

# DOMAIN NAME SYSTEM



Security and  
Mitigation



[sales@advantal.net](mailto:sales@advantal.net)

[www.advantaltechnologies.com](http://www.advantaltechnologies.com)



## 1. INTRODUCTION

The Domain Name System (DNS) is a foundational component of digital infrastructure. As the first protocol touched by nearly every network transaction, DNS is frequently targeted by attackers seeking to disrupt service availability, exfiltrate data, redirect traffic, or compromise users.

This document outlines the complete DNS threat landscape and describes how the organization's DNS solution provides multi-layered security, governance, observability, and automated countermeasures against modern DNS-based attacks.



## 2. DNS THREAT LANDSCAPE OVERVIEW

The Domain Name System operates as a globally distributed, hierarchical, and latency-sensitive protocol, making it an attractive target across multiple threat vectors. DNS attacks today are not limited to simple spoofing or volumetric floods; adversaries increasingly target protocol weaknesses, recursive resolver logic, authoritative server trust chains, and even DNS-based metadata for reconnaissance and infiltration activities.

To understand the full scope of DNS threats, the landscape can be classified into the following major domains, each consisting of numerous sub-attacks, protocol abuses, and architectural risks which are as follows:

- 1. Availability Attacks (DDoS, Flooding, Amplification)**
- 2. Integrity Attacks (Cache Poisoning, Spoofing, Tampering)**
- 3. Confidentiality Attacks (Data Exfiltration, Tunneling)**
- 4. Reconnaissance & Abuse (Zone Walking, Enumeration)**
- 5. Policy & Access Breaches (Unauthorized Changes, Privilege Misuse)**
- 6. Misconfiguration-Driven Risks**
- 7. Transport & Channel Attacks (MITM, Downgrade, Replay)**

Each class contains multiple sub-attacks described in detail below, along with the exact mitigation mechanisms provided by the DNS platform.

### 3. DETAILED DNS ATTACKS & MITIGATION STRATEGIES

The following attack mitigations reflect the real capabilities built into the ML-DNS Analyzer, Log Streamer, and DNS stack deployed by the organization.

#### 3.1 DNS DDOS ATTACKS

##### 3.1.1 Query Flooding

Attackers send extremely high query volumes causing CPU, memory, socket buffer, or network exhaustion.

##### Mitigation Implemented

###### 1. Kernel-Level & ADVANTAL’S DNS-Level Rate Controls

- Per-IP QPS limiting
- Per-subnet throttling
- Per-QType rate policing
- Token-bucket algorithm for burst absorption

###### 2. ML-Based Flood Pattern Detection (Implementation)

**Pyhton based Log Streamer → ML Analyzer** pipeline extracts the following features continuously:

Feature	Why it's important
query_entropy	Flood attacks often have low entropy repetitive patterns
digit_ratio	Bot-generated loads often contain numeric bursts
subdomain_count	Floods attempt randomized subdomain prefixes
client_frequency_change	Sudden QPS shift indicates attack
NXDOMAIN ratio	NXDOMAIN floods spike this metric

##### The Analyzer uses:

- **Isolation Forest** → Detects sudden abnormal deviations in incoming QPS patterns
- **Autoencoder** → High reconstruction error = unusual query distribution, flagged

## When anomaly is detected:

- ML engine sends “**BLOCK-SCORE > threshold**”
- A dynamic RPZ rule is generated
- Rule is pushed into DNS to drop/ignore traffic

## 3. Active-Active DNS Cluster

DNS cluster splits traffic between nodes, automatically redistributing load when attacks occur.

## 3.2 DNS AMPLIFICATION ATTACKS

Exploit large DNS responses to amplify traffic.

