FlowMon ADS

User Guide

29th February 2012
# Content

1. Introduction............................................................................................................................................ 3  
   1.1. Features and capabilities.................................................................................................................. 3  
   1.2. Limitations........................................................................................................................................ 4  
   1.3. Selected detection methods............................................................................................................. 4  
   1.4. Basics of application....................................................................................................................... 5  
2. Installation and configuration................................................................................................................ 8  
   2.1. Installing on probe/collector............................................................................................................ 8  
   2.2. Quick configuration......................................................................................................................... 8  
   2.3. Detailed configuration..................................................................................................................... 9  
3. Detection methods.................................................................................................................................. 17  
   3.1. Introduction to detection methods................................................................................................ 18  
   3.2. Common network behavior patterns............................................................................................... 19  
   3.3. Advanced network behavior patterns............................................................................................. 29  
   3.4. Derived behavior patterns.............................................................................................................. 35  
   3.5. Anomaly detection system............................................................................................................. 36  
   3.6. Network traffic system procedures................................................................................................. 40  
   3.7. General system procedures............................................................................................................ 41  
4. User interface......................................................................................................................................... 43  
   4.1. Basic controls.................................................................................................................................... 43  
   4.2. Dashboard....................................................................................................................................... 47  
   4.3. Events.............................................................................................................................................. 50  
   4.4. Profiles........................................................................................................................................... 57  
   4.5. Reports............................................................................................................................................ 63  
5. Contact information............................................................................................................................... 66  
   5.1. Vendor............................................................................................................................................. 66  
   5.2. Distributor....................................................................................................................................... 66
1. Introduction

FlowMon ADS is a modern system for detection of anomalies and patterns of undesirable network behavior, which is based on an analysis of data flows in the network (NetFlow). The main goal of the solution is to increase external and internal security of a computer network. The main advantage over standard IDS systems lies in orientation on the overall behavior of the device on a network, which enables to respond to yet unknown or specific threats for which the signature is not available. Integrated dashboard displays a quick overview of the latest events, overall statistics of events or used and provided services. This allows for immediate identification of problems or problematic devices in the network.

User documentation is divided into the following chapters:

- **Introduction** – the first chapter, which aims to familiarize users with the features and capabilities of the FlowMon ADS plug-in
- **Installation and configuration** – the second chapter designed for system administrators is dedicated to the installation and detailed configuration of the plug-in
- **Detection methods** – the third chapter exactly specifies the features of the application, part of the chapter describes best practices and interpretation of results
- **User interface** – the fourth chapter is intended for ordinary user working with the application
- **Contact information** – a summary of contacts for the vendor and distributor of the plug-in

1.1. Features and capabilities

- **Plug-in for FlowMon solution, easy to install on probe/collector**
- **Support for NetFlow v5/v9 and for IPv4 and IPv6**
- **Implementation of Bidirectional flows standard (RFC 5103)**
- **Building long-term behavioral profiles of devices on the network in terms of provided and used services, traffic volume and communication partners**
- **Predefined set of rules for detection of undesirable behavior patterns – operational issues, attacks, unwanted services**
- **Predefined set of rules for detecting network anomalies such as behavior change of devices on the network, discovering new network services, etc.**
- **A comprehensive dashboard with a direct indication of problems in the network**
- **Interactive visualization of events and relevant context in the form of directed graphs**
- **Complex filtering options and event prioritization linked to reporting and alerts**
● Integration of tools for obtaining additional information (DNS, WHOIS)
● Support for adding custom information about IP addresses (name, role, username...)
● Automated outputs via e-mail

1.2. Limitations

Application is designed for following environment:

● Data flow up to 5000 flows/s
● Behavior profiling for 5000 unique IP addresses
● General anomaly detection system based on change of behavior for 500 unique IP addresses
● In case of deploying the application in an environment which does not fulfill the requirements please contact the application vendor

1.3. Selected detection methods

The analysis of behavioral profiles and change detection:

● Behavior profile (data flows)
● Behavior profile (client/server)
● Behavior profile (communication partners)
● Behavior profile (traffic structure)
● Behavior profil (activity)

Detection of network anomalies:

● Anomaly detection system based on changes in the behavior profile
● Detection of heterogeneous communication
● Detection of transmission of large volumes of data in the network
● Detection of service unavailability
● Detection of parasite device

Detection of remote management:

● Detection of remote management services
● Detection of Telnet protocol
Detection of attacks:

- Detection of sharing desktop using TeamViewer
- Detection of dictionary attacks on SSH services
- Denial of Service type attacks
- Detection of TCP scans
- Detection of attacks on web servers
- Detection of outbound spam

Error checking at the configuration level:

- Detection of IP addresses without reverse DNS records
- Detection of a bad configuration of automatic updates
- Detection of delays on the network

Usage of unwanted services:

- Detection of Instant Messaging (ICQ, Jabber, MS Messenger, Google Talk...)
- Detection of BitTorrent and DC++ P2P networks
- Detection of different Voice-over-IP protocols
- Detection of different VPN connections and tunnels
- Detection of direct communication into the Internet
1.4. Basics of application

FlowMon ADS is available as a standard plug-in for the FlowMon probe/collector. It is a web application that uses modern scripting technology (Java Script and AJAX) and displays data through Adobe Flash. The application is optimized for Firefox 3 and later, among the other supported browsers are:

- Internet Explorer 8
- Opera 9
- Google Chrome 2
- Safari 4

User interface is divided into three main parts. In the upper part of the application is the status and information bar, on the left shows the application main menu, which you can hide if necessary. The remaining area of the user interface is the user's desktop, where you see the information and functionality combined under the currently selected item in the main application menu.
Another means of controlling application is a **context menu** available by right clicking on relevant object. Possibility of showing context menu is indicated by icon on status and information bar when cursor is placed on this object.

Tables in the application allow multi-level sorting (by pressing SHIFT key). IP addresses in the tables and text statements can be dragged and drop onto other application objects by pressing Ctrl and left mouse button simultaneously.

**Figure 1.4.2: User interface preview**
2. Installation and configuration

2.1. Installing on probe/collector

FlowMon ADS is a plug-in that can be run on the probe and the collector. Installation on probe/collector is carried out through Install/Update function found under Version tab in the FlowMon Configuration Center. More information on installing plug-ins can be found in the FlowMon probe/collector documentation.

Installation process will automatically apply Common company configuration template configuration template to the application. Common used detection methods and parameters will be activated by this process. There is also prepared one NetFlow data source for the first monitoring port on the probe. This NetFlow source must be activated manually. Information about NetFlow source configuration are describe in chapter 2.3.2 Configuration of NetFlow data sources.

2.2. Quick configuration

The basic configuration of the plug-in consists of five steps:

1. **Log into the plug-in** – use the username "adsadmin" and password "adsadmin" to login. You can change your password and define other users through FlowMon Configuration Center under System tab. More information on the management of user accounts can be found in the FlowMon probe/collector documentation.

2. **Configuring the NetFlow data sources** – in section Configuration\NetFlow sources set up particular sources of NetFlow data that will be processed by the application. From the aspect of data collection the applications works like a collector capable to receive data in NetFlow v5/v9 format. For each source:
   - Enter a unique name (Name)
   - Enter the IP address (IP address) and port (Port) from range 6001-6050, which will be active to receive data. If you run FlowMon ADS on the probe, then IP address is always "127.0.0.1", if you run the plug-in on the collector, enter the IP address of the collector
   - Set all data sources you want to use as active

3. **Configuring the exporters** – in FlowMon Configuration Center, part Exporters, add more export targets ("exporter targets") for all monitored ports of the device for which you configured NetFlow data sources in step 2. When connecting monitoring of the line through the TAP set export of data for both used monitored ports of the device into a single
NetFlow source (identical pair of IP address, port) prepared in the plug-in. To reduce the number of flows that are generated by the probe following values are appropriate:

- active timeout – 300 s
- inactive timeout – 30 s

4. **Configuring filters** – in section Configuration\Filters describe your network from the perspective of used IP addresses at the required level of detail. Use defined filters when configuring the detection methods or when searching for events in the user interface of the application.

5. **Configuring detection methods** – in section Configuration\Methods set and activate the desired detection methods. When setting up perform:

- reduction of input data set for individual detection methods by assigning filters (Assign filters)
- configuration of specific parameters of the detection methods (Configure)
- activation of required methods (Activate)

Steps 4 and 5 can be automated using configuration template. In section Configuration\General configuration apply selected configuration template for the plug-in (Apply configuration template).

### 2.3. Detailed configuration

#### 2.3.1. General configuration of the plug-in

Functions for managing the overall configuration of the plug-in are available in section Configuration\General configuration. All user data can be deleted anytime (Clean-up all data) or you can bring a device into the factory setting (Reset to factory defaults), which also includes deleting all user data. User data includes all events and collected behavior profiles. Deletion of data or resetting the device to factory defaults requires restarting the device or restarting the plug-in through FlowMon Configuration Center under the Version tab. If reset is not performed before midnight, clean-up data settings and reset to factory defaults settings are deleted. More information on managing the plug-in can be found in the FlowMon probe/collector documentation.

To simplify the configuration of devices there are pre-defined templates for plug-in settings available (Apply configuration template). Templates include configuration of NetFlow data filters, individual detection techniques and perspectives setting. Application of template can be enforced
(Force), which means that the current setting which is in conflict with the selected template is overwritten. There are currently following templates:

- **Common company configuration template** – template designed for small and medium-sized organizations. Filter settings include commonly used private addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Activated detection methods and their settings correspond to the typical security needs of small and medium sized organizations. Automatic anomaly detection system is not activated network-wide; it must be activated afterwards on selected portion of the network. Within the perspective settings the highest priority is given to events that might indicate an attack or a serious breach of network security.

- **Large company configuration template** – template designed for large enterprises. Filter settings include commonly used private addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Activated detection methods and their settings correspond to the typical security needs of large sized organizations. Automatic anomaly detection system is not activated network-wide; it must be activated afterwards on selected portion of the network. Within the perspective settings the highest priority is given to events that might indicate an attack or a serious breach of network security.

- **Internet service provider trunk template** – template designed for large backbone networks. Filters are not part of the template. Activated detection methods and their settings correspond to the typical security needs of ISP networks focused on massive attacks and anomalies in the network.

It is possible to save current application configuration and restore if needed. Application configuration is not portable between application version.

Access to external services (Internet services) might be allowed or denied using **External services** option. If internet access is denied geolocation service, whois service or detection methods depending on external sources are unavailable.

Size of ADS database can be limited by setting upper boundary in GiB (**Change max size of database**). Parameter **Delete type** determines data processing. "Fast" mode speeds up application by deleting old unprocessed data in the queue (useful for large high-speed networks like ISP), "safe" mode deletes data after processing only. Parameter **Delete data after** is used to stop deleting old data. It’s usefull for archiving events and profiles for an later analysis. The value “Never” sets data lifetime to infinity while “After default period” sets the default values (event – 28 days, profiles – 183 days).

The application uses all available CPUs. Parameter **Maximal count of computational threads** allows limit the number of CPU cores, which application can utilize.

The application allows to resolve event source IP address immediately after event detection. IP addresses which should be resolved are defined by **Filter that defines which IPs to resolve online**.

The application allows to clean up the part of the least relevant entries per day (e.g. the entries
with the least number of transferred packets). Amount of these entries is defined by parameter **Percentile used for cleaning profiles**. The cleaning is related to these profiles: "Traffic", "Client/Server", "Country Reputation", "Flows" and "Incoming and Outgoing traffic".

The application stores resolved DNS names for a short time period. It can be deleted using the **Clean internal DNS cache** button.

It is possible to gain the additional information about IP addresses from **ePolicy Orchestrator** (product of McAfee company).

You can use the **Show configuration changes** button to show list of plugin changes that were made. Changes are shown in tree form and sorted by username and date when change was made. You can use search criteria filter for searching in changes.

![Show Configuration changes](image)

**Figure 2.3.1: Show Configuration changes**

### 2.3.2. Configuration of NetFlow Data sources

NetFlow data sources represent individual monitored points of the network and are one of the licensing restrictions (number of simultaneously active NetFlow data sources). The second licensing restriction is the number of concurrent users working with plug-in user interface. Configuration of NetFlow data sources is done in section **Configuration\NetFlow sources**. For each monitored point of the network a NetFlow data source must be created in the plug-in. Configuration of data source includes:

- unique data source name
- IP address – when installing on FlowMon probe it’s always 127.0.0.1, when installing on FlowMon collector it is always the IP address of the collector
- port – for plug-in there are reserved ports 6001-6050
● status (active/inactive)

When installing on the collector it is necessary to enable used ports on the firewall. In FlowMon Configuration Center, part Remote Services\User Firewall Rules, enable all previously activated ports of NetFlow data sources. Set “udp” as L4 protocol. More information on managing the plug-ins can be found in the FlowMon collector documentation.

Among the optional settings are the collector IP address (Collector) and name of the profile (Profile), which stores the analyzed data in long term. As a collector we always set the address 127.0.0.1 or “localhost”. The profile must be between the so-called live profiles. More comma-separated profiles can be specified. Entering multiple profiles can be useful when monitoring through TAP, which divides both traffic directions into two separate profiles. More information on profiles can be found in the FlowMon probe/collector documentation. Collector and profile configuration is required for interactive visualization of events in the form of directed graph, where the data relevant for the event is obtained from the collector.

After configuring NetFlow data sources you should configure the NetFlow data exporters. In FlowMon Configuration Center, part Exporters, add other export targets (“exporter targets”) for all monitored ports of the device for which you configured NetFlow data sources in step 2. When connecting monitoring of the data line through the TAP set data export for both used monitored ports of the device into a single NetFlow source (identical pair of IP address, port) prepared in the plug-in. Details on configuring the exporters can be found in FlowMon probe documentation. The granularity of flows impacts the accuracy of detection methods. To reduce the number of flows that are generated by the probe following values are appropriate:

● active timeout – 300 s
● inactive timeout – 30 s

Immediately after installation there is the Generic source. This source is built-in without any possibility of manipulation by the user and is used to generate events that can not be directly bound to any user-defined NetFlow data source.

