Személyes tűzfalak

Készítő: Fuchs András (afuchs@freemail.hu)

Projekt: LDAP

Dátum: 2002. 05.10.

Budapesti Műszaki és Gazdaságtudományi Egyetem
Schönherz Zoltán Kollégium
Kollégiumi Számítástechnikai Kör
http://kszk.sch.bme.hu

Tartalomjegyzék

1. A kollégium jelenlegi firewall-rendszere

Ez az, ami nincs sehol sem korlátozva. Minden user a neki legszimpatikusabb firewall-t használja, ami gyakran galibához vezet. Ezekre a dolgokra részletesen kitérek a dokumentum megfelelő fejezetében. A dokumentum célja, a ma piacon lévő (lehetőleg ingyenes) firewall software-ek bemutatás mellett, egy a kollégium jelenlegi rendszerének leginkább megfelelő kiválasztása.

1.1 Jelenlegi problémák

A kollégiumi hálózat jelenleg is gond nélkül működik, de sok fejfájást okoznak a kollégisták gépein rosszul konfigurált tűzfalak. A legnagyobb gond a Windows-háló menedzselésével van. Emellett fontos lenne a kollégium minden gépének általános védelmét megoldani.

1.2 Későbbi tervek

A jelenlegi kollégiumi rendszer kisebb, de inkább nagyobb változásokon fog keresztülmenni a közeljövőben. A tűzfal kiválasztásánál fontos, hogy a következő generációs rendszerben is gond nélkül működjön. Amelyik erre nem alkalmas, az nem versenyképes.

2. Tesztelés

A tesztelés folyamán csak Windows alatt futó tűzfal megvalósításokat vizsgáltam. Emellett próbáltam lehetőleg ingyenesen letölthető, legális software-eket keresni, mivel a tesztsorozat végén legjobbnak talált firewall-t minden kollégista számára elérhetővé kell tenni.

2.1 Tesztelési körülmények

A tesztelés első fázisában egy Windows XP rendszerrel megáldott Celeron 300-as gépen próbáltam ki az egyes jelölteket. Ez volt a funkcionális teszt, amely során ellenőriztem, hogy a kívánt funkciókat egyáltalán tudja-e biztosítani a software.

A második fázisban történt az első szűrőn sikeresen átjutottak pontos konfigurálása. Ennek menetere illetve a pontos beállításokra majd a 3. fejezetben fogok kitérni, a tesztelés menetének ismertetésénél ennek nincs különösebb jelentősége.

A harmadik fázisban élesítettem a tűzfalat, mind Windows XP mind pedig Windows 98-as rendszereken, az alapvető szolgáltatásokat ellenőrizve.

A végső fázisban a domainen belüli viselkedést vizsgáltam hosszabb ideig, a végleges beállításokkal. A hosszabb idő a szűkös határidő miatt nem volt több 24 óránál.

2.2 Tesztelési szempontok

A tesztelési szempontok szinte csak felsorolva, rövid ismertetővel a következők voltak:

- gyártó: a gyártó cég neve
- név: a firewall software teljes neve
- homepage: a cég homepage-e
- aktuális verziószám
- a legutóbbi verzió kibocsátásának dátuma
- operációs rendszer: értelemszerűen a firewall által támogatott operációs rendszerek listája
- licence: free / xx day demo / retail - ingyenes / xx napos demo / pénzért megvehető software
- update: (E) email newsletter - e-mailben kaphatunk értesítést az esetleges frissülésekről
  (S) software info - a firewall automatikusan jelzi, ha új verzió jelent meg
  (D) download - a firewall letölti a frissebb verziót
  (I) install - a firewall automatikusan frissíti saját magát

- system service: NT rendszereknél a services közt megjelenő megnevezés

- NETBIOS konfiguráció: nincs
  van, de nehézkes
  van, és egyszerű
- NETBIOS konfiguráció csak trusted domainre: nincs
  van
- Microsoft Windows Network: nem működik
  megfelelő beállítás mellett működik
  egyből működik
- konfigurációs file: nincs
  van, de nem másolható
  van, és minden különösebb gond nélkül másolható
- konfiguráció file kézzel módosítható: bináris file
  text file
- logolás: nincs
  van de egyszerű
  van és nagyon komoly
- traffic monitor: nincs
  van
- preset: nincs
  van
- preset bővítési lehetőség: nincs
  van, de csak automatikus
  van, és manuálisan is bővíthető (egy egyszerű text file)
- pop-up firewall rule állítás: nincs
  van, de nehézkes
  van, és jól használható
- utólagos firewall rule állítás: nincs
  van, de túl egyszerű vagy nehezen kezelhető
  van, és világos szerkezetű, könnyen használható
- email védelem: nincs
  van
- szerverek futnak: egyik sem megy
  ftp vagy web nem megy
  ftp és web megy
- extrák: minden egyéb plusz

