PANDORA FMS

NETWORK DEVICE MONITORING

Version 2 二版
www.version-2.com

PANDORAFMS

INTRODUCTION

This document aims to explain how Pandora FMS is able to monitor all network devices available on the marke such as 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 things that Pandora FMS can do with your network:

* Avoid bottlenecks in the network bandwidth and the server.

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

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

* Reduce bandwidth and acquisition costs to better fit your actual load.

* To answer the following questions: where, how and by whom is your bandwith 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 average load, 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: Tests (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, receiving a SNMP trap is an asynchronous operation, that could happen or not, usually applied 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.

The requirements for working with SNMP devices are to:

1. Know what the SNMP protocol is, and how it 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 other network servers to make queries, in case the assigned server should fail, they'll be made using 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. SNMP devices return data in different formats: numeric, incremental counters, chains or boolean.

6. There are many wizards and automatic systems that allow the user to make a device discovery, and automatically monitor its interfaces, without registering or finding out individual OID's for each of them. The same applies 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 functions with **SNMP v1, v2, v2c and v3.**

1.1 SNMP Polling

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, to be able to translate them we need to have the device's MIB installed. These MIBs can be loaded from Pandora FMS Console through **MIB Uploader.**

Extracting modules one by one through the target OID can be hard work. Because of that Pandora FMS integrates 2 SNMP Explorers that quickly help us extract all the information from monitored devices.

1.1.1 SNMP Interface Wizard

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

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

1.1.2. SNMP Wizard

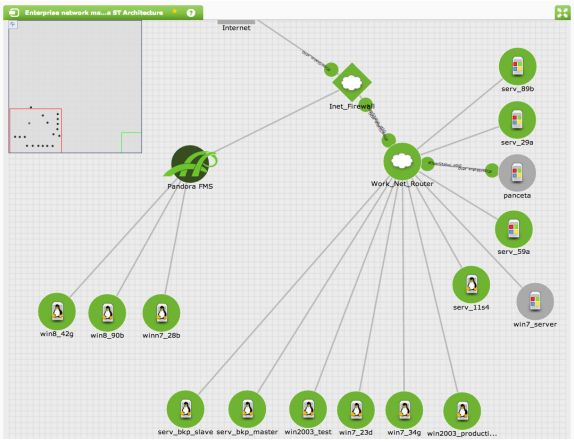
The SNMP Wizard allows us to extract the following information from the device as long as you can obtain the specified OIDs from the network:

* 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 the entire network, including its topology (at its link level), hierarchy, and OS,** which automatically explores the system and monitors several metrics of all the available interfaces (Operative status, Inbound and Outbound traffic, MAC address).

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 from the ARP tables of every device, and also detecting the gateways between peered networks.

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 on the SNMP console. You can set an OID-based alert (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 command Pandora FMS to "copy" the information onto a special text module in the agent. If the agent is defined this operation is called SNMP Trap Transfer.

Trap sending configuration must be carried out on each network device meant to be monitored. On 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 (which makes checks through nmap helping achieve a much higher rate of checks than with the Open server), such as sending a **ping** check to the device, calculate the **latency (RTT)** between the Pandora FMS server and the device, or checking the **port status,** if they are open or closed. By default, TCP checks only test if the destination port is open or not. Optionally, a text chain can be sent and you can wait to recieve anything that'll be treated as data directly by Pandora FMS. The amount of checks to be performed per second, and the level of network traffic that will be used by these checks depends on the latency found in the network.

3. TRANSACTIONAL WEB MONITORING

Pandora FMS allows monitoring 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 to make distributed tests (among different servers), including timeout times and custom retries, and also the possibility to use the robot to capture numerical data and/or chain types.

Pandora FMS also has an advanced component to perform web transactions through a "zombie" browser (IE, Mozilla,Firefox, Chrome). This system allows executing flash, javascript, java applets and avoids any difficulty implementing 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 on Pandora FMS's public module library (Nagios modules can be reused). The administrator can easily program its own scripts:

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

* **check_asa_status.pl.-** This complement allows you to view amount of total memory available, how much has been used and how much is used; as well as CPU usage over the last 5 seconds, 5 minutes, and the last minute.

* **Iptraf collector.-** This collector allows network traffic monitoring using Pandora FMS and the IPTraf 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 a specific name.

