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

LEHETSÉGES CISCO ALAPÚ TŰZFALVÉDELMI MEGOLDÁSOK AZ OKTATÁSI INTÉZMÉNYEKBEN

POSSIBLE CISCO BASED FIRE PROTECTION SOLUTIONS IN EDUCATION INSTITUTIONS

Bálint Krisztián

Óbudai Egyetem Biztonságtudományi Doktori Iskola. Budapest, Magyarország,
balint.krisztian@phd.uni-obuda.hu

Abstract

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

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

Összefoglalás

A Cisco alapú tűzfalvédelmi megoldások számos olyan lehetőséget nyújtanak, amelyek által hatékonyabban lehetne megvédeni az iskola működéséhez szükséges szerteágazó adatmennyiséget. Először is virtuális hálózat létrehozásával megnehezíthető az adathalászok dolga. Az IDPS alapú behatolási rendszer lehetővé teszi azt, hogy a menedzsmentközpont időben észrevegye a lehetséges veszélyt. Továbbá a Cisco új generációs tűzfala ellenőrízni tudja a titkosított adatokat, úgy, hogy közben nem végez dekódolást, nem hallgat bele a kommunikációba. Egy iskola esetében az AAA keretrendszer sem elhanyagolható, hiszen egy hálózatban elengedhetetlenül fontos az, hogy a hozzáférés szabályozva legyen.

Kulcsszavak*: adatbiztonság, oktatási intézmény, Cisco.*

1. Bevezetés

A modern tűzfalak nagy előnye, hogy számos bevált technológiát egyesítenek egy platformon, ez által átfogó biztonsági megoldásokat nyújtanak. Ilyen modern tűzfal a CISCO ASA (Adaptive Security Appliance – Adaptív Biztonsági Eszköz) is. Ezt az **1. ábra** szemlélteti.

1. ábra. *Cisco ASA tűzfal*

A Cisco rendszereket feltételezhetően hatékonyan lehetne használni az oktatási intézményekben is.

2. Cisco alapú tűzfalvédelmi megoldások

A Cisco ASA NGFW (Next-Generation Firewalls / Új generációs tűzfal) számos olyan biztonsági szolgáltatást nyújt, mint az:

– **SSL** (Secure Socket Layer) egy olyan protokoll, amely a webböngészés alatt biztosítja a biztonságos kommunikációt a kliens (a honlap látogatójának a böngészője) és a szerver (a honlapot kiszolgáló tárhely) között. Az SSL kapcsolat nélküli honlapok esetében a jelszavak és a felhasz-

nálónevek titkosítatlanul (egyszerű szövegként) kerülnek továbbításra a két fél között, ami azt jelenti, hogy ha bárki elkapja ezt az információt, akkor könnyedén kiolvashatja belőle a felhasználónevünket és a jelszavunkat. Az SSL kapcsolat használata esetén az adatok titkosítva kerülnek továbbításra, ami azt jelenti, hogy még ha el is kapja valaki őket, akkor sem fogja tudni megszerezni a számunkra kényes információkat. A legegyszerűbben onnan tudható, hogy SSL kapcsolaton keresztül zajlik a kommunikáció, hogy az adott honlap címe nem http-vel kezdődik, hanem https-sel [1].

– **IPsec** (Internet Protocol Security) a kódolási rendszerben valamilyen módon megoldást kell találni a kulcsok cseréjére; -Az IPSec esetében ezt az IKE (Internet Key Exchange) algoritmus oldja meg. Kezeli és elosztja a kulcsokat, továbbá beállítja az SA-t (Security Association), azaz a kapcsolat paramétereit. A kulcscserén kívül a forgalom védelmét is biztosítja az IPSec, erre alkalmas az AH (Authentication Header) protokoll. Egy hash függvény segítségével lenyomat készül a csomagról, majd miután a csomag célba ért, a lenyomat újbóli elkészítésével eldönthető, hogy sértetlen maradt-e az átvitt adat. Az AH utódja az ESP (Encapsulaing Security Protocoll) protokoll, mely az előbbieken túl titkosításra is képes a DES, 3DES ill. AES algoritmusok segítségével. Transzport módban az AH/ESP fejléc az IP csomag eredeti fejléce mögé kerül be. Tunnel módban teljesen új IP csomag jön létre, amelynek új fejléce van, ezt követi az AH/ESP fejléc, majd az eredeti IP csomag. Ezáltal lehetőség van arra, hogy például a routerek IPSec proxy funkciót lássanak el, ami azt jelenti, hogy a hostok helyett ők végzik el a titkosítást, illetve a dekódolást. A kliens gépeken nem szükséges IPSechez kapcsolódó semmilyen feldolgozás, csak az IPSec átjáró elérését kell biztosítani. A támadó nem tudja, hogy hova lettek címezve a csomagok, mindössze azt ismeri, hogy mely két átjáró között haladt át [2]. Az 1. táblázat a IPSec beállításának parancssorait mutatja be.

