防火墙可视化配置系统典型经验

一、引言

防火墙可以给网络环境带来保护，但是由于windows（或linux）主机防火墙设置比较复杂，不直观,对运维人员技能要求和操作要求都很高，给日常运维工作带来了困难，效率难以提升。

本系统旨在通过对特定ip，端口，协议的可视化控制，简化防火墙的配置，提高配置效率。

1. 问题描述

日常运维工作可能要面对一些问题，这些问题的解决有利于提高运维人员的工作效率，这些问题总结如下：

1.不同操作系统的防火墙规则配置命令不一致，容易记混

2.配置命令参数过多，书写容易出错

3.查看已配置过的规则不方便

4.不同操作系统之间规则不通用

5.管理主机过多的情况下，同一条规则在不同主机上需要多次配置，工作繁琐，容易漏配置，误配置

6.要管理主机过多，系统密码管理不便

1. 典型做法

本系统采取了C/S架构，把系统分成两个部分中控和agent，其中中控部分是客户端，负责管理总体规则；agent部分是服务器端，负责根据操作系统等情况具体实现。agent的规则存放在中控上。在agent和中控通信实现中，我们采用了AES加密客户端和服务器的通信。中控和agent均可以在windows和linux两大主流操作系统平台上运行，中控我们采用了PyQT图形界面库开发，agent采用命令行界面运行，中控和agent均需要一直运行。中控agent间的操作命令传递规则类似http协议的参数传递方式，使得命令交互更简单可靠。中控和agent都有操作日志记录每一个通信请求以及命令的执行情况。