It is possible to save current application configuration and restore if needed. Application configuration is not portable between application versions.

Access to external services (Internet services) might be allowed or denied using External services option. If internet access is denied geolocation service, whois service or detection methods depending on external sources are unavailable.

2.3.3. Configuring filters

Correct settings of NetFlow data sources and the logical network topology affects the results of the detection methods and the overall plug-in predicative capability. The basic distinguishable entity
in the plug-in is the IP address. When the occurrence of an event is detected, the event is bound to an IP address that caused it and to NetFlow data source on which the event has been detected. In contrast, the behavior profile of device on the network is bound only to the IP address and does not distinguish between NetFlow data sources. That implies a number of limitations when IP addresses are dynamically allocated and stable allocation of identical IP addresses to each network device is not guaranteed. In such case it is not possible to derive a direct responsibility of particular user for the event detected in the network nor is it possible to use behavioral profiles.

Configuration of filters is done in section **Configuration\Filters**. Filters are named logical groupings of arbitrary IP addresses. Each filter has a unique name, can be linked to the defined NetFlow data sources and includes any number of IP address ranges. Filters are also used by detection methods for limiting the range of the addresses relevant for each detection method. Binding to NetFlow data source can further reduce the processing of NetFlow data in the detection method (see example later in this section). IP addresses for filters can be specified in the following ways:

- Network address/mask for the IP version 4 and 6 (e.g. 192. 168. 1. 0 /24)
- Range of IP addresses for IP Version 4 and 6 (e.g. 10. 0. 1. 2-10. 0. 1. 10)
- Single IP address for IP version 4 and 6 (e.g. 192. 168. 2. 1) or comma separated list of single IP addresses

New filter can be created also as substract of two another filters. This can be perform by the **Subtract filters** button. Similarly, **Invert the filter** button creates a new inverted filter from already existing one.

It is posible to use **Import filters** button for import filter definitions from the text file. Format of the file is one filter definition per line where IP adress definition is in the first column, Name of the filter is in the second column. Columns are separated by semicolon. IP adress can be specified in the same ways as manual filter defining. If the name of the filter already exists in the aplication, you will be noticed and import fails.

**Example filter definition file:**

```
192.168.1.0/24;LAN
192.168.10.0-192.168.10.25;LAN
192.168.1.1;SMTP
```

If the checkbox "Overwrite existing filters" is checked then the IP ranges of the filters with same name as in the uploaded file are overwritten by new ones that are given in the file.

**Example filter configuration** – consider environment of organization monitoring its network at two points. The first point connected to probe port 1 and 2 is the Internet connection behind a
firewall, which is monitored via TAP. The second monitored point is a central switch of the organization connected to the probe port 3 via SPAN port. In the FlowMon ADS plug-in we define WAN data source representing the Internet connection and LAN data source representing the central switch. We are going to export data from probe port 1 and 2 into the WAN source and data from probe port 3 into the LAN source. Next, we create a filter LANout comprising addresses 192.168.1.0/24 and bind it to the WAN source and filter LANin comprising also the addresses 192.168.1.0/24 which we bind to the LAN source. We activate detection of instant messaging services on the LANout filter, since this detection does not make sense for internal communication, while we activate the building of behavior profiles on the LANin filter where all traffic of each device can be captured. If we didn't bind filters with NetFlow data sources, there would be duplication in the detection of Instant Messaging (identical data would be processed twice independently), and behavioral profiles would be biased (in/out Internet traffic would be counted twice in the profile).

Is possible to add custom IPs information from CSV text file by using Import information about IP addresses operation. Information can be downloaded back by "Export" button. Remember, the import deletes all previous information! Following fields are supported:

- **IP** - IP address to which the information relates
- **Host** - domain name of IP address (max. 32 characters)
- **Username** - responsible user (max. 32 characters)
- **OS** - running operating system (max. 50 characters)
- **HWconfig** - hardware description (max. 1000 characters)
- **Role** - role of devices on the network (max. 32 characters)
- **Notes** - additional notes (max. 1000 characters)

The text file consists of a header and records. The header contains list of fields separated by a semicolon. It must include required field "IP" and at least one optional (Host, Username, OS, HWconfig, Role, Notes). Each record is on single line. The fields are separated by a semicolon. Empty lines are ignored. More records can be added to one IP address.

Example custom IPs information file:

```
IP;Host;Role;Username;OS;HWconfig
192.168.1.1;stone.foo.com;LAN gateway;;CentOS 5.5;
192.168.1.33;pc33.foo.com;client-station;Johny;WindowsXP;Virtual Machine
```

### 2.3.4. Configuration of detection methods

Detection methods are predefined by the manufacturer and used to detect various potentially
undesirable activities on the network or to cumulate appropriate information (behavior profiles). Thus they build the core of FlowMon ADS plug-in. The various methods are described in detail in third chapter. Configuration of detection methods is performed in the Configuration\Methods. Part of the configuration is:

- activation/deactivation of a method
- assignment of filters to methods (any number of filters can be assigned)
- specific configuration (methods may have specific configuration parameters that can be set or actions that can be performed)

Depending on the method nature some of the above options can be inactive. For example system methods (e.g. event reporting) can not be turn off nor assigned with filters. All configuration changes will take effect immediately upon next batch processing of NetFlow data by given method.

2.3.5. Configuration of perspectives

In section Configuration\Perspectives you can create your own event perspectives that will assign events with priorities according to their type of, the network segment where they occurred (based on the filter) and to the NetFlow source, that provides NetFlow data used for event detection. If the Generic NetFlow source is chosen, priority is assigned to events from all NetFlow sources. These perspectives can then be used when reporting events, alerting or searching in the application UI. Each perspective is uniquely named group of assignments of priorities to events of given type (i.e. to events generated by given detection method), and thus either network-wide or depending on the filter. Application offers five event priorities:

- VERY HIGH
- HIGH
- MEDIUM
- LOW
- VERY LOW

2.3.6. Configuration of categories of events

In section Configuration\Event categories you can define your own event categories into which you can then assign events through Manage event categories context menu item. This way you can mark interesting events that should be further explored; marks can be used in subsequent searches.
2.3.7. Configuration of the network topology

In section Configuration\Topology it is possible to define the network topology which can subsequently be used when viewing the events. This view in combination with perspectives reveals the most problematic network parts. Network topology has a tree structure; it is possible to define several distinct network topology trees through Add new topology. To simplify the creation of network topology you can copy the topology from defined filters by checking Copy filters option. Each filter creates one segment comprising the IP addresses corresponding to the filter. Segments are named as the filter. When defining the network segments manually it is possible to create arbitrarily deep topology tree. Particular IP addresses within the given segment can be defined solely on the lowest (leaf) level in the topology tree and are defined in the same way as filters. Segments may overlap; the relevant events will be included in both segments.

2.3.8. Configuration of event reporting

In section Configuration\Event reporting you can define regular reports which will be sent via e-mail by the application.

Each e-mail report must be uniquely named and bound to just one perspective. A report has active/inactive state. The inactive report is defined in the system but not sent regularly. The report can be assigned with any number of recipient addresses by Add New Mail. There is also an option to suppress sending of an empty report (Prevent empty report) and option to set minimum priority of events to be reported (Minimal priorities this report). Reports are sent by the following rules:

- VERY HIGH – reporting immediately after the batch processing of NetFlow data, approximately every 5 minutes, a blank report is never sent.
- HIGH – reporting hourly summaries
- MEDIUM – reporting six hour summaries
- LOW – reporting daily summaries
- VERY LOW – no reporting
- hour, six hour and daily summaries also include all events of higher priority which occurred in a given period of time, e. g. also all VERY HIGH events for the past hour are reported in the hour summary

It is possible to send reports using your own SMS gateway. Please contact the vendor, company AdvaICT, a.s., if you want to use this possibility.

Application supports event export in chosen format (e.g. Common Event Format) to one remote syslog which can be configured in Event reporting section. All events are exported according to selected perspective, it can be chosen the severity of syslog message according to this perspective,
too (VERY HIGH priority fits to alert severity). This feature is not available in the model FlowMon ADS 101.

Application supports exporting events using SNMP, too. Events are generated as a SNMP traps, that are generated based on MIB file ADVAICT-ADS-MIB.txt (this file can be downloaded from the authentized section of www.advaict.cz pages). It is needed to configure the IP address and the port number of the device, that is dedicated to receive the traps. Then it is needed to choose the perspective. This feature is not available in the model FlowMon ADS 101.

2.3.9. Configuration of false positives

Detected events can be marked as false positives through Mark as false positive context menu item. This mark means that the event of given type caused by given IP address will no longer be reported. Validity of marking an event as false positive can be limited to individual days of the week and time intervals. Removal of rules for false positives marking is done in the Configuration\False positives section. Rules for ignoring false positives are organized in a tree structure. In the first level they are categorized according to the event type, the second level consists of individual event originators (IP addresses) and the third level represents periods of rule validity. Removal of selected rules can be done through Delete Selected.

2.3.10. Configuration of ADS exceptions

During detection mode, you can select specific IP addresses, for which will be taught new values for the baseline. Old values for inserted IPs will be deleted immediately after clicking the "Save", so it is important to consider the decision carefully. Only one IP address can be entered into the field for the IP address. The "Add IP address" button allows you specific more IP addresses. For each IP address is needed to specify how many days should be in a learning mode. Here you can also find previously saved IP addresses and number of days remaining until the end of the learning. The "delete" button allows you to set an IP address back into the detection mode.

2.3.11. Configuration of User preferences

User can set own parameters of user interface. It is possible to enable logout confirmation dialog box, select default language for user interface, set the session timeout, enable displaying of the application tips, enable automatic domain names resolving, showing the welcome screen window and disabling the automatic load of the dashboard tables.
3. Detection methods

Detection methods are the core of FlowMon ADS. They serve for detecting various potentially undesirable activities on the network or to cumulate appropriate information (behavior profiles). Detection methods are predefined by the manufacturer who guarantees their development and expansion according to the current trends in the area of network services and security of computer networks in particular. Detection methods can be imagined like signatures for IDS systems (e.g. SNORT). Unlike signatures which represent particular strings to be searched in individual packets, detection methods contain specific behavior patterns of network devices. FlowMon ADS uses the principle of detection methods also for other tasks (e.g. event reporting etc). Detection methods are divided into the following groups:

- **Common network behavior patterns** – common network behavior patterns that generate events always when processing the current batch of NetFlow data (typically every 5 minutes).

- **Advanced network behavior patterns** – advanced network behavior patterns that detect long term trends in network behavior based on continuous processing of NetFlow data.

- **Derived behavior patterns** – derived behavior patterns that generate characteristics of individual devices. They do not directly depend on processing of the NetFlow data. Typically they use the outputs of the above two detection method groups and are run periodically (every hour).

- **Anomaly detection system** – methods of general anomaly detection system based on changes in the behavior of network devices.

- **Network traffic system procedures** – system procedures for the processing of NetFlow data.

- **General system procedures** – system procedures ensuring correct application run and other related functions (e.g. event reporting).

A typical duty cycle of the FlowMon ADS application includes performing of following steps:

- **Receive and store NetFlow data** – receiving of NetFlow data batch representing the actual network traffic, typically every 5 minutes.

- **Processing of NetFlow data batch** – application of all active detection methods on given NetFlow data batch which results in events generation, behavior profiles update and event reporting. Applications leverages multi-threading to increase overall processing throughput.

Independently of processing the NetFlow data the application performs regularly every hour active detection methods from General system procedures and Derived behavior patterns groups.
3.1. Introduction to detection methods

All detection methods have many common features and they are configured via uniform user interface. The remaining text of this section is devoted to description of individual detection methods in terms of the principle of their operation, their configuration and interpretation of their results, which is typically based on practical experience with detection methods. Information on the detection method always includes a general description, tips for method configuration. For detection methods from the groups Common network behavior patterns, Advanced network behavior patterns, Derived behavior patterns or Anomaly detection system it also contains instructions for interpretation of results.

3.1.1. Common configuration options

- The option for method activation/deactivation – each method, except for the system ones, can be activated or deactivated (Activate/Deactivate). This option is reflected immediately, precisely when processing the next batch of NetFlow data.
- Assigning filters to the method – most methods may be restricted in terms of processed traffic by assigning filters to them (Assign filters). This setting is reflected immediately, precisely when processing the next batch of NetFlow data.
- Method configuration – specific configuration of detection methods is available through function Configure. This includes not only settings of the specific options of the detection method, but also running specific actions associated with the methods.

3.1.2. Common features

- Events generating – most detection methods generate events. Events always include event originator (IP address), event type (corresponding to a type of the method which detected the event), the time stamp of event occurrence according to NetFlow data, link to the NetFlow data source, event details (additional information on the event according to its type) and the list of all event targets (IP addresses).
- Periodic deletion of events – all detection methods which generate events offer their periodic deletion through a configuration option "DeleteEventsAfter" indicating the number of days for which the events remain in application memory. Older events are automatically deleted. When the option is set to value "0" events are never deleted.
- Periodic deletion of behavior profiles – all detection methods that generate behavior profiles offer their periodic deletion through a configuration option "DeleteProfileAfter" indicating the number of days for which profiles remain in application memory. Older profiles are automatically deleted. When the option is set to value "0" profiles are never deleted.
3.2. Common network behavior patterns

3.2.1. ALIENDEV – Alien device method

Method description – a method for detecting parasite device in monitored network. Within the method configuration is necessary to set the filter, that is exactly corresponding to the IP addresses that are assigned to specific network devices ("KnownSegment" parameter) and the filter ("LANFilter" parameter) that is corresponding to the whole used network segment (including addresses that can be assigned by the DHCP server).

Method configuration – it is appropriate to activate this method network-wide for all traffic on the network. Appropriate place for monitoring the traffic is the central switch.

Interpretation of results – this method is able to detect unknown (or forgotten) devices that are connect to the monitored network.

