# 基于SDP与DNS融合的零信任安全增强策略模型

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

软件定义边界工作组官网网址：

https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter

# 序言

DNS 作为互联网重要的基础服务之一，承担着将域名指向可由计算机识别的 IP 地址的重要作用，堪称互联网的“导航系统”，同时在企业的内网环境也承担着同等重要的职责。DNS 的安全是保障网络畅通的核心和基础，也是数据安全的底层基石。

思科相关安全研究数据显示，近 91.3%的已知恶意软件被发现使用 DNS 作为主要手段，但 68%的企业却忽略了这个问题，并没有对 DNS 解析进行监管，这种现象称之为“DNS 盲点”。

正因为 DNS 如此重要的作用，其一旦出现漏洞或遭受攻击，必然会对网络的正常访问和使用造成严重影响，给政府和企业带来巨大的损失。

很多企业投入大量财力、物力、人力构建完善的安全防护体系，虽然网络安全架构已经十分完善，但 DNS 系统安全依旧成为百密一疏的防护漏洞，并且传统的安全防御体系在日益频繁 DNS 攻击的抵御防护中尤为吃力。

2022 年 5 月 CSA 正式发布了《SDP 标准规范 2.0》。SDP 为网络运营者提供动态灵活的边界功能部署能力，聚焦于保护关键的组织资产，实现精准授权，降低网络攻击的可能性。帮助零信任安全实现最小授权原则并隐蔽网络和资源。

本文通过 2 个实际用例解释了如何将 DNS、企业管理 DDI 系统与 SDP 结合，使用 DNS 及企业管理 DDI 系统为 SDP 提供设备及网络行为的上下文信息，作为 SDP 系统输入，增强访问控制策略的决策能力，从而提供改进的安全可见性、恢复能力及响应能力，帮助组织机构通过零信任架构获取的安全保障更上一层楼。

最后感谢参与本次翻译和支持的工作者们的无私奉献。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

# 致谢

《基于SDP和DNS融合的零信任安全增强策略模型（Integrating SDP and DNS Enhanced Zero Trust Policy Enforcement）》由CSA软件定义边界工作组专家编写，CSA大中华区秘书处组织翻译并审校。

## 中文版翻译专家组（排名不分先后）：

**组 长：**陈本峰

**翻译组：**单美晨 江 坤 石瑞生 汪 海 谢 琴 杨正权

于继万 于新宇 余晓光

**审校组：**谢 琴 姚 凯

**研究协调员：** 潘国强 李 杰 李金瑞 陈 龙

**感谢以下单位的支持与贡献：**

北京奇虎科技有限公司

北京启明星辰信息安全技术有限公司

北京天融信网络安全技术有限公司

华为技术有限公司

江苏易安联网络技术有限公司

上海安几科技有限公司

云深互联(北京)科技有限公司

中国电信股份有限公司研究院

湖州市大数据发展促进会

湖州市吴兴区大数据发展管理局

西塞数字安全研究院

## 英文版本编写专家

**主要作者：**Jason Garbis Juanita Koilpillai Srikrupa Srivation PG Menon

**贡献者：**Michael Roza

**审核者：**Nader Zaveri Andrea Knoblauch

**CSA 全球员工:**Shamun Mahmud

**献辞**

本文是为了纪念 Juanita Koilpillai，一位安全领袖、影响者、导师和朋友。

软件定义边界(SDP)和零信任工作组是云安全联盟(CSA)的一个研究工作组，旨在促进采用零信任安全原则，为组织机构能够并应该如何在云和非云环境中采用这些原则提供实用和技术上可靠的指导。该小组将以美国国家标准与技术研究所(NIST)的零信任研究和方法为基础并发挥作用。该工作组还将推广SDP作为实现零信任价值和原则的推荐架构。此外，它将修订和扩展SDP规范以获取和编纂从过去的经验中获得的知识。最后，在推广和推荐SDP的同时，该工作组将采取包容性的方法替代安全架构，并客观地支持它们（前提是符合零信任哲学）。

在此感谢以上专家。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给与雅正! 联系邮箱：research@c-csa.cn；国际云安全联盟CSA公众号。

# 目录

# 1.引言

在网络复杂度飙升和安全威胁加剧的背景下，组织机构需要能够简化、优化并保护网络通讯的解决方案。域名系统（DNS）将人类可读的域名（例如，cloudsecurityalliance.org）映射到互联网协议（IP）地址，对于可靠的互联网运营和连接至关重要。无论网络连接是从用户的Web浏览器、在线设备还是业务服务器发起，几乎每个都是以DNS查询开始。不幸的是，DNS的无处不在以及该协议的开放性、无连接性和未加密性，使得DNS成为恶意软件渗透到网络中并窃取数据（通常不易被发现）的常用目标。但是，组织机构可以集成软件定义边界（SDP）架构与DNS，获得安全能力的提升。DNS可作为一个零信任网络策略执行点，与SDP策略执行点协同工作，通过挖掘出有价值的DNS数据，加快SDP的威胁响应速度。

网络连接规模化所需的另外两个核心服务是动态主机配置协议（DHCP） 和互联网协议地址管理（IPAM）。这三个核心网络服务统称为 DDI（DNS、DHCP、IPAM）。集成这三个组件有助于为当今高度分布式的现代化网络提供控制力、自动化和安全性。DDI 组合具有独特的优势，可以记录网络上的人员、人员的去向以及（更重要的是）去过的地方。当DDI系统与威胁情报源结合使用时，将具备足够信息，在控制平面和DNS层配置并实施策略。

在DNS层配置和实施策略的好处是，它不是计算密集型的，并且可以扩展到数百万级别。但是，我们必须注意到DNS层的策略是粗粒度的（例如域名）。因此，需要其他机制提供细粒度的策略框架和实施方案，以利用好DDI数据库。DDI服务可以为企业提供可见性和控制力，并且，当它与软件定义边界SDP结合使用时，可以在很大程度上提高安全性并帮助组织机构在零信任安全之旅中更上一层楼。

## 1.1 目的

本研究文档的目的是解释DNS和企业管理的DDI系统可以如何与软件定义边界SDP结合，以提供改进的安全可见性、恢复能力和响应能力。

## 1.2 范围

本白皮书探讨了企业管理的DDI与SDP集成以提高安全性、上下文感知能力和响应能力的两个用例。这种类型的集成（将传统意义上不同的系统结合在一起以得到更全面的实施方案）是零信任安全方案的标志。本文并不涉及DNS基础设施安全性本身。

## 1.3 受众

本文档的目标读者包括：

- 部署零信任/SDP产品的企业架构师和安全领导者，他们希望采取整体方案。
- 负责企业DNS、DHCP和IPAM系统的安全和IT从业人员，他们寻求提高系统安全有效性的方法。
- 在产品或解决方案中实施零信任/SDP架构的供应商或技术提供商。

## 1.4 域名系统（DNS）

DNS 是一种分层命名系统，它构建在一个为计算机、服务或任何连接到互联网或专用网络的资源而设的分布式数据库上。DNS将域名转换为与网络设备关联的数字标识符，定位和寻址全球设备。类似于系统“电话簿”，DNS使浏览器将“https://cloudsecurityalliance.org”转换为CSA Web服务器的实际IP地址。

公共DNS面向所有互联网用户，以递归名称服务器方式运行。公共DNS服务的示例包括Cisco OpenDNS，Google Public DNS，Cloudflare以及由大多数互联网服务提供商（ISP）运营的公共DNS服务器。但是，公共DNS服务器或包含在许多互联网服务包中的DNS通常并不适合企业。通常，组织机构使用商业或开源DNS服务器作为私有DNS服务器，增强控制力、安全性、可靠性和内部使用速率。

这些参考文献中描述了几种不同的 DNS 服务器类型。[1][2]它们必须协同工作才能将域名解析为IP地址。如果DNS服务器不具备这些属性，就可能会查询其他DNS服务器（一种称为“递归”的操作）。递归过程如“图1：企业中的递归DNS解析”所示。

