随方网络安全管理中心

SAFEIN NETWORK SECURITY MANAGEMENT CENTER

北京随方信息技术有限公司

Beijing Safein Information Technolgy Limited

目录

1 公司简介
我们是谁

2 产品介绍
我们要做什么

3 优势及案例
我们怎么做

1、公司简介

公司历程

北京随方信息技术有限公司成立于2013年。“随方”取意“君子如水，随方就圆”。公司以此为精神，以创新、进取、务实、可信的专业姿态，致力于让中国的网络更安全!

产品及服务

- 配置合规性检查
- 资产自动侦测与管理
- 主机审计与漏扫
- WEB审计
- 网络建模与仿真
- 公有云O2O检查平台

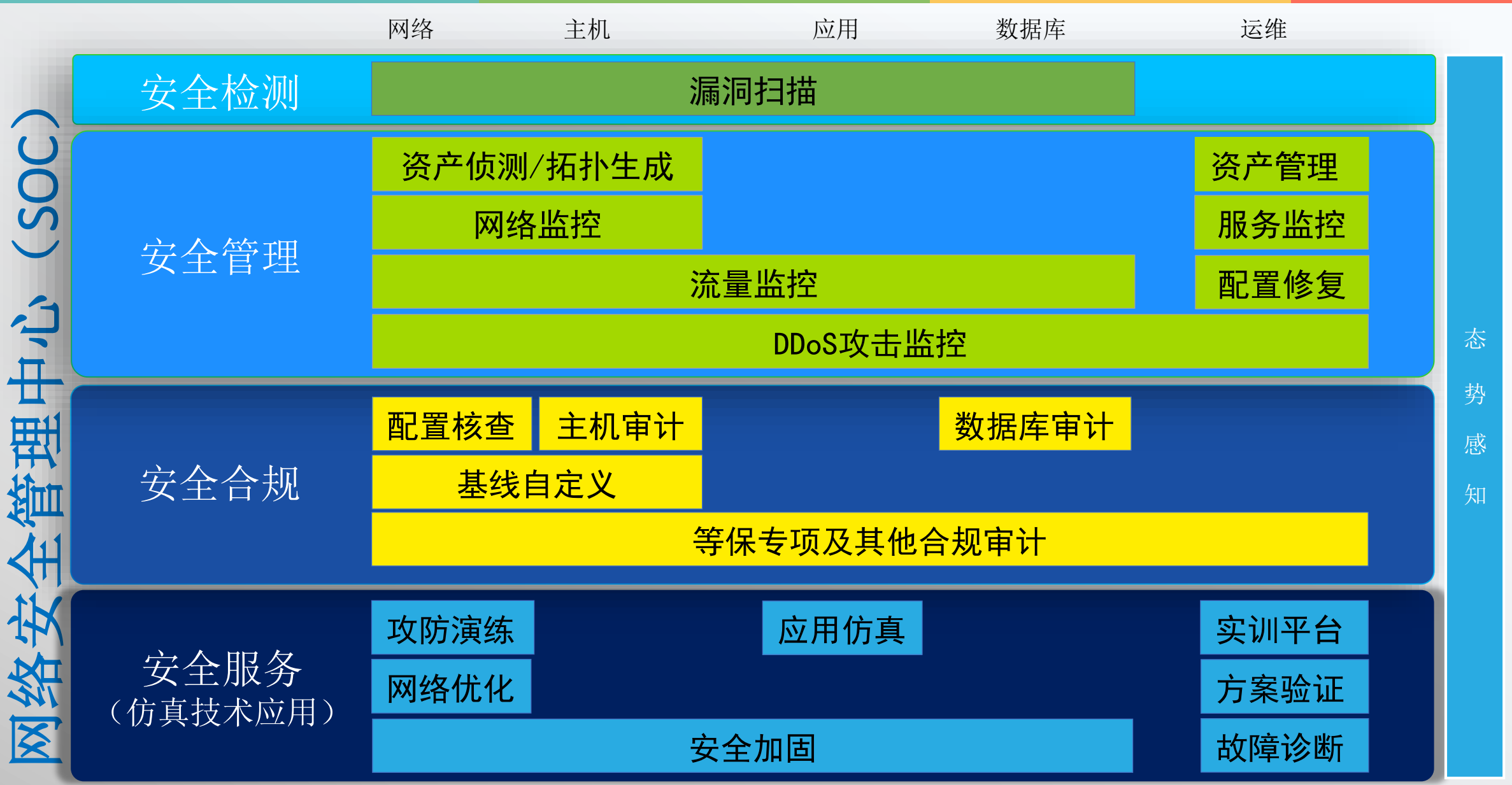
荣誉认可

获得多项创新基金 -
拥有多项发明专利、软件著作权 -
通过ISO9001，27001认证 -

客户群

- 政府机构
- 行业客户
- 企业用户

2、产品介绍—2.1产品概要（产品功能）



2、产品介绍—2.1产品概要（产品价值）

高性价比

同类产品完整功能采购成本的1/10

整体解决方案

- 发现且解决网络问题
- 全程全网全覆盖
- 首创非接入生产环境检测方法
- 5分钟上手，全自动化执行

技术及创新

- 前沿仿真技术实用化，低成本满足攻防演练、建设方案验证、上线前测试需要
- 全国产化，7项专利、3件软著
- 突破了对虚拟设备、无IP设备的检测盲区
- 万条规则库储备，实现对20+主流厂商全面支持
- 高扩展性

  一周内完成未知厂商支持

  2小时内完成1条新规则定制

2、产品介绍—2.1产品概要（客户收益）

- 安全的网络环境保障企业健康发展
- 强化业务连续性管理
- 优化网络基础架构
- 建立趋势（风险）管理体系
- 推进企业管理标准化

- 网络运行状态尽在掌控
- 提前预警，预防网络风险
- 安全管理，快速管控全局
- 安全规章制度定制化落地
- 第三方验证安全工作绩效
- 适用于网络安全审计管理

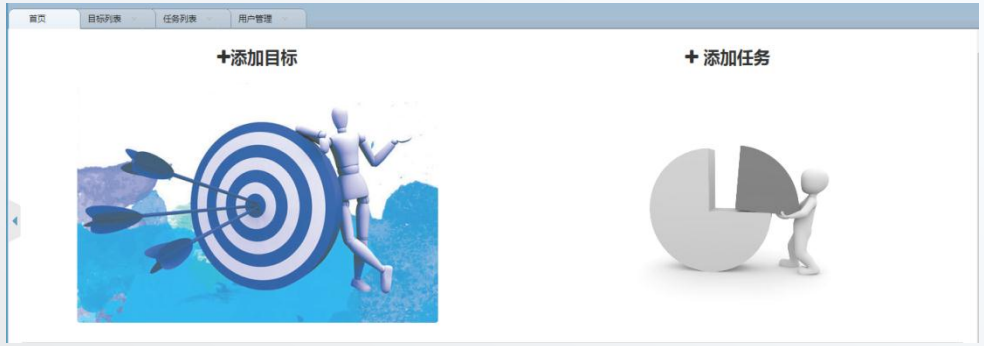
- 随时掌控网络资产
- 支持设备联网检测
- >99%准确率，精准锁定目标
- 一键式操作，自动化处理
- 快速排错，极大地提高效率

2、产品介绍—2.2产品介绍—2.2.1安全检测（漏洞扫描1）

漏洞扫描

网络漏洞扫描（主动扫描）：通过网络来扫描计算机中的漏洞

可以检测远程系统和应用程序中的安全问题
系统：windows（Windows XP，Windows Vista，Windows 7，Windows 8，Windows 8.1，Windows10等）、
unix(Mac OS X和Linux发行版（如Debian，Ubuntu,Red Hat,Centos等)
应用程序：OpenSSL的脆弱性检查（中间人漏洞检查、xauth命令注射、算法的脆弱性检查、提权漏洞检查）、远程SSH服务漏洞检查（弱MD5或MAC算法检查）、主流数据库漏洞检查（mysql、Oracle、DB2、SqlServer等）、http服务漏洞检查（PUT和DELETE请求是否允许）



