Stepping out of the IDS Stereotype:
Applying Suricata's Full Potential

With Support from:

Introduction

Lukáš Šišmiš

Roles:

- Core Suricata team member
- Researcher @ CESNET and DynaNIC
- Ph.D. student @ Brno University of Technology

linkedin.com/in/sismis
lukashino

© OISF | All rights reserved. | www.suricata.io

Agenda

- Suricata introduction
- Showcase of Suricata uses:
  - IDS/IPS
  - Flow Probe
  - Network Security Monitor
  - Misconfiguration detection
  - Firewall
  - Library

© OISF | All rights reserved. | www.suricata.io

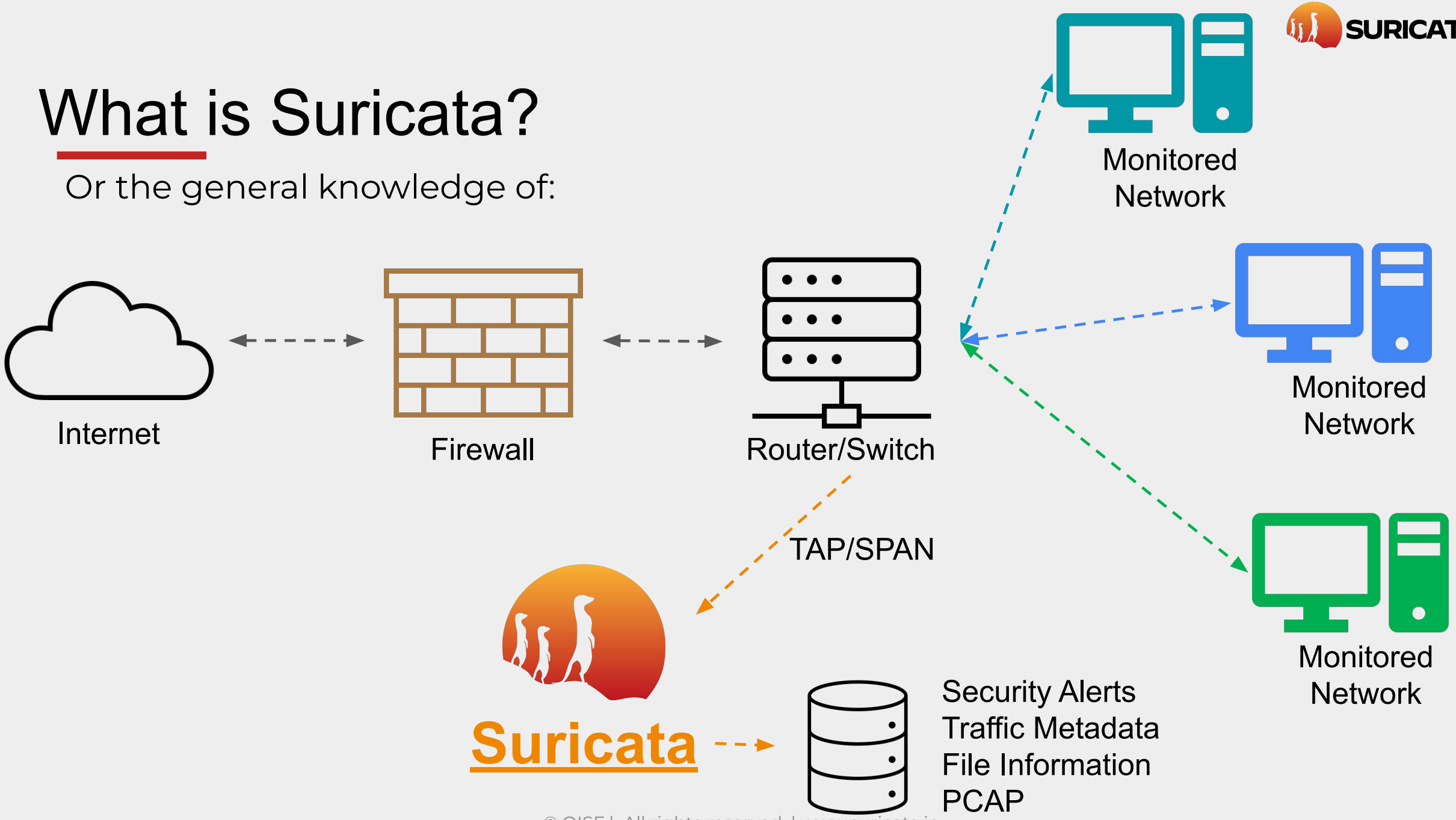
Suricata

An open-source high-performance network monitoring and security engine with active/passive monitoring, metadata logging and real-time file identification and extraction

Source: Stamus Networks

What is Suricata?