3.2.2. ANONYMIZER – Anonymizer usage

Method description – a method for detecting communication with IP addresses which serve as anonymizer services on the Internet. If the method is active the list of IP addresses is periodically updated (every hour). Within the method configuration you can set monitoring of selected types of blacklists (WebProxies). Option “StrictMode” set to “strict” allows you to monitor only communications initiated from monitored network towards anonymizer IP addresses.

Method configuration – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet connection line. To update the list of IP addresses correctly it is necessary not to block the communication of the device (probe/collector) to port 80 (standard web traffic).

Interpretation of results – this method achieves very reliable results due to the use of renowned lists of anonymizer services. If the event originator is some of the IP addresses of the organization, it is likely that this IP address user uses a service to anonymize his activities on the Internet.

3.2.3. BITTORRENT – BitTorrent

Method description – a method for detecting P2P networks of the BitTorrent type. This method consists of four different detection methods that analyze network traffic concurrently. The incidents detected by individual methods are compared. The event is generated in case of detecting Bittorrent traffic by multiple methods. The option „MinimalProbability“ allows you to set the minimum number of methods, that have to detect the incident, in the form of percentages.
In this way, it is possible to detect almost any Bittorrent clients. Parameter „LANFilter“ enables the reduction of false positive by excluding internal network communication from detection. Next parameters are „MinSeeds“ and „MinHighPorts“ allowing to set minimal count of remote peer sources, where data are downloaded from, and minimal count of connections on ports higher than 10240.

Method configuration – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses excluded from communications on the LAN by the option "LANFilter". Appropriate place for monitoring the traffic is the Internet connection line.

Interpretation of results – this method achieves very reliable results in detection of notorious P2P downloaders. On the other hand, incidental and occasional use of P2P networks may not be detected, especially when strict mode is set on. Furthermore, this method may alert to spyware infected devices, whose symptoms are often similar to the symptoms of P2P networks.

### 3.2.4. BLACKLIST – Blacklist

Method description – a method for detecting communication with IP addresses which are included in the renowned blacklists. Typically they are the control centers of botnets or world-renowned attackers. The list of IP addresses is periodically updated (every hour), if the method is active. Within the method configuration you can set up monitoring of selected types of blacklists (BotnetActivities, SpammerActivities, AttackerActivities and VirusActivities). Option "StrictMode" set to "strict" allows you to monitor only communications initiated from monitored network towards blacklisted IP addresses. The method also supports communication control based on its own blacklist, whose address is set by parameters "CustomListServer" and "CustomListLocation". Parameter „IgnoreUnreachable“ allows ignoring ICMP type 3 (destination unreachable) replies to request from blacklisted IPs.

Method configuration – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet connection line. To update the list of IP addresses correctly it is necessary not to block the communication of the device (probe/collector) to port 80 (standard web traffic).

Interpretation of results – this method achieves very reliable results due to the use of renowned lists of anonymizer services. If some of the blacklisted IP addresses are marked as the event originator it's probably a network attack on the organization. If some of the organization IP addresses is the event originator it's likely to be part of botnet or infected with some form of malware.
3.2.5. DCPLUSPLUS – DC++

Method description – a method for detecting P2P networks of the DC++ type. Method uses two stages, first identifying the addresses suspect of connection establishment and exchange of information in DC++ networks, thereby obtaining a list of suspect addresses. If any of the suspect addresses also downloads large volumes of data, corresponding event is generated. The detection method offers the option "IgnorePorts" enabling the reduction of false positives along with potential increase in false negatives. If this option is active (value "ignoring"), data downloads must take place on different ports than those used by well-known services. Another means of protection against false positives is the option "LANFilter" which enables to rule out communication between the local addresses of detection.

Method configuration – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses excluded from communications on the LAN by the option "LANFilter". Appropriate place for monitoring the traffic is the Internet connection line.

Interpretation of results – this method achieves very reliable results in detection of notorious P2P downloaders. On the other hand, incidental and occasional use of P2P networks may not be detected, especially when strict mode is set on. Very often this method may alert to spyware infected device which exhibits similar symptoms as P2P networks like DC++.

3.2.6. DIRINET – Direct Internet Communication

Method description – this method detects devices that are communicating direct into the Internet (out of the segment defined by parameter "LANSegment"). It is possible to ignore unsuccessful and successful communication out of the allowed network segment using parameters "IgnoreTries" (eventually "IgnoreCommunication").

Method configuration – it is appropriate to activate this method for addresses from own network, that shouldn't be able to communicate direct into the Internet (e.g. due to security guidelines). Appropriate place for monitoring the Internet connection line.

Interpretation of results – this method is capable to detect devices that communicate direct into the Internet even if they are expected not to do this (they should use proxy server or they should communicate only with other devices inside the local segment).

3.2.7. DIVCOM – Diverse Communication

Method description – a method for detection of detect devices which exhibit great diversity of communication. The method determines for each IP address its communication factor as a product
of the unique destination address and unique destination ports. If the defined tolerance limit (value of "CommunicationFactor" option) is reached corresponding event is generated. Parameter "ExcludeServers" specifies name of filter that defines servers IP addresses, which should be excluded from detection. The servers have a greater diversity of communication than client stations.

**Method configuration** – it is appropriate to activate this method for addresses from own network or for all addresses when monitoring public available server farms. Appropriate place for monitoring the traffic is the central switch and the Internet connection line.

**Interpretation of results** – this method is capable of detecting devices that scan ports, spyware infected devices or misconfigured devices. Typical false positives include detection of devices implementing SNMP Monitoring such as Zabbix.

### 3.2.8. DNSANOMALY – Anomalies in DNS traffic

**Method description** – a method for detection of suspicious communication in DNS traffic. The method is capable to notify about UDP traffic greater than 576 B (this follows from DNS service standard) or large data transfers on TCP port 53. UPD packet size control defined in RFC 1035 can be disabled, if you set "IgnoreRFC1035" parameter to 1 (default value is 0). Sensitivity in the detection of large data transfers can be adjusted via the option "TCPTransferLimit". This method is extended by a detection of using DNS servers that are not allowed in the monitored network. This extension is activated by the choice of the filter "DNSServers" that defines IP addresses of allowed DNS servers. There could be computed simple numeric model of DNS servers usage, too. The parameter "LearnCycles" defines how long should be the model trained. The parameter "MinimalRatio" defines the minimal ratio (in percents) of count of connections that should the DNS server satisfy to be considered as usually used DNS server.

**Method configuration** – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet connection line.

**Interpretation of results** – this method is capable of detecting DNS service abuse for other undesirable activities, which typically include tunneled traffic. The sudden change of usage of DNS servers could indicate the malware infection.

### 3.2.9. DNSDOS - DNS Denial of Service

**Method description** – a method for detecting the increased difference between volume of replies from DNS server and volume of requests. The event is reported when this difference exceeds the
value of MinimalReplies parameter and the ratio of current to previous growth rate is greater than
ThresholdChange parameter (example of the ratio: if the last numbers of replies are constant and a
new difference is twice as large as previous, the ratio is greater than 30).

**Method configuration** – it is appropriate to activate this method network-wide for all traffic on the
network regardless of IP addresses. Appropriate place for monitoring the traffic is the central
switch.

**Interpretation of results** – this method alerts to the increased number of unrequested replies from
DNS server, which can mean DoS attack by using the DNS server. In this case, DNS server acts as
attacking tool and the real attacker is undetectable.

### 3.2.10. DOS – DoS/DDoS

**Method description** – a method for detection of Denial-of-Service or Distributed-Denial-of-Service
attacks. These attacks are characterized by massive TCP communication (connection attempts)
towards one destination IP address and one service (port). The aim of DoS/DDoS attack is to flood
the destination IP address and thus prevent the legitimate users from using provided service. The
method offers the option "AttemptsThreshold" whose value specifies the minimum number of
connection attempts to be considered a DoS/DDoS attack, then it is possible to restrict minimal
count of attackers ("AttackersThreshold") and configure a filter to ignore the LAN-to-LAN events.
Note that if an event is generated the victim of the attack is marked as the event originator and
attackers are listed as the event targets.

**Method configuration** – it is appropriate to activate this method network-wide for all traffic on the
network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet
connection line or the central switch (for large organizations with vast network).

**Interpretation of results** – this method reliably alerts to the DoS/DDoS attacks of the specified
minimum range.

### 3.2.11. HIGHTRANSF – High data transfers

**Method description** – a method for detection of massive usage of the data link by one user (IP
address). Method aggregates all traffic for each IP address and checks exceeding the maximum
limit. The option "TransferThreshold" specifies the absolute data volume threshold for single IP
address. When this limit is reached or exceeded an event is reported. This event has set only the IP
addresses with which was transferred at least the given percentage (parameter “TargetPercentile")
of maximal transfer between two IP addresses. Parameter “ExcludeServers” specifies name of filter
that defines servers IP addresses, which should be excluded from detection The servers have a
higher data transfers than client stations. Parameter “LegalServers” specifies the name of filter that defines IP addresses with which are the high transfers allowed.

Method configuration – it is appropriate to activate this method only for IP addresses from own network. Appropriate place for monitoring the traffic is the Internet connection line. The method can be trivially set up to detect certain amount of data transferred within 5 minutes by setting appropriate "LinkCapacity" and "TransferThreshold".

Interpretation of results – this method reliably alerts to the IP addresses which transferred more data than it is allowed.

3.2.12. HONEYPOT – Honeypot method

Method description – this method is inspired by so called honeypots. Honeypots are the network traps – computers on that is not expected the incoming traffic. All such traffic can be considered as anomaly. This method works similar. The IP addresses representing honeypots are defined as a filter and if there is got any access to these IP addresses, the event is generated.

Method configuration – it is appropriate to activate this method network-wide for all traffic on the network except the IP addresses from which we except the access to the honeypots (e.g. because of configuration). It is necessary to set up the name of the filter defining honeypots the method to work properly. Appropriate place for monitoring the traffic is the Internet connection line or the central switch.

Interpretation of results – this method alerts to the unauthorised access on chosen computers in the network. It could mean horizontal scan or attempt to network-wide ssh attack.

3.2.13. HTTPFLOOD – HTTP Servers Flooding

Method description – a method for detection of special case of Denial-of-Service attacks against web servers. The attack is based on generating absurd demands to which the web server responds by an error message (typically HTTP 404 – Web page not found). The aim of the attack is to overload the web server. The method offers the option "FloodThreshold" whose value specifies the minimum number of requirements from one source that should be considered an attack.

Method configuration – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet connection line or the central switch (for large organizations with vast network).

Interpretation of results – the method reliably alerts to the http flooding attack of the specified
minimum range. The method may also notify about misconfigured devices, e.g. devices periodically trying to update from the wrong source or spyware infected devices.

### 3.2.14. ICGUARD – Internet Connection Guard

**Method description** – detection method monitors usage of internet connection line and is able to alert excessive usage per host (user) or in total based on defined threshold values. Within the configuration it is necessary to set connection type (symmetrical line, asymmetrical line) and define the line speed in Mbps. Another configuration option is “LANFilter” which defines local IP addresses, communication between these addresses is computation of line usage ignored. Setting up the local addresses is mandatory. This method can detect high count of packets per second transferred over connection to internet. Event is detected if the overall sum of packets per second exceeds the value of “TotalPPS” parameter.

**Method configuration** – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet connection line or the central switch.

**Interpretation of results** – this method show clearly excessive usage of internet connection.

### 3.2.15. INSTMSG – Instant Messaging

**Method description** – a method for detection the use of instant messaging services even if they mask through the ports reserved for other services (e.g. port 80 for web traffic). Based on the statistical characteristics of the instant messaging traffic the method distinguishes between OSCAR protocol (ICQ and its derivatives), XMPP (Jabber service and its derivatives, including Google Talk), Microsoft Messenger and Skype. Any client of any of the above listed services is sufficient for successful detection. Detection of particular instant messaging type can be suppressed by setting the "Ignore" option. For suppression of false positives which may arise from the local network, there is the option "LANFilter" available, which allows you to specify the name of the filter comprising a local network addresses between which the traffic exhibiting instant messaging characteristics is ignored. Parameter „IgnorePorts“ allows to ignore communication on ports 993 and 443 for reducing false positives during XMPP instant messaging detection.

**Method configuration** – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet connection line or the central switch (with option "LANFilter“ set).

**Interpretation of results** – although this is a heuristic method it achieves very reliable results with real traffic. In some cases the confusion of roles event originator/event target occurs, i.e. IP address
from a local network running instant messaging client is marked as the event target and server of the service as the event originator.

3.2.16. **ONLINEMSG – Online Messaging**

**Method description** – a method for detection the use of online instant messaging clients, based on communication with service controlling server (e.g. icq2go, meebo, …).

**Method configuration** - it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet connection line or the central switch (with option "LANFilter" set).

**Interpretation of result** – this method reliably alerts to the IP addresses on the network that used online instant messaging service clients.

3.2.17. **MSPPTP – Microsoft PPTP VPN**

**Method description** – detection method reveals data transfers using VPN connections via Microsoft Point-to-Point Tunneling Protocol. Within the configuration it is necessary to set the minimal length of VPN connection using parameter "ConnectionLength" and the minimal amount of transferred data using parameter "Transferred" in kilobytes. The event source is always the IP addresses which sends monitored amount of traffic.

**Method configuration** – it is appropriate to activate this method according to VPN usage policy. Appropriate place for monitoring the traffic is the Internet connection line.

**Interpretation of result** – this method reliably alerts to the IP addresses on the network that generate Microsoft PPTP VPN traffic.

3.2.18. **MULTICAST – Multicast traffic**

**Method description** – a method for detection of IPv4 multicast traffic based on use of multicast addresses (224.0.0.0 to 239.255.255.255), directed broadcast addresses (X.Y.Z.255) and all-host broadcast address (255.255.255.255). Detection of directed broadcast and all-host broadcast traffic can be suppressed by setting the option "IgnoreBroadcast" to value "Yes". Minimum number of multicast requests to be reported can be set via option "MinimalAttempts". Parameter „UpdateAddresses“ allows to activate periodically update information (from Internet) about known multicast addresses. Otherwise, the offline version is used.

**Method configuration** – in the case of network problems or suspicion to problems associated with
multicast traffic, it is appropriate to activate this method network-wide for all communication in the network regardless of IP addresses. Appropriate place for monitoring the traffic is the Internet connection line or the central switch.