2、产品介绍—2.2产品介绍—2.2.1安全检测（漏洞扫描2）

漏洞扫描报告

扫描报告内容：简要说明主机扫描的信息主要包括以下内容：

- 总结
- 漏洞检测结果
- 漏洞检测方法
- 解决方案
- 参考

2、产品介绍—2.2产品介绍—2.2.2安全管理（设备侦测）

全新的探测技术

自动侦测未知网络

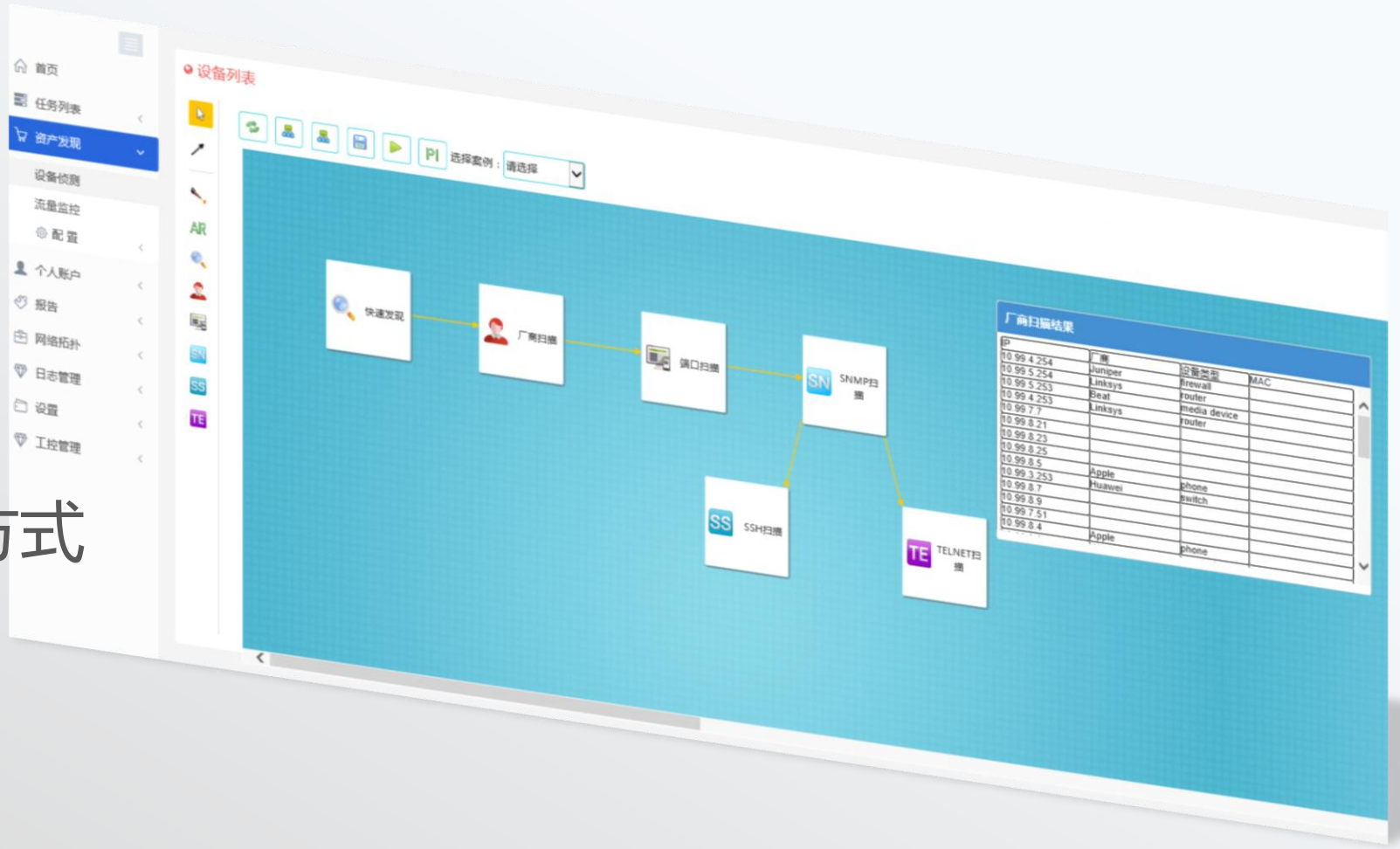
支持所有类型设备，包括接入网络的手机，平板等

区别于SNMP侦测方式

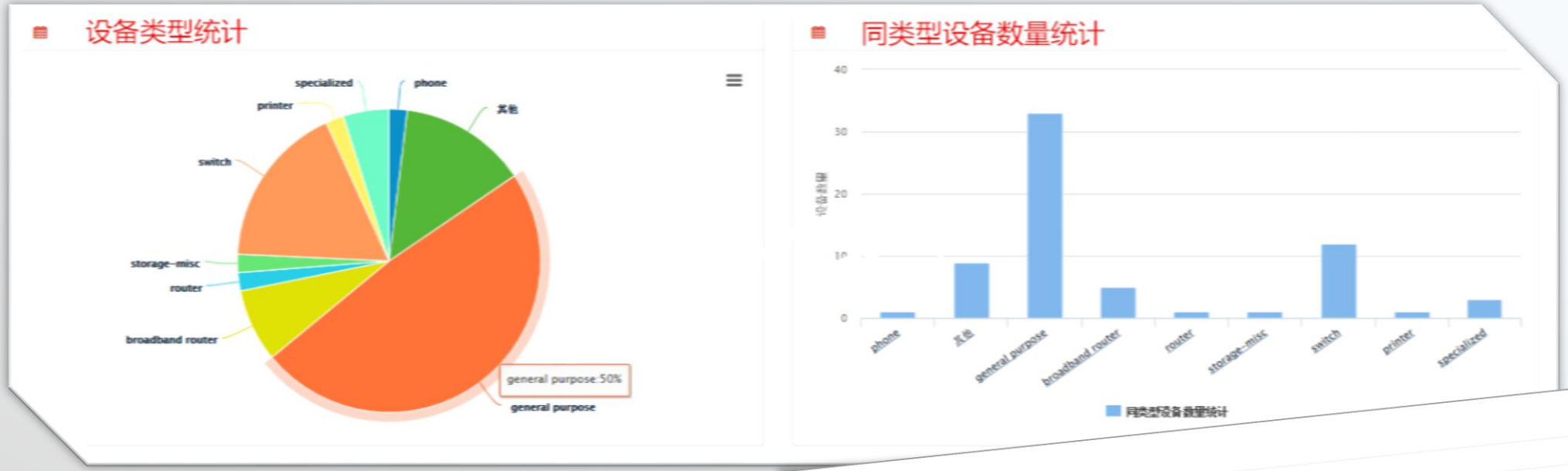
SNMPv2存在安全隐患

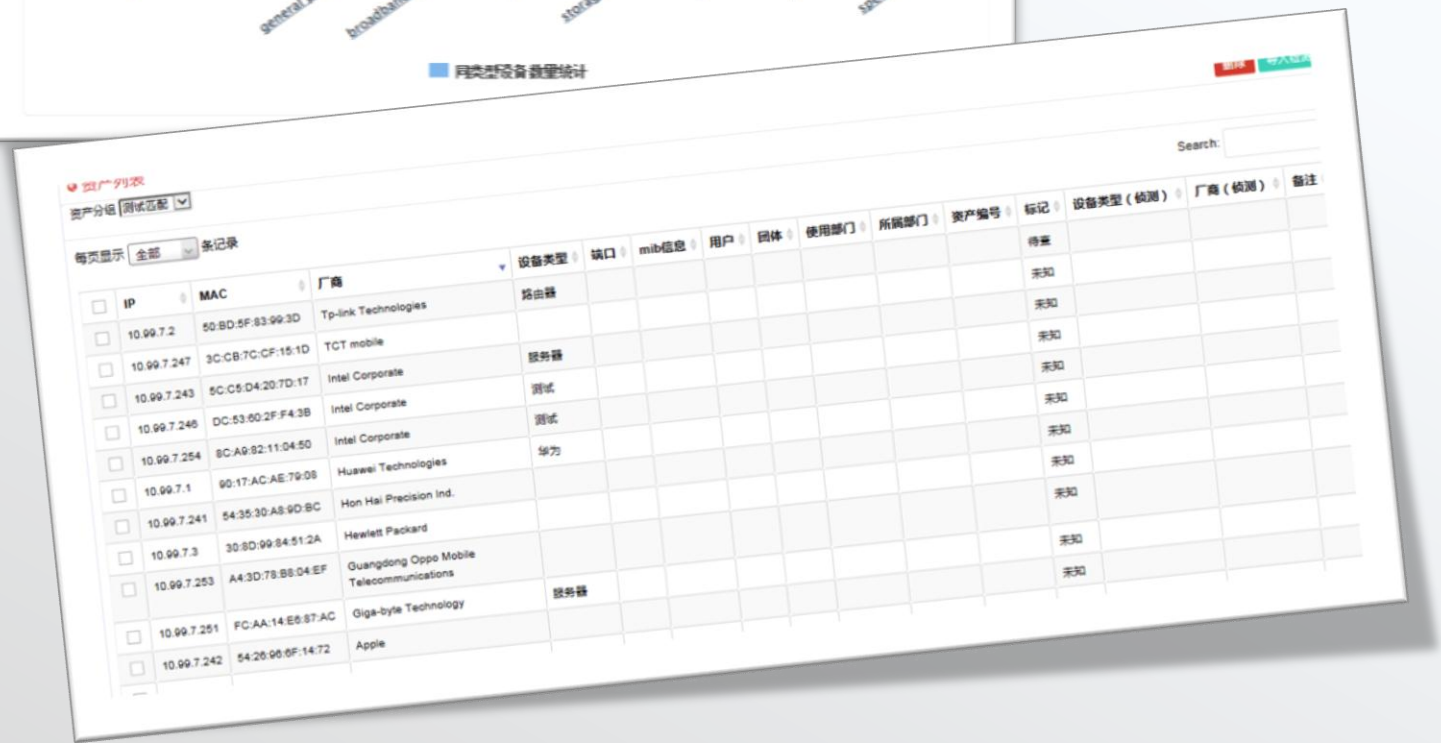
设备必须支持并配置SNMP

未知设备无法实现侦测和管理



2、产品介绍—2.2产品介绍—2.2.2安全管理（资产管理）





- 可自定制关键词进行分类统计
- 支持资产编号，所属部门等字段的输入

2、产品介绍—2.2产品介绍—2.2.2安全管理（网络监控）

网络监控：实时监控网络内设备使用情况，可按需选择性监控，也可全网全覆盖监控。

2、产品介绍—2.2产品介绍—2.2.2安全管理（流量监控）

流量监控：通过镜像流量将网络中所有流量信息直观展现出来

既可以查看网络流量详细也可以查看网络流量整体信息

流量数据详细信息

每页显示 10 条记录　　检索：

	ip地址	相关信息	操作系统类型	开机时间	第一次出现时间	最后一次出现时间	总数
⊟	5.45.76.23	俄罗斯	Linux 3.11 and newer	0 days 1 hrs 13 min (modulo 198 days)	2016/12/15 下午3:13	2016/12/15 下午3:13	5
	操作	应用	端口	发包数量			
	⊟	未知	22	5			
		⊟	服务端:10.99.1.88	局域网	总数量:5		
⊞	5.102.212.48	以色列	Linux 2.2.x-3.x (barebone)	未知	2016/12/15 下午3:17	2016/12/15 下午3:17	2
⊞	201.173.130.60	墨西哥	未知	未知	2016/12/15 下午3:18	2016/12/15 下午3:18	1
⊞	189.219.45.234	墨西哥	未知	未知	2016/12/15 下午3:13	2016/12/15 下午3:13	1
⊞	178.156.128.201	罗马尼亚	未知	未知	2016/12/15 下午3:13	2016/12/15 下午3:13	1
⊞	176.98.135.242	俄罗斯	未知	未知	2016/12/15 下午3:20	2016/12/15 下午3:20	1
⊞	123.249.12.230	贵州省黔西南州兴义市	Windows XP	未知	2016/12/15 下午3:13	2016/12/15 下午3:13	60
