Computer Science and Application 计算机科学与应用, 2025, 15(10), 287-295
Published Online October 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.1510268

Hans汉斯

基于NAT边界的应用层泄露与纵深防御研究

杨　乐

中国民用航空新疆空中交通管理局空管中心气象中心，新疆　乌鲁木齐

收稿日期：2025年9月15日；录用日期：2025年10月20日；发布日期：2025年10月29日

摘　要

本文通过研究网络地址转换(NAT)的工作原理，在网络层将地址重写隐藏的内部真实地址有可能在上层应用时被地址绕过，其安全性被削弱。通过实验搭建，复现网络攻击，论证出NAT技术在配置使用时存在一定的安全漏洞，攻击者利用该类漏洞，有可能穿透NAT映射并获取内部服务器的真实IP地址，进而绘制出内部网络拓扑。针对这种网络安全漏洞，本文提出将NAT技术结合防火墙策略的收紧、数据流量的清洗及网络构架的优化和主动监测告警系统，构建多层防护体系下的网络安全模型，为构建安全加固的网络架构提供支撑。

关键词

NAT穿越，网络安全，信息泄露，防火墙

Application Layer Leakage and Defense-in-Depth in NAT-Bounded Networks

Le Yang

Xinjiang ATMB Meteorology Center, Civil Aviation Administration of China, Urumqi Xinjiang

Received: September 15, 2025; accepted: October 20, 2025; published: October 29, 2025

Abstract

This paper examines the working principles of Network Address Translation (NAT) and demonstrates that the internal addresses concealed through network-layer address rewriting can be bypassed at the application layer, thereby undermining its security. By constructing experimental scenarios and replicating network attacks, we validate that certain security vulnerabilities can arise from the

文章引用: 杨乐. 基于 NAT 边界的应用层泄露与纵深防御研究[J]. 计算机科学与应用, 2025, 15(10): 287-295.
DOI: 10.12677/csa.2025.1510268

configuration and use of NAT technology. Attackers may exploit these vulnerabilities to penetrate NAT mappings and obtain the real IP addresses of internal servers, subsequently mapping the internal network topology. To address this network security vulnerability, this paper proposes combining NAT technology with tightening firewall policies, cleaning data traffic, optimizing network architecture, and an active monitoring and alarm system to build a network security model under a multi-layer protection system, providing support for building a secure and reinforced network architecture.

Keywords

NAT Traversal, Network Security, Information Leakage, Firewall

1. 引言

目前，基于 IPv4 的因特网已经运行多年，32 位 IPv4 只能提供大约 43 亿个地址，而其编址方案造成了很多地址空洞和浪费[1]，另一方面，智能终端的出现又加剧了地址的消耗，随着互联网技术的发展，NAT 如今已经成为计算机网络中的一个支撑级技术，它的出现，不仅有效缓解了 IPv4 地址短缺，也被普遍认为“NAT 即安全”而被广泛应用[2]。实际上，各类 NAT 应用带来的网络安全问题也愈发显著。NAT 的主要功能在于地址转换与复用，并未真正提供完善的安全防护机制。查阅相关文档，现有技术都集中在如何实现 NAT 穿透[3]，人们发现可通过多种手段绕过 NAT 的限制，例如利用 ICMP 协议进行网络探测、通过 DNS 隧道窃取数据，甚至借助用户误配置的 UPnP 功能打开内部网络的“后门”，借助自动化软件绘制基于漏洞的网络拓扑[4]。然而，在研究如何提高 NAT 技术使用的安全性方面研究却少之甚少。

2. NAT 技术基础与安全局限性分析

2.1. NAT 技术工作原理

NAT (Network Address Translation)是一种网络通信协议，该技术在网络层将私有网络中的内部 IP 地址转换为公网 IP 地址[5]，实现将内部服务或应用发布至公网、或者多台内部设备共享一个地址的功能，通过修改数据包的源地址和目标地址，将内部私有网络的 IP 地址与外部公网 IP 地址进行对应。NAT 能实现的功能主要有：地址转换、端口转换、连接追踪[6]。其工作原理是，NAT 设备会创建一个映射表，记录内部设备的 IP 地址、端口号及外部 IP 地址、端口号之间的对应关系，进行后续数据包的转发和回复[7]。这一过程的高效性保障了网络通信的正常运行，但 NAT 的有效性严重依赖于应用层的安全实践。

