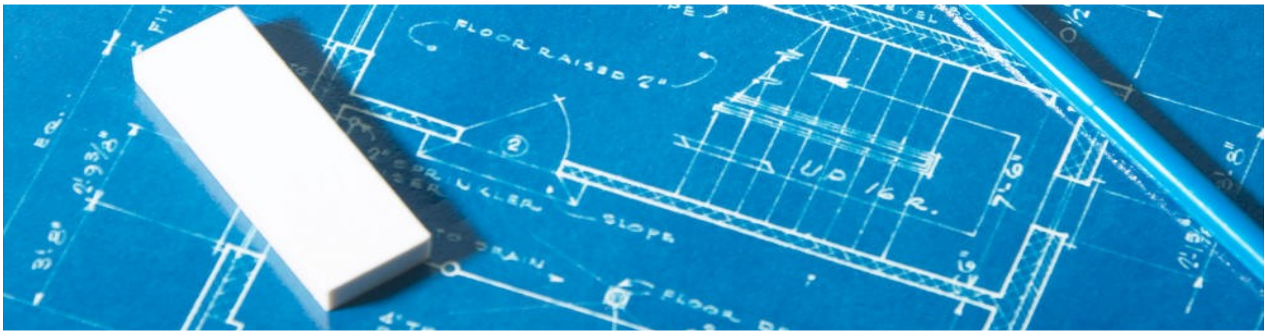
360-FAAR User Guide

360-FAAR / 360-FAAR Enhanced

Examples and Explanations of Options



Purpose of This Document

This documents purpose is to describe how to use 360-FAAR.

Intended Audience

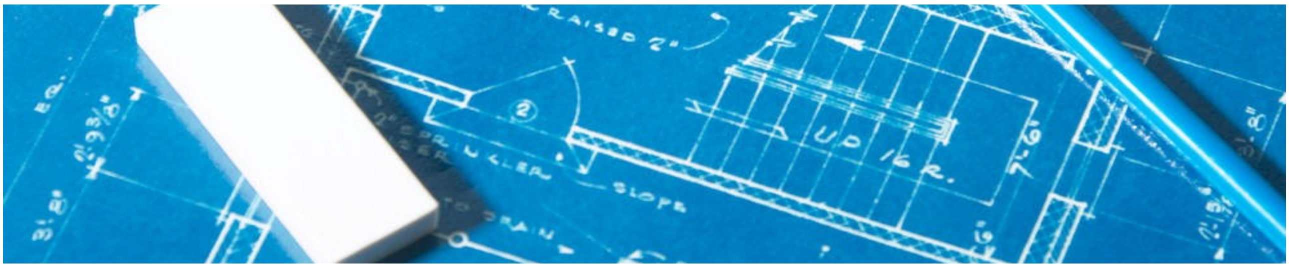
This documents intended audience are technical professionals, technical managers, operations teams, and company directors interested in technologies that offer a distinct advantage over competitors solutions.

About the Author

Dan Martin is the Director of 360 Analytics Ltd. Prior to this, he worked as a Network and Security Analyst/Engineer for fourteen years, employed by companies such as Intel, Nokia Internet Communications, Sun Microsystems, Qualcomm, Verison, Diageo Ltd, Party Gaming Ltd. and 'The Cloud' wifi network.

Table of Contents

End of Contents



Text Conventions Used in this Documentation:

```
Text in mono spaced font indicates terminal output from 360-FAAR
```

`Text in bold mono spaced font indicates user input to 360-FAAR via the terminal`

The text: "360-FAAR ENHANCED" indicates features only available in the ENHANCED version

Text in Times New Roman indicates information about a feature

The text: "NOTE: xxxx" lists useful information

1. System requirements

1.1 *Memory Requirements*

360-FAAR can run with as little as 50MB of memory, but it is recommended that you have at least 2GB of memory available.

1.2 *Drive Space*

360-FAAR requires 4MB of drive space, and enough space to output the 'print' and 'rr' mode text files.

1.3 *Software Requirements*

Perl 5.8 or higher with the Perl Modules: Shellwords and IO::Handle.

1.4 *Terminal Requirements*

Any Linux Terminal application will have the necessary functionality, in Windows a DOS prompt can be used but a bash terminal is recommended. Cygwin's bash terminal works well.

Its also recommended to run 360-FAAR in a 'screen' session and to log the session to a file as an audit trail. 360-FAAR outputs to STDOUT for almost everything so a full record can easily be made.

2. Overview of 360-FAAR

360-FAAR is Perl script that reads firewall configs and log files and then presents an interactive text user interface. From the menu you can choose to output filtered object analysis spreadsheets or process firewall policies and logs to generate new firewall policies. The new policies can be loaded back into 360-FAAR and cross referenced with existing policies using '`rr`' mode, or used as a template for rules to translate to new firewall locations with '`bldobj`' mode.

2.1 360-FAAR Modes

The modes are the options presented in the user interaction loop after the configuration builder has finished loading the configuration and log files. The modes allow a user to output analysis spreadsheets, filter policies, regroup rule connectivity across the whole rulebase or within existing rules, or compare one firewall policy to another regardless of policy type or firewall language.

2.2 'print' Modes

The '`print`' and '`srvcprint`' modes output unfiltered lists of all firewall objects relationships to one another, their sub and supernets, policy usage, log file analysis, inbound and outbound services or networks from the policy as well as log analysis.

The '`fltprint`' and '`fsrvcprint`' modes provide filters to the object analysis output.

2.3 'rr' Mode

The rule rationalisation mode. This mode processes existing rulebases, by examining the policies connectivity profile, merging existing profiles together if required, and comparing these to filter policies, destination configurations, CIDR filters, Text filters, Service and port filters.

An expanded filtered rulebase is printed to STDOUT, if log file analysis is selected, unused connectivity from the policy vs connectivity in the log file, is filtered out of the rule build process.

The rule build subs then wrap connectivity in the largest / smallest groups possible or assigns groups from a hash and then groups similar connectivity profiles together before outputting the new rulebase and the objects and groups needed to build it.

The rulebase can be translated to use matching objects and groups from another existing configuration bundle, and output new rulebases using these objects for installation on the destination firewall in that firewalls native CMD language.

2.4 'bldobj' Mode

Build Objects mode reads firewall rules in odumper CSV format and locates the objects and groups needed to build the rules from three of the loaded configuration bundles before outputting the rulebase and policy objects in the chosen firewalls language.

If a destination configuration is selected source objects and groups are translated to matching objects and groups from the destination configuration preventing duplicate creation.

3. Running 360-FAAR

3.1 *Running 360-FAAR and getting 'help'*

Run the following commands to get help from 360-faar.pl:

```
./360-faar.pl -h
```

Or:

```
./360-faar.pl --help
```

Or:

```
perl 360-faar.pl -h
```

Or:

```
perl 360-faar.pl --help
```

Run the following commands to get help from 360-FAARen.pl:

```
./360-FAARen.pl -h
```

Or:

```
./360-FAARen.pl --help
```

Or:

```
perl 360-FAARen.pl -h
```

Or:

```
perl 360-FAARen.pl --help
```

360-FAAR will output the following help text:

```
./360-faar.pl --help

   ________   _______________           ________________      _____ __________
   \_____  \ /  _____/\   _  \          \_   _____/  _  \    /  _  \\______   \
     _(__  </   __  \ /  /_\  \    ______ |    __)/  /_\  \  /  /_\  \|       _/
    /       \  |__\  \\  \_/   \ /_____/ |     \/    |    \/    |    \    |   \
   /______  /\_____  /  \_____  /         \___  /\____|__  /\____|__  /____|_  /
          \/       \/         \/              \/         \/         \/       \/

=========================================================================================
             360 Analytics Ltd.   Firewall Analysis Audit and Repair
=========================================================================================
                  360-FAAR Copyright (C) 2009-2013  Dan Martin

This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions; see the GPLv3 license.


360-FAARen.pl v0.4.7 Help
---------------------------------------------------------

How to run:
---------------------------------------------------------
./360-faar.pl od=|ns=|cs=config_file[,log_file,nat_file]

eg: to run the TestData files provided in the 360AnalyticsLtd.zip, copy them to the
360-FAAR folder and run:
./360-faar.pl od=TestData.csv od=TestData2.csv od=TestData3.csv

you can cat many log files together, checkpoint and syslog headers are recognised within
the new log file
if you dont have a file, touch (create) a file called fake and use this as a place holder

CONFIG[,LOG,NAT] TYPES SUPPORTED:
---------------------------------------------------------
odumper/ofiller format:          od= (csv format config), (checkpoint logexported logs),
(fwdoc format nats)
  eg: ./360-faar.pl od=configfile.csv
  eg: ./360-faar.pl od=configfile.csv,logexport.log
  eg: ./360-faar.pl od=configfile.csv,logexport.log,fwdocnats.csv

netscreen screenos format:       ns= (screenos6 "get config" format config), (syslog
format netscreen logs), (fwdoc nats (not required but option))
  eq: ./360-faar.pl ns=configfile.txt
  eg: ./360-faar.pl ns=configfile.txt,syslog.txt
  eg: ./360-faar.pl ns=configfile.txt,syslog.txt,fwdocnats.csv

cisco pix or asa format:         cs= (pix asa 8.3+ config), (syslog format pix asa logs),
(fwdoc nats (not required but option))
  eg: ./360-faar.pl cs=configfile.txt
  eg: ./360-faar.pl cs=configfile.txt,syslog.txt
  eg: ./360-faar.pl cs=configfile.txt,syslog.txt,fwdocnats.csv
```

3.2 *Starting 360-FAAR with no configs files loaded – load configs after startup*

Run:
`./360-FAARen.pl`
or:
`perl 360-FAARen.pl`
or:
`./360-faar.pl`
or:
`perl 360-faar.pl`

The program will start and display:

```
   ________  _______________          ________________      _____ __________
   \_____   \ /   _____/\   _   \        \_   _____/  _   \    /  _  \\______   \
    _(__  </   __   \ /  /_\  \  ______ |    __)/  /_\  \  /  /_\  \|       _/
   /       \  |__\  \\  \_/    \ /_____/ |     \/    |    \/    |    \    |   \
   /______  /\______  / \______  /        \___  /\____|__  /\____|__  /____|_  /
          \/        \/         \/             \/         \/         \/       \/

=========================================================================================
             360 Analytics Ltd.   Firewall Analysis Audit and Repair
=========================================================================================
                  360-FAAR Copyright (C) 2009-2013  Dan Martin

This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions; see the GPLv3 license.

No Configs specified at startup: use 'load' mode to create config bundles...



     _                 _    ____             __ _         ___        _
    | |    ___   __ _ __| |  / ___|___  _ _  / _(_)__ _   / _|___    | |    ___   __ _ ___
    | |__/ _ \/ _` / _` | | (__/ _ \ ' \|  _| / _` | > _|_ _|  | |__/ _ \/ _` (_-<
    |____\___/\__,_\__,_|  \___\___/_||_|_| |_\__, | \_____|   |____\___/\__, /__/
                                              |___/                      |___/
-----------------------------------------------------------------------------------------
    SPECIFY A NEW CONFIG BUNDLE TO LOAD:

       Enter the type of the new config to load in the format:
       Odumper/Ofiller Config File      = od
       Netscreen Config File            = ns
       Cisco Config File                = cs
```

You should enter one of the following configuration types:

- Enter '**`od`**' to load a Checkpoint Firewall-1 configuration in odumper format
- Enter '**`ns`**' to load a Juniper Netscreen Firewall configuration in 'get config' format
- Enter '**`cs`**' to load a Cisco ASA Firewall config in 'show run' format.

You will be asked to enter the file name of the configuration:

```
Enter the name of the new config file to load
```

Enter the name of an existing file. For the purpose of the examples in this manual, we are going to load one of the TestData files supplied in the 360AnalyticsLtd Zip file.

