

LanSecS[®]

网络边界完整性检查管理系统

LanSecS[®] 网络边界完整性检查管理系统

产品背景

- ▶ 网络内部私接无线Wifi设备,大大扩展及破坏了内网的网络边界;
- ▶ Wifi安全性较差,很容易遭受攻击和破解;
- ▶ 受使用者安全意识及技术水平的限制,Wifi设备自身的安全防护能力较差;
- ▶ 随Wifi接入的手机、PAD等设备,自身应用多而繁杂,安全性差,安全隐患大,安全风险难以管控。



- ▶ 管理者缺乏技术手段,难于发现无线Wifi等设备私接,无法实施有效监管;
- ▶ 随身Wifi、无线AP便携小巧,接入方式隐蔽而灵活;
- ▶ 存在HUB接入的网络,难于区分清楚是合法的普通HUB还是违规的无线AP;
- ▶ 通过NAT或NAT+MAC地址克隆方式接入的路由类设备,欺骗和隐蔽性更高。

“以前边界安全检查主要是防非法外联,防一机两用,非法外联会给边界开个后门,捅个窟窿,危害很大;现在发现通过无线wifi私接手机、PAD入网,同样会给边界捅个更大的窟窿,现在人手一部手机,私接入网的概率很高,危害可能更大,在用这套系统之前,我们一直没有合适的技术手段去发现去解决它。”

-----某市信息中心主任

“在边界完整性检查方面,等保有很具体的要求,既对非法外联有要求,又对违规内联有要求,我们测评时也主要考察用户单位有没有上非法外联的技术手段,有没有上网络准入的控制手段,但用户上了这些手段后的效果如何,我们没有专业工具进行评估,我们准备把这套系统作为我们的测评工具来用。”

-----某市局网监处

所谓的边界,在LanSecS网络边界完整性检查系列产品中,是指政府、企业或组织定义的合法的终端范围;而边检,则是对既定的网络或终端范围做边界完整性检查,主要针对是否有私接AP、私接路由器、私接随身Wifi等把边界扩展到移动设备(手机、平板电脑)上的行为;这种检查可以是上级主管部门检查,也可以是自查。

▶ 产品概述

LanSecS网络边界完整性检查系统是圣博润结合在等保检查工作中的多年技术积累和丰富的实践经验,并结合全民便携时代政府及企业在边界完整性检查方面的具体要求而推出的,是集私接AP、随身Wifi等违规内联行为检测、定位与阻断控制能力于一体的边界完整性检查及管理产品,可帮助监管者快速评估现有网络在网络边界完整性保护方面是否存在漏洞,降低由此引发的安全风险。



▶ 产品功能

1 快速检测无线路由设备（无线AP）、随身Wifi及软件Wifi的违规接入

系统通过网络扫描的方式可快速检测内网中接入的无线路由设备(无线AP)、随身Wifi及软件Wifi分享接入行为。

无线接入设备由原先的无线路由器到随身USB无线Wifi接入设备到免费的Wifi分享软件,提供便捷的Wifi接入,同时也给内网边界及内网安全带来了安全隐患。

2 快速定位、隔离网络中破坏网络边界的行为

无须改变现有网络拓扑,无须客户端代理,通过与交换机互动,来完成对破坏网络边界的行为快速定位,并可根据预定策略实现对破坏网络边界行为的自动阻断控制,响应时间大大缩短,将损失降到最低。

3 提供针对违规IP的完整回溯能力

详细记录内网中每一MAC地址使用不同IP地址的对应时段,记录每一MAC地址在网络设备的接入点及接入时段,可跟踪及还原每一终端PC在网络内部的IP地址使用轨迹和内部接入轨迹,保证系统能够根据其他安全设备提供的违规IP地址或MAC地址,追踪及还原其在网络内部的原始定位。

4 快速检测基于NAT接入的路由类设备

系统可快速检测基于NAT模式工作并接入的路由类设备。路由类设备(包括无线路由)提供的NAT(地址转换)接入模式,最大的特点就是部署简单、方便,不受已有网络IP段规划的限制,是扩充私网的理想模式,对监管者而言,只能监

测到NAT后的合法IP,而NAT之前的私接网络是不受监管的,最难于监管是MAC克隆结合NAT接入的路由设备,可以轻松突破用户已有的安全接入控制措施(如交换机端口绑定)。

5 多种拓扑展示与管理模式

系统支持IP拓扑及位置拓扑等多种拓扑展示方式;支持自动区分级联口和HUB接入端口;支持自动发现及自动绘制网络拓扑;支持人工调整网络拓扑;支持基于拓扑的可视化操作管理。

6 网络设备端口的统一安全监管

提供对网络交换设备端口的统一安全监管,自动识别设备端口是否进行了安全绑定,对设备长期不使用的闲置端口进行自动统计,并可根据策略要求自动关闭闲置端口,防止非授权接入。

▶ 产品特色

- ▶ 国内首款专业网络边界完整性检查系统,既可作为检查工具提供,又可常态化部署于用户内网以7*24小时保证边界完整。
- ▶ 基于网络扫描,旁路部署,无需客户端,支持大型网络分级部署,集中管理。
- ▶ 提供B/S管理方式,支持HTTPS,提供用户分权控制。
- ▶ 可提供检查工具版本,用于上级主管部门检查或自查,或

用于安全测评。

▶ 产品性能及兼容性

- ▶ 部署环境:基于Windows操作系统, CPU 2.4G四核及以上, 内存4G及以上。
- ▶ 网络环境:扫描峰值带宽占用小于3M。
- ▶ 网络规模:单系统可扫描范围8000点。
- ▶ 交换设备兼容: Cisco、H3C、华为、锐捷、3Com、HP、北电、迈普等;支持与Cisco、华为、华三及锐捷等主流厂商AC的联动。
- ▶ 随身Wifi兼容: 360WIFI、小米WIFI、小度WIFI、Fast WIFI、Mercury WIFI等。
- ▶ 无线AP兼容: TP-Link、D-Link、FAST、Mercury、Tenda、奇虎360、华为、Netgear等。

▶ 产品资质

公安部颁发的销售许可证



 **北京圣博润高新技术股份有限公司**
BEIJING SBR HIGH-TECH CO.,LTD

地址: 北京市海淀区高梁桥斜街59号院2号楼3层 / 邮编: 100044 / 电话: 010-82138088 / 技术支持热线:
8008102332/4009662332 / 技术支持邮箱: support@sbr-info.com / 网址: www.sbr-info.com