Agenda

• Intro / Recap
• Methodology
• New Tests, New Results
• Battle Royale: Suricata vs. Snort 2 and Snort 3
• Summary
What we learned from last time
A very brief recap
Key Findings from Suricon 2017

• We performed over 23 distinct test scenarios for Suricon 2017, results in appendix (to be included in posted copy)
• Here are a few of the key findings related to performance we learned at the time
1. Suricata Gets better with age!

- **Suricata 2.0.9**
- **Suricata 3.0.2**
- **Suricata 3.2.4**
- **Suricata 4.0.1**
- **Suricata 4.0.1 --disable-gccmarch-native**

---

**Graph:**
- X-axis: Seconds
- Y-axis: Megabits/s
- Suricata 2.0.9 Breakingpoint
- Suricata 4.0.1 Breakingpoint

---

**Legend:**
- Suricata 2.0.9
- Suricata 3.0.2
- Suricata 3.2.4
- Suricata 4.0.1
- Suricata 4.0.1 --disable-gccmarch-native
2. Suricata Scales Nicely!

And scales nicely as long as you have available cores (16 in this example)
3. Most features have negligible impact on performance

- Network Profiling logged all DNS/HTTP/SSL transactions
- File Store only matched on select HTTP files, while file logging logged all files on all protocols
Key Areas of interest from the Community

• What about the latest and greatest versions of Suricata?
  – Suricata 4.1 and Suricata 5.0 (including new feature perf)
  – Hyperscan on modern processing
• How do rulesets and signatures impact performance?
• How does Suri differ from Snort with respect to performance?
Test Methodology: Suricon 2019
Test Methodology Overview: HW

- Traffic Generation Equipment: Ixia PerfectStorm1 Fusion
- Dell PowerEdge R730
  - 2 x 14-core Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz
    - We limit thread count to match generation HW
  - 64GB RAM DDR4 2400Mhz
  - 4 port Intel 1Gbit I350 Interface Card
Test Methodology Overview: SW

- Ubuntu 16.04
- Suricata (various), Snort
- AF_Packet Mode
- ETPro Signature Pack
  10/15/2019 (final tests)
- Latest Snort rules
  download on
  10/15/2019
- Breakingpoint 8.4.0
Test Topology

2x direct connect 1Gbps Interfaces

Out of Band Management

Laptop for Executing Tests
Test Methodology

• Controls:
  – Same traffic profile
  – Same HW/OS
  – Same method to identify breaking point
  – Canary Traffic
  – Each test we run up to 1Gbps in each direction (max 2Gbps) plus Canary Traffic
  – Suricata Version, Base Configuration, Signature Set
    • *Except in specific tests which measure these configurations.

• Steps:
  – Compile and/or Configure Suricata / Snort based on given test.
  – Run Ixia Test
  – Collect Results
  – Restart Suricata / Snort for next test (fresh process each round.)
Test Traffic Description

• Ixia features over 3k Applications/Protocols, including real world apps. Traffic is generated at test setup, and is rich in content, and also varied.

• Ensures that you are not just replaying the same traffic over and over, while giving tester complete control of crafting the test and measuring the results.

• Protocols / Distribution (in BW)
  - SSL: 32%
  - Skype: 3%
  - HTTP Text: 7%
  - Pandora 4%
  - NTP: .5%
  - DNS 2%
  - HTTP Video: 11%
  - SMTP: 11%
  - NetFlix: 11%
  - SSH: 2%
  - Video Call/Conference: 10%
  - HTTP Audio: 4%
  - FTP: 2.5%

• Canary Test Traffic
  - Continuously trigger 2018885 (Windows XP Command.exe Shell Connection) throughout tests (Suricata set to drop) to ensure active detection.
Traffic Ramp Profile

- We use a stair-step approach to continuously increase the load/session rate of the system. We fully open/transmit data/close sessions.

- Every Second we increase the session setup rate by 65 up to 3 mins
Baseline Suricata Configuration

• Suricata 5.0.0, default compilation
• AF_Packet, 8 traffic threads (4 send / 4 receive)
• Only Eve logging, no pcap, filestore, or debug
• No profiling
• All stock flow settings for Suricata 5.0
  – Hyperscan
  – Rust
  – Medium Detection Profile
Suricata ETPro Policy

- All ETPro Signatures (10/15/2019) enabled in alert mode
  - Roughly 48,000 Signatures
- Canary Signature 2018885 set to Drop to ensure that detection is active.
Determining Breakingpoint

• We want to identify the maximum performance at which Suricata is operating at its full capacity.

• Ensure the following:
  – Consistent Performance
  – No Packet Loss
  – No Session setup or Application Transaction Failures
  – Suricata’s detect is not degraded (e.g. repeated canary attack to make sure Suricata is not missing traffic.)