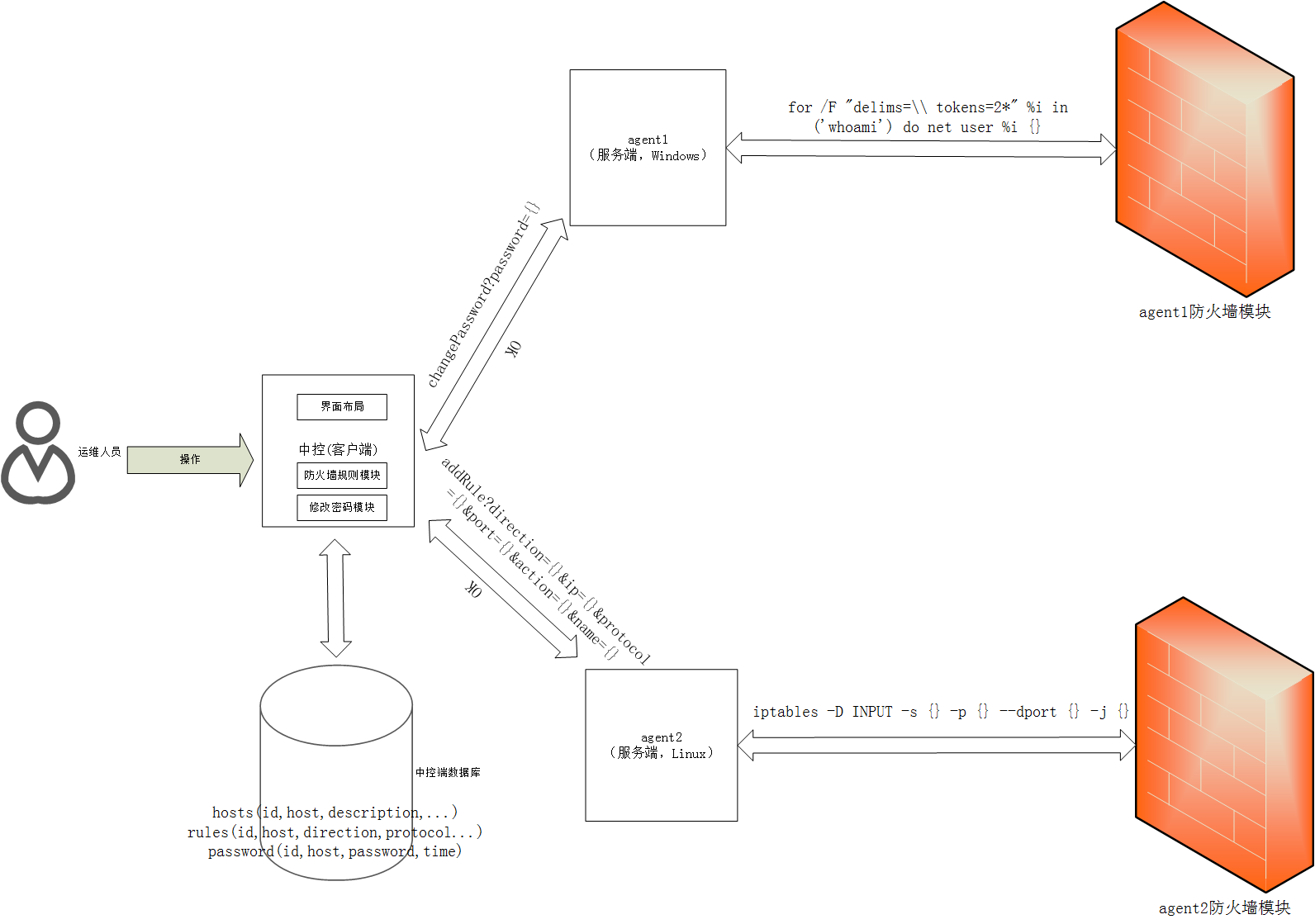


图1 系统整体架构图

下面对这些部分作详细一点的介绍：

1.C/S架构

在系统实现中，中控作为客户端，agent作为服务端，中控连接服务端进行配置操作。采用C/S架构可以中心化的管理主机群，只需要在中控配置好规则，便可以把规则自动推送到对应的主机上，避免了登录主机手写命令的繁琐流程，对防火墙规则的操作均可以在中控上操作实现快速部署。

1. 通信加密

由于网络环境不一定可信，存在被窃听的风险，所以为保证安全性，中控和agent之间的通信必须加密。目前采用固定的CBC模式的AES密钥加密中控和agent之间的通信。后续考虑通过RSA加密算法加密AES秘钥的密钥交换算法。

1. 中控端规则存放

中控通过数据库暂存各agent的防火墙规则，通过可视化编辑数据库，进行规则的添加更新删除等操作。规则包含ip，端口，协议，方向，采取动作等部分，ip支持常规的ip，网段等，端口支持常规端口，端口范围等，协议支持tcp，udp和all。

1. 运行界面

中控采用PyQT开发，跨平台，操控简便直观。Agent为命令行模式，可以在后台运行。使用Python3开发，跨平台支持在Windows和Linux上运行。

1. agent扩展

运维人员可能会面对购置新机器，修改主机ip等情况。因此需要考虑agent的扩展性。新加入一个agent只需要在agent运行服务器端程序并在中控端添加其ip地址即可。

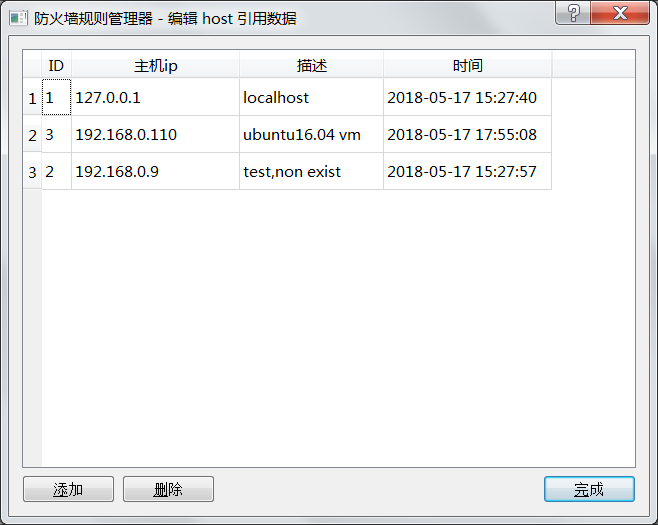


图2 添加agent

1. 参数传递规则

中控和agent间采用类似http的参数传递规则，例如中控给agent传递下列字符串表示在agent上添加一条防火墙规则，{}是参数的值，如果需要一次传递多条规则，只需要在每个参数里面一次使用”,”分隔。addRule?direction={}&ip={}&protocol={}&port={}&action={}&name={}

这样的参数传递规则意义显而易见，也方便记录日志。

1. 日志记录

中控和agent都会对操作过程进行记录，中控日志记录了发出的命令和收到的返回以及执行途中的异常，agent日志记录了收到的命令和发出的命令结果以及每次执行的系统命令和系统命令输出和执行异常。如果遇到了异常情况，可以保留日志以帮助后期程序的bug修复。

