

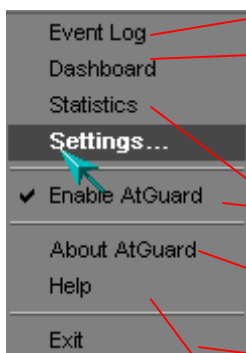


AtGuard (3. 22) Hálózati útmutató Windows'95/98/98SE/NT4-hez. (Ver. 0. 1beta)

Az AtGuard általam ismert információk szerint Windows 2000SP1-en, és Windows Me-n nem fut. A programtelepítés után (majd az ezt követő újraindítás után) a Windows tálcán egy apró ikonral örvendeztetni meg a nagydémüt: . Windows NT alapú rendszerben a Szolgáltatások között találunk még egy **WRQ IAM** nevezetű jövevényt is. NT alatt ugyanis fennállhat egy érdekes helyzet: amikor a számítógépet bekapcsoltuk, de a felhasználó még nem jelentkezett be. Ilyen esetekben a hálózati kommunikáció szűrését OPERÁCIÓS **ENDSZER (System)** felhasználó végzi. Ha a szolgáltatások listájában Automatikusan elindultnak rögzíti, akkor nincs semmi gond. Ellenkező esetben a kedves felhasználó idővel megcsodálhatja a csodaszép KÉK eget rendszerének használata során. A  ikonra kattintva a következő menü hívható elő:




Az **Event Log** (eseménynapló)-ban gyökeretnek majdan a különféle naplózott események, [Erről később](#). A **Dashboard** (pedig a képernyő – általában felső – csíkját jelenti:

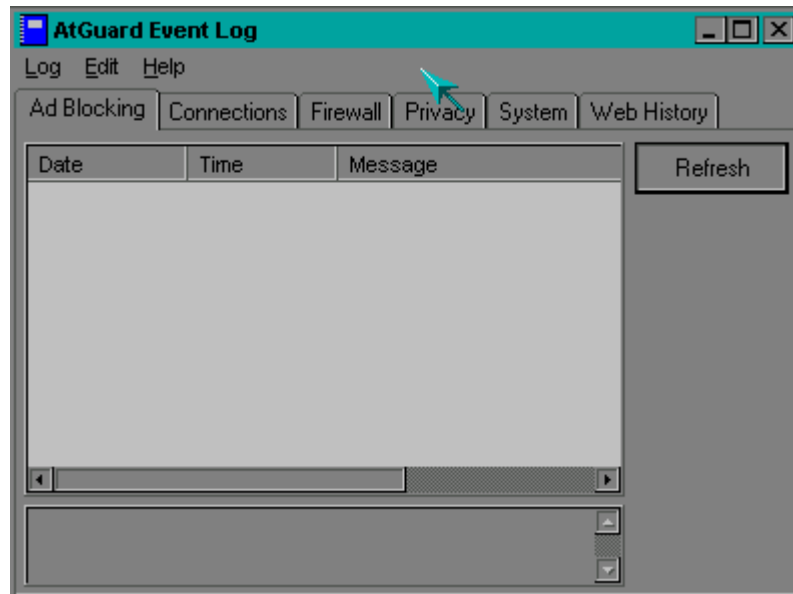


Kezeléséről szintén később. A **Settings**-el a tűzfal szabályokat állíthatjuk be. Erről részletesen [itt](#).

A **Statistics** (statisztika) segítségével hálózati kapcsolatunk(-aink) valós idejű „EKG-képet” követhetjük nyomon. Az **ENABLE AtGuard** -al a tűzfalat kapcsolhatjuk be, ki. Ha látunk „pipát” akkor a tűzfal jelenleg is működik. Az **About AtGuard**-al a tűzfalkészítő (R.I.P) névjegye

