NCAT, RAT, and Config Parsing

by Bryce L. Meyer
(with help)

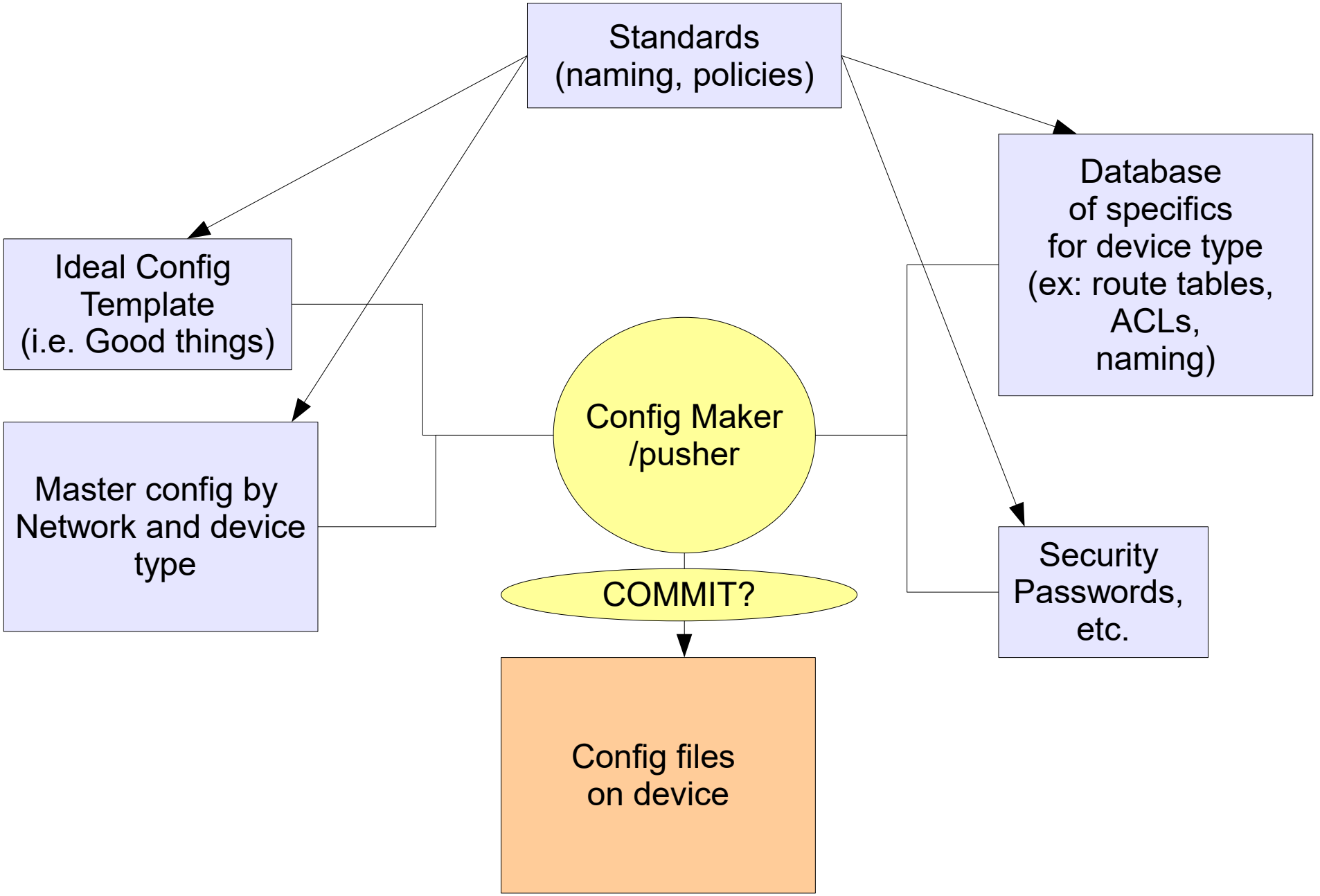
for St. Louis Unix Users Group (SLUUG)