[1] Johnson, D. (2021, February 16). What is a DNS server? How Domain Name System servers connect you to the internet. Business Insider. Retrieved March 9, 2022, from https://www.businessinsider.com/what-is-a-dns-server?r=US&IR=T

[2] OmniSecu.com. (n.d.). Recursive and Iterative DNS Queries. Retrieved March 9, 2022, from https://www.omnisecu.com/tcpip/recursive-and-iterative-dns-queries.php

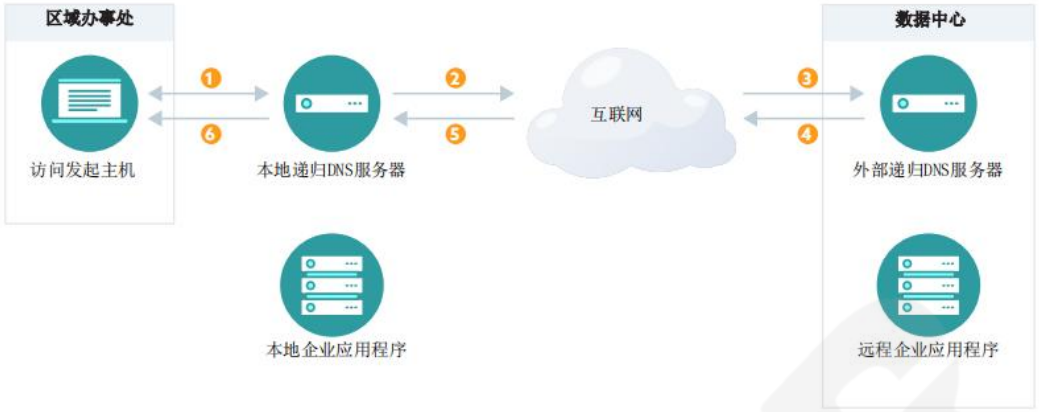


图 1: 企业中的递归 DNS解析

| # | 动作 | 描述 |
|---|---|---|
| 1 | 客户端到本地DNS | 客户端（访问发起主机）将 DNS 查询发送到本地 DNS 服务器以获取它所查找的应用程序的IP地址。本地DNS服务器如果具有该信息（即本地企业应用程序的IP地址），则会响应。 |
| 2 | 本地DNS服务器到互联网 | 如果本地DNS服务器没有该信息，它会将查询请求转发给其他 DNS 服务器。 |
| 3 | 互联网到外部DNS服务器 | 所有域都根据域名层次结构注册。DNS服务器可能通过其他递归层解析查询。 |
| 4 | 外部DNS服务器到互联网 | DNS响应通过互联网返回。 |
| 5 | 互联网到本地DNS服务 | 本地DNS服务器缓存该响应以供将来使用。 |
| 6 | 本地DNS服务器到客户端 | 本地DNS服务器将该响应转发给客户端。 |

### 1.4.1 动态主机配置协议 （DHCP）

DHCP 是一种自动配置协议服务，可在连接时将 IP 地址分配给网络设备，这对于将设备连接到网络至关重要。每个设备都必须有一个 IP 地址才能通信。DHCP允许自动配置设备，无需网络管理员干预，并提供一个中央数据库跟踪连接到网络的设备。此外，DHCP 可防止两个设备被意外地配置了相同的 IP 地址。

DHCP和DNS在开放系统互连（OSI）模型的“第7层或应用层”上运行。

## 1.4.2 互联网协议地址管理（IPAM）

互联网协议地址管理是企业在私有网络上管理DNS和DHCP的系统。IPAM系统可以对网络中如何分配和解析IP地址提供计划、跟踪和管理。通常，DNS和DHCP等技术被用于协同执行这些任务。然而，一个使用IPAM架构的、设计良好的DDI会集成DNS和DHCP服务数据，以便每个服务都能发现其他服务的变化。

例如，DNS通过DHCP知道分配给客户端的IP地址，然后对自身进行相应的更新。另外，知道分配给客户端的IP地址也使得私有DNS可以通过主机名解析客户端，即便通过DHCP动态分配IP地址时也是如此。

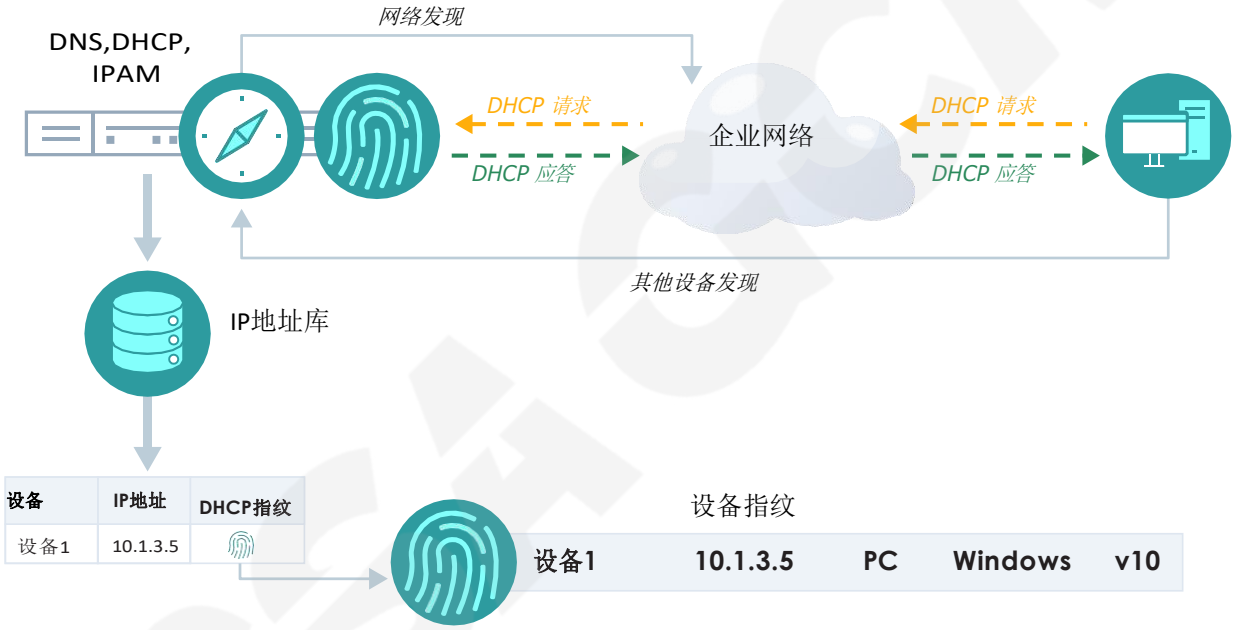


图 2: DDI中可用的上下文信息

## 1.4.3 实现云端管理

DNS传统上是在本地部署和管理的。然而，就像许多企业IT和安全基础设施元素一样，由企业运营的DDI的部署模式已经转向云端管理。

在云端管理的DDI中，管理和控制平面转移到云端，轻量级协议引擎部署在本地。轻量级协议引擎可以是容器化的也可以是虚拟机形式的。本地部署提供了本地存活性。即使互联网被切断，在远程站点拥有上百个传感器的钻井机仍可以继续运行，制造中心也可以继续生产。而将控制和管理能力转移到云端，也可以带来一些与软件即服务（SaaS）相关的好处。包括：

- 生命周期管理是自动化的。
- 消费模式更像SaaS。
- 无需过度准备。
- 组织机构可以根据业务需求增加或减少其使用量。
- 不像本地部署管理，云端管理可以扩展到成百上千个远程站点，例如加油站和零售商店。


图3: 云端管理私有 DNS

## 1.5 基于DNS的安全

基于域名系统的安全性对于早期检测和阻断网络内的恶意软件活动至关重要。恶意软件通常需要利用DNS解析命令和控制（C&C）服务器的IP地址。域名解析系统也被恶意软件用作隐蔽通信通道，以避免被企业安全机制检测到。

