护网行动ESPC培训

产品支持部　　李倩

CONTENTS 目 录

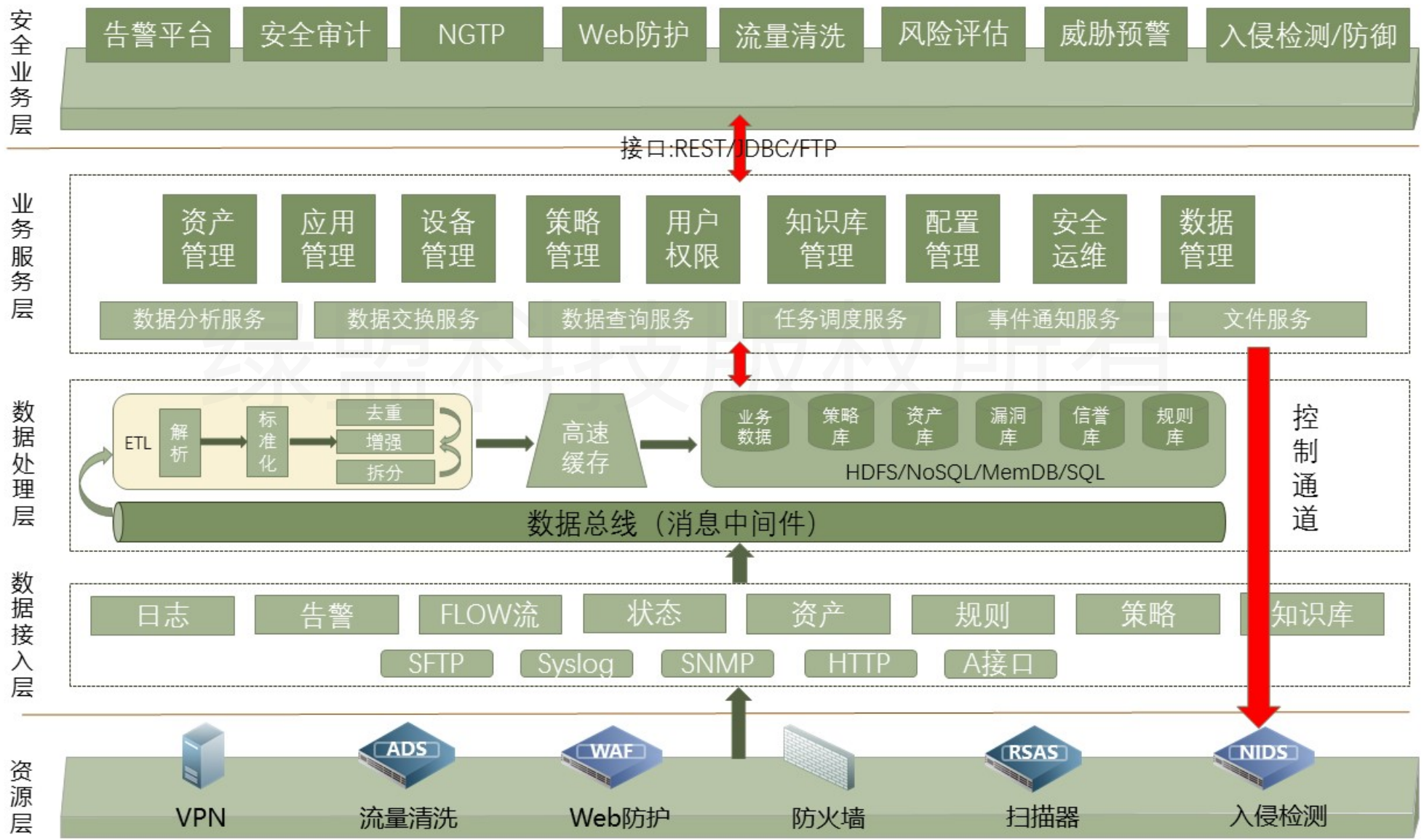
01

ESPC工作原理介绍

ESPCV7是（绿盟企业安全中心）一款Linux产品，它是绿盟科技安全产品的统一管理平台。

功能：设备管理、日志报表、告警平台、策略管理、资产管理、用户管理、系统管理、级联功能等。

功能模块介绍


安全业务层
告警平台
安全审计
NGTP
Web防护
流量清洗
风险评估
威胁预警
入侵检测/防御
接口:REST/JDBC/FTP
业务服务层
资产管理
应用管理
设备管理
策略管理
用户权限
知识库管理
配置管理
安全运维
数据管理
数据分析服务
数据交换服务
数据查询服务
任务调度服务
事件通知服务
文件服务
数据处理层
ETL
解析
标准化
去重
增强
拆分
高速缓存
业务数据
策略库
资产库
漏洞库
信誉库
规则库
HDFS/NoSQL/MemDB/SQL
数据总线（消息中间件）
控制通道
数据接入层
日志
告警
FLOW流
状态
资产
规则
策略
知识库
SFTP
Syslog
SNMP
HTTP
A接口
资源层
VPN
ADS
流量清洗
WAF
Web防护
防火墙
RSAS
扫描器
NIDS
入侵检测

