NAME

rapolicy – compare a **argus(8)** data file/stream against a Cisco Access Control List.

SYNOPSIS

rapolicy -r *argus-file [***raoptions***] [-- filter-expression]*

DESCRIPTION

Rapolicy reads **argus** data from an *argus-file* list, and tests the argus data stream against a Cisco access control list configuration file **Rapolicy** can do many things as defined by its configuration file. The configuration file in not optional and the example below is well commented. The ACL file is specified in the configuration file.

OPTIONS

Rapolicy, like all **ra** based clients, supports a large number of options. Options that have specific meaning to **rapolicy** are:

-f <rapolicy configuration file> defines the actions of the client.
-D 3 Print the output of the state event machine.

See **ra(1)** for a complete description of **ra options**.

EXAMPLE INVOCATION

rapolicy -f rapolicy.conf -r argus.file

CISCO ACL SYNTAX

Rapolicy handles both standard and extended, numbered and named Cisco Access Control Lists

EXAMPLE CONFIGURATION

This example is provided as an example only.

```
#
#  Argus Software
#  Copyright (c) 2000-2014 QoSient, LLC
#  All rights reserved.
#
#  This program is free software; you can redistribute it and/or modify
#  it under the terms of the GNU General Public License as published by
#  the Free Software Foundation; either version 2, or (at your option)
#  any later version.
#
#  This program is distributed in the hope that it will be useful,
#  but WITHOUT ANY WARRANTY; without even the implied warranty of
#  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#  GNU General Public License for more details.
#
#  You should have received a copy of the GNU General Public License
#  along with this program; if not, write to the Free Software
#  Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.
#
#
# Example rapolicy.conf
#
# Rapolicy, like most ra* programs, can read a program specific
# configuration file.  This is an example configuration for rapolicy()
# that provides the opportunity to modify the default behavior of
# parsing a Cisco ACL definition, and reporting on flows that match
# aspects of the policy defined by the ACL.
```

```
#
# This file is read by rapolicy() from the command line using the
# " -f rapolicy.conf " option.
#
# RA_POLICY_DUMP_POLICY is a debugging aid. If it is set to yes, then rapolicy() will read
# and parse the ACL file and output an English language description of the actions associated
# with each ACL entry. After outputting the explaination, rapolicy will exit.

RA_POLICY_DUMP_POLICY="yes"

# The rapolicy client parses a Cisco IOS ACL and constructs a filter which is used
# to permit or deny flows. Under normal circumstances the packets meeting the
# criteria for a permit rule are output by the client. There are circumstances where
# it is useful to see the flows that are dropped. RA_POLICY_SHOW_WHICH can be set
# to a value of "deny" in these cases.

RA_POLICY_SHOW_WHICH="permit"

# Under normal operating conditions, only the flow records that match a permit
# or a deny rule (depending on the value of RA_POLICY_SHOW_WHICH) are output. In
# some instance like baselining the actions of an ACL, the goal is to have a fully
# labeled set of flows regardless of the ACL's permit or deny determination. In these
# instances, a value of yes for RA_POLICY_JUST_LABEL will allow the full processing of
# the flows and will label them according to the settings of the label flags but all of
# the flows handled by the ACL will be output

RA_POLICY_JUST_LABEL="no"

# A Cisco IP ACL normally has no impact on non-IP traffic eg: ARP, DDCMP, Slotted-Aloha
# RA_POLICY_PERMIT_OTHERS can be set to "yes" for the normal behavior or "no" to block
# non-IP traffic

RA_POLICY_PERMIT_OTHERS="yes"


# The rapolicy client can add a label to a flow indicating the action (permit, deny,
# or implictDeny), the ACL name or number) and the line within the ACL that caused the
# action.
#
# if RA_POLICY_LABEL_LOG is set to "yes" labels will be added to flows matching ACL
# entries that have a log qualifier.

RA_POLICY_LABEL_LOG="no"

# If RA_POLICY_LABEL_ALL is set to "yes" regardless of the value of RA_POLICY_LABEL_LOG,
# any flow that matches an ACL entry will be labeled

RA_POLICY_LABEL_ALL="no"

# Every Cisos IOS ACL has an implicit deny as its last entry. Flows that do not match any
# ACL entry are usually dropped silently. RA_POLICY_LABEL_IMPLICIT will label flows that
# are dropped by the implicit deny rule. Under normal circumstances, these flows are not
# labeled. The values of RA_POLICY_LABEL_ALL and RA_POLICY_LABEL_LOG do not govern the
# labeling of these flows.
```

```
RA_POLICY_LABEL_IMPLICIT="no"

# The ACL is contained in a standard ASCII text file which is identified by the value of
# RA_POLICY_ACL_FILE Since rapolicy is not designed to be a syntax checker, it is a
# good idea to create the ACL on a Cisco device and take the output of show running
# (or the appropriate equivalent command) as the input ACL for rapolicy()
# The policy file should be defined as the last item in the rapolicy.conf file
# or there may be unexpected side effects

RA_POLICY_ACL_FILE="/tmp/ACL03.txt"
```

COPYRIGHT

AUTHORS

Carter Bullard (carter@qosient.com).
David Edelman (dwedelman@acm.org)

SEE ALSO

ra(1), **rarc**(5), **argus**(8)