云防火墙

实践教程

产品文档

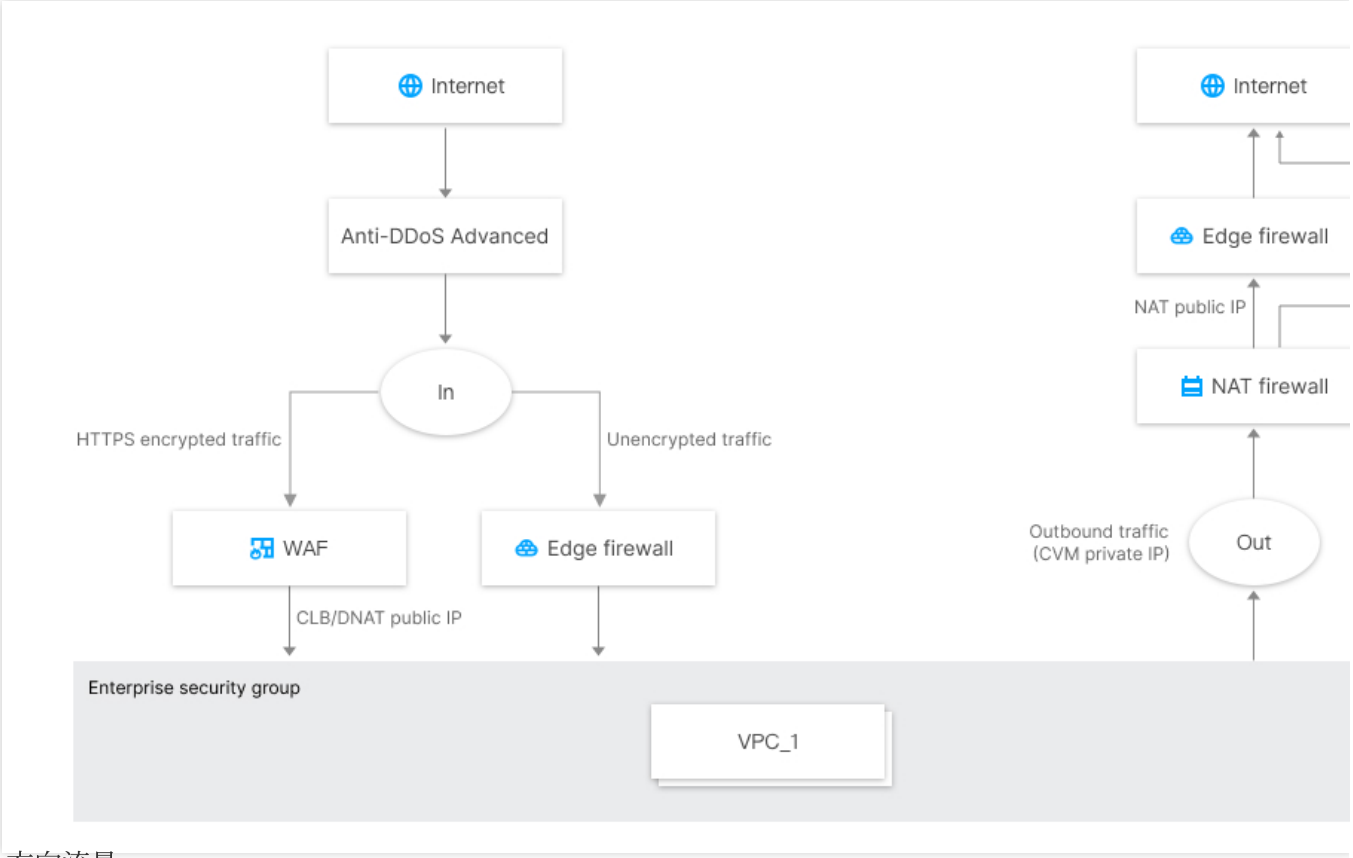
腾讯云

文档目录

实践教程
云防火墙与其他产品的联合防护

最近更新时间：2023-12-11 16:40:32

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 的流量仍然会经过互联网边界 FW。

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：2023-12-11 16:40:39

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：

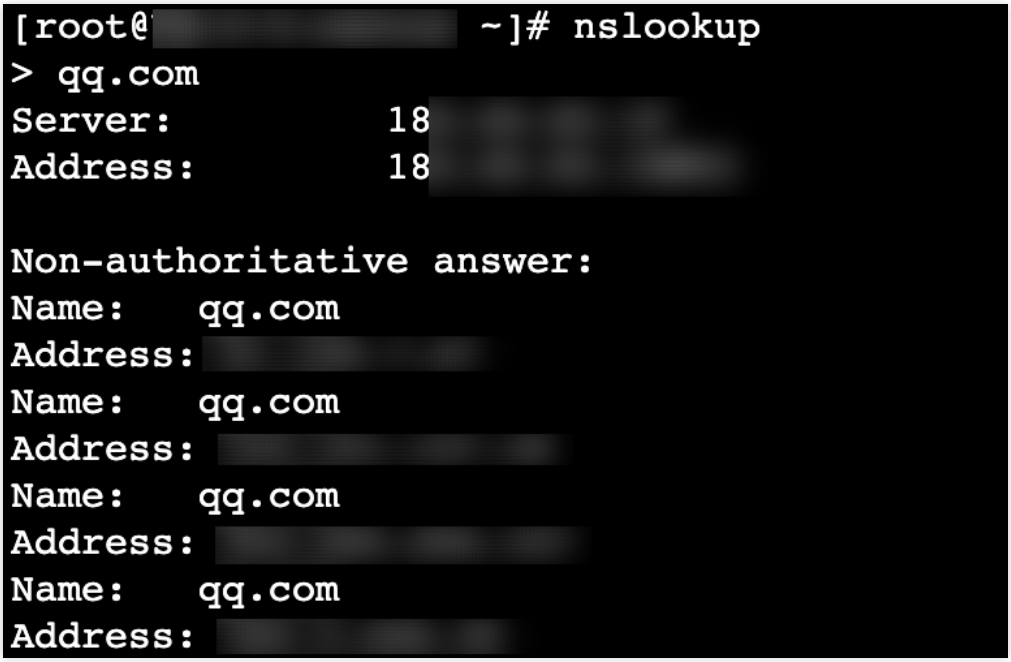
