

# INFOBLOX FOR EXTERNAL AUTHORITATIVE DNS

Reference Architecture



# TABLE OF CONTENT

<b>INFOBLOX OVERVIEW .....</b>	<b>3</b>
<b>EXTERNAL AUTHORITATIVE DNS .....</b>	<b>3</b>
What Is DNS? .....	3
Types of DNS Servers .....	4
<i>Authoritative DNS</i> .....	4
<i>Recursive DNS</i> .....	4
<i>Hidden Primary External DNS</i> .....	4
External DNS.....	5
<b>INFOBLOX FOR EXTERNAL AUTHORITATIVE DNS .....</b>	<b>6</b>
Portfolio Components.....	6
Infoblox Universal DDI™ Product Suite .....	7
Infoblox NIOS DDI for External DNS.....	7
DNS Infrastructure Protection.....	7
Brand Protection Services.....	7
Control Plane vs. Data Plane .....	8
<b>DEPLOYMENT SCENARIOS .....</b>	<b>9</b>
SaaS-Hosted External Authoritative DNS .....	9
Why Customers Choose This Deployment Model .....	12
SaaS-Hosted with Hidden Primary on NIOS .....	12
Why Customers Choose This Deployment Model .....	15
Self-Hosted External Authoritative DNS.....	15
Why Customers Choose This Deployment Model .....	18
Hybrid-Hosted External DNS (NIOS + SaaS in Multi-Provider DNS) .....	18
Why Customers Choose This Deployment Model .....	21
<b>CONCLUSION .....</b>	<b>21</b>
<b>GLOSSARY.....</b>	<b>22</b>

## INFOBLOX OVERVIEW

Infoblox is the leader in **DNS, DHCP, and IP address management (DDI)**, uniting networking, security, and cloud across hybrid, multi-cloud environments. Infoblox's portfolio combines hardened NIOS appliances, cloud-native Infoblox Universal DDI™, and a software-as-a-service (SaaS) control plane to deliver these **enterprise-grade critical network services** everywhere customers run applications, data centers, branches, public cloud infrastructure, and SaaS. With **Universal DDI Management**, teams can manage internal, external, and cloud-native DNS across the Infoblox Grid, hyperscalers and SaaS DNS providers such as Cloudflare and Akamai from a single API and portal, applying consistent policy and automation.

For NetOps, this turns legacy “plumbing” into a governed control plane. Infoblox replaces, and in some cases allows management of, fragmented Windows/BIND DNS servers, cloud DNS, and SaaS stacks with **hardened DDI infrastructure (NIOS)** at the edge and **SaaS-based Universal DDI Management** as the control plane. Teams gain unified configuration and IP address management (IPAM) policy plus **DNS Traffic Control** for global load balancing and automated failover—reducing configuration errors, overlapping address space and outage risk.

For SecOps, **DNS becomes a front line defensive control point. DNS Infrastructure Protection**, a NIOS software add on, protects mission-critical authoritative DNS infrastructure from DDoS, DNS hijacking, cache poisoning and other DNS-based exploits, helping keep web applications up and running even when DNS infrastructure is under heavy attack. It uses **Infoblox Threat Adapt™** technology to automatically update protections as new DNS attack vectors and signatures are identified, keeping DNS defenses current, and giving security teams a resilient, high-fidelity choke point for protecting external services.

For CloudOps and DevOps, Infoblox provides a unifying DDI and visibility layer across AWS, Azure, Google Cloud, and SaaS platforms. **Universal DDI** orchestrates DNS and IP addressing consistently across on-prem Grids, cloud DNS, and SaaS-based external DNS. NIOS-X as a Service delivers cloud-native DNS and DHCP as a service for branches without infrastructure deployment. **Infoblox Universal Asset Insights™** helps identify zombie assets and dangling DNS records before they lead to outages or compromise. The result is faster cloud delivery, stronger security, and confidence that expansion will not erode resilience or availability.

## EXTERNAL AUTHORITATIVE DNS

### WHAT IS DNS?

The Domain Name System (DNS) is a foundational network service that, among other things, translates human-readable domain names (e.g., [www.example.com](http://www.example.com)) into the IP addresses that computers use to communicate with systems across the internet and private networks. In this role, it functions as the internet's phone book, mapping names to IP addresses. By acting as the internet's naming and directory system, DNS allows users, applications and services to reach websites, email servers, cloud platforms and internal resources without needing to remember numerical addresses. This simple capability is critical because nearly every digital interaction—web browsing, email delivery, application logins and API calls—depends on reliable name resolution. In business environments, DNS is especially vital: it supports core operations such as connecting employees to internal applications, enabling customer-facing services and ensuring third-party integrations function correctly. When DNS is slow, misconfigured or unavailable, the impact is immediate and widespread, causing outages that interrupt workflows, transactions and communications even if the underlying infrastructure and applications are still running. DNS also plays an important role in security and governance, helping organizations route traffic appropriately and publish records used for authentication and policy, for example, in email and certificate controls. In almost all situations, navigation on the internet simply does not work without DNS. Due to the criticality of this protocol, reliable, secure, and consistent DNS is imperative for modern business processes.

DNS servers can be configured to authoritatively host private or public zones, conditionally forward to other DNS servers for domains that they are not authoritative for, recursively resolve domains, or some combination of roles. When DNS servers are used to host private zones, it is normally referred to as internal authoritative DNS, or simply, internal DNS. Similarly, when DNS servers are used to host public zones to enable the internet presence of an organization, it is called external authoritative DNS, or simply, external DNS.

## Types of DNS Servers

### Authoritative DNS

An **authoritative DNS** server holds the official records for a zone (e.g., example.com) and answers with final, authoritative responses for that zone. Authoritative servers can be deployed in several ways:

#### Internal authoritative DNS

- Hosts zones reachable only inside the corporate network (e.g., corp.example.com, api.internal)
- Often integrates with identity systems (e.g., AD integrated DNS) and internal IPAM
- Controls name resolution for servers, services, endpoints, and internal APIs

#### External authoritative DNS

- Hosts public zones, such as example.com or api.example.com
- Is reachable from the internet and underpins websites, email, business-to-business integrations, and public APIs
- Frequently delivered via NIOS, cloud DNS, or SaaS DNS providers such as Cloudflare and Akamai

### Recursive DNS

A **recursive resolver** receives a client query (e.g., “What is the IP for www.example.com?”) and takes responsibility for finding the answer:

- Performs **iterative lookups** on behalf of the client
- Caches results to speed up subsequent responses to queries
- Commonly operated by enterprises (e.g., NIOS recursive Grid), internet service providers (ISPs) or public resolvers

### Hidden Primary External DNS

In a **hidden primary** architecture:

- An internal, non-internet-accessible primary DNS server (often Infoblox NIOS) is the authoritative source of truth for external zones
  - » A Hidden Primary is “hidden” because its NS records are not published, which generally means it cannot be found/referenced by other name servers
  - » The concept of a hidden primary is applicable for both internal and [external DNS](#), and is a best practice for both
- One or more **secondary DNS services**—usually SaaS or cloud DNS platforms—receive zone data via zone transfers or API synchronization and answer queries from the internet

For some commonly used DNS terminology, please refer to the [Glossary](#).