### 1.5.1 恶意软件控制点

当需要命名空间解析时，DNS是传播恶意软件的失陷设备的第一个通信点。这意味着DNS拥有一个观测恶意软件活动的“前排座位”，并可以检测和响应恶意软件攻击。通过在DNS服务器上使用高质量的聚合威胁情报，组织机构可以破坏C&C通道，并防止恶意软件活动的执行，包括勒索软件活动。这可以通过使用响应策略区域（RPZ）实现。该区域可以有效阻止到已知恶意的或已知C&C服务器的外部域名（例如webdisk.yakimix[.]com）的DNS解析。威胁情报包括失陷的主机名、域名和URL。这些信息可以用来阻止通向这些目的地址的DNS解析。

安全DNS在攻击开始之前破坏攻击链

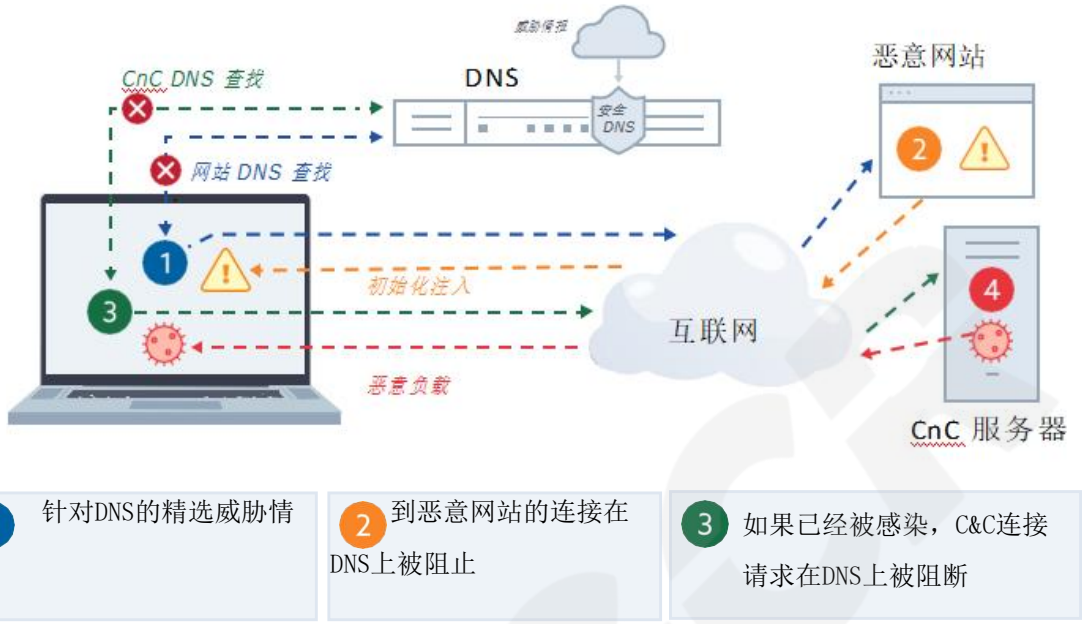


图 4: 在DNS上使用威胁情报来阻止恶意软件活动

## 1.5.2 阻止数据泄露

DNS还可以充当将数据从企业中泄露出去的反向通道。恶意攻击者可以使用标准的隧道工具包或自定义方法绕过传统的安全技术（如防火墙、入侵检测系统【IDS】等）。例如，近年针对医疗机构的Ryuk勒索软件活动就使用了DNS隧道[3]。在这种情况下，聪明的黑客意识到，他们可以通过将命令和数据隐藏到格式有效的DNS请求中，进而与目标计算机秘密通信。这个想法利用了DNS隧道的核心[4][5][6]。

不幸的是，各种隧道的变体很难检测到，因为它们使用了以前未知的方法，目的地址可能还没有添加到不可信名单中（这意味着它们不被认为是恶意的，并且不会出现在任何威胁源中）。缓解0Day数据泄露/隧道的最佳方法是对DNS查询使用基于人工智能/机器学习（AI/ML）的分析。机器学习模型有助于检测和允许合法的隧道（一些防病毒软件使用DNS隧道更新端点），同时阻

[3] Cybersecurity & Infrastructure Security Agency. (2020, November 2). *Ransomware Activity Targeting the Healthcare and Public Health Sector* | CISA. https://www.cisa.gov/uscert/ncas/alerts/aa20-302a

[4] Green, A. (2020, October 19). *What is DNS Tunneling? A Detection Guide*. Varonis. https://www.varonis.com/blog/dns tunneling

[5] Palo Alto Networks. (n.d.). *What Is DNS Tunneling?* Retrieved March 9, 2022, from https://www.paloaltonetworks.com/ cyberpedia/what-is-dns-tunneling

[6] Roblyer, K. (2021, August 2). *3 Things NIST Taught Us About DNS Security*. BlueCat Networks. https://bluecatnetworks. com/blog/3-things-nist-taught-us-dns-security/

止用于泄露数据的恶意隧道。基于AI/ML的分析还有助于检测高级威胁，如域名生成算法（DGAs）、Fast Fllux以及仿冒域名。

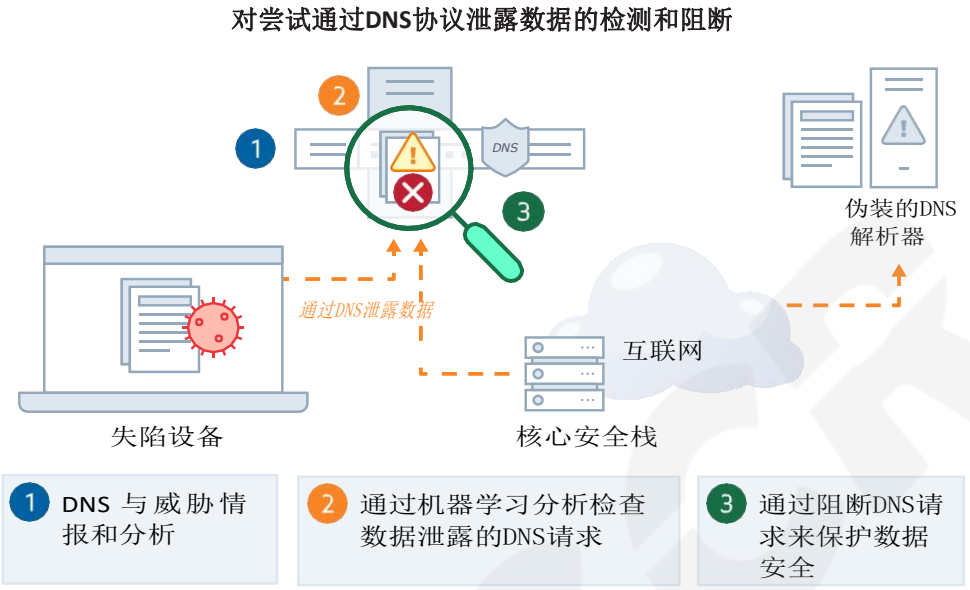


图 5: 检测和阻断DNS数据泄露

### 1.5.3 域名生成算法 (DGA) 控制点

域名生成算法(DGA)用于生成域名，使得黑客能够绕过静态的、基于域名的URL阻断系统（如防火墙黑名单）的检测和阻断。通常情况下，黑客会编写恶意软件入侵网络，并利用DGAs连接到由其控制的服务器。但恶意软件并没有使用静态域名，而是尝试连接到由算法生成的动态域名。首先，黑客将注册由相同算法生成的一些域名，并在该域名上运行“恶意”服务器（即命令和控制服务器，或称C&C服务器）。最后，恶意软件将连接C&C服务器。