创建相关地区 NAT 防火墙接入 VPC 网络。

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）

开启 DNS 开关进行验证 DNS 地址。

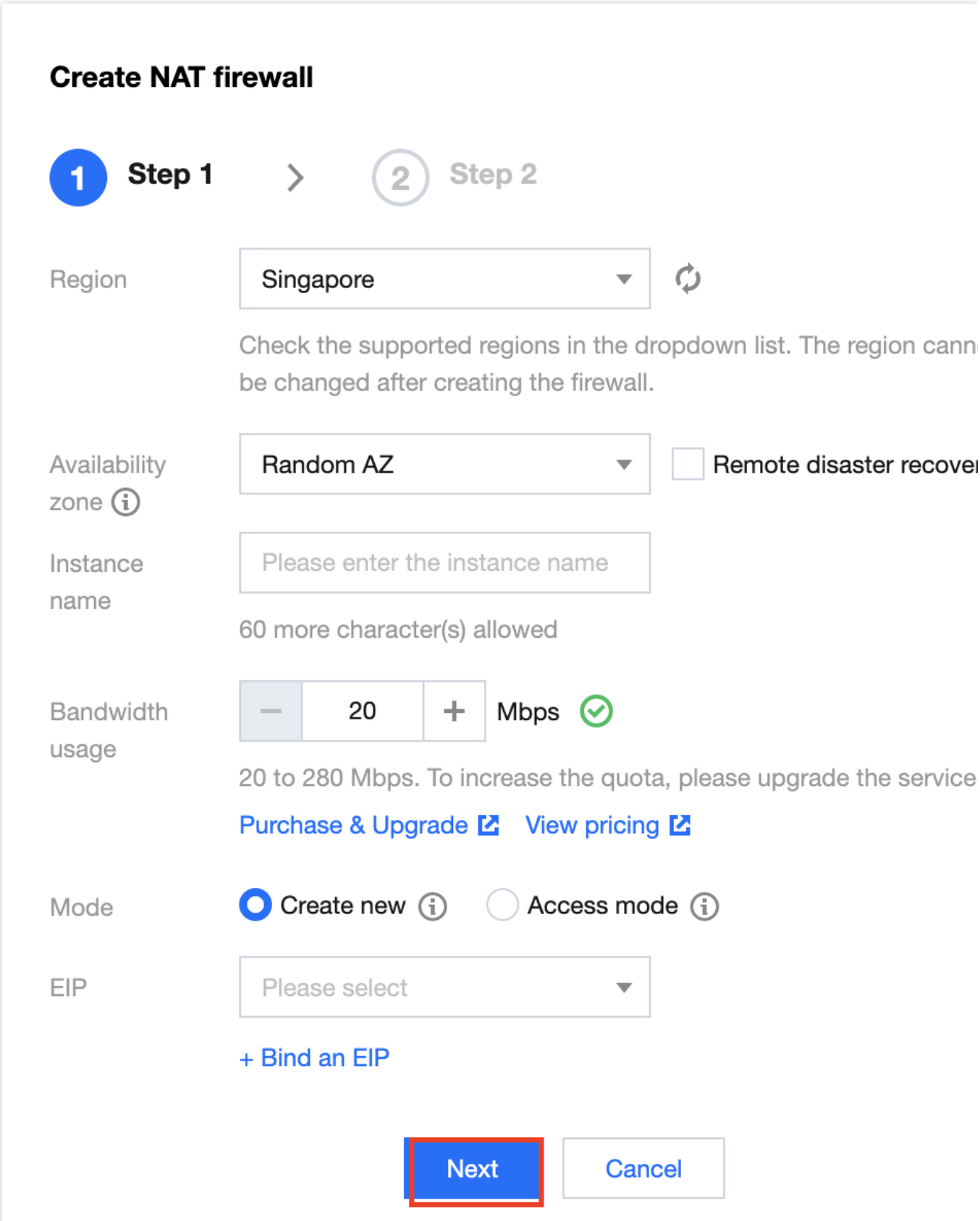
使用 NAT 防火墙访问控制限制 DNS 解析（验证）。

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。

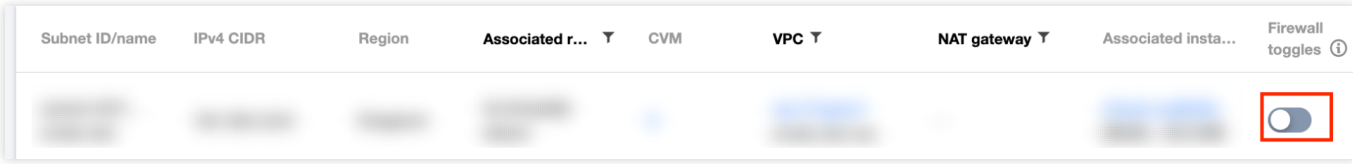
弹性 IP：若选择新建弹性 IP，系统会自动为用户申请一个弹性 IP，用户也可从所有闲置的弹性 IP 中选择一个进行绑定。

