华域 DNS 安全接入网关 技术白皮书

摘要

该文档阐述了深圳华域通信技术有限公司(Shen Zhen Huau Communication technology Co., Ltd.)的荣誉产品华域 DNS 安全接入网关产品的需求、特点和应用，欢迎垂询。

文档密级：公开

公司名称：深圳华域通信技术有限公司
服务电话：400-6996-601
服务邮箱：service@huautech.com
公司网站：www.huautech.com

文档更改记录

版本	修改内容描述	修改人	日期	备注
1.0.0	建立白皮书	王翔宇	2023 年 4 月 28 日	
1.0.1	补充威胁域名说明和其它部分	金帅超	2023 年 7 月 18 日	
1.0.2	修改内容措辞和错误	金帅超	2023 年 8 月 18 日	
1.0.3	优化内容和增加 RFC 协议	王翔宇	2023 年 8 月 31 日	
1.0.4	更新拓扑图	金帅超	2023 年 9 月 4 日	

版权信息

文档保证声明

注意

由于产品版本升级或其它原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

联系方式

公司地址：深圳市福田区福田街道福南社区福虹路 9 号世贸广场 A 座 1902-1B

电话：400-6996-601

服务邮箱：service@huautech.com

公司网站：www.huautech.com

目录

一、公司简介

深圳华域通信技术有限公司是一家专注于域名系统、网络应用优化的高科技互联网公司。公司研发团队紧贴用户实际需求，立足“开放、创新、安全”的产品理念，立志为用户打造更加科学、高效、便捷、安全的网络优化解决方案。

二、产品介绍

2.1. 产品需求

2.1.1. DNS 安全标准推广

随着网络发展日益迅速，网络安全日益完善，Web 服务得到快速发展，其安全标准也得以大力推广，而核心服务之一的 DNS 服务，其安全标准发展却相去甚远。

根据国际知名网络安全机构 Efficient IP 与 IDC 合作发布的《2022 年全球 DNS 威胁报告》指出，在过去一年中，88%的组织遭受了与 DNS 相关的攻击，平均每家公司有七次，其中包括 DNS 隧道、DDoS 攻击、DNS 劫持和云配置错误滥用等技术手段，与上一年相比，所有类别的攻击频率都有所增加，尤以 DNS 劫持最为显著。

无论是 519 事件、百度域名劫持事件，还是近期热门的路由器 DNS 劫持事件，都与 DNS 使用过程中，管理人员缺乏对 DNS 安全标准的认知有关。DNS 安全标准的认知不仅限于 DNS 安全加固，还包括更多深层次要求，如相关软硬件信息屏蔽、服务区域锁定、自动化动态策略等等。

随着互联网技术飞速发展，物联网、云服务、超融合、元宇宙等新概念层出不穷，无论何种新兴网络技术发展均离不开 DNS 安全标准的有力支持！

2.1.2. DNS 防护策略变化

2021 年 9 月，国家发展改革委等 11 部门联合发布《国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知》，互联网恶意域名防护再次受到重视，DNS 安全防护再一次受到全民关注。


中华人民共和国中央人民政府
www.gov.cn

国务院 | 总理 | 新闻 | 政策 | 互动 | 服务 | 数据 | 国情 | 国家政务服务平台

首页 > 政策 > 国务院政策文件库 > 国务院部门文件

标　题：	国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知	发文机关：	国家发展改革委 中央宣传部 中央网信办 工业和信息化部 公安部 财政部 人民银行 税务总局 市场监管总局 银保监会 国家能源局
发文字号：	发改运行〔2021〕1283号	来　源：	发展改革委网站
主题分类：	财政、金融、审计\货币（含外汇）	公文种类：	通知
成文日期：	2021年09月03日	发布日期：	2021年

【字体：大 中 小】

国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知

发改运行〔2021〕1283号

各省、自治区、直辖市人民政府，新疆生产建设兵团：

为有效防范处置虚拟货币“挖矿”活动盲目无序发展带来的风险隐患，深入推进节能减排，助力如期实现碳达峰、碳中和目标，现就整治虚拟货币“挖矿”活动有关事项通知如下：

近年来，随着降费提速、限定区域、认证入网、“挖矿”防护等各种新政策及事件的出现，导致 DNS 使用环境及方式发生了极大变化。传统单一的 DNS 服务已经跟不上用户网络环境变化速度，对 DNS 安全防护策略的要求也越来越高，通过网络设备策略或 DNS 服务器自身限制等防护方式已经不能满足网络安全要求。