Enter one of the Test Data CSV file names:

`TestData.csv`

You will then be asked to enter the name of the log file to analyse the firewall configuration with:

```
Enter the name of the new log file to load, or type '.' to skip
```

The log file should be in the following formats:

• Checkpoint Firewall-1:	logexported text files
• Cisco ASA:	syslog format text files
• Juniper Netscreen:	syslog format text files

Or you can skip this step by typing `'.'` To use the TestData, skip this step.

NOTE: skipping log file loading disables several of 360-FAAR's modes.

The next prompt asks you to enter a valid NAT file for processing:

```
Enter the name of the new nats file to load, or type '.' to skip
```

NAT files can be added in the formats:

- FWDoc CSV format
- FWRules CSV format

Or you can skip this step by typing `'.'` To use the TestData, skip this step.

NOTE: NAT files are optional for Cisco and Netscreen configurations because the NAT config info is included in the main config file its self.

3.3 Starting 360-FAAR with one or more configuration / log / NAT files listed on the command line at startup.

To run 360-FAAR Open Source, enter:

```
./360-faar.pl od=TestData.csv,logfile.txt,natfile.txt
```

To run 360-FAAR Enhanced, enter:

```
./360-FAARen.pl od=TestData.csv,logfile.txt,natfile.txt
```

The prefixes in the format “xx=” are as listed above, as are the formats of the files.

The order of the files is fixed, if you need to load a configuration with a NATs file but no log file you must use an empty file as a place holder e.g:

```
touch fake.txt
./360-FAARen.pl od=TestData.csv,fake.txt,NATs.csv
```

Only the config file name is required, the extra files can be omitted.

For example to load all three TestData files in the 360AnalytisLtd zip run:

```
./360-FAARen.pl od=TestData.csv od=TestData2.csv od=TestData3.csv
```

To load two netscreen configurations, one with a log file, run:

```
./360-FAARen.pl ns=Netscreencfg.txt ns=Netscreencfg2.txt,syslog.txt
```

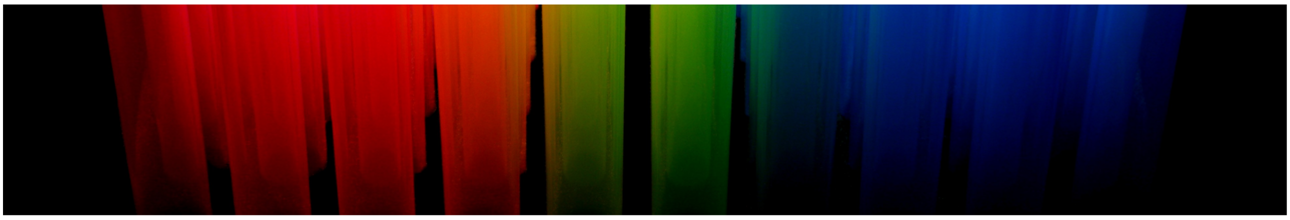
3.4 Configuration Load Output

When 360-FAAR has enough information it will start loading the configuration and output info about the objects and rules it finds, such as incomplete objects, rules or group definitions.

```
./360-faar.pl od=TestData3.csv

   ________  _______________           _________________     _____ __________
   \______  \ /  ______/\   _   \          \_   ______/  _   \    /  _  \\_______  \
     _(__  </   ___  \ /  /_\  \  ______  |     __)/  /_\  \  /  /_\  \|       _/
    /       \  |__\  \\  \_/   \ /______/ |      \/     |    \/     |    \      |   \
   /_______  /\______  / \______  /         \____  /\_____|__  /\_____|__  /_____|_  /
          \/        \/          \/               \/          \/          \/        \/

=========================================================================================
             360 Analytics Ltd.   Firewall Analysis Audit and Repair
=========================================================================================
                  360-FAAR Copyright (C) 2009-2013  Dan Martin

This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions; see the GPLv3 license.

Beginning Analysis of Checkpoint FW-1 Config:
-------------------------------------------------
TestData3.csv...
-------------------------------------------------
FOUND RULEBASE: Test1
FOUND RULEBASE: Test2
  WARNING: UNKNOWN OBJECT Unknown-Nets used as DEST in RULE Test2 no: 30  OBJECT DROPPED
FOUND RULEBASE: GoodTestMergeFrom
  WARNING: UNKNOWN SERVICE gWindows_RDP used as DEST in RULE GoodTestMergeFrom no: 31
PORT ADDED AS TYPE: portunknown
  WARNING: UNKNOWN SERVICE gWindows_RDP used as DEST in RULE GoodTestMergeFrom no: 32
PORT ADDED AS TYPE: portunknown
  WARNING: UNKNOWN SERVICE gWindows_RDP used as DEST in RULE GoodTestMergeFrom no: 33
PORT ADDED AS TYPE: portunknown
FOUND RULEBASE: GoodTestMergeTo
-----------------------------------------------------------------------------------------
 OBJECT, RULE AND BASE GROUP BUILDING COMPLETE:
   network objects processed     = 973
   service objects processed     = 767
   network groups  processed     = 24
   service groups  processed     = 2
   duplicate objects found       = 1
   rules processed        = 40
   rule objects processed = 23
-----------------------------------------------------------------------------------------
 CHECKING BASE LEVEL OBJECT DEFINITIONS:
-----------------------------------------------------------------------------------------
 NETWORK SUBGROUP BUILDING COMPLETE:
   net subgroups found           = 986
-----------------------------------------------------------------------------------------
 RUNNING CONSISTENCY CHECKS ON NETWORK GROUP OBJECTS:
-----------------------------------------------------------------------------------------
 SERVICE SUBGROUP BUILDING COMPLETE:
   service subgroups found       = 0
-----------------------------------------------------------------------------------------
```

```
 RUNNING CONSISTENCY CHECKS ON SERVICE GROUP OBJECTS:
-----------------------------------------------------------------------------------------
 STARTING NETWORK OBJECT TO BINARY IP RESOLUTION:
-----------------------------------------------------------------------------------------
 BINARY IP TO OBJECT NAME RESOLUTION TABLE COMPLETE:
   IP's and networks processed   = 972
   Binary IP groups processed    = 24
   duplicate IP's processed      = 0
-----------------------------------------------------------------------------------------
 RUNNING CONSISTENCY CHECKS ON BINARY IP TO OBJECT AND GROUP NAME TABLE:
   WARNING:  No BINARY IP for    NET_OBJ object:  empty
-----------------------------------------------------------------------------------------
 STARTING SERVICE OBJECT TO PROTO/PORT RESOLUTION:
   S-ALERT:  Large high port range  (64512 ports) in range object "tcp-high-ports"
           Ranges of this size      ^^^  should be considered    INSECURE
   S-ALERT:  Large high port range  (64512 ports) in range object "udp-high-ports"
           Ranges of this size      ^^^  should be considered    INSECURE
-----------------------------------------------------------------------------------------
 PORT TO SERVICE OBJECT NAME RESOLUTION TABLE COMPLETE:
   portgroups processed          = 2
   ICMP ports processed          = 27
   IGMP ports processed          = 0
   TCP  ports processed          = 64907
   UDP  ports processed          = 64709
   RCP  ports processed          = 0
   Protos     processed          = 11
   ICMP port duplicates          = 27
   IGMP port duplicates          = 0
   TCP  port duplicates          = 393
   UDP  port duplicates          = 200
   RCP  port duplicates          = 0
   Protocol  duplicates          = 7
   unknown ports processed= 0
-----------------------------------------------------------------------------------------
 RUNNING CONSISTENCY CHECKS ON PORT TO SERVICE OBJECT NAME TABLE:
-----------------------------------------------------------------------------------------
 STARTING RULEBASE MATCH ANALYSIS:
...................................................250000  matches processed
...................................................500000  matches processed
...................................
-----------------------------------------------------------------------------------------
 BINARY RULE MATCH TABLE COMPLETE:
   src/dst/port matches procssd  = 677993
   derived from rules numbering  = 40
-----------------------------------------------------------------------------------------
 CHECKING BINARY RULE MATCH TABLE:
   WARNING:  Bad PROTO OBJ for   Rule: 31 SRVC object:  gWindows_RDP  proto:
(portunknown) this object will only be matched against its NAME not its PROTO/PORT
   WARNING:  Bad PROTO OBJ for   Rule: 32 SRVC object:  gWindows_RDP  proto:
(portunknown) this object will only be matched against its NAME not its PROTO/PORT
   WARNING:  Bad PROTO OBJ for   Rule: 33 SRVC object:  gWindows_RDP  proto:
(portunknown) this object will only be matched against its NAME not its PROTO/PORT
-----------------------------------------------------------------------------------------
 CHECKING NETWORK AND SERVICE OBJECTS - POST RULE PROCESSING:
   WARNING:  No BINARY IP for    NET_OBJ object:  empty
   WARNING:  Bad PROTO OBJ for   SRVC_OBJ object:  gWindows_RDP  proto: (portunknown)
this object will only be matched against its NAME not its PROTO/PORT
-----------------------------------------------------------------------------------------
 STARTING NAT RULEBASE ANALYSIS:

-----------------------------------------------------------------------------------------
 NAT RULE TABLE BUILD COMPLETE:
   objects processed             = 0
   from rules numbering    = 0
-----------------------------------------------------------------------------------------
 ANALYSIS BUNDLE COMPLETE: TYPE: Checkpoint FW-1 CONFIG: TestData3.csv

-----------------------------------------------------------------------------------------
 STARTING USER INTERACTION LOOP ...hit enter!
```

4. 360-FAAR Menu Options



4.1 User Menu Output

```
   ________   ________________           ________________      ______ __________
   \______ \ /  ______/\  _   \         \_   ______/  _  \    /  _  \\_______  \
     _(__  </   ___ \ /  /_\  \   _______ |   ___)/ /_\  \   / /_\  \|       _/
    /       \  |__\  \\  \_/   \ /______/ |     \/    |    \/    |    \    |   \
   /_______ /\______ / \______ /          \____ /\_____|__ /\_____|__ /_____|_ /
          \/       \/        \/              \/         \/         \/        \/

==========================================================================================
             360 Analytics Ltd.   Firewall Analysis Audit and Repair
==========================================================================================
                  360-FAAR Copyright (C) 2009-2013  Dan Martin

    360-FAAR Enhanced v1.0.0 MENU:
    ------------------------------------

       print    = Prints the 360-FAAR Object Analysis Spreadsheet.

       fltprint = Prints a filtered Object Analysis Spreadshset in the same format as
                  'print' mode.
```

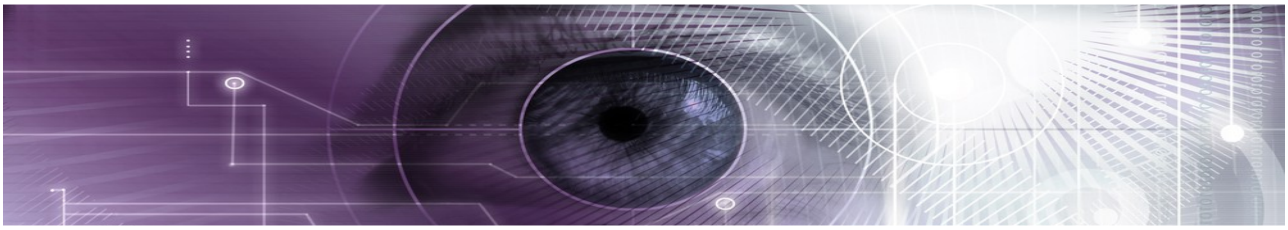
- **360-FAAR ENHANCED: srvcprint**

```
      srvcprint = Prints the 360-FAAR Service Object Analysis Spreadsheet.
```

- **360-FAAR ENHANCED: fsrvcprint**

```
     fsrvcprint = Prints a filtered Service Object Analysis Spreadshset in the same
                  format as 'print' mode.

       rr       = Rationalize Rules and generate new rule bases, or clean/filter existing
                  rules.

       bldobj   = Read rules in odumper/ofiller format and identify objects and
                  groups needed to build them.

       load     = Load a new config bundle.  Loading an existing config name will
                  overwrite the existing config.

       copylog  = Associate an existing log with a different config.  The original
                  log will be over written.

       mergelog = Merge a binary log from one config with another.

       help     = Print help info to screen.

       exit     = EXIT the script.

    ---------------------------------------------------------
    Chose one:
```

5. Print Modes



5.1 Print Mode

The mode 'print' outputs the 360-FAAR Object Analysis Spreadsheet.

