National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP 800-81r1 Checklist Items and Secure64 Appliance

Secure64 with Signer version 2.0.2, and Authority version 2.4.6
Date created: 04/23/2008
Last modified: 11/09/2009

This document is intended to be a companion piece to NIST Special Publication 800-81r1. NIST SP 800-81r1 contains the text and descriptions of the checklist items listed below, but does not contain full descriptions of other DNS implementations. This supplement is intended to help administrators of these other DNS implementations to meet the checklist items in the Special Publication. Some checklist items in SP 800-81r1 do not apply to DNS server configuration but instead address general zone configuration or network architecture recommendations. These checklist items are listed in the table below, but only for completeness as they do not directly apply to the configuration or operation of a Secure64 DNS deployment.

Secure64 Authority uses NSD as its base code, so many of the checklist items listed below come from the NSD supplement. The Secure64 appliance add additional features with leads to differences in administration over the open source NSD package. These changes will be detailed below when applicable. Many of the OS hardening recommendations would not be applicable the same way as Secure64 uses its SourceT OS to provide system security.

In the table below –
Checklist Item: Refers to the numbered checklist items in the text of NIST SP 800-81r1.
Applicable: Yes if the checklist item applies to the operation of a Secure64 system. No otherwise.
Compliance: Yes if the Secure64 system contains a feature or option that meets the checklist item. No otherwise.
Feature used: The specific feature or configuration option used to meet the checklist item.
Notes: Any other information about the feature or option. Or more information as to why the checklist item is not relevant or why compliance was not met.

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
1 (Section 7.4)	No	N/A		Refer to product documentation when upgrading or installing newer versions of the software.
2 (Section 7.4)	Yes	Yes	Secure64 does provide email/phone support for customers.	NSD forums may be useful for configuration of the name server component, but some solutions may not apply to the version of NSD used in the Secure64 system.
3 (Section 7.4)	Yes	Yes	`hide-version` or `identity` statements in nsd.conf	While in the authdnsadmin role, in nsd.conf "`server:`" block add - `hide-version yes;` -or- `identity <string>;` where

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
				<string> is any text string. See Chapter 3 of the Administration Guide.
4 (Section 7.4)	No	N/A		Depends on network architecture. A Secure64 server would only be part of the architecture.
5 (Section 7.4)	Yes	Yes	In authdnsadmin role and editting the nsd.conf file - Zone statement block with the correct `provide-xfr` and `request-xfr` statements.	A Secure64 system can act as a hidden master, or as a secondary to a hidden master.
6 (Section 7.4)	Yes	No		NSD cannot to multiple views of a single zone. Separate zone names must be used.
7 (Section 8.3)	Yes	Yes	In sysadmin role, Secure64 SourceT OS provides a means to construct rules to limit/allow network communication. In authdnsadmin role: `provide-xfr:` statements in nsd.conf	ACL's and rules can be generated to match various network architecture roles.
8 (Section 8.3)	Yes	Yes	In authdnsadmin role- `key:` statement block in nsd.conf	No TSIG key generation utility, but Secure64 can use sufficiently long secret strings as TSIG "keys"
9 (Section 8.3)	Yes	Yes (See Note)	In authdnsadmin role- `key:` statement block in nsd.conf	nsd.conf file allows for multiple key statement blocks. Tested version (2.02) of Secure64 Signer can only support use of HMAC-MD5, which may not be approved for use in certain organizations. Recent versions suport SHA-1 and SHA-2 family. See Chapter 3 of the Administration Guide.
10 (Section 8.3)	Yes	Yes	Secure64 SourceT OS is role based. The authdnsadmin role controls all the DNS server administration functions, but no other functionality.	All files would be needed and used by the authdnsadmin role. No other role would need access to TSIG key material.
11 (Section 8.3)	No	N/A		Out of band for administration. Depends on the organization's security policy.
12 (Section 8.3)	Yes	Yes	`include:` statement in `key:` statement block. -or- SourceT OS security.	Possible, but Secure64 role based SourceT OS provides lower level security. All files used by the name server are owned by the authdnsadmin role only, no other role can have access to it.

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
13 (Section 8.3)	Yes	Yes	authdnsadmin by default. Provided by SourceT OS	SourceT OS provides role based access to the DNS name server. No need to do separate configuration in nsd.conf file.
14 (Section 8.3)	Yes	Yes (See Note)	`key:` statements and options in `zone:` statement block to identify TSIG key to use.	Secure64 Authority supports the use of TSIG to secure NOTIFY, zone transfer messages and dynamic update. Secure64 does not support TSIG for use with query/response transactions. See Chapter 3 of the Administration Guide.
15 (Section 9.10)	Yes	Yes	none.	If a signed zone is loaded, DNSSEC enabled responses will be sent when the DNSSEC-OK bit is seen in the query. Secure64 Signer Guide Chapter 2 contains information and configuration options for automated DNSSEC operations.
16 (Section 9.10)	Yes	Yes	Secure64 SourceT OS provides security for key material	
17 (Section 9.10)	Yes	Yes (See Note)	Secure64 can be configured to generate keys on demand or have a keypool being generated as a background task.	While generated keys are stored on the active server, the Secure64 appliance is FIPS 140-3 certified as a Hardware Security Module (HSM). Meaning generated keys are adequately protected and may not need to be stored off-line unless specific policy requires it.
18 (Section 10.5)	No	N/A		Zone file management tool is responsible for these items
19 (Section 10.5)	No	N/A		Zone file management tool is responsible for these items
20 (Section 10.5)	No	N/A		Zone file management tool is responsible for these items
21 (Section 10.5)	No	N/A		Zone file management tool is responsible for these items
22 (Section 10.5)	No	N/A		Zone file management tool is responsible for these items
23 (Section 10.5)	No	N/A		Zone file management tool is responsible for these items

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
24 (Section 10.5)	Yes	Yes (See Note)	In nsd.conf file – `dnssec-siglife:` option (global or zone).	Secure64 Signer signature lifetime option covers whole zone, not just DNSKEY RRset. See the Signer Administrator's Guide.
25 (Section 10.5)	Yes	Yes (See Note)	In nsd.conf file – `dnssec-siglife:` option (global or zone).	Secure64 Signer signature lifetime option covers whole zone, not just DNSKEY RRset. See the Signer Administrator's Guide.
26 (Section 10.5)	Yes	Yes (See Note)	In nsd.conf file – `dnssec-nsec-settings:` <OPTOUT> <iterations> <salt> option (global or per zone)	Secure64 Signer does not have a feature to automate changes to the salt value, but values can be changed manually. See the Signer Administrator's Guide.
27 (Section 10.5)	Yes	Yes (See Note)	In nsd.conf file – `dnssec-nsec-settings:` <OPTOUT> <iterations> <salt> option (global or per zone)	Secure64 Signer does not have a feature to automate changes to the iterations value, but values can be changed manually.
28 (Section 11.4)	Yes	Yes	In nsd.conf file - `dnssec-ksk-rollover:` and `dnssec-zsk-rollover:` statements. Options can be per zone or global.	This should be addressed in an organization's security policy and implemented in Secure64 configuration files. Once configured, the system automates ZSK and KSK rollover. See the Signer Administrator's Guide.
29 (Section 11.4)	Yes	Yes	Default operation in DNSSEC automation.	Secure64 systems follow the pre-publish process for ZSK rollover and the dual-signature process for KSK rollover. Manual communication with the parent zone is still required unless parent zone also uses Secure64 systems.
30 (Section 11.4)	Yes	Yes	Default operation in DNSSEC automation.	
31 (Section 11.4)	No	N/A		This should be addressed in an organization's security policy. Secure64 systems do have ability to manually start a key rollover process.
32 (Section 11.4)	No	N/A		This should be addressed in an organization's security policy. Secure64 systems do have utilities to automate KSK rollovers if it is the primary master for the zone.
33 (Section 11.4)	Yes	Yes	In the nsd.conf file - `dnssec-signing-time:`	This should be addressed in an organization's security policy. Secure64 configuration file can be used to implement an automated process for this. See the Signer Administrator's Guide.

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
34 (Section 11.4)	Yes	Yes	Handled by automated signing process.	SOA incrementing can be turned off if necessary for network operation. See Chapter 2 in Secure64 Signer Administration Manual.