### Mitigation Implemented

- Response Rate Limiting (ADVANTAL'S RRL)
- EDNS buffer auto-reduction
- Minimal response mode (minimal-responses yes;)
- Dropping ANY queries
- ML Analyzer flags repeated identical queries from spoof patterns

ML-detected amplification patterns → **auto-blocked via RPZ.**

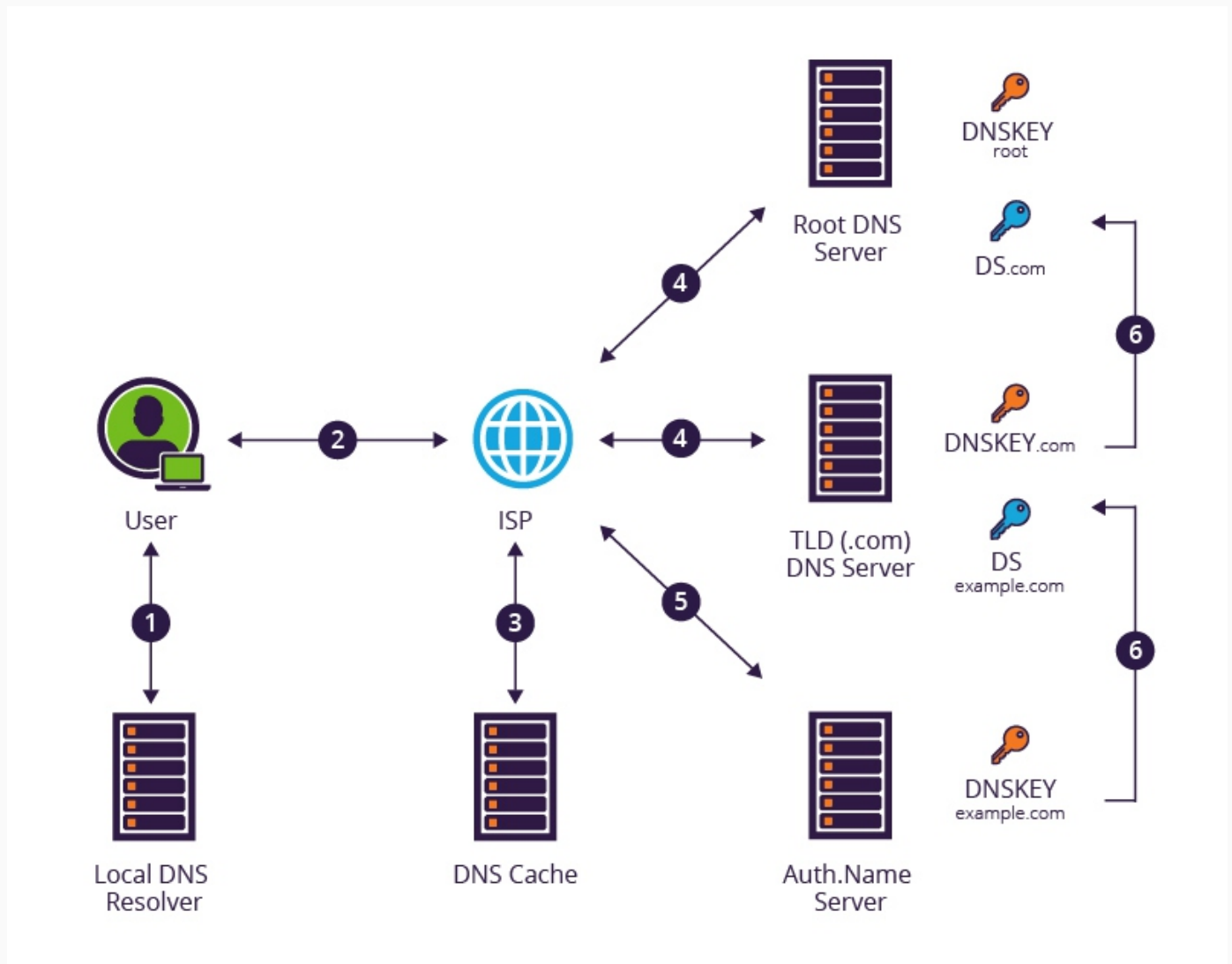
## 3.3 CACHE POISONING ATTACKS

Attacker injects forged responses into cache.

### Mitigation Implemented

#### 1. DNSSEC Validation

Inline signing + signature validation prevents forged answers.



## 2. Source Port + Query ID Randomization

Configured in DNS

## 3. ML-Based Poison Detection

### Features extracted:

- TTL variance anomalies
- sudden NS change patterns
- entropy of response domain
- suspicious glue record behaviour

Random Forest classifier is trained to mark suspicious responses as **poison-likely** → written to a separate DB table for audit + mitigation.

