Nacionalni CERT
Croatian National CERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Arbor Networks Peakflow X

NCERT-LAB-PUBDOC-2011-12-003

Contents

1 Introduction

Companies nowadays need reliability, speed and safety of their network infrastructure. Network systems are getting greater and more complex, and it is well-known that complexity is one of the greatest enemies of safety. Therefore, the focus is not only on protecting assets any more, but monitoring the system operation and, what is even more important, receiving key information on time. It is important to have a global network display, and a simple way of monitoring the safety policy. Something similar can be achieved with the help of a device that can single out individual security threats from an enormous amount of data passing through the network within companies. Such a device must also discover threats in real time and have an option of monitoring individual users operation.

One of the methods for achieving the abovesaid goals is monitoring the network operation in such a manner that the monitoring devices “learn” what kind of traffic and behaviour within the network is normal. Such an access uses NBA (Network Behavioural Analysis) technology implemented by Peakflow X device of Arbor Networks company.

2 Arbor Networks Peakflow X

2.1 Arbor Networks

Arbor Networks company is one of the leading global providers of computer network monitoring and protection solutions. Its devices protect from safety threats, such as distributed denial-of-service attacks (DDoS) and botnet network attacks. They are also intended for providing reliability and quality of service. Arbor's clients are large international companies and Internet Service Providers (ISPs).

Arbor is especially proud of their solutions enabling MPLS (Multiprotocol Label Switching) networks and implementation of safety, based on defence from distributed denial-of-service attacks (DDoS). The company offers its users timely information concerning safety and global Internet traffic. That is achieved through a unique ATLAS system (Active Threat Level Analysis System) which monitors traffic from 300 international Internet Service Providers and network operators. Such companies share their network traffic anonymously on an one-hour basis, and the data are aggregated and analysed with the data collected from Arbor sensors, as well as from third parties. The goal is to enable companies to make key decisions concerning network safety, but also concerning the analysis of the market, trends and possible traffic transfer partners. Of course, the system brings data on threats as well, such as malware, exploits, phishing and botnet networks.

2.2 Peakflow X

By its insight into the network traffic and possibilities of detecting safety threats in real time, Arbor Peakflow X solution optimizes network performances and safety within large companies. The device is automatically and constantly “learning” about the behaviour of workstations within the network, i.e. who communicates with whom and how. That enables dealing with different internal and external safety threats, but with normal business operation maintained. The device consists of two types of components - collectors and controllers. The collectors are in charge of collecting traffic that they then send to the controller. The users access the controller's web interface in order to have an insight into the statistics and to be able to perform all other necessary operations.

Apart from the abovesaid, Peakflow X integrates data collected from Arbor's global system ATLAS. The device analyses network flow (Netflow, etc.) traffic in search for anomalies that it detects with the help of its NBA technology. That makes it possible to detect an attack even before signatures (definitions) are available for it. Some of the features of the device are:

- resolving threats and monitoring the network on the second layer, with a possibility of simple removal of problematic workstations from the network, without influencing the operation of other nodes in the network
- risk assessment in real time, i.e. quick assessment of threats within the network which have the largest risk factor (that the device calculates automatically) and which computers and which users are involved in risky activities
- Flexible monitoring of the identity and recording the user activities (login / logoff) and their IP addresses

Arbor also points out that the device can replace the existing solutions for monitoring VPN traffic, as well as solutions based on safety of CPE (customer premises equipment) devices, and it can add new options.

Arbor designed Peakflow X as a device comprising safety management and network operability. From the aspect of safety, the device enables:

- detecting distributed denial-of-service attacks (DDoS), defence against viruses, botnet network, worms and other current threats
- detecting and removing phishing attacks
- adjusting the network in order to prevent future attacks
- managing user access and removing possibility of attacks from within

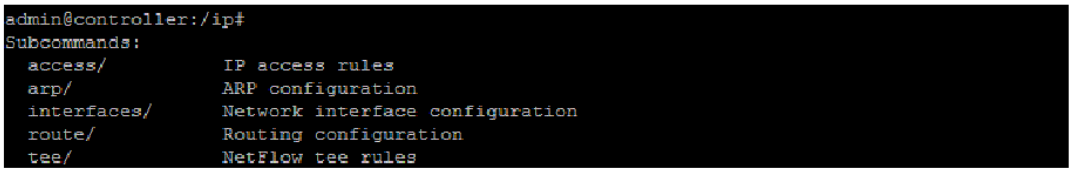
The device is designed to simplify implementation of safety policies and standards, such as PCI DSS, ITIL, ISO 17799 etc., in companies. Apart from a physical device, Arbor also developed Peakflow X as a virtualised solution intended for virtual systems VMware ESX and ESXi. That is the solution we used in our text. Virtualised solution offers the same options as a physical device, naturally, at a more favourable price.

3 Device Interface

Peakflow X system has command line interface (CLI) and Web interface. Basic settings such as network, flow data sources and connection of the collector and controller in Peakflow X virtual system are configured in CLI interface. After initiating the service, Web interface can be used as well.

3.1 Command Line Interface (CLI)

The command line interface of the Peakflow X system provides an insight into the status and modification of the existing configurations of the device. CLI can be accessed via SSH, Telnet, or directly via the console. The interface enables moving through menus and imputing commands. The commands are distributed hierarchically, similarly as in the file system. The root menu is marked by "/". Moving through menus is similar to moving through the file system. Within each menu, we can execute certain commands characteristic for that menu.

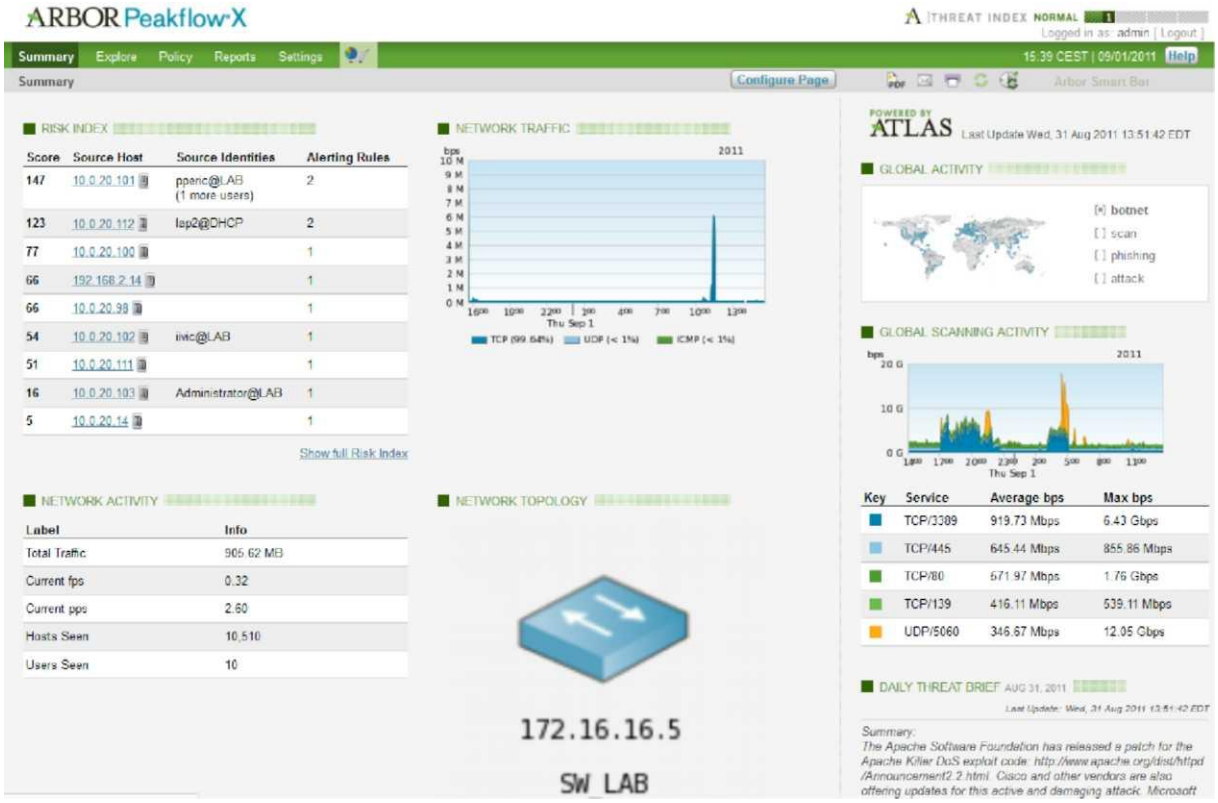


3.1: Appearance of CLI interface

A command shell can operate in two modes: "Edit" marked by "#" and "Disabled" marked by ">". Edit enables all configuration modifications. In case the user logs in as an administrator, the system will initiate the "edit" mode automatically. Disabled mode enables minimum configuration modifications, and it mostly means reading configuration settings. The user without administrator's authorities must enter the Edit mode with the command **edit** ion order to change configuration. The command shell also contains basic functions of other CLI systems, such as automatic ending the command by pressing the "TAB" key, review of options by pressing "?", command help, etc. The configuration is saved to the disk by command **config write.**

