防火墙管理

实践教程

腾讯云

【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

实践教程
企业安全组封禁高危端口实践教程

最近更新时间：2026-03-18 15:37:52

本教程指导您如何通过防火墙管理的策略管理功能，批量封禁指定的高危端口（如TCP 20, 3389），并为内网特定 IP 地址创建例外放行规则。

前提条件

已授权使用腾讯云防火墙管理产品。具体操作请参见 欢迎页操作指南 。

步骤一：创建高危端口封禁规则组

1. 登录 防火墙管理控制台 ，在左侧导航中，选择**策略管理 > 规则组管理**。
2. 单击**云防火墙-企业安全组**，切换到云防火墙-企业安全组界面。
3. 单击**新建规则组**，在添加规则组窗口中，配置相关参数。

参数名称	说明
规则组名称	**企业安全组封禁高危端口实践教程**。
所属产品	选择**云防火墙-企业安全组**。
组内优先级	自动设置为**1**。
IP 类型	选择 **IPv4**。
访问源	选择 **IP/CIDR** 并输入全0的 IP 地址，同步所有实例。也可选择资源标签，配置步骤可参考 创建标签 、绑定资源 。

访问目的	选择 IP/CIDR 并输入全0的 IP 地址，同步所有实例。也可选择资源标签，配置步骤可参考 创建标签 、绑定资源 。
目的端口	选择**手动填写**并输入20,3389。
协议	选择 TCP。
生效范围	选择**安全组**。
策略	选择**拒绝**。
描述	**封禁高危端口#仅下发访问目的**。

4. 单击**确定**。规则组将出现在列表中，此时规则尚未下发，不会生效。

步骤二：创建内网白名单 IP 地址

为使内网特定 IP 地址能正常访问高危端口，需先在私有网络（VPC）中创建一个 IP 地址参数模板作为白名单。

1. 访问 私有网络控制台 ，在左侧导航中，选择**安全** > **参数模板**。
2. 在**参数模板** > **IP 地址页面**，单击**新建**。
3. 参考 创建 IP 地址参数模板 ，配置相关参数。单击**确定**。

4. 在 IP 地址页签中，可以看到刚刚创建的加白 IP 地址参数模板。

步骤三：在规则组中添加内网放行规则

返回云防火墙控制台，在已创建的规则组中添加一条优先级更高的允许规则。

1. 返回 防火墙管理控制台 ，在左侧导航中，选择**策略管理 > 规则组管理**。
2. 单击**云防火墙-企业安全组**，切换到云防火墙-企业安全组界面。
3. 在规则组列表中找到您在 步骤一：创建高危端口封禁规则组 中创建的规则组，单击其操作栏的**编辑**。

4. 在编辑页面，单击**新建规则**，配置相关参数。

参数名称	说明
组内优先级	设置为1（确保优先级在 步骤一：创建高危端口封禁规则组 中创建的规则之上）。
IP 类型	选择 IPv4。
访问源	选择**参数模板**，然后选中您在 步骤二：创建内网白名单IP地址 创建的内网放行白名单。
访问目的	选择 IP/CIDR 并输入全0的 IP 地址，同步所有实例。也可选择资源标签，配置步骤可参考 创建标签 、绑定资源 。
目的端口	选择**手动填写**并输入20,3389
协议	选择 TCP。