tekinthető meg. A **Help** az angol nyelvű súgót hozza előtérbe, az **Exit**-tel pedig a -t zárhatjuk be. NT-ek figyelmébe ajánlom a tűzfal leállításánál az említett **WRQ IAM** -szolgáltatást is. A tűzfal teljes leállításához ezt a szolgáltatást is le kell állítani. Ehhez adminisztrátor szintű jogosultság szükséges. A tűzfal NT- telepítésekor néhány vezérlőjét bepakolja a \Winnt\System32 könyvtárba, ill. ennek alkönyvtárába. Ezekre mind a System (Operációs Rendszer)-nek, mind a Felhasználói csoportnak (User Group) csak olvasás, és futtatás (Read, Execute) jogok szükségesek. Az adminisztrátor Full Control (Teljes hozzáférés) jogát talán nem célszerű elvenni a program file-ok a \Program Files\AtGuard könyvtárban le lehetők fel. Itt, a felhasználói jogok beállításánál csupán azt kell szem előtt tartani, hogy a program a valós idejű naplózásra a ***.rel** fájlokat használja, vagyis ezekhez kell mind az Operációs Rendszernek (System), mind a Felhasználói csoportnak (User Group) Módosítási joggal (Change) rendelkeznie. Amennyiben ehhez nincs joga sem a felhasználónak, sem a rendszernek, úgy a tűzfal-napló megtekintése gyakorlatilag a lehetetlennel párosul. A fájlok a tűzfal működése során gyakorlatilag állandóan nyitott stádiumban vannak. Hiszen ez a hálózati kommunikáció valós idejű nyomkövetéséhez elengedhetetlen.

Event Log:



Az **Ad Blocking** naplózza a program által **HIRDETÉS** –nek talált eseményeket. Amelyik esemény előtt a **BEHAJTANI TILOS** jelenik értelemszerűen a visszautasított kéréseket, amelyiknél a **ZÖLD TÁBLA**, az pedig a fogadott kéréseket jelenti.

A **Connections**-nál az érvényben levő hálózati kapcsolatok jelennek meg.

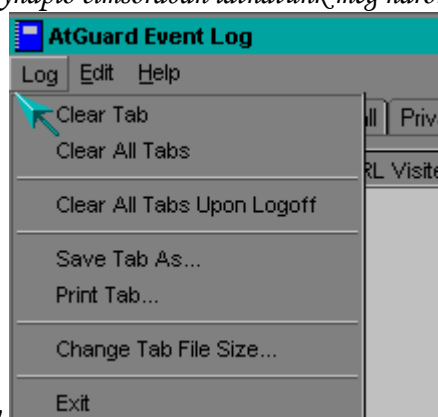
A **Firewall** valójában a **TŰZFAL-LOG**-ként nevezett napló, valójában ebben szerepelnek ezek az információk, melyek a számítógép elleni támadásokat rögzítik.

A **Privacy**-ban szerepelnek a különféle böngészés közben előforduló **Cookies**, **Java Applet**, stb. „**Web**laptya válogattya” elven működő naplózása. Hiszen vannak olyan weblapok, melyek **JavaScript**, vagy **Cookies** nélkül nem elérhetők, vagy megjelenésük enyhén szólva is kívánnivalót hagy(ma)-ga után.

A **System** –ben a rendszerszintű események nyilvántartását csodálhatjuk meg, pl. mikor indult el a tűzfalalkalmazás, mikor állt le, stb.

A **Web-History** az általunk megtekintett **Web**-címekeket rögzíti. Ez roppant hasznos, gyakorlatilag egy szinte korlátlan **VISSZA** gombnak felel meg. Feltéve, ha tudjuk, hogy mit keresünk. Például az **index**-en nem kell állandóan kívárni a **Témák/Törzssasztal/Kjástam a Csatabárdot**, hanem innen kiválasztva csupán kétszer rákattintunk, és már meg is nyílik a böngészőablak, és újra tölti be az oldalt. Persze a **HTML**-hieroglifák, kérdőjelek, hétköznapi felhasználók számára értelmezhetetlen számok nem igazán adnak támpontot, hogy „ha erre rákattintok, akkor mi történik” de idővel megszerezhető –ha meg nem is érthető – az a gyakorlat, amivel ez alapján beazonosíthatóak ezek a hivatkozások.

