BlueCat DNS Edge

Solution Brief

Table of Contents

Introduction

As organizations undergoing major digital transformation with respect to cloud, automation, and security, a core functionality involved that is often overlooked is the Domain Name System, more commonly referred to as DNS. Having an effective DNS infrastructure with visibility and control can help your organization reduce costs, stop cyberattacks, and increase efficiency.

BlueCat DNS Edge™ (Edge) is a new approach to enterprise security that utilizes the pervasive nature of a customer's DNS infrastructure to gain enterprise-wide visibility into the intent of every device on a network. Using that visibility, Edge provides real-time insight into threats within an environment and assesses the risk of an intended action by leveraging the context that DNS provides. Edge enables control, making it easy for customers to define and deploy granular security policies on all devices—managed or unmanaged, and control DNS resolution paths with designated namespaces.

In the world of DNS, the IP address of the client executing the DNS query is often lost in the chain of recursion. Because of the hierarchical nature of DNS, it is very common for a caching DNS server to have to forward a DNS request (query) through several DNS servers before the authoritative DNS server is identified and returns a query response. At each hop in this recursion process the IP address of the querying endpoint is replaced with the IP address of the most recent DNS server being queried. In other words, once the request passes the caching DNS server the client IP address is lost and the IP address of the caching server is used for the next hop.

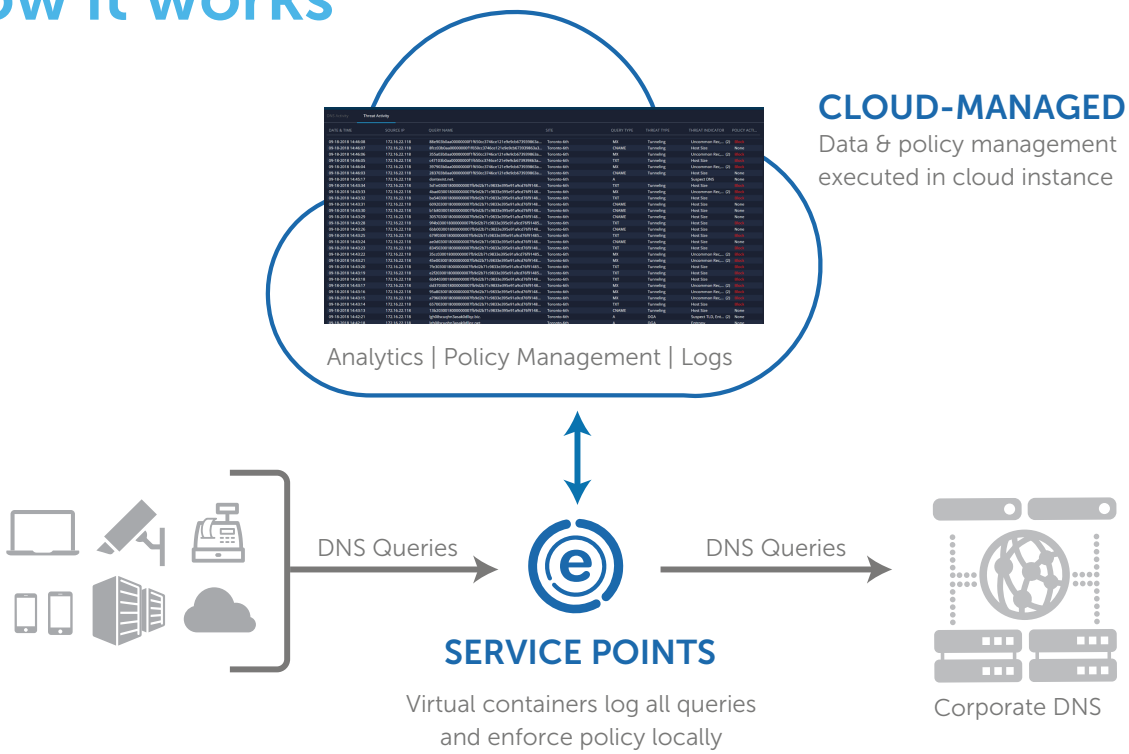
From a cybersecurity standpoint this is problematic since one of the most important pieces of information required for an investigation is the source IP. Without this data point, the security team will need to use other systems or correlated events to uncover the source.

Edge sits between a network endpoint such as a client, server, IoT device, etc. and the upstream DNS server, making it the first hop from the endpoint device. This unique position in the infrastructure gains visibility and provides control at the first hop before the initial DNS server and always has visibility into the source client IP through to the query response, providing both "sides" of the conversation.

What is BlueCat DNS Edge

Edge is a SaaS solution that includes a DNS caching layer between your client devices and upstream DNS infrastructure, which provides visibility and control of your DNS traffic while acting as a client-facing DNS policy enforcer. It resolves queries from client devices by forwarding them to your DNS servers and logs the complete query and response along with source IP of the requesting client in a web-based cloud console. In addition, you can apply granular policy actions to block, redirect or monitor DNS queries as per corporate or regulatory policies as well as identify threats such as tunneling, domain generating algorithms (DGA) and more.