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

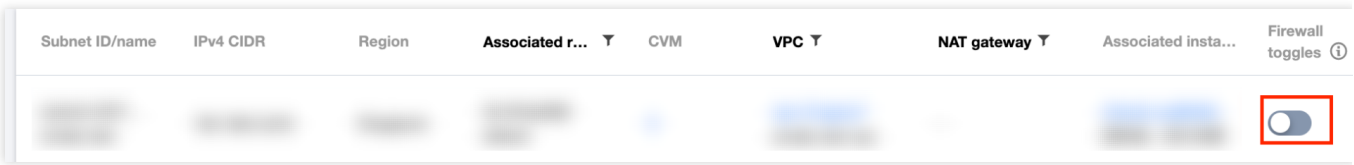
在 NAT 边界开关页面，单击**防火墙开关**，根据实际需求选择数据库所在的子网，单击

开启防火墙开关。



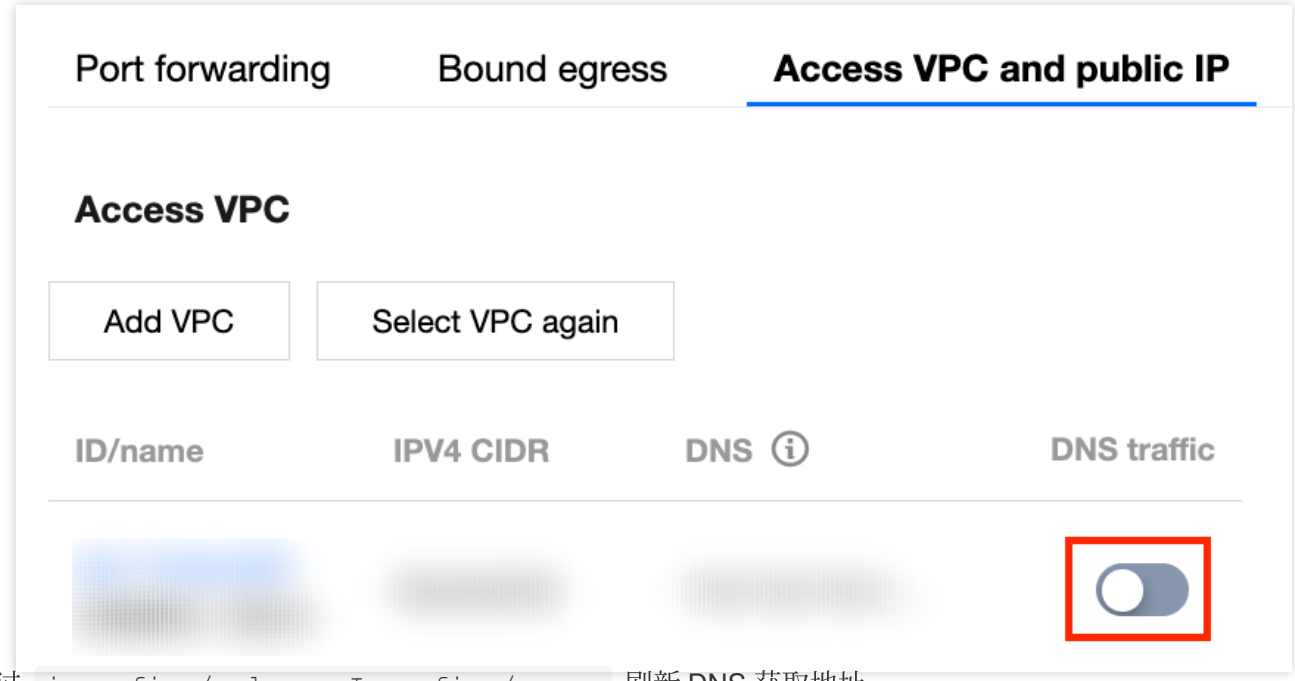
步骤3：开开启和验证 DNS

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**。

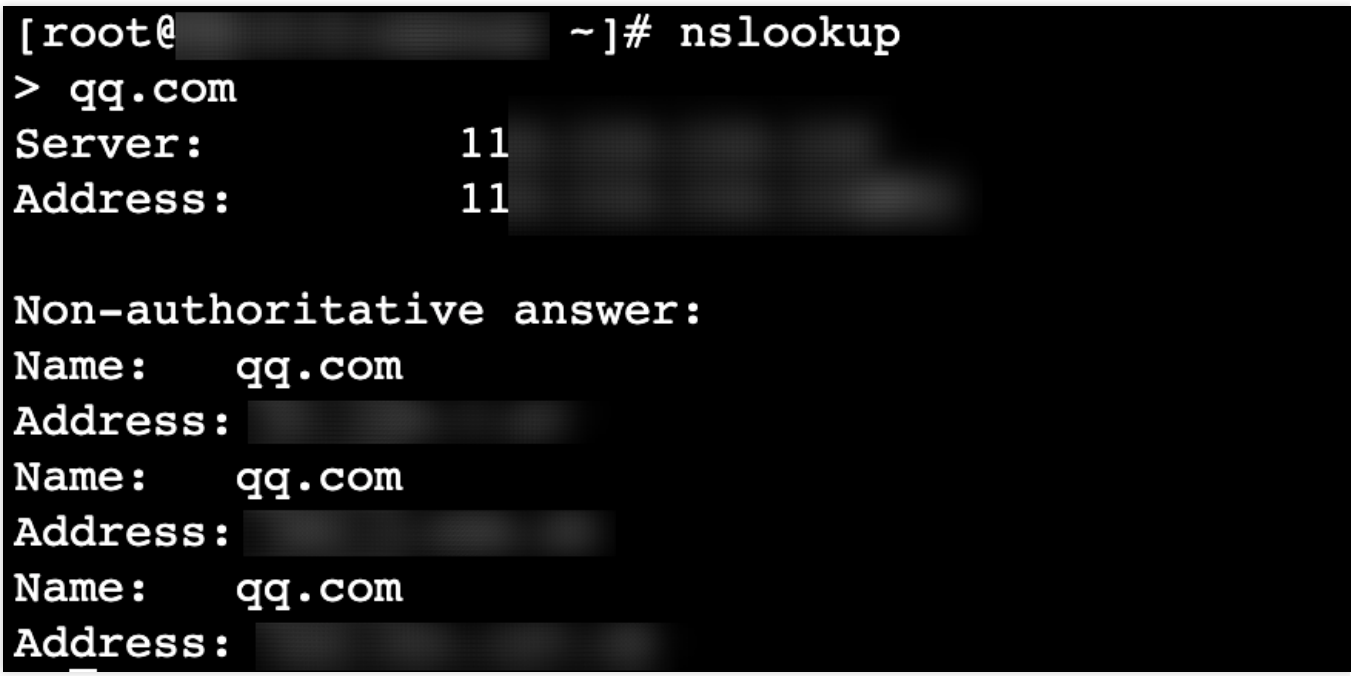