2.2. NAT 应用中的问题

NAT 对内部网络的模糊化，在 NAT 技术的保护下，内部网络结构对外不可见，外部主机无法直接获取内网设备的真实 IP 地址。NAT 穿越是允许网络应用程序能证明自身位于 NAT 转换设备之后，以此获得外部地址，并通过自动程序将端口映射为程序所使用的内部端口[8]。内网通过复用 IP 地址，将内网向外发送的数据包映射成合法地址。

但在某些特定条件下，网络层的转换可被绕过。首先是 IP 地址伪装，攻击者可以通过发送伪造的数

据包，造成 NAT 映射表错误映射，从而将数据包转发到错误的目标设备；其次是端口扫描和攻击，攻击者可以对 NAT 设备进行端口扫描，探测网络内部所有开放的端口和服务器地址，继而发动针对内部服务器和端口的攻击；再次是 DNS 劫持，攻击者可以通过篡改 DNS 设置，将用户发布的 DNS 查询重新定性到其指定的恶意地址，窃取用户信息；最后是 DDOS 攻击，攻击者发送大量的网络请求，占用该 NAT 设备的资源，造成正常的网络通信无法进行。

由此可见，NAT 的工作原理对于应用层发起的攻击或各种 NAT 穿越技术也是无能为力，所以对于这种静态的、传统的网络安全防护手段，应该与其他安全机制结合起来使用。

3. NAT 中 IP 泄露的技术路径分析

3.1. 应用层数据泄露

应用层数据泄露是造成 NAT 之后内部服务器 IP 地址暴露的一种重要途径，企业的对外信息发布 web 服务器一般采用 HTTP/HTTPS 协议，数据包响应的头部、报错界面或者返回的内部链接稍不注意就会返回真实的服务器或服务集群主机地址信息。还有就是建立 FTP 连接、在调用大数据平台 API 接口的时候，返回的数据包里都有可能是真实服务器地址以及原始的数据信息。

3.2. 网络层旁路探测

攻击者可以利用工具，向 NAT 设备发送其构造的数据包，并观察和记录 NAT 服务器的响应返回值和返回时间。由于 IP 包在经过路由器时 TTL 值会有所变化，因此可通过简单的 ping 或者 tracert 命令对公网 IP 地址进行探测，取回 TTL 值，并分析比较该值的变化。此外，可以通过扫描全 IP 地址网段，探测其内部哪些服务器是存活状态，且可以记录哪些服务器开放了 web 服务端口，对符合公网开放端口的服务器进行进一步查看，若内容与 NAT 映射之后的服务相同，就能推断出真实的服务器地址。

3.3. 社会工学信息拼凑

企业内部开发人员在论坛或发布的技术文档中无意间粘贴的截图或设备配置文件或技术贴有可能泄露到对外服务系统的源码，而不同的厂商在做项目时都有自己较为常用的密码命名方式，以上信息都有可能成为攻击者搜集的数据。通过公开的各类信息、钓鱼邮件、公开的服务器的系统版本都有为攻击者所使用，拼凑出有价值的信息，从而进一步实施精准攻击。

4. 针对 NAT 安全性加固

4.1. 第一层：NAT/防火墙设备强化

针对 NAT 与防火墙设备的强化策略，需用“最小化”原则加以配置策略。首先，应结合 PAT (Port Address Translation)技术，通过 IP 地址 + 端口的双重转换，若对外链路中存在多重三层网络设备，可进行多次 NAT 转换，以提高 NAT 的隐蔽性和安全性[9]。其次，缩紧防火墙策略，严格限制从外部到内部的访问流量，过滤异常的非法流量和数据包。记录经过防火墙的会话，同时开启 ACL 访问控制列表。冗余的策略往往给攻击者可乘之机，对防火墙策略定期开展审查和优化，可避免潜在的安全漏洞。最后，定期更新防火墙设备的固件版本和病毒特征库，通过更新可修复已知的漏洞，提升设备安全性。