08 June 2016

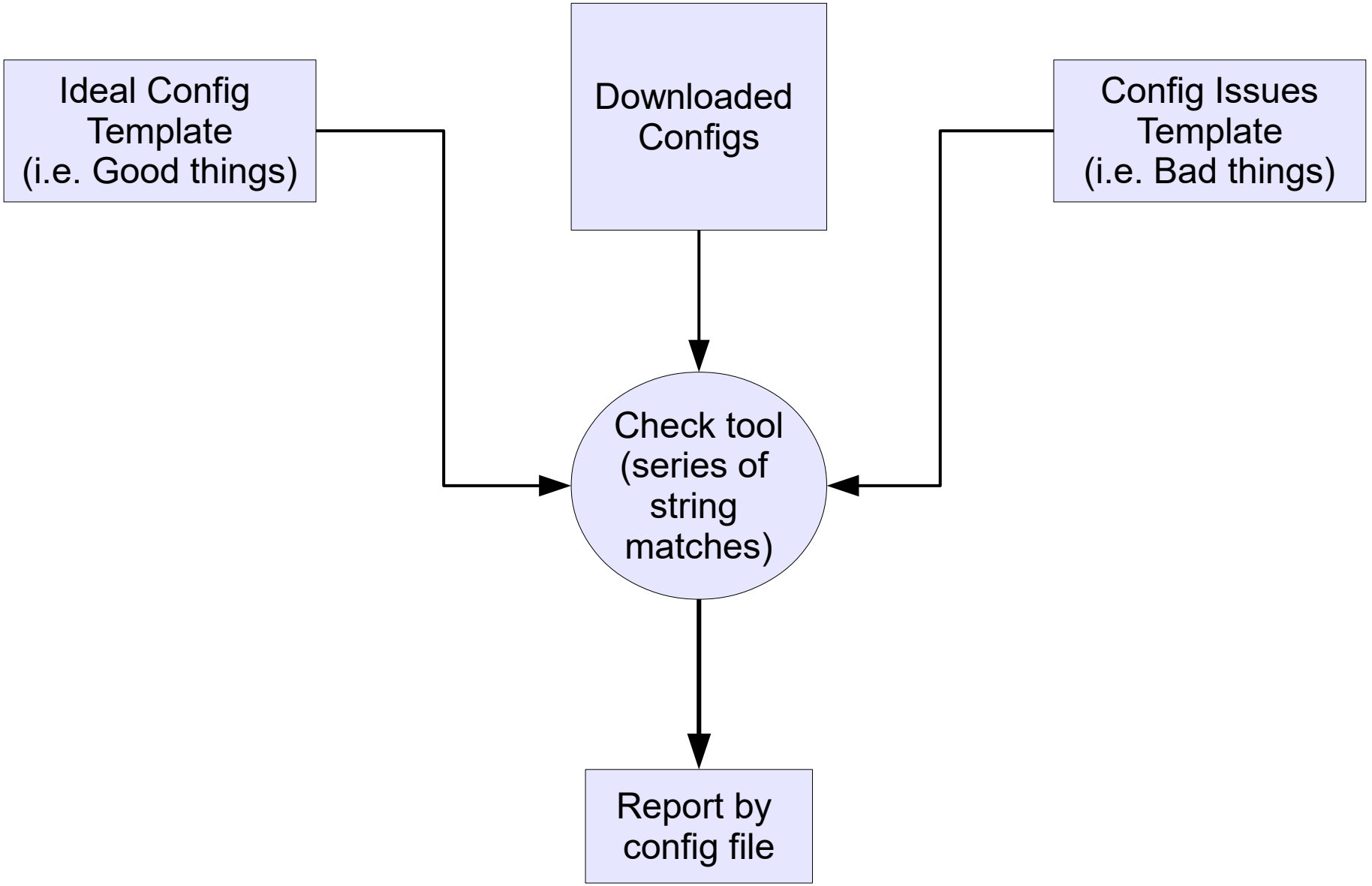
Outline

- Ideal World of Config Creation and Checking
- Center for Internet Security and history
- RAT and NCAT
- Tricks in use

