Network Traffic Performance & Security Monitoring

Project proposal – minimal project

Orsenna; Invea-Tech
Contents
1. Introduction ........................................................................................................................................... 2
   1.1. General System Requirements ................................................................................................. 2
   1.2. Technical Requirements ........................................................................................................ 2
2. FlowMon Monitoring System ........................................................................................................... 3
   2.1. FlowMon Probes ................................................................................................................ 4
   2.2. FlowMon Collectors ............................................................................................................ 4
   2.3. Extension possibilities .......................................................................................................... 6
       2.3.1. FlowMon Reporter ..................................................................................................... 7
3. Deployment of the System in Enterprise Network ........................................................................ 8
4. Price Quotation .................................................................................................................................... 9
5. Company Profile .................................................................................................................................. 10
   5.1. About Invea .......................................................................................................................... 10
   5.2. About Orsenna .................................................................................................................... 10
   5.3. References ............................................................................................................................ 10
1. Introduction

The aim of the project proposal is to design a system for network traffic monitoring. The project proposal is based on the system requirements of IT department. The main objective of the project plan is to uncover the network data communication (in real-time and long-term) in order to ensure network security, detect attacks, monitor network communications, effectively administrate the network (saving the operating costs) and detection of bad configuration and network bottlenecks.

1.1. General System Requirements

List of system requirements:

- complete solution for real-time and long-term network communications monitoring,
- monitoring of Internet/uplink communications, monitoring of communications with key servers (mail server, file server, etc.), and monitoring of LAN and users,
- enhancement of network security by sending alerts when the problem in network is detected,
- possibility to extend the system to more branch offices.

1.2. Technical Requirements

List of technical requirements:

- easy and non-invasive installation into the current infrastructure (no influence to the current network functioning/operation),
- flexible and scalable architecture,
- IPv4, IPv6 & MPLS support.
2. FlowMon Monitoring System

FlowMon is complete solution for network monitoring based on IP flows. This NetFlow technology based solution provides complete overview of the network traffic. The FlowMon provides detailed information’s about all communications that take place in the network to the contrary of the SNMP technology, which provides only total counts of transferred bytes/packets. The FlowMon especially provides information about who communicates with whom, when, how long, how often, using what protocol and service, or how much data was transferred.

Deployment of the FlowMon solution enables to:

- enhancement of network security,
- monitoring of services and users activities,
- real-time network traffic monitoring,
- long-term storage of network traffic statistics,
- detection of internal and external attacks,
- effective supervising of network incidents,
- internet usage monitoring,
- and much more.

The FlowMon solution is perfectly scalable and offers flexible architecture that includes intelligent probes for NetFlow data export and collectors for NetFlow data storage and visualization.

![Figure 1: FlowMon solution architecture](image)
2.1. FlowMon Probes

The FlowMon probes are passive network devices dedicated to collecting packets, calculating statistics of IP flows and exporting detailed NetFlow v5/v9 statistics to the collectors. It is non-invasive compact device which is easy to deploy into the current network infrastructure using mirror ports (SPAN port) or TAP (Ethernet hub – copper or optic). Each probe has one administrative port used for remote configuration and export of NetFlow data, and one or more monitoring ports used for network monitoring.

The probes are configured remotely via web interface. Administrative port is used for remote access and communication is always encrypted (HTTPS, SSH). After the first configuration the probes are working fully automatically without the necessity of any other maintenance action. The probes also include built-in collector with FlowMon Monitoring Center application for storage and visualization of generated statistics.

2.2. FlowMon Collectors

The FlowMon collectors are stand-alone devices with high disk capacity dedicated for collection, long-term storage and visualization of network statistics generated by probes (or other NetFlow sources). Presentation of stored NetFlow data and its analysis (search, aggregation, extraction and so on) is done by secured web interface. The collector core application is called FlowMon Monitoring Center and is used for storage and visualization of statistics.

The data stored on the collectors can be displayed and analysed. The system allows for example the following operations:

- generation of long-term graphs and overviews with different types of views divided into the categories according to the amount of transferred data (bytes, packets, flows), IP traffic (TCP, UDP, ICMP, other), or protocol (HTTP, IMAP, SSH),
- generation of statistics and detailed extracts over the selectable time periods,
- extract of Top N statistics according to the different criteria (number of transferred bytes, packets, flows and so on) which allows you to list the most active or abnormal computers participating in network traffic,
- sending of email notification to administrators based on user defined event,
- creation of profiles for saving the data that comply with defined filters,
• detailed text extracts of particular flows with the possibility of filtering and aggregation.

Basic configuration of FlowMon Collectors contains two applications – FlowMon Configuration Center (FCC) which is used for setting up the device and FlowMon Monitoring Center (FMC) which is used for collecting and visualization of the network statistics. Besides these two modules there are available additional modules (plug-ins) that extend the functionality of the collector.
2.3. Extension possibilities

Functionality of the FlowMon monitoring system (probe or collector) can be extended by other plugins for different purposes:

- **Invea FlowMon Reporter** – intelligent reporting tool,
- **Invea FlowMon HTTP Logger** - monitoring of visited web pages,
- **FlowMon ADS** – anomaly detection system,
- **Invea NAT Detective** - detection of illegal NAT routers (for example wifi access points),
- **Invea FlowMon Firewall Auditor** - effective tool for firewall settings audit,
- **Invea Data Retention** - data retention law solution,
- **CognitiveOne** - network behavior analysis system,
- **Zabbix** - powerful monitoring tool for supervising over the network elements (servers, computers, switches, probes) and services provided by these elements (mail, www, etc.).

Overview of all available plugins can be found on our website [www.invea-tech.com](http://www.invea-tech.com) and you can try it online at [https://demo.invea-tech.com](https://demo.invea-tech.com).

