Improvement of Network in an Educational Institution According to Demands of Industry 4.0

Bertalan Beszédes[1], György Molnár[1], Attila Sáfár[1]
1 Óbuda University, Alba Regia Technical Faculty, Budai Str. 45, H-8000 Székesfehérvár
{beszedes.bertalan, molnar.gyorgy, safar.attila}@amk.uni-obuda.hu

***Abstract*— Gap between education and demand of industry is broadening as new and new technologies become viral every year. In order to sort out this phenomena educational institutes must be able to prepare its students for real life challenges, by imitating industrial environment as much as it is possible. This article describes the possibility and implementation of a network that fulfils requirements of modern educational and research work.**

I. INTRODUCTION

Neglecting cyber security may put industries, economies, countries and even private life in danger.

In informatics firewalls are such network security systems which monitor data traffic, both ingress and egress, control them according to rules set by network administrator, hence implementing a barrier between the reliable network inside and the not always reliable network outside the firewall.

Next Generation Firewalls (NGFW) (Fig. 1) are part of third generation firewalls, uniting the network filtering functions with traditional firewall roles, like Deep Packet Inspection (DPI), Intrusion Prevention System (IPS), application monitoring, website filtering, antivirus, SSH, TLS/SSL encrypted traffic monitoring, LDAP, RADIUS, QoS etc. Figure 2. demonstrates main features of Next Generation Firewalls. [1], [2]

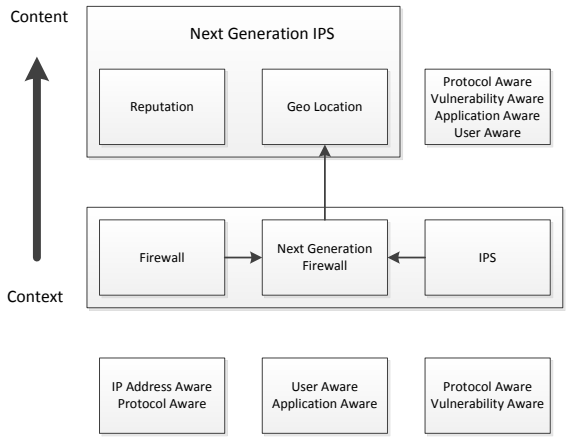

Figure 1. Services of Next Generation Firewalls

II. THEORY

Basic principles of NGFW is to monitor as many OSI model Layers as possible (maybe all 7) in order to extend classic firewall roles (packet filtering, NAT, VPN), implementing a more profound inspection in content of packets and matching of validations.

In order to make communication safer through the internet HTTPS, SSL, and TLS protocols were created. The most important feature of these protocols is that the data is passing through the channel in an encrypted way that is only understandable for the sender and the receiver, with the use of presaged keys. Nowadays more and more network attack is making use of this encrypted "camouflage" as in order to filter these contents deep inspection compatible instruments are needed. NGFWs are capable of monitoring encrypted data traffic, in the way that the gateway decrypts data before forwarding, and sends it to destination only if it is malware free. Administrators can decide if it is needed to inspect all the data traffic or only traffic based on predefined ACLs, or based on black/white list, data coming from or going towards not reliable destinations. By decryption of traffic, we are able to monitor traffic of our network, improve the efficiency of our filters, block unwanted data stream, control access based on predefined rules. [3]

The two main method of revealing network threats are Signature-based detection and Statistical anomaly detection. The basis of signature-based detection is that the system is seeking for typical patterns in code based on a continuously updated list. In case the list doesn't contain the particular pattern, it is added to it for successful preventions in future. The Statistical anomaly detection is looking for network traffic patterns that diverge from usual usage. In case the surveyed sample differs from the calculations of the system, prevention occurs. [4][5]

Centralized authentication, authorization, account management (AAA) is implemented by RADIUS (Remote Authentication Dial-In User Service) network protocol. RADIUS is a client/server protocol, running in application layer. The client is traditionally a NAS (Network Access Server), RADIUS server is usually a UNIX or Windows based daemon process running on the computer. Typically network gateways contain RADIUS client, which helps communication with central server, to identify remote access requesting users. Client forwards request to RADIUS server, and offers service according to the response. This process takes place with the help of UDP (User Datagram Protocol), therefore connection is not guaranteed, in return network traffic is less oppressed. RADIUS server authenticates by PAP, CHAP, EAP methods, and sends approval along with necessary parameters of session, which are valid during the

existence of the connection. There is a chance to collect accounting data using RADIUS services, with what security can be improved, moreover billing can be implemented. Transactions between client and server take place by the help of never sent secret keys, passwords are sent in encrypted format in the network. [6], [7], [8]

LDAP (Lightweight Directory Access Protocol) controls access of directory services. Database, on what it is based, optimized for rapid requests, tree structured (Directory Information Tree, DIT). Suitable for centralized monitoring individual users and groups, directory management. In network environment rapid access of data, management of its organization is inevitable duty, LDAP is perfect service for this role, which helps reaching data quicker, and search is well organized. Main idea while creation was that it is intended for more reading process than writing, therefore synchronization process is allowed. Applications access requested services simply and quickly.