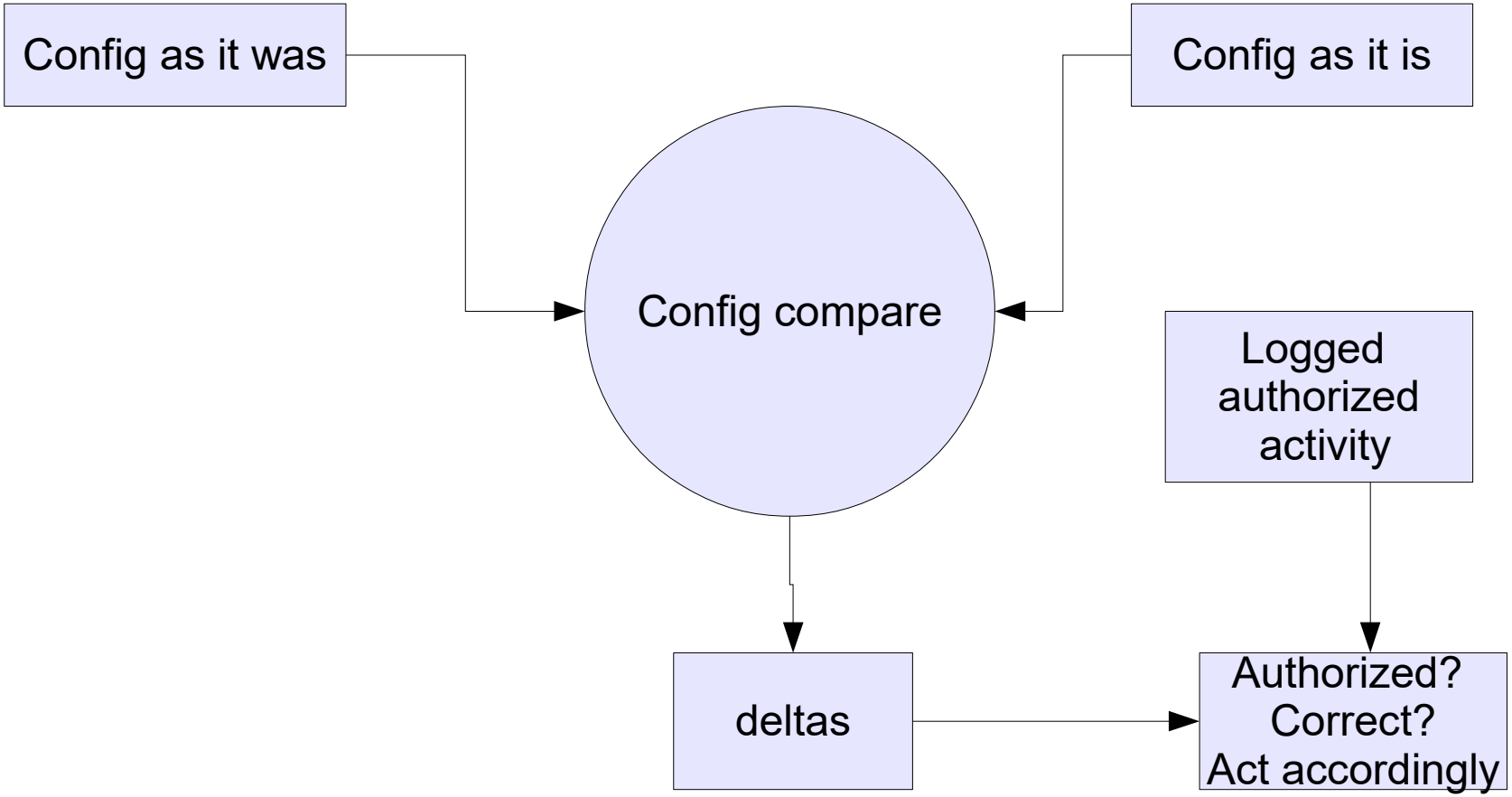
Config make theory



Config Check Theory



Config Comparsion/Control



CIS
Center for Internet Security

- A coalition of groups to secure networks and servers for mostly commercial use, especially paycard, banks, etc.
- Pay to join, though some items are free for trial use.
- Partnered with NSA, FBI, and CERT https://www.cisecurity.org/
- Makes/Controls: Multi-State Information Sharing and Analysis Center (MS-ISAC), CIS Security Benchmarks, and CIS Critical Security Controls

MISSION:

- Identify, develop, validate, promote, and sustain best practices in cybersecurity;
- Deliver world-class security solutions to prevent and rapidly respond to cyber incidents; and
- Build and lead communities to enable an environment of trust in cyberspace

See PDF

NCAT+RAT

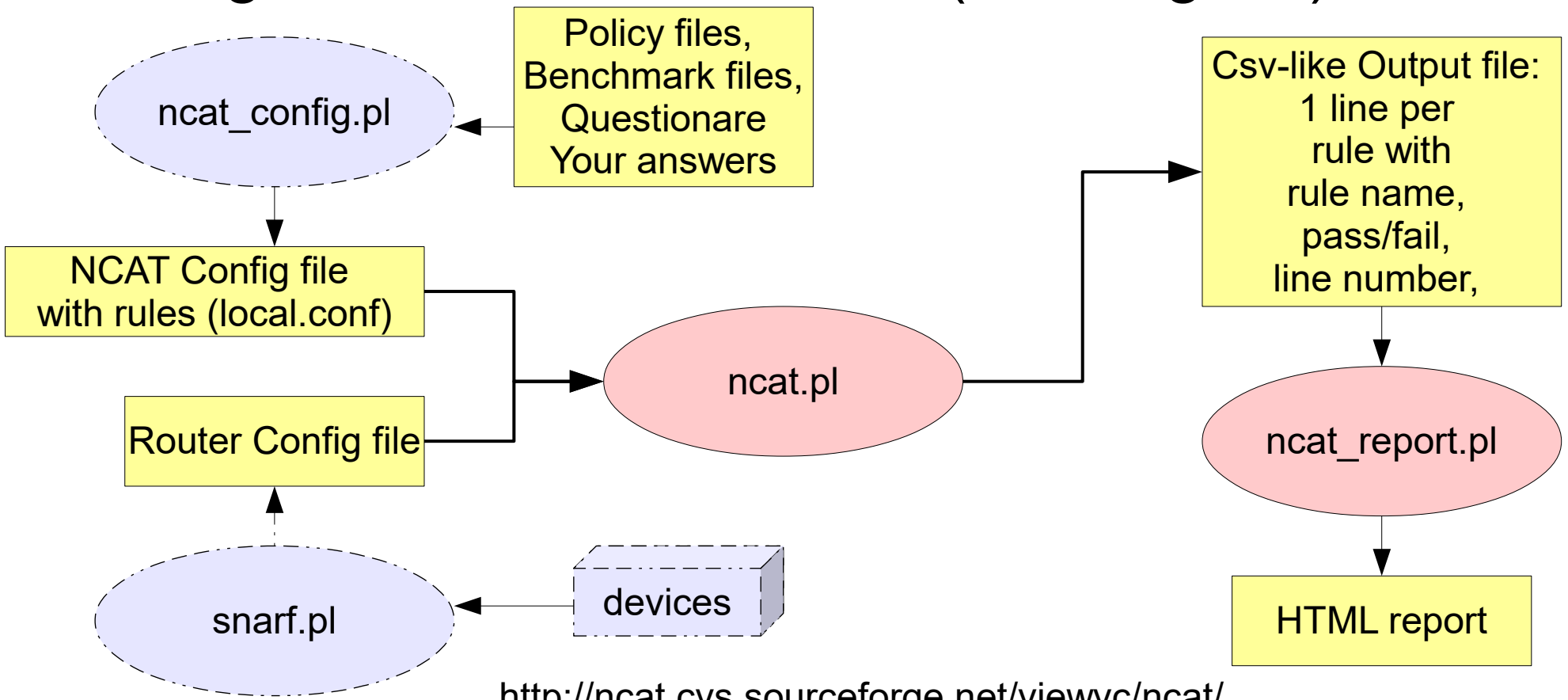
Network Config Audit Tool, Router Auditing Tool:

- Created by George M. Jones (CIS) +team in 2001-2003
- In PERL, can be found here: http://ncat.sourceforge.net/
- CIS license for RAT, copyrighted to CIS
  - V2.2 here: https://community.cisecurity.org/download/?redir=/cisco/rat-2.2-dist.sh.g
- Executables for Windows too.
- Need: A quick and easy way to make sure devices are using the best guidence for configurations and security.