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

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

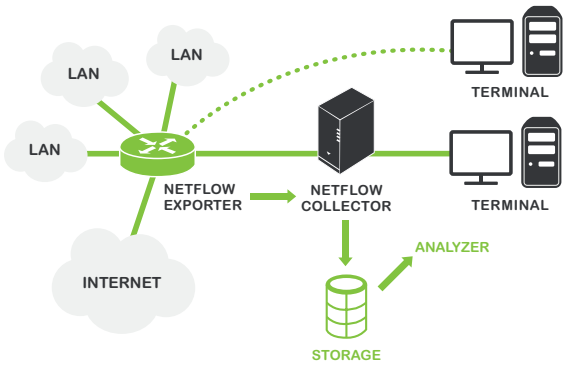
* **Cisco IP SLA.** Plugin that uses the new Cisco standard to measure the network performance in realtime. Some of the metrics measured by tags are MOS, ICPIF, out of sequence packets, late packets, average Jitter, Packetloss SD/DS, RTT, RTT DNS and Tcp RTT.

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

5. NETFLOW

Pandora FMS can monitor the IP traffic using the NetFlow protocol. It allows showing 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 network trafficking industry 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 featu-

re is activated, it generates "Netflow registries/logs" which are small pieces of information that send to a central device or Netflow server (or Netflow collector), which is recieving the information from the devices (or Netflow probes), and later keeps it and processes it. This information is transmitted through the Netflow protocol, based on UDP or STCP. Each Netflow registry es a small packet that has a minimum information capacity, but in any case contains raw data about the traffic, ie, it does not send the payload of traffic that circulates through the collector but instead provides statistics data.

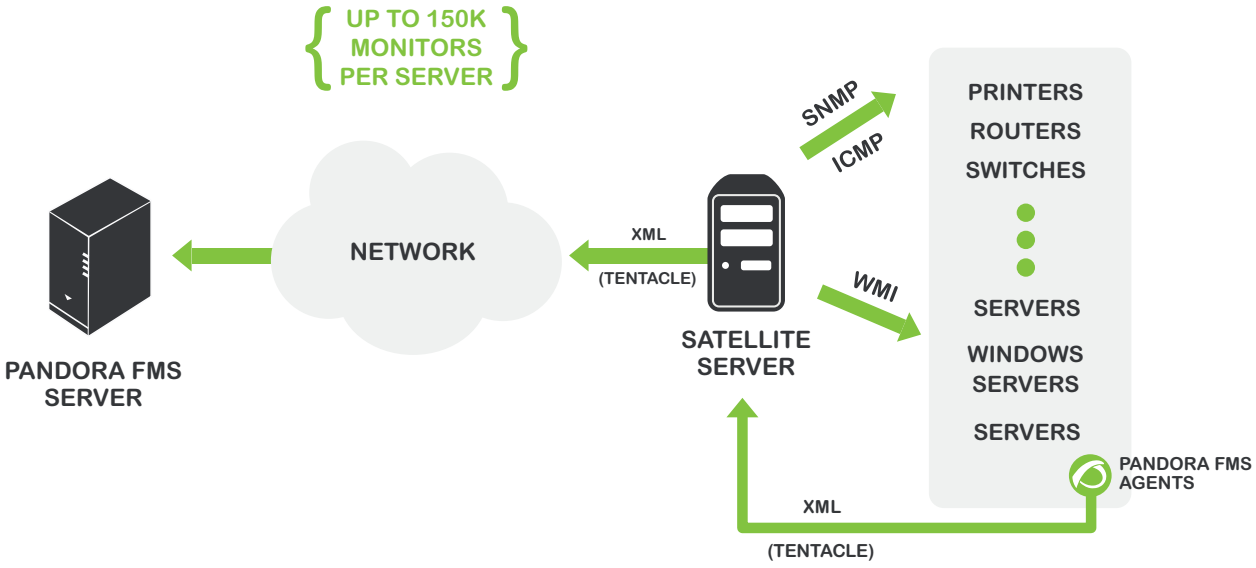
In Pandora FMS we can get this data through reports, direct data from the agent or view it directly through the Netflow viewfinder, which allows immediate and historic analysis. There are several differences from the implementation of the original version of NetFlow, so some versions incorporate some 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 dedicated server to show inventory information **(inventory server).** To extract it, it executes custom scripts that contact with the device in question and extracts the necessary information.

The are serial scripts to get the Cisco devices inventory, obtaining the **CPU, IOS version, interfaces**

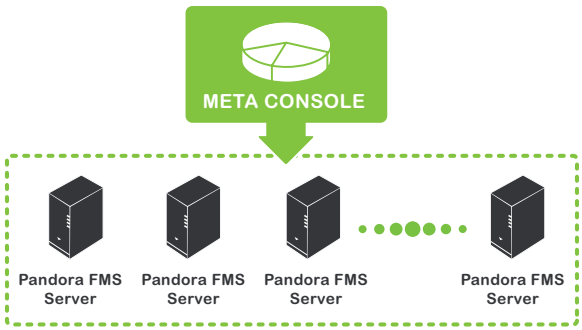


and other hardware information (version, s/n). The tool administrator can develop his remote inventory scripts.