⊞	122.223.146.121	日本	未知	未知	2016/12/15 下午3:14	2016/12/15 下午3:14	1
⊞	122.176.35.215	印度	未知	未知	2016/12/15 下午3:12	2016/12/15 下午3:12	1

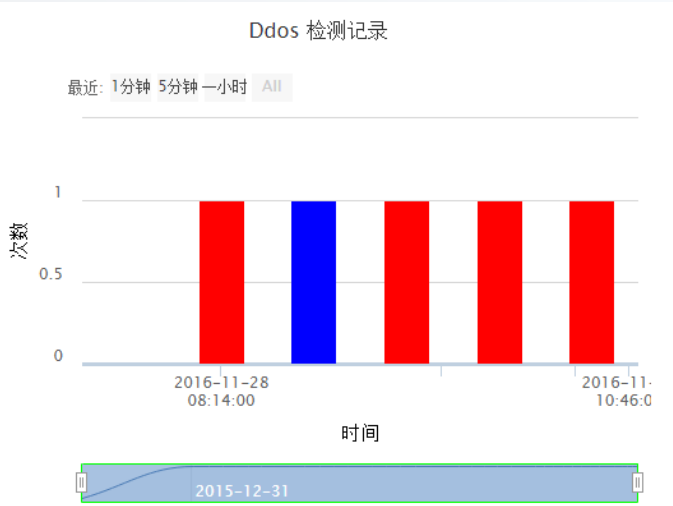
动态流量总体情况

2、产品介绍—2.2产品介绍—2.2.2安全管理（DDoS监控）

DDOS攻击监控

DDos检测

发现Ddos攻击总次数:5次
已处理次数:1次
未处理次数次数:4次
----------详细情况----------
ip地址:10.99.2.202
攻击类型:icmp_flood
发现攻击时间:2016/11/28 下午6:45
收包pps峰值:1 pps
发包pps峰值:20397 pps
收包bps峰值:0 mbps
发包bps峰值:12 mbps
是否处理: 未处理



通过DDOS攻击检测结合流量数据分析实时展现网络内DDOS攻击情况，更好的实现网络的安全管理。

ip地址	收包速率(pps)	发包速率(pps)	Ddos攻击类型	时间	是否处理	操作
10.99.2.205	0	23411	icmp_flood	2016/11/28 下午6:42	未处理	抓包分析|标记为已处理|下载pcap文件
10.99.2.204	4	22144	icmp_flood	2016/11/28 下午6:41	已处理	抓包分析|标记为未处理|下载pcap文件
10.99.2.203	0	21525	icmp_flood	2016/11/28 下午4:14	未处理	抓包分析|标记为已处理|下载pcap文件
10.99.2.202	1	20397	icmp_flood	2016/11/28 下午6:45	未处理	抓包分析|标记为已处理|下载pcap文件
10.99.2.201	22	27281	icmp_flood	2016/11/28 下午6:43	未处理	抓包分析|标记为已处理|下载pcap文件

2、产品介绍—2.2产品介绍—2.2.2安全管理（端口温控）

省心

化繁为简，重要资产运行信息一目了然

01

便捷

配置文件中分散在各个设备的信息，**自动采集**，**自动生成**直观的图表

02

省时

节省人力成本、时间成本，减轻了运维人员的工作量，更快速的发现故障的网络资产

03

省力

自动采集、自动分析高温预警

04

2、产品介绍—2.2产品介绍—2.2.3安全合规（主机审计）

主机安全审计

根据国际标准、国家法规、技术标准、行业要求或者自定义标准进行主机审计出具详细的审计报告。

2、产品介绍—2.2产品介绍—2.2.3安全合规（WEB安全审计）

WEB安全审计

不改变现有网络体系结构、不占用WEB服务器任何资源、不影响WEB服务器性能的情况下，旁路方式快速部署到业务系统网络中，从而满足企业对WEB应用实时监控与审计的需求。