**威胁情报/信誉列表对该攻击方式无效**

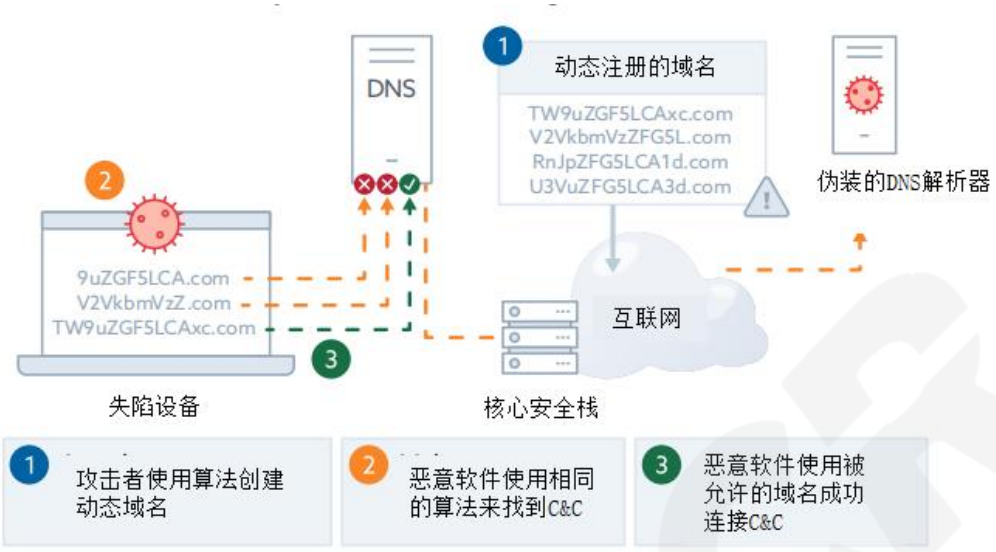


图 6: DGAs如何工作

**机器学习识别基于算法的域名查询**

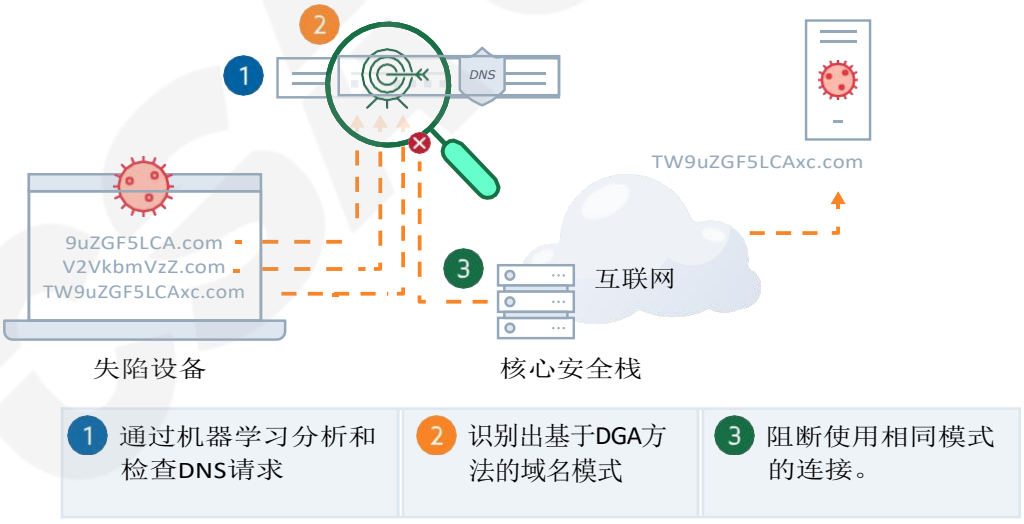


图 7: 检测和阻断DGA

Fast flux是一种DNS技术，用于通过在包含失陷主机(作为代理)的网络中快速跳转来隐藏僵尸网络。这些代理拥有大量与合法域名关联的IP地址，使攻击者能够延缓或逃避检测。

仿冒域名是为收集敏感信息而创建的伪造(钓鱼)网站。例如，诱骗用户“登录”伪装成合法银行网站的虚假网页等。

使用AI/ML模型分析DGA之类的威胁涉及观测大量此类威胁以预测使用诸如熵(不确定性级别)、语言分析、频率和大小等技术的未知版本[7]。

### 1.5.4 基于类别的过滤

除检测和阻断基于DGA的攻击之外，DNS可以作为一个强大的网络策略执行点，用于阻止访问特定的内容类别，如社交媒体、暴力、赌博等。例如，一家公司可能想阻止大多数员工访问社交媒体，但又要允许有需要的营销人员访问，因为访问社交媒体是他们工作的一部分。

许多企业已经为网络设备部署了DNS过滤服务，以便对用户强制实施这些策略。

## 1.6 零信任策略执行

美国国家标准与技术研究所NIST（National Institute of Standards and Technology）的特别出版物800-207首先通过描述满足零信任（Zero Trust）需求所需的核心组件（参见下图8）揭示零信任。总的来说，零信任架构首先需要有三个核心组件，然后才能应用逻辑决策。这三个核心组件包括：

1. 通信：实体访问资源的请求以及由此产生的访问或会话。
2. 身份：请求访问资源的实体身份（用户或设备），需要一定程度的身份验证。
3. 资源：目标环境中的任何资产。

除了这三个核心组件外，零信任还有另外两个基本要素：

- 策略：定义“谁、如何、什么和何时”目标资源可被访问的治理规则。
- 数据源：用于动态更新策略的上下文信息。

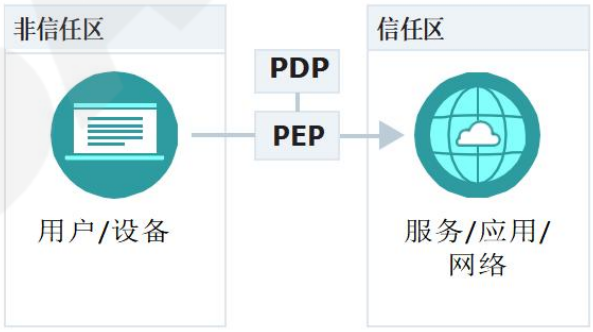


图8:NIST 800-207零信任组件[8]

这些策略是用于确定“谁”可以访问“什么”、“何时”、“多长时间”和“出于什么目的”的“规则”。NIST 零信任工作流程通过两种机制定义、管理和执行策略：

[7] Yu, B., Pan, J., Gray, D., Hu, J., Choudhary, C., Nascimento, A. C. A., and de Cock, M. (2019, April 15) Weakly Supervised Deep Learning for the Detection of Domain Generation Algorithms. IEEE Access. Vol. 7, pp. 51542-51556. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8691763

[8] Rose, S. (2020, August 11). SP 800–207, Zero Trust Architecture | CSRC. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-207/final

- 策略决策点（PDP）
- 策略执行点（PEP）

它们放置在流量的访问工作流中共同调节对资源的访问。

策略决策点（PDP）确定适用于每个被验证身份的“规则”，并传达给策略执行点（PEP）。

策略执行点（PEP）充当逻辑网关，确保已向正确的实体授予正确的访问权限，以及对已批准资源的正确访问级别。

### 1.6.1 SDP和零信任策略执行

SDP架构旨在提供按需的、动态调配的、并且逻辑隔离的网络[9][10]。隔离网络指的是与所有不安全网络隔离的受信任网络，减轻来自于网络的攻击。实施零信任需要在授予访问权限之前验证尝试连接到资产的任何元素，并在整个连接期间持续评估会话。“基于软件定义边界（SDP）的零信任实现方案使组织机构能够防御现有的、以边界为中心的网络和基础设施中不断出现的旧攻击方法的新变体。实施SDP可以改善企业的安全状况，由于攻击面日益复杂并且不断扩大，企业需要不断适应这种挑战。[11]”。企业必须监控资产的完整性和安全状况（NIST SP 800-207 2020第7页）。SDP通过启用默认的“拒绝所有”防火墙策略，只有用户/设备经过身份验证和授权后，才可以访问由SDP系统保护的资产。此外，SDP通过预审查连接，审查谁可以连接、从哪些设备连接、到哪些服务和基础设施以及其他参数，控制所有通向受信任区域的连接[12]。

