

December 18, 2008

To: Joint Interoperability Test Command
From: InfoWeapons, Inc.
Subject: Letter of Compliance for SolidDNS v3.0

InfoWeapons Inc. is submitting two SolidDNS 3.0 servers for JITC certification. These servers consist of our hardened FreeBSD 7.0-based operating system titled SolidOS, with our SolidDNS 3.0 Dual-stacked DNS application, which uses Bind 9.5.0p2. This bundled software will be hosted on Dell PowerEdge SC 1435 hardware.

InfoWeapons Inc. has completed two versions of IPv6 compatibility testing against our SolidDNS 3.0 product. The first was the Tahi Self Test (testing guidance from the IPv6 Forum for IPv6 Ready Certificate). The second was the DEPARTMENT OF DEFENSE INTERNET PROTOCOL VERSION 6 GENERIC TEST PLAN VERSION 3.

Our primary IPv6 Compliance Test Engineer provided a summary of his test results to communicate our current level of support for applicable Request for Comments (RFC).

Based on the results below, we believe SolidDNS 3.0 is compliant with Joint Interoperability Test Command (JITC) requirements for an IPv6 Simple Server.

List of IPv6 Compatibility RFCs for a Simple Server, Supported in SolidDNS v 3.0:

#	RFC	Title	SDNS Support
1	2460	Internet Protocol, Version 6 (IPv6) Protocol Specification	Supported
2	2461	Neighbor Discovery for IPv6	Supported
3	2464	IPv6 over Ethernet	Supported
4	2710	Multicast Listener Discover for IPv6	Supported
5	3319	DHCPv6 Options for Session Initiation Protocol (SIP) Servers	Supported
6	3633	IPv6 Prefix Options for DHCPv6	Supported
7	3646	DNS Configuration Options for DHCPv6	Supported
8	4007	Scoped Address Architecture	Supported
9	4075	Simple Network Time Protocol(SNTP) Configuration Option for DHCPv6	Supported
10	4193	Unique Local IPv6 Unicast Addresses	Supported (but no address generator)
11	4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	Supported (dual-stack implementation)
12	4242	Information Refresh Time Option for DHCPv6	Supported
13	4291	IPv6 Addressing Architecture	Supported

14 4443 Internet Control Message Protocol (ICMPv6)

Fully supports RFC 2463 (older ICMPv6 RFC). Supports all RFC 4443 requirements except "Test v6LC.1.2.11: Unrecognized Routing Type - Intermediate Node". SolidDNS failed to respond with an ICMPv6 Type 4 (Parameter Problem Message). We believe this is acceptable behavior because SolidDNS will not act as an Intermediate Node during actual deployment; it will act as an End Node.

15 4704 DHCPv6 Fully Qualified Domain Name (FQDN) Option Supported

16 None Disable Auto-configuration Supported - Default

Based on the above test results, InfoWeapons believes that our SolidDNS 3.0 product (Dual-Stack DNS server) meets Internet Engineering Task Force (IETF) RFC conformance for an IPv6 Simple Server.

We are officially requesting that our SolidDNS 3.0 product be scheduled for JITC IPv6 Interoperability certification testing for a Simple Server product class.

In addition to the above interoperability RFC supported, we are providing a list of DNS-specific RFCs have been implemented within SolidDNS 3.0:

List of specific DNS RFCs implemented in SolidDNS 3.0:

RFC	Title
1034	Domain names - concepts and facilities
1035	Domain names - implementation and specification (See notes [1] and [2])
1123	Requirements for Internet Hosts - Application and Support
1183	New DNS RR Definitions
1348	DNS NSAP RRs (See notes [6])
1535	A Security Problem and Proposed Correction With Widely Deployed DNS Software
1536	Common DNS Implementation Errors and Suggested Fixes
1706	DNS NSAP Resource Records
1712	DNS Encoding of Geographical Location
1750	Randomness Recommendations for Security
1876	A Means for Expressing Location Information in the Domain Name System
1886	DNS Extensions to support IP version 6
1982	Serial Number Arithmetic
1995	Incremental Zone Transfer in DNS
1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
2163	Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)
2181	Clarifications to the DNS Specification

2230	Key Exchange Delegation Record for the DNS
2308	Negative Caching of DNS Queries (DNS NCACHE)
2535	Domain Name System Security Extensions (See notes [3] and [4])
2536	DSA KEYs and SIGs in the Domain Name System (DNS)
2537	RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)
2538	Storing Certificates in the Domain Name System (DNS)
2539	Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
2671	Extension Mechanisms for DNS (EDNS0)
2672	Non-Terminal DNS Name Redirection
2673	Binary Labels in the Domain Name System
2782	A DNS RR for specifying the location of services (DNS SRV) (See notes [6])
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
2930	Secret Key Establishment for DNS (TKEY RR)
2931	DNS Request and Transaction Signatures (SIG(0)s) (See note [5])
3007	Secure Domain Name System (DNS) Dynamic Update
3484	Default Address Selection for Internet Protocol version 6 (IPv6)
3596	DNS Extensions to Support IPv6 (Obsoletes RFC 1886)

Clarification Notes:

[1] Queries to zones that have failed to load return SERVFAIL rather than a non-authoritative

response. This is considered a feature.

[2] CLASS ANY queries are not supported. This is considered a feature.

[3] Wildcard records are not supported in DNSSEC secure zones.

[4] Servers authoritative for secure zones being resolved by BIND 9 must support EDNS0 (RFC2671), and must return all relevant SIGs and NXTs in responses rather than relying on the resolving server to perform separate queries for missing SIGs and NXTs.

[5] When receiving a query signed with a SIG (0), the server will only be able to verify the signature if it has the key in its local authoritative data; it will not do recursion or validation to retrieve unknown keys.

[6] RFCs are not fully supported. We don't have a UI to manually add these records. However, these records can be added thru imports, zone transfers (secondary) and dynamic updates.



M. Luis Gopez
CEO
InfoWeapons, Inc.