Split Horizon DNS 的原理与实现

黄京

Jul 09, 2025

现代网络环境中普遍存在一个核心矛盾：内部服务需要通过私有 IP 地址访问，而公网用户则需要访问公网 IP。这种双重访问需求常见于企业 OA 系统、家庭 NAS 等场景。同时，安全层面要求隐藏内部拓扑结构，例如数据库服务器或管理后台的真实地址。Split Horizon DNS 正是为解决此类问题而生的技术方案，其核心定义是根据 DNS 请求的来源 IP 返回不同的解析结果，实现「同一域名，内外网解析差异化」的目标。

1　核心原理剖析

DNS 查询遵循「发起请求 → 递归解析 → 权威应答」的标准流程。在 Split Horizon DNS 的实现中，请求源 IP 成为关键判断依据。当客户端发起 DNS 查询时，DNS 服务器会检测该请求的源 IP 地址是否属于预设的内网地址段。这一判断触发差异化响应机制：若请求来自内网，则返回私有 IP；若来自公网，则返回公有 IP。
技术实现主要依赖三种机制：首先是视图（View）技术，以 BIND 为例，通过配置不同视图区块实现基于源 IP 的解析隔离。其次是策略路由，借助防火墙或路由器对 DNS 请求进行标记与转发。最后是分离式 DNS 服务器架构，通过物理隔离的两台 DNS 服务器分别处理内外网请求。这三种方式在实现成本、维护复杂度上存在显著差异。

2　主流实现方案详解

2.1　BIND 实现方案

作为最经典的 DNS 服务软件，BIND 通过视图功能实现分离解析。以下配置示例展示了典型的内外网视图划分：

```
view "internal" {
   match-clients { 192.168.0.0/24; }; // 仅匹配内网 IP 段
   zone "example.com" {
      type master;
      file "internal.example.com.zone"; // 指向内网专用解析文件
   };
};
view "external" {
   match-clients { any; }; // 匹配所有其他请求
   zone "example.com" {
      type master;
```

```
        file "external.example.com.zone"; // 公网解析文件
    };
};
```

此处 match-clients 指令定义视图的生效范围，其 CIDR 格式的 IP 段需严格匹配内网规划。view 区块的声明顺序具有优先级特性，系统将按配置文件中的顺序进行视图匹配。调试时可使用 named-checkconf 验证配置语法，通过 rndc querylog 动态开启查询日志观察匹配过程。

2.2 Windows Server 实现方案

在 Windows Server 环境中，主要通过条件转发器（Conditional Forwarder）实现分离解析。管理员可在 DNS 管理器图形界面中，为特定域名指定转发到内部 DNS 服务器的规则。当与 Active Directory 域控集成时，此方案能自动处理域内设备的动态注册。配置路径为：DNS 管理器 → 条件转发器 → 新建基于 IP 段的转发规则 。

2.3 云服务方案

AWS Route 53 通过私有托管区域（Private Hosted Zone）实现 VPC 内部的专属解析。该区域仅对关联的 VPC 生效，外部请求无法获取其记录。Azure DNS 的类似功能称为私有 DNS 区域。云服务的特殊优势在于可与路由策略联动，例如根据请求来源的地理位置（Geolocation）返回不同结果。但需注意这并非严格的内外网分离，而是更细粒度的地域划分。

2.4 轻量级替代方案

对于简单场景，Dnsmasq 可通过 --server 指令指定内网域名的解析路径，例如 dnsmasq --server=/internal.example.com/192.168.1.53 将所有对该域名的查询转发至内网 DNS。而 Hosts 文件修改作为本地临时方案，存在维护成本高、无法集中管理的明显缺陷。

3 典型应用场景

在企业网络架构中，erp.company.com 域名对内解析至内网服务器 192.168.1.100，对外则指向公网负载均衡器 VIP 203.0.113.5。混合云场景下，本地数据中心与云 VPC 通过 DNS 策略共享服务发现机制，实现无缝迁移。家庭实验室用户可为自建 NAS 配置内网直连（如 192.168.1.200），外网访问则通过 DDNS 指向动态公网 IP。

4 安全性与常见陷阱

安全加固的首要措施是关闭递归查询（recursion no;），防止内部 DNS 被外部滥用。同时需限制区域传输权限：allow-transfer { none; }；可阻断未授权的区域数据同步。配置中常见的错误包括视图顺序颠倒导致匹配失效，例如将 any 匹配的视图置于特定 IP 段视图之前。另一个典型问题是缓存污染：内网 DNS 服务器缓存了外网解析记录，可通过设置 max-cache-ttl 缩短缓存时间缓解。在部署 DNSSEC 时，需确保内外网区域的签名密钥一致性，否则会导致验证失败。

5 进阶：与其他技术联动

与负载均衡器结合时，内网解析直接返回真实服务器 IP（如 10.0.1.12），外网则返回 SLB 的虚拟 IP（如 203.0.113.88）。在动态 DNS 更新场景中，DHCP 客户端可自动向内网 DNS 注册记录，Windows AD 环境通过安全动态更新实现此功能。容器化场景下，CoreDNS 的 `view` 插件可实现 Kubernetes 集群内的分离解析，配置示例如下：

```
.:53 {
    view cluster.local {
        expr type() == 'A'
        rewrite stop {
            name regex (.*)\.cluster\.local {1}.default.svc.cluster.local
            answer name (.*)\.default\.svc\.cluster\.local {1}.cluster.local
        }
        forward . 10.96.0.10
    }
    view external {
        forward . 8.8.8.8
    }
}
```

该配置实现了 `cluster.local` 域名的专用解析链，外部域名则转发至公共 DNS。其中 `rewrite` 模块进行域名重写，保持内部域名的访问一致性。

Split Horizon DNS 的核心价值在于平衡网络安全性与访问体验。中小企业可选择 Windows DNS 或 BIND 作为基础方案，云原生架构则更适合采用 Route 53 或 Azure DNS 等托管服务。未来发展趋势将聚焦与零信任网络（SDP）的深度集成，同时 DoH（DNS over HTTPS）和 DoT（DNS over TLS）的普及带来了新挑战：加密传输使得传统基于 IP 的来源识别更加困难。

> 您的企业如何实现内外网解析分离？欢迎在评论区分享实践案例与挑战。