



# 物联网防火墙

---

## 产品白皮书

本档为深圳市九方智联科技公司所有，未经所有者书面许可，不得以任何形式进行复制和传播

# 目录

1. 前言.....	2
2. 物联网防火墙.....	4
2.1 产品概述.....	4
2.2 功能架构.....	5
2.3 主要功能.....	5
2.3.1 基础网络功能.....	5
2.3.2 传统防火墙功能.....	6
2.3.3 VPN 远程互联.....	6
2.3.4 认证与鉴权.....	6
2.3.5 智能流量管理.....	7
2.3.6 基于深度识别的入侵防御.....	7
2.3.7 协议深度解析.....	7
2.3.8 实时网络拓扑图.....	7
2.3.9 流量可视化.....	8
2.3.10 攻击溯源.....	9
2.4 技术优势.....	9
2.4.1 区域安全隔离.....	9
2.4.2 深度数据包解析引擎.....	9
2.4.3 全方位可视化.....	10
2.4.4 集中管控平台.....	10
2.4.5 数字证书认证.....	10
2.4.6 完善的事件日志审计.....	11
3. 客户价值.....	12
3.1 全面的威胁防御能力，保障生产有序进行.....	12
3.2 更少的成本，更高的性能.....	12
3.3 可视化管理、轻松运维.....	12
3.4 政策合规、满足监管.....	12
4. 关于我们.....	13
4.1 公司介绍.....	13
4.2 公司目标.....	13

# 1. 前言

伴随着互联网+、工业 4.0、工业物联网 (IIoT)、人工智能物联网 (AIoT) 等概念的提出与泛化，驱动了物联网市场以及传统工业领域的飞速发展。据《中国互联网发展报告 (2021)》统计，2020 年的物联网市场规模就已高达 1.7 万亿。如此大的市场规模已经成为行业界不得不重视的关键领域。物联网作为一种传统网络的扩展与延伸，融入了更多、更大、更广的产品体系，从日常生活中的无线路由器、网络电视、智能家居到公司企业中的交换机、路由器、扫描仪、打印机、门禁、投影仪、IP 摄像头、公共广播等，基本是无处不在，涉及到我们工作生活的方方面面。物联网在带来便利的同时，也因为其固有的特点和特定的场景带来了各种不确定的安全风险。多方面的因素导致了物联网已经逐步成为网络信息安全“重灾区”，其中既有物联网技术本身技术特点逐步累积形成的特性，也有新兴行业在高速发展过程中存在的通病。而在产业高速发展、规模急剧扩张的背后，是物联网厂商安全意识淡薄，安全投入不足的现状。

通过对以上问题的深入分析，当前物联网设备以及传统工控类设备安全问题已经迫在眉睫，传统防火墙对物联网协议以及工控协议的解析和有效防护已经很难满足安全的需求，市场迫切需要有更符合物联网安全要求的产品来进行安全防护，全新的物联网防火墙应具备以下基本功能来应对威胁的进化：

1. 标准的基本防火墙能力：包过滤、网络地址转换(NAT)、状态检测、传统协议分析等等。

2. 应用的洞察与控制：识别应用和在应用层上执行独立于端口和协议，具备多种物联网协议、工控网络协议、工业以太网协议的检查、过滤、报警和阻断功能。

3. 网络入侵防御：具备基于漏洞库的入侵防御功能和基于机器智能学习引擎的主动防御功能。
4. 深度数据包解析功能：拥有智能学习引擎、深度数据包解析引擎和开放式特征匹配引擎三大功能引擎。
5. 数据加密传输功能：支持数字证书认证，集成 VPN 智能互联技术，动态更新会话密钥，保障远程数据传输安全。
6. 集中管控功能：支持平台集中管理、远程维护、实时监控及大规模分布式网络统一部署及更新。