- RAT wraps NCAT
- SNARF can be used to get config files from devices.
- Old versions Sourceforge, CIS has moved on.
- ***NOTE: Tools can be re-purposed to check for many standards/policies/etc!***

NCAT
Network Config Audit Tool

- Performs a tree walk and string pattern match using wildcards of a text file (a config file)



http://ncat.cvs.sourceforge.net/viewvc/ncat/

https://sourceforge.net/projects/ncat/

http://ncat.sourceforge.net/

Rules file overall (local.conf)

- The file has classes, globals
- Classes have classes or rules, parents.
- Rules have match strings, optional use, forbidden or not, importance, parse order, parents.
- Data values can be set in the file, can be tied to rules and classes (i.e. parents).

From NCAT.pl: Config file globals

The following global config fields are defined:

```
%ConfigGlobalFieldNames:ConfigVersion:[\d\.]+
%ConfigGlobalFieldNames:ConfigOrganization:.*
%ConfigGlobalFieldNames:ConfigDocumentType:.*
%ConfigGlobalFieldNames:ConfigPlatforms:.*
%ConfigGlobalFieldNames:ConfigFeedbackTo:.*
%ConfigGlobalFieldNames:ConfigIntroText:.*
%ConfigGlobalFieldNames:ConfigTrailingtext:.*
%ConfigGlobalFieldNames:ConfigRulesAlias:.*
%ConfigGlobalFieldNames:ConfigOutputGroups:.*
%ConfigGlobalFieldNames:ConfigGlobalParseOrder:\d+
```

```
ConfigVersion:1.9.0
ConfigOrganization:Center for Internet Security
ConfigDocumentType:Benchmark
ConfigPlatforms:Cisco IOS Routers
ConfigFeedbackTo:rat-feedback@cisecurity.org
ConfigRulesAlias:cisco-ios-benchmark.html
```

From NCAT.pl config classes

A class is simply an instance of a "Configuration Object" with no additional attributes. Configuration Objects are hierarchical objects used to represent rules, data objects and, in this case, abstract classes. This allows classes, rules and data objects to be organized in any way that makes sense. All config objects have at least the following fields. The descriptions will not be repeated.

The following Configuration Class fields are defined

```
%ConfigClassFieldNames:ConfigClassName:\w[\w\s\-]+
%ConfigClassFieldNames:ConfigClassDescription:.*
%ConfigClassFieldNames:ConfigClassParentName:[\w\s\-,]*
%ConfigClassFieldNames:ConfigClassChildrenNeeded:[\w\s,\-]*
%ConfigClassFieldNames:ConfigClassConflictsWith:[\w\s,\-]*
%ConfigClassFieldNames:ConfigClassQuestion:.*
%ConfigClassFieldNames:ConfigClassAsked:\d
%ConfigClassFieldNames:ConfigClassOptional:([Yy][Ee][Ss]|[Nn][Oo])
%ConfigClassFieldNames:ConfigClassSelected:([Yy][Ee][Ss]|[Nn][Oo])
%ConfigClassFieldNames:ConfigClassParseOrder:\d+
```

From NCAT.pl config classes examples

ConfigClassName:GMT Rules
ConfigClassParentName:**Logging Rules Level 1**
ConfigClassConflictsWith:Localtime Rules
ConfigClassQuestion:Use GMT for logging instead of localtime
ConfigClassSelected:Yes
ConfigClassDescription:\
  Use GMT for logging, etc. Not compatible with localtime.\
  This should be selected if you manage devices in several timezones

From NCAT.pl: Config Rules

A ConfigRule is a configuration object that describes a rule to be checked.

The following rule fields are defined:

```
    %ConfigRuleFieldNames:ConfigRuleName:\w[\w\s\-]+
    %ConfigRuleFieldNames:ConfigRuleDescription:.*
    %ConfigRuleFieldNames:ConfigRuleParentName:[\w\s\-,]*
    %ConfigRuleFieldNames:ConfigRuleChildrenNeeded:[\w\s,\-]*
    %ConfigRuleFieldNames:ConfigRuleConflictsWith:[\w\s,\-]*
    %ConfigRuleFieldNames:ConfigRuleQuestion:.*
    %ConfigRuleFieldNames:ConfigRuleAsked:\d
    %ConfigRuleFieldNames:ConfigRuleOptional:([Yy][Ee][Ss]|[Nn][Oo])
    %ConfigRuleFieldNames:ConfigRuleSelected:([Yy][Ee][Ss]|[Nn][Oo])
    # Unique to Rule
    %ConfigRuleFieldNames:ConfigRuleVersion:.*
    %ConfigRuleFieldNames:ConfigRuleContext:(IOSGlobal|IOSInterface|IOSLine|IOSSNMPCommunity|
IOSLocalUser|IOSTunnelNumber|IOSLoopbackNumber|IOSTFTPServer)
    %ConfigRuleFieldNames:ConfigRuleInstance:.*
    %ConfigRuleFieldNames:ConfigRuleType:(Required|Forbidden)
    %ConfigRuleFieldNames:ConfigRuleMatch:.*
    %ConfigRuleFieldNames:ConfigRuleCallout:.*
    %ConfigRuleFieldNames:ConfigRuleImportance:\d+
    %ConfigRuleFieldNames:ConfigRuleReason:.*
    %ConfigRuleFieldNames:ConfigRuleWarning:.*
    %ConfigRuleFieldNames:ConfigRuleDiscussion:.*
    %ConfigRuleFieldNames:ConfigRuleFix:.*
    %ConfigRuleFieldNames:ConfigRuleParseOrder:\d+
```