How it works



Edge consists of 2 main components, a cloud instance (CI) and service points (SP). The CI is a Cloud-hosted management console to create sites, set policies, view DNS logs, and set resolution paths with designated namespaces, while additionally providing numerous analytical insights to identify DNS-based anomalies and threats. All changes made in the CI are then pulled down into the SP during its next check-in. Service Points check into the CI every few seconds to push query logs into the CI as well as pull down new config data, policy settings, namespaces, etc.

Service points act as a DNS caching layer between client devices and your existing DNS servers that enforce policies, determine or guide resolution path, and log queries for visibility and detection of threats. Service Points can be installed in your networks as virtual machines on-premises, or in your cloud environments (AWS and Azure).

When an endpoint makes a DNS query, the first hop is to the Service Point which then checks to see if there is a policy action for that query. If there is none, it forwards the query to its upstream DNS server for resolution. When the SP receives a response, it checks the policy again to see if there are any policy actions to apply now that the answer to the query is known. The response is returned to the client if allowed by policy while the SP logs the source IP of the client device, initial query, query response along with other DNS data which is then fed into the CI. If a policy action such as block, redirect, or monitor is triggered then the appropriate action is taken before returning a response to the client device.

Additionally, queries logged are checked against various threat indicators and algorithms to flag potential threats that may not be flagged by corporate policies, such as suspicious or malicious DNS activity like DGA, and tunneling.

Sample Data Flow (Browser-based DNS Lookup):

1. User types in the resource request in the web browser, such as https://hr.example.com
2. The endpoint then initiates a DNS query to the SP to request the IP address of hr.example.com
3. The SP takes in the query and performs below actions in the following sequence:
    a. The query is compared against policies stored to determine if any action should be taken based on those policies, such as block the query, redirect it, or simply monitor it for closer review.
    b. If a block is defined then the query is not resolved and a NXDOMAIN response is sent back to the client.
    c. If no block, or redirect is defined then the SP checks its local cache to see if the IP address has already been cached.
    d. Assuming the caching server does not have the IP address, the query is forwarded to a recursive DNS server for resolution.
    e. The recursive DNS server will follow standard DNS processes to identify the appropriate authoritative DNS server for hr.example.com and identify the IP address of that resource.
    f. The response is then once again checked against all applicable policies, and if not affected by a block policy, sent to the client device while the client source IP, query request and response is then all logged in the CI along with other DNS data.
4. All relevant information about the query is then viewable in the cloud instance (CI), along with all insights derived by various analytics within the Edge platform.

Edge Architecture

Edge is a cloud-managed, Software as a Service (SaaS) solution that has been designed to allow for fast and simple integration to existing infrastructure and processes. The architecture of the solution was chosen with several key objectives in mind:

Agentless Deployment: Edge provides visibility, control and detection to protect any device that leverages DNS without the need to deploy an agent or client on those devices. This is particularly important when dealing with non-traditional IoT devices like wireless security cameras, point-of-sale systems, ATMs, smart-sensors, etc. These devices are difficult to manage with traditional capabilities and have been targeted and manipulated extensively to launch attacks against IT infrastructures, data and services.

Operational Simplicity: Edge is built to integrate with existing tools and processes so that adoption of the solution does not require extensive training or re-architecting of a customer's current practices. Configuration and policy definitions can be set in the cloud instance (CI) which is then sent down to a Service Point (SP). Important DNS event information triggered by policies can be sent to an existing SIEM via simple API-based integration.

Scalability & Availability: Edge, built on a resilient enterprise cloud infrastructure, will dynamically scale to meet any collection, storage and processing requirements without interruption. The underlying cloud infrastructure allows for local high availability as well as geographic failover to ensure availability during local or regional disasters.

a) Cloud Instance (CI)

The cloud instance (CI) is where clients can access their query logs, set policy and configure their Edge deployment. The CI provides the main dashboard where users can configure policy actions, DNS resolution paths, monitor and view DNS activity, as well as detect malicious DNS behavior like tunneling, DGA, etc. Managed resources within the cloud instance are deployed in three different availability zones to ensure high availability of services. Archived data as well as data in transit is encrypted via AES-256 and SSL.

b) Service Points (SP)

Service Points (SP) are the main control mechanism that forms the DNS caching layer in Edge. SPs are containerized, purpose-built software instances that are installed on-premises or into your public or private cloud and become the first hop between client devices, servers, etc. and an organization's DNS infrastructure.

SPs are tied logically to an entity called a Site within Edge, which means any policy action or DNS resolution path that's applied to a Site is enforced by the SP tied to that particular Site. Sites can be

defined by geographical boundaries, business functions or any logical grouping that requires client devices that have similar behavior.