**Interpretation of results** – this method reliably alerts to the IP addresses on the network that generate multicast traffic.

### 3.2.19. LATENCY – Network Latency

**Method description** – a method for measurement of delay at the network level, i.e. delay between the recording the first request packet and the first response packet. The method uses Bidirectional flows standard (RFC 5103), i.e. classification of data flows such as requests and responses. The delay has to be measured for a given group of IP addresses specified by a filter. Within the configuration it is necessary to set the option "LatencyThreshold" whose value determines the maximum tolerated value of the delay between the request and response. Another option is "StrictMode" which determines whether the delay will be measured for addresses matching the filter assigned to the detection method or exclusively between these addresses (value "strict" of the option). It is possible to change the behavior of this method using option "TCPFlags" which enables to detect latency only during connection establishment.

**Method configuration** – it is appropriate to activate this method according to network topology and the objectives of the measurement. In any case, it makes no sense to measure the delay on any targets in the Internet. Optimal place for monitoring the traffic is for example data link between two workplaces of the organization or line to the organization servers.

**Interpretation of results** – this method shows a particular value of the delay between recording the first request packet and the first response packet. This value thus indicates the delay at the network layer and can help in analyzing the problem of latency in selected application or data link. The method can also be used to check the SLA on the selected data link.

### 3.2.20. OUTSPAM – Outgoing SPAM

**Method description** – a detection method based on the assumption that in the corporate environment emails should be sent only in a defined way. The method detects sending or attempts to send mails through other than explicitly defined mail servers. In addition, parameter "SpamCounter" can activate detection of increased number of sent emails from one station. The increased number is specified by parameter "Multiplicator", which defines times the average number of other stations. The average is computed only from stations which sent more than "MinimalMailLimit" messages in one hour. The method cares about the TCP/25 (SMTP) and TCP/465 (Secured-SMTP). Based on the number of flows and responses from the mail servers the method estimates the number of emails and whether the emails were actually sent. This
information is then available in the detail of the generated event. Event targets represent all mail servers through which attempts to send mail were made. The option "ServersFilter" identifies legitimate SMTP servers through which you can send mail. The option „StrictMode“ set to value „strict“ means that IP addresses assigned to the method by the filter have to be sources of the event. The option “ExcludeMailServers” set to value “exclude” means that IP addresses from “ServersFilter” list are excluded from detection. The option „IgnoreSecuredSMTP“ allows to ignore secured SMTP traffic (port TCP/465). The option "IgnoreScans" allows to ignore too small transmission, that can’t be an e-mail traffic.

**Method configuration** – it is appropriate to activate this method for IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch and the Internet connection line.

**Interpretation of results** – this method not only detects attempts to spam, but also may help to identify spyware infected devices. Further it may help detecting employees that use other than corporate mail servers, which may indicate bad configuration as well as intention.

### 3.2.21. REMOTEMAN – Remote Management

**Method description** – a method for detection of remote management traffic by known pairs of port/protocol. The practical applicability of the method is limited to a strict corporate environment and selected devices. The method is especially useful for detecting the Windows Remote Desktop, VNC, TeamViewer, Remote Administrator or LogMeIn. For suppression of false positives which may arise from the local network, there is the option "LANFilter" available, which allows you to specify the name of the filter comprising a local network addresses between which the traffic exhibiting remote management characteristics is ignored.

**Method configuration** – it is appropriate to activate this method for explicitly selected IP addresses of organization whose traffic structure is known or expected. Appropriate place for monitoring the traffic is the Internet connection line or the central switch.

**Interpretation of results** – this method can alert to the fact that the employees use remote management service to access their home devices or that some of the devices in the organization is remotely managed. The method may exhibit certain degree of false positives due to the detection system based on a pair of port/protocol.

### 3.2.22. SCANS – TCP Scans

**Method description** – a detection method used to detect common and used techniques of mapping the network and running services through port scanning. The method distinguishes different types
of scans (SYN scan, FIN scan, Xmas scan and Null scan) and styles (horizontal scan, vertical scan, chaotic scan). Parts of details are the number of scans, number of unique targets, information about response from scanned device and list of scanned ports. To adjust the sensitivity of the method serves the option "ScansThreshold" whose value indicates the minimum number of attempts to scan from a single source that should be recognized as an event. The option “IgnoreChaotic” allows to ignore chaotic scans and detect only horizontal and vertical scanning. The option “IgnoreUnsucc” allows to ignore scans with no response.

**Method configuration** – it is appropriate to activate this method for all IP addresses. Appropriate place for monitoring the traffic is the central switch and the Internet connection line.

**Interpretation of results** – apart from detecting attempts to deliberate port scanning this method may detect misconfigured devices which are unsuccessfully trying to establish a connection or devices infected with malware that is trying to replicate itself to other devices.

### 3.2.23. SRVNA – Service not available

**Method description** – a detection method used to detect unavailable services (IP address/port number tuple), to which clients want to access. These method can be restricted by minimal count of attempts to the service (“AttemptsThreshold”) and by filter that defines IP addresses of the provided services (parameter "ServiceProviders"). In case the event is generated, source IP address is the address of the unavailable service provider.

**Method configuration** – it is appropriate to activate this method for all IP addresses. Appropriate place for monitoring the traffic is the central switch and the Internet connection line.

**Interpretation of results** – apart from detecting successful Denial of Service attack this method may detect an erroneous configuration – either on server, which does not provide the service, that should be provided, or on the clients, which demands services, that are not provided.

### 3.2.24. TEAMVIEWER – TeamViewer

**Method description** – a method used to detect sharing desktop using TeamViewer

**Method configuration** – it is appropriate to activate this method only for IP addresses from the monitored network. Appropriate place for monitoring the traffic is the central switch.

**Interpretation of results** – this method detects devices that are sharing theirs desktop using TeamViewer.
3.2.25. TELNET – Telnet Traffic

Method description – a method used to detect increased use of Telnet service. Telnet service is obsolete and currently should not be used at all for safety reasons. Eventually its use should be subject to a special regime. The method detects all connections to TCP port 23 (Telnet service) including connection attempts and counts the number of connections for individual IP addresses. Within the method configuration you must set up the minimum number of Telnet connections to be considered unwanted through the option "TelnetThreshold. Detection may include all connection attempts including scans or only successfully established connections (option "IgnoreScans" and value "yes").

Method configuration – it is appropriate to activate this method for all IP addresses. Appropriate place for monitoring the traffic is the central switch and the Internet connection line. By setting the option "IgnoreScans" to value "yes" it is possible to detect devices that are infected with some form of malware (e. g. botnet Chuck Norris) invading other network devices such as routers, IP cameras, etc.

Interpretation of results – this method detects devices using or attempting to use the Telnet service (depending on configuration). The method can also detect specialized devices that are infected with some form of malware oriented to misuse specialized network devices.

3.2.26. TOR – The Onion Router

Method description – a method designed to detect using anonymity protocol Tor while browsing the Internet. The method configuration allows to set the minimal count of concurrently started connections (parameter "ConcurrentStart") and the minimal duration of the long-standing connection (parameter "LongConnection"). It is possible to limit the false positives by setting the filter that defines local network segment (parameter "LANFilter") and minimal probability of the event to be reported (parameter "MinimalProbability").

Method configuration – it is appropriate to activate this method for client station of monitoring network. Appropriate place for monitoring the traffic is the Internet connection line.

Interpretation of results – this method detects client stations that are using the Tor protocol while they are browsing the Internet.

3.2.27. UPLOAD – Upload detection

Method description – this method monitors amount of transferred data between individual communicating stations and checks the ratio of data transferred from computers of monitoring
network and data transferred in the opposite direction. When user-defined ratio or absolute
threshold is exceeded, the event is generated. Parameter „ExcludeServers“ specifies name of filter
that defines servers IP addresses, which should be excluded from detection. The servers have a
higher upload than client stations.

**Method configuration** – it is appropriate to activate this method for client station of monitoring
network. Appropriate place for monitoring the traffic is the Internet connection line.

**Interpretation of results** – this method reports the stations from which a file was uploaded, so it
may be an attempt to sensitive data leakage.

### 3.2.28. VOIP – VoIP detection

**Method description** – a method for detection of VoIP traffic by known pairs of port/protocol. The
practical applicability of the method is limited to a strict corporate environment and selected
devices and is appropriate for detecting SIP and H. 323 traffic. The method enables detecting
network devices that generate standard VoIP traffic.

**Method configuration** – it is appropriate to activate this method for explicitly selected IP addresses
of organization whose traffic structure is known or expected. Appropriate place for monitoring the
traffic is the Internet connection line.

**Interpretation of results** – this method focuses solely on pairs of port/protocol therefore it can
produce large number of false positives in case that it is misconfigured.

### 3.2.29. VPN – VPN connections and tunnels

**Method description** – a method for detection of VPN connections and tunnels by pairs of
port/protocol. Parameter „Advanced“ allows to activate advanced VPN tunnels detection based on
station communication with external network which is characterized by long connection to the one
IP address. Basic detection is appropriate for detecting Microsoft PPTP, IKE Key Exchange or
OpenVPN traffic on standard ports. Advanced detection allows to detect general VPN traffic to
external servers. Parameter “LanFilter” specifies local network. Other parameters “MinimalTime”
and “MinimalData” defines minimal length of connection with external VPN server and minimal
amount of transferred data in five-minute batch.

**Method configuration** – it is appropriate to activate this method for explicitly selected IP addresses
of organization whose traffic structure is known or expected. Appropriate place for monitoring the
traffic is the Internet connection line.
Interpretation of results – this method allows to determine devices on your network using VPN/tunnels. Basic detection is focused solely on pairs of port/protocol therefore it can produce large number of false positives in case that it is misconfigured. Advanced detection successfully detects general VPN traffic where all station communication with external network is going through.

3.2.30. IPV6TUNNEL – Ipv6 through Ipv4 tunnels

Method description – the IPV6TUNNEL detection method allows you to detect network devices, which are communicating through tunneled IPv6 protocol over Toredo or 6in4 protocol.

Method configuration – it is appropriate to activate this method for all IP addresses. Appropriate place for monitoring the traffic is the central switch and the Internet connection line. It is possible to set method for ignoring Toredo protocol (Value of „IgnoreToredo” is set to „yes”) or for ignoring 6in4 protocol (Value of „Ignore6in4” is set to „yes”).

Interpretation of results – the method detects devices communicating over tunneled IPv6

3.2.31. WEBSHARE – Web sharing

Method description – the WEBSHARE detection method allows to identify network devices, which downloads from webshare services (e.g. RapidShare).

Method configuration – it is appropriate to activate this method for all IP addresses. Appropriate place for monitoring the traffic is the central switch and the Internet connection line. Method can be configured to ignore unsuccessful connections (Value of „IgnoreSNGL” is set to „yes”).

Interpretation of results – accuracy of detection depends on the database of web-sharing services.

3.3. Advanced network behavior patterns

3.3.1. Profiling the behavior of devices on the network

Profiling methods, in contrast to the common methods for recognizing network behavior patterns, do not generate events. Instead they regularly update behavior profile of each network device. Behavior profile summarizes all activities of a network device in terms of L3/L4 network layer. Granularity of behavior profiles is 1 day which practically means that all traffic data of given network device are aggregated within a given day. Thus grows the application long term comprehensive statistics about the behavior of a device based on number of aspects:
● client/server – the percentage rate of the client/server behavior (PRFCLISRV)
● volume of incoming/outgoing/total traffic (PRFRNSF)
● structure of incoming and outgoing traffic, divided into requirements, responses and flows without answers (PRFFLOWS)
● communication partners (PRFPEERS)
● structure of provided and used services by ports/protocols (PRFTRAFFIC)
● overview of abroad communication (PRFCOUNTRY)
● device activity (PRFACTIVE)

The resulting profiles are available in the application either directly (Profiles\Hosts) or further processed. Data generated by PRFTRNSF method are displayed on the dashboard in the table Top 10 IPs by data volume, according to the volume of data transferred. Data generated by PRFFLOWS method are displayed in the table Top 10 IPs by connection count. Data generated by PRFTRAFFIC method are displayed in table Top 10 services. Data generated by PRFCountry method are displayed in table Top 10 countries by connection count and Top 10 countries by data volume. The information from behavior profiles is further used in group of methods for detection of derived behavior patterns, the relevant dependencies are listed for each detection method.

Using behavioral profiling is limited to networks or network segments with fixed IP addresses assigned. In the case of dynamic addresses it is not exactly a behavior profile of the device, it is rather a behavior profile of given IP address that can not be directly associated with the device.

Behavior profiling should be limited to IP addresses from own network. Monitoring of IP addresses that are outside the managed network makes sense only on selected external servers. In that case it is a behavior profile of the device from the perspective of network in which monitoring takes place, since by definition it is not possible to capture all traffic of a device that is outside the scope of monitoring.

### 3.3.2. Collection of statistics and specific measurements

Methods designed for collection of statistics and specific measurements register on regular basis (each processed portion of data) measured values and store them with time stamp of moment of processing. Method code of methods designed for collection of statistics and specific measurements start always with prefix STAT. Results of the measurements are available in user interface through interactive graphs and summarization tables.

### 3.3.3. PRFCLISRV – Behavior profiling (Client/Server)

**Method description** – this method determines the daily percentage rate of client/server or
unclassified behavior for each monitored device based on the ratio between the number of requirements, responses or flows without responses. Classification of flow to requirements, responses and flows without responses is performed in accordance with Bidirectional flows standard (RFC 5103).

**Method configuration** – it is appropriate to activate this method for IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities in the behavior profile.

**Interpretation of results** – this method determines general roles of the network devices. The results of the method can be used to map the network, search for new network servers or for the audit. Abnormal rate of unclassified behavior of a network device may indicate bad configuration, undesirable activities such as network scanning or spyware infection.