3.2 Web interface

The web interface home page is **"Summary",** which contains the overview of the current status in the network, while to the right; it offers certain information that is collected from the ATLAS system. The image displays the appearance of the said page. The page can be configured in the manner that it shows only desired data. Initially, at the top left side there is information about the biggest risks in the network, ranged in accordance with the risk index.



3.2: appearance of the home page ("Summary") of the web interface

Below that, there is information about the total traffic in the network, network topology, and further below there are alerts, generated in the past 24 hours. There are also loads per interface, number and type of generated alerts, some basic information on the controller and collector status, while a system modifications log (audit trail) is at the very bottom. At the top, there is a main menu bar, offering a selection of five options:

- **Summary** (mentioned home page)
- **Explore**
- **Policy**
- **Reports**
- **Settings**

Option Explore offers an insight into traffic (including statistics about clients, servers, services with most traffic, groups, interfaces, QoS, etc.), of the current connection, and risk factors. Under Policy, activities in the network can be observed, according to the severity factor **("severity")** of certain safety threat (it can amount from 1 to 10). It is also possible to

define one's safety policy, i.e. rules **("User-Defined Rules")** that, when met, will lead to alert generation. It is also possible to see a list of installed conduct rules **("Active Threat Feed"),** which includes rules concerning malware detection, attempt to use vulnerabilities, revealing traffic on social networks, IRC, anonymisation networks, etc. Active Threat Feed is upgraded regularly with new definitions of safety threats. There are also five special behaviours categorised under "Builtin Behaviours", representing basic types of threats. They are:

- **Flood** (flooding with TCP, ICMP or IP packages, i.e. denial-of-service attacks)
- **Host Scan** (scanning/detecting computers in the network)
- **Long Lived Sessions** (sessions lasting longer than maximum time they are configured for)
- **Port Scan** (scanning computer ports)
- **Worm** (here it is possible to define services and ports that are ignored in case of detecting a worm within the network)

The Reports part is in charge of scanning the existing reports and generating new ones. Different types of reports can be made based on different network parameters. More about those in the following sections of the document.
Finally, Settings menu is in charge of managing and insight into general settings of the device, such as defining DNS and SMTP servers that will be used, insights into logs of performed changes in the system (audit trail), safety copies, ATF and ATLAS upgrades management, user accounts (including the domain accounts). Basic configurations of groups, services and Time Objects can also be configured from there.

4 Device Configuration

4.1 Basic network settings

After installing Peakflow X virtual systems to VMware ESXi server, network configuration must be performed in the console window, followed by the remaining configuration through CLI.
In the console window, we configure hostname, one network interface (mgtO) and we define networks from which we shall administrate the device.

Peakflow X has 4 virtual network interfaces:

- **mgtO** serves for administering the device or receiving data flow
- **flowO** represents additional interface for receiving data flow
- **pccO** and **peci** are interfaces intended for packet capture.

PCC interfaces are used for monitoring user identity in the network with the help of DHCP or radius. They must be connected in a local network, since Peakflow X requests and maps IP addresses with user IDs based on DHCP and RADIUS. The identity may be monitored by linking with Microsoft AD as well.

```
admin@collector:/# ip interfaces show mgt0
mgt0  Gigabit Ethernet, Interface is UP, mtu 1500
          Hardware: 00:0C:29:7A:3D:E3
          Media: Ethernet autoselect
          Status: 1000Mb/s Full
          Inet: 10.0.14.99 netmask 255.255.255.0 broadcast 10.0.14.255
          Inet6: fe80::20c:29ff:fe7a:3de3 prefixlen 64
          Input: 1062931 pkts, 69643002 bytes, 0 errors
          Output: 1506440 pkts, 1431257361 bytes, 0 errors, 0 collisions
          Interrupts: 2024480
```

4.1: Appearance of network interface mgtO

4.2 Netflow Data Source Configuration

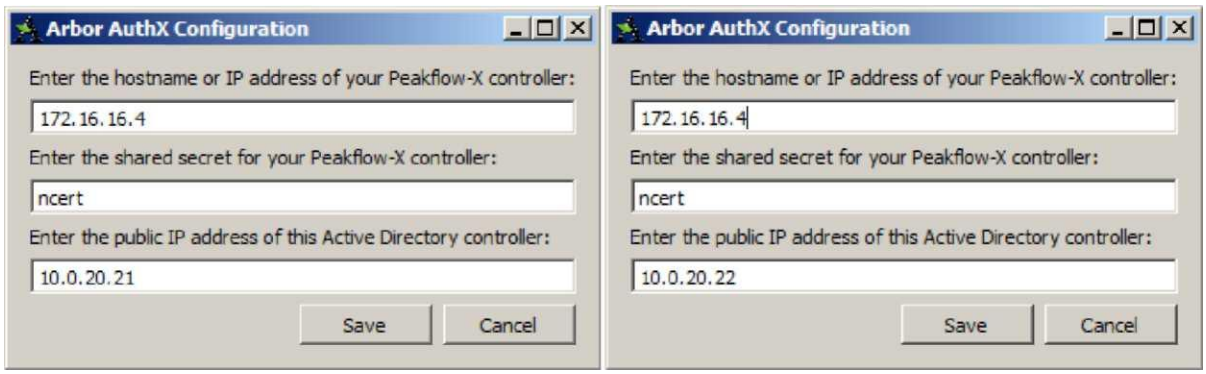
Peakflow X supports three types of "flow" data: NetFlow, cflowd and sFlow. Flow data can be sent directly to the controller. In case of large networks, collectors serve for collecting the data and then sending them to the controller. The number of flow sources depends on the type, i.e. licence of the device we use. In our testing we collect the flow data to the collector flowO interface, and we forward them to the controller flowO interface.

Peakflow X also supports the monitoring of network devices with SNMP protocol. In that manner, we can see the status of individual network interfaces, and in case of using SNMP with read/write rights, we can turn off problematic network interface via the Web interface. After adding, Peakflow X displays hostname and IP address of the device through the Web interface.

4.3 "Identity tracking" software installation

Arbor PX supports user identification by using several different technologies, such as DHCP, Radius, Microsoft Active Directory and Novell eDirectory. In our test environment, Microsoft Active Directory was used.
User identification work on the principle of mapping the user ID with IP address.
In case of using Microsoft AD, it is necessary to install **AuthX** on each domain controller, an agent that uses HTTPS protocol to send information towards Arbor controller.
The installation of the programme is very simple, and out of configuration data, it is necessary to enter IP addresses of Arbor and AD controller and the common key.

