

DNS AUTHORITY



KEY BENEFITS

- Remains fully responsive during DDoS attacks
- Eliminates BIND security vulnerability patching
- Enables 99.999% service availability
- Reduces TCO because servers need no protective security appliances

KEY FEATURES

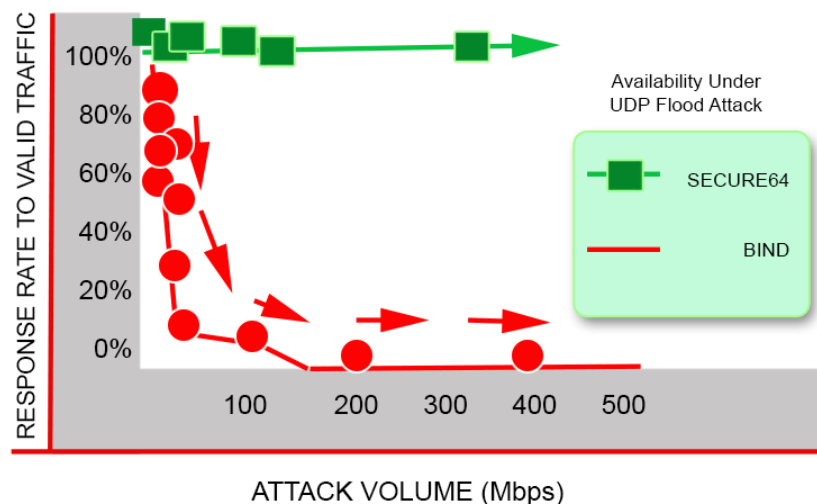
- Built-in denial-of-service detection and mitigation
- Immune to injection of rootkits and malware
- No downtime on restarts
- Built-in support for anycast
- Enables reverse DNS records on the fly

Y
L
I
T
Y
A
U
T
H
O
R
I
T
Y
D
N
S

In today's increasingly hostile internet, the question is not whether your DNS will come under attack, but when. Attackers have realized that the DNS is a perfect target, because if they can bring down the DNS, they can take their target off the web, as well as bring down email and users.

But defending against today's DNS attacks can be costly and complex, as best practices involve hardening and constant patching of vulnerable operating systems and DNS software, as well as protecting them with expensive security appliances that introduce unwanted latency and additional points of failure into the network.

Secure64 DNS Authority is a DNS authoritative server that provides the highest levels of security, availability and resiliency under attack without the cost and complexity of conventional solutions. Unlike hardened systems, DNS Authority is Genuinely Secure: it has been designed from the ground up with a secure architecture that makes it immune to compromise from rootkits and malware and resistant to network attacks. Combined with its built-in support for anycasting and its non-stop DNS architecture, this allows DNS Authority to remain highly available at all times, even when under attack or during restarts.



Always Available

Integrated DDoS protection

Under attack conditions, detection and mitigation technology instantly engages to identify and block attack traffic, while still responding to queries from legitimate sources. It simultaneously provides attack information through syslog and/or SNMP traps that can be used to set upstream router filters.

Network bandwidth protection

DNS amplified flood attacks can easily consume the available bandwidth even of large service providers. DNS Authority's PipeProtector™ feature protects the network by automatically identifying the sources of amplified flood attacks and communicating with the upstream router to blackhole the attack traffic.

Built-in BGP for easy anycasting

DNS Authority can easily be set up in an anycast configuration, which provides greater resiliency against denial-of-service attacks as well as improved performance. After BGP is initially configured, the administrator can insert and withdraw the server from the anycast cluster without making router changes, greatly simplifying administration.

No downtime on restarts

Zones can be dynamically added or deleted and the name server restarted without interrupting query responses.

Unmatched Security

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 specialized OS (SourceT) utilizes security capabilities unique to the server hardware to eliminate all paths for injection or execution of malicious code at runtime.

Non-BIND based

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

Secured zone data

DNS Authority ensures end-to-end integrity of zone data by supporting DNSSEC, TSIG and ACLs for queries, notifies and zone transfers.

Scalability and IPv6

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.

Full IPv6 support

DNS Authority fully supports IPv6 in either dual stack or IPv6-only mode.

Zone propagation

Whether there are one hundred zones, or hundreds of thousands, new, deleted or modified zones are quickly propagated to slave servers, meeting even the most stringent Service Level Agreements.

ENUM

Scalability

DNS Authority scales easily to handle the millions of records required for a large ENUM deployment with no performance degradation.

Standards support

DNS Authority supports ENUM standards, including RFC 3163 (SIP initiation protocol), RFC 6116 (storage of data for E.164 numbers in the DNS) and 3GPP TS 29.303 (DNS procedures for the Evolved Packet System).

Compatibility

Interoperability

DNS Authority interoperates with other name servers running BIND or Microsoft Windows DNS software and can directly read existing BIND configuration files.

Split horizon DNS

Views allow configuration of an authoritative server to provide different functionality and responses based on characteristics of the requesting client.

© Secure64 Software Corporation. All rights reserved. Secure64® and SourceT® are trademarks of Secure64 Software Corporation. Other marks are owned by their respective companies.

SECURITY

- Genuinely secure micro OS
- Built-in DDoS detection and mitigation
- Secure SSH2 CLI
- Role-based access control
- Password, certificate, LDAP or RADIUS authentication
- ACLs on notifies and zone transfers
- TSIG signed zone transfers
- DNSSEC support certifications
- IPv6 Ready Phase 2 Gold

HARDWARE

- HP Integrity servers
- HP Integrity iLO management processor
- Integrated TPM security chip
- Available with redundant power supplies, fans and disks
- 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