Az eseménynapló címsorában láthatunk még három hivatkozást:



A **Log**-ban a **Clear Tab**-al törölhetjük az éppen megjelenő „hasábot”, pl. **Ad Blocking**, vagy **System**. A **Clear All Tabs**-al az összes hasábot töröljük. A **Clear All Tabs Upon Logoff** pedig az összes addig nyilvántartott „hasábot” törli amint kijelentkezünk a gépből. A **Save Tab As...**-csupán egy hasábot képes menteni. Ami nem feltétlenül hátrány, tekintve, hogy gyakorlatilag minden támadás a **Firewall** hasábjában megtalálható. A **Print Tab...**-bal pedig kinyomtathatjuk kedvenc „hasáb”-unkat, hogy az unokáinknak meséljük el NE-Ten megesett „kalandjainkat”. Másra nem igen megyünk velük, azon kívül, hogy –az egyre drágább- papírt pocsékoljuk, mivel a tűzfal-logot, úgyis e-mail-ben továbbítjuk az Internet-szolgáltatónak. A **Change Tab File Size...**-vel állíthatjuk be az adott hasáb méretét.

32K, 64K, 128K, 256K, 512K, 1024K, 2048K méreteken. Én a **Firewall**-ra ajánlanám a 2048Kbyte-ot, a **Web History**-ra a 128Kbyte-ot, a többire pedig a 32Kbyte-ot. De mivel izlések, és pofonok különbözőek nyugodtan ebbe bele lehet kötni ☺. Ahhoz, hogy az Új fájl méret érvénybe lépjen, a rendszer újraindítása szükséges. Tehát „használatba vétel előtt” –értsd: Internetre tárcsázás előtt – célszerű beállítani. Különbözően tárcsázhatunk újra –gyarapítva az éppen aktuális telefonszolgáltató egyébként is dagadozó kasszáját (eme csekély megjegyzést „a nem telefonnal, hanem egyéb módon csatlakozók” nyugodtan figyelmen kívül hagyhatják)

Az **Edit**-ben (nem nőnemű kétlábú egyed, hanem **Szerkesztés**) illetve az azon belüli **Copy**, **Select All** a „kijelölöm, beillesztem máshova” szindróma gyakorlóit hivatott kielégíteni. (Csak stílusosan)

A **Help** pedig a már ismert angol nyelvű sűgőt hozza előtérbe.



DASHBOARD

Az itt található pipa segítségével a tűzfalat szintén ki/be lehet kapcsolni. Ez az opció megfelel a korábban említett Enable AtGuard-nak,

Az itt megjelenő szám a netezés közben visszautasított hirdetések száma. Amennyiben a pipát kivesszük az Ads szócéska elől, úgy a továbbiakban a program a hirdetéseket nem vizsgálja.

Ide kattintva az egérgombbal, kilistázódnak a valós idejű hálózati kapcsolataink. Küldött/Fogadott bájtok, a kapcsolatot irányító alkalmazás. Valamint a kapcsolat távoli, és helyi portja.

Itt jelennek meg a program által visszautasított kérések (Web-szűrés) Amennyiben a pipát kivesszük, úgy ezt a lehetőséget kikapcsoljuk. Vannak olyan weblapok, ahonnan csak akkor tudunk letöltést indítani, ha innen a pipát átmenetileg (a letöltés elindulásáig) töröljük. Erre ezek a weblapok általában figyelmeztető üzenetet küldenek.

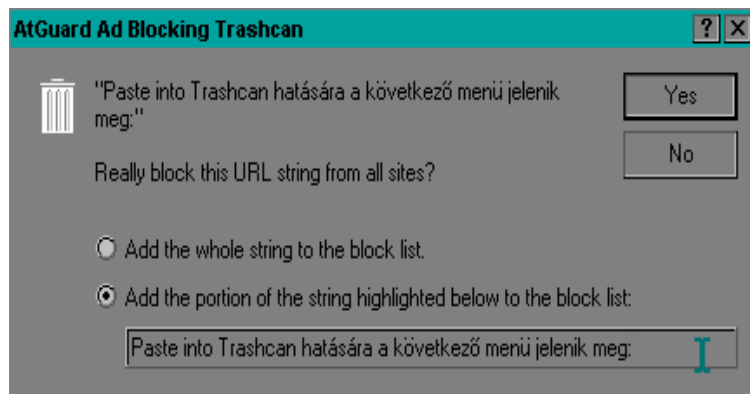
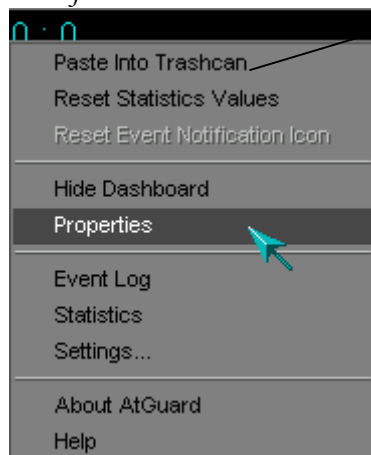
Itt jelennek meg aktív web-es kapcsolataink száma. Ezt a program nem listázza ki részletesen. Ezt a statisztikát a program a böngészőprogramok által generált hálózati forgalom alapján állítja ki.

