CS-044 · Network

DNS Security

Protecting the internet's naming system from spoofing, hijacking, and abuse.

Executive Summary

The Domain Name System translates human-readable names into IP addresses, and because nearly all internet activity begins with a DNS lookup, it is a prime target for attackers. DNS security covers protecting the integrity of those lookups, detecting abuse of DNS as a covert channel, and hardening the servers that run it. DNSSEC, encrypted DNS, and monitoring are core defenses.

What It Is

DNS is the distributed directory that maps domain names such as a website address to the numeric IP addresses that computers use to connect. When a device needs to reach a name, a resolver queries a hierarchy of servers, from root to top-level domain to the authoritative server for the domain, and caches the answer for efficiency. DNS security is the set of practices that keep this process trustworthy: ensuring answers are authentic and unaltered, keeping queries private, preventing attackers from redirecting users, and stopping DNS from being used to smuggle data or control malware. Historically DNS was built for reliability rather than security, which is why protective extensions were added later.

Why It Matters

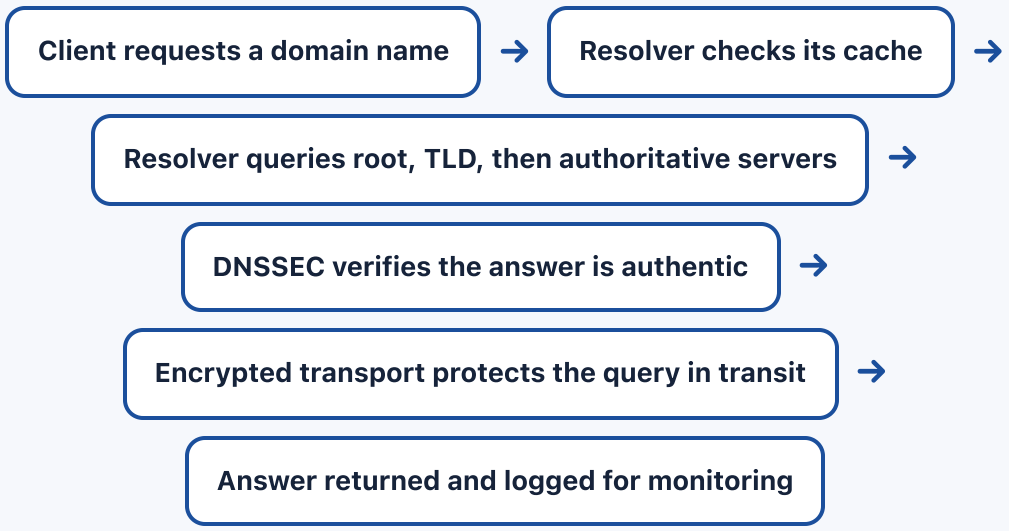
Because a DNS lookup precedes almost every connection, corrupting it lets an attacker silently send victims to fraudulent sites, intercept traffic, or block access. Cache poisoning and hijacking can undermine even well-secured applications, since the user never reaches the real destination. DNS is also abused as a covert channel, with attackers hiding stolen data or command traffic inside DNS queries that many networks fail to inspect. For defenders, DNS logs are among the richest sources of early warning, revealing connections to malicious domains.

Understanding DNS security is therefore valuable across network defense, incident response, and cloud operations.

How It Works

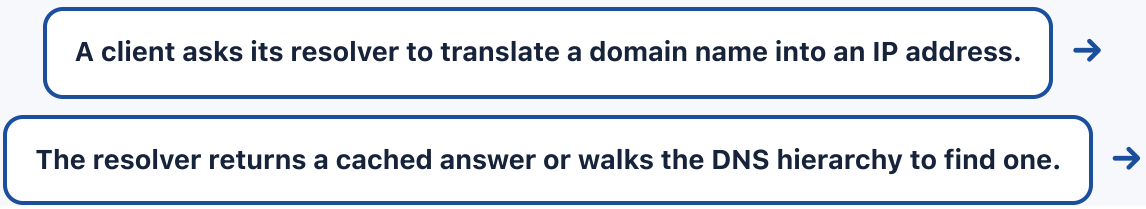
Several layers of protection address different DNS risks. DNSSEC adds cryptographic signatures to DNS records so a resolver can verify that an answer genuinely came from the authoritative source and was not altered, which defends against forged responses. Encrypted transports such as DNS over HTTPS and DNS over TLS protect the confidentiality of queries between a client and its resolver, preventing eavesdropping and on-path tampering. On the operational side, defenders restrict who can perform zone transfers, harden and patch DNS servers, use reputable filtering resolvers that block known-malicious domains, and monitor query logs for anomalies such as unusually long or high-volume requests that can indicate tunneling.