### 3.3.4. PRFFLOWS – Behavior profiling (Flows)

**Method description** – this method determines the daily structure of inbound and outbound traffic for each monitored device in terms of number of requests, responses, and flows without responses, and that in the dimensions of the volume of data transferred, number of packets and number of flows. Unlike commonly used distinction between incoming and outgoing traffic method provides more detailed information and in particular distinguishes between traffic initiated by given device and traffic created on request of another device. An example might be the division of outgoing server traffic to requests (traffic generated by a device itself) and responses (traffic generated by a device on the request of the neighborhood).

**Method configuration** – it is appropriate to activate this method for IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities in the behavior profile.

**Interpretation of results** – the results of this method can be used to map network or search for devices, which heavily load the network or for the audit. Increased number of flows may indicate undesirable activities such as P2P networks or spyware infection.

### 3.3.5. PRFTRNSF – Behavior profiling (Transferred)

**Method description** – this method determines the daily volume of incoming, outgoing and the overall traffic in bytes for each monitored device. Within the configuration of the method it is possible to set (option StrictMode) whether the profile should be calculated for only the addresses
specified by the associated filter (option value "yes") or also for addresses that have communicated with given filter. This can be useful when detecting the addresses, with which the IP addresses from monitored network exchanged large amounts of data.

**Method configuration** – it is appropriate to activate this method for IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities it the behavior profile.

**Interpretation of results** – the results of this method can be used to map network or search for devices, which heavily load the network or for the audit. Increased volume of traffic on client workstations may indicate sharing of illegal content, such as movies.

### 3.3.6. PRFPEERS – Behavior profiling (Communication peers)

**Method description** – this method determines the daily unique communication partners of the device divided by roles (client, server, not classified) for each monitored device based on the type of communication with the device. Comprehensive information on the number of unique communication partners and a list of communication partners is available. The method is able to answer the question whether the devices did communicate in a given period.

**Method configuration** – it is appropriate to activate this method for IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities it the behavior profile.

**Interpretation of results** – the results of this method can be used to map network or search for devices, which perform the surveillance over the network elements or for the audit. The increased number of communication partners can indicate an attack, spyware infection or P2P network activity.

### 3.3.7. PRFTRAFFIC – Behavior profiling (Traffic structure)

**Method description** – this method determines the daily structure of provided and used services for each monitored device in terms of number of requests, responses, and flows without responses, and that in the dimensions of the volume of data transferred, number of packets and number of flows. Each service is distinguished by a pair of port/protocol. The method provides very detailed information covering not only the traffic generated by the device, but also typical traffic coming to the device. An example may be the profile of structure of traffic of the device, which runs a POP3 mail client. Profile includes both the number and volume of requests to all POP3 servers, and the
number and volume of responses received from these servers. Similarly, for a web server is available the typical number of requests that come to the server and the server responses to these request. Within the configuration of the method it is possible to exclude minor traffic from the profile structure, based on a specified threshold of flows (ThresholdFlows), packets (ThresholdPackets) and bytes (ThresholdTransferred). The resulting profile then does not include the traffic from a processed batch, that doesn't reach specified limits simultaneously in all three dimensions.

Method configuration – it is appropriate to activate this method for IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities it the behavior profile.

Interpretation of results – the results of this method can be used to map network or to monitor provided and used services or for the audit. Profile also monitors trends in the use and provision of services on the device or can detect the use or provision of unwanted services.

3.3.8. PRFCOUNTRY – Behavior Profiling - Country Reputation

Method description - this method determines the daily country of communication peers for each of monitored device. It stores count of flows and amount of transferred data between country and monitored devices. The traffic statistics are divided according to this, whether communication was initialized by IP address from out of monitored network (reply) or by IP address from monitored network (request).

Method configuration – it is appropriate to activate this method for IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities it the behavior profile.

Interpretation of results – the results of this method can be used to identify IP address communicating with the potentially dangerous country destinations.

3.3.9. PRFACTIVE – Behavior Profiling - Activity

Method description - this method determines the count of connections and volume of sent data for each of monitored device and each five minutes.

Method configuration – it is appropriate to activate this method for IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from
Internet connection line, but not both places at the same time, because that would generate duplicities in the behavior profile.

**Interpretation of results** – the results of this method can be used to identify if the device was on or off and how active was the device according to the network average.

### 3.3.10. STATLATENC – Network Latency Long Term Statistics

**Method description** – this method monitors and stores on long term basis the highest network latency between two designated IP addresses (volba IPAddress1, IPAddress2) reached in each process portion of data. Within the method configuration it is possible to set up lowest latency to store if this value is not reached zero is stored. Latency is calculated based on the difference between timestamps of request and reply data flow. It is possible to change the behavior of this method by using option "TCPFlags" which enables to detect latency only during connection establishment.

**Method configuration** – this method is useful in network latency troubleshooting. Proper place for monitoring depends on network architecture and topology for particular case and issue to solve.

**Interpretation of results** – this method is able to distinguish reliably between application layer and network layer latency while application latency does not appear in the measurements. Setting up the monitoring in proper place it is possible to identify the source of the network latency or monitor network latency in long term period.

### 3.3.11. STATPERF – Network Performance Long Term Statistics

**Method description** – this method monitors and stores on long term basis the average latency, amount of transferred data, count of flows and count of communication peers for defined IP address in every processed batch of data. Latency is calculated based on the difference between timestamps of request and reply data flow. It is possible to change the behavior of this method by using option "TCPFlags" which enables to detect latency only during connection establishment and not between all request and reply data flows. Method allows monitoring up to 3 IP address.

**Method configuration** – this method is useful in device performance profiling or troubleshooting. Proper place for monitoring depends on network architecture and topology for particular case and issue to solve.

**Interpretation of results** – this method provides complex overview of device load from different perspective and its evolution over time.
3.3.12. **SSHDICT – SSH Dictionary attacks**

**Method description** – this method is used to detect attempts to guess user name /password or login by forged certificate for SSH service (TCP/22). The method builds a persistent tree of attackers and victims and in the case of the exceeding limit values (20 experiments from a single IP address or value of the options **AttackAttempts**) for a pair of attacker/victim an event is reported. The method is also capable to detect a successful attack based on abrupt change of statistical properties of the traffic and ending of the attack. With this method it is possible to promptly detect the ongoing attack and block the attacker before he can guess the password. If there is greater delay between attackers activities (more than 30 minutes or value of the option **AttackHole**), the attack from a single IP address can be interpreted as more separate attacks.

**Method configuration** – it is appropriate to activate this method for all IP addresses and monitor not only attacks against own servers, but also the attacks from own network to the Internet. Appropriate place for monitoring the traffic is the central switch and the Internet connection line.

**Interpretation of results** – the results of this methods are relatively straightforward, the method detects an attack against the SSH service. The method may produce false positives when evaluating activities of some surveillance systems using the SSH protocol.

3.3.13. **STATTOP – Top Ports Long Term Statistics**

**Method description** – this method monitors amount of traffic and number of flows for top used services in the network. Within the method configuration it is possible to set up the highest monitored port and maximal number of monitored services.

**Method configuration** – it is appropriate to activate this method for all IP addresses. Appropriate place for monitoring the traffic is the central switch and the Internet connection line. This method should be activated for only one NetFlow source.

**Interpretation of results** – this method provides long term detailed statistics of top used services on the network.

3.3.14. **TOPPORTS – Top Ports**

**Method description** – this method is used to detect significant and sudden changes in services (distinguished by ports) used network-wide in monitored network. Within the method configuration it is necessary to adjust the level of sensitivity on level of changes in the volume of transmitted data (in megabytes) and changes in the number of flows.
Method configuration – it is appropriate to activate this method for all IP addresses. Appropriate place for monitoring the traffic is the central switch and the Internet connection line.

Interpretation of results – this method detects a sudden change in the structure of used services. In the case of change the event is generated that contains in its details the previous and current state of most popular services. Sudden change in network behavior can mean a significant anomaly, in the case of a change of number of flows it is typically a virus spreading or an attack.

### 3.3.15. DNSQUERY – DNS query

Method description – a method for detection of increased number of DNS queries sent by one station. Number of DNS queries is counted for last hour. The event is reported in case, that the number is n-times greater than the average of the other stations, where n is defined by parameter "Multiplicator". The average is calculated only from stations, that sent more than "MinimalQueryLimit" queries. The DNS servers can be excluded from this detection (value of the parameter "ExcludeDNS" is set to yes, default value is no).

Method configuration – it is appropriate to activate this method network-wide for all traffic on the network regardless of IP addresses. Appropriate place for monitoring the traffic is the central switch.

Interpretation of results – this method reliably alerts to the increased number of DNS queries which can indicate the viral infection of the station identified as the event source.

### 3.3.16. BROKENSEN – Broken Sensors

Method description – This method is intended to control active sensors, that are sending the measured data in regular time periods. The method works on machine learning principles. Classifier for sensor is in learning state as long as the parameter “LearnCycles” determines. Minimal coverage of training data, that has to be satisfied by a classifier, is defined by parameter "MinimalCoverage". The tolerance used to control individual variables is defined by parameters "PeriodTolerance" and "TrafficTolerance".

Method configuration – it is appropriate to activate this method only for IP addresses that belongs to sensors. All non-sensors IP addresses in the controlled range would cause high amount of false positives. Appropriate place for monitoring the traffic is the central switch.

Interpretation of results – this method alerts to the wrong behavior of sensor (based on transmission period, bytes per packet or transmissions per hour). It is necessary to consider how large and often deviation from standard behavior can be caused by defective sensor.
3.4. Derived behavior patterns

3.4.1. UPDMISSING – Device update missing

Method description – this method detects devices that are active on the network, but do not communicate with given IP address in specified manner. Larger organizations typically run a local Windows Update Server and all stations based on the Windows OS update from the local Windows Update Server. The method then detects the devices that do not communicate with the local Windows Update Server. Within the configuration it is necessary to set the IP address of the Windows Update Server (UpdateDevice), optional is to set the mode of communication (UpdatePort, UpdateProtocol). It is also possible to determine the minimum amount of data that has to be sent by the device daily to be included in detection (MinimalTransfer). The method uses the outputs from behavior profiles PRFFLOWS and PRFPEERS, when given the method of communication also PRFTRAFFIC.

Method configuration – when using internal update server it is appropriate to activate the method for all IP addresses that should communicate with the update server. Prerequisite is to monitor the network in place, where the communication with the update server takes place. Appropriate place for monitoring the traffic is the central switch of the organization.

Interpretation of results – this method can effectively detect devices that do not communicate with central update server because of bad configuration. The method may also alert to new or unauthorized devices on the network.

3.4.2. DNSREVERSE – DNS Reverse missing

Method description – this method detects network devices without reverse DNS record. Reverse DNS record is a standard device configuration, which allows the device to convert IP addresses to DNS names. It is also possible to determine the minimum amount of data that has to be sent by the device daily to be included in detection (MinimalTransfer). The method uses the output of PRFFLOWS behavior profile.

Method configuration – it is appropriate to activate the method for all the IP addresses of the organization depending on the DNS configuration policy of the organization. Appropriate place for monitoring the traffic is the central switch and the Internet connection line.

Interpretation of results – this method can detect configuration problems, and also alert to new or unauthorized devices on the network.
3.4.3. PEERSCOUNT – Peers count

**Method description** – this method aggregates unique communication peers collected by the PRFPEERS method to their total numbers in individual days. The goal of the method is performance optimization in large networks. The results of the method are available on Dashboard in top communication peers table.

**Method configuration** – method should be activated in case of problems with the display of top communication peers table.

**Interpretation of results** – aggregated communication peers count is updated each hour.

3.4.4. CNTTABLE - Profile table generator

**Method description** – this method is used for calculating communication profiles from data provided by detection method PRFCOUNTRY.

**Method configuration** – this method can’t be configured.

**Interpretation of results** – this method summarizes results of method PRFCOUNTRY.

3.5. Anomaly detection system

3.5.1. Basic principles of anomaly detection

Automatic anomaly detection system that is offered by FlowMon ADS plug-in, works on the principle of learning the standard behavior of the network (i.e. network behavior during learning) and reporting the subsequent deviations from the learned behavior (at the time of detection of anomalies). Between the recognized anomalies are:

- change in the rate of client/server behavior – identifying situations where a client starts to behave as a server or vice versa (ADSCLISRV)
- change in the structure of outgoing traffic (requirements, responses, flows without responses) – change in traffic volume, number of flows, number of packets (ADSFLOWS)
- change the number of communication partners – a significant increase or decrease of the number of communication partners (ADSPEERS)
- changes in the structure provided or used services – identifying new provision or use of services, identifying significant changes in the degree of use (ADSTRAFFIC)
During the learning mode the calculation and update of the average values of the standard behavior of individual IP addresses is performed (the so-called determination baselines). Anomaly detection system granularity is one day, thus the baseline involves behavior in one day. FlowMon ADS distinguishes between working and not working days and maintains different baselines for working and not working days. Length of learning mode depends on the variability of the traffic, the optimal value is 14 days. By default automatic switch from learning to detection mode takes place after 14 days.

Using the automatic anomaly detection system is limited to networks or network segments with fixed IP addresses assigned. In the case of dynamic addresses it is not possible to use behavior detection system or there is no guarantee of good baselines compared with actual values. Compared IP addresses can be identical, but the devices assigned to these IP addresses may differ.

Automatic anomaly detection system is suitable for devices which should report stable behavior over time (production servers, active network elements, etc). If some changes occur in the network, which have a negative effect on current baselines of anomaly detection system (new device, new services, etc) it is possible to drop learned baselines and repeat the process of learning (action Reset available for each detection method of automatic anomaly detections) or to switch to learning mode and let the current baselines update. In case that changes occur only on some stations, you can let the system rebuild baselines only for these IPs. This can be done by setting ADS exceptions, which is described in the "Configuring of ADS exceptions" chapter.

Automatic anomaly detection system implements protection against event overload, which guarantees that given type of anomaly is for given IP address reported at most once a day. If the anomaly lasts, details of existing event will be updated instead of generating new event.

