防火墙自动化运维

田国华

高级网络安全经理

携程旅行网

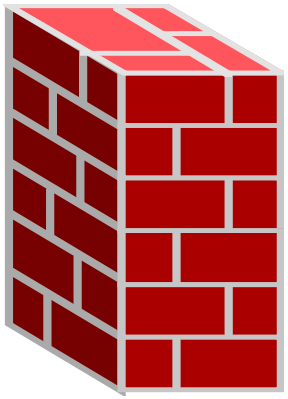
GITC 2016 上海

目录

防火墙运维之痛

架构层面问题

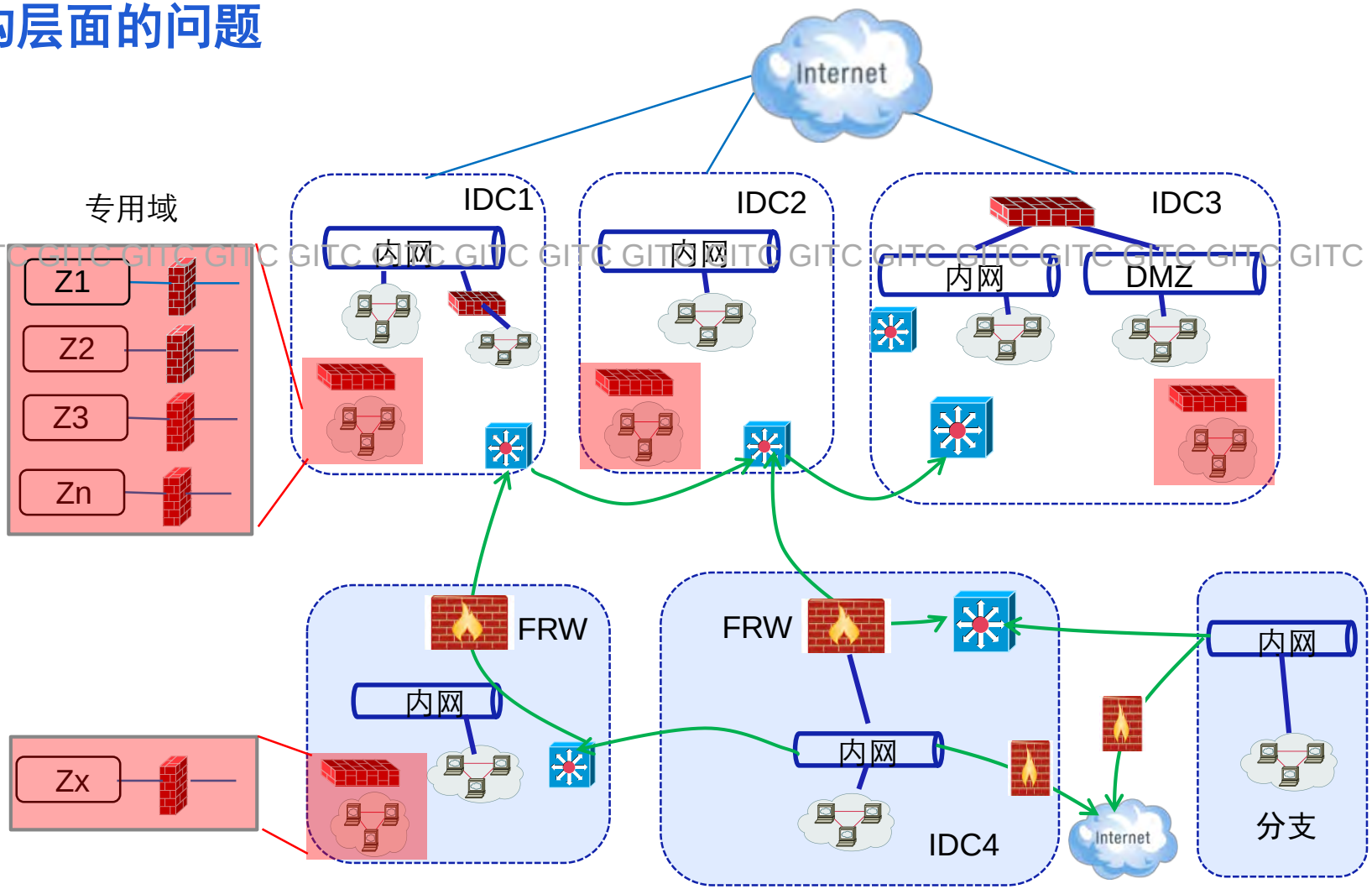
单一品牌防火墙



多品牌防火墙

防火墙运维之痛

架构层面的问题



防火墙运维之痛

运维层面的问题

用户