Or the general knowledge of:



© OISF | All rights reserved. | www.suricata.io

OISF - Open Information Security Foundation

- US 501(c)3 non-profit organization that ensures Suricata remains world-class.

- Dedicated to preserving the integrity of open source security technologies and the communities that keep them thriving. Our team and our community includes world-class security and non-profit experts, programmers, and industry leaders dedicated to open source security technologies.

- Funding for Suricata comes from donations from world-class security organizations committed to our mission. A list of these organizations is available on our Consortium Members page.

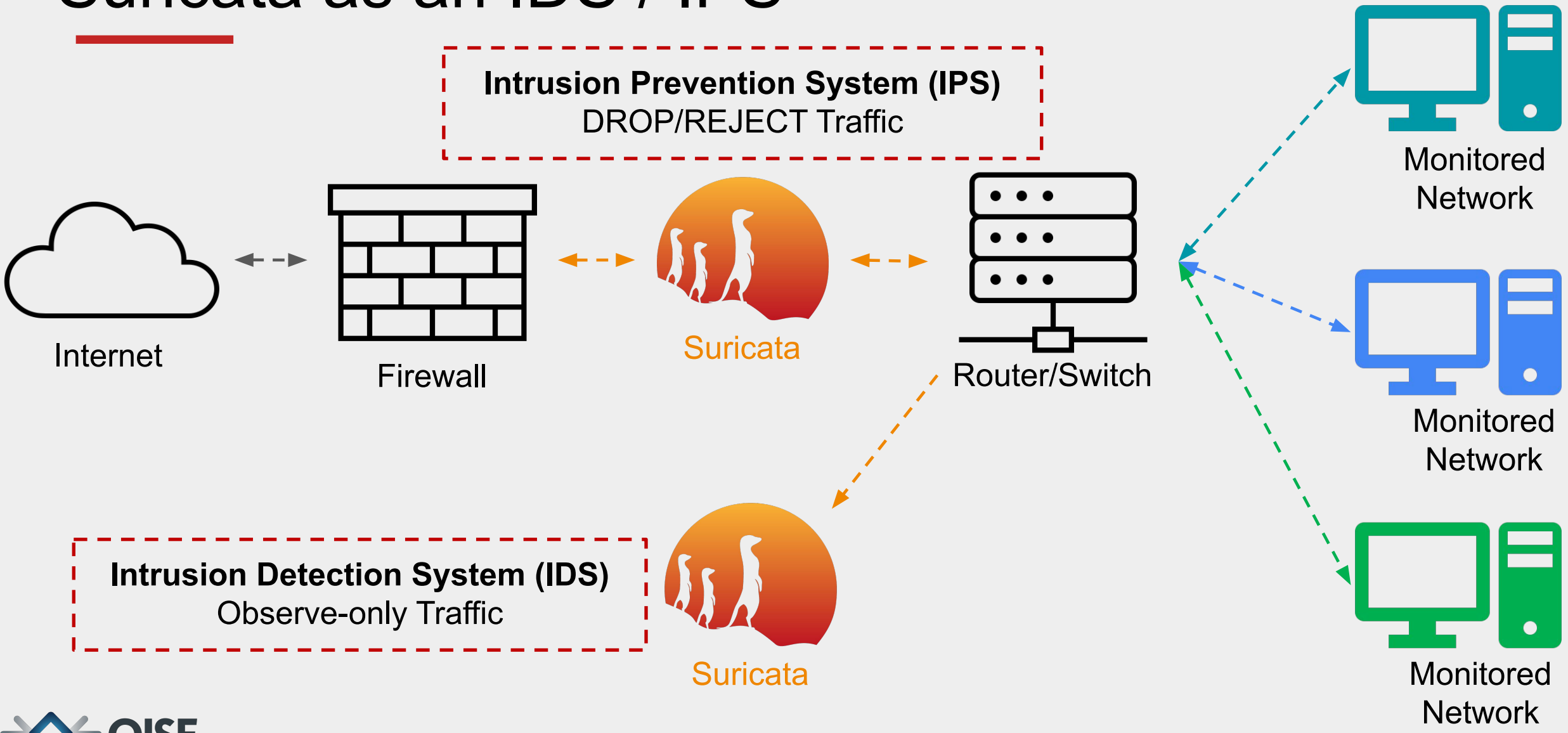
© OISF | All rights reserved. | www.suricata.io

Suricata running as:

- IDS/IPS
- Flow probe
- Network Security Monitor
- Misconfiguration detection
- Firewall
- Library

