



Suricata IDS/IPS

Help and Quick Start Guide

Instructions for Windows

tested on Win XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008R2 64 bit.

Date: 24 May 2012

Version: 1.1

Author: Peter Manev





BEFORE YOU START SURICATA IDS/IPS	3
Rules	3
Configuration	4
Running Suricata	8
MORE INFO AND DOCUMENTATION	11



Before you start Suricata IDS/IPS

You **MUST** have [WinPcap](#) installed in order to run Suricata IDS/IPS !

Rules

You will need rules, because Suricata inspects traffic based on rules. The rules usually reside in the “*INSTALLDIR\rules*” directory. There are non-installed by default. You can install them in any directory you wish, just make sure you change the path in the suricata.yaml configuration file.

You can get them from:

- ✓ [Emerging Threads](#) – the rules there are specially tailored for Suricata, in order to use its abilities to the maximum.
- ✓ [Snort](#) – Snort IDS/IPS developed by [Sourcefire](#).
- ✓ Write them yourself – if you have previous experience or you would like just a specific traffic to be inspected, you can write the necessary rules by yourself. You can find some more info on rule writing here:
 - [Snort Rule Writing Manual](#)
 - [Suricata Rule Writing Manual](#)

After you have the rules – specify which rules would you like to activate or deactivate. For example, if you would like to deactivate a rule put a “#” at the beginning of the line:

```
580 # Set the default rule path here to search for the files.
581 # if not set, it will look at the current working dir
582 default-rule-path: c:/suricata/rules/
583 rule-files:
584 - attack-responses.rules
585 - backdoor.rules
586 - bad-traffic.rules
587 - chat.rules
588 - ddos.rules
589 - deleted.rules
590 - dns.rules
591 - dos.rules
592 - experimental.rules
593 - exploit.rules
594 - finger.rules
595 - ftp.rules
596 # - icmp-info.rules
597 # - icmp.rules
598 # - imap.rules
599 # - info.rules
600 # - local.rules
601 # - misc.rules
602 # - multimedia.rules
```

The ones in green are deactivated.

Configuration

It is important that you configure Suricata properly.

Suricata's configuration file is called "suricata.yaml" and holds special syntaxes and all your configurational variables – i.e. networks, interfaces, log/rules directories and many more.

Suricata.yaml already has default values and config options, here we will go over some of them very briefly, so that you can get acquainted better.

For example , if you are not happy with the default options you can change them

–

```
"default-log-dir: C:\Suricata\log
```

```
.....
```

```
- file:
```

```
  enabled: yes
```

```
  filename: C:\Suricata\suricata.log
```

```
.....
```

```
default-rule-path: C:\Suricata\rules\
```

```
classification-file: C:\Suricata\classification.config
```

```
.....
```

```
HOME_NET: "[192.168.0.0/16]" - (here actually you put any network you want Suricata to inspect)
```

```
"
```

or in some graphic:

```
suricata.yaml
22 # Preallocated size for packet. Default is 1514 which is the classical
23 # size for pcap on ethernet. You should adjust this value to the highest
24 # packet size (MTU + hardware header) on your system.
25 #default-packet-size: 1514
26
27 # Set the order of alerts based on actions
28 # The default order is pass, drop, reject, alert
29 action-order:
30 - pass
31 - drop
32 - reject
33 - alert
34
35
36 # The default logging directory. Any log or output file will be
37 # placed here if its not specified with a full path name. This can be
38 # overridden with the -l command line parameter.
39 default-log-dir: C:\Suricata\log
40
41 # Configure the type of alert (and other) logging you would like.
42 outputs:
43
44 # a line based alerts log similar to Snort's fast.log
45 - fast:
46     enabled: yes
47     filename: fast.log
48     append: yes
49
50 # log output for use with Barnyard
51 - unified-log:
52     enabled: no
53     filename: unified.log
54
55     # Limit in MB.
56     #limit: 32
57
```

Normal text file length: 23826 lines: 661 Ln: 39 Col: 33 Sel: 0 Dos\Windows ANSI as UTF-8 INS

```
suricata.yaml
461 #
462 # This value is overridden by the SC_LOG_FORMAT env var.
463 #default-log-format: "[%i] %t - (%f:%l) <%d> (%n) -- "
464
465 # A regex to filter output. Can be overridden in an output section.
466 # Defaults to empty (no filter).
467 #
468 # This value is overridden by the SC_LOG_OP_FILTER env var.
469 default-output-filter:
470
471 # Define your logging outputs. If none are defined, or they are all
472 # disabled you will get the default - console output.
473 outputs:
474 - console:
475   enabled: yes
476 - file:
477   enabled: yes
478   filename: C:\Suricata\suricata.log
479 - syslog:
480   enabled: no
481   facility: local5
482   format: "[%i] <%d> -- "
483
484 # PF_RING configuration. for use with native PF_RING support
485 # for more info see http://www.ntop.org/PF_RING.html
486 pfring:
487 # Number of receive threads (>1 will enable experimental flow pinned
488 # runmode)
489 threads: 1
490
491 # Default interface we will listen on.
492 interface: eth0
493
494 # Default clusterid. PF_RING will load balance packets based on flow.
495 # All threads/processes that will participate need to have the same
496 # clusterid
```