在最简单的SDP形态中，包括发起主机、接受主机和SDP控制器。发起和接受主机通过控制平面上的安全通道与SDP控制器交互，管理它们之间的连接操作。SDP控制器是一种策略定义、验证和决策机制（零信任策略决策点），维护着有关哪些用户/组可以使用哪些发起主机（即用户设备）通过哪些接受主机（本地或云中）访问哪个组织资源的信息。数据通过数据平面中单独的安全通道通信，接受主机（通常部署为SDP网关）隔离在受信任区域中。SDP网关（零信任策略执行点）充当受保护服务的前置系统，并执行由SDP控制器维护的身份验证和授权规则。因此，在SDP中，控制平面与数据平面分离，建立灵活和高度可扩展的系统架构。

---

[9] For an introduction to the SDP Architecture: https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/

[10] For an introduction to the SDP Architecture: https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

[11] NIST. (2020, October). Implementing a Zero Trust Architecture. National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zta-project-description-final.pdf

[12] NIST. (2020, October). Implementing a Zero Trust Architecture. National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zta-project-description-final.pdf

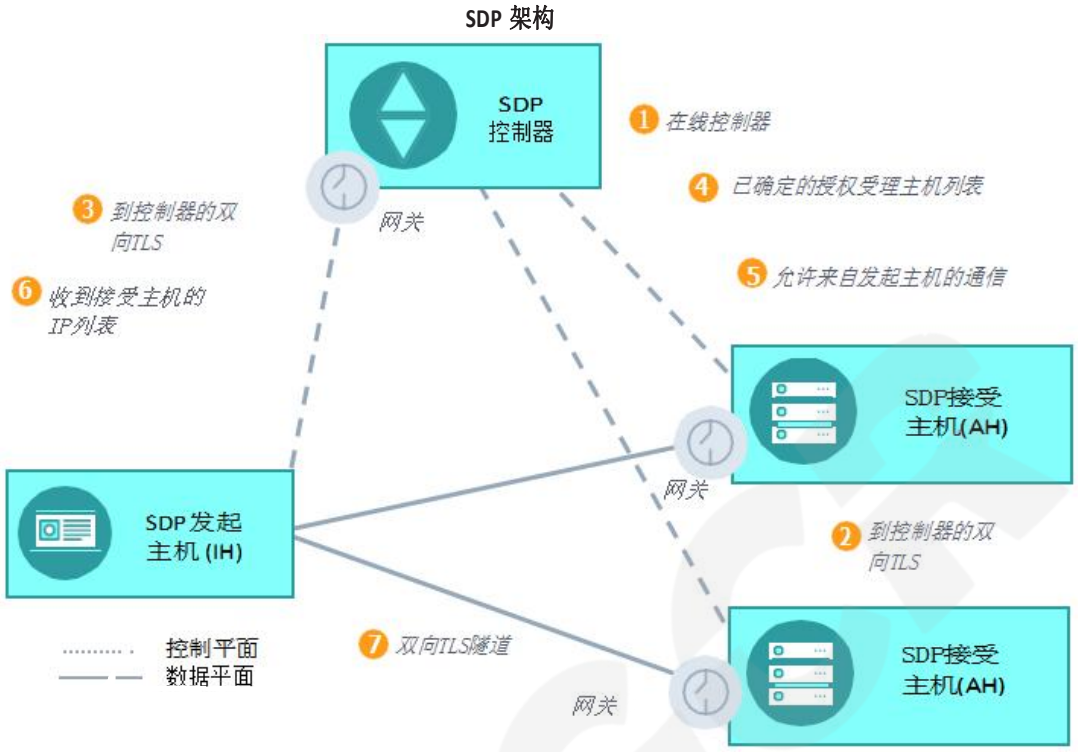


图9: SDP 架构[13]

在SDP中，网关是零信任策略执行点，确保用于决定“谁”可以访问“什么内容”、“什么时间”、“多长时间”和“出于什么目的”的“规则”得到执行。

### 1.6.2 DNS和零信任策略执行

零信任原则鼓励企业将安全生态系统的元素整合在一起，提供更多的上下文，并更好地通过零信任策略执行点（PEP）实施访问控制。如上所述，SDP是一个经过充分验证的用于实现零信任原则的架构，并提供以身份为中心和基于上下文感知的策略执行。因此，将DNS与企业管理的DDI和SDP整合在一起是零信任之旅中自然而有价值的一步，将帮助企业从这些基础设施元素中获得更多价值，并提高环境的安全性和响应能力。下面将探讨两个用例，说明这些要素是如何连接起来并执行零信任策略的。

策略执行是将控制机制应用于网络访问。规则或策略可能基于许多准则。DNS 和企业管理的 DDI 提供了基本信息，可以为是否允许用户访问网络提供决策支持，并且可以成为策略执行的关键组件。

当新设备加入网络时，DNS和企业管理的DDI解决方案提供的监测模块可以向策略执行工具发

[13] Cloud Security Alliance. (2019, May 7). SDP Architecture Guide v2. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/

送警报。为了添加到网络，新设备会发出DHCP请求。已存储的数据使DDI能够识别设备，并通过“指纹”跟踪其活动。DDI支持将基于MAC（媒体访问控制）地址和操作系统的IP地址分配映射为基本DHCP过程的一部分。如果公司的设备启用策略中定义了对任何未执行漏洞扫描的新设备的访问限制， NAC（网络访问控制）解决方案可以通过使用DDI解决方案中的警报阻止对该设备的访问。这个过程可以动态、实时地进行。

策略执行还与安全目标直接相关。例如，绝大多数基础的DNS监控具备快速发现通过DNS泄露数据等恶意活动的能力。安全生态系统工具（如漏洞扫描器）和网络访问控制（NAC）解决方案（如SDP）也同样可以在基于网络或安全事件的应用策略中使用DDI数据。例如，当检测到已知或潜在恶意域名的DNS请求时，可以触发设备扫描以检查设备是否存在漏洞和恶意软件。或者，可以隔离有问题的设备，并且只有在其漏洞得到修复后才允许重新连接。类似地，当实施零信任SDP时，策略执行点（PEP）可以阻止来自失陷设备的连接。

# 2 SDP/零信任和DNS用例

在实施零信任的软件定义边界环境中，上下文信息对访问策略的决策非常关键。因此，基于身份、资源和通信进行风险评估至关重要。以下两个用例说明了DDI和SDP系统可以整合在一起。

## 2.1 用例#1: DNS向SDP提供上下文和元数据

本用例侧重于使用DNS和企业管理的DDI中的元素提供有关设备和网络行为的上下文信息，并将此上下文信息作为零信任SDP系统的输入，增强访问控制策略的决策能力。

在此用例中，企业使用SDP控制用户对企业受控资源的访问。图10描述了一个常见的零信任SDP部署模型。[14]关键在于零信任SDP使用逻辑上集中的控制器作为策略决策点，并通过控制平面将访问控制策略传递到SDP网关（策略执行点）。该企业还采用了私有DDI基础设施。在此用例中，DNS服务器充当“天线”，向SDP控制器提供有关设备和网络活动的额外信息，从而增强系统的访问控制决策的能力。

图10所示的模型描述了分布式SDP中的DNS、DHCP和IPAM（DDI）。SDP控制器可以利用DDI数据和其他信息，根据相应的策略，向受SDP网关保护的位于不同信任区域中的应用（云应用或者数

[14] Specifically, this figure depicts the Client-to-Gateway model for clarity. The use cases in this document are equally applicable across all SDP deployment models.

