Suricata - Feature #3310

ease suricata configuration with xdp

11/03/2019 10:19 AM - Peter Manev

Status: Feedback
Priority: Normal
Assignee: Eric Leblond
Category: TBD
Effort:
Difficulty:

Description
In cases where XDP is used some configuration changes are made in ebpf/xdp_filter.c - for example flow4/flow6 tables, RSS/CPU queues/maps.
I wonder if this can be part or mapped from within the suricata.yaml config so there is only one place to edit.

/* Set BUILD_CPUMAP to 0 if you want to run XDP bypass on kernel *
 * older than 4.15 */
#define BUILD_CPUMAP 0

/* Increase CPUMAP_MAX_CPUS if ever you have more than 64 CPUs */
#define CPUMAP_MAX_CPUS 64

/* Set to 1 to bypass encrypted packets of TLS sessions. Suricata will *
 * be blind to these packets or forged packets looking alike. */
#define ENCRYPTED_TLS_BYPASS 0

/* Set it to 0 if for example you plan to use the XDP filter in a *
 * network card that don't support per CPU value (like netronome) */
#define USE_PERCPU_HASH 0

/* Set it to 0 if your XDP subsystem don't handle XDP_REDIRECT (like netronome) */
#define GOT_TX_PEER 0

/* set to non 0 to load balance in hardware mode on RSS_QUEUE_NUMBERS queues *
 * and unset BUILD_CPUMAP (number must be a power of 2 for netronome) */
#define RSS_QUEUE_NUMBERS 32

/* no vlan tracking: set it to 0 if you don't use VLAN for tracking. Can *
 * also be used as workaround of some hardware offload issue */
#define VLAN_TRACKING 0

...  

struct bpf_map_def SEC("maps") flow_table_v4 = {  
#if USE_PERCPU_HASH  
    .type = BPF_MAP_TYPE_PERCPU_HASH,
#else  
    .type = BPF_MAP_TYPE_HASH,
#endif  
    .key_size = sizeof(struct flowv4_keys),  
    .value_size = sizeof(struct pair),  
    .max_entries = 627680,
};

struct bpf_map_def SEC("maps") flow_table_v6 = {  
#if USE_PERCPU_HASH  
    .type = BPF_MAP_TYPE_PERCPU_HASH,
#else  
    .type = BPF_MAP_TYPE_HASH,
#endif  
    .key_size = sizeof(struct flowv6_keys),  
    .value_size = sizeof(struct pair),

09/05/2020
```cpp
max_entries = 632768;
```

**History**

**#1 - 11/04/2019 12:02 PM - Victor Julien**
- Status changed from New to Feedback
- Assignee set to Eric Leblond
- Target version set to TBD

I suppose some of the settings could be communicated to the bpf program using a config map. Others are compile time things.

Eric, any ideas on how to improve this?

**#2 - 11/04/2019 12:03 PM - Victor Julien**
- Description updated