Itt jelenik meg a fogadott, és visszautasított kérések aránya. Jelige: Nem kell kétségbe esni.

Vigyázzó szemeiteket indiánok ide vessétek. Ez itt a „**kis piros jegyzetomb**” helye. Ez egy figyelmeztetés, mely szerint kápas van. A tűzfal megfogott egy sápadtarcút.

Élelmes indiánok észreveszik, hogy rágcásáljuk jobb szemét megnyomva Az alábbi menü gördül lefele erőteljesen:

Paste into Trashcan hatására a következő menü jelenik meg:

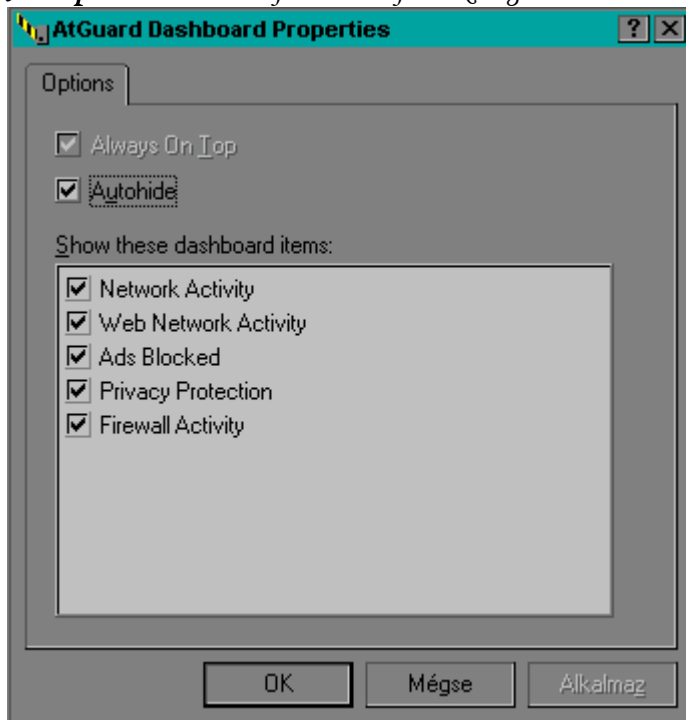


Ennek az újabb ablaknak a segítségével tiltólistára vehetünk fel nem kívánatos HTML kódokat, egyebeket. Csak hozzáértőknek való, aki tudja, hogy mit utasított vissza a programmal. Szélsőséges esetben előfordulhat, hogy egy teljesen ártatlan web-lap sem jelenik meg megfelelően.

A **Reset Statistics Values** –el lenullázhatjuk a statisztikai értéket, ami egy idő után (3-4számjegyű adatok) igencsak hasznos lehet.

A **Hide Dashboard** ezt a szépséges sávot elrejtí a továbbiakban szemünk elől. A sárol tudni érdemes, hogy az „Office Iránytópulthoz” hasonlóan működik, vagyis a képernyő tetszőleges részén elterpeszkédhet,, nem muszáj a felső sávot elfoglalnia.

A **Properties** hatására újabb menü jelenik meg:



Itt szabályozhatjuk a Dashboard megjelenését. Amennyiben az **Always on Top**-on tartjuk, vagyis mindig szem előtt legyen, úgy a hasznos képterület ezzel arányosan csökken. Egyes játékok ezt nem igazán veszik jónéven. Ha problémát tapasztalunk, akkor jelöljük be az **Autohide**-t: ebben az esetben csak akkor jelenik meg a Dashboard, ha a képernyő legfelső pontjához visszük az egérmutatót.