据中心中应用）授予访问权限。这个图说明了DNS和SDP如何协同工作以提供安全和无缝的用户体验， SDP控制器一旦确定用户设备（发起主机，IH）是可信的，就将建立从用户设备到SDP网关的安全隧道，这些隧道能够安全地传输应用流量和DNS请求。这使得用户可以访问私有或远程DNS服务器，而不用将其暴露在互联网上。当域名解析后，用户流量的传递会从用户设备开始，通过网关到达目标业务应用。

除了DNS解析之外，DNS服务器还可以提供设备的上下文信息以增强SDP工作流。

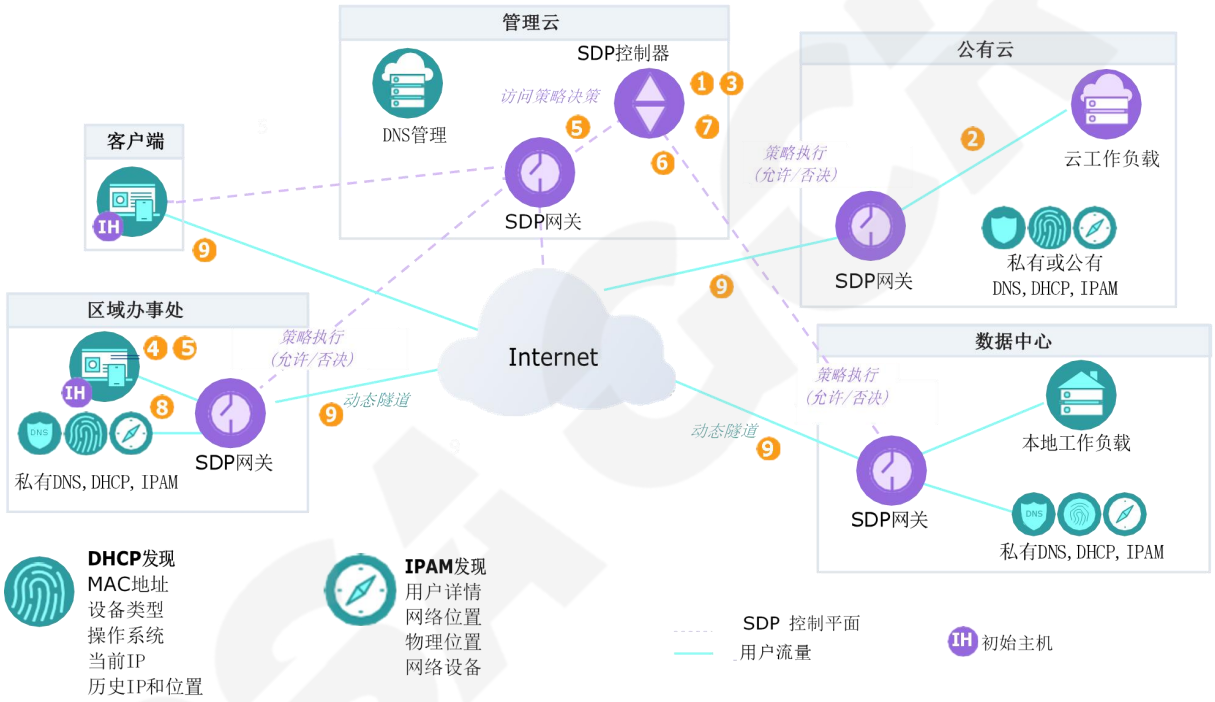


图10：DNS和SDP协同工作

图 10中展示的步骤描述了该用例的典型事件序列。

| 序号 | 步骤 | 描述 |
| --- | --- | --- |
| 1 | SDP控制器启动 | 一个或多个 SDP 控制器加载上线并连接到适当的身份验证和授权服务（可选项。例如，PKI、IAM、身份验证、设备管理、地理定位和其他服务）。 |
| 2 | 接受主机启动 | 一个或多个 AH加载上线（SDP 网关是所述部署模型中的 AH）。这些网关连接到控制器,并进行身份验证。但是，它们不回应来自任何其他主机的通信请求，并且不会响应任何未配置的请求。 |
| 3 | 发起主机启动 | IH上的一个或多个客戶端上线后，SDP 控制器对每个用戶（或非个人实体NPE）进行身份验证。此步骤可能包括 SDP 控制器的 DNS 解析。 |
| 4 | 发起主机IH到SDP控制器 | 当接入的 IH 重新上线时（例如，设备重启后或用戶启动连接时），会连接到 SDP 控制器并进行身份验证。 |
| 5 | SDP 控制器到发起主机IH | 在对 IH 进行身份验证后（在某些场景下，由对应的身份提供者IdP完成），SDP 控制器会向IH提供一个已授权通信的网关列表，用于后续通信。 |
| 6 | SDP控制器到DNS | SDP 控制器从 DNS 服务器检索该设备上下文信息。例如，如果设备被认为是恶意的，则不允许 IH 请求。 |
| 7 | SDP控制器到SDP 网关 | SDP 控制器指示网关接受来自 IH 的通信，以及提供用于建立双向加密通信的用户、设备和服务等相关信息。 |
| 8 | 发起主机IH到SDP网关 | IH 使用单包认证 (SPA) 协议启动与每个授权的 SDP 网关的连接，该网关验证 SPA 中的信息（用于执行）。 然后IH建立到这些 SDP 网关的双向 TLS 连接。此步骤可能包括 SDP 网关的 DNS 解析。 |
| 9 | DNS递归解析 | IH发出的DNS 解析请求（解析目标为处于SDP 网关后的远程主机）都通过 SDP 隧道路由到远程私有 DNS 服务器。 |

### 2.1.1 用例 1 中的策略执行

在零信任环境中，访问策略通常包括用户、设备和要访问的服务。

#### 2.1.1.1 网络上下文和身份信息

随着越来越多的设备加入网络，DNS 和企业管理的 DDI 可以共享所有设备的综合视图，实现高效的资产管理、降低风险和支撑合规政策。此外，DDI 系统管理的 IP 记录还包含了能进一步描述资产，并带来额外潜在效用的元数据。


图 11: 网络上下文和身份信息

DNS 、 DHCP 和 IPAM 数据可以为 SDP 控制器提供额外的上下文信息，例如来自特定用户或客户端设备的 DNS 请求。 DDI 中可用的详细上下文信息提供了相关网络活动的完整指纹，包括：

- DHCP 发现
  - MAC地址
  - 操作系统 (OS) 系列类型
  - 操作系统版本
  - 当前 IP 地址
  - 历史 IP 地址和位置
- IPAM 元数据
  - 用户详细信息（通过与 IAM 集成）
  - 子网/网络位置
  - 由管理员提供的物理位置（例如，楼层、建筑物、地理位置）

软件定义边界SDP系统也可以使用这些上下文信息做出更好的访问控制决策。注意，私有 DDI 系统通常无法为远程用户提供此级别的信息，因为这些用户不再直接连接到企业网络。通常，诸如 VPN 之类的远程访问解决方案会混淆内部企业 DDI 系统中的用户和设备（即，将所有远程用户映射到一个共享的私有IP 地址或 NAT）。SDP系统通过提供统一的深度上下文和用户/设备相关信息（不考虑位置）弥补这一点。虽然只有本地用户会使用 DDI 的 DHCP，但内网（指接入企业内网）

和外网（例如，居家远程办公）用户都将因为 DNS 请求而实施 DDI 系统。因此，DDI 可以向 SDP 系统提供这些请求的相关信息。

图 12描述了下面两个用户的活动：

- Natalia 在办公室工作，使用企业局域网 (LAN) 中的 DHCP 服务器获取 IP 地址，并使用本地 DNS 服务器处理所有的 DNS 请求，因此，Natalia的 DNS访问活动是全部可见的。

- Jim 在家工作，并使用本地路由器提供的DHCP服务，因此，企业 DDI 系统无法查看他的 DHCP 请求或指纹。但是，SDP系统可以确保他对企业资源的 DNS 请求送入 SDP 隧道并由企业 DNS 服务器解析，从而获得Jim的 DNS 访问活动的完全可见性。注意，SDP 实现可以将 Jim 的全部或部分 DNS 流量放在隧道内传输。通常来说，这个机制是可配置的。