服务器配置要求

	性能规格	小数据低配	小数据推荐	大数据低配	大数据高配
硬件规格	CPU	I7 系列 4核心 8线程	E5 系列 8核心 16线程	E5 系列 12核心 24线程	E5 系列 16核心 32线程
	内存	16G	32G以上	48G	64G以上
	硬盘（可用空间）	500G及以上	1T及以上	2T及以上	4T及以上
部署	部署模式	小数据	小数据	大数据	大数据
	数据库	postgresql	postgresql	postgresql+hive	postgresql+hive

建议使用的浏览器：Chrome 最新版 、 Firefox 最新版、 IE 11

大数据和小数据处理对比

- 大数据处理模式：设备的安全日志是存储HDFS，其它数据包括审计日志、用户信息和模块的运行数据仍然存储在postgres中。
- 小数据处理模式：所有数据存储在postgres中。

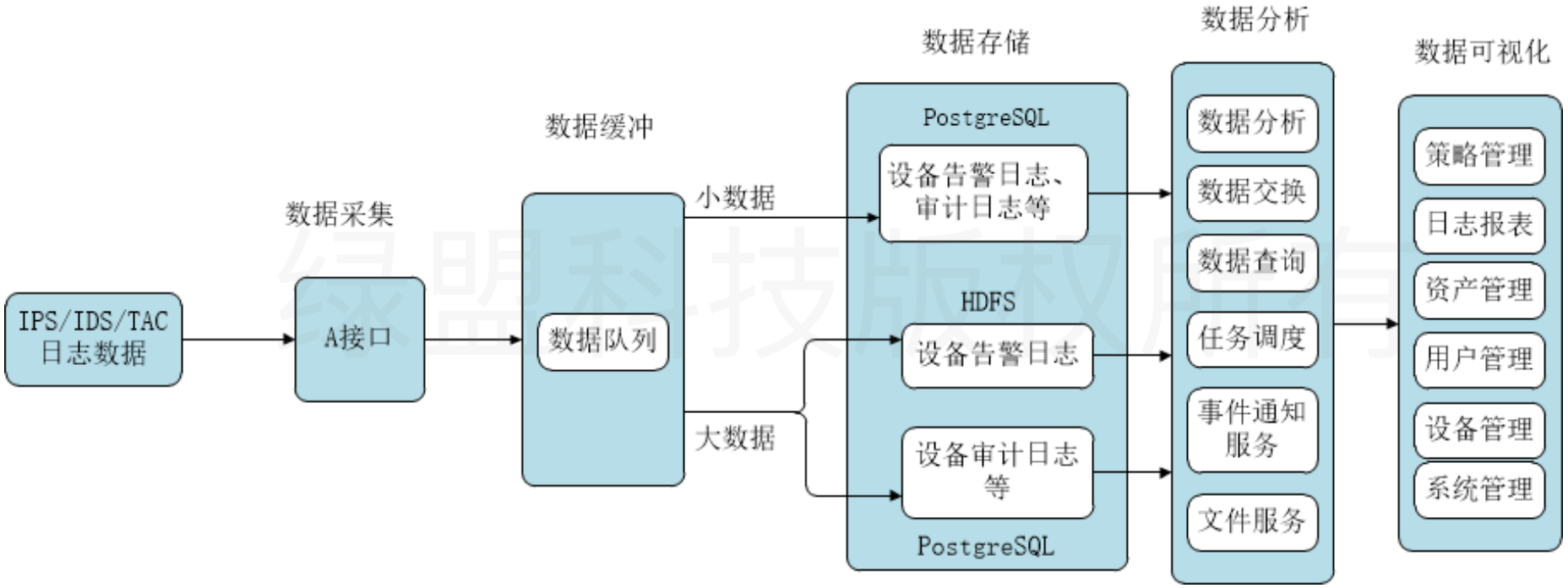
10.5.16.20

数据接入	数据存储	数据处理	应用容器	基础服务
Kafka	Redis	小数据处理	应用进程管理器	HTTP服务器
NPAI-V2	postgreSql			业务服务器
NPAI-V3	存储服务			业务组件
	注册中心			

10.5.16.17

数据接入	数据存储	数据处理	应用容器	基础服务
Kafka	HDFS	Hive	应用进程管理器	HTTP服务器
NPAI-V2	Redis	Spark		业务服务器
NPAI-V3	postgreSql	大数据处理		业务组件
	存储服务	小数据处理		
	注册中心			

数据处理流程


数据采集
数据缓冲
数据存储
数据分析
数据可视化
IPS/IDS/TAC
日志数据
A接口
数据队列
小数据
大数据
PostgreSQL
设备告警日志、
审计日志等
HDFS
设备告警日志
设备审计日志
等
PostgreSQL
数据分析
数据交换
数据查询
任务调度
事件通知
服务
文件服务
策略管理
日志报表
资产管理
用户管理
设备管理
系统管理