2. 在接入 VPC 与公网 IP 页面，选择所需 ID，单击

开启 DNS 流量。

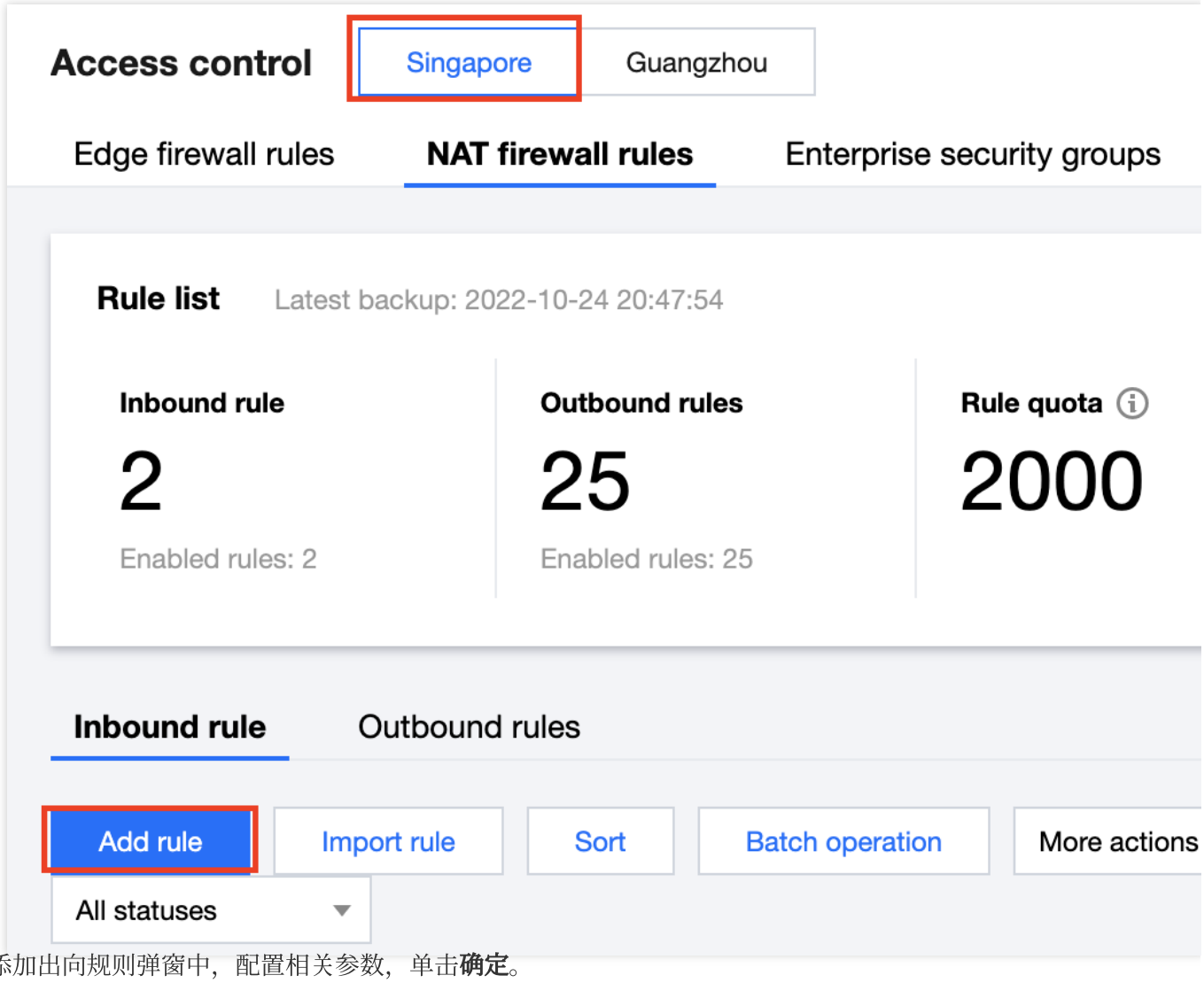


3. 通过 `ipconfig /release Ipconfig /renew` 刷新 DNS 获取地址。

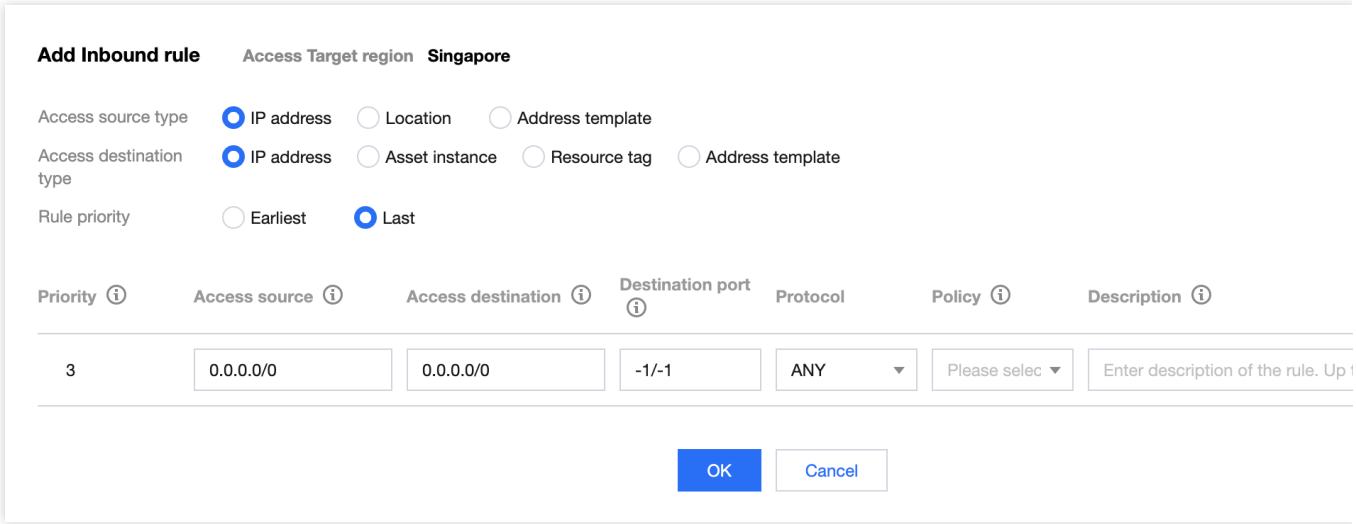


步骤4：限制 DNS 解析

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：

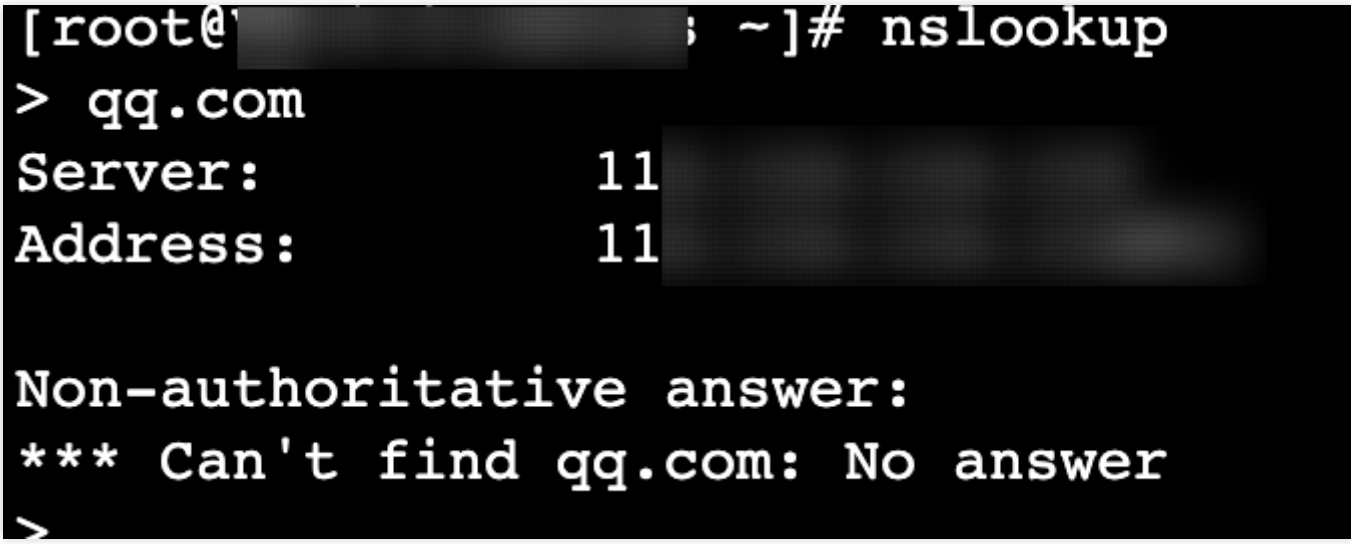
放行：放通命中规则的流量，记录命中次数但不记录访问控制日志，且记录流量日志。

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，但不记录流量日志。

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。



云防火墙防挖矿实践教程

最近更新时间：2024-07-09 16:26:55

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）
		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。