## 3.4 DNS SPOOFING / MITM

Attacker injects spoofed packets.

### Mitigation

- DNSSEC strict mode
- TSIG for transfers and dynamic updates
- TLS-secured GUI/API
- ML detection of abnormal RTT patterns (MITM creates timing anomalies)

## 3.5 DNS HIJACKING / UNAUTHORIZED REDIRECTS

### Mitigation Implemented

#### 1. Governance (Maker-Checker)

Records cannot be changed without 2-step approval.

#### 2. Enforcement via RBAC

Least privilege access ensures only authorized users can modify critical DNS records.

#### 3. ML-Assisted Change Monitoring

Whenever a DNS A/MX/CNAME record changes:

- Feature extraction occurs
- The Autoencoder checks if this change matches historical behaviour
- If anomaly detected → Alert + rollback suggestion to admin

#### 4. Full Record Versioning

Allows instant rollback to pre-compromise version.

## 3.6 NXDOMAIN FLOODING

### Mitigation

#### 1. Negative Caching + Rate Limits

Configured in Advantal's DNS.

#### 2. ML-Based NXDOMAIN Spike Detection

Analyzer tracks:

- NXDOMAIN ratio per IP
- Entropy of requested subdomains
- Label length patterns

**Isolation Forest model** detects abnormal surges → Auto-block via RPZ.

## 3.7 DNS TUNNELING& COVERT CHANNELS

ML Analyzer is **strong in detecting tunneling** due to advanced log parsing.

### Mitigation Implemented

#### 1. Deep Feature Extraction

For each query:

- length
- entropy
- digit\_ratio
- special\_char\_count
- number\_of\_labels

#### 2. Autoencoder Detector

High reconstruction error indicates non-human, encoded, or tunnel-style queries.

### 3. CNN-Based Classifier for Tunneling DNS Patterns

Trained on:

- dnscat2
- iodine
- OzymanDNS
- Base64 query payloads

### 4. RPZ Auto-Blocking

Detected tunneling domain or client IP → **Automatic addition to “rpz-malicious.local” zone.**

## 3.8 DOMAIN GENERATION ALGORITHM (DGA) ATTACKS

### Mitigation Implemented

#### 1. CNN-Based DGA Detection Model (Codebase)

This identifies:

- pseudo-random domain patterns
- malware DGA seeds
- algorithmically generated subdomains

#### 2. Random Forest Domain Classifier

Uses features:

- entropy
- digit ratio
- length
- vowel ratio
- dictionary word presence

A final **DGA\_SCORE** is computed and logged.

Domains above threshold → **Added to DGA-RPZ blocklist automatically.**



## 3.9 ZONE TRANSFER ATTACKS (AXFR/IXFR)

### Mitigation

- TSIG-mandatory transfers
- Strict IP-based ACL
- Hidden Primary architecture
- ML Analyzer alerts on unusual AXFR frequency (important!)

## 3.10 DNS ZONE WALKING (NSEC/NSEC3)

### Mitigation

- NSEC3 hashed names
- Opt-out mode
- Negative caching protection
- Log Analyzer identifies repeated sequential queries → flagged as zone-walking attempts

## 3.11 OPEN RESOLVER ABUSE

### Mitigation

- Recursive access restricted per subnet
- RPZ enforcement for external clients
- ML flags IPs making cross-zone recursion attempts

## 3.12 ROGUE DNS SERVER ATTACKS

### Mitigation

- DHCP pushes only approved resolvers
- DNSSEC rejects forged responses
- ML engine detects unknown upstream resolvers in logs

## 3.13 DNS REBINDING ATTACKS

### Mitigation

- Rebinding protection module
- RPZ filtering
- ML monitors “public→private IP shift” patterns in A records

## 3.14 PHANTOM DOMAIN ATTACKS

### Mitigation

- Lame server auto-blacklisting
- Reduced retry timers
- ML monitors “repeated timeout patterns” in the log stream

