NetFlow Based Network Protection

Vojtech Krmicek[1] and Jan Vykopal[2]

[1] Faculty of Informatics, Masaryk University, Brno, Czech Republic
vojtec@ics.muni.cz

[2] Institute of Computer Science, Masaryk University, Brno, Czech Republic
vykopal@ics.muni.cz

Abstract. Protecting network perimeter against adversaries both from inside and outside is a crucial task for nowadays network administrators. Inspecting all network traffic by traditional deep packet inspection is very resource intensive task in high speed networks and scalable solutions are needed. In our work, we describe network protection system based on NetFlow data. It uses hardware accelerated monitoring center (HAMOC) for inspecting network traffic, generating NetFlow data and also for active filtration/blocking of malicious traffic. Active network protection use case against brute force dictionary attacks is presented and also other network protection use cases are discussed. Main contribution of this work are: (i) scalable solution suitable for current high-speed networks (10 Gbps and more), (ii) use of hadrware accelerated HAMOC platform performing both monitoring and traffic filtering, (iii) light-weight alternative using software tools instead of hardware platform suitable for protection of networks with lower amount of traffic.

Keywords: active network defense, NetFlow, flow monitoring, HAMOC.

1 Motivation

Information and communication infrastructure is an integral part of nowadays IT world and provides a wide set of crucial services used in everyday life. Therefore it is necessary to use, study and develop new technologies securing this infrastructure, especially against frequent network attacks from Internet world. Such technologies include firewalls, intrusion detection/prevention systems, vulnerability scanners, network access control systems, honeypots, etc. Although it is necessary to provide security also inside monitored network, we will focus on securing observed network against network threats from outside in the following.

Network-based intrusion detection and prevention systems are deployed to serve for this purpose. The malicious traffic is traditionally detected by deep packet inspection: the payload is searched for signatures of known attacks. However, this is very resource-intensive task and scalability is a growing problem in present large and multigigabit networks. On the contrary, intrusion detection based on an analysis of network flows scales well and is capable to capture some kinds of attacks [3]. So we are focused on research of NetFlow monitoring and intrusion prevention.

M. Rajarajan et al. (Eds.): SecureComm 2011, LNICST 96, pp. 543–546, 2012.

2 Used Technologies

2.1 NetFlow Monitoring

A network flow (NetFlow) is defined as unidirectional sequence of packets with some common properties that pass through a network device, e. g., IP addresses, protocol and ports [2]. These flow statistics were originally generated by routers and switches for accounting and management purposes only. Nowadays there are many network devices (including stand-alone probes) exporting NetFlow for network behaviour analysis and anomaly detection too. Using flow-based approach the detection is feasible even in 10 gigabit networks without any packet loss because the flow exporting process inspects only packet headers, not the entire payload. In our experience of deploying and running many NetFlow probes at campus network, NetFlow monitoring is very usable and powerful tool.

2.2 Hardware-Accelerated Monitoring Center

In our work, we use *Hardware-Accelerated Monitoring Center* (HAMOC) platform [1] to perform both network traffic monitoring (NetFlow/IPFIX acquisition and deep packet inspection) and network traffic filtering at high speed networks (10 Gbps). This platform provides hardware acceleration to already available and well-known monitoring applications.

The HAMOC is based on commodity PC platform. The lack of computing power for high-speed network applications is solved by COMBO hardware accelerator performing time critical operations. Used FPGA technology enables flexible firmware changes according to specific demands in particular tasks.

A set of network monitoring tools was tuned and tested with HAMOC platform to be able to proceed 10 Gb/s traffic at line rate, including traffic analysis tools (*tcpdump, tcpreplay, Wireshark*) and deep packet inspection tools (*Snort, Bro, Sucirata, OpenDPI*). The HAMOC platform provides also filtration capability with possibility to change filtration rules without packet loss and traffic distribution among multiple processors to increase computational power.

2.3 Light-Weighted Alternative

An alternative suitable for deployment in the lower speed networks (up to 1 Gb/s) is a usage of software probe (*fProbe*[1], *nProbe*[2]) for NetFlow acquisition and Linux *iptables* as traffic blocking tool instead of hardware platform HAMOC. This software variant is also able to protect observed network against network threats, but it is limited by various factors, e.g., incomplete traffic statistics during heavy attacks ((D)DoS) and inaccurate timestamps of network flows.