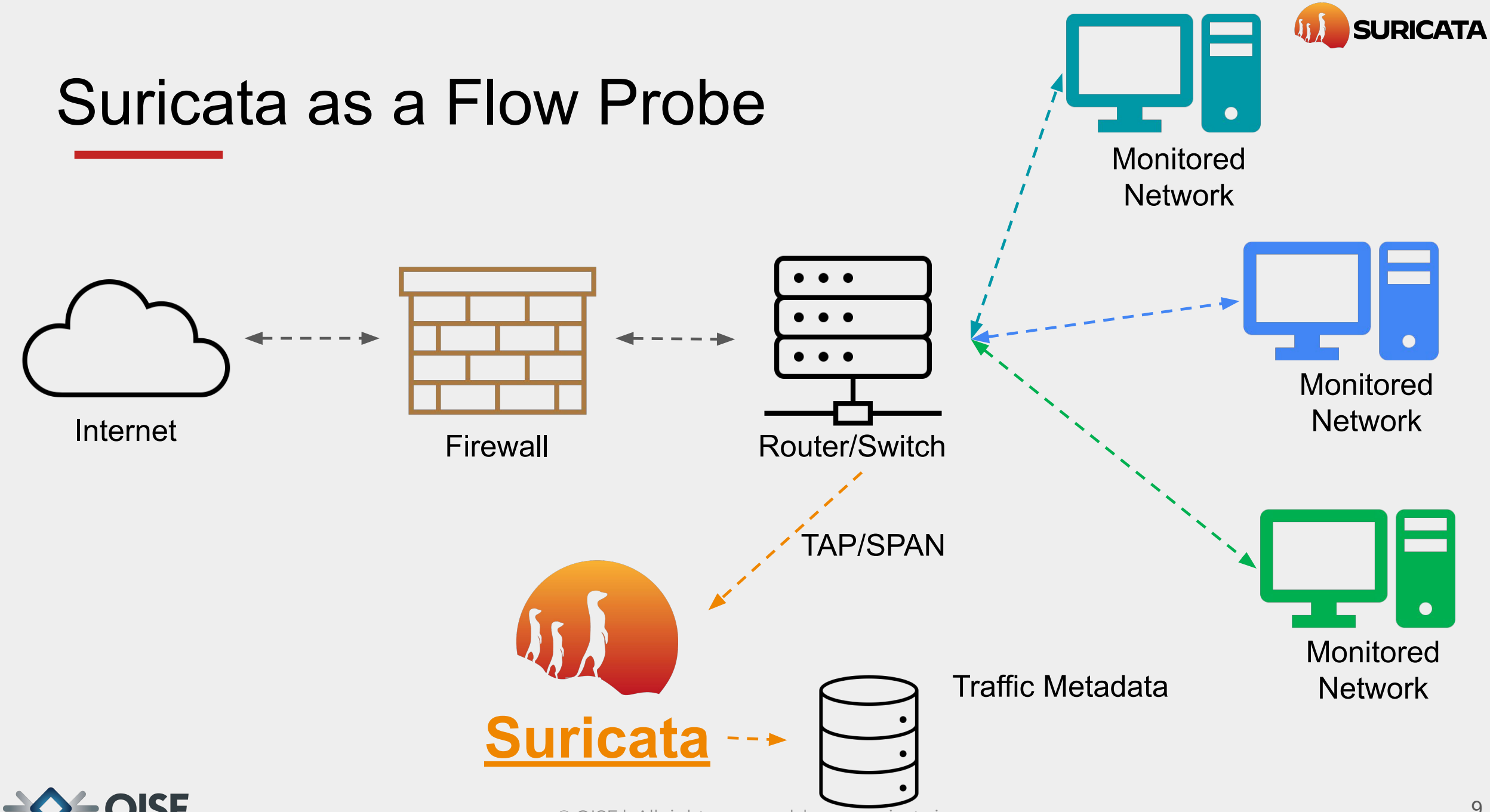
© OISF | All rights reserved. | www.suricata.io