SPs retrieve configuration and policy information from the CI by making RESTful calls over HTTPS to the CI. SPs are designed as light-weight software instances that provide policy enforcement, intelligent DNS resolution path navigation, DNS resolution via forwarding, and DNS logging by sending all DNS events to the CI.

c) APIs

Edge is designed to be API driven if desired—all actions performed in the Edge user interface (UI) can be orchestrated through APIs. We utilize a short-lived token which is provided upon login and can be used to call our APIs securely through HTTPS.

d) Securing your data

Data in each CI for a customer is stored in a separate Edge cloud account with no direct access by any entity outside of BlueCat's master Service Operations instance which also resides in the same cloud environment. Only BlueCat employees with a specific need have access to the CI backend on an as-needed basis to maintain the system.

Data in transit between the SP and CI is encrypted with SSL. Archived DNS activity log data is stored in customer-specific Edge cloud storage and encrypted via AES-256.

Features

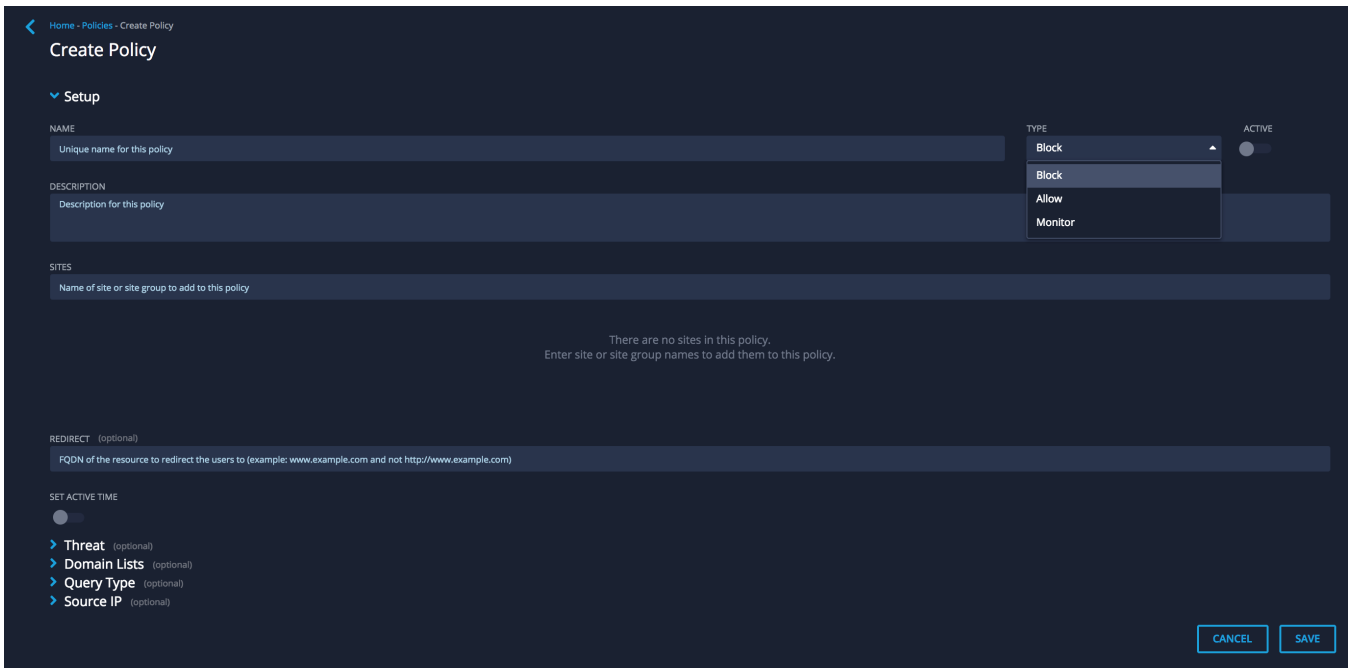
a) Policies

Service points can be configured to enforce policies on DNS traffic from client devices or to services within an organization. Edge allows operators to configure 3 different kinds of policies and are evaluated on the service point in the following order – Block, Redirect and Monitor. Policies can be set to be active during certain time windows or indefinitely.

Block policies can be used to block endpoint devices from querying bad domains based on corporate / regulatory policies or based on threat intelligence or threat indicators. A block policy can be configured through the policy page in the Edge CI.

Redirect policies can be used to redirect users trying to access a restricted resource. Many organizations will leverage a warning page that instructs their users to contact their IT department for further action or to serve as an alert when visiting a blocked domain.

Monitor policies allow users to flag traffic within their environment and can be defined based on domain lists, threat types or source IPs.



