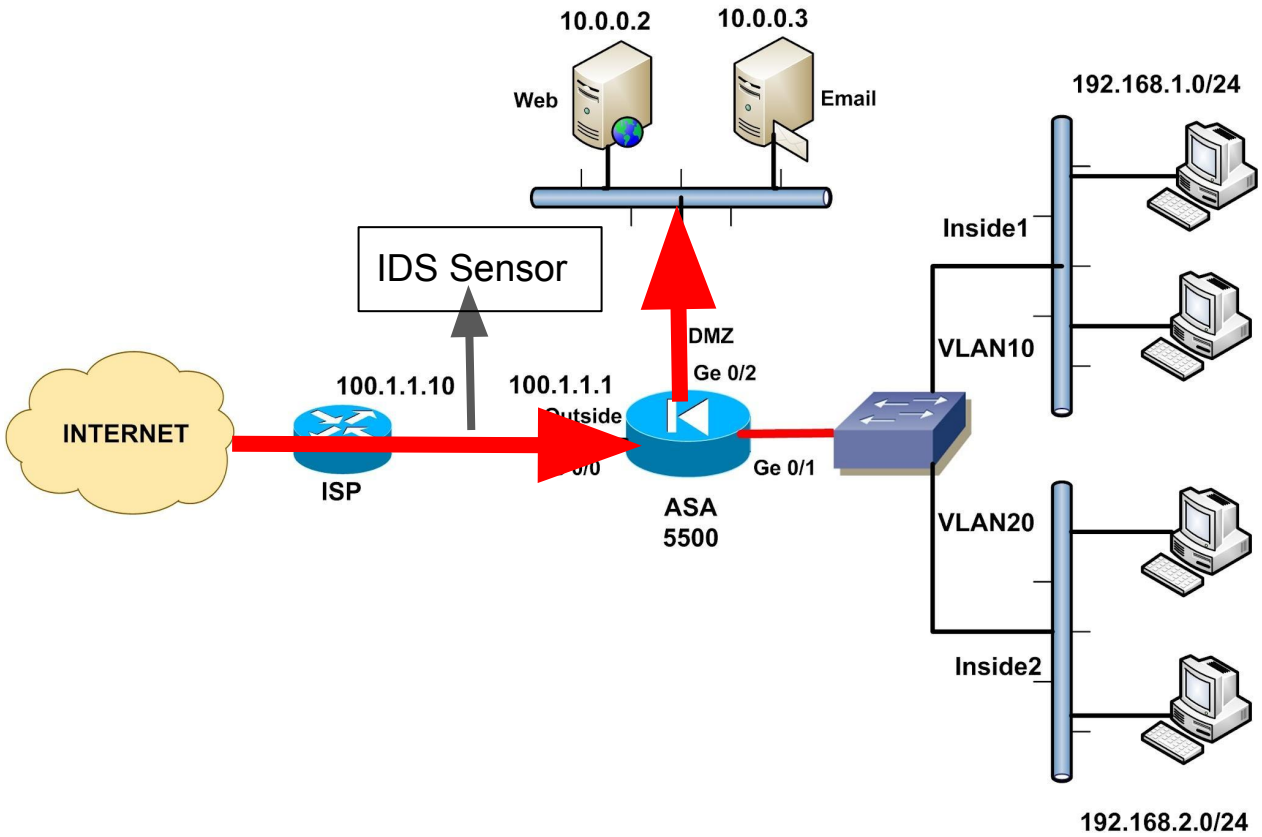
metadata: tags useful;

metadata: previous_works BETTER, previous_works Aristotle;

