说明: logoword

**防火墙自动化配置平台使用手册**

**编写部门：网络通讯**

**编写日期：2016.12**

1. **防火墙自动化配置平台简介**

登录火墙自动化配置平台，地址为：<http://22.1.111.29:8002>。

目前系统可通过导入工单，分析需求，评估经过的防火墙和交换机，生成对应配置。

1. **系统登录**

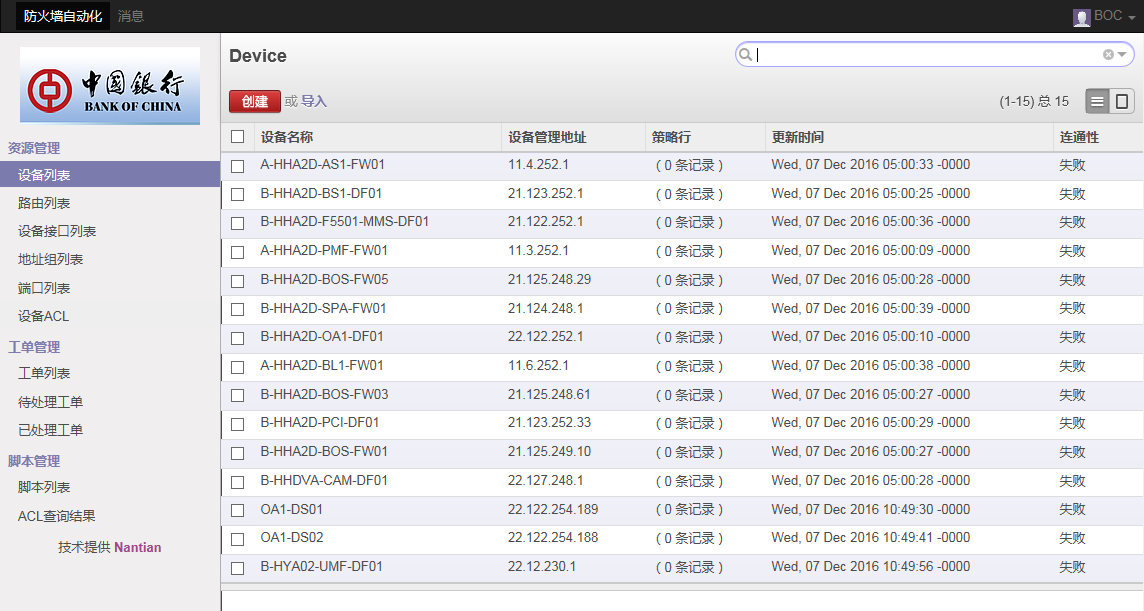
用户名：boc 密码：123456



1. **系统界面**

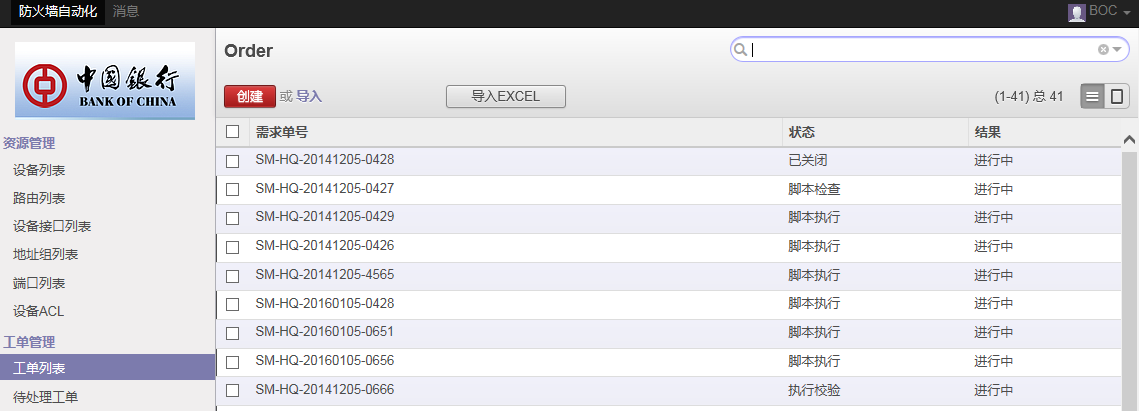
目前设备支持思科ASA和防火墙模块，NX-OS的交换机ACL的配置生成，目前调试通过的防火墙和交换机清单如下，如有新增设备请联系李融进行调试。目前还不能支持NAT的防火墙及其他品牌。

