# DNS 安全防护

DNS 协议在设计之初就只注重其可用性，忽视其安全性，而由于协议的重要性和特殊性，几乎所有的技术防御措施都允许 DNS 协议类型数据报文不受限制的传输。随着时间的推移，DNS 暴露出越来越多的安全问题。

DNS 在整个互联网体系中处于入口的重要位置，近年来利用或针对 DNS 的网络攻击呈愈演愈烈之势。近 91.3%的已知恶意软件被发现使用 DNS 作为通讯手段，但 68%的企业却忽略了这个问题，并没有对 DNS 解析进行监测，思科将这种现象称之为“DNS 盲点”。根据收集到的信息也表明，在城域网级别的 DNS 流量中，大约有万分之一到万分之五的 DNS 访问是恶意的。

无论是办公网、生产网，无论是服务器、桌面终端、移动终端、I0T 设备，无论是勒索病毒、挖矿病毒、蠕虫病毒、僵尸网络还是 APT，只要攻击者利用了 DNS 系统，基于 DNS 的威胁安全检测方案都可以检测发现。DNS 安全防护系统，从根本上解决内网 DNS 安全和外网 DNS 安全，通过 DNS 安全防火墙可以阻止数据泄露，阻止访问恶意网址等行为。

DNS 安全防御立足于 DNS 协议特点，打造 DNS 协议防护平台，通过多层次、预先集成的防护策略，防护各种 DNS 攻击行为。并且与威胁情报厂商合作，具备基于威胁情报的访问阻断能力。当发现威胁访问时停止解析，从而阻断威胁对外连接，切断敏感信息对外泄漏的途径，保护客户的信息安全。

**威胁情报全面、准确**

联合威胁情报厂商在 DNS 数据之上开展了各种安全分析和应用探索，覆盖 DNS 相关的各个安全视角。内置 DNS 威胁情报库，同时提供恶意域名 API 接口，可以和情报威胁厂商、态势感知厂商进行接口联动，满足客户的需求。---*过 RPZ（DNS Response Policy Zones）技术重定向、封禁或丢弃特定的 DNS 解析请求，用于限制用户访问某些网站等或防止用户访问 Internet 一些恶意网站等，并支持与第三商业机构提供的 RPZ 进行对接，或支持自定义 RPZ 恶意域名或域 list 名单。*

基于威胁情报的 DNS 安全防护的技术优势:

- DNS 解析请求与威胁情报实时碰撞，高效发现恶意访问威胁;
- 威胁情报提供恶意域名情报类型丰富，可直观发现恶意访问的威胁类型;
- 可针对威胁情报类型和信誉等级，自定义处置策略(告警/阻断);
- 威胁情报数据实时更新，保证恶意域名情报库的实时性。

安全防护配置方式

1. 在 DNS 安全管页面通过添加域名库或者通过 API 关联第三方特征库，包括 360、深信服、天融信等。
2. 设置规则策略，通过规则策略对添加的域名进行规则匹配。
3. 规则关联 DNS 解析，触发响应操作。

RPZ防火墙设置

网站信息：　www.oki.com

触发操作：

安全厂商：

域名不存在
存在无响应
不启用策略
强制TCP
丢弃
域名劫持

开启设置

RPZ防火墙开启

配置　取消