4.2. 第二层：网络架构优化与隔离

在防火墙前端部署抗 DDOS 设备，对于大量的非法访问攻击进行阻断，同时在线路中串联入侵防御设备(IPS)进一步对数据包进行检测，分析和识别威胁，阻断常见的恶意攻击。此外，部署应用防火墙(WAF)，

可对于常见的攻击如 SQL 注入、脚本攻击、网页篡改行为等进行精准的防护，保障业务系统的安全性。在企业对外提供服务的网络构架中，设置 DMZ (隔离区) [10]，将对外提供服务的服务器部署在该区域，并与内网通过网闸等单向设备严格隔离，可以最大限度降低外部攻击对底层核心设备造成的影响。

4.3. 第三层：主动监控与响应

部署网络监控也是十分重要的，可以让维护人员及时地发现一些可能存在的安全隐患，在第一时间就看到有异常行为，比如一些可疑的连接，多次未授权的访问等，当监控系统发现异常的时候就会报警，运维人员就可以采取应对措施[11]。通过内、外网双视角渗透测试和漏洞扫描，可以模拟攻击者从内网、外网发现潜在的漏洞和薄弱点，也可以检测网络监控系统的可用性和有效性。对系统内各类设备的日志进行集中采集和相关事件的关联，可以快速定位异常行为，提高安全事件响应速度。

5. 实验验证与案例分析

5.1. 实验环境搭建

搭建气象信息服务网站，通过专线对用户提供跑道自动观测(Awos)数据、机场预报预警信息、机场多普勒雷达图、风云 4 号卫星云图等气象数据的实时网页展示[12]。设置核心区域、DMZ 区域、以及对外服务区域的三级网络架构。内部核心区中部署核心气象数据库系统，作为核心数据的存储和处理；DMZ 区中部署气象数据服务系统，通过将内部核心区的数据单向摆渡至 DMZ 的对外服务数据库中，再经由防火墙过滤发送至 2 台 WEB 服务器，结合 Nginx 负载均衡技术，将接收到的用户请求分发至不同的服务器上；在对外服务区中，通过防火墙作为网络边界，建立专线向用户提供前端数据展示。具体网络拓扑见图 1。

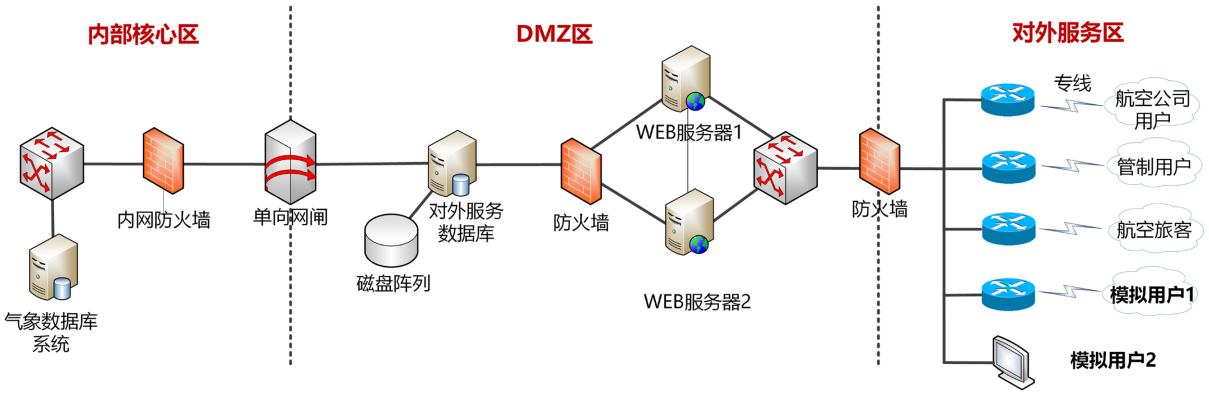

Figure 1. Network topology diagram of the experimental setup
图 1. 实验搭建网络拓扑图

通过该三级架构设计，将内网气象数据库中的气象数据通过单向网闸发送至 DMZ 区域的气象数据服务器。WEB 服务器 1 和 WEB 服务器 2 作为负载均衡的 Nginx 服务器进行反向代理[13]，实现高可用与并发处理。通过 DMZ 区和对外发布区之间的防火墙将负载均衡后的气象数据服务 web 网站发布至外网用户访问，NAT 转换后的公网 IP 为 172.20.1.20。在对外服务区域中部署模拟攻击终端，通过该终端，可访问 NAT 转换后的公网 IP 的服务网页(见图 2)。

