SECURE64®

DATA SHEET

Secure64® DNS CACHE™

Secure, Scalable, Caching DNS

FEATURING:

- Self-defending DNS caching name server protecting against DDoS, DNS and protocol attacks.
- Scalable, predictable performance.
- Integration with the Secure64® Vizion™ platform for security event visibility, alerting, and reporting.
- Integration with the Secure64® Guard™ platform for security event blocking, such as phishing, malware, ransomware etc.

Industry-Leading Security

Secure64® Caching DNS is a powerful, self-defending caching DNS platform for carrier and enterprise networks. Security, safety, and stability are central to the architecture, ensuring maximum uptime for the platform, high performance, and advanced additional features.

The caching DNS server needs to scale and be performant even nder heavy loads and network attacks. Secure64® Caching DNS performs under heavy loads, scales linearly, and defends against DDOS & network attacks. Caching DNS is fundamental to any network's operation.

DNS Cache provides fine-grained DDoS detection, reporting, and mitigation rules, allowing the server to continue to respond to egitimate queries while throttling traffic from attackers in situations where conventional DNS solutions would crash or become unavailable. These rules can be used to protect against a wide variety of attacks including direct attacks, reflected attacks, amplified attacks, as well as application layer attacks such as pseudo-random subdomain attacks or excessive querying for particular record types.

Secure64® has built protection and reporting mechanisms into different layers of network stack. In-depth defense is the best protection against the range of attacks that are prevalent against DNS servers. The optional Tunnel Guard application allows the operator to prevent Data exfiltration and revenue theft via DNS. This sophisticated add-on works without user intervention using machine learning and analysis of the traffic in real time.

Product Highlights

Non Bind-Based DNS

BIND is the world's most widely deployed DNS software, making it a primary target for attackers seeking to cause maximum worldwide damage. Secure64® DNS Cache™ is a completely different implementation that shares no code with BIND, making it immune to all BIND-specific vulnerabilities.

Open Linux Deployment or Containers

Secure64® DNS Cache™ can be installed on top of a Linux kernel or within a container solution, such as a Kubernetes deployment. Having this open nature allows for deploying security policies and access specific to the customer.

DATA SHEET

Secure64® DNS CACHE™

Secure, Scalable, Caching DNS

Cache Poisoning Protection

In addition to industry standard source port randomization and 0x20 defenses against spoofed responses, DNS Cache supports all the DNSSEC RFCs, providing maximum protection against Cache poisoning attacks.

Secure64® Vizion Capable

Secure64® Vision allows the administrator to see DDoS attacks and Guard events in near real-time using a simple web-based GUI display installed inside the network. The information from security events can also be exported in a standardized format to external platforms for further SOC and compliance analysis, monitoring, and reporting.

DNS Security Services

Protecting users and the network from malicious activity is becoming increasingly important for both legal and operational reasons. Malicious sites infect clients with malware, which then uses the network to send spam, conduct fraud, or participate in Denial-of-Service attacks. DNS Cache supports the DNS Guard security services, which identify and block infected devices before they can cause damage. DNS Cache also allows the definition of one or more internal lists of undesirable domains and specification of whether queries for domains on a list are to be dropped, responded to with an error, or redirected to a portal or walled garden where information and remediation instructions can be provided to the client.

High Availability

The DNS is a mission-critical networking service that must always be available to service client requests. Conventional DNS servers must be restarted to make configuration changes or use diagnostic tools. DNS Cache allows changes to a running server to be made on the fly, including rules modification, with no loss of service continuity, ensuring that the service can meet even the most stringent availability requirements.

Anycasting with Fast Failover BGP anycasting has long been deployed by root and top-level domain operators as a best practice for high DNS availability and resiliency. DNS Cache not only supports BGP anycasting, but it also allows it to be augmented by Bidirectional Forwarding Detection (BFD) for sub-second failover in the event of a server failure, thus ensuring high levels of DNS service continuity.

Scalable Performance Throughout

DNS Cache provides the highest performance of any resolver software, which minimizes hardware resources required and saves on capital and operating expenses.

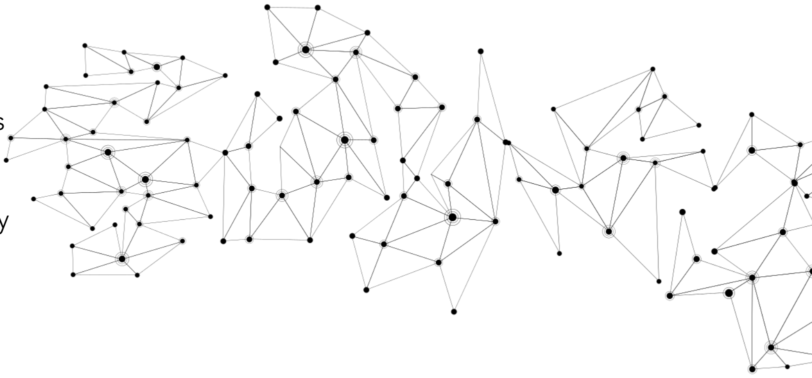
Simple Management and Monitoring

DNS Cache allows customers to monitor the network, operating system, and application in real time while supporting a variety of leading network monitoring systems. Detailed information is available through SNMP v3, allowing the monitoring system to easily determine the

server's availability, security, and operational health in real-time.

Centralized Management

DNS Cache servers can be managed individually, or they can be centrally managed and monitored through Secure64® Vizion™ and Manager.



Learn more about Secure64 DNS Solutions at www.secure64.com

SECURE64®

303.242.5890 | www.secure64.com