IPA 技术在网络运营商安全保障中的探索与应用

康雅萍　王升元　王建宏
（中国移动通信集团内蒙古有限公司，内蒙古 呼和浩特 010090）

摘要：网络空间安全（以下称网络安全）事关人类共同利益，事关世界和平与发展，事关各国国家安全，因此各大网络运营商建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。近年来的安全保障和应急演练工作越来越频繁，网络运营商基层安全保障人员和基础设施运维人员数量有限，难以支撑快速发展的安全保障需求。在 RPA 技术可模拟人机交互过程，执行预定程序，操作规则固定、高重复性、高准确度的任务；RPA 以低代码开发、快速部署、替代人工的特点，在各行各业均有成功的应用。在网络安全保障和运维工作中，可以充分释放优势，实现“IT 换人”，降本增效的目标。

关键词：网络安全保障；软件机器人；IP 封堵

一、背景

随着我国互联网新技术、新应用的快速发展，以及国内外局势的不断变化，我国网络安全形势也面临着日益严峻的挑战。在《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》《信息通信行业发展规划（2021–2025 年）》中多次强调要加强重要领域数据资源、重要网络和信息系统安全保障。因此在我国多次举办重大活动中，网络运营商作为央企需要全力保障“春节”“东奥”“党的二十大”等重大活动，提供强有力的信息服务支撑。同时，为提高网络运营商网络安全事件应急处置能力，国家公安部、工信部等主管部门每年都会组织开展网络安全应急演练。在安全保障或应急演练期间，上级单位会 7x24h 不间断下发问题 IP，网络运营商需要第一时间在互联网边界防火墙进行 IP 封堵。由于封堵操作须遍历每台边界防火墙，且封堵任务下达时间具有不确定性，致使人工封堵操作重复性高、耗时长、任务重、效率低，给保障工作带来了极大挑战。

为改善当前面临的困难，从封堵要求和操作流程入手，全面梳理 IP 封堵的流程节点、边界防火墙类型及版本，并对流程节点耗时情况、防火墙封堵命令特点等内容进行定向分析，利用 IPA 技术实现自动化封堵。

（一）应急演练 IP 封堵工作面临的问题

应急演练或安全保障期间，上级单位通过网络监测，主动发现计算机或系统收到的外部攻击，并将攻击源 IP 下发至网络维护人员，维护人员通过防火墙和路由器配置，封锁某个 IP，禁止链接，达到抵御攻击的效果。因此网络维护人员需根据上级单位要求，对互联网边界防火墙进行 7x24h 不间断的 IP 封堵。封堵操作须遍历每台边界防火墙，封堵操作呈现出重复性高、耗时长、任务重、效率低的特点，给保障工作带来了极大挑战，具体体现在以下 4 个方面：

1. 应急演练持续周期长：年均 3 次应急演练，单次演练最短持续周期为 12 天，最长为 21 天，累计共计 47 天。

2. 封堵操作过程繁复：上级单位发布封堵信息的时间具有不确定性，维护人员需 7x24h 持续关注通知群内动态，且封堵操作步骤繁多，执行时效性要求高，人工操作压力大、易疲劳、准确性差、耗时费力。

3. 网络维护人员数量不足：每位网络维护人员人均维护千台设备，持续开展 7x24h 值守难度大。

4. 封堵操作日志记录缺失：人工执行封堵操作无法及时记录操作信息，难以支持后续分析回溯。

（二）RPA 技术介绍

RPA 定义。机器人流程自动化（Robotic Process Automation，简称 RPA）指用软件自动化方式模拟人工操作计算机完成工作任务，它通过软件机器人自动处理大量重复的、基于规则的工作流程任务，通常被称为 RPA 机器人。

不同于传统开发，RPA 机器人以非侵入式在系统表现层通过模拟人工操作完成数据流转和整合，不需要对现有系统进行改造，也不需要对其他系统进行接口打通和二次开发。

二、整体方案

（一）IP 地址封堵操作流程标准化

根据 RPA 技术应用特点，首先需要将人工操作标准化和流程化，因此先对网络安全保障期间可疑 IP 地址封堵的操作步骤进行了梳理和归类，形成标准化流程，明确了各节点操作要求、操作方法和操作规则。

