Műszaki Tudományos Közlemények vol. 11. (2019) 31–34.
https://doi.org/10.33894/mtk-2019.11.04
Hungarian: https://doi.org/10.33895/mtk-2019.11.04
https://eda.eme.ro/handle/10598/31237

POSSIBLE CISCO-BASED FIRE PROTECTION SOLUTIONS IN EDUCATION INSTITUTIONS

Krisztián BÁLINT

Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary,
balint.krisztian@phd.uni-obuda.hu

Abstract

Solutions based on Cisco firewall protection provide numerous possibilities for more efficient protection of the abundant quantity of data that is necessary for the operation of an educational institution. Firstly, data phishing can be complicated by the constitution of a virtual network. The IDPS-based access system enables the management center to identify a potential threat in a timely manner. Furthermore, the Cisco-type firewall of a new generation is able to verify the encrypted data in a way that avoids decoding and listening the communication itself. The AAA framework is also an imperative, as in case of a network, control of access is of the utmost importance.

Keywords*: data security, educational institute, Cisco.*

1. Foreword

A great advantage of modern-day firewalls is that they unify numerous tried and tested technologies on a single platform, thus providing all-round security solutions. One of these up-to-date firewalls is the CISCO ASA (Adaptive Security Appliance) shown in **Figure 1**.

Cisco systems could potentially be used effectively in educational institutions.

2. Solutions based on Cisco firewall protection

The Cisco ASA NGFW (Next-Generation Firewall) provides numerous security services, such as:

SSL (Secure Socket Layer)) which is a protocol securing the secure communication during web surfing between the client (the browser of the website's visitor) and the server (the drive serving the website). In the case of websites without SSL secure link, the passwords and usernames are passed between parties as an unencrypted simple text, which means that whoever intercepts this information may easily read the usernames and passwords in question. In the case of SSL, data will be forwarded in an encrypted form, which means that if the strings are intercepted, the delicate information would not be acquired. The simplest way of determining if the communication is flowing through an SSL link is that the website does not have an address starting with *http*, but with *https* **[1]**.

Figure 1. *The firewall appliance Cisco ASA*

– **IPsec** (Internet Protocol Security) a solution of some sort must be found in the coding system for the changing of the keys; - In case of the IPSec, it is achieved by the algorithm IKE (Internet Key Exchange). It manages and distributes the keys, and furthermore, sets the SA (Security Association), e.g. the parameters of the connection in question. Besides the changing of the key, the IPSec provides net traffic protection, for which task the AH (Authentication Header) protocol is the most suitable. By the use of a hash function, a footprint is made of the package, and upon the package's arrival, the repeated verification will

decide if the transferred data has remained intact. The descendant of the AH, is called ESP (Encapsulating Security Protocol), which is capable of all the mentioned functions, plus even the encryption, with the help of algorithms DES, 3DES or AES. In transport mode, the AH/ESP header will be located behind the original header of the IP-package. In tunnel mode, a whole new IP-package will be created, with a new header, followed by the AH/ESP header, then the original IP-package. Thus, a possibility arises that the routers for example, perform IPSec proxy functions, which means, that the encryption or the decoding will be completed by them, instead of the host. It would be unnecessary to have data processing on the client machines of any sort in connection with the IPSec, as access to the IPSec gateway needs to be secured. The attacker does not know the addresses to which the packets were addressed; he/she may only have the information about which two gateways were used by the package [2]. Table 1. table shows the command lines used in setting up the IPSec.

– **VPN** (Virtual Private Network)) is originally a technique elaborated for the connection of two networks via the Internet. Its advantage is that the VPN is suitable for connecting full networks, and terminals with networks alike. The own Internet-providers do not have any information at their disposal, which website was visited by a client. It complicates the process of data phishing in case of public Wi-fi networks (without it, their job would be very simple). The visited web servers are considered to belong to the country in which the provider's server is located. Its drawback is slower access to the Internet [4]. VPN enables access to the inner resources by remote operators. The protocol uses secure implementation, and it encrypts all communication between the source and the target. This secure package will be transferred through the network. Upon arrival at its destination, the package is unpacked, and the unencrypted contents are restored. [5].