The spreadsheet lists all network objects and information relating to their policy usage and log file information.

The spreadsheet outputs each network objects info, its group memberships, supernets, subnets, hosts (if network), policy usage inbound and outbound services as well as connection information from the log files and all comments and section headers from the firewall policies.

Enter an output file name, and choose verbose output. The output file is written as a text CSV.

```
     ---------------------------------------------------------
    Chose one: print

 ___     _     _       _             _         _       __  __         _     
| _ \_ _(_)_ _| |_    /_\  _ _  __ _| |_  _ __(_)___  |  \/  |___  __| |___ 
|  _/ '_| | ' \  _|  / _ \| ' \/ _` | | || (_-< (_-< | |\/| / _ \/ _` / -_)
|_| |_| |_|_||_\__| /_/ \_\_||_\__,_|_|\_, /__/_/__/ |_|  |_\___/\__,_\___|
                                       |__/                                 
------------------------------------------------------------------------------------------
 OUTOUT OBJECTS DETTAILS AND RULE USAGE INFO SPREADSHEET:
------------------------------------------------------------------------------------------


      Enter the name of the spreadsheet you want to print analysis to:

PrintOutput.csv

      Do you want info printed to the screen?
      [yes|no] or type '.' for default (no)

.
      * ADDED Option: no


      Printing TestData2.csv ANALYSIS to FILE: PrintOutput.csv... this may take a few
      minutes


------------------------------------------------------------------------------------------
ANALYSIS FILE: PrintOutput.csv WRITTEN        !!WEHAYY!!!
------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

5.2 Fltprint mode

The 'fltprint' mode outputs the same format spreadsheet as 'print' mode but includes menu options to filter the output using CIDR addresses, and in 360-FAAR Enhanced with Service Names and Port Ranges:

```
    ---------------------------------------------------------
    Chose one: fltprint

  ___ _ _           _       _       _              _         _        __  __          _
 | __| | |_ _ __ _ _(_)_ _ | |_    /_\  _ _  __ _| |_  _ __(_)___  |  \/  |___  __| |___
 | _|| |  _| '_ \ '_| | ' \|  _|  / _ \| ' \/ _` | | || (_-< (_-<  | |\/| / _ \/ _` / -_)
 |_| |_|\__| .__/_| |_|_||_\__| /_/ \_\_||_\__,_|_|\_, /__/_/__/  |_|  |_\___/\__,_\___|
           |_|                                     |__/
-------------------------------------------------------------------------------------------
 OUTOUT OBJECTS DETTAILS AND RULE USAGE INFO SPREADSHEET:
-------------------------------------------------------------------------------------------
```

Filename output:

Enter the name of the file you want to output the CSV to.

```
      Enter the name of the spreadsheet you want to print analysis to:

FilterPrintOutput.csv
```

Verbose output:

Choose if you want verbose info printed to the screen while writing the analysis CSV, or enter '.' for default option ('no' in this case).

```
      Do you want info printed to the screen?
      [yes|no] or type '.' for default (no)

.
      * ADDED Option: no
```

Text Filters:

Enter the text strings to either include or exclude from the output of the analysis.

```
      Enter the TEXT STRINGS (without spaces) that you wish to either include or exclude
       in the format:

      [IN|EX] TEXT_STRING
      Enter '.' when done:

IN TextStringForObjects
.
```

CIDR Filters:

Enter CIDR filters that will either be matched exactly or matched for all subnets, and will be included or excluded accordingly. Exclude over rides Include.

```
      Enter the IP ADDRESS and MASK LENGTH of networks you wish to either include or
       exclude in the format:
      [IN|EX] IP MASKLENGTH
      Enter '.' when done:

IN 10.0.0.0 8
EX 10.0.0.0 18
.
```

Service Filters:

Enter the service names or proto ports or port ranges to either include or exclude.

360-FAAR ENHANCED: Service Filters

```

      Enter the PROTO and PORT (RANGES) you wish to either include or exclude in the
      format:
      Port ranges smaller than 10 ports will added if they have ports in the selected
      range
      [IN|EX] PROTO PORT_FROM-NUM_or_NAME (PORT_TO-NUM <-optional)
      Enter '.' when done

IN tcp ssh
IN tcp 3300 3500
EX tcp 3389
.
```

Filter Precedence:

The 'fltprint' filters are cumulative:

- All INclude filters must be matched
- Any EXclude filter match excludes the objects
- if only EXclude filters are specified in a section all objects not excluded are included.

CSV Output:

Output is then written to the chosen file:

```
      Printing FilterPrintOutput.csv ANALYSIS to FILE: FilterPrintOutput.csv... this may
      take a few minutes


-----------------------------------------------------------------------------------------
ANALYSIS FILE: FilterPrintOutput.csv WRITTEN         !!WEHAYY!!!
-----------------------------------------------------------------------------------------


-----------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

5.3 Srvcprint mode

360-FAAR ENHANCED: Service Print Mode

The mode 'srvcprint' outputs the 360-FAAR Serrvice Object Analysis Spreadsheet.

The spreadsheet lists all service objects and information relating to their network object policy usage and log file information.

The spreadsheet outputs each service objects info, its group memberships, inbound/outbound hosts and networks policy usage as well as connection information from the log files.

The spreadsheet is output as a CSV file.

The following is a 'srvcprint' mode output example:

```
     ----------------------------------------------------------
    Chose one: srvcprint

  ___              _           ___     _      _        _            _         _
 / __| ___ _ ___ _(_)__ ___   | _ \_ _(_)_ _| |_     /_\  _ _  __ _| |_  _ __(_)___
 \__ \/ -_) '_\ V / / _/ -_)  |  _/ '_| | ' \  _|   / _ \| ' \/ _` | | || (_-< (_-<
 |___/\___|_|  \_/|_\__\___|  |_| |_| |_|_||_\__|  /_/ \_\_||_\__,_|_|\_, /__/_/__/
                                                                      |__/
-----------------------------------------------------------------------------------------
 OUTOUT OBJECTS DETTAILS AND RULE USAGE INFO SPREADSHEET:
-----------------------------------------------------------------------------------------


      Enter the name of the spreadsheet you want to print analysis to:

ServicePrintOutput.csv

      Do you want info printed to the screen?
      [yes|no] or type '.' for default (no)

.
      * ADDED Option: no


      Printing TestData2.csv ANALYSIS to FILE: ServicePrintOutput.csv ... this may take
      a few minutes


-----------------------------------------------------------------------------------------
ANALYSIS FILE: ServicePrintOutput.csv WRITTEN       !!WEHAYY!!!
-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

5.4 Fsrvcprint mode

- **360-FAAR ENHANCED: Filter Service Print Mode**

The 'fsrvcprint' mode outputs the same format spreadsheet as 'srvcprint' mode but includes menu options to filter the output using CIDR addresses, and in 360-FAAR Enhanced with Service Names and Port Ranges:

```
   ---------------------------------------------------------
   Chose one: fsrvcprint

  ___              ___ _ _   ___     _      _       _             _         _
 / __|_ ___ _____  | __| | |_| _ \_ _(_)_ _| |_    /_\  _ _  __ _| |_  _ __(_)___
 \__ \ '_\ V / _| | _|| |  _|  _/ '_| | ' \  _|  / _ \| ' \/ _` | | || (_-< (_-<
 |___/_|  \_/\__| |_| |_|\__|_| |_| |_|_||_\__| /_/ \_\_||_\__,_|_|\_, /__/_/__/
                                                                    |__/
-----------------------------------------------------------------------------------------
 OUTOUT OBJECTS DETTAILS AND RULE USAGE INFO SPREADSHEET:
-----------------------------------------------------------------------------------------
```

Filename output:

Enter the name of the file you want to output the CSV to.

```
      Enter the name of the spreadsheet you want to print analysis to:

SvcFilterPrintOutput.csv
```

Verbose Output:

Choose if you want verbose info printed to the screen while writing the analysis CSV, or enter '.' for default option ('no' in this case).

```
      Do you want info printed to the screen?
      [yes|no] or type '.' for default (no)

.
      * ADDED Option: no
```

Text Filters:

Enter the text strings to either include or exclude from the output of the analysis.

```
      Enter the TEXT STRINGS (without spaces) that you wish to either include or exclude
       in the format:

      [IN|EX] TEXT_STRING
      Enter '.' when done:

IN TextStringForSrvcObjects
.
```

CIDR Filters:

Enter CIDR filters that will either be matched for all subnets, and will be included or excluded accordingly. Exclude over rides Include.

```
      Enter the IP ADDRESS and MASK LENGTH of networks you wish to either include or
       exclude in the format:
      [IN|EX] IP MASKLENGTH
      Enter '.' when done:

IN 10.0.0.0 8
EX 10.0.0.0 18
.
```

Service / Proto Port Filters:

Enter the service names or proto ports or port ranges to either include or exclude.

```
      Enter the PROTO and PORT (RANGES) you wish to either include or exclude in the
      format:
      Port ranges smaller than 10 ports will added if they have ports in the selected
      range
      [IN|EX] PROTO PORT_FROM-NUM_or_NAME (PORT_TO-NUM <-optional)
      Enter '.' when done

IN tcp ssh
IN tcp 3300 3500
EX tcp 3389
.
```

Filter Precedence:

The 'fsrvcprint' filters are cumulative:

- All INclude filters must be matched
- Any EXclude filter match excludes the objects
- if only EXclude filters are specified in a section all objects not excluded are included.

CSV Output:

Output is written to the selected file:

```
      Printing ANALYSIS to FILE: SvcFilterPrintOutput.csv... this may take a few minutes


---------------------------------------------------------------------------------------
ANALYSIS FILE: SvcFilterPrintOutput.csv WRITTEN     !!WOOP!!!
---------------------------------------------------------------------------------------



---------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

6. Rash Rules Mode

6.1 'rr' mode SOURCE configurations

Rash Rules mode, is 360-FAAR's rule processing algorithm.

It is in this mode that new rulebases are built. The options of the rule building algorithms are described in this section.

```
    ---------------------------------------------------------
    Chose one: rr

  ___       _   _              _ _           ___      _           __  __         _
 | _ \__ _| |_(_)___ _ _  __ _| (_)___ ___  | _ \_  _| |___ ___  |  \/  |___  __| |___
 |   / _` |  _| / _ \ ' \/ _` | | (_-</ -_) |   / || | / -_|_-<  | |\/| / _ \/ _` / -_)
 |_|_\__,_|\__|_\___/_||_\__,_|_|_/__/\___| |_|_\\_,_|_\___/__/  |_|  |_\___/\__,_\___|

--------------------------------------------------------------------------------------------
  COLLECTING INFO FOR RULEBASE RATIONALIZATION:
```

Choose SOURCE Configuration:

The SOURCE config is the configuration bundle from which rules are pulled to be rationalised. The config bundles that are loaded are listed and given option numbers alphabetically. A configuration can be chosen by entering its number or name.

```
   The following firewall configs have been loaded:

    Choose the SOURCE config:

        Option: 1    TestData.csv
        Option: 2    TestData2.csv
        Option: 3    TestData3.csv

       Choose the config you want to pull rules FROM in the rationalization?
       Enter a config name or number and hit RETURN.

1
```

Choose SOURCE Rule Groups:

The rule group names are firewall rulebases:

- For Checkpoint firewalls rulegroups are the loaded and saved policies,
- For Netscreen firewalls each zone to zone mapping has its own rulegroup, and
- For Cisco ASA firewalls each access-list is a rulegroup.

