BLUECAT™

BlueCat Edge Intelligent Forwarding

How it works & how BlueCat customers use it.

Table of Contents

Introduction to BlueCat Edge

BlueCat Edge:

BlueCat Edge is an intelligent DNS resolver and caching layer that leverages existing DNS infrastructure to provide unprecedented visibility and control over DNS traffic. As a first hop DNS resolver, BlueCat Edge intelligently manages DNS forwarding policy and logs all queries to offer intuitive analytics and data governance.

While monitoring all DNS queries and IP addresses with BlueCat Edge, enterprises can also leverage BlueCat's advanced Threat Protection and policy-based network/security features to protect the enterprise against cyber threats, such as domain generation algorithms (DGA), command and control (C&C), and tunneling that lead to data exfiltration or network downtime. Threat Protection leverages threat feeds from Crowdstrike.

Intelligent Forwarding:

Intelligent Forwarding enables network teams to architect the most optimal and creative DNS resolution routes by leveraging namespaces in BlueCat Edge. By intelligently managing DNS forwarding policy governing hybrid cloud, enterprises can unlock new innovative architectures that deliver efficient SaaS services or direct internet access (DIA).

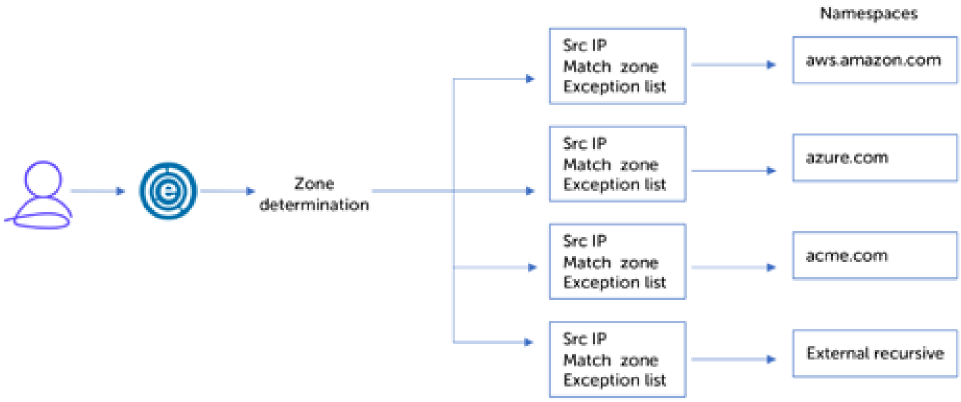
Namespaces:

To leverage Intelligent Forwarding, a namespace must be configured with one or more DNS forwarders, and can optionally include match and exception domain lists. Each site in BlueCat Edge will have at least one associated namespace, up to a maximum of ten. DNS cache is segmented across namespaces to prevent mixing of responses from different resolution paths. This permits BlueCat Edge to fully optimize query performance and maintain "state" between a variety of DNS authorities to ensure optimal client experience.

How BlueCat Edge Intelligent Forwarding works:

When BlueCat Edge receives a DNS query it goes through a process called zone determination to decide which DNS namespace(s) to use based on matching destination zone, source IP/network, security policies, and priority order of forwarders.

A typical namespaces configuration for a Cloud Only customer.



The above diagram shows a customer that has resources in AWS and Azure both while having a domain called acme.com. If none of the queries match then it will forward to an external resolver.

Based on the results of the zone determination, BlueCat Edge will select the proper DNS namespace(s) for resolution. Once it has determined a set of potential forwarders to query, it will try each of the selected namespaces in order, looking for a valid response. Should the resolver get a negative response from a namespace, it will remember the answer through policy based on the specific negative response status. It will then move on to the next namespace and attempt to resolve the query again until it receives a positive response. If all namespaces are exhausted without a positive response, then a negative response is returned to the client.