Table 1. *IPSec setup [3]*

```
R1(config)#crypto ipsex transform-set MySet esp-
  3des-esp-sha-hmac
R1(cfg-crypto-trans)#mode transport
R1(config)#crypto dynamic-map MyMap 10
R1(config-crypto-map)#set transform-set MySet
R1(config)#crypto map L2TP-Map 10 ipsec-isakmp
  dynamic MyMap
R1(config)#interface FastEthernet0/0
R1(config)#crypto map L2TP-Map
```

– **IDPS** Computer based systems often become targets of various attacks, by which individuals try to gain unauthorized access from outside or from inside, thus causing varying degrees damage. The aim of the incursion preventing systems is that they identify the attack and, if need be, perform an intervention thus preventing the unauthorized access, also to send a notification to the management center about the event [6].

The firewall provides a possibility for a full network remote control, based on SSL and IPsec. Operating at network layer, it provides a full connection for a remote user, to be utilized with virtually every application or network resource. The network access is secured by the Cisco SSL VPN client, or the Cisco IPsec VPN client software.

3. The Cisco AAA (Authentication, Authorization, and Accounting) framework

Access regulation is of utmost importance in a network. The exact setup of authorizations is an imperative, as much as the registering of various activities. The complex accomplishment of these tasks can be performed with the help of the AAA-framework. The authentication, authorization and registering of the activities constitute an integrated system. These tasks can be accomplished in place on the network device (router) in question, or on an outside server.

Access control is performed with the help of the server and the AAA-mechanism. The AAA-mechanism is an essential tool for the centralization of the whole network access solution. The AAA performs 3 tasks:

– identification;
– authorization management;
– logging.

The local setup of rules of engagement enables the router to communicate with the radius server built within the network. The devices are authenticated by the users, and they permit the work sessions. As the first step, the radius server must be installed on a server unit, then via a UDP-connection, the server and the Cisco-unit must be coupled. Table 2. shows the access control setup.

4. The Cisco-based three tier security protection

The Cisco Cloud Email Security application checks attachments and URL addresses, while blocking link phishing for passwords and files recognized as ransomware. Through a deeper

Table 2. *AAA-setup [7]*

```
Router2911(config)#aaa new-model
Router2911(config)#radius-server host x.x.x.x /ip
Router2911(config)#aaa authentication login default
  radius local
Router2911(config)#aaa authentication attempts login 3
Router2911(config)#aaa authorization exec default
  radius
Router2911(config)#aaa authorization commands
  default radius
Router2911(config)#aaa accounting exec default start-
  stop
Router2911(config)#aaa accounting commands default
  start-stop
```

analysis, as a proxy, it shows a picture of the suspicious website, so the real entering is decided by the user, with the help of the visual information mentioned.

The second layer of defence is provided by the Cisco Umbrella performing DNS-web proxy functions. The Cisco Umbrella is a Secure Internet Gateway. By its use, the mobile endpoints become protected too, which task becomes outstandingly important after the leaving of the corporate system. The system automatically detects if the user has exited from the dependable network, so the data will receive a further protection at corporate level.

Finally, the Cisco AMP (Advanced Malware Protection) provides a solution for retrospective protection, so it checks and follows every file admitted to the network and if it later proves to be infected, the software promptly notifies and isolates the users involved. This is of critical importance, because an infection may have been undetected for months. On the other hand, the Cisco Advanced Malware Protection is capable of a less than 6 hour detection time on the average [8].

5. Analysis of encrypted data traffic

As a growing percentage of Internet-based data traffic becomes encrypted, the cyber-criminals abuse the possibilities of encryption ever more frequently. By 2019, 80 percent of Internet-based data traffic will presumably be encrypted, while 50 percent of the criminals' campaigns for spreading malware will be based on https addressing solutions (or provided with various other types of encryption). Thus, it is no wonder that the companies specializing in networking and security are continuously developing technologies, by which malware codes and harmful content would be filtered from instances of encrypted communication. This method already has some solutions, but these usually utilize tactics including licenses, in order to gain introspection into the data traffic during a security analysis. Of course, the mentioned methods are the result of privacy concerns. Cisco has developed a technology called ETA - Encrypted Traffic Analytics, which is able to classify the encrypted data traffic from an aspect that does not need any decrypting, e.g. listening into the communication [9]. **Figure 2.** demonstrates ETA analysis:

