



SolidDNS 2.0

Lawrence E. Hughes, Chairman

InfoWeapons, Inc.



InfoWeapons – the creator of SolidDNS

- Founded in 2004, InfoWeapons is based in Atlanta, Georgia, in the U.S. We have a development team of 80 people in Asia and a smaller team in Eastern Europe.
- We specialize in network infrastructure with two key features:
 - Military grade security (resistance to hacking, and good use of strong cryptography for privacy and strong authentication)
 - Full support for all relevant IPv6 standards, including the prestigious and universally recognized “IPv6 Ready” certification, which proves compliance and interoperability
- We also create infrastructure for telcos, that help them achieve IP convergence and migrate their customers to IPv6
- We have a strong management team with prior IT company successes and large telco experience



SolidDNS 2.0 Overview

- The first product from InfoWeapons is a fully dual stack (IPv4 and IPv6) DNS and DHCP server appliance. The current release is 2.0, but 3.0 is due soon.
- It works equally well in an IPv4-only, Dual Stack or IPv6-only network environment.
- All protocols (including management, NTP, SNMP, etc) work over both IPv4 and IPv6. The underlying OS is BSD which is years ahead of Linux in IPv6 support.
- The Graphics User Interface (GUI) has extensive support for rapid and error-free entry of IPv6 addresses.
- Minimal information is captured in an internal database, from which BIND configuration files are programmatically generated.
- The OS is hardened and layer after layer of anti-hacking measures (Defense in Depth) protect all of its systems



Definitions

- **DNS** – Domain Naming Service
 - Like a phonebook or address book for the Internet
 - Maps domain names (e.g. fred.x.com) to and from IP addresses (e.g. 123.45.67.89 or 2001:ec8:5:1::53)
 - Also publishes names of key servers for SMTP (mail), LDAP (network directory), SIP (VoIP), for a domain.
 - Worldwide distributed database
- **DHCP** – Dynamic Host Configuration Protocol
 - Provides IP address and network configuration data to nodes when they first come online
 - IPv6 version requires radically different architecture, different actual server, than IPv4 version.



DNS

- We include the most recent version of BIND, with simple GUI based administration wrapped around it in a highly secure implementation
- The BIND engine is good, but notoriously difficult to administer.



DHCP

- We provide both DHCPv4 and DHCPv6 servers, with simple GUI administration.
- The DHCPv6 server supports all relevant RFCs, and operates in two modes:
 - Stateless – we provide only data that is the same for every node, such as DNS server address, gateway address, etc. IP address is obtained via stateless autoconfig.
 - Stateful – we provide stateless information *and* a unique IP address to each node.
- Note that stateful DHCPv6 is required to cluster IP addresses per group or per department, to keep firewall or NAC rules simple. This can be very difficult or impossible when addresses are assigned via stateless autoconfig.
- It is possible to assign IPv6 addresses from allocation pools, or randomly generated from address ranges, avoiding the possibility of scanning for EUI-64 based addresses.



System Administration

- Using BIND (the underlying engine) directly requires extensive knowledge of UNIX and BIND (one must be familiar with most of the inch thick “BIND and DNS 5th Edition” from O’Reilly to be effective)
- Our two primary interfaces are simple GUI point-and-click, with no knowledge of UNIX or BIND required. Even an entry level network administrator can quickly become proficient with it, and produce error-free configurations rapidly.
- The main interface is web/PHP based. The other is a Microsoft Management Console snap-in (intentionally similar to the Windows Server DNS management tool). Neither require use of Java, which many administrators consider a serious security risk.



Secure Remote Administration

- All administration is done over SSL/TLS, using a server certificate generated on box, or from an external CA. It is simple to install the box's root certificate into any browser.
- When SolidDNS is first installed, administrators can use username/password authentication. Optionally, they can generate digital certificates (on box or from an external CA) for strong client authentication. Once all administrators have digital certificates, the username/password authentication mechanism can be deactivated for greater security. For highest security, the administrator credentials can be generated in security tokens.
- This makes it simple and completely safe to do remote administration from anywhere on a connected Internet.
 - The box can be at a central site and administered by one or more administrators throughout your organization
 - Remote boxes can be administered from a central NOC



Security and Functionality

Updates

- A key part of securing any network infrastructure is to obtain security patches, verify them as authentic and intact, then apply them on a timely basis.
- It is also convenient to obtain and install functionality updates online, to keep your product at the most recent release.
- We provide an “update server” (available as a separate product for internets not connected to the main Internet) from which each SolidDNS server can automatically obtain updates.
- Each update is digitally signed (more secure than simple MD5 checksums) by InfoWeapons, and verified using our public key (which is installed in every appliance). This insures that the updates are intact (not tampered with) and authentic (definitely from us). We continually scan for security patches to all open source components in the product, test them, and publish them on our update server on a timely basis.

