# 基于网络安全态势感知的主动防御系统设计与实现

莫禹钧 黄 捷 潘愈嘉

（贵港市人民医院 贵港 537100）

〔摘要〕 从下一代防火墙、上网行为管理、终端检测与响应、安全感知系统4 方面阐述基于网络安全态势感知的主动防御系统设计以及具体实现，介绍系统应用效果，指出该系统从医院网络边界、内部网络、终端等方面提供全方位防护，极大提高响应威胁的时效性和精准度。

〔关键词〕 网络安全态势感知；下一代防火墙；终端检测与响应

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673－6036. 2020. 03. 014

**Design and Implementation of Active Protection System Based on Network Security Situation Awareness**

*MO Yujun, HUANG Jie, PAN Yujia, Guigang City People's Hospital, Guigang 537100, China*

〔**Abstract**〕 The paper expounds on the design and implementation of active protection system based on network security situation awareness from four parts of Application Firewall (AF), Access Control (AC), Endpoint Detection and Response (EDR), and Security Information Perception (SIP), introduces the application effects of system, points out that the system provides all－round protection from aspects of hospital network boundary, internal network, endpoint, etc., which greatly improves the timeliness and accuracy of responding to threats.

〔**Keywords**〕 network security situation awareness; Application Firewall (AF); Endpoint Detection and Response (EDR)

## 1 引言

近年来随着“互联网＋医疗”的快速发展和业务数字化转型，医院信息网络安全显得越来越重要。越来越多的医疗业务向公众、各级卫生健康委员会、第3 方组织等开放，但同时信息开放程度的加大、网络边界的模糊化以及黑客攻击的产业化使得网络安全事件较以往成指数级增长。面对频发的安全事件，如网站篡改、被挂黑色链接、窃取数据、漏洞利用、僵尸网络和勒索病毒等，传统安全防御体系的设备和产品已不能应对复杂的网络威胁攻击[1]。传统安全防护体系有3 个弊端：一是医院内部网络未实现全局性的安全感知与可视功能；二是缺乏有效检测各类攻击的手段，无法应对潜入内部的高级威胁；三是缺乏对威胁影响的评估。通过构建网络安全态势感知平台[2]可以帮助网络安全管理员及时发现潜在的攻击威胁，但需要人工响应，无法保证时效性。而基于网络安全态势感知的主动防御系统[3－4]可通过设备间的联动使系统主动处理部分威胁，无需人工干预，响应快，极大提高时效性和准确性。

〔收稿日期〕 2019－07－10

〔作者简介〕 莫禹钧，硕士，工程师，发表论文7 篇；通讯作者：黄捷，工程师，发表论文4 篇。

## 2 系统架构

### 2.1 下一代防火墙（Application Firewall，AF）

防火墙是网络边界的一道必备防线，但传统防火墙关注重点在于防护内部网络在被外部攻击时不被入侵，无法预知事前风险和检测、响应事后影响，从业务风险的生命周期看，仅具备事中防护是不完整的。而且传统防火墙基于已知特征只工作在L2～4 层，无法应对复杂多变的网络环境，故本系统选用下一代防火墙，也称智慧防火墙，技术架构，见图1。其能够在事前自动识别医院内部服务器与开放端口以及漏洞、弱密码等，同时判断识别出医院内部资产是否有对应的安全防护策略及其有效性。下一代防火墙在事中防御方面融合多种安全技术，为 L2～7 层提供完整的安全防御系统，同时通过防火墙内部模块之间的联动封锁和其他安全设备或软件联动、策略智能联动等安全联动形式加强整个网络安全防御系统的时效性和有效性。下一代防火墙具有检测事后影响和快速响应技术，即使在黑客入侵后也可帮助医院网络安全管理员及时发现恶意行为，如医院内部僵尸主机对外发起的恶意行为检测、篡改网页、植入黑链和 Webshell 后门检测等，快速生成并推送警报事件，协助管理员进行及时的响应处置。