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

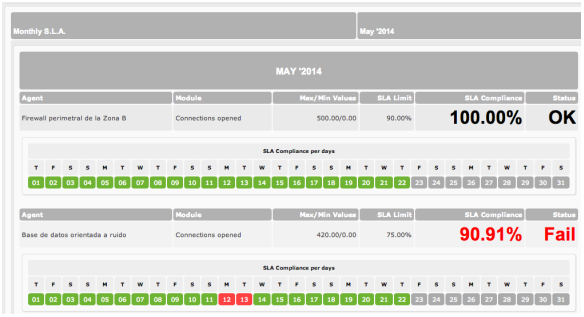
With elements such as a **Satellite Server** that allows monitoring thousands of systems with low latency (1-5 minutes), and the Metaconsole, that allows a lineal scalability using a federated server system, Pandora FMS makes it possible to have a unique global vision while monitoring thousand of devices,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

The specific cases of **Telefónica Spain** (8000 devices), and **Rakuten** (9000 devices), allow us to exemplify with real world cases of our system's technical implementation.

8. REPORTING

8.1 SLA Reports

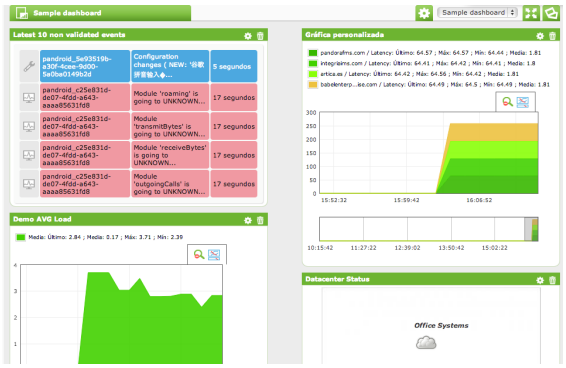
Pandora FMS has several SLA reports, which include compliance rates of service for each monitored metric, excluding the data of the scheduled system downtime (including stops scheduled for afterward, if the system administrator allows it). The SLA reports include different graphs in order to agilize and make their analysis easier.



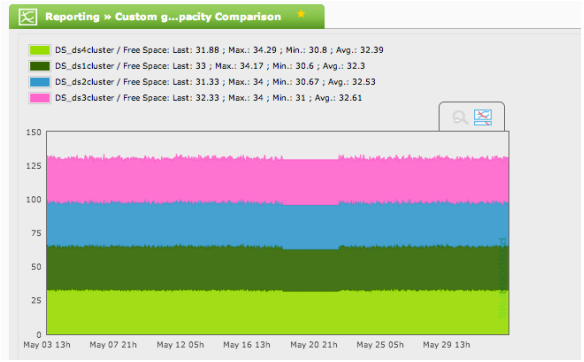
SLA reports view

8.2 Graphs & Dashboards

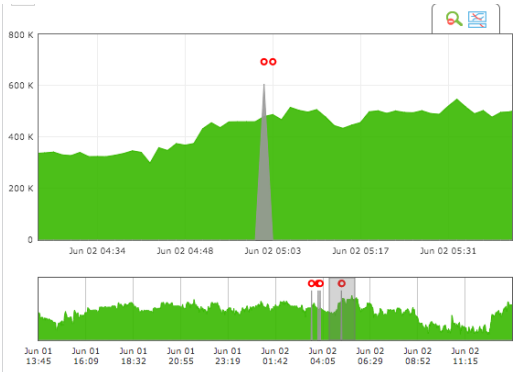
Pandora FMS can show both simple and combined graphs (with more than 1 piece of data in the same graph), and put it all together in one or several dashboards, and make them automatically rotate on the screen. They are very useful in control centers.



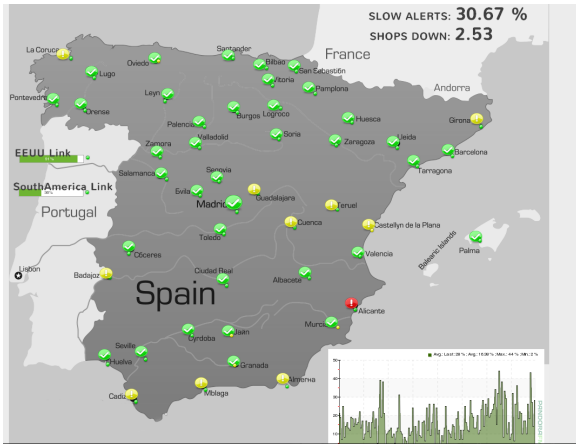
Dashboard reporting



Customized graph



Customized graph



Combined graph