融讯光通
RONG XUN GUANG TONG

# 网络安全系列产品彩页

**北京融讯光通科技有限公司**

**2023 年 12 月**

融讯光通
RONG XUN GUANG TONG

# RT-CADP

## 网络靶场实训演练系统

# RT-CADP 网络靶场实训演练系统

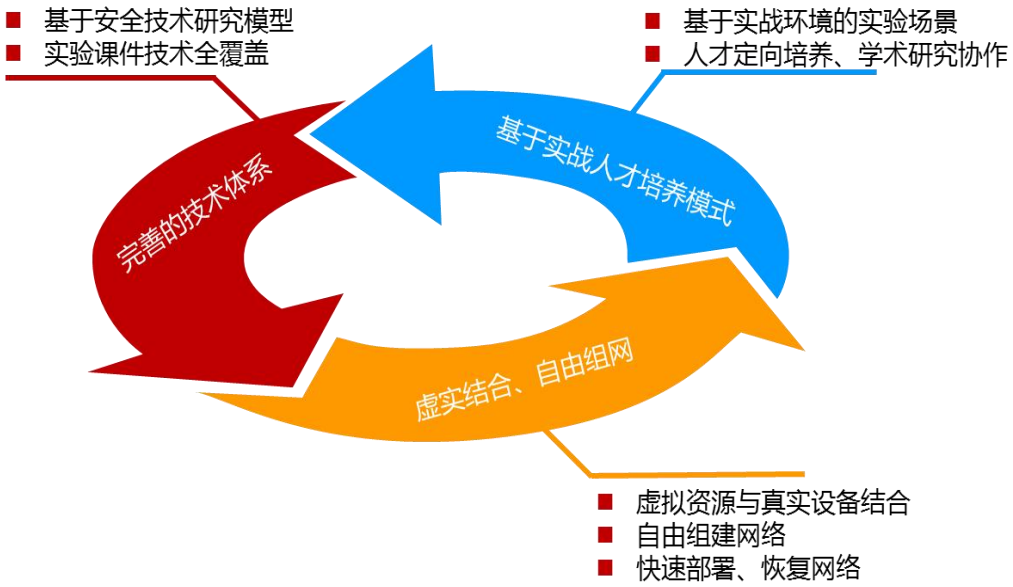
## 产品概述

RT-CADP 网络靶场实训演练系统是北京融讯光通科技有限公司科技专家根据网络安全从业经验及技术积累而开发的一款具有自主知识产权的网络安全领域革命性产品。系统通过融讯光通独特的虚拟化技术实现虚实结合，实现复杂网络环境模拟。系统从教学实训、考核竞赛、应急演练、攻防对抗和网络靶场 5 个方面进行构建，由低到高，逐层次培养，为用户构建一个全方位的网络安全人才培养解决方案。

网络靶场实训演练系统可广泛用于教育（高校、高职和中职）、运营商、军队和研究机构以及其他需要进行信息安全人才培养的组织与单位。融讯光通网络攻防实训系统的主要目标是通过教学实训、考核竞赛、应急演练、攻防对抗、网络靶场等方式，提供一体化的解决方案，来达到多层次人才培养、考核和选拔的目的

融讯光通
RONG XUN GUANG TONG

## 产品特性




- 虚实结合：系统能够将虚拟网络接入真实设备，实现共同组网，搭建更为复杂的网络环境。
- 快速组网：系统基于虚拟化技术，可以一键部署实验环境、竞赛及攻防场景。
- 完善的网络安全技术体系:依据特有的技术体系设计出一套完全易于学习理解的安全技术课程，设计不同实验场景、设计不同实战环境供学员进行学习与实战演练。

## 产品功能

- 网络靶场：组建网络靶场，与物联网，人工智能，工控安全设备等进行联动，建设大型网络安全防御演练场景。
- 红蓝对抗：模拟真实网络环境，设定对抗规则，受训人员分红蓝组进行攻防对抗，裁判员监控违规行为，观察员查看双方进度及对抗结果。
- 竞赛考核：竞速、夺旗、闯关等多种模式，内置考核题目，可自由设置考核内容。
- 教学实训：内置教学课件，包含原理介绍、视频演示、模拟实战等内容，支持用户创建新课件。
- 无线安全实训：配套专用无线路由设备、无线网卡设备，进行无线安全实训、包含 NS2、NS3 无线配置、无线破解等实验。
- 虚拟仿真测试：通过虚拟仿真与虚实结合能力，对网络进行复制和还原、对系统、软件进行渗透测试和攻击演练，并支持攻击回放和数据获取。
- 场景设计：自由上传操作系统、攻击工具，可结合物理设备，快速组网，构建复杂场景。场景可保存。