界面如下：



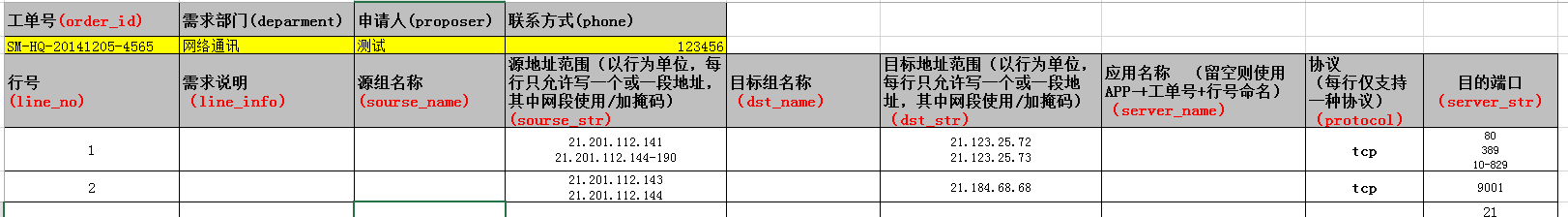
1. **工单导入**

点击工单列表：



选择导入EXCEL：

EXCEL模板参见附件，格式如下：



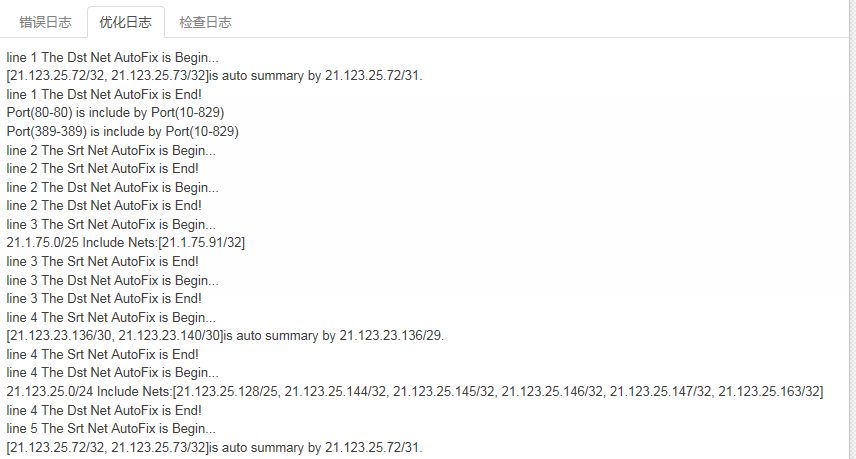
其中相关格式要求参见表头，导入成功后，点击对应工单号，出现下面的界面：



同意后进行格式检查，如果有误，对应行的格式的沟会去掉，对应格式的问题会出现在错误日志。



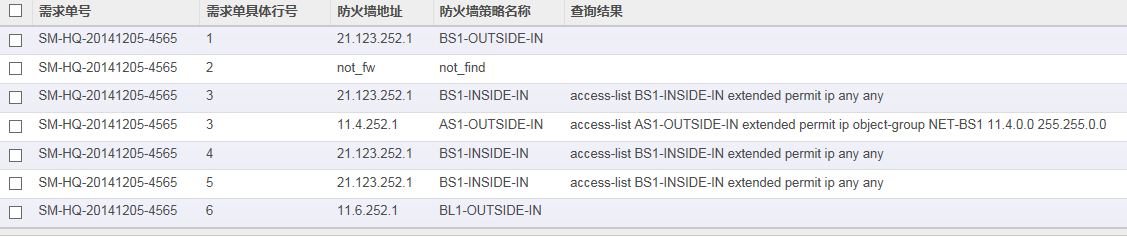
目前需求地址会进行检查及汇总，汇总的日志在优化日志下面。



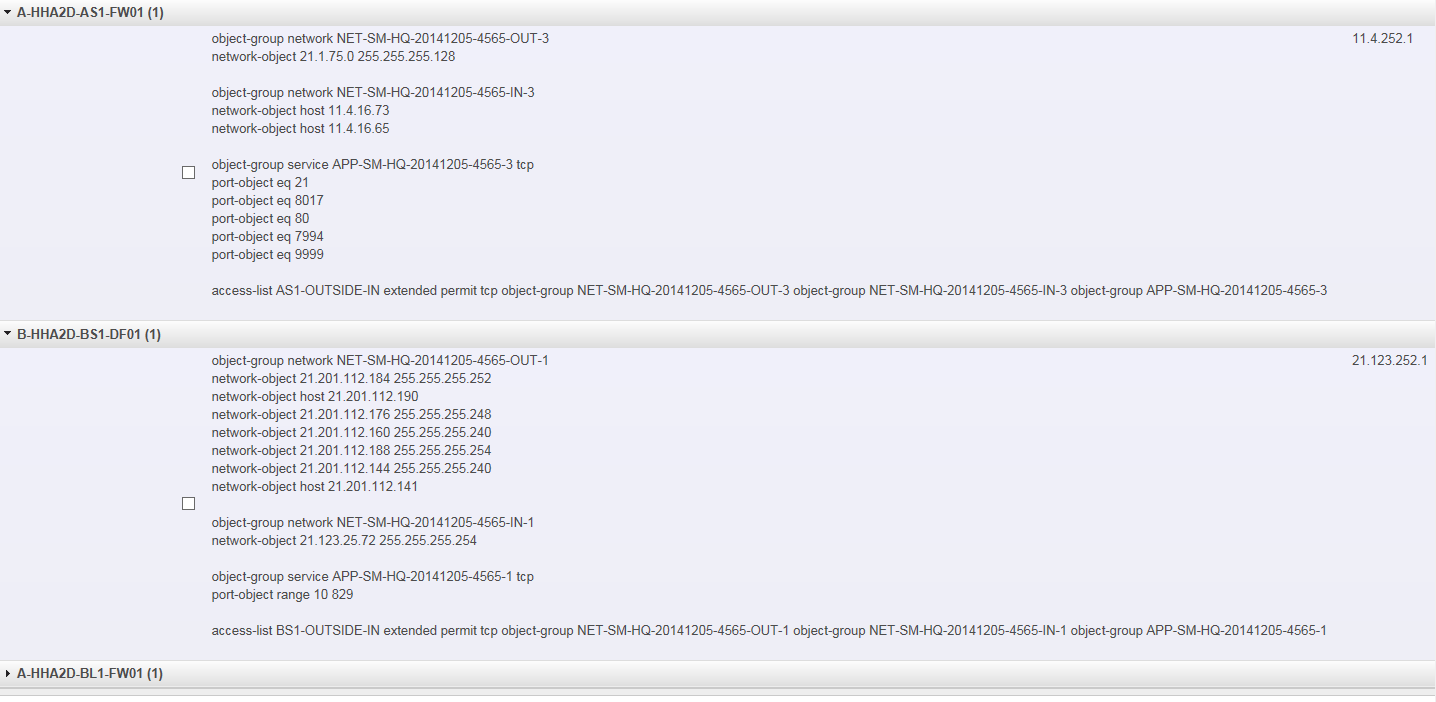
同意后进行合规和防火墙策略检查，目前暂时未执行合规检查。检查完成后会出现检查结果。



检查结果如下，已放开的需求会显示对应的查询结果，未查询到防火墙的提示为not\_fw，原因为涉及安全设备未能纳管（备注：如果一行需求经过该系统纳管的安全设备，又经过未纳管的设备，只能识别纳管设备的策略，无法提示未纳管的设备的情况）：



同意后进行配置生成，生成的设备配置如下：



目前系统完成在以上阶段，后续步骤为推送至CMCS，目前版本调试中，未实现。

1. **防火墙自动化配置平台支持情况**

支持无NAT的思科防火墙，防火墙模块的配置查询及生成。

支持NX-OS的交换机ACL的查询及生成。

1. **防火墙自动化配置平台使用注意事项**

目前防火墙的配置生成规则如下：防火墙配置的数据库为每天早上5:00生成，其中配置生成会查询对应需求是否被覆盖，覆盖策略不会生成配置，对于未执行的策略不会进行检查。

防火墙的配置生成按工单号及行号进行组的建立，如果目标地址和端口被现有策略完全包含，会沿用之前的源策略组名称生成。

交换机配置生成时，目前版本仅会根据需求直接生成不带行号的配置，对于存在DENY的情况需要手动指定行号。