SECURE64®

# Secure64® DNS Proxy

Protect your subscribers' traffic and information without sacrificing performance or visibility

DATA SHEET

## KEY BENEFITS

- Provides low total cost of ownership
- Preserves client specific services
- Scales easily as DoH traffic increases

## KEY FEATURES

- Scalable architecture
- Preserves traffic control and visibility
- Onboard cache
- High availability

As more and more of our lives move online, privacy has become a major topic of conversation, and tools that increase user privacy are in high demand. An increasingly common solution is DNS-over-HTTPS (DoH), a method that uses a proxy server to encrypt DNS traffic. This approach can be effective at securing user traffic from eavesdropping and other interference, and has been adopted by all major browsers, including Firefox, Google, Safari, and Edge. With DoH's increasingly widespread adoption, it is crucial that network operators offer their own solution, to keep from losing control of their network traffic.

Maintaining control over your own traffic is vital, both for enabling the value-added services you offer your subscribers and preserving the necessary visibility into network traffic needed for effective management. Secure64 Proxy was developed to enable CSPs to offer a DoH solution to subscribers that is performant, scalable, and entirely under their control. Integrated seamlessly into your existing Secure64 DNS architecture, Secure64 Proxy let's you satisfy your subscribers demand for privacy without forfeiting control of your network.

## Optimal Performance

While any DNS-over-HTTPS will take some toll on network performance, our engineers have built DNS Proxy to minimize the impact and provide the strong, consistent performance demanded by modern networks. With Secure64 DNS Proxy supporting up to **280,000 queries per second**, you can provide DoH encryption to your subscribers without damaging their end user experience.

## Scalability

DNS over HTTPS is extremely CPU intensive, as each client must establish a TLS connection with the server and each query must be decrypted and each response encrypted. Large numbers of clients sending small numbers of queries can quickly overwhelm DoH solutions not designed to handle extremely large numbers of simultaneous connections.

DNS Proxy uses a highly scalable architecture that takes advantage of today's high-density CPU cores to manage hundreds of thousands of simultaneous client connections.

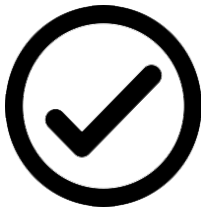
## Visibility

Without deploying your own DoH solution, traffic details get lost to 3rd party solutions. If traffic is being channeled through a DoH solution from Google or Firefox, it is stripped of information that is vital for security, monitoring, and other value-added services. Deploying your own DNS Proxy keeps the traffic on your network and under your control.

## Onboard Caching

DNS Proxy is more than just a DoH proxy; it includes an onboard cache, allowing the proxy to answer previously cached queries directly. This architecture greatly reduces the load on the back end resolvers while minimizing query latency.

## High Availability



DNS Proxy can be deployed in an anycasted architecture, providing high availability and fast failover without having to deploy load balancers. In addition, anycasting allows simple scaling as DoH traffic on the network increases over time.

## Security

Secure64 DNS Proxy is based on SecureOS, a hardened Linux distribution with a secure kernel augmented with integrated DDoS defenses, role-based authentication, and other security features necessary in carrier-grade systems.

## Monitoring

DNS Proxy provides a comprehensive SNMP MIB, allowing network monitoring systems to have full visibility into the health and status of the proxy server.