PANDORA FMS

NETWORK DEVICES MONITORING

PANDORAFMS

INTRODUCTION

This document aims to explain how Pandora FMS can monitor all the network devices available in the market, like Routers, Switches, Modems, Access points, etc.

Pandora FMS can measure your network bandwidth by consulting your router/switch through SNMP or by processing the network statistics sent by your routers. Getting the correct information about the bandwidth and the consumption of the network devices is crucial to achieve a better network management.

These are some of the main important things that Pandora FMS can do with your networks:

* Avoid bottlenecks in the network bandwidth and the server.

* Localize what applications and which servers are consuming your bandwidth.

* Provide a better quality services to the users being proactive.

* Reduce costs in the acquisition of the bandwidth and the hardware that better fits your actual load.

* Get answer to the questions: Who uses your bandwidth, where and how is it used?

Routers, Switches, modems, AP's and other network devices use a common language: SNMP. With Pandora FMS you can set up a device with just a few clicks and start to monitor the bandwidth, the interface, the load average, memory usage and many other things. You will also get different reports to obtain useful information about the performance of your systems, besides all the information that we can capture through the **SNMP protocol**, the ICMP protocol (status and latency) and TCP (information about the ports).

1. SNMP

When we talk about SNMP Monitoring, the most important thing is to separate two concepts: Test (polling) and Traps.
SNMP testing involves ordering Pandora FMS to execute a snmpget command to the SNMP device such as a router or a switch or even a computer with a SNMP agent installed. This is a synchronous operation (every X seconds).

In the opposite, receive a SNMP trap is an asynchronous operation, that could happen or not, usually used to get alerts coming from the device like, for example, when your switch drops a connection with a port, or when your device gets too hot.

Pandora FMS works with SNMP using individual OID's. To Pandora FMS, each OID is a network module. So, if you want to monitor a 24 port Cisco Catalyst Switch, and be aware of the operative status of each port as well as the incoming and outgoing traffic, we have to define a total of 72 modules (24x3). The number of checks to be performed per second and the level of the network traffic that will use these checks will depend on the latency of the network.

To work with SNMP devices is required:

1. Know what is and how the SNMP protocol works (described in the RFC3411 published by the IETF).

2. Know the IP and the SNMP community of the remote device.

3. Enable the SNMP management of the device so that can make SNMP queries from the network server. This network server should be the one assigned by the agent where we are going to define the network modules. Also, we must take into

account that if we want that other network servers make queries in case of the assigned server falls, they will make it with a different IP address.

4. Know the exact OID of the remote device we want to monitor.

5. Learn how to manage the data returned from the device. The SNMP devices send data back in different formats: numeric, incremental counters, chains or boolean.

6. There are many wizards and automatic systems that allow to make a device discovery, and automatically monitor their interfaces, without registering or finding out individual OID's of each of them. The same is applied to other elements that can be monitored by SNMP within a network device (CPU, memory, storage, etc.).

Pandora FMS can work with any device that supports SNMP although now Pandora FMS works with **SNMP v1, v2, v2c and v3.**

1.1 Polling SNMP

To monitor any element through SNMP we should know at least its IP and its SNMP community. It's also interesting to know the OID that needs to be monitored, although it can be obtained through an SNMP Walk.

OIDs can appear translated or not, for being able to translate them we need to have the MIB of the device installed. These MIBs can be loaded from Pandora FMS Console through **MIB Uploader.**

Extract the modules one by one through the OID is a very hard work, and for that Pandora FMS integrates 2 SNMP Explorer that help us to quickly extract all the information of the devices to monitor.

1.1.1 SNMP Interface Wizard

With de **SNMP Interface Wizard** we could get, among other things, elements such as:

* Interface name
* Input and output traffic
* Errors
* Status
* IP address and MAC

1.1.2. SNMP Wizard

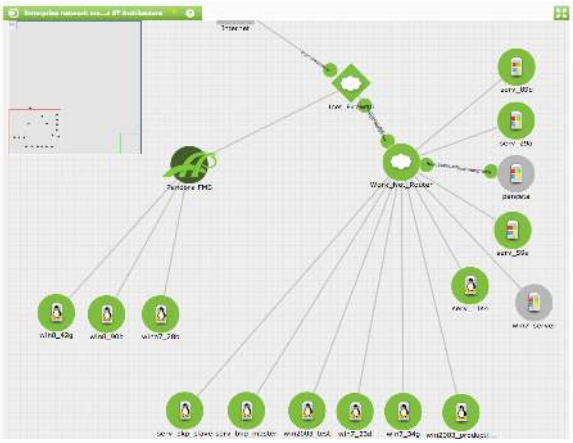
The SNMP Wizard allows us to extract the following information from the device as long as you can get from it the specific OIDs:

* Devices (read and write bytes).
* Processes (status).
* Free space on disk / memory.
* Temperature sensors.
* Other data (CPU, RAM).