Important: *Namespaces permit zone overlap. This capability allows simplistic view management of DNS resource records. Individual records in a zone can be added or modified in an authoritative server without the requirement that all resource records are available in that zone. Zone overlap is a critical requirement for dynamic environments such as cloud computing where different networks may utilize the same zone but require different answers for a subset of the records. The forwarding policy in BlueCat Edge, unlike traditional conditional forwarding rules or other resolver solutions, enables this critical level of flexibility with simple administration. Many of the advanced use cases discussed below leverage this unique capability.*

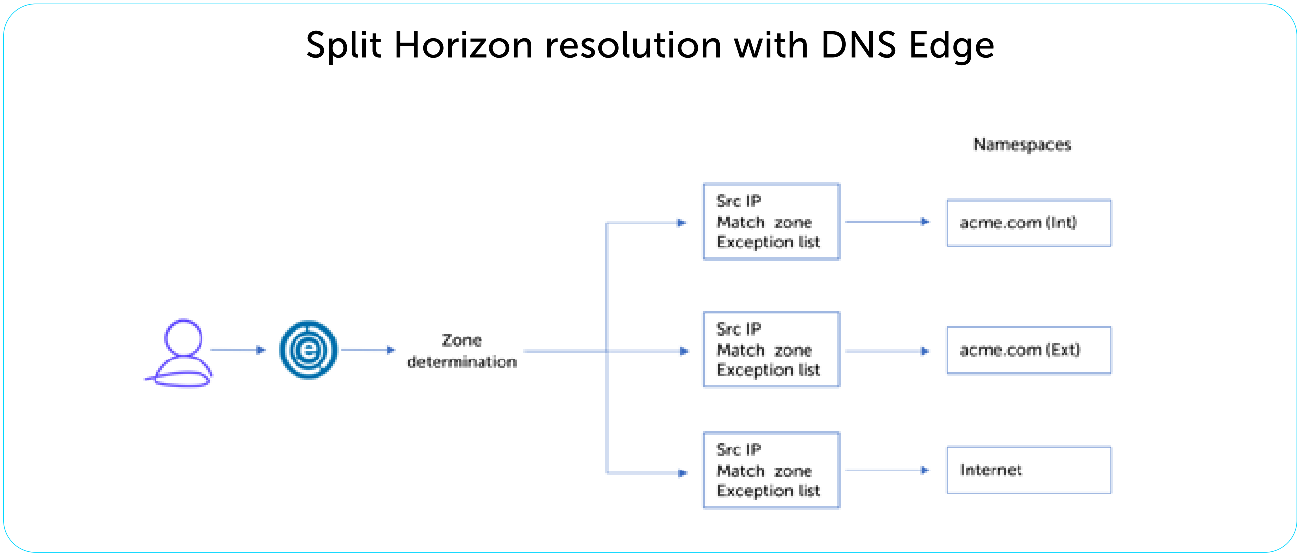
Use Cases For Intelligent Forwarding

Split View DNS Zones

Many enterprises use different views of the same zone for both private and public DNS. This allows for the same services, with the same names, to be resolvable internally and externally. Split View (often referred to as split-brain or split-horizon) allows for the distinct management of these views as if they were different zones.

However, resource records in the external view of the zone need to be maintained in the internal view as well. This leads to errors. Enterprises attempted to solve for this using web proxies, by having the proxy arbitrate the location of the service. In this scenario, there may be an "internal root" that overrides the public root zone, and completely segments these DNS namespaces. The rapid push to Direct Internal Access breaks this paradigm, and leaves enterprises without a solution for the proper resolution of split view DNS resource records.

