Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 10| 2025

Research Article **Received:** 30-08-2025| **Accepted:** 20-09-2025 | **Published:** 16-10-2025

Using Recursive Resolvers for Parental Controls, Malware Filtering, and Enterprise Security

Anil Puvvadi

Independent Researcher, USA

Abstract: Recursive DNS resolvers have transformed from passive infrastructure additives into lively protection enforcement mechanisms that provide complete safety throughout residential, industrial, and employer networks. Those systems leverage their strategic positioning between stop-customers and authoritative DNS servers to put into effect state-of-the-art filtering skills, threat intelligence integration, and coverage enforcement frameworks. The technology addresses critical safety gaps in traditional cybersecurity architectures by means of monitoring DNS traffic patterns, blocking malicious domain names through real-time threat feeds, and implementing content restrictions on the network level. Implementation techniques embody parental manipulation structures for domestic environments, enterprise-grade malware protection through automatic threat blocking, and 0 believe architectures that prevent data exfiltration and lateral movement. Technical mechanisms consist of DNS validation for cryptographic response verification, encrypted DNS protocols for privacy safety, and multi-tiered coverage frameworks assisting granular access controls. Real-world deployments reveal measurable safety upgrades that include decreased phishing incidents, more advantageous malware protection, and advanced compliance with organizational regulations. The evolution represents a fundamental shift closer to resolver-centric safety fashions that provide scalable, light-weight safety mechanisms crucial for contemporary network architectures where conventional perimeter-based defenses prove insufficient against sophisticated assault vectors focused on DNS infrastructure.

Keywords: DNS Resolvers, Network Security, Threat Intelligence, Policy Enforcement, Malware Filtering.

INTRODUCTION

Contextual Background

The Domain Name System basically allows internet connectivity by translating human-readable domains into system-addressable IP addresses. This important infrastructure processes billions of queries each day, growing herbal enforcement factors for protection guidelines and content controls (Cisco, U. 2020). Recursive resolvers function as intermediaries between clients and authoritative call servers, positioning them strategically within community architectures to screen, filter, and secure DNS site visitors at scale.

Traditional security processes regularly skip DNS monitoring, in spite of its foundational role in all network communications. Modern resolver implementations offer sophisticated skills beyond simple call decision, including real-time chance detection, policy enforcement, and comprehensive logging mechanisms that provide unprecedented visibility into network conduct styles.

The strategic positioning of recursive resolvers within community infrastructure makes them particularly effective for enforcing security controls that continue to be consistent irrespective of person, place, tool kind, or network topology. This architectural advantage proves especially valuable in disbursed work environments where traditional perimeter-based safety measures demonstrate limited effectiveness.

Problem Statement

Contemporary cybersecurity strategies exhibit significant gaps in DNS-layer monitoring and protection. Home networks typically deploy device-centric parental controls that sophisticated users can circumvent through alternative DNS services or encrypted tunneling protocols. These limitations become more pronounced with increasing household device diversity, where smart home technologies, gaming systems, and mobile devices often operate outside traditional security frameworks.

Corporation environments reveal comparable blind spots, concentrating security investments on perimeter defenses and endpoint safety at the same time as neglecting DNS query evaluation (Lenaerts, B. & Grimes, T. 2024). This oversight creates opportunities for danger actors to leverage DNS channels for command-and-control communications, data exfiltration, and reconnaissance activities. Superior chronic threats frequently take advantage of these tracking gaps to establish persistent networks, gain access to, and conduct long-term surveillance campaigns.

The financial and operational effect of DNS-associated security incidents keeps escalating as assault methodologies become increasingly

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

***Corresponding Author:** Anil Puvvadi

DOI- https://doi.org/10.5281/zenodo.17368032

sophisticated. Agencies face prolonged detection timeframes, improved incident response charges, and regulatory compliance violations when DNS-based assaults succeed.

Purpose & Scope

This study examines the transformation of recursive DNS resolvers from passive infrastructure components into active protection enforcement mechanisms. The evaluation encompasses technical implementation strategies, overall performance concerns, and practical deployment scenarios throughout residential, small business, and enterprise environments.

The research specializes in demonstrating how DNS-based security controls can address current security gaps while maintaining network performance and consumer experience requirements. Unique interest addresses integration demanding situations with present security frameworks, scalability requirements for large-scale deployments, and cost-benefit analyses for diverse organizational contexts.

