Pandora FMS

User Manual

Monitoring with IPTraf

User Manual Monitoring with IPTraf

Index

1 Changelog

Date	Author	Change	Version
10/07/12	Dario	First Version	v1r1

2 Introduction

Pandora FMS allows you to monitor network traffic statistics processed by **IPTraf**.

IPTraf collects network activity statistics from one or all interfaces and stores all information in a logfile.

A **passive collector** filters the information based on rules and creates a tree structure with all the information. One XML file per IP detected will be generated using the network activity information contained in the tree structure.

Once XML files are processed, one agent per IP detected will appear in Pandora FMS, these agents will have several modules with their network traffic information.

3 Compatibility Matrix

Was tested in these systems	• IPTraf 1.1.1

It should work in these systems	• IPTraf 1.1.1 and higher

4 Documentation provided by the requesting area

These parameters must be provided by the area which request the monitoring services:

- Full path of IPTraf logfile
- Filtering rules for logfile (explained below)

4.1. Filtering rules

To understand filtering rules first we must understand IPTraf logfile structure.

4.1.1. IPTraf logfile structure

And example of a log line is:

```
Mon Nov 22 15:41:59 2010; TCP; eth0; 52 bytes; from 192.168.50.2:54879 to
91.121.0.208:80; first packet
```

After the date and hour record there is the protocol, the interface name, the number of bytes transfered, the source ip and port and the destination ip and port. After will appear some information in this case indicates this communication is the first package.

Important data in this line are the interface name, the number of bytes transfered, the source IP and port and the destination IP and port.

4.1.2. Collector filtering rules

The rules have the following structure:

```
[process/discard] [!][ip_src/ip_dst] ip/mask [!][port_src/port_dst] port [!]
[protocol] protocol
```

The **first parameter** could be *process* if you want to process the records which match this rule or *discard* if you want to discard the record that match.

The **second parameter** set the match with source (ip_src) or destination IP (ip_dst). This parameter could be denied with the character (!) before, indicating we want the records that DON'T match with this IP.

The **third parameter** is an IP following by a network mask. If you want only an IP you can set the IP without mask or the mask 32. If a mask is specified all IP in the range will be considered.

For example, 192.168.50.0/24 will be IPs in range 192.168.50.1-192.168.50.254. Otherwise 192.168.50.23 y 192.168.50.23/32 are the same IP 192.168.50.23.

The **fourth parameter** is similar to second one but this time the instead of IP we will filter by source (port_src) or destination port (port_dst). Also it is possible to use character (!) before port to

denied these ports.

The **fifht parameter** are the port numbers which will be used to match the record.

You can specify the following parameters:

- One port with a number. For example 8080.
- An interval separated by a dash character. For example 21-34 to match all ports from 21 to 34 both included.
- A port enumeration separated by comma. For example 21,23,80,8080.
- A combination of intervals and enumerations. For example 21-34,80,8080,43234-43244.

The **sixth parameter** is the protocol used to perform the communication. This parameter could be denied with character (!) before, it indicates you want the records which DON'T match with this protocol. es el protocolo por el que se realiza la comunicacion. Este parametro puede ir negado con el caracter de exclamacion (!) delante, indicando que queremos los registros que NO coincidan con ese protocolo.

You can use the following formats:

- A protocol. For example TCP.
- Several protocol separated by comma. For example TCP,UDP,FTP.
- A special word "all" to match all protocols.

4.1.2.1. Examples

Some valid rules are:

```
discard src_ip 192.168.70.222/32 !port_dst 21-23,80,8080 protocol all
process src_ip 192.168.70.0/24 !port_src 0 !protocol TCP
process src_ip 192.168.80.0/24 !port_dst 80,8080 protocol UDP,TCP
```

These rules will process the following records:

- All records with source IP an IP in network 192.168.80.X while don't have 80 or 8080 as destination port and use TCP or UDP protocols.
- All records with source IP in network 192.168.70.X with any source port that don't use TCP protocol except record discard by the first rule. The first rule discard record with source IP 192.168.70.222 and destination port different from 21,22,23,80 and 8080 using any protocol.

5 Modules of this plugin

The plugin creates modules dinamically based on filtering rules defined and on network traffic detected by IPTraf.

Inside Pandora FMS will appear one agent per IP detected with several modules showing the network statistics for this IP.