Examples of state definitions

Table of Contents

Model, Data and Command

Model script
Example data

Command to run

```
./saf.py --db  data/db/dnsflows_100rec.sqlite --model tests/bscripts/example_states.b --pretty
```

Model script reproduced:

```
[header]
NAMESPACE = EXAMPLES
NAME = STATES
QUALIFIER = { }[_eventno=1:20]
IMPORT = NET.APP_PROTO.DNSREQRES

[states]
state_A  = {sipaddr = '10.1.11.2', dipaddr='10.1.4.2'}
state_B  = {sport > 53}
state_C  = {sipaddr=$state_A.dipaddr}
state_D  = {sport=$state_B.sport, dnsqrflag=1}
state_E = DNSREQRES.dns_req()
state_F = DNSREQRES.DNS_REQ_RES()
state_G = DNSREQRES.DNS_REQ_RES(sport > 30000)
state_H  = {sipaddr='10.1.*'}

[behavior]
# For now it is important to include the definition of the state on which the
# dependent state is dependent
b1 = (state_A  and state_C)
b2 = (state_B and  state_D)

[model]
CONSTANT_STATES_1(eventno, eventtype, sipaddr, dipaddr, sport, dport) = (state_A)
CONSTANT_STATES_2(eventno, eventtype, sipaddr, dipaddr, sport, dport) = (state_B)
DEPENDENT_STATES_1(eventno, eventtype, sipaddr, dipaddr, sport, dport) = b1
DEPENDENT_STATES_2(eventno, eventtype, sipaddr, dipaddr, sport, dport) = b2
IMPORTING_STATES(eventno, eventtype, sipaddr, dipaddr, sport, dport) = state_E
IMPORTING_BEHAVIORS_AS_STATE(eventno, eventtype, sipaddr, dipaddr, sport, dport) = state_F
IMPORTING_BEHAVIORS_AS_STATE_W_CUSTOMIZATION(eventno, eventtype, sipaddr, dipaddr, sport, dport) = sta
WILDCARDING(eventno, eventtype, sipaddr, dipaddr, sport, dport) = state_H
```

Output

Output for CONSTANT_STATES_1

```
====================================
Instances satisfying CONSTANT_STATES_1
====================================
```

```
Total Matching Instances: 9

-----------------------------------------------------------------------------------------------------
    eventno      |    eventtype     |     sipaddr      |     dipaddr      |      sport       |      dp
-----------------------------------------------------------------------------------------------------
       1         |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      10486       |
-----------------------------------------------------------------------------------------------------
       13        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      60435       |
-----------------------------------------------------------------------------------------------------
       25        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      20205       |
-----------------------------------------------------------------------------------------------------
       37        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      47955       |
-----------------------------------------------------------------------------------------------------
       49        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      34950       |
-----------------------------------------------------------------------------------------------------
       61        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      59662       |
-----------------------------------------------------------------------------------------------------
       73        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      62147       |
-----------------------------------------------------------------------------------------------------
       85        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      38762       |
-----------------------------------------------------------------------------------------------------
       97        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      25074       |
-----------------------------------------------------------------------------------------------------
```

Output for CONSTANT_STATES_2

```
====================================
Instances satisfying CONSTANT_STATES_2
====================================

Total Matching Instances: 9

-----------------------------------------------------------------------------------------------------
    eventno      |    eventtype     |     sipaddr      |     dipaddr      |      sport       |      dp
-----------------------------------------------------------------------------------------------------
       1         |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      10486       |
-----------------------------------------------------------------------------------------------------
       13        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      60435       |
-----------------------------------------------------------------------------------------------------
       25        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      20205       |
-----------------------------------------------------------------------------------------------------
       37        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      47955       |
-----------------------------------------------------------------------------------------------------
       49        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      34950       |
-----------------------------------------------------------------------------------------------------
       61        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      59662       |
-----------------------------------------------------------------------------------------------------
       73        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      62147       |
-----------------------------------------------------------------------------------------------------
```

```
       85        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      38762       |
-------------------------------------------------------------------------------------------------
       97        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      25074       |
-------------------------------------------------------------------------------------------------
```