## 3.15 MISCONFIGURATION THREATS

### Mitigation

- Automated config checks (named-checkconf + internal validation)
- DNSSEC key expiry alerts
- Serial mismatch alarms
- ML detects unusual configuration patterns (spikes in SERVFAIL)

## 3.16 TRANSPORT LAYER ATTACKS

### Mitigation

- TSIG
- Mutual TLS
- Strict TLS cipher policies
- ML watches for timing anomalies suggesting spoofing/downgrade

## 4. DNS SECURITY ARCHITECTURE PROVIDED BY THE PLATFORM

The organization's DNS platform follows a multi-layered, defense-in-depth architecture that integrates high availability, cryptographic controls, machine learning-based threat detection, policy-based firewalls, and strong governance. Each component contributes to a robust and resilient DNS environment capable of withstanding modern cyber threats while delivering predictable, secure, high-performance service.

### 4.1 MULTI-SITE HIGH AVAILABILITY & RESILIENCE (ACTIVE-ACTIVE / ACTIVE-STANDBY)

The DNS infrastructure is designed for **continuous uptime**, **geographically distributed resilience**, and **automated failover**.

#### Key Architecture Capabilities

##### 1. Per-Site Active-Active / Active-Standby Deployment

Each site contains two or more DNS nodes configured for:

- **Active-Active mode:** Both nodes serve traffic concurrently with full zone synchronization.
- **Active-Standby mode:** The standby node maintains warm data replication and takes over immediately during primary node failure.

##### 2. Multi-Site Cross-Region Sync

Zones are replicated using:

- **Synchronous replication (low-latency DC pairs)**  
Ensures consistency and instant propagation.
- **Asynchronous or timed IXFR-based replication (geo-distributed DCs)**  
Optimizes performance across distant sites.
- **Real-time sync using Advantal's DNS inline-signing + serial auto-management**  
Ensures DNSSEC zones remain consistent across sites.

### 3. GSLB-Aware DNS Failover (Integrated with ML Signals)

The platform integrates:

- Health checks (TCP/UDP/HTTPS)
- Node availability scoring
- ML anomaly signals

If a node or site exhibits:

- High QPS anomaly
- High NXDOMAIN ratio
- Latency deviation
- Timeouts

It is automatically deprioritized or removed from GSLB routing.