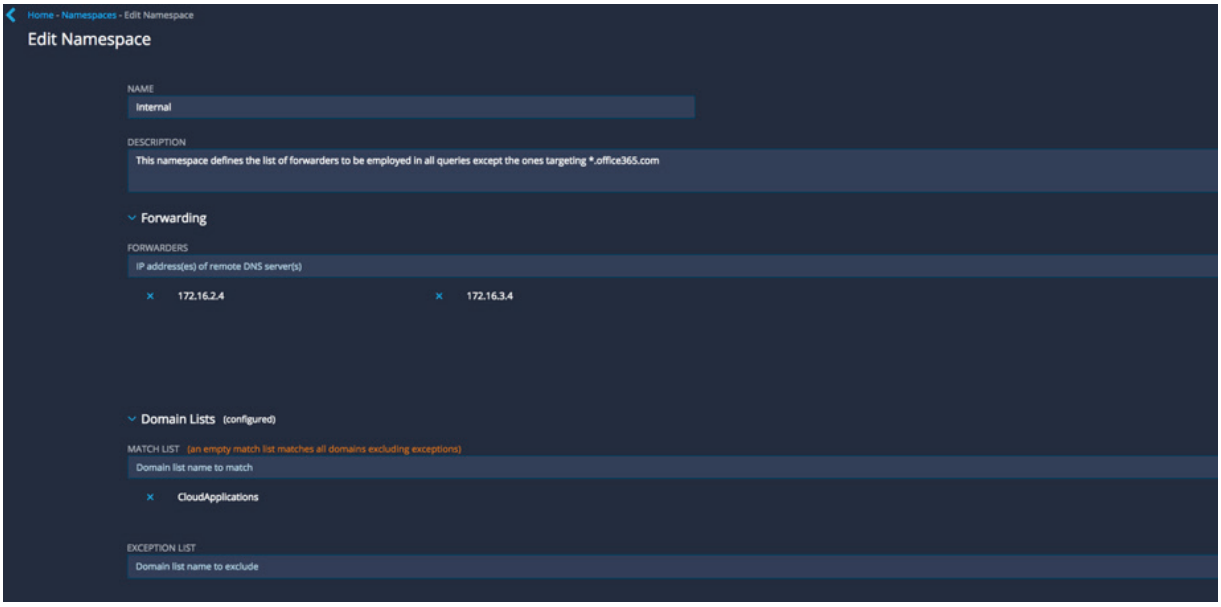
b) Namespaces

A DNS Namespace represents a mapping of domain names to DNS information. In this context, each Namespace represents a different set of authoritative Domain Name System (DNS) servers. An example Namespace use-case, could be an organization with its corporate services reachable both internally and externally (to support remote workers, partners, etc). In this case, records for the same server reside both internally and externally. This can lead to confusion and error when trying to maintain manually. By utilizing Edge, externally accessible records can be maintained on the external authoritative server only, yet resolved for internal clients using Edge's unique ability to query the external server if the internal does not return a result.

In BIND, the same concept of a separate Namespace is referred to as a DNS view, but the functionality provided by BIND views is different. BIND will only answer a given query from a single view, but Edge can look in multiple Namespaces when answering a single query. Where views configured on BIND provide the ability to present different Namespaces to different clients, in Edge, Namespaces represent the views provided to Edge by the DNS servers that Edge forwards to.

A Namespace is configured with a (non-empty) default group of Forwarder servers to be employed in the resolution of that Namespace, and optionally, a set of Domain Lists that limit the domain namespace this Namespace will resolve:

- If no Domain Lists are configured as Match Lists to the Namespace, then all queries are eligible to be resolved employing the Namespace's defined Forwarders.
- If Domain Lists are attached as Exception Lists, then the queries targeting the domains in these lists will not be forwarded to the Namespace's defined Forwarders.
- If one or more Domain Lists are configured as Match Lists, then the Namespace will apply to all queries targeting the domains in these lists, with the exception of the queries matching the domains in the Exception Lists (if any defined).



All of the Service Points associated with a Site receive the Namespace configuration as part of a scheduled cycle and use the Namespaces in the order that they are set for query resolution.

