SECURE64®

DATA SHEET

Secure64® DNS AUTHORITY™

Safe, Secure, High-Performance
DNS Authority Server

FEATURES

- Carrier-grade DNS Authority server.
- Non BIND-Based platform running on Redhat Enterprise Linux (RHEL)
- Self-Defending architecture to protect against DDoS, DNS protocol attacks, and network attacks.

Safe, Secure, High-Performance DNS Authority Server

Secure64® DNS Authority™ is a self-protecting DNS authority server is designed for both Carrier-Grade and Enterprise deployments on a bare metal appliance, virtual machine, or container-based platform including Kubernetes.

Designed and built to support the largest deployments with millions of zones and resource records, performance is paramount to delivering solutions at the scale required from a modern DNS platform.

For large-scale or high-performance DNSSEC deployments, the platform supports all relevant RFCs and extends its capabilities via off-platform signers for FIPS 140-2 certified for Level 2 and Level 3.

Security is built into the architecture with layers of protection to prevent DDoS, DNS protocol, and application attacks. As the architecture is not based on BIND, the platform is not susceptible to the same attacks.

Management and reporting are available via the command line, and a full-featured GUI to ensure ease of use. Non-stop high availability for moves, adds, and changes ensure no downtime or reboots when a change is required to the zone or resource record. Supporting all common RFC's for DNS, Secure64® DNS Authority™ is built for the requirements of carrier and enterprise deployments.

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 Authority™ is a completely different implementation that shares no code with BIND, making it immune to all BIND-specific vulnerabilities.

Full DNSSEC Support

Secure64® DNS Authority™ supports all of the DNSSEC RFCs, ensuring that appropriately configured resolvers can validate signed zones. The platform integrates with the Secure64® Signer, allowing FIPS 140-2 compliance for Level 2 and Level 3 and HSM features for extra levels of security and performance when signing and resigning zones.

Response Rate Limiting

Attackers can abuse authoritative DNS servers to reflect large amounts of DNS response traffic towards a victim server. Response rate limiting algorithms detect patterns in arriving queries and reduce the rate at which replies are sent if the patterns suggest abuse, thus protecting server load, network bandwidth, and the end victim server itself.

SECURE64®

DATA SHEET

Secure64® DNS AUTHORITY™

Safe, Secure, High-Performance
DNS Authority Server

Centralized Management

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

High-Availability Dynamic Zones

Adding or deleting zones in traditional DNS servers requires restarting the server before changes take effect. Restarts can take a long time, leading to reduced service availability during the restart. Conversely, restarting the server only during a scheduled maintenance window preserves service availability SLAs, but may not meet zone propagation SLAs, as new zones may only be visible after a few hours.

Secure64® DNS Authority™ allows zones to be added, amended and deleted on the fly, with no restart required and no loss of query responsiveness during the update, allowing operators to meet even the most stringent requirements for both service availability and zone propagation time.

Dynamic Configuration Changes

DNS is a mission-critical networking service that must always be available to service client requests. Conventional DNS servers must be restarted to make changes to configurations or to turn on diagnostic tools. Secure64® DNS Authority™ allows changes to a running server, including rules modification, to be made on the fly 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. Secure64® DNS Authority™ not only supports BGP anycasting, but 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.

DATA SHEET

Secure64® DNS AUTHORITY™

Safe, Secure, High-Performance
DNS Authority Server

Simple Management and Monitoring (SNMP)

Secure64® DNS Authority™ allows customers to monitor the network, operating system, and application in real time using Secure64® management applications as well as supporting a variety of leading network monitoring systems such as syslog, SNMP, and external third-party tools and applications.

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.

Feature-Rich Split Horizon DNS

Views allow the configuration of an DNS Authority Server to provide different functionality and responses based on the characteristics of the requesting client.

Redhat Enterprise Linux (RHEL) OS or Cloud-based Deployment

Secure64® DNS Authority is capable of being deployed on Redhat Enterprise Linux (RHEL) as well as Kubernetes and containerized deployments.

Query Statistics

A wealth of aggregate statistics are available from the server, including the number of queries broken down by type, class, and opcode, over UDP versus TCP, over IPv4 versus IPv6, and responses broken down by response code. Statistics can also be gathered and reported on a per-zone basis. NFV-Ready Authority provides a restful API that enables external orchestration and management systems to configure, monitor, and manage it throughout its lifecycle. This promotes network automation and elastic scaling – two key goals in the shift towards virtual network functions.

Synthesized PTR Records

Reverse DNS records for IPv6 addresses or other large address blocks can be generated on the fly, preserving compatibility with other systems that rely upon the existence of these reverse records. The feature reduces memory usage and improves performance compared other systems.

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

SECURE64®

303.242.5890 | www.secure64.com