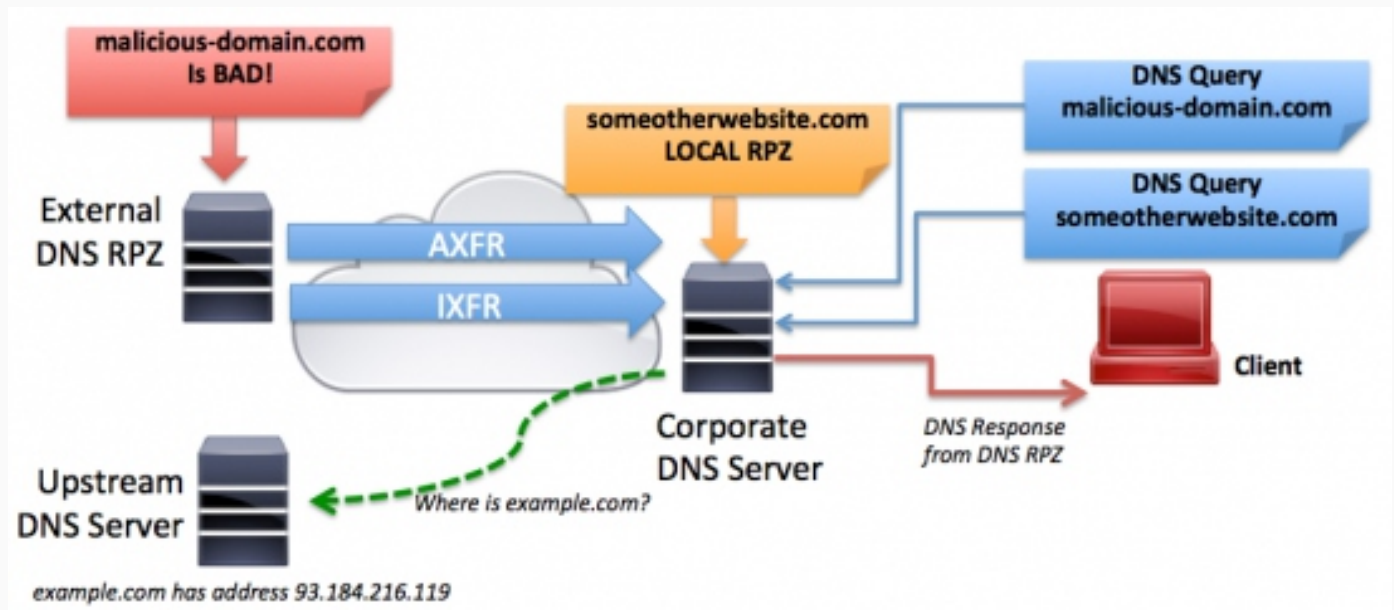
### 4. No Single Point of Failure

- Multi-node per site
- Multi-site redundancy
- Multi-network-path redundancy
- Local HA + Global HA

This ensures RTO < 1 minute and RPO  $\approx$  0 seconds for DNS operations.

## 4.2 DNS FIREWALL (RPZ) – DYNAMIC, ML-DRIVEN, POLICY ENFORCEMENT LAYER

The DNS firewall is powered by **Response Policy Zones (RPZ)** combined with **ML auto-generated threat rules**.



## Key Technical Capabilities

### 1. Real-Time RPZ Enforcement

DNS enforces RPZ policies to:

- Block malicious domains
- Redirect suspicious queries
- Deny tunneling attempts
- Quarantine DGA or anomalous domains

Rules are applied at:

- Response stage
- Query rewrite stage
- NXDOMAIN rewrite stage

### 2. ML → RPZ Automation Pipeline

ML-DNS Analyzer generates:

- **AUTO-BLOCK** rules for detected DGAs
- **AUTO-TUNNEL-BLOCK** for tunneling patterns
- **SUSPICIOUS-SCORE** flags based on entropy, digit ratio, label structure
- **CLIENT-IP BLOCK** for malicious sources

These rules flow from:

LogStreamer → FeatureExtraction → MLModel → RuleGeneration →  
RPZZoneUpdate → AutomaticEnforcement

### 3. Integration with Threat Intelligence & Internal Governance

The RPZ engine supports:

- Third-party feeds (phishing, malware, C2)
- Custom bank/government blacklists
- Internal governance-based domain restrictions
- Auto-expiry rules for temporary blocks

## 4.3 DNSSEC (AUTHORITATIVE & RECURSIVE) – FULL TRUST CHAIN ENFORCEMENT

The platform provides full DNSSEC lifecycle management.