Statistics

Itt jelenik meg egy mindent kielégítő bőséges – ha kell valósidejű - statisztika. Amit elmenthetünk, kinyomtathatunk kényünkre-kedvünkre.

Magyarázatot csupán a **Network Connections**-hoz fűznék:

Network Connections						
Proto	Exec...	Remote	Local	Sent	Recv	Time
A mouse cursor is pointing at the empty table area.						

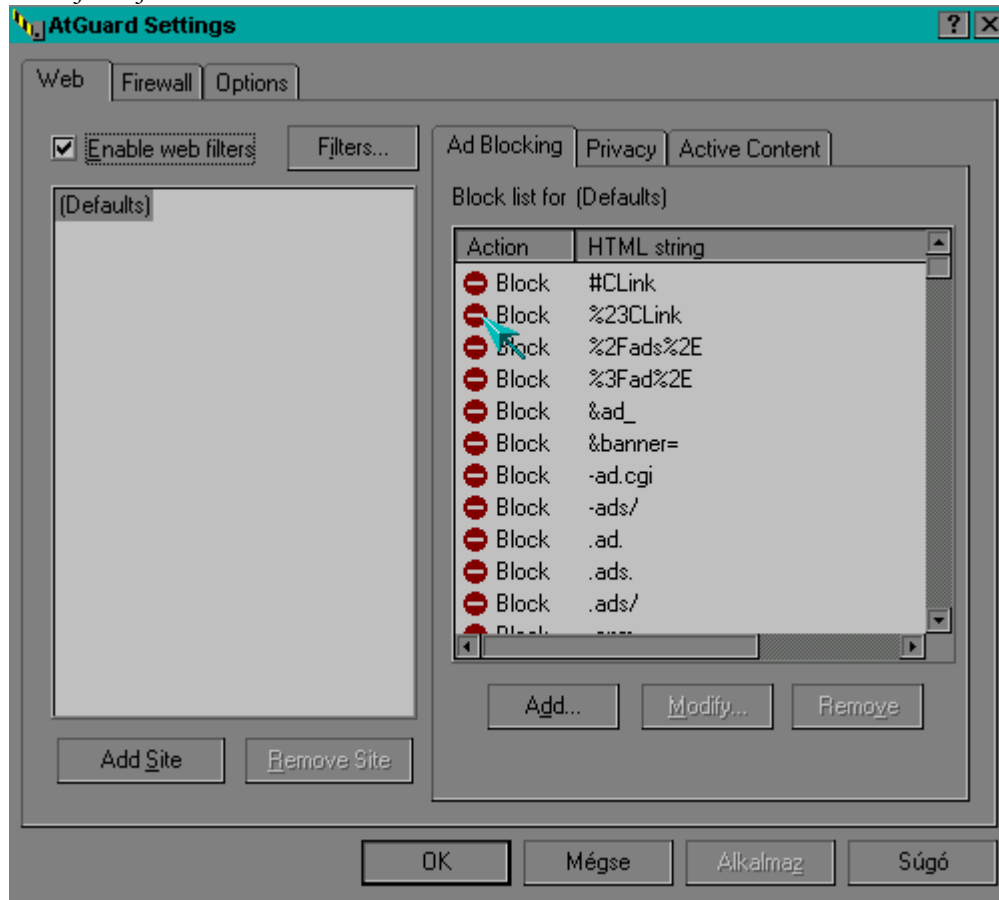
Amennyiben nemkívánatos **TCP** kapcsolatot látunk a listában – (A **Proto** –nál láthatjuk, hogy TCP, vagy UDP) – akkor jobboldali egérgombbal rákattintva feljön egy **Terminate Connection**-nevű opció.

Amire, ha rákattintunk, akkor megszünteti a hálózati kapcsolatot. Erről tudni kell, hogy sajnos nem mindig működik. Pl: A Windows Commander Ftp-kapcsolatai időnként a listában ragadnak. (A pláne az, hogy hiába zárja be a kedves felhasználó a wincmd.exe-t.) UDP kapcsolatot sem tud kilőni.