Suricata as an IDS / IPS



© OISF | All rights reserved. | www.suricata.io

Suricata as a Flow Probe

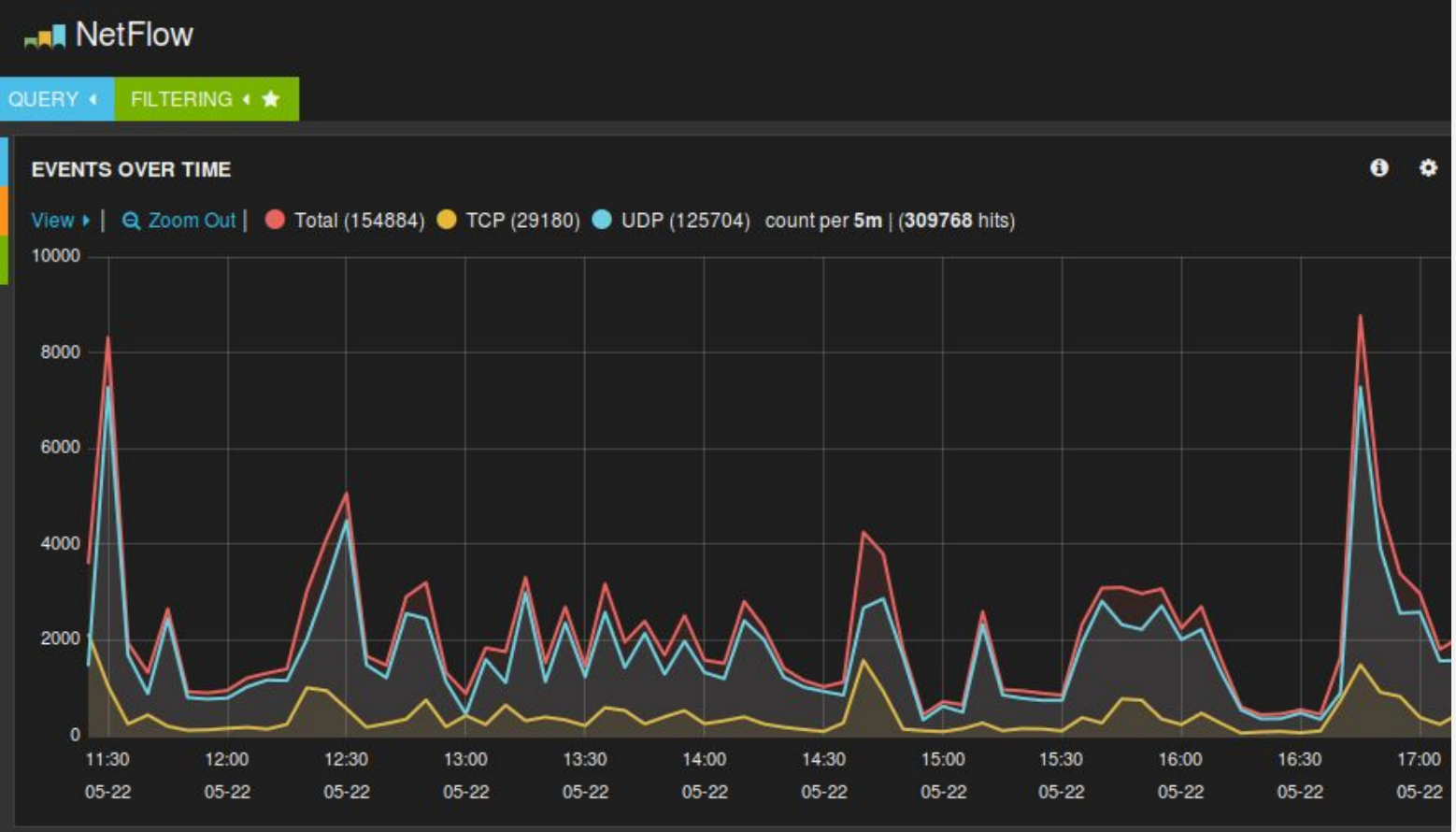


© OISF | All rights reserved. | www.suricata.io

Suricata as a Flow Probe

- Main use-case - export the flow information:
  - Where the traffic flows (who communicates with whom),
  - How much,
  - What protocols are prevalent,
- Export options:
  - Bidirectional flow - **flow record** by default
  - Unidirectional flow - netflow-like record
- Collect the data to the central logging platform/SIEM (e.g. ELK)

© OISF | All rights reserved. | www.suricata.io




```
{
  "timestamp": "2004-05-13T12:17:07+0200",
  "event_type": "netflow",
  "src_ip": "145.254.160.237",
  "src_port": 3372,
  "dest_ip": "65.208.228.223",
  "dest_port": 80,
  "proto": "TCP",
  "app_proto": "http",
  "netflow": {
    "pkts": 16,
    "bytes": 1351,
    "start":
"2004-05-13T12:17:07.311224+0200",
    "end": "2004-05-13T12:17:37.704928+0200",
    "age": 30,
    "min_ttl": 128,
    "max_ttl": 128,
  },...
}
```


STATS

2.00GB (total)

Query	count	min	max	mean	total	std_deviation
Total	151.25KB	0.00	136.58MB	13.57KB	2.00GB	712.65KB
TCP	28.50KB	0.00	136.58MB	71.47KB	1.99GB	1.60MB
UDP	122.76KB	0.00	4.03KB	137.14B	16.44MB	125.93B

STATISTICS FOR NETFLOW.AGE

16 s (mean)

Query	min	max	mean	std_deviation
Total	0 s	12,676 s	16 s	189 s
TCP	0 s	12,676 s	76 s	390 s
UDP	0 s	6,335 s	2 s	86 s

Suricata as a Flow Probe

Looks nice but...

