

NAME

reconfigure - reconfigure firewall subsystems

SYNOPSIS

reconfigure [*subsystem*]

DESCRIPTION

The TUNIX firewall is configured through a small set of high-level configuration files that, at some point, must be translated into the low-level configuration files that the operating system uses. This is primarily what `reconfigure` does.

`reconfigure` activates the configuration changes on the firewall and can be used to either reconfigure all subsystems at once or individual subsystems separately.

The following *subsystem* names are recognized:

named

Reconfigures all DNS subsystems, i.e. the *extended* DNS configuration tables from the `FW_I_XXX_...` variables in `config.root(5)` and from the `config.named(5)` files, the *simple* DNS configuration tables from the `FW_NAMED_{INT,EXT}_...` variables in `config.root(5)`, and the resolver configuration.

mail

Reconfigures the mail subsystem and is typically used after making changes to `FW_MAILPLUG_TO` or to the mapper file `config.mailmap(5)`.

logger

Reconfigures the logging subsystem and is typically used after making changes to the configuration file `config.logger(5)`.

services

Reconfigures the type and number of available services on the firewall, reconfigures all low-level files needed by the proxy servers (proxies), stops or starts daemons, and will pay attention to the actual client classes in `config.oper(5)`. This is typically used after you've made changes to client classes in the file `config.oper(5)`, after modifying the `config.txp2(5)` configuration file, or after modifying the `FW_SERVICES` variable in `config.root(5)`. Reconfigure services is also necessary after updates of the authentication database.

checksys

Reconfigures the `checksys` subsystem. This is hardly ever used, because the `checksys` subsystem has no high-level configuration file that the firewall administrator maintains.

cron

Reconfigures the actions that influence the periodic actions started through `cron`. This is typically used after modifying the `config.crontab(5)` file. It is also required if the mailbox addresses (`FW_MAILOPER`) of firewall administrators who receive the logging and alerting messages have changed.

all

This reconfigures all basic subsystems in the correct order: `named`, `mail`, `logger`, `services`, `checksys`, and `cron`. This is also the default action if `reconfigure` is called without an argument.

tftp

This special reconfigure command enables TFTP on the firewall if the `tftp(7)` package is installed. TFTP is typically enabled by the firewall administrator to upload router configuration files or to download new OS images in the router. Make sure to *disable* TFTP by running `reconfigure services` immediately after completing your work, because an active TFTP server poses a security risk.

SEE ALSO

The TUNIX Firewall Manual, `config.crontab(5)`, `config.logger(5)`, `config.mailmap(5)`, `config.named(5)`, `config.oper(5)`, `config.root(5)`, `config.txp2(5)`.

BUGS

Please report bugs to fwsupport@tunix.nl.

AUTHOR

Copyright 1999-2003 TUNIX Internet Security & Opleidingen

VERSION

Version \$Revision: 1.6 \$ \$Date: 2003/05/16 13:54:32 \$ (\$Name: ROOT_12 \$)