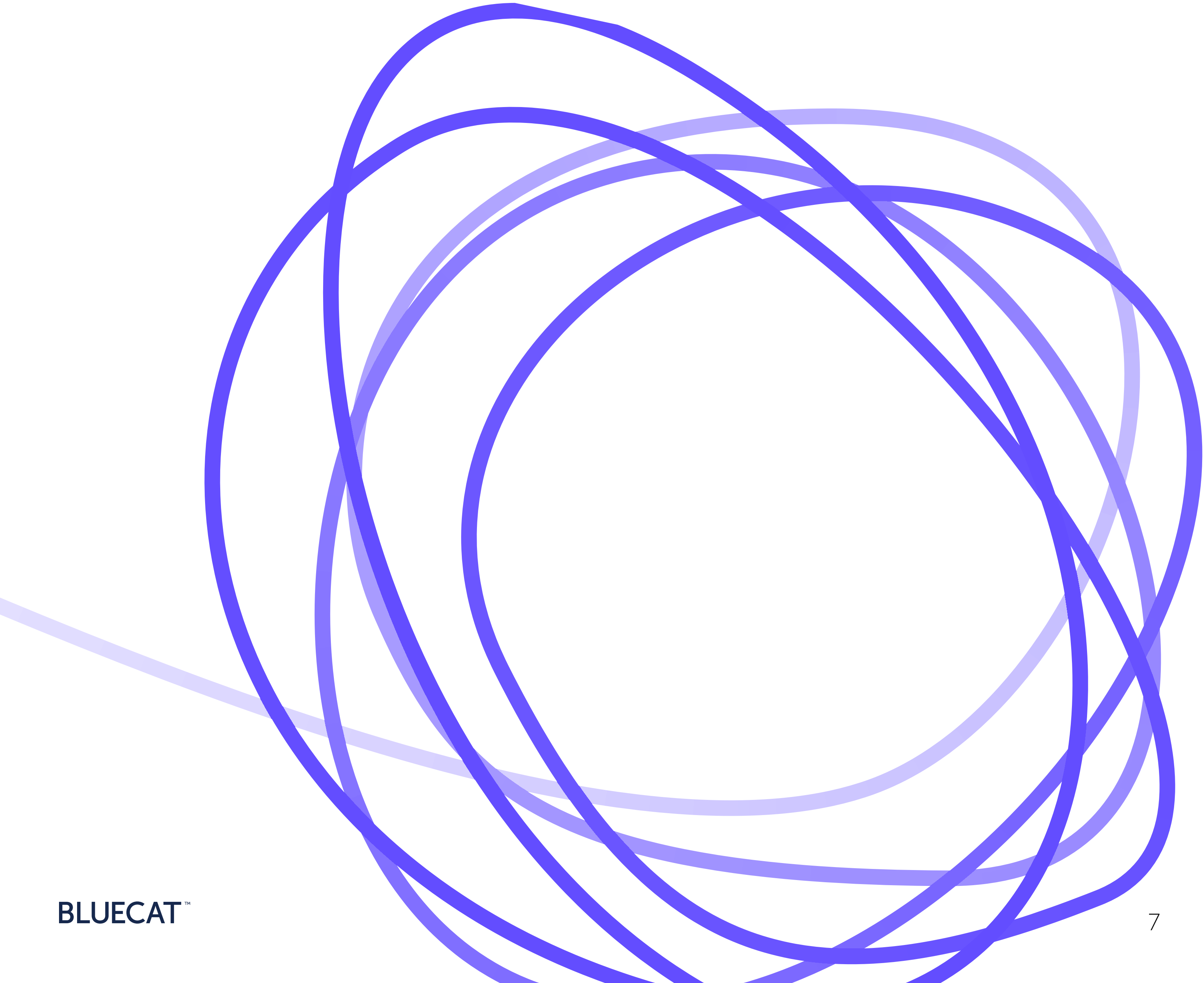
BlueCat Edge effectively solves the problem of having two (or more) different views of the same DNS zone. It acts at the DNS level, allowing clients to resolve across multiple views and enable direct internet access for zones that are not hosted on a corporate DNS infrastructure.


Split Horizon resolution with DNS Edge

When a customer has the same domain name internally and externally, oftentimes ensuring that the proper resolution path is utilized is the biggest challenge.