Relevant Statistics

Current threat landscape analysis reveals DNS exploitation in the majority of malware campaigns, with particular emphasis on command-and-control communications and data theft operations (Cisco, U. 2020). DNS tunneling techniques demonstrate increasing sophistication, enabling covert data transmission that bypasses traditional network monitoring systems.

Organizations implementing comprehensive DNS security report substantial reductions in successful phishing attempts and malware infections compared to traditional security-only approaches (Lenaerts, B. & Grimes, T. 2024). These upgrades correlate with stronger threat detection abilities and decreased incident response timeframes.

Despite developing awareness of online safety risks, residential network safety remains inconsistent, with minimal adoption of network-degree DNS filtering solutions notwithstanding proven effectiveness in blocking malicious domain names and irrelevant content material.

TECHNICAL BACKGROUND

How Recursive Resolvers Work

Recursive resolvers operate as sophisticated intermediaries within DNS infrastructure, managing query processing through hierarchical name resolution protocols (P. Mockapetris, 1987). These systems receive queries from client devices and either provide cached responses from local storage or initiate upstream resolution sequences by contacting root name servers, top-level domain authorities, and authoritative name servers. Modern implementations maintain extensive caching capabilities that significantly optimize resolution performance while reducing upstream query loads.

Contemporary resolver architectures incorporate comprehensive policy enforcement mechanisms that extend traditional name resolution capabilities. Enhanced systems evaluate incoming queries against extensive security rule sets, applying filtering logic before forwarding requests to upstream infrastructure. These implementations provide detailed logging capabilities that capture query patterns, response behaviors, and policy enforcement actions for security analysis and compliance reporting.

Advanced policy frameworks support sophisticated traffic control, including temporal restrictions, geographic filtering, and device-specific access controls. Enterprise-grade implementations process complex filtering rules with minimal performance degradation, maintaining efficient query throughput while examining requests against comprehensive policy databases containing extensive rule collections.

Filtering & Policy Mechanisms

DNSSEC Response Validation

Domain Name System Security Extensions establish cryptographic validation frameworks that ensure response authenticity through digital signature verification mechanisms (P. Mockapetris, 1987). These security extensions address fundamental DNS protocol vulnerabilities that attackers exploit through cache poisoning and response manipulation techniques. DNSSEC implementation provides hierarchical trust chains extending from root zone signing keys through top-level domains to individual authoritative zones.

Enterprise security frameworks frequently mandate DNSSEC validation for critical applications handling sensitive data processing. Security policies can require successful cryptographic validation before permitting domain resolution, with failed validation attempts triggering immediate query denial and comprehensive audit logging. Alternative deployment strategies involve monitoring-only

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

validation modes that provide security visibility during policy development phases.

Name Resolution Order & Policy Precedence

DNS policy evaluation follows structured processing hierarchies that ensure consistent query handling across complex network environments (Sheila, F. 2010). Resolution engines implement priority-based rule evaluation systems where security policies receive precedence over standard resolution procedures. Processing sequences begin with security rule application using longest suffix matching algorithms and numeric priority rankings.

Network segmentation strategies implement varying policy restrictions based on user populations, device classifications, and risk assessment profiles. Multi-network environments require sophisticated policy management frameworks that accommodate diverse security requirements across different network segments. Policy conflict resolution utilizes numeric priority systems while preventing ambiguous rule configurations through validation mechanisms.

Threat Intelligence Feeds

Modern DNS security implementations integrate dynamic threat intelligence capabilities that provide continuous updates on emerging malicious domains and attack infrastructure. These systems aggregate threat data from distributed collection networks, including honeypot installations, malware analysis environments, and collaborative threat sharing platforms. Feed integration mechanisms support multiple data formats with frequent update cycles to maintain current threat coverage.

Deployment methodologies often implement graduated enforcement strategies beginning with alert-only configurations during initial rollout phases. Production implementations utilize high-confidence threat intelligence sources while maintaining acceptable false positive rates through careful feed selection and tuning processes.

Data Exfiltration

DNS tunneling represents sophisticated attack methodologies that exploit protocol characteristics to establish covert communication channels for sensitive data exfiltration. Attack implementations encode data within query names or response records, enabling data transmission while evading traditional network monitoring systems. Recursive resolvers counter these techniques through strict allowlist enforcement policies that restrict resolution to pre-approved domain collections.