02

设备管理功能介绍

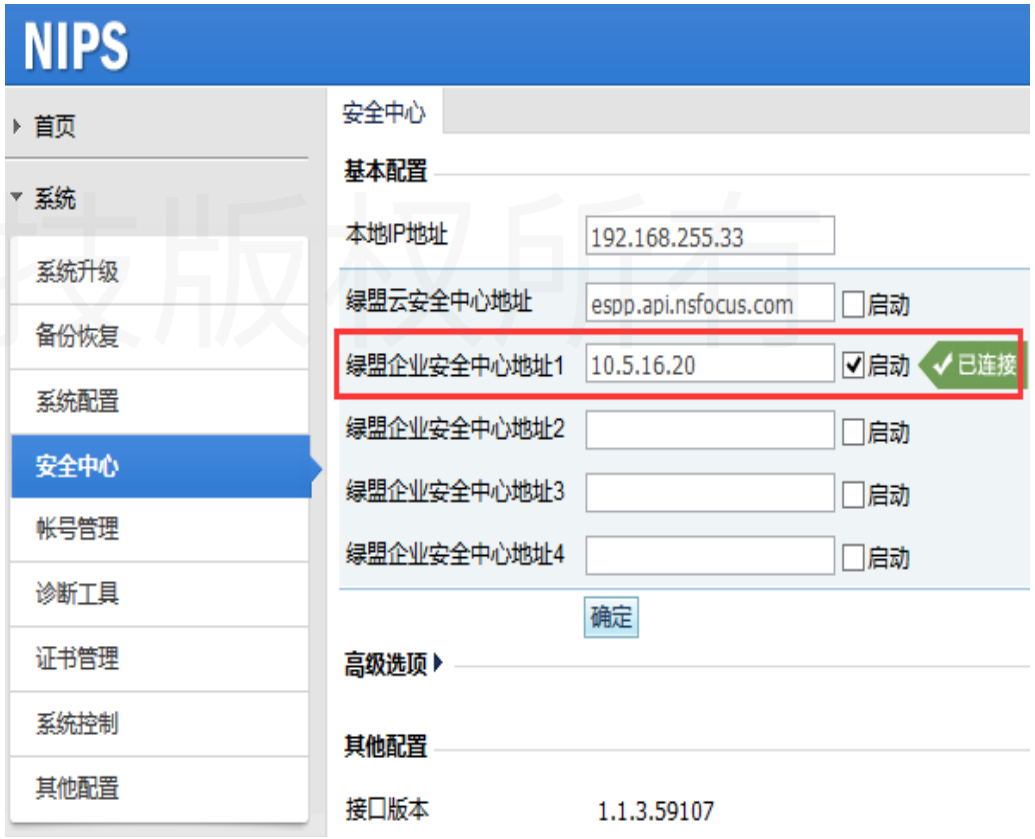
设备联动

第一步：设备上添加ESPC的地址

适用于NIPS/NIDS V5.0R06F10、TACV2.0R01F00SP01等新A接口设备

点击确定生效

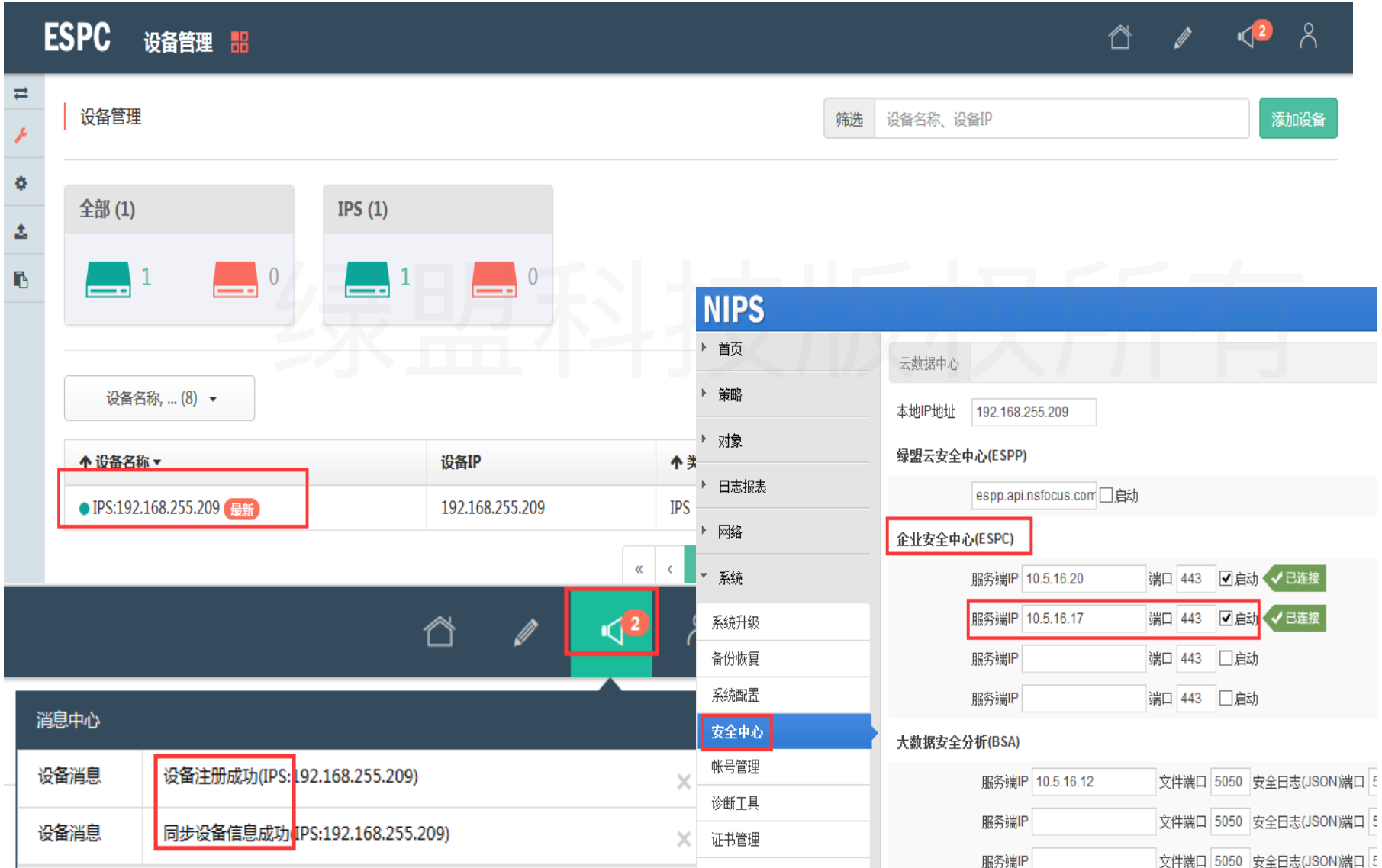
