BLUECAT™

Edge DNS Global Service Load Balancing (GSLB)

Intelligent, flexible load balancing at the DNS layer

Challenge

Application GSLB keeps control locked in siloed teams and expensive appliances, limiting agility, increasing costs, and making it hard to extend smart traffic steering to where users and applications live.

Solution

BlueCat Edge DNS GSLB introduces intelligent, policy-driven traffic control into the DNS layer, providing DDI teams with real-time, scalable, and cost-effective control over how users access applications.

Benefits

- Route traffic based on real-time health and network typology
- Enforce DNS policies without relying on external teams
- Lower cost and deploy anywhere — no need for costly GSLB appliances

Contact us

Bring back DNS GSLB to the teams that own DNS resolution

BlueCat Edge DNS Global Server Load Balancing (GSLB) orchestrates DNS response delivery with precision by dynamically prioritizing answers based on real-time health status and network topology. This step ensures reliable application delivery and optimal traffic routing across multiple network segments and geolocations.

In large enterprises, DNS GSLB management is often decentralized. For instance, it may fall under the purview of teams managing F5 load balancers, rather than the DNS, DHCP, IPAM (DDI) team. This decentralization can create challenges for the DDI team when implementing changes at scale, particularly in disaster recovery situations.

DDI teams can regain control of DNS GSLB by leveraging capabilities within a DNS proxy or first-hop DNS resolver solution such as BlueCat Edge, which has DNS GSLB capabilities built in.

Solution overview: What is BlueCat Edge DNS GSLB?

As BlueCat Edge primarily serves as the first-hop recursive DNS resolver in the query path, it offers DNS GSLB capabilities that utilize customizable rules to automate load balancing optimization and disaster recovery. By deploying cost-effective and highly available Edge service points to deliver DNS GSLB closer to clients and endpoints, network teams can cover the entire enterprise network footprint, which would be impossible to accommodate with costly application load-balancing infrastructure. This deployment method makes delivering zero TTL decision-making DNS GSLB services through BlueCat Edge a value add, providing streamlined, reliable, and cost-effective traffic distribution for enterprises using expensive or less advanced GSLB solutions for DNS resolution.

How does it work?

The DNS GSLB functionality enhances load balancing by operating close to the client as a first-hop resolver and can operate in conjuction with existing GSLB investments. This functionality ensures low-latency, tailored responses at the time of the query that meet specific client and application needs, whether as a standalone solution or in conjunction with existing GSLB investments. By utilizing Edge DNS GSLB as a smart policy engine, network teams can refine responses from on-path GSLB solutions more effectively.

Additionally, teams can maintain the order of preferred IP addresses within high-priority networks or exclude unnecessary responses to minimize the risk of exposure while maximizing value and safeguarding existing infrastructure. Furthermore, network teams can easily configure and prioritize responses through a user-friendly interface, allowing administrators to create unique resolution paths with rules and exceptions for segmented devices, applications, and services.

The brains behind the balancing: A rules-based order that starts at the network/subnet level

Organizing sites using DNS segmentation and zero-trust DNS methods provides critical controls for handling traffic and implementing security policies suited to different client types, such as IoT devices. By organizing devices into specific DNS segments, administrators can enhance routing, enforce access controls, and safeguard against malicious activities. Zero-trust DNS also verifies that devices communicate only with authorized endpoints, enhancing security through real-time threat identification and proactive policy enforcement.

Migration is easy. NetOps teams that have current DNS business logic organized by site, country, region, city, or other breakout typologies, can easily transfer that logic to Edge DNS GSLB. What's more, Edge DNS GSLB implements rules at the network level, ensuring that traffic distribution is based on subnets, with exceptions made at the domain level.