4.4 Object configuration



4.2: AuthX configuration dialogue on AD and AD2 servers

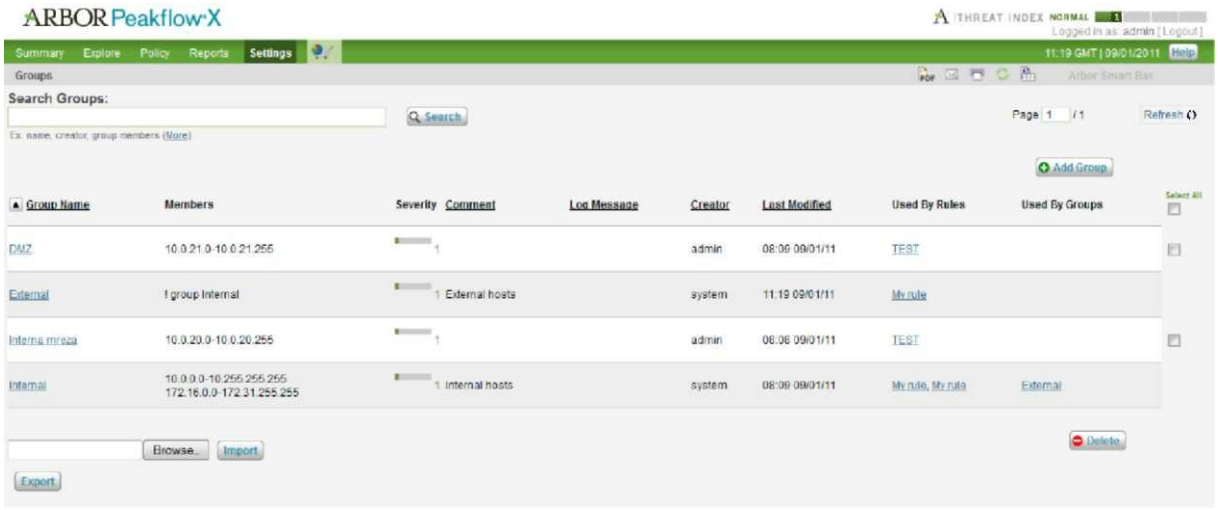
It must be stressed that the software does not support operation by multiple users on the terminal servers, where several users are active on the same IP address.

4.4.1 Groups

As with other devices of similar use, PeakFlow X (under *Settings -> Groups)* offers simple defining of computer groups. They can be identified individually based on IP address, or jointly as a group based on the scope of addresses. A threat severity factor can be defined for each group, from 1 to 10, which is important in case one wished to spot an alert on time, during the attack on the most important resources in the network. When editing the current group, the interface displays all the safety policy rules referring to the said group.

4.4.2 Services

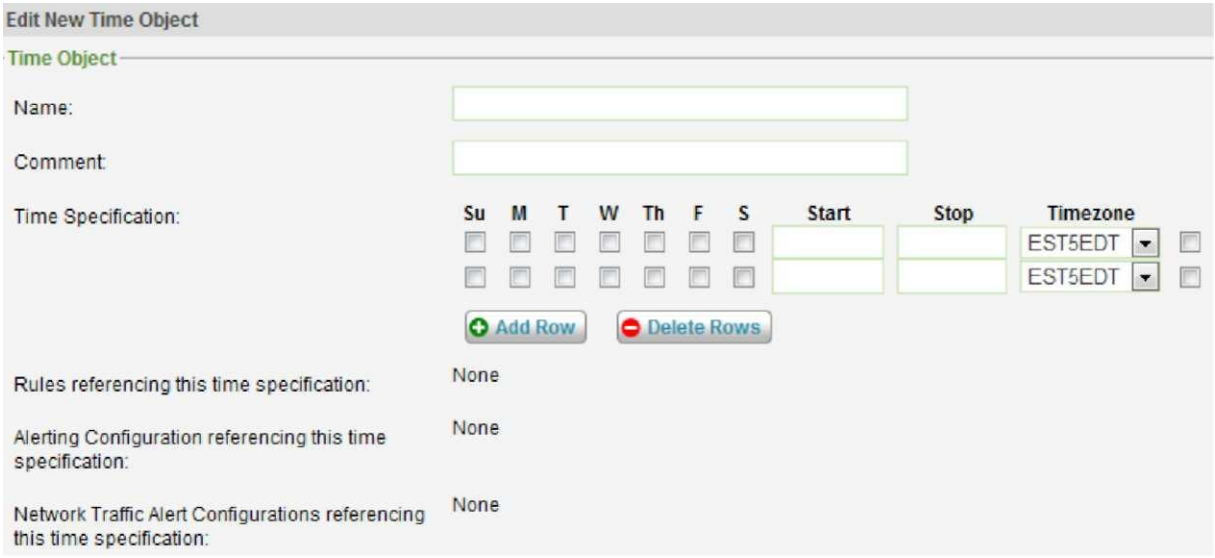
Own services or groups of services can also be defined. They can be defined by the port they use, like some of the standard services, or by the application the device is capable of detecting. For this object, the threat severity factor can be defined as well.



4.3: defining groups

4.4.3 Time objects

Peakflow X offers a simple configuration of time objects that can be defined by individual days of the week and by hours (it is possible to define several different combinations, which are in that case valid at the same time).



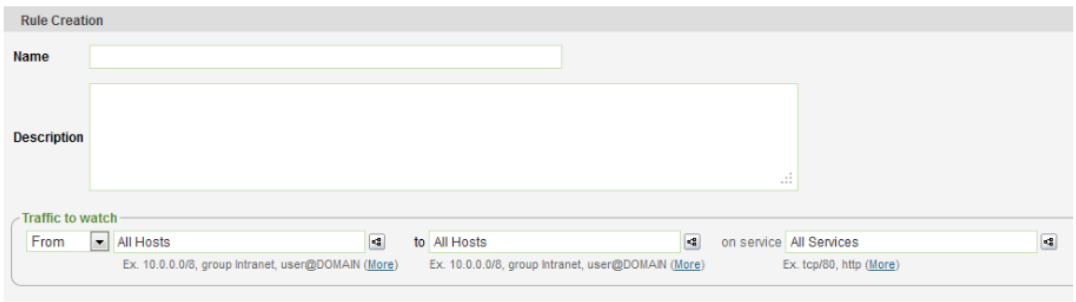
4.4: defining time objects

4.4.4 Notification objects

With the help of Notification objects, the recipient of notifications is defined in case of generating certain alerts. Peakflow X supports sending alerts via electronic mail, SNMP trap or syslogs. Accordingly, when making a new object of this kind, it is possible to define several different e-mail addresses, up to four servers that will receive SNMP messages, and up to four servers that will receive syslog records.

4.5 Defining safety policy rules

Under Policy -> Management -> User-Defined Rules safety policy rules are defined. It must be defined to which traffic the rules will apply (scope of addresses from, to or between entities, i.e. the most common group or users). Types of alerts that will generate the rules are also defined, and when changing the existing rule, it is possible to define (select offered traffic) exceptions as well, for which no alerts will be generated.



4.5: defining new safety policy rule

5 Alerts and drafting reports

Alerts, of course, serve to give timely warning about safety threats and events, such as network nodes crashing or unsuccessful backup. In large networks, it is important to distinguish the importance among various alerts that must be visible, therefore PeakFlow X offers a simple insight into the events causing the generation of alerts. Such events are listed in accordance with the risk safety factor.

Reports serve primarily for observing network operation through a longer period of time. They are usually used by the management or section monitoring the usage of network infrastructure. They are also a big help in the implementation of various safety standards that many companies must observe.

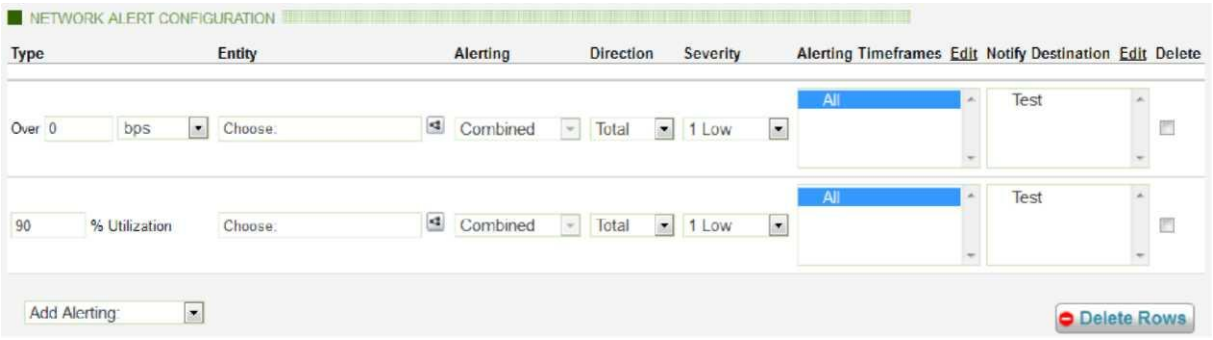
5.1 Alerting

For each behaviour in the network that PeakFlow X may detect, it is possible to define the event (if it is within the object-defined time interval and/or group) that will cause the system to generate a certain Alert Type. Some of the alert types are as follows (each type is displayed by a separate icon within the interface):