How BlueCat Edge helps:

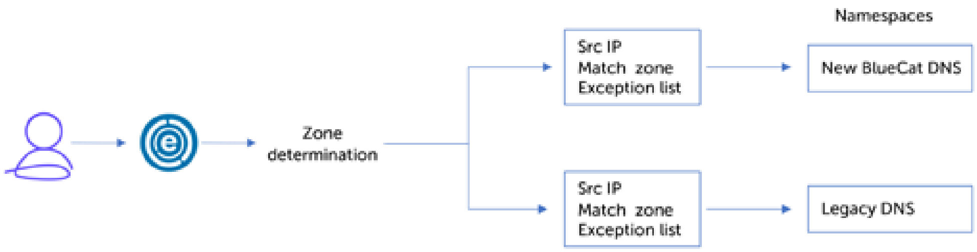
With the use of BlueCat Intelligent Forwarding, you can create two namespaces that reference acme.com – the internal view and external view. Edge provides the ability to continue resolving upon receiving a negative response to ensure that resolution is successful. A query destined for acme.com would have a matching zone indicating that it should be queried in both the internal and external acme.com namespaces, returning the external answer only if there is no internal answer. This capability completely removes the requirement to manage split-view.



Migrations: Mitigating Risk of Outage Due to Misconfiguration or Missing DNS Data

Most migrations are still done via traditional methods, using planned migration cuts to move the data. One of the core concerns of most companies performing any type of migration, DNS being no different, is the risk of an outage. During every migration event (some migrations take upwards of 50 events spanning several years), there is the risk that missing or misconfigured DNS data in the new environment could cause an outage. Mitigating that risk is critical.

Initial state of a Reduced-Risk migration



This is typically the initial state when using BlueCat Edge with a traditional DNS migration

How BlueCat Edge helps:

During this process, BlueCat Edge Intelligent Forwarding can be used to create resilient DNS infrastructure and eliminate the risk of outage due to missing or misconfigured DNS data.

To do this, BlueCat Edge Intelligent Forwarding is configured to query the newly installed BlueCat infrastructure first. If a negative response is received, BlueCat Edge will then query the legacy DNS Server.

Migrations: Stealth Migration for Faster Completion & Reduced Outage Risk

DNS can be migrated with zero downtime to services, however migration projects can be slow, labor-intensive, expensive, and loaded with risk, depending on the state of the current infrastructure, and the tolerance for service disruption. Before most migrations can be completed, a monumental amount of effort is put into cleansing the existing DNS data to ensure that only accurate and relevant DNS data is migrated to the new environment.

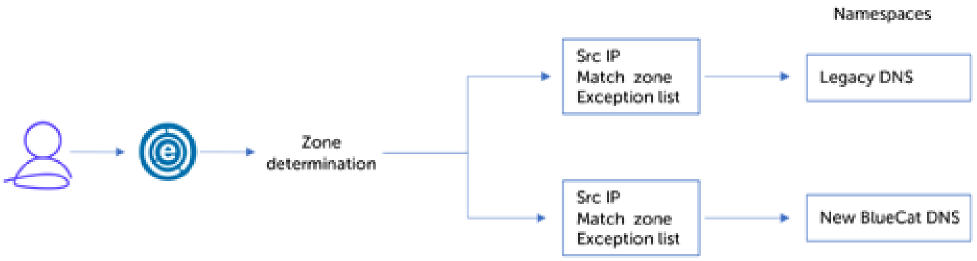
With BlueCat Edge, a quality DNS data migration can be carried out programmatically, passively, and efficiently.

How BlueCat Edge helps:

A Stealth Migration uses the query log from BlueCat Edge to programatically migrate the data as the records are queried. Leveraging namespaces, the records can be migrated on-the-fly, allowing resolution to still occur and removing the need for a traditional cut.

Our first step in the Stealth Migration process is setting up BlueCat Edge to forward DNS queries to the legacy DNS environment. Then, should it receive a negative response, it will query the new BlueCat DNS infrastructure. Records that return from the legacy infrastructure are recreated and copied into the new BlueCat DNS infrastructure.

