**中移在线服务有限公司**

**网络策略工单管理规定**

**中移在线服务有限公司IT系统部**

**2019版**

**目录**

[**第一章 总则** 3](#_Toc6419793)

[**第二章 安全策略的审批** 4](#_Toc6419794)

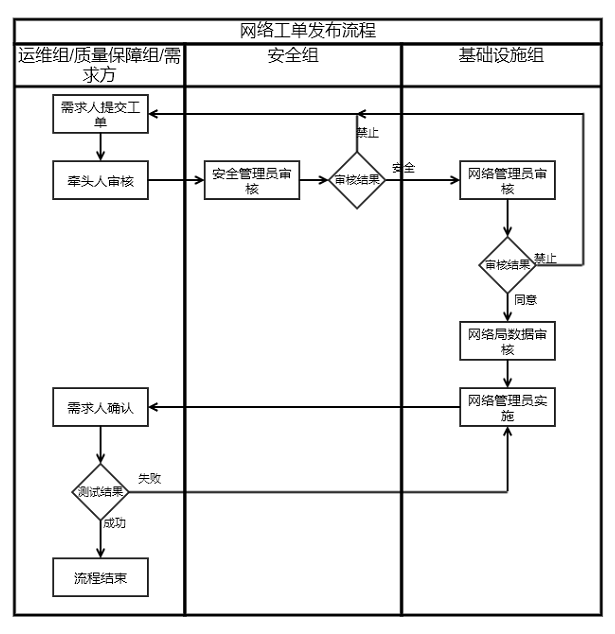
[**第一节 安全策略开通审批步骤** 4](#_Toc6419795)

[**第二节 安全策略开通审批原则** 4](#_Toc6419796)

[**第三节 安全策略的变更及删除审批步骤** 7](#_Toc6419797)

[**第三章 安全策略的制作、审核及发布** 8](#_Toc6419798)

**第一章 总则**

1. 研发云网络支撑工单是在线公司各安全域防火墙、负载均衡器策略开通、修改、删除的唯一依据，任何安全策略必须能够在工单系统中回溯
2. 运维组负责提交开发环境、生产环境系统架构中为实现系统功能而需要的网络策略工单；质量保障组提交测试环境的相关网络策略工单；运营使用网络、业务推广或者用户的网络，由需求方对接人直接提交。安全组审核对外部暴露范围，基础设施组审核各网络环境安全域之间访问合规性，审核完毕后，由基础设施组执行策略制作及发布

**第二章 安全策略的审批**

**第一节 安全策略开通审批步骤**

1. 安全策略开通，首先应由业务团队、运维组或质量保障组提交需求，运维组审批需求的真实性、必要性、合理性，如果确实需要开通策略，则由运维组将业务需求转化为IP互通需求，并填写网络支撑工单，在工单中需要详细描述申请理由
2. 运维组审批后，应由安全组审核对外资产暴露合规性，对互联网/承载网严禁暴露敏感端口，对于高密级的业务系统，如：数据库、存储等，严禁直接暴露给外部用户。
3. 安全组审批后，应由基础设施组依据《中移在线服务有限公司网络安全域管理规定》，审核业务跨安全域访问的合规性

**第二节 安全策略开通审批原则**

1. 安全策略提交原则
2. 运维组负责提交开发环境、生产环境系统架构中为实现系统功能而需要的网络策略部分。
3. 测试环境的相关策略由质量保障组进行提交。
4. 运营使用网络、业务推广或者用户的网络，由需求方对接人直接提交。
5. 工单提交时，务必在工单标题中明确写明策略主要用途。
6. 备注信息中写明是否涉及互联网访问、涉及的地址、互联网地址是否已经备案、所属业务负责人是谁。
7. 若有相应的审核附件、集成方案文档，需作为附件上传。
8. 运维组审批标准
9. 不同环境（生产、测试、研发环境）之间默认不能互访，如需互访，需召集安全组、运维组、基础设施组相关人员进行评审，评审通过后提交网络申请并附上评审会议纪要。
10. 总部各单位发起的网络工单审核时，运维侧负责审核网络工单中总部所属业务地址、端口是否填写正确，并在审核意见中反馈审核结果。
11. 分公司发起的网络工单审核时，运维侧负责审核分公司所填写信息是否完善、清晰，并按照分公司描述审核是否存在不同环境相互访问的情况，具体地址及对应业务的正确性，由分公司自行负责。
12. 运维组在审核意见中，需要注明工单涉及业务系统是否是面向互联网的业务，工单策略是否涉及互联网访问。
13. 网络工单中如涉及IP地址为“所有”的情况，由运维组审核，安全组确认是否需要提前备案、纳入常态化安全扫描等信息后，网络侧支撑。
14. 对于新增上线业务的网络申请，需明确业务系统部署方案，核实并标注出业务系统用途、业务形态（WEB、APP等），是否面向互联网等情况，特别是面向互联网业务要重点详细说明；原则上不正式接入生产业务前不开放互联网访问，如需开放必须由安全组提供的安全扫描通过证明，并纳入后续的常态化安全扫描。
15. 安全组审批标准
16. 测试系统、演示系统、未在使用或退网系统、后台管理类系统，以及后台管理类端口（包括21、22、23、1433、3306、3389、1521、27017等），不允许对互联网开放。如果有需求，需经过评审并填写特殊网络策略申请单并提交安全组；
17. 公司内部自用的网站、系统原则上应部署在VPN内部进行保护，不允许对互联网开放；
18. 互联网暴露的网站开通互联网策略时，要依据系统最小化原则，能确定访问源地址的要进行源地址限制，减小互联网资产暴露面。
19. 所有对互联网开放业务，开通公网访问网络策略前需与安全组沟通，同时做好以下工作：
20. 定级备案：对所有自有系统进行定级备案，并覆盖系统内所有资产，相关资产信息和IP地址使用情况必须在定级备案报告中进行完整描述；
21. 域名备案：对需域名访问的业务系统，需完成域名备案才能对互联网开放；
22. 新业务新技术评估：对互联网暴露面资产需开展新技术新业务评估；
23. 安全扫描：对互联网暴露面系统开展漏洞扫描、渗透测试和安全加固工作，特别要避免Apache Struts 2、心脏出血、永恒之蓝等漏洞反复出现；
24. 弱口令检查：对互联网暴露面操作系统、中间件和应用系统帐号口令进行梳理，杜绝弱口令和易猜解口令。
25. 基础设施组审批标准