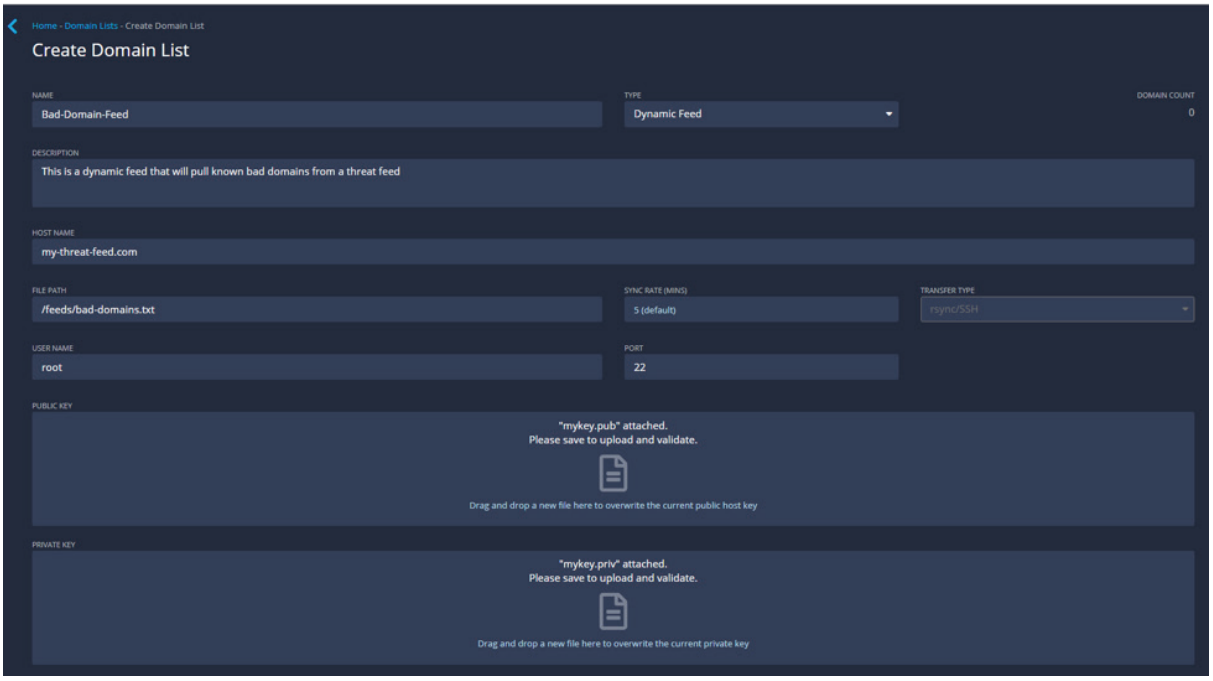
Resolution follows these rules:

1. When more than one Namespace is configured for a site, the Service Point attempts resolution against all matching Namespaces in the order they are defined, until a response other than NXDOMAIN is returned. When any response other than NXDOMAIN is returned, no further namespaces are evaluated.
2. If the currently employed Namespace returns NXDOMAIN, continue with the next Namespace.
3. If all of the Namespaces are evaluated and none return a non-NXDOMAIN response, the last Namespace's NXDOMAIN is returned. If the query cycles through all of the selected Namespaces and no match is found because the query doesn't match the Match Domain List(s) on any Namespace, or is included in an Exception List, then an intentional NXDOMAIN response is returned.

c) Threat Feeds

Edge supports the ability to pull domains from a threat feed into what's known as a "Dynamic Feed Domain List". This allows Edge operators to ingest a constant feed of malicious/suspicious domains from a source of their choosing. Supported protocols available to pull from a threat feed are "rsync" over "ssh".

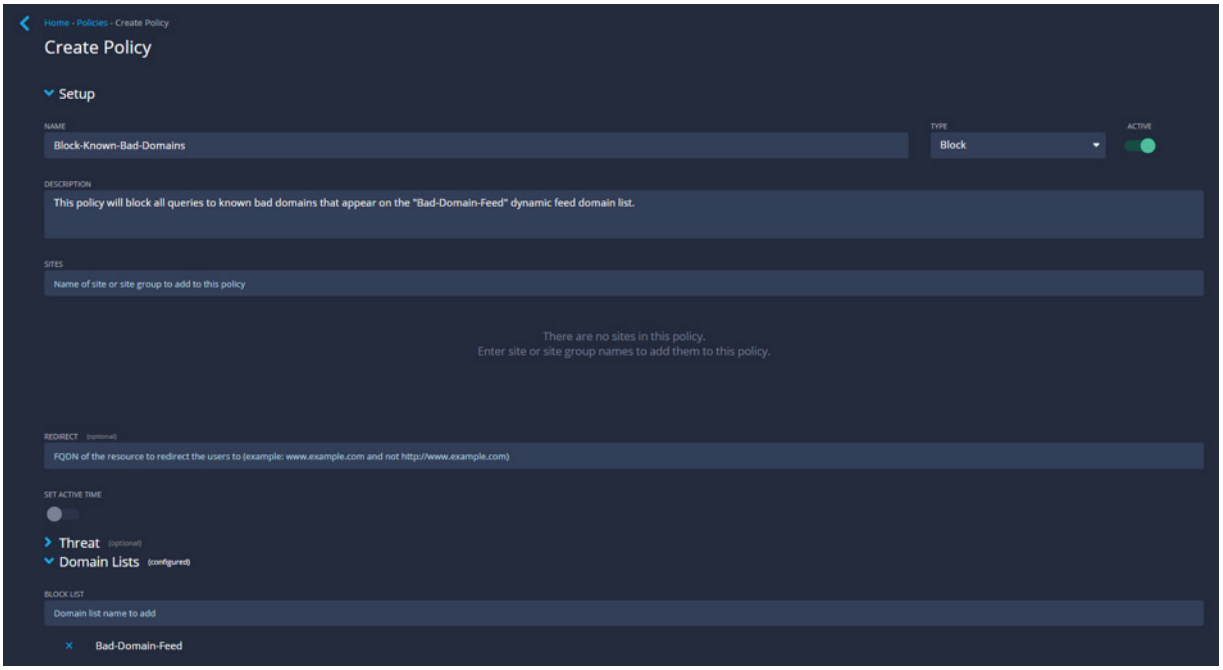
Below is a sample of the configuration parameters required to setup a Dynamic Threat Feed.