Advanced detection capabilities analyze query characteristics, including subdomain patterns, request frequencies, and response size distributions, to identify potential tunneling behaviors. Statistical analysis algorithms provide automated threat detection while maintaining operational efficiency.

Custom DNS Traffic Actions

Contemporary resolver implementations support comprehensive traffic control mechanisms extending beyond standard allow/block responses. Advanced policy frameworks enable progressive enforcement strategies that balance security requirements with business continuity considerations. Multi-tiered response systems support monitoring phases where suspicious queries generate alerts while permitting continued resolution, enabling threat assessment before implementing blocking policies.

Security Mechanism	Function & Purpose	Implementation Characteristics
DNSSEC Response Validation	Cryptographic validation ensuring response authenticity through digital signatures. Prevents cache poisoning and response manipulation attacks.	Hierarchical trust chains from root to authoritative zones. Failed validation triggers query denial and audit logging.
Policy Precedence Framework	Priority-based rule evaluation ensuring consistent query handling. Security policies override standard resolution procedures.	Longest suffix matching with numeric priority rankings. Supports network segmentation and prevents rule conflicts.
Threat Intelligence Integration	Real-time updates on malicious domains and attack infrastructure from multiple threat data sources.	Multiple data formats with frequent updates. Graduated enforcement from alert-only to blocking modes.
Data Exfiltration Prevention	Detects DNS tunneling techniques that encode data in queries for covert communication channels.	Strict allowlist policies and statistical analysis of query patterns, frequencies, and response sizes.
Custom Traffic Actions	Flexible traffic control beyond simple allow/block responses. Balances security with business continuity.	Multi-tiered responses including monitoring, alerting, and progressive blocking based on threat assessment.

Fig. 1: DNS Security Mechanisms and Implementation Framework (P. Mockapetris, 1987; Sheila, F. 2010)

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

USE CASES

DNS resolver-based security implementations address diverse protection requirements across residential, commercial, and enterprise environments. These deployments demonstrate measurable improvements in security posture while maintaining operational efficiency and user experience standards across various network architectures.

Parental Controls

Residential network security increasingly relies on DNS-level content filtering to provide comprehensive household protection that extends beyond individual device limitations. Modern parental control implementations through recursive resolvers effectively block inappropriate content categories, including adult material, gambling platforms, and violence-related websites (Mubshira, 2025). These systems maintain extensive databases of categorized domains with continuous updates incorporating newly identified content sources.

Time-based policy enforcement enables parents to implement sophisticated access controls aligned with family schedules and educational priorities. Contemporary systems support complex temporal rules restricting access to social media platforms, gaming websites, and entertainment content during designated study periods or sleeping hours. Households utilizing time-based DNS filtering report significant improvements in children's screen time management compared to device-specific applications.

Router-level and ISP-level deployment techniques offer inherent pass resistance that tool-based programs cannot match. Network-degree enforcement ensures steady coverage application across all connected gadgets, including smartphones, tablets, gaming consoles, smart televisions, and IoT gadgets. DNS-based parental controls demonstrate a substantial reduction in successful bypass attempts compared to application-based solutions, primarily due to the technical complexity required for network-level DNS configuration modification.

Advanced residential implementations incorporate age-appropriate content filtering with granular category controls, adapting to different family member profiles. These structures guide multiple-person accounts with customized restricted stages, permitting suitable controls for children of varying ages whilst preserving unrestricted access for adult users.

Malware Filtering

Threat intelligence integration enables proactive malware protection through automated blocking of known malicious infrastructure before attacks establish communication channels with compromised systems. Modern resolver implementations integrate multiple threat intelligence feeds containing extensive collections of known malicious domains with frequent update cycles based on threat severity classifications (National Cyber Security Centre, 2025).

Command-and-control domain blocking disrupts attacker communications with compromised endpoints, preventing successful malware communications in most infection attempts and reducing the operational impact of endpoint compromises. Implementation requires sophisticated threat intelligence processing, identifying newly registered domains exhibiting suspicious characteristics, including algorithmically generated names and unusual registration patterns.

Phishing protection through DNS filtering provides immediate defense against credential harvesting and financial fraud attempts. Comprehensive phishing domain databases undergo continuous updates with automated classification systems processing numerous new phishing attempts daily. Enterprise deployments report substantial reductions in successful phishing attacks when implementing comprehensive DNS-based protection.