### Technical Capabilities

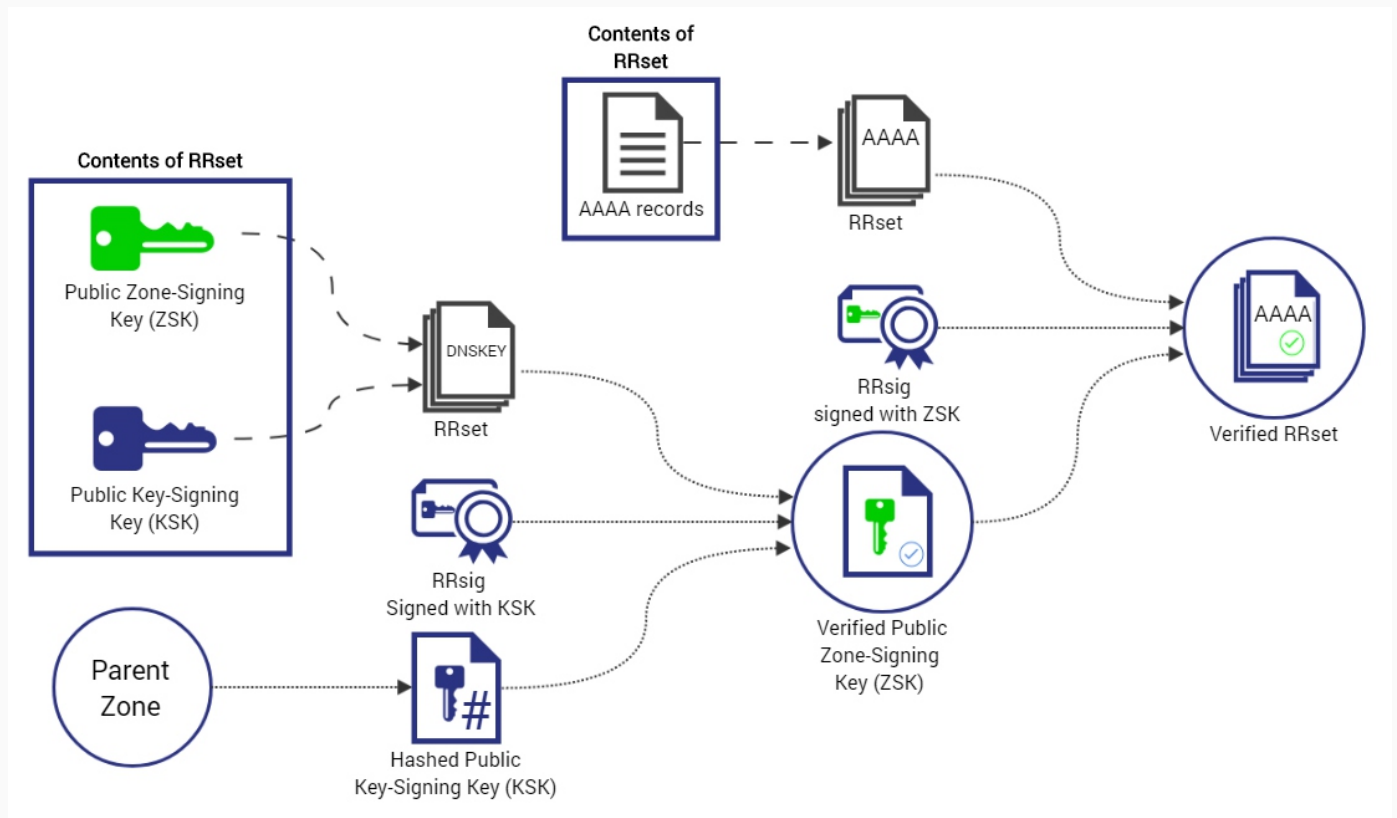
#### 1. Automatic Signing & Inline-Signing

DNS performs:

- Inline signing
- RRSIG generation
- NSEC/NSEC3 generation
- Serial management

#### 2. Key Lifecycle Management

- ZSK/KSK generation
- Scheduled rollover
- Parent DS submission support
- Validation monitoring (ML alerts on DS mismatch or expiry)



### 3. Recursive Validation

Recursive resolvers enforce:

- Full trust chain validation
- Replay protection
- Denial of existence proofs via NSEC3

Any response failing validation is:

- Dropped
- Logged
- Forwarded to ML anomaly analysis

## 4.4 SECURE MANAGEMENT & GOVERNANCE

The platform provides strong operational governance, critical in BFSI and regulated environments.

## 1. RBAC (Role-Based Access Control)

Granular roles:

- DNS Administrator
- Zone Administrator
- Record Manager
- Security Analyst
- Auditor
- API-only clients

Each API call or GUI operation is permission-evaluated.

## 2. Maker-Checker Approval Workflow

High-risk operations (zone changes, record updates) follow:

- Maker drafts change
- Checker reviews and approves
- Change logged and cryptographically timestamped
- Versioning snapshot created

## 3. Authentication Controls

- Multi-Factor Authentication (MFA)
- SSO via SAML/OAuth
- Certificate-based API authentication

## 4. Audit Trails (Immutable Log Architecture)

Logs include:

- User identity
- Terminal/IP
- Operation type
- Old vs new record
- Timestamp
- Session key



Logs stored in:

- MySQL
- Syslog
- SIEM (ELK, QRadar, Splunk)

## 4.5 REAL-TIME MONITORING & SIEM INTEGRATION

The DNS monitoring and telemetry layer provides deep visibility for NOC/SOC teams.