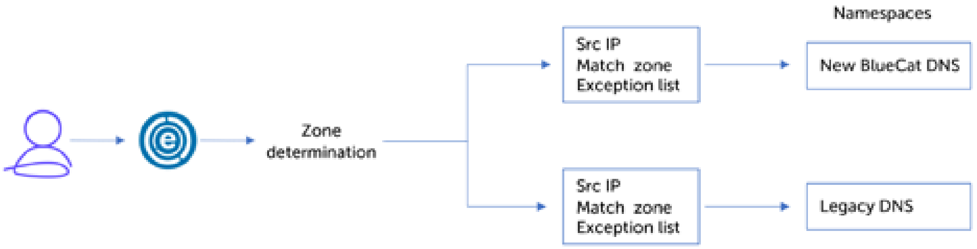
Initial state of a Reduced-Risk migration



This is typically the initial state when using BlueCat Edge with a traditional DNS migration

After a given amount of time the order of the namespaces will be swapped, making the new BlueCat DNS infrastructure the primary for DNS queries. Any query that receives a negative response from BlueCat will then query the legacy DNS infrastructure. Should the query be resolved by the legacy DNS infrastructure, that record will then be recreated in the new BlueCat DNS infrastructure.

Final state of a Reduced-Risk migration



This is typically the final state when using BlueCat Edge with a traditional DNS migration.

Mergers and Acquisitions: Network Integration via DNS

Integrating a merger or acquisition with existing infrastructure, without outages or problems caused by name conflicts, overlapping IP space, and complex forwarding rules, often requires substantial manual intervention.

Using BlueCat Edge ensures that queries from legacy and acquired networks can overcome resolution failures by querying authoritative DNS servers directly. This has the added benefit of improving an IT team's ability to find and correct conflicts in the DNS data. Coupled with the previously described stealth migration process this allows the rapid merging of DNS data while retaining a passive and reduced-risk approach.

How BlueCat Edge helps:

BlueCat Edge is configured using domain lists to point clients to the correct DNS server. BlueCat Edge then uses the stealth DNS migration to ensure that only relevant and accurate data is migrated between the organizations. After the migration process has been completed, the namespace order will be updated to ensure optimal resolution paths.

DNS Query Route Optimization

One of the largest shortcomings of the traditional hub and spoke network design is the need to backhaul all non-local traffic to a core data center. This often causes problems with localization of DNS query responses and can cause potential saturation of already highly utilized and expensive WAN circuits.

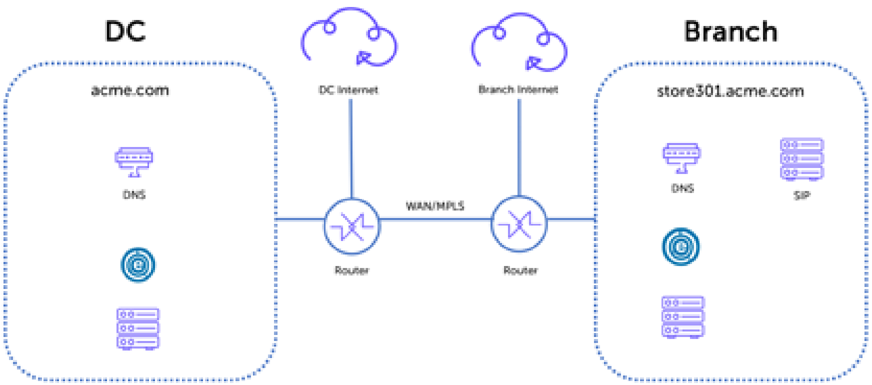
Edge can help optimize the DNS query path, so that customers can purchase smaller routers than they would have with the additional traffic. This, in turn, can reduce infrastructure requirements at branch locations and overall WAN spend. An optimized query path also has the hidden benefits of reducing latency and unblocking end-user access to more localized services.

