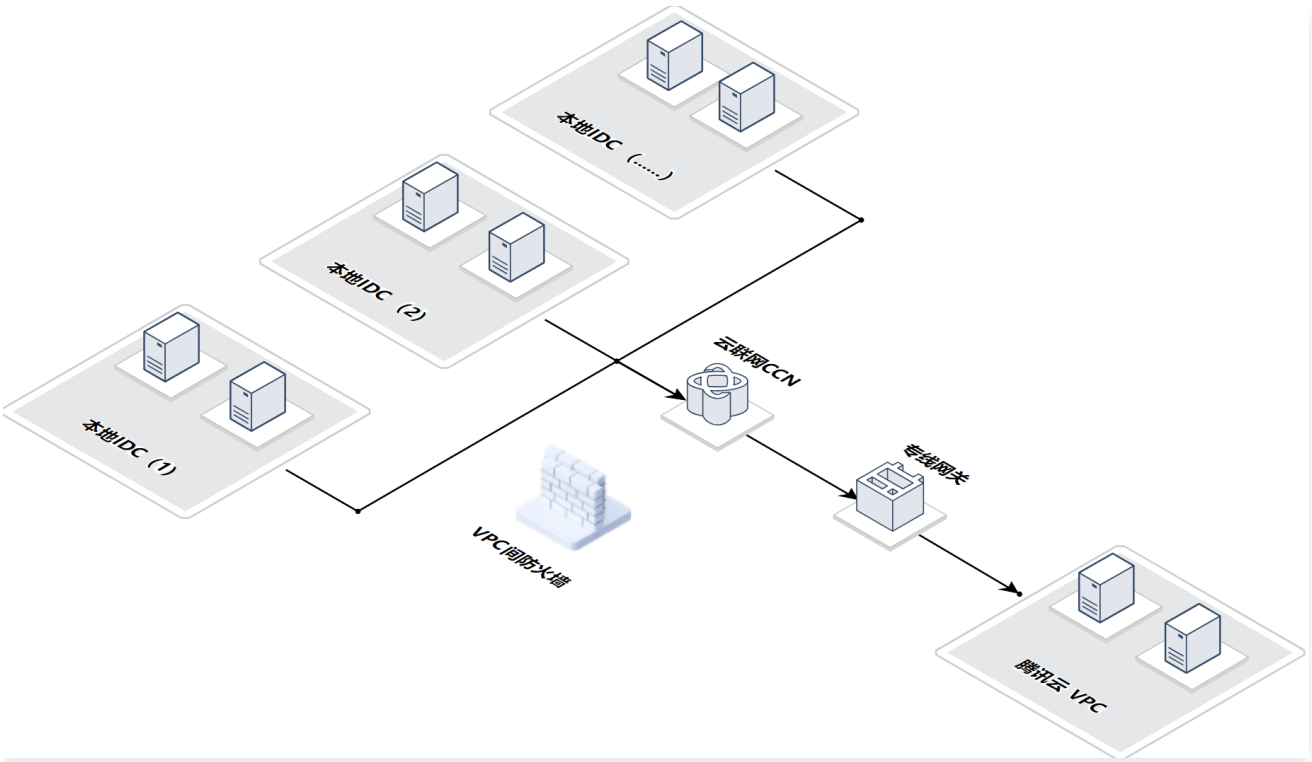
- 用户需求：采用 VPN 连接办公网和公有云，核心业务和数据在公有云上，办公网安全监控情况低于生产网。
- 业务挑战：当因为钓鱼等攻击导致本地办公网失陷时，攻击者可以很轻易的通过 VPC 专线攻击云上核心业务。
- 解决方案：接入 VPC 间防火墙，并开启入侵防御拦截模式，自动阻断监测办公网对云上业务的访问行为，阻断扫描、攻击流量。
- 实践配置：参考 新建 VPC 间防火墙 进行配置，选择**云联网模式**接入，防火墙 VPC 选择**自动选择**，路由模式选择**单点互通**。