1. 获取 IP 封堵消息。根据上级单位的工作部署，IP 封堵消息一般来源于邮件、微信、飞信或企业内部沟通工具，通过查看上述软件消息记录，查找“IP 封堵”等关键字，确定待封堵 IP。

2. 执行封堵操作。IP 封锁指防火墙维护 IP 黑名单，一旦发现向黑名单中地址的请求数据包，就直接将其丢弃，源主机得不到目标主机的及时响应而引发超时，从而达到屏蔽对目标主机的访问的目的。封堵操作可通过执行防火墙封堵命令实现，因此可通过机器人自动生成防火墙封堵命令，激活防火墙命令窗口，并执行封堵命令，从而实现封堵的目的。

3. 记录日志和消息反馈。获取封堵日志信息保存至 excel 文件用于备查或 IP 地址解封使用，并自动生成“XXXX 地址已封堵”的信息，再沟通工具中实时报备。

图 1 流程标准化设计

（二）封堵消息识别与处理

RPA 机器人定时激活微信、飞信或其他工具的应急演练群或者安全保障群对话框任务窗口，获取实时封堵信息。根据消息关键字段，例如“封堵”“IP”等获取到待封堵的信息，并利用正则表达式对获取到的信息准确性（是否为正确 ipv4 或 ipv6 格式）进行校验，同时记录信息至 excel 留档。

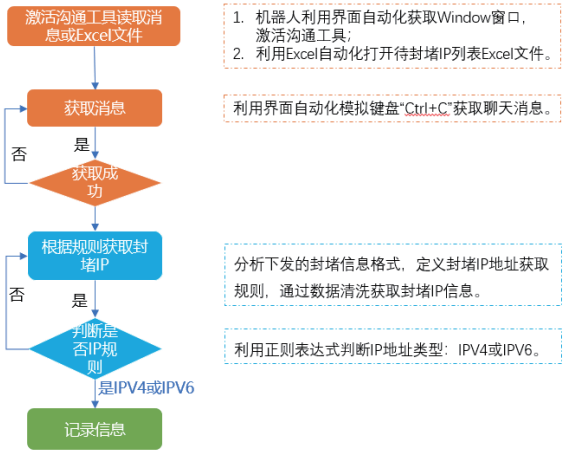

图 2 消息识别和处理流程设计

1. 上级部署群消息获取。RPA 机器人利用界面自动化获取 Window 窗口，激活消息沟通工具窗口，以备提取待封堵 IP 地址。利用界面自动化模拟键盘操作“Ctrl+C”和“Ctrl+V”获取聊天消息。

2. 消息接收和处理。分析下发的封堵信息格式，定义判断封堵 IP 地址关键字，制定获取 IP 规则，通过数据清洗获取待封堵 IP 信息。利用正则表达式判断 IP 地址类型是 IPV4 或者是 IPV6。

3. 待封堵 IP 记录。将提取到的 IP 通过 RPA 机器人利用界面自动化、Excel 自动化模拟“Ctrl+C”和“Ctrl+V”操作，将 IP 地址和获取时间写入制定单元格的数据内容。

（压到）防火墙命令编辑与执行

梳理定义防火墙封堵命令数据库，然后依据获取到的 IP 信息，自动完成命令的匹配和编辑，并遍历至已配置的地址域 JSON 数组。激活 4A 防火墙命名窗口，并定义自动刷屏，防止设备自动锁定。根据 JSON 数据中的地址域以及命令规则在防火墙命令窗口中执行对相应的封堵命令。

1. 防火墙 IP 封堵命令生成。防火墙的 ACL 命令集条目数量存在上限，为确保封堵命令的有效性，RPA 机器人利用文件处理组件打开配置文件获取防火墙的命令集条目数量，如若超过阈值则自动创建新的命令集。通过 Excel 自动化组件，读取待封堵 IP 内容，依据到的 IP 信息，自动完成防火墙封堵命令的匹配和编辑，并遍历至已配置的地址域 JSON 数组中，从而生成封堵命令。