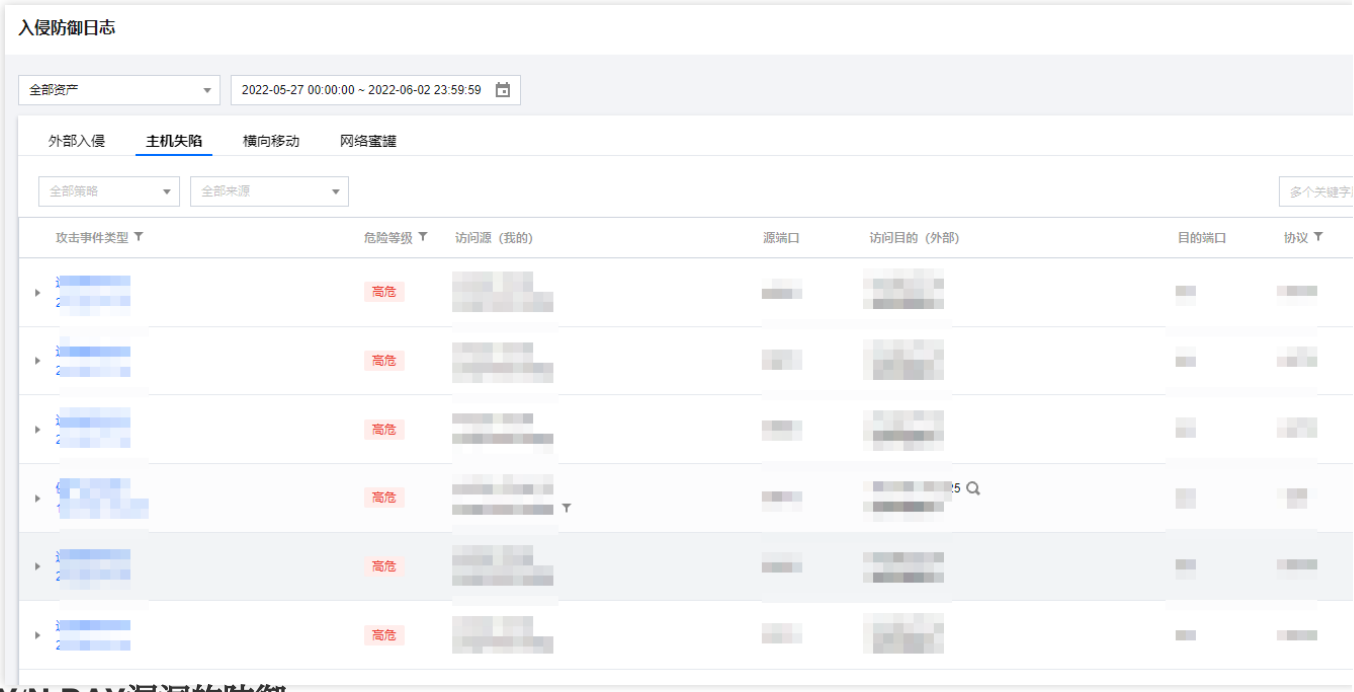
说明

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

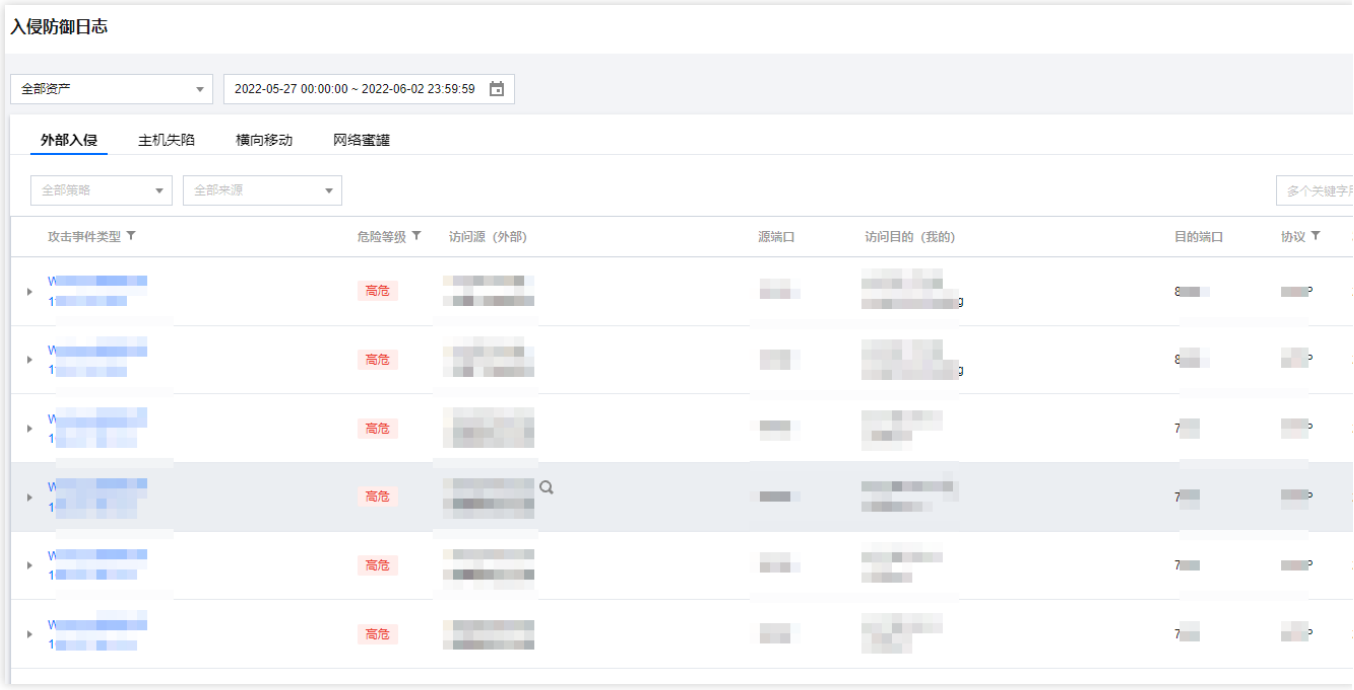
一些热门 0 Day、N Day 漏洞修复不及时，被挖矿蠕虫利用感染的风险较大。云防火墙利用腾讯云情报中心实时获取漏洞情报，可及时发现关于 0 Day、N Day 的漏洞，并且能第一时间获取漏洞 POC，并落地形成虚拟补丁规则库，在与黑客的攻防对抗中占得时间先机。如下所示：