1.2. Recon/SNMP exploration tasks

There is a kind of SNMP exploration that allows us to **detect all network, including topology (at link level), hierarchy (network level) an OS,** which automatically explores the system and monitors several metrics of all the available interfaces (Operative status, Inbound and Outbound traffic, MAC).

Through templates/policies it's possible to add more customized modules to start monitoring your devices automatically. A full Class B network can be detected and monitored **in less than an hour.**



Pandora FMS visualizes network maps and allows their modification by the administrator, adding nodes manually or automatically (through a new detected systems area). The topology is detected through SNMP, connecting the interfaces of each device depending on the information of the ARP tables of every device, and also detecting the gateways between networks at level 3.

1.3 SNMP Traps

Using SNMP traps is totally different. You can receive traps from any device without having to configure anything (except the **SNMP console**) When a trap is received, it will appear in the SNMP console. You can set an alert based on OID (the code that identifies a trap, something similar to 3.4.1.1.4.5.24.2), on an IP agent or custom data (data that can be in the trap). You can also order Pandora FMS to "copy" the information in a special text module in the agent. If the agent is defined this operation is called SNMP Traps Transfer.

The configuration of the sending of traps must be carried out in each network devices that will be monitored. In Pandora FMS we must authorize only those communities that will receive the traps and the network.

2. ICMP & TCP MONITORING

Besides the whole SNMP monitoring from which we can extract advanced monitoring, we can make basic checks through the network server or the ICMP Enterprise server (it makes checks through the nmap helping a much higher rate of checks than with the Open server), such as a **ping** to the device, calculate the **latency (RTT)** between the Pandora FMS server and the device, or checking the **status of the ports,** if they are open or closed. By default, TCP checks only test if the port of destination is open or not. Optionally it can be sent a text chain and wait to receive anything that will be directly treated by Pandora FMS as data. The amount of checks to be performed per second, and the level of network traffic that will use these checks depends on the latency that is in the network.

3. WEB TRANSACTIONAL MONITORING

Pandora FMS allows to monitor complex web transactions using a programmable robot. That includes logins, verification response, latency measurement and completeness of the whole transaction (n steps). Includes a session recorder (Firefox extension) and the possibility of make tests in a distributed way (in different servers), including timeout times and custom retries, and also the possibility to use the robot to capture numerical data and/or chain type.

Pandora FMS also has an advanced component to perform web transactions through a "zombie" browser (IE, Mozilla,Firefox, Chrome). This system

allows to execute flash, javascript, applets java and avoids any difficulty to implement a transactional monitoring over a web.

4. REMOTE PLUGIN

Pandora FMS allows to monitor complex web transactions using a programmable robot. In this paragraph we specify some existing plugins to extract remote information through the plugin server to different network devices. There are hundreds of plugins available at the public module library of Pandora FMS (Nagios modules can be reuse). The administrator can easily programm his own scripts:

* **cisco_check_command.pl .-** It's a generic script to analyze an output of the command on a Cisco device through Telnet. Could be used to test the version, the status of the power supply, etc.

* **check_asa_status.pl.-** This complement allows you to view the free memory available, used, total and know the CPU usage in the last 5 seconds, 5 minutes and last minute.

* **Iptraf collector.-** This collector allows to monitor the network traffic using Pandora FMS and the IP-Traf application.

* **Cisco Configuration Remote Inventory Plugin.-** This remote inventory plugin uses the block mode to show and detect changes in the configuration.

* **DNS Response Time.** Returns the response time of a specific server to solve an specific name.

* **IPMI.** Specific monitoring of server hardware and communications, usually to get status or environment parameters (temperature, traffic, power supplies, etc).

* **PacketLoss.** Packet loss (based on ICMP tests).