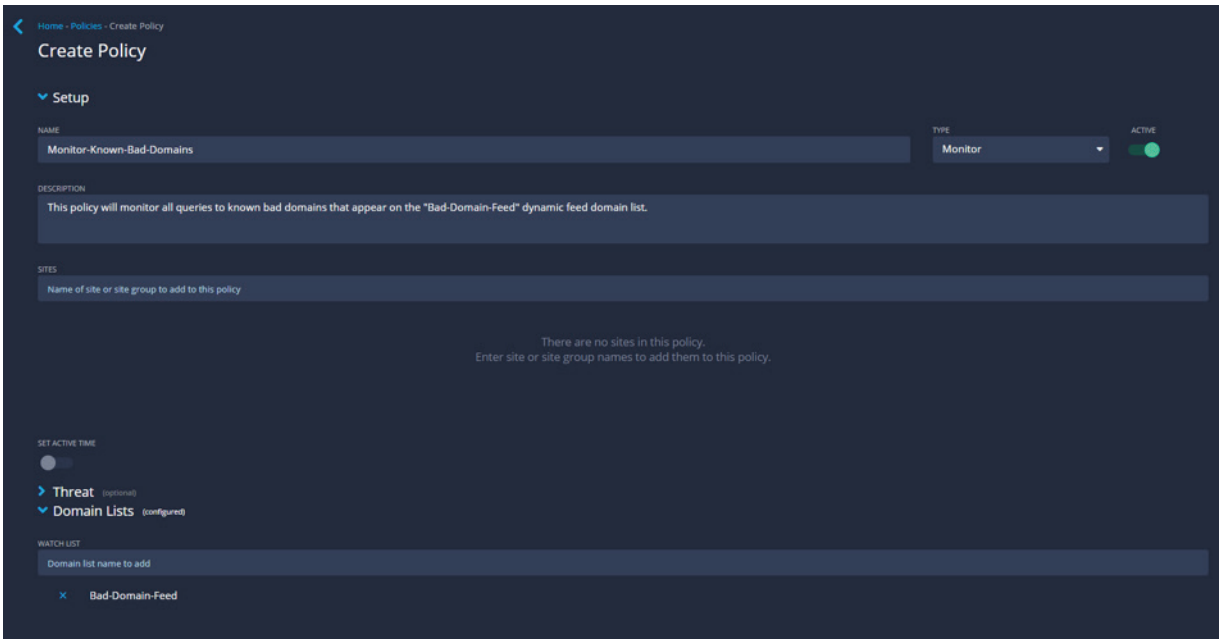


Blocking/Monitoring Queries to Domains in Threat Feed

To act on domains ingested into a Dynamic Feed Domain List, an Edge operator can set up an Edge Block Policy to mitigate attacks involving those domains, or setup a Monitor Policy to flag domains for closer review.

Below are examples of how you might configure policies to Block/Monitor domains in a dynamic feed domain list.





BlueCat also provides a threat intelligence feed source called BlueCat Threat Protection as an add-on which provides a list of known-bad domains including feeds from security partners.

d) Anycast

Service Points can be configured to participate in an Anycast setup, operating with either Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF) protocols. Organizations using Anycast are afforded optimized response latency and improved service availability.

When a client device sends a query to the Anycast IP, the routing infrastructure will route the DNS query to the topologically closest Service Point based on the Anycast parameters configured, therefore achieving lowest latency.

"Topologically" does not mean geographically, but denotes the SP attached to the route with the best/lowest cost path as configured by the network administrator via the routing protocol(s) in use.

While lower latency is a primary benefit of Anycast, we also gain service resiliency and higher availability. If a Service Point goes down, it will stop advertising itself as a member of the Anycast pool, routers will age out the route to this server point from their routing table and route the DNS queries to the other Service Points.

Threat Indicators

Edge has built-in analytics to detect suspicious or malicious DNS-based patterns of behavior by flagging DNS queries that match a "threat indicator". Some threat indicators in Edge are also mapped to threat types such as DGA, and Tunneling.

