Hello,

I have problems with Suricata when I use a bridge in Linux Debian Squeeze.

Configuration:

1. `brctl addbr br0`
2. `brctl addif br0 eth1 eth2`
3. `ifconfig br0 up`
4. `ifconfig eth1 up`
5. `ifconfig eth2 up`
6. `iptables -A INPUT -j NFQUEUE --queue-num 0`
7. `suricata -c suricata.yaml -l /var/log/suricata/ -q 0`

With this rule, Suricata can log the alert:

```
alert tcp any any -> any 80 (msg:"/etc/passwd"; content:"/etc/passwd"; nocase; sid:9900005; rev:2;)
```

But when I change "alert" to "drop" or "reject", Suricata fails with error code: `SC_ERR_LIBNET_WRIT`.

If I enable the log in iptables:

```
1. iptables -F
2. iptables -A FORWARD -j LOG
3. iptables -A INPUT -j NFQUEUE --queue-num 0
4. suricata -c suricata.yaml -l /var/log/suricata/ -q 0
```

Iptables said this error:

```
[1675.365811] IN=br0 OUT=br0 PHYSIN=eth2 PHYSOUT=eth1 SRC=192.168.2.1 DST=192.168.2.104 LEN=64 TOS=0x00 PREC=0x00 TTL=64 ID=24988  [2407] 2/1/2000 -- 02:45:36 - (respond-reject-libnet11.c:172) <Error> (RejectSendLibnet11L3IPv4TCP) -- [ERRCODE: SC_ERR_LIBNET_WRIT]
```

Suricata hunts the alert but it can't drop or reject the packet.

Thx you and sorry for my English :(

---

**History**

#1 - 08/25/2010 01:32 AM - Joaquin Moreno

Sorry:

Is not INPUT, I use FORWARD:

"iptables -A INPUT -j NFQUEUE --queue-num 0" -> "iptables -A FORWARD -j NFQUEUE --queue-num 0"

Thx.

#2 - 08/25/2010 01:34 AM - Victor Julien
Are you sure you're getting the SC_ERR_LIBNET_WRIT error even with only "drop" rules? That would be strange as the reject code should not be activated in that case.

Hello,

you're right, the error is only when the reject is enable, no drop. Sorry. The full error with reject option is this:

```
[ 1675.365811] IN=br0 OUT=br0 PHYSIN=eth2 PHYSOUT=eth1 SRC=192.168.2.1 DST=192.168.2.104 LEN=64 TOS=0x00 PREC=0x00 TTL=64 ID=24988
```

Now, drop works in bridge mode if i change the iptables rule:
```
iptables -A FORWARD -j NFQUEUE --queue-num 0
```

For that rule:
```
iptables -A FORWARD -j NFQUEUE --queue-num 0 -m physdev --physdev-in eth2 --physdev-out eth1
```

It works now but only in one direction.

Now i am working for read in two directions but i can't do it.

PD: Next week i want to import private certificate web for read SSL sesions(it's posible?)

---

**#4 - 08/25/2010 02:15 PM - Pablo Rincon**

Hi Joaquin.

As far as I know suricata cannot read ssl session (even with the certificate). If you find a way to inject decrypted traffic temporarily to an interface/nfqueue, then you can inspect it as normal. But suricata doesn't decrypt ssl sessions itself. Anyway, if you find a way to do it, please, share it here ;)  

Regarding to directions, if you specify --physdev-in eth2 --physdev-out eth1 it will only work from eth2 to eth1. I'm not familiar to nfqueue, but what about specifying
```
iptables -A FORWARD -j NFQUEUE --queue-num 0 -i br0
```

Does it work?

**#5 - 09/02/2010 04:29 AM - Victor Julien**

- Status changed from New to Closed

Assuming fixed. Please reopen if it isn't.