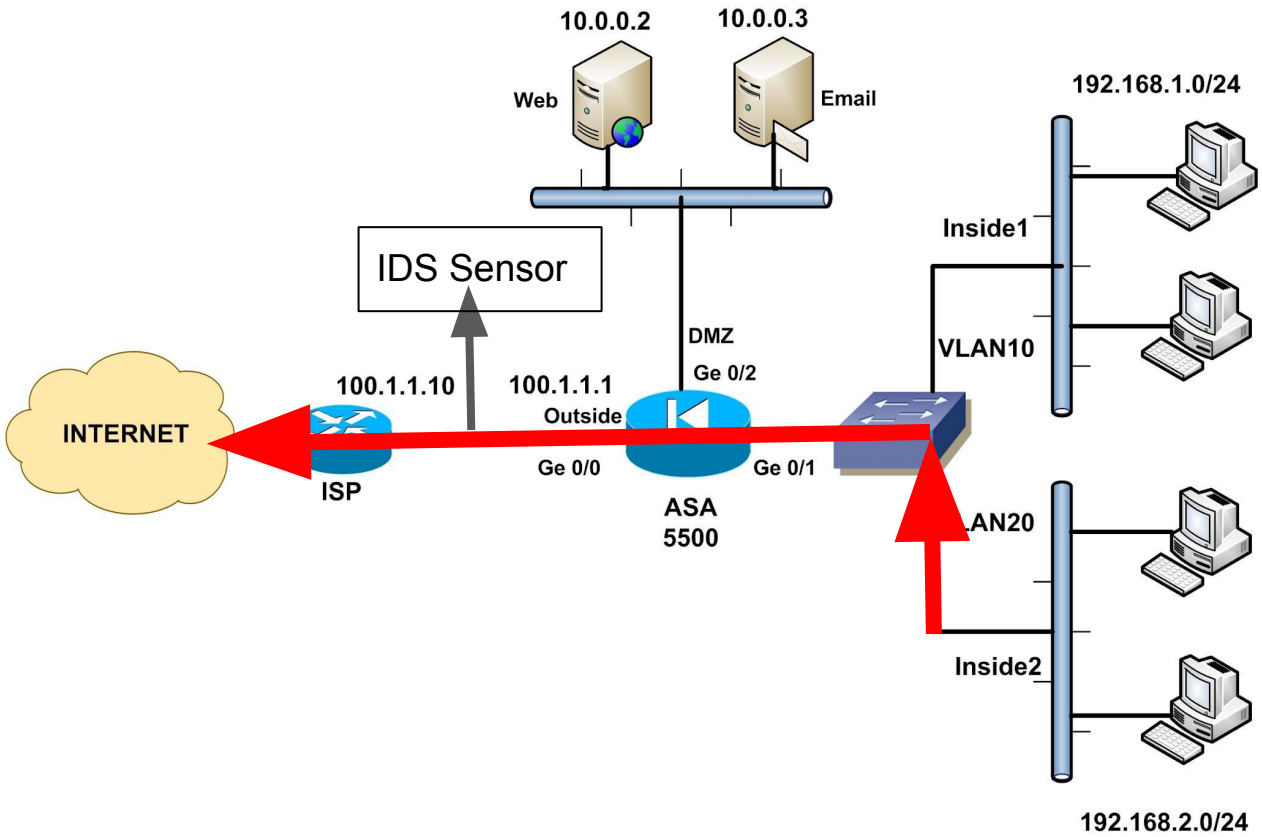
Presented by David Wharton in 2019 Suricon

```
python aristotle.py -r examples/example.rules
    -f examples/example1.filter
    -o newrules.rules
```

metadata: tuning_ruleset high-level;



metadata: tuning_ruleset high-level;



metadata: usage how-to;

6.2.8. metadata

The metadata keyword allows additional, non-functional information to be added to the signature. While the format is free-form, it is recommended to stick to key, value pairs as Suricata can include these in eve alerts. The format is:

```
metadata: key value;
metadata: key value, key value;
```