At least one source rule group must be chosen. Many rulegroups can be merged together.

How they are merged depends on the rule building mode chosen.

The open source rule build methodologies merge all rules into one set of accept rules, and the processing engine allots a random order for their processing.

```
        The firewall config "TestData.csv" has its rules grouped by these groupnames:

         Option: 1    GoodTestMergeFrom
         Option: 2    GoodTestMergeTo
         Option: 3    Test1
         Option: 4    Test2

        Which Rulegroups do you want to pull rules FROM?
        Enter each group name or number and hit RETURN.
        Enter '0' to CHOOSE ALL OPTIONS.
        Enter '.' when done....

1
.
```

360-FAAR ENHANCED: standard and complex rule build algorithms.

The Enhanced rule build methods are capable of the same with the addition that the rulebases are merged in the order that they are chosen.

Rules can be merged into a single set of accept rules as per the open source versions but also rulebases can be appended to one another retaining the rule action changes in relation to later rules.

Later rules rules can be filtered for connectivity that appears in earlier sections. Drop rules are retained in full, in their relative position within the merged rulebases. Encrypt rules can be treated in the same way if the option is chosen.

Choose 'InstallOn' Locations:

Choose the firewall locations from which rules should be included.

- For Checkpoint firewalls these are the 'Install on' firewalls
- For Netscreen firewalls these are the source zones of rules
- For Cisco ASA firewalls these are the access-group combined with directons (in / out)

Many installation locations can be chosen at once.

```
       The firewall config "TestData.csv" has its rules installed on these firewalls:

        Option: 1   Cluster1
        Option: 2   Cluster2
        Option: 3   Cluster3
        Option: 4   Cluster4
        Option: 5   MergeFromCluster
        Option: 6   MergeToCluster

       Which firewalls do you want to pull rules FROM?
       Enter each firewall/installon number or vaule and hit RETURN.
       Enter '0' to CHOOSE ALL OPTIONS.
       Enter '.' when done....

0


       * ADDING Option: Cluster1
       * ADDING Option: Cluster2
       * ADDING Option: Cluster3
       * ADDING Option: Cluster4
       * ADDING Option: MergeFromCluster
       * ADDING Option: MergeToCluster
```

Choose Rule Types:

Firewalls can have many types of rules. This are listed and the desired rule types can be chosen by adding the appropriate rule type or option number.

Rules can be:

- Security Rules
- Disabled Security Rules
- Sec NAT Rules
- Disabled Sec NAT Rules

```
       The firewall config "TestData.csv" has the following rule TYPES configured:

        Option: 1   security_rule

       Which rule TYPES do you wish to include in the rationalization?
       Enter each rule type or number and hit RETURN.
       Enter '0' to CHOOSE ALL OPTIONS.
       Enter '.' when done....

1
.
```

Using this option disabled rules can be removed or included, as can access-lists associated with NAT rules or any other types of rules that are listed.

Choose Rule Actions:

Rule actions are the type of action each rule should carry out when a packet is matched.

- Accept rules included can be matched against log file connectivity
- Encryption rules can be handled in several different ways – described later in this document
- Drop rules can either be used to filter following rules of connectivity or included in output rulebases in **360-FAAR ENHANCED**. This is dependant on the rule build mode chosen.

```
       The firewall config "TestData.csv" has the following rule ACTIONS configured:

        Option: 1    Accept
        Option: 2    Drop
        Option: 3    Encrypt

       Which rule ACTIONS do you wish to include in the rationalization?
         !!IMPORTANT!!
       If DROP rules are not included the resulting rulebase could be insecure
       Enter each rule action or number and hit RETURN.
       Enter '0' to CHOOSE ALL OPTIONS.
       Enter '.' when done....

0

       * ADDING Option: Accept
       * ADDING Option: Drop
       * ADDING Option: Encrypt
```

Choose Log Types:

Rule log types are the type of logging defined in each configuration. Differently logged rules can be filtered separately using this menu. Rules that are not logged cannot be matched against log file connectivity profiles and are included in output rulebases by default.

```
       Choose the log types of the rules you wish to include for rationalization:

        Option: 1    Log

       Which logging types do you want to pull rules with?
       Enter each log type or number and hit RETURN.
       Enter '0' to CHOOSE ALL OPTIONS.
       Enter '.' when done....
0

       * ADDING Option: Log
```

6.2 'rr' mode FILTER configurations

Filter configs can be chosen from the list of loaded configuration bundles.
A filter configs rules are used to filter out connectivity from the chosen SOURCE configurations rules, before the rule building algorithms build new rules from the remaining connectivity.
The connectivity to be filtered is held in the '`mergeto`' rulebase.

Choose Filter Configuration:

Filter configs can be chosen by entering the option number or configuration bundle name.

```
-----------------------------------------------------------------------------------------
    Choose the FILTER config:

       The following configs are available to pull rules from
       to use as a FILTER for the rationalization

        Option: 1    TestData.csv
        Option: 2    TestData2.csv
        Option: 3    TestData3.csv

       Choose the config you want to pull FILTER rules from in the rationalization?
       The selected rules will be added to the MERGE TO rulebase.
       Matching access rules from the MERGE FROM rulebases will be filtered out.
       Enter each config name or number and hit RETURN.
       Enter '.' to skip...

2
```

Choose FILTER Rule Groups:

The rule group names are firewall rulebases:

- For Checkpoint firewalls rulegroups are the loaded and saved policies,
- For Netscreen firewalls each zone to zone mapping has its own rulegroup, and
- For Cisco ASA firewalls each access-list is a rulegroup.

No rulegroups need to be chosen in this menu, however many rulegroups can be chosen and merged together.

```
       The firewall config "TestData2.csv" has its rules grouped by these groupnames:

        Option: 1    GoodTestMergeFrom
        Option: 2    GoodTestMergeTo
        Option: 3    Test1
        Option: 4    Test2

       Which Rulegroups do you want to pull FILTER rules FROM?
       Enter each group number or name and hit RETURN.
       Enter '0' to CHOOSE ALL OPTIONS.
       Enter '.' when done....

2
.
```

The order in which they are chosen has no effect because all rules selected from the FILTER config are processed into the mergeto rulebase (to be used as a connectivity filter for SOURCE rules) before SOURCE rules are filtered against it.

Choose FILTER InstallOns:

Choose the firewall locations from which rules should be included into the mergeto rulebase.

- For Checkpoint firewalls these are the 'Install on' firewalls
- For Netscreen firewalls these are the source zones of rules
- For Cisco ASA firewalls these are the access-group combined with directons (in / out)

Many installation locations can be chosen at once.

```
       The firewall config "TestData2.csv" has its rules installed on these firewalls:

        Option: 1    Cluster1
        Option: 2    Cluster2
        Option: 3    Cluster3
        Option: 4    Cluster4
        Option: 5    MergeFromCluster
        Option: 6    MergeToCluster

       Which firewalls do you want to pull rules FROM?
       Enter each firewall/installon name or number and hit RETURN.
       Enter '0' to CHOOSE ALL OPTIONS.
       Enter '.' when done....

6
.
```

Choose FILTER Rule Types:

Firewalls can have many types of rules. This are listed and the desired rule types can be chosen by adding the appropriate rule type or option number.
Rules can be:

- Security Rules
- Disabled Security Rules
- Sec NAT Rules
- Disabled Sec NAT Rules

```
       The firewall config "TestData2.csv" has the following rule TYPES configured:

        Option: 1    security_rule

       Which rule TYPES do you wish to include in the filter rulebase?
       Enter each rule type or number and hit RETURN.
       Enter '0' to CHOOSE ALL OPTIONS.
       Enter '.' when done....

0
       * ADDING Option: security_rule
```

Using this option disabled rules can be removed or included, as can access-lists associated with NAT rules or any other types of rules that are listed.

- NOTE: The type of rules chosen is not matched between the SOURCE configuration and the FILTER configuration, only the connectivity profile of the rules is significant.

Choose FILTER Rule Actions:

Rule actions are the type of action each rule should carry out when a packet is matched.

- Accept rules included can be matched against log file connectivity
- Encryption rules can be handled in several different ways – described later in this document
- Drop rules can either be used to filter following rules of connectivity or included in output rulebases in **360-FAAR ENHANCED**. This is dependant on the rule build mode chosen.

```
      The firewall config "TestData2.csv" has the following rule ACTIONS configured:

       Option: 1    Accept
       Option: 2    Drop

      Which rule ACTIONS do you wish to include in the filter rulebase?
        !!IMPORTANT!!
      If DROP rules are not included the resulting new filter rulebase could
      filter rules that are needed out of the new rationalised rulebase
      Enter each rule action or number and hit RETURN.
      Enter '0' to CHOOSE ALL OPTIONS.
      Enter '.' when done....

0
      * ADDING Option: Accept
      * ADDING Option: Drop
```

- NOTE: The rule actions chosen are not matched between the SOURCE configuration and the FILTER configuration, only the connectivity profile of the rules is significant. If a connection profile from a FILTER config matches a connection profile of rules pulled from a SOURCE configuration, the SOURCE rules connection is filtered out

6.3 'rr' mode DESTINATION configurations

Choose DESTINATION configurations:

DESTINATION configuration are chosen from the loaded configuration bundles.

DESTINATION configs are the location that firewall rules pulled from SOURCE configurations that made it through the filters are to be translated and written to.

```
------------------------------------------------------------------------------------------
    Choose the DESTINATION config:

       The following configs are available for merging rules TO

        Option: 1   TestData.csv
        Option: 2   TestData2.csv
        Option: 3   TestData3.csv

       Choose the config you want to merge rules TO in the rationalization?
       Enter each config name or number and hit RETURN.
       Enter '.' to skip...

2
```

Network and Service Objects from the SOURCE config with matching definitions in the DESTINATION configurations are translated, as are matching groups.

Choose the configuration bundle to merge SOURCE rules to. Configuration bundles can be chosen by entering the option number or the config name.

Objects and Groups from the DESTINATION configurations that match objects and groups used in the SOURCE configurations are translated.

The DESTINATION config is the configuration bundle from which rules are pulled to be used as the merge to rulebase a filter for the connectivity in the chosen SOURCE configs rule group.

The config bundles that are loaded are listed and given option numbers alphabetically.

Choose DESTINATION Rule Group:

A rulegroup can be chosen by entering its number or name.

```
       The firewall config "TestData2.csv" has rules are grouped by these groupnames:

        Option: 1   GoodTestMergeFrom
        Option: 2   GoodTestMergeTo
        Option: 3   Test1
        Option: 4   Test2

       Choose a rulebase to merge the previous rulebases with
       Connections that exist in the rulebases you choose here will not apprear
       in the new rules created.

       Enter each group name or number and hit RETURN.
       Enter '0' to CHOOSE ALL OPTIONS.
       Enter '.' when done....
.
```

The chosen rule groups connectivity profile is removed from the SOURCE rules and the SOURCE configurations objects and groups are translated to matching objects and groups from the DESTINATION configuration.

- NOTE: If a DESTINATION configuration is chosen but no rule group is selected then only objects and groups are translated. No connectivity is filtered out.

Choose DESTINATION Rule 'InstallOn':

Choose the firewall locations from which rules should be included into the mergeto rulebase.