Normal text file | length: 23826 lines: 661 | Ln: 478 Col: 28 Sel: 11 | Dos\Windows | ANSI as UTF-8 | INS

```
suricata.yaml
514 ipfw:
515
516 # Reinject packets at the specified ipfw rule number. This config
517 # option is the ipfw rule number AT WHICH rule processing continues
518 # in the ipfw processing system after the engine has finished
519 # inspecting the packet for acceptance. If no rule number is specified,
520 # accepted packets are reinjected at the divert rule which they entered
521 # and IPFW rule processing continues. No check is done to verify
522 # this will rule makes sense so care must be taken to avoid loops in ipfw.
523 #
524 ## The following example tells the engine to reinject packets
525 # back into the ipfw firewall AT rule number 5500:
526 #
527 # ipfw-reinjection-rule-number: 5500
528
529 # Set the default rule path here to search for the files.
530 # if not set, it will look at the current working dir
531 default-rule-path: C:\Suricata\rules\
532 rule-files:
533 - emerging-current_events.rules
534
535 classification-file: C:\Suricata\classification.config
536 #reference-config-file: /etc/suricata/reference.config
537
538 # Holds variables that would be used by the engine.
539 vars:
540
541 # Holds the address group vars that would be passed in a Signature.
542 # These would be retrieved during the Signature address parsing stage.
543 address-groups:
544
545 HOME_NET: "[192.168.0.0/16]"
546
547 EXTERNAL_NET: any
548
549 FTN_SERVERS: !HOME_NET
```

Normal text file | length: 23826 | lines: 661 | Ln: 531 | Col: 31 | Sel: 11 | Dos\Windows | ANSI as UTF-8 | INS

Please make sure that the directories are created or exist (if you decide to change the default ones)!!

Running Suricata

Open a cmd and go to your Suricata Directory OR just double click the icon on your desktop and execute:


```
Administrator: C:\Windows\System32\cmd.exe - suricata.exe -c suricata.yaml -i 192.168.1.71
filename: http.log
[4452] 6/11/2011 -- 19:06:14 - <alert-debuglog.c:542> <Info> <AlertDebugLogInitCtx> -- Alert debug log output
initialized, filename: alert-debug.log
[4452] 6/11/2011 -- 19:06:14 - <alert-syslog.c:170> <Info> <AlertSyslogInitCtx> -- Syslog output initialized
[4452] 6/11/2011 -- 19:06:14 - <log-droplog.c:176> <Info> <LogDropLogInitCtx> -- Drop log output initialized.
filename: drop.log
[4452] 6/11/2011 -- 19:06:14 - <runmode-pcap.c:126> <Info> <ParsePcapConfig> -- Unable to find pcap config for
interface \Device\NPF_{DD7E8C68-52C7-439D-B3A7-199ABB22A849}, using default value
[668] 6/11/2011 -- 19:06:14 - <source-pcap.c:318> <Info> <ReceivePcapThreadInit> -- using interface \Device\NPF_{DD7E8C68-52C7-439D-B3A7-199ABB22A849}
[668] 6/11/2011 -- 19:06:14 - <source-pcap.c:359> <Info> <ReceivePcapThreadInit> -- Going to use pcap buffer s
ize of 0
[4452] 6/11/2011 -- 19:06:14 - <runmode-pcap.c:229> <Info> <RunModeIdsPcapAuto> -- RunModeIdsPcapAuto initiali
sed
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:346> <Info> <StreamTcpInitConfig> -- stream "max_sessions": 26214
4
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:358> <Info> <StreamTcpInitConfig> -- stream "prealloc_sessions":
32768
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:368> <Info> <StreamTcpInitConfig> -- stream "memcap": 33554432
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:374> <Info> <StreamTcpInitConfig> -- stream "midstream" session p
ickups: disabled
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:380> <Info> <StreamTcpInitConfig> -- stream "async_oneside": disa
bled
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:397> <Info> <StreamTcpInitConfig> -- stream "checksum_validation"
: enabled
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:407> <Info> <StreamTcpInitConfig> -- stream."inline": disabled
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:416> <Info> <StreamTcpInitConfig> -- stream.reassembly "memcap":
67108864
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:426> <Info> <StreamTcpInitConfig> -- stream.reassembly "depth": 1
048576
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:449> <Info> <StreamTcpInitConfig> -- stream.reassembly "to_server_
chunk_size": 2560
[4452] 6/11/2011 -- 19:06:14 - <stream-tcp.c:451> <Info> <StreamTcpInitConfig> -- stream.reassembly "to_client_
chunk_size": 2560
[4452] 6/11/2011 -- 19:06:14 - <tm-threads.c:1806> <Info> <TmThreadWaitOnThreadInit> -- all 16 packet processi
ng threads, 3 management threads initialized, engine started.
```

NOTE:

If you need to run Suricata on a un-ip'd interfaces (thanks to Rich Rumble for pointing that out):

You can get the NIC UUID in a variety of ways, the simplest is using a single command for WMIC:(from cmd prompt paste in the following)

```
wmic nicconfig get ipaddress,SettingID
```

If you know your NIC's IP you can filter the results with findstr:

```
wmic nicconfig get ipaddress,SettingID | findstr 1.2.3.4
```



(replace 1.2.3.4 with your NIC's IP)

Then use that as your interface argument:

```
suricata.exe -c suricata.yaml -i \\DEVICE\NPF_{EE7B2A76-9343-449F-B3D8-3CB0F37DCA49}
```

Make sure the double slashes are used, and a backslash is placed before the curly braces!

More Info and Documentation

You can find much more info about setting up and tuning Suricata here:

<https://redmine.openinfosecfoundation.org/projects/suricata/wiki>

If you would like to compile Suricata from scratch on your windows system please find detailed step by step guide here -

<https://redmine.openinfosecfoundation.org/projects/suricata/files>

