Tartalomszűrő megoldások

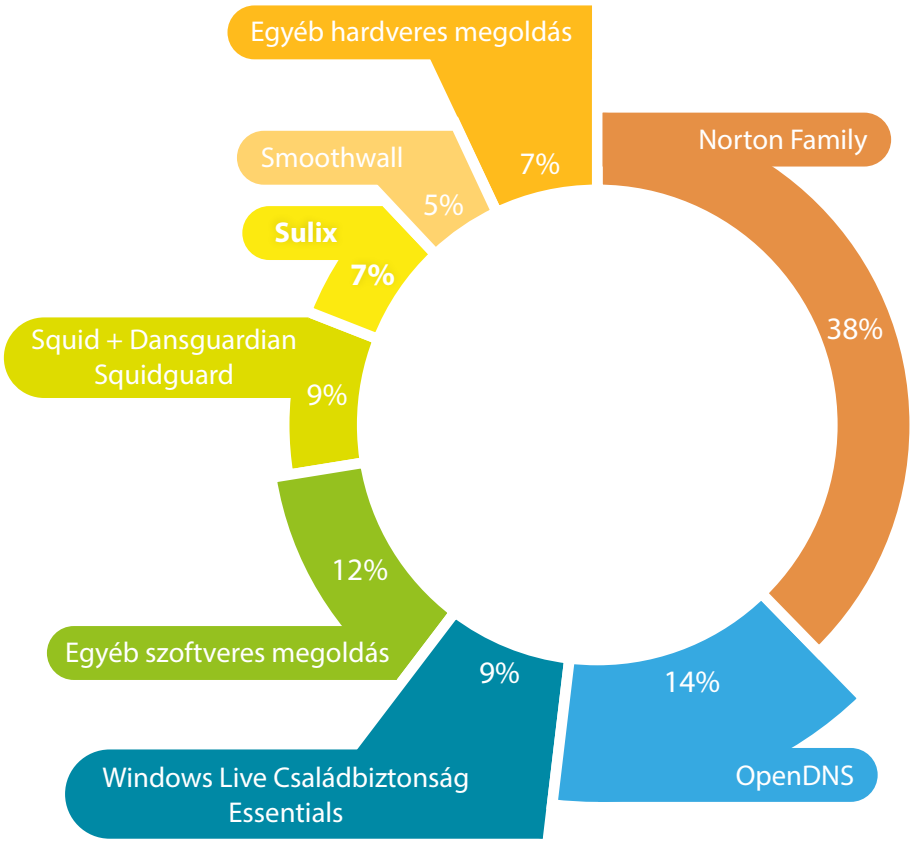
Nemzeti Információs Infrastruktúra Fejlesztési Intézet

1132 Budapest, Victor Hugo utca 18-22

Kedves Olvasónk!

Az NIIF Intézet 2013. január 1-től vette át a korábbi szolgáltatóktól a Sulinet infrastruktúra üzemeltetését, ezen belül a központi szolgáltatások nyújtását és a hálózati hozzáférés biztosítását is. 2015. év első felében merült fel bennünk a gondolat, hogy számos köznevelési intézmény döntéshozójának és rendszergazdájának munkáját segíthetnénk azzal, ha összegyűjtenénk az iskolai, kollégiumi rendszerek üzemeltetése során, az Önök által felhalmozott tapasztalatot, esetlegesen kiegészítve saját ötleteinkkel is.

Jelen kiadványunk apropóját az adja, hogy a nemzeti köznevelésről szóló 2011. évi CXC. törvény módosítása 2014. szeptember 1-től az intézményekre nézve, a gyermekek és tanulók védelme érdekében újabb kötelezettséget ír elő. Ennek értelmében az intézmények kötelesek gondoskodni a gyermekek, tanulók számára hozzáférhető, internet-hozzáféréssel rendelkező számítógépek szűrőszoftverekkel történő ellátásáról.



Bár Intézetünk az Elektronikus Hírközlési Törvény alapján honlapjáról legalább egy, a kiskorúak védelmét lehetővé tevő, magyar nyelvű, könnyen telepíthető és használható szoftver letöltését biztosítja (http://sulinet.niif.hu/szuroszoftver), a gyakorlatban több megoldással is találkozunk. Ezeket szeretnénk most Önökkel is megosztani. A kiadványban szereplő adatok és a megoldások sorrendje az önkéntesen adott és hozzánk beküldött válaszokon alapulnak, az egyszerűsítő értékelést csak a felhasználás megkönnyítése érdekében jelenítettük meg.

eBiztonság Minősítés

A programot a European Schoolnet (Európai Iskolahálózat, www.eun.org) alapította, a szervezet 31 európai oktatási minisztérium hálózatából áll, nonprofit szervezetként célja az oktatási és tanulási innováció eljuttatása az érintettekhez: oktatási minisztériumokhoz, iskolákhoz, tanárokhoz, kutatókhoz és gazdasági partnerekhez.

