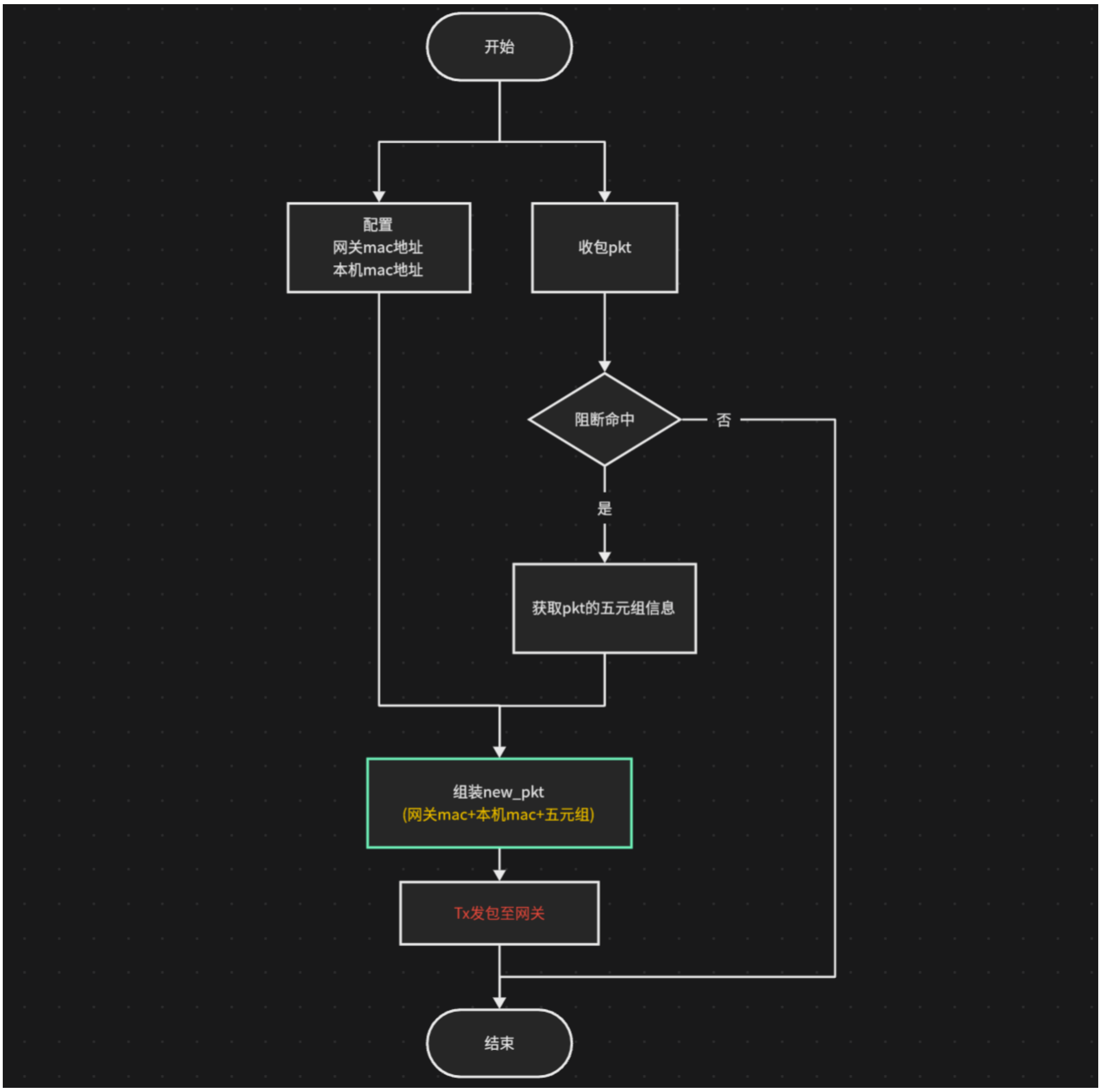
suricata阻断项目手札

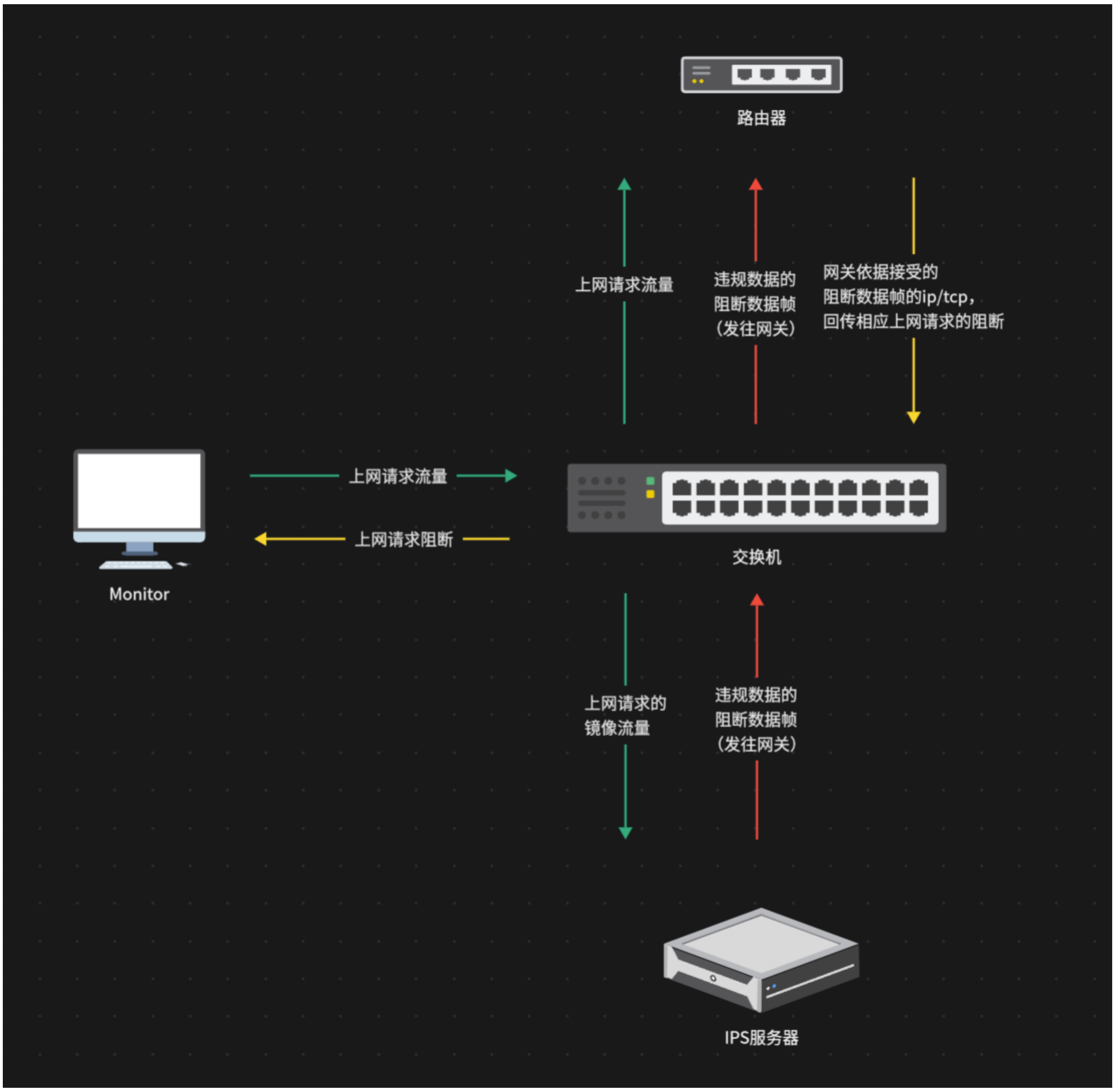
一、阻断逻辑流程



注意：

- 所使用的阻断数据包，需要依据所阻断的pkt数据帧，进行相应的Tcp层seq/ack值的计算；
- 阻断数据包的mac地址，不使用原数据中两端的mac地址；

二、架构网络拓扑图



三、suricata的阻断使用

再suricata的使用中，要实现阻断的及时相应，有以下两种实践方法：

1.使用单包的tcp阻断规则

```
reject tcp-pkt any any -> any any (msg: "ATTACK [PTsecurity] Spring Core RCE aka Spring4Shell Attempt"; content: "news.cn"; reference: url, github.com/ptresearch/AttackDetection; reference: url, www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html; classtype: attempted-admin; sid: 10007107; rev: 1;)
```