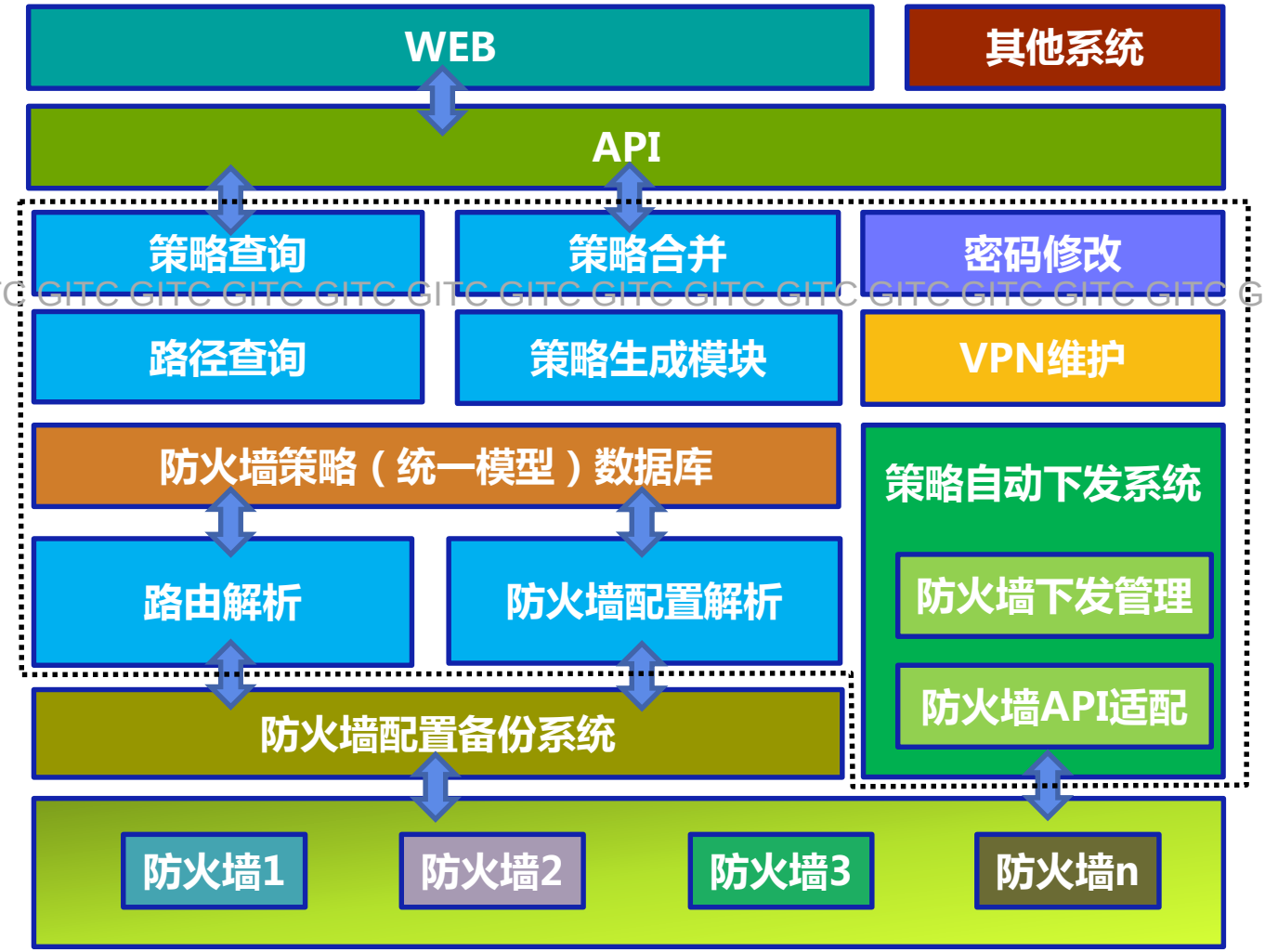
安全工程师

目标

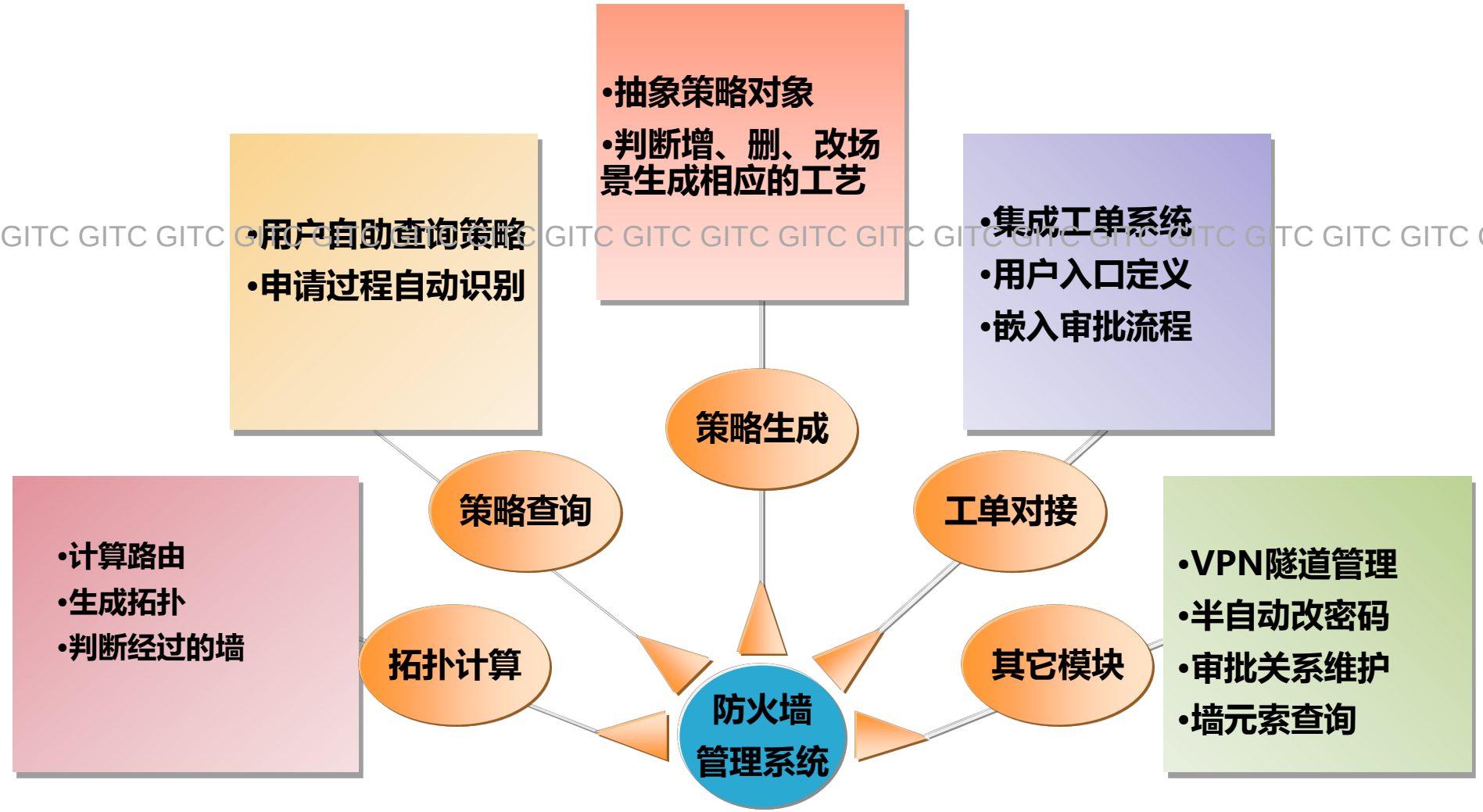
透明、规范、自动化、高效

防火墙运维管理系统介绍

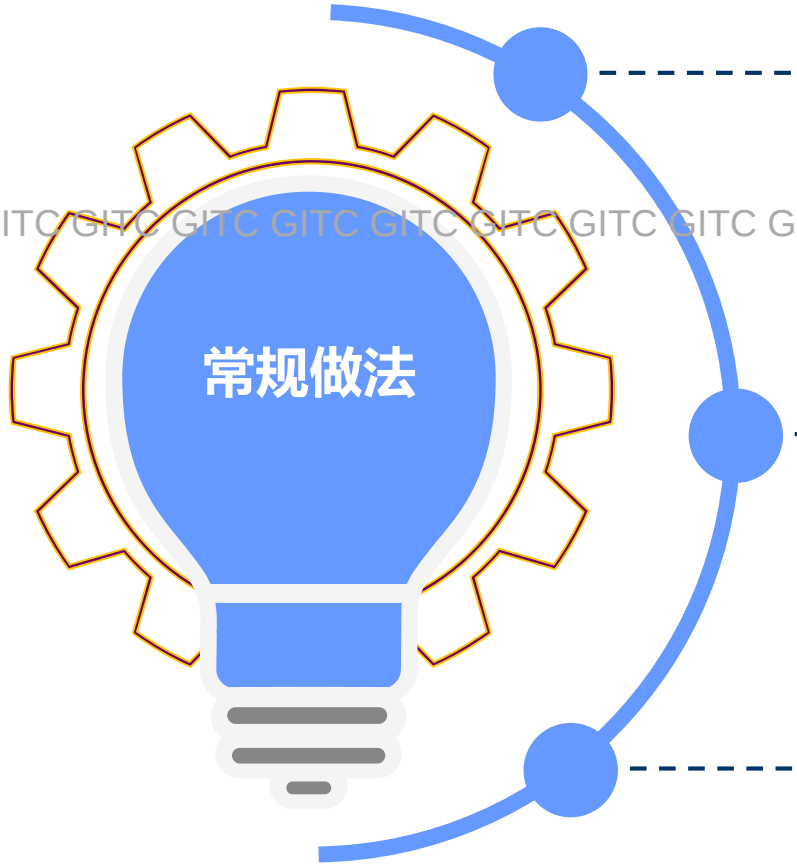
系统架构



系统核心功能模块



拓扑计算



1.问题

- 防火墙数量较多情况下
- 难以判断两个IP是否过墙
- 或者经过哪几台墙

2.传统方法