5.2. 攻击复现

使用 NAT 转换后的 IP 地址访问气象数据服务网站时，通过查看开发者工具中的 Network 标签，观察到请求的响应头信息如下图中“Reest initiator chain”，其中暴露了服务器的真实 IP 地址信息(见图 3)。

Figure 2. Test accessing the web page after NAT translation
图 2. 测试访问 NAT 转换后的网页

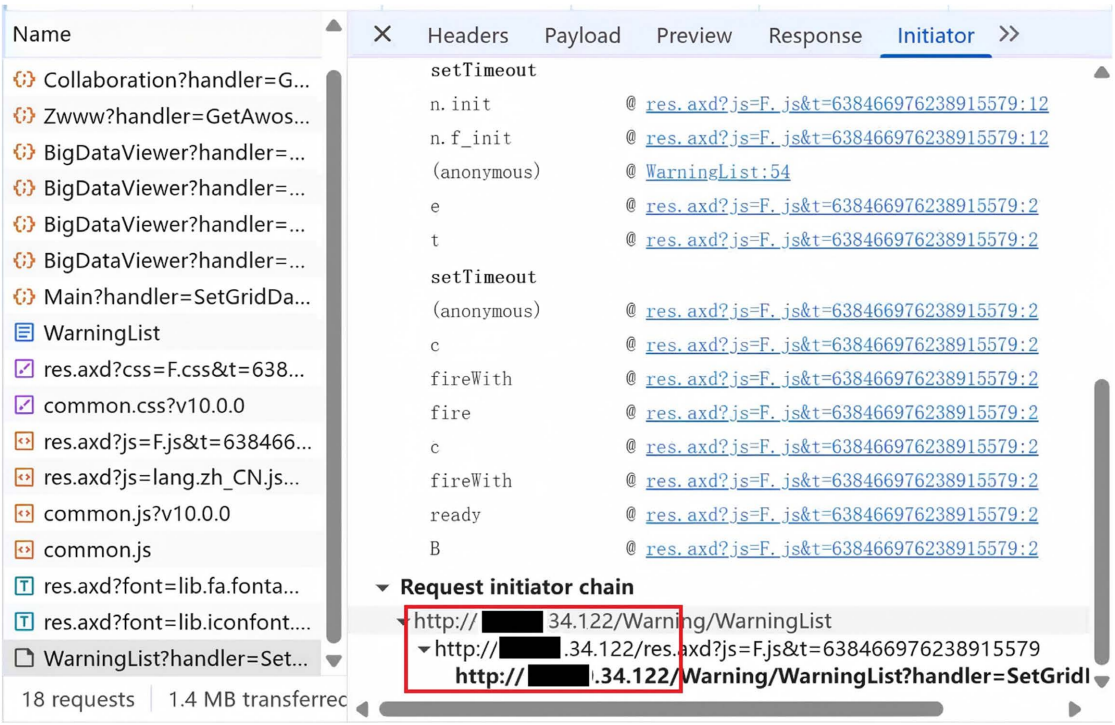

Figure 3. Address leakage in the browser
图 3. 浏览器中的地址泄露

通过在模拟攻击主机上使用扫描类工具(本文采用 IP Scanner)对浏览器中返回的真实地址段进行扫描。通过对该 10 网段进行探测，探测结果如下图所示，在没有设置禁 ping 策略时，通过该主机可扫描到系统内部真实服务器地址 254 个，其中活动主机 72 个，开放端口 23 个(见图 4)。