## EXTERNAL DNS

**External authoritative DNS** refers to the public, internet-accessible DNS servers that are the *source of truth* for a domain, such as example.com. These authoritative name servers publish record types like **A/AAAA** (IP addresses), **MX** (email routing), **TXT** (text, often used for domain verification and email security policies) and **CNAME** (aliases to other resource records). They are called *authoritative* because they don't "hunt around" the internet to find answers the way a recursive resolver does—they directly answer queries based on the zone data they host. They are called *external* because they are reachable from outside your organization and serve the public internet, enabling customers, partners and global users to resolve data in your domain(s).

In practice, external authoritative DNS can be hosted on-premises or in the public cloud on Infoblox appliances, by a managed DNS provider to, or a hybrid combination to maximize availability, performance (through global distribution) and resilience against attacks (like DDoS). The availability of external DNS servers is crucial because if authoritative DNS fails, users may be unable to reach business-critical services even when those services are otherwise healthy. External authoritative DNS data is served from an authoritative DNS server, but how do users find an authoritative DNS server on the Internet? Domains on the Internet are connected to the global DNS namespace through **delegation**: the domain owner's registrar (or the parent zone) adds **name server (NS) records within the parent domain that list the names of the subdomain's authoritative name servers** (and in some cases A/AAAA records for those server names, which are known as "glue" records).

Let's look at a sample query flow of a typical public name lookup to understand this better:

1. **Client (stub resolver)** asks its configured **recursive resolver**:  
"What is the A/AAAA record for www.example.com?"
2. The **recursive resolver** checks its **cache**. If there's a valid cached answer (time to live (TTL) not expired), it returns it immediately.
3. If not cached, the resolver asks a **root name server**:  
"Where do I find information for .com?"
4. Because it is not authoritative for .com, but it is a subdomain of the root, the **root server** responds with a **referral** to the **.com TLD name servers (the delegation information)**.
5. The resolver asks a server that is authoritative for **.com (at this level they are often referred to as TLD servers)**:  
"Which name servers are authoritative for example.com?"
6. The **TLD server** returns a referral: the **NS records** for example.com (often including "glue" IP addresses for those name servers).
7. The resolver asks the **external authoritative DNS server** for example.com:  
"What is the A/AAAA record for www.example.com?"
8. The authoritative server returns the **authoritative answer** (e.g., an IP address or a **CNAME** to another hostname along with any related records, such as RRSIG for DNSSEC-signed zones). The resolver **caches** the responses for each record's TTL and returns the final IP to the client.

A simple visual of the path:

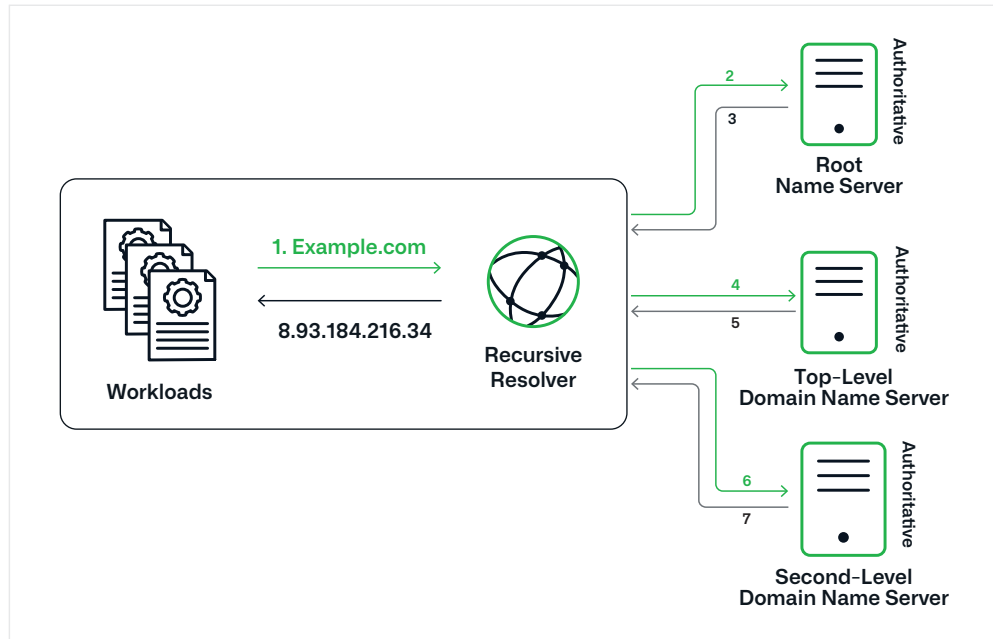


Figure 1. External DNS query flow (iterative lookup)

## INFOBLOX FOR EXTERNAL AUTHORITATIVE DNS

Infoblox for External Authoritative DNS is the next evolution of a solution that has safely delivered external DNS for more than 20 years, now expanded into a modern portfolio that pairs Infoblox’s industry-leading DDI reliability and security—trusted by the majority of the Fortune 500—with new cloud-based management, DDoS-resilient infrastructure and brand protection services for all of your public facing assets: websites, email, cloud apps and APIs.

Whether you self-host external DNS on NIOS, use cloud or SaaS providers like Cloudflare and Akamai, or run a hybrid model, Infoblox gives you a single, consolidated control plane to manage all of your external DNS records, protects self-hosted infrastructure against DDoS and other DNS infrastructure attacks and adds brand protection services to detect and take down lookalike domains targeting your customers and reputation.

With Infoblox for External Authoritative DNS, the company can:

- Eliminate expensive, potentially disruptive errors by controlling all DNS services from the same place, in the same consistent way
- Block cyberattacks hammering away at exposed external authoritative DNS services while ensuring that legitimate traffic keeps flowing
- Spot fake websites seeking to impersonate your business, and shut down bad actors before they harm customers or damage the brand

The company gets control, simplicity, and security, no matter where its DNS lives.

## PORTFOLIO COMPONENTS

The Infoblox for External Authoritative DNS portfolio is built from four core components that work together to secure and simplify public-facing DNS.

## Infoblox Universal DDI™ Product Suite

- Manage all DNS services—internal and external, including third-party services like Akamai, Cloudflare, Google Cloud, Microsoft Azure and AWS Route 53—in the same way, using the same consistent tools. Consolidated management and visibility for DDI also prevents DNS configuration errors, IP address conflicts and other risks across your hybrid, multi-cloud environment before they bring down your websites and other mission-critical network applications.
- Use a SaaS control plane (Infoblox Portal) to manage **internal and external DNS**, including third-party providers such as **Akamai, Cloudflare**, and major public clouds, from a **single API and portal**
- Unify IPAM and DNS zone management to identify and prevent configuration errors, overlapping subnets and IP address conflicts across hybrid and multi-cloud environments

## Infoblox NIOS DDI for External DNS

- Extend the industry-leading visibility, automation and control that NIOS provides for internal DNS to the external networks that keep your websites, email and other critical public-facing applications online
- Deliver **authoritative external DNS** using hardened NIOS appliances (physical or virtual) that feature Grid-based management, automation, and high availability (HA).
- Support **hidden primary** deployments and secondary servers with infrastructure sized for high QPS external workload.