## 2. 物联网防火墙

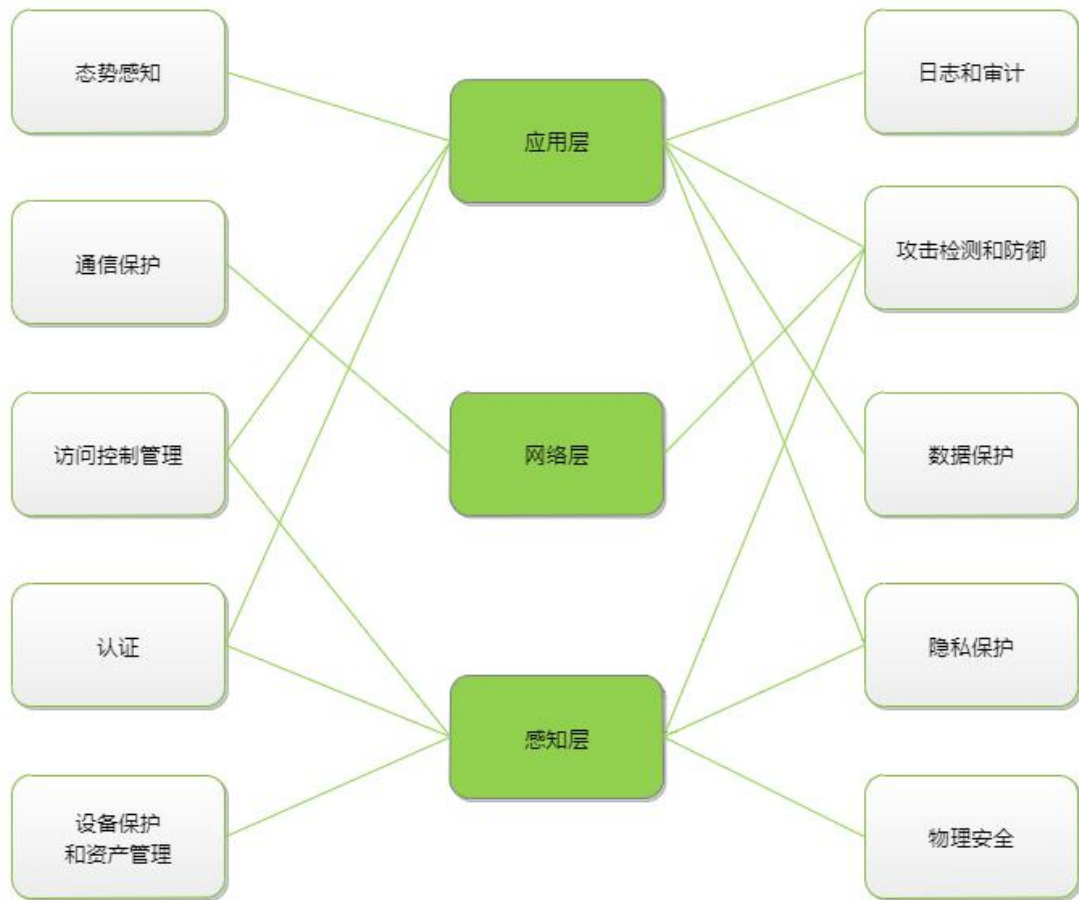
### 2.1 产品概述

九方智联物联网防火墙是深圳市九方智联科技有限公司在网络安全行业多年的技术、经验积累的基础上，专门为政府、教育、金融、能源、广电、军队、大小型企业精心打造的一款高性能防火墙产品。

九方智联物联网防火墙可以灵活部署在各种复杂的网络应用环境的边界，提供既包括传统防火墙产品的状态检测、NAPT、VPN、流量控制、应用识别、用户认证等综合安全功能外，也具备对 IOT 设备以及工业联网设备的特殊防控功能，例如工业漏洞防护，物联网协议、工控网络协议、工业以太网协议的检查、过滤、报警和阻断等，并拥有智能学习引擎、深度数据包解析引擎和开放式特征匹配引擎三大功能引擎，全方位多角度保障防护区域内的网络信息安全。