融讯光通
RONG XUN GUANG TONG

# RT-CSRC

# 网络安全风险预警防御系统

## 产品概述

RT-CSRC 网络安全风险预警防御系统以主动防御为目标，基于网络攻防渗透技术融合云计算、大数据和人工智能等技术，将网络安全被动防御转变为主动防御，以自动化方式，通过网络安全巡检、信息收集、虚实仿真、风险发现、风险利用验证评估和风险报告等功能综合分析，建立防护方案，实现是事前主动发现安全风险，验证风险，评估风险等，进而主动修复风险，最终构建网络安全风险预警防御体系。

## 产品功能

### 基础信息识别

- 设备基础信息识别：风险管控系统内置的探测引擎可以识别设备端口、服务、操作系统类型；同时也可以识别设备类型、设备厂家等。
- 工控信息识别：风险管控系统通过探知可以识别工控设设备，识别工控协议。同时可以识别工控设备的端口、服务、操作系统等。
- Web 应用信息识别：风险管控系统通过指纹库的比对，WEB 应用信息采集引擎可探测 WEB 服务器操作系统版本类型和版本号、WEB 服务器类型和版本号、中间件类型和版本号以及数据库类型和版本号等信息收集和判断。不但可以识别国外应用系统,还可以识别国内应用系统。

### 网络安全巡检

- 监控资产在线状态。
- 监控应用状态。
- 应用状态异常报警，非法接入报警。

### 场景仿真

- 内置丰富的镜像模板，系统具备强大的虚实结合场景仿真能力。
- 支持界面拖拽方式可视化场景拓扑构建，所见既所得。
- 系统内置丰富镜像资源，同时支持动态调整网络。
- 支持动态分配 IP: DHCP 动态分配 IP。

- 支持智能链接校验： 网段、端口等智能校验。

## 风险发现

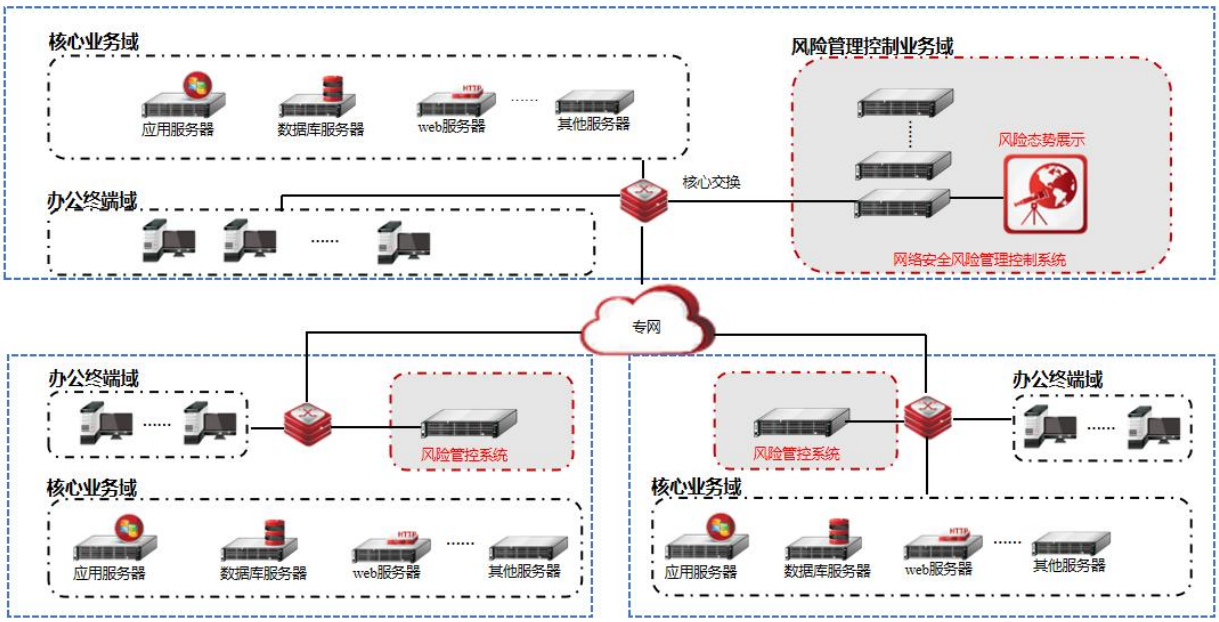
- 内置漏洞库，包含漏洞 118126 个，月度更新。
- 内置脚本库，包含漏洞检测脚本 48643 个。
- 内置特有脚本库，100+；月度更新。
- 内置常见漏洞检测插件 43 个，常见 CMS 漏洞检测 348 个，系统采用插件式设计，支持可扩展。