## DNS Infrastructure Protection

- Dedicated infrastructure security for DNS servers, protecting self-hosted external DNS against volumetric and protocol-level DDoS attacks, NXDOMAIN floods and other threats while continuing to respond to legitimate queries
- Maximized uptime and performance of websites and mission-critical external networks by protecting against DDoS attacks, DNS hijacking and other threats targeting external DNS services—often the worst kind of cyberattacks, which can cause extremely disruptive web outages

## Brand Protection Services

- **Lookalike Domain Monitoring** and **Domain Mitigation/Takedown** services continuously discover, score, and help remove malicious lookalike domains targeting a brand and its customers.

These components are orchestrated through the **Infoblox Portal** as a unified control plane for **all DNS (internal, cloud, external)** and integrated with broader Universal DDI and security capabilities.



## DEPLOYMENT SCENARIOS

This section describes recommended architectures for three core patterns (plus an advanced hybrid-hosted pattern):

1. **SaaS-Hosted External Authoritative DNS**
2. **SaaS-Hosted with Hidden Primary on NIOS**
3. **Self-Hosted External Authoritative DNS**
4. **Hybrid-Hosted External DNS (NIOS + SaaS in Multi-Provider DNS)**

## SAAS-HOSTED EXTERNAL AUTHORITATIVE DNS

### Sample Customer Scenario: Acquisition-Driven Global Retailer (Multi-Cloud + SaaS DNS)

This scenario is about a company that already uses multiple authoritative DNS providers (often due to mergers, different cloud choices or regional teams), and they want to stop managing external DNS like a collection of disconnected islands. Rather than forcing a disruptive “move everything to one DNS provider” project, they keep authoritative DNS where it is (Route 53, Azure DNS, Cloudflare, Akamai, etc.) but introduce Infoblox External DNS as the control plane for consistent workflows and visibility.

The payoff is speed and safety: teams get a single operational model for DNS changes (portal + API automation), fewer handoffs between consoles, less configuration drift, and easier governance. It’s the “standardize management, not necessarily infrastructure” approach.

### Customer Context

- A global retailer has grown through acquisitions.
- DNS is fragmented:
  - » Brand A uses **AWS Route 53**
  - » Brand B uses **Azure DNS**
  - » Brand C uses **Cloudflare**
  - » Marketing uses **Akamai** for campaign subdomains

### Challenges

- **Separate DNS Silos**
  - » Self-hosted authoritative DNS on BIND or Windows DNS for some domains
  - » Cloud DNS (e.g., AWS Route 53, Azure DNS, Google Cloud DNS) for app and cloud-native workloads
  - » SaaS-hosted DNS providers such as Cloudflare and Akamai for high-traffic websites and CDNs
- **Inconsistent Management Interfaces and APIs**
  - » Each provider has its own portal, CLI, and API semantics.
  - » Automation teams must maintain multiple sets of scripts and Terraform/Ansible modules, increasing fragility.
- **Manual, Error-Prone Change Processes**
  - » DNS changes for a single application may need to be applied in several systems.
  - » No single source of truth for public zones; risk of record drift and misconfiguration grows over time.

- **Limited Cross-Environment Visibility and RBAC**
  - » No unified view of all external zones across clouds and providers.
  - » Access control is managed differently per platform, making least privilege difficult to implement and audit.

### Negative Business Impact

- High risk of outage causing configuration errors when teams “swivel chair” between consoles
- Slow, inconsistent change management across public DNS, delaying feature rollouts and incident response
- Fragmented logging and monitoring; troubleshooting DNS issues across multiple providers is slow and complex
- Difficult to standardize security practices (DNS Security Extensions (DNSSEC), change controls) across the external DNS footprint

### Architecture with Infoblox Universal DDI

- Authoritative DNS hosting stays where it is (Route 53/Azure DNS/Cloudflare/Akamai).
- Infoblox External DNS (Infoblox Portal + API) becomes the central management plane for authoritative DNS records and zones across all providers.
- Optional: Keep internal DNS and IPAM under Infoblox as well, so internal/external naming, ownership models, and management processes are aligned.

### Key Components

- **External DNS Providers (Data Plane)**  
Cloudflare, Akamai, Route 53, Azure DNS, Google Cloud DNS for serving public DNS
- **Universal DDI Management (Control Plane):**
  - » Central management of external zones across all providers through the Infoblox Portal, using a single API and workflow
  - » Unified IPAM and DNS management to detect configuration errors and overlapping IP address space spanning internal, cloud, and external DNS
- **Brand Protection Services**  
Continuous discovery and takedown support for malicious lookalike domains operating outside the organization’s own DNS infrastructure

### Architecture View

- **Control Plane**  
App teams and NetOps use:
  - » Infoblox Portal UI for controlled changes
  - » Continuous integration (CI)/continuous delivery (CD) or GitOps pipelines calling the Infoblox API for automated record lifecycle (create/update/delete)
- **Data Plane**  
Internet queries still resolve directly against the configured authoritative providers (Cloudflare/Akamai/Route 53/Azure DNS).

## Typical Flow

1. Architects and NetOps teams manage public zones (e.g., adding api.example.com) via the Infoblox Portal.
2. Portal pushes configuration changes via connectors/APIs to each external provider (Cloudflare, Akamai, cloud DNS).
3. Public resolvers query providers directly; Infoblox does not sit on the query path but acts as the source of truth and orchestrator.
4. Universal DDI IPAM continuously assesses address usage and overlaps, while Brand Protection monitors for lookalike domains targeting the brand.

## Design Considerations

- **Multi-Provider Strategy**

Use multiple external DNS providers for diversity and regional optimization, but standardize management via Universal DDI to avoid operational silos.

- **Governance and RBAC**

- » Use Infoblox Portal roles and access views to delegate per zone or per environment control (e.g., marketing microsites vs. core transactional zones) without over-privileging application teams.
- » Role-based access and administrative domains span all DNS services, including external zones and providers.
- » Supports Zero Trust-aligned least-privilege models for DNS administration.

- **Risk Limitations**

SaaS-hosted-only designs inherit the provider's outage profile; if your DNS host experiences a broad incident, you may not have a viable fallback. For customers that cannot tolerate this, move to hidden primary or hybrid hosted patterns below.