• Once breakingpoint is found (above), we identify the highest performance observed prior to that point.
  – While Suricata can go much higher, it will have real world impacts. We’re not concerned about absolute performance numbers, but more around rate of change.

• Run each test 3 times and pick the median performance result
Determining Breakingpoint

- Example Scenarios
- Flow Exceptions
- Application Transaction Failure
- Attacks not blocked
We will publish all test reports!

• I got special permission from Ixia/Breakingpoint this year that we can share the full test results (including the Breakingpoint test configs if you have a Breakingpoint to recreate the traffic).

• Over 3GB of Test Reports in PDF format, everything you ever wanted to know about Suricata Performance Testing and much more!
  – Including reports from all tests in 2017 and 2019

• Will provide the location after talk and update this presentation for posting with the location.
That was then, this is now

New Tests, New Results, New Insights
What we’re going to look at

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suricata Version Impact</td>
<td>Pick up where we left off by testing Suricata 4.0, 4.1, and 5.0</td>
</tr>
<tr>
<td>Hyperscan Impact</td>
<td>Retest Hyperscan impact on performance w/Suricata 5.0</td>
</tr>
<tr>
<td>Optimized Rules</td>
<td>How ETPro optimized rules impact performance</td>
</tr>
<tr>
<td>Rule Counts and Performance</td>
<td>How the quantity of rules impacts performance</td>
</tr>
<tr>
<td>Poorly Written Rules</td>
<td>How rules that are poorly written can have a big impact on performance</td>
</tr>
</tbody>
</table>
Contemporary Suricata Performance

- Note, the slight performance drop from 4.0 to 4.1 is likely due to the shift to Rust being on by default (but very worth the extra security!)
- Hyperscan provides a large performance boost over stock Aho-Corasick!
Optimized Rule Versions and Performance (Suricata 5.0)

- Suricata 2.0 Optimized: 1220 Mbps
- Suricata 4.0 Optimized: 1400 Mbps
- Suricata 5.0 Optimized: 1500 Mbps

Suricata 5.0 optimized ruleset also includes JA3 rules not in Suricata 2 or 4 optimized rulesets.
Rule Quantity Impact on Perf

- **Suricata 5.0 (No Rules)**: 1600 Mbps
- **Suricata 5.0 (10k Rules)**: 1560 Mbps
- **Suricata 5.0 (25k Rules)**: 1500 Mbps
- **Suricata 5.0 (All ETPro Rules)**: 1500 Mbps

Mbps values are based on different rule quantities, with Suricata 5.0 (No Rules) achieving the highest Mbps at 1600 Mbps.
Tip your Sig Writers!


I have a ton more test results including from new features like Suricata Rule Transforms, File Store, and other bad signature scenarios. Will post the test results with the deck so we can keep this presentation at 30 mins.
Battle Royale: Suricata vs. Snort

The main event
## What we’re going to look at

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suricata 5.0</td>
<td>Suricata 5.0, All ETPro Rules, AF_Packet</td>
</tr>
</tbody>
</table>
| Snort 2.9.15 (Single Instance)    | Snort 2.9.15, AF_Packet  
  • All ETPro Rules  
  • Talos Community Only Rules  
  • Talos Registered Rules |
| Snort 3.0 Beta, 1 Thread           | Snort 3.0 Beta, AF_Packet  
  • Talos Community Only Rules  
  • Talos Registered Rules     |
| Snort 3.0 Beta MultiThread         | Snort 3.0 Beta, AF_Packet,  
  • Talos Community Only Rules  
  • Talos Registered Rules     |
Notes on Snort Deployments

• Used all default compilation and configuration options except:
  • Disabled alert logging (which impacted performance when left on by default)
  • Ran in AF-Packet Mode
  • Focused only on compiled rules, did not include Shared Object Rules (but those are not the same rules as the compiled ones, and adding them would negatively impact performance)
  • Snort 3, we do not officially support that for ETPro yet, so only tested with Community and Registered Rules
  • Same exact test traffic, same device used for Suri testing
Snort 2.9.15 vs. Suri 5

• Community (3900 sigs)
• Registered
  – (12195 sigs)
• ETPro All
  – (48k sigs)
• Suricata 5
  – ETPro All
  – 48k sigs
  – *Note that Suricata AF_Packet must have 2 Threads (one per interface). Cannot run AF_Packet in Single Mode
  – ** Still Suricata is almost 5x faster than Snort if we factor this in!
Snort 3 Beta

• Community Rules
  – 3488

• Registered Rules
  – 12261

• Snort 3 MultiThread
  – Community Rules

• Suricata 5
  – 48k rules
Just the facts: Suricata vs. Snort

• Snort is ok for <300Mbps deployments, but really shows it’s age, particularly if deployed inline

• Multi-Instance of Snort is not equivalent to Suricata!
  – Much more complex configuration, requires more expensive hardware, more difficult to operate and troubleshoot, lots of output logs to monitor. Simply no comparison to Suricata!