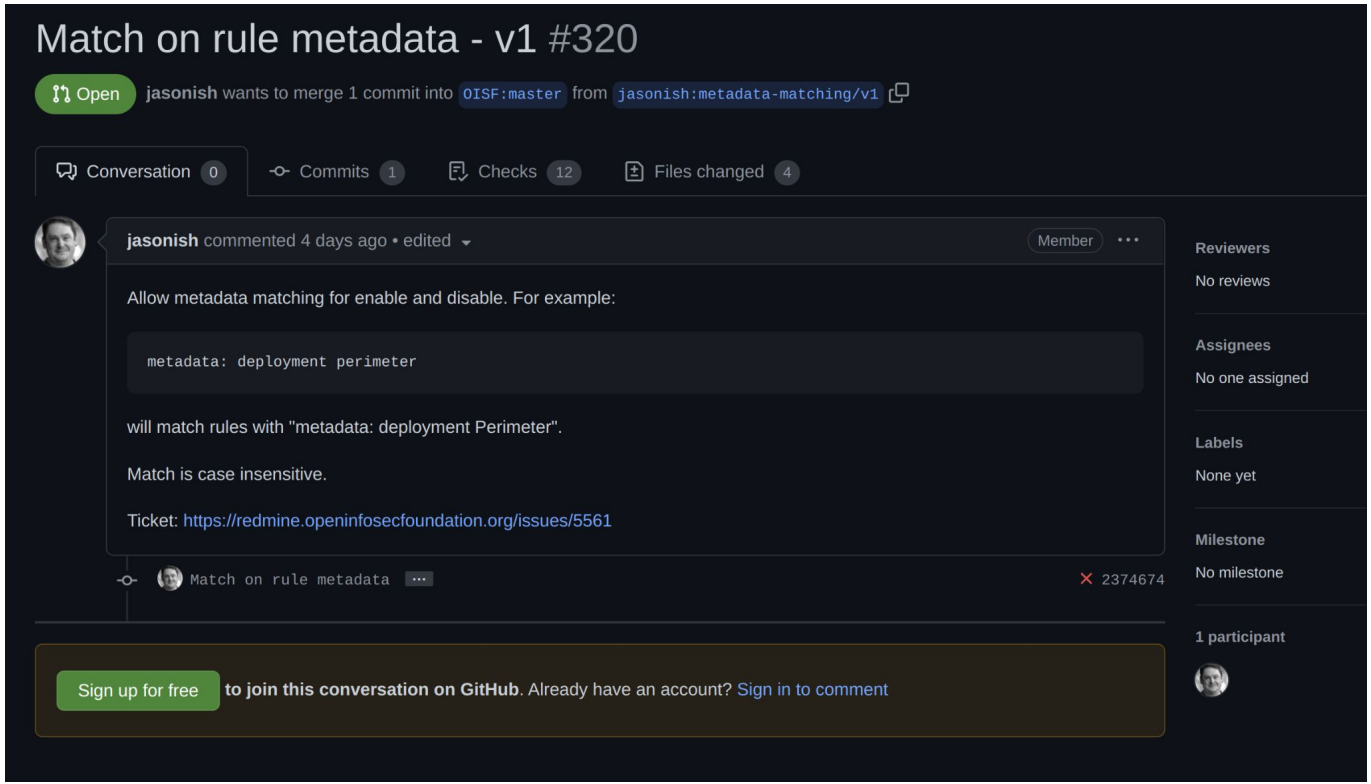
metadata: useful in-logs;


```
  "signature": "ETPRO MALWARE RedLine Stealer TCP CnC net.tcp Init",
  "category": "A Network Trojan was detected",
  "severity": 1,
  "metadata": {
    "affected_product": [
      "Windows_XP_Vista_7_8_10_Server_32_64_Bit"
    ],
    "attack_target": [
      "Client_Endpoint"
    ],
    "created_at": [
      "2021_09_22"
    ],
    "deployment": [
      "Perimeter"
    ],
    "former_category": [
      "MALWARE"
    ],
    "malware_family": [
      "Redline"
    ],
    "signature_severity": [
      "Major"
    ],
    "updated_at": [
      "2022_03_24"
    ]
  }
```

metadata: useful in-rulesets;

attack_target	signature_severity	deployment	performance_impact	confidence
Client_and_Server Client_Endpoint DNS_Server FTP_Server IoT Linux/Unix Mobile_Client Networking_Equipment Server SMB_Client SMB_Server SMTP_Server SQL_Server Web_Server	Critical Informational Major Minor	alert_only Datacenter Internal Internet Perimeter SSLDecrypt	Low Moderate Significant	Low Medium High

metadata: usable in-suricata-update;



metadata: usable in-suricata-update;

```
> cat disable.conf
metadata: deployment sssldecrypt
  /tmp
```

metadata: usable in-suricata-update;

```
horization-bypass7; reference:cve,2022-25237; classtype:attempted-a
data:attack_target Server, created_at 2022_06_03, cve CVE_2022_2523
yment SSLDecrypt, former_category WEB_SPECIFIC_APPS, performance_im
inor, updated_at 2022_06_03;)
10/11/2022 -- 03:38:19 - <Info> -- Disabled 663 rules.
10/11/2022 -- 03:38:19 - <Info> -- Enabled 0 rules.
10/11/2022 -- 03:38:19 - <Info> -- Modified 0 rules.
10/11/2022 -- 03:38:19 - <Info> -- Dropped 0 rules.
10/11/2022 -- 03:38:19 - <Info> -- Enabled 134 rules for flowbit de
10/11/2022 -- 03:38:19 - <Info> -- Backing up current rules.
10/11/2022 -- 03:38:22 - <Info> -- Writing rule files to directory
total: 36109; enabled: 27929; added: 0; removed 3324; modified: 0
10/11/2022 -- 03:38:23 - <Info> -- No changes detected, exiting.
```

metadata: presentation complete;

Please submit rule feedback at

https://feedback.emergingthreats.net