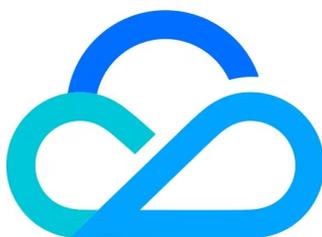


防火墙管理 实践教程



腾讯云

【 版权声明 】

©2013–2026 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 】



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

实践教程

企业安全组封禁高危端口实践教程

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。

添加规则组

基础配置

规则组名称	企业安全组封禁高危端口实践教程	15/50
所属产品	云防火墙-企业安全组	

规则编排

① 配置规则需手动下发：创建规则后，请前往【策略管理-规则下发管理】模块，点击【立即下发】以使规则生效。

② 基于 IP 配置的风险提示：在资产 IP 不重复的情况下，您可通过 IP 地址快捷配置安全组规则。但需注意：若某 IP 绑定了多个实例，该 IP 的规则将对其下所有实例生效。后续如因资产变更导致该 IP 对应了新的实例，此规则也将自动扩展至所有关联实例。

组内优先级	IP类型	访问源	访问目的	目的端口	协议	生效范围	策略	描述	操作
1	IPv4	IP/C... 0.0.0.0/0 关联 120 个实例 详情	IP/C... 0.0.0.0/0 关联 120 个实例 详情	手动填写 20,3389	TCP	安全组	拒绝	封禁高危端口#仅下发访问目的	删除 重置

新增一条 您还可以增加0条

确定 取消

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。

规则组名称	规则组ID	规则数量	关联下发表数数量	关联下发表组	最近更新人	规则更新时间	创建人	创建时间	操作
企业安全组封禁高危端口访问教程	fwmg-igk36c	1	0	-		2026-02-04 14:51:49		2026-02-04 14:51:49	编辑 删除
www	fwmg-azmk36	1	0	-		2026-02-04 14:48:48		2026-02-04 14:48:48	编辑 删除
g测试风控风险	fwmg-5gybcr	3	1	最先执行		2026-02-04 14:42:39		2026-01-11 17:08:10	编辑 删除
自动g测试下发-LH	fwmg-en1h021a3	100	1	最先执行		2026-02-04 11:27:22		2026-01-11 15:31:51	编辑 删除
VPC资产实例测试	fwmg-u0abuk1r	2	0	-		2026-02-03 14:23:11		2026-01-29 15:37:08	编辑 删除
ENI参数模板	fwmg-jbebilm	2	1	最先执行		2026-02-02 20:21:50		2026-02-02 18:51:32	编辑 删除

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**。

新建 IP 地址 ×

名称

IP 地址

IP 地址 (i)	备注	操作
<input type="text" value=""/>	<input type="text" value="内网地址"/>	×

[+ 新增一行](#)

标签 (i)

标签键 (v)

标签值 (v)

×

[+ 添加标签](#) | [键值粘贴板](#) | [历史记录](#) (v)

确定
取消

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。

ID名称	详情	标签	最后更新时间 ↓	操作
内网放行			2025-02-04 14:55:53 (UTC+08:00)	管理 删除 查看关联 编辑标签
			2025-08-11 14:58:20 (UTC+08:00)	管理 删除 查看关联 编辑标签
			2024-11-08 16:13:32 (UTC+08:00)	管理 删除 查看关联 编辑标签

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。

规则组名称	规则组ID	规则数量	关联下发账号数量	关联下发阶段	最近更新人	规则更新时间 ↑ ↓	创建人	创建时间 ↑ ↓	操作
(手动)测试下发-高危不同资产	fwmg-5ygz98x	39	1	最后执行		2025-02-04 15:12:39		2025-01-08 19:17:48	编辑 删除
企业安全组封禁高危端口实践教程	fwmg-4kq3bc	1	0	-		2025-02-04 15:10:36		2025-02-04 14:51:49	编辑 删除
ww	fwmg-4zmk36	1	0	-		2025-02-04 14:48:48		2025-02-04 14:48:48	编辑 删除
测试构造风险	fwmg-5pybcnr	3	1	最先执行、最后执行		2025-02-04 14:42:39		2025-01-11 17:08:10	编辑 删除
(手动)测试下发-LH	fwmg-m1H921a3	100	1	最先执行		2025-02-04 11:27:22		2025-01-11 15:31:51	编辑 删除

4. 在编辑页面，单击新建规则，配置相关参数。

添加规则 ✕

① **配置规则需手动下发**：创建规则后，请前往【策略管理-规则下发管理】模块，点击【立即下发】以使规则生效。

② **基于 IP 配置的风险提示**：在资产 IP 不重复的情况下，您可通过 IP 地址快捷配置安全组规则。但需注意：若某 IP 绑定了多个实例，该 IP 的规则将对其下所有实例生效。后续如因资产变更导致该 IP 对应了新的实例，此规则也将自动扩展至所有关联实例。

组内优先级	IP类型	访问源 ①	访问目的 ①	目的端口 ①	协议	生效范围	策略 ①	描述 ①	操作
1	IPv4	参数... 内网放行	IP/C... 0.0.0.0/0	手动填写 20,3389	TCP	安全组	允许	高危端口白名单访问规则	编辑 删除

+ 新增一条 您还可以增加9条

确定
取消

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。

企业安全组变动 (共21条) ×

云服务器 (77)
弹性网卡 (17)
云数据库 (8)
负载均衡 (1)
轻量应用服务器防火墙 (0)

资产实例

Q 支持按照资产实例ID、资产实例名称、IP地址、VPCID进行模糊搜索

资产实例ID/名称	IP地址	所属网络	地域
<input checked="" type="radio"/>	公网: 1 内网: 1 IPv6: -	vpc-	广州
<input type="radio"/>	公网: 8 内网: 1 IPv6: -	vpc-	上海
<input type="radio"/>	公网: 4 内网: 1 IPv6: -	vpc-	法兰克福
<input type="radio"/>	公网: 1 内网: 1 IPv6: -	vpc-	上海

实例所绑定的安全组和规则 (按照优先级排序)

入站规则 出站规则

▼ cfws- | : 2

来源	协议端口	策略	备注
+	TCP:20,3389	允许	【fwmg-】高...
+	TCP:20,3389	拒绝	【fwmg-】封...

立即下载
关闭

5. 预览无误后，单击**立即下载**。

⚠ 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
2028-02-04 16:23:56		规则下发管理	云防火墙-企业安全组	添加规则	89 fwrrg_y64ym8ndf	详情
2028-02-04 16:23:47		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 fwrrg-e68t8ia (-5)	详情
2028-02-04 16:23:38		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 fwrrg-e68t8ia	详情
2028-02-04 16:23:21		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 fwrrg-e68t8ia	详情
2028-02-04 16:22:41		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 fwrrg-e68t8ia	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](#)。