Rule Example: from NCAT.pl

ConfigRuleName:IOS 12 - no directed broadca
ConfigRuleParentName:**Routing Rules**
ConfigRuleVersion:version 12\.*
ConfigRuleContext:IOSInterface
ConfigRuleInstance:**.***
ConfigRuleType:**Forbidden**
ConfigRuleMatch:**<code>^ ip directed-broadcast</code>**
ConfigRuleImportance:7
ConfigRuleDescription:Disallow IP directed broadcast on each
ConfigRuleReason:Router interfaces that allow directed broadca
attacks.
ConfigRuleDiscussion:See <rscg>page75</rscg> for more information.
ConfigRuleQuestion:Forbid directed broadcasts (on IOS 12)
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:**<code>router(config)# <cmd>interface <param>INSTANCE</param></cmd>**
router(config-if)# <cmd>no ip directed-broadcast</cmd>
router(config-if)# <cmd>exit</cmd></code>

REGEX:
Anywhere,
Any instance

If it sees this, it is bad

Between
the <code> tags
is the thing to match,
^ is REGEX
(so if it said 'no ip broadcast',
this rule is a pass,
If it just said 'ip broadcast'
it fails (Forbidden)

Yes, check for it,
yes it must be graded

Tells you how to fix it

From NCAT.pl: Config Data

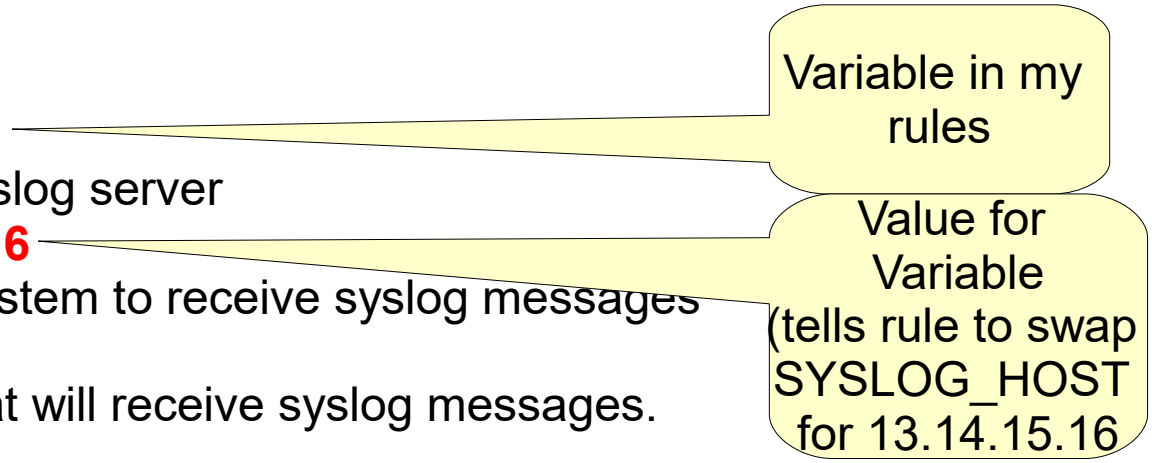
ConfigData is a configuration object that describes data needed.

The following data fields are defined:

```
%ConfigDataFieldNames:ConfigDataName:\w[\w\s\-]+
%ConfigDataFieldNames:ConfigDataDescription:.*
%ConfigDataFieldNames:ConfigDataParentName:[\w\s\-,]*
%ConfigDataFieldNames:ConfigDataChildrenNeeded:[\w\s,\-]*
%ConfigDataFieldNames:ConfigDataConflictsWith:[\w\s,\-]*
%ConfigDataFieldNames:ConfigDataQuestion:.*
%ConfigDataFieldNames:ConfigDataAsked:\d
%ConfigDataFieldNames:ConfigDataOptional:([Yy][Ee][Ss]|[Nn][Oo])
%ConfigDataFieldNames:ConfigDataSelected:([Yy][Ee][Ss]|[Nn][Oo])
# Unique to Data
%ConfigDataFieldNames:ConfigDataHowToGet:.*
%ConfigDataFieldNames:ConfigDataDefaultValue:.*
%ConfigDataFieldNames:ConfigDataParseOrder:\d+
```