Az eBiztonság Minősítés célja, hogy az internet- és eszközhasználat, az online megjelenés biztonságos legyen, az intézmények könnyen lépést tarthassanak az eBiztonsági kihívásokkal, értékelhessék saját intézményük infrastruktúráját, irányelveit és gyakorlatát. Segítségével kiderül az intézmény eBiztonsági szintje, illetve hiányosságok esetén az, hogy milyen feladatok elvégzése szükséges a biztonság teljes körű kiterjesztése érdekében.

A minősítésben résztvevő iskolák azon túl, hogy összemérhetik saját intézményük internet biztonsági szintjét más iskolákéval, az értékelés után egy plakettet kapnak, mely első esetben bronz, majd ezüst és, ha minden követelménynek megfelelnek, akkor arany fokozatú. A plakettet az iskola honlapján is elhelyezhetik, jelezve a szülők és a nyilvánosság felé, hogy az iskola számára fontos az eBiztonság.

A programban való részvétel más előnyökkel is jár, az iskolák a közösségen belül megosztják tapasztalataikat, jó gyakorlataikat és más hasznos anyagokat is, továbbá olyan információkat érhetnek el, melyek előrejelzik és segítik kezelni az eBiztonsággal kapcsolatos incidenseket, és fejlődési lehetőséget is biztosítanak a tanárok számára.

További információ: esafetylabel.eu

Fontos megjegyezni, hogy a kiskorúak védelme egy olyan veszélyes közegben, mint az Internet fél-anonim, kontrollszegény világa, valóban rendkívül fontos, azonban mint a társadalmi problémákra általában, erre sem adható pusztán technológiai megoldás. Egy célprogram, vagy infrastruktúra szinten megvalósított szűrés mellett elengedhetetlen az oktatás, nevelés, az Interneten való eligazodáshoz szükséges ismeretek átadása is. A gyermekeket fel kell készíteni arra, amivel az Interneten találkozni fognak és meg kell tanítani őket a szükséges viselkedési mintákra is. Az állandó tanári, nevelői felügyelet biztosítása feltétlenül javasolt, bár hosszú távon nem megoldható, ezért a cél olyan digitális állampolgárok nevelése, akik felismerik a nem megfelelő tartalmakat és akik tudják, hogyan kerüljék el azokat, valamint mit tegyenek, ha mégis találkoznak ilyen helyzetekkel. Ezen cél, kihívás elérésében segíti az iskolákat az Európa-szerte ismert, és már Magyarországon is elérhető eBiztonság Minősítés is. A program az esafetylabel.eu portál segítségével támogatja, hogy a biztonságos internethasználat az oktatási intézményekben a mindennapok részévé váljon.

Köszönjük, hogy megtisztel minket kitüntető figyelmével és ezúton szeretnénk külön kifejezni hálánkat, ha tapasztalatai megosztásával, vagy értékes kérdéseivel is hozzájárult jelen kiadványunk elkészüléséhez!

A Sulinet infrastruktúra üzemeltetői, illetve az NIIF Intézet munkatársai nevében:

Márton Iván
Alkalmazásfejlesztési és -üzemeltetési osztályvezető

Norton Family

Testreszabható és egyszerűen használható szűrőszoftver, mely igen sok előnnyel rendelkezik más tartalomszűrő programokhoz viszonyítva. Az alapcsomag ingyenessége mellett ez is elősegítette, hogy a felhasználó iskolák által legszélesebb körben alkalmazott program legyen, és általános elégedettséget vívjon ki felhasználói körében.

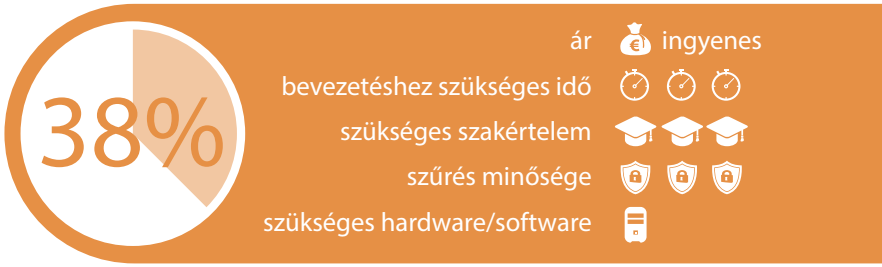
Az üzembe helyezés első lépése a Norton Family fiók létrehozása, mely a szoftver holnapján érhető el. Ezt követően kell telepíteni a szűrőprogramot minden Windows operációs rendszert futtató PC-re (vagy akár Android vagy iOS operációs rendszert futtató okostelefonra). Telepítése egyszerű, felhasználóbarát, nem igényel különösebb szakértelmet, hardver igénye igen alacsony, régebbi, mára már korszerűtlen gépeken is telepíthető (még a sok helyen előforduló Windows XP operációs rendszerre is).