### 1. Real-Time Metrics (Cluster-Wide)

- QPS
- Cache hit ratio
- Failure rate
- SERVFAIL/NXDOMAIN distribution
- Recursion depth
- Per-zone and per-application stats

### 2. ML-Integrated Telemetry

ML analyzer generates:

- Domain risk scores
- Client risk profiles
- Time-series deviations
- Query-type anomalies
- DGA probability

All metrics logged in MySQL and pushed to dashboards.

### 3. SIEM Integration (Enriched Events)

DNS logs forwarded with:

- Query source
- Threat type
- ML score

- Action (block/allow/escalate)
- RPZ policy triggered

Supported formats:

- JSON
- CEF
- Syslog RFC5424

## 4.6 BUILT-IN ML-BASED THREAT DETECTION

This is where custom-built ML-DNS Analyzer becomes central.

### ML Techniques Actually Used by the Organization

#### 1. Entropy-Based Detection

Checks for:

- High randomness (DGA, tunneling)
- Low randomness (bot floods)
- Unusual patterns in labels

#### 2. CNN-Based DGA Classification

CNN model identifies:

- Malware-generated domains (Conficker, Kraken, etc.)
- Pseudo-random domain seeds
- High-probability algorithmic naming

#### 3. Isolation Forest for Outlier Detection

Used for:

- Sudden QPS spikes
- Unusual client behavior
- Unseen domain structures

## 4. Autoencoder for Query Behavior Modeling

Learns normal DNS traffic behavior and flags:

- Tunneling
- Enumeration
- Rebinding
- Phantom domain triggers
- Abnormal NXDOMAIN patterns

