

★完全公开

奇安信网神网络安全准入 系统 NAC V8.0 产品彩页

地址：北京市西城区西直门外南路26号院1号

邮编：100044

1 产品概述

目前大多数企业构建的还是开放式的网络,过去在 Interner 接入安全和服务器安全领域投入了大量的资金,虽然网络出口处部署了防火墙、IPS、防病毒服务器等安全设备,但是网络安全事件依然层出不穷;虽然在终端上安装了杀毒软件,但病毒感染还是泛滥成灾;为什么?企业内部网络接入层采用开放式的网络架构,这种开放网络给企业业务开展确实能够带来便捷,但也有严重的安全风险,随着IT技术的快速发展,各种网络应用的日益增多,病毒、木马、蠕虫以及黑客等等不断威胁并入侵企业内部网络资源,使得企业网络的安全边界迅速缩小,开放的内部网络访问已经严重影响到企业IT基础设施的稳定运行和数据安全,因此需要构建新一代的内部终端准入安全防御体系。

1.1 产品参数

产品系列		NAC-A2110-PA
支持终端数		1000
吞吐量		5Gbps
最大并发认证数 (tps)		1000
最大并发连接数(pbr)		30w
最大每秒新建连接数(pbr)		1w
操作系统		国产化操作系统 OpenEuler 22.03
CPU 型号		国产化CPU: 海光 C86 3250
CPU 主频		2.8GHz
核心数		八核心
线程数		十六线程
内存		8G
硬盘		4T
机箱		2U
电源		350w 冗电
接口配置	标准网络接口	4个电口、4个光口、1个MGT管理口、1个调试口
	可用扩展槽位	1个
尺寸与重量	机箱尺寸	440mm (宽) × 560mm (深) × 88mm (高)
	主机重量	13.5kg
电源参数	额定输入电压	100V AC~240V AC, 50Hz/60Hz

环境参数	工作温度	0℃ ~ 40℃
	工作湿度 (RH)	5% ~ 85%无结霜
	储存温度	-20℃ ~ 70℃
	气压	40kpa-110kpa
	海拔	≤5000m
其他	支持协议	支持 IPV4 和 IPV6 协议
	开放接口	提供开放接口, 实现对接联调

1.2 产品形态及构架

奇安信网神网络安全准入系统采用分层架构设计实现,层与层之间相互解耦,保障产品的稳定性同时,极大地提升了产品性能,依托于高效的资产识别、行为分析、基线检查、设备汇总和威胁防护引擎,准入系统支持持续对网内设备进行身份及合规行为检测,发现设备身份信息或合规状态变化时,第一时间采取处置手段,产品系统技术架构图如图 1 所示:



图 1

产品由准入控制设备、控制中心、准入客户端三部分组成。

1.2.1 准入控制设备

准入控制设备是系统的核心，负责接入认证及流量处理等重要的准入控制职能，采用专业的工业控制设备，由标准机架式软硬一体设备和小型可灵活部署的设备和型号选择。

1.2.2 控制中心

控制中心采用 B/S 架构，支持浏览器远程对设备进行访问，对准入控制设备下发配置策略，进行操作和监测管理。配置管理由设备发现、设备管控及告警、

安检合规、入网控制等功能构成，能够对网络边界的安全风险和安全事件进行实时的监视和在线的管理。

准入控制器中内置控制中心页面，同时支持在外部服务器通过软件安装包安装控制中心，满足不同规模客户单机管理或分布式集中管理的需求。

提供全网监控统计功能，实时显示全网监控状态信息的资产动态、安全违规事件、设备信息、在线终端统计、终端类型统计、终端厂商分类统计、实时告警、终端安全分析统计等信息。

1.2.3 准入客户端

提供适用于 windows、Linux、国产化等操作系统的准入客户端，客户端可以根据管理员定义策略进行身份认证、终端设备合规检测、违规设备网络隔离和引导修复功能。

2 产品功能

奇安信网神网络安全准入系统基于模块化授权，针对不同用户场景及需求，提供设备入网合规管控全流程的功能特性，包括设备发现识别、网络边界管理、网络准入、访问控制、IoT 设备合规评估、终端准入合规、高级威胁等功能。