Ettől eltekintve ha néha-néha bentragad a böngészőnk egy olyan webcímen, amit már régen „elhagytunk”, és a Küldött (sent) illetve Fogadott (received) bájtok száma már egy jó ideje nem változik, akkor nyugodtan löjük kifele. Nem jellemző, de néhanapján előfordul.

SETTINGS!!!!!!

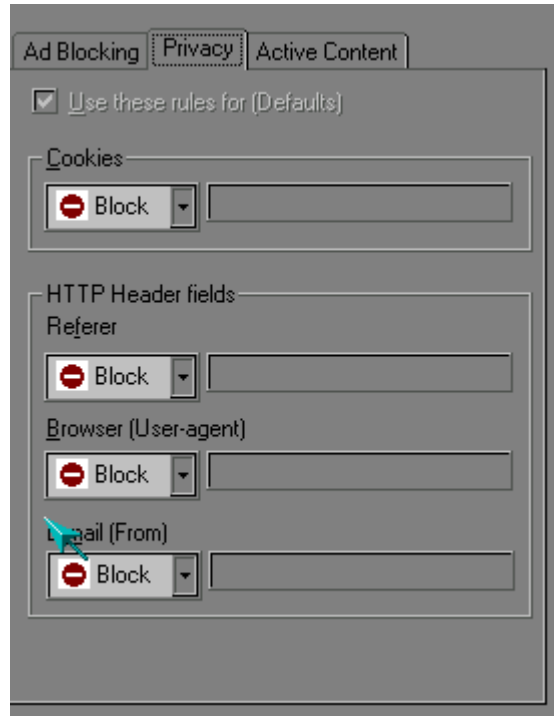
Most jön a java:



Ez a program lelke. A beállítások 3 fő részre tagolódnak. A **WEB** (WEB szűrés), **FIREWALL** (tűzfal), és az **OPTIONS**.

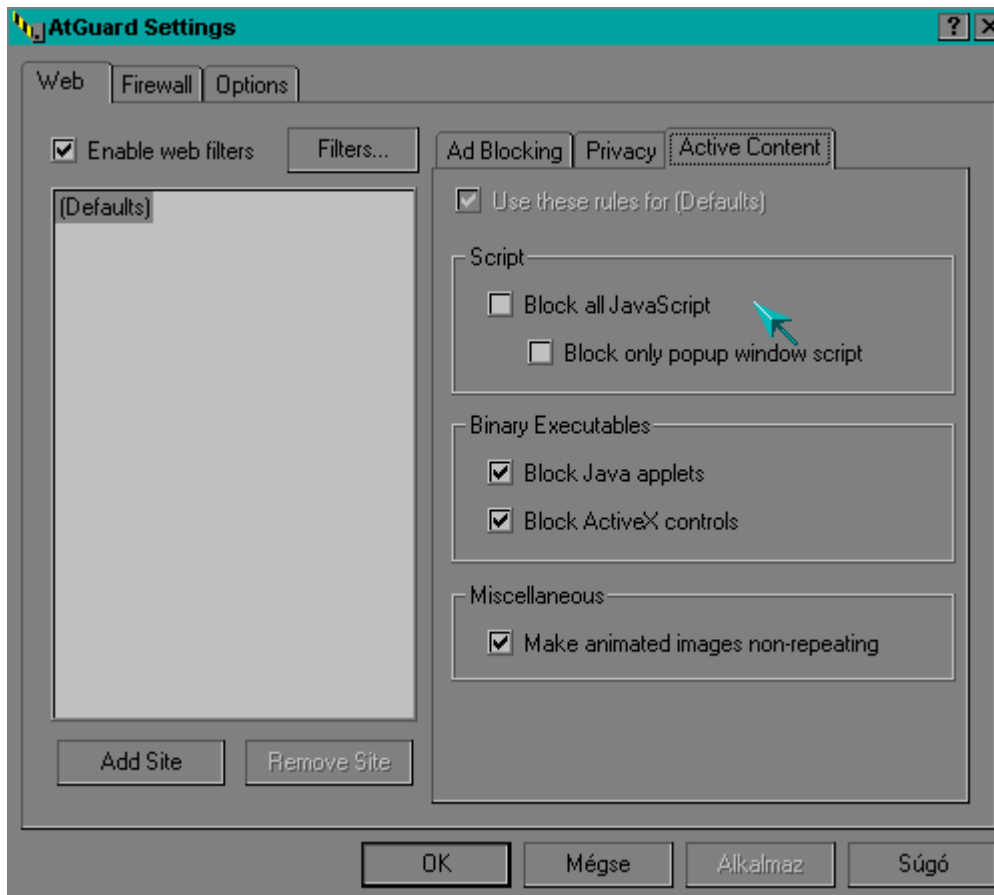
A **WEB**-en belül rendszerszinten, illetve minden egyes weblapra külön külön is beállíthatunk szabályokat. Az **AD Blocking** listán az **Add**-ra kattintva célszerű felvenni azokat a web-helyeket, melyek számunkra semmilyen információval nem szolgálnak fölöslegesen terhelik az amúgy is lassú sávszélességet. Pl: audit.median.hu, illetve a különféle hirdetési nyavalyák. Különböző **HTML** kódokat is felvehetünk a listára, melyeket „látni sem bírunk” 😊.

