Quad9 Guidance for Internet Service Providers

Introduction

Quad9 is a free, open recursive DNS anycast resolver with over 124 POPs globally at IntereXchange points (IX) and other locations. Quad9 provides end users a DNS filtering service which blocks criminal sites such as malware distribution locations, phishing destinations, botnet command and control, and other systems which are harmful to end users and network elements. While providing security, Quad9 also has a dedication to end user privacy and neither stores nor transmits any personally identifiable information (PII). It has been designed with GDPR compliance as a baseline goal.

The list of blocked domains is created/selected from a set of 19 (as of Quarter 2, 2018) threat intelligence (TI) providers, both in the commercial and open community. Quad9 works in cooperation with these TI providers to feed back the effectiveness of blocked domains for continual improvement of the security protection.

The service is provided at no cost, and there is no commercial “upsell”. The organization is not-for-profit, and collects no marketing or demographic data for support of commercial or other services. There is an option for ISPs to acquire on-premise equipment for higher performance, which does have an installation and upkeep charge, but most organizations will be able to use existing instances if they have good latency to a Quad9-served IX.

Recommendation

We recommend that ISP users send requests to Quad9 secure service addresses to give users and their networks protection from malware and malicious sites.

Maintenance or installation of a local caching resolver on-premise at the ISP is a preferred option even if not provided by Quad9, as this will improve latency for frequently requested items. Quad9 can be used as a “forwarding resolver” by the local cache if one already exists. However, ISPs who wish to avoid the GDPR/privacy issues surrounding data on recursive resolvers at rest may wish to redirect end users directly to Quad9 resolver addresses without an intermediate caching layer.

Technical Detail

Secure DNS service addresses:

IPv4: 9.9.9.9 & 149.112.112.112
IPv6: 2620:fe::fe & 2620:fe::9

Non-secure (no blocklist) service addresses:

IPv4: 9.9.9.10 & 149.112.112.10
IPv6: 2620:fe::10 & 2620:fe::fe:10

Secure addresses offer:

- Domain blocklist from 19 different malware/threat providers
- DNSSEC validation on lookups

Non-secure addresses offer:

- Extended Client Subnet (ECS) included on authoritative lookups
- No DNSSEC validation
- No blocklist
- These might be useful for testing validation.

All service addresses offer:

- DNS-over-TLS supported on port 853
- DNS-over-HTTPS supported on port 443 (pending IETF standardization, expected in 2018)
- Alternate ports available (support@quad9.net for details)

Note: Use only one of these sets of addresses – secure or unsecured. Mixing secure and unsecured IP addresses in your configuration may lead to your system being exposed without the security enhancements, or your private data may not be fully protected. For consistent results, do not specify secure Quad9 addresses in combination with any other open recursive resolver as this may result in your systems being unprotected for 50% of your queries.

Blocking

Use case studies with large user base organizations (20,000 or more users) have shown a reduction in intrusion and malicious behaviours of more than 75%. These measurements were performed by examining IDS and malware detection software on edge routing management points before and after Quad9 implementation. In environments such as ISP networks where all devices are essentially unmanaged, this provides a transparent and highly effective way to minimize threats against devices, customers, and the network, all of which have distinct cybersecurity risks that can in some ways be mitigated by Quad9's DNS security model.

Currently NXDOMAIN is provided on secure service addresses for blocked sites. There are potential plans to provide "splash page" redirect for blocked sites, which include threat information for faster customer service identification. Optional service addresses with NXDOMAIN will be delivered when splash page is implemented.

NXDOMAIN returns with authority (AD) bit set “off” for blocked domain replies for local logging convenience.

ISP Threat Feeds

ISPs which monitor threats and deploy blocks on their own networks have the ability to continue to do this with Quad9 offering an additional layer of security. Quad9 is not a replacement for network-layer or client-installed threat mitigation such as IDS or virus software. Quad9 functions as a significant additional perimeter of defence for clients, protecting in rapid response to threats presented to your customer base. Consider Quad9 as a “low band pass filter” against a wide range of risks, letting your end users or network security systems focus more effectively on the more pervasive security issues which remain.

Performance

Quad9 is implemented at IX locations worldwide. There may be IX locations which are not served at this time; please contact support@quad9.net for details on how Quad9 might be able to participate in your IX. To most effectively gain access to Quad9 services, your ASN would need to peer with AS42 at an IX where Quad9 is present. See https://www.pch.net/about/peering and contact peering@pch.net to arrange this interconnection. Quad9 can also be deployed on-site to exclusively serve your customer base, but there is an installation and ongoing operational cost for equipment and management. Contact support@quad9.net for details.