DNS 相关漏洞出现，无法及时更新，如何实现 DNS 防护？

多个 IP 地址，具有特定字段的 DNS 正常请求，大量攻击 DNS，如何实现 DNS 防护？

认证入网环境中，不同身份人员网络出访，如何实现 DNS 基于身份信息链路优化指向？

多出口网络环境下复杂的流量调度策略，如何完成 DNS 服务有效配合？

上述问题在网络环境多样化的今天十分常见，怎样完成 DNS 全方位防护以及策略自动调度变化，这是摆在管理人员面前的一道难题。

2.1.3. DNS 数据信息加密

DNS 劫持是目前网络攻击中最常见且最有效的攻击方式之一，其原理是伪造虚假响应欺骗客户端去访问恶意网站或重定向到事先预设好的钓鱼网站，趁机下载恶意代码到客户计算机并攫取客户个人信息。

默认情况下，DNS 查询和响应以明文形式（UDP 或 TCP）发送，这意味着它们可以被网络、ISP 或任何能够监视传输的人读取。

如何有效防止以上情况发生？最优解就是将 DNS 数据进行加密，DNS 数据加密是 DNS 安全发展的必然趋势，但当前环境下多数 DNS 不能加密数据信息。

2.1.4. 威胁域名拦截

近年来西方敌对势力组建的网络部队、黑客组织、民间极端团体以网络精准打击破坏国家机关、军队、企业数据，窃取加密数据勒索赎金作为主要目的，对我国带来了以下方面的严重威胁：

1）数据安全：引起数据泄密、数据公开，威胁商业、科研秘密。

2）生产经营：扰乱生产经营秩序，导致生产产量和产品质量的下降，直接影响发展；

3）公共安全：引发严重的生产设施损害、环境灾难、人员伤害等公共安全危机。

4）国家安全：泄漏国家战略产业、设施、物资的布局、生产、储备等秘密。

DNS 是攻击行为经常利用的中间途径，因此，提高 DNS 对威胁域名的发现、拦截为网络安全的重中之重。

2.1.5. DNS 安全事件审计

在当前网络信息安全事故频发情况下，网络管理人员越发意识到网络安全的重要性，网络环境也出现了越来越多的网络安全产品，但是针对 DNS 服务，DNS 安全事件排查仍处于大海捞针水平，即从海量日志信息中进行筛选，缺乏具有针对性的专项记录和审计，DNS 日志数据安全操作记录更是一片空白。一旦出现运维事故，难以进行回溯追责。

2.2. 产品目标与特性

华域智能 DNS 安全接入网关以 DNS 安全标准为基础，以零信任为设计理念，规范 DNS 使用方式，提供网络、应用、数据、日志等全方位防护，帮助客户完成符合 DNS 安全标准的服务升级，满足 DNS 服务的智能化流量调度，威胁域名拦截，多重策略防护，数据安全加密，深层安全事件记录及告警等多样化需求，快速实现 DNS 安全加固与技术更新，加速互联网 DNS 安全标准的普及。具体特性包括：

2.2.1. 安全性

华域智能 DNS 安全接入网关从底层系统核心、安全模块和硬件兼容性等各个层次进行了精心的设计和优化，支持威胁情报订阅拦截，支持缓存投毒（0x20）检测与抵御，从系统底层支持使用随机端口向外递归、头部 ID 字段随机，支持设置黑白名单防劫持，保证 DNS 业务的高可靠和安全性，提供运营商级的 DNS 服务，为企业构建安全的 DNS 架构。

2.2.2. 高可靠性

具有更高容错能力，支持多机负载以及热备功能，保证 7x24 小时不间断提供服务。

2.2.3. 可扩展性

随着基于 IP 新业务（云计算、虚拟化等）的增长和 IPv6 应用普及，跨多业务需求越来越多，产品实施开放性原则，方便与其他不同厂商网络设备进行联动，各种协议和接口均符合国际标准。

2.2.4. 模块化管理

华域智能 DNS 安全接入网关，单台设备即可满足中小型企业单位需求。面对大型企业，可以通过独有的集群及模块化方案，满足跨地域、复杂网络环境下的统一部署、集中管理需求。

2.2.5. 易用性

系统采用统一的 GUI 配置界面，同时每项配置均有内容提示，使得操作简单易上手。同时我们提供全面的产品文档和全方位的技术支持服务，以协助管理员对系统进行实施与维护。