- Suricata is slow and I'll never deploy it
  - Septun III shows 400 Gbps throughput https://www.youtube.com/watch?v=132mNItgiH0
- Suricata exports data only when the flow ends
  - It was discussed on Suricon 2024 and is planned to be added to Suricata 8.0 (no major interest for this feature before?)
- Existing work on top of this presented already in 2014 https://blog.inliniac.net/2014/07/28/suricata-flow-logging/

  https://suricon.net/wp-content/uploads/2019/11/SURICON2019-ntopng-and-Suricata_Merging-Network-Visibility-and-Security.pdf

© OISF | All rights reserved. | www.suricata.io

Suricata as a Network Security Monitor

- Main use-case - export the traffic metadata from all net layers:
  - Export flow records,
  - Protocol transactions such as:
    - DNS queries,
    - HTTP logs, TLS fingerprinting,
    - SMB/KRB5
    - SMTP/IMAP
  - Export deduplicated files / file information - filestore
  - Record deduplicated packet captures

Supported application-layer protocols:

http (either HTTP1 or HTTP2), http1, http2, ftp, tls (this includes ssl), smb, dns, dcerpc, dhcp, ssh, smtp, imap, pop3, modbus (disabled by default), dnp3 (disabled by default), enip (disabled by default), nfs, ike, krb5, bittorrent-dht, ntp, dhcp, rfb, rdp, snmp, tftp, sip, websocket

© OISF | All rights reserved. | www.suricata.io

Suricata as a Network Security Monitor

- TLS fingerprinting - JA3 is obsolete - use JA4 + JA3s

```
...
"event_type": "tls",
...
"tls": {
  "sni": "cloudflare-quic.com",
  "version": "TLS 1.3",
  "ja3": {
    "hash": "cd08e31494f9531f560d64c695473da9",
    "string": "771,4865-4866-4867-49195-49199-49196-49200-52393..."
  },
  "ja3s": {
    "hash": "eb1d94daa7e0344597e756a1fb6e7054",
    "string": "771,4865,51-43"
  },
  "ja4": "t13d1516h2_8daaf6152771_e5627efa2ab1"
}
...
```

© OISF | All rights reserved. | www.suricata.io

Suricata as an anomaly / misconfig monitor

- Suricata-included rules are focused on detection engine events
- The engine "complains" about the traffic, the traffic is never ideal

- Engine (app-layer-event) events:
  - dns.name_too_long
  - dns.infinite_loop
  - http.host_header_ambiguous
  - http.request_header_invalid
  - tls.invalid_certificate

- Not recommended to always have them enabled -> alert fatigue
  - Instead, enable them when deploying Suricata

© OISF | All rights reserved. | www.suricata.io

Suricata as an anomaly / misconfig monitor

- It can detect:
  - Misconfigured network:
    - Asymmetric routing
    - Running out of TTL hops
  - Misconfigured devices:
    - Verify behavior of unmanaged endpoints - IoT devices, printers, switches, industrial devices, etc.
    - Devices "calling home"
    - Unusual protocols or ports in use
    - Identify abnormal traffic patterns (excessive requests, repeated resets) caused by faulty software or routing loops.