A gyermek profilok létrehozása meglehetősen kényelmes, hiszen csak nevet, nemet és születési évet kell megadnunk a szülői fiókban, nem igényel újabb fiókok regisztrációját. Sajnos egy szülőprofilhoz maximum 15 gyermek profil tartozhat, de semmilyen szabály nem tiltja több szülői profil létrehozását (például egy nagyobb iskola esetén). Gyakran felmerül a kérdés, hogy a szoftver otthoni célú felhasználás mellet oktatási, iskolai célokra is ingyenesen használható-e. A tulajdonos Symantec által, az NMHH részére átadott nyilatkozat alapján a kérdés megnyugtatóan tisztázott. Az állásfoglalás alapján az ilyen célú felhasználás teljes mértékben legális.

A webes felületen keresztül lehet párosítani az eszközöket és a létrehozott gyermek profilokat. Az internetes tevékenységek szűrését számos menüponton keresztül lehet konfigurálni. Apró hátrányként említhető meg, hogy minden gyermekprofilhoz külön kell alkalmazni a beállításokat, ez sokgépes rendszer esetén igen macerás feladattá nőhet. A program lehetőséget nyújt weboldalak „blacklist" alapú blokkolásra, vagy „whitelist" alapú engedélyezésre, emellett majdnem 50 féle tartalom kategória választható ki blokkolásra. Gyorsbeállítási lehetőségként korcsoportonként előre definiált kategóriák is választhatók. Keresés alapú szűrés esetén a legnépszerűbb webes keresőmotorok eredményeinek megjelenítését tudja blokkolni, letilthatók az egyes közösségi oldalak, időkorláttal szabályozhatóak a felhasználók, valamint tilthatók az egyes gépekre telepített alkalmazások futtatása is.
A felhasználók minden webes tevékenysége monitorozható, a rendszer erről naplózást és részletes statisztikát készít, valamint e-mailben értesíti az adminisztrátorokat az esetleges tartalomblokkolásokról, szabályszegési kísérletekről.

Komoly hátrányként lehet megemlíteni a frissítéshez kötött újraindítási kötelezettséget. Számos intézményben van kialakítva a vírusfertőzés és egyéb biztonsági okok miatt az informatikai rendszer úgy, hogy a számítógépek induláskor egy központi rendszerből másolják le a „telepített Windowst" a számítógépre. Mivel minden induláskor egy korábbi működő rendszer beállításait tölti be a gép, ezért a Norton Family letöltött frissítései nem lesznek implementálva az újraindítás ellenére sem. Ez igen sok kellemetlenséget tud okozni, mivel az újraindítást a gomb megnyomása után igen agresszívan, minden program bezárásával (folytatott munkák elvesztésével) hajtja végre. A jelenség kiküszöbölésére a központi rendszerben elvégzett rendszeres frissítés javasolt.

Norton by Symantec



OpenDNS

Az OpenDNS nemcsak hagyományos DNS szolgáltató, névszervereinek használatával (felhő alapú) tartalomszűrés is biztosítható a hálózatunkon, azaz blokkolhatjuk a károsnak ítélt oldalakat.

Két lehetőségünk is van: a regisztrációhoz kötött szolgáltatás használatával testre szabhatjuk, hogy a saját hálózatunkon milyen jellegű tartalmakat szeretnénk szűrni, közel 60 féle kategória alapján lehetséges ezt biztosítani egy kényelmes webes felületen keresztül, az általunk megadott IP címekkel rendelkező hálózatokra, gépekre. Ebben az esetben tudunk konkrét domainre, vagy akár egy domain összes aldomainjére is szűrni; bekapcsolhatjuk a logolást; statisztikákat nézhetünk; illetve testre is szabhatjuk a blokkolt tartalom megnyitásakor jelentkező figyelmeztető szöveget.