- For Checkpoint firewalls these are the 'Install on' firewalls
- For Netscreen firewalls these are the source zones of rules
- For Cisco ASA firewalls these are the access-group combined with directons (in / out)

Many installation locations can be chosen at once.

```
        The firewall config "TestData2.csv" has its rules installed on these firewalls:

         Option: 1   Cluster1
         Option: 2   Cluster2
         Option: 3   Cluster3
         Option: 4   Cluster4
         Option: 5   MergeFromCluster
         Option: 6   MergeToCluster

        Which firewalls do you want to merge rules TO?
        Enter each firewall/installon name or number and hit RETURN.
        Enter '0' to CHOOSE ALL OPTIONS.
        Enter '.' when done....

.
```

All rule types, actions and log types are added to the 'merge to' rulebase.

This is because the destination configuration may handle connectivity from the SOURCE configuration differently as it is assumed that the firewall on which the DESTINATION rule groups are installed is in a different location in the network, e.g: the destination firewall might encrypt matching traffic for transmission to another site via a VPN.

Adding Accept rules to a policy such as described above would potentially exempt the traffic from the VPN.

If more granular filtering is needed use the FILTER config, and select no DESTINATION rule groups.

6.4 'rr' mode FILTERS

The 'rr' mode filter section is where CIDR addresses, text, service and port filters can be added and used to further filter the connectivity from the SOURCE rulegroups.

Choose CIDR Filters:

These filters work in conjunction with the FILTER configuration. Connectivity that is not included in the FILTER configuration or the DESTINATION configuration is filtered by the filters defined in this section.

```
-------------------------------------------------------------------------------------------
    Choose the FILTER details:

       Enter the IP address ranges you wish to either include or exclude in the format:
       [IN|EX] IP MASKLENGTH
       Enter '.' when done

IN 172.16.0.0 12
       Resolved IN to Binary Match: 101011000001
EX 172.24.0.0 16
       Resolved EX to Binary Match: 1010110000011000
.
```

CIDR IP addresses can be entered here in the format IN for include and EX for exclude.

- Filtered CIDR addresses must match at least one include statement if at least one include statement is entered.
- Excluded CIDR addresses always exclude the connectivity from the output.
- If only exclude statements are entered all connectivity not excluded is included.
- If no include or exclude statements are entered, all connectivity is included.

Choose Service / Proto Port Filters:

These filters filter new rulebases to either include or exclude the services, protocol and port ranges.

360-FAAR ENHANCED: service and port filters

```
       Enter the PROTO and PORT (RANGES) you wish to either include or exclude:
       Port ranges smaller than 10 ports will added if they have ports in the selected
       range:
       [IN|EX] PROTO PORT_FROM-NUM_or_NAME (PORT_TO-NUM <-optional)
       Enter '.' when done

IN tcp ssh
       Resolved IN to PORT Match: tcp, 22
       Resolved IN to PORT Match: tcp, ssh
IN udp 123
       Resolved IN to PORT Match: udp, 123
IN tcp 3389
       Resolved IN to PORT Match: tcp, 3389
IN tcp 50 500
       Resolved IN *RANGE* Match: tcp, FROM: 50 - TO: 500
       Resolved IN to PORT Match: tcp, 50
       Resolved IN to PORT Match: tcp, 51
       Resolved IN to PORT Match: tcp, 52
       Resolved IN to SRVC Match: tcp, 53
       Resolved IN to SRVC Match: tcp, domain-tcp
       Resolved IN to PORT Match: tcp, 54
      ...
       Resolved IN to SRVC Match: tcp, 79
       Resolved IN to SRVC Match: tcp, finger
       Resolved IN to SRVC Match: tcp, 80
       Resolved IN to SRVC Match: tcp, http
       Resolved IN to PORT Match: tcp, 81
       Resolved IN to PORT Match: tcp, 82
       Resolved IN to PORT Match: tcp, 83
      ...
       Resolved IN to PORT Match: tcp, 141
       Resolved IN to PORT Match: tcp, 142
       Resolved IN to SRVC Match: tcp, 143
       Resolved IN to SRVC Match: tcp, imap
       Resolved IN to PORT Match: tcp, 144
       Resolved IN to PORT Match: tcp, 145
      ...
       Resolved IN to PORT Match: tcp, 499
       Resolved IN to PORT Match: tcp, 500
.
```

Service names, ports and port ranges can be entered here in the format IN for include and EX for exclude.

- Filtered ports must match at least one include statement if at least one include statement is entered.
- Excluded ports always exclude the connectivity from the output.
- If only exclude statements are entered all connectivity not excluded is included.
- If no include or exclude statements are entered, all connectivity is included.
- If a port entered, matches a range of ports, smaller than 10 ports, the whole range is included in the include or exclude filter.

Choose Text Filters:

If you wish to enter text filters choose 'no' at the skip text filters option.

```
       SKIP TEXT Filters?
       [yes|no] - or '.' for default (yes)

no
```

Enter Text Strings Rules Must Include:

Include rule text filters match to against the original text of the rule in its original syntax of each firewall rule from the SOURCE rulegroup.

- If an include string is entered all rules must contain this string in their original syntax.

```
       Enter any strings you wish to INCLUDE filter each rule for
       Enter '.' when done....

Development
.
```

Enter Text Strings That Rules Section Headers Must Include:

```
        Enter any strings you wish to INCLUDE filter each header section for
        Enter '.' when done....
.
```

Include section header text filters to match against the original text of a rules section header in its original syntax from the SOURCE rulegroup.

- If an include string is entered all rules must be from sections that have headers that contain this string in their original syntax.
- For Netscreen policies, the closest remark higher up the policy is a rules section header
- For Cisco policies, the closest remark higher up the access-list is a rules section header
- For Checkpoint FW-1 rulebases, section headers are just that.

Enter Text Strings Rules Must Exclude:

```
        Enter any strings you wish to EXCLUDE filter each rule for
        Enter '.' when done....
.
```

Exclude rule text filters to match against the original text of the rule in its original syntax of each firewall rule from the SOURCE rulegroup.

- If an exlcuded string is entered all rules matching this string in their original syntax are ecluded.
- If no include statements are entered, all connectivity not excluded is included.

Enter Text Strings That Rules Section Headers Must Exclude:

```
        Enter any strings you wish to EXCLUDE filter each header section for
        Enter '.' when done....
.
```

Exclude section header text filters to match against the original text of a rules section header in its original syntax from the SOURCE rulegroup.

- If an exclude string is entered all rules from the sections that have headers that contain this string in their original syntax will be exlcuded.
- For Netscreen policies, the closest remark higher up the policy is a rules section header
- For Cisco policies, the closest remark higher up the access-list is a rules section header
- For Checkpoint FW-1 rulebases, section headers are just that.

6.5 'rr' mode options

Rationalisation options control the way in which:

- Filters are applied,
- Encrypt rules are handled,
- Groups are matched
- 'Any' objects are handled
- and various other aspects of the rulebase building algorithms workings.

Choose Default Option Set:

You can choose default sets of these options that are optimized for various jobs or enter '**no**' when asked to choose a default option set and choose each option individually.

- Each of the sets of defaults can be used in many situations.
- The default sets most common uses are described in the next section.
- These descriptions are not exhaustive, they are meant to be instructive as to a default sets common usage scenarios.

```
-----------------------------------------------------------------------------------------
    Choose the OPTIONS for the rationalization:

      To choose OPTIONS MANUALLY select:
       [no]    - CHOOSE OPTIONS MANUALLY
```

Choose Simple Defaults:

The SIMPLE defaults are designed to be easily usable in the majority of situations. Filters match subnets of entered CIDR ranges, and include connectivity to and from any matched addresses in output rulebases. No log file need be loaded. NATs are not translated. 'Any' objects are not resolved and encryption rules are not used to mask later accept rule connectivity.

```
      To use DEFAULT settings select one of the following OPTIONS:
       [yes]   - Choose SIMPLE Defaults
```

Choose NAT Defaults:

The NAT defaults are the same as SIMPLE defaults except that the CIDR filters match against the NATed addresses.

```
       [nat]   - Choose SIMPLE Defaults AND TRANSLATE NAT for CIDR FILTERS
```

Choose LOG Defaults:

The LOG defaults are designed to be the easiest usable defaults when filtering a rulegroups connectivity profile using the loaded logfiles. LOG defaults aim to build the simplest filtered rulebases from connectivity seen in the log and matched to the policy.

```
        [log]   - Choose FILTER WITH LOG Defaults
```

Choose High Resolution Defaults and Resolve 'Any' Objects:

The HIGH RESOLUTION defaults are designed to give the highest possible viability of which policy elements were in use from the connectivity seen in the loaded log files. 'Any' objects are resolved where ever possible and any connectivity not used is filtered out of the new rulebases.

```
        [res]   - Choose RESOLVE 'Any' OBJECTS FROM LOGGED CONNECTIVITY
```

Choose 'cplx' Defaults:

360-FAAR ENHANCED: cplx defaults

The COMPLEX defaults are designed to be used on complex enterprise firewall policies, when 'Drop' rule significance needs to be maintained and rulebases need to be filtered to remove unused connectivity or decommissioned networks or split into smaller policies while maintaining the same security restrictions. COMPLEX rulebases also simplify existing rules as much as is possible.

```
        [cplx]  - Choose COMPLEX Defaults and FILTER WITH LOG
```

Choose 'cplxn' Defaults:

360-FAAR ENHANCED: cplxn defaults

The COMPLEXN defaults are designed to work in the same way as COMPLEX defaults but without using log files to filter the rulebases accept rules. This mode can be used to build simplified and condensed rulebases of all existing connectivity from a rulegroup while maintaining the existing security policy.

```
        [cplxn] - Choose COMPLEX Defaults
```

Choose 'no' Defaults option set, and select options manually:

```
       [yes|no|nat|log|res|cplx|cplxn] - or '.' for default (yes)

no
```

Include Connectivity To / From Filtered Connectivity:

Include subnets and host that match the CIDR filters or filter for exact CIDR addresses only?

```
       INCLUDE objects from the SUBNETS of the CIDR FILTERS in the new rulebase?
       Choose to match only the exact networks in the filters, or match their subnets as
       well?
       [yes|no] - or '.' for default (yes)

.
       * ADDED Option: yes
```

Choose The Filter Type, and Standard or Complex Build Methods:

The filter types are listed below:

```
       Choose FILTER TYPE and FILTER rules based on CONNECTIONS FOUND in the LOG?
       NOTE: loose(n) modes require no answer in next question
       [yes|complex|loose]        - to filter with CIDR and LOG
       [no|complexn|loosen]       - to filter with CIDR only
       [none]                     - do not to filter
                           - or type '.' for default (no)

.
       * ADDED Option: no
```

Choose the filter type and policy build mode:

- `yes` = filter the policy using logs and CIDR / Service / Text strings
- `no` = filter the policy using CIDR / Service / Text strings
- `loose` = filter the policy using logs and EX CIDR and Service filters / Text string filters
- `loosen` = filter the policy using EX only CIDR and Service filters / Text string filters
- `cplx` = filter the policy using logs and CIDR / Service / Text strings, build complex policy
- `cplxn` = filter the policy using CIDR / Service / Text strings, build complex policy
- `none` = dont filter the policy using CIDR / Service but still filter with Text strings and filter configurations.