## Advantages

- Using multiple SaaS-external DNS providers under Universal DDI Management delivers built-in redundancy and higher availability for public zones
- Unified Infoblox control plane makes it straightforward to shift traffic or fully transition between providers as needed, reducing outage risk and avoiding DNS vendor lock-in
- Consistent workflows and APIs across all external DNS services
- Reduced risk of misconfiguration by eliminating manual, multi-portal changes
- Centralized visibility and logging across disparate DNS providers
- Easier to enforce global DNS standards (naming, TTLs, DNSSEC, security policies)

## Positive Business Outcomes

- Fewer outages and faster changes for websites and public applications due to unified automation and reduced operator error
- Lower operational overhead by collapsing multiple DNS management stacks into one platform
- Faster multi-cloud adoption, as cloud teams can use a common, well-governed DNS interface instead of provider-specific tooling
- Stronger compliance and audit posture through consistent RBAC, change-tracking, and DNS policy enforcement across all external DNS

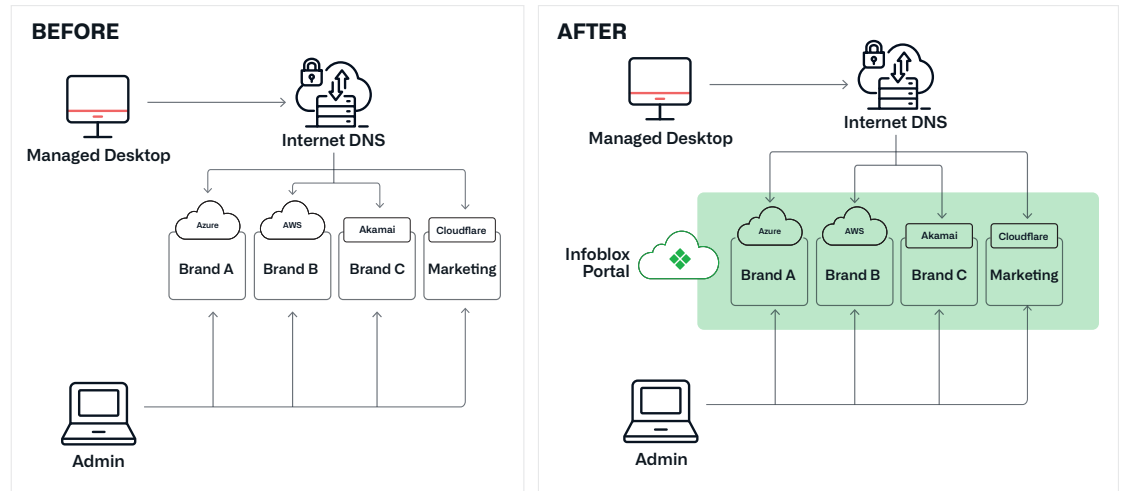


Figure 3. SaaS-hosted external DNS

## Why Customers Choose This Deployment Model

They want **one control plane** for external DNS operations across multiple clouds and DNS hosts, without forcing a disruptive “move all DNS to one provider” project.

## SAAS-HOSTED WITH HIDDEN PRIMARY ON NIOS

### Sample Customer Scenario: Regulated Bank with “Keep Control, But Serve at Global Scale” Policy

This pattern is the classic “best of both worlds” for external authoritative DNS. The customer wants tight internal control over zone management (compliance, audit, separation of duties) while still taking advantage of a large external DNS provider’s global authoritative serving footprint. The key architectural idea is a hidden primary: Infoblox NIOS is the source of truth for zone content, but it is not exposed as a public name server.

The security benefit is straightforward: because the primary doesn’t answer internet queries directly, it is insulated from brute-force scanning and high-volume floods, keeping the source of truth more protected while shifting that exposure to the internet-facing secondaries, where you can apply targeted controls such as rate limiting, DDoS protection, and tighter monitoring.

Operationally, it also reduces risk because changes are managed on the primary server and then safely propagated to the external serving layer.

### Customer Context

- A regional bank must keep authoritative zone management under tight internal control (audit/compliance).
- They also need global performance and resilience for internet queries (especially during spikes).

### Challenges

- **DNS Records Mastered in SaaS/Cloud DNS**
  - » External authoritative records are created and managed directly in the SaaS provider (e.g., Cloudflare) with limited central oversight.
  - » Self-hosted DNS, if present, plays a secondary or legacy role only.

- **Fragmented Record Ownership**  
Different teams (web, DevOps, regional IT) manage records in different consoles, with no central authority.
- **Limited Integration with Internal DDI and IPAMI**  
Public DNS decisions are decoupled from internal IPAM and network policy, increasing the chance of stale or conflicting records.

### Negative Business Impact

- No single authoritative source of truth for public DNS data
- Risk of drift between self-hosted and SaaS-hosted zones
- Difficulty enforcing DNSSEC, security policies, and change controls across all external DNS endpoints

### Architecture with Infoblox

- **Infoblox NIOS authoritative DNS** acts as the **hidden primary**
  - » Hosts the “source of truth” zone content
- Not directly exposed to the internet (not in public NS delegation, not generally reachable from the internet)
- A **SaaS authoritative DNS host** (e.g., a large global provider) acts as the **public secondary/serving layer**.
- **Infoblox External DNS** provides unified management and/or synchronization workflows so changes to the primary zone are reflected in the serving layer.

### Key Components

- **NIOS Hidden Primary (Source of Truth):** NIOS Grid (typically an HA pair) hosting all authoritative copies of external zones
- **SaaS Provider Secondaries:** Cloudflare/Akamai configured as secondaries that receive zone transfers from NIOS
- **DNS Infrastructure Protection (optional but recommended):** Protects NIOS hidden primaries from DDoS and protocol abuse, particularly if they are exposed (e.g., for transfers or specific fallback scenarios)
- **Universal DDI Management:** Centralized zone management in the Portal, which orchestrates changes on NIOS and provides visibility into SaaS provider configurations
- **Brand Protection Services:** For lookalike detection and takedown

### Architecture View

- **Control Plane**
  - » DNS changes are made centrally in Infoblox (portal/API).
  - » Zone data is synchronized to the SaaS DNS layer using zone transfers (AXFR/IXFR).
    - Note: SaaS DNS layer must support acting as a secondary authoritative DNS server to an external primary authoritative DNS server
- **Data Plane**
  - » Domain registrar delegates bank.com NS records to the SaaS authoritative name servers (public-facing).
  - » Internet resolvers query SaaS name servers only.

## Typical Flow

1. Zones and records are authored in the Infoblox Portal and stored on NIOS as the **hidden primary**.
2. SaaS providers are configured as **secondaries**; they pull zones via secured AXFR/IXFR from NIOS.
3. End-user queries are answered by SaaS providers' global DNS networks.
4. NIOS remains the source of truth; all changes flow from NIOS outward.

## Design Considerations

- **Centralized Control**

- » Treat NIOS as the single source of truth for all public zone data. Disable or tightly control direct edits in SaaS provider consoles to avoid drift.
- » SaaS/cloud providers as secondary distribution layer (if supported)
  - Cloudflare, Akamai, or cloud DNS services receive zone transfers or are updated from Infoblox, serving as globally distributed secondaries.

- **Resiliency**

Ensure NIOS primaries are deployed in HA pairs and sized for zone transfer volumes, not external QPS (since they are not directly answering public queries).

