🔎 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

资源 - 设备详细信息 - 配置

修改netconf参数

```
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 800063A2808042000856050000001
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
   🖵 资源 > 増加设备
        设备基本信息
        主机名或IP地址*
                                 184.35.0.52
        设备标签
                                                          ?
        掩码
        设备分组
                                                        • ?
                                                        • ?
        登录方式
                                 Telnet
        ✔ 将设备的Trap发送到本网管系统
        ✔ 设备支持Ping操作?
        Ping不通也加入⑦
        将LoopBack地址作为管理IP
       +配置SNMP参数
        ➡配置Telnet参数
       + 配晋SSH参数
  3. 配置设备netconf模板
```

增加netconf配置

🖧 资源 > T9K (18	34.35.0.52)			参 加入收藏 (2帮助
设备详细信息				动作	~
设备标签 设备状态 IP地址	184.11.0.130:8080/imc/netconf/select.jsf?beanNat 184.11.0.130:8080/imc/netconf/select	 同步 副新 取消管理 			
掩码 sysOID	5		a 删除 □、Telnet		
设备型号 类型 系统描述	传输层协议 访问URL协议	SOAP HTTP	yright (c) 2004-	web网管 Ⅲ Ping Ⅲ 路由跟踪	
服务信息	調山号 (1-65535) 访问路径 用户名	80 /soap/netconf/ admin		⊗ 拓扑定位 ◀ MIB管理 □ Telnet/SSH代理	
▶服务监控	用户密码	****** 多次 删除	國定制	国打开设备面板 す。SSH	
性能监视	+	返回		配置	~
监視指标 CPU利用率(% CPU利用率(%		00005	電范 修改显示指标 操作 停止监视 停止监视	 参改系统组属性 参改SNMP参数 参改Telnet参数 参次NETCONF参数 	

4. 增加安全业务设备管理

业务 - 安全业务管理 - 设备管理

设备同步	管理 虚拟 。 删除 刷 解	2. (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)			搜索设备标签或Ⅱ	2	Q, ¥
	状态 ≎	设备标签 \$	设备型号 \$	设备系列	同步时间 \$	同步状态 💲	操作
	●严重	H3C(192.168.216.110)	H3C SecBlade IV IPS	V7	2015-10-23 10:47:04	🙁 失敗	
	●严重	H3C(184.38.0.200)	H3C Unknown Product	V7	2015-10-23 10:47:04	🙁 失敗	
	●正常	Т9К (184.35.0.52)	H3C Unknown Product	V7	2015-10-23 10:47:04	🙁 失败	
共有	93条记录,当前 取时间:2015-	第1 - 3 , 第 1/1 页。 10-23 11:25:51			« < 1 >	» 50	•

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

Res 26	> 安全业务管理 > IPS业务配置 > 特征库	♀ ⊨ Global ▼ ★加入收	·*						
设备将证库列表 将证库文件列表									
升级	▼回滚 自动升级 同步 刷新				设备标签	Q,			
	设备标签 \$	当前IPS特征库版本 \$	上一次IPS特征库版本 \$	当前AV特征库版本 \$	上一次AV特征库版本 ≎	操作			
	H3C(192.168.216.110)					2			
	T9K (184.35.0.52)	1.0.14(20151010)	1.0.13(20150907)	1.0.14(20150827)	1.0.6(20150516)				
	H3C(184.38.0.200)	1.0.13(20150918)	1.0.14(20151010)	1.0.14(20150917)	1.0.10(20150516)				
共有3条记录, 当前第1-3, 第1/1页。 🔍 🔍 50									

同步完成后可以在ips业务配置 - 规则管理中看到具体特征

III 业务 > 安全业务管理 > IPS业务配置 > 规则管理						
刷新	1	舰则名称	୍	. ×		
严重级别 \$	規则各称 ◆		攻击类型 ≎			
<mark>!</mark> 重要	GNU Bash CVE-2014-6271 远程命令执行漏洞		漏洞			
<mark>!</mark> 重要	GNU Bash 单字节溢出漏洞(CVE-2014-7187)		漏洞			
<u>+</u> 重要	(MS10-017)微软 Office Excel MDXTUPLE 记录堆溢出漏洞		漏洞			
<mark>!</mark> 重要	(MS12-015) 做软 Visio Viewer 2010 VSD 文件格式内存破坏(CVE-2012-0019)漏洞		漏洞			
<mark>!</mark> 重要	(MS13-055) 微软 Internet Explorer 内存破坏漏洞(CVE-2013-3148)		漏洞			
<mark>!</mark> 重要	(MS14-012) 微软 Internet Explorer 內存破坏漏洞(CVE-2014-0302)		漏洞			

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

	策略名称 *					
	策略描述					
	拷贝指定策略规则	○是●否				
列表						
1JID		规则名称				
则类型	全部 🔻	规则级别	全部	-		
则状态	全部 ▼	规则动作	全部	•	查询 重置	

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

瑞士加 城可说到 翻铃											
	序号	規则名称	源域	目的域	地址类型	源IP地址组	目的IP地址组	服务组	时间段	过滤选项	日志功能
	1	Trust_Untrust_1	Trust	Untrust	IPv4	any	any	any		深度检测	😵 未启用
共有	1条记录	,当前第1-1,第 1/1 页。							« <	1 > >	50 🔻
数据获	取时间:	2015-10-23 12:00:02									
金澤市											
	设备	状态 \$	设备标识	5 0				设备IP ≎			
	• ī	E常	Т9К					184.35.0.52			
共有1条记录,当前第1 - 1 , 第 1/1页。 🔍 💙 50 💌											
数据获取时间: 2015-10-23 12:00:08											
職会 取消											

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