**Suricata - Feature #2174**

Need a special keyword and functionality for ip address extraction from a content (html body for ex.) and comparing it to src,dst_ip/EXTERNAL,HOM_NET

07/07/2017 11:26 AM - ajaxtpm ajaxtpm

| Status: | New |
| Priority: | Normal |
| Assignee: | Community Ticket |
| Category: | |
| Target version: | TBD |

**Description**

Need a special keyword and functionality for ip address extraction from a content (html body for ex.) and comparing it to src,dst_ip/EXTERNAL,HOM_NET

For example:

```
ip_extract: <bytes to convert>, <offset>, relative, endian, string, comparator
```

Where:

- `<bytes_to_convert>`: Number of bytes to pick up from the packet. The allowed values are 7 to 15 when used against string. Should not be used if applied against binary data.
- `<offset>`: Number of bytes into the payload to start processing
- `<relative>`: Use an offset relative to last pattern match
- `<endian>`: Endian type of the ip address being represented by binary data:
  - big: Process data as big endian (default)
  - little: Process data as little endian
- `<string>`: IP address is stored in string format in packet
- `<comparator>`: One of 4 values specifying what the extracted ip address should be compared to:
  - is_srcip: extracted ip address is checked whether it is equal to the source address of ip packet
  - is_dstip: extracted ip address is checked whether it is equal to the destination address of ip packet
  - is_external: extracted ip address is checked whether it is in $EXTERNAL_NET ip address space
  - is_home: extracted ip address is checked whether it is in $HOME_NET ip address space

I attached a screenshot of an example http session where I'd like to extract ip address and compare whether it is from $EXTERNAL_NET

**History**

**#1 - 07/08/2017 04:55 PM - ajaxtpm ajaxtpm**

I'm sorry, of course there must not be any `<bytes_to_convert>` parameter because ip address takes 4 bytes in binary representation and from 7 to 15 bytes as a string and we do not know exact ip string size before extraction. So, no `<bytes_to_convert` there. Also it may be useful to skip trailing spaces after `<offset>` bytes in case of string ip representation. And of course all of this is about IPv4 and it may be better to name it "ipv4_extract".

**#2 - 07/18/2017 03:31 PM - Andreas Herz**

- Assignee set to Anonymous
- Target version set to TBD

**#3 - 02/23/2019 10:20 PM - Andreas Herz**

- Assignee set to Community Ticket

**Files**

| Cнимок.PNG | 21.5 KB | 07/07/2017 | ajaxtpm ajaxtpm |

07/15/2022