适用于NIPS/NIDS V5.6.7-5.6.9等老A接口设备



重启引擎生效

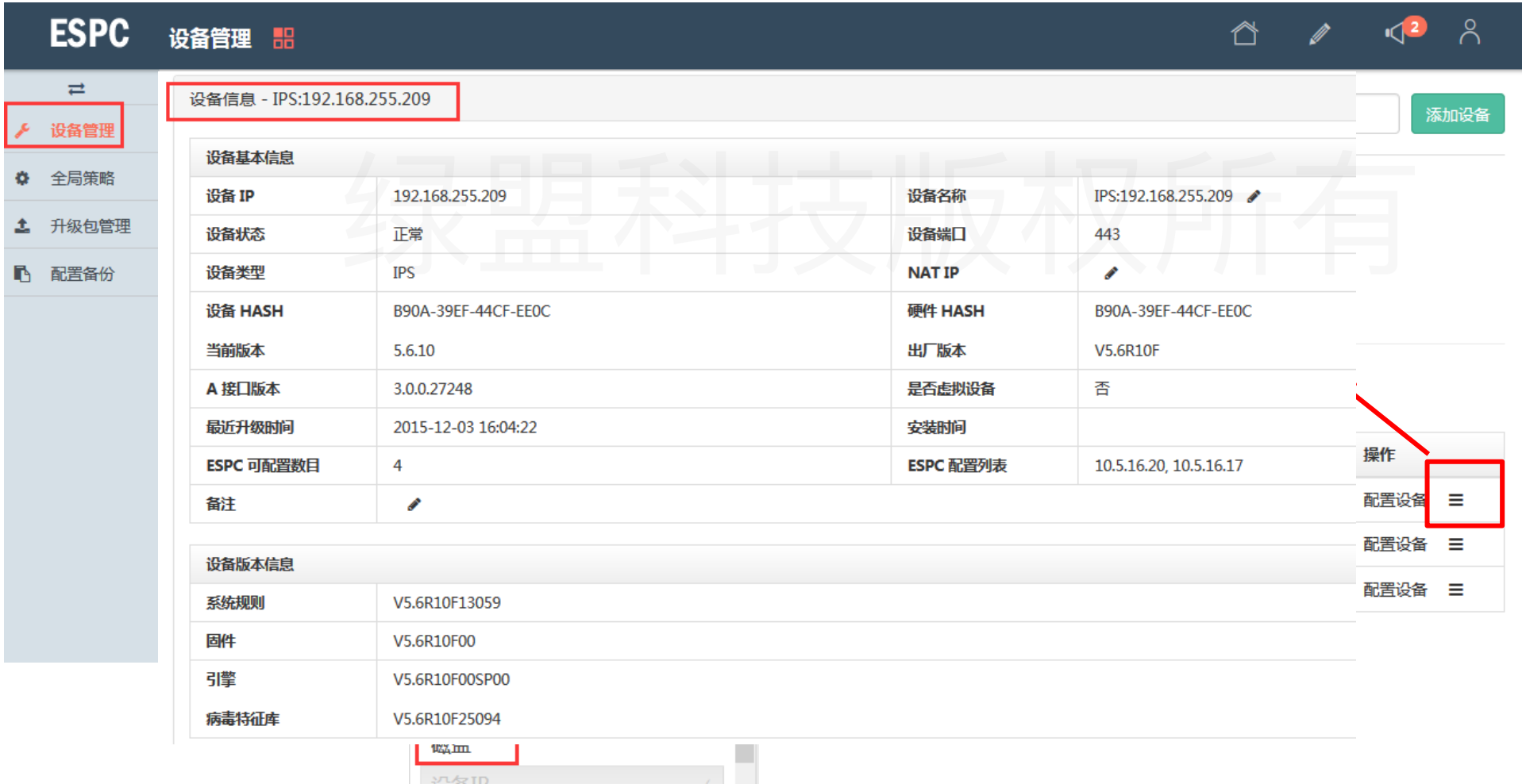
设备联动

第二步：稍后，发现ESPC上注册成功



设备列表展示内容

- **最新**：设备刚接入，执行修改设备基本信息，查看了证书信息、启用、禁用等操作后，“最新”标签消失
- **升级**：升级包管理中下载了该设备可升级的升级包