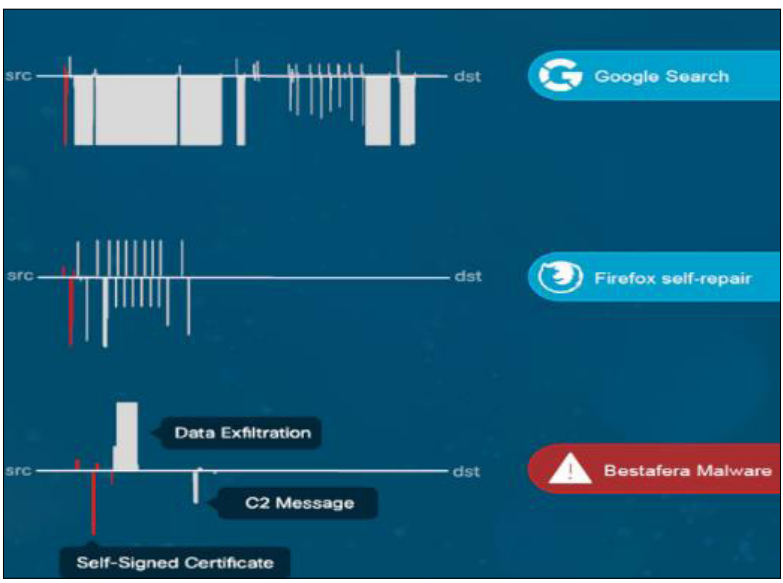

Figure 2. *ETA analysis [10]*

6. Conclusions

In order to secure the effective operation of a computer system in an environment such as an educational institute, data concerning the employees and the students must be protected. The databases may become vulnerable without up to date solutions for firewall protection of new generation, and at an insufficient rate of backup data savings, even data retrieval may become an insurmountable task.

The Cisco based solutions for firewall protection are, however, providing possibilities for schools and universities, by which the data can be stored fairly securely. To this day, ransomware viruses have rendered numerous systems inoperable, so at least, the search for possibilities concerning the aim of increasing the security level of saved data is food for thought.

References

[1] Website creation Pécs: *What is SSL encryption and why it is important for websites?* 2014. (accssed 2018.10.25.). https://goo.gl/ch9r8h

[2] Baracsi P., Kovács Z., Terdik S.: *MPLS alapú virtuális magánhálózatok napjainban.* (MPLS based virtual private network in nowadays). Debreceni Egyetem, 2010. http://hdl.handle.net/2437/95373

[3] Cisco, *Security for VPN with IPsec Configuration.* 2018 (accssed: 2018.10.25.). https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-3s/sec-sec-for-vpns-w-ipsec-xe-3s-book/sec-cfg-vpn-ipsec.html

[4] ITKommandó, Szigetvári Z.: *About the VPN*. 2014, (accssed: 2018.10.25.). https://www.itkommando.hu/site/a-vpn-rol/

[5] BravoGroup, *VPN*. 2017. (accessed: 2018.10.25). http://bravogroupoffice.hu/halozat/vpn

[6] LAN computing, *Firewall, IPS. UTM.* 2016. (accssed: 2018.10.25.). https://www.lan.hu/tuzfal_IPS_UTM_1

[7] Cisco, *Configurating Basic AAA on an Access Server*. 2018. (accssed: 2018.10.25.). https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

[8] [8] Cisco Cloud Security, *The most effective protection against blackmail viruses*. 2017. (accssed: 2018.10.25.). https://bitport.hu/a-leghatekonyabb-vedelem-a-zsarolovirusokkal-szemben-cisco-cloud-security

[9] Biztonságportál, *Titkosított adatforgalomból is kiszűri a vírusokat a Cisco*. (Cisco also scans viruses for encrypted date traffic). 2018. (accssed 2018.10.25.). https://biztonsagportal.hu/titkositott-adatforgalombol-is-kiszuri-a-virusokat-a-cisco.html

[10] Moor Insights & Strategy, *Cisco Live Day 3: Leaning Into Security* 2018. (Letöltve 2018.10.) http://www.moorinsightsstrategy.com/cisco-live-day-3-leaning-into-security/