Choose if Include Filters Will Include Connectivity when only source or destination is matched:

Match include CIDR filters for source, destination or both, or require both source and destination are matched by the filters. Exclude filters always match either or both.

```
       INCLUDE objects that CONNECT to the OBJECTS RESOLVED, by the filters?
       [yes|no] - or '.' for default (yes)


.
       * ADDED Option: yes
```

Translate NATs for Filtering with CIDR Address filters:

Translate NATed connectivity to the NATed addresses and filter with the CIDR filters?
The original rules are output.

```
       TRANSLATE log connections IP's using NATS while FILTERING for IN EX CIDRs?
       NOTE: These translations are only for the IN EX filters to match using.
       [yes|no] - or '.' for default (no)


.
       * ADDED Option: no
```

Resolve Network 'Any' Objects Where Possible:

Translate 'Any' objects in policies to the most speciffic network or host in the firewalls configuration that matched connectivity in the loaded logfiles, and build new rules using these objects in place of 'Any' where possible.

```
       Resolve NETWORK OBJECT "Any" to the most speciffic netobejcts SEEN IN THE LOG
       FILES?
       NOTE: This requires log files and can produce much larger rulebases.
       [yes|no] - or '.' or default (no)


.
       * ADDED Option: no
```

Resolve Service 'Any' Objects:

Translate 'Any' objects in policies to the closest service in the firewalls configuration that matched connectivity in the loaded log files and add seen but unknown proto-ports to rulebases, and report. New rules use these objects in place of 'Any' where possible.

```
       Resolve SERVICE OBJECT "Any" to the speciffic services SEEN IN THE LOG FILES?
       NOTE: This requires log files and can produce much larger rulebases.
       [yes|no] - or '.' or default (no)


.
       * ADDED Option: no
```

Match Previously Expanded Rules:

As rules are expanded check each rule against previously processed rules and remove any connectivity that matches the already expanded rules.

```
       Match rules and supernets against PREVIOUSLY EXPANDED rules?
       Check each rule as its being expanded against already expanded rules
       [yes|no] - or '.' for default (no)

.
       * ADDED Option: no
```

Match Accept Rules Against Previously Expanded Encrypt Rules:

As encrypt rules are expanded, add them to the 'merge to' rulebase so that following accept rules with the same connection set will be filtered out. This option also removes the encrypt rules because they are added to the merge to policy and not the filter policy that is used to build new rules.

```
       Match ACCEPT rules against ENCRTPYION rules FROM EARLIER in the MERGE FROM
       rulebase?
       Check each rule as its being expanded against already expanded encryption rules
       [yes|no] - or '.' for default (no)

.
       * ADDED Option: no
```

Include Encryption Rules from the MergeTo Rulebase:

Add encrypt rule from the destination firewalls rule groups to the mergeto rulebase so that the source configurations rules will be filtered out if they match.

```
       Include ENCRYPTION rules from the MERGE TO rulebase in the filter match rulebase?
       Check each accept rule against expanded accept rules AND ENCRYPTION rules?
       [yes|no] - or '.' or default (yes)

.
       * ADDED Option: yes
```

Choose Smallest Net Group Size To Match:

360-FAAR ENHANCED: Fuzzy netgroups

Choose the smallest number of objects a group must have to be matched during rule building.

```
       Use FUZZY logic for NETWORK GROUP MATCH?
       Enter the SMALLEST group size (number of objects per group) that will be MATCHED
       [integer >= 0] - or '.' or default (0)

.
* ADDED Value: 0
```

Choose To Match Net Groups With Missing Objects:

360-FAAR ENHANCED: Fuzzy netgroups

Choose the largest number of objects that can be missing from a group while still matching and being included in rule building.

```
       Use FUZZY logic for NETWORK GROUP LOOSE MATCH?
       Enter the LARGEST number of OBJECTS per group, that can be MISSING, before the
       group is NOT MATCHED
       [integer > 0] - or '.' or default (1)

.
       * ADDED Value: 1
```

Choose The Smallest Service Group To Match:

360-FAAR ENHANCED: Fuzzy srvcgroups

Choose the smallest number of objects a service group must have to be matched during rule building.

```

       Use FUZZY logic for SERVICE GROUP MATCH?
       Enter the SMALLEST group size (number of objects per group) that will be MATCHED
       [integer >= 0] - or '.' or default (0)

.
       * ADDED Value: 0
```

Choose To Match Service Groups With Missing Objects:

360-FAAR ENHANCED: Fuzzy srvcgroups

Choose the largest number of objects that can be missing from a service group while still matching and being included in rule building.

```
       Use FUZZY logic for SERVICE GROUP LOOSE MATCH?
       Enter the LARGEST number of OBJECTS per group, that can be MISSING, before the
       group is NOT MATCHED
       [integer > 0] - or '.' or default (1)

.
       * ADDED Value: 1
```

Choose To Use The Smallest or Largest Net Groups:

360-FAAR ENHANCED: rule build options

Wrap the new rule groups using the smallest or largest groups that matched the connectivity from the filtered policies.

```
       MATCH the MOST SPECIFFIC NETWORK groups possible? Use the SMALLEST possible
       groups?
       Selecting 'no' matches the largest groups possible - this can reduce rulebase
       sizes further.
       [yes|no|rand] - or '.' or default (no)

.
       * ADDED Option: no
```

The rule grouping options are:

- 'yes' - build rules using smallest groups. This produces rulebases with the highest viability of group usage, as larger groups don't mask smaller groups.
- 'no' - build rules using largest groups. This produces the simplest rulebases.
- 'rand' - build rules using the groups matched in a random order – open source

- NOTE: The rule grouping options have significant effect on the output from the rule building algorithms. The connectivity profile remains the same but the rules will be grouped differently.
- The best option is to try all three and decide on the most suitable.

Choose To Use The Smallest or Largest Service Groups:

360-FAAR ENHANCED: rule build options

Wrap the new rule groups using the smallest or largest service groups that matched the connectivity from the filtered policies.

```
       MATCH the MOST SPECIFFIC SERVICE groups possible? Use the SMALLEST possible
       groups?
       Selecting 'no' matches the largest groups possible - this can reduce rulebase
       sizes further.
       [yes|no|rand] - or '.' or default (no)

.
       * ADDED Option: no
```

The rule grouping options are:

- 'yes' - build rules using smallest service groups. This produces rulebases with the highest viability of group usage, as larger groups don't mask smaller service groups.
- 'no' - build rules using largest service groups. This produces the simplest rulebases.
- 'rand' - build rules using the service groups matched in a random order – open source

- NOTE: The rule grouping options have significant effect on the output from the rule building algorithms. The connectivity profile remains the same but the rules will be grouped differently.
- The best option is to try all three and decide on the most suitable.

Choose Verbose Output:

Print debug info for all sections. Output Accept or Drop Rule connectivity matches for all policy and log entries. There is a lot of this but its useful... hopefully.

```
       Output VERBOSE information during Rule Rationalization?
       [yes|no] - or '.' or default (no)


.
       * ADDED Option: no
```

Choose The Rule Build Algorithm:

The types of rule building algorithms wrap new rules using different orderings of when each type of grouping happens, this combined with the structure of the connectivity works together to provide three types of rule building and one derived rule building algorithm.

```
-----------------------------------------------------------------------------------------
     Choose the TYPE OF RULEASE you want to build:

       TYPES: ds     = dst-src-srvc priority   - primary
              sr     = srvc-dst-src priority
              hc     = sort rules by hit count - requires loaded logs and 'yes' in log
                       filter
              cl     = clean original rules
       [ds|sr|hc|cl] - or '.' or default (ds)


.
       * ADDED Option: ds
```

The rule build types are:

- **`ds`** - build rules with the priority destination / source / service
- **`sr`** - build rules with the priority source / service / destination
- **`hc`** - build rules with the *most hit* rules at the top (this mode is experimental)

The rule build mode **`cl:`**

- **`cl`** rule build type uses `ds` rule building within each current rule number to rebuild original rules with new groups, filter connectivity out of an existing rulebase, remove duplicate objects, regroup in smallest or largest groups within rules.

6.6 'rr' mode PROCESSING

Build NAT Tree:

Nat rules are converted to connectivity profiles for processing

```
------------------------------------------------------------------------------------------
 BUILDING NAT MATCH TREE:
```

Build SOURCE, DESTINATION and FILTER Trees:

The '`mergeto`' or '`DESTINATION`', and '`FILTER`' trees are built first and are used to filter the '`SOURCE`' policies tree.

360-FAAR ENHANCED: rule build options

Rulebases and Action Sections are reported in all modes but are only significant in '`complex`' and '`complexn`' type rulebase builds.

Complex rule build and filter types can merge rulebases sequentially, retain '`Drop`' and '`Reject`' rules and allow later policies to be filtered using the connectivity of earlier rules, to filter '`Accept`' and '`Permit`' rule connectivity from later policy sections.

360-FAARen retains the order that the '`SOURCE`' policies were chosen in and concatenates them in this order. Rule Action Sections are processed using '`ds`', '`sr`' or '`hc`' buld algorithms.

```
------------------------------------------------------------------------------------------
 STARTING FILTER MATCH ANALYSYS:

---------------------------------------------------0       MERGE BASE DONE
.................................
---------------------------------------------------33854   FILTER BASE DONE

FOUND Rulebase: GoodTestMergeFrom      Section: 1,         ACTION: Accept
---------------------------------------------------        --------------

FOUND Rulebase: GoodTestMergeFrom      Section: 2,         ACTION: Encrypt
---------------------------------------------------        --------------
.
FOUND Rulebase: GoodTestMergeFrom      Section: 3,         ACTION: Accept
---------------------------------------------------        --------------
..................................................50000    Subnet matches processed
...................................................100000  Subnet matches processed
...................................................150000  Subnet matches processed
...................
---------------------------------------------------169410  RULE BASE DONE
```

Output NAT Rule Matches:

The objects and rules that matched connectivity in the NAT rule and the associated security rule

```
TRANSLATION RULES IN USE:
-----------------------------------------------------------------------------------------
NAT Rule Num, Orig Source, Orig Dest, Orig Service, Associated Security Rule,
      …
      …
      …
```

Output Original Rules in Original Format:

The original rules included in the policy rebuild are listed.

They are output in their original format.

```
-----------------------------------------------------------------------------------------
 ORIGINAL RULES INCLUDED IN RATIONALIZATION:
   These are the original rules that were evaluated:

Global 31, Rule: 1,security_rule,Management-Net2,Development-ALL,VPN-1,ssh
gWindows_RDP,Accept,Log,MergeFromCluster,Any,Management Rule1
Global 32, Rule: 2,security_rule,Management-Net1,Development-ALL,Any,ssh
gWindows_RDP,Encrypt,Log,MergeFromCluster,Any,Management Rule1
Global 33, Rule: 3,security_rule,Management-ALL,Development-ALL,Any,ssh
gWindows_RDP,Accept,Log,MergeFromCluster,Any,Management Rule1
Global 35, Rule:
5,security_rule,Development-Hosts,GroupTrans-GROUP1,Any,smtp,Accept,Log,MergeFromCluster,
Any,Management Rule1
```

Output Original Rules after Filters Have Been Applied in Expanded Format:

The original rules are output again, this time with only the expanded objects that we're not filtered out of the selected policies. This policy is filtered by the '`FILTER`' and '`DESTINATION`' policies selected, the CIDR, Text and Service filters as well as rule options.

The logfile comparison / filtering has not yet been applied.

The rules are output in the format:

- `Original Rule Num,`
- `Expanded and filtered Source Network Objects,`
- `Expanded and filtered Destination Network Objects,`
- `Expanded and filtered Service Objects,`
- `Original Rule Action,`
- `Description: FILTERED RULE`

```
The original rules included in the policy rebuild are listed. They are output in their
original format.

-----------------------------------------------------------------------------------------
 RULE FILTER SECTION COMPLETE:
   These are the original objects and rules that matched the filters:

ORIG RULE, SRC, DST, SERVICE, ACTION, DESCRIPTION
      ...
      ...
      ...
      ...
```

Start Rule Building Algorithm:

Once built the rules are output in simplified format to the terminal

```
----------------------------------------------------------------------------------------
 STARTING DST SRC PRIORITY RULE BUILD: - primary rule building mode

----------------------------------------------------------------------------------------
 STARTING RULE COMPARISON:
   ports rationalized..............................DONE!
   destinations rationalized.......................DONE!
   sources rationalized............................DONE!
```

Output Rulebase To Screen:

The new rulebase is output:

Using objects and groups from the 'SOURCE' configuration.