All detection methods that ensure proper functioning of the automated anomaly detection system are identified by the prefix ADS. Besides the methods grouped in Anomaly Detection System there are also system methods of group Network traffic system procedures and General system procedures. All detection methods of the Anomaly Detection System group have a configuration option LearningMode, whose value determines whether the method is in detecting or in learning mode. There is a central assignment of filters to individual anomaly detection method. Filters are assigned to ADS method. Within the configuration of automated anomaly detection system it is necessary to:

- define the addresses that will be comprised in the automated anomaly detection system – assigning filters to ADS detection method, this assignment is than applied to the following anomaly detection methods
- configure the various methods of group Anomaly Detection System
3.5.2. ADSCLISRV – Anomaly Detection System (Client/Server)

**Method description** – this method determines in a learning mode for each IP address the baseline rate of client, server and unclassified behavior. The detection mode it reports deviations from the baseline, always once a day (midnight). Within adjusting the sensitivity of detection method it is necessary to set lower and upper tolerance limit as a percentage of the learned baseline.

**Method configuration** – it is appropriate to activate this method for selected IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities it the behavior profile.

**Interpretation of results** – this method is capable to alert to a situation where there is a change in the general role of network device (server changes its behavior to client behavior, etc) or a situation where the device changes its behavior towards unclassified behavior (i.e. spyware infection, etc).

3.5.3. ADSFLOWS – Anomaly Detection System (Amount of traffic)

**Method description** – this method determines in a learning mode for each IP address and type outbound traffic (requirements, response, fbws without responses), baseline volume of transmitted data, the number of flows and the number of packets. In the detection mode it reports deviations from the learned baseline. When exceeding the baseline corresponding event is reported immediately. When the baseline is not reached, the corresponding event is generated once a day (at midnight). Within adjusting the sensitivity of detection method it is necessary to set lower and upper tolerance limit as a percentage of the learned baseline.

**Method configuration** – it is appropriate to activate this method for selected IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities it the behavior profile.

**Interpretation of results** – this method is capable to alert to a situation where the volume of outgoing traffic of the device is exceeded/not reached. Such behavior can have many causes. Note that this method addresses only the volume of outgoing traffic of the device, which, in case of monitoring own devices, is more interesting that the volume of incoming traffic (for example it can detect sending of large amounts of corporate data, etc). Volume of incoming traffic, among other things, deals with method ADSTRAFFIC.
3.5.4. ADSPEERS – Anomaly Detection System (Communication peers)

**Method description** – this method determines in a learning mode for each IP address baseline number of communication partners (clients, servers and unclassified partners). When exceeding the baseline corresponding event is reported immediately. When the baseline is not reached, the corresponding event is generated once a day (at midnight). Within adjusting the sensitivity of detection method it is necessary to set lower and upper tolerance limit as a percentage of the learned baseline.

**Method configuration** – it is appropriate to activate this method for selected IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities it the behavior profile.

**Interpretation of results** – this method is capable to alert very efficiently to a device infected with some form of malware or to device being established as a part of the botnet network. Penetrative/step increase in the number of communication partners is not the normal behavior of network devices.

3.5.5. ADSTRAFFIC – Anomaly Detection System (Traffic structure)

**Method description** – this method determines in a learning mode for each IP address and service (protocol/port), baseline volume of transmitted data, the number of flows and the number of packets for all traffic types (requirements, responses, flows without responses). In the detection mode it reports deviations from the learned baseline. When exceeding the baseline corresponding event is reported immediately. When the baseline is not reached, the corresponding event is generated once a day (at midnight). Within adjusting the sensitivity of detection method it is necessary to set lower and upper tolerance limit as a percentage of the learned baseline. To reduce false alarms there is the configuration option **AbsoluteToleration** available, which allows ignoring the processing of minor traffic. Absolute tolerance determines the significance rate of the traffic as the product of the number of traffic flows and the bytes-per-packet value for given service (protocol/port).

**Method configuration** – it is appropriate to activate this method for selected IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities it the behavior profile.

**Interpretation of results** – this method is capable to alert to a massive attack on the service, detect a new service provided by the server or to notify about service outage.
3.6. Network traffic system procedures

3.6.1. ADS – Anomaly Detection System (Data harvesting procedure)

Method description – a system method of data collection for automated anomaly detection system. Method can not be deactivated. Within the method configuration it is necessary to set the addresses that will be subject to the traffic analysis by the automatic anomaly detection system. That is done by assignment of filters. Method supports automatic switching of the learning mode to the detection mode. Parameter value SwitchToDetectMode determines the number of days after which all the detection methods from the group Anomaly Detection System will be switched from learning to detection mode.

Method configuration – it is appropriate to activate this method for selected IP addresses of the organization. Appropriate place for monitoring the traffic is the central switch or the to/from Internet connection line, but not both places at the same time, because that would generate duplicities in the behavior profile.

Interpretation of results – this method does not generate any output directly presented to the user.

3.6.2. NFPAIR – NetFlow Pairing

Method description – this method implements Bidirectional flows standard (RFC 5103), i.e. it performs the classification of NetFlow records of requirements, responses and flows without responses. Within the method configuration it is possible to set up so-called pairing constant (TimeWindow), which determines the maximum allowable tolerance between the timestamp of the two flows, so that these flows could be classified as a pair of request, response. When changing the value it is necessary to propagate the change by running the action Apply which causes the restart process ensuring the reception of NetFlow data and classification of flows to requirements, responses and flows without responses.

Method configuration – default value of pairing constant is 1000 ms, in the case of monitoring latency on the network it should be increased to 2000 ms to detect delays longer than 1000 ms.

Interpretation of results – this method does not generate any output directly presented to the user.

3.6.3. PROXY – Proxy Correlation (Experimental)

Method description – this method performs the replacement two flows client-proxy and proxy-server by one flow client-server. This correlation allows detection methods, that are not able to detect events correctly in the network with proxy, to work properly. Within the method
configuration it is possible to set up the tolerated data amount difference between two particular flows, that should be correlated (Tolerance) and counts of miliseconds, that could take the flows outer the proxy longer (ReqDurationOverload – request, RepDurationOverload – reply). The correlation has got high accuracy and coverage but it is not absolute.

Method configuration – the correlation of flows before and behind the proxy is possible only if the network is monitored at two points – inside the network behind the proxy server and outside the proxy server. It is necessary to set up the IP addresses of outer and inner interfaces at the NetFlow sources. It is possible to define one proxy server for each NetFlow source.

Interpretation of results – the method does not generate any output directly presented to the user.

3.7. General system procedures

3.7.1. ADSBASE – Anomaly Detection System (Baseline computation)

Method description – a system procedure that periodically updates the baselines of automated anomaly detection system.

Method configuration – this method does not require any configuration by the user.

Interpretation of results – the method does not generate any output directly presented to the user.

3.7.2. ADSREP – Anomaly Detection System (Detection and reporting)

Method description – a system procedure that periodically generates events of automated anomaly detection system based on higher or lower than memorized baselines.

Method configuration – this method does not require any configuration by the user.

Interpretation of results – this method does not generate any output directly presented to the user.

3.7.3. REPORTER – Event reporter

Method description – this method provides a periodic processing of all generated events and their sending by e-mail reports to all defined recipients according to defined rules.

Method configuration – event reporting via e-mail is configured in section Configuration\Event Reporting.
Interpretation of results – this method does not generate any output directly presented to the user.

3.7.4. SYSCLEAN – System clean-up procedure

Method description – this method periodically deletes temporary data and optimizes data structures for high performance of the application.

Method configuration – method does not require any configuration by the user.

Interpretation of results – this method does not generate any output directly presented to the user.

3.7.5. SYSLOGGER – Event syslog

Method description – this method provides a periodic processing of all generated events and their delivery in CEF format using syslog transport protocol. It could be set if the event priority is used as a syslog severity.

Method configuration – event reporting via syslog is configured in section Configuration\Event Reporting.

Interpretation of results – this method does not generate any output directly presented to the user.
4. User interface

The FlowMon ADS plug-in offers a complete Web user interface based on JavaScript and AJAX technology. For basic control and accessing various parts of the application there is the main menu on the left side. The upper part displays the status and information bar, the rest of the window area serves as the user workspace. Another means of controlling application is a context menu available by right clicking on relevant object. Possibility of showing context menu is indicated by icon on status and information bar when cursor is placed on this object.

Tips of the day are part of the application displayed after successful user login. After login to the application a welcome screen is displayed. You can find here some important information what should be done before start using the application.

4.1.1. Drag and drop support

IP address in tables and text statements can be drag and drop onto other objects. To activate IP address dragging, press Ctrl and left mouse button simultaneously. IP address can be dragged onto some of left menu items or search criteria form. While dragging the IP address, all possible target objects in UI are highlighted by an "plus" icon.

Dropping an IP address onto the search criteria form starts searching according to the current form settings and given IP address. Dropping an IP address onto the main menu item causes search according to the recently used form settings and given IP address.

Figure 4.1: Example of moving IP address to left menu
4.1.2. Checklist items searching

The forms in application contain checklists. All checklists support quick search function for searching items of list by typing the first letters of item name. Click on the checklist label opens a new window allowing easy selection of desired items. The availability of function is indicated by an icon before label.

![Example of checklist items searching](image)

Figure 4.2: Example of checklist items searching

4.2. Basic controls

4.2.1. Main application menu

The main application menu is basic a guidepost to all perspectives and features available in the application. Related functions and views are brought together in joint groups. The main application menu contains the following items:

- **Home** – return to the basic interface of probe/collector
- **Dashboard** – overview of current network status
  - **Events** – overview of most important and recent events, summary of all recognized events
  - **Profiles** – top network users according to amount of transferred data and flow count
  - **Network** – whole picture of network usage according to used and provided network services
- **Events** – set of views on events
  - **Aggregated view** – aggregated view brings together neighbor events of the same type of individual device into contiguous blocks, which are then
graphically displayed on the timeline

- **Simple list** – a simple list of events, advanced searching and filtering of events
- **By hosts** – a view of events grouped by IP addresses, which relate to the events
- **By topology** – a view of events grouped according to defined network topology

- **Profiles** – a set of views of behavior profiles of network devices
  - **Host profile** – a comprehensive view of behavior profile of a particular network device
  - **Host lookup** – search for servers and clients in the network by the extent of client/server behavior and provided/used services
  - **Communication abroad** – view of communication abroad profile of individual station.
  - **Country profiles** – view of communication abroad profile of individual country.
  - **Statistics** – visualization of values measured by statistics collection methods

- **Reports** – a set of HTML reports (reports on request) that summarize all the information about individual IP addresses available in the plug-in
  - **General report** – generic report that allows detailed definition of report context
  - **Manager’s report** – report adjusted to the needs of managers with the possibility to edit the report content

- **Configuration** – function used to configure and manage plug-in
  - **General configuration** – general configuration of the plug-in, configuration templates, backup and recovery of a device
  - **NetFlow sources** – NetFlow data source configuration
  - **Filters** – filter configuration (structure of addresses in monitored network)
  - **Methods** – configuration of detection methods
  - **Perspectives** – configuration of perspectives for prioritization of events
  - **Event categories** – event categories management
  - **Topology** – configuration of the network topology
  - **Event reporting** – management of automatic event reporting
- **False positives** – management of false positives
- **ADS exceptions** – management of exceptions from detection mode of ADS methods
- **User preferences** – management of user UI preferences

About – brief information about the application and its version, information about the number of processed flows, license information, access to user documentation, information about skipped methods and batches during the data processing

Configuration and management of plug-in is described in detail in Chapter 2 (Installation and configuration). In this chapter we are not dealing with functions of the **Configuration** group and we describe only ordinary user’s work with the applications.

The currently selected menu item is always grounded by arrow shape facing toward the user’s workspace. Each main menu section can be shown/hidden by clicking on the section label. Configuration section is hidden by default. The main application menu can be hidden as well and thus increase the available workspace of the user. For hiding/displaying the main menu of the application there is a pane separating main menu from the workspace of the user with the arrow icon (left – to hide, right – see).

### 4.2.2. Status and information bar

Status and information bar indicates selected basic information concerning the application and its user interface to the user (items are listed left to right):

- **Application model**
- **The current location of the users within the application** – the name of the page where the user is currently located
- **Filter templates** - allow managing of the saved parameters of search criteria for reuse. Current setting of the search criteria filter can be saved. Selected template can be deleted or used on search criteria. There is preconfigured set of filter templates for a following views: General Report, Events – Simple list, Events – By host.
- **The availability of the context menu indicator** – active indicator signals the availability of the context menu for selected item (item, above which is the mouse cursor).
- **The availability of the context menu indicator** – active indicator signals the availability of the context-sensitive help for selected item (item, above which is the mouse cursor).
- **The NetFlow sources problem indicator** – active indicator signals that there is some problem with at least one of the active NetFlow sources (e.g. there are no data to
process).

- **Language switch** – immediately switches the user interface of the application to the language selected by positioning the language switch (available English and Czech)
- **Logged on user** – the name of currently logged on user
- **Logout** – logs out currently logged user

### 4.2.3. Context menu

Context menu is a means for fast control of the application. Context menu brings together all the actions that can be performed with element that is selected in the user interface. Availability of the context menu is indicated by the context menu icon in status and information bar. Context menu appears after clicking the right mouse button.