2.3 Teszteredmények

gyártó	*Agnitum*	*Kerio / Tiny*	*Sygate*	*ZoneLabs*
név	Outpost Firewall FREE	Kerio Personal Firewall 2 / Tiny Personal Firewall	Sygate Personal Firewall	ZoneAlarm
homepage	www.agnitum.com	www.kerio.com / www.tinysoftware.com	soho.sygate.com	www.zonelabs.com
aktuális verziószám	1.0.1617	2.1.4 / 2.0	5.0.1117	2.6.362
legutóbbi verzió dátuma	2002.05.20.	2002.04.15. / 2001.10.30.	2002.05.17.	2002.05.06.
operációs rendszer	Win 95, 98, Me, NT, 2000, XP	Win 98, NT, ME, 2000, XP	Win 95, 98, Me, NT, 2000, XP	Win 95, 98, Me, NT, 2000, XP
licence	free	free	free	free
update	S D I	E S	S	E S D
system service	Outpost Firewall Service	Kerio Personal Firewall / Tiny Personal Firewall	Sygate Personal Firewall	TrueVector Basic Logging Client, TrueVector Internet Monitor
NETBIOS konfigurálás	✓	✓	✓	✓
NETBIOS trusted domainre	✓	✓	✗	✗
MS Windows Network	✓	✓	✓	✗
konfigurációs file	✓	✓	✓	✗
konfigurációs file manuálisan	✓	✗	✗	✗
logolás	✓	✓	✓	✓
traffic monitor	✓	✓	✓	✓
preset	✓	✗	✗	✓
preset bővítési lehetőség	✓	✗	✗	✗

gyártó	*Agnitum*	*Kerio / Tiny*	*Sygate*	*ZoneLabs*
pop-up firewall rule	✓	✓	✓	✓
utólagos firewall rule	✓	✓	✓	✓
e-mail védelem	✓	✗	✗	✓
server teszt	✓	✓	✓	✓
extra	plug-in támogatás, sok ingyenes plug-in, 30 napos Tauscan kiegészítő a trojanok ellen	MD5 signature vizsgálat	MD5 signature vizsgálat, MAC szám alapú szűrés, webes felületű security check	szép, marketinges design

2.4 Megjegyzések és kiegészítések a tesztekhez

Minden tűzfalhoz hozzáfűznék egy-két szót, csak röviden a használati tapasztalataimról.

Outpost: a project egy nyílt forráskódú firewallból nőtte ki magát, ha jól tudom, akkor most már nem nyílt, de ingyenes. Ez a legjobban konfigurálható illetve bővíthető a jelöltek közül. Felülete barátságos, minden ott van, ahol lennie kell. A betanulási ideje jelentősen lecsökkenthető, ha sok *presetet* használunk. A „gyári" *presetek* hibátlanul működtek, és meglepően sok programhoz elkészítették őket, de ez a lista akár a felhasználó által is bővíthető.

Tiny: a táblázatban közös oszlopba soroltam két gyártó software-ét. Ennek igen egyszerű oka van: a Tiny software az ingyenes firewall programjának fejlesztését befejezte a 2.0-ás verziónál. Ennek ugyan megjelent a 3.0-ás folytatása, ami rendkívül jó, de az sajnos már nem ingyenes. A 2.0-ás verzió teljes támogatása is megszűnt. Kerio semmi jelentőset nem csinált, az általa nyújtott tűzfal teljesen megegyezik a Tiny fejlesztésével. Kerio viszont a jövőbeni támogatást biztosít.

Sygate: a firewall alapvetően nem rossz, viszont van egy-két gyenge pontja: a kisebbik baj, hogy elég szerényre sikerült a grafikus felület. Általában egy tűzfal esetében ez nem nagy gond. A nagyobb gond, hogy nincs konfigurációs file, és nincsenek *presetek* sem. Ezért nagyon hosszúra nyúlhat a betanulási idő, és pontatlanok lehetnek a beállítások. Nagyon jó funkcióknak tartom az extrában felsorolt dolgokat. Sajnos az utolsó fázisban a firewall domainen belüli használatánál igen jelentős teljesítmény-visszaesést észleltem, ami nem megengedhető.