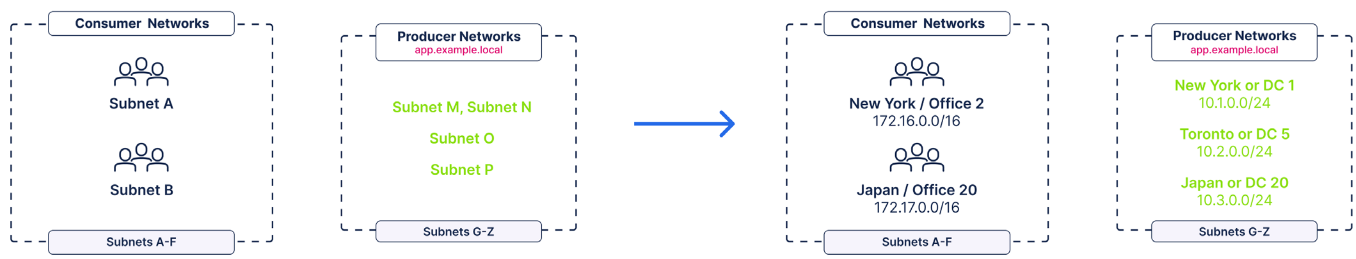

Figure 1. DNS GSLB network/subnet methodology fits any existing network typology

To ensure that traffic routing decisions, based on existing network typology, are effective and responsive to real-time conditions, Edge DNS GSLB employs mechanisms and strategies that allow for intelligent server selection and optimal query responses through:

- **Network-based policies**
  Define intelligent routing rules based on client (consumer) and application (producer) network groupings. By using IP address lists to represent logical network segments—such as regional data centers, departments, or business units—administrators can craft dynamic, policy-driven routing tailored to organizational and geographic needs. Policies can be applied globally, with support for domain-specific rules or a combination of both, enabling precise traffic steering.

  Example: Direct traffic from EMEA-based users to EMEA data center endpoints by matching source IP addresses to an IP address representing the EMEA region and applying prioritized routing logic.

- **Real-time, health-aware routing**
  Continuously assess endpoint health through customizable checks (e.g., ICMP, HTTP/S, TCP) and make routing decisions dynamically for every DNS query. This real-time evaluation ensures clients always receive answers pointing to available and responsive services, without waiting for DNS propagation or manual refreshes.

  Advantage: If an endpoint becomes unavailable, it is instantly excluded from responses at query time—keeping services available without any delay or administrative overhead.

Use cases

1. Multiregion disaster recovery

When delivering critical services such as **`app.example.local`**, ensuring availability across multiple geographic regions requires a routing solution that responds intelligently to network conditions. With Edge DNS GSLB, organizations define resolution logic based on consumer and producer subnet groupings, making it easy to match your current infrastructure rather than forcing changes to fit a rigid DNS model.

Let's walk through a disaster recovery scenario, illustrated across Figures 2, 3, and 4:

In Figure 2, consumer networks **Subnet A** and **Subnet B** represent users in two different geographic regions, each attempting to resolve app.example.local. At this point, Edge DNS GSLB has completed real-time health checks and determined that both **Subnet M** and **Subnet N** (the primary production networks) are healthy. DNS responses are optimized and distributed between M and N, based on policies that align with business logic—such as geographic affinity, capacity, or performance metrics.

