



## Suricata

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its **supporting vendors**.

### Top 3 Reasons You Should Try Suricata:

#### 1. Highly Scalable

Suricata is multi threaded. This means you can run one instance and it will balance the load of processing across every processor on a sensor Suricata is configured to use. This allows commodity hardware to achieve 10 gigabit speeds on real life traffic without sacrificing ruleset coverage.

#### 2. Protocol Identification

The most common protocols are automatically recognized by Suricata as the stream starts, thus allowing rule writers to write a rule to the protocol, not to the port expected. This makes Suricata a Malware Command and Control Channel hunter like no other. Off port HTTP CnC channels, which normally slide right by most IDS systems, are child's play for Suricata! Furthermore, thanks to dedicated keywords you can match on protocol fields which range from http URI to a SSL certificate identifier.

#### 3. File Identification, MD5 Checksums, and File Extraction

Suricata can identify thousands of file types while crossing your network! Not only can you identify it, but should you decide you want to look at it further you can tag it for extraction and the file will be written to disk with a meta data file describing the capture situation and flow. The file's MD5 checksum is calculated on the fly, so if you have a list of md5 hashes you want to keep in your network, or want to keep out, Suricata can find it.

*Suricata has many more **great features**, and we hope you give it a run. It's free, it's fast, and it's going to be here long term!*

## RELEASES

Stable 2.0.3  
Development 2.1beta1

## TWITTER

Follow @Suricata\_IDS

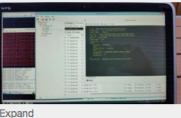
**Zentyl** @zentyl 16 Sep  
#HowTo install IDS on #Zentyl Server: [bit.ly/1oJscD7](http://bit.ly/1oJscD7) by using #Suricata  
t3 Retweeted by Suricata IDS/IPS  
Expand

**Network Security age** @Networksecur\_ag 16 Sep  
Suricata Intrusion Detection: Part Four [ift.tt/1qYUgDY](http://ift.tt/1qYUgDY) #networksecurity  
t3 Retweeted by Suricata IDS/IPS  
Expand

**Jasonish** @jasonish 12 Sep  
#Suricata + ELK in Docker [blog.jasonish.org/2014/09/suricata...](http://blog.jasonish.org/2014/09/suricata...)  
t3 Retweeted by Suricata IDS/IPS  
Expand

**Drizt** @drizt\_dourden 12 Sep  
#Suricata stats.log parser [github.com/dendewey/Suricata...](https://github.com/dendewey/Suricata-Stats-Log-Parser)  
t3 Retweeted by Suricata IDS/IPS  
Show Summary

**Erik Barnett** @Erik\_Barnett 9 Sep  
@stelligence \* #suricata logs are now being collected/sent to the #mongodb \* Oh the goodness I'm seeing. WOOT! [pic.twitter.com/psauxOq3h](http://pic.twitter.com/psauxOq3h)  
t3 Retweeted by Suricata IDS/IPS



Expand



## SEARCH

SEARCH

## LINKS

Eric Leblond (regli)

OISF

Planet Suricata

Redmine development

Victor Julien (inliniac)

## FOLLOW SURICATA NEWS VIA EMAIL

Enter your email address to follow this blog and receive notifications of new posts by email.

FOLLOW

## META

Register

Log in

Entries RSS

Comments RSS

Blog at WordPress.com.