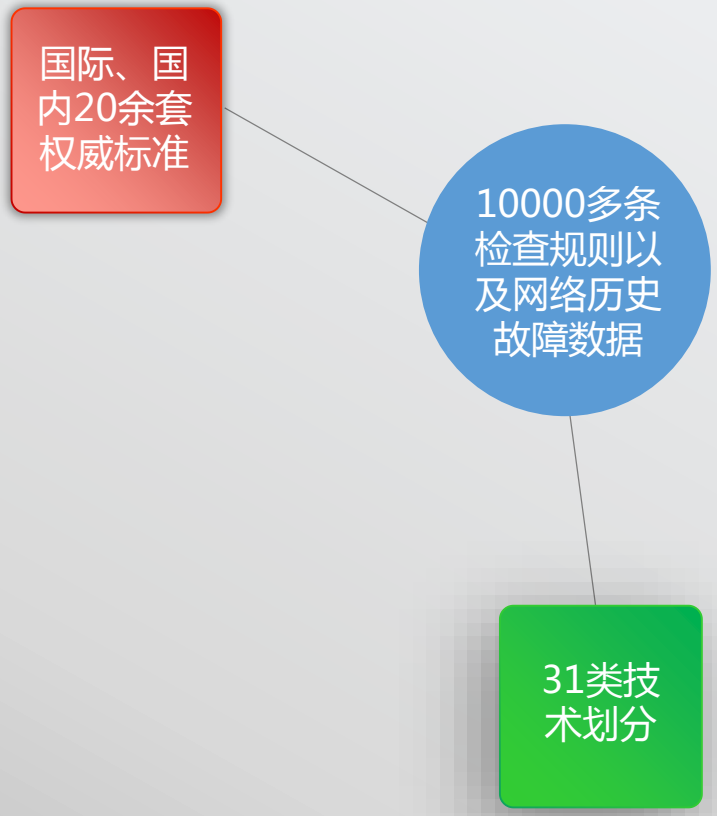
汇总报告

名称	内容
项目名称	adcc
扫描对象	https://10.99.1.188/login.do
开始时间	2016-10-13 18:51:05.0
结束时间	2016-10-13 18:54:17.0
扫描用时(单位:秒)	192
协议	https
域名	10.99.1.188
已访问url	241
url总数	241
漏洞个数	50

漏洞名称	漏洞级别	描述	漏洞介绍	关键字	修复建议
跨站脚本	中危漏洞	发现了一个跨站脚本漏洞: "https://10.99.1.188/nea/finddongle.do" ,发送了 POST 请求.发送的数据是: "userName=qdidk%22qdidk&password=safein%40123" ,这修改了参数: "userName" .	客户端脚本被广泛使用的现代Web应用程序，他们执行从简单 的功能（如文本的格式）到全操作的客户端数据和操作系统的相互作用。 跨站脚本（XSS）允许客户将任意脚本代码请求和服务器返回到客户端的响应脚本 这是因为应用程序是以不可信的数据（从客户端在这个例子中，）和重用，不执行任何验证或编码。	qdidk\qdidk	为了弥补XSS漏洞，这是从来没有在一个HTML页面的代码不受信任或未经过滤的数 据使用的重要。 不可信的数据不仅来源于形式的客户但可能 三分之一方或先前上传文件等过滤不可信数据通常需要将特殊字符转换为HTML 实体编码的对应体（然而，其他方法确实存在，见 引用）。这些特殊字符包括:

通过WEB防护功能，防止各种WEB应用层攻击，如：SQL 注入、跨站攻击、表单绕过等等

2、产品介绍—2.2产品介绍—2.2.3安全合规（配置检查1）



国际

ISO-27002信息安全管理实务守则、PCI数据安全标准

国内

信息安全等级保护管理办法

美国

美国国家安全局--路由器安全配置指南、萨班斯·奥克斯利法案

厂家

思科IOS基线配置指南、思科防火墙基线配置指南

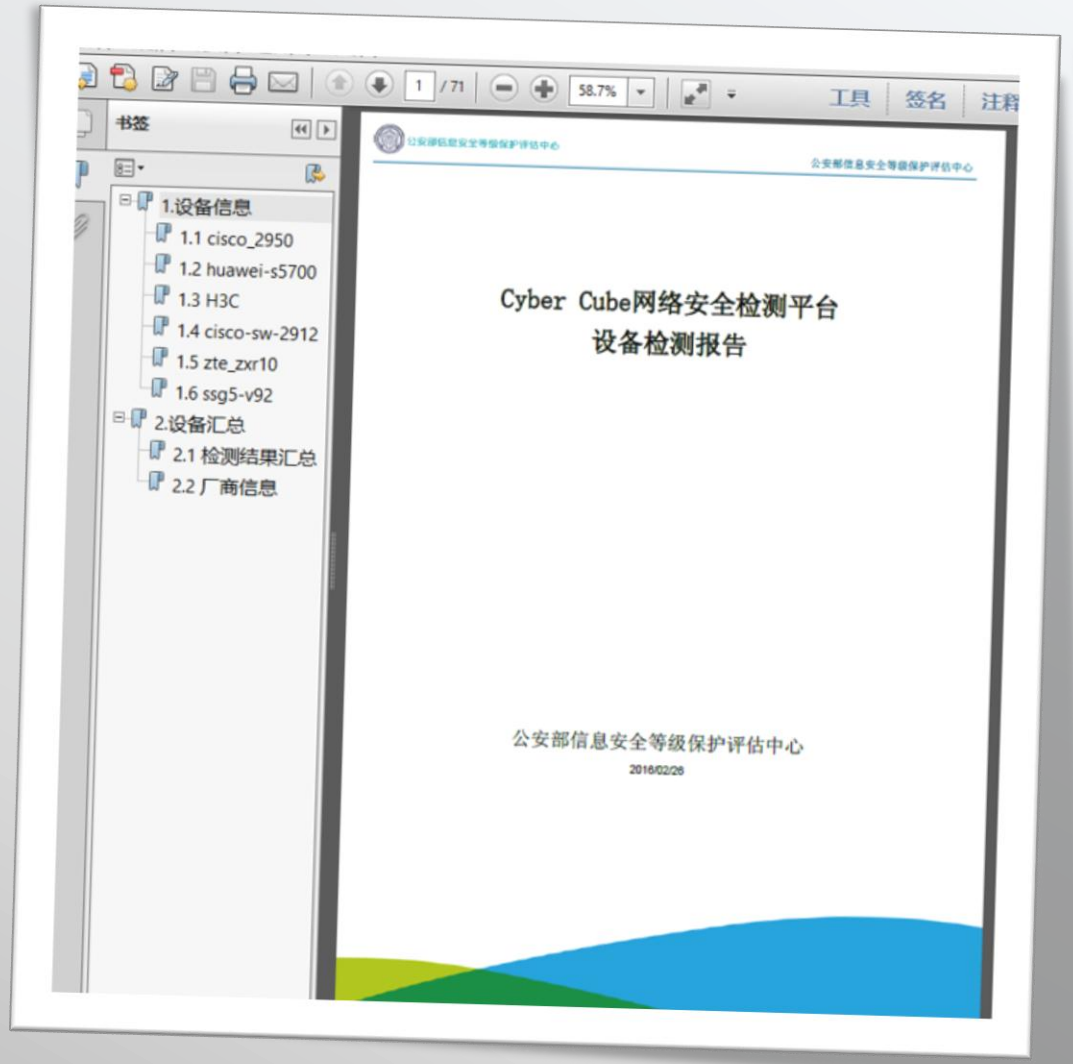
设备基础管理	OSPF路由	ARP协议
安全服务	ISIS路由	AAA技术
远程登录	BGP路由	防火墙技术
系统日志与审计	路由策略	SNMP协议
交换接口	策略路由	IP地址类
IP接口	VLAN技术	HSRP协议
DHCP协议	生成树协议	VRRP协议
NAT技术	访问控制列表	VPN技术
静态路由	QoS服务质量	生命周期通知
RIP路由	IP组播	安全预警
EIGRP路由		