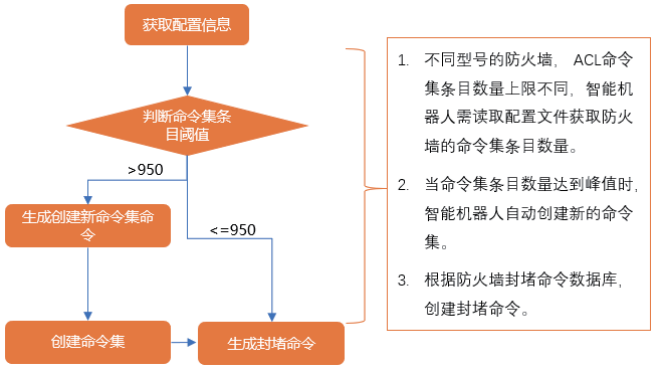

图 3 封堵命令生成流程设计

2. 激活防火墙命令窗口并执行。RPA 机器人通过界面自动化的 Window 窗口组件，激活防火墙命令窗口。根据 JSON 数据中的地址域及命令逐个在防火墙命令窗口中执行对相应的封堵命令。通过 Excel 自动化新建工作表用于记录执行信息，使用正则表达式及 split 方法快速获取到对应命令的执行记录，利用界面自动化的键盘组件模拟“Ctrl+C”和“Ctrl+V”的操作将执行信息写入 Excel 文档用于后期回溯或 IP 解封使用。

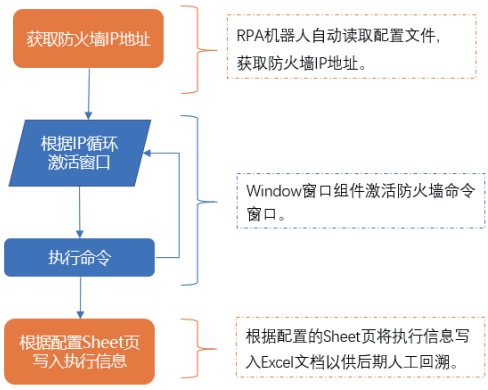

图 4 封堵命令执行流程设计

（四）封堵 IP 状态记录与消息回复

1.IP 状态记录。

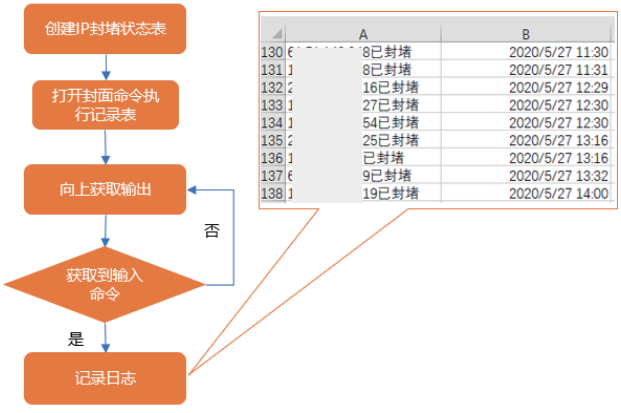

图 5 封堵 IP 日志记录设计

通过 Excel 自动化新建工作表用于记录 IP 的封堵状态、封堵时间、执行封堵命令结果日志行、是否反馈等信息，并自动读取命令执行表获取 IP 信息。利用 Excel 写入组件逐行记录 IP 封堵命令执行情况，对 IP 封堵和反馈回复状态进行标记。

2. 消息回复。RPA 机器人利用读取单元格内容组件，逐行判断当前 IP 是否封堵、是否反馈的信息，利用正则表达式确定需要反馈回复的 IP，并生成“XXXXXXXXIPV4 或 IPV6 地址已封堵”的信息。通过 Window 窗口组件打开沟通群窗口，搜索关键字定位群，用鼠标组件模拟“双击”打开封堵群，并在沟通群中实时通报。

四、应用情况

通过将 RPA 技术应用到各大企业的网络安全保障中，使其能够模拟人工封堵的方式，自动执行封堵消息接收、消息处理、封堵命令编辑、设备登录、封堵命令执行、封堵执行情况记录、封堵执行结果回复等一系列封堵操作流程步骤，无需人工干预。以某网络运营商省级单位在“两会”、春节等重大活动安全保障或者是上级单位 HW 期间，一年约自动封堵 IP 地址 3658 个，解决了长期以来，网络安全保障所面临的困难。

参考文献：

[1] 王福明 . 网络通信信息安全的保障措施探索 [J]. 中国信通信，2023，25（15）：95-97.

作者简介：康雅萍（1988 —） 女，研究生，副高级工程师。主要研究方向：RPA、AI、数字孪生等新技术研究。