- **Client** - generated when detecting a computer that has not been noticed before within a certain network traffic (group)
- **Server** - generated when detecting a new server
- **Connection** - any connection that does not observe the defined safety policy
- **Over / Under Rate** - traffic is in the period exceeding two minutes above or below the configured value
- **Over / Under Baseline** - traffic is in the defined period above or below baseline[1] value
- **Host Pair** - traffic between two computers that has not been seen before within the monitored group

There are also special types of alerts for system events, such as: fall of collectors or lifting collectors, flow data source, etc. They can be configured under *Policy-> Management -> System Events.* There are also network alerts that can be configured under *Policy -> NetworkAlerts.* They are alerts used for monitoring the status of network traffic for certain routers, interfaces and groups of interfaces. When such traffic is above or below the configured value, Peakflow X generated alerts. That value can be defined according to the percentage of used interface bandwidth maximum.

[1] it is a value that clearly differs from the value the device “learnt” in the period of at least a week, during which time it monitored the network traffic



5.1: configuring new network alert

The above mentioned *Activity* page of the interface *[Policy -> Activity)* serves primarily for monitoring the current status of the network. The status can be monitored through events that led to alerts generation, through events that do not generate alerts, through an alert generated by the AFT system, based on alerts that occurred as a result of violating safety policy rules or through alerts that occurred as a result of violating the rules defined by the user (currently logged in).

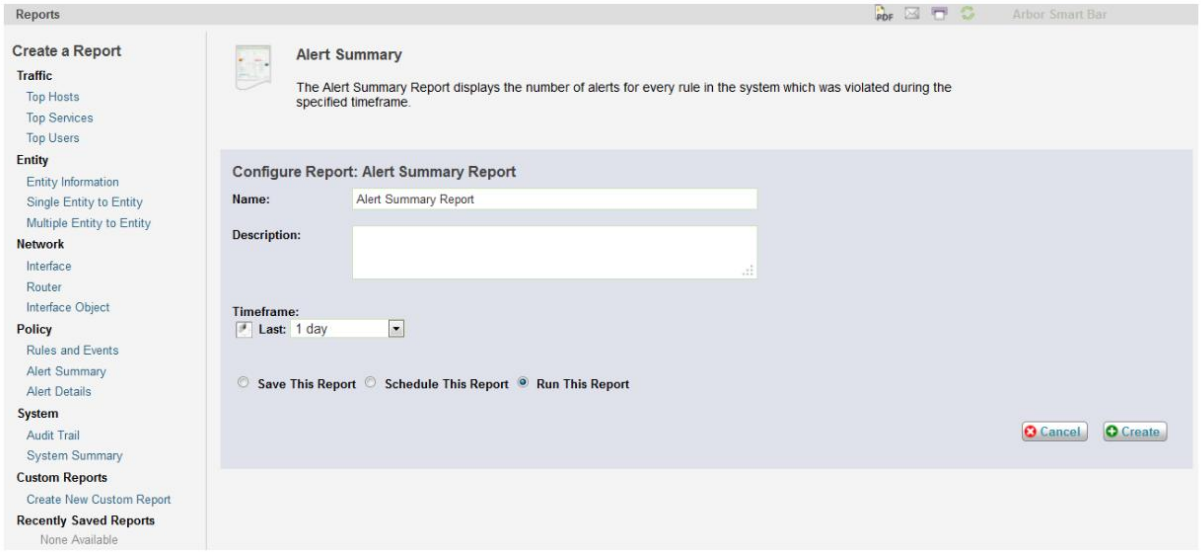
Severity	Behavior	Creator	Traffic Over 24h	Approved Traffic (Avg / Max)	Unapproved Traffic (Avg / Max)	Alerts (1)	First Alert	Last Alert
10	Phishing Hosting Server Traffic Identification	ATF		0 bps / 0 bps	0 bps / 0 bps	2 clients	N/A	2 days 18h04m
7	ICMP ping flood to 10.0.21.61	system		0 bps / 0 bps	2.43 Mbps / 3.04 Mbps	100000 clients	N/A	Ongoing
7	US Embargoed Nation(s) Traffic Identification: Iran	ATF		0 bps / 0 bps	0.84 bps / 2.24 bps	1 client	N/A	0h47m
7	US Embargoed Nation(s) Traffic Identification: Syria	ATF		0 bps / 0 bps	2.24 bps / 2.24 bps	1 client	N/A	0h47m
7	US Embargoed Nation(s) Traffic Identification: Libya	ATF		0 bps / 0 bps	0.75 bps / 0.75 bps	1 client	N/A	0h10m
6	Host Scans	system		0 bps / 0 bps	252.41 kbps / 408.44 kbps	1 client, 1 service, 1 connection	N/A	Ongoing
5	Flood test	admin		0 bps / 0 bps	1.60 Mbps / 8.32 Mbps	3 high bandwidth	N/A	0h40m
5	The Onion Routing (TOR) Traffic Identification	ATF		0 bps / 0 bps	643.65 bps / 95.10 kbps	3 clients	N/A	23h01m
5	Port Scans	system		0 bps / 0 bps	17.09 bps / 4.92 kbps	6 clients, 6 connections	N/A	1h32m
5	Dark IP Traffic	ATF		0 bps / 0 bps	13.87 bps / 56.64 bps	1 client	N/A	0h46m
3	TEST	admin		0 bps / 0 bps	8.01 bps / 942.27 bps	4 clients	N/A	1h39m
1	Long Lived Sessions	system		0 bps / 0 bps	1.06 bps / 154.03 bps		Never	Never

5.2: list of generated alerts (Activity)

On the smaller graphic display, traffic can be observed in the past 24 hours, and apart from other information, the amounts of the approved traffic are also visible (through defined exceptions in rules), as well as traffic that has not been approved.

5.2 Reports

In order to monitor the manner the network infrastructure is used in, Peakflow X enables preparing reports from the data the device collects all the time. There is a special part in the web interface menu for that purpose, under a shortcut *"Reports"*.