ZoneAlarm: sokak kedvence. Ennek egyetlen okát tudom elképzelni, az igényes design. Sajnos funkcionálisan jelentősen elmarad a versenytársaktól. Nem térnék ki a részletekre, a táblázatból is elég sok dolog kiolvasható. Számomra egyértelmű, hogy nem alkalmas a kollégiumi rendszerben való használatra.

2.5 Összegzés

A tűzfalak közül csak kettő volt alkalmas arra, hogy a tesztsorozat utolsó fázisába léphessenek: Agnitum Outpost és Sygate Personal Firewall. Ezek rendelkeznek minden szükséges funkcióval, láthatólag megfelelő a támogatásuk, folyamatosan fejlesztik őket, illetve bővítik adatbázisaikat. A Sygate viszont nem lenne könnyen használható tömeges közös konfigurálásra és a *presetek* kiterjesztésére. Égető gondja továbbá a már említett

teljesítményvisszaesés használata közben. Szerintem azonban nem kellene még keresztet vetni fölötte. Bár az tény, hogy jelenleg jóval erősebb az **Agnitum** által fejlesztett **Outpost**. Rendkívül rugalmas az egész, jól használható, bővíthető, folyamatosan fejlesztik, és megvalósítható az általunk megcélzott konfiguráció-átültetés rengeteg kliensre.

3. Konfigurálás

Ez a fejezet egy rövid ismertető az általában használt portokról és szerepükről, valamint javaslat egy ilyen számítógép tűzfal beállításaira.

3.1 Kiemelt programok és általuk használt portok

System

TCP port 445: NETBIOS megosztási lehetőség (File és Printer megosztás)

UDP port 445: NETBIOS megosztási lehetőség (File és Printer megosztás)

WinLogon

TCP port 389: LDAP

UDP port 1046: Internet Printing Protocol (IPP)

Generic Host Porcess (SVCHOST.EXE)

UDP port 123: Time Synchronizer

TCP port 135: DCOM: RPC Endpoint Mapper

UDP port 135: DCOM: RPC Endpoint Mapper

TCP port 1025: NAT - web browser side

UDP port 1026: DNS - client side

UDP port 1027: DNS - client side

UDP port 1039: ?

UDP port 1900: SSDP

TCP port 5000: NAT (network address translation) - intranet outgoing server

LSA Shell (LSASS.EXE)

UDP port 500: IKE (Internet Key Exchange)

UDP port 1028: RPC Server Service (Remote Procedure Call)

IIS 5.1 (INETINFO.EXE)

TCP port 80: HTTP server

TCP port 443: HTTPS server

TCP port 1040: NMS Service (Network Monitoring System Service)

TCP port 1964: NETBIOS

UDP port 3456: Windows Media Player - Broadcasting

3.2 Biztonsági megfontolások

Általános irányelv, hogy amilyen portra nincs szükségünk, azokat ne hagyjuk nyitva. Kissé alaposabb, hosszabb lefutású tesztet kellene végezni ahhoz, ezen portok megtalálásához. Viszont felhívnám a figyelmet a fent említett komoly biztonsági résekre (135-ös, 1046-os port) . Az Outpost automatikusan védelmet biztosít az RPC-s támadások ellen, viszont az IPP-s ellen, nem nyújt védelmet. Más kérdés, hogy az ilyen jellegű támadások igen ritkák. Elsődleges javaslat nyilvánvalóan a május 1-i patch felrakása, de sajnos ez nem minden rendszeren megoldható. Mivel ez a szolgáltatás egy átlagos felhasználót nem érint, ezért az 1046-os port tiltását javasolnám.

3.3 Portok engedélyezésére tett javaslatok

Átlagos esetben nem szükséges különösebben módosítani az eredeti beállításokon. Természetesen ha egy komoly szerverről van szó, akkor mindenképpen érdemes, egy legalább 2-3 napos vizsgálódás után a nem használt portokat és alkalmazásokat eltiltani a külső hozzáféréstől.

4. A kiválasztott firewall konkrét konfigurálása és FAQ

HTML-ben mellékelve.