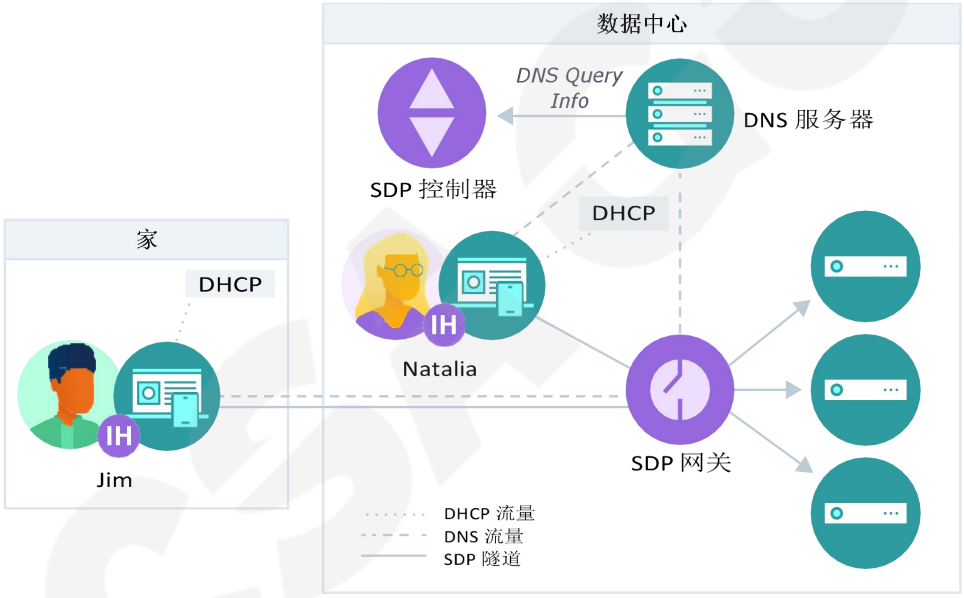


图 12: 内网与外网的用户流量

SDP的一种实现可以利用网络上下文和身份数据定义SDP控制器的策略，并在SDP网关上强制执行。SDP控制器可以集成许多如身份信息提供者(目录)和漏洞扫描器之类的信息源，提供可执行的细粒度策略。

## 2.1.2 响应恶意行为

如图12所示，私有DNS服务器通常是恶意行为(或被入侵迹象)发生的起始位置。例如，一个终端感染后向与勒索软件关联的C&C服务器发出DNS请求。

DNS是将行为归因于某特定设备的一种非常有效的方法。此外，DDI的检测功能可用于触发SDP的响应，例如设备的网络访问变更、增强的认证要求、以及让用户采取特定行动等。例如，如果许多远程用户从SDP网关到受保护资源的网络流量映射到本地网络上的一个共享IP地址（例如，源NAT配置），SDP可以帮助消除网络行为的歧义。

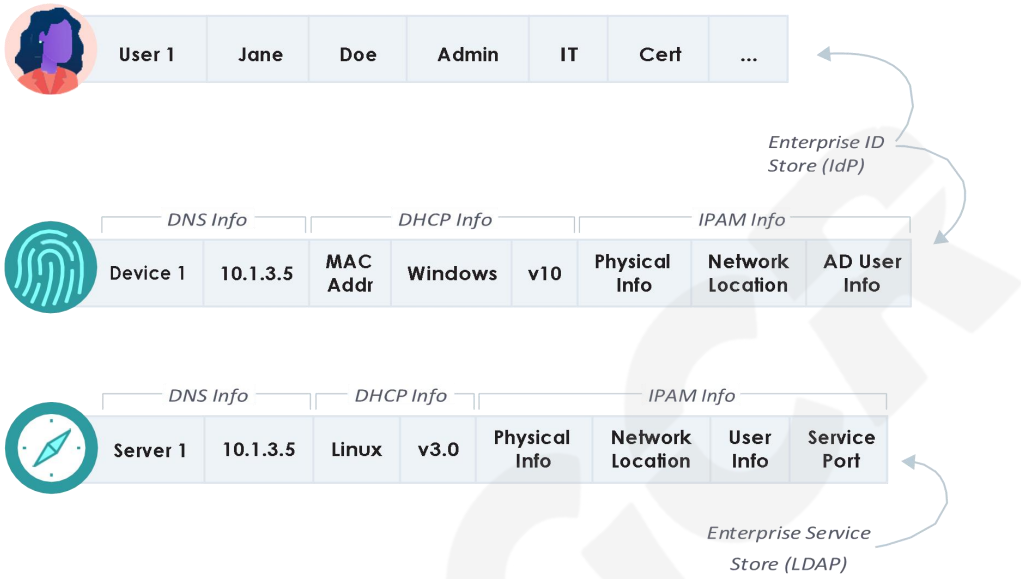


图13: 使用DNS、DHCP和IPAM信息精准识别受感染的设备

### 2.1.3 基于位置的访问控制

根据用户或设备的地理位置，诸如用户所接入的网络、交换机端口或无线接入点，可以选择是否授予访问权限。例如，一个使用手推车采集病人生命体征信息的医疗机构可以制定政策规定这些设备只能从临床侧而不是服务前台获得网络访问权。网络分段是确保资源安全、减少攻击风险和渗透影响的关键。在这种情景下，IPAM元数据，如网络和物理位置，可以告知SDP控制器某个设备的行踪。

### 2.1.4 基于设备的访问控制

零信任是指在尽可能早时、尽可能多地了解设备的情况以建立信任。因此，在DHCP工作过程中提取信息并收集设备数据是至关重要的。利用DHCP指纹（在试图检索IP地址时识别请求DHCP租约的设备）和MAC分析等技术，可以获得丰富的设备元数据，包括：

- 硬件供应商
- 设备类别（电话/平板电脑/PC/IoT）
- 操作系统和版本号
- MAC地址
- IP地址

SDP控制器可以利用这些信息确定设备是否允许接入，尤其是在常见的BYOD场景中。允许这些设备访问网络资源意味着要确保它们足够安全。例如，运行最新iOS版本的iPhone或许网络访问的风险相对较低；而运行过时版本的旧安卓手机或许会产生足够高的恶意软件风险，有必要阻止或限制其网络访问。

此设备上下文对于零信任策略决策点(SDP控制器)是必要的，因为SDP控制器会评估策略，确定它们是否适用于给定的主体。具体实施中SDP是从本地用户代理(SDP Client)获取这类信息。

设备元数据应该包含在可靠的零信任部署的策略分配标准中。

### 2.1.5 基于用户的访问控制

前面的场景可以扩展到只允许特定的用户访问特定的应用程序。例如，通过与企业目录集成，用户信息和DNS提供的IP地址信息可以集成到SDP系统中，作为附加的上下文或附加的完整性检查策略。

## 2.2 用例#2- SDP控制器将策略结果发布到DNS

DNS和SDP控制器可以协同提高安全性的另一个用例是SDP控制器将访问策略结果发布到本地DNS服务器，以便提供一层额外的控制。例如，假设财务部中只有经过认证的用户才能访问finance.internal.company.com的Web应用程序。相对的，只有工程部用户应该能够访问git.internal.company.com服务器。所有员工都应该能够访问email.internal.company.com服务器，并且所有设备都应该允许对外部域(例如，cloudsecurityalliance.org)的DNS查询，如图14所示。