九方智联物联网防火墙采用了高性能、高稳定性的多核硬件架构，接口支持拓展，为用户提供高效、稳定、可拓展的安全保障。

## 2.2 功能架构



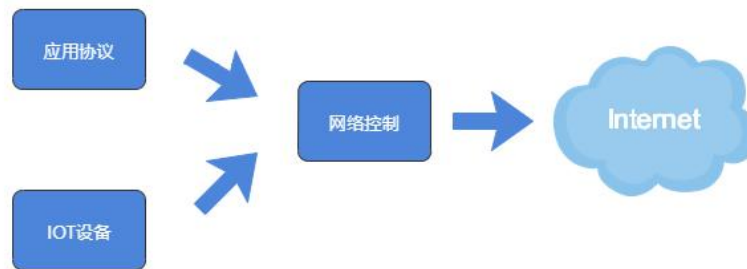
## 2.3 主要功能

### 2.3.1 基础网络功能

支持静态 IP, PPPOE 以及 DHCP 的联网方式、支持静态路由、策略路由、多播路由的转发、支持动态路由协议 (RIP、OSPF)、支持 PPPOE 服务器、支持 DHCP 以及多链路负载均衡及带宽叠加功能。

### 2.3.2 传统防火墙功能

支持自定义安全区、状态检测和支持基于七元组（源 MAC/目的 MAC/源 IP/目的 IP/源端口/目的端口/传输层协议类型）及时间段的安全策略控制功能，支持会话策略、智能流控策略以及策略优先级调整，支持对多种常见的 DDOS 攻击和扫描攻击检测和防护，支持 NAT 功能，对源地址和目的地址及端口进行转换。



### 2.3.3 VPN 远程互联

除了支持 PPTP、L2TP、IPSEC 和 SSLVPN 等通用 VPN 协议外，我们更拥有独创的智联通以及智联客户端隧道技术，其针对 VPN 隧道内的应用连接进行优化，实现单边加速，并且能动态更新会话密钥，保障 VPN 隧道流量的安全高效传输。

### 2.3.4 认证与鉴权

支持 IP/MAC 绑定识别技术；能主动发现网络中的各种设备，并支持用户名+密码的上网认证功能；并能与 RADIUS、LDAP、AD、POP3、TACACS+ 等认证服务器进行单点登录联动，通过身份识别技术，帮助管理人员准确识别网络访问者。

### 2.3.5 智能流量管理

通过基于人员、设备和应用的识别，物联网防火墙可以帮助管理员实现灵活的带宽分配策略。可以将物理线路分为三级虚拟通道，为每个虚拟通道分配动态的带宽，并能依据通道内设备在线情况对共享带宽进行动态调整。并通过保证带宽的分配保障核心应用的基础带宽，避免出现网络拥塞。

### 2.3.6 基于深度识别的入侵防御

基于的深度识别的入侵检测技术解决了基于端口的入侵防御对端口逃逸应用的入侵检测失效性，同时提供漏洞、木马、蠕虫、后门、缓冲区溢出、扫描和 SQL 注入等多种攻击或威胁方式的检测和防御，并能远程动态更新漏洞特征库。