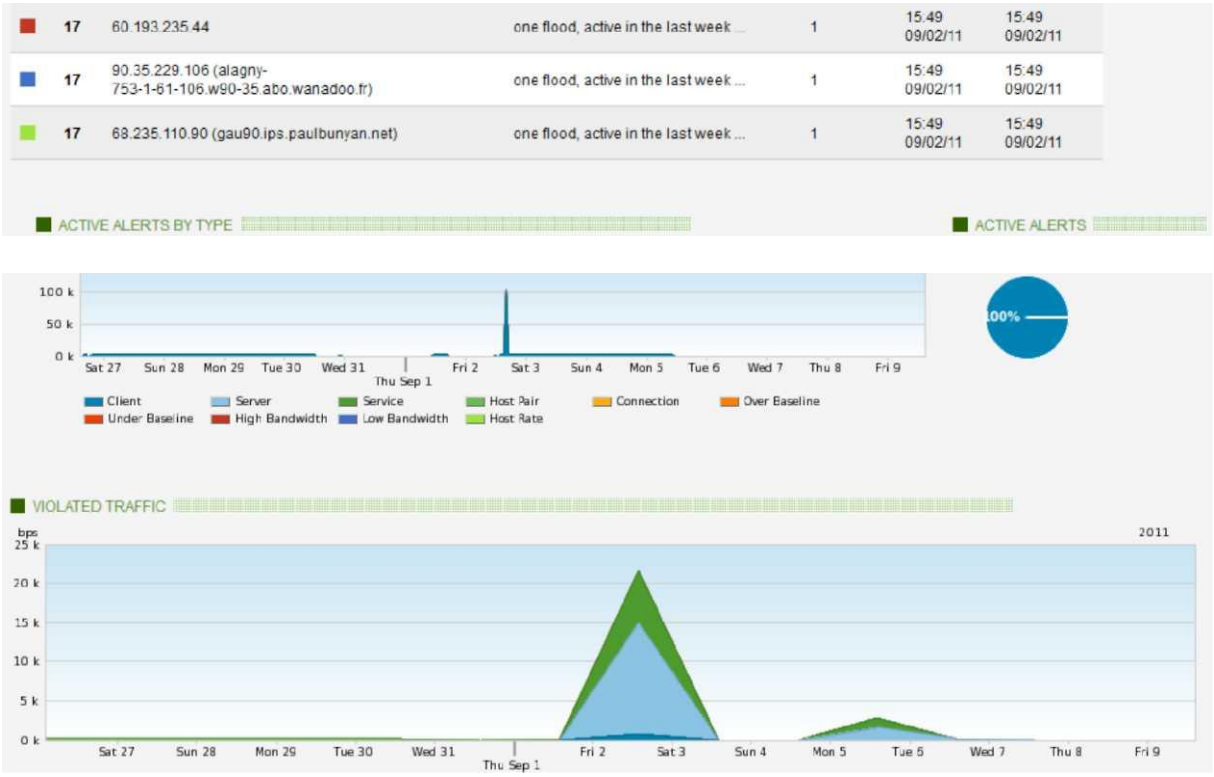


5.3: new report drafting

It is possible to draft various types of reports (which is visible on the menu on the image, to the right): per computers, services, servers, entities (that can be a computer, user, server, service, etc.), web traffic, visited URLs, interfaces, routers, braking safety rules, generated alerts, etc. It is necessary to define the time frame to be considered for all mentioned types of reports. When defining an entity, the device is searching the traffic in the following order:

1. IP addresses
2. CIDR blocks of IP addresses
3. names of computers
4. names of groups

Reports can be generated instantly, configured in advance (and draw up later on) or their automatic, time-defined generation can be set up *("Scheduled Reports").* In case the last option is used, the reports can be forwarded automatically, via e-mail to defined recipients (listed within the selected notification object). They can be made in three different formats: PDF, XLS or CSV. Ordinary users may review all reports, but the reports can be deleted only by the users who made them. The system keeps the reports for a year, and deletes them after that period. In case we wish to find one of the existing reports, there is an option, i.e. field *"Search Recent Reports".* Reports can be searched by ID, title or name of the user who had it generated.



5.4: excerpt from report sample

As can be seen, the manufacturer paid special attention to the reports, which is not surprising considering their multiple use in a company.

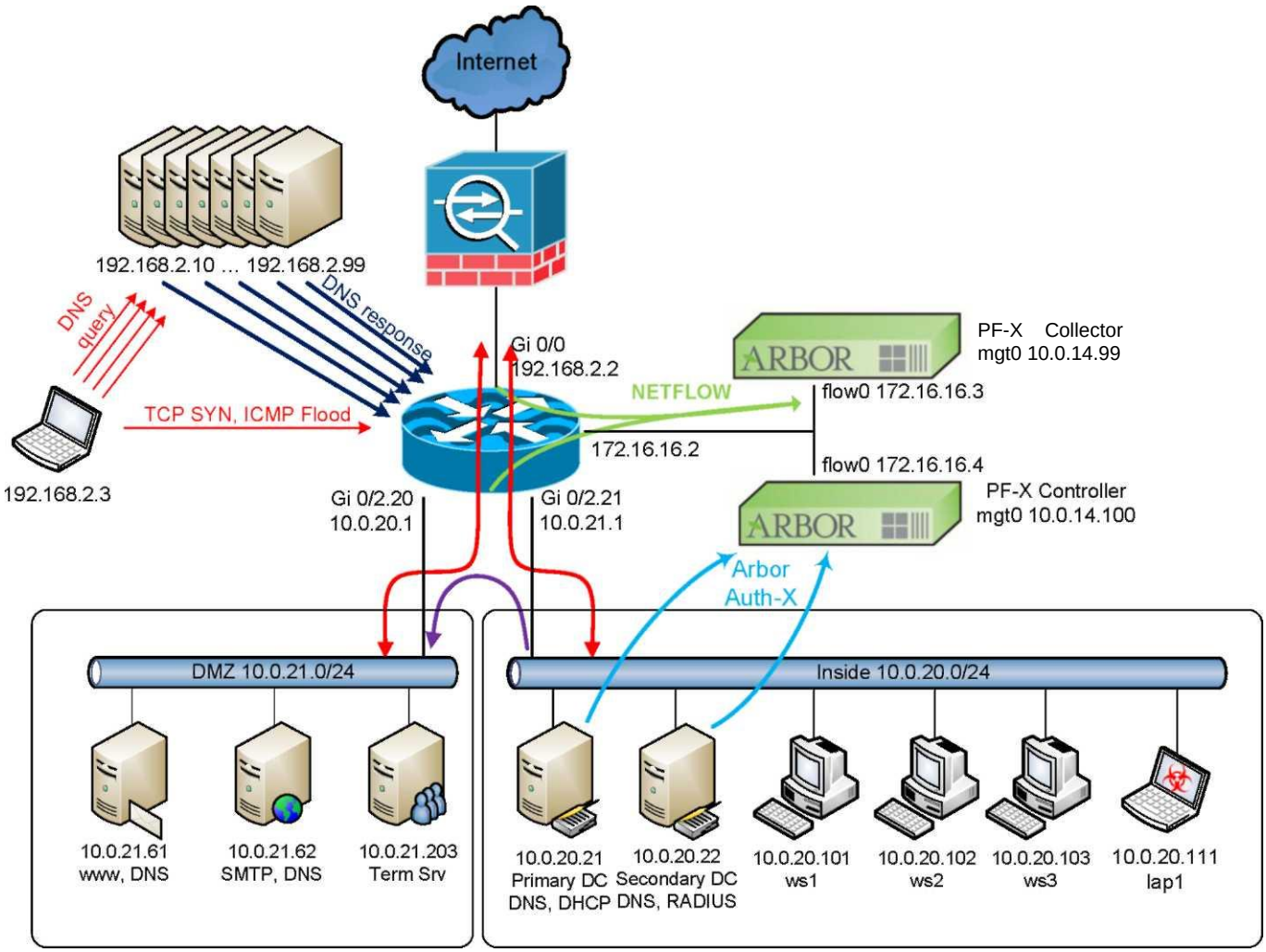
6 Testing

Concerning testing Arbor Peakflow X device, it is important to stress that the focus of this test was on testing the abilities of the device from the aspect of safety, and not from the aspect of monitoring the operability of the computer network.

6.1 Network and configuration test

Image 6.1 displays the topology of the network used when testing the device. Two networks have been configured: internal with the scope of IP address of 10.0.21.0/24, and DMZ with the scope of 10.0.20.0/24. Internal network holds workstations and two Microsoft Active Directory servers (AD1 and AD2), and in DMZ web and mail server and Terminal Server. For performing the test, Cisco 2911 router was used, which sends NetFlow data of version 5. Peakflow X is otherwise supported by NetFlow version 1, 5, 7 and 9. The router is configured in such a manner to collect Netflow from interface Gi 0/2.20, Gi 0/2.21 and Gi 0/0.

The management of interfaces on Peakflow X virtual devices (mgtO) are configured per documentation and IP addresses 10.0.14.99 (collector) and 10.0.14.100 (controller) are assigned to them. Interfaces for Netflow traffic (flowO) are connected to a separate network. The collector accepts Netflow traffic from the router (IP 172.16.16.2) on IP address 172.16.16.3, and after processing and conversion into Arborflow format, sends it to the controller to IP 172.16.16.4.



6.1 : topology of tested networks

Arbor PF-X client software was installed on both domain controllers and it sends to the controller the user names logged on individual computers, i.e. IP addresses. That enables monitoring the activities of individual users, regardless of the computer they are logged on.

6.2 Simulation of users in internet network

For the purpose of this test, several user accounts have been created on the domain controller. User workstations were simulated in the test for the usual office traffic, i.e. they were used for viewing the web portal, downloading files via HTTP and FTP, etc.

6.3 Detecting applications

Under *Policy-> Management,* there is a list of predefined safety policy rules. Among them, there are rules that enable detection of individual applications. We tested detection of Bittorent traffic and Facebook applications.