Typical Administration Tasks – Define Networks

- You first define each network for which you will be entering node data. These are used to create the *reverse zones*. This involves entering the *network address* and subnet length (e.g. 192.168/16 or 2001:ec8:4008:1/64). Once the network is defined, PTR record creation is automatic, for both IPv4 and IPv6. Reverse zones for IPv6 are particularly difficult to get right when using BIND directly.
- When you define an IPv6 network, you can name it (e.g. “main”). After this, when you define a node, you can choose the network name from a pulldown list, which defines the first 64 bits of the address automatically. If in the future, if you change providers, you can easily redefine the prefix for each network name, which causes all forward and reverse DNS records to be updated in seconds, even for a very large network. This provides the functionality the deprecated A6 resource record was supposed to provide, with no downside (only AAAA records are actually written in the BIND configuration files).
- You can view the automatically generated PTR records any time.



Typical Administration Tasks – Domains & Nodes

- You can easily define any number of domains (e.g. x.com) or subdomains (e.g. w.x.com). Each of these causes a *forward zone* to be created in BIND. You have full control over *Start of Authority* (SOA) values for each domain. The default SOA values will work in most cases, so entry level admins can ignore these.
- Once a domain is created, it is simple to define any number of nodes in that domain (e.g. fred.x.com), each of which can have any number of IPv4 and/or IPv6 addresses.
- Entry of node addresses is very simple and as error-free as we could make it. Only valid values are accepted, with clear error messages for invalid data or values. Entry of IPv6 addresses is especially easy and error-free using our named networks.
- Defined domains are presented in a hierarchical tree view, including support for BIND “views” (required only for networks with NAT)



Advanced System

Administration

- It is possible to delegate administration of a subdomain to another administrator, which is useful in a large organization
- It is also possible for multiple organizations to share a single SolidDNS server, without being able to see or modify each other's domains, networks or nodes. This makes it ideal for ISPs or telcos to provide DNS services to customers, where they can manage their own DNS easily, intuitively and securely.
- There is also a Command Line Interface (CLI) for advanced tasks such as loading mass node data.
- There are real time graphs (MRTG based) for monitoring CPU and memory utilization, DNS query activity, etc.
- Experienced administrators can view any generated BIND configuration file to assure themselves that we have generated the correct data.



Online Help

- There is extensive online help available (over 1500 printed pages worth), which is also available offline in PDF format.
- The same master file generates online help for the web/PHP and MMC interfaces.
- Help is available in various ways:
 - Context sensitive
 - Index
 - Keyword search
- Help files include extensive images from the GUI mixed with the text explanations.

Sold as Hardware Appliance, Sofpliance or Virtualized

- Hard Appliance sold on a rack mount hardware platform
- 64-bit hardware running native 64-bit software
- OS already installed and hardened
- Web/PHP and/or MMC snap-in secure remote management



SolidDNS™ Competitor Comparison

	Infoblox	BlueCat Networks	InfoWeapons
Product	DNSOne 1000	Adonis 1000	SolidDNS™ 100*
Price: Hardware Appliance	\$9,995	\$9,995	\$9,595
Sofpliance	none	none	\$5,995
Annual Maintenance Fees	25%	25%	20%
Operating System	Linux	Linux 2.4	SolidOS™
IPv6 Certified	No	No	Yes
BIND version	9.2.3	9.3.1	9.4.1
Throughput per interface**	23,000	20,000	32,000
High Availability	Yes	Yes	Yes
Client Software	Java Client	Java Client	Web-based, MMC, CLI, API
Internationalization	No	No	Yes
User Administration	Yes	Yes	Yes
DHCPv6	No	Yes	Yes

* SolidDNS™ is also offered as a sofpliance and a virtualized version.

** Peak Queries Per Second



Summary

- SolidDNS provides two key infrastructure components (DNS and DHCP) for IPv4-only, dual stack, or IPv6-only networks.
- We are the only such product to have obtained the prestigious IPv6 Ready certification
- There is no need for expensive UNIX or BIND experts to achieve error free configuration with minimum administrator time. Keep them in reserve for your really demanding administrative tasks.
- With our strong cryptography and PKI support, administration can be done from any node with Internet connectivity to the box, allowing maximum freedom in deployment.
- Our Update Server makes it possible to keep your SolidDNS servers as secure and functional as possible with minimum effort.



Thank You