1. táblázat. *IPSec beállítás [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
```

– **VPN** (Virtual Private Network) a „virtuális magánhálózat” eredetileg két hálózat, az Interneten keresztüli összekötésére kidolgozott technika. Előnye, hogy a VPN teljes hálózatok összekötésére, munkaállomás-hálózat kapcsolat kiépítésére egyaránt alkalmas. A saját internetszolgáltatónak nem áll rendelkezésére információ mely oldal került meglátogatásra. Nyilvános WiFi hálózat használata esetén megnehezíti az adathalászók dolgát (ez nélkül a dolguk nagyon egyszerű). A meglátogatott webszerverek abból az országból érkezőnek tekintenek, ahol a szolgáltató szervere van. Hátrányként fogalmazható meg a lassabb internetelérés [4]. A VPN lehetővé teszi a belső erőforrásokhoz történő hozzáférést a távmunkát végzők számára. A forrás és a cél közti összes kommunikációt titkosítja a biztonságos beágyazást használó protokoll. Ez a biztonságos csomag kerül továbbításra a hálózaton. A célállomáshoz megérkezve a csomagot kicsomagolják és visszaállítják a titkosítatlan tartalmat. [5].

– **IDPS** behatolás megelőzés Az informatikai rendszereket gyakran érik különböző támadások, kívülről vagy belülről próbálnak illetéktelenül hozzáférni a hálózathoz, kisebb-nagyobb károkat okozva ezzel. A behatolás megelőző rendszerek célja, hogy észleljék és szükség esetén beavatkozással megakadályozzák az ilyen helyzeteket, valamint értesítést küldjenek az eseményről a menedzsmentközpont felé [6].

A tűzfal lehetőséget biztosít az SSL és IPsec alapú teljes hálózati távvezérlésre. A hálózati rétegben működő, teljes értékű távoli felhasználói kapcsolatot biztosít gyakorlatilag bármely alkalmazáshoz vagy hálózati erőforráshoz. A hálózatelérést a Cisco SSL VPN-klines, vagy a Cisco IPsec VPN klinsprogram biztosítja.

3. Cisco AAA (Authentication, Authorization, and Accounting) keretrendszere

Egy hálózatban elengedhetetlenül fontos, hogy a hozzáférés szabályozva legyen. Szükségszerű a jogokat pontosan beállítani, valamint azt, hogy a különböző tevékenységek nyilván legyenek tartva. Ennek a komplex megvalósítása történhet az AAA keretrendszer segítségével. A hitelesítés, feljogosítás és tevékenység-nyilvántartás egységes rendszert valósít meg. Ezek történhetnek helyben az adott hálózati eszközön (routeren), vagy egy külső szerveren.

A hozzáférés-vezérlés a szerver és az AAA mechanizmus segítségével valósul meg. Az AAA

mechanizmus központi eszköz a teljes hálózati hozzáférési megoldás központosítására. Az AAA 3 feladatot lát el, úgy mint:
– azonosítás;
– jogosultságkezelés;
– könyvelés.

A helyileg beállított kezelési szabályok lehetővé teszik a router számára, hogy kommunikáljon a hálózatba telepített radius szerverrel. Az eszközöket a felhasználók hitelesítik, valamint engedélyezik a rajtuk végzett munkát. Első lépésként a radius szervert telepíteni kell a szerveregységen, majd pedig UDP kapcsolat által össze kell kötni a szervert a Cisco egységgel. A **2. táblázat** a hozzáféréshez-vezérlés beállításait szemlélteti:

2. táblázat. *AAA beállítás [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
```

4. Cisco alapú háromszintű biztonsági védelem

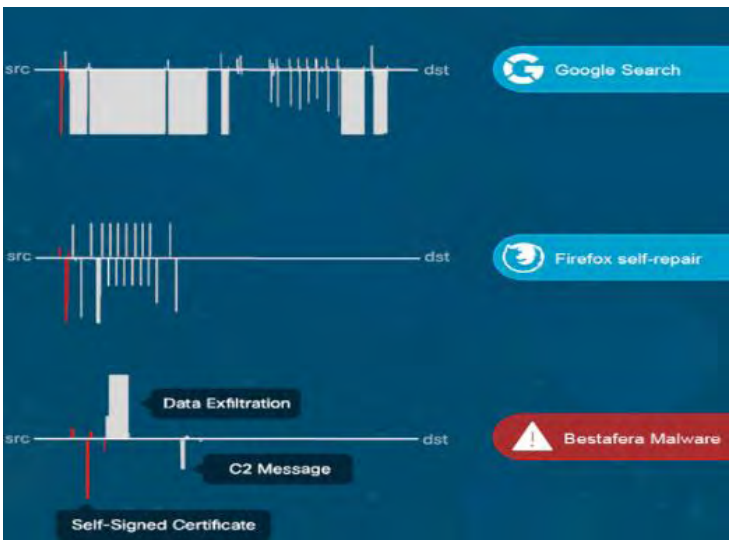
Cisco Cloud Email Security csatolmány és URL ellenőrzést végez, blokkolva a jelszóhalász linkeket és ransomware állományokat. Mélyebb elemzéssel proxyként, kép formában megjeleníti a meglátogatni kívánt, gyanús oldalt, melynek valódi megnyitásáról a vizuális információ ismeretében dönthet a felhasználó.