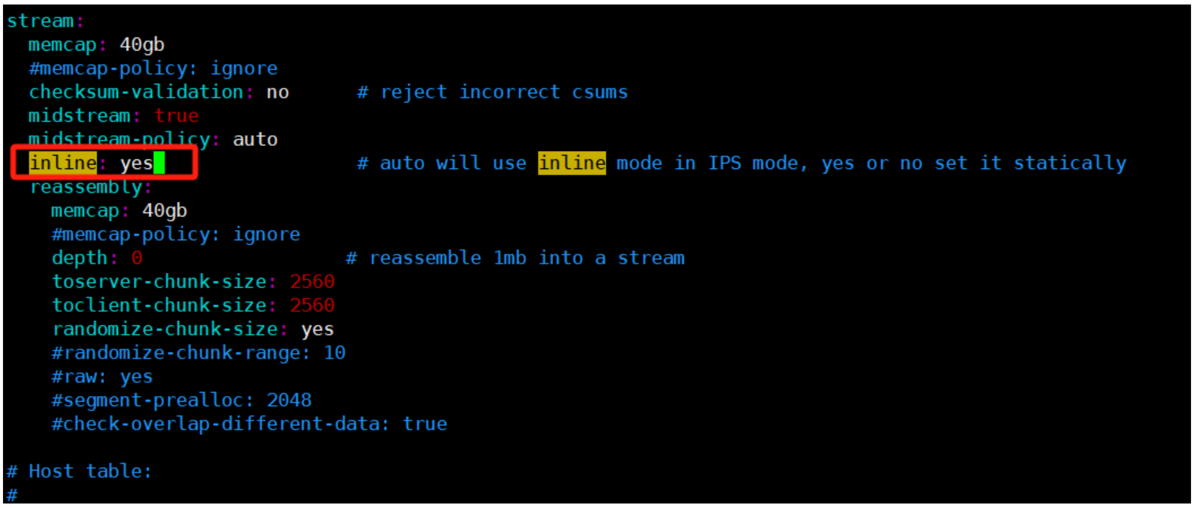
在suricata中，单包规则就会执行：来一个pkt，就对该包tcp的payload部分进行conten规则匹配，从而进行rst阻断可以更及时。

2.使用流stream的阻断规则

```
reject http any any -> any any (msg: "ATTACK [PTsecurity] Spring Core RCE aka Spring4Shell Attempt"; flow: established, to_server; http.host;content: "news.cn"; reference: url, github.com/ptresearch/AttackDetection; reference: url, www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html; classtype: attempted-admin; sid: 10007107; rev: 1;)
reject tcp any any -> any any (msg: "ATTACK [PTsecurity] Spring Core RCE aka Spring4Shell Attempt"; content: "news.cn"; reference: url, github.com/ptresearch/AttackDetection; reference: url, www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html; classtype: attempted-admin; sid: 10007107; rev: 1;)

```

第一步：开启stream处理inline模式：

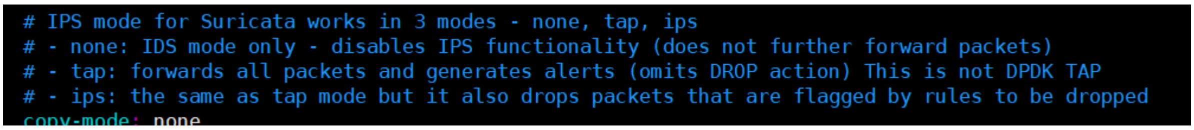


```
stream:
  memcap: 40gb
  #memcap-policy: ignore
  checksum-validation: no      # reject incorrect csums
  midstream: true
  midstream-policy: auto
  inline: yes                  # auto will use inline mode in IPS mode, yes or no set it statically
  reassembly:
    memcap: 40gb
    #memcap-policy: ignore
    depth: 0                  # reassemble 1mb into a stream
    toserver-chunk-size: 2560
    toclient-chunk-size: 2560
    randomize-chunk-size: yes
    #randomize-chunk-range: 10
    #raw: yes
    #segment-prealloc: 2048
    #check-overlap-different-data: true

# Host table:
#
```

第二步：开启IPS

1、对于程序支持IPS使用，则在相应的网卡配置中指定：ips模式



```
  # IPS mode for Suricata works in 3 modes - none, tap, ips
  # - none: IDS mode only - disables IPS functionality (does not further forward packets)
  # - tap: forwards all packets and generates alerts (omits DROP action) This is not DPDK TAP
  # - ips: the same as tap mode but it also drops packets that are flagged by rules to be dropped
  copy-mode: none
```

2、程序不方便开启IPS模式，可以使用的一种

```
1、命令行指定强行使用IPS(该模式下)
    --simulate-ips
```