There are 5 different types of threat indicators in Edge:

1. **entropy** – The entropy threat indicator flags on domains that are suspected to be generated by a domain generation algorithm (DGA). DGAs are used by malicious actors in their malware to generate large numbers of domain names which can be used to reach its point of command. queries in Edge that match the entropy threat indicator are mapped to the "DGA" threat type.

2. **uniqueChar** – The uniqueChar threat indicator flags on domains that have higher than usual occurrences of unique characters in the host name. This type of activity can be indicative of arbitrary data being encoded in DNS queries, also known as "DNS tunneling". Queries in Edge that match the uniqueChar threat indicator are mapped to the "Tunneling" threat type.

3. **uncommonRec** – The uncommonRec threat indicator flags DNS queries that are not commonly seen on a network, such as MX or APL queries. These can also be indicative of DNS tunneling happening on your network. Queries in Edge that match the uncommonRec threat indicator are mapped to the "Tunneling" threat type.

4. **hostSize** – The hostSize threat indicator flags DNS queries with an abnormally large amount of characters (70 or more) in the host name. This is also an indicator of DNS tunneling. Queries in Edge that match the hostSize threat indicator are mapped to the "Tunneling" threat type.

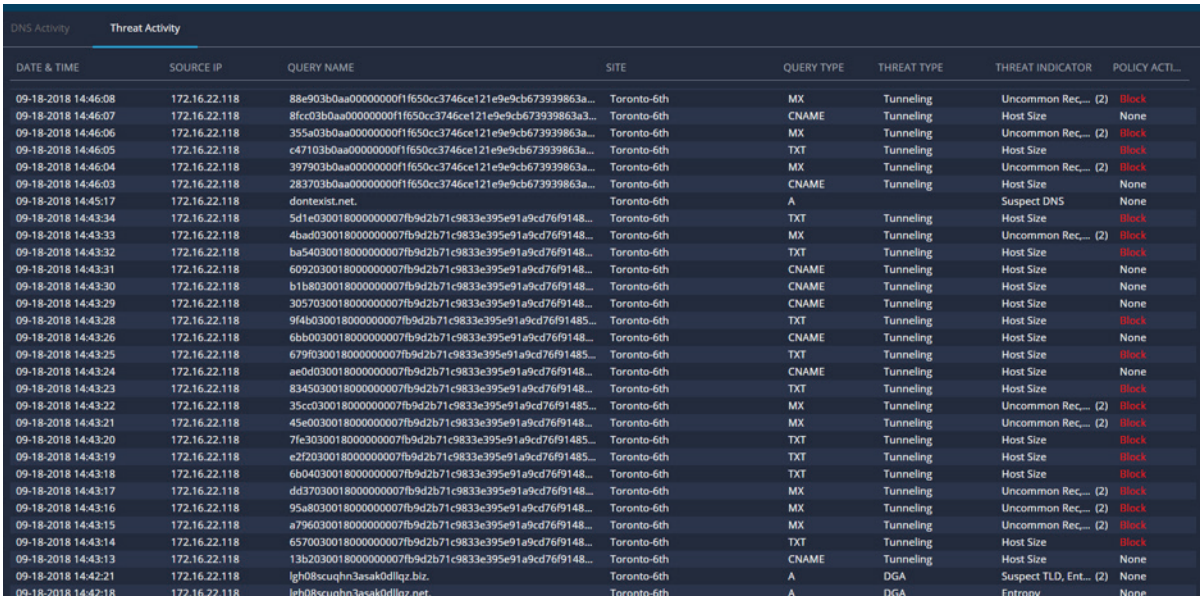
5. **volTunnel** – The volTunnel threat indicator flags queries to multiple unique subdomains (75 or more) of the same parent domain in an abnormally short amount of time (one hour). This is a common indication of DNS tunneling. Queries in Edge that match the volTunnel threat indicator are mapped to the "Tunneling" threat type.

There are also 2 additional types of threat indicators:

1. **Suspect TLD** – The Suspect TLD threat indicator will flag queries that have top-level-domains (TLDs) that known to be subject to abuse by malicious actors such as the ".biz" TLD.

2. **Suspect DNS** – The Suspect DNS threat indicator will flag queries to domains owned by commonly abused dynamic DNS providers such.

Using the "Threat Activity" tab in Edge, operators can view which queries are matching on threat indicators.