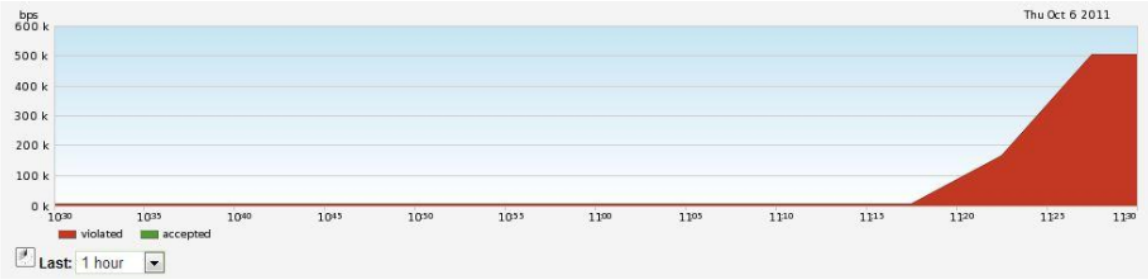
6.3.1 BitTorrent

As listed in the description of rules, the device detects familiar BitTorrent ports (TCP 68816889). It then detects "peer" computers as clients, servers or both. During the test, the device successfully detected a computer using bittorrent and compiled a list of peer/seed computers from where BitTorrent communication had been established.

Severity	Client	Client Interface	Num Servers	Num Servic
5	10.0.20.112	arbor-test (172.16.16.2): arborPX - interna mreza Gi0/2.20 GigabitEthernet0/2.20	713	564
5	173.255.125.116 (116.125.255.173.bc.googleusercontent.com)	arbor-test (172.16.16.2): up-link Gi0/0 GigabitEthernet0/0	1	1
5	85.60.124.237 (237.pool85-60-124.dynamic.orange.es)	arbor-test (172.16.16.2): up-link Gi0/0 GigabitEthernet0/0	1	6
5	208.64.36.69	arbor-test (172.16.16.2): up-link Gi0/0 GigabitEthernet0/0	1	3
5	195.222.89.198 (ppp-195-222-89-198.pe1-dynamic.solo.hr)	arbor-test (172.16.16.2): up-link	1	2

6.2: computer in a local network and other peer computers

As well as for other rules, time frames can be defined when usage is enabled (pause, outside working hours) and services and networks for which we wish the device to generate alerts can be defined.



6.3: display of BitTorrent traffic

6.3.2 Facebook

The device checks HTTP and HTTPS traffic towards Facebook networks after ASN number (autonomous system) 32934. In the description of safety policy, a list of Facebook IP addresses (networks) is given, in case traffic towards them wishes to be blocked manually on the firewall, etc.

Trigger

This policy looks for HTTP and HTTPS traffic destined to the Facebook network in ASN 32934.

Affected Platforms and Versions

Any computer with a web browser can be used to access the Facebook website.

Remediation

A number of third party products are able to block Facebook access via DNS and other means.

Workaround

We recommend blocking the known Facebook IP address ranges to prevent login and website use. These address ranges are: 66.220.144.0/20,69.63.176.0/20,74.119.76.0/22, and 204.15.20.0/22.

General References

Date	Organization	Author	E-mail Address	Title
2008-07-08	Facebook			Facebook website

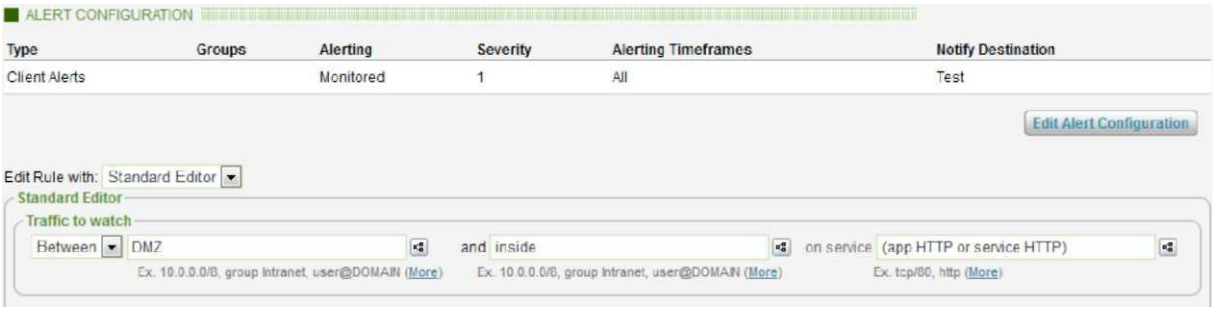
Revision History

5 - Fix spelling typo, add note about Koobface Trojan.
6 - Add support for new Facebook CDN routes in AS32934.
7 - Update BGP routes.

6.4: part of description of predefined rule enables detection of Facebook application

6.4 Detecting new clients in the network

A rule for detecting new users of the HTTP service within DMZ network has been detected:



6.5: rule for detecting new users

Each time a new user connects from the internal network to a web server, administrators receive an e-mail with an alert and link to more detailed information on the incident, such as:

Excerpt from the received e-mail:

```
------------------------------
Type:     Unapproved Client
Rule:     TEST
URL:       https://controller.lab.cert.hr/event_detail/alertdetail/?type
search_text=client+10.0.20.21&id=233
Severity: 1
Client:   10.0.20.21
Server:   10.0.21.61
Service:  TCP/80
```

Detailed display in web interface of Peakflow X controller, shown in image 6.6.:

6.6: alert about new user in the network

6.5 Port Scan

Port scan of mail servers within DMZ was initiated from the computer in an external network. Soon, an alert appeared on the controller's web interface about the recorded port scan in progress.

6.7: port scan alert

More detailed display of recorded scanning within web interface is shown on the image below:

6.8: port scan details

6.6 Denial of Service attacks

Since viruses are used in further tests, as well as spoofed source addresses of packages, the tests were, for safety reasons, performed completely disconnected from the Internet. Otherwise, a virus could be spread, information could leak, or unwanted packages could be sent outside the network, as an

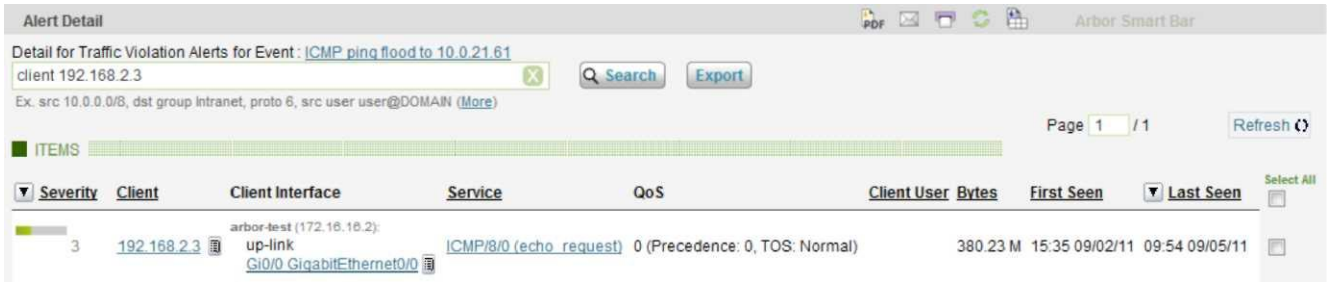
answer to the spoofed incoming packages.

6.6.1 Ping Flood

An ICMP flood attack was initiated from a laptop computer in an external network, first without using cover-up techniques, then with spoofed source addresses. Some of randomly generated addresses were from IP areas of the sanctioned countries, and special alerts were generated for them (image 6.10).

Excerpt from the received e-mail:

```
Type:      Static High Bandwidth
Rule:      Flood test
URL:       https://controller.lab.cert.hr/event_detail/alertdetail/?id=234&
type=4&units=0
Severity: 5
Expected: 1.00 Mbps
Actual:    4.85 Mbps
```



6.9: alert about ICMP Flood attack

6.10: alert about ICMP Flood attack with forged IP addresses

Since the attack was simulated through a gigabit link without limiting the bandwidth, about 25000 ICMP echo requests were generated every second. PeakFlow-X Virtual license limits the number of netflow records that may be processed per second to 16000 (HW appliance can process 32000 records per second).