- **Unified Policy, Security and Automation**

- » DNSSEC signing, DNS Infrastructure Protection can be applied centrally to the primary zone data.
- » CI/CD and IaC pipelines integrate with a single Infoblox API, rather than multiple provider-specific APIs.

- **Security**

- » Use TSIG (if supported) or lock down zone transfer ACLs to provider IP ranges; monitor transfer logs for anomalies
- » Apply DNS Infrastructure Protection around the primaries to guard against reconnaissance and targeted attacks

## Advantages

- Centralized control over all external authoritative data, while retaining the elasticity of SaaS DNS distribution
- Consistent security posture (DNSSEC, DNS Infrastructure Protection) applied once at the Infoblox layer
- Simplified automation and change control; DevOps interacts with one primary source instead of many

## Positive Business Outcomes

- **Reduced Operational Complexity:** One primary system of record with multiple high-scale distribution options.
- **Stronger Security and Compliance:** DNSSEC and DNS layer protections are centrally enforced on all external DNS.
- **Faster Innovation:** Application teams can roll out changes quickly via streamlined pipelines without worrying about where DNS is physically hosted.

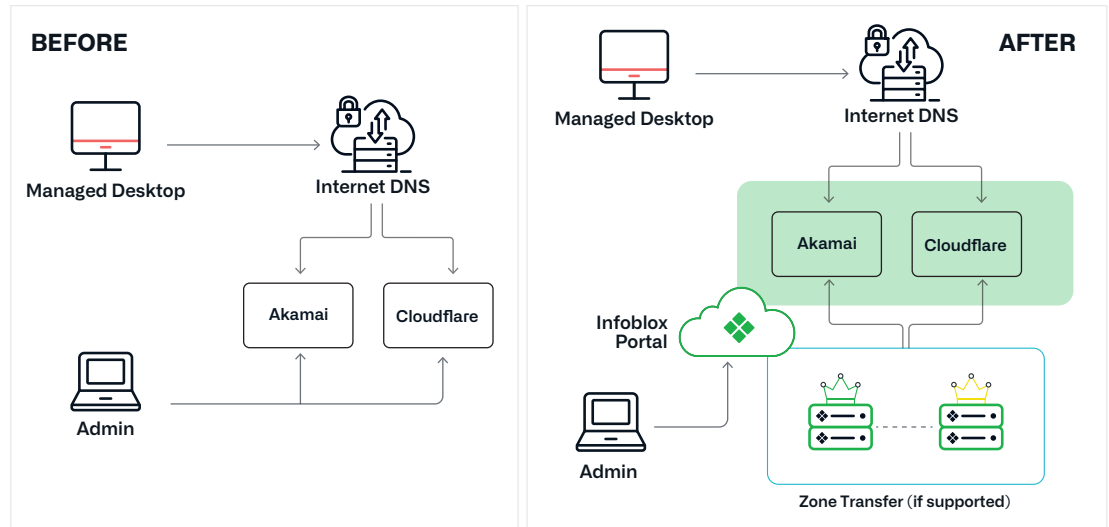


Figure 4. SaaS-hosted external DNS with Infoblox as hidden primary

## Why Customers Choose This Deployment Model

They want the **governance and compliance comfort** of controlling the primary zone internally while using SaaS for **global authoritative serving scale** and reduced exposure of the primary.

## SELF-HOSTED EXTERNAL AUTHORITATIVE DNS

### Sample Customer Scenario: National Utility with Sovereignty Requirements and High Attack Risk

This scenario is for organizations that cannot use SaaS authoritative DNS (or choose not to) due to sovereignty, regulatory requirements, or operational control mandates. They run external authoritative DNS themselves, which means their name servers are exposed to the internet and must be treated like any other critical, attackable public service.

The architectural emphasis is resiliency and survivability: deploy self-hosted authoritative DNS on Infoblox NIOS across multiple sites and add DNS Infrastructure Protection to improve availability during DoS/DDoS and other DNS-targeted attacks. This pattern is less about “simplifying provider sprawl” and more about “operate safely under real-world threat conditions.”

### Customer Context

- A national utility must self-host authoritative DNS due to:
  - » Sovereignty requirements
  - » Strict governance
  - » Operating constraints that prohibit using SaaS for authoritative DNS
- The organization has elevated exposure to DDoS attempts and disruptive activity.

### Challenges

- **External DNS Is “Just Infrastructure”**
  - » Public authoritative DNS servers are exposed to the internet without specialized DNS-layer protection.
  - » DDoS and DNS-specific attack protections are left entirely to upstream providers or generic firewalls.

- **Limited or No DNS-Layer Threat Intelligence**

There is no integrated capability to detect DNS-based threats like reflection/amplification, NXDOMAIN floods, or malicious domain usage.

- **Fragmented security event visibility**

DNS logs (if available) are not enriched with threat context, making it hard for SecOps to detect or investigate DNS vectors.

### Negative Business Impact

- Increased risk that DDoS or DNS-targeted attacks take down external authoritative servers
- No systematic way to detect and respond to malicious queries
- Security and networking teams lack shared, actionable DNS telemetry

### Architecture with Infoblox

- Self-hosted authoritative DNS on Infoblox NIOS deployed as a resilient Grid
  - » At least two geographically separated sites (e.g., two data centers)
  - » Optional additional nodes for regional presence
- DNS Infrastructure Protection is deployed to detect/report/stop DoS/DDoS and other attacks targeting authoritative DNS servers.
- The registrar delegates public zones directly to the organization's authoritative name servers.

### Key Components

- **NIOS External DNS Grid**

- » **External hidden primary pair** (VRRP HA) hosting all authoritative public zones
- » One or more **external secondaries** that answer internet traffic, typically [anycast](#) for resiliency and performance
  - Note: External anycast is significantly more complex to design and operate than internal anycast. Typically not recommended.

- **DNS Infrastructure Protection**

Enabled on external authoritative servers to mitigate DDoS, reflection, NXDOMAIN floods, and protocol abuse

- **Infoblox Portal (Universal DDI Management)**

- » Central administration for external zones on NIOS, with RBAC and API-driven automation
- » Optional: Management of related internal DNS, IPAM, and discovery for coherent change management

### Architecture View

- **Control Plane**

- » DNS operations teams manage zones/records on NIOS (directly or via the Infoblox portal/API, depending on operational model)
- » Security operations receives telemetry/alerts and integrates signals into SIEM/SOAR workflows (implementation-specific)

- **Data Plane**

- » Internet resolvers query the utility's public authoritative DNS servers
- » DNS Infrastructure Protection provides DNS-specific mitigations to maintain service under attack conditions

### Typical Flow

1. Public resolvers query www.example.com.
2. Queries are routed to external NIOS secondary servers.
3. DNS Infrastructure Protection inspects and filters malicious traffic while permitting legitimate queries.
4. Zone changes (new records, TTL adjustments, DNSSEC settings, if applicable) are managed in the **Infoblox Portal**, pushed to the hidden primary, then replicated to secondaries.