2.1 设备发现与识别

奇安信网神网络安全准入系统实现对入网设备的即时发现，提供网络资产自动采集功能，并能够自动分类网络中的接入设备，如交换路由设备、PC 设备、服务器、网络打印机等，自定义用户限额，支持终端资产智能识别发现，对外来终端的接入行为进行告警，并识别收集设备的关键信息，实时扫描检测设备的在线状态，提供 IP 地址管理功能，并支持对网络内设备链路质量进行检测。

2.1.1 接入发现

随着信息化网络的不断建设，网络中存在的设备类型、设备品牌、设备信息

变更已无法通过传统的台账进行手动维护。奇安信网神网络安全准入系统通过主动扫描，实时监控网络内设备的通讯流量、广播流量，以及通过采集交换机上接口连接信息等方式来实时发现网络中各种类型设备的接入事件，并展示设备类型、设备品牌、设备 IP 地址、设备 MAC 地址、设备接入位置等信息。同时系统支持记录设备信息变更，帮助管理员全面掌握网内资产状况。

2.1.2 设备识别

奇安信网神网络安全准入系统能够通过识别设备的网络流量特征，扫描获取设备开放端口、运行服务等网络特征，同时通过适配大量智能设备专用管理协议，准入系统能够精准识别网络中设备的类型、品牌、操作系统、设备名称、甚至型号信息。系统支持 Window 终端、Linux 终端、信创终端、移动终端、服务器、虚拟机等终端设备，及网络打印机、IP 电话、视频会议系统、网络摄像头、网络摄像机、门禁等常用 IoT 设备。同时系统提供便捷的设备识别规则配置系统，通过简单配置识别规则即可对网络内的专属设备进行规则库配置。

同时系统对网络内设备的主机名、开放端口、IP 等信息进行实时监测、支持对设备主机名变更、开发端口变更、IP 变更等配置变更进行实时审计。

2.1.3 资产管理

奇安信网神网络安全准入系统提供针对网内设备的提供资产管理功能，可管理不同类型入网资产，对入网资产可发现、可审批入网。可以帮助资产管理人员监控关键设备活动状态，及时发现活动状态异常的设备。

2.1.4 地址管理

当管理员缺乏有效的手段对网络 IP 地址资源进行管理时，常常会造成 IP 地址随意使用、地址资源利用率低、地址冲突等问题。奇安信网神网络安全准入系统提供 IP 地址管理功能，在 IP 地址池中可直观展示当前地址池中所有 IP 在线离线状态，分配未分配状态，并可直观查看每一个 IP 当前的使用人信息。通过对设

备变更 IP 的审计，准入系统能够帮助管理员方便地查找到特定时间使用某个 IP 的设备信息。

同时，奇安信网神网络安全准入系统内置 DHCP 服务，管理员可利用准入系统提供全网动态 IP 分配服务，同时丰富的动态地址、固定地址、保留地址的配置，能够很好地满足各种 DHCP 需求，帮助管理员有效管理全网 IP，最大化地利用地址池资源，并杜绝 IP 冲突事件发生。

2.2 网络准入

奇安信网神网络安全准入系统提供客户端的准入模式和无客户端准入模式，可供自定义部署和管理。提供多种准入控制手段和多种设备入网验证流程，针对计算机、移动终端、各类哑终端在无线及有线场景下实施严格的身份认证与绑定约束。

对路由、无线、AP、HUB 等环境下的终端实施准入控制，支持对 Windows 操作系统、非 Windows 系统设备、国产系统设备的识别并实施准入控制。

2.2.1 用户管理

奇安信网神网络安全准入系统内置用户管理功能，当用户没有身份管理系统时，可使用准入系统创建、管理和维护用户身份。系统支持创建或导入组织结构信息，支持创建、导入用户信息或允许终端用户自助注册账号，系统支持账号有效期、密码有效期、同时在线数限制、首次登录强制系统修改密码等策略配置，同时支持为用户配置例如手机号、员工号等各类自定义属性类型。同时系统支持从企业已有的 AD/LDAP 身份系统定时自动同步组织与用户信息。

同时系统支持第三方账号的准入策略配置，当使用第三方认证源或证书认证方式进行身份认证时，无需修改第三方系统上的账号状态，在准入系统上对对应的第三方账号进行配置即可进行账号停用，有效期设置，在线数限制等安全设置。