2、产品介绍—2.2产品介绍—2.2.3安全合规（配置检查2）

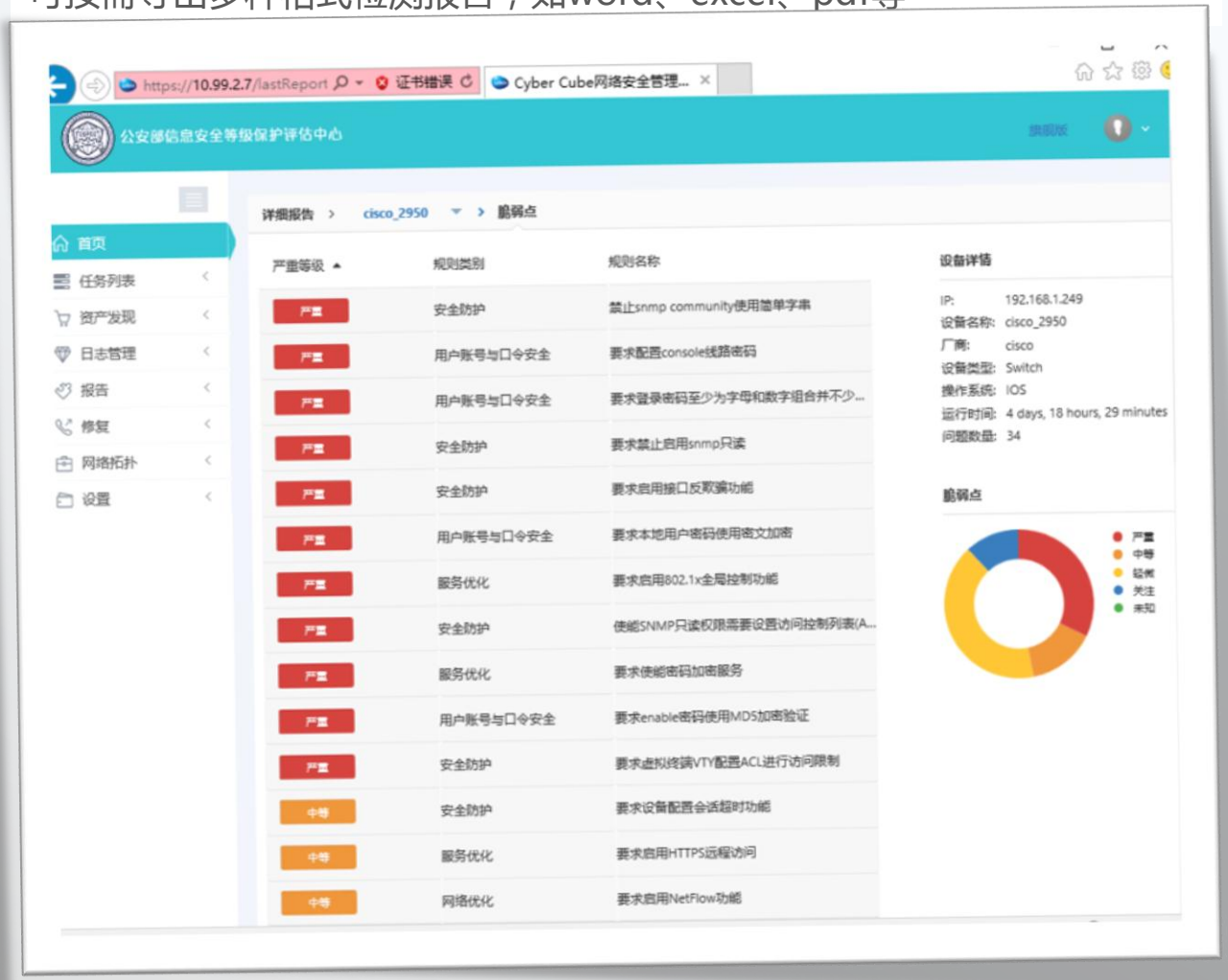
配置检查汇总结果

2、产品介绍—2.2产品介绍—2.2.3安全合规（配置检查3）

多种报告呈现方式



可按需导出多种格式检测报告，如word、excel、pdf等



2、产品介绍—2.2产品介绍—2.2.3安全合规（配置检查4）

详细报告内容

严 重

问题详情

发现问题

本设备的如下VTY没有配置ACL: vty 0 4。

规则定义

设备配置的VTY虚拟终端线路应该设置ACL进行限制,以阻止从禁止的范围内向服务器尝试未经授权的访问。

理论依据

可以通过访问控制列表（ACL）实现对通过VTY用户界面的登录进行限制，在配置VTY用户界面的登录限制前，需要先在特权模式(系统视图)下执行acl命令创建一个访问控制列表并进入ACL模式(视图)，然后执行相关命令增加相应访问控制列表的规则。

修复方法

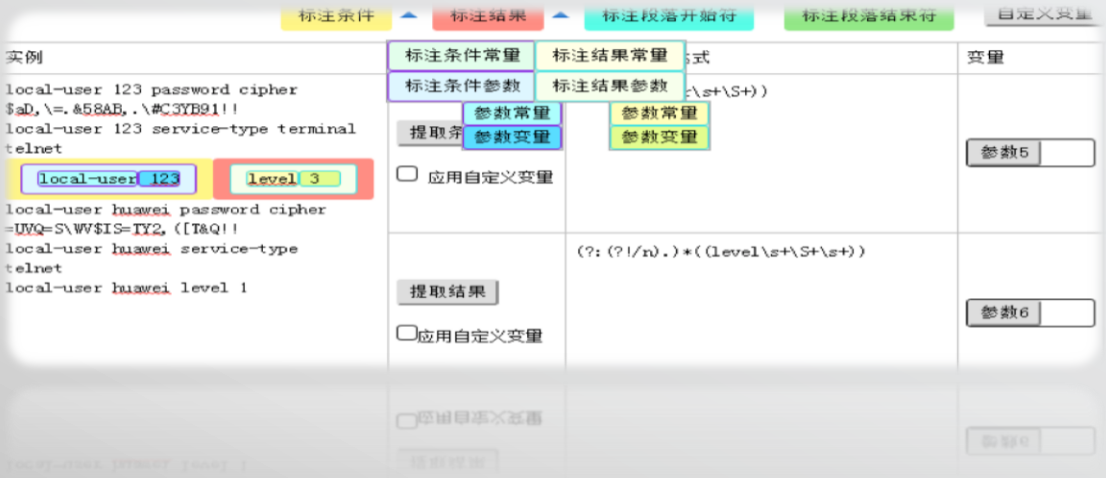
参考命令：hostname(config-line)#access-class acl-numberin

参考文献

PCI数据安全标准（版本号2.0）
信息技术安全标准NIST 800-53
北美电力可靠性协会互联系统运行准则
GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

2、产品介绍—2.2产品介绍—2.2.3安全合规（基线自定义1）

要求内容	应按照用户分配账号，避免不同用户间共享账号。避免用户账号和设备间通信使用的账号共享。
判定条件	I. 配置文件中，存在不同的账号分配 II. 网络管理员确认用户与账号分配关系明确
检测操作	使用 display current-configuration 命令，如下例： aaa local-user 123 password cipher $aD,\=.&58AB,.\#C3YB91!! local-user 123 service-type terminal telnet local-user 123 level 3 local-user huawei password cipher =UVQ=S\WV$IS=TY2,([T&Q!! local-user huawei service-type telnet local-user huawei level 1



