V7防火墙 和V7 IPS设备加入IMC进行ssm管理步骤

Syslog日志 冉博文 2016-04-14 发表

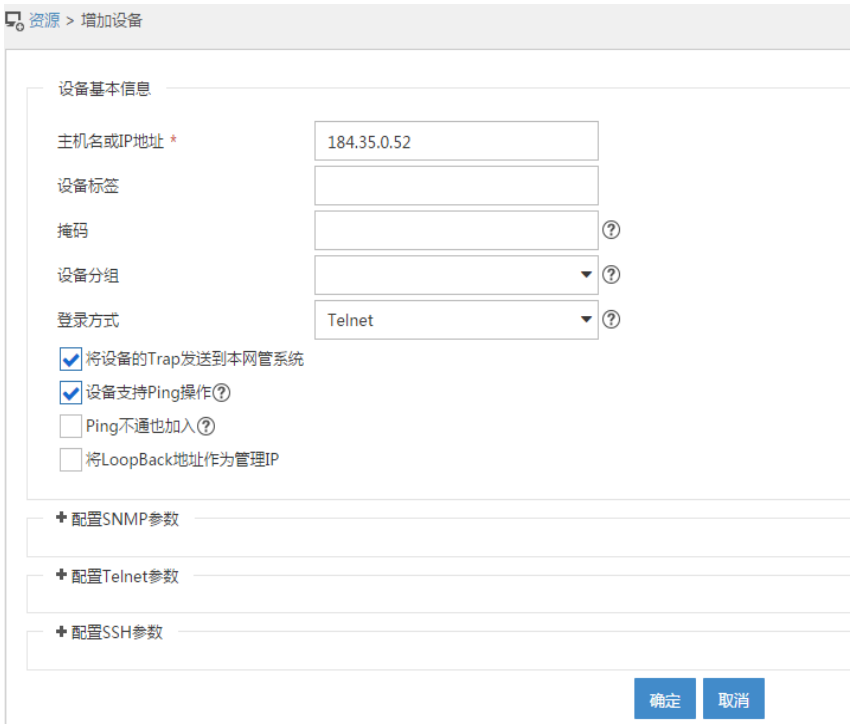
客户需要将V7防火墙日志或者V7 IPS设备通过IMC的ssm组件进行管理，下发策略，并将IPS的日志发送到ssm组件。

1. 设备上开启netconf、snmp、telnet 功能，并创建对应权限用户

```
#
telnet server enable
#
snmp-agent
snmp-agent local-engineid 800063A2808042000856050000000l
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version all
#
ssh server enable
#
domain default enable system
#
netconf soap http enable
netconf soap https enable
#
#
local-user admin class manage
password hash $h$6$UbIhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babIIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
service-type ssh telnet terminal http https
authorization-attribute user-role level-3
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
info-center loghost 184.11.0.130 port 30514————————————将日志输出到imc
#
```

2. 将设备加入imc

资源 - 增加设备页面

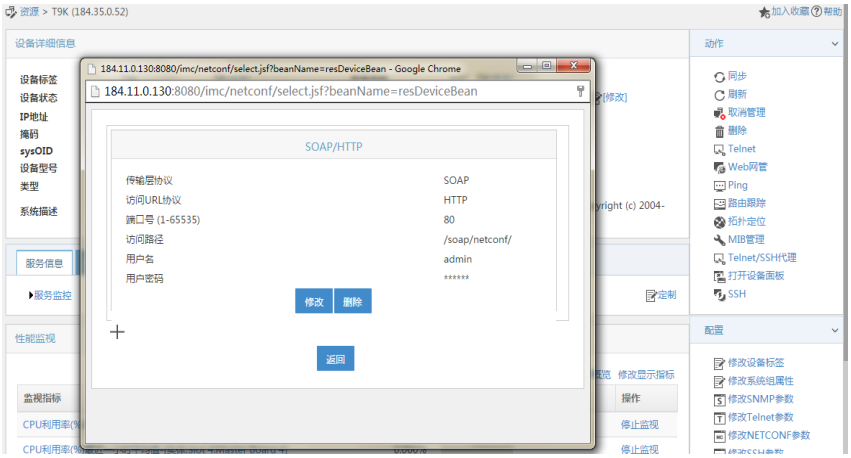


3. 配置设备netconf模板

资源 - 设备详细信息 - 配置

修改netconf参数

增加netconf配置



4. 增加安全业务设备管理

业务 - 安全业务管理 - 设备管理

5. 同步特征库

业务 - 安全业务管理 - IPS业务配置 - 特征库管理

点击操作中的按钮

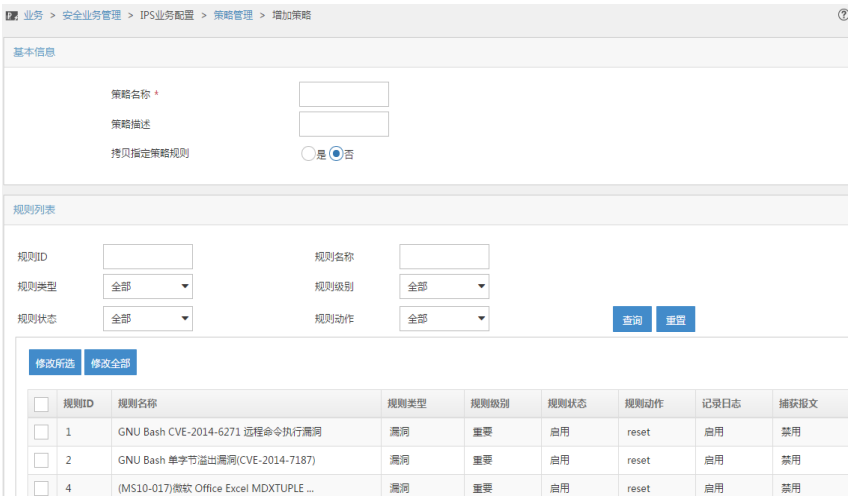
同步时会提示需要先保证所有ips设备特征库一致，且需要都为最新版本

同步完成后可以在ips业务配置 - 规则管理中看到具体特征

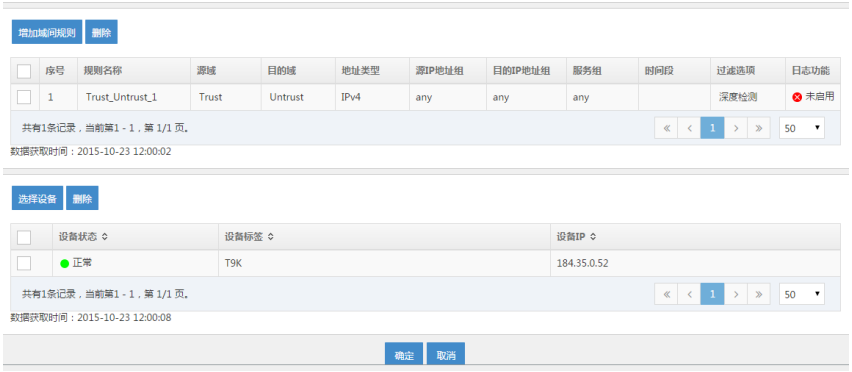
6. 下发策略

业务 - 安全业务管理 - IPS业务配置 - 策略管理 - 增加策略

可以修改所有规则和所选规则



增加域间策略、选择设备后点击确定就可以将策略下发到设备上了
域间策略可以在安全业务管理 - 全局资源中增加，也可以在设备管理中从设备上同步



设备上开启netconf、snmp、telnet 功能，并创建对应权限用户。