智能 DNS 系统

测试报告

V1.0

2024 年 9 月

一、 测试概述

1.1 测试目标

对三个厂商的智能 DNS 系统（****核心网络服务系统、**智能 DNS 系统、****安全 DNS 系统）进行测试，从产品功能、系统完善程度、系统稳定性、售后服务、客户案例、硬件资源占用等方面，结合我校实际情况，对比三家产品的特点，为采购做出评判依据。

1.2 测试需求

1. 是否支持多网卡配置
2. 是否支持双主机部署方式
3. 是否支持国产操作系统和 EDR 安装
4. 是否能支撑校内全部用户上网解析
5. 是否支持内、外网分域管理
6. 是否支持 DNS 域名添加、修改、删除，TTL 修改等基本操作
7. 是否支持 A、AAAA、CNAME、NS、MX、泛域名、TXT 等解析类型
8. 是否支持恶意域名拦截
9. 是否能和出口防火墙联动智能选路
10. 是否支持 QPS 统计
11. 日志查询是否易用
12. 是否能统计僵尸域名
13. 是否支持短期域名自动禁止解析

1.3 测试人员

东北师范大学信息化办-系统运行部

1.4 测试时间

2024 年 6-9 月

二、 测试准备

2.1 设备准备

序号	设备名称	数量	备注
1	域名服务器	6 台	每个产品 2 台

2.2 资源准备

序号	设备名称	数量	备注
1	域名数据		nenu. edu. cn 域的子域名
2	出口设备联动配置		读取出口设备带宽数据作为智能解析的依据

三、 测试结果

3.1 功能测试

带*为重点功能

功能概述

功能/模块	****	**	****
多网卡配置（内网 IP/联通 IP/教育网 IP）*	支持	支持	支持
双主机部署方式*	支持	支持	支持
国产操作系统和 EDR 安装*	支持	支持	支持
支撑校内全部用户上网解析*	支持	支持	支持
内、外网分域管理*	支持	支持	支持

DNS 域名添加、修改、删除，TTL 修改等基本操作*	支持	支持	支持
是否支持 A、AAAA、CNAME、NS、MX、泛域名、TXT 等解析类型*	支持	支持	支持
恶意域名拦截*	支持	支持	支持
与出口防火墙联动智能选路*	支持	支持	支持
QPS 统计*	可查询最近三个月数据	可查询实时数据，不支持历史数据查看	可查询 30 天内数据
日志查询	支持	支持	不显示在线日志，需自定义查找
统计僵尸域名	暂不支持	支持	目前版本不支持
短期临时域名到期后自动禁止解析	支持	支持	直接删除而且查不到记录

3.1.1 多网卡配置（内网 IP/联通 IP/教育网 IP）

测试项	多网卡配置（内网 IP/联通 IP/教育网 IP）
测试目的	验证产品是否支持校内用户上网解析及权威域教育网和联通双路场景
测试步骤	在每个产品的两台服务器上分别配置内网 IP（*.*.*段）/联通 IP（*.*.*段）/教育网 IP（*.*.*段）
测试结果	****:支持 **：支持 ****：支持

3.1.2 双主机部署方式

测试项	双主机部署方式
测试目的	验证产品是否支持双主机架构，每一台主机独立提供解析服务。能统一

	管理，数据实时同步
测试步骤	每个产品部署两台服务器，分别测试解析服务
测试结果	****:支持 **：支持 ****：支持

3.1.3 EDR 安装

测试项	支持安装 EDR
测试目的	验证产品是否支持安装 EDR，增强安全性
测试步骤	在系统上安装 EDR
测试结果	****:支持 **：支持 ****：支持

3.1.4 支撑校内全部用户上网解析

测试项	支撑校内全部用户上网解析
测试目的	验证产品性能及稳定性
测试步骤	将全部上网认证用户依次切换到每个 DNS 产品上，分别服务两周时间
测试结果	****:支持 **：支持 ****：支持

3.1.5 内、外网分域管理

测试项	内、外网分域管理
测试目的	验证产品是否支持：非白名单权威域名仅对校内网发布，白名单域名对外网发布
测试步骤	1.设置校内解析视图，为校内用户提供解析服务

	2.添加测试域名，设置该域名的解析范围为非校内地址，测试解析效果
测试结果	****：支持 **：支持 ****：支持

3.1.6 DNS 域名添加、修改、删除，TTL 修改等基本操作

测试项	DNS 域名添加、修改、删除，TTL 修改等基本操作
测试目的	考察产品是否满足域名日常运维需要
测试步骤	日常运维使用
测试结果	****： 添加：支持批量及单独添加 修改：可直接修改域名值，但是如果修改解析类型，需要删除新建，下一个版本能支持 删除：支持批量及单独删除 TTL 修改：支持批量修改 **： 添加：支持批量及单独添加 修改：可直接修改域名解析类型及值 删除：支持批量及单独删除 TTL 修改：支持批量修改 ****： 添加：支持批量及单独添加 修改：可直接修改域名值，但是如果修改解析类型，需要删除新建 删除：支持批量及单独删除 TTL 修改：支持批量修改

3.1.7 是否支持 A、AAAA、CNAME、NS、MX、泛域名、TXT 等解析类型

测试项	是否支持 A、AAAA、CNAME、NS、MX、泛域名、TXT 等解析类型
测试目的	考察产品是否满足域名日常运维需要
测试步骤	将现有域名系统的解析记录类型导入测试系统中进行测试
测试结果	****:支持 **：支持 ****：支持