How BlueCat Edge helps:

Configuring BlueCat Edge with match lists of domains/zones to a namespace ensures that queries are routed in the optimal manner. It also helps prevent localization problems and removes unneeded/unwanted DNS traffic from WAN links.

In the example below, queries from the servers for anything in the store301.acme.com zone would stay local instead of backhauling the traffic to the core data center. Traffic bound for pre-defined, trusted external services such as Office 365 and Google Workspace (formerly G Suite) is routed directly to a local external resolver using the branch's own ISP connection, ensuring better performance, reduced WAN cost, and a more localized DNS response.

Typical configuration with direct internet access



Utilizing BlueCat Edge to provide local breakout to trusted services, while ensuring local resolution occurs properly.

Cloud DNS Integration: Creating a Single Source of Truth

Cloud native DNS is typically managed as an isolated DNS infrastructure. Since it is a separate DNS infrastructure, this prevents customers from achieving their goal of maintaining a single unified DDI solution that represents a single source of truth for their networks. Adopting hybrid cloud almost certainly introduces complex forwarding rules to ensure that DNS resolution continues to function, which results in inefficient routing of network traffic across VPN/dedicated network connections. Customers that move to a Multi-Cloud solution will struggle with complex forwarding rules between the different cloud providers. Moreover, cloud migrations and deployments can lead to DNS resolution and performance issues that cannot be debugged easily without complete visibility.

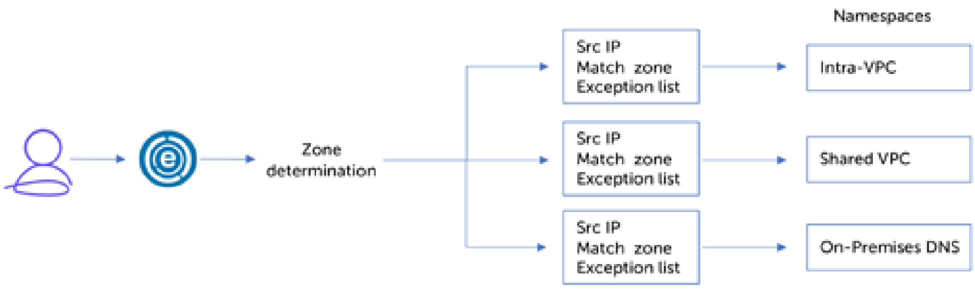
By using BlueCat Edge, customers can ensure that all cloud-centric DNS traffic is routed to a local DNS resolver, which decides on the most appropriate resolver to forward to. This allows the cloud DNS data to be managed alongside on-premises DNS to create a single pane of glass management experience.

Importantly, BlueCat Edge solves issues resulting from the utilization of Private Link services in the major clouds. These services often utilize the same zones across virtual private clouds or VNETs (e.g., privatelink.database.microsoft.net). With the unique capability to resolve across overlapping zones, specific private link records are resolved correctly.

How BlueCat Edge helps:

With BlueCat Edge, customers can configure namespaces in one of two ways. The first method is to configure the namespace using the domain list to include the appropriate domain name for their cloud provider. The second method is to configure the namespaces in a priority order that will look for intra-VPC (Virtual Private Cloud) traffic first, then the shared services VPC, then the on-premises DNS.

Cloud Only setup for Cloud Integrations



This is typically the way that a cloud integration would be configured. Queries would go inside the VPC/VNET, then to a shared services VPC/VNET, then to the on-premises DNS.

All resolution data is available for auditing and debugging purposes, attributed to the source of the query, and with full visibility to latency and other performance data.

Cloud compute is usually broken down into segmented services that are predictable in their utilization of DNS. This provides ample opportunity to segment DNS with simple policy in order to reduce the risk of exploited systems utilizing DNS for command and control, or simply to access remote services.