© OISF | All rights reserved. | www.suricata.io

Suricata as an anomaly / misconfig monitor

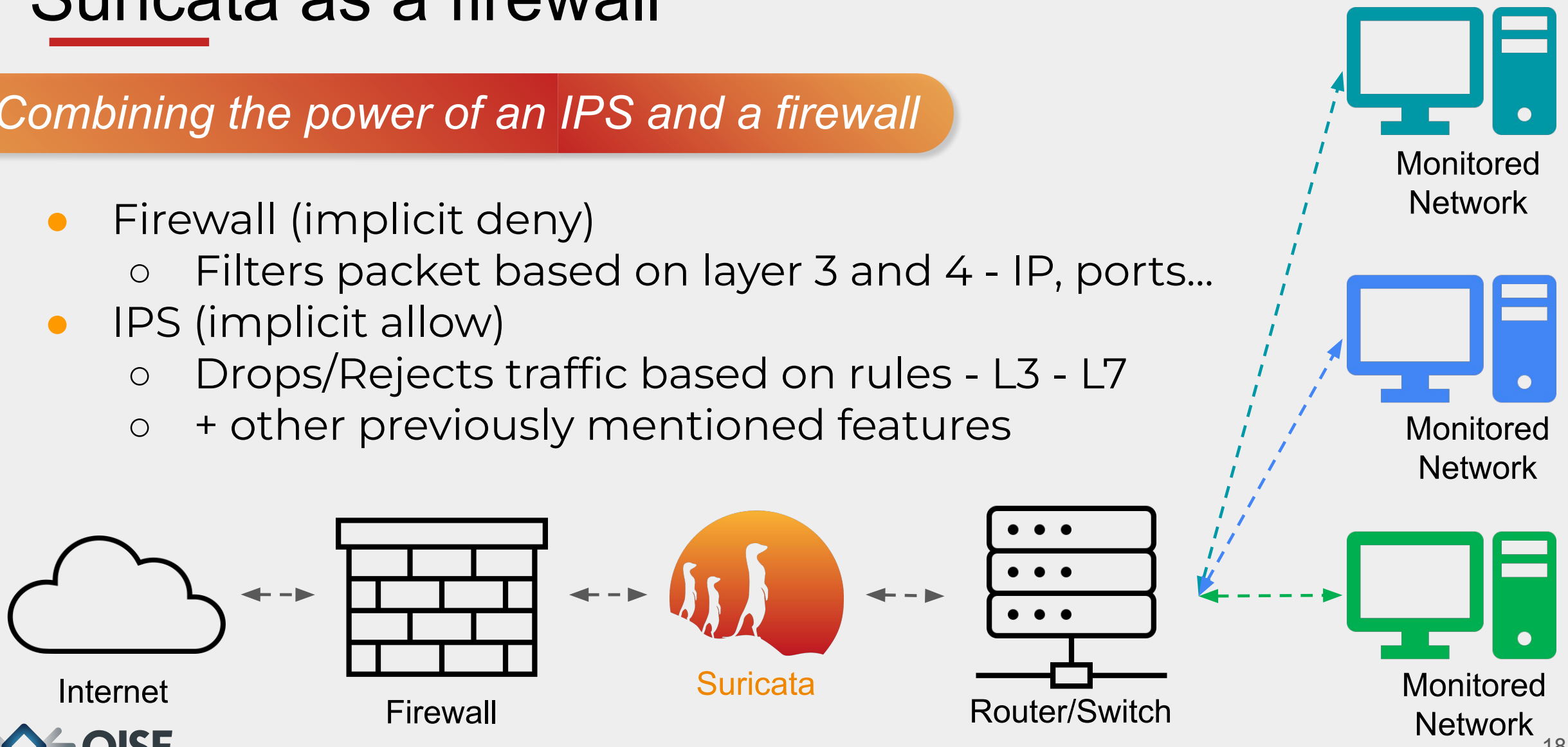
- Detecting asymmetric routing
  - seeing a lot more SYN than SYNACKs or vice versa
  - remedy:
    - fix the routing or
    - enable stream.async-oneside
- Detecting expired/invalid TLS certificates
  - it is highlighted with a rule with tls.invalid_certificate event
  - remedy:
    - fix your TLS certs!
      - alert tls any any -> any any (msg:"SURICATA TLS invalid certificate"; flow:established; app-layer-event:tls.invalid_certificate; flowint:tls.anomaly.count,+,1; classtype:protocol-command-decode; sid:2230004; rev:1;)