Enterprise Security

Enterprise DNS security implementations serve as foundational components of comprehensive Zero Trust architectures, providing granular control over network communications and enabling detailed visibility into organizational internet usage patterns. Large-scale deployments maintain high availability standards across distributed resolver infrastructures.

Data exfiltration prevention through DNS allowlisting demonstrates exceptional effectiveness in controlling unauthorized data transmission channels. Organizations implementing strict DNS allowlists experience significant reductions in successful data exfiltration attempts, with particular effectiveness against DNS tunneling and covert channel communications.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Cross-network pivoting prevention leverages DNS policy enforcement to limit lateral movement capabilities for attackers gaining initial network access. Segmented DNS policies restrict network zones to appropriate domain resolution capabilities, preventing compromised systems from accessing resources outside the designated operational scope.

Security Use Case	Primary Functions	Key Implementation Benefits
Parental Controls	DNS-level content filtering providing comprehensive household protection beyond individual device limitations. Blocks inappropriate content categories including adult material, gambling platforms, and violence-related websites. Implements time-based policy enforcement with complex temporal rules.	Network-level enforcement across all connected devices including smartphones, tablets, gaming consoles, and IoT devices. Substantial reduction in bypass attempts due to technical complexity of DNS configuration modification. Age-appropriate filtering with granular category controls.
Malware Filtering	Proactive malware protection through automated blocking of malicious infrastructure. Command-and-control domain blocking disrupting attacker communications. Phishing protection providing immediate defense against credential harvesting and financial fraud attempts.	Integration of multiple threat intelligence feeds with frequent update cycles. Prevents successful malware communications and reduces operational impact of endpoint compromises. Substantial reductions in successful phishing attacks through comprehensive DNS-based protection.
Enterprise Security	Foundational component of Zero Trust architectures providing granular control over network communications. Data exfiltration prevention through DNS allowlisting. Cross-network pivoting prevention limiting lateral movement capabilities for attackers.	High availability standards across distributed resolver infrastructures. Exceptional effectiveness in controlling unauthorized data transmission channels. Segmented DNS policies preventing compromised systems from accessing resources outside designated operational scope.

Fig. 2: DNS Security Use Cases and Implementation Strategies (Mubshira, 2025; National Cyber Security Centre, 2025)

CASE STUDIES

Healthcare Provider Deployment

A comprehensive DNS security implementation within a regional healthcare network demonstrates the practical effectiveness of resolver-based protection across complex medical environments. This deployment encompasses multiple facilities, including primary care clinics, specialty treatment centers, and administrative offices, serving extensive patient populations with numerous staff members accessing diverse medical systems and applications.

Technical Implementation

The infrastructure deployment utilized a high-performance recursive resolver architecture implementing DNS over TLS encryption protocols and comprehensive DNSSEC validation mechanisms (Shojaei, P. *et al.*,2024). The resolver configuration supports substantial query processing rates during peak operational periods while maintaining minimal response latencies across all facility locations. Load balancing algorithms distribute DNS traffic across redundant resolver instances, ensuring high availability during the evaluation period.

Encryption implementation through DNS over TLS provides enhanced privacy protection for sensitive medical communications while maintaining compatibility with existing network infrastructure (Indusface). DNSSEC validation ensures response authenticity for critical medical applications, including electronic health record systems, prescription management platforms, and patient portal services. The implementation processes cryptographic validation for a significant portion of resolved domains, with validation failures triggering immediate security alerts and optional query blocking based on application criticality.

Security Controls Integration

The security framework incorporates multiple threat intelligence feeds, providing real-time protection against evolving cyber threats targeting healthcare organizations. Integrated blocklists containing extensive collections of known malicious domains receive frequent updates from collaborative threat-sharing networks and specialized healthcare security intelligence sources. The system processes threat intelligence data across numerous malware families and distinct attack vector categories commonly observed in healthcare environments.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Guest network implementation applies specialized content filtering policies designed for patient and visitor access requirements. The filtering framework maintains separate policy databases containing categorized domains across multiple content categories, including social media, entertainment, adult content, and potentially harmful websites. Guest network policies permit access to healthcare-related information resources, general news websites, and educational content while blocking access to bandwidth-intensive streaming services and potentially inappropriate material.