Proxy Bypass and Direct Internet Access

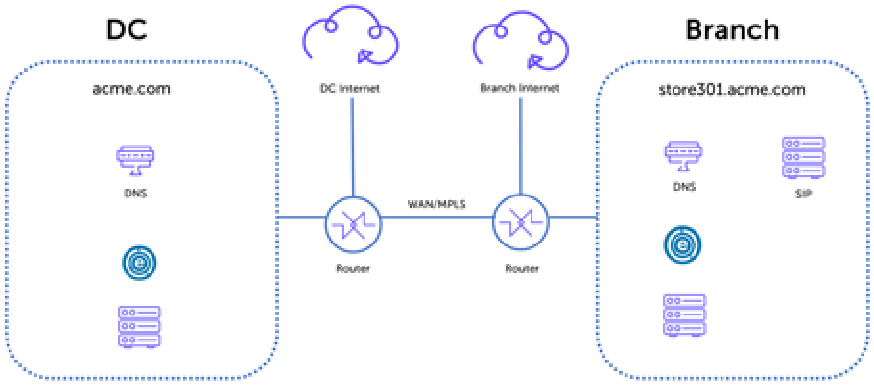
Proxy servers are typically centrally located in core data centers for cost optimization purposes. Thus, internet-bound traffic is forced to route to central locations, which can often cause problems with inaccurate service localization, high latency, and a poor user experience. The centralization of proxy servers further complicates local internet breakout at remote and branch offices.

By using BlueCat Edge, customers can ensure that clients can resolve all queries, both internal and external, while enabling local breakout for direct internet access for trusted services and maintaining the control and oversight needed by security teams to ensure that they maintain a proper security posture.

How BlueCat Edge helps:

With the use of BlueCat Edge namespaces customers can configure DNS traffic to query an internal (acme.com) resolver, external (acme.com) resolver, or an internet-based resolver based on the targeted domain name. BlueCat Edge is deployed in the remote/branch offices to provide local breakout.

Proxy Bypass with Direct Internet Access



Typical configuration for Proxy bypass with Direct Internet access from a remote branch.

Securing Internet of Things and Purpose-Built Devices

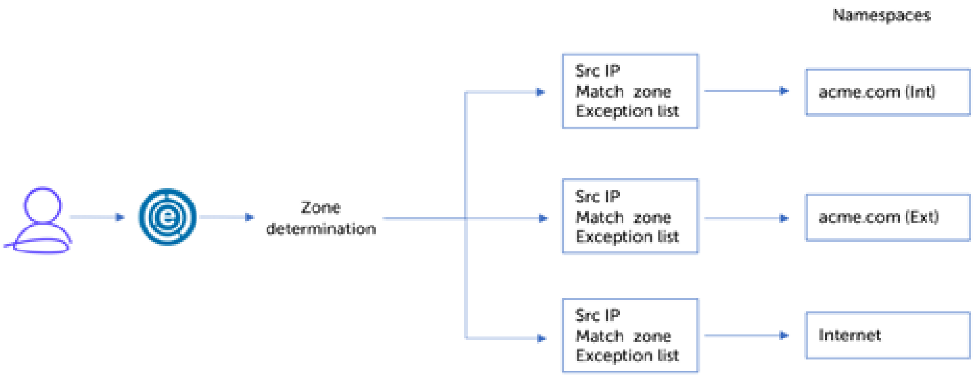
Internet of Things (IoT) devices are often targeted by hackers since infrequent updates or completely lacking security patches make them vulnerable to easy attacks. While IoT devices are largely serviced like any other node on the network, the nature of these devices often leads to a lack of monitoring of their activity. This, combined with the fact that many have unfettered access to DNS data, makes them a lucrative target.

Thus BlueCat believes that IoT devices should be tightly controlled on a corporate network. Using BlueCat Edge, DNS access by IoT devices can be restricted to specific pre-approved records, and effective security policies can be applied to these devices even when traditional controls such as security agents may not be available.