A Privacy-nál



állíthatjuk be a képen látható értékeket. A **BROWSER BLOCKED** kiválasztásával megakadályozhatjuk a böngészőnek, hogy a weblapok részére közvetítse operációs rendszerünk, illetve használt böngészőprogramjaink típusát, stb. Azt azonban tudni kell, hogyha a Javascriptet engedélyezzük, akkor a webhely mégis képes megszerezni ezeket az információkat. Pl: kezdő.com. Ezeket a beállításokat (vagyis mindent tiltani) célszerű beállítani a (Defaults)-ra. De csak arra!

Az Active Contents

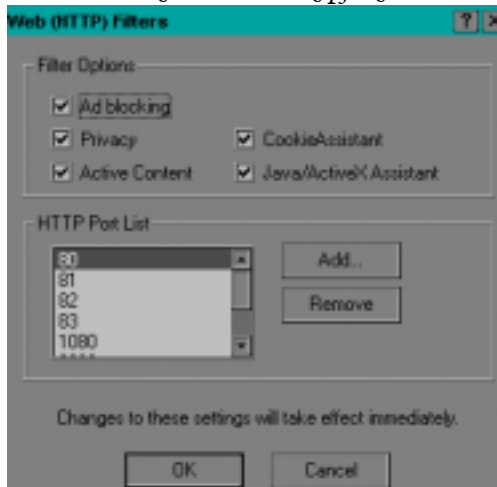


alatt a különféle Java illetve ActiveX vezérlőkre. A (Defaults) értékekre a képen látható a javasolt.

A **Block only popup window script** nem minden esetben célravezető, ugyanis az AtGuard rákérdez ugyan minden weblapnál amelyik Javascript-et használ, azonban mégha akkor engedélyezzük is, akkor sem jeleníti meg a felvillanó ablakokat. Ami elengedhetetlenül szükséges ha pl. a freemail.hu-t szeretnénk használni.

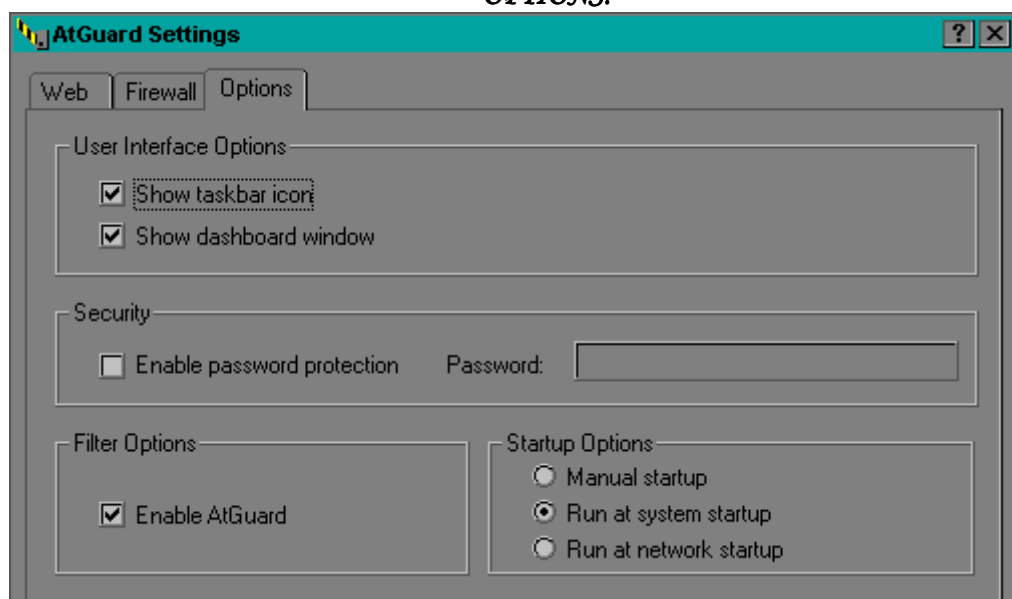
A **Make animated images non-repeating** pedig az animált GIFeknek jelent egy kisebb korlátozást, ugyanis ha ezt bejelöljük, akkor csak egyszer játszsa le a böngésző az animációt megtakarítva egy keveset rendszererőforrásainkból.