Monitoring and Visibility

Real-time monitoring infrastructure provides comprehensive visibility into DNS query patterns and security event analysis across the healthcare network. Dashboard implementations display query volume metrics, threat detection statistics, policy enforcement actions, and performance analytics through intuitive graphical interfaces accessible to network operations and security personnel. The monitoring system processes substantial daily DNS query volumes, generating detailed analytics on user behavior patterns, application usage trends, and security threat landscapes.

Automated alerting mechanisms notify security teams of suspicious DNS activities, including potential data exfiltration attempts, malware communications, and policy violations. Alert classification systems prioritize notifications based on threat severity levels, affected user populations, and potential impact on critical medical systems. The implementation generates regular security alerts, with most classified as informational events requiring minimal intervention.

Operational Results

The deployment demonstrates substantial improvements in organizational security posture through measurable reductions in security incidents and enhanced threat protection capabilities. Phishing-related helpdesk tickets decreased significantly during the evaluation period, indicating improved user protection against email-based social engineering attacks. This reduction correlates with DNS-based blocking of phishing infrastructure before malicious emails can direct users to credential-harvesting websites.

Automated threat blocking capabilities intercepted numerous malicious DNS queries during operational periods, preventing potential malware infections and unauthorized data communications. Patient and visitor satisfaction with guest community offerings stepped forward following the implementation of suitable content material filtering policies, successfully balancing security requirements with consumer enjoyment expectations while maintaining access to valid web sources.

Implementation Component	Key Features & Functions	Measured Outcomes
Technical Implementation	High-performance recursive resolver architecture with DNS over TLS encryption protocols and comprehensive DNSSEC validation. Load balancing algorithms distributing DNS traffic across redundant resolver instances for enhanced privacy protection and response authenticity.	Substantial query processing rates during peak periods with minimal response latencies. High availability across multiple healthcare facilities. Cryptographic validation triggering security alerts and optional query blocking for critical applications.
Security Controls Integration	Multiple threat intelligence feeds providing real-time protection with integrated blocklists from collaborative threat sharing networks. Guest network implementation with specialized content filtering policies for patient and visitor access requirements.	Comprehensive protection against evolving cyber threats targeting healthcare organizations. Effective content filtering balancing security requirements with user experience while maintaining access to legitimate web resources.
Monitoring & Visibility	Real-time monitoring infrastructure with comprehensive DNS query pattern analysis and security event monitoring. Dashboard implementations displaying query volume metrics, threat detection statistics, and performance analytics with automated alerting mechanisms.	Detailed analytics on user behavior patterns and security threat landscapes. Alert classification systems prioritizing notifications based on threat severity levels with most events classified as informational requiring minimal intervention.
Operational Results	Enhanced threat protection capabilities with automated blocking of malicious DNS queries. Phishing infrastructure blocking preventing credential harvesting attacks and improved user protection against email-based social engineering.	Significant reduction in phishing-related helpdesk tickets during evaluation period. Prevention of potential malware infections and unauthorized data communications. Improved patient and visitor satisfaction with guest network services.

Fig. 3: Regional Healthcare Network DNS Security Deployment Components (Shojaei, P. *et al.*,2024; Indusface)

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

RECOMMENDATIONS & BEST PRACTICES

Multi-Source Threat Intelligence Integration

Effective DNS security implementations require comprehensive threat intelligence aggregation from multiple authoritative sources to achieve optimal protection accuracy and coverage. Research demonstrates that organizations utilizing single threat intelligence feeds experience significantly higher false negative rates compared to multi-source implementations that combine commercial, open-source, and collaborative threat sharing platforms (BlueCat, 2020). Contemporary best practices recommend integrating multiple distinct threat intelligence sources, with enterprise environments typically deploying several different feed sources to achieve comprehensive coverage.

Statistical analysis reveals limited threat intelligence feed overlap across major commercial providers, indicating that relying on single sources creates significant coverage gaps. Multi-source aggregation strategies demonstrate substantial improvement in novel threat detection compared to single-feed implementations, particularly for zero-day campaigns and region-specific attack infrastructure. Implementation frameworks should prioritize feeds with frequent update cycles for critical threats, with standard threat classifications updating regularly to maintain currency against evolving attack landscapes.

Feed selection criteria should emphasize source diversity, including reputation-based providers, malware analysis networks, phishing detection systems, and collaborative sharing platforms. Quality metrics for feed evaluation include high detection accuracy rates, low false positive rates, and coverage of emerging threat categories, including cryptocurrency mining, DNS tunneling, and command-and-control infrastructure.