2.2.6. 通用性

符合国际标准：RFC-1034、RFC-1035、RFC-1123、RFC-1536、RFC-1886、RFC-1995、RFC-1996、RFC-2136、RFC-2181、RFC-2308、RFC-2317、RFC-2535、RFC-2541、RFC-2671、RFC-2782、RFC-2845、RFC-2930、RFC-3596、RFC-3645、RFC-3646、RFC-4033、RFC-4034、RFC-4035、RFC-7766、RFC-7858、RFC-7873、RFC-8484。

2.3. 特点介绍

2.3.1. 权威递归分离

华域智能 DNS 安全接入网关在 DNS 安全标准基础上，结合用户实际网络环境，针对 DNS 服务进行合理规划，定义 DNS 安全策略，规范各种网络环境下 DNS 使用方式，保证其安全、稳定地运行。安全隔离内外网用户的 DNS 解析业务，避免因权威、递归一体化情况下的递归业务面临安全风险，防止 DNS 遭遇外

网攻击导致递归解析异常，防止 DNS 面临内网攻击导致权威解析失效。

2.3.2. 安全升级

华域 DNS 安全接入网关针对域名、IP、缓存、软硬件等条件进行标准化控制，通过对网络、系统、服务、数据、日志等方面的全面防护，实现深层次 DNS 服务的安全加固，大幅提升 DNS 安全防护级别。

图 1 全面防护

2.3.3. 威胁域名拦截

DNS 是各种危险木马、病毒等攻击常见的涉及对象，华域 DNS 系统内置业界最先进的 DNS 威胁情报订阅服务，威胁域名数据具有多种来源，包括自主采集验证、国家安全应急中心、教育科研网、合作安全厂商、网络安全威胁情报联盟等等，可实现包括：C&C 节点、恶意网站、数字货币、恶意软件、赌博、 钓鱼网址、 垃圾邮件、色情网站、僵尸网络等恶意域名的访问检测、拦截、封禁、分析等。

系统提供恶意域名库模块接口，支持与第三方机构（如安全厂商、管理平台）对接，帮助客户实现恶意域名自动化防护。

图 2 恶意域名来源

2.3.4. 智能调度

华域智能 DNS 安全接入网关能够根据网络环境特点，实现以源地址、出口链路、用户身份、终端应用等多种方式的流量调度，结合时间、安全等多种策略，完成 DNS 智能化管理。

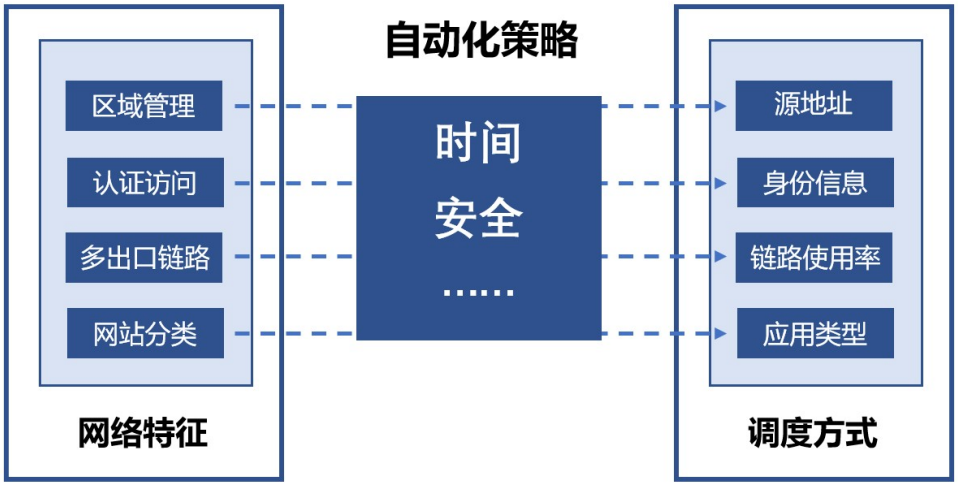


图 3 智能调度

2.3.5. 缓存窥探

华域智能 DNS 安全接入网关能够通过修改 DNS 缓存信息，有效防止“DNS 缓存窥探”。DNS 缓存窥探是当有人查询 DNS 服务器，以找出“窥探”，如果 DNS 服务器缓存了特定 DNS 记录，从而推断 DNS 服务器的所有者 (或其用户) 最近访问了特定站点。这可能会显示有关 DNS 服务器所有者的信息，例如他们使用的供应商、银行、服务提供商等，特别是在一段时间内多次“窥探”确认这一点。“DNS 缓存窥探”甚至可用于收集统计信息，例如，DNS 服务器的所有者通常在什么时间访问他的网库等。缓存 DNS 记录的剩