The most frequently used context menu is a menu of IP address/events which includes the following items:

- **General information** – the translation of IP address on the DNS name, obtaining WHOIS information and displaying custom information about IP address (if specified – see Configuring filters). The data are displayed in a floating window
- **Related events** – a view of events associated with the IP address, transition to the perspective of **Events\By hosts**
- **Host profile** – a view of behavior profile of the IP address, transition to the **Profiles\Hosts** view
- **Abroad communication** – a view of abroad communication profile of the IP address, transition to the Profiles\Communication Abroad view.
- **Aggregated events** – a view of aggregated events on timeline associated with the IP address, transition to the Events\Aggregated view.
- **Resolve all IP addresses** – translation of all visible IP addresses to DNS names
- **IP Tools** – common diagnostic IP tools
  - **Locate in map** – traces the physical location of IP address and displays it on the map. This function communicates with an external service (Yahoo Maps) and for its functionality it is necessary not to block the communication of the device (probe/collector) to port 80 (standard web traffic).
  - **Ping** – check availability of selected IP addresses
  - **Traceroute** – is a computer network tool for measuring the route path and transit times of packets across an Internet Protocol (IP) network
- **Manage event categories** – the classification of events into a user-defined categories
- **Mark as false positive** – marks the event as a false alarm, it will be no longer reported
- **Event details** – transition to event details, displaying of related information (categorization, notes)
- **Visualize event** – a view of the events through an interactive chart based on NetFlow data caused by the event. The menu item is only available if the given address of your NetFlow collector data is tied to the event.
- **Event evidence** – a detailed view of events including all data flows from which the event has been generated. The view is primarily intended for exporting the evidence from the application; displayed Web page is adapted to copy its contents in plain text to the clipboard
- **Export as image** – this function opens focused dashboard or events table in new window as image. It can be saved or copied into clipboard. This function is available for Firefox viewer only.
- **Display help page** – displays context-sensitive help for the selected user interface element. The menu item is available for all user interface elements that have an associated context sensitive help.
- **Visualize LATENCY** – a view of LATENCY events. It is available only from “Simple list” where are shown only the LATENCY events.

Other specific context menus are given under the relevant parts of the user interface description, namely the context menu available at some dashboard tables. Above the context menu there is also a tooltip for IP addresses available. Tooltip contains information about the country where IP address is located.
4.3. Dashboard

Dashboard is a basic interface element that is displayed to the user right after logging on to the application. Dashboard is used to obtain an overall picture of what is happening on the network via a set of top 10 statistics. The default view shows events and statistics for the last 24 hours with the possibility of adjusting the view by changing the search criteria:

- **From, To** – the relevant period for displaying the information on the dashboard, the period can be specified directly or chosen from associated calendar.
- **IPs** – IP addresses, which are to be given information on the Dashboard, individual IP addresses can be separated by a comma. It is also possible to enter the network address/mask, instead of IP addresses you can enter the DNS name.
- **Event types** – types of events to be included in the Dashboard
- **Filters** – selection of the IP addresses, which are to be displayed on the Dashboard, all predefined filters are available.
- **NetFlow sources** – selection of data sources for which the events are to be displayed on the Dashboard
- **Refresh online** – automatic renewal (update) Dashboard every 5 minutes
- **Reset** – reset of the preset form values to the default values
- **Search** – a view of the events and information about IP addresses with applied filters and conditions specified in the form

According to dashboard part (Events, Profiles, Network) only relevant search criteria are available.

4.3.1. Events

Top 10 events by priority

The table shows the 10 most important events from the chosen perspective. Within the table, you can:

- Change the perspective through the **Perspective** drop-down list
- Switch table/graph view
- Restore the contents of the table according to currently configured filters
- View all events according to selected perspective, transition to the **Events\Simple list** view
Latest 10 events

Table displays 10 newest events. Within the table, you can:

- View event details (i.e. the date and the objectives of the event), will extend the table
- Restore the contents of the table according to currently configured filters
- View all events according to selected perspective, transition to the Events Simple list view

Top 10 events by event type

The table shows the top 10 event types, along with the number of occurrences of the events of that type. Within the table, you can:

- Switch table/graph view
- Restore the contents of the table according to currently configured filters
- View the complete table of all kinds of events along with the number of occurrences of the events of given type in a new window
- Display context menu above the type of event, which allows you to search all events of the type (Display events of this type), the transition to Events Simple list view

Top 10 IPs by event count

The table shows the 10 IP addresses, which produce the greatest number of events. Within the table, you can:

- Switch table/graph view
- Restore the contents of the table according to currently configured filters
- View the complete table of all kinds of events along with the number of occurrences of the events of given type in a new window

Events in last batch

The table shows maximum 10 event types, which was detected during the last processed batch of data. Within the table, you can:

- View event details (i.e. the date), will extend the table
- Restore the contents of the table according to currently configured filters
- Display context menu above the type of event, which allows you to search all events of the type (Display events of this type), the transition to Events Simple list view

The transition to Events Simple list view
4.3.2. Profiles

Top 10 IPs by data volume

Trinity tables showing the IP addresses that have transferred the largest amount of data (inbound traffic, outbound traffic, and total traffic). Contents of the tables are created using PRFTRNSF method. Within the table, you can:

- Switch table/graph view
- Restore the contents of the table according to currently configured filters
- View a table of all IP addresses along with volumes of transferred data

Top 10 IPs by connection count

The table shows the IP addresses that generated the greatest number of flows (connections). Contents of the tables are created using PRFFLOWS method. Within the table, you can:

- Switch table/graph view
- Restore the contents of the table according to currently configured filters
- View a table of all IP addresses along with connection count

Top 10 IPs by communication peers count

The table shows the IP addresses that communicated with the greatest number of unique peers. The summary row contains total number of unique peers. Contents of the tables are created using PRFPEERS method. Within the table, you can:

- Restore the contents of the table according to currently configured filters
- View a table of all IP addresses along with communication peers count

Top 10 IPs by country diversity

The table shows the IP addresses that communicated with the greatest number of countries. Contents of the tables are created using PRFCOUNTRY method. Within the table, you can:

- Restore the contents of the table according to currently configured filters
- View a table of all IP addresses along with communication peers count

4.3.3. Network

TOP 10 services

A pair of tables showing the most used and provided services in the network. Contents of the tables are created using PRFTRAFFIC method. Within the table, you can:

- Switch table/graph view
- Restore the contents of the table according to currently configured filters
● View the table of used/provided services
● View context menu of the service, which lets you view information about the service (Protocol details) or see its clients/servers (Display service details)

TOP 10 countries
A pair of tables showing the most frequent nationality of communication peers sorted by count of connection and amount of transferred data. Contents of the tables are created by CNTTABLE and PRFCOUNTRY method. Within the table, you can:

● Switch table/graph view
● Restore the contents of the table according to currently configured filters
● View the table with all detected countries

4.4. Events

4.4.1. Aggregated view

Aggregated view presents events of particular device in an intuitive graphical way considering the aspect of time. Events are filtered by following search criteria.

- **From, To** – the relevant period for displaying the information on the dashboard, the period can be specified directly or chosen from associated calendar.
- **Event types** – types of events to be displayed in the Dashboard
- **IPs** – selection of the IP addresses, which are to be displayed by direct setting of IP addresses
- **Filters** – selection of the IP addresses, which are to be displayed, all predefined filters are available.
- **NetFlow sources** – selection of data sources for which the events are to be displayed

![Figure 4.4.1: Search criteria in Aggregated view](image)
Categories – user-defined categories of events
Perspective – rules for the prioritization of events
Reset – reset of the preset form values to the default values
Search – a view of events matching the search filters

Each event type the device takes place in is represented by one line called a **swimline**. Event occurrence is represented by a colored rectangle in a particular swimline. According to the selected scale, neighbor events are aggregated into one rectangle. Width of the rectangle corresponds to the time length of the event. Time goes from left to right at the x axis. For clarity night and day alternation is displayed.

### Controls

**Zoom**

User can zoom in visualization (showing in larger scale) by using left mouse button to select requested time interval. There are "Undo" and "Redo" icons on the right side above the visualization to navigate through changes of the scale. Use the icons "Plus" and "Minus" can change the size of colored rectangles in swimline.

**Event detail**

By right clicking on the event (green rectangle) is possible to display context menu allowing displaying event details (IP address, start time, end time, summary) or transition to Events\Simple list of corresponding events. The detail summary can be shown only for events detected after installation of application version 2.08.00 because of migration to new technologies, which allow us to aggregate the events into the high level events better.
Computing aggregated event details which consists of more than 25 events is accelerated by sampling. When sampling is used, there is an information about lower accuracy of data in event detail.

Device activity

The activity of the device can be shown in this view, too. Activity is displayed as added swimline ACTIVE. When the cursor is over the IP address, the representation of activity is extended over all swimlines as a coloured background.

4.4.2. Simple list

View of events in the form of a simple list (events table). It is primarily sorted by the time of the event creation. The search criteria are the same as in the case of Events\Aggregated view.

The result of query is divided into pages where one page contains a maximum of 500 items of the result. The result is a table that includes the following items:

- **Row number** – number of the table row
- **Event source** – event originator (IP address)
- **Type** – type of event, in fact a reference to the detection method which recognized the event
- **Detail** – detailed information on the event
- **Timestamp** – time stamp of event generation
- **NetFlow source** – NetFlow data source on which the event has been generated
- **Targets** – event targets (a list of IP addresses). At most 10 items is shown in the table. If more targets are associated with the event, there are available on request in new window.

It is possible to export the output into the csv file by clicking Export events to .csv in context menu.

4.4.3. By hosts

A table view of the events grouped according to the sources and targets of events. There are the same search criteria as in the case of Events\Simple list available in addition extended with following option:

- **IP's role** – specifies the role of selected IP addresses in the events, whether they should be source or destination of the events.
The result table is sorted according to the IP addresses, for each IP address the number of events where the IP address is the source or the target of the event is displayed. Consequently, it is possible to view a list of event types related to the IP address. For each event type can be displayed specific events in the form of a separate table, which includes the same data as in event table Events\Simple list.

![Figure 4.4.3:: Example view of events grouped by IP addresses](image)

### 4.4.4. By topology

A view on events that is based on a defined network topology. Network topology is configured in the section Configuration\Topology. In combination with perspectives it is suitable for identifying problematic parts of the network. There are the following filter criteria available:

- **From, To** – the relevant period for displaying the information on the dashboard, the period can be specified directly or chosen from associated calendar.
- **Perspective** – rules for the prioritization of events
- **Categories** – user-defined categories of events
- **Reset** – reset of the preset form values to the default values
- **Search** – update of the topology tree according to the specified filters

In the displayed topology tree a number of events in a given network segment is indicated. If the
perspectives are used, the events are also divided into groups according to severity and the marked in color. Clicking on a group displays a table of events.

Events of priority HIGH:

<table>
<thead>
<tr>
<th>#</th>
<th>Event source</th>
<th>Type</th>
<th>Detail</th>
<th>Timestamp</th>
<th>Netflow source</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.1.37</td>
<td>SMTP</td>
<td>SMTP [TCP:25] (unique hosts: 1, mail count: 1, legitimate server responses)</td>
<td>2019-04-19 11:54:27</td>
<td>127.0.0.1</td>
<td>81.19.4.86</td>
</tr>
<tr>
<td>3</td>
<td>10.0.1.37</td>
<td>DVCOM</td>
<td>distinct destination IP: 15, distinct destination ports: 108</td>
<td>2019-04-19 11:48:15</td>
<td>127.0.0.1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10.0.1.73</td>
<td>DVCOM</td>
<td>distinct destination IP: 42, distinct destination ports: 27</td>
<td>2019-04-19 10:36:53</td>
<td>127.0.0.1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10.0.1.73</td>
<td>DVCOM</td>
<td>distinct destination IP: 45, distinct destination ports: 45</td>
<td>2019-04-19 09:34:49</td>
<td>127.0.0.1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10.0.1.73</td>
<td>DVCOM</td>
<td>distinct destination IP: 33, distinct destination ports: 32</td>
<td>2019-04-19 09:22:54</td>
<td>127.0.0.1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>10.0.1.96</td>
<td>HIGHTRANSF</td>
<td>transferred: 122902875:B</td>
<td>2019-04-19 08:20:03</td>
<td>127.0.0.1</td>
<td></td>
</tr>
</tbody>
</table>

Figure 4.4.5: An example of HIGH priority events view

4.4.5. Event details

The Event details view is unlike other event views available only through the context menu. Event details include all available information about the event, event comments category.

Event details include following information:

- **Type** – type of event, in fact a reference to the detection method which recognized the event
- **Timestamp** – timestamp of event generation
- **Event source** – event originator (IP address)
- **Event source host name** – DNS name assigned to the IP address at the time of event detection
- **Detail** – detailed information on the event
- **Probability** – probability with which the event has been detected
- **NetFlow source** – NetFlow data source on which the event has been generated
- **False positive** – indicates whether it is a false positive (according to rules for marking events as false positives currently in effect)
- **Targets** – event targets (a list of IP addresses). At most 10 items are shown in the table. If there are more targets associated with the event, they are available on request in new window.
Event can be marked as a false positive (Mark as false positive). When marking an event, it is necessary to enter time relevance of marking (individual days of the week, time tolerance). Marking an event as a false positive means that events of the same type and originator will not be generated if there is a rule for marking of false positive in effect. Note that the event can be marked as a false positive also by `Mark as false positive` context menu item.

**Figure 4.4.6: Example of event details**

<table>
<thead>
<tr>
<th>#</th>
<th>comment</th>
<th>Author</th>
<th>timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Logáři provoz</td>
<td>adsadmin</td>
<td>10:07:40</td>
</tr>
</tbody>
</table>

**Figure 4.4.7: Marking the event as a false positive**

Mark event as false positive?

- Event: High data transfers
- Detected for: 10.0.1.163
- Detected on: 2019-10-22, 05:50:12

Mark this event on this ip address as false positive also for every:

- Mo Tu We Th Fr Sa Su Whole week
- 30 minutes tolerance interval

- [ ] Delete false positive events

**Cancel**  **Submit**
Further for each event there are chronologically listed related comments. The comment always includes the author (Author) and timestamp of comment insertion (Timestamp). Comments may be changed (Change) or deleted (Delete) depending on the author and currently logged on user. It is always possible to add a new comment (Add new comment).

Event details also include event category. The category always includes the author (Author) and the timestamp (Timestamp). Individual categorization can be removed (Remove) or added (Add to category). Note that the management of event categories is also available through Manage event categories context menu item.

### 4.4.6. Interactive event visualization

The Interactive event visualization view enables to view the network traffic data, based on which the event was detected. The view is available for each event detected on the basis of network traffic through the Visualize event context menu item. Similarly as in the Event details view, event...
details are displayed first in the table to make clear what the event is visualized.

