FQDN and URL Filtering Categories

FQDN / URL Filtering Categories

Multicloud Defense uses threat intelligence from WebRootTM BrightCloud (www.brightcloud.com) to categorize web sites based on their risk score. This includes fully qualified domain names (FQDNs), sometimes referred to as domain names, and URLs. This provides sites across 84 categories when traffic from your public cloud environment makes outbound connections (egress) to these sites:

- FQDNs (domains) - 1+ billion categorized FQDNs (domains)
- URLs - 45+ billion categorized URLs

To improve efficiency in recognizing and processing traffic, The gateway will pre-load a cache of the top 1 million FQDNs/URLs and their categories. The gateway will also utilize a runtime cache of 10k FQDNs/URLs and their Categories that are not part of the top 1 million. If traffic contains any of the cached FQDNs/URLs, then the categories will be known immediately. If the FQDN/URL is not found in the cache, the gateway will query the Controller to resolve the category via BrightCloud. This operation is expected to complete in no more than 200ms. If it completes within the expected time, then the traffic will be processed based on the learned category and the profile will operate on the traffic based on the policy defined for the category. If the operation does not complete within the expected time, then the traffic will be processed as Uncategorized and the profile will operate on the traffic based on the policy defined for Uncategorized. Once the resolution returns, the learned category will be added to the cache for subsequent resolutions, even if the resolution occurs for the available the expected time and the traffic has already been processed. If the run-time cache is exhausted, the gateway will purge the oldest accessed FQDNs/URLs and their categories in batches of 10 entries to ensure space is available for more recently accessed FQDNs/URLs and their categories.

Note FQDN filtering with categories happens for:

1. SNI in TLS client hello
2. DNS queries for FQDN lookups
3. HTTP hostname header (for cleartext HTTP traffic)

Malicious Categories

Multicloud Defense considers the following categories to be particularly malicious:

Table 1: Malicious Categories Multicloud Defense considers the following categories to be particularly malicious

Category Name	Category Description
Malware Sites	Siteshosting malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code.
Phishingand Other Frauds	Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personalinformation from a user. These sites are typically quite short-lived, so they don't last long in terms of uptime.
Proxy Avoidance and Anonymizers	Proxyservers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering.
Keyloggers and Monitoring	Softwareagents that track a user's keystrokes or monitor their web surfing habits. Often used for collecting sensitive data such as usernames and passwords.
SPAM URLs	Sites known to distribute unsolicited email (spam) messages.
Spywareand Adware	Spywareor Adware sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or the organization, also unsolicited advertising popups and programs that may be installed on a user's computer.
Bot Nets	These are URLs, often IP addresses, which are determined to be part of a Bot network, fromwhich network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.

Multicloud Defense offers traffic analysis when viewing traffic via **Discover** > **Traffic** > **DNS** and **Investigate** > **Flow Analytics** > **Traffic Summary**, where a pre-defined *Malicious Categories* filter can be selected to show instances and VPCs communicating with these Malicious Category FQDNs and URLs.

The full list of categories is shown below.

Full List of Categories

Category Name	Category Name	Category Name	Category Name
Abortion	Games	Motor Vehicles	Sex Education
Abused Drugs	Government	Music	Shareware and Freeware
Adult and Pornography	Gross	News and Media	Shopping
Alcohol and Tobacco	Hacking	Nudity	Social Networking
Auctions	Hate and Racism	Online Greeting Cards	Society
Bot Nets	Health and Medicine	Open HTTP Proxies	SPAM URLs
Business and Economy	Home and Garden	Parked Domains	Sports
Cheating	Hunting and Fishing	Pay to Surf	Spyware and Adware
Computer and Internet Info	Illegal	Peer to Peer	Streaming Media
Computer and Internet Security	Image and Video Search	Personal sites and Blogs	Swimsuits and Intimate Apparel
Confirmed SPAM Sources	Individual Stock Advice and Tools	Personal Storage	Training and Tools
Content Delivery Networks	Internet Communications	Philosophy and Political Advocacy	Translation
Cult and Occult	Internet Portals	Phishing and Other Frauds	Travel
Dating	Job Search	Private IP Addresses	Uncategorized
Dead Sites	Keyloggers and Monitoring	Proxy Avoidance and Anonymizers	Unconfirmed SPAM Sources
Dynamically Generated Content	Kids	Questionable	Violence
Educational Institutions	Legal	Real Estate	Weapons
Entertainment and Arts	Local Information	Recreation and Hobbies	Web Advertisements
Fashion and Beauty	Malware Sites	Reference and Research	Web Hosting
Financial Services	Marijuana	Religion	Web-based Email
Gambling	Military Search Engines	Services	

Associating a Filtering Profile with a Policy Ruleset Rule

- Refer to FQDN Filtering to create/edit FQDN Filtering Profiles
- Refer to URL Filtering to create/edit URL Filtering Profiles

BrightCloud URL / IP Lookup Tool

BrightCloud offers an online URL / IP Lookup Tool (https://www.brightcloud.com/tools/url-ip-lookup.php) that can be used to understand what category a particular FQDN / URL is classified as along with its Web Reputation.