2.2.2 第三方认证源

当前企业网络结构复杂，账号服务器多样化，如何保证和这些服务器实现联动，统一认证管理？奇安信网神网络安全准入系统在网络适应性上提出兼容多种认证源的认证方式，支持本地用户、AD 认证、LDAP 认证、Email 认证、Http 认证适应用户不同网络环境，满足用户实名制认证、集中统一管理的入网需求。

准入系统支持第三方认证源缓存，当第三方服务器异常时确保已认证终端的正常使用，同时系统提供第三方认证源的高可用方案及自动逃生方案，可通过配置第三方认证源资源池，确保单个认证源服务异常时可及时切换至备选认证源或执行自动认证逃生，不影响设备入网。

2.2.3 资产登记

若用户没有身份管理系统，同时又有设备实名诉求，或者对于 IP 电话、打印机、摄像头等 IoT 设备，无法进行身份认证但又有人机关联需求时，可使用资产登记功能进行使用人信息登记。

对于 PC 类办公终端，奇安信网神网络安全准入系统提供页面登记或联动天擎客户端进行信息登记两种资产登记方式，新终端接入网络时，将被准入系统第一时间将网络访问请求重定向至资产登记页面或客户端登记引导页面，信息填写完毕并经过管理员审核后，终端即可正常入网。而对于 IoT 设备，资产使用人可提前登录资产登记页面，提前录入设备信息，管理员审批通过后，IoT 设备即可正常入网。

资产登记所有字段均支持自定义，同时若用户存在资产台账或一机一档系统，准入支持定制从用户已有资产系统中同步资产数据，避免终端用户重复登记。

2.3 准入控制技术

奇安信网神网络安全准入系统面对不同网络场景的准入需求，提供接口级准入和边界级准入不同级别的入网安全控制，支持接入网关、软阻断等多种接入控制模式以实现网络梯级防御。

2.3.1 接口级准入

接口级准入通过控制NAS（网络接入）设备连通性来进行未认证或未合规终端的入网管控，终端未入网前无法访问同网络下其他已入网设备。

2.3.1.1 802.1X 准入

802.1接入认证是通过标准802.1x协议，在网络接入层做准入认证、根据认证授权情况确定是否能访问网络，支持动态VLAN/ACL片段的下发，可绑定多种认证因素实现强认证管理，结合入网合规性检查策略，根据合规性下发网络访问权限，802.1x认证可提供接口级的强准入认证方案，并支持认证授权、合规检查、隔离修复、访问控制“一站式”的全流程接入管理。

802.1x 是联动交换机进行 EAP 认证，最终目的就是确定交换机接口是否可以通讯，对于一个接口，如果认证成功那么就授权这个接口，允许网络报文通过；如果认证不成功就使这个接口保持未授权状态，此时只允许 802.1X 的 EAPOL 认证报文通过，此认证技术方案兼容国内外大多数常用交换机或无线 AC，支持有线和无线网络环境下的接入认证。

优势特点：

- 接口级的入网控制强度，适应强入网控制需求
- 支持复杂网络环境的认证，支持有线、无线、手持终端、HUB 环境的入网认证
- 支持多种认证绑定控制策略，支持身份、设备、位置等混合绑定、支持同时认证在线数限制等
- 支持多种认证方式，账号、主机、Ukey、证书认证等
- 支持多种逃生方式，双机热备 HA、冷备、一键逃生、第三方服务器异常自动放行等
- 支持基于设备连接方式、认证客户端类型、接入位置、认证用户进行动态授权，支持 vlan（组）、acl 片段、其他厂家 radius 属性下发。

2.3.1.2 MAB 准入

当网络交换机开启 802.1X 认证后，网络中的所有终端必须安装准入客户端才可接入网络，为保证网络中打印机、IP 电话或者某些未安装客户端的特殊终端设备的入网需求，可开启

MAB 认证功能。管理员可通过提前录入白名单 MAC 地址或者对待入网设备审批方式允许特定终端入网。

使用 MAB 方式进行设备认证的同时，准入设备可配合动态授权及绑定策略，进一步限制 MAB 入网终端的网络访问权限和接入位置、接入 VLAN 等属性，确保 MAB 入网设备的行为可控。