配置设备网络、路由、DNS等

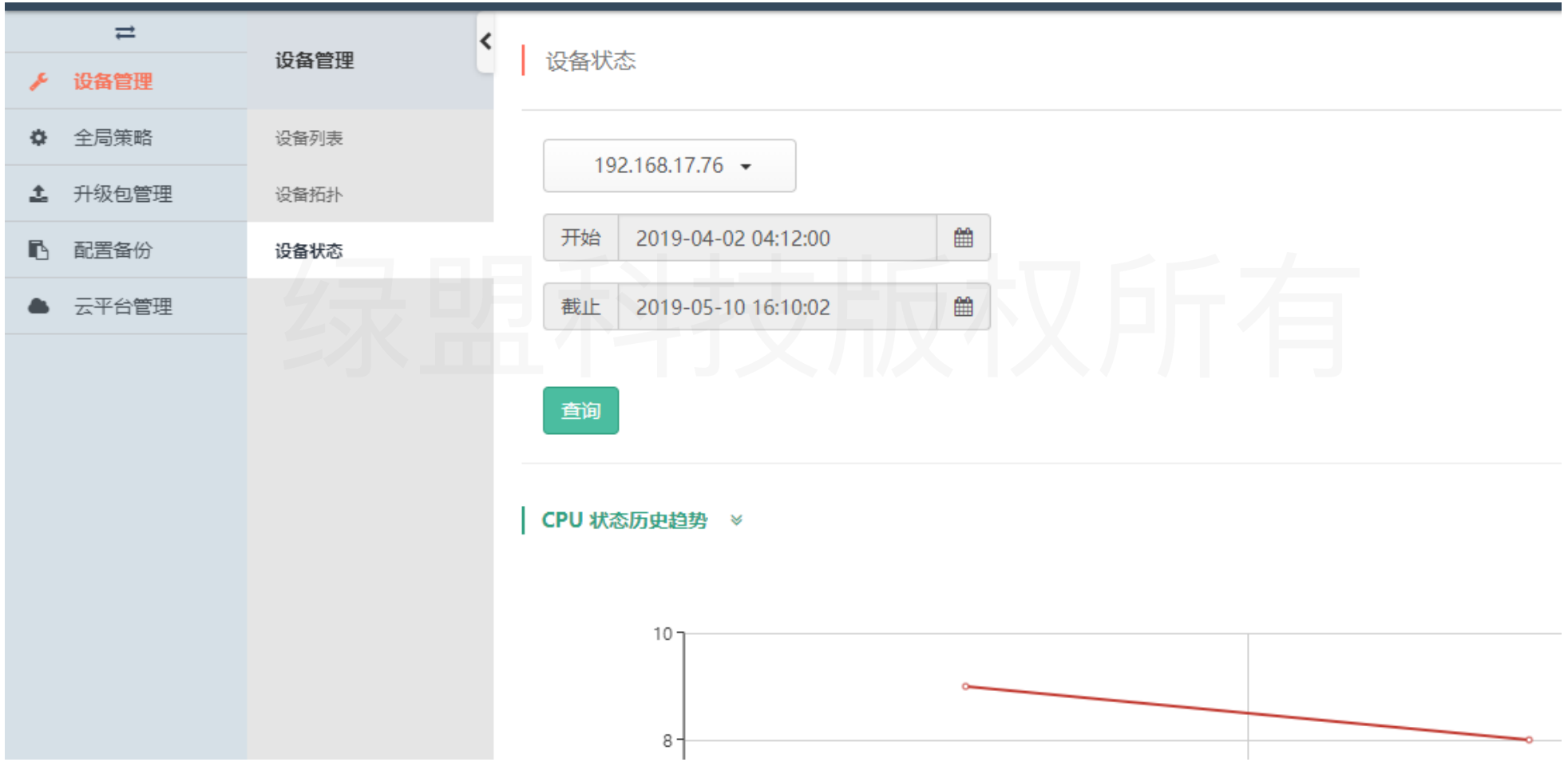
设备名称	设备IP	类型	当前版本	内存	CPU	流量	状态	操作
TAC:192.168.255.39 升级	192.168.255.39	TAC	2.0.1	3%	22%	676bps/0bps	正常	配置设备
IPS:192.168.255.209 升级	192.168.255.209	IPS	5.6.10	76%	15%	9.8Kbps/0bps	正常	配置设备

设备告警（针对单台设备）

功能介绍：若开启该功能，则当设备的CPU、内存、磁盘等达到阈值时便会发出告警。告警方式可选，可配置邮件告警或声音告警。

设备历史状态查询

- 可以展示设备CPU状态历史趋势、内存状态历史趋势、磁盘状态历史趋势、CF卡状态历史趋势、流量状态历史趋势



全局策略-设备升级（针对所有设备）

- 只检查不下载：检查到有新的升级包时，会通知用户。
- 检查并下载：检查到有新的升级包时，会将升级包下载到ESPC服务器，并通知用户。
- 下载并升级：检查到有新的升级包时，会将升级包下载到ESPC服务器，并自动升级安全设备。