6.11: alert about neglected Netflow traffic

6.6.2 “DNS Amplification” attack

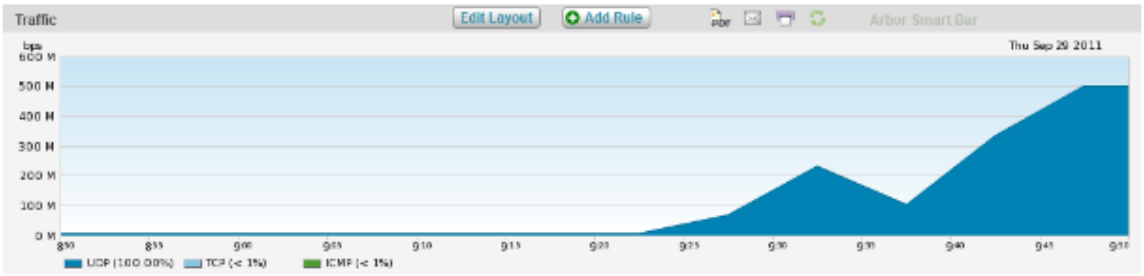
From the computer in the external network, a large number of DNS requests was generated towards open DNS servers. And the original address was spoofed in order to send all DNS server responses to the attack target, in our case to the web server on IP address 10.0.21.61. In order to increase the effect of the attack, requests are set for the domain with great textual (TXT) records, which increases the amount of each individual response manifold.

Incoming traffic on server 10.0.21.61:

No.	Time	Source	Destination	Protocol	Info
15	1.872734	192.168.2.24	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT
16	1.872737	192.168.2.25	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT
17	1.872740	192.168.2.26	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT
18	1.872744	192.168.2.27	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT
19	1.872840	192.168.2.28	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT

6.12: incoming packages on web server

Traffic overview on server 10.0.21.61:

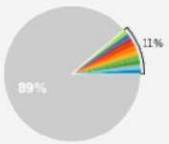


6.13: review of amount of traffic on external interface of the router

Review of *“Top Connections”* gives a detailed display of 10 connections with the largest traffic. As traffic comes from 90 DNS server, each server generates approximately 1.1% of the total traffic.

TOP CONNECTIONS

Key	Client	Server	Service	Bytes	bps	% total bps	Packets	pps	Flows	fps
	192.168.2.73	10.0.21.61	UDP/53 (DNS)	300.67 M	3.08 Mbps	1.1%	593.04 k	760.30	11	0.01
	192.168.2.63	10.0.21.61	UDP/53 (DNS)	300.67 M	3.08 Mbps	1.1%	593.03 k	760.29	11	0.01
	192.168.2.15	10.0.21.61	UDP/53 (DNS)	300.66 M	3.08 Mbps	1.1%	593.02 k	760.28	11	0.01
	192.168.2.84	10.0.21.61	UDP/53 (DNS)	300.66 M	3.08 Mbps	1.1%	593.02 k	760.28	11	0.01
	192.168.2.36	10.0.21.61	UDP/53 (DNS)	300.66 M	3.08 Mbps	1.1%	593.02 k	760.28	11	0.01
	192.168.2.19	10.0.21.61	UDP/53 (DNS)	300.66 M	3.08 Mbps	1.1%	593.02 k	760.28	11	0.01



6.14: review of connections with the largest traffic

6.7 Malware occurrence and spreading in internal network

Peakflow X has predefined safety policy rules that should recognize malware activity and prevent further damage. Some of famous malwares for which rules exist are SpyEye, Zeus and Stuxnet. Malware activity is recognised based on communication with the control (C&C) servers and specific computers on the Internet. The following tests were performed separately from the Internet for safety reasons. Since most malwares check the connection to the Internet before communicating with the

control servers, we were not able to check this functionality in more detail.

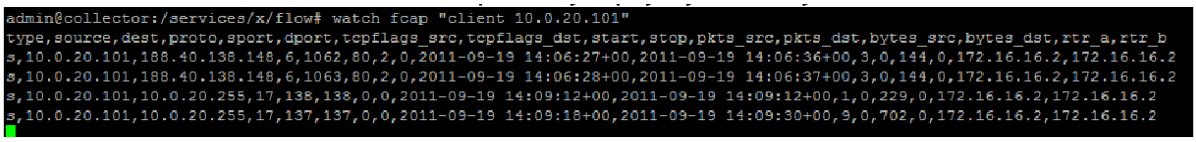
In order to obtain the display of the malware behaviour as accurate as possible, the tests have been implemented in several iterations, and servers which malware tried to access were added manually (actual IP addresses were added, received from DNS requests in a given moment) for each iteration on local DNS servers (AD, AD2). In that manner, malware samples were enabled to at least attempt to connect to the Internet, which is clear from the router, and in Netflow records.

6.7.1 SpyEye

At the end of 2009, a new type of malware was detected, similar to the infamous banking Trojan horse Zeus. It is SpyEye, a malware designed specifically for steeling Internet banking data. The malware author, i.e. organisation behind it, sells a toolkit (SpyEye builder) on the black market, for constructing a malware which technically less skilled criminals then share in order to infect as many computers as possible, and in that manner gain as much financial benefit as possible. The infected computer than becomes a part of the botnet network which is controlled via the control servers. Accordingly, after the malware has been installed on the computer, it first sends a DNS request for one of its control servers in order to connect, i.e. in order to be ready for receiving commands.
By analysing the network traffic with network programme Wireshark, it is clear that DNS request for server xiti.42t.com was sent, and that an attempt has been made to connect to the accompanying IP address.

6.15: attempt to connect to the control server [image for Wireshark tools]

It is also visible on the collector that there was an attempt to connect to the external IP address 188.40.138



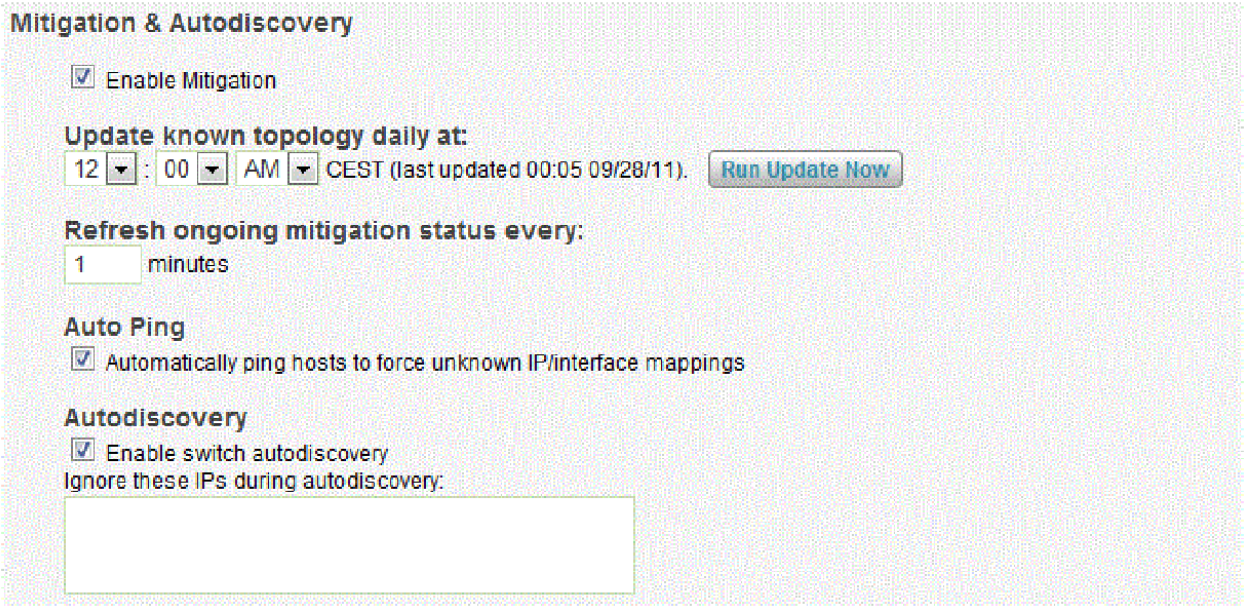
6.16: collector also sees the attempt to connect to the control server

Since the tests were performed when disconnected from the Internet, the connection could not have been established, and PeakFlow in such circumstances does not detect SpyEye.