- 根据经验模糊判断
- 人工查询、手动验证
- 甚至查阅日志

3.缺点

- 费时费力，效率低下
- 判断可能产生差错
- 差错对业务环境产生影响

自动化拓扑计算

路由匹配

a. 防火墙静态路由匹配（最长路由匹配），若存在匹配路由，则转到b，否则继续查询其他防火墙。

接口比较

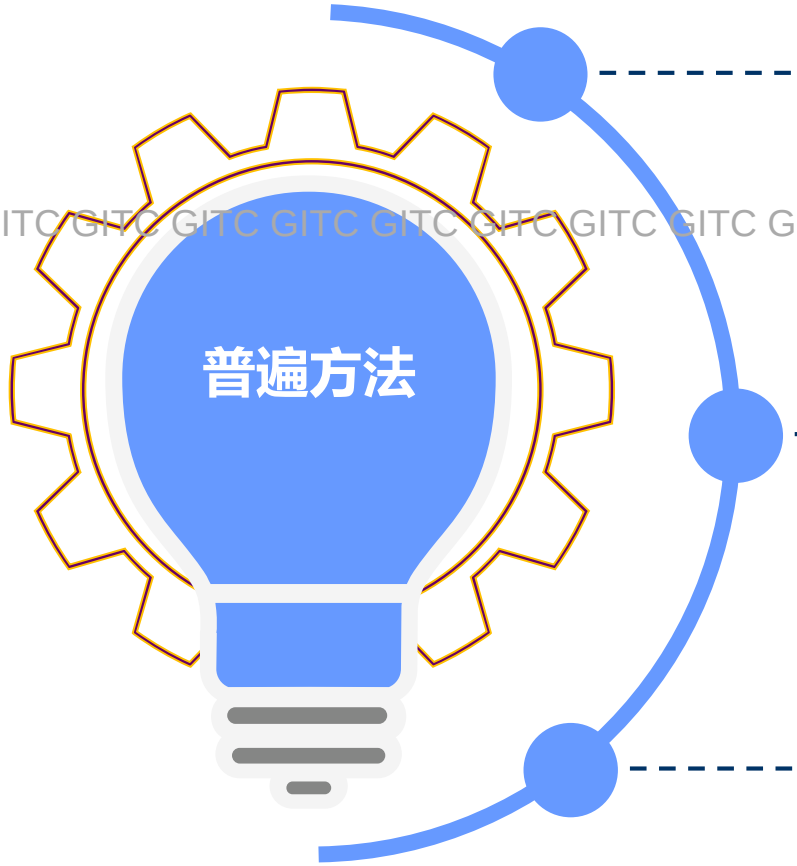
b. 判断匹配到的路由对应的接口是否相同，若相同，则对应的防火墙添加到拓扑中。