全局策略-告警（针对所有设备）

03

日志、报表功能介绍

日志查询功能说明

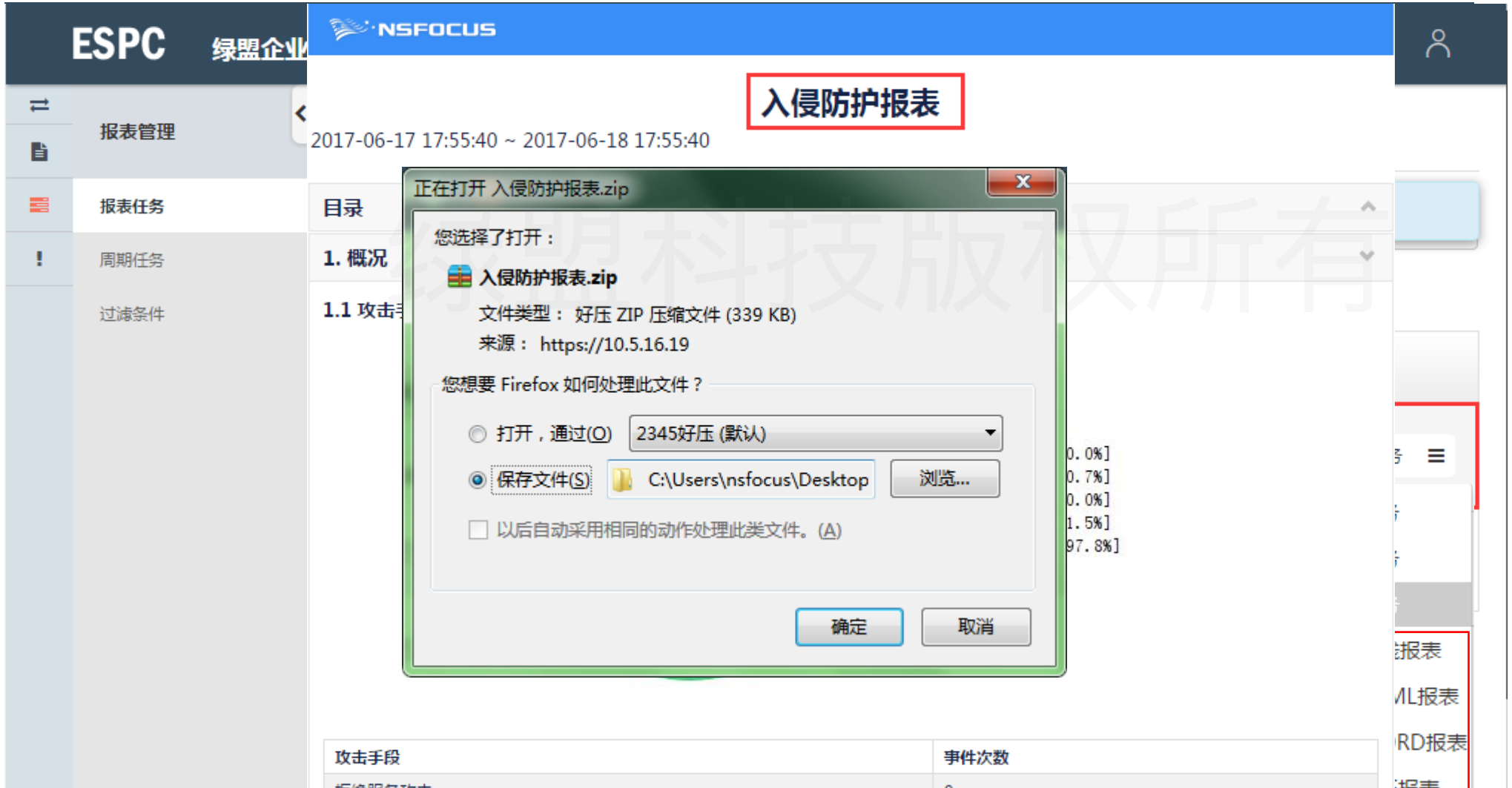
- 日志类型依据联动的设备不同，展示的也不同。
- 日志查询拥有“高级查询”功能，可选择动作、危险程度等，也可根据事件的名称、源目的IP等进行查询。
- 日志显示的表格列支持自定义，可任意选择查看哪几项，最多支持同时查看6项内容。
- 表格列的右上方有“日志导出”功能，支持将日志以excel格式导出，最多导出10W条。
- 表格列的下方有获取日志总数按钮，点击可获取日志总数。

日志查询


ESPC
绿盟企业安全中心
日志分析
入侵防护事件
数据防泄漏
信誉防护事件
URL 过滤日志
防病毒事件
应用管理日志
内容审计
数据库审计
WEB 安全日志
无线热点发现
防火墙日志
认证日志
入侵防护事件
开始
2017-06-18 15:19:37
截止
2017-06-18 16:19:37
查询
高级查询
日志导出
出全部 (Excel)
基础检索
上报设备
192.168.255.134, ... (8)
动作
允许
阻断
旁路阻断
隔离
危险程度
低风险
中风险
高风险
流行程度
高
中
低
攻击手段
拒绝服务攻击
获取权限攻击
信息收集行为
可疑网络活动
网络操作监控
服务类型
www
CGI
FTP
TELNET
事件检索
事件名称
协议摘要
动作
允许