6.8 SNMP mitigation

Peakflow X enables us to monitor and configure interfaces of the network devices via SNMP protocol. In that manner, an insight is obtained into the load and status of individual interfaces. Problematic interfaces can be turned off through the web interface.

New devices can be added manually or we can initiate the function *"Autodiscovery"* which successfully finds all network devices that have SNMP settings set correctly.



6.17: defining automatic detecting of network devices

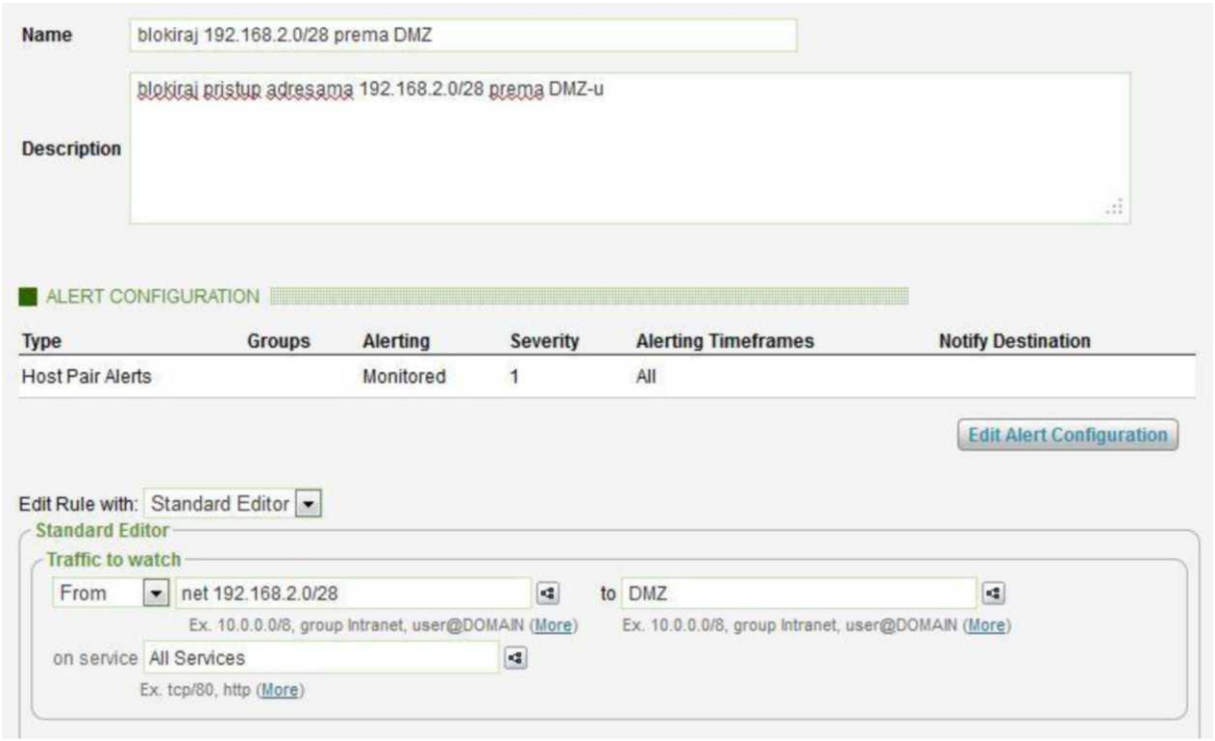
We used router Cisco 2911 and switch Cisco 3560 in the test. We added one manually, while the other was found by the device alone, using the "autodiscovery" function. For L3 interfaces, Arbor PX successfully recognized problematic IP addresses on several occasions, and it offered an option of shutting down the interface through which problematic traffic was passing.

Interface Name	Description	Attached MAC	Attached IP	Status	
Ba0/3	Backplane-GigabitEthernet0/3 50:3d:e5:7f:45:2b	Unknown	Unknown	Enabled	
Gi0/0	GigabitEthernet0/0 50:3d:e5:7f:45:28	00:0c:29:23:2d:ea VMware, Inc.	192.168.2.9	Enabled	Disable
Gi0/1	GigabitEthernet0/1 50:3d:e5:7f:45:29	50:3d:e5:7f:45:29	172.16.16.2	Enabled	Disable
Gi0/2	GigabitEthernet0/2 50:3d:e5:7f:45:2a	Unknown	Unknown	Enabled	

6.18: found interfaces on various devices

6.9 Access Control List (ACL)

A useful characteristic of the device is that it creates access lists (ACL) concerning the safety policy rules automatically. Such lists provide the network devices administrators with simple implementation of the safety policy, by using a “copy-paste” method.
In the test, we created a new rule that we wish to use to prevent network 192.168.2.0/28 from accessing DMZ.

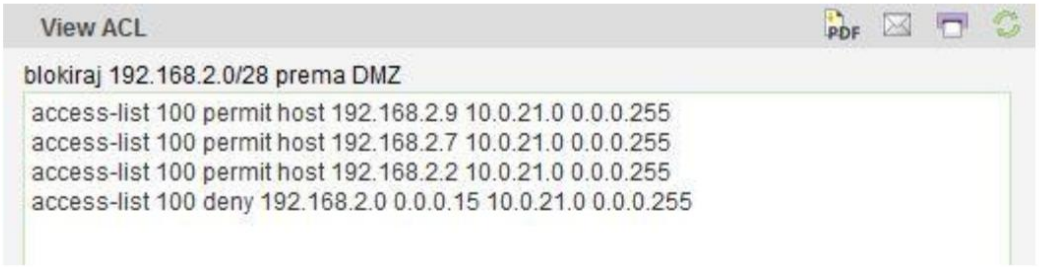


6.19: new safety policy rule

When a new rule is defined, we can exclude some computers from the rule and indicate their traffic only as legitimate.

6.20: computers we wish to enable access to the network to

Access lists are created automatically based on our defined rules. We can see it by clicking *"View ACL"*. The access list can be modified by adding and deleting computers or networks whose traffic we wish to indicate as legitimate.



6.21: example of automatically generated ACL list

7 Conclusion

The network traffic amount and the number of used services within large business environment is growing more and more quickly. On the other hand, safety threats are becoming more and more complex. So complex, in fact, that they cannot be precisely described without expert technical knowledge of the environment. From the aspect of informational safety, the focus, therefore, shifts from protecting the most important resources to the possibility of extracting individual and significant information about threats. NBA (Network Behavioral Analysis) technology implemented by Peakflow X enables us to do just that. Moreover, Arbor, through its global system ATLAS, provides an insight into networkand makes it easier for the users to implement necessary safety measures for threats that have, at that moment, occurred on the other side of the world. Since safety threats within a global network nowadays cannot be observed in isolation, Arbor meets the trend with the abovesaid system.

The possibilities that Peakflow X offers concerning network monitoring are exceptional. Network traffic can, in that manner, be monitored per interfaces, services (applications and ports), users, amount of traffic, etc. The device generates warnings in case of violation of the predefined rules or rules created by the user. A very convenient option is also a possibility to define the severity factor within various parameters, which facilitates disclosure of misuse, i.e. safety threats that attack one of important resources in the network. After two weeks of use, the device sets up to normal values of various network traffic parameters, with the help of its “learning” techniques, in order to be able to exclude unusual behaviour within the network it monitors. During testing, the device correctly detected the use of applications such as Facebook and BitTorrent. It also detected new users within the network, as well as different forms of denial-of-service attack (DoS). Through the installed definitions of malware and its ATLAS system, the device is able to detect various forms of malware; however, it was not possible to inspect it fully in this test. The options of monitoring and managing network devices via SNMP protocol and the option of defining ACL lists are also useful. Peakflow X also enables automated drafting of reports (as well as their drafting upon request) pursuant to a wide range of parameters.

Peakflow X displayed how, with the help of one network device, safety risk for the entire network can be assessed on time, and how necessary information can be obtained for preventing possible misuse, whether it originates from without or within.