## 风险利用与验证

- 平台内置渗透攻击模块 1847 项，,可实现对目标机器的远程攻击验证，向用户展示漏洞的危害性。
- 平台自动对目标进行信息收集，根据收集的资产信息，如端口、服务搜索可能存在的漏洞，并检索内置的产品库、漏洞库，智能选择合适的检测和攻击脚本，实现一键式自动化攻击验证。

## 网络部署

系统支持集群化部署，旁路部署于核心交换或者汇聚交换上即可。



融讯光通
RONG XUN GUANG TONG

# RT-FW

# 下一代多功能防火墙

## 产品概述

RT-FW 系列下一代防火墙是 T 比特级 7 层防火墙，以保障用户应用安全为目标，立足于高性能的矢量操作系统和一体化引擎，通过 L2-L7 层全面威胁防御及强大应用安全管控技术，为用户提供超高性能的网络安全解决方案。

下一代多功能防火墙集成了基本防火墙、入侵防御/检测、web 应用防火墙、VPN、防病毒网关、抗 DDoS 网关等的功能，能提供多种防护能力，是未来网关类产品发展的趋势，能够实现深层防御、精确阻隔。

## 产品特性

- 平台通用性、普适性广。
- 一站式管理，简化网管维护。
- 统一安全引擎技术。
- 全面威胁检测与防护。
- “四位一体”，细粒度安全防护。
- 支持虚拟化、云化部署。
- 支持通用 X86 平台架构。
- 支持“信创”飞腾 CPU 平台。
- 支持“信创”鲲鹏 CPU 平台。
- 即将支持工业防火墙 IFW 和工业安全审计 IAD。
- FW、IPS、WAF、数据库防火墙、数据库审计等形态可自由控制。
- 支持各类大型行业客户安全微定制。

## 产品功能

- 基本防火墙
- 入侵检测技术
- 抗 3 至 7 层 DDoS
- 流量可视

- 流量管控与优化
- 负载均衡
- 高可用性
- 高可靠性

## 应用场景

### 常规部署模式

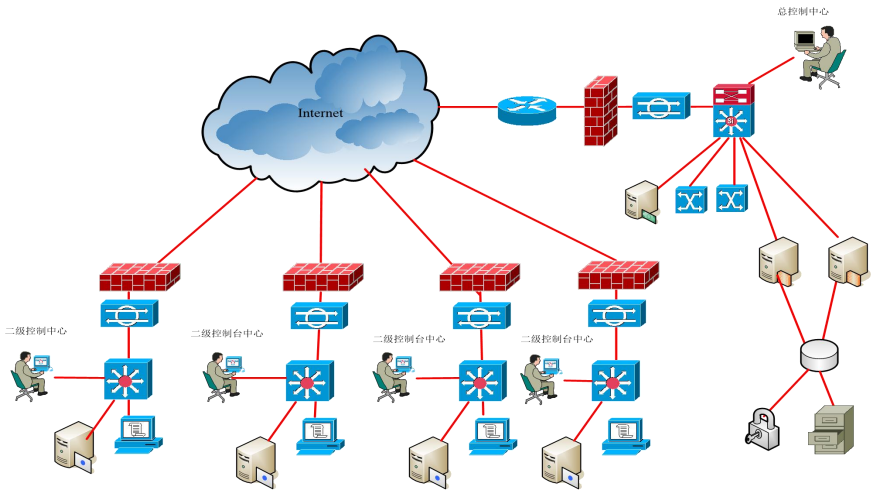
- 边界防护，放置在防火墙的外面；内部防护，放在防火墙设备的后面，作为第二道大门存在。

### 双重链路部署

- 双链路部署，一台检测引擎上可以串接两路防御。在有设备冗余备份的环境中，可以使用一台设备就完成冗余备份的需求。

### 多层结构部署

- 支持大规模跨地域的管理部署模式，控制中心可以下接防御引擎，也可以挂接子控制中心。可灵活设置成与行政业务管理流程紧密结合的集中监控、多层管理的分级体系。通过策略下发机制，使上级部门能够统一全网的安全防护策略；通过信息上传机制，使上级部门能够及时了解和监控全网的安全状态。



融讯光通
RONG XUN GUANG TONG

# RT-ZGate

# 零信任泛终端安全网关

## 产品概述

RT-ZGate 系列零信任泛终端安全网关属于全终端接入管控、网络准入、安全防护设备，基于流量，来真正解决物联网时代，海量物联网终端接入安全防护以及内网安全防护的难点和痛点问题。

RT-ZGate 系统是一种网关类单机产品，具备资产探测、资产防冒用检测、资产行为分析、防火墙、轻量 IPS 功能。该产品最初面向的需求为哑终端设备的入网安全检查及防护，主要解决哑终端入网审核和网络访问控制问题。所谓哑终端即具备单一功能的网络终端，主要为有线终端。这类终端具有分布广、数量多、种类杂、功能单一、无人值守的特点。