手动报表

- 支持IPS/IDS、SAS、NF、SAS-H、WAF 手动报表生成（报表模板内置，不支持自定义）
- 生成的报表在报表任务列表中查看和下载

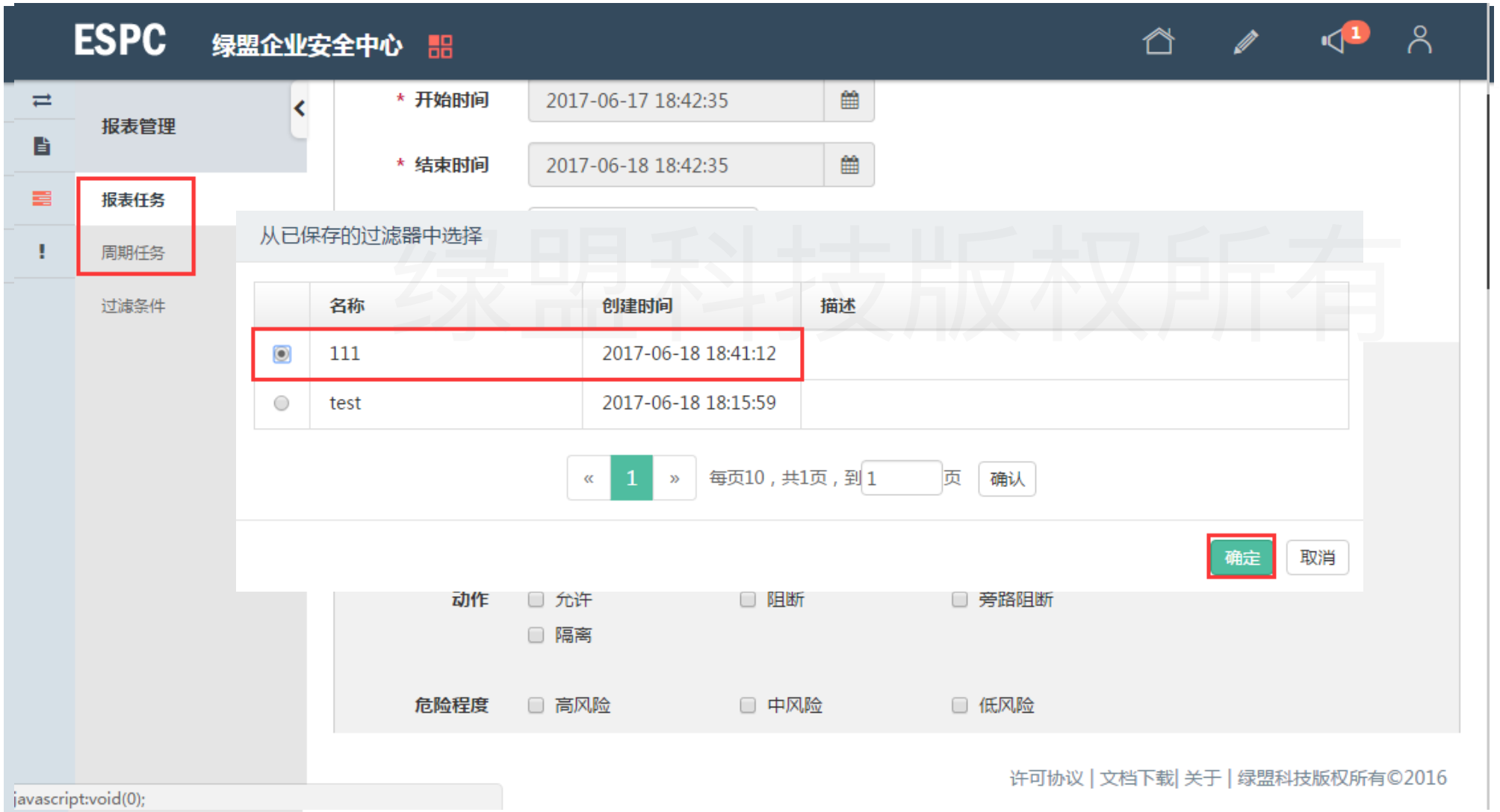


周期报表

- 支持IPS/IDS、SAS、NF、SAS-H、WAF 周期报表生成
- 周期报表每执行一次生成一个子任务，每次执行的报表结果在子任务列表中查看和下载

报表过滤

- 将常用报表内容过滤条件保存成过滤器，生成手动报表/周期报表时直接引用

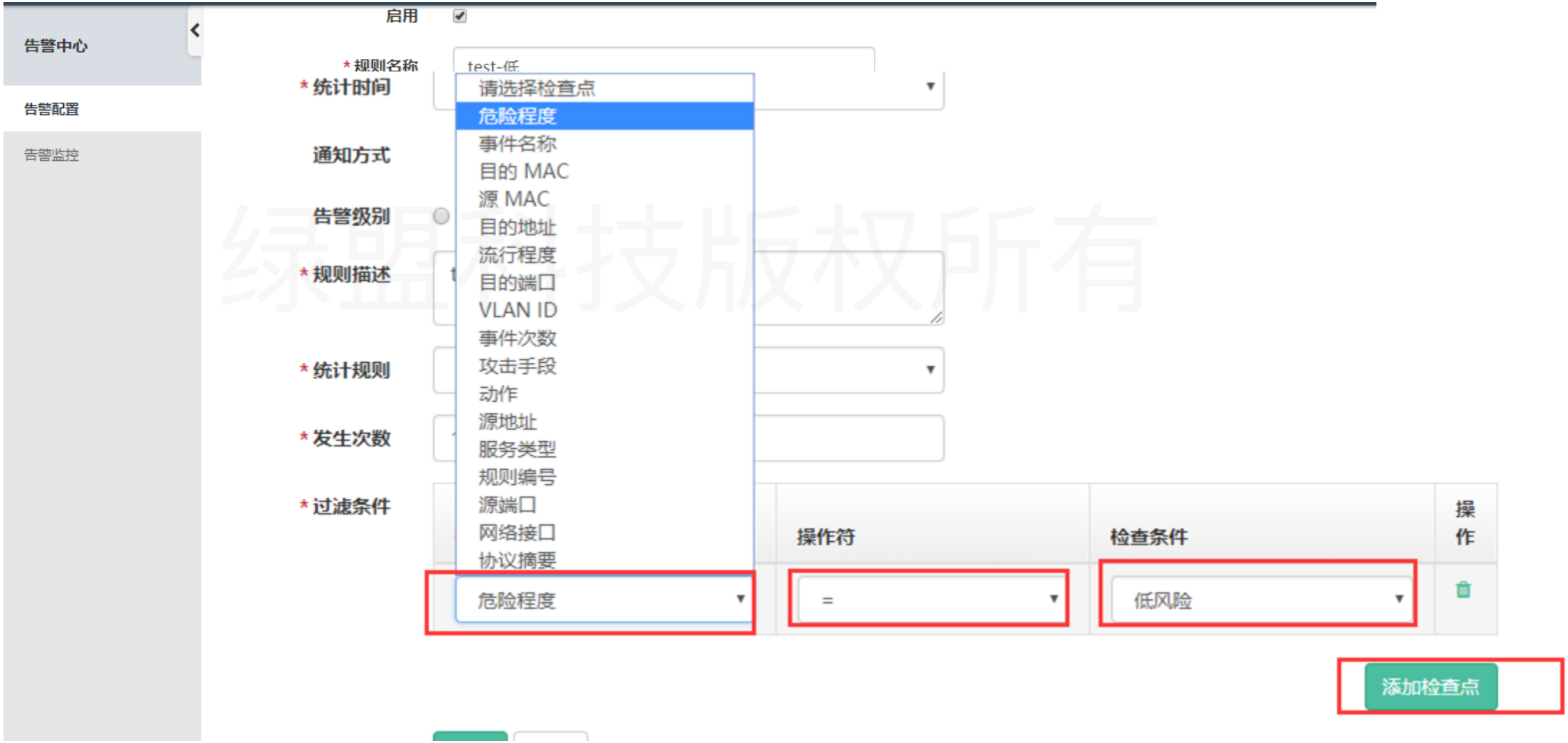


04

告警平台功能介绍

事件告警配置

ESPC v7.0R00F03版本新增告警平台模块，支持针对部分告警事件进行邮件通知。具体配置方法如下：



告警配置-说明

- **统计规则：**分为计数和求和两种；

  统计规则选择计数时：

  指的是对匹配上规则的事件进行计数。比如：若配置的是统计规则编号为10000的日志在30分钟内发生了K次就告警，进行匹配时是当有一条规则编号为10000的日志发生一次就计数一次，最后将30分钟内该事件发生的次数进行求和M。若最后M>=K,则就产生告警，若M<K则不告警。

  统计规则选择求和时：

  指的是对匹配上规则的事件的求和字段进行求和，统计其阈值。比如：若配置的是统计规则编号为10000的日志在30分钟内危险程度阈值超过K时就告警，进行匹配时是当有一条规则编号为10000的日志发生一次统计其危险程度的值一次（比如高：3 中：2 低 1），若30分钟内该事件的危险程度,高危险的发生了A 次/中危险的发生了B次/低危险的发生了C次。则在这30分钟内，该事件危险程度的总统计值为M=3A+2B+C。若最后M>=K,则就产生告警，若M<K则不告警。

