绿盟物联网准入网关

技术白皮书

■ 文档编号		■ 密级	内部公开
■ 版本编号	V1.1	■ 日期	2019.04

■ **版本变更记录**

时间	版本	说明	修改人
2018-11	V1.0	新增	
2019-04	V1.1	修改部分技术细节	刘军 4

■ **适用性声明**

本模板用于撰写绿盟科技内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

一. 产品概述

随着企业向数字化业务的发展，物联网技术和商业模式也以惊人的速度发展。当前物联网应用遍布在智慧家居，智慧大厦，智慧能源，智慧交通，智慧城市等行业。物联网感知设备数量巨大，分布广泛，存在漏洞极易被黑客利用。

2015 年，国内知名视频设备厂商，被江苏省公安厅通报，部分设备已被境外 IP 地址控制，需要对该品牌设备进行全面清查；2016 年 Mirai 蠕虫感染摄像头造成美国域名管理服务器供应商遭受攻击，导致大量网站宕机，数小时才陆续恢复；2017 年 WannaCry 蠕虫通过 MS17-010 漏洞在全球范围大爆发，感染的计算机被植入敲诈者病毒，导致文件被加密，病毒会提示支付价值相当于 300 美元的比特币才可解锁，事件波及上百个国家。

绿盟科技根据多年的研究，设计的物联网准入网关切实考虑了物联网的网络架构特征，无需改变原有网络架构，不需安装任何代理，采用双引擎的工作方式，通过高效协同工作实现单向获取数据和发送控制指令，即实现了有效管理又保证了相对封闭和隔离。绿盟物联网准入网关以行为分析为基础，以先进的数理模型自动建立网络访问关系白名单，帮助用户全面了解网络内发生的行为，将非法的行为提取出来；采用行为分析识别攻击活动，使攻击者无法隐藏自己；能够对全网众多的物联网设备进行发现、管理和监控；更可以通过地址分析、行为分析和漏洞扫描发现异常活动，阻断异常设备；计算全网的安全风险指标，控制安全风险。

绿盟物联网准入网关从资产管理、运行监测、安全控制三个维度出发，集设备自动发现、漏洞自动探知、接入自动甄别、行为自动分析、违规自动阻断等多种安全功能于一身,从边界到行为再到核心数据,逐步深入,形成立体监控,建立纵深防御,在加强安全运行管理同时,将用户从繁重的日常事务中解放出来,轻松实现资产一目了然、设备故障实时报警、安全风险实时掌控、非法入侵及时阻断等功能,全方位解决物联网安全运行问题。

图 1.1 物联网概述

二. 技术架构

物联网准入网关主要分为网络行为分析和阻断、设备自动发现和监控、设备入网和准入、三大核心功能。

- 网络行为分析和阻断功能通过数据采集、统计设备流量，自动识别网络中的正常业务的行为、异常的行为及未知的可疑行为，识别产生异常行为的设备并进行告警。
- 设备自动发现和监控功能通过主动探测自动发现网内设备，识别设备类型、品牌、型号、进行 IP/MAC 地址绑定，监控设备流量和行为异常设备，监测设备离线、类型变更、地址冲突。
- 设备入网和准入通过注册登记流程，对物联网设备进行准入控制，发现非法接入设备并进行阻断，防止恶意接入网内导致数据泄露。

三. 功能介绍

3.1 设备和入网管理

3.1.1 设备识别

设备识别是物联网安全管理的基础，因此系统需支持强大的设备识别能力。系统支持设备主动发现功能，发现过程不需在原有设备中安装任何程序，发现过程不对网络造成影响；能够获取物联网中在网设备的 IP 和 MAC 地址、品牌、型号、发现时间等信息；支持弱密码风险的自动识别。

系统支持多种识别方式，系统提供丰富识别规则，支持根据预定义规则的组合发现设备的信息；支持结果指纹识别；支持使用预定义 python 或 lua 脚本对设备的发现，可以灵活的定义设备发现方法。

3.1.2 设备流量

物联网中设备流量的异常会影响物联网业务的正常开展，对设备的流量进行统计分析从中发现问题所在十分必要。系统通过旁路抓包方式实现对所有在网设备进行上下行流量、上下行流量包、发现时间的实时监控。

3.1.3 地址冲突

物联网设备量大、分布广泛，同时又属于多人管理，信息上的不同步使得管理人员在使用 IP 地址时极易产生混乱，从而导致 ip-mac 地址冲突事件的发生，系统通过支持自动检查设备的 IP 地址、MAC 地址冲突及时发现问题并报警，提醒管理人员进行相关处置。

因此，要求系统支持自动检查设备的 IP 地址、MAC 地址冲突；支持地址冲突设备列表展示，列表信息 至少包括 IP 地址、MAC 地址、设备类型、地址组、管理员、冲突 MAC、冲突设备类型、状态等。