A regisztráció nélküli verzióban csak a DNS szerverek IP címeit kell kicserélni a következőkre: 208.67.220.220 és 208.67.222.222 és a tartalomszűrés már az OpenDNS saját adatbázisa alapján történik, nem konfigurálható módon. Szintén regisztráció nélküli speciális lehetőség – az úgynevezett FamilySheild csomagban – a 208.67.222.123 és 208.67.220.123 IP címek használata, ez az alap szolgáltatási csomagtól annyival nyújt többet, hogy nemcsak a veszélyes kódot tartalmazó, adathalász, illetve az egyéb káros hatású oldalakat szűri, hanem a felnőtt tartalmakat is, az ízléstelen besorolásúaktól kezdve egészen a pornográf tartalmakig.

Az OpenDNS nemcsak a tartalomszűrésben segít, hanem a böngészési élményben is. Egyrészt azáltal, hogy gyors hálózattal és névszerverekkel rendelkeznek, így nem fordulhat elő, hogy a névfeloldás lassúsága miatt kell várnunk az egyes oldalak betöltésére. Másrészt használatával az URL-ekben elkövetett leggyakoribb elütések is azonnal korrigálásra kerülnek.

A szolgáltatás használatának előnye az egyszerű beállítás, jó minőségű és hatékony tartalomszűrés, könnyű kezelhetőség és testreszabhatóság, a platformfüggetlenség, valamint az, hogy egyáltalán nem erőforrás igényes; hátránya, hogy bár az OpenDNS használata otthoni használatra ingyenes, azonban oktatási, nevelési intézményekben való alkalmazása már speciális árazás alapján történik, illetve a szolgáltató az alkalmazott megoldások használatával követheti a böngészési szokásainkat.

OpenDNS

Windows Live Családbiztonság

A Microsoft Windows Live programcsomag részeként telepíthető ez a tartalomszűrő szoftver, mely ingyenesen hozzáférhető a cég honlapján. Mivel széles körben elterjedt a Windows operációs rendszer, ezért kézenfekvő megoldás lehet a fejlesztő saját szoftvere, mely egy könnyen telepíthető és üzemeltető szolgáltatást nyújt.

A szoftver telepítése és használata a Microsoft termékekre jellemzően igen egyszerű („tovább, tovább, dőljön hátra, kész!"). A telepítést követően (gépenként) regisztrálni kell hozzá egy Microsoft fiókot, melyet a családbiztonság webes felületén családtagként kell hozzáadni a felügyelő fiókhoz. Így a hozzáadott gépek ezen a felületen keresztül válnak konfigurálhatóvá. Szükség esetén kiegészíthető a fiók további „felnőtt" (felügyelő vagy admin) hozzáadásával.

Sajnos a program nem ad lehetőséget csoport beállítások egységes alkalmazására, viszont egy-egy felhasználó beállítása előre definiált sablonok alapján gyorsan elvégezhető. Elsődlegesen egy lista alapján tiltja bizonyos weboldalak letöltését. Lehetőség van tartalom kategóriák tiltására, mint például az alkohol, drogok, bombagyártás stb. Beállítható ezen kívül még egyéb szabályrendszer is, például a fájlok letöltésének tiltása, játék és programfuttatási korlátozások, a felhasználóknak kiszabható időkorlát, valamint nyomon követhetők a Messenger programmal folytatott beszélgetések is.

A konfigurálást követően a rendszer máris éles. A blokkolt tartalmak betöltésére tett kísérlet esetén jelezi a blokkolást a felhasználónak valamint értesítést küldd a sikertelen próbálkozásról az adminisztrátornak. Nagy előnye ennek a szoftvernek, hogy egy fiók alá tetszőleges számú másik fiókot rendelhetünk hozzá, így több gépterem gépeinek felügyelete is megoldható egy központi fiókból. A webes felület mindenre kiterjedő részletes statisztikát készít a felhasználói eseményekről, és ezekről értesítést is küld. Mivel a tartalom szűrését nem egy a böngészőbe épülő bővítmény, hanem a telepített program végzi, ezért általánosságban minden böngészővel működik. Kifejezetten nagy hátránya, hogy a https alapú weboldalak (például a legtöbb közösségi oldal) nem blokkolhatók, valamint a Windows XP operációs rendszert futtató gépekre a szűrőszoftver nem telepíthető.

Komoly hátrányként lehet megemlíteni, hogy Opera böngésző alatt szinte semmilyen korlátozást nem lehet érvényre juttatni, ezért ennek a böngészőnek a használatát érdemes adminisztratív eszközökkel tiltani. Általános tapasztalat, hogy egyéb böngésző alatt a szoftver kiválóan működik.