生成拓扑

c. 若所有防火墙已被遍历，则输入防火墙拓扑图，否则，转到a，进行下次循环。

自动化完成防火墙拓扑计算

策略查询



1.问题

- 安全策略不断增加
- 策略数多到几千条时
- 查询策略变得困难

2.传统方法

- 根据经验模糊判断
- 人工查询、手动验证
- 甚至查阅日志

3.缺点

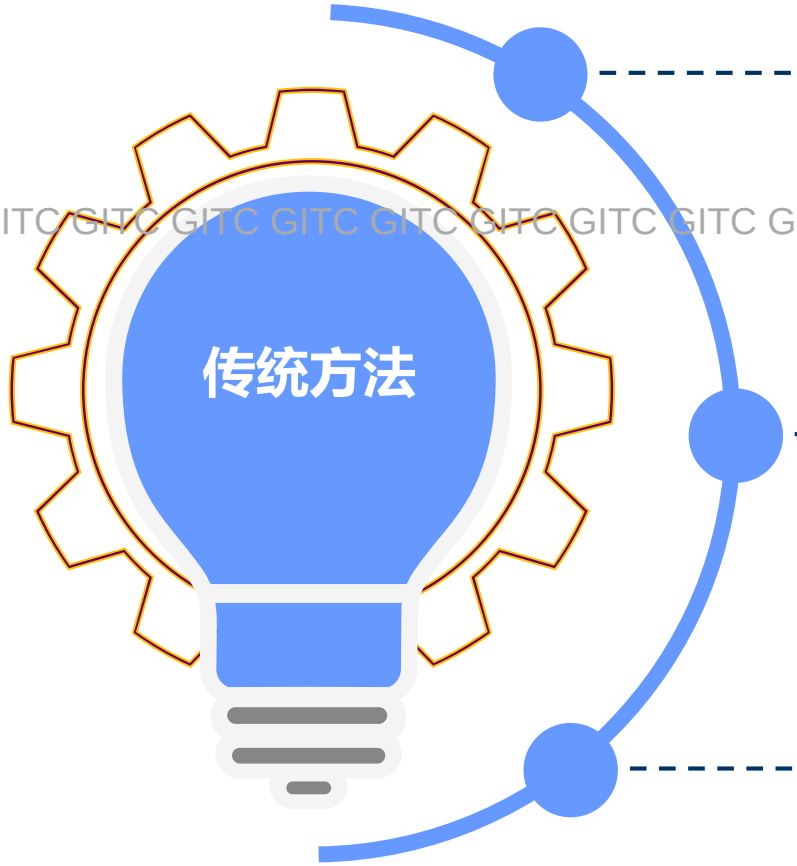
- 效率低下
- 可能漏查
- 用户满意度差

自动化策略查询

匹配目标	匹配目标协议	匹配源	循环
a.匹配destination是否包含查询条件中的目的地址（dst），若包含，则转到b否则，继续匹配下一条策略。	b.匹配协议（protocol和ports）是否包含查询条件中的协议（proto）和端口（port），若包含，则转到c	c. 匹配source是否包含查询条件中的源地址（src），若包含，则输出查询结果，否则，转到d	d. 若所有策略已匹配完，则输出查询结果，否则，继续下一条策略。