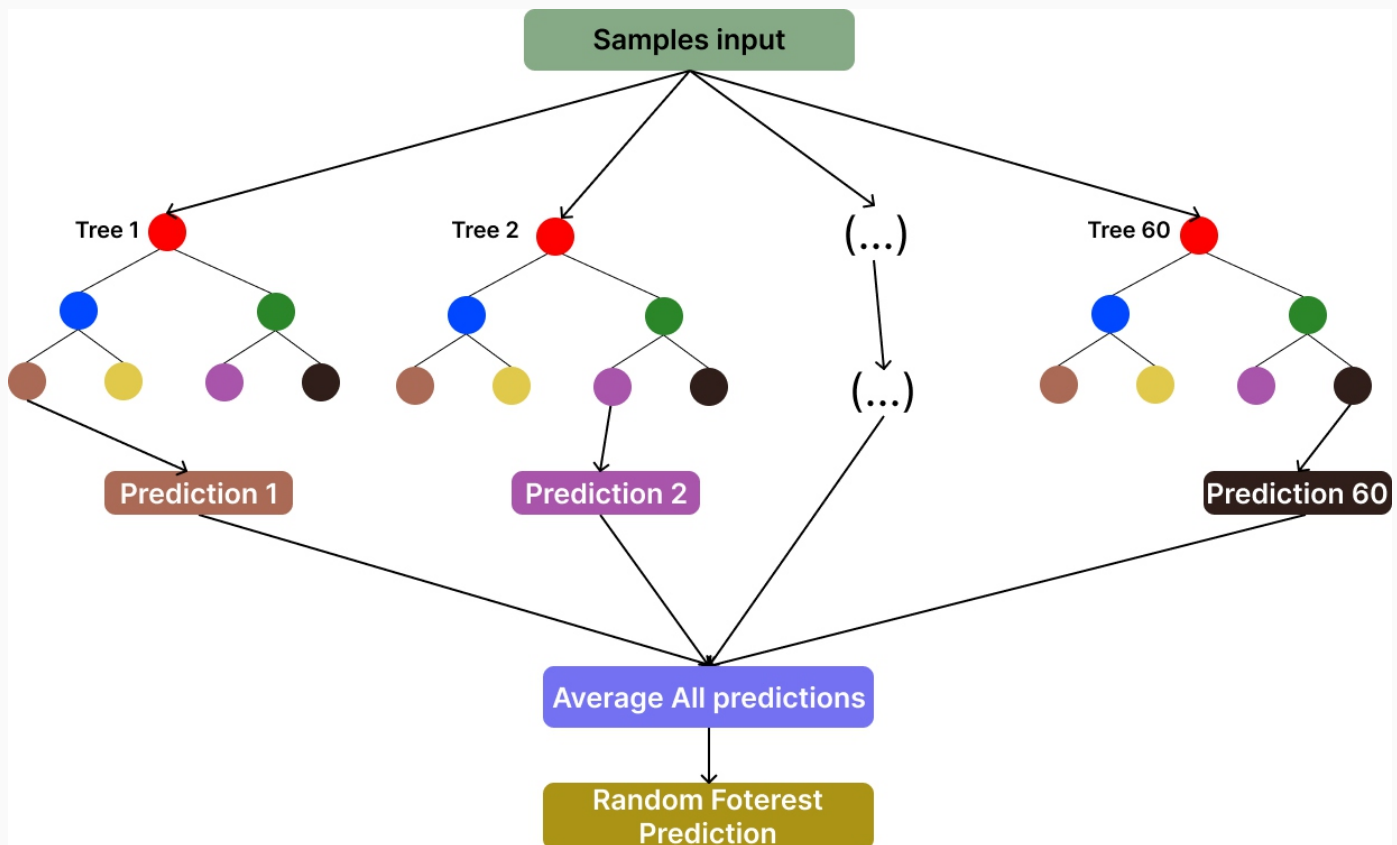
## 5. Random Forest Classifier

Used to classify domain queries using:

- Digit ratio
- Vowel ratio
- Dot count
- Domain length
- TLD distribution
- Subdomain length variance

Final scores are applied as:

- ALLOW
- SUSPICIOUS → Log
- BLOCK → RPZ update



## 5. COMPLIANCE & REGULATORY ALIGNMENT

The DNS security architecture is built to directly satisfy compliance requirements for Indian BFSI, Government, Telecom, and Defense environments.

### 5.1 RBI Cyber Security Framework

To meet RBI-mandated controls:

- Maker-Checker workflow for DNS changes
- Immutable audit logs retained for mandated periods
- DNSSEC to prevent spoofing and redirections
- Real-time alerting to SOC via SIEM
- Incident response integration (auto-blocking rules)
- Cross-site DR (DC/DR architecture)

## 5.2 ISO 27001 & 22301

ISO 27001 Alignment:

- Access control (RBAC, MFA, SSO)
- Cryptographic control (DNSSEC, TSIG, TLS)
- Logging & monitoring (SIEM integration)
- Secure configuration guidelines
- Business continuity procedures

ISO 22301 Alignment:

- Multi-site DNS HA ensures service continuity
- RTO < 1 minute, RPO  $\approx$  0
- Automatic failover & replication ensures disaster resiliency

## 5.3 CERT-In Guidelines

The platform complies with:

- Mandatory logging & timestamping
- Secure configuration hardening
- Threat intelligence ingestion (RPZ feeds)
- Proactive mitigation via ML
- Reporting of suspicious events

## 5.4 NIST 800-53 & 800-207 Zero Trust

The DNS layer supports Zero Trust principles:

- All DNS events are authenticated, logged, and analyzed
- DNSSEC ensures no implicit trust in responses
- Continuous ML evaluation = continuous trust assessment
- Policy-based RPZ = dynamic trust reassignment
- Network segmentation using access controls

## 5.5 DoT Trusted Telecom Requirements

- Component transparency
- Config hardening
- Cryptographic controls
- No dependence on unverified external SaaS
- End-to-end auditability

## 5.6 BFSI-Specific Hardening

The DNS system supports:

- Air-gapped deployment
- Strict approval workflows
- Encryption at rest + transit
- Multi-site failover
- Integration with bank SOC

## EXPERIENCE ADVANTAL DNS IN ACTION





**Scan to Request a Free Demo**



Talk to our experts and discover how automated, secure, and high-performance DNS can modernize your entire network stack.

**Advantal Technologies Limited**  
(Make In India OEM)

---

-  [sales@advantal.net](mailto:sales@advantal.net)
-  [kartikay.shukla@advantal.net](mailto:kartikay.shukla@advantal.net)
-  +91 99711 61261
-  [www.advantaltechnologies.com](http://www.advantaltechnologies.com)

EAL2+, NDPP, NDcPP Certified