

Suricata User Guide

This is the documentation for Suricata 9.0.0-dev.

- [1. What is Suricata](#)
 - [1.1. About the Open Information Security Foundation](#)
- [2. Quickstart guide](#)
 - [2.1. Installation](#)
 - [2.2. Basic setup](#)
 - [2.3. Signatures](#)
 - [2.4. Running Suricata](#)
 - [2.5. Alerting](#)
 - [2.6. EVE Json](#)
- [3. Installation](#)
 - [3.1. Source](#)
 - [3.2. Binary packages](#)
 - [3.3. Advanced Installation](#)
- [4. Upgrading](#)
 - [4.1. General instructions](#)
 - [4.2. Upgrading to 9.0.0](#)
 - [4.3. Upgrading to 8.0.1](#)
 - [4.4. Upgrading 7.0 to 8.0](#)
 - [4.5. Upgrading 6.0 to 7.0](#)
 - [4.6. Upgrading 5.0 to 6.0](#)
 - [4.7. Upgrading 4.1 to 5.0](#)
- [5. Security Considerations](#)
 - [5.1. Running as a User Other Than Root](#)
 - [5.2. Containers](#)
- [6. Support Status](#)
 - [6.1. Levels of Support](#)
 - [6.2. Distributions](#)
 - [6.3. Architecture Support](#)

- 7. Command Line Options
 - 7.1. Unit Tests
- 8. Suricata Rules
 - 8.1. Rules Format
 - 8.2. Meta Keywords
 - 8.3. Ethernet Keywords
 - 8.4. IP Keywords
 - 8.5. TCP keywords
 - 8.6. UDP keywords
 - 8.7. ICMP keywords
 - 8.8. IGMP keywords
 - 8.9. Payload Keywords
 - 8.10. Integer Keywords
 - 8.11. Transformations
 - 8.12. Prefiltering Keywords
 - 8.13. Flow Keywords
 - 8.14. Bypass Keyword
 - 8.15. HTTP Keywords
 - 8.16. File Keywords
 - 8.17. DNS Keywords
 - 8.18. mDNS Keywords
 - 8.19. LLMNR Keywords
 - 8.20. SSL/TLS Keywords
 - 8.21. SSH Keywords
 - 8.22. JA3/JA4 Keywords
 - 8.23. Modbus Keyword
 - 8.24. DCERPC Keywords
 - 8.25. DHCP keywords
 - 8.26. DNP3 Keywords
 - 8.27. ENIP/CIP Keywords
 - 8.28. FTP/FTP-DATA Keywords
 - 8.29. Kerberos Keywords
 - 8.30. SMB Keywords
 - 8.31. SNMP keywords
 - 8.32. NTP Keywords
 - 8.33. Base64 keywords
 - 8.34. SIP Keywords
 - 8.35. SDP Keywords
 - 8.36. SCTP Keywords
 - 8.37. RFB Keywords

- 8.38. MQTT Keywords
- 8.39. IKE Keywords
- 8.40. HTTP2 Keywords
- 8.41. Quic Keywords
- 8.42. NFS Keywords
- 8.43. SMTP Keywords
- 8.44. WebSocket Keywords
- 8.45. Generic App Layer Keywords
- 8.46. Generic Decode Layer Keywords
- 8.47. Xbits Keyword
- 8.48. Alert Keywords
- 8.49. Thresholding Keywords
- 8.50. IP Reputation Keyword
- 8.51. IP Addresses Match
- 8.52. Config Rules
- 8.53. Datasets
- 8.54. Lua Scripting for Detection
- 8.55. Differences From Snort
- 8.56. Multiple Buffer Matching
- 8.57. Tag
- 8.58. VLAN Keywords
- 8.59. LDAP Keywords
- 8.60. PGSQL Keywords
- 8.61. Email Keywords
- 8.62. Rule Types and Categorization
- 8.63. Rule Processing
- 9. Rule Management
 - 9.1. Rule Management with Suricata-Update
 - 9.2. Adding Your Own Rules
 - 9.3. Rule Reloads
 - 9.4. Rules Profiling
- 10. Making sense out of Alerts
- 11. Performance
 - 11.1. Runmodes
 - 11.2. Packet Capture
 - 11.3. Tuning Considerations
 - 11.4. Hyperscan
 - 11.5. High Performance Configuration
 - 11.6. Statistics
 - 11.7. Ignoring Traffic