国际、国内权威规范，

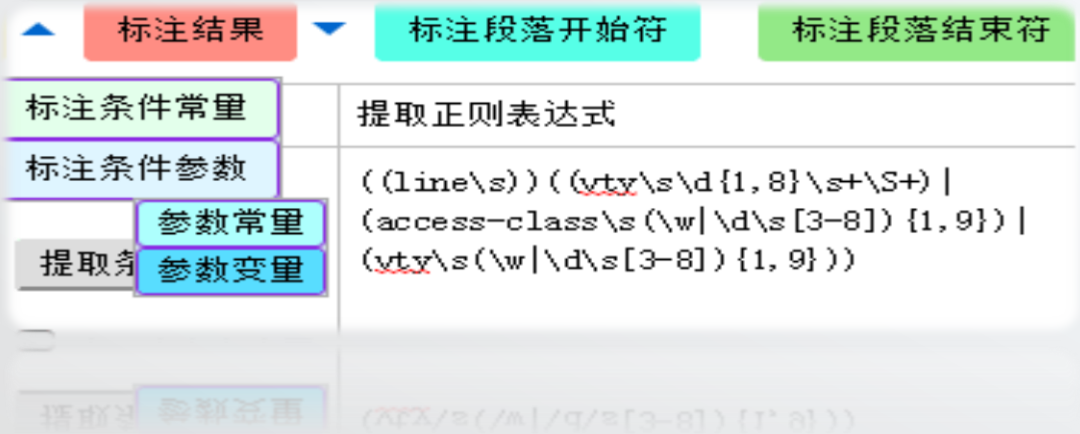
行业规范

特定信息系统规范

图形化界面选择关键字，自动生成正则表达式

简单快捷无需编程经验

2、产品介绍—2.2产品介绍—2.2.3安全合规（基线自定义2）



自动生成正则表达式和检查代码，
对被检查设备批量自动执行规则
全网设备应查尽查

自动生成检查报告，
支持多种格式，pdf，html, excel, xml 等

2、产品介绍—2.2产品介绍—2.2.3安全合规（等保专项）

针对等保的物理安全，网络安全，主机安全，应用安全，管理安全等相关内容采用自动检查与人工访谈相结合的方式进行等保测评

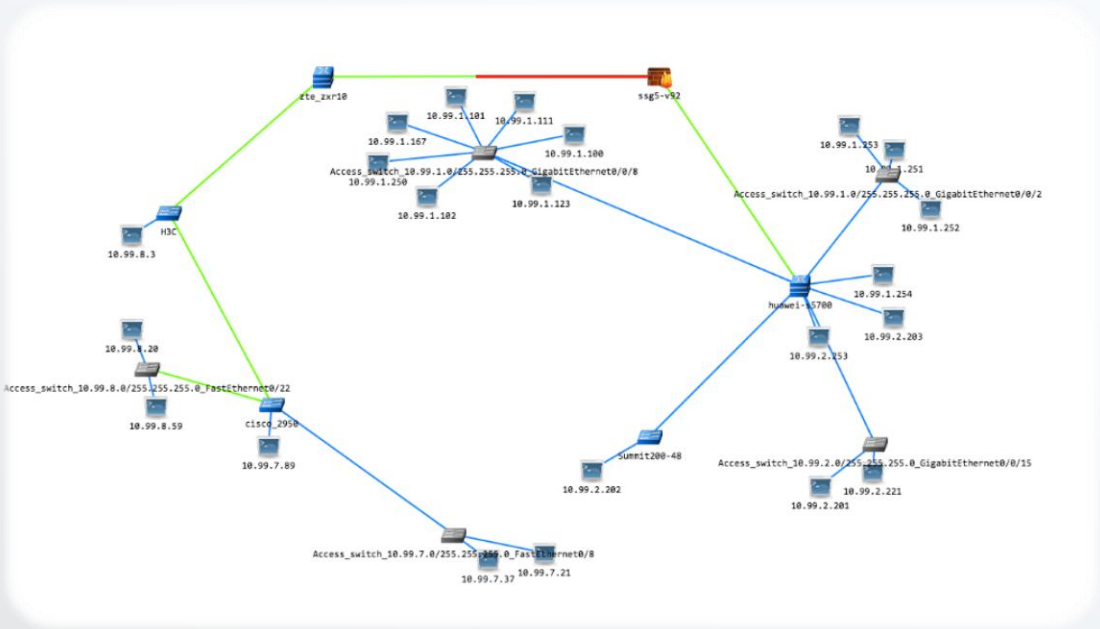
按需选择对应的等保级别进行检测，出具相应完整等保测评报告。

安全保护等级	信息系统定级结果的组合
第一级	S1A1G1
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4
第五级	S1A5G5，S2A5G5，S3A5G5，S4A5G5，S5A4G5，S5A3G5，S5A2G5，S5A1G5

