FreeBSD Administration - Bug #277

Snort on pfSense Router Not Sending Alerts to MySQL Database

12/27/2013 02:51 PM - Daniel Curtis

Status:	Closed	**Start date:**	12/27/2013
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Intrusion Detection/Prevention	**Estimated time:**	0.50 hour
Target version:	pfSense 2.1.5	**Spent time:**	1.00 hour

Description

I encountered a problem during the configuration of the Snort IDS with Barnyard2 where the alerts triggered by Snort were not being sent to the remote database configured to receive the alerts. I checked the configuration in Services -> Snort -> *{Snort Interface}* -> *{Interface}* Barnyard2 and found it to be set to:

```
alert, mysql, user=user password=pass dbname=snorby host=IP
```

This however is incorrect, I needed to set it to the proper configuration:

```
output database: alert, mysql, user=user password=pass dbname=snorby host=IP
```

Once I set the proper configuration Barnyard2 began sending alerts to the remote MySQL database.

History

#1 - 02/16/2015 02:13 PM - Daniel Curtis

- Project changed from 32 to FreeBSD Administration

- Category set to Intrusion Detection/Prevention

- Target version set to pfSense 2.1.5