How BlueCat Edge helps:

Using BlueCat Edge, customers implement specific DNS configurations and security policies to centrally manage these devices. DNS policies are applied to permit only predefined internal and external services to be accessed. With the use of namespaces you can also specify which devices the IoT devices are permitted to query.

Securing DNS for IoT Devices



IoT devices only permitted to use certain secure DNS servers. Anything else is blocked.

Augmenting Cisco Umbrella with Visibility Into Source IP of Queries

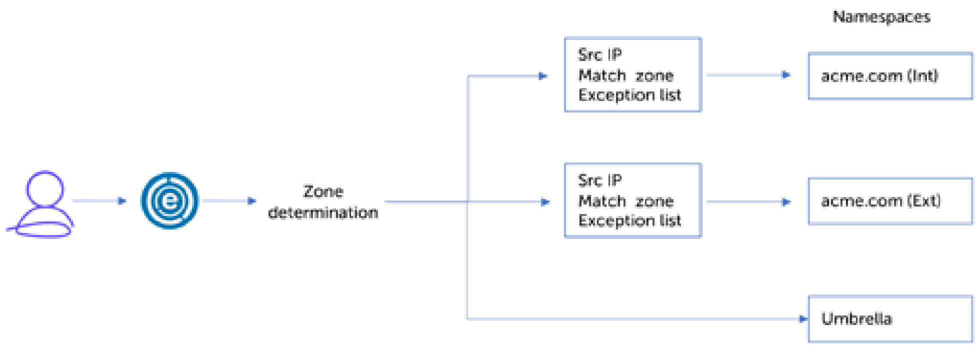
Cisco Umbrella provides cloud based resolvers to identify and block queries associated with specific threats. One of the drawbacks to this solution is that all the DNS requests must recurse through internal DNS servers before reaching the Cisco Umbrella external recursive system. Because of this, Cisco Umbrella loses the source IP of the client performing the queries, leading to blind spots on the internal network.

BlueCat exclusively partners with Cisco Umbrella for external-facing DNS threat protection. With the inclusion of BlueCat Edge in an overall DNS solution, customers gain full internal visibility to complement the external visibility provided by Cisco Umbrella. All outbound client traffic is directly routed to Cisco Umbrella for filtering and resolution, while BlueCat supplies the supplemental information to show what the internal source of the query was when a block has occurred.

How BlueCat Edge helps:

To correct this, BlueCat Edge is configured with namespaces to route all internal traffic to local DNS resolvers. All DNS requests destined for external destinations are forwarded to Umbrella directly, preserving the client's IP address through the use of the EDNS (Extension Mechanisms for DNS) Client Subnet (ECS) data flag, where we augment the Cisco Umbrella solution with the client source IP via EDNS.

BlueCat Edge configuration with Cisco Umbrella Integration



This is the configuration that is used when having the same domain internally and externally. If the query is destined to the internet it is then forwarded to Cisco Umbrella

Conclusion

BlueCat Edge addresses use cases that could cause more traditional DNS solutions to flounder. It was specifically designed to fill the gap between the enterprise and cloud, providing security and policy enforcement, forwarding DNS traffic, and streaming it into the cloud while providing visibility into its activities through its cloud-based management layer.

Whether the challenge is a DNS migration that needs to be bulletproof and outage-free, a corporate merger or acquisition that needs integration of two or more environments, or a cloud integration to produce a single source of DNS truth, BlueCat Edge eliminates risk and speeds what can be tedious and error-prone processes. In branch offices, it optimizes query routing to cut costs and minimize latency.

Overarching everything is security. BlueCat Edge provides visibility into the source IP for queries, and protects IoT devices and the networks they're connected to by applying restrictive DNS configurations and policies designed to prevent their use by attackers.

You’ve probably got a lot of questions about how it all works.

You’re in luck.

We’ve got all the technical detail you need right here.

Learn more about BlueCat’s solutions

bluecatnetworks.com