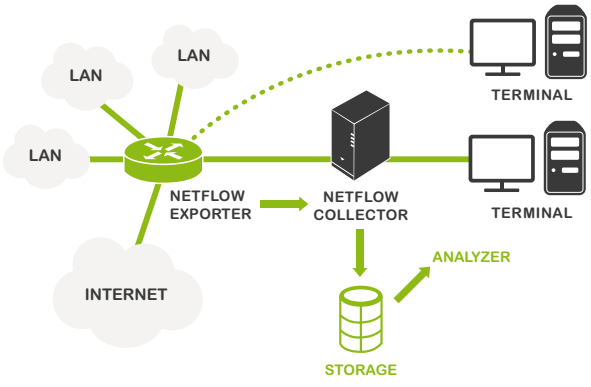
* **Cisco IP SLA.** Plugin that uses the new Cisco standard to measure the network performance on realtime. Some of the metrics measured by tag are MOS, ICPIF, out of sequence packets, late packets, average Jitter, Packetloss SD/DS, RTT, RTT DNS and Tcp RTT.

* **Cisco QoS.** Plugin that analyzes the average of loss, sending and reception of QoS specific filters.

5. NETFLOW

Pandora FMS can monitor the IP traffic using the NetFlow protocol. It allows to show patterns and general data about the traffic that are very useful.

Netflow is a network protocol developed by Cisco Systems to collect information about the IP traffic. Netflow has become a standard in the industry of network traffic monitoring, and actually it's supported by several platforms appart from Cisco IOS and NXOS, such as in devices from manufacturers like Juniper, Enterasys Switches and in Operating Systems like Linux, FreeBSD, NetBSD and OpenBSD.



Devices with Netflow enabled, when Netflow feature is activated, generates "Netflow records" that are small pieces of information that send to a central device or Netflow server (or Netflow collector), which is who receives the information from the de-

vices (or Netflow probes), keeps it and processes it. This information is transmitted through the Netflow protocol, based on UDP or STCP. Each Netflow re-gister es a small packet that has a minimum infor-mation capacity, but in any case contains raw data of the traffic, ie, it does not send the payload of tra-ffic that circulates through the collector but statis-tics data.

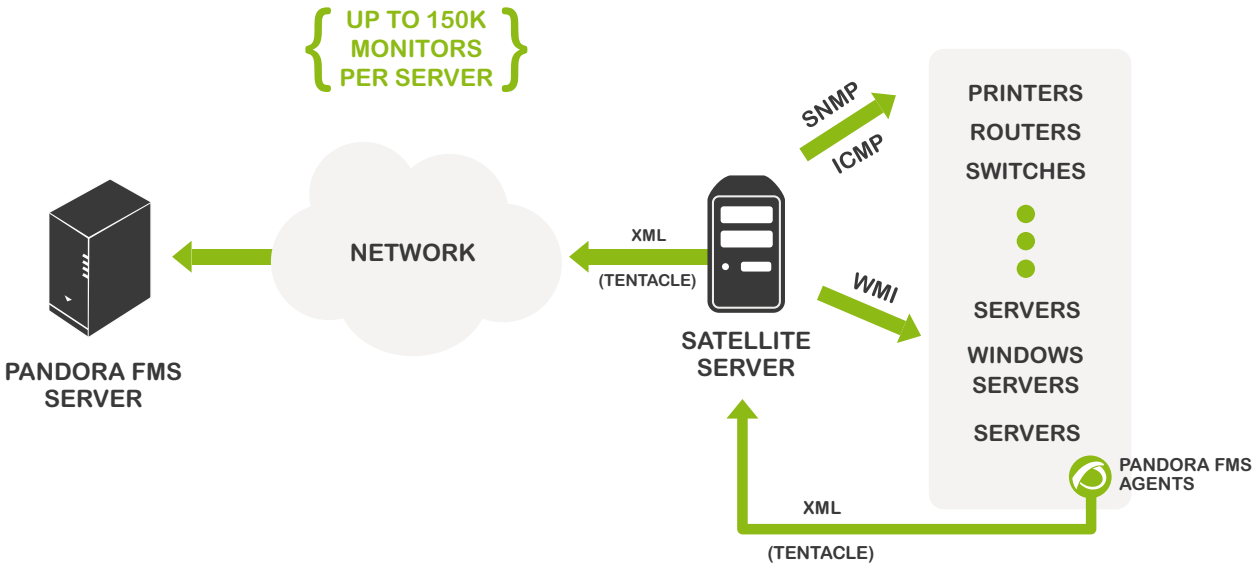
In Pandora FMS we can get those data through reports, direct data from the agent or view it directly through the Netflow viewfinder, what allows analysis and historic. There are several differences between the implementation of the original version of NetFlow, so some versions incorporate some more details, but overall, the basic Netflow sends at least the following information:

* Source IP address.
* Destination IP address.
* UDP or TCP de source port.
* UDP or TCP destination port.
* IP protocol.
* Interface (SNMP ifIndex).
* IP type of service.