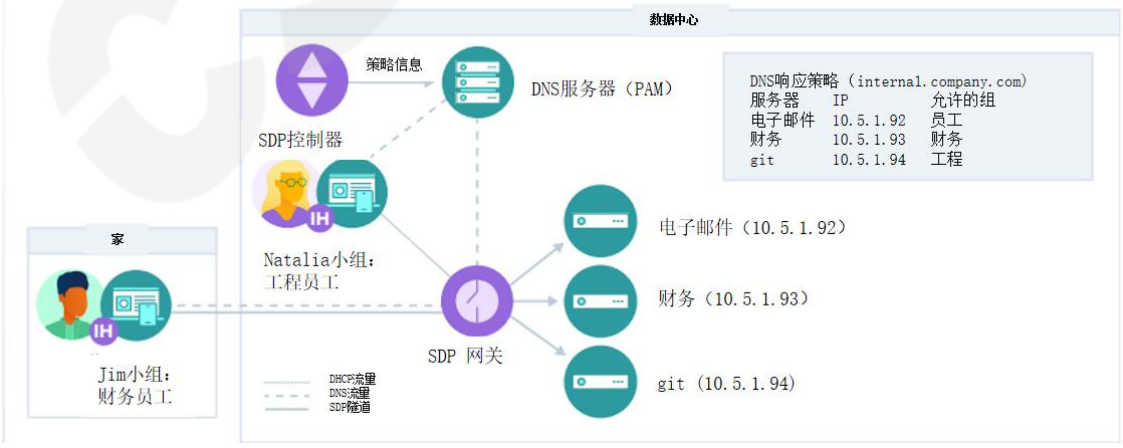


图14: 使用SDP策略进行DNS解析

图14展示了SDP控制器如何将策略信息推送到DNS服务器，并展示了应该允许哪些目录组解析哪些内部服务器的主机名。(注意，此图假设DNS服务器已从一个企业目录服务获得用户到组的映射，在图中并未展示。或者，SDP控制器也可以将此信息提供给DNS服务器)。远程用户Jim将其对内部资源的DNS请求通过SDP网关隧道传输到私有DNS服务器。本地用户Natalie将DNS请求直接路由到同一台DNS服务器，该服务器部署在本地的内网。在这两种情况下，DNS服务器都可以区分哪个用户正在发出DNS请求，还可以知道每个用户属于哪些组。SDP控制器已向DNS服务器发布了策略信息，指示需要哪些目录组成员身份才能访问哪些服务，如图中的DNS响应策略表所示。基于所有这些信息，只有当发出请求的用户在匹配的组中时，DNS服务器才会响应查询请求并返回一个IP地址。所以用户Jim将能够获得电子邮件和财务服务器的IP地址，但不能获得git服务器地址。

### 2.2.1 在DNS中的策略执行-一个额外的安全层

DNS访问控制是一种简单、可扩展且经济有效的方法，可用于在零信任/SDP环境中保护应用程序和数据。在DNS层面检测和阻止恶意软件通信，并基于类别过滤并阻止访问某些类别的内容（如社交媒体、暴力、赌博等），可以显著减少对NGFW和网关的恶意流量。该威胁卸载方案保留了防火墙和网关的处理能力（这些通常是昂贵的外围解决方案），提高了这些解决方案的投资回报率（ROI）。

需要注意的是，相对通过受信任安全区的 SDP 网关进行基于网络的策略执行而言，该方法应被视为一个可部署的额外控制措施，阻止特定目标服务器的DNS解析。如上所示，这个场景会阻止未经授权的访问，但不能替代内部策略的实施。例如，攻击者可以创建一个具有目标服务器的IP地址的hosts文件条目，从而降低了基于DNS过滤的有效性。或者，攻击者可以简单地枚举IP地址，而不需要对主机名执行DNS解析。

# 3.结论

本白皮书探讨了企业 DDI 系统如何同 SDP系统实现集成和增强，提升组织机构的安全性、韧性和响应能力。企业 DDI 通过过滤已知的不良站点和检测失陷指标（IoC）提升组织机构的安全性，SDP 为实施安全策略提供了丰富的上下文信息，这两个系统都可以通过集成而受益。DNS可以为SDP控制器提供增强的上下文设备和活动信息，以便后者更好地制定策略决策。此外，DNS系统可以使用来自 SDP控制器的零信任上下文信息和决策，扩展SDP的覆盖范围，并有效地使企业 DNS 成为一个关键的零信任策略执行点。

信息安全将始终是多层级的，纵深防御就是其中一个关键概念。而基于SDP的零信任是一种有效的方案，将企业安全基础架构的许多其他组件集成而使企业受益。企业DNS 就是其中一个例子，上面探讨的两个用例很好地说明了这一点。

# 4.参考文献


Cloud Security Alliance. (2014, April 30). Software-Defined Perimeter (SDP) Specification v1.0. CloudSecurity Alliance. https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

Cloud Security Alliance. (2019, May 7). SDP Architecture Guide v2. Cloud Security Alliance. https:// cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/

Cloud Security Alliance. (2019, October 27). Software-Defined Perimeter as a DDoS Defense Mechanism. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/software-defined- perimeter-as-a-ddos-prevention-mechanism/

Cybersecurity & Infrastructure Security Agency. (2020, November 2). Ransomware Activity Targeting the Healthcare and Public Health Sector | CISA. https://www.cisa.gov/uscert/ncas/alerts/aa20-302a

Garbis, J., and Chapman, J. W. (2021) Zero Trust Security: An Enterprise Guide. Apress. https://www. apress.com/us/book/9781484267011

Green, A. (2020, October 19). What is DNS Tunneling? A Detection Guide. Varonis. https://www. varonis.com/blog/dns-tunneling

Infoblox. (2019) Using Artificial Intelligence/Machine Learning to Detect Domain Generation Algorithms. Infoblox. https://info.infoblox.com/resources-whitepapers-artificial-intelligence-to- detect-domain-generation-algorithms

Infoblox. (n.d.). Infoblox Glossary. Infoblox. https://www.infoblox.com/glossary/

Infoblox. (2019, January). Ryuk Ransomware Cyber Report. Infoblox. https://insights.infoblox.com/ threat-intelligence-reports/threat-intelligence--3

Infoblox. (2019). Powering SOAR Solutions from the Foundation. Infoblox. https://insights.infoblox. com/solution-notes/infoblox-solution-note-powering-soar-solutions-from-the-foundation

Johnson, D. (2021, February 16). What is a DNS server? How Domain Name System servers connect you to the internet. Business Insider. Retrieved March 9, 2022, from https://www.businessinsider. com/what-is-a-dns-server?r=US&IR=T

NIST. (2020, October). Implementing a Zero Trust Architecture. National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zta-project- description-final.pdf

OmniSecu.com. (n.d.). Recursive and Iterative DNS Queries. Retrieved March 9, 2022, from https:// www.omnisecu.com/tcpip/recursive-and-iterative-dns-queries.php

Palo Alto Networks. (n.d.). What Is DNS Tunneling? Retrieved March 9, 2022, from https://www. paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

Roblyer, K. (2021, August 2). 3 Things NIST Taught Us About DNS Security. BlueCat Networks. https:// bluecatnetworks.com/blog/3-things-nist-taught-us-dns-security

Rose, S. (2020, August 11). SP 800–207, Zero Trust Architecture | CSRC. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-207/final

Waverley Labs, SDP Center, Open Source Reference Implementation (funded by DHS), 2021, available at http://sdpcenter.com/test-sdp/

Yu, B., Pan, J., Gray, D., Hu, J., Choudhary, C., Nascimento, A. C. A., and de Cock, M. (2019, April 15) Weakly Supervised Deep Learning for the Detection of Domain Generation Algorithms. IEEE Access. Vol. 7, pp. 51542-51556. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8691763

# 5.缩略词

**AI/ML:** 人工智能/机器学习

**BYOD:**自带设备

**DDI: DNS、DHCP、IPAM**

**DGA:** 域名生成算法

**DHCP:** 动态主机配置协议

**DNS:** 域名系统

**DDoS:** 分布式拒绝服务

**EDR:** 端点检测和响应

**IaaS:** 基础设施即服务

**IP:** 互联网协议

**IPAM:**互联网协议地址管理

**ISP:** 互联网服务提供商

**MAC:** 媒体访问控制

**NAC:** 网络访问控制

**PaaS:** 平台即服务

**PEPS:** 策略执行点

**RPZ:** 响应策略区域

**SDP:** 软件定义边界

**SIEM:** 安全信息和事件管理

**SOAR:** 安全编排，自动化和响应

**TLD:** 顶级域名

**ZTNA:** 零信任网络访问