混合云场景

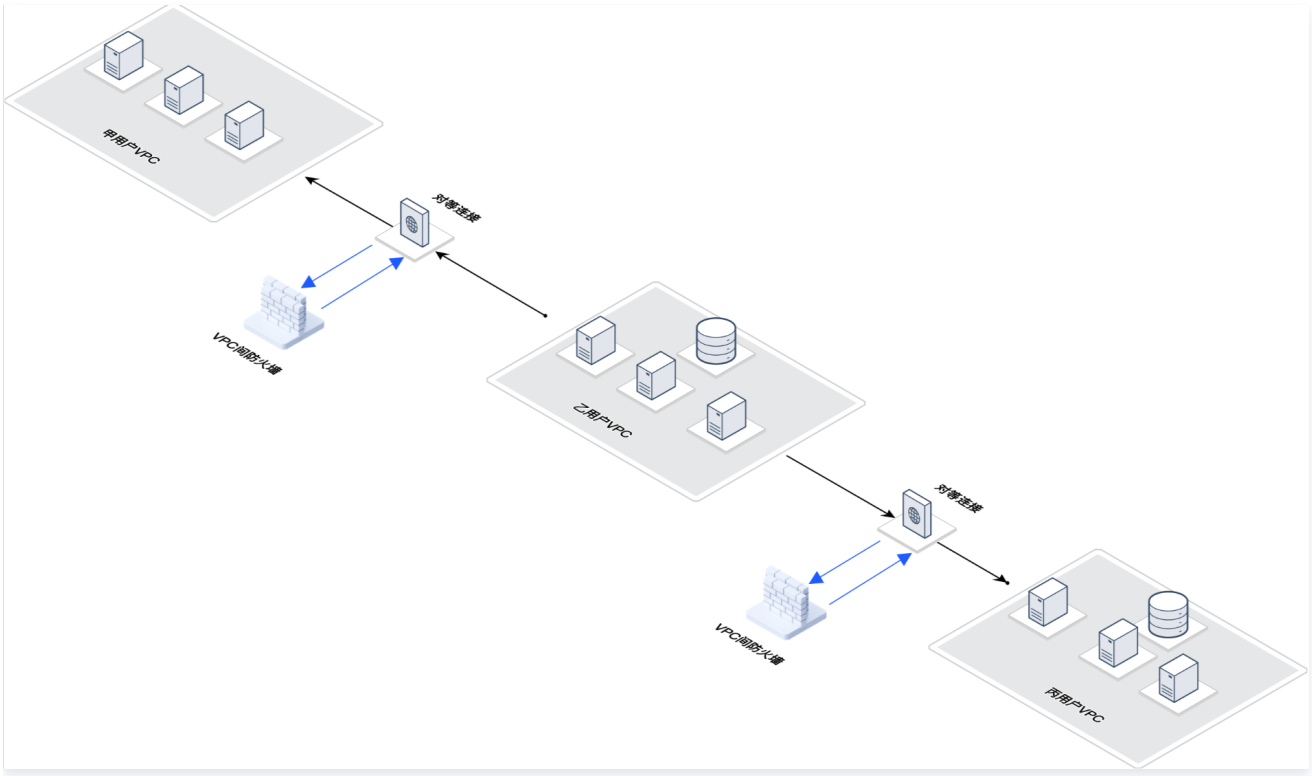
- 用户需求：客户有多个本地 IDC，通过云联网互联，并使用专线打通公有云 VPC。
- 业务挑战：当需要隔离部分 IDC，不允许这些 IDC 访问公有云业务；同时需要避免本地 IDC 失陷后 ，横向扩散到云上。
- 解决方案：接入 VPC 间防火墙，并开启入侵防御。设置访问控制规则，对源地址为某些 IDC 的进行阻断。
- 实践配置：参考 新建 VPC 间防火墙 进行配置，选择**云联网模式**接入，防火墙 VPC 选择**自动选择**，路由模式选择**多点互通**（如本地 IDC 数量较少，可选择单点互通）。

版权所有：腾讯云计算（北京）有限责任公司



跨账号对等连接场景

- 用户需求：乙用户云上业务，需要向甲、丙用户获取数据，要求数据只进不出。
- 业务挑战：需要允许乙用户 VPC 访问甲、丙 VPC，为了确保数据安全，需要阻断甲用户 VPC、丙用户 VPC 对乙用户的访问。
- 解决方案：接入 VPC 间防火墙，配置访问控制规则，对目的地址为乙用户 VPC 的流量全部阻断。
- 实践配置：参考 新建 VPC 间防火墙 进行配置，选择**私有网络模式**接入，防火墙 VPC选择**自动选择**，路由模式选择**单点互通**。



热点问题

接入 VPC 间防火墙是否对业务有影响?

接入时会出现极短的闪断，建议选择业务较空闲时段进行。云防火墙可提供研发支持，根据经验，接入 VPC 间防火墙对业务影响较小。如担心对业务产生影响，可在测试环境进行尝试。

能否通过安全组替代 VPC 间防火墙?

VPC 间防火墙可以进行日志的审计，观察到命中的规则和放行的流量，但服务器的安全组则无此功能。同时，VPC 间防火墙的入侵防御功能可以应对流量中的威胁，监测发起的扫描流量和攻击流量，而安全组则不具备此功能。

版权所有：腾讯云计算（北京）有限责任公司