Besides standardly offered plugins it is possible to modify the solution or to add a brand new functionality based on the requirements.
2.3.1. FlowMon Reporter

Invea FlowMon Reporter (IFR) is an extension plugin for FlowMon probes and collectors. It enables user to visualise network traffic statistics in pie graphs, continuous graphs and tables. User doesn't have to be skilled in computer networks to get all information necessary for control the usage of servers in local network and internet and to supervise network users communication. It allows user to visualize the structure of traffic and used services, identify top talkers, plan the link capacity and much more.

- Top reports - top communicating hosts, services and conversations in selected traffic shown in table and pie graph.
- Traffic report - traffic visualisation for selected time period, the graph shows traffic intensity in time and evaluate basic statistics including 95 percentile.
- Each user can create its own set of reports consisting of pre-defined chapters including tables and graphs. To work with reports user doesn't need to be technically skilled in computer networks. The set of pre-defined chapters can be extended by network administrator according to the needs of users.
- Periodically sends selected report to user email, PDF or CSV format is supported.

![Image of top network services and structure of specific protocol traffic]

Figure 4: User defined statistic.
3. Deployment of the System in Enterprise Network

Based on the requirements of IT department and our experiences with deploying of the system following infrastructure was designed:

- Using one SPAN/mirror port on the backbone switch connected to monitoring port of probe FlowMon Probe 1000 (one metallic GbE port), which can handle up to 500 000 packets per second. It enables to get view into all network communications going through central network unit – i.e. communications of users with Internet and servers, all servers communications and complete traffic from/to Internet.

- For data collection a built-in collector on probe will be used. Its storage capacity of 500 GB is sufficient for storage of the data for up to several months.

Note: For smaller networks (up to approx. 100 PCs) it is possible to use probe FlowMon Probe 100 Office (one metallic port 100 MbE) with performance of 150 000 packets per second and storage capacity of 80 GB.
4. Price Quotation

Price quotation including extended support is in the following tables:

Option with FlowMon Probe 1000

<table>
<thead>
<tr>
<th>P/N</th>
<th>Description</th>
<th>Your price</th>
<th>Qty</th>
<th>Final price without VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFP-1000-CU</td>
<td>FlowMon Probe 1000</td>
<td>3 599 €</td>
<td>1</td>
<td>3 599 €</td>
</tr>
<tr>
<td>FP-INST</td>
<td>Installation, configuration and training - 1 day</td>
<td>990 €</td>
<td>1</td>
<td>990 €</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>4 589 €</strong></td>
</tr>
</tbody>
</table>

Option with FlowMon Probe 100 Office

<table>
<thead>
<tr>
<th>P/N</th>
<th>Description</th>
<th>Your price</th>
<th>Qty</th>
<th>Final price without VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFP-100-CU</td>
<td>FlowMon Probe 100 Office</td>
<td>1 599 €</td>
<td>1</td>
<td>1 599 €</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>1 599 €</strong></td>
</tr>
</tbody>
</table>

Gold support

<table>
<thead>
<tr>
<th>P/N</th>
<th>Description</th>
<th>Your price</th>
<th>Qty</th>
<th>Final price without VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>GS-IFP-1000-CU</td>
<td>Gold Support: FlowMon Probe 1000</td>
<td>684 €</td>
<td>1</td>
<td>684 €</td>
</tr>
<tr>
<td>GS-IFP-100-CU</td>
<td>Gold Support: FlowMon Probe 100 Office</td>
<td>304 €</td>
<td>1</td>
<td>304 €</td>
</tr>
</tbody>
</table>

12-month extended support and maintenance include all updates and upgrades (new functions), support web access, email and phone customer support in working hours (8x5), remote SSH support, 4 hours of network expert consultations and bring in hardware support with 5 days response time.
5. Company Profile

5.1. About Invea

INVEA-TECH is devoted to the development of state-of-the-art solutions for networks from 10Mb/s to 100Gb/s. Product portfolio covers especially field of monitoring and security of network traffic (technology NetFlow, SNMP, filtering) and field of lawful intercept and data retention law. Regarding services INVEA-TECH offers security analyses of networks based on real measurements of network traffic that provides detailed view into network and discovers security, configuration and performance problems in network.

5.2. About Orsenna

ORSENNA is devoted to network monitoring and auditing solutions. Product portfolio covers especially field of network and application monitoring (technology NetFlow, SNMP, WMI, JMX). ORSENNA is the 1st engineering partner for products like WhatsUp, Orion & Scrutinizer. Regarding services ORSENNA offers implementation on site of solutions

5.3. References

GEANT2: pan-European multi-gigabit network – monitoring solution FlowMon based on the NetFlow (security). Deployment on the backbones – Switzerland (SWITCH), Netherlands (SURFnet), Greece (Grnet), Czech Republic (CESNET), Bulgaria (Bren) and more.


Public administration (ministry, municipalities, regions, hospitals), academic organisations (universities, The Academy of Sciences of the Czech Republic, National Library of the Czech Republic), private segment (AVG, Aegon, Uniq, MVV Energie, Seznam.cz, Marius Pedersen, etc.)
Contact Details

ORSENNA
14 Rue Gambetta
78600 Mesnil Le roi
France

Web: www.orsenna.com
Email: info@orsenna.com
Tel.: +331 34 93 35 35

INVEA-TECH a.s.
U Vodárny 2965/2
Brno 61600
Czech Republic

Web: www.invea-tech.com
Email: info@invea-tech.com
Tel.: +420 511 205 250

Copyright

Any information herein is believed to be reliable. However, ORSENNA assumes no responsibility for the accuracy of the information. Except as stated herein, none of the document may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form or by any means including, but not limited to, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of ORSENNA.

Copyright © 2011 ORSENNA All rights reserved.