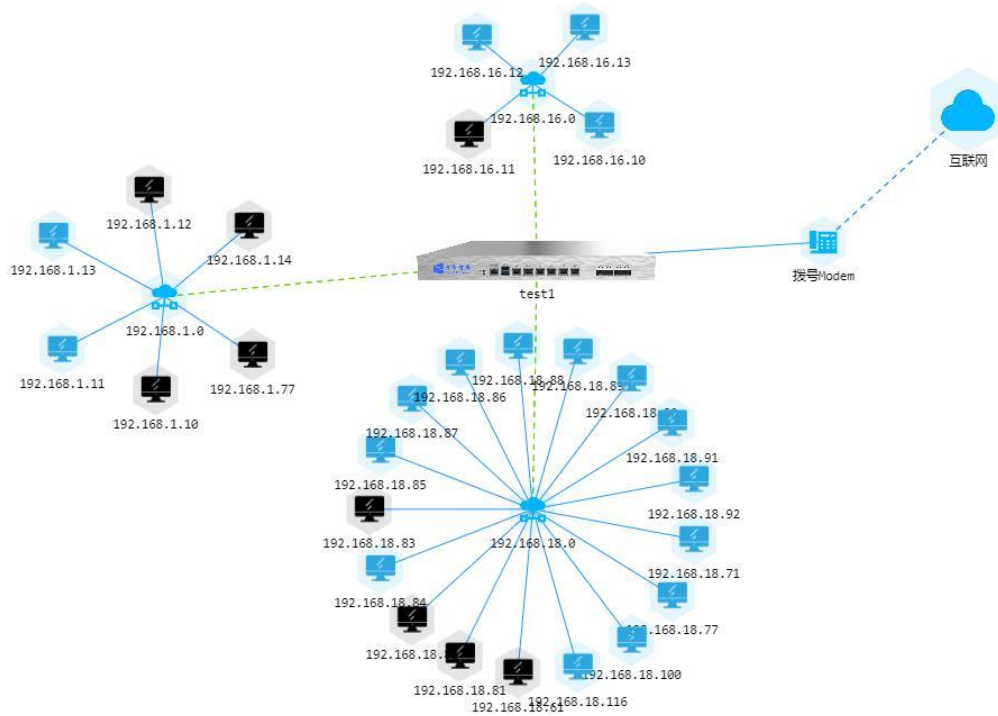
### 2.3.7 协议深度解析

支持 smb、ftp、bacnet、beckoff、cip、dnp3、enip、fox、hart\_ip、IEC61850、modbus、modicon、omron、opc、s7、profinet 等众多工控协议，报文深度解析粒度可达值域级，支持报文格式检查、功能码控制、动态端口识别、寄存器控制，连接状态控制等的检测。

### 2.3.8 实时网络拓扑图

实时展现已接入网络的产品设备，并能对设备进行自动统一布局，动态学习新接入设备，实时监测网络，并能对网络中设备的变更进行实时预警。





## 2.3.9 流量可视化

监测各个网络接口的上下行实时流量，支持实时展现所有通过防火墙的数据流量，对各设备历史流量依据时间进行统计、分析、排序，展示设备和协议占比的 TOP10，并能对设备的异常流量进行一键屏蔽。

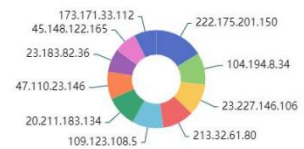


## 2.3.10 攻击溯源

监测各类网络攻击事件，对攻击信息依据国家和 IP 地址进行统计风险，并可视化展现出最新的攻击事件。



基于国家攻击次数TOP10



基于IP攻击次数TOP10

## 2.4 技术优势

### 2.4.1 区域安全隔离

可适应于各种复杂的网络拓扑环境，物联网防火墙可以根据实际网络情况进行自定义区域划分，对每个区域进行数据保护，做到横向隔离，纵向保护的安全数据过滤隔离。通过访问控制实现网络的结构安全性，满足实际应用需求。

### 2.4.2 深度数据包解析引擎

具备智能学习引擎、深度数据包解析引擎和开放式特征匹配三大功能引擎，支持传统互联网协议、工控协议和工业以太网协议，同时适用于 PLC、DCS、SCADA 等现场环境，不

仅具备多种工控网络协议数据的检查、过滤、报警、阻断功能，同时拥有基于最新漏洞库的黑名单入侵防御功能，和基于机器智能学习引擎的白名单主动防御功能以及大规模分布式实时网络部署和更新等功能。