3.1.4 设备异常

物联网通过设备准入管理仅能实现最基本的安全控制，黑客通过特殊技术较容易“凿穿”准入措施接入物联网，因此需要通过设备的网络行为异常作为补充，完善安全控制机制；系统通过旁路分析自动识别网络行为，根据行为的特点自动判断网络行为是否为异常行为并产生报警，实现设备异常监控。

系统支持根据异常行为自动产生设备异常报警；设备异常状态分为异常和分析中，支持相关异常和分析中数量显示，分别用不同颜色进行报警，点击能弹出与该设备有关的异常对话框；支持设备异常列表。

3.1.5 设备离线

物联网设备物理上分布广泛，发生故障而产生离线时很难通过巡检及时发现问题，因此需要对设备在线状态进行实时检测及时发现故障点。系统通过主动探测技术，以设备识别为基础，实时检测所有在网设备的在线状态，支持产生设备离线报警。

因此，要求系统支持对设备状态进行实时检测，并将离线设备记录为离线状态；支持离线设备列表，列表信息至少包括 IP 地址、MAC 地址、设备类型、地址组、管理员、最近离线时间、恢复时间、离线时间、状态等。

3.1.6 设备漏洞

物联网由于前端设备数量庞大，维护人员在进行管理时为了方便常使用弱密码对同一类型设备进行管理，这无形中增加了物联网的安全隐患。系统通过主动探测技术，以设备识别为基础，自动探测在网设备、特别是前端设备的弱口令，及时产生设备风险报警。

3.1.7 IP 地址管理

前端设备作为物联网组成部分，基数庞大，采用静态 IP 地址接入方式，更好的 IP 地址管理非常必要，系统支持 IP 地址自动管理，实现 IP 地址自动统计、自动回收，支持已用 ip、可用 ip、ip 设备类型等详细化管理。

要求拥有仿冒终端智能识别功能，对于非法仿冒前端设备 IP/MAC 的终端，通过多级指纹判断，自动告警、定位并阻断。

3.1.8 设备入网登记注册

系统识别的终端信息可编辑，可对物联网设备、网络设备、终端等设备进行注册、登记（包括 MAC 地址、物理位置、IP 地址、型号、厂商等）。确保物联网所有 IP 设备的规范化管理，统一注册、统一审批，落实责任人。

3.2 非法行为监控阻断

3.2.1 流异常活动

物联网通过设备准入管理仅能实现最基本的安全控制，黑客通过特殊技术较容易“凿穿”准入措施接入物联网，因此需要通过设备的网络行为异常作为补充，完善安全控制机制。

因此，要求系统支持通过行为分析自动识别物联网中的异常行为，并记录为异常活动；支持异常活动报警列表，列表信息至少包括策略名称、级别、协议类型、源地址、源端口、目的地址、目的 端口、字节数、包数、报警时间、payload 等；支持查看异常活动报警的 payload 信息；支持通过 协议、源 IP、源端口、目的 IP、目的端口、时间查询异常活动报警。

3.2.2 网络行为审计

要求系统支持通过行为分析自动识别并归纳物联网中的访问服务器、协议扫描、端口扫描、常用协议、一对一访问等网络行为；支持网络行为列表，列表信息至少包括策略名称、协议、源地址、源端口、目的地址、目的端口等。

3.3 集中管理多级部署

3.3.1 总体安全状态监控

物联网准入网关支持监控主视图，在监控主视图上集中展示主要监控指标、态势曲线及重要的报警信息；支持总体安全指标显示，安全指标计算包含待准入设备、离线设备、地址冲突设备、异常活动设备、弱口令设备等因素；支持部署资产台数、在线率、已运行天数显示。

3.3.2 多级分布式部署

物联网准入网关支持集中式管理和多级部署，支持上下级之间的控制指令下发和设备、报警信息上报；支持监控主视图，在监控主视图上集中展示主要监控指标、态势曲线及重要的报警信息；支持接受上级阻断命令、接受上级控制指令。

四. 关键技术

4.1 超高速设备探测和发现

物联网准入网关为了提高内网设备探知速度，采用了无连接探测技术，绕开 tcp/ip 栈进行探测，能够以最快的速度完成对网络内设备分布的探知。

图 4.1 设备探测发现流程

4.2 发现未知的攻击行为

物联网准入网关以网络行为安全分析为基础，自动把网络中的正常系统访问行为识别为白名单，只要发生网络攻击行为，无论攻击者采用何种攻击方法，难免要在网内进行探测、攻击、传输、下载等活动，这些攻击活动在行为白名单的过滤下将自动浮出水面，迅速暴露出来。

4.3 智能联动阻断异常设备

物联网准入网关支持非备案设备、异常设备自动阻断，实时将非法设备“拒之门外”，有效防止非法接入风险。

4.4 旁路流量监控

物联网准入网关使用探测引擎检测网络中的物联网设备，通过设备指纹特征精确识别设备类型，覆盖主流的摄像头、NVR、CVR、DVR、视频网关、流媒体服务器、门禁卡、打印机等物联网设备。