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

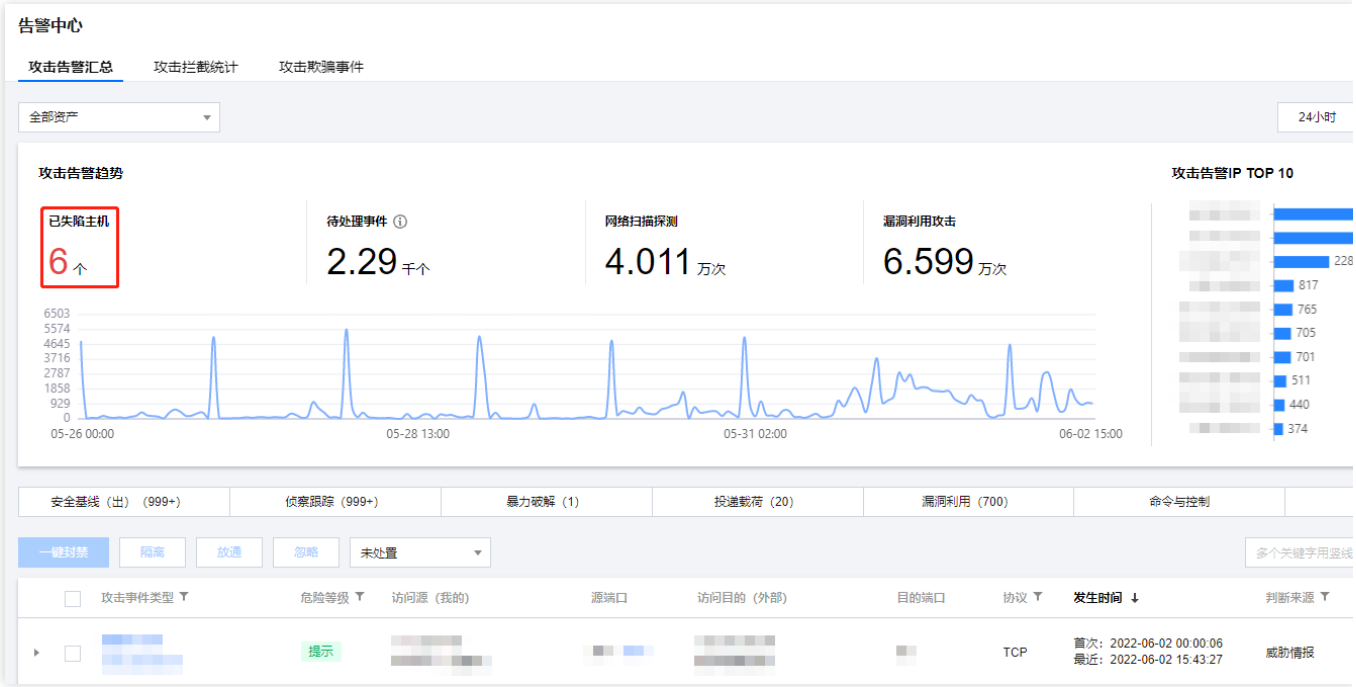
开启虚拟补丁开关，并选择防护模式为拦截模式或者严格模式。

3. 在 入侵防御日志页面，可以查看入侵日志详情。



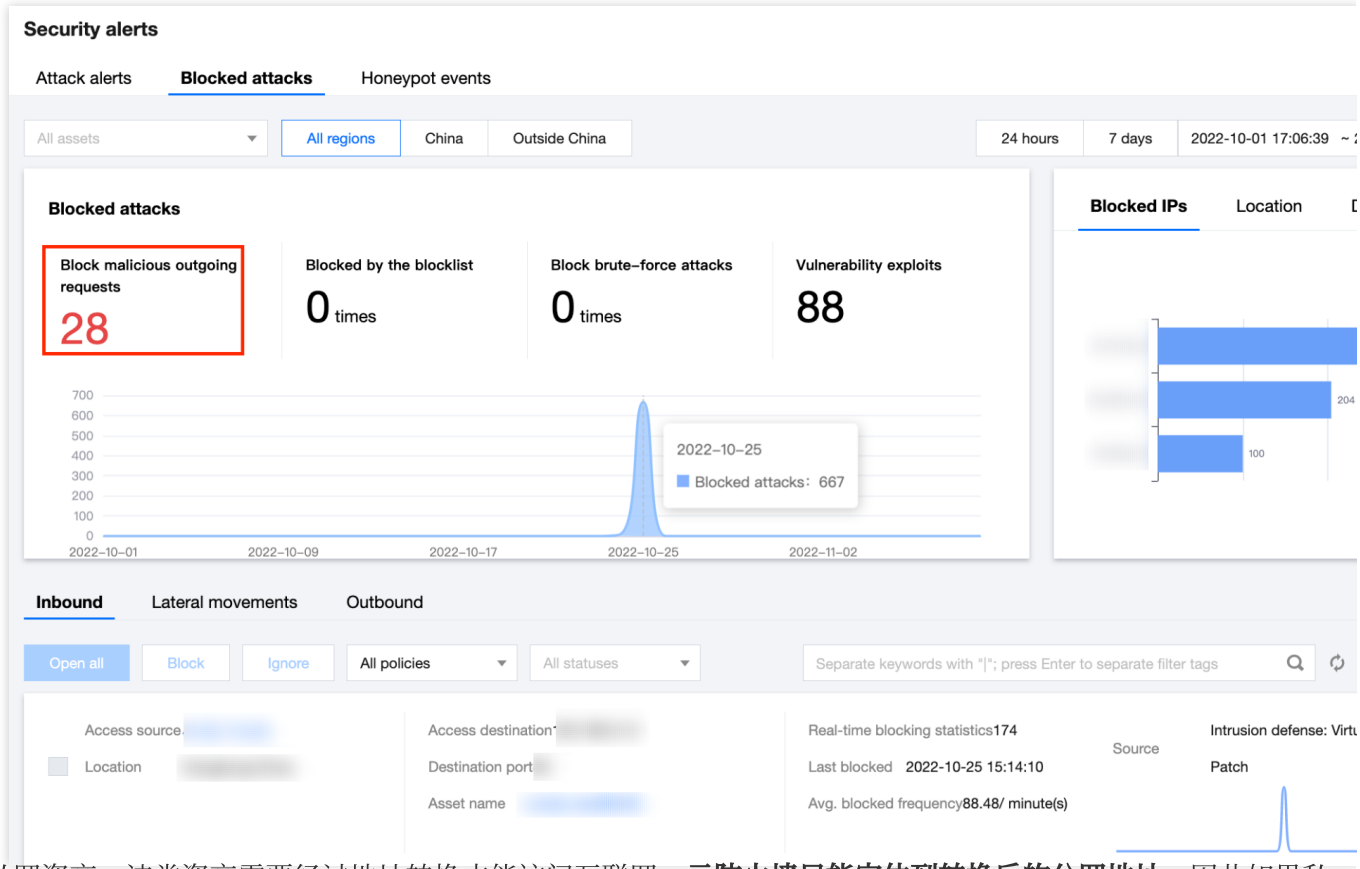
云防火墙检测挖矿蠕虫的原理