ár	ingyenes
bevezetéshez szükséges idő	
szükséges szakértelem	
szűrés minősége	
szükséges hardware/software	

Egyéb szoftveres megoldás

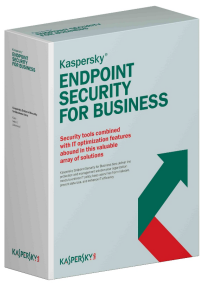
Az egyes, kisebb számban alkalmazott megoldásokat - az eddig megismertekhez hasonlóan – alapvetően két részre oszthatjuk (talán az intézmények számára legfontosabb tulajdonság alapján): az ingyenes és térítésköteles konstrukciókra. Az utóbbi kategóriába a következő megoldások tartoznak: Dolphin Knight School, G Data Endpoint Protection Business, Kaspersky Endpoint Security For Business, K9 Web Protection, Norton ConnectSafe

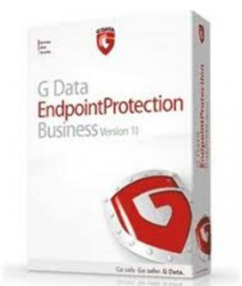
Dolphin Knight School
Teljes mértékben magyar fejlesztés, több verzió érhető el belőle, köztük a speciálisan iskolák részére kifejlesztett Dolphin Knight School verzió. Számtalan előnnyel rendelkezik: 7 éves tapasztalat a magyar iskolai és könyvtári környezetben, magyar nyelvű ügyfélszolgálat és technikai segítség, egy számítógépről vezérelhető az intézmény összes gépén lévő szűrőszoftver; alacsony hardverigény, régebbi Windows verziók támogatása XP-től kezdve; képfeltöltés engedélyezése; facebook tiltás; internet használati idő beállítása; tartalomszűrés teljes domainekre, konkrét URL-ekre, kulcsszavak, szótöredékek alapján; chat, képek és portok szűrése, naplózás stb.
http://school.dolphinknight.com/hu/

G Data Endpoint Protection Business / Kaspersky Endpoint Security For Business
Ezen termékek esetén professzionális, többfunkciós alkalmazásokról beszélhetünk. Tartalmaznak többek között víruskeresőt, tűzfalat, tartalomszűrőt, behatolásmegelőző rendszert. Több platformra is elérhetőek, Active Directory kapcsolattal rendelkeznek. Szerver oldalon van lehetőség saját szabályok beállítására, melyek alapján a hálózaton lévő kliensek elvégzik a tartalomszűrést. A kezelőfelületük átlátható, egyértelmű, sokrétű szűrési szabályt támogatnak, azonban a szükséges hardverigény miatt elsősorban újabb gépek használata esetén javasoltak.
https://www.gdatasoftware.co.uk/business/g-data-endpointprotection
http://www.kaspersky.com/business-security

K9 Web Protection
Ez a szoftver kifejezetten egy webszűrőt takar. A tartalomszűréshez ugyanazt az adatbázist használja, amelyet a gyártó cég (Blue Coat) vállalati partnereinek is értékesít. Telepítés után kényelmes webes felületen konfigurálhatjuk az ízlésünknek megfelelően, szűrhetünk közel 60 kategória alapján, amelyeket akár egyesével tovább is finomíthatunk. Ezen felül lehetőségünk van itt is kulcsszavak alapján történő blokkolásra, időbeni korlátozásra, fekete- és fehérlisták használatára. A megjelenített oldalakról – a kényelmesebb böngészési élmény biztosítása érdekében – a reklámokat is eltüntethetjük segítségével. A hardverigénye és bevezetési ideje alacsony, nem igényel speciális tudást.
http://www1.k9webprotection.com/

Norton ConnectSafe
Az OpenDNS regisztráció nélküli szolgáltatásához hasonló megoldást kínál (előnyök és hátrányok tekintetében is), azonban itt háromféle szabály rendszer alapján tudjuk a tartalomszűrést biztosítani. Az „A" csomagban a károsnak ítélt weboldalakat és programokat, plusz az adathalászatot szűrhetjük. A „B" csomag a pornográf jellegű oldalak szűrésével egészül ki, a „C" csomag tartalmazza az „A" és „B" csomag szűréseit, kiegészítve a nem családbarát tartalmakkal (alkohol, dohány, kábítószerek, erőszak, szerencsejáték, gyűlölet, stb.). Mindhárom csomaghoz két-két, különböző IP címeken elérhető névszerver tartozik.
https://connectsafe.norton.com/





Egyéb szoftveres megoldás

Az alábbiakban ismertetett megoldások közös tulajdonsága, hogy ingyenesen igénybe vehetőek, azonban mind a beüzemeléshez szükséges szakértelem, mind az elérhető platformok tekintetében jelentősen eltérnek.