### Design Considerations

- **High Availability and Placement**
  - » Deploy hidden primaries as **VRRP HA pairs** in separate failure domains (e.g., distinct data centers or availability zones).
- **Security**
  - » Apply **DNS Infrastructure Protection** on all public-facing authoritative servers.
  - » Use access controls and ACLs for zone transfers (AXFR/IXFR) between hidden primary and secondaries.
  - » **Hardened external authoritative DNS infrastructure**
- NIOS with DNS Infrastructure Protection protects against **DDoS, amplification/reflection, NXDOMAIN floods, UDP floods, and DNS hijacking** while continuing to serve legitimate queries.
- **Operations**
  - » Manage zones centrally in the Portal, not directly on individual NIOS appliances, to avoid drift and ensure consistent policy.
  - » Integrate logs (queries, responses, attack telemetry) into your SIEM via NIOS and/or Universal DDI connectors.

### Advantages

- DNS infrastructure remains available even under heavy attack, preserving external service uptime.
- DNS becomes a high-value detection point for advanced threats using public-facing infrastructure.
- Network and security teams share a unified view of DNS threats and behavior.

### Positive Business Outcomes

- **Reduced risk of DNS-based outages and downtime** for public services due to DDoS and infrastructure-focused attacks
- **Earlier detection of sophisticated attacks**, improving mean time to detect (MTTD) and mean time to respond (MTTR)
- **Better regulatory alignment** for critical infrastructure, where DNS resilience and security are explicit expectations

## Why Customers Choose This Deployment Model

They need **full control** (self-hosted authoritative) and specialized protection for a service that is commonly targeted and business-critical.

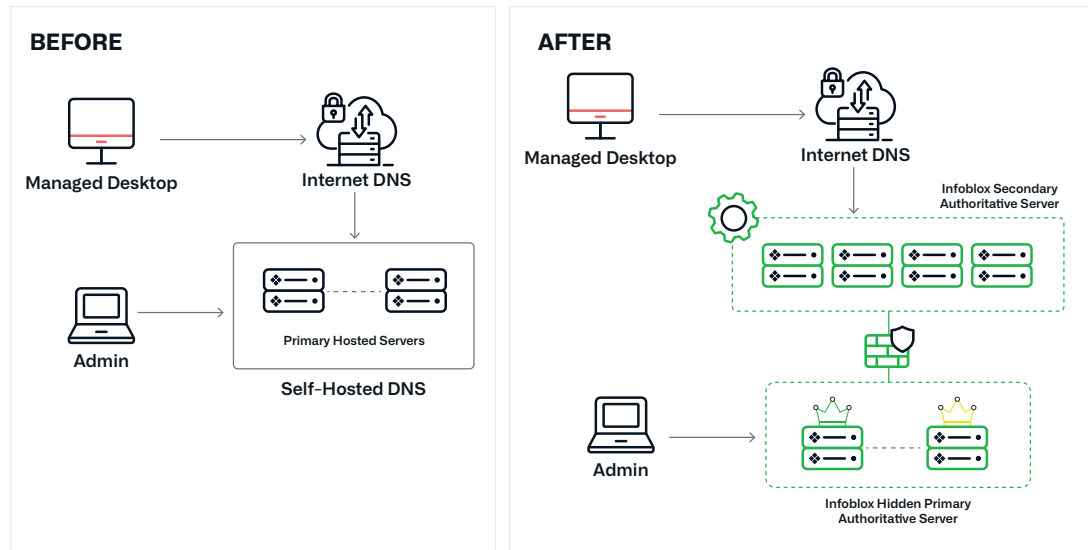


Figure 5. Self-hosted external authoritative DNS

## HYBRID-HOSTED EXTERNAL DNS (NIOS + SAAS IN MULTI-PROVIDER DNS)

### Sample Customer Scenario: Global E-Commerce Brand Designing for DNS Provider Failure

This scenario is built around one simple belief: for a top-line digital business, external DNS is a Tier-0 dependency, and relying on a single authoritative DNS provider creates a business risk that is hard to justify. The architecture uses two authoritative DNS providers in parallel, with both sets of name servers published for the domain, so the internet can still resolve the zone even if one provider suffers an outage.

Infoblox's role in this pattern is the "synchronization and consistency engine." It helps administer the zone like one logical system while serving it from two independent authoritative platforms. The benefit is measurable: materially improved continuity and a cleaner operational model for keeping both providers aligned.

### Customer Context

- A high-revenue e-commerce company treats DNS as a Tier-0 dependency.
- Leadership is concerned about the business impact of a **single DNS provider outage**.
- They **cannot tolerate downtime** in external websites and APIs, even if a SaaS DNS provider suffers a catastrophic outage.
- High-value brands and services where **business continuity** and **regulatory expectations** demand redundant authoritative paths.

## Challenges

- **Single External DNS Provider:** (e.g., Cloudflare or a hyperscaler DNS service) hosts all authoritative zones for public websites and SaaS apps.
- **No Self-Hosted or Backup Authoritative Infrastructure**
  - » No on-prem or alternate DNS hosting in place.
  - » DR planning assumes the external provider is always available.
- **Limited or Ad Hoc Health Checks and Failover**  
Application-level failover may exist, but DNS itself has no multi-provider DNS redundancy across providers.

## Negative Business Impact

- **Single point of failure**, meaning a major outage at the SaaS DNS provider directly translates into website/API/email outages (“SaaS DNS Outage = Website Outage”).
- The business is fully dependent on the provider’s change control, incident response, and SLAs.
- Little control over how quickly DNS recovery can occur in a catastrophic provider failure scenario.

## Architecture with Infoblox

This pattern extends the hidden primary model by adding **self-hosted NIOS** secondaries in parallel with the SaaS provider.

- Two authoritative DNS providers are operated in parallel:
  - » Provider A: SaaS DNS host used today (often chosen for performance features)
  - » Provider B: An alternate provider or **self-hosted authoritative** (e.g., NIOS) for diversification
- **Infoblox External DNS** is used as the **central control plane**, so both providers stay synchronized.
- At the registrar (or parent zone), the domain’s NS set includes authoritative name servers from **both providers** (within registrar limits).

## Key Components

- **NIOS Hidden Primary (HA pair)**
- **SaaS Provider Secondaries** (global anycast footprint)
- **NIOS External Secondaries**
- **DNS Infrastructure Protection** on NIOS external servers (hidden primary and secondaries)
- **Universal DDI Management** as control plane, plus Brand Protection Services

## Architecture View

- **Control Plane**
  - » Infoblox manages zone content and pushes updates to both Provider A and Provider B.
  - » Operational dashboards highlight drift and record parity issues (implementation detail—commonly via reporting and automated checks).
- **Data Plane**
  - » Internet resolvers can query either provider’s authoritative name servers.
  - » If Provider A is impaired, resolvers will still be able to get authoritative answers from Provider B.