LDAP record is a set of information assigned to the user. Each record comprises there main information: distinguished name (DN), group of attributes, group of object classes. DN explicitly defines the record and its place in the tree structure. Attributes contain the data of records, possess a type, null or more attribute options, set of values, which build up a data. Type defines, how the record must be managed by the LDAP clients and servers, while attribute options hold metadata.

Object classes define group of attribute types. Each record is assigned to group of objects, therefore defines, what kind of object it represents.

LDAP also applies client/server model, where the client accesses the server by TCP/IP protocol (in case of OpenLDAP slapped server and slurped server). Client communicates with slapped, which forwards requests to databases in the background, and response also forwarded to client through slapped. Function of slurped is the multiplication, therefore redundancy, and the sustainability of security. [9], [10], [11], [12]

III. CURRENT INFRASTRUCTURE

Local Area Networks (LAN) can be segmented by VLANs (Virtual Local Area Network), according to its function, project group, application or by any other aspect, independently from where the user or the device is physically in the institute. Devices in the same VLAN behave as they were in a totally separate network, despite the fact, that they might be using the same infrastructure as other devices in other VLANs. Each VLAN make up a logically independent network, domain, and all the packets sent to other VLANs must go through a device that is capable of routing. Different levels of security policy, and different access of users can be set to each VLAN .

Currently the network of the laboratory is a sub-network of VLAN set up for teachers (VLAN10), by the help of a router in-between (Fig. 2.). The PLCs, laptops, PCs are assigned static IP, while router is responsible for the dynamic IP assigned to mobile devices as DHCP server. Devices use router as default gateway, which exclusively communicates the other segments of the above network. For security reasons the connection to wireless network is only possible with usage of password, furthermore it is also the routers responsibility to filter devices connection to network according to their MAC address – based on a pre-defined client list -, broaden segregation in the lab's network.

The size and the manageability of current automation laboratory is a great advantage. Network configuration on the router can be implemented and modified easily in short time, by authorized person with the possession of passwords, and proper background of knowledge. Further filtering might be implemented, such type which might

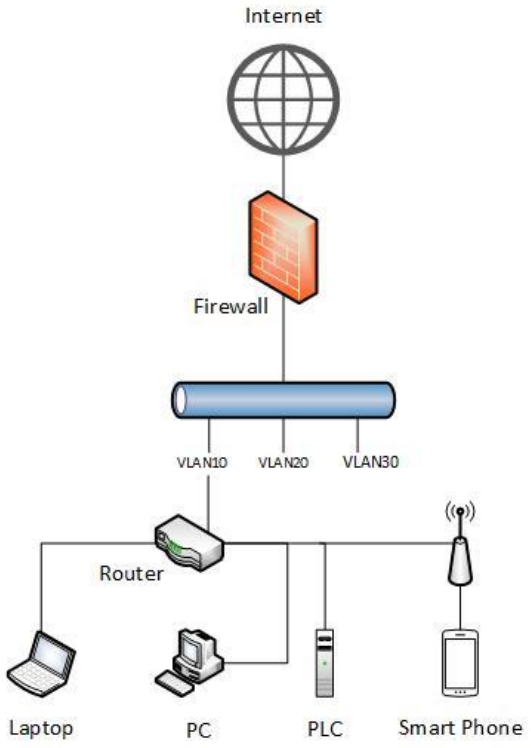

Figure 2. Current Infrastructure

not be used on institutional level, but this level of security still cannot be compared to the security level of a Next Generation Firewall, as the system is maximum as secure as its weakest point. Unfortunately, the previous firewalls are not armed with modern defensive functions, dedicated equipment is necessary in order to make use of these features.

IV. IMPROVED INFRASTRUCTURE

As soon as the improvement of network of the institute takes place, we will have the opportunity to restructure the network of the laboratory. The purchase of a Next Generation Firewall will bring about the main change in our institute. According to decision maker's plan, a Stormshield SN910 device will be purchased in near future. As the whole network of the institute will be reformed, new VLANs will be created, and as a result a dedicated VLAN will be created for the automation laboratory (Fig. 3), which will give the chance to a comprehensive configuration of a separate VLAN. Due to the separate VLAN, other laboratories, physically located at different parts of the faculty, can be connected easily, therefore ease shared projects and research work. Implementation of port filtering and other security

functions (IPS, deepscan) might seem exaggeration in an educational environment, nevertheless it helps creation of a network as similar to an industrial environment as it can be. Thanks to this option, developments from the beginning will take place in the end-usage imitating environment. We will have the opportunity to test the security of the system involving students as well, considering ethical hackers opinions – making use of knowledge students of Óbuda University ethical hacker faculty.