物联网准入网关使用旁路的分析引擎监测并分析网络中数据流量，监控网络行为关系。

五. 产品部署

物联网准入网关部署不需要改变已有网络结构，不用在网络内串接设备，不用在系统上安装代理，可以很方便的完成部署，无论逻辑上还是物理上都采用旁路工作模式，彻底杜绝单点故障。

物联网准入网关典型部署模式如下：

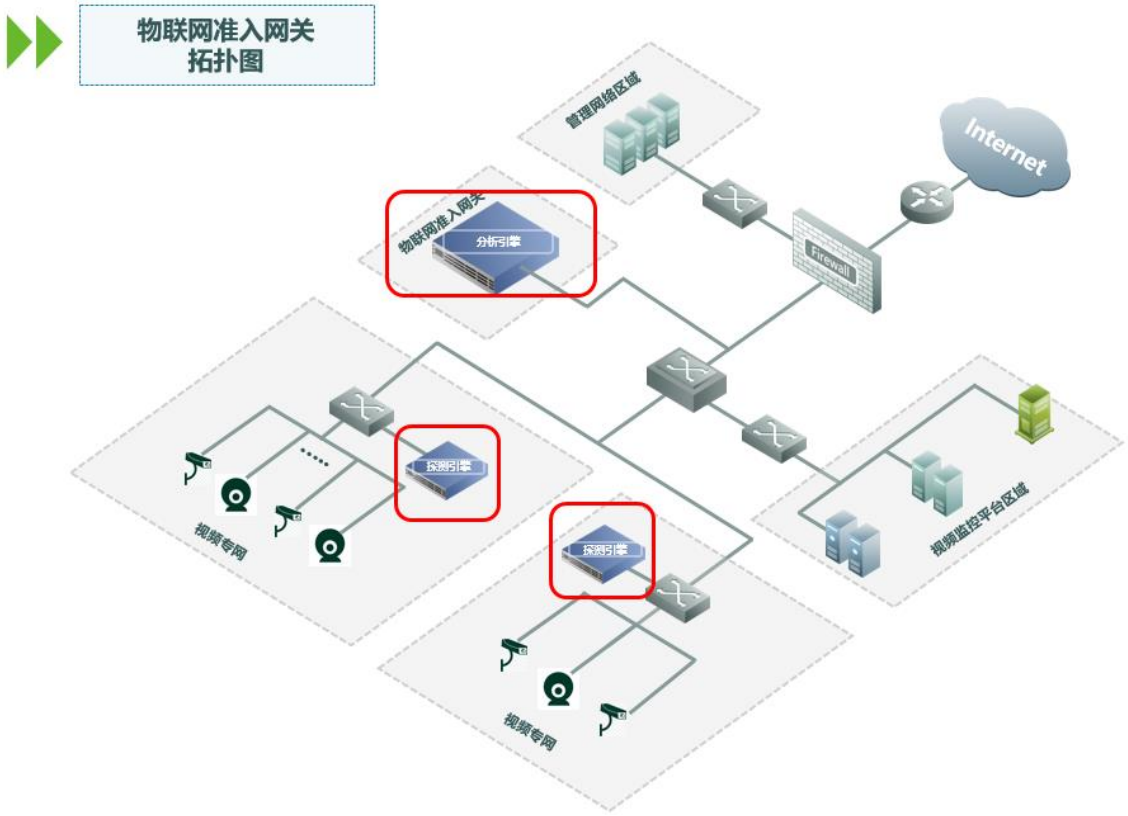

图 5.1 产品部署图

六. 产品优势

6.1 方案合规，产品可信

物联网准入网关通过公安三所针对产品安全功能的针对性测试，并具备公安部颁发的《安全专用产品销售许可证》等安全证书，为用户构建一张安全合规的网络。

6.2 多个层面，全面防护

物联网准入网关通过设备资产管控、网络行为管控、应用管控三个层面实现安全控制，只有通过认证的 IP、MAC 地址，并且网络行为符合物联网业务需求，所使用的应用符合物联网应用的行为才能放行，其他 IP、MAC 地址和流量全部阻断。

6.3 功能实现，针对性强

物联网准入网关内置了主流物联网设备资产特性及网络协议，用户部署后即可实现监测和报警功能。系统功能实现从可视化监测、资产管理、运行监测、安全控制等多方面入手，全面解决物联网资产管理、设备故障、非法入侵等问题，帮助用户全方位解决物联网安全运行问题，实现物联网可知、可控、可管理。

6.4 可视管理，精确定位

物联网准入网关支持支持网内设备、违规报警、异常设备、未知连接数量等运行指标可视化展示，支持白名单 top5、设备流量 top5、协议流量 top5 等流量指标可视化展示，支持网络行为、异常设备的集中图形化展示，让用户从全局的角度去掌控网络状况。

6.5 部署简单，无单点故障

物联网准入网关的部署不需要改变已有网络结构，不用在网络内串接设备，不用在系统上安装代理，可以很方便的完成部署，无论逻辑上还是物理上都采用旁路工作模式，彻底杜绝单点故障。