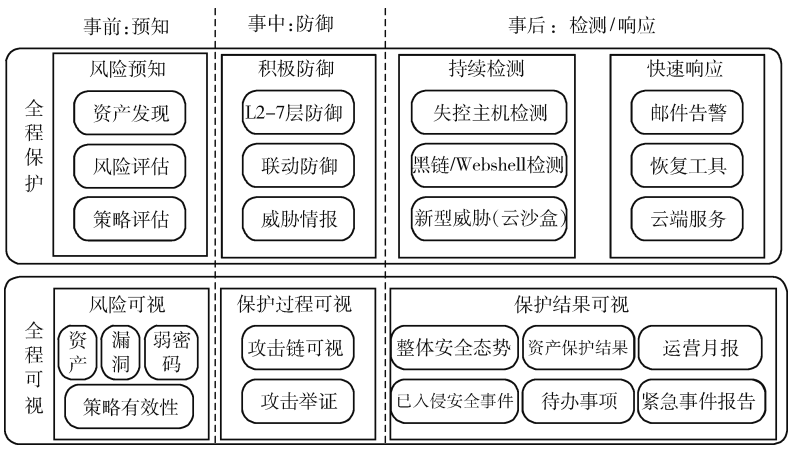


**图1 下一代防火墙技术架构**

### 2.2 上网行为管理（Access Control，AC）

在“互联网＋医疗”推进之前贵港市人民医院外网和内网为物理隔离，外网对于医院业务的影响几乎为零，通过移动终端自助支付医疗费用和云胶片等业务不断开展的过程中，内网和外网改为逻辑隔离，外网在业务中发挥重要作用，其稳定性和安全性越来越重要。本系统将 AC 部署在外网出口、防火墙和外网核心交换机之间，用于管控外网资产。AC 根据需要进行带宽管理，保证核心用户、业务所需的上网带宽，限制其他无关业务对带宽资源的占用，同时对网络应用进行管控，例如禁止医务人员在院内终端进行与业务、学习无关的事宜，分时段限制看视频、听音乐等，实现员工岗位工作与上网权限的匹配。此外 AC 可通过内容过滤、管理控制文件和邮件发送行为等为对外发布信息进行把控，对医院网络中的异常流量和用户行为及时生成警报，日志保留在数据中心，风险智能报表发现潜在的泄密和被攻击用户，实现事前预防、事中拦截、事后溯源。另外对于已中毒的终端，AC 会检测内部终端和外部网络间的异常流量，自动阻断并发起报警，加强医院局域网安全。

### 2.3 终端检测响应平台（Endpoint Detection and Response，EDR）

终端安全解决方案，由端点安全软件和管理平台软件两个部分组成。EDR 统一对终端进行资产管理、合规检查和安全体检，管理支持微隔离的访问控制策

略，能够一键隔离和处理安全事件以及对历史行为数据的可追溯性分析、远程协助取证调查分析。端点软件具有防病毒、防火墙隔离、入侵防御和数据收集上报、一键式处理安全事件等功能。EDR 以内部终端资产为中心，具备精准、持续的检测能力，协同响应帮助医院网络安全管理员快速、准确处理问题。终端检测响应平台技术架构，见图 2。

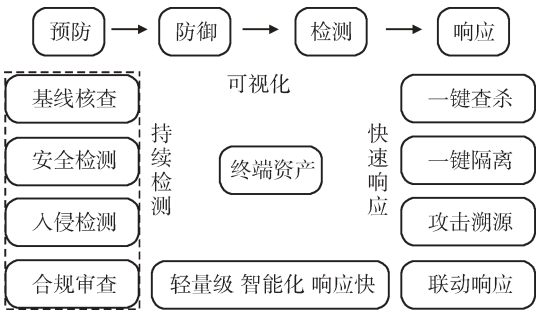


图 2 终端检测响应平台技术架构

### 2.4 网络安全态势感知系统（Security Information Perception，SIP）

展示内网业务和流量，持续检测内部攻击、异常和违规操作行为，使用威胁情报、机器学习、流量监测等核心技术高效识别潜在的攻击和威胁，利用可视化平台实时展现医院内部网络安全情况[5]，及时发现内部违规人员和外部黑客，从而解决安全问题。网络安全态势感知系统由 3 个部分组成：威胁情报、潜伏威胁探针（STA）和安全感知平台（SIS）。威胁情报是通过云平台获取的、来自互联网大数据分析成果的云端威胁情报库，与 SIS 对接，SIS 通过实时接收来自威胁情报的数据增加威胁识别效率和准确率。STA 通过旁路部署在核心交换机，通过网络流量镜像获取医院内部网络全流量，提取有效数据上报到 SIS。SIS 接收威胁情报和 STA 数据后进行分析处理，提供检索支持、生成告警和可视化界面。

## 3 系统实现

### 3.1 接入拓扑

基于网络安全态势感知的主动防御系统接入拓扑，见图 3。用于业务的内网与办公的外网是逻辑隔离，将下一代防火墙（AF）和上网行为管理（AC）部署在外网边界，终端安全软件部署在所有内网终端，终端检测响应管理平台接入内网服务器区，潜伏威胁探针的两个采集口分别接入外网和内网核心交换机，通过网络镜像获取核心交换机和汇聚交换机之间的所有流量，网络态势感知平台和潜伏威胁探针的管理口都接入外网服务器区，SIS 和 STA 之间通过管理口传输数据。