From NCAT.pl: Config Data Example

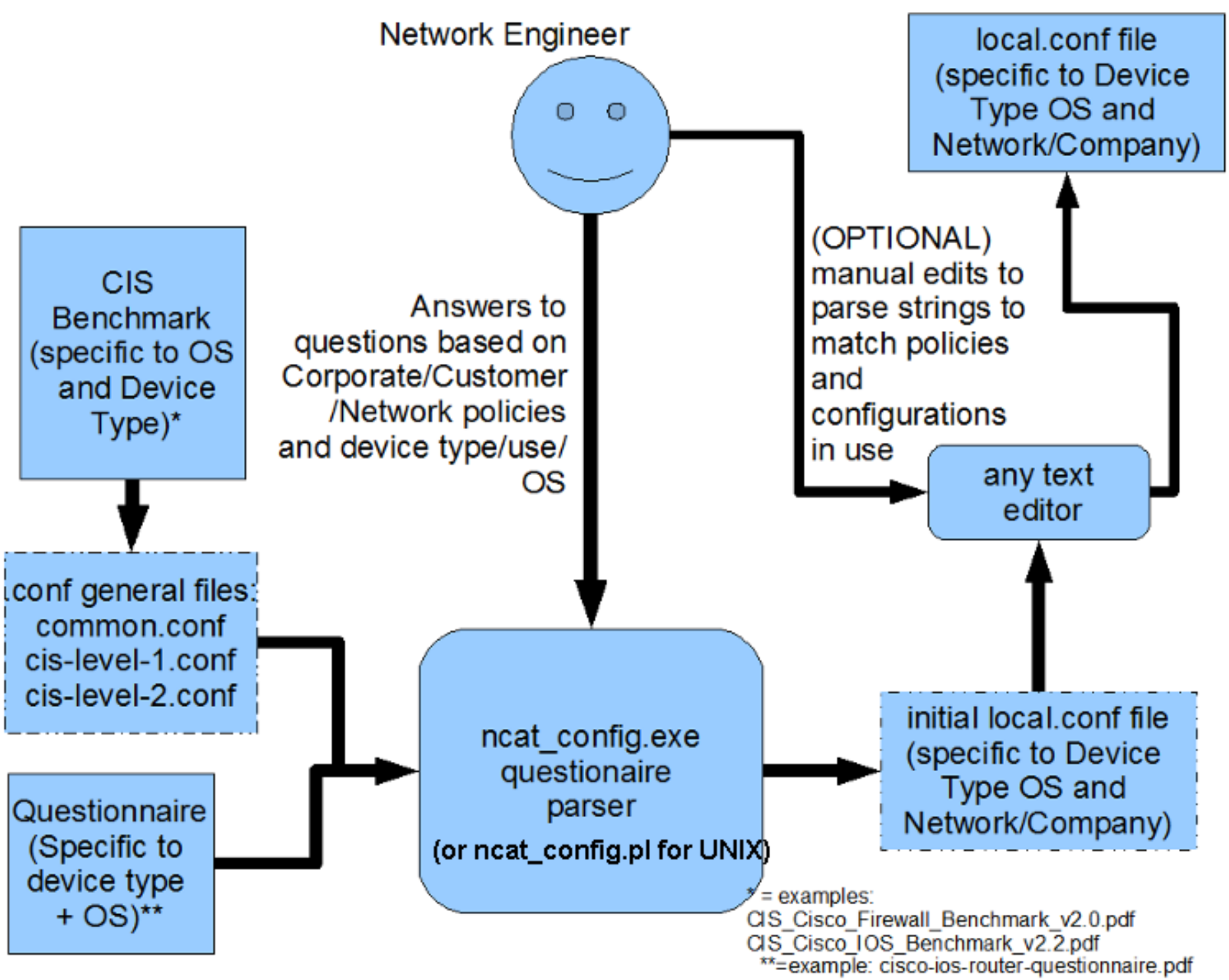
ConfigDataName:**SYSLOG_HOST**
ConfigDataQuestion:Address of syslog server
ConfigDataDefaultValue:**13.14.15.16**
ConfigDataHowToGet:Choose a system to receive syslog messages
ConfigDataDescription:\
  The IP address of this system that will receive syslog messages.



```
ConfigVersion:2.2
ConfigOrganization:Center for Internet Security
ConfigDocumentType:Draft Benchmark
ConfigPlatforms:Cisco PIX Firewalls

ConfigFeedbackTo:rat-feedback@cisecurity.org

ConfigRulesAlias:cisco-pix-benchmark.html

configintrotext:\

<h2>Introduction</h2>\

<BLOCKQUOTE>\
This file lists rules that were used by the \
<a href=http://www.cisecurity.org/bench_cisco.html>PIX-Router Audit Tool</a>,\
a free tool for checking security configurations of Cisco PIX Firewalls\
published by \
<a href=http://www.cisecurity.org>The Center for Internet Security (CIS)</a>.\
<p>\
This file is automatically generated each time the PIX-Router Audit Tool\
is run and may reflect local configuration of the rules.\
<p>\
For a full description of the rules defined by the CIS\
benchmark, see the  benchmark\
document which is distributed with the PIX-Router Audit Tool.\
</BLOCKQUOTE>
ConfigTrailingText:Send feedback about the PIX-Router Audit To
ConfigClassName:Selectable
ConfigClassDescription:Root class for all selectable classes/rules/data
ConfigClassParentname:root node
ConfigClassQuestion:Apply some or all of the rules that are selectable
ConfigClassOptional:No
ConfigClassSelected:Yes
ConfigClassParseOrder:7

ConfigClassName:CIS Level 1
ConfigClassDescription:CIS Level 1 Config Class is the root for all Level 1
ConfigClassParentname:Selectable
ConfigClassQuestion:Apply some or all of CIS level 1 rules
ConfigClassOptional:yes
ConfigClassSelected:yes
ConfigClassParseOrder:16

ConfigClassName:PIX Group - Management Plane Level 1
ConfigClassDescription: Services, settings, and data streams related to\
      setting up and examining the static configuration of the PIX device, \
    and the authentication and authorization of PIX \
      administrators. Examples of management plane services include:\
      administrative telnet or ssh, SNMP, TFTP for image file upload, \
    and authentication protocols like RADIUS and TACACS+.
ConfigClassParentname:CIS Level 1
ConfigClassQuestion:Check rules and data related to system management
ConfigClassOptional:no
ConfigClassSelected:Yes
ConfigClassParseOrder:17

ConfigClassName:PIX Group - SNMP Rules
ConfigClassDescription:Disable SNMP and check for common mis-configurations.
ConfigClassParentname:PIX Group - Management Plane Level 1
ConfigClassQuestion:Apply standard SNMP checks
ConfigClassOptional:no
ConfigClassSelected:Yes
ConfigClassParseOrder:27

ConfigRuleName:PIX Rule - no snmp-server
ConfigRuleDescription:Disable SNMP if not in use.
ConfigRuleParentname:PIX Group - SNMP Rules
ConfigRuleQuestion:Disable snmp-server
ConfigRuleOptional:yes
ConfigRuleSelected:no
ConfigRuleParseOrder:35
ConfigRuleVersion:PIX Version 6\.[123]
ConfigRuleContext:PIXGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>^snmp-server</code>
ConfigRuleImportance:10
ConfigRuleReason: SNMP allows remote monitoring of the PIX device.  Older \
version of the protocol do not use any encryption for the community \
strings (passwords).  SNMP should be disabled unless you intend to use it.
ConfigRuleDiscussion:See <a href="http://www.cisco.com/">PIX Command Reference,
Chapter 8</a> for more information.
ConfigRuleFix:<code>pix(config)# <cmd>no snmp-server</cmd></code>
```