© OISF | All rights reserved. | www.suricata.io

Suricata as a firewall

Combining the power of an IPS and a firewall

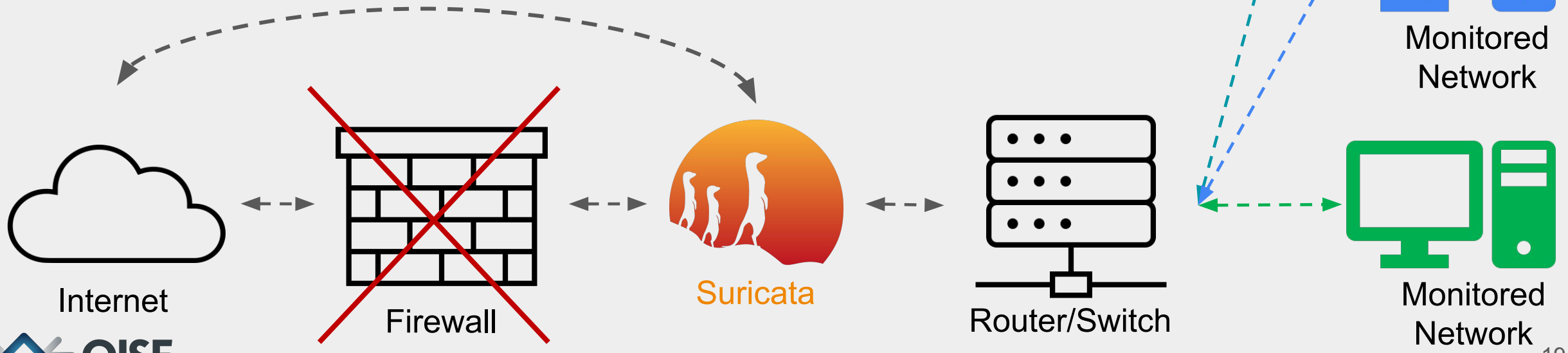
- Firewall (implicit deny)
  - Filters packet based on layer 3 and 4 - IP, ports...
- IPS (implicit allow)
  - Drops/Rejects traffic based on rules - L3 - L7
  - + other previously mentioned features



© OISF | All rights reserved. | www.suricata.io

Suricata as a (next generation) firewall

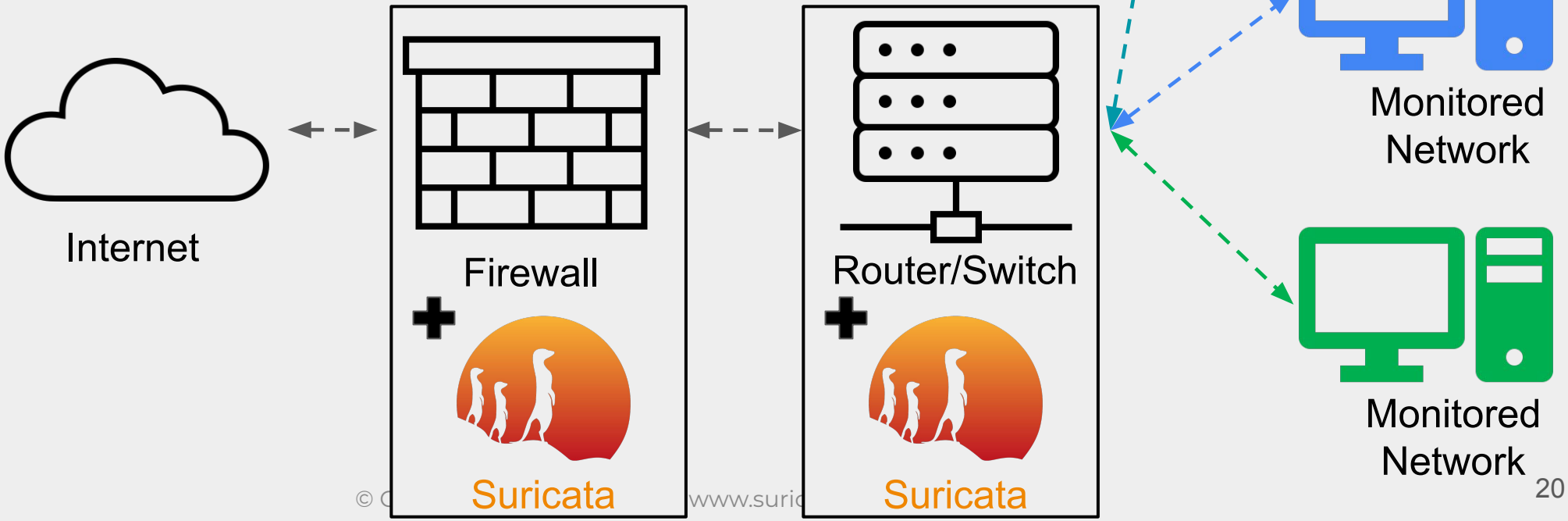
- NGFW == Firewall + IPS
  - IP-only rules substitute firewall rules
  - IPS rules provide application-layer blocking
  - Suricata Exception policies provide failover policy
  - AWS Network Firewall