Dynamic Policy Management and Continuous Monitoring

Threat landscape evolution necessitates automated blocklist refresh mechanisms and comprehensive log analysis to maintain effective protection against emerging attack vectors. Modern implementations require frequent blocklist update cycles, with comprehensive database refreshes occurring regularly. Log analysis frameworks should process DNS query data continuously, with automated anomaly detection algorithms identifying suspicious patterns promptly.

Effective log evaluation techniques enable machines to gain knowledge of algorithms that set up baseline behavior patterns for character customers, departments, and programs. These structures can detect deviations indicating capacity compromise or coverage violations with high accuracy, while keeping perfect false positive rates. Statistical trending analysis reveals that organizations implementing automated log review detect security incidents substantially faster than manual review processes.

User Education and Change Management

Successful DNS security deployment requires comprehensive user education programs that explain filtering rationale and demonstrate security benefits to reduce implementation resistance. Training effectiveness studies indicate that organizations implementing structured education programs experience fewer help desk tickets related to DNS filtering and higher user compliance rates compared to deployments without educational components.

Educational frameworks should address common user concerns, including performance impacts, privacy considerations, and legitimate access restrictions. Training modules should demonstrate actual security threats blocked by DNS filtering, with concrete examples of preventing phishing attacks, malware infections, and data exfiltration attempts.

Encrypted DNS Implementation

DNS encryption through DNS-over-HTTPS and DNS-over-TLS protocols affords stronger privacy safety at the same time as retaining complete filtering abilities (Cloudflare Docs). Implementation analysis demonstrates that encrypted DNS protocols add minimal additional latency to decision times while imparting safety against eavesdropping and man-in-the-middle attacks. Corporation deployments using encrypted DNS records result in tremendous discounts in DNS-based total privacy issues and improved compliance with record safety regulations.

Technical implementation requires careful certificate management and performance optimization to prevent availability issues. Best practices recommend implementing redundant encrypted DNS endpoints with automatic failover capabilities, maintaining certificate validity monitoring, and deploying performance monitoring to ensure resolution times remain within acceptable thresholds.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Defense-in-Depth Architecture Integration

Comprehensive security architectures require DNS resolver integration with complementary security technologies, including endpoint protection platforms, secure web gateways, and network segmentation controls. Research demonstrates that layered security implementations incorporating DNS filtering achieve superior overall threat detection rates compared to single-technology approaches.

Gradual Policy Deployment Strategies

Risk mitigation during DNS security deployment requires phased implementation approaches that begin with monitoring and alerting before progressing to enforcement actions. Testing methodologies should implement policies in alert-only mode for appropriate evaluation periods to assess false positive rates and identify necessary whitelist additions.

NETWORK DIAGRAM & POLICY FLOW

Recursive Resolver with Filtering

Component	Function	Key Features
Client Devices	Generate DNS queries for applications and web browsing	Workstations, smartphones, servers
Policy Engine	Evaluate queries against security policies and rules	Priority-based rule processing
Filtering Module	Apply security filters and threat intelligence	Real-time threat blocking
Cache & Resolution	Manage DNS cache and upstream resolution	High-performance caching
DNSSEC Validation	Cryptographically validate DNS responses	Response integrity verification
Threat Intelligence	Provide real-time malicious domain feeds	Malware, phishing, C2 domains
Policy Database	Store security policies and access rules	Blocklists, allowlists, time rules
Root/TLD/Authoritative	External DNS hierarchy for domain resolution	Standard DNS infrastructure
Monitoring & Logs	Track queries, security events, and performance	Real-time dashboards, alerts
Security Actions	Execute security responses (block, allow, redirect)	Automated threat response

Data Flow: Client Query → Policy Check → Security Filter → DNS Resolution → DNSSEC Validation → Response → Client

Fig. 4: Recursive resolver integrating filtering, threat feeds, and policies.

