

**PANDORA**FMS  
E N T E R P R I S E

**Pandora FMS**  
**Manual Usuario**  
**Monitorización con IPTraf**



## ***Manual Usuario Monitorización con IPTraf***

© Artica Soluciones Tecnológicas 2005-2012

### **Índice de contenido**

1	Histórico de cambios.....	3
2	Introducción.....	4
3	Matriz de compatibilidad.....	5
4	Documentación que debe entregar el Área que requiere la monitorización.....	6
4.1	Reglas de filtrado .....	6
4.1.1	Estructura del log de IPTraf .....	6
4.1.2	Reglas de filtrado del recolector .....	6
4.1.2.1	Ejemplos .....	7
5	Modulos del plugin.....	8



## 1 HISTÓRICO DE CAMBIOS

---

Fecha	Autor	Cambio	Versión
10/07/12	Dario	Primera Versión	v1r1

## 2 INTRODUCCIÓN

---

Con Pandora FMS es posible realizar una monitorización del tráfico de red que resulta del procesamiento realizado por la aplicación **IPTraff**.

A través de la utilidad de estadísticas de red IPTraff se recogerá la actividad de la red en una interfaz determinada (IPTraff también nos da la posibilidad de escoger todas las interfaces). Toda la actividad de la red es almacenada en un log.

Un **recolector pasivo** filtra la información basándose en unas reglas establecidas y crea un árbol con la información. Con este árbol, que contiene toda la información de la actividad de red, se generará un archivo XML por cada dirección IP detectada con toda la información de su tráfico de red.

Una vez los archivos XML son procesados por Pandora FMS verá un agente por cada IP detectada y como módulos la información de su tráfico de red asociado.

### 3 MATRIZ DE COMPATIBILIDAD

---

**Sistemas donde se ha probado**

- IPTráf 1.1.1

**Sistemas donde debería funcionar**

- IPTráf 1.1.1 y superiores

## 4 DOCUMENTACIÓN QUE DEBE ENTREGAR EL ÁREA QUE REQUIERE LA MONITORIZACIÓN

Los parámetros necesarios para la monitorización que tiene que proporcionar el área que requiere los servicios de monitorización son:

- Ruta del archivo de log de IPTraf
- Reglas de filtrado para el log (se describen más abajo)

### 4.1. Reglas de filtrado

Para entender las reglas debemos entender primero la estructura del log que nos generara el IPTraf.

#### 4.1.1. Estructura del log de IPTraf

Un ejemplo de registro del log:

```
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
```

Tras el registro de la fecha y hora de registro, aparece el protocolo, el nombre de la interfaz, el numero de bytes transferidos, la ip y puerto de origen y la ip y puerto de destino de la comunicacion. Después aparecera algo mas de informacion que en este caso es un indicardor de que la comunicacion se trata del primer paquete.

Los datos importantes de este registro de cara al script sera el nombre de la interfaz, el numero de bytes transferidos y las IPs y Puertos de origen y destino.

#### 4.1.2. Reglas de filtrado del recolector

Las reglas tienen la siguiente estructura:

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

El **primer parametro** puede ser process si queremos que los registros que coincidan con la regla se introduzcan en el arbol o discard si por el contrario queremos descartar las coincidencias.

El **segundo parametro** indica si la coincidencia debe ser con la ip de origen (ip\_src) o de destino (ip\_dst). Este parametro puede ir negado con el caracter de exclamacion (!) delante, indicando que queremos los registros que NO coincidan con esa IP.

El **tercer parametro** es una IP seguida de una mascara de red. Si se desea solamente una IP en la regla se podra especificar o bien sin mascara o bien con la mascara 32. Si se especifica otra mascara se consideraran las IPs que esten dentro de dicho rango.

Por ejemplo, 192.168.50.0/24 serán las IPs del rango 192.168.50.1-192.168.50.254. En cambio 192.168.50.23 y 192.168.50.23/32 corresponden de igual manera a la IP 192.168.50.23.

El **cuarto parametro** es parecido al segundo, solamente que en vez de con la IP se especifica si vamos a procesar o descartar (dependiendo de que aparezca o no el simbolo de exclamacion delante) un puerto de origen (port\_src) o de destino (port\_dst).

El **quinto parametro** es el puerto o conjunto de puertos que la regla hara coincidir.

Se pueden especificar en los siguientes formatos:

- Un solo puerto con tan solo poner dicho numero. Por ejemplo 8080.
- Un intervalo de puertos con un guion como separador. Por ejemplo 21-34 para que evalúe los puertos del 21 al 34 ambos incluidos.
- Una enumeracion de modulos separados por comas. Por ejemplo 21,23,80,8080.
- Una combinacion de intervalos y enumeraciones. Por ejemplo 21-34,80,8080,43234-43244.

El **sexto parametro** 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.

Se pueden especificar en los siguientes formatos:

- Un solo protocolo. Por ejemplo TCP.
- Una enumeración de protocolos. Por ejemplo TCP,UDP,FTP
- Una palabra especial para indicar que se escuchen las transferencias de todos los protocolos. En lugar de los puertos se pone la palabra "all"

#### 4.1.2.1. Ejemplos

Algunos ejemplos validos de reglas serian:

```
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
```

La combinacion de estas reglas nos hara que se procesen:

- Todos los registros que tengan como IP origen IPs de la red 192.168.80.X siempre que no tengan como puerto destino ni el 80 ni el 8080 y sean de protocolo TCP o UDP.
- Todos los registros que tengan como IP origen IPs de la red 192.168.70.X independientemente del puerto de origen y que no sean de protocolo TCP excepto los descartados por la primera regla, que serán aquellos registros con la IP 192.168.70.222 de origen cuyo puerto destino sea diferente a los puertos 21,22,23,80 y 8080 independientemente del protocolo.

## 5 MODULOS DEL PLUGIN

---

El plugin crea los módulos de forma dinámica en base a las reglas definidas y al tráfico de red analizado por la herramienta IPTraf.

En Pandora FMS aparecerán tantos agentes como IP sean detectadas y los módulos de estos agentes contendrán las estadísticas de red para dichas IP.