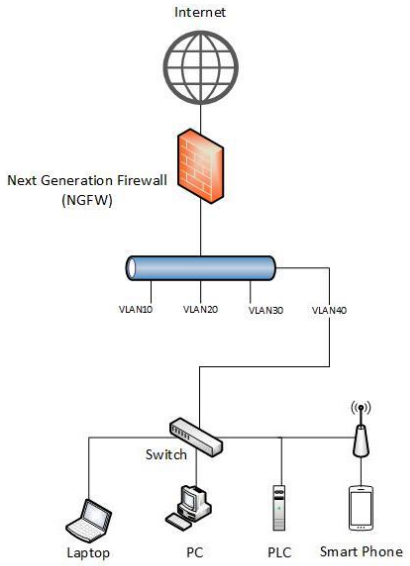

Figure 3. Improved Infrastructure

One of the most important service is the authentication of users and user groups, therefore assigning the appropriate network segment based on authorization. The system applies two methods for this task, which complete each other: LDAP and RADIUS. Implementation of LDAP by Microsoft is well known today as Active Directory. According to the expectations a programme running in a dedicated equipment will serve its purposes of the institute more stably and for longer time period, compared to a virtualized service. Further security is offered by RADIUS, also a service run by firewall. This completes and adds more functions to services of LDAP. LDAP manages user accounts by the help of RADIUS server, while providing encryption itself [13].

As an institute providing studies and research in informatics it is highly important to keep the network secured. Hopefully the technology purchased according to potentials of the university will help us reach the goal. Thanks to IPS/IDS system the NGFW will be able to filter the communication in encrypted channels, reveal anomalies in network traffic, alert network administrators, and even implement automatized steps to eliminate problem if necessary.

V. Practice Application

In order to keep up new trends, we cooperate and discuss with partners from industry, who describe their views on new developments. This attitude lead to the test of SIEMENS Simatic IoT 2020 device. This equipment serves as a gateway between various devices, which not necessarily use the same communication protocol nor data format, but with the help of this device it is easy to use a common platform for communication. The operation system running on Simatic IoT 2020 is the Linux based Node-RED. The device can be easily expanded by Arduino shields and miniPCIe cards. Beside programming in high level programming languages Simatic IoT also offers great a user friendly graphical interface accessible by built in webserver. This interface also offers a great opportunity for programming and controlling through mobile devices, and also ease access of numerous equipment it has connection with. The main reason of application of the device in industry is the reliability, longevity and robust, compared to widely used IoT equipment which are less appropriate (let's say useless) choice in industrial environment [14].

In our laboratory various devices are connected by this method, from different vendors from different years. The main concept is to make use of OPC Unified architecture (OPC UA) which is a machine to machine communication protocol developed particularly for industrial automation [15]. With the Simatic IoT it is even possible to make older series of PLC-s to communicate with the IoT device, therefore it is possible to connect to server and to other clients. This can result financial savings in industry, as by this solution it is not necessary to replace immediately devices from older series, in order to make them compatible with demands of Industry 4.0 and Internet of Things.

Conclusion

In this article, after presenting the current network of our institute, we considered the most up to date solutions of network development in harmony with potentials of the university.

Next Generation Firewalls provide the most effective response to virtual attacks coming from cyber world, and as privacy and data security is the most important issue recently worldwide, we believe that every institute must be prepared for these challenges, keeping themselves and their users secured. This paper gives the opportunity to take a glimpse of modern security systems, and consider further steps according to the needs of particular organizations.

Acknowledgment

The authors wish to thank the support to the Arconic Foundation.

References

[1] Next-Generation Firewall. [Online] November 2017. https://en.wikipedia.org/wiki/Next-Generation_Firewall

[2] Next-generation firewall (NGFW). [Online] November 2017. http://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW

[3] Managing SSL/TLS T. [Online] 2017. November. https://www.cisco.com/c/en/us/td/docs/security/asacx/9-2/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_2/prsm-ug-cx-decryption.pdf

[4] The basics of network intrusion prevention systems [Online] August 2018 https://searchsecurity.techtarget.com/feature/The-basics-of-network-intrusion-prevention-systems

[5] What is an intrusion prevention system? [Online] 2017. November. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

[6] How Does RADIUS Work? [Online] 2017. November. https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

[7] RADIUS. [Online] 2017. November. https://en.wikipedia.org/wiki/RADIUS

[8] RADIUS (Remote Authentication Dial-In User Service). [Online] 2017. November. http://searchsecurity.techtarget.com/definition/RADIUS

[9] Introduction To LDAP. [Online] November 2017. http://quark.humbug.org.au/publications/ldap/introldap.html

[10] LDAP-ról pár szóban. [Online] 2017. November. http://padre.web.elte.hu/ldap.html

[11] Lightweight Directory Access Protocol. [Online] 2017. November. https://hu.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

[12] Basic LDAP Concepts. [Online] November 2017. https://www.ldap.com/basic-ldap-concepts

[13] Firewalls play by new rules. [Online] November 2017. http://searchsecurity.techtarget.com/feature/Firewalls-play-by-new-rules

[14] Széll Károly, Manhertz Gábor, Development of a web-based training module in robotics, 2016 International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS), Narvik, Norvégia, 2016.06.21-2016.06.24., IEEE, 2016. pp. 1-6.

[15] Széll Károly, Czmerk András, Korondi Péter, Friction with Hysteresis Loop Modeled by Tensor Product, AUTOMATIKA 55:(4) pp. 463-473. (2014)