novicom

# Concept

## Central Monitoring and IP Address Administration

# Concept of Central Monitoring and IP Address Administration

*Novicom Company together with its partner Invea-tech offer a unique concept of Centralized monitoring of infrastructure, network and applications integrated with IP administration tools.*

*The concept covers all monitoring and IP address space management needs of large scale organizations. It increases the reliability and efficiency of basic operational services and provides high level of security to the network and network access.*

*We are able to provide unified environment for network and infrastructure administration. One application allows the management of systems that would have been otherwise operated separately, often by different administrators.*

## The main goals are

- Make network management way more simple and efficient.
- Significantly increase operational reliability of the core network services.
- Bring maximum level of network security.
- Provide complete overview of monitored infrastructure, network and applications.

## The example of Central monitoring and IP network administration in use

Integrating AddNet together with network behavior analyzing system ADS FlowMon and advanced monitoring system MoNet brings rapid increase of operational flexibility when solving security incidents.

| | |
|---|---|
| 1. Security anomaly is noticed | => FlowMon ADS |
| 2. Anomaly is presented in the monitoring application | => MoNet |
| 3. Details of the security anomaly are determined | => FlowMon ADS |
| 4. Details about a device are presented (IP/MAC/Location/History) | => AddNet |
| 5. Compromised device is disconnected from the network | => AddNet |

Concept may be used entirely with all of its features as well as implemented gradually according to the priorities of our customer.

# Overview of All Areas of the Concept

## MoNet

Universal Monitoring

- Applications
- Applications serv.
- Database
- Operating syst.
- Virtualization
- Hardware
- Network components
- Environment

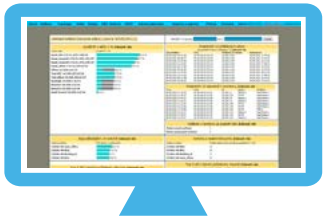
Independent monitoring

Distributed monitoring

Open monitoring

SLA Reporting

## AddNet



IPAM

- IP address space management
- IP Monitor – history IP/MAC

DDI – Core net services

- DHCP
- DNS
- RADIUS

Active net components

- Repository
- Port monitor

Security

- Authentication, Authorization ( 802.1x )
- BYOD and mobile devices
- Crisis sets

## FlowMon ADS

Collection of traffic data

- NetFlow v5/v9
- Content is not monitored

Operation statistics

- Volumetric characteristics
- Listings of communications
- Analysis of the peaks

Behavioral analysis

- Anomaly
- Attacks
- Strange behavior
- Operational problems

Dashboard

- Top statistics
- Security incidents

# AddNet

*AddNet is a unique system which highly increases the efficiency of IP address management and access control in large networks. It is achieved by integrating IP address management system, core network services (DHCP, DNS, Radius) and communication with networking hardware.*

## AddNet Provides:

### Central IP address management

› Forcing IP address policies, reserving address blocks

### Support of emergency scenarios

› Preset emergency settings – mass operations for emergency solutions

### IP/MAC address and port monitoring

› Locating point of connection and thoroughly logging all events.

### Increasing network security by using 802.1x authentication and authorization.

› MAC authentication –Terminate network connection of unauthenticated devices.

› MAC authorization – Assigning devices to corresponding VLANS

### Increasing operational reliability and security of core network services

› N+1 redundancy of Active-Active type for DHCP, DNS and Radius

### Making IP network administration much easier

› increases efficiency of network administrators by more than 90%
- Adding devices, relocating IP address space, track locations and incidents etc.

## Key advantages of AddNet

**› Saves significant amount of network administrator's time**

Over 90% time saved.

**› Centralizes network administration and standardizes operational procedures**

**› Network access control**

Unauthenticated devices unable to communicate in the network.

**› Fully automated BYOD administration**

**› Increasing operational reliability of DHCP, DNS and Radius**

N+1 Redundancy of core services.

High scalability, possibility of HiPerformance DHCP/DNS services.

# MoNet

*Developed for central monitoring in large organizations. Especially useful in hierarchical and holding organizations. It allows to compare all monitored services not only through all the layers but also through all the locations of large networks. Supports monitoring of heterogeneous technologies and can be run as a main monitoring system.*

## MoNet provides

### Monitoring on all layers

› Environment, hardware, virtualizations, operating systems, databases, application servers, applications.

