PDNS（Protective Domain Name Service）

PDNS介绍

域名系统（Domain Name Syetem，DNS）是从根服务器到顶级域名服务器再依次向下的分布式管理系统，用于识别通过互联网或其他互联网协议（IP）可访问的计算机、服务和其他资源，将人类容易记忆的域名（baidu.com）转换为计算机可识别的 IP 地址。

但 DNS 既可用于合法寻找互联网资源，也可被攻击者进行恶意利用，几乎在网络运营的所有范围内，都是用域名，如图 1 所示。

图1：从网络钓鱼，恶意链接到利用常见网址拼写错误的虚假 URL，域名在多维度易遭受网络攻击

因此，如何确定发往 DNS 的请求是合法的、可疑的亦或是恶意的，是亟待解决的问题。在此背景下，PDNS 应运而生。PDNS 的设计是为了阻止恶意攻击者对 DNS 的利用，极大的增强了 DNS 的事件检测和响应能力，进而提升互联网基础设施的安全性。主要有如下特性：

1. **更大的覆盖范围：**PDNS **以设备为中心**，保护组织网络和独立设备，而不考虑设备或网络的未知位置，此特性为更多设备提供了更强的安全性，同时也具有更大的覆盖范围。另外，除了传统的未加密 DNS:53 的流量之外，该服务还支持IPv6和IPv4上的现代协议，如加密 DNS（DOT,DOH）。
2. **更广的威胁情报来源：**PDNS 基于已有的威胁情报来对设备进行保护，PDNS 的威胁情报来源广泛，包括政府机构、企业合作伙伴等多方的非机密威胁情报。
3. **更高的实时性：**一旦发现潜在的恶意 DNS 请求时，PDNS 利用应用程序编程接口向相关机构进行提醒，提高了早期响应能力，防止安全隐患。
4. **更强的可见性和可访问性：**PDNS 允许相关部门通过直观的网络应用程序访问记录和威胁趋势，进而识别常见威胁和潜在目标，以便采取进一步的行动和进行威胁搜寻。
5. **零信任架构：**根据零信任概念（*零信任模型认为，主机无论处于网络的什么位置，都应当被视为互联网主机。它们所在的网络，无论是互联网还是内部网络，都必须被视为充满威胁的危险网络*），PDNS 保护以前难以保护的设备，如移动、代理和路由设备等。

工作原理

PDNS 的一个核心功能是根据威胁情报对域名进行分类，威胁情报的来源通常包括已经开源的恶意域名信息、商业和政府信息等，威胁情报的质量和覆盖面，往往决定着 PDNS 对恶意域名分类和过滤的效果，通常会分为以下几类：

1. **网络钓鱼：**托管恶意收集个人或组织信息的应用程序的网站。这些域名（例如，针对 baidu.com，恶意攻击者可能会抢注 ba1du.com 域名【仅仅是举例】，进而达到混淆视听的作用）往往被恶意攻击者抢注，和真实域名非常相似，正常用户因为视觉差异或者手误等原因，访问到恶意域名，PDNS 可以保护用户免受此类潜在威胁。
2. **恶意网站的跳转和转发：**提供恶意内容或被恶意攻击者控制用来触访问发恶意软件的网站。例如，托管恶意 JavaScript 文件的网站或托管广告的域名，PDNS 可以终止已知的恶意连接尝试。
3. **域名生成算法：**部分恶意软件使用程序生成域名来规避静态检测。网络威胁行为者使用恶意软件的域生成算法（DGA），通过根据预设种子以编程方式生成域名，绕过静态阻止（通过域名或IP）。PDNS 可以通过分析每个域名的文本属性并标记与已知 DGA 属性相关的属性（如高熵）来提供对恶意软件 DGA 的保护。
4. **恶意内容的筛选和过滤：**网站内容属于违反组织访问策略的特定类别的网站。PDNS 可以使用各种域名用例的分类（例如，“赌博”），并警告或阻止那些在给定环境中被视为风险的域名。

注册和使用

所有政府机构或者和政府机构相关的实体单位均可以注册并使用 PDNS。对于使用 CITEC 管理的 DNS 服务器，会自动启用 PDNS，没有使用 CITES 管理的 DNS 服务器，可以注册使用 PDNS，步骤非常简单，确保要保护的设备具有 IP 地址，并直接在线申请。

相关文献

1. Selecting a Protective DNS Service.
2. PROTECTIVE DOMAIN NAME SYSTEM (DNS) RESOLVER SERVICE.
3. A Guide to Protective DNS Security.
4. DNS Hosting, Resolution and Protection.
5. https://www.ncsc.gov.uk/information/pdns.
6. https://www.iboss.com/solution-briefs/ncsc-protective-dns/
7. https://umbrella.cisco.com/blog/protective-dns-what-it-is-why-it-matters-and-what-you-need
8. https://www.dnsfilter.com/blog/protective-dns-overview

9. https://www.infoblox.com/dns-security-resource-center/dns-security-faq/what-is-protective-dns-pdns/
10. https://www.forgov.qld.gov.au/information-and-communication-technology/cyber-security/cyber-security-services/protective-dns-service