精确定位涉及防火墙的具体策略

策略工艺生成



1.问题

- 多品牌防火墙问题
- 各墙操作工艺不同

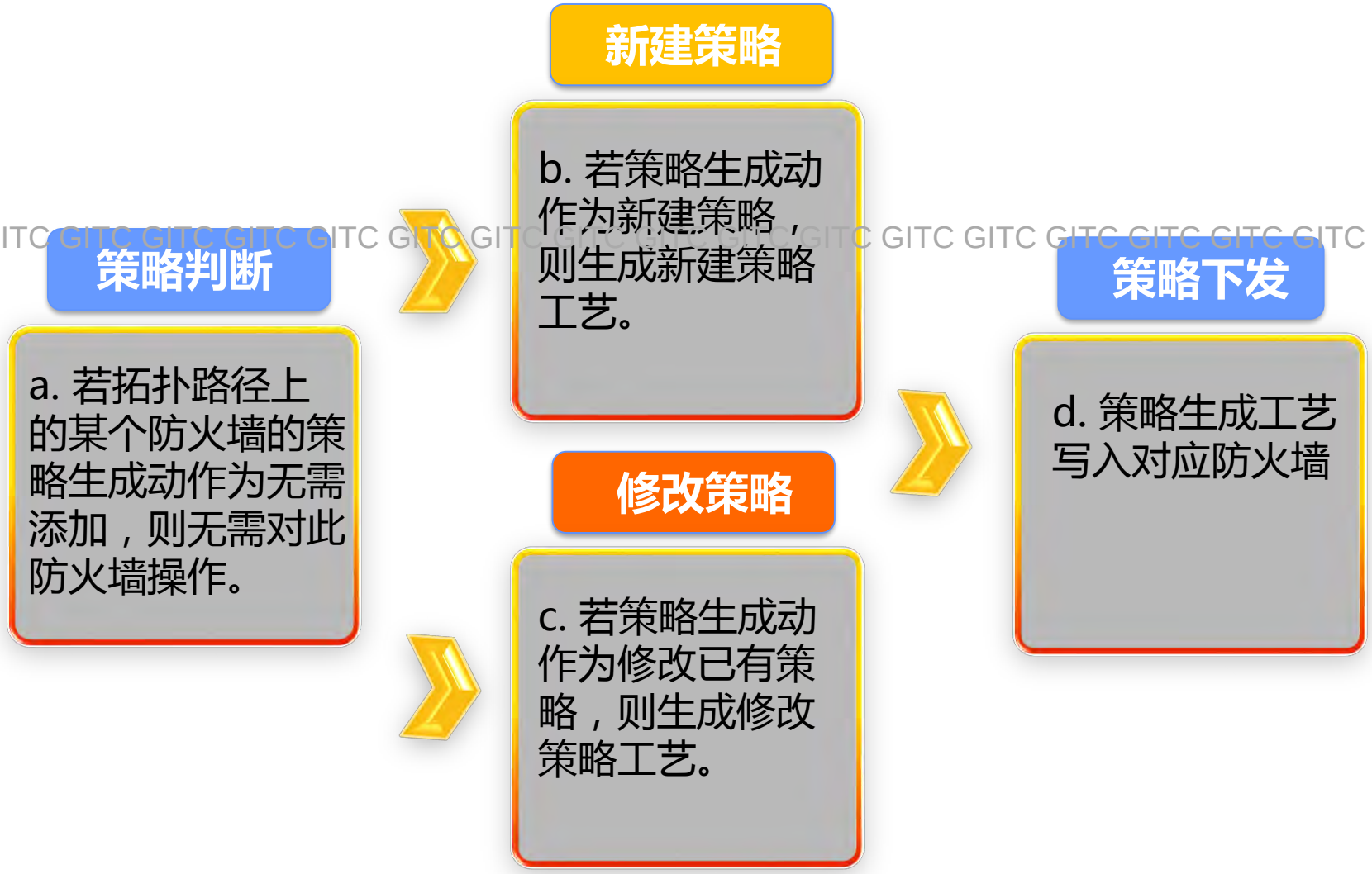
2.传统方法

- 根据不同品牌
- 人工采取不同操作
- 如CLI或GUI

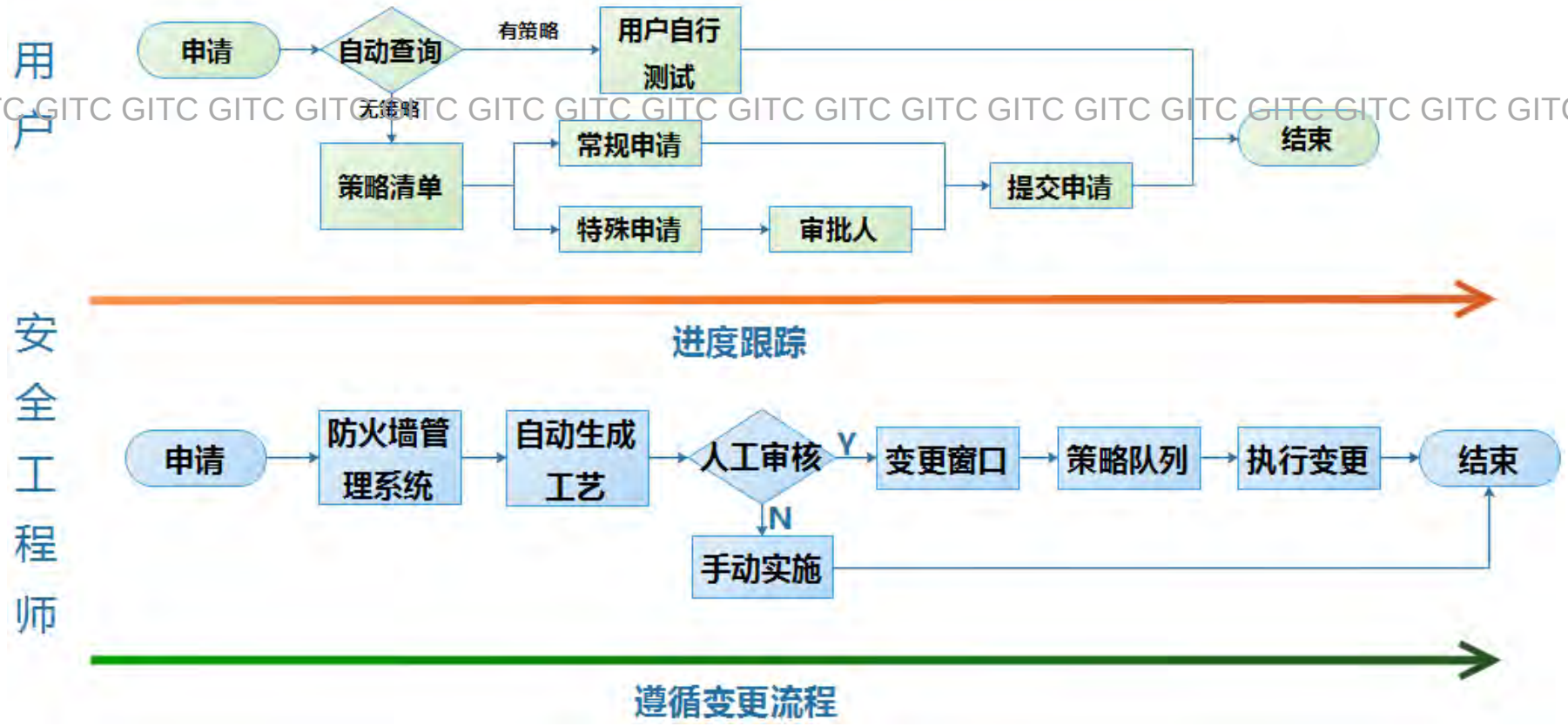