A védelem második rétegét a DNS-webproxy funkciót nyújtó Cisco Umbrella rendszere szolgáltatja. A Cisco Umbrella egy biztonságos Internet átjáró, ún. Secure Internet Gateway. Alkalmazásával a mobil végpontok is védhetővé válnak, mely feladat a nagyvállalati rendszer elhagyását követően válik különösen fontossá. A rendszer automatikusan észleli, ha kilépett a felhasználó a megbízható hálózatból, így adatai továbbra is nagyvállalati szintű védelmet kapnak.

Végül a retrospektív védelmi megoldást nyújtó Cisco AMP (Advanced Malware Protection) minden, a hálózaton beengedett állományt nyomon követ, és ha később fertőzöttnek bizonyul, arról haladéktalanul értesíti és izolálja az érintetteket. Ez azért különösen fontos, mert enélkül akár hónapokig is rejtve maradhat egy fertőzés. A Cisco Advanced Malware Protection ezzel szemben átlagosan alig 6 óra alatti észlelési időre képes **[8]**.

5. Titkosított forgalomelemzés

Ahogyan az internetes adatforgalom egyre nagyobb hányada titkosítottan zajlik, úgy élnek visszsza mind gyakrabban a kiberbűnözők a titkosítás adta lehetőségekkel. Előreláthatóan 2019-re az internetes adatforgalom 80 százaléka titkosított lesz, miközben a kártékony programok terjesztése érdekében indított alvilági kampányok 50 szá-



2. ábra. *ETA analízis [10]*

zaléka https alapú (vagy különféle kódolással ellátott) megoldásokra fog épülni. Ezért nem csoda, hogy a hálózati és biztonsági cégek folyamatosan fejlesztik azokat a technológiáikat, amelyek révén a titkosított kommunikációból is kiszűrhetővé válhatnak az ártalmas kódok, tartalmak. Erre jelenleg is léteznek megoldások, de azok általában tanúsítványokkal „trükköznek” annak érdekében, hogy betekintést lehessen nyerni az adatforgalomba a biztonsági elemzések során. Persze mindez adatvédelmi aggályokat is felszínre hoz. A Cisco egy olyan technológiát fejlesztett ki (ETA - Encrypted Traffic Analytics), amely a titkosított adatforgalmat olyan módon képes védelmi szempontból minősíteni, hogy közben nem kell dekódolást végeznie, azaz belehallgatnia a kommunikációba **[9]**. A **2. ábra** az ETA analízist szemlélteti:

6. Következtetések

Ahhoz, hogy egy iskolai rendszer hatékonyan működhessen az ott dolgozók és tanulók adatait megfelelően kell védeni. Modern új generációs tűzfalvédelmi megoldások nélkül sebezhetővé vállnak az adatbázisok, hiányos biztonsági mentések mellett pedig a helyreállítás is megoldhatatlan feladattá vállhat.

A Cisco tűzfalvédelmi megoldások azonban olyan lehetőségeket biztosíthatnak az iskolák és az egyetemek számára, amely által az adatokat meglehetősen biztonságossan lehet tárolni. A zsarolóvírusok ez idáig számos rendszert tettek működésképtelenné, már csak ezért is elgondolkodtató olyan lehetőségek után kutatni, amelyek azt a cél szolgálják, hogy növeljék a tárolt adatok biztonsági szintjét.

Szakirodalmi hivatkozások

[1] Honlapcentrum, Szabó P.: *Mi is az az SSL titkosítás és miért fontos a weboldalak számára?* 2014. (Letöltve 2018.10.25.). https://goo.gl/ch9r8h

[2] Baracsi P., Kovács Z., Terdik S.: *MPLS alapú virtuális magánhálózatok napjainban*. Debreceni Egyetem, 2010. http://hdl.handle.net/2437/95373

[3] Cisco, *Security for VPN with IPsec Configuration.* 2018 (letöltve: 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.: *A VPN-ről.* 2014, (letöltve: 2018.10.25.). https://www.itkommando.hu/site/a-vpn-rol/

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

[6] LAN Számítástechnikai és Szolgáltató Kft., *Tűzfal, IPS. UTM.* 2016. (letöltve: 2018.10.25.). https://www.lan.hu/tuzfal_IPS_UTM_1

[7] Cisco, *Configurating Basic AAA on an Access Server*. 2018. (letöltve: 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] BitPort, *A leghatékonyabb védelem a zsarolóvírusokkal szemben*. 2017. (letöltve: 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*. 2018. (Letöltve 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/