产品支持旁路模式或者透明串式部署，一般旁路或串接网络域的网关前汇聚后，通常部署于二层网络域，也可以作为防火墙网关和部署于三层网关处。

## 产品功能

- 在线 IP 资产发现，通过流量识别和主动扫描建立联网资产信息表，识别资产类型如打印机、摄像头，识别设备厂商。
- 检查资产在线下线状态。
- 识别 IP 资产的 mac、操作系统、开放端口（及服务器类型和版本，可进一步识别漏洞）、snmp 信息、banner 信息。
- 资产指纹异常发现及告警。
- 能对合规入网 IP 资产进行审批，可设置对未审批资产禁止联网。
- 资产以 IP、mac 或 IP 与 mac 共同作为资产唯一索引。
- 通过实时流量分析可发现在线资产，可采集到 mac 地址（二层流量）、ttl、开放端口、操作系统类型（p0f 分析）。可采集到设备的的 dns 解析内容，可辅助判别设备类型。
- 基于端口主动扫描的主动探测可识别到几乎全部定义指纹，但主动扫描存在一些问题：受设备自身或网络中的访问控制规则影响，不能获取到准确信息；主动探测可能会触发安全设备的响应；主动探测可能会对目标设备系统或者网络造成影响。
- 可进行基于 mac、时间、五元组、通行行为基线的网络访问控制，超出规则外告警。

- 能支持 mac 白名单、黑名单；能支持 IP 白名单、黑名单；支持 IP/mac 绑定；支持协议/端口黑名单；支持 dns 黑/白名单，对发现的 dns 解析进行检查、如果是在黑名单内，则阻断该 dns 解析通信，检测到黑名单内容即告警
- 支持旁路阻断技术
- 支持交换机联动

## 产品特性

- 支持虚拟化、云化部署
- 支持通用 X86 平台架构
- 支持“信创”飞腾 CPU 平台
- 支持“信创”鲲鹏 CPU 平台
- 支持各类大型行业客户安全微定制

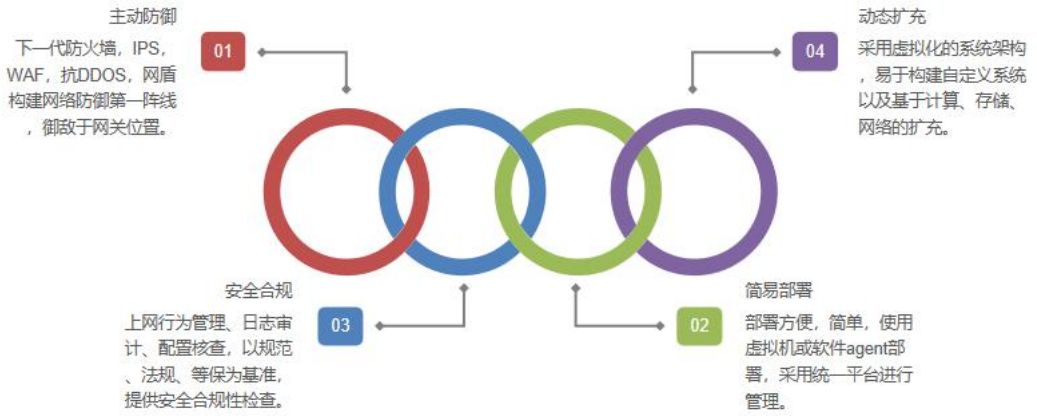
## 系统架构

# 合规神器-等保通

## 产品概述

合规神器等保通以“主动防御、简易部署、安全合规、动态扩充”为核心，打造专用于解决等保 2.0 建设难点与痛点的快速解决方案，帮助用户实现统一的安全运营及管理。。

## 功能架构




## 产品特点

- 单台设备提供等保二级、三级套餐防护，综合了审计类、防护类和主机安全类三大块； 业务灵活编排，根据等保需求，可以灵活增加或者减少业务应用软件包，提供个性化安全增值服务；统一运维平台：多业务应用软件运维平台统一； 支持其它软硬件平台扩展，包括服务器、工控机、云计算资源等。


## 产品功能

- 主动防御：下一代防火墙，IPS，WAF，抗 DDOS，云安全 IP 盾构建网络防御第一阵线，御敌于网关位置。
- 安全合规：上网行为管理、日志审计、配置核查，以规范、法规、等保为基准，提供安全合规性检查。
- 简易部署：部署方便，简单，使用虚拟机或软件 agent 部署，采用统一平台进行管理。
- 动态扩展：采用虚拟化的系统架构，易于构建自定义系统以及基于计算、存储、网络的扩充。

## 产品部署