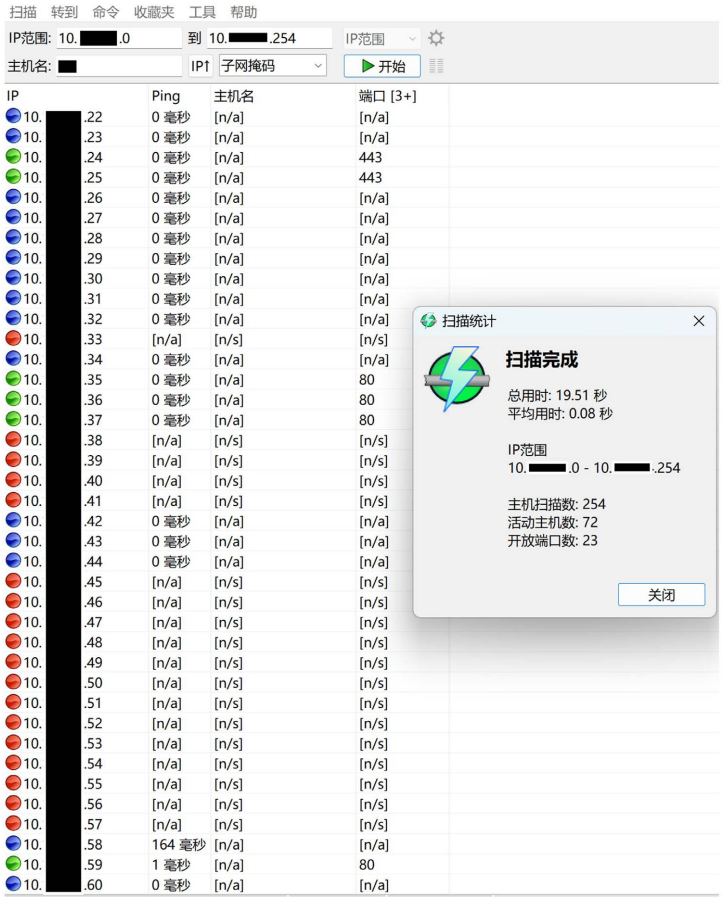

Figure 4. Tool scan results
图 4. 工具扫描结果

通过已扫到的开放 80 端口和 443 端口的 IP 主机地址。进一步通过 tracert 跟踪筛选，就可以清楚地看到走过的网络路径地址(见图 5)，绘制出系统的内部网络拓扑结构。

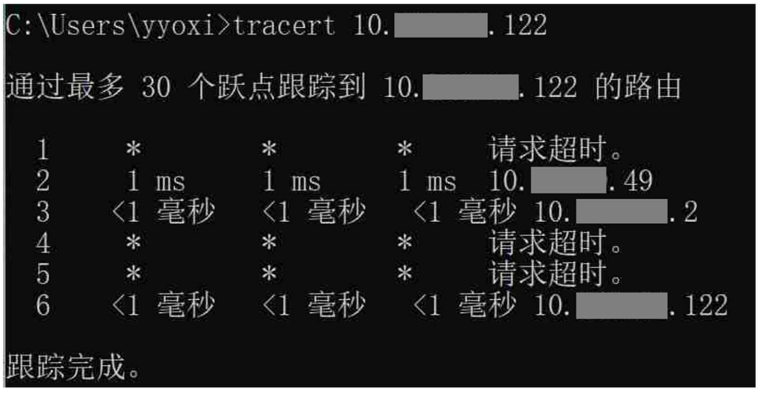

Figure 5. Tracert network address tracing results
图 5. Tracert 跟踪网络地址结果

通过 IP 地址和暴露端口进行综合推断，在模拟终端上可以直接访问真实网址(见图 6)访问成功，说明攻击者可以穿越防火墙的 NAT 转换，通过网络路径直连内网服务。

Figure 6. Access the server webpage using its real address
图 6. 访问真实地址的服务器网页

通过以上步骤成功复现了基于信息泄露的内网直连攻击，证明了只通过防火墙做 NAT 转换能提供给外网访问一个映射关系，但并不能阻止攻击者通过响应头、DNS 解析、错误配置等方式获取内网信息，NAT 的配置使用不当，将暴露出网络边界防御的安全问题。