Privacy

End-user privacy is a first-order priority for Quad9.

End-user IP address data is never stored to disk, or transmitted outside of the POP in which it is received[1]. There is no way to correlate DNS queries to specific IP addresses within any telemetry or logging system we utilize, and we go to great lengths to ensure that queries are not able to be associated with end-users.

Quad9 has been constructed with the most stringent privacy guidelines available (including GDPR advisement) so that our compliance is automatic by the nature of the data we do not collect, rather than by the way in which we handle data that we do collect. This lack of private data collection serves our goals by eliminating many technical and policy guidelines, and is possible because Quad9 has no other services or intentions for data of that type. Quad9 has a single goal: to provide secure DNS service to as many people as possible. There are no ulterior motives or products that rely on private data collection, which means your

[1] Except in limited security events or denial-of-service conditions – see https://www.quad9.net/policy/ for details. For more details about what Quad9 does with telemetry data, please see https://www.quad9.net/quad9-yourdata/.

client base and their personally identifiable information is not treated as a product by Quad9.

User Experience

Currently when users try to access a blocked domain, they received back a message (NXDOMAIN) that the domain has not been resolved. It may be the case in the future that secure service addresses will deploy a “splash page” which provides additional information to the end user on port 80.

Support

Support is available at support@quad9.net with one (1) business day turnaround time on most queries.

You can check for blocked domains at https://quad9.net/.

Further information is available at https://quad9.net/faq/#How_resilient_is_the_Quad9_DNS_infrastructure

False Positives

Quad9 places an exceptionally high priority on providing accurate data to end users. False positives, though rare, are treated as critical issues and examined quickly to determine if they should be removed from the combined threat domain list. Partners or end users may report false positives through a web portal or via a support email thread. The false positive rate is extremely low – less than one (1) per day (as of Quarter 2, 2018) and those typically are sites which are in fact distributing malware or being used as phishing collectors but which are also being used for other legitimate purposes – typically link sharing or file sharing websites.

There are a number of safeguards that are implemented to avoid including legitimate or highly utilized domains in the threat feed. Each domain added by Quad9 TI partners is examined against recent history data streams before inclusion, and domains which fall outside a prescribed set of values of “positiveness” are reviewed by staff before being allowed to be included into the threat feed. In the event that a TI partner accrues a large number of false positive events, that feed is then suspended and evaluated by Quad9 staff with the TI provider to determine the root cause of those domains being marked as malicious.

History and Founding Organizations

Quad9 is a not-for-profit organization created from the collaboration of Packet Clearing House (PCH), the Global Cyber Alliance, and IBM. The intent was to provide security and privacy to end users on a global scale by leveraging the DNS service to deliver a comprehensive threat intelligence feed.

An invited beta test group of educational institutions, local and state/provincial government IT organizations, and enterprise users utilized the Quad9 system over the course of a year as the POP rollout increased to 100 locations at the launch in November 2017. Since then (as of Quarter2, 2018) the platform has grown 35-fold in query volume and has added an additional 24 cities, with many more in pre-deployment testing and provisioning status. Target goals for 2018 include expansion to cover 150 POPs.

Most of Quad9's instances are currently co-located with and receive transit from PCH, a not-for-profit organization, though Quad9 is also expanding this transit portfolio. PCH has a history dating back 25 years of running core DNS infrastructure across the Internet and was the first network to operate anycast authoritative resolvers. Currently PCH operates one of the world's largest DNS arrays, with approximately 120 country code top-level domains (.ca, .in, etc.) using their resolving systems, two of the thirteen root nameservers delivering packets on their network and infrastructure, and a large number of extremely high-volume commercial organizations also trusting PCH for delivery of critical authoritative DNS and DNSSEC signing services.

GCA is a nonprofit whose initial requirements for a secure DNS-based platform were the genesis of what became Quad9. Their charter is to effectively protect as many people as possible from cybercrime by eradicating cyber risk. GCA, in turn, is sponsored by several agencies whose focus is on the lawful use of the Internet, who entrusted GCA with funding technical projects that make a difference in cybersecurity with the best return on investment.

IBM sponsors Quad9 with a threat intelligence data feed and support in various marketing and deployment projects, as well as having provided the 9.9.9.0/24 network which provides the namesake of the effort.