2、产品介绍—2.2产品介绍—2.2.4安全服务（流量仿真）

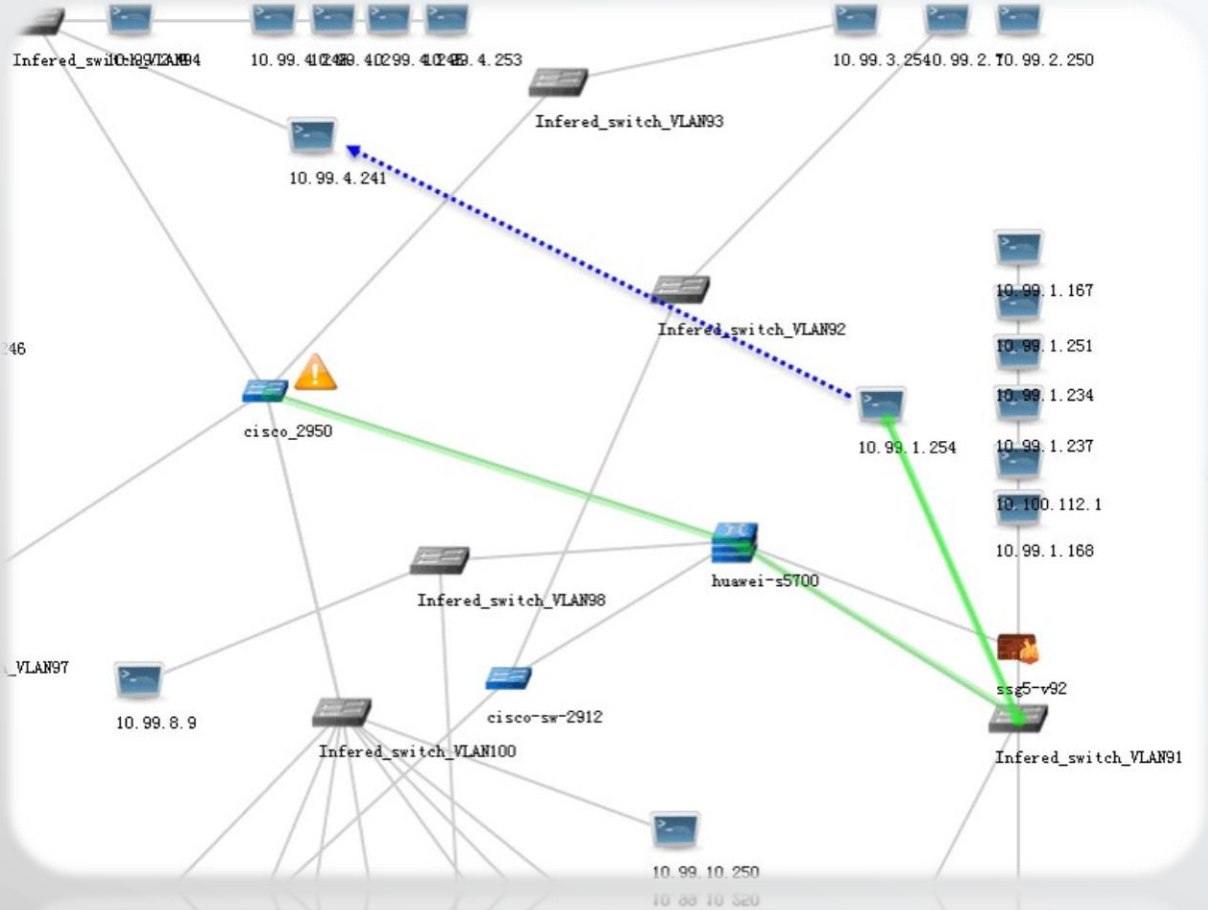
创建虚拟仿真流量（包括业务流和攻击流），部署到仿真环境中

流量播放器，显示不同时间网络的流量状况



显示业务流量和攻击流量对网络的影响：链路拥塞，节点故障

2、产品介绍—2.2产品介绍—2.2.4安全服务（路径仿真1）



A 流量路径可视化，ACL配置方案仿真校验

B 检查ACL访问控制的有效性，发现冗余ACL配置

C 提前发现ACL配置缺陷，提升抵抗入侵防御能力

2、产品介绍—2.2产品介绍—2.2.4安全服务（路径仿真2）

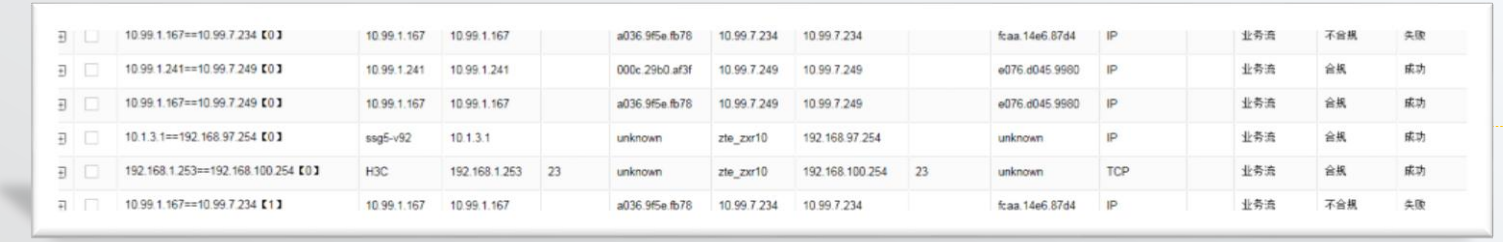
网络兵棋推演系统 CWG

Cyber War Gaming

- 全网推演
- 态势感知
- 威胁情报

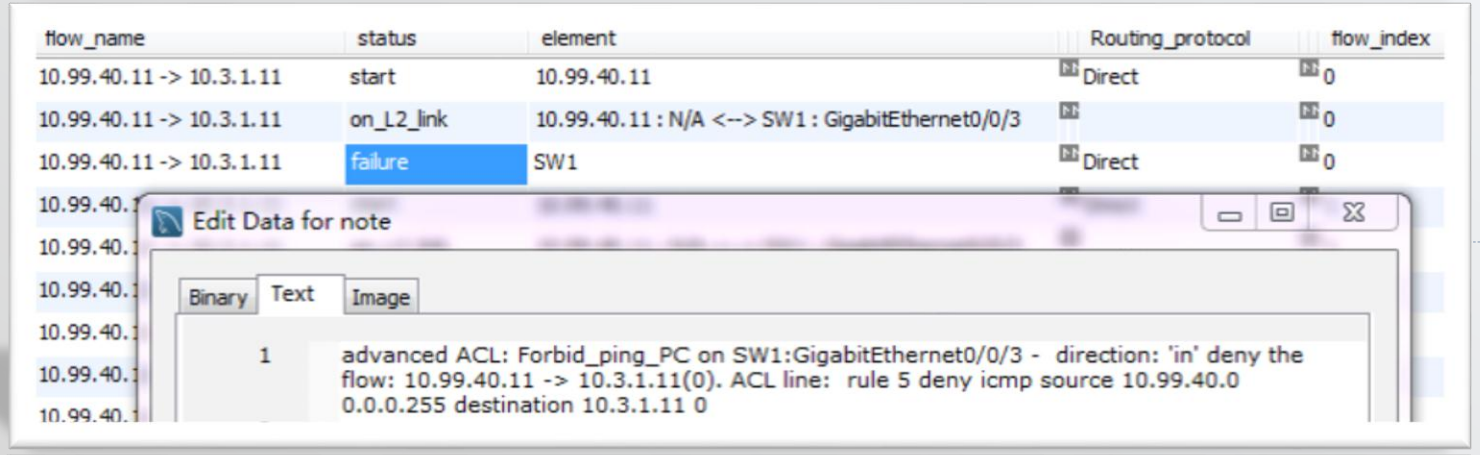
2、产品介绍—2.2产品介绍—2.2.4安全服务（攻击仿真1）

攻击路径仿真示例



10.99.1.167==10.99.7.234 【0】	10.99.1.167	10.99.1.167		a036.9f5e.fb78	10.99.7.234	10.99.7.234		fcaa.14e6.87d4	IP	业务流	不合规	失败
10.99.1.241==10.99.7.249 【0】	10.99.1.241	10.99.1.241		000c.29b0.af3f	10.99.7.249	10.99.7.249		e076.d045.9980	IP	业务流	合规	成功
10.99.1.167==10.99.7.249 【0】	10.99.1.167	10.99.1.167		a036.9f5e.fb78	10.99.7.249	10.99.7.249		e076.d045.9980	IP	业务流	合规	成功
10.1.3.1==192.168.97.254 【0】	ssg5-v92	10.1.3.1		unknown	zte_zxr10	192.168.97.254		unknown	IP	业务流	合规	成功
192.168.1.253==192.168.100.254 【0】	H3C	192.168.1.253	23	unknown	zte_zxr10	192.168.100.254	23	unknown	TCP	业务流	合规	成功
10.99.1.167==10.99.7.234 【1】	10.99.1.167	10.99.1.167		a036.9f5e.fb78	10.99.7.234	10.99.7.234		fcaa.14e6.87d4	IP	业务流	不合规	失败

01 创建一个新的攻击流



flow_name	status	element	Routing_protocol	flow_index
10.99.40.11 -> 10.3.1.11	start	10.99.40.11	Direct	0
10.99.40.11 -> 10.3.1.11	on_L2_link	10.99.40.11 : N/A <--> SW1 : GigabitEthernet0/0/3		0
10.99.40.11 -> 10.3.1.11	failure	SW1	Direct	0

Edit Data for note

Binary | Text | Image

1 advanced ACL: Forbid_ping_PC on SW1:GigabitEthernet0/0/3 - direction: 'in' deny the flow: 10.99.40.11 -> 10.3.1.11(0). ACL line: rule 5 deny icmp source 10.99.40.0 0.0.0.255 destination 10.3.1.11 0

02 攻击流的检查的结果

```
rule 5 permit ip source 10.99.40.0 0.0.0.255
rule 10 permit ip source 10.99.40.0 0.0.0.255 destination 10.3.1.0 0.0.0.255
acl name test1 3998
acl name Forbid_ping_PC 3999
rule 5 deny icmp source 10.99.40.0 0.0.0.255 destination 10.3.1.11 0
rule 10 permit tcp source 10.99.30.0 0.0.0.255 destination 10.3.1.11 0 destination-port eq 3389
rule 15 deny tcp destination 10.2.1.11 0 destination-port eq 3389
```