余 TTL 值可以提供非常准确的数据。

2.3.6. 信息校验

华域 DNS 安全接入网关针对权威、递归两个方面进行信息校验。权威方面，比如域名记录配置是否符合标准，备案信息完整性情况如何，是否存在多余的无效域名；递归方面，如稳定运行情况下某网站解析结果突然出现变化，域名 Whois 反查信息是否属于合规公司，有 CDN 业务网站解析结果比对等等。有效避免稳定运行网络环境下域名劫持、缓存污染等情况出现。

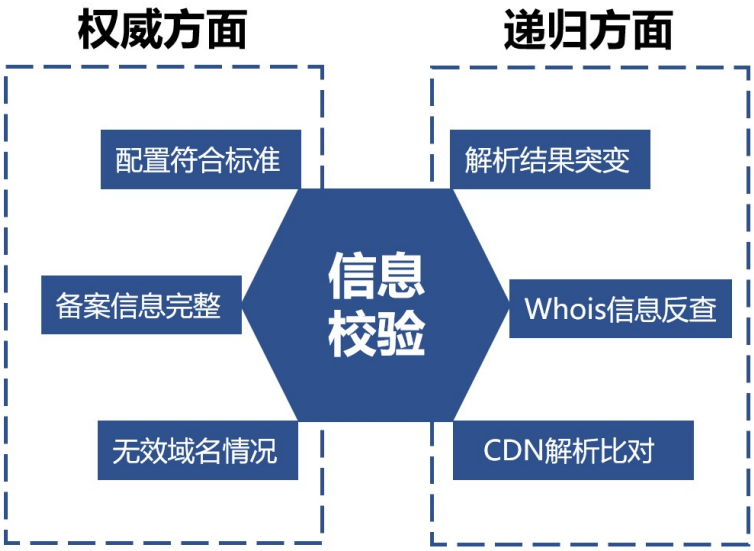


图 4 信息校验

2.3.7. 多递归回源

华域 DNS 安全接入网关支持设置多递归回源 DNS，支持负载均衡算法，可实现多递归回源动态负载，且系统支持设置备用回源 DNS，实现在一级回源 DNS 不可用情况下，自动使用备用回源 DNS，保障 DNS 业务可靠性。

2.3.8. 事件记录

华域 DNS 安全接入网关全面记录安全事件，提供多层次安全报表。不仅包括威胁域名、常见攻击、异常请求等基础安全报表，还包括针对 DNS 服务的异常通信报表，如数据上传下载、非 DNS 协议通信等等，同时对于日常管理中可能出现的异常操作、配置安全的异常行为报表，如导致 DNS 业务失效的配置行为、DNS 数据调用行为、日志信息推送动作等等。

图 5 多层次报表

2.3.9. 监控告警

DNS 服务作为网络重要基础服务之一，不间断地提供可靠性服务非常重要。华域 DNS 安全接入网关实时监控 DNS 服务状态，聚焦 DNS 安全防护，针对不同级别安全事件，提供邮件、电话、短信、微信等多种告警方式，帮助管理人员掌握 DNS 状态，加固 DNS 安全。