5.3. 防御策略有效性验证

优化防火墙策略，加入禁止 icmp 的出入站规则，把连接用户侧的端口状态禁止 ping，并对不同区域间的流量实施进一步策略禁止控制，设置完成后，利用扫描工具可以发现内部服务器的响应并及时拦截，阻止简单的 Ping 探测获取设备存活状态，进一步使用 Nmap 工具以及 IPScanner 软件扫描端口开放状态时，发现防火墙策略有效地屏蔽了非授权端口的探测行为，只有映射后的虚拟地址能够正常响应，活动主机数由 72 降至 2 (见图 7)。

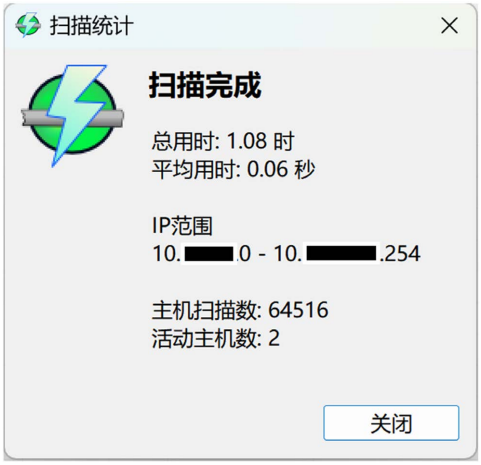

Figure 7. Scan results after firewall policy optimization
图 7. 优化防火墙策略后扫描结果

如下图，通过防御策略的调整后，扫描工具已经无法获取到内部真实 IP 的响应信息了，只能获取到与防火墙相连的接口为活动地址，再次对原来探测到的真实地址进行跟踪，均显示为请求超时不可达(见图 8)。

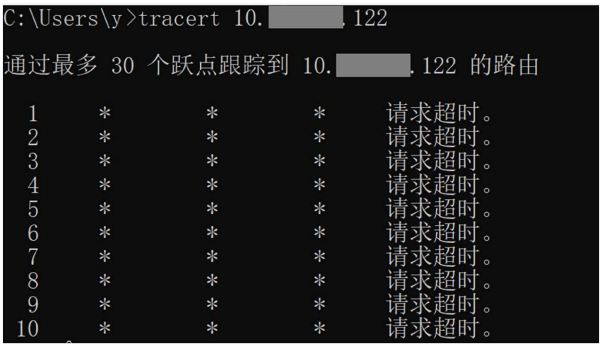

Figure 8. Tracert request timed out
图 8. tracert 追踪地址超时

然而，此时从终端依然可以打开转换前真实地址的服务网页。经排查，由于测试终端为防火墙上端口直连设备，处于同一内部网络区间(直连地址段无需配置路由)，所以仍可通过二层转发直接访问内部服务。由此将防火墙跟用户连接的线路中串联入侵防御设备(IPS)、出口路由器及抗 DDOS 攻击设备，网络拓扑图见图 9。