- **过滤条件：**对日志事件的一些过滤条件，最多可以建5条，这些过滤条件之间是与的关系，即需要同时满足这些过滤条件。

求和时统计字段对应的数值

类型	字段	数值
入侵防护日志	gr_pop(流行程度)	1-高；2-中；3-低；4-其他
	gr_type(攻击手段)	16-拒绝服务攻击；32-获取权限攻击；48-信息收集行为；64-可疑网络活动；80-网络操作监控
	action(动作)	1-允许；2-阻断；3-旁路阻断；4-隔离
	gr_danger(危险程度)	1-高风险；2-中风险；3-低风险
	gr_service(服务类型)	1-www;2-CGI;3-FTP;4-TELNE;5-POP;6-NETBIOS;7-SSH;8-SMTP;9-IMAP;10-DNS;11-TFTP;12-FINGER;13-KERBEROS;14-LINUXCONF;15-LDAP;16-SUNRPC;18-RSH;19-RLOGIN;20-SQL;21-LPD;22-IRC;23-

告警监控

可查看产生的实时告警及全部告警。

告警平台-注意事项

- 使用邮件告警前需要配置邮件告警服务器
- 告警监控分为实时监控和历史监控。实时监控可以对最近2小时告警进行查看。历史监控是可以对所有告警进行查看。
- 当新建多个告警规则时，各个规则之间是相互独立的关系。

谢谢！

NSFOCUS