pfSense
FreeBSD-re épülő tűzfal és routing platform, rengeteg konfigurálási lehetőséggel. Webes felülete bonyolult, kezdeti beállítása szakértelmet igényel és meglehetősen időigényes, cserébe viszont bőven kínál szűrési lehetőségeket: kategória, domain, URL, kulcsszavak, illetve feketelista alapján. Természetesen saját figyelmeztető üzenet is beállítható blokkolt tartalom elérésekor. Képes LiveCD-ről is futni, ekkor nem igényel semmiféle telepítést, de a beállításokat lementhetjük egy pendrivera és bármikor visszatölthetjük azt. Hardverigénye rendkívül alacsony, de külön szervert igényel.
https://www.pfsense.org/

Untangle NG (Next Generation) Firewall
Ez a szoftver egy Debian-alapú, moduláris felépítésű programcsomag, amely a privát hálózatot hivatott védeni. Tartalmaz többek között víruskeresőt, spamszűrőt, tűzfalat, behatolásmegelőzőt (IPS) és természetesen tartalomszűrésre is használható. Nemcsak szoftverként elérhető, hanem külön eszközként (appliance) is megvásárolható előre telepített megoldásokkal. A szoftverből létezik ingyenes verzió, amely alkalmas a tartalomszűrés megvalósítására, azonban speciális, intézményekre szabott árazás szerint elérhető a közszolgálati csomag, amely igazolt állami és önkormányzati intézetek részére biztosít 50% kedvezményt az összes programmodult tartalmazó, teljes funkcionalitású és előre összeállított konfigurációjú megoldás számára. Telepítése egyszerű, azonban – alacsony hardverigényű - dedikált gépet igényel az internet és az intézményi hálózat között.
https://www.untangle.com/

FoxFilter
Némileg kilóg a sorból, hiszen ez egy böngésző bővítmény, amely tartalomszűrésre specializálódott. Már nem hű a nevéhez, hiszen Google Chrome-ra is elérhető, nemcsak Mozilla Firefox-ra. Segítségével tilthatunk domaineket, de kulcsszavak alapján is blokkolhatjuk a nem kívánt tartalmakat. Sajnos az ingyenes verzióban nem tudjuk megakadályozni, hogy a bővítmény letiltásra, eltávolításra kerüljön, ez a funkció csak a fizetős változatban érhető el – a beállításaink több gépen való megosztásának lehetőségével együtt. Előnye, hogy bármilyen gépen használható, ahol a fenti böngészők megtalálhatóak, egyszerűen beállítható, ugyanakkor mivel saját adatbázist használ, a szűrés minősége hagyhat némi kívánnivalót maga után. Nem biztosítja továbbá a támogatott böngészőkön túli védelmet, ezért adminisztratív módszerekkel kell megakadályozni például az Inernet Explorer, vagy az Opera böngészők használatát.
http://www.inspiredeffect.com/FoxFilter/

hosts fájl
Valószínűleg senkinek sem kell bemutatni. Egy lokálisan tárolt szövegfájlról van szó, amely az IP cím és domain név összerendelésekért felelős, bizonyos operációs rendszerek (elsősorban Unix alapú és Windows) esetén még mielőtt a DNS-ben történő névfeloldás következne. A hátránya is ebből fakad, tartalomszűrésre nehézkesen használható, hiszen minden egyes gépen külön kell karbantartani a fájlt, és a használatával figyelmeztető szöveget sem tudunk megjeleníteni, fejlett - kategória, kulcsszó, illetve szolgáltatás alapú - szűrésről nem is beszélve.
http://en.wikipedia.org/wiki/Hosts_(file)

pfSense untangle FOX FILTER

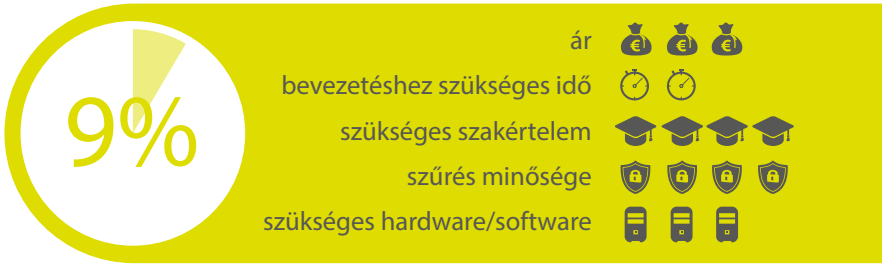
ár	változó
bevezetéshez szükséges idő	változó
szükséges szakértelem	változó
szűrés minősége	változó
szükséges hardware/software	változó