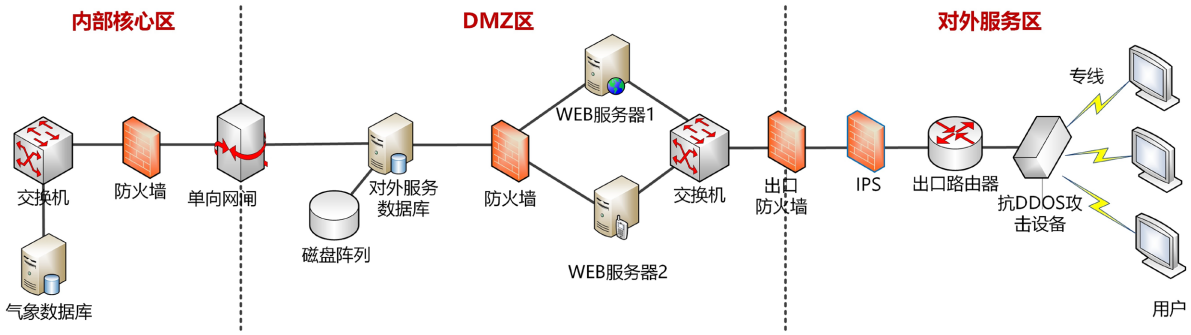

Figure 9. Optimized network topology diagram
图 9. 优化后的网络拓扑图

优化后的网络拓扑，结合 IPS 入侵防御、出口路由器二次地址转换以及抗 DDOS 攻击进行流量清洗。经测试，此时从外部用户端进行各类扫描，已无法探测到任何内部服务响应，真实服务器地址也得以隐藏。即使攻击者使用社工等方式获取到内部地址信息，此时也无法建立有效连接，防御策略实现闭环。

5.4. 实验结果

通过以上实验，防火墙 NAT 的有效性依赖于应用层的安全防护，如应用层配置使用不当有可能造成内网信息泄露，攻击者借助查看暴露在 http 响应里的信息，再配合 IP 扫描工具以及 tracert、TTL 等，就能找到内网真实的地址，从而做到直接连接到真实的服务器上，内网结构全然暴露，防御的边界也就成了摆设。因此，缺乏防火墙访问策略的精确把控，没有入侵检测等防御手段，单纯依靠地址转换，很难抵挡住攻击行为，要构建稳固的网络安全防线，就得把 NAT 技术同诸多防御设备和策略联系起来使用，以此保护内部信息的安全。

6. 未来工作展望

NAT 技术为当前互联网解决 IPv4 地址紧张的问题提供了解决方案，也是保证网络安全重要的一环，未来随着互联网的发展，网络安全威胁会越来越多，以及 IPv6 地址的普及，网络边界将越来越模糊，所以要提升对新型攻击的防护能力，结合人工智能，提供更加灵活、智能、自动化的防御方式，利用深度学习和大数据分析，实现及时识别异常行为，迅速主动地阻断潜在的攻击路径，使安全防护从被动封堵到主动感知。

参考文献

[1] 张立斌, 钟瑶. IPv6 在下一代通信网中的协议扩展与性能优化[J]. 无线互联科技, 2025, 22(2): 8-11.

[2] Huston, G., 李想. 2024 年 IPv6 地址分配和互联网前景展望——2024 年全球 IP 地址回顾(三) [J]. 中国教育网络, 2025(6): 29-33.

[3] 郭慧. IPSec 的 NAT 穿越技术应用[J]. 自动化应用, 2024, 65(10): 282-284.

[4] 李腾飞, 李强, 余祥, 等. 基于拓扑漏洞分析的网络安全态势感知模型[J]. 计算机应用, 2018, 38(S2): 157-163, 169.

[5] 王格. 基于华为防火墙的双向 NAT 技术研究与实现[J]. 信息记录材料, 2025, 26(9): 214-217.

[6] 刘风华, 丁贺龙, 张永平. 关于 NAT 技术的研究与应用[J]. 计算机工程与设计, 2006(10): 1814-1817.

[7] 白伟华, 李吉桂. NAT 技术及其穿越方案研究[J]. 计算机科学, 2005(8): 44-45, 222.

[8] 黄亮. 一个基于 UDP 协议的 P2P 即时通讯软件的设计与实现[D]: [硕士学位论文]. 武汉: 华中科技大学, 2011.

[9] 陈恒勋, 闫永航, 孟丹, 等. NAT 穿越技术研究[J]. 现代信息科技, 2020, 4(6): 94-98.

[10] 张婷, 姜园园, 刘梦荞, 等. 计算机视觉与机器学习在 IT 运维中的应用[J]. 电子技术, 2024, 53(6): 374-375.

[11] 杨乐, 朱国栋, 陈福康. 基于网络安全域的民航气象信息服务系统设计[J]. 民航管理, 2019(6): 72-74.

[12] 杨乐, 朱国栋, 孙少明. 民航气象数据存储管理系统设计与应用[J]. 民航学报, 2022, 6(1): 65-68.

[13] 陈思. 基于 Nginx 和 Redis 的高并发 Web 场景下缓存的研究与设计[D]: [硕士学位论文]. 抚州: 东华理工大学, 2021.