3.1.8 恶意域名拦截

测试项	挖矿行为探测、威胁域名探测
测试目的	验证产品是否支持挖矿行为及威胁域名拦截
测试步骤	对全校用户开启挖矿行为及威胁域名拦截功能，测试时间为一周
测试结果	****（8.26-9.1）： 1. 策略设置：数字货币、proxy 代理、被黑网站/病毒木马、恶意网站、僵尸网络、自定义情报、TOR 节点、垃圾邮件、恶意软件、色情、钓鱼网址、C&C 节点、勒索软件、赌博、恶意软件下载链接 2. 共拦截 151183 次，威胁域名 1695 个，失陷终端 12875 个 3. 可导出 pdf 报表 **（6.16-6.22）： 1. 策略设置：挖矿木马、网络钓鱼、垃圾邮件、恶意软件、病毒木马、APT、C&C 节点、僵尸网络、色赌毒、勒索软件、挖矿木马、网络犯罪 2. 共拦截 143360 次，威胁域名 729 个，失陷终端 22241 个 3. 可导出 pdf 报表 ****（9.6-9.12）： 1. 策略设置：色情、赌博、垃圾邮件、钓鱼网址、勒索软件、僵尸网络、恶意软件、C&C 节点、扫描器节点、TOR 节点、proxy 代理、Web 攻击、数字货币、恶意软件下载链接、恶意网站

	2. 共拦截 150055 次，威胁域名 3486 个，失陷终端 150415 个 3. 不能导出 pdf 报表，需要手工计算

3.1.9 与出口防火墙联动智能选路

测试项	与出口防火墙联动智能选路
测试目的	验证产品与出口防火墙联动智能选路
测试步骤	1.通过 snmp 协议联动读取出口防火墙流量数据，判断带宽占用比例 2.流量超过出口带宽 80%，切换为其他转发策略，减少向某一线路出口的递归转发，下一个检测周期检测到出口带宽占比下来后，就重新调整为原递归转发策略
测试结果	****:支持 **：支持 ****：支持

3.1.10 QPS 统计

测试项	QPS 统计
测试目的	性能监控
测试步骤	在管理后台查询 QPS 数据
测试结果	******：** **能查询到历史 QPS 记录，最高为：7636** **： 能查询实时 QPS 数据，查询不到历史数据 ****： 能查询到 30 天内的 QPS 数据，最高 6111 导出 qps 数据导致管理界面崩溃（原来 8 核 cpu，增加至 32 核 cpu）

3.1.11 日志查询

测试项	日志查询

测试目的	日常管理中日志查询
测试步骤	查询解析日志（请求、成功、失败）、审计日志、运行日志、操作日志
测试结果	******：** **1. 操作管理日志、审计日志可以保存 180 天，满足网络安全法要求。** **2. 解析日志中能查询到解析用时** **： 1. 操作管理日志、审计日志可以保存 180 天，满足网络安全法要求。 2. 解析日志中查询不到解析用时 ****： 1. 操作管理日志、审计日志可以保存 180 天，满足网络安全法要求。

3.1.12 统计僵尸域名

测试项	统计僵尸域名情况
测试目的	考察产品是否可以统计僵尸域名
测试步骤	在管理界面查看权威域名解析情况，一段时间（例如 6 个月）解析量为 0，被判定为僵尸域名
测试结果	****: 不支持，下一个版本能支持 ****：** **能统计近半年的域名解析情况，统计出僵尸域名，可导出报表** ****： 目前版本没有（可人工在后台执行命令查询），下个版本有

3.1.13 短期域名自动禁止解析

测试项	短期域名自动禁止解析
测试目的	用于短期域名管理
测试步骤	新建测试域名，设置有效截期

测试结果	****：到期可选禁用或删除 **：到期后停用不删除 ****：到期直接删除，查不到删除记录

四、 售后服务

	****	**	****
是否有本地售后	**有**	**有**	无（在沈阳）

五、 用户案例

	****	**	****
厂商提供的用户案例数量	**505（教育行业）**	62（教育行业）	32

六、 硬件资源占用情况

	****	**	****
硬件资源占用	**每台虚拟机占用 8 核 CPU、32G 内存**	每台虚拟机占用 32 核 CPU、32G 内存	每台虚拟机占用 32 核 CPU、16G 内存

七、 总体评价

7.1 ****

产品情况：重点测试功能全部满足。测试期间未发生系统崩溃、服务中断等情况。产品功能有一些不足需要改进：1.修改域名的类型由 A 改为 CNAME，需要先删除再新建，不能无缝修改。2..不能统计所有权威域名的解析数据，实现不了僵尸域名的定期统计。

7.2 **

产品情况：重点测试功能全部满足。测试期间未发生系统崩溃、服务中断等情况。产品功能有一些不足需要改进：1.查询不到 QPS 历史数据。2.解析日志中查询不到解析用时。

7.3 ****

产品情况：重点测试功能全部满足。在测试期间，发生过在导出 qps 数据过程中，管理界面崩溃。产品功能有一些不足需要改进：1.短期域名到期直接被系统删除，查询不到删除的是哪个域名。2.查询不到实时解析日志，需自定义搜索。3.本版本不能统计所有权威域名的解析数据，实现不了僵尸域名的定期统计。4.DNS 安全统计不能导出 pdf 报表，需要手工计算。

八、测试结论

综合产品功能、系统完善程度、系统稳定性、售后服务、客户案例、硬件资源占用等方面，本次测试得出的购买顺序为：****、**、****