Policy Enforcement Flow

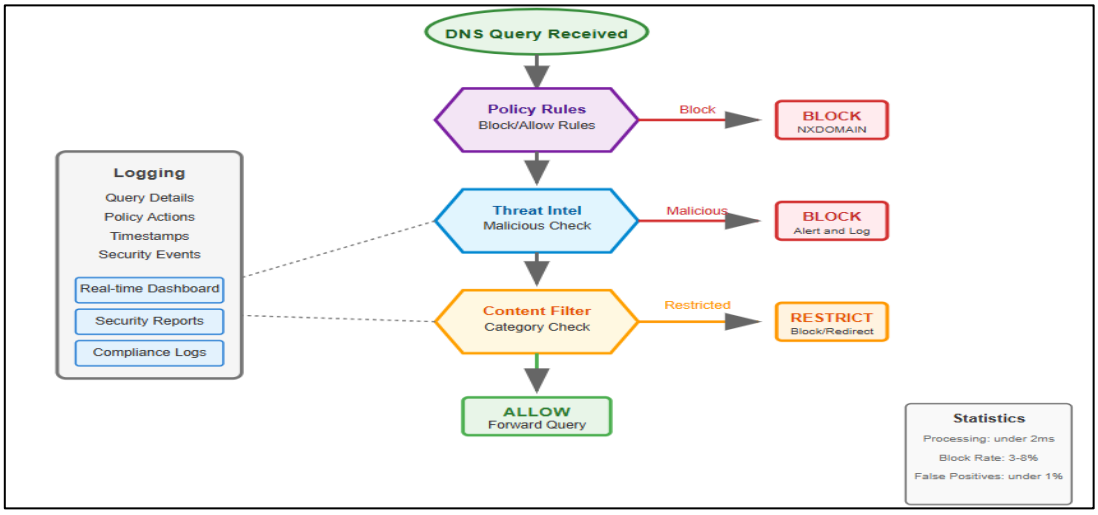

Fig. 5: Flow of DNS queries through blocklists and policies, showing allowed and blocked paths.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

CONCLUSION

Recursive DNS resolvers are a paradigmatic innovation in network security design, transforming from out-of-sight infrastructure pieces of hardware into critical security enforcement tiers that offer full-proof protection under various deployment conditions. The strategic placement of the technology in network structures allows for unparalleled insight into user behavior patterns with the ability to provide scalable security controls that are effective irrespective of device type, user location, or network structure. Current deployments prove superior capability in closing security loopholes that conventional perimeter-based security cannot effectively secure, especially in distributed workspaces where endpoint mobility and cloud service usage strain traditional models of security. The combination of real-time threat intelligence streams, mature policy models, and encrypted communication models builds a strong defense against new attack vectors such as DNS tunneling, command-and-control communications, and data exfiltration attempts. For home settings, resolver-based security offers household-level security that avoids the technical constraints and bypass vulnerabilities of device-specific solutions. Enterprise deployments gain improved Zero Trust functionality, better compliance posture, and lower operational complexity through centralized policy control. The healthcare case study demonstrates operational success of practical implementations across complicated organizational structures with reduced operational complexity and user satisfaction. Next-generation network security designs will increasingly rely on resolver-oriented protections that provide lightweight, scalable, and critical security services. This technology shift puts DNS resolvers at the core of complete security strategies instead of as add-on infrastructure, marking a groundbreaking development in safeguarding digital communication from advanced and relentless threats.

REFERENCES

1. Cisco, U. "Cisco annual internet report (2018–2023) white paper." *Cisco: San Jose, CA, USA* 10.1 (2020): 1-35.
2. Lenaerts, B. & Grimes, T. "2024 DNS Threat Landscape." *Infoblox*, (2024).
3. P. Mockapetris, " Domain Names - Implementation and Specification." *Data Tracker*, RFC 1035, (1987).
4. Sheila, F. "Guidelines for the Secure Deployment of IPv6: Recommendations of the National Institute of Standards and Technology." *NIST special publication; 800-119*, (2010).
5. Mubshira, "How to Implement DNSSEC: Best Practices and Setup Tips." *DMARC Report*, (2025).
6. National Cyber Security Centre, "Network security fundamentals." (2025).
7. Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. "Security and privacy of technologies in health information systems: A systematic literature review." *Computers* 13.2 (2024): 41.
8. Indusface, "DNS Over TLS (DoT): Definition, Key Benefits, and Potential Limitations."
9. BlueCat, "Best Practices Guide: DNS Infrastructure Deployment," (2020).
10. Cloudflare Docs, "DNS over HTTPS."

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Puvvadi, A. "Using Recursive Resolvers for Parental Controls, Malware Filtering, and Enterprise Security." *Sarcouncil Journal of Engineering and Computer Sciences* 4.10 (2025): pp 94-102.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher