

9.1	<code>dnsec-tool.conf</code> Configuration File	93
9.2	<code>keyrec</code> Files	96
9.3	<code>zonuts</code> Rule Files	98
A	Reference	13

- **pfmilter-1. . _dn _ec _ho _to.txt** contains instructions for adding DNSSEC valid

3 General Build Instruction

Most of the tools, perl modules, and libraries described on <http://www.dnsec-tool.org> are easily installed by following the instructions in the **INSTALL** file.

4 DNS Libraries

The DNSSEC-Tools distribution includes two libraries: one that is capable of sending queries to and receiving answers from a DNSSEC-aware resolver and one that is capable of sending queries to and receiving answers from a DNSSEC-unaware resolver.

un

2.1 Installation

Download `endm-il-1.3.3.tar.gz` from `ftp://ftp.endm-il.org/pub/endm-il/`.

This distribution must be unpacked and

3.2 Use

The DNSSEC patch adds a new command line option to *sfilter*: *-s <i>*

3.3 Testing

Start *sfilter* with the above DNSSEC patch applied and start *sendmail* with the appropriate configuration for *sfilter*.

3.3.1 Basic Scenario : DNSSEC Validation of the SPF Record

The following table gives a summary of the basic scenarios. The policy columns show the successful completion result.

Domain	Policy
--------	--------

mechanism	Record Cond
-----------	-------------

- *logwatch* is installed in \$LOGWATCH_DIR (by default this would be */etc/log.d*).

You may edit the *logwatch* config files and scripts to change these names if you ha

name can be whatever you want, but if you use something other than `/var/log/dnsec` or `/var/log/resolver`, you will need to mod

6 DNSSEC Library

.2 val_getaddrinfo() DNSSEC-validated address trans


```
        return 0;
    }
```

ALERT

getho tbyn me

}

NOTES

This version of

.1 *dnstflood*

N

```
--o=STRING
--output-file
```


-L

Include rules that equate live queries of data. Generally, these rules are ones that concentrate on pulling remote DNS data to test; for example, parent/child zone relations.

Your configuration file (e.g., `$HOME/.donut.conf`) may have lines in it that look like this:

```
# change the default minimum number of local NS records from 2 to 1
name: LANS_ULI LE_NS
min_srecords: 1

# change the level of the follow rule from 8 to 5
```


-x Send the *wiff* output in the email message as well as the *wonuts* output.

-t TMPDIR

Store temporary files in TMPDIR.

-i INPUTZ

ma er -l tot -s t

.5 *clean*

keygen

Ensure t

.

AL

Net::DNS::Tool ::keyrec.pm(3)

-ne

This option displays the new `LS` Keys in a *keyrec* file.

-pub

This option displays the published `LS` Keys in a *keyrec* file.

-ob

This option displays the obsolete `LS` Keys in a *keyrec* file. This option must be given if obsolete `LS` Keys are to be displayed.

Record-Attribute Option

These options select subsets of the *keyrecs* chosen by the record-selecti

.11 *ti etrans*

NAMES

timet ans - Conve ts

Example 7: Converting 1814421 seconds into time units

\$ (4

.12 `zonesigner`

NAME

`zonesigner` - Generates encryption keys and signs a DNS zone.

SYNOPSIS

```
zonesigner [options] <zone-file> <zone-out>
```

DESCRIPTION

This script combines into a single command many actions that are required to sign a DNS zone. It generates the required `KS` and `LS` keys, adds the key data to a zone record file, and then

th

zo esi er defaults

Ex

```
keyrec_type      "rsa"
```

8 Supporting Module

Several modules have been developed for DNSSEC-Tools to assist in maintaining DNSSEC-secured domains. These routines manipulate DNSSEC-Tools files, pro-

.1 QW r

.2 son .pm

NAME

Net::DNS::SEC::Tools::conf - DNSSEC tools configuration file routines.

SYNOPSIS

```
use Net::DNS::SEC::Tools::conf;

%dtconf = parseconfi ();
%dtconf = parseconfi ("localzone.keyrec");
```

DESCRIPTION

The DNSSEC tools have a configuration file routine. The routine is called `parseconfi` and it takes an optional argument. The argument is the name of the configuration file. If no argument is given, the routine will use the default configuration file, `localzone.keyrec`.

p r econf(8)(confile)

This routine reads and parses a caller-specified DNSSEC tools configuration file. The parsed contents are put into a hash table, which is returned to the caller. The routine quietly returns if the configuration file does not exist.

3 keyrec.pm

NAME

Net::DNS::SEC::Tools::Keyrec - DNSSEC-Tools *keyrec* file operations

SYNOPSIS

```
use Net::DNS::SEC::Tools::Keyrec;
```

```
Keyrec_read("localzone.Keyrec",&file,"" ! yrec_ 5j 50 1 55 0 55 5
```



F

and *keyrec*

This routine returns a list of the *keyrec* names from the file.

keyrec_read(keyrec_file)

This interface reads the specified *keyrec* file and passes it into a *keyrec* hash table and a file contents array. **keyrec_read()** must be called prior to any of the other **Net::DNS::SEC::Tool::keyrec** calls. If another *keyrec* is already open, then it is saved and closed prior to opening the new *keyrec*.

Upon success, **keyrec_read()** returns the number of *rec*

```
0  if the creatio succeeded
-1 i valid type as ive
```

k

.4 timetrans.pm

NAME

Set:

An empty string is returned if the no seconds count was given or if the seconds count is less than one.

APPENDIX A

timetrans(1)

.5 tooloptions.pm

NAME

`/usr/share/perl5/DNSSEC/Tools/tooloptions` - DNSSEC-Tools option routines.

SYNOPSIS

```

opts_setcsopts(@specopts);

opts_createKrf();

opts_suspend();

opts_restore();

opts_drop();

opts_reset();

```

DESCRIPTION

DNSSEC-Tools supports a set of options common to all the tools in the suite. These options may have defaults set in the `dnsec-tool.conf` configuration file, in a *keyrec* file, from command-line options, or from any combination of the three. In order to enforce a common sequence of option interpretation, all DNSSEC-Tools should use the **tooloption()**

\$keyrec_file Name of the *keyrec* file to be searched.

\$keyrec_name Name of the *keyrec* that is being

If `opt_getkey ()` isn't passed any arguments, it will act as if both `$keyrecfile` and `$keyrec`

9 Data File

A few data files are used by the DNSSEC-Tools components.

These DNSSEC-Tools files are:

dnsec-tool.conf - Configuration file for DNSSEC-Tools programs

keyrec - Key and zone configuration files for DNSSEC-Tools programs

wonuts.rules - Rule definition files for *wonuts*.

This section contains man pages describing these commands.

keygen

The path to

9.3 *donuts* Rule Files

NAME

`donuts Rules Files` - Define donuts DNS record-checking rules

DESCRIPTION

This class wraps around a

of test, such as “DNSSEC”. The better-named the rules, the more powerful the user will have for selecting certain types of rules via *bonuts -i* and

```
name: DNSSEC_ES_SO E_SECURE_FEATURE
ruletype: record
```

type

Rules that

There are two types of

ALERT

donut ()

Net::DNS, Net::DNS::RR

<http://dnsec-tool> .

t

et