基础设施组依据《中移在线服务有限公司网络安全域管理规定》对工单合规性进行审核



**第三节 安全策略的变更及删除审批步骤**

1. 安全策略的变更及删除，有可能影响现网业务的稳定性，风险等级较高，需要业务方、运维组、安全组、基础设施组共同确认后，才可以执行
2. 安全策略的变更及删除，由以下四种情况产生：
3. 业务变更或停用
4. 主机IP变更或退网
5. 存在安全问题或安全隐患的策略
6. 安全策略长时间（三个月以上）没有流量匹配
7. 业务变更或停用，需由业务团队对接运维组提交需求，运维组根据业务流量、业务重要性等，评估业务变更或停用的风险，如果符合变更或下线条件，则由运维组将业务需求转化为IP地址的变更或删除需求，并填写策略变更或删除工单，在工单中需要详细描述变更或删除理由
8. 主机IP变更或退网，需由运维组根据业务流量、业务重要性等，评估主机变更或退网的风险，如果符合变更或退网条件，由运维组填写策略变更或删除工单，在工单中需要详细描述变更或删除理由
9. 存在安全问题或安全隐患的策略，由安全组审核评估后，通知运维组停止业务服务，并由安全组提交网络策略停用工单，在工单中需要详细描述停用理由
10. 安全策略长时间（三个月以上）没有流量匹配，由基础设施组按月统计安全策略匹配次数，将长时间0匹配或流量无增长的安全策略提交给运维组，由运维组对接业务团队，评估安全策略的存在必要性，如符合删除条件，由运维组填写策略变更或删除工单，在工单中需要详细描述变更或删除理由
11. 运维组或安全组提交安全策略变更或删除工单后，由基础设施组依据安全策略的流量匹配次数，再次评估工单风险，及时预警
12. 对于风险较高的策略变更或删除，需由运维组牵头，组织业务团队、基础设施组、安全组开会彻底了解业务架构，明确风险后，才能实施

**第三章 安全策略的制作、审核及发布**

1. 工单审批完成后，由基础设施组负责策略脚本的制作、审核及发布
2. 安全策略制作包括新增、删除及修改等操作。
3. 安全策略制作应遵循可信性、及时性、准确性。
4. 安全策略制作的可信性

安全策略制作的依据是：总部运维组通过研发云网络支撑系统提交的工单，且工单经过安全组及基础设施组审批完毕，除此以外的其它形式一律无效

1. 安全策略制作的及时性

每周二、周四中午12点之前完成安全审批的工单，基础设施组应在每周二、周四晚12点以后，完成策略发布

1. 安全策略制作的准确性

基础设施组应安排专人负责安全策略的制作，除一人进行安全策略的制作工作外，应有另一人进行核对工作。安全策略制作后，在条件允许的情况下须立即进行相关测试工作，以验证数据制作的准确性。

1. 安全策略脚本制作，脚本核查，脚本发布，质检
2. 安全策略脚本制作，脚本核查，脚本发布，质检过程应包括事前、事中、事后三个阶段。安全策略制作人员及核对人员需在安全策略制作记录上签名备查或完成相关电子流程

1、事前：安全策略制作脚本文件要求一人制作、另一人核查，事前做好异常情况应对预案。

2、事中：安全策略脚本发布需落实“一人发布，另一人核查”管理要求，下发时密切关注执行结果，确保执行成功，发现异常及时倒回。

3、事后：应根据脚本进行数据质检核查，联系业务部门测试验证、并关注相关告警信息等，如有问题及时处理或倒回。

1. 任何操作记录和安全策略脚本应保留至少一年。