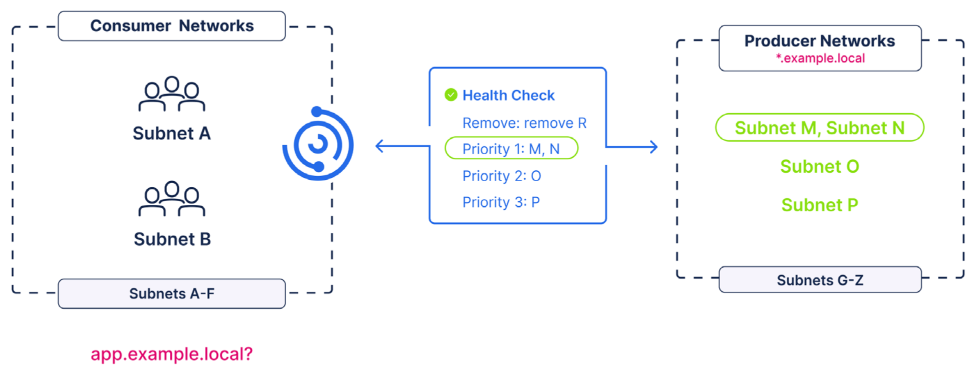

Figure 2. Normal operations with primary endpoints online

Suddenly, disaster strikes. In Figure 3, health checks now indicate that **Subnet M** and **Subnet N** are unavailable—possibly due to power outages, fiber cuts, or a DDoS attack affecting health-check enabled applications. Instead of waiting for TTL expirations or manual DNS reconfigurations, DNS GSLB dynamically reroutes traffic to **Subnet O** for those applications that are located in a different city or cloud region but are also capable of serving app.example.local. This automatic failover ensures uninterrupted service to users, minimizing downtime and preserving customer trust.

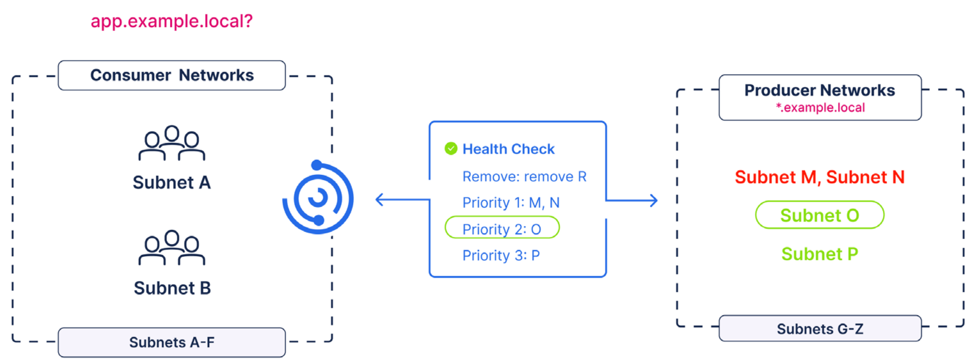

Figure 3. Full failover triggered by outage in primary subnets

In a less severe scenario, illustrated in Figure 4, only Subnet N becomes unavailable. Edge DNS GSLB immediately shifts all traffic for app.example.local to Subnet M without any user or application intervention. Once health checks verify that Subnet N is back online, traffic rebalances based on the original priority logic, restoring normal operations without any manual adjustments.

In addition, it is possible to support scenarios where a single gateway or shared service fronts multiple applications. By configuring a health check on that gateway, administrators can monitor its availability and use a single GSLB rule to redirect traffic for all dependent applications if the gateway becomes unavailable. This step simplifies failover logic, ensuring that groups of related services remain available without requiring individual checks or rules for each one.

Edge DNS GSLB empowers network and infrastructure teams to implement robust disaster recovery strategies without relying on brittle workarounds or slow propagation mechanisms. By utilizing subnet-level policies, real-time health checks, and intelligent prioritization logic, Edge DNS GSLB ensures that users are always directed to healthy, geographically appropriate endpoints—even during partial or complete site outages.