[1] http://fprobe.sourceforge.net/

[2] http://www.ntop.org/nProbe.html

3 Active Network Protection Scenarios

NetFlow based network protection can be built up from various components. In our research we focus on the following scenarios:

1. NetFlow probe(s) + collector + RTBH – Several probes exports NetFlow to the central collector where the analysis is done, the detection module can set *Remotely Triggered Black Hole Filtering* (RTBH) [4] at routers.
2. HAMOC running NetFlow probe and firewall – NetFlow acquisition, storage and detection as well as attack prevention is done at the HAMOC center.
3. HAMOC running quarantine – To protect users from phishing, all traffic destined to the known phishing websites is redirected to quarantine by HTTP proxy running at the HAMOC center.
4. HAMOC running NetFlow probe, collector and attack tools – Similar to the second scenario, but HAMOC is capable of conducting a counterattack.
5. HAMOC running NetFlow probe, collector and traffic limiter – Similar to the second scenario, but HAMOC is capable of limiting traffic incoming from the attack source.

The second scenario is described in a detail in the following section.

4 Use Case: Active Protection against Network Attacks

One of a possible application of the HAMOC platform is a network protection against various types of network threats and attacks. HAMOC is deployed as a NetFlow probe and packet filter (see Figure 1) at the borders of network. Acquired NetFlow data are sent to the NetFlow collector where are stored and analyzed by a detection tool. If an attack is found, the detection tool sends an event to the control center. The center assesses the severity of the event and issues a command to the packet filter running in HAMOC.

An example scenario of network protection against SSH brute-force attack follows:

1. the attacker probes the protected network for SSH servers by TCP SYN scanning,
2. the attacker starts brute-force attack against the SSH service running at the hosts that responded in the previous step,
3. TCP SYN scans and the brute-force attack are found by detection tool (plugin for the NetFlow collector), which processed acquired NetFlow data; these events are sent to the control center,
4. the control center processes the events, and as a result, instruments HAMOC to block all TCP traffic from the attacker's IP address to the TCP/22 port in the protected network,
5. the attacker continues with the brute-force attack but all SSH packets incoming to the protected network are dropped.

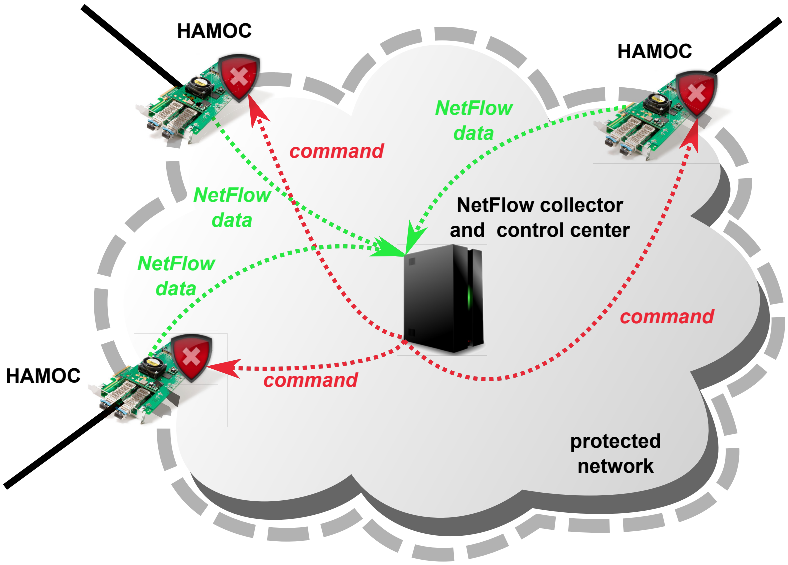

Fig. 1. NetFlow based network protection using HAMOC platform

5 Conclusion

In this work, we have presented NetFlow based active network protection. Network protection system was implemented in high-speed networks by using NetFlow monitoring and hardware accelerated monitoring center (HAMOC). Current work is focused on detailed system evaluation in both laboratory testbed and real network. The quality of network protection, system performance during heavy attacks and protection against new network threats are subjects of future research.

References

[1] Celeda, P., Krejci, R., Bariencik, J., Elich, M., Krmicek, V.: Cesnet technical report 9/2010 (2010), `http://www.cesnet.cz/doc/techzpravy/2010/hamoc/`

[2] Claise, B.: Cisco Systems NetFlow Services Export Version 9. RFC 3954 (Informational) (October 2004), `http://www.ietf.org/rfc/rfc3954.txt`

[3] Sperotto, A., Schaffrath, G., Sadre, R., Morariu, C., Pras, A., Stiller, B.: An Overview of IP Flow-Based Intrusion Detection. IEEE Communications Surveys & Tutorials 12(3), 343–356 (2010), `http://doc.utwente.nl/72752/`

[4] Cisco Systems. Remotely triggered black hole filtering, Whitepaper (2005), `http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd80313fac.pdf`