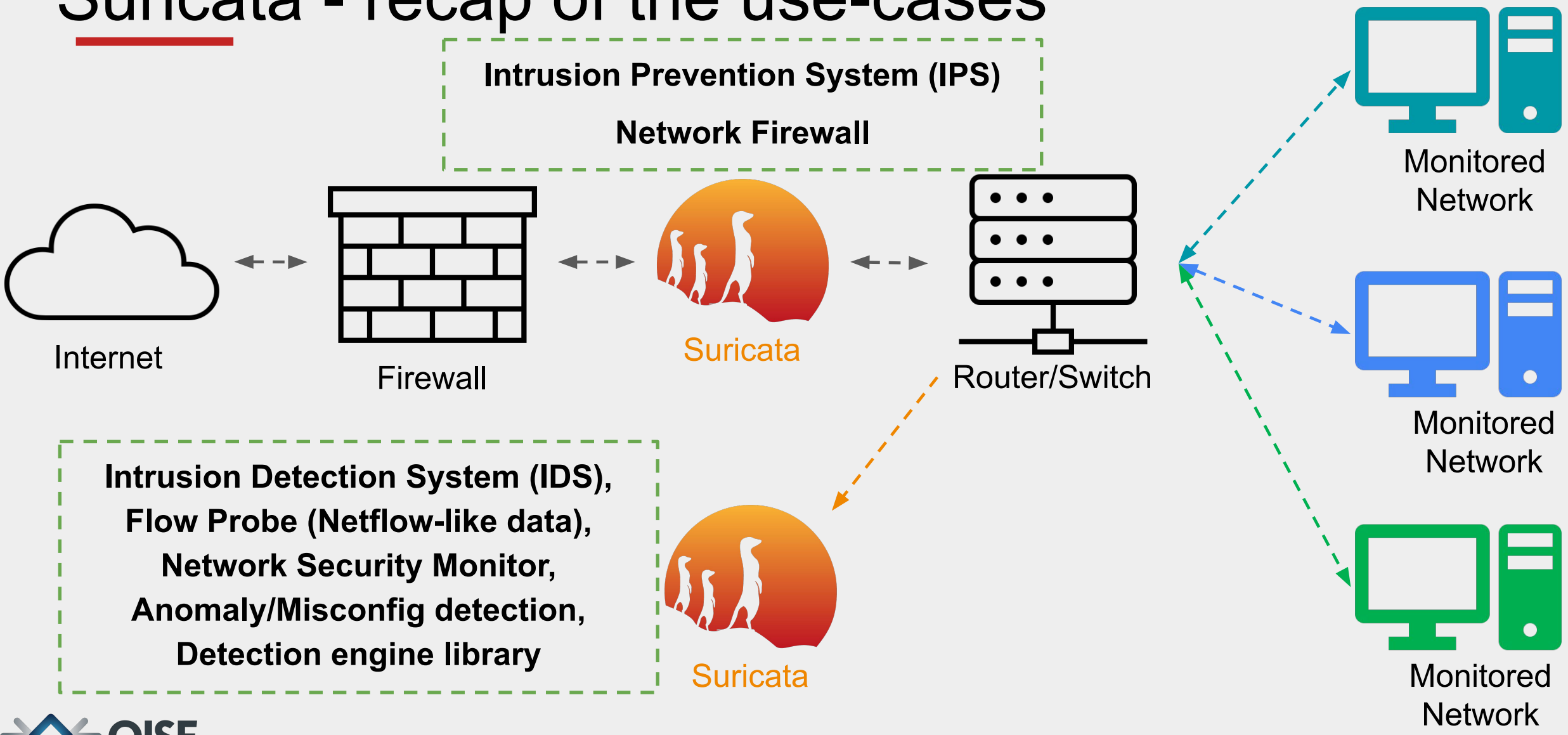
© OISF | All rights reserved. | www.suricata.io

Suricata as a library

- Embed detection on the traffic directly in the custom application/solution
- Direct API of the Suricata detection engine
- Prevents redundant packet processing
- Part of Suricata 8.0 release



Suricata - recap of the use-cases



© OISF | All rights reserved. | www.suricata.io

Major Updates

- **Suricata 8.0** is soon getting into feature-steady phase
  - All last-minute contributions are welcome
  - Please help test Suricata 8.0-beta when it is out
  - Full 8.0 release will happen this year, likely in fall.
- CVE issuing - Suricata contains bugs too that need to be fixed - it helps to publicly motivate for upgrades
- Suricata 8.0 interesting features:
  - New protocols: ARP, LDAP, MySQL, frame support in many
  - Rules using Lua scripts
  - Granular NUMA affinity settings

© OISF | All rights reserved. | www.suricata.io

Suricon

- Community conference to network, share ideas, exchange the news, form the new Suricata features
- Suricon 2024 materials published https://suricon.net/suricon-2024-madrid/

- Suricon 2025 is in Montreal, Canada
- Trainings are available
- The exact dates will be set soon

© OISF | All rights reserved. | www.suricata.io

Thank you!

Website
suricata.io

Forum
forum.suricata.io

E-mail
info@oisf.net

Discord
discord.gg/t3rV2x7MrG