Squid + Dansguardian / Squidguard

A Squid egy teljes körű szolgáltatásokat nyújtó webes proxy gyorsítótár-kiszolgáló, amely proxy és gyorsítótár-szolgáltatásokat biztosít a HTTP, FTP és más népszerű hálózati protokollokhoz. A Squid képes SSL kérések gyorsítótárazására és proxyzására, DNS-kikeresések gyorsítótárazására és transzparens gyorsítótárazásra. A Squid proxy gyorsítótár-kiszolgáló kitűnő megoldás átfogó és részletes hozzáférés-felügyeleti mechanizmusokhoz

Dansguardian
Ingyenesen szerveroldali tartalomszűrő, mely több tartalomszűrő módszert egyesít egy központilag irányított programban. Egyelőre csak Unix alapú operációs rendszeren érhető el. A kifejezés párosítástól kezdve a weboldal címkék alapján történő blokkoláson át az URL tiltó listázásig terjedően sokrétű megoldást nyújt a nem kívánt tartalmak kiszűrésére, mely egy rugalmasan kezelhető, jól konfigurálható rendszerben kap helyet. Hátránya, hogy mivel szerveroldali alkalmazásról lévén szó, magasabb hardver igénnyel rendelkezik (a Squid proxy beállítások miatt sok fizikai memória szükséges) más programokhoz képest, valamint magasabb szakértelmet igényel a konfigurálása, viszont a blokkolás kliens gépekről nem, vagy csak nagyon nehezen kikerülhetőek és azok erőforrásait nem felemésztő megoldást ad.

Squidguard
Szintén ingyenes URL átirányító, amelynek segítségével központilag oldható meg egyes weboldalak feketelistára helyezése. Működési alapját adatbázisokban tárolt listák képezik (ezek között vannak ingyenesen letölthető, de akár fizetős, kereskedelmi listák is), de tud kifejezésekre is szűrni, valamint forráscím és időpont is megadható. Testreszabható, nagyon rugalmas.



Sulix

Az ULX Kft. kereskedelmi terméke, amit az OpenEDU program biztosít iskolák részére. Az OpenEDU programhoz a hazai közoktatási intézmények szabadon és térítésmentesen csatlakozhatnak. A csatlakozást követően a csatlakozott intézmények díjmentesen tölthetik le a program keretében elérhető SuliX szoftverek speciális OpenEDU változatát, a kapcsolódó szolgáltatásokat és a jelentős magyar nyelvű dokumentációt, valamint lehetőséget kapnak a termékekhez tartozó támogatás igénybevételére.

A SuliX egy Linux alapú, nyíltforrású operációs rendszer, amely tartalomszűrő szolgáltatást (Squid alapú proxy szerver) is tartalmaz. Ennek segítségével a SuliXerver által felügyelt hálózaton belül egy átlátható grafikus felületen lehet az internethez kapcsolódó számítógépek számára tartalomszűrést beállítani. A funkciógazdag tartalomszűrési funkció a Biztonság menüpontban a Hozzáférések lapon található meg, segítségével lehetőségünk van az intézményben terem alapú szabályozásra, fehér- és feketelisták használatára, 60-nál is több gyártói kategória alapján történő szűrésre, de időintervallumokra vonatkozó szűrési szabályokat is definiálhatunk. Itt sem maradhat ki a domainek és kulcsszavak alapján történő tartalomszűrés. Ha egy blokkolt oldalt próbálnának elérni a felhasználók, akkor egy nagyméretű, piros színű STOP tábla figyelmezteti őket, hogy tiltott oldalra tévedtek.

Az ULX Kft. egy – a weboldalon bárki számára elérhető – gyártói nyilatkozatban biztosítja, hogy a SuliX szoftverrendszer által biztosított tartalomszűrés teljes mértékben megfelel a vonatkozó törvény által biztosított követelményeknek.

A SuliXerver hardverigénye alacsony, a szolgáltatást elegendő egy megfelelő szervergépen bekonfigurálni, így a kliensgépeken a böngészőkben már csak a proxy beállításokat kell módosítani. Hátránya, hogy nem platformfüggetlen megoldás, valamint – ahol ez nem adott – külön szerver biztosítása és megfelelő hálózat kialakítása szükséges.

http://sulix.hu/

Smoothwall Express

A Smoothwall Express az egyik legnépszerűbb open source, Linuxra épülő tűzfal megoldás. Egyszerűen telepíthető, kevés konfigurálást igénylő program, mélyebb Linux ismeretek nélkül is használható alkalmazás. A webes (akár távolról is elérhető) admin felület letisztult, számtalan beállítási, monitorozási, statisztikai lehetőséget biztosít számunkra. Nemcsak a beállított kategóriák szűrésére képes, hanem tartalom alapján is – megadott kulcsszavak, szótöredékek segítségével. Lehetőségünk van teljes domain vagy megadott elérési út [URL] alapján a tartalomszűrést elvégezni. Testre szabhatjuk a blokkolt tartalom megnyitásakor jelentkező figyelmeztető szöveget. Beállíthatunk mindig engedélyezett címeket fehérlista (whitelist) segítségével, valamint definiálhatunk időintervallumokra vonatkozó szűrési szabályokat. A tartalomszűrési szabályok saját magunk által is karbantarthatók, de frissíthetőek központi adatbázisokból is tetszőleges rendszerességgel.