2.3.1.3 DHCP 准入

准入系统提供DHCP服务，对于使用DHCP进行IP地址管理的用户环境，可使用准入DHCP服务进行动态地址分配，同时准入可通过基于终端合规状态和审批结果分配不同IP地址的方式，对不合法终端分配访客区的IP，限制其只允许访问特定修复服务区，并对不合法的终端的业务访问流量进行重定向引导其修复。通过访客区与业务区IP段的ACL规则配置，可实现未合法终端与合法终端无法互访的隔离需求。

同时使用DHCP对网络内设备进行地址分配，能够极大地提升网络内地址的使用率，降低地址冲突等常见问题，对于终端的IP变更事件，准入系统有详细的变更记录，方便管理员第一时间追溯到问题IP的关联终端与个人。

2.3.1.4 WebAuth 准入

WebAuth 是一种基于交换机的 Portal 入网控制方式，当新终端接入交换机或无线 AC 时，交换机或 AC 发现该终端未经身份认证，则将其浏览器请求重定向至 Portal 认证页面，用户通过身份认证成功后即可正常访问网络。未经身份认证的终端无法访问其他已认证终端或未认证终端。

2.3.2 边界级准入（IP 流量控制）

IP 流量控制是一种通过流量欺骗或流量过滤的技术，对网络内终端穿越 NAC 防护边界的流量进行检测与控制的方案，支持旁路镜像、策略路由、透明网桥等三种设备部署方案，通过监听终端经过 NAC 访问服务器的网络数据流，并做连接跟踪，对内网数据流进行合法性检测并对非法连接进行阻断和控制，保护核心区域访问的安全。它基于用户核心业务保护概念，对非法访问用户核心资源进行访问限制，确认身份的合法后才能正常访问。

★ 支持多种入网流程，用户可以根据需求灵活选择

- 用户经过 portal 认证/用户注册，可直接访问受保护服务器，注册用户需经管理员审批确认或自动审批确认。
- 用户下载并安装准入客户端，使用客户端进行用户身份认证或设备身份认证后才能访问受保护服务器，注册用户需经管理员审批确认或自动审批确认。
- 用户下载并安装准入客户端，提交资产登记信息并经过管理员审批之后才能访问保护服务器。

2.3.2.1 旁路镜像

旁路部署模式下的 NAC 设备，通过交换机流量镜像方式获取流量数据。旁路部署不改动客户原有网络拓扑，不改变客户原有使用习惯，这种部署模式下，即使接入控制器宕机也不会对客户网络造成中断。

2.3.2.2 策略路由

策略路由是一种基于终端认证及合规状态而动态进行路由选择的机制。部署时，管控区需要与访问区域处于不同网段，网关需更改原有路由配置，将报文转发至 NAC 设备，NAC 设备通过评估终端的认证及合规状态，选择是继续转发报文、重定向或丢弃，从而对网络内终端穿越边界行为进行管控。

2.3.2.3 透明网桥

在不支持策略路由或者旁路镜像的环境下，为了满足客户网络环境下的准入控制需求，准入系统提供透明网桥的部署模式。奇安信网神网络安全准入系统在不改变现有拓扑的情况下将网桥串接到网络当中，采用 ACL 的方式对流量 IP 进行过滤，对不合法不合规的终端流量进行重置或丢弃，从而阻断其网络流量。