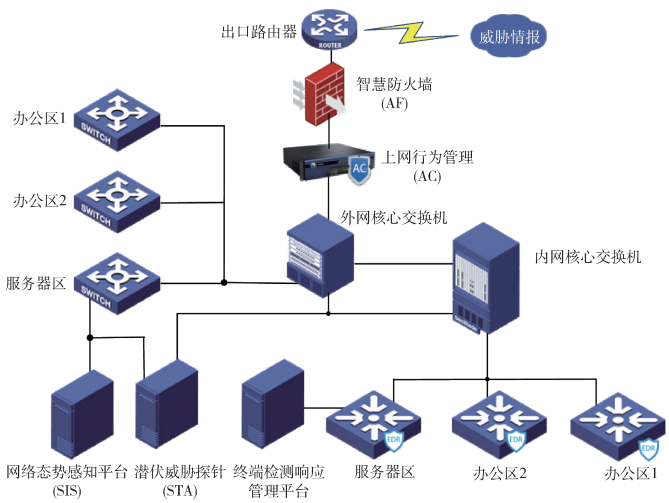


图 3 基于网络安全态势感知的主动防御系统接入拓扑

### 3.2 技术架构（图 4）

技术架构 4 个部分并不是简单的叠加、单独运行，而是一个整体系统，相互联动、共同防御。传统网络安全体系获取到的只是各个安全产品碎片化的攻击日志信息，以统计报表展示，不能结合医院业务分析内部资产安全状态，而本系统中 SIS 数据来源除威胁情报和 STA 外，还有来自防火墙采集的外部和内部网络间流量数据、EDR 采集的服务器和 PC 上的有效数据以及通过 syslog 标准格式收集的第 3 方设备日志，保证数据来源的精准性和广泛性。SIS 是整个系统安全的核心，是检测、预警、响应处置的大数据分析平台，以全流量分析为核心，结合威胁情报、行为分析建模、失陷主机检测、机器学习、大数据关联分析、可视化等技术，实现全网业务、威胁、攻击与异常流量可视化、业务弱点与防御体系薄弱评估等，帮助网络安全管理员及时发

现和定位威胁。SIS 分别与 AF、AC、EDR 进行联动。SIS 与 AF 联动可以在安全事件发生后将某主机或外网 IP 作为源或目的进行封锁，即禁止主机发生外联行为，也可以配置访问控制策略以更加灵活的方式对主机进行隔离封锁。SIS 和 AC 联动主要有弹窗提醒、冻结账号两个功能，弹窗提醒功能适用于某个终端 IP 发生安全事件后提醒该终端在线用户存在的风险。冻结账号功能适用于发生安全事件后对此 IP 上的在线用户进行冻结，防止风险扩展。SIS 和 EDR 联动，在发生安全事件后可直接对主机进行隔离或封锁。

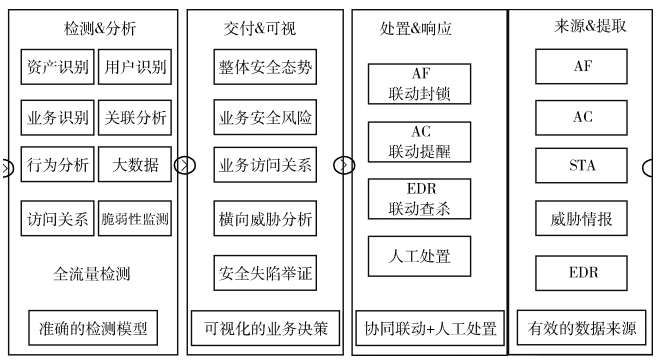


**图 4 基于网络安全态势感知的主动防御系统技术架构**

## 4 应用效果

贵港市人民医院在 2018 年构建网络安全态势感知系统，实现了精准预防与查杀，但是感知平台的数据来源仅限于威胁探针在核心交换机上通过镜像获取，缺少外部和内部网络之间的流量数据和内部终端数据，仍然不够全面。建立基于网络安全态势感知的主动防御系统，有助于网络安全管理员更加全面而准确地了解医院网络中存在的威胁与攻击。此外由于网络威胁攻击时刻存在，仅靠网络安全管理员持续观察，无法及时响应，而通过本系统中各部分的联动响应能及时自动处置部分威胁攻击，防止其快速扩散。

## 5 结语

本系统采用多个安全设备和软件，融合多种安全技术，为医院业务提供全流程的防护，包括事前对医院内部资产风险预知、策略有效性检测，事中提供各种安全防御手段，事后对网络持续检测以及快速响应机制，将全过程中所有相关信息通过多种方式展现给医院网络安全管理员。系统为医院内部网络提供全程保护、可视及自动联动处置。通过设备间的联动自动处置威胁，结合人工处理，极大提高响应威胁的时效性和精准度。等保 2.0 的正式发布对网络安全提出更高要求，本系统能满足等保 2.0 对通信网络、区域边界、计算环境以及管理中心安全等方面的要求，标志着医院网络安全主动式防御系统已经建成。

## 参考文献

1 管磊，胡光俊，王专．基于大数据的网络安全态势感知技术研究［J］．信息网络安全，2016，16（9）：45－50.
2 莫禹钧，潘愈嘉，黄捷．医院网络安全态势感知系统的构建［J］，医学信息学杂志，2018，39（9）：25－28.
3 刘世文，马多耀，雷程，等．基于网络安全态势感知的主动防御技术研究［J］．计算机工程与科学，2018，40（6）：102－109.
4 章学妙，傅翀，卢嘉．基于网络安全态势感知的网络系统自防御体系［J］．计算机应用与软件，2017，34（9）：166－172.
5 董海．基于 GA－RBF 神经网络的网络安全态势感知系统的研究与实现［D］．银川：宁夏大学，2017.