In the format:

- `New Rulebase Rule Num,`
- `Source Net Objects and Groups,`
- `Destination Net Objects and Groups,`
- `Service Objects and Groups,`
- `Original Global Rule Number,`
- `Hit Count ('hc' build type only).`

```
   RATIONALIZED RULES:

Rule: 1, Bastion-Nets, DMZ-Hosts, Internal-ServiceGroup ssh, 34
Rule: 2, Management-ALL, Development-ALL, gWindows_RDP ssh, 31 32 33
Rule: 3, Development-Hosts, GroupTrans-GROUP1, smtp, 35
Rule: 4, Management-ALL, GroupTrans-GROUP, snmp, 36
```

Choose The Output Format Of The Rash Rule Process:

Rules are output in the following formats:

- 'od'   Odumper/Ofiller CSV Format and 'dbedit' to File.
- 'ns'   Netscreen ScreenOS 6 'get config' Format to Screen.
- 'cs'   Cisco ASA 'show run' Format to Screen.
- 'no'   Return to the Menu and Do Not Output Rules and Objects

```

----------------------------------------------------------------------------------------
 RASH RULE COMPARISON COMPLETE:

       Would you like to print the most recent rulebase to file
       [no|od|ns|cs]

       Choose: ns
```

Choose Checkpoint FW-1 dbedit / ofiller CSV Output:

'od' Rules and Objects are Output in Odumper/Ofiller CSV Format and 'dbedit' to Two Files. The file names and a new rulebase name are required.

To output a 'od' fomat policy, enter:

- A file name to save the odumper/ofiller format CSV.
- A file name to save the dbedit text.
- A Destination Rulebase name to add to the 'DESTINATION' firewalls smart centre by loading the dbedit file.

```
        Choose: od
------------------------------------------------------------------------------------------
  Rules Built From Hit Connetions output in Odumper format
------------------------------------------------------------------------------------------
 OUTPUT ODUMPER AND DBEDIT TEXT:


        Enter the name of the CSV file to be saved: nufing.csv


        Enter the name of the dbedit file to be saved: nufing.dbedit


        Enter the name of the Checkpoint FW-1 RULEBASE to write rules to: NuFing



------------------------------------------------------------------------------------------
        FILE: nufing.csv WRITTEN   !!*%*%*-HURRAY-*%*%*!!
------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------
 DBEDIT FILE: nufing.dbedit WRITTEN    !!*%*%*-SWEEET-*%*%*!!
------------------------------------------------------------------------------------------


------------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

Objects, flattened Network and Service Groups and policy rules are output file.

The new CSV rulebase can be loaded back into 360-FAAR using 'load' mode.

The new dbedit rulebase can be loaded onto the desired firewall after careful checking and testing in a staging environment.

The CSV can be modified and rebuilt using the 'bldobj' mode.

Choose Netscreen Output:

'`ns`' Rules and Objects are Output in `Netscreen ScreenOS6` Format to screen.

To output a '`ns`' fomat policy, enter:

- A Destination Netscreen Configuration, to pull zone matches from object definitions, routes and interfaces, to use to assign zones to the '`SOURCE`' configs objects.
- Or Zone CIDR Information
- Or both ^^^ to override '`DESTINATION`' Configuration Zone
- If no zones or destination configs are provided the default zone is used for all objects.
- Choose the rule number to start numbering rules with, or accept the default.

```
------------------------------------------------------------------------------------------
  Rules Built From Hit Connetions output in Netscreen ScreenOS format
------------------------------------------------------------------------------------------
 NETSCREEN CONVERSION:

   Define route to zone mappings in the format:
   ZONE IP MASKLENGTH

   type '.' to finish zone input

IN 10.0.0.0 8
INNER 10.0.0.0 12
INNEST 10.0.0.0 18
OUT 0.0.0.0 0
DMZ 172.16.0.0 12
INISH 292.168.0.0 16
             INPUT FORMAT ERROR: enter: ZONENAME IPADDR MASKLENGTH
.

      MAX EXISTING RULE NUM: 16

      Enter a number to override the above rule count or press enter to accept:
```

Rules, groups and objects are output...

```
      …
      …
      …
```

Objects, flattened Network and Service Groups and policy rules are output to STDOUT.

These new rulebases can be copied to a file and loaded back into 360-FAAR using '`load`' mode.

Choose Cisco ASA Output:

'cs' Rules and Objects are Output in 'Cisco ASA' Format to STDOUT.

To output a 'od' format policy, Enter:

- A file name to save the odumper/ofiller format objects CSV.
- A Destination access-list name to add to the 'DESTINATION' ASA firewalls configuration.

```
      Choose: cs



--------------------------------------------------------------------------------------------
  Rules Built From Hit Connetions output in Cisco ASA and Odumper CSV format
--------------------------------------------------------------------------------------------
  OUTPUT ODUMPER CSV AND CISCO ASA CMD TEXT TO SCREEN:


      Enter the name of the file to be saved: nuasa.csv


      Enter the name of the access-list to write rules to: NewASA



name 10.0.0.1 Control-Host-1 description Comment 1 blue   TRANSLATED Object:
Management-Host-1 matches the IP of host Control-Host-1
name 10.0.0.10 Control-Host-10 description Comment 10 blue   TRANSLATED Object:
Management-Host-10 matches the IP of host Control-Host-10
name 10.0.0.11 Control-Host-11 description Comment 11 blue   TRANSLATED Object:
Management-Host-11 matches the IP of host Control-Host-11
      …
      …
      …
```

Objects, flattened Network and Service Groups and access-list statements are output to STDOUT.

These new rulebases can be copied to a file and loaded back into 360-FAAR for further analysis using 'load' mode.

Hit Enter To Return To The Menu:

Press the enter key with your finger.

```
--------------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

This Page is Intentionally Blank! Why?

7. 'bldobj' mode

7.1 Rebuild Rule Objects Mode:

Rebuild Rule Objects Mode reads firewall policies in odumper CSV or numberrules.pl helper format and identifies objects from three loaded configuration bundles.

The policy is then translated, as is, to the destination configuration bundles objects and groups where possible.

New objects are created for objects identified from the other two configuration bundles and output in the same way as rr mode rulebases are output.

Input formats are:

- Odumper/Ofiller CSV or numberrules.pl helper format.

Formats of translated rulebase output are:

- Checkpoint FW-1 dbedit script and odumper/ofiller format CSV.
- Netscreen ScreenOS6 – network and service objects and groups and multi-line policy entries
- Cisco ASA, – name, object, group, proto group, service groups, access-lists

Choose The Odumper Or Hleper Script Format CSV Filename

```
    --------------------------------------------------------
    Chose one: bldobj

 ___      _ _    _   ___      _         ___  _     _        _        __  __         _
| _ )_  _(_) |__| | | _ \_  _| |___    / _ \| |__ (_)___ __| |_ ___ |  \/  |___  __| |___
| _ \ || | | / _` | |   / || | / -_)  | (_) | '_ \| / -_) _|  _(_-< | |\/| / _ \/ _` / -_)
|___/\_,_|_|_\__,_| |_|_\\_,_|_\___|   \___/|_.__// \___\__|\__/__/ |_|  |_\___/\__,_\___|
                                                |__/
----------------------------------------------------------------------------------------
 IDENTIFY OBJECTS TO BUILD RULE DEFINITIONS:
----------------------------------------------------------------------------------------
   Enter rule definitions in odumper format to build a policy

       Enter the name of the spreadsheet you want to
       read rules from:

nufing.csv
```

Enter the filename you wish to load.

Choose Output Format

Enter the type of output configuration you want to translate nufing.csv to.

Rules are output in the following formats:

- `'od'` `Odumper/Ofiller` CSV Format and `'dbedit'` to File.
- `'ns'` Netscreen ScreenOS 6 `'get config'` Format to Screen.
- `'cs'` Cisco ASA `'show run'` Format to Screen.

```
      Enter the type of config you would like to build [od|ns|cs]:

cs
```

Choose Source Configuration One:

Choose the first source configuration to identify rule objects from.

```
      Enter the config bundle name of the firewall you are
      merging rules and objects from:

       Option: 1    TestData3.csv
       Option: 2    TestData4.csv

      Which CONFIG do you want to match objects FROM?
      Enter a CONFIG NAME or NUMBER and hit RETURN.

1
```

Choose Source Configuration Two:

Choose the second source configuration to identify rule objects from.

```
      Enter the secondary config bundle name of the firewall you are
      merging rules and objects from:

       Option: 1    TestData3.csv
       Option: 2    TestData4.csv

      Which SECONDARY CONFIG do you want to match objects FROM?
      Enter a CONFIG NAME or NUMBER and hit RETURN.

2
```

Choose Destination Configuration:

Choose the destination configuration to identify rule objects from and translate objects and groups to, where possible.

```
      Enter the config bundle name of the firewall you are
      merging rules and objects to:

       Option: 1   TestData3.csv
       Option: 2   TestData4.csv

      Which CONFIG do you want to translate objects TO?
      Enter a CONFIG NAME or NUMBER and hit RETURN.


2
```

Output Objects and Groups Detected Count:

```
-----------------------------------------------------------------------------------------
 SCANNING FILE nufing.csv FOR RULE DEFINITIONS:
-----------------------------------------------------------------------------------------
   Found Rules Numbering: 4

   POLICY PACK: TestData3.csv
    Objects:        465
    Obj Groups:           3
    Services:       8
    Srvc Groups:    1
   POLICY PACK: TestData4.csv
    Objects:        0
    Obj Groups:           0
    Services:       0
    Srvc Groups:    0
   POLICY PACK: TestData4.csv
    Objects:        213
    Obj Groups:           6
    Services:       0
    Srvc Groups:    0
-----------------------------------------------------------------------------------------
  OUTPUT ODUMPER CSV AND CISCO ASA CMD TEXT TO SCREEN:

      Enter the name of the file to be saved: nufingASAodobjs.csv

      Enter the name of the access-list to write rules to: NuFingASA


name 10.0.0.1 Control-Host-1 description Comment 1 blue Matching object name in dest
config: Control-Host-1
name 10.0.0.10 Control-Host-10 description Comment 10 blue Matching object name in dest
config: Control-Host-10
name 10.0.0.11 Control-Host-11 description Comment 11 blue Matching object name in dest
config: Control-Host-11
```

If You Chose Checkpoint FW-1 dbedit / ofiller CSV Output:

'`od`' Rules and Objects are Output in Odumper/Ofiller CSV Format and '`dbedit`' to Two Files. The file names and a new rulebase name are required.

Objects and Group Names will be translated to the Destination Configuration Bundles names.