Interactive visualization displays individual IP addresses as nodes and data transmission between the IP addresses as edges. Size of nodes and edges is proportional to the volume of transmitted data and their colors ranged from green to red are corresponding to the number of flows. Event visualization can be interactively traversed; each node has a context menu marked by symbol "+". The item More data of this menu ensures downloading of all relevant communications of the IP address. The item Info obtains and displays the details of the network traffic in the form of a floating table. For nodes it displays table of aggregated communications with other IP addresses. For inbound traffic the communication is aggregated on source IP address, destination port and protocol. For the outbound traffic it is aggregated on the destination IP address, source port and protocol. For edges it displays a table of individual data flows that constitute the edge including details such as the duration of the connection, flags and the type of service (TOS).

Special type of node is called aggregation. Aggregation represents a larger number of IP addresses and is visualized as a circle shaped node. Clicking on such node displays a list of IP addresses that constitute the aggregation. Selecting any of the displayed IP address will tear it from the aggregation. Furthermore it is possible to work with the IP address and details of its communication by standard means that are described above.

### 4.4.7. Event evidence

The Event evidence view provides the means to export the evidence (network data flows based on which the event was detected) from the application. Displayed web page is ready having its content copied to the clipboard in plain text. For each event there is the event type, timestamp of event creation, event originator, event details and targets. Next comes the histogram, which could display relations between various pairs of variables. Below is displayed the list of data flows (raw NetFlow data from the collector). The displayed information includes source and target IP address, time stamp of the data flow, its duration, protocol, source and destination port, the volume of transferred data, number of transmitted packets and the type of service.
4.4.8. Visualize LATENCY

The Visualize LATENCY view is designed to show the latency within the whole network. It could lead to simple identification of problematic network element. The view is available from context menu of Simple list view that is showing only the LATENCY events.
4.5. Profiles

4.5.1. Host profile

The Profiles\Host profile view displays the results of detection methods that build behavior profiles. Behavior profile can be viewed for any time period of just for one IP address. There are the following filters available:

- **IP address** – IP address whose profile is required
- **From, To** – the relevant period for behavior profile that can be entered directly or chosen from associated calendar.
- **Max. rows** – the maximum number returned results (limit on the number of rows in a traffic structure table)
- **Device roles** – roles of device to be included in the result (Client, Server and Unclassified)
The result is a detailed behavior profile of chosen device. The profile includes the outputs of detection methods PRFCLISRV, PRFFLOWS, PRFPEERS and PRFTRAFFIC and consists of the following parts:

**Client/Server behavior – summary:** The overall client and server behavior of the device over a given period. It is the outputs of the method PRFCLISRV that are displayed in the form of pie chart with the option to switch to a table (Toggle table/chart display).

**Client/Server behavior – by days:** The overall client and server behavior of the device in given days. It is the outputs of the method PRFCLISRV, suitable for monitoring trends, that are displayed in the form of bar graph form with the option to switch to a proportional bar graph (Rotate charts) or to a table (Toggle table/chart display).

**Amount of Traffic – summary:** Traffic volumes of the device (total, inbound, outbound), divided into requirements (RQ), responses (RP) and requests without responses (S), i.e. unpaired flows. It is the outputs of the method PRFFLOWS that are displayed in the form of pie chart with the possibility of switching between the monitored dimensions (transferred data volume, the number of packet and byte count) by function Rotate charts and the possibility to switch to a table (Toggle table/chart display).

**Amount of Outgoing/Incoming/Total Traffic – by days:** Trinity of individual tables/graphs displaying outgoing, incoming and total traffic volumes of the device over each day, divided into requirements (RQ), responses (RP) and requests without response (S), i.e. unpaired flows. It the outputs of the method PRFFLOWS, suitable for monitoring trends, that are displayed in the form of pie chart with the possibility of switching between the monitored dimensions (transferred data volume, the number of packet and byte count) by function Rotate Charts and the possibility to switch on the table (Toggle table/chart display).

**Communication peers – summary:** Total number of communication partners divided to clients and servers. It is the outputs of the method PRFPEERS that are displayed in the form of pie chart with the possibility to switch to the table (Toggle table/chart display). On demand (Details) there is a list of all communication partners available.

**Communication peers – by days:** Number of communication partners divided to clients and
servers by individual days. It is the outputs of the method PRFPEERS, suitable for monitoring trends, that are displayed in the form of bar graph form with the option to switch to a proportional column chart (Rotate charts) or to a table (Toggle table/chart display). In the table you can request a detailed listing of all communication partners for given day (click on the date which is an active link).

**Traffic structure – summary:** Structure of services used and provided by the device over given period. It is displayed in the form of pie chart with the possibility of switching between the monitored dimensions (transferred data volume, the number of packets and number of bytes) functions Rotate Charts and the possibility to switch to the table (Toggle table/chart display). It is also possible to further limit the view of the traffic structure profile to a single day (Select date). In the table view there is a feature Chart available which renders the trend of use/provision of selected service (service is a triad of device role, protocol, port). It is the outputs of the method PRFTRAFFIC.

**Host activity:** Activity ratio by connection count and sent data volume to average values of whole monitored network according to the time. It is displayed in the form of line chart with the possibility to switch to the table (Toggle table/chart display). There are displayed only the non-zero values of the chart. It is the output of the method PRFACTIVE aggregated to fixed count of values.

**4.5.2. Host lookup**

One of the possible uses of building the behavior profiles lies is searching of network clients and servers. Searching uses the output of method PRFCLISRV that can be combined with the profile of used/provided services, i.e. outputs of PRFTRAFFIC method. It is possible to use following search filters:

- **From, To** – the relevant period for searching clients and servers, the period can be specified directly or chosen from associated calendar.
- **IPs** – IP addresses which should be included in the search; individual IP addresses can be separated by a comma. It is also possible to enter the network address/mask and instead of IP addresses you can enter the DNS name.
- **Filters** – specification of IP addresses to be included in the search in form of predefined filters.
- **Server(%)** – the required rate of server behavior in the percentage range from-to.
- **Client(%)** – the required rate of client behavior in the percentage range from-to.
- **Unclassified(%)** – the required rate of unclassified behavior in the percentage range from-to.
Max. rows – the maximum number of returned results.

Traffic kind – search limit based on information about used and provided services by the device role (Device roles), port (Port) and service protocol (Protocol).

The result is a list of IP addresses that meet specified criteria, displayed in tabular form. For each address, the date (Date) and individual behavior percentage rates are displayed.

4.5.3. Communication abroad

The view Profiles\Communication abroad allows to display communication abroad of individual IP address according to search criteria. The view uses the outputs of PRFCOUNTRY method. It is possible to use following search filters:

- From, To – the relevant period for searching communication abroad of device, the period can be specified directly or chosen from associated calendar
- IPs – IP addresses which should be included in the search; individual IP addresses can be separated by a comma. It is also possible to enter the network address/mask, instead of IP addresses you can enter the DNS name.
- Filters – specification of IP addresses to be included in the search in form of predefined filters.
- Flow count – minimal flow count to include IP address in the search
- Transferred (MB) – minimal amount of transferred data to include IP address in the search
- Count of countries – minimal number of countries the device communicate with to
include IP address in the search

- **Max. Rows** – maximum rows of output
- **Traffic direction** – search limit based on direction of establishing connection (client – from monitored network, server – to monitored network, both – both direction)
- **Transferred / flow count** – type of data transfer information to display
- **Value type** – type of communication peers count value (relative – in percent, absolute – absolute number)

The result is list of IP address that meet search criteria, displayed in tabular form. For each address following cols are displayed: the most frequently countries (Countries), count of this countries (Count of countries) and amount of transferred data (Flows/Transferred). The amount of transferred data does not include communication within local networks.

<table>
<thead>
<tr>
<th>#</th>
<th>IP Address</th>
<th>Flows</th>
<th>Count of countries</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.1.42</td>
<td>2060</td>
<td>40</td>
<td>CZ (49.4%) US (17.7%) IE (9.9%) RU (9.9%) HU (3.9%) UK (3.7%) BE (3.2%) SI (1.5%)</td>
</tr>
<tr>
<td>2</td>
<td>10.0.1.43</td>
<td>2781</td>
<td>37</td>
<td>CZ (44.3%) US (20.7%) BE (9.1%) IE (9.9%)</td>
</tr>
<tr>
<td>3</td>
<td>10.0.1.53</td>
<td>3843</td>
<td>47</td>
<td>CZ (88.2%) US (24.2%) BE (9.5%) UNK (4.5%)</td>
</tr>
<tr>
<td>4</td>
<td>10.0.1.74</td>
<td>8026</td>
<td>50</td>
<td>CZ (81.4%) US (12.7%) UNK (2.6%) IE (2.4%)</td>
</tr>
</tbody>
</table>

Figure 4.5.4: Search criteria in Profiles\Communication abroad

Figure 4.5.5: Example of view Profiles\Communication abroad
4.5.4. Country profiles

The view Profiles\Country profiles allows to display communication abroad by country. Output can be filtered by search criteria. The view uses the outputs of PRFCOUNTRY method. It is possible to use following search filters:

- **From, To** – the relevant period for searching communication abroad, the period can be specified directly or chosen from associated calendar
- **Countries** – select the countries which should be included in the search
- **Flow count** – minimal flow count to include country in the search
- **Transferred (MB)** – minimal amount of transferred data to include country in the search
- **Minimal IP count** – minimal number of IP address communicate with country to include country in the search.
- **Traffic direction** – search limit based on direction of establishing connection (client – from monitored network, server – to monitored network, both – both direction)
- **Transferred / flow count** – type of data transfer information to display
- **Value type** – type of communication peers count value (relative – in percent, absolute – absolute number)

The result is list of countries that meet search criteries, displayed in tabular form. For each country following cols are displayed: TOP IP addresses communicating with country (IP addresses), count of this addresses (Count of IPs) and amount of transferred data (Flows/Transferred).
4.5.5. Statistics

View **Profiles\Statistics** makes available values measured by methods designed for statistics collection like top services or network latency. Measurements are visualized in graphs with linear or logarithmic scale. Graph is interactive while it is possible to dynamically hide and show particular numerical series. It is possible to switch from graph view to table view which summarizes all the measurements for selected time period. Individual measurement values are available through context menu for selected table row. It is possible to use following search filters:

- **From, To** – the relevant period for searching devices of selected properties, the period can be specified directly or chosen from associated calendar.
- **Method** – statistical method selection.
- **Value** – particular measurement kind selection for previously selected statistical method.
- **Max. rows** – the maximum number of returned results (may increase graph lucidity)

Summary table offers for each key total sum, average value and minimal and maximal measured value.
4.6. Reports

The reports are a means to obtain complete information about the IP address/IP addresses registered in the application. Reports combine the information on events and data from behavioral profiles into a single assembly which is optimized for printing from a browser (e.g., into PDF format). To print reports correctly following print parameters are necessary:

- Print Background (colors & images)
- Margins 0
- Headers & Footers --blank--

4.6.1. General report

General report offers users the ability to create arbitrary report by combining a series of three main criteria (General filter, Traffic kind filter and Client/Server behavior filter). General filter allows defining the period (From, To), entering the IP address in question (IPs, Filters) and selecting relevant event types (Event types) with the option to limit search results to the IP addresses, which produce some of the selected events (Restrict selected).
Next filtering option is **Traffic kind filter** which includes the results of the method PRFTRAFFIC. IP addresses included in the report can also be limited by their kind or by provided network services. Within the configuration it is necessary to specify the role of the device (**Device role**) and enter the desired pair of protocol (**Protocol**), port (**Port**).

![Traffic kind filter](image1)

**Figure 4.6.3: Traffic kind filter**

The last group of filters is Client/Server behavior filter, which uses the results of the method PRFCLISRV. IP addresses included in the report can also be limited in terms of client and server behavior rate. Within the configuration it is necessary to specify required range (0-100 percent) of each type of behavior (**Server**, **Client** and **Unclassified**). It is also possible to specify the number of days, for which the condition has to be met.

![Client/Server behavior filter](image2)

**Figure 4.6.4: Client/Server behavior filter**

After configuring the filtering criteria you can select the information that should be included in the final report for each IP address:

- **Events** – graph and table Top 10 events
- **Transferred** – volumes of traffic (inbound, outbound, total), outputs of method PRFTRNSF
- **Client/Server behavior** – rate of client and server behavior, outputs of method PRFCLISRV
- **Flows** – the detailed structure of the incoming and outgoing traffic from the perspective of requirements, responses and flows without responses, outputs of the method PRFFLOWS
- **Comm. peers** – number of communication partners, outputs of the method PRFPEERS
- **Traffic** – the traffic structure by used and provided services (top 10), output of the method PRFTRAFFIC
The resulting report can be generated through Generate report. Report is generated in a new window/tab of the web browser and is optimized for printing. Information about each IP address begins on new page.

4.6.2. Manager's report

Manager’s report offers users the ability to create editable report including summary of the most important events and network statistics. The report is generated according to desired criteria specified by General filter. General filter allows defining period (From, To), entering relevant IP address (IPs, Filters) and determine important events by selecting view (Perspective) and minimal events priority (Minimal priority).

Generating editable report is started by Generate report button. Report is generated in a new window/tab browser and it is optimized for landscape orientation printing. The whole report is displayed on one page.

Objects of the report can be edited by clicking the left button on them. Editing allows rename and move title of the report, date and period. It is also possible to edit text in all cells of the table.
Figure 4.6.7: Manager’s report output
5. Contact information

5.1. Vendor

AdvaICT, a.s.
Jundrovská 618/31
Brno 624 00

Web: www.advaict.com
E-mail: adva@advaict.com
Tel.: +420 511 112 170

5.2. Distributor

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

Web: www.invea-tech.com
E-mail: info@invea-tech.com
Tel.: +420 541 143 072
Copyright

This document is subject to change without prior notice. All information in this document are assumed to be true, but the author nor AdvaICT, a.s. bear no responsibility for the accuracy of the information herein. No part of this document can be reproduced in any form or by any means without prior permission of AdvaICT, a.s.

FlowMon logo is a trademark registered to CESNET s.r.o. association. Other brands and product names are trademarks of their respective owners.

This product contains NfSen and Nfdump software Copyright (c) 2004, SWITCH – Teleinformatikdienste fuer Lehre und Forschung.

All other trademarks are the property of their respective owners.