• Snort 3:
  – Has been in alpha / beta for ~5+ years, development started in 2005!*
  – Lots of dependencies, build process poorly documented
  – Multi-thread doesn’t appear stable for AFPacket
  – Performance is lower head to head
  – Suricata has overtaken Snort on features, stability, release velocity

*Source: Marty Roesch, CanSecWest 2008: https://cansecwest.com/csw08/csw08-roesch.pdf
Summary
In Summary

- Suricata performance is rock solid and scalable even as new features are introduced
- Most features have minimal impact on performance
- Rule performance is very scalable, so long as you have high quality rules
- Suricata dramatically beats Snort in performance and rule scale, Snort 3 does not appear ready for primetime
- Many more tests and scenarios we want to evaluate!
Appendix
Including full results from Suricon 2017
## Test Matrix

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suricata Version Perf Comparison</td>
<td>Same Config, test on Suricata 2.0.9, 3.0.2, 3.2.4, and 4.0.1</td>
</tr>
<tr>
<td>ETPro Rule Impact</td>
<td>1 Rule, 12,000 Rules, 37,000 Rules</td>
</tr>
<tr>
<td>Suricata mode performance</td>
<td>AutoFP vs. Workers</td>
</tr>
<tr>
<td>Suricata Thread Count Performance</td>
<td>1, 2, 4, 8, 16 send/receive thread performance (so 2, 4, 8, 16, 32 threads total)</td>
</tr>
<tr>
<td>Pattern Matching Algorithm</td>
<td>AC, AC-BS, AC-KS, Hyperscan</td>
</tr>
<tr>
<td>Detect Engine Profile</td>
<td>Low, Med, High, Custom (Documented High Performance)</td>
</tr>
<tr>
<td>GCC Native Arch</td>
<td>On/Off</td>
</tr>
</tbody>
</table>

Note that aside from Suricata version performance test, all other tests are on 4.0.1
<table>
<thead>
<tr>
<th>Test Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Logging</td>
<td>Enable File Logging and test impact</td>
</tr>
<tr>
<td>File Store</td>
<td>Enable File Store and test impact</td>
</tr>
<tr>
<td>Rolling PCAP</td>
<td>Enable Packet Capture and test impact</td>
</tr>
<tr>
<td>Statistics</td>
<td>Enable Statistics and test impact</td>
</tr>
<tr>
<td>Profiling</td>
<td>Enable Rule/Packet/Engine profiling and test impact</td>
</tr>
<tr>
<td>Alert Logging</td>
<td>Enable Alert Logging with extended fields for DNS/HTTP/SSL/SSH/SMTP/</td>
</tr>
<tr>
<td></td>
<td>Packet Logging</td>
</tr>
<tr>
<td>Network Profile Logging</td>
<td>Enable DNS/HTTP/SSL logging and test performance impact</td>
</tr>
</tbody>
</table>

Note that aside from Suricata version performance test, all other tests are on 4.0.1
### Test Matrix continued 3

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lua</td>
<td>Enable Lua with ET Lua Rules / Scripts and test impact</td>
</tr>
<tr>
<td>LuaJIT</td>
<td>Enable LuaJIT with ET Lua Rules/Scripts and test impact</td>
</tr>
<tr>
<td>PCRE-JIT</td>
<td>Enable PCRE-JIT and test performance</td>
</tr>
<tr>
<td>Rust</td>
<td>Enable rust and separately enable rust experimental parses and test performance</td>
</tr>
<tr>
<td>HomeNet Any</td>
<td>Set HomeNet to Any and test impact</td>
</tr>
<tr>
<td>Enable IP Reputation</td>
<td>Enable IP Reputation w/ET Intel replist and test performance</td>
</tr>
<tr>
<td>Bypass Rule Impact</td>
<td>Configure a bypass rule to bypass majority of sessions and test impact</td>
</tr>
<tr>
<td>Pass Rule Impact</td>
<td>Configure a pass rule to bypass majority of sessions and test impact</td>
</tr>
<tr>
<td>Rule Thresholding</td>
<td>Enable Rule Threshold and test impact</td>
</tr>
</tbody>
</table>

Note that aside from Suricata version performance test, all other tests are on 4.0.1
Results!
Test Methodology Overview: HW

- Traffic Generation Equipment: Ixia PerfectStorm1 Fusion
- Dell PowerEdge R710
  - 2x 8-Core Intel(R) Xeon(R) CPU L5520 @ 2.27GHz
  - 64GB RAM DDR3 1600Mhz
  - 4 port Broadcom NetExtreme II Gbit Interface Card
Test Methodology Overview: SW

