Carriers and service providers face the difficult challenge of designing their DNS infrastructure for both high performance and security. Rising query loads and heightened user expectations for responsiveness create a need for high throughput and low latency, while increasingly visible DNS attacks increase the need for security to protect end users from fraud. At the same time, carriers and service providers are under constant pressure to increase revenue and profitability.

Secure64 DNS Cache is high-performance, highly secure caching DNS software, providing unmatched throughput and consistently low latency with the greatest protection against cache poisoning attacks. In addition, DNS Cache’s integrated NXDOMAIN redirection module allows service providers to monetize web errors using their choice of major redirection vendors, without adding additional hardware into the network.

By combining high performance and security with integrated web error redirection, DNS Cache allows service providers to reduce costs while increasing revenues and differentiating their service offering.

### Key Benefits
- Provides headroom for growth
- Improves user experience
- Consolidates servers
- Protects against forgery attacks
- Generates incremental revenue

### Key Features
- 125,000 queries per second
- Consistently low latency
- Industry-leading five layer cache poisoning protection
- Integrated NXDOMAIN redirection

Secure64 DNS Cache delivers significantly better performance than BIND
Highest Performance

High query throughput
DNS Cache delivers industry-leading performance of 125,000 queries per second. This high level of throughput easily handles today’s load while providing substantial headroom for growth.

Consistently low latency
DNS Cache provides extremely low latency regardless of the query load. This low latency improves the end user’s experience, especially in time sensitive applications.

Unmatched Security

Five layer forgery defense
DNS Cache utilizes five layers of defense that effectively eliminate the threat from cache poisoning attacks.

Impedance Layer – DNS Cache can be configured to randomize source ports, source and destination IP addresses, and domain name case for 48 bits of total randomness on average, dramatically decreasing the odds of a successful attack.

Filter Layer – Query responses are filtered using guidelines from RFC 2181 and industry best practices to discard untrustworthy data that could be used to contaminate the cache.

Detection Layer – When a query response is received with a mismatched transaction ID or domain name case, DNS Cache will save the mismatched response information, discard the response and requery.

Alert Layer – When a mismatched query response is detected, DNS Cache will provide an alert, allowing the operator to take appropriate remedial action.

Validation Layer – DNS Cache provides full support for DNSSEC and Domain Lookaside Validation (DLV). Cryptographic validation of DNSSEC signatures provides the highest level of protection against forgery attacks.

Automatic blacklisting
DNS Cache automatically detects clients exceeding a user-defined query threshold and temporarily blacklists them while logging information about the offending client. This capability reduces the operational cost of managing misconfigured clients and eliminates inadvertent participation in a denial-of-service attack.

High Availability

Ancast with fast failover
DNS Cache can be easily anycasted utilizing sub-second failover protocols that minimize the impact of hardware or network failures on end users.

NXDOMAIN Redirection

Powerful redirection rules
DNS Cache’s integrated NXDOMAIN redirection module allows service providers to redirect NXDOMAIN responses from authoritative servers to a provider-branded search portal. DNS Cache’s powerful rules engine provides fine-grained control over which responses are redirected, while its built-in support for opt-out simplifies management and deployment.

Choice of redirection partner
DNS Cache supports a wide variety of redirection portals from leading redirection vendors, allowing the service provider to choose the redirection vendor best suited to meet their business requirements.

CERTIFICATIONS

IPv6 Ready Phase 2 Gold

HARDWARE

HP Integrity® rx2660, rx3600, or BL860c server
- Single, dual core processor
- 2 GB RAM minimum
- HP Integrity iLO 2 management processor
- Integrated TPM security chip
- Redundant power supply (optional)
- RAID disk (optional)

DNS RFCs SUPPORTED

<table>
<thead>
<tr>
<th>Subject</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>1034, 1035</td>
</tr>
<tr>
<td>Localhost</td>
<td>1918</td>
</tr>
<tr>
<td>Clarifications</td>
<td>2181</td>
</tr>
<tr>
<td>Negative caching</td>
<td>2308</td>
</tr>
<tr>
<td>EDNS(0)</td>
<td>2671</td>
</tr>
<tr>
<td>Indicating resolver support for DNSSEC</td>
<td>3225</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>4033, 4034, 4035</td>
</tr>
<tr>
<td>NSEC3</td>
<td>5155</td>
</tr>
<tr>
<td>DNS Resiliency</td>
<td>5452</td>
</tr>
</tbody>
</table>

Learn more about Secure64’s DNS solutions at www.secure64.com