2.4 终端合规检查

奇安信网神网络安全准入系统提供适用于 Windows、Linux、信创客户端的独立准入客户端，提供超过 20 种的终端安全合规检查项，提供终端入网环境安全检

查功能，包含屏保检查、远程桌面检查、共享资源检查等。接入终端受准入系统约束，入网时需强制安装准入客户端并进行合规检查，只有满足合规要求方可接入网络。

安检项名称	功能描述
远程桌面检查	禁止开启远程桌面服务
U 盘自动检查	禁止开启 U 盘自启动
防火墙检查	要求防火墙必须开启
IP 获取方式检查	要求 IP 获取方式必须是手动或自动获取
共享资源检查	禁止存在共享文件夹或有 everyone 权限的共享文件夹
补丁检查	要求系统必须或禁止存在某补丁
服务检查	要求系统必须或禁止存在某服务
进程检查	要求系统必须或禁止存在某进程
软件检查	要求系统必须或禁止存在某软件
IE 代理检查	禁止开启 IE 代理
密码强度检查	要求 Windows 策略中配置相应密码强度
杀毒软件检查	要求终端的杀毒软件符合特定设定
非法外联检查	禁止访问特定地址
域检查	检查当前系统是否加入域
Guest 账号检查	禁止当前登录账号为 Guest 账号
操作系统检查	要求当前操作系统必须为指定类型
注册表检查	要求注册表必须或禁止包含某项
关键文件检查	要求必须或禁止存在某文件
系统账号检查	本地系统账号名称必须为限制范围内的账号
屏幕保护检查	必须开启屏幕保护
开放端口检查	禁止开放指定的端口
计算机名检查	要求计算机名符合名称规范
实名检查	实名认证成功后才能入网

2.4.1 强制推送客户端

奇安信网神网络安全准入系统支持对未安装客户端的终端进行网络重定向，在其访问网页内容时，将其访问原网页重定向为轻量的网络准入客户端或天擎终端一体化安全管理软件安装页面。终端设备只有安装安全软件并认证成功后方可入网。通过准入系统强制推送客户端，解决了困扰管理员很久的终端安全软件安装率低、去化率高、部署工作量大的困扰。

2.4.2 违规外联

奇安信网神网络安全准入系统准入客户端支持周期性探测设备是否能够连通互联网地址或管理员设置的检测地址，当终端能够连通互联网地址时，系统将判定终端存在违规外联能力，将违规终端进行断网或隔离，确保内网安全。

2.4.3 安全运维

奇安信网神网络安全准入系统支持自动生成运维管理网络整体拓扑图，在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息；支持在界面上提供对该网络设备进行 TELNET、SSH 等管理。

2.4.4 密码策略

奇安信网神网络安全准入系统准入客户端支持对终端设备的密码策略及设备的登录口令强度进行检查。通过设置密码策略检查规则，可以强制终端用户设置密码时必须符合复杂性、最小长度、最大最小使用期限、保留历史密码个数等基础要求。同时客户端还可针对终端用户登录系统时使用的账号密码进行检查，当用户未设置密码或使用不满足强度要求的密码登录系统时，将阻止终端的网络流量，其中弱口令规则库支持管理员自定义添加，以适应不同的用户场景。

2.4.5 终端隔离修复

奇安信网神网络安全准入系统准入客户端内置多项安检项，可满足常见终端保护要求。自定义安全基线检查。要求对未认证通过用户入网时进行阻断。终端安检不通过时，准入系统会对其进行隔离以避免对单位内网网络环境造成安全威胁，管理员可通过定义隔离策略限制隔离终端仅允许访问特定的某几个地址进行软件下载、补丁更新等操作。针对单个终端进行相关操作，包括设为禁用、阻断、保护、注册信息填写等操作。同时，这些隔离中的终端会自动修复或提示用户手动进行安全修复，在修复完成后继续投入正常使用，减少管理员的维护时间成本。

2.4.6 入网安全检查

提供终端入网的安全基线检查功能，包含 SP 补丁检查、系统补丁检查、系统时间检查、计算机名规范检查、防病毒软件检查（支持软件版本检查）、IP/MAC 绑定检查、Windows 防火墙检查、操作系统版本检查等。

提供准入 IP/MAC 黑白名单管理功能，处于黑名单表中的 IP 和 MAC 会被准入设备判定为非法设备，处于白名单表中的 IP 和 MAC 会被准入设备信任。

提供终端安装软件的检查和软件运行情况的检查，提供白名单、黑名单、红名单管理方式。

提供多种智能及非智能终端的准入控制，通过身份认证以及安全域控制等手段，保证接入网络的终端可信程度，并控制可信计算机的访问权；自定义安全基线检查；提供资产管理功能，可管理不同类型入网资产，对入网资产可发现、可审批入网；

提供终端 USB 设备授权管控，可对终端外设（键盘、鼠标）、移动存储、其他 USB 设备设置允许或禁止使用；

提供终端在接入受控网络后，可对受控网络内的终端安全状态进行定期检查，以保证终端安全状态始终符合安全策略要求。