- 11.8. Packet Profiling
- 11.9. Rule Profiling
- 11.10. Tcmalloc
- 11.11. Performance Analysis
- 12. Configuration
 - 12.1. Suricata.yaml
 - 12.2. Global-Thresholds
 - 12.3. Exception Policies
 - 12.4. Snort.conf to Suricata.yaml
 - 12.5. Multi Tenancy
 - 12.6. Dropping Privileges After Startup
 - 12.7. Using Landlock LSM
 - 12.8. systemd notification
 - 12.9. Includes
- 13. Reputation
 - 13.1. IP Reputation
- 14. Init Scripts
- 15. Output
 - 15.1. EVE
 - 15.2. Lua Output
 - 15.3. Syslog Alerting Compatibility
 - 15.4. Custom tls logging
 - 15.5. Log Rotation
- 16. Lua support
 - 16.1. Lua usage in Suricata
 - 16.2. Lua functions
 - 16.3. Lua Libraries
- 17. File Extraction
 - 17.1. Architecture
 - 17.2. Settings
 - 17.3. Output
 - 17.4. Rules
 - 17.5. MD5
 - 17.6. Updating Filestore Configuration
- 18. Protocols
 - 18.1. App-Layer

- 18.2. Further Reading
- 19. Public Datasets (PCAPs)
- 20. Using Capture Hardware
 - 20.1. AF_PACKET
 - 20.2. Endace DAG
 - 20.3. Napatech
 - 20.4. Myricom
 - 20.5. eBPF and XDP
 - 20.6. Netmap
 - 20.7. AF_XDP
 - 20.8. DPDK
 - 20.9. PCAP File Reading
- 21. Interacting via Unix Socket
 - 21.1. Introduction
 - 21.2. Commands in standard running mode
 - 21.3. Commands on the cmd prompt
 - 21.4. PCAP processing mode
 - 21.5. Build your own client
- 22. Plugins
 - 22.1. nDPI
- 23. IPS Mode
 - 23.1. IPS Concept
 - 23.2. Setting up IPS/inline for Linux
 - 23.3. Setting up IPS/inline for Windows
- 24. Firewall Mode
 - 24.1. Firewall Mode Design
 - 24.2. Firewall Ruleset Examples
 - 24.3. Firewall Mode Stats
- 25. 3rd Party Integration
 - 25.1. Symantec SSL Visibility (BlueCoat)
- 26. Man Pages
 - 26.1. Suricata
 - 26.2. Suricata Socket Control
 - 26.3. Suricata Control
 - 26.4. Suricata Control Filestore

- [27. Acknowledgements](#)
- [28. Licenses](#)
 - [28.1. GNU General Public License](#)
 - [28.2. Creative Commons Attribution-NonCommercial 4.0 International Public License](#)
 - [28.3. Suricata Source Code](#)
 - [28.4. Suricata Documentation](#)
- [29. Suricata Developer Guide](#)
 - [29.1. Working with the Codebase](#)
 - [29.2. Contributing](#)
 - [29.3. Suricata Internals](#)
 - [29.4. Extending Suricata](#)
 - [29.5. LibSuricata and Plugins](#)
 - [29.6. Upgrading](#)
- [30. Verifying Suricata Source Distribution Files](#)
 - [30.1. Verification Steps](#)
- [31. Appendix](#)
 - [31.1. EVE JSON Schema](#)
 - [31.2. EVE Index](#)