ncat_config.pl

- http://ncat.cvs.sourceforge.net
- Makes NCAT config files for a local use from a questionaire and policy files
- Optional: You can also directly create the config files (they are easy to edit).


Network Engineer
local.conf file (specific to Device Type OS and Network/Company)
CIS Benchmark (specific to OS and Device Type)*
Answers to questions based on Corporate/Customer /Network policies and device type/use/ OS
(OPTIONAL) manual edits to parse strings to match policies and configurations in use
any text editor
.conf general files: common.conf cis-level-1.conf cis-level-2.conf
ncat_config.exe questionaire parser
(or ncat_config.pl for UNIX)
initial local.conf file (specific to Device Type OS and Network/Company)
Questionnaire (Specific to device type + OS)**
* = examples:
CIS_Cisco_Firewall_Benchmark_v2.0.pdf
CIS_Cisco_IOS_Benchmark_v2.2.pdf
**=example: cisco-ios-router-questionnaire.pdf

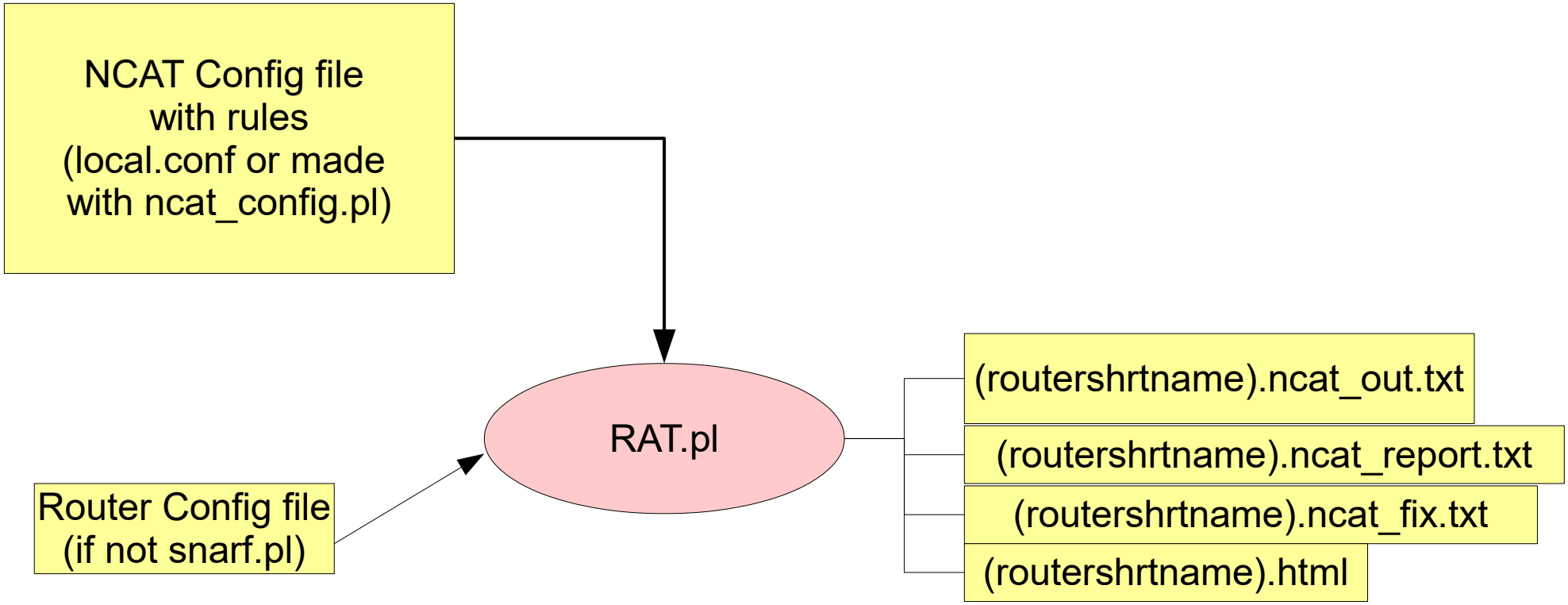
RAT as it was

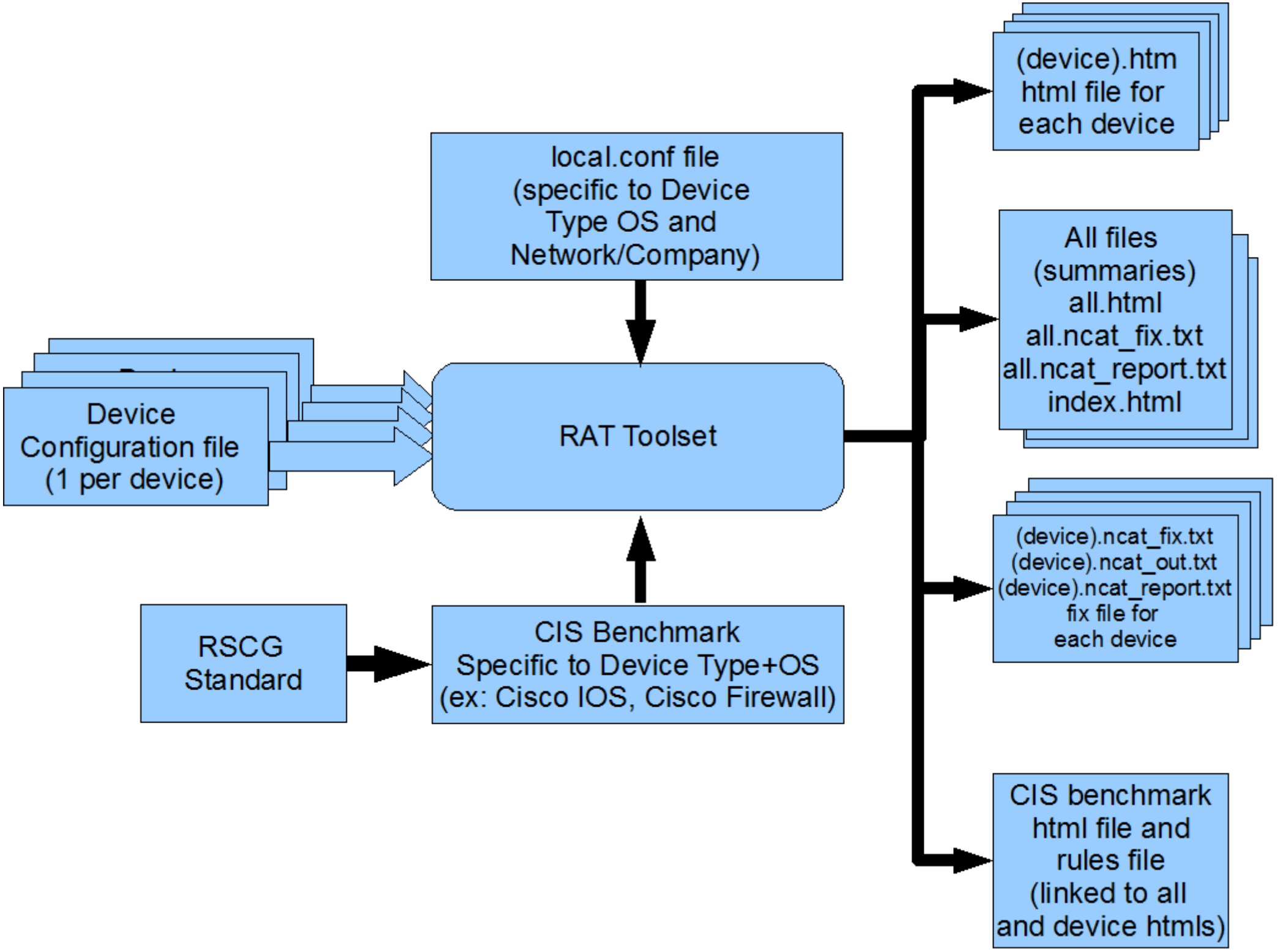
- RAT= Router Assessment Tool
- (see http://ncat.sourceforge.net/RouterAuditTool.ppt)
- Wraps NCAT and uses a CIS + NSA standard

https://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=tools.rat.archive

https://benchmarks.cisecurity.org/downloads/show-single/?file=rat.unix.253

RAT.pl


NCAT Config file
with rules
(local.conf or made
with ncat_config.pl)
Router Config file
(if not snarf.pl)
RAT.pl