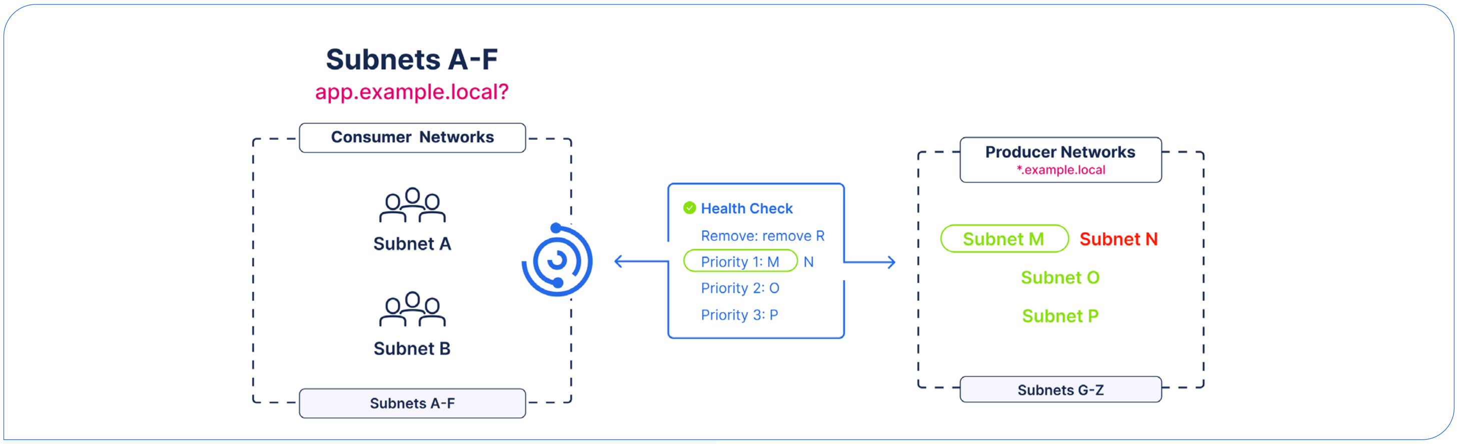

Figure 4. Partial failover and load redistribution

2. Per application multinetwork delivery

Edge DNS GSLB allows organizations to define precise, domain-specific routing policies tailored to the needs of each application, even within the same consumer network block. This flexibility enables different applications to utilize separate network paths and priorities, tailored to operational, security, or performance requirements, without requiring additional infrastructure or manual intervention.

In Figure 5, all DNS queries from IP Block A are routed to Subnet M by default, as defined by the general block-level GSLB rules. However, an override is in place for `app.example.local`, which is instead directed to Subnet P. This setup ensures that critical applications can have custom delivery paths based on business needs, while other traffic continues to follow standard DNS steering rules.

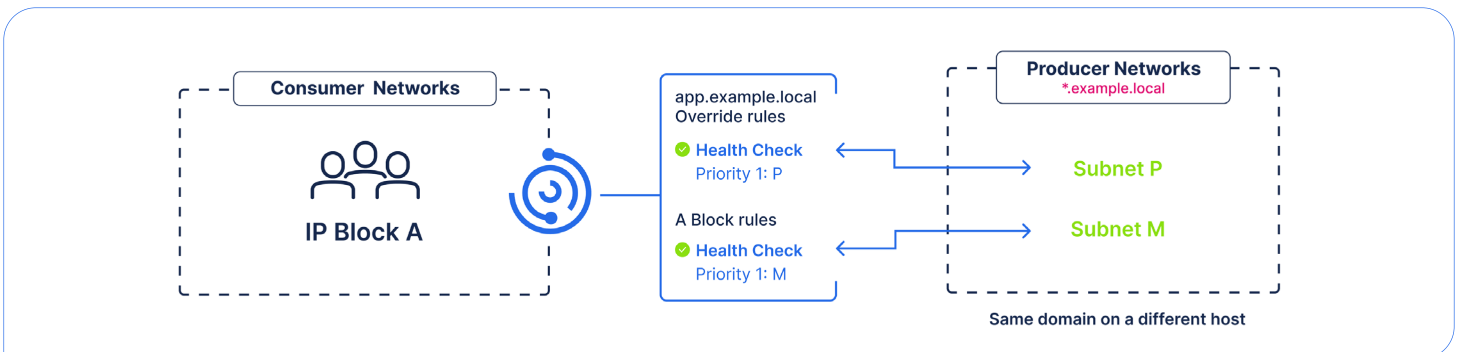

Figure 5. Multinetwork delivery with applied exceptions for a specific domain

In Figure 6, internal users in IP Block A, such as members of an research and development group, access multiple internal services. Queries for dev.example.local are routed to Subnet P for performance or proximity reasons, while hr.example.local traffic is explicitly directed to Subnet M, perhaps due to compliance or data residency requirements. This demonstrates per-application routing within a shared consumer network, enabling optimized delivery for each service independently.