A **Filters**-re kattintva ezt kapjuk:



A **CookieAssistant** és a **Java Assistant** az öntanuló módhoz nyújt egy „pluszt”. Ugyanis rákérdez öntanuló módon minden egyes webhelynél, ami használ Cookiest/Java-t, hogy a rendszer fogadja-e vagy sem! A http port listát is testre szabhatjuk, Csak ügyesen!

OPTIONS:

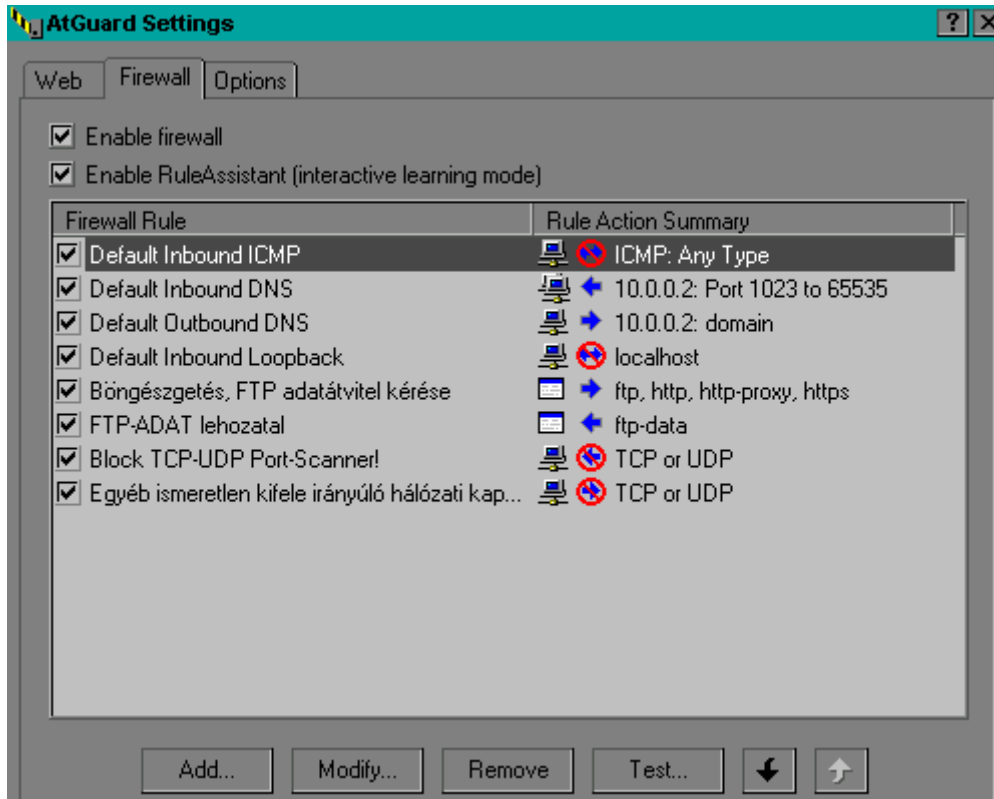


A **Show taskbar icon** jelenti meg a Windows Tálcán az  ikont. A **Show Dashboard window** pedig értelemszerűen a