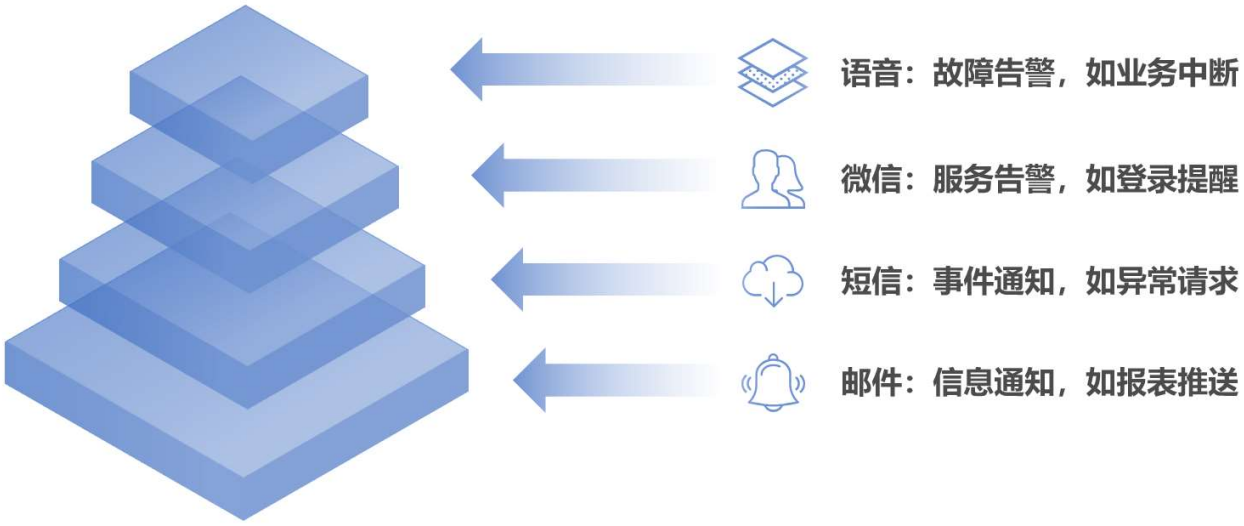


图 6 分类告警

2.3.10. 数据加密

由于传统 DNS 协议形成于互联网早期，直接基于 UDP 或 TCP 协议，未虑及现代安全性的需要，未利用密码学等手段进行加密或验证。因而，其无法抵御现代互联网常见的 DNS 投毒污染等攻击手段或非法监听。

华域 DNS 安全接入网关通过数据加密技术为 DNS 协议提供可靠性传输方式，有效防止 DNS 在查询过

程中出现 DNS 投毒、污染、劫持及恶意篡改等情况。在 DNS 数据加密情况下，只有 DNS 安全接入网关才能完成 DNS 数据包级别监控，其它产品均无法获取 DNS 数据包信息。