› Many advanced monitoring plugins available for MoNet as well as API to create plugins for uncommon technologies. MoNet is also compatible with Nagios based plugins.

### Monitoring in large networks

› Client-server-server model provides the possibility to set administrators for specific regions while being able to supervise the whole network from one central location.

› Each network contains independent probes which continue monitoring even if the connection with parent server is lost.

› Independent probes also give a great opportunity to compare (graphically – correlate) different technologies and locations.

### Full audit of supervised infrastructure

› Probes are able to monitor and pool data even when the network is unavailable which lets you track incidents into very specific place.

### Admin notifications for unexpected events

› Flexible notifications (SMS, e-mail, web services…) for unexpected network or service events.

› Can be set up individually for each location.

### Automated restoration measures

› MoNet makes systems more resilient by allowing the creation of automated restoration operations – inserting administrator's know-how right into the system.

## Key advantages of MoNet

**Open monitoring**

Ability to monitor uncommon technologies as well as standard ones.

**Integrated application monitoring**

Enables to simulate the behavior of application users.

**High level of operational reliability**

Ability to keep monitoring when disconnected from remote network services.

High scalability of solution.

**Automated evaluation of SLA parameters**

Based on real-life data.

# FlowMon ADS

*FlowMon ADS is a modern system for detection of data network anomalies and undesirable behavior, which is based on permanent evaluation of network traffic statistics. The goal of the solution is to reveal operational problems and to increase external and internal security of a data network. The main advantage over standard IDS systems and SNMP monitoring lies in orientation on the overall behavior of devices in a network, which enables to respond to yet unknown or specific threats for which the signature is not available.*

## FlowMon ADS Provides:

Know the network at any time and any point

Monitor network traffic in real-time

Secure the network against internal and external threats

Track the historical data and drill-down to any host, application or conversation

Analyze the network flows for an efficient capacity planning and traffic engineering

Fulfill the data retention law (lawful intercept)

Troubleshoot the network failures fast and precisely

Recognize anomalies like worms or DDOS attacks

Introduce intelligent traffic and financial reporting

Plan and monitor QoS policy in detail

Check the peering and service level agreements (SLA)

Introduce IP based billing and accounting

Find out who are the top users and get their statistics

## Key advantages of FlowMon ADS

- **Network security increase**
- **Real time network traffic monitoring**
- **User's and service's activities monitoring**
- **Long-term storage of statistics about network traffic**
- **Fast and effective troubleshooting**
- **Detection of internal and external threats**
- **Internet usage oversight**

# References



## AddNet

*Focuses on large networks and on networks where premium security and operational reliability of core network services (DHCP,DNS,Radius) is required.*

### *Major customers:*

- *OZP – Health Insurance*
- *Tomas Bata University*
- *Charles University in Prague, Faculty of Science*
- *Ministry of Defence of the Czech republic*
- *Ministry of the Interior of the Czech republic*
- *Czech Post*

## MoNet

*Focuses on large networks and on networks where premium security and operational reliability of monitoring is required.*

### *Major customers:*

- *OZP – Health Insurance*
- *Tomas Bata University*
- *Charles University in Prague, Faculty of Science*
- *Ministry of Defence of the Czech Republic*
- *Ministry of the Interior of the Czech Republic*
- *Czech Post*
- *Ministry of Finance of the Czech Republic*
- *Czech National Radio*
- *Wuestenrot*
- *Toptrans*
- *OfficeDepot*

## FlowMon ADS

*Focuses on medium or large networks and on networks where premium security is required.*

### *Major customers:*

- *SWITCH (SUI)*
- *Surfnet (NL)*
- *Cesnet*
- *Tomas Bata University*
- *AVG*
- *Aegon*
- *Uniqa*
- *Marius Pedersen*
- *Seznam.cz*

novicom

Novicom s.r.o. Koněvova 67a
130 00 Praha 3, Czech Republic

+420 271777231-2

www.novicom.eu

sales@novicom.cz