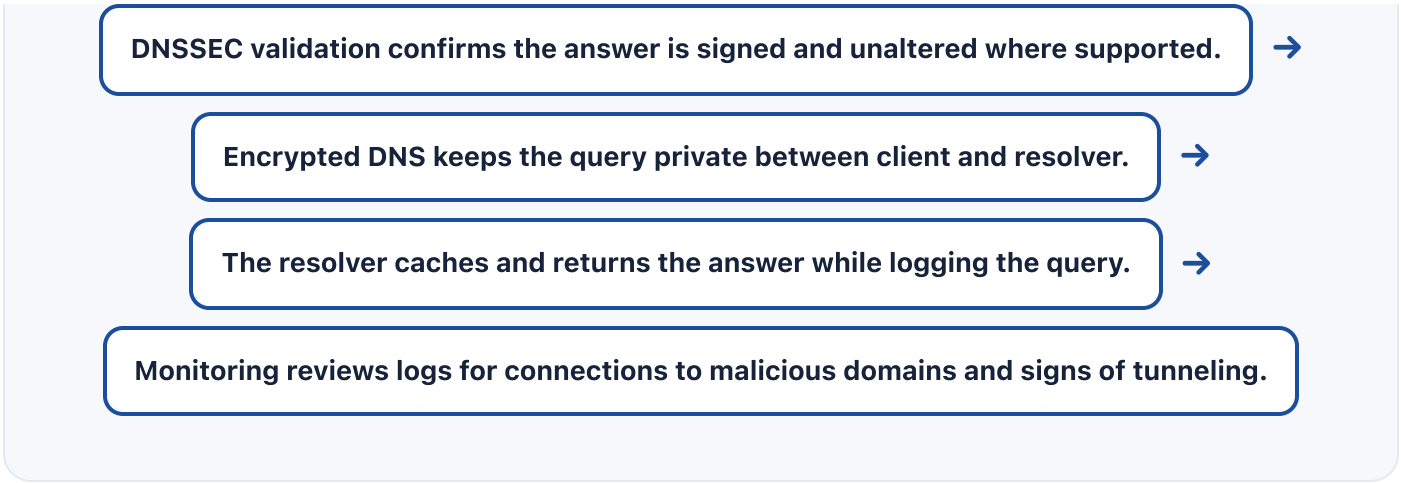
Architecture Diagram



A DNS lookup travels from client to resolver up the server hierarchy; security controls protect authenticity, confidentiality, and monitoring at each step.

Visual Workflow





Common Attacks

- DNS cache poisoning that inserts forged records into a resolver
- DNS hijacking that changes settings to redirect users to attacker servers
- DNS spoofing that returns a fraudulent answer to a query
- DNS tunneling that hides data exfiltration or command traffic inside queries
- Distributed denial-of-service floods against DNS infrastructure

Common Mistakes

- Leaving DNS servers unpatched and exposed to known vulnerabilities
- Allowing unrestricted zone transfers that leak internal records
- Never inspecting DNS logs, missing an early signal of compromise
- Trusting untrusted or default resolvers with no filtering
- Assuming DNSSEC encrypts queries when it only authenticates records

Best Practices

- Enable DNSSEC to validate the authenticity and integrity of DNS answers
- Use encrypted DNS such as DNS over HTTPS or DNS over TLS for query privacy
- Use a filtering resolver that blocks known-malicious and newly registered domains
- Restrict zone transfers to authorized secondary servers only
- Log and monitor DNS queries to detect tunneling and malicious lookups

Quick Checklist

- [x] DNSSEC validation is enabled on resolvers where supported
- [x] DNS queries use an encrypted transport to a trusted resolver
- [x] Zone transfers are restricted to authorized servers
- [x] DNS servers are patched and hardened to a known baseline
- [x] DNS query logs are collected and reviewed for anomalies

Recommended Tools

Recursive resolver with filtering
Resolves names while blocking known-malicious domains

DNS query logging and analytics
Records lookups to detect tunneling and malicious connections

DNS diagnostic tools
Query records and verify DNSSEC signatures during troubleshooting

Passive DNS database
Provides history of domain-to-IP mappings for investigations

Industry Standards

RFC 4033 to 4035 (DNSSEC)
Define the DNS Security Extensions for record authentication

RFC 8484 (DNS over HTTPS)
Defines encrypted DNS transport over HTTPS

NIST SP 800-81
Secure Domain Name System deployment guide

Career Relevance

DNS security is a daily concern for network security engineers, SOC analysts, security engineers, and cloud security engineers. Analysts pivot on DNS logs during investigations,

engineers deploy DNSSEC and filtering resolvers, and responders trace malware through its domain lookups. Because DNS underpins almost every connection, understanding how to protect and monitor it is a high-value skill across the roles that AI-Governance-Jobs.com serves.

Interview Questions

- What problem does DNSSEC solve, and what does it not solve?
- How does DNS cache poisoning work, and how do you defend against it?
- What is DNS tunneling, and how might you detect it?
- How do DNS over HTTPS and DNSSEC differ in what they protect?
- Why are DNS logs so valuable during incident response?

Related Certifications

CompTIA Security+ | **GIAC Certified Intrusion Analyst (GCIA)** | **CompTIA Network+**

Further Reading

- NIST SP 800-81: Secure DNS Deployment Guide
- IETF RFC 4033: DNS Security Introduction and Requirements
- CISA: Protecting Against Malicious Use of the DNS

Key Takeaways

- DNS translates names to IP addresses and precedes almost every connection.
- DNSSEC authenticates DNS records, while encrypted DNS protects query privacy.
- Cache poisoning, hijacking, and tunneling are common DNS-based attacks.
- Filtering resolvers and restricted zone transfers reduce DNS risk.
- DNS logs are among the richest early-warning signals for defenders.

FAQ

▶ **Does DNSSEC encrypt my DNS queries?**

▶ **What is DNS tunneling?**

▶ **Why is DNS such a common attack target?**

Related Careers

RELATED ROLES

Network Security Engineer

Soc Analyst

Cloud Security Engineer

RELATED CERTIFICATIONS

CompTIA Security+

GIAC Certified Intrusion Analyst (GCIA)

CompTIA Network+

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides

Role roadmaps

Salary data

Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **DNS Security**
3. Go deeper: Ports & Protocols
4. Go deeper: Firewalls
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-042 Ports & Protocols | CS-043 Firewalls | CS-045 VPNs | CS-047 Intrusion Detection Systems (IDS) | CS-001 Cybersecurity