03 真实的ACL配置

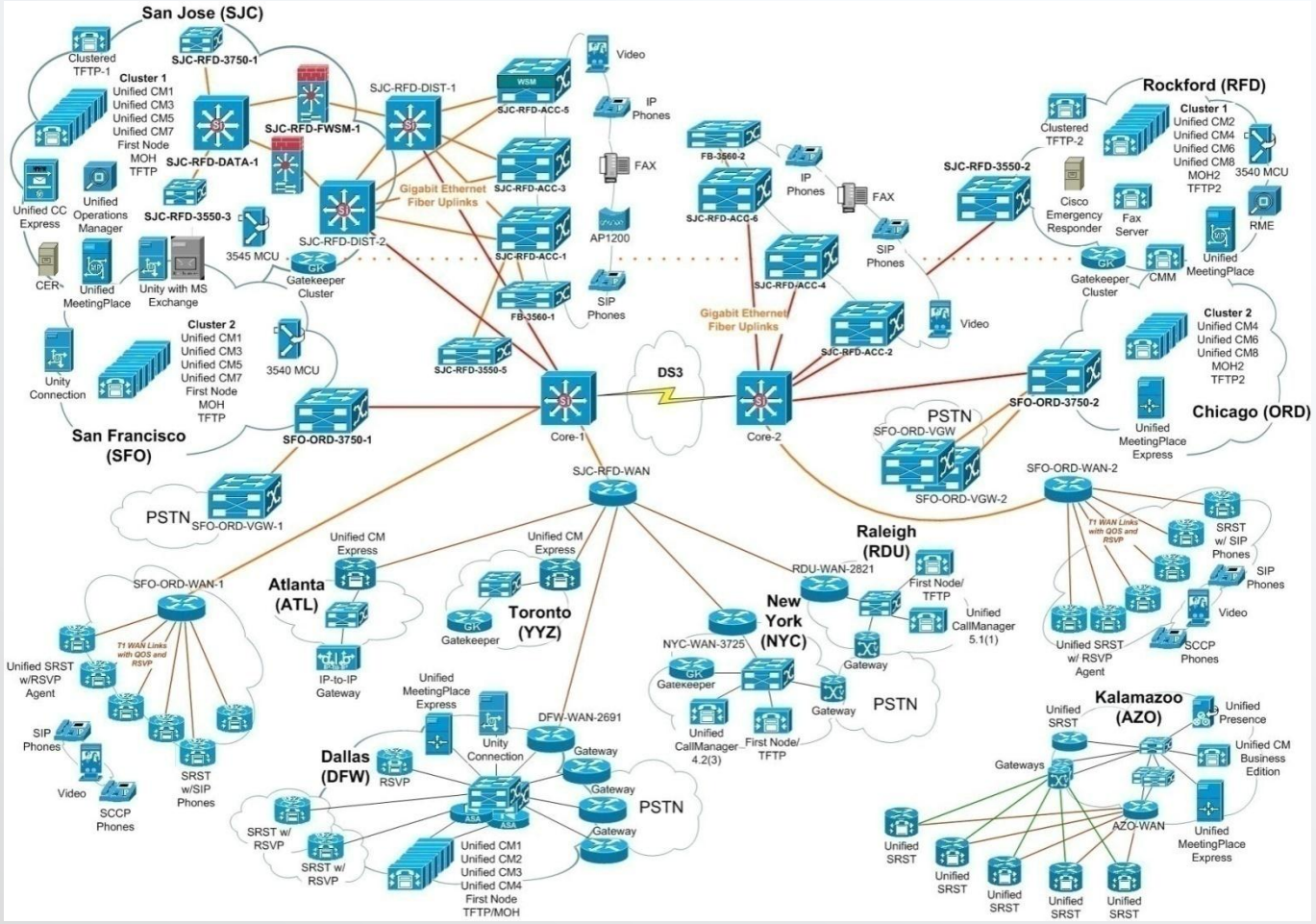
2、产品介绍—2.2产品介绍—2.2.4安全服务（攻击仿真2）

通过攻击仿真准确找出网络的脆弱点

中医讲“不治已病，治未病”

事前感知，提前发现隐患

由被动防御变主动防御



2、产品介绍—2.2产品介绍—2.2.4安全服务（应用仿真）

利用服务器后台模拟网络设备和应用系统进行网络情况仿真

- 安全的替用户进行应用仿真
- 快速的替用户进行故障的定位
- 虚实结合的仿真更具真实性
- 通过半实物仿真实现网络可视化
- 让网络变得更加直观和安全

3、优势及案例—3.1产品形态

手持终端（小型）

云平台（公安部、蓝云）

Saf-Nsmp1100（sc）机架服务器

运维服务

硬件环境	描述
冗余电源设计 FSP400-601UG	AC100-240VAC 6A,60-50Hz
中央处理器/E3-1231V3	英特尔至强4核线程 3.4GHz
散热器/	AVC
内存/SOD	8G
硬盘/SSD	SSD 固态 256G（RAID）

3、优势及案例—3.2产品特点

	网络安全管理中心	传统工具
全网自动侦测和设备发现	全网自动快速侦测网络资产，包括主机、网络和安全设备，全面了解网络资产和网络边界	人工采集已知的网络设备
自动构建网络拓扑	根据采集的网络信息自动还原拓扑结构	人工绘制网络拓扑图
配置检查	对采集的网络信息进行虚拟建模+海量规则库进行全面检查	文本对比
规则覆盖范围	单机和联网规则	单机规则
风险报告和整改建议	自动快速生成详细的风险报告和给出权威的整改建议	无
自动修复技术	能够对部分网络设备问题进行人工审核后的自动修复	无
攻防仿真	能够对网络的访问控制进行有效性检验，自动推算出数据包经过的路径和受到的访问控制	无

3、优势及案例—3.3覆盖厂商

“Cyber Cube 网络安全仿真管理平台”，支持多样化网络及安全设备，包括主流设备思科全系列，华为全系列，H3C全网络等设备体系，未来将适配更多网络及安全设备。

3、优势及案例—3.4案例分享一

背景

2007年6月22日，公安部、国家保密局、国家密码管理局、国务院信息工作办公室，联合发布公通字[2007]43号文《信息安全等级保护管理办法》

2014-02-27中央网络安全和信息化领导小组成立，组长习近平。网络安全已经提到国家安全层面。

解决方案

- 网络自动侦测功能，清晰化网络边界，为风险评估提供必要的环境准备。
- 建立完整的等保网络安全评估规则库，并实现自动化工具执行，大大提高检查效率、效果。
- 提供完整详尽的检查报告，为网络安全加固、调优提供专业化技术支撑
- 利用离线检查技术，实现对网络非接触式无损检查方法，首次实现了网络的安全检查。

面临挑战

- 缺乏有效工具无法做到应查尽查
- 设备型号众多，检查难度高
- 网络边界模糊，风险评估难度较高
- 缺乏安全的检查手段

客户评语

随方的产品，为我们进行等保备案用户的网络安全检查提供了很大的支持

3、优势及案例—3.4案例分享二

背景

云计算风起云涌，仅中国的公有云IaaS市场从2009年到2014年的增长率一直保持在50%以上

由于成本的革命性降低以及使用维护的便捷，SaaS模式的软件目前成为软件产业的核心力量，是软件业态发展的必然趋势。

解决方案

- 离线体检技术，实现了网络检查的O2O模式
- 提供完整详尽的检查报告，为网络安全加固、调优提供专业化技术支撑
- 大量完整的规则库，满足了企业安全防护的需要
- 方便便捷的应用，为企业尤其是中小企业，节省了大量的人力、物力
- 自动化实现，弥补了技术不足的难题
- 一键自动修复功能，使网络安全加固和优化不再是专业的技术问题

面临挑战

- 中小企业人员、资金不足
- 中小企业技术能力不足
- 云安全将成为安全发展的趋势

客户评语

云化是目前信息化发展的大趋势，随着Saas服务的大量普及，基础架构层面网络安全成为云应用的基础性依托。安全云化，是我们面临的新的课题和挑战。随方的产品在这个方面做出了有益的尝试，为我们提供了良好的技术支撑。让我们在这个方面迈出了坚实的一步。

safein 随方信息
网络安全 尽在掌握

谢谢观赏

BUSINESS
POWERPOINT

THANKS

北京随方信息技术有限公司