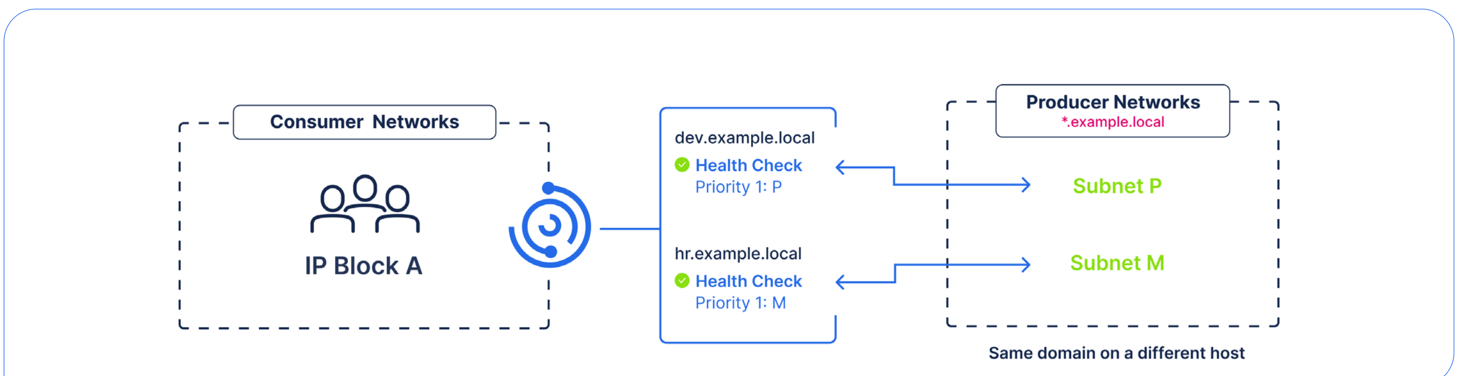

Figure 6. Application-aware routing across multiple internal services

This use case highlights how Edge DNS GSLB supports nuanced, application-level routing policies across shared network environments. Whether you need to prioritize particular subnets for specific applications or override default behaviors for strategic workloads, GSLB enables granular control without increasing network complexity. This flexibility is key for organizations looking to optimize internal application delivery while maintaining centralized visibility and control.

Key differentiators

The Edge DNS GSLB solution employs a network/subnet methodology that provides:

1. **Simplified management:** By applying rules at the network level, Edge DNS GSLB reduces the complexity of managing DNS configurations. Instead of creating rules for each domain, administrators can create rules for entire subnets with exceptions for domains, making the process more efficient.

2. **Enhanced performance and availability:** The methodology, combined with response randomization, ensures that traffic is distributed across multiple servers, improving the overall performance and availability of services. Health checks and prioritization further enhance the network's reliability.

3. **Flexibility:** Edge DNS GSLB provides flexibility in how traffic is managed and distributed. Administrators can easily adjust rules and priorities in response to changing business logic, network conditions, or evolving business requirements.

Solution benefits

Shifting DNS GSLB back to the DDI team delivers significant benefits to the enterprise:

- **Lower costs**
  Deploy cost-effective, scalable DNS GSLB to regions and sites that cannot afford costly load balancers.
- **Reduce risk**
  Enforce routing rules that keep traffic aligned with policies, even during outages, to minimize downtime, misrouting, and compliance gaps.
- **Complete control**
  Bring DNS GSLB under the control of tools and teams that own resolution and traffic policies at the source.
- **Delight users**
  Ensure end users get the most reliable, performant, and localized service every time they open their browser.

Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
Phone: 1-416-646-8400 | 1-866-895-6931

bluecat.com

SB-Edge DNS GSLB-07-07-2025