### Typical Flow

1. Public resolvers see multiple NS records for each public zone—pointing to both SaaS provider name servers and NIOS external secondaries.
2. Under normal conditions, both paths answer successfully, spreading query load.
3. If the SaaS provider experiences an outage or systemic error, public resolvers fall back to NIOS secondaries, which remain fully authoritative and protected by DNS Infrastructure Protection.
4. All changes still originate from the NIOS hidden primary via Universal DDI, replicated to both SaaS and NIOS secondaries.

### Design Considerations

- **Zone NS Records**
  - » Publish at least **two SaaS NS** records and **two NIOS NS** records per zone for diversity.
- **Multi-Provider DNS redundancy**
  - » DNS queries can be served by either the SaaS service or the Infoblox self-hosted infrastructure.
  - » If the SaaS service fails, NIOS continues answering queries, keeping websites and APIs reachable (“DNS Redundancy = Websites Still Reachable”).
- **Capacity and Sizing**

Size NIOS external secondaries so that they can handle full production QPS if the SaaS provider is unavailable.
- **Routing and Policy**

Use DNS Infrastructure Protection and upstream network controls (ACLs, rate limiting, scrubbing) to safeguard NIOS secondaries from attack amplification when they are the only active path.
- **Operations**
  - » Maintain a single authoring workflow via the Infoblox Portal. Avoid special case management during failover.
  - » Regularly test failover from SaaS to NIOS by simulating provider outages and verifying resolution continuity and performance.

### Advantages

- Eliminates DNS as a single point of failure for external services.
- Allows organizations to continue using existing SaaS DNS for scale and distribution while owning a resilient fallback.
- Provides operational visibility and control during an outage, not just at the mercy of the SaaS provider.

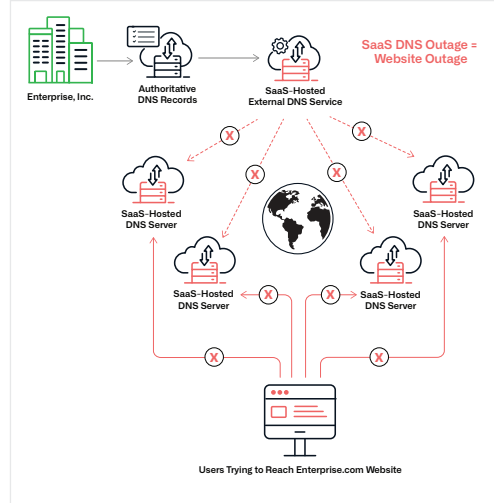
### Positive Business Outcomes

- **Significantly improved uptime** for public websites, customer portals and APIs, even during catastrophic SaaS DNS failures
- **Reduced revenue loss and reputational damage** from external DNS outages
- Better alignment with **BC/DR and regulatory expectations**, demonstrating that DNS resiliency is not fully outsourced
- Enhanced customer trust by guaranteeing reachability for critical digital services

## Why Customers Choose This Deployment Model

They want a **provider-diversified authoritative DNS posture** to reduce the probability that a single vendor outage becomes a customer-facing outage.

### SaaS-Hosted External DNS Only



### Hybrid Hosted External DNS Redundancy

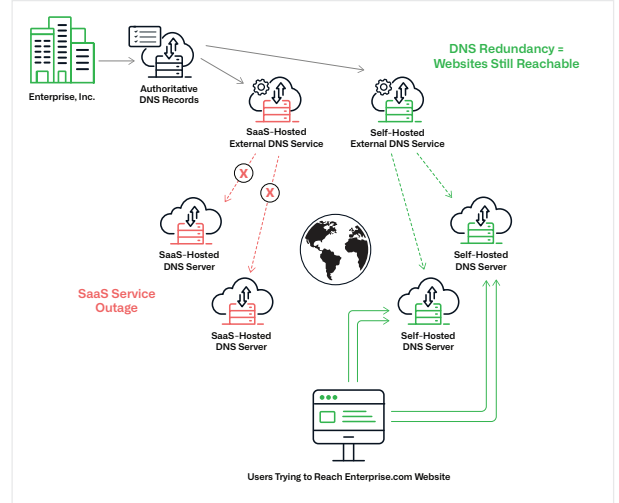


Figure 6. Hybrid-hosted external DNS—failure scenario

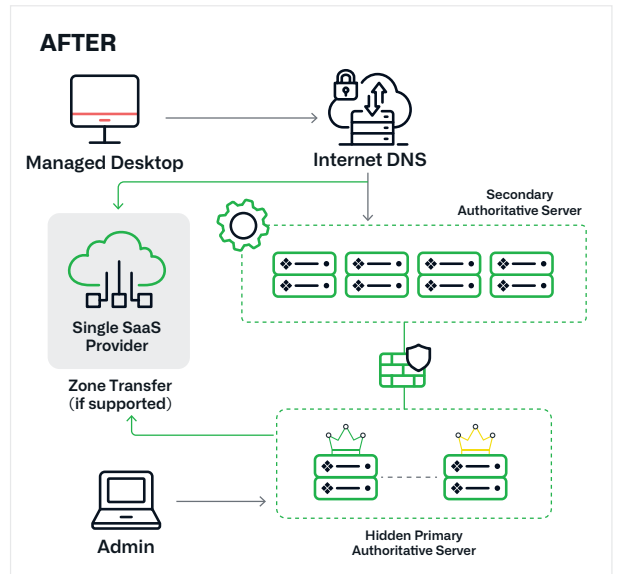
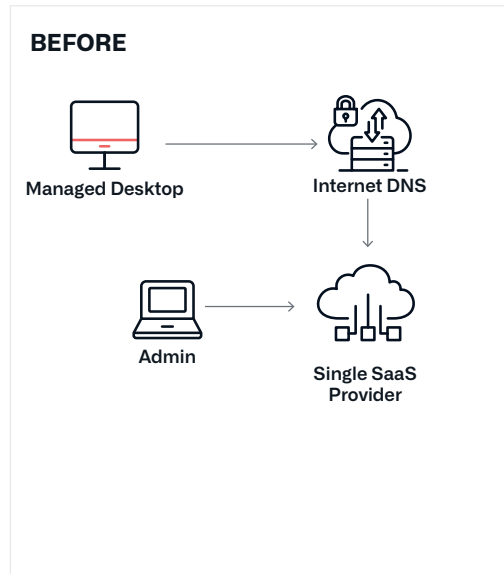


Figure 7. Hybrid-hosted external DNS

## CONCLUSION

Infoblox for External Authoritative DNS gives organizations a pragmatic, future-proof way to close one of the most critical gaps in modern infrastructure: the disparity between how carefully internal DNS is managed and how exposed, fragmented, and under-governed external DNS often is. At a strategic level, this reference architecture shows how to treat external DNS as **foundational business infrastructure**—on par with core networking and identity—by standardizing on a single control plane, enforcing consistent policy, and building in redundancy that can withstand both provider outages and targeted attacks.