A Smoothwall Express előnye tehát a rendkívül sokrétű – saját igényeink alapján is módosítható és – hatékony szűrési lehetőség, az ingyenes használat, az átlátható kezelőfelület, az egyszerű telepíthetőség. Az alkalmazás hardverigénye minimális, több éves PC-ken is probléma nélkül működik, elegendő egy megfelelő szervergépen bekonfigurálni, így a kliensgépeken már semmit sem szükséges módosítani. Hátránya, hogy nem platformfüggetlen, csak Linuxra érhető el, valamint – ahol ez nem adott – külön szerver biztosítása és megfelelő hálózat kialakítása szükséges.

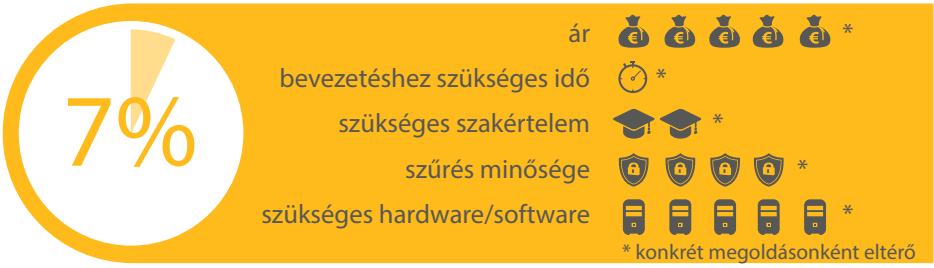
smoothwall®
Web Filtering + Security

Egyéb hardveres megoldás

A felmérésben résztvevő intézmények tartalomszűrésre jellemzően routereket használnak, amennyiben hardveres oldalról közelítik meg a problémát. A legtöbb esetben kisvállalati célra használható routerek vannak használatban, azon egyértelmű előnyüket kihasználva, hogy alacsonyabb áron elérhetőek, mint a professzionális, nagyvállalati megoldások. Az irodai, kisvállalati környezetben alkalmazható routerek hátránya sok esetben, hogy alapértelmezetten nem biztosítanak tartalomszűrést, vagy csak korlátozott funkcionalitású beépített megoldást kínálnak (általában csak néhány előre definiált, gyártói kategória alapján lehetséges a szűrés). Ha nem biztosít tartalomszűrési szolgáltatást az adott eszköz, akkor ezt a már megismert OpenDNS vagy Norton ConnectSafe megoldásokkal tudjuk áthidalni, ugyanis a legtöbb router esetén lehetőség van a DNS kiszolgáló módosítására. Bizonyos gyártóknál előfordul, hogy alapértelmezetten biztosítják ezt a funkciót egyes termékeiknél (pl. Netgear).

Jellemzően magasabb árkategóriájú routereken azonban már komoly tartalomszűrési megoldásokat alkalmaznak a gyártók. Nemcsak a gyártó által karbantartott adatbázisok alapján történik a szűrés, hanem nemzetközi szolgáltatók folyamatosan karbantartott listája szerint (pl. a K9 Web Protection szoftvernél megismert Blue Coat adatbázis alapján – lásd bizonyos ZyXEL eszközök). Az esetek többségében ezeken az eszközökön is beállíthatunk domain, URL, kulcsszó és port alapú tartalomszűrést, amelyeket az egyedi igényeknek megfelelően tovább lehet finomítani. A konfigurálást az egyes routerek webes adminisztrációs felületén tudjuk elvégezni.

Összefoglalva: a hardveres megoldások előnye egyértelműen az, hogy egy külön eszköz végzi a tartalomszűrést, ezáltal a mögötte található hálózaton már semmi módosításra nincs szükség az egyes klienseken (legyen szó akár a hálózatra wifin keresztül kapcsolódó eszközökről). A szükséges módosításokat ebből kifolyólag egy helyen elegendő elvégezni, ami kisebb adminisztrációt és munkaráfordítást igényel. A megoldások hátránya a – jellemzően magasabb – egyszeri, bekerülési költség, valamint egy működő, jól strukturált helyi hálózat megléte.



NETGEAR

ZyXEL