3.缺点

- 效率低下
- 可能产生误操作
- 用户满意度差

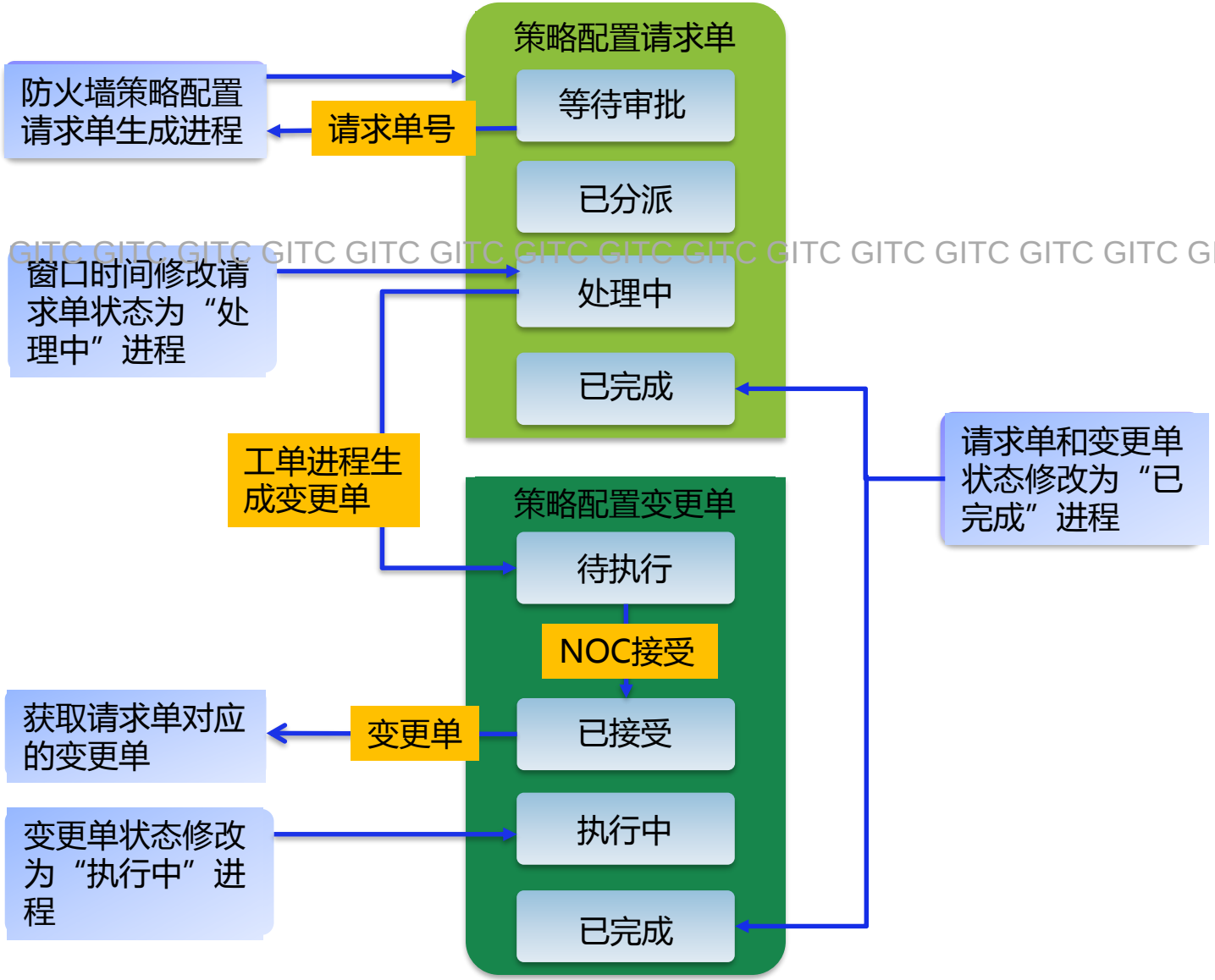
自动化策略工艺生成下发



流程梳理



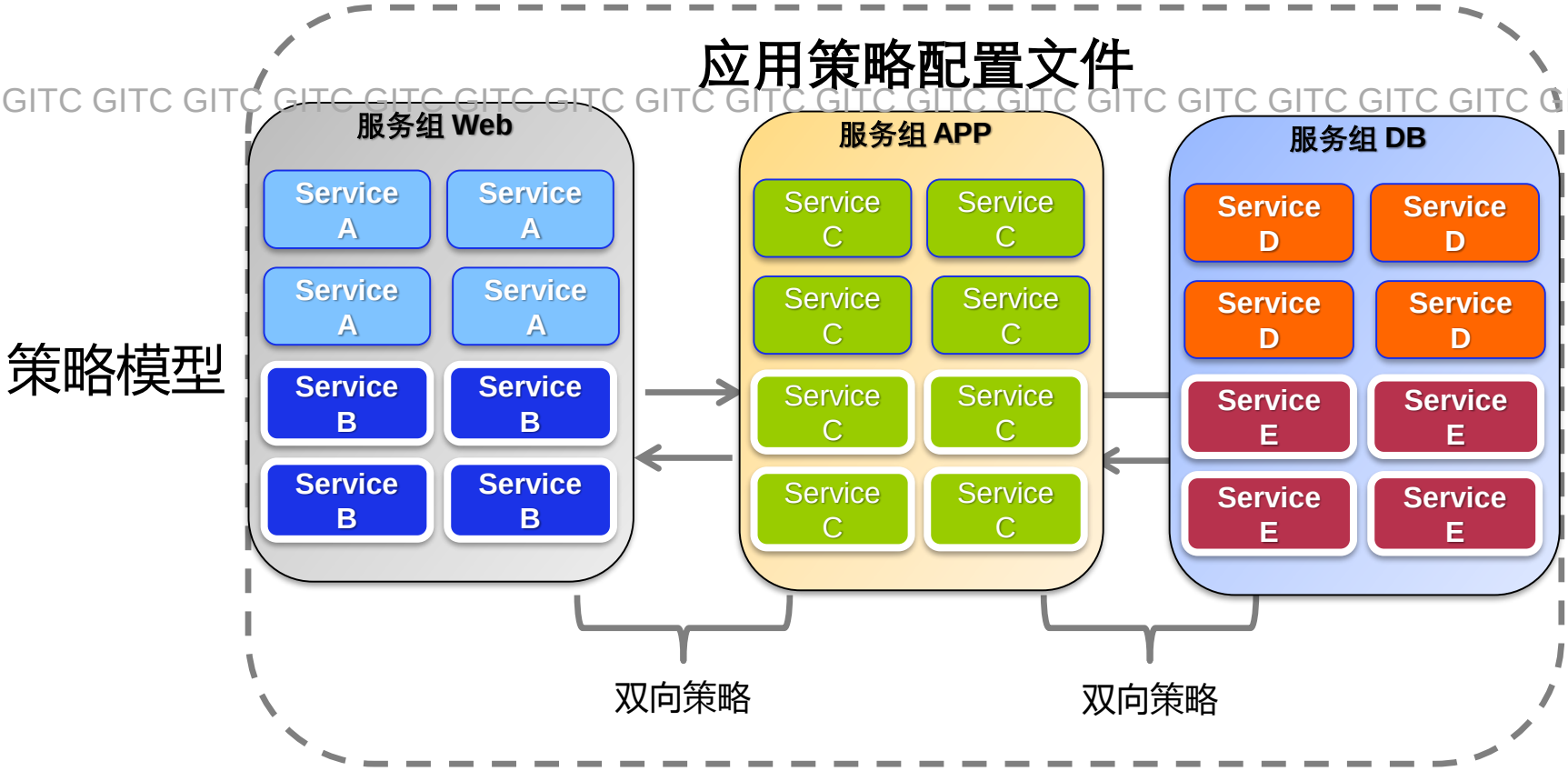
对接工单系统



防火墙管理系统界面

展望（以应用为基础的策略模型）

应用策略配置文件是一组规则， 用于定义它们之间通讯的策略。



以应用为基础的策略模型

- 策略配置与IP解耦
- 配置更加智能化，减少人工干预
- 速度更快，服务器上线秒级完成策略同步
- 更加规范和易于维护的策略
- 统一的模型与使用何种硬件设备无关

Q&A

谢 谢

Ctrip 携程