From a technical standpoint, the designs in this document outline clear patterns for **self-hosted**, **SaaS-hosted**, and **hybrid-hosted** external DNS, with NIOS, Universal DDI Management, DNS Infrastructure Protection, and Brand Protection Services each playing well-defined roles. Architects can adopt these patterns incrementally: starting with unified management of existing SaaS DNS, hardening self-hosted authoritative servers with DNS Infrastructure Protection, then evolving into hybrid multi-provider DNS deployments where NIOS and SaaS providers share authoritative responsibility. Throughout, the Infoblox Portal remains the single source of truth for zones, records, IP address, space, and automation workflows.

For leaders, the outcome is reduced outage risk, stronger brand protection, and a clearer, auditable control model for a service that directly underpins revenue, customer experience, and regulatory obligations. For technical teams, the outcome is a **coherent, automatable architecture** that replaces ad hoc scripts and siloed consoles with a repeatable design: centralized policy and visibility at the control plane, diverse and resilient service at the data plane, and integrated security that treats DNS not just as plumbing, but as a strategic enforcement and observability point.

## GLOSSARY

Term	Definition
anycast	A routing technique where the same IP address is advertised from multiple, geographically distributed servers; Routing protocols steer each client to the “nearest” healthy instance.
authoritative DNS/ authoritative name server	Hosts the official DNS records for a zone (e.g., example.com) and responds with final answers. In external DNS, these servers are the “source of truth” the internet relies on to reach your public sites, email, and API endpoints. If they fail or are misconfigured, your public presence goes dark.
CNAME/dangling CNAME	A CNAME record makes one name an alias of another (e.g., www.example.com → app.provider.com). A dangling CNAME occurs when the target is removed, but the alias remains, potentially allowing attackers to register the orphaned target and hijack traffic—making CNAME hygiene a key part of external DNS security.
DDoS against DNS	Distributed denial-of-service attacks that flood DNS servers or abuse protocol behaviors (amplification, reflection, NXDOMAIN floods) to make domains unreachable. External DNS must be protected with DNS-aware defenses that absorb these attacks while continuing to serve legitimate queries.
DNS cache/ caching resolver	A DNS cache stores recently resolved answers (e.g., the IP address of www.example.com) so subsequent queries can be answered locally without walking the full DNS hierarchy again. This dramatically reduces latency and offloads traffic from external authoritative servers, but it also means changes to external DNS (cutovers, DR events, record fixes) won’t be seen until cached entries expire according to their TTL. Well-designed external architectures therefore pair appropriate TTLs with clear cache flush procedures during planned changes and incident response.

Term	Definition
DNSSEC (Domain Name System Security Extensions)	Adds cryptographic signatures to DNS data so resolvers can verify that responses haven't been altered in transit. In external DNS, DNSSEC helps prevent cache poisoning and domain hijacking; primaries like NIOS typically handle signing and key management while public secondaries serve the signed data.
external authoritative DNS (external DNS)	Public-facing authoritative DNS that lets anyone on the internet resolve your domains to the correct IP addresses. It underpins websites, SaaS apps, email and public APIs, and must be reachable globally, which makes it both mission-critical and a prime target for attack.
FQDN (fully qualified domain name)	The complete, absolute domain name for a host, including all labels and the root (e.g., www.api.example.com.). External DNS designs rely on consistent FQDN patterns to structure zones, automate record creation, and maintain clarity across multiple clouds and providers.
hidden primary (hidden master)	An authoritative server that holds the master copy of zones but is not exposed to the internet; it publishes data to public secondaries via zone transfer. This pattern lets you centralize control and security (e.g., on NIOS) while using cloud or SaaS DNS as the distributed edge for performance and redundancy.
MX and SRV records	MX records define the mail exchangers for a domain, while SRV records advertise specific services (such as SIP or LDAP), including the host and port offering the service. Misconfigurations in these records can break email and key federation or VoIP services globally, so they are high-impact objects in any external DNS architecture.
NS records (name server records)	NS records indicate which authoritative name servers are responsible for a zone and are used for delegation (e.g., from .com to example.com, or from example.com to a delegated subzone). For external DNS, keeping NS records consistent between parent and child zones—and correctly aligned with your external DNS providers—is critical for reliability, DNSSEC chains of trust, and clean failover behavior.
NXDOMAIN	A DNS response code meaning “nonexistent domain.” At scale, attackers can generate huge NXDOMAIN volumes to exhaust resources on external authoritative servers, so monitoring and rate limiting these patterns are important for public zones.
recursive resolver	A DNS server that takes a client's query and walks the DNS hierarchy (root → TLD → authoritative) until it finds an answer, caching results along the way. This is the natural control point for Protective DNS, because it sees all outbound queries to external domains.

Term	Definition
root name servers	A small, globally distributed set of servers that host the DNS <b>root zone</b> , which lists all TLDs. Recursive resolvers query root servers when they don't know which TLD server to ask next, so external DNS architects must ensure resolvers can reliably reach the root and handle failures gracefully, even though they never operate these servers themselves.
secondary DNS server	A read-only authoritative server that receives zone data from a primary (or hidden primary) and answers queries for that zone. Multiple secondaries, often across regions and providers, improve performance and resilience for external DNS while keeping change control centralized.
SOA record (start of authority)	Specifies the primary authoritative server for a zone and timers for refresh, retry, expiry, and default TTL. SOA parameters influence how quickly secondaries and resolvers learn about changes, directly affecting cutovers, DR, and DNSSEC key rollover operations for external zones.
TLD (top-level domain)	The highest-level label in a domain name, such as .com, .org, or country codes, like .jp and .in. Each TLD is managed by a registry with its own authoritative name servers; when you register a domain, you are effectively inserting NS records at the TLD so the rest of the internet can discover your authoritative DNS for that zone.
TTL (time to live)	The time a DNS answer is considered valid and may be cached by resolvers and clients before they must re-query. Short TTLs give agility for cutovers and failover (e.g., BC/DR scenarios), while longer TTLs reduce query load and latency for stable records.
zone transfer (AXFR/IXFR)	Mechanisms for copying zone data from primary to secondary servers: <b>AXFR</b> for full transfers, <b>IXFR</b> for incremental. Secure, well-governed zone transfers are essential in hidden primary and hybrid external DNS designs to keep public secondaries in sync without exposing unnecessary attack surface.
zone/zone file	A DNS zone is a specific, manageable portion of the <a href="#">Domain Name System</a> (DNS) namespace, typically encompassing one or more domains or subdomains. It acts as an administrative space delegated to a particular organization, allowing for granular control over DNS records, such as mappings between domain names and IP addresses. Zone files on authoritative servers define these records and are the unit of change, delegation, and replication in external DNS architectures.
Iterative Lookup	An iterative lookup is a DNS query process where a DNS resolver, or client, queries multiple DNS servers sequentially (e.g., Root → TLD → Authoritative) to resolve a domain name. Each server responds with the best information it has—often a referral to another server—until the final IP address is found, putting the onus of follow-up on the client.



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

**Corporate Headquarters**  
2390 Mission College Blvd, Ste. 501  
Santa Clara, CA 95054

+1.408.986.4000  
[www.infoblox.com](http://www.infoblox.com)