1. 密码修改

agent的密码要定期修改，我们在程序中有一个线程专门用于更新agent的密码，这个线程从数据库读取到达修改密码期限的主机或者新加入的主机，生成一个随机的字符串作为主机的密码，通过通信机制传输到agent上，执行修改密码的系统命令更新运行当前agent脚本的用户的密码，更新记录记录在数据库里，可以在中控界面可以看到各agent的每一次密码修改记录，以便登录agent的时候查询或者在出现意外时恢复。

1. 主机过滤器

由于防火墙规则较多，比较混乱，查找起来不方便，因此实现了一个简单的主机过滤器。主机过滤器可以过滤出满足一定条件的主机的所有规则和密码修改记录，使得运维人员可以更快找到关心的主机，并为其配置规则。

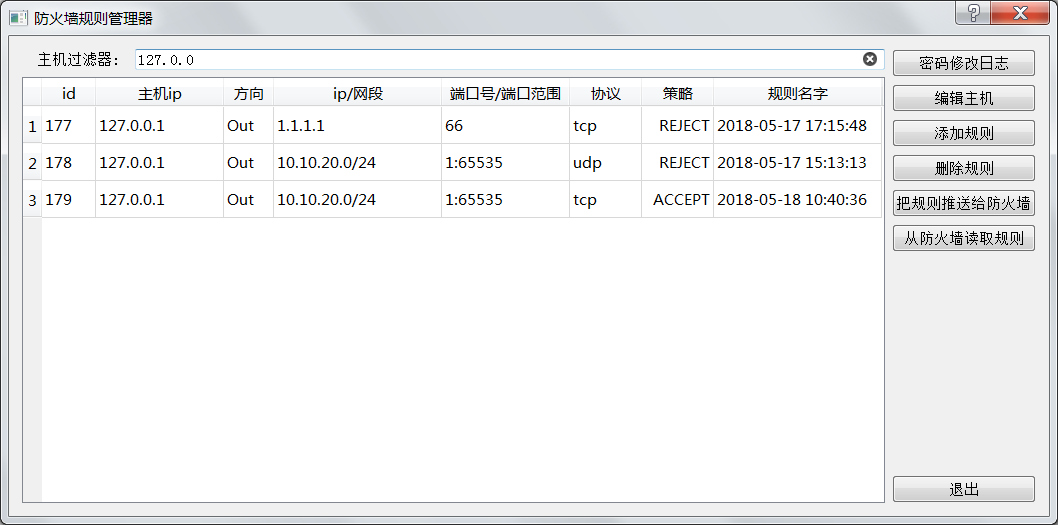


图3 防火墙规则主机过滤器

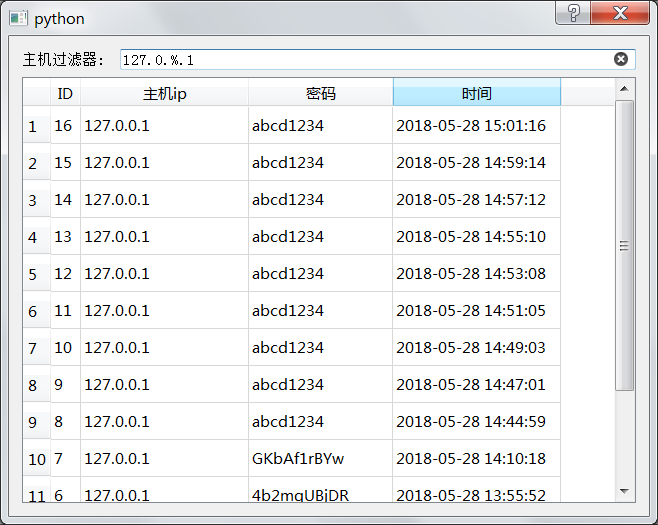


图4 密码主机过滤器

四、经验总结

为解决防火墙配置的复杂性和易错性，我们开发了一套防火墙可视化配置系统，该系统旨在让防火墙配置变得简单，解决当前防火墙配置的问题，该系统除了可以配置防火墙外也提供了定期修改机器系统密码的功能。本文档总结了开发过程的典型经验，从架构，通信加密等9个部分介绍了本系统的设计原理和代码实现。