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。

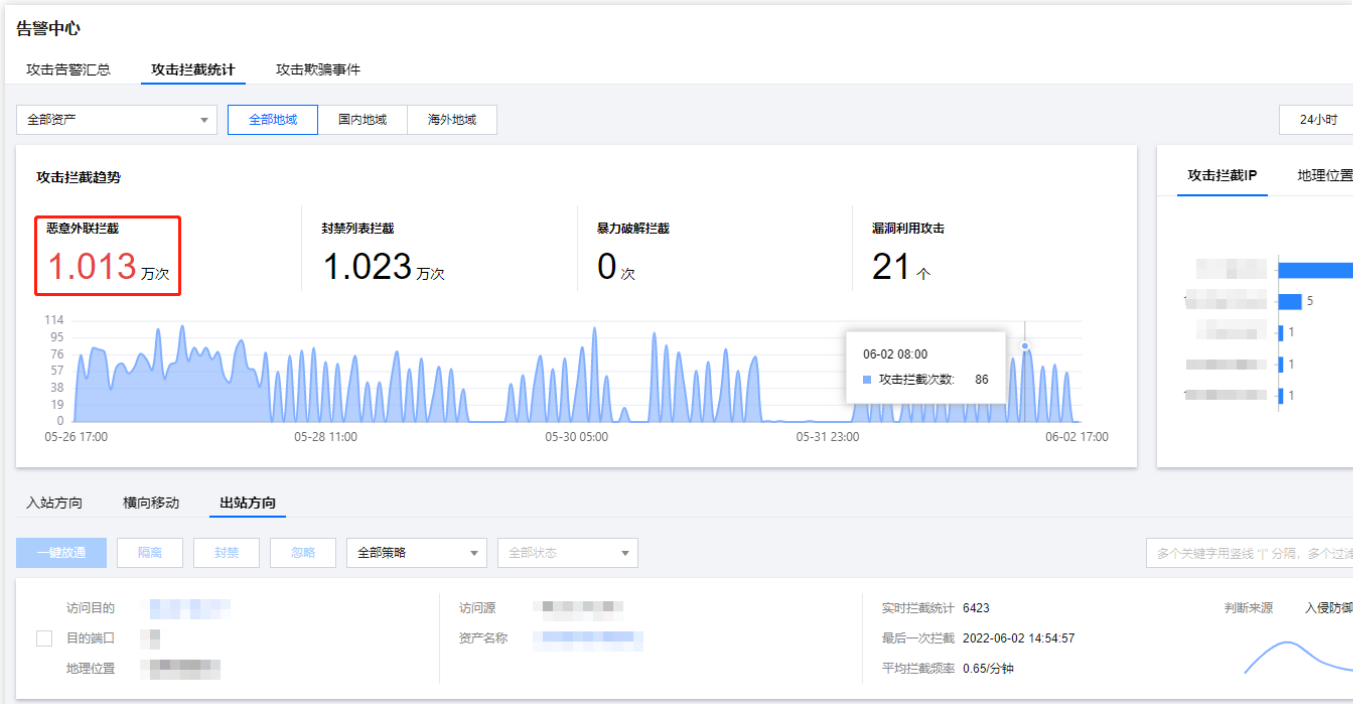


入侵后如何利用云防火墙快速止血

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，再利用云镜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。