(routershrtname).ncat_out.txt
(routershrtname).ncat_report.txt
(routershrtname).ncat_fix.txt
(routershrtname).html


local.conf file
(specific to Device
Type OS and
Network/Company)
Device
Configuration file
(1 per device)
RAT Toolset
(device).htm
html file for
each device
All files
(summaries)
all.html
all.ncat_fix.txt
all.ncat_report.txt
index.html
(device).ncat_fix.txt
(device).ncat_out.txt
(device).ncat_report.txt
fix file for
each device
RSCG
Standard
CIS Benchmark
Specific to Device Type+OS
(ex: Cisco IOS, Cisco Firewall)
CIS benchmark
html file and
rules file
(linked to all
and device htmls)

Practical use

- Build a PERL program to parse output, or use a .bat (win) or shell script
- there are windows.exe versions of each .pl
- Just directly create the rules file (local.conf) for each OS type
- Download your own configs using RANCID or similar (GitHub, etc.)

Competing Tools

- Cisco SDM
- https://www.us-cert.gov/related-resources
  - OVAL via CERT http://oval.mitre.org/
- SolarWinds
  - http://www.solarwinds.com/network-configuration-manager
- Etc..
- (honestly its easy to make a parser, hard to get a list of things to check against).

links

- https://www.cisecurity.org/
- https://www.us-cert.gov/
- http://ncat.sourceforge.net/
- https://benchmarks.cisecurity.org/downloads/browse/
- http://www.cisco.com/c/en/us/products/ios-nx-os-soft
- http://www.cisco.com/c/en/us/support/docs/ip/access
- https://www.iad.gov/
-

BACKUP