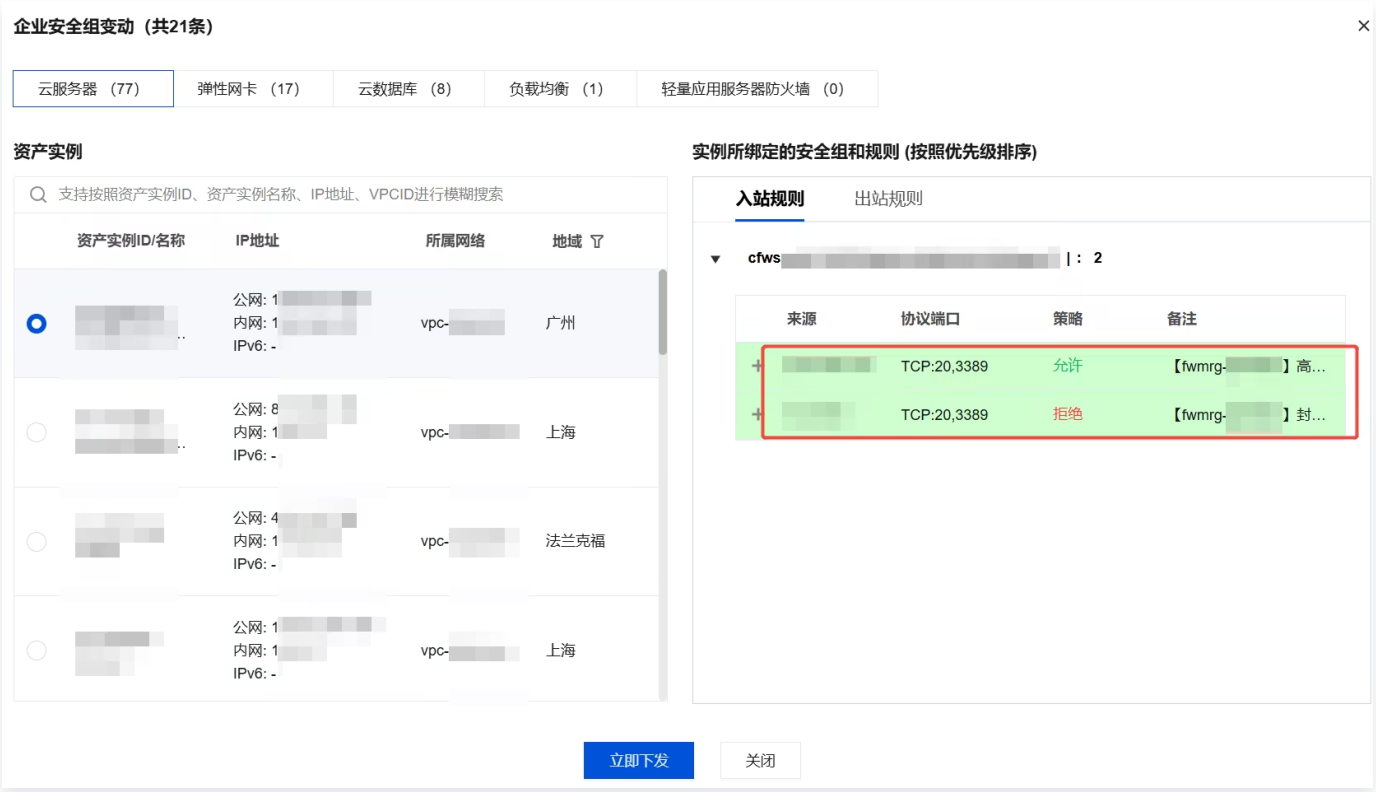
生效范围	选择**安全组**。
策略	选择**允许**。
描述	**高危端口白名单访问规则**。

5. 单击**确定**。规则组将出现在列表中，此时规则尚未下发，不会生效。

步骤四：预览并下发规则

规则配置完成后，必须下发才能生效。下发前建议预览变动。

1. 登录 防火墙管理控制台 ，在左侧导航中，选择**策略管理** > **规则下发管理**。
2. 单击**云防火墙-企业安全组**，切换到云防火墙-企业安全组界面。
3. 在云防火墙-企业安全组页面，单击**预览变动**。
4. 在预览变动页面，可查看企业安全组变动。
   - 页面左侧为资产实例，包括云服务器、弹性网卡、云数据库、负载均衡以及轻量应用服务器防火墙。
   - 页面右侧为实例所绑定的安全组和规则（按照优先级排序），分为入站规则和出站规则，其中若变动为新增，则背景色为绿色。若变动为删除，则背景色为红色。



5. 预览无误后，单击**立即下发**。

> **注意：**
> 下发会将所有安全产品中所有的未下发、待下发以及下发失败规则进行下发。

步骤五：查看操作日志

您可以在日志中追溯所有配置操作，便于审计和排障。

1. 登录 防火墙管理控制台 ，在左侧导航中，选择**日志管理** > **策略管理**。
2. 在**策略管理**页面，系统记录所有与规则组和下发相关的操作，如“创建规则组”、“添加规则”、“立即下发”等。您可以查看操作时间、账号、具体行为及关联的规则组。
3. 单击**详情**可查看操作日志的详细信息。

操作时间	操作账号	操作模块	产品	操作行为	关联规则组名称及ID	操作
2026-02-04 16:23:56	[redacted]	规则下发管理	云防火墙-企业安全组	添加规则	99 fwmrg_y6e4yn6ncf	详情
2026-02-04 16:23:47	[redacted]	规则下发管理	云防火墙-企业安全组	立即下发	企业安全组封禁高危端口实践教程 (+5) fwmrg-e68lrnia	详情
2026-02-04 16:23:38	[redacted]	规则下发管理	云防火墙-企业安全组	添加规则	企业安全组封禁高危端口实践教程 fwmrg-e68lrnia	详情
2026-02-04 16:23:21	[redacted]	规则管理	云防火墙-企业安全组	添加规则	企业安全组封禁高危端口实践教程 fwmrg-e68lrnia	详情
2026-02-04 16:22:41	[redacted]	规则管理	云防火墙-企业安全组	创建规则组	企业安全组封禁高危端口实践教程 fwmrg-e68lrnia	详情

相关文档

当您的腾讯云账号下拥有多种云产品资源时，例如云服务器实例、云硬盘实例、对象存储桶等资源，您可以通过创建标签并绑定资源来完成资源的分类和统一管理。配置步骤可参考 创建标签 、绑定资源 。