- Ubuntu 15.1
- Suricata 4.0.1 (various versions/configs)
  - AF_Packet Mode
- ETPro Signature Pack 11/8/2017 (final tests)
- Ixia 7.9 / Breakingpoint 3.5.0

*Note that we do test different versions of Suricata, but this is the base version.*
Test Topology

2x direct connect 1Gbps Interfaces

Out of Band Management

Laptop for Executing Tests
Test Methodology

• Controls:
  - Same traffic profile
  - Same HW/OS
  - Same method to identify breakingpoint
  - Canary Traffic
  - Each test we run up to 1Gbps in each direction (max 2Gbps) plus Canary Traffic
  - Suricata Version, Base Configuration, Signature Set
    • *Except in specific tests which measure these configurations.

• Steps:
  - Compile and/or Configure Suricata based on given test.
  - Run Ixia Test
  - Collect Results
  - Restart Suricata for next test (fresh process each round.)
Test Traffic Description

- Ixia features over 3k Applications/Protocols, including real world apps. Traffic is generated at test setup, and is rich in content, and also varied.

- Ensures that you are not just replaying the same traffic over and over, while giving tester complete control of crafting the test and measuring the results.

- Protocols / Distribution (in BW)
  - SSL: 32%
  - Skype: 3%
  - HTTP Text: 7%
  - Pandora 4%
  - NTP: .5%
  - DNS 2%
  - HTTP Video: 11%
  - SMTP: 11%
  - NetFlix: 11%
  - SSH: 2%
  - Video Call/Conference: 10%
  - HTTP Audio: 4%
  - FTP: 2.5%

- Canary Test Traffic
  - Continuously trigger 2018885 (Windows XP Command.exe Shell Connection) throughout tests (Suricata set to drop) to ensure active detection.
Baseline Suricata Configuration

• Suricata 4.0.1, default compilation
• AF_Packet, 16 traffic threads (8 send / 8 receive)
• Only fast logging, no pcap, filestore, or debug
• No profiling
• AC pattern matching, detection profile medium
• All stock flow settings
Suricata ETPro Policy

- All ETPro Signatures (11/8/2017) enabled in alert mode except categories:
  - Policy
  - Decoder Events
- Roughly 37,000 Signatures
- Canary Signature 2018885 set to Drop to ensure that detection is active.
Suricata Version Performance Comparison

Suricata 2.0.9
Suricata 3.0.2
Suricata 3.2.4
Suricata 4.0.1
Suricata 4.0.1 --disable-gccmarch-native

Suricata 4.0.1 Breaking Point
Pattern Matching Algorithm Selection

![Bar Chart](chart.png)

- **AC**
- **AC-BS**
- **AC-KS**
- **HS**
- **PCRE-JIT**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>1070</td>
</tr>
<tr>
<td>AC-BS</td>
<td>725</td>
</tr>
<tr>
<td>AC-KS</td>
<td>1200</td>
</tr>
<tr>
<td>HS</td>
<td>1050</td>
</tr>
<tr>
<td>PCRE-JIT</td>
<td>1150</td>
</tr>
</tbody>
</table>
Suricata Thread Count Performance Impact

The chart illustrates the performance impact of Suricata with different thread counts. The x-axis represents the thread count (1, 2, 4, 8, 16, 32 Send/Receive), and the y-axis represents the MBPS (500, 770, 813, 945, 1070, 850). The chart shows an increase in MBPS as the thread count increases, indicating improved performance.
Run Mode AutoFP vs. Workers

<table>
<thead>
<tr>
<th>MBPS</th>
<th>AutoFP 16 Threads</th>
<th>Workers 16 Threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1200</td>
<td>1070</td>
<td>575</td>
</tr>
</tbody>
</table>
ETPro RuleSet Size Perf Impact

- 1 Rule
- 12k Rules
- 37k Rules
- HomeNet ANY
- Thresholding Enabled
Lua, LuaJIT, IPRep

Baseline: 1070 Mbps
Lua: 970 Mbps
LuaJIT: 1005 Mbps
Suricata Performance w/Logging/FileExtract/PCAP

- Standard: 1070 Mbps
- File Logging: 980 Mbps
- File Store (HTTP Only): 700 Mbps
- PCAP-AutoFP: 550 Mbps

Proofpoint
Stats, Alert Logging, Network Profiling

- Baseline: 1070 MBPS
- Network Profiling: 800 MBPS
- Alert Logging: 980 MBPS
- Alert Logging with Packet Data: 980 MBPS
Rust!

![Graph showing Mbps for Baseline, Rust, and Rust with Experimental Parsers]