SECURE64®

Secure64® DNS CACHE™

Scalable, secure caching DNS

DATA SHEET

DNS CACHE

KEY BENEFITS

- Protects against DDoS attacks
- Immune to BIND security vulnerabilities
- Easily scales to future loads
- Generates incremental revenue

KEY FEATURES

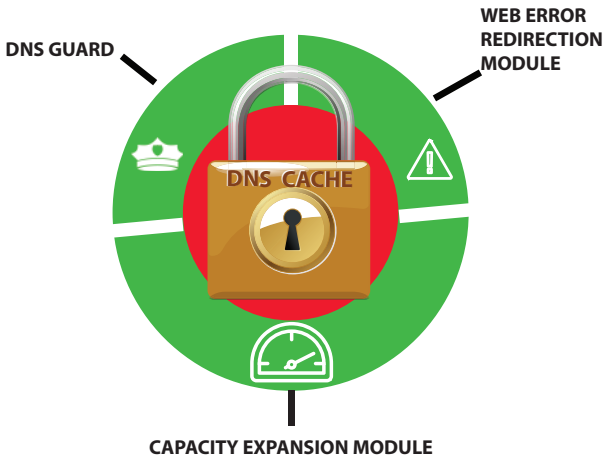
- Scalable performance with simple software upgrade
- Industry leading security
- Non-BIND based DNS
- Real time query monitoring
- Integrated Web Error Redirection Module

DNS CACHE

Ensuring DNS security has become a primary concern of service providers, given the increased frequency and size of denial-of-service attacks on the DNS and the steady stream of security vulnerabilities in BIND. Designing an infrastructure that can withstand today's attacks can be expensive and complicated, while performing emergency vulnerability patching of the DNS is both disruptive and time consuming. At the same time, rising query loads makes capacity planning more challenging, especially in order to avoid future costly DNS server additions or upgrades.

Secure64 DNS Cache is a scalable, highly secure DNS caching server, providing built-in protection against high volume denial-of service attacks and immunity to BIND-specific security vulnerabilities. In addition, DNS Cache can be easily scaled to meet future query loads through the optional Capacity Expansion Module™, which doubles performance through a simple software license upgrade.

DNS Cache serves as a secure, scalable platform for deployment of additional optional security and revenue-generating services. Secure64® DNS Guard™ is a family of security services that protect users and the network from malicious activity, while the Web Error Redirection Module allows service providers to improve the end user's experience while generating incremental revenues that flow right to the bottom line.



Scalable Performance

DNS Cache delivers performance where it matters most – under real-world traffic conditions. At a 90% cache hit rate, DNS Cache delivers over 125,000 queries per second, which can easily be increased to 280,000 queries per second through the optional software-based Capacity Expansion Module™. This software performance scalability allows building scale for tomorrow's load without locking into fixed-capacity appliances or servers.

Unmatched Security

Non-BIND based DNS

BIND is the most widely deployed DNS software in the world, which makes it a primary target for attackers seeking to cause maximum damage. DNS Cache is a completely different implementation that shares no code with BIND, making it immune to BIND-specific vulnerabilities.

System authentication

Digital signatures of the firmware, operating system and application code are all validated during the boot process. This ensures that neither the operating system nor the application code images on disk have been compromised by a rootkit.

Secured runtime environment

The Secure64 proprietary OS, SourceT®, utilizes security capabilities unique to the server hardware to eliminate all paths for injection or execution of malicious code at runtime.

Built-In DDoS Protection

Built-in DDoS detection and mitigation allows DNS Cache to continue to respond to legitimate queries even while fending off high volume denial-of-service-attacks, unlike conventional DNS solutions that crash or become unavailable at much lower levels of attack traffic. In addition to mitigating high volume attacks, DNS Cache also automatically detects individual 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 helps prevent inadvertent participation in a denial-of-service attack.

Network protection

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, in turn, 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 malicious activity before it 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.

Simple Management and Monitoring

SNMP

DNS Cache provides several MIBs, allowing customers to monitor the chassis, network, operating system and application in real time, while supporting a variety of leading network monitoring systems. In addition, DNS Cache directly provides alerts of critical operational conditions through SNMP traps without requiring special configuration within the network monitoring system.

Centralized management

DNS Cache servers can be managed individually, or can be centrally managed and monitored through Secure64® DNS Manager™. DNS Manager simplifies the management of a large DNS network by managing configurations and revisions, upgrading software versions, managing and synchronizing blacklists, and monitoring key performance indicators across multiple Secure64 servers in the network.

Real-time Statistics

DNS Cache, when combined with DNS Manager, provides real-time statistics including the top clients querying the server and the top fully qualified, top-level and sub domains queried. These statistics can provide new insights into legitimate as well as abusive DNS behavior.

DNSSEC validation overrides

DNS Cache can be easily configured to validate DNSSEC signed answers. Because DNSSEC configuration errors are not uncommon, operators can readily identify domains failing validation and specify which of these should be allowed to resolve normally.

Web Error Monetization™

DNS Cache's optional Web Error Redirection Module allows service providers to redirect NXDOMAIN responses from authoritative servers to a provider-branded search portal that helps guide users to their intended destination while generating incremental advertising revenues. 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.

D N S C A C H E

OPTIONAL MODULES

- Capacity Expansion Module
- Web Error Redirection Module

SECURITY

- Easily scales to future loads
- Generates incremental revenue
- Genuinely secure micro OS
- Secure SSH2 CLI
- Password, certificate, LDAP or RADIUS authentication
- Role based access control
- Access control list
- DNSSEC support
- Immune to BIND security vulnerabilities

CERTIFICATIONS

- IPv6 Ready Phase 2 Gold

HARDWARE

- HP Integrity® servers HP Integrity iLO management processor
- Integrated TPM security chip
- Redundant power supplies, fans, disks available
- Call Secure64 for specific models and configurations

A Genuinely Secure operating system has a secure architecture that fully utilizes the hardware to make applications immune to compromise from rootkits and malware and resistant to network attacks, unlike a hardened OS that is typically manipulated to minimize exposure to its insecurities.

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

Secure64 Software Corporation

303-242-5890

www.secure64.com