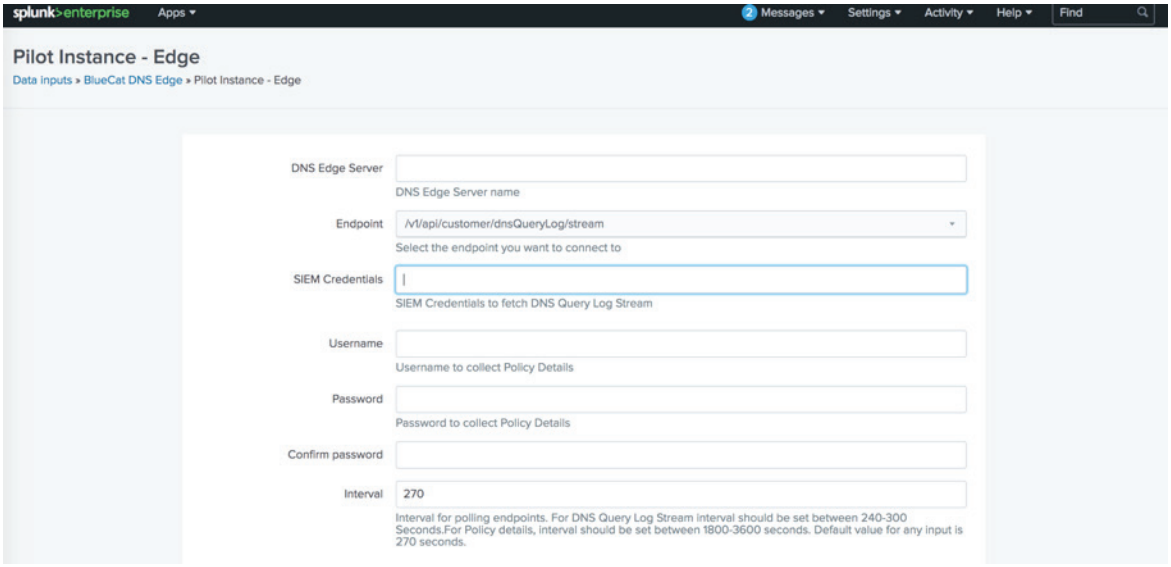


Integrations

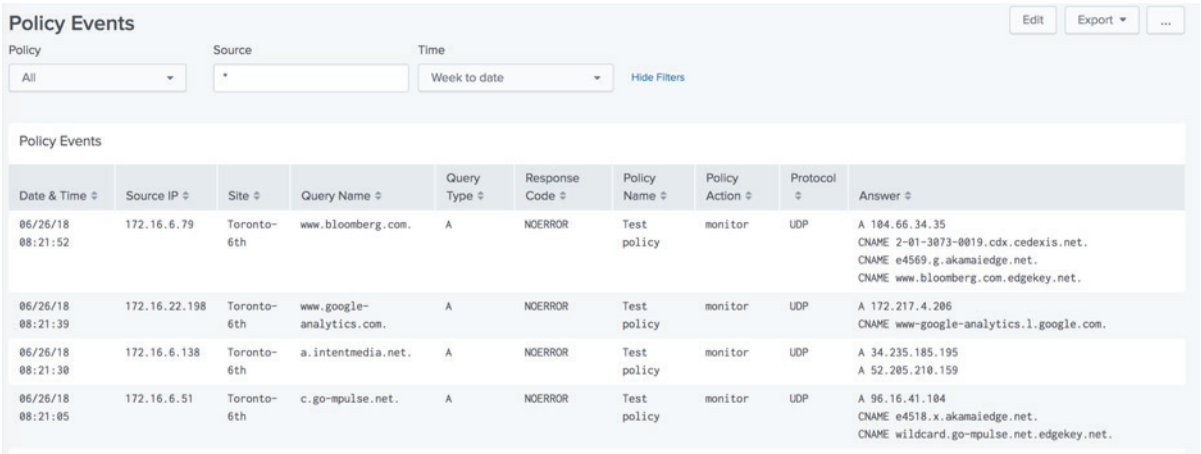
Edge is built with an open ecosystem in mind and the architecture is designed such that all functionality in the CI to configure, analyze or control the SPs is built using RESTful APIs.

Splunk

Edge has a direct integration with Splunk via an app on the Splunk marketplace. This integration allows you to send policy-triggered DNS events to your Splunk instance. Instructions on how to install the Edge add-ons for Splunk can be found in the /help section within Edge as well as the deployment guide. To configure the integration's data input module, you will need the SIEM API key that was furnished to the super admin user when the Edge CI was initially created.



The Edge Splunk app provides all the details of the DNS query and response as well as the policy applied within the Splunk interface. Having DNS event information within your SIEM provides added context from a DNS perspective during an investigation.



Conclusion

The visibility and control that BlueCat DNS Edge provides, along with its ubiquitous nature and key position within an organization's infrastructure make it a natural point of both inspection and control for both networking and cybersecurity teams. Edge has been designed and built to unlock the value of DNS in an efficient, effective platform.

About BlueCat

BlueCat is the Enterprise DNS Company™. The largest global enterprises trust BlueCat to provide the foundation for digital transformation strategies such as cloud migration, virtualization and cybersecurity. Our Enterprise DNS platform improves control and compliance across entire networks, enabling organizations to centralize and automate DNS services for security and operational efficiency. For more information, please visit www.bluecatnetworks.com.

20181029-003