6. NETWORK DEVICES INVENTORY

Within the Enterprise version, Pandora FMS includes a server dedicated to show inventory information **(inventory server).** To extract it, it executes custom scripts that contacts with the device in question and extracts the necessary information.

The are serial scripts to get the Cisco devices inventory, obtaininf the **CPU, IOS version, interfaces** and other hardware information (version, s/n). The

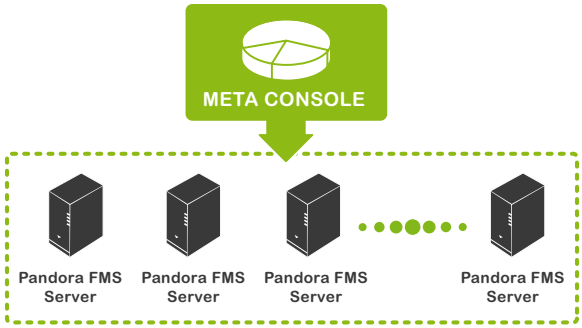


tool administrator can develop his own scripts of remote inventory.

7. FLEXIBLE ARCHITECTURE

7.1 Distributed Monitoring

There are different components (Satellite Server, Broker Agents, Distributed Servers, Export Servers, Tentacle Proxy) that allow different strategies at the time of monitoring a complex network environment, with limited connectivity complex topologies, intermitent connections, delegation of the monitoring to independent equipments, etc.



7.2 Scalability

With elements such as **Satellite Server** that allows to monitor thousands of systems with low latency (1-5 minutes), and the Metaconsole, that allows a lineal scalability using a federated server system, Pandora FMS makes possible to have a unic global vision while monitoring thousand of devices.

The specific cases of **Telefónica Spain** (8000 devices), and **Rakuten** (9000 devices), allow us to speak with names of actual cases of technical implementation of our system in the real world.

8. REPORTING

8.1 SLA Reports

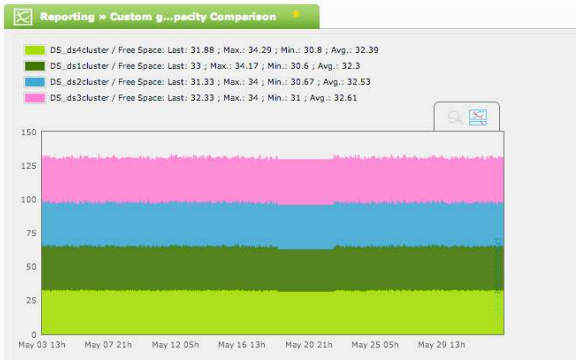
Pandora FMS has several SLA reports, which include compliance rates of service for each monitored metric, excluding the data of the scheduled system downtime (scheduled stops a posteriori included, if the system administrator allows it). The SLA reports

SLA reports view

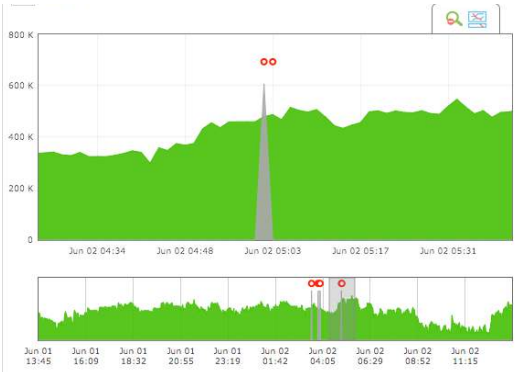
8.2 Graphs & Dashboards

Pandora FMS can show simple graphs, combined (with more than 1 data in the same graph), and put it all together in one or several dashboards, and make them automatically rotate in the screen. They are very useful in control centers.

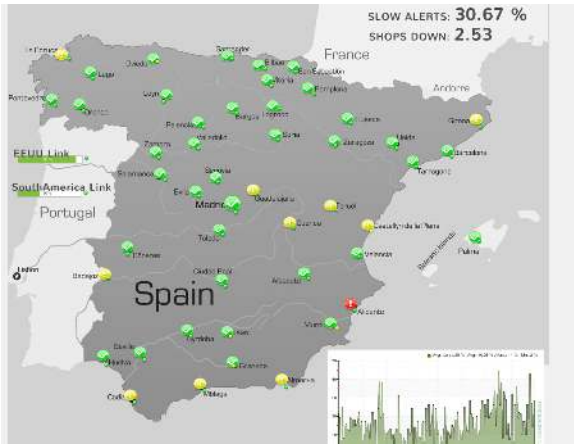
Dashboard reporting



Customized graph



Customized graph



Combined graph