Output for DEPENDENT_STATES_1

```
=====================================
Instances satisfying DEPENDENT_STATES_1
=====================================

Total Matching Instances: 4

-------------------------------------------------------------------------------------------------
    eventno      |    eventtype     |     sipaddr      |     dipaddr      |      sport       |      dp
-------------------------------------------------------------------------------------------------
       1         |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      10486       |
-------------------------------------------------------------------------------------------------
                                        Behavior: DEPENDENT_STATES_1.b1
       8         |    PACKET_DNS    |     10.1.4.2     |    10.1.11.2     |        53        |      10
-------------------------------------------------------------------------------------------------
       13        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      60435       |
-------------------------------------------------------------------------------------------------
                                        Behavior: DEPENDENT_STATES_1.b1
       20        |    PACKET_DNS    |     10.1.4.2     |    10.1.11.2     |        53        |      60
-------------------------------------------------------------------------------------------------
```

Output for DEPENDENT_STATES_2

```
=====================================
Instances satisfying DEPENDENT_STATES_2
=====================================

Total Matching Instances: 4

-------------------------------------------------------------------------------------------------
    eventno      |    eventtype     |     sipaddr      |     dipaddr      |      sport       |      dp
-------------------------------------------------------------------------------------------------
       1         |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      10486       |
-------------------------------------------------------------------------------------------------
                                        Behavior: DEPENDENT_STATES_2.b2
       2         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------
                                        Behavior: DEPENDENT_STATES_2.b2
       3         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------
       13        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      60435       |
-------------------------------------------------------------------------------------------------
```

Output for IMPORTING_STATES

```
Instances satisfying IMPORTING_STATES
=====================================

Total Matching Instances: 2

-------------------------------------------------------------------------------------------------------
    eventno      |    eventtype     |     sipaddr      |     dipaddr      |      sport       |      dp
-------------------------------------------------------------------------------------------------------
       1         |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      10486       |
-------------------------------------------------------------------------------------------------------
       13        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      60435       |
-------------------------------------------------------------------------------------------------------
```

Output for IMPORTING_BEHAVIORS_AS_STATE

```
================================================
Instances satisfying IMPORTING_BEHAVIORS_AS_STATE
================================================

Total Matching Instances: 2

-------------------------------------------------------------------------------------------------------
    eventno      |    eventtype     |     sipaddr      |     dipaddr      |      sport       |      dp
-------------------------------------------------------------------------------------------------------
                                          Behavior: DNS_REQ_RES.b
       1         |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      10486       |
       8         |    PACKET_DNS    |     10.1.4.2     |    10.1.11.2     |        53        |      10
-------------------------------------------------------------------------------------------------------
                                          Behavior: DNS_REQ_RES.b
       13        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      60435       |
       20        |    PACKET_DNS    |     10.1.4.2     |    10.1.11.2     |        53        |      60
-------------------------------------------------------------------------------------------------------
```

Output for IMPORTING_BEHAVIORS_AS_STATE_W_CUSTOMIZATION

```
================================================================
Instances satisfying IMPORTING_BEHAVIORS_AS_STATE_W_CUSTOMIZATION
================================================================

Total Matching Instances: 1

-------------------------------------------------------------------------------------------------------
    eventno      |    eventtype     |     sipaddr      |     dipaddr      |      sport       |      dp
-------------------------------------------------------------------------------------------------------
                                          Behavior: DNS_REQ_RES.b
       13        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      60435       |
```

```
       20        |    PACKET_DNS    |     10.1.4.2     |    10.1.11.2     |        53        |      60
-------------------------------------------------------------------------------------------------------
```

Output for WILDCARDING

```
================================================================
Instances satisfying WILDCARDING
================================================================


================================
Instances satisfying WILDCARDING
================================

Total Matching Instances: 20

-------------------------------------------------------------------------------------------------------
    eventno      |    eventtype     |     sipaddr      |     dipaddr      |      sport       |      dp
-------------------------------------------------------------------------------------------------------
       1         |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      10486       |
-------------------------------------------------------------------------------------------------------
       2         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       3         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       4         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       5         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       6         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       7         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       8         |    PACKET_DNS    |     10.1.4.2     |    10.1.11.2     |        53        |      10
-------------------------------------------------------------------------------------------------------
       9         |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       10        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       11        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       12        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       13        |    PACKET_DNS    |    10.1.11.2     |     10.1.4.2     |      60435       |
-------------------------------------------------------------------------------------------------------
       14        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
       15        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
```

```
      16        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
      17        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
      18        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
      19        |    PACKET_DNS    |     10.1.6.3     |     10.1.4.2     |        53        |      32
-------------------------------------------------------------------------------------------------------
      20        |    PACKET_DNS    |     10.1.4.2     |    10.1.11.2     |        53        |      60
-------------------------------------------------------------------------------------------------------
```