### 2.4.3 全方位可视化

设计上秉承安全“可视化”的理念，产品集成了强大的分析监控功能，能够根据需要对系统资源状态、流量态势、网络拓扑、协议分析和攻击溯源进行监控和分析，让用户更直观、准确、及时的了解网络运行及安全状况。通过对海量数据进行关联分析和数据挖掘，以形象的图表和数据展现了网络应用、安全威胁、流量分布、内容安全、人员网络使用情况等多方面的信息，帮助用户在使用过程中不断了解自己的网络安全状况，并在此基础上进行更好的策略和配置的优化，使管理者清晰的认知网络运行状态，从而实现对内部任一主机乃至全网络的网络应用情况及安全事件信息进行准确的定位与实时跟踪，实现更为有效的网络安全管理。

### 2.4.4 集中管控平台

"集中管控平台"是一款由九方智联完全自主研发的智联云端可视化管控产品。该产品能实时查看及管控所有接入终端设备的状态信息，主动获取和下发终端设备的配置文件，并能通过云端加密通道对终端设备进行远程维护，实时监控及大规模分布式网络统一部署及更新。

### 2.4.5 数字证书认证

与传统的 ID 密码认证方式不同，数字证书认证系统基于 PKI 技术，实现数字证书的

申请、审核、签发、查询、发布，证书吊销列表的签发、查询、发布等全生命周期管理功能。

支持各种对称、非对称算法，包括 SM2、RSA、SM4、SM3、SHA1、SHA256 等。RSA

密钥长度可在 1024、2048 和 4096 之间选择。

## 2.4.6 完善的事件日志审计

采用事件监测引擎对控制网络实现实时告警，通过特定的安全策略，快速识别出系统中存在的非法操作、异常事件、外部攻击并实时告警，提高了整个系统的监测预警能力有利于对每个目标的安全防护。

## 3. 客户价值

### 3.1 全面的威胁防御能力，保障生产有序进行

有效应对来自传统网络威胁以及工控网络的脆弱性风险，降低各类网络攻击所带来的各种损失，保证生产安全有序进行。

### 3.2 更少的成本，更高的性能

采用了单路径处理引擎，数据包仅需一次解码即可完全应用识别和所有安全检测，搭配高性能硬件平台，具有较高的整机性能，并可将安全功能开启带来的性能衰减控制在合理范围。整机性能的提升，使物联网防火墙适用于更广泛的部署场景，有助于提升大型网络的应用层安全防护能力。

### 3.3 可视化管理、轻松运维

提供丰富的可视化界面，将网络攻击、流量态势、网络拓扑等以美观、直接的方式呈现出来，方便运维人员及时发现并处理网络故障事件。

### 3.4 政策合规、满足监管

符合等保 2.0 及公安部的安全区域边界防护的相关要求，适用于各类物联网的安全防护场景。

## 4. 关于我们

### 4.1 公司介绍

深圳市九方智联科技有限公司（简称九方智联）是全新一代专注于工业智能物联网、边缘计算、区块链应用、网络安全及文件安全领域的研发厂商，是国内工业智能化和信息安全产品研发领域的新兴力量。公司目前是深圳市双软企业和深圳软件协会会员单位。

九方智联秉承"以客户为中心、以市场需求为导向"的理念，适应市场瞬息的变化，满足客户不断发展的需求和期望，以"自主创新、团结协作、攻坚克难、追求卓越"的精神不断研发和完善产品，为客户创造价值，为用户打造专业、安全、可靠、领先的创新型产品和服务。

### 4.2 公司目标

九方智联将致力于为客户提供"专业、安全、可靠、领先"的优秀网络和信息安全产品和服务，立志做新一代物联网和信息安全领域的创新者及领导者，成为有自主研发创新实力、有核心竞争力、对社会有贡献、受社会尊重的企业，为早日实现中国梦贡献我们全部的力量。