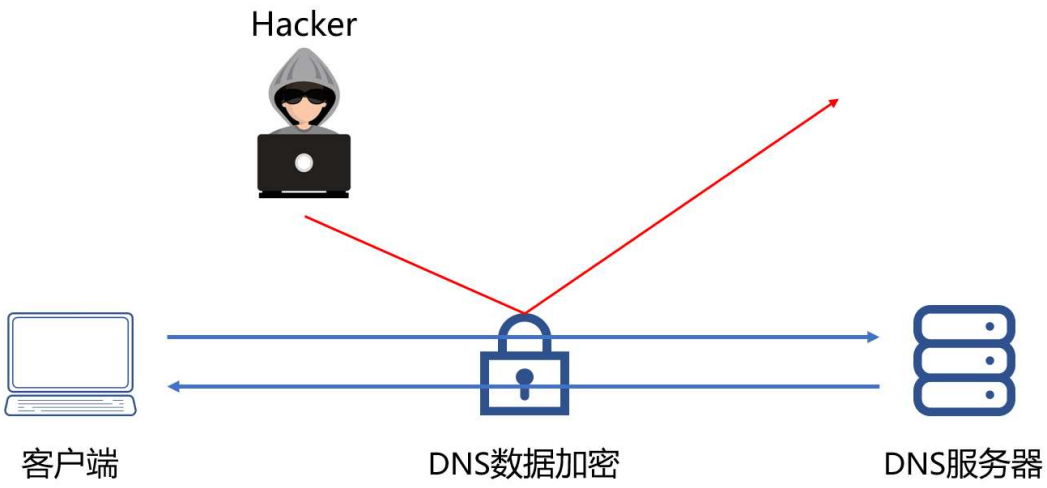


图 7 数据加密

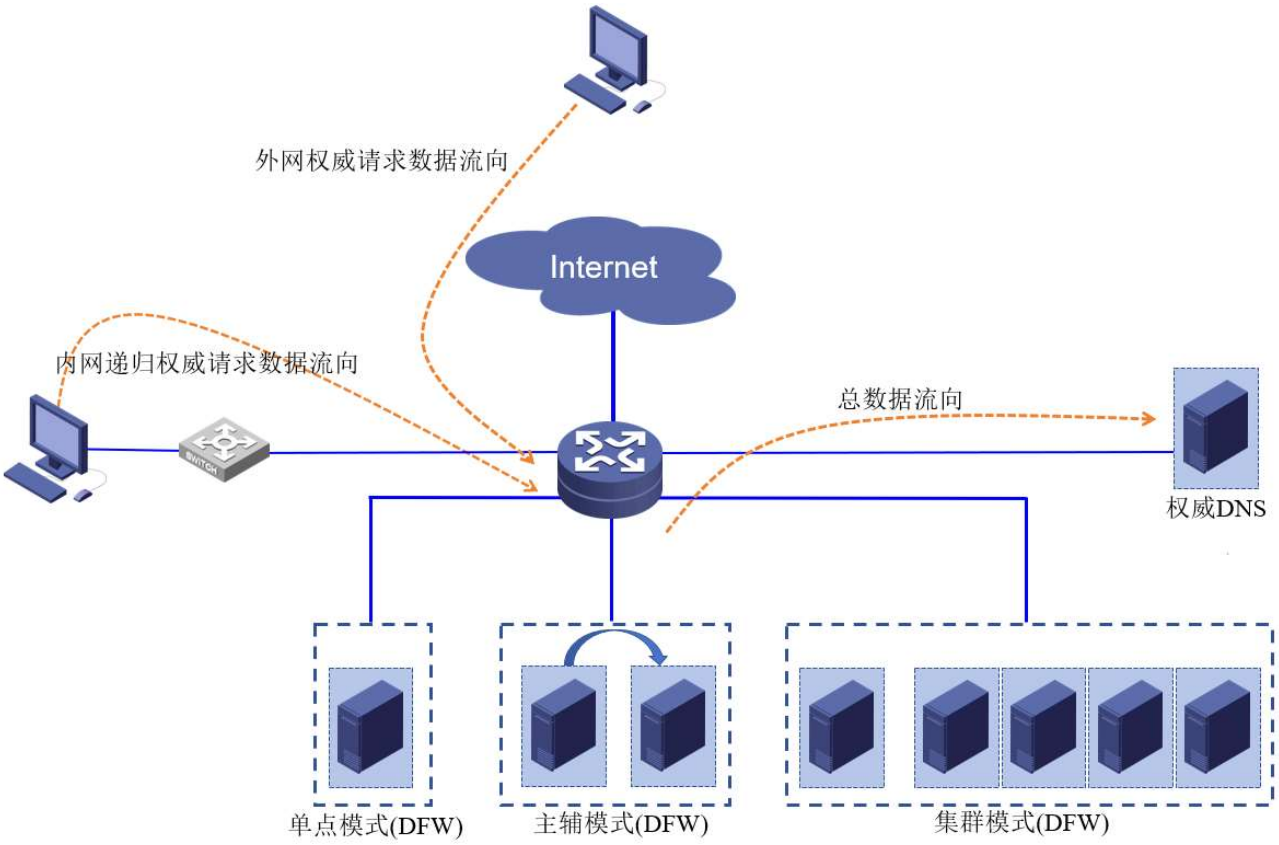
2.3.11. 技术革新

1983 年 DNS 技术诞生，为互联网发展至今奠定了基础。如今 DNS 已成为网络世界中不可或缺的一部分，上网第一个请求的服务就是 DNS 服务，因此对 DNS 的安全性和稳定性都提出了极高的要求。

华域 DNS 安全接入网关实现针对 DNS 服务的全方位、多类别数据管控，包括域名、IP、数据包等，支持 DNS 服务策略调度，包括时间、源地址、目标地址等，各种功能均服务于 DNS 服务的安全和稳定，同时系统支持 DNSSEC、DoT、DoH 等 DNS 技术，为各种 DNS 提供合理的技术升级方式，全面实现 DNS 服务的技术革新。

2.4. 系统部署

华域 DNS 安全接入网关支持灵活的部署方式。可以根据不同需求进行各种方式部署。整体部署方式图如下：



2.4.1. 单点模式

在网络中部署一台 DNS 安全接入网关做域名解析服务器，此种模式适合于中小型网络规模，可有效实现权威递归分离，拦截危险域名，保障域名解析服务。

2.4.2. 主辅模式

DNS 设备承担着核心网络服务的职能，业务的稳定性、可用性非常重要。当网络中的设备出现故障后，需要高效恢复业务。为更好的保证域名解析服务，通常网络中都会配置两台或两台以上的 DNS 安全接入网关做主辅域名解析服务器，所有数据均采用自动同步方式保证服务一致性。华域 DNS 安全接入网关在主辅模式下辅机可与主机同时平均分配解析负载。

2.4.3. 集群模式

在大型和超大型网络中，主辅模式和主备模式已经不能灵活、稳定的对外提供业务。这时通常会采用集群模式将多台设备集中起来提供服务，来获得更高的计算速度，而在客户端看来就像是只有一个服务器。