To output a '`od`' fomat policy, enter:

- A file name to save the odumper/ofiller format CSV.
- A file name to save the dbedit text.
- A Destination Rulebase name to add to the '`DESTINATION`' firewalls smart centre by loading the dbedit file.

```
      Choose: od
------------------------------------------------------------------------------------------
  Rules Built From Hit Connetions output in Odumper format
------------------------------------------------------------------------------------------
 OUTPUT ODUMPER AND DBEDIT TEXT:


      Enter the name of the CSV file to be saved: nufing.csv


      Enter the name of the dbedit file to be saved: nufing.dbedit


      Enter the name of the Checkpoint FW-1 RULEBASE to write rules to: NuFing



------------------------------------------------------------------------------------------
      FILE: nufing.csv WRITTEN  !!*%*%*-HURRAY-*%*%*!!
------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------
 DBEDIT FILE: nufing.dbedit WRITTEN    !!*%*%*-SWEEET-*%*%*!!
------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

Objects, flattened Network and Service Groups and policy rules are output file.

The new CSV rulebase can be loaded back into 360-FAAR using '`load`' mode.

The new dbedit rulebase can be loaded onto the desired firewall after careful checking and testing in a staging environment.

The CSV can be modified and rebuilt using the '`bldobj`' mode.

If You Chose Netscreen Output:

'ns'	Rules and Objects are Output in `Netscreen ScreenOS6` Format to screen.

Objects and Group Names will be translated to the Destination Configuration Bundles names.

To output a 'ns' fomat policy, enter:

- A Destination Netscreen Configuration, to pull zone matches from object definitions, routes and interfaces, to use to assign zones to the 'SOURCE' configs objects.
- Or Zone CIDR Information
- Or both ^^^ to override 'DESTINATION' Configuration Zone
- If no zones or destination configs are provided the default zone is used for all objects.
- Choose the rule number to start numbering rules with, or accept the default.

```
------------------------------------------------------------------------------------------
  Rules Built From Hit Connetions output in Netscreen ScreenOS format
------------------------------------------------------------------------------------------
 NETSCREEN CONVERSION:

   Define route to zone mappings in the format:
   ZONE IP MASKLENGTH

   type '.' to finish zone input

IN 10.0.0.0 8
INNER 10.0.0.0 12
INNEST 10.0.0.0 18
OUT 0.0.0.0 0
DMZ 172.16.0.0 12
INISH 292.168.0.0 16
             INPUT FORMAT ERROR: enter: ZONENAME IPADDR MASKLENGTH
.

      MAX EXISTING RULE NUM: 16

      Enter a number to override the above rule count or press enter to accept:
```

Rules, groups and objects are output...

```
      …
      …
      …
```

Objects, flattened Network and Service Groups and policy rules are output to STDOUT.

These new rulebases can be copied to a file and loaded back into 360-FAAR using 'load' mode.

If You Chose Cisco ASA Output:

'cs' Rules and Objects are Output in 'Cisco ASA' Format to STDOUT.

Objects and Group Names will be translated to the Destination Configuration Bundles names.

To output a 'od' format policy, Enter:

- A file name to save the odumper/ofiller format objects CSV.
- A Destination access-list name to add to the 'DESTINATION' ASA firewalls configuration.

```
      Choose: cs



-----------------------------------------------------------------------------------------
  Rules Built From Hit Connetions output in Cisco ASA and Odumper CSV format
-----------------------------------------------------------------------------------------
  OUTPUT ODUMPER CSV AND CISCO ASA CMD TEXT TO SCREEN:


      Enter the name of the file to be saved: nuasa.csv


      Enter the name of the access-list to write rules to: NewASA



name 10.0.0.1 Control-Host-1 description Comment 1 blue   TRANSLATED Object:
Management-Host-1 matches the IP of host Control-Host-1
name 10.0.0.10 Control-Host-10 description Comment 10 blue   TRANSLATED Object:
Management-Host-10 matches the IP of host Control-Host-10
name 10.0.0.11 Control-Host-11 description Comment 11 blue   TRANSLATED Object:
Management-Host-11 matches the IP of host Control-Host-11
      …
      …
      …
```

Objects, flattened Network and Service Groups and access-list statements are output to STDOUT.

These new rulebases can be copied to a file and loaded back into 360-FAAR for further analysis using 'load' mode.

Hit Enter To Return To The Menu:

Press enter key with finger.

```
-----------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

8. 'merge' and 'copy' logs modes.

360-FAARs policy engine allows engineers to combine a firewalls logs and its configuration to create a detailed map of all connectivity used, hit counts specific to individual types of traffic and the locations of connections source and destination points.

This map can be related to the firewalls policy and can be used to provide detailed information regarding each rules usage in their current format.

The policy engine can also build new rules from the existing policy and apply the connection map to these new rules instead.

The rules output can be ordered via usage statistics either based on connectivity or how often an object spoke or was spoken to etc. They can also be organised alphanumerically or by their netmask or IP address.

To facilitate this 360-FAAR holds its logs in a pseudo binary format. The logs can be copied or merged with logs from other configurations.

8.1 Copy Logs

Copy logs directly copies one log reference over another deleting forever the log entry it overwrote.

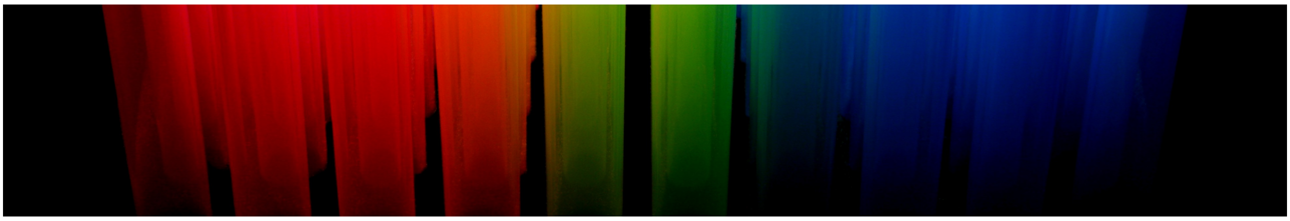
8.2 Merge Logs

Merge logs copies each individual source log entry into the destination log tree, and outputs a count of hits and misses for already existing entries.

Using copy logs you can attach logfiles from already loaded configurations bundles, with historical log file information, to newly loaded current rulebases and process them with 'rr' mode.

Print Mode and Srvc Print Mode Output will not change with the addition of logs from copy log or merge logs mode.

9. 'load' mode



Using 'load' mode you can load new configuration bundles and logs into 360-FAAR

```
     _                 _    ___           __ _         __      _
    | |   ___  __ _ __| |  / __|___ _ _  / _(_)__ _  / _|___  | |   ___  __ _ ___
    | |__/ _ \/ _` / _` | | (__/ _ \ ' \|  _| / _` | > _|_ _| | |__/ _ \/ _` (_-<
    |____\___/\__,_\__,_|  \___\___/_||_|_| |_\__, | \_____|  |____\___/\__, /__/
                                              |___/                     |___/
------------------------------------------------------------------------------------------
    SPECIFY A NEW CONFIG BUNDLE TO LOAD:

       Enter the type of the new config to load in the format:
       Odumper/Ofiller Config File      = od
       Netscreen Config File            = ns
       Cisco Config File                = cs
```

You should enter one of the following configuration types:

- Enter '**od**' to load a Checkpoint Firewall-1 configuration in odumper format
- Enter '**ns**' to load a Juniper Netscreen Firewall configuration in 'get config' format
- Enter '**cs**' to load a Cisco ASA Firewall config in 'show run' format.

You will be asked to enter the file name of the configuration:

```
       Enter the name of the new config file to load
```

Enter the name of an existing file. For the purpose of the examples in this manual, we are going to load one of the TestData files supplied in the 360AnalyticsLtd Zip file.

Enter one of the Test Data CSV file names:

TestData.csv

You will then be asked to enter the name of the log file to analyse the firewall configuration with:

```
       Enter the name of the new log file to load, or type '.' to skip
```

The log file should be in the following formats:

• Checkpoint Firewall-1:	logexported text files
• Cisco ASA:	syslog format text files
• Juniper Netscreen:	syslog format text files

Or you can skip this step by typing `'.'` To use the TestData, skip this step.

NOTE: skipping log file loading disables several of 360-FAAR's modes.

The next prompt asks you to enter a valid NAT file for processing:

```
Enter the name of the new nats file to load, or type '.' to skip
```

NAT files can be added in the formats:

- FWDoc CSV format
- FWRules CSV format

Or you can skip this step by typing `'.'` To use the TestData, skip this step.

NOTE: NAT files are optional for Cisco and Netscreen configurations because the NAT config info is included in the main config file its self.

10. Help Mode Output

Help outputs the following text:

```
    Chose one: help


     _  _     _         __  __
    | || |___| |_ __   |  \/  |___ _ _ _  _
    | __ / -_) | '_ \  | |\/| / -_) ' \ || |
    |_||_\___|_| .__/  |_|  |_\___|_||_\_,_|
               |_|

    360-FAAR v0.4.6 HELP MENU:
    ------------------------------------

      print  = Prints the details relating to all objects name, ip, rule and policy
usage, group membership, supernets,
               subnets, hosts on networks, etc to a headded CSV, and a reduced csv to the
screen for info.

       fltprint = Prints the same format object analysis spreadsheet as 'print' and
allows you to specify inclusive and
               exclusive, text and CIDR filtering of the objects output.

      rr     = Rationalize selected rules together and filter using CIDR and strings if
required
               Pull encryption rules from a second config (if traffic is encrypted
between to and from firewalls)
               Merge to a third firewall cluster and match and filter existing
connectivity out of new rules.
               This process can also translate objects and groups and gives details in
the od, cs and ns output stage
               in the commemts section of the object definitions.
               This mode has three rule build methods. The dst src, service, and original
rule filter and regroup.

      bldobj        = Resolve rule objects from odumper format file and translate objects
and rules to a new firewall cluster
               Identify objects from the file using two of the loaded configuations and
enter a third to translate
               objects to and write details to the comments.
               USE this mode to allow you to read modified or new rulebases and associate
objects from the configs
               before writing the dbedit to make the rules to the screen and an od format
file

      load   = Load a new config bundle.  Loading an existing config name will overwrite
the existing config.
               This mode allows you to add new config bundles to an already runing
instance of 360-FAAR.
               With this mode, and copylog mode, you can load an updated config file and
associate an already loaded
               log for use in rr mode rationalizations

      copylog       = Associate an existing log with a different config.  The original
log will be over written.
               This mode copies log information for rr mode rationalizations only, print
mode info will be unaffected.

       mergelog = Merge a binary log from one config with another config.  The FROM log
entries will be merged with the
               destination TO log entries.  Use this mode to update an existing
configurations binary log info.
```

```
      exit   = EXIT the script.

    Output Types:
    ------------------------------------

      od     = The legendary odumper/ofiller format with rules on, defaults on, object
checking off
               and nats in the legendary fwdoc csv file format

               rr mode    - Outputs odumper format files of its suggested policies, and
at the moment uses a blank
                            field for "Any" rules so that the files can be read by
ofiller, and you can diff
                            mine and fillers dbedit output for double consistency!!.
                            It also the dbedit to create the rulebase to the screen.
                            The dbedit objects and groups are translated, the csv file
is not

               bldobj mode- outputs the same file and dbedit but keeps comments and
rules from the input config
                          - use the numberrules helper script to make the csv's more
readable, modify the csv's
                            and then read them in this or odumper format using the
bldobj mode.
                            The dbedit and the csv files objects and groups are
translated, rule comments are kept

      ns     = Netscreen ScreenOS 6 format, you need supply either a netscreen config to
merege to, or
               ZONE IP NM statements when you output the commands to update the
firewalls, or both, if you want to
               override the configs default route zone

      cs     = Cisco.  Output objects and groups in ASA 8.4+ format, and rules as ACE's
in an access list name
               specified during the output stage.

    ---------------------------------------------------------

-----------------------------------------------------------------------------------------
 Hit Enter to return to the menu...
```

11. Exit 360-FAAR

11.1 Exit the script

Exit!

End of 360-FAAR User Guide

Contact and Company Details

360 Analytics Ltd.

LUTIDINE HOUSE
NEWARK LANE
RIPLEY, SURREY
UNITED KINGDOM
GU23 6BS
TEL: +447960 028 070
Company No. 07533060

- For General Information Visit: www.360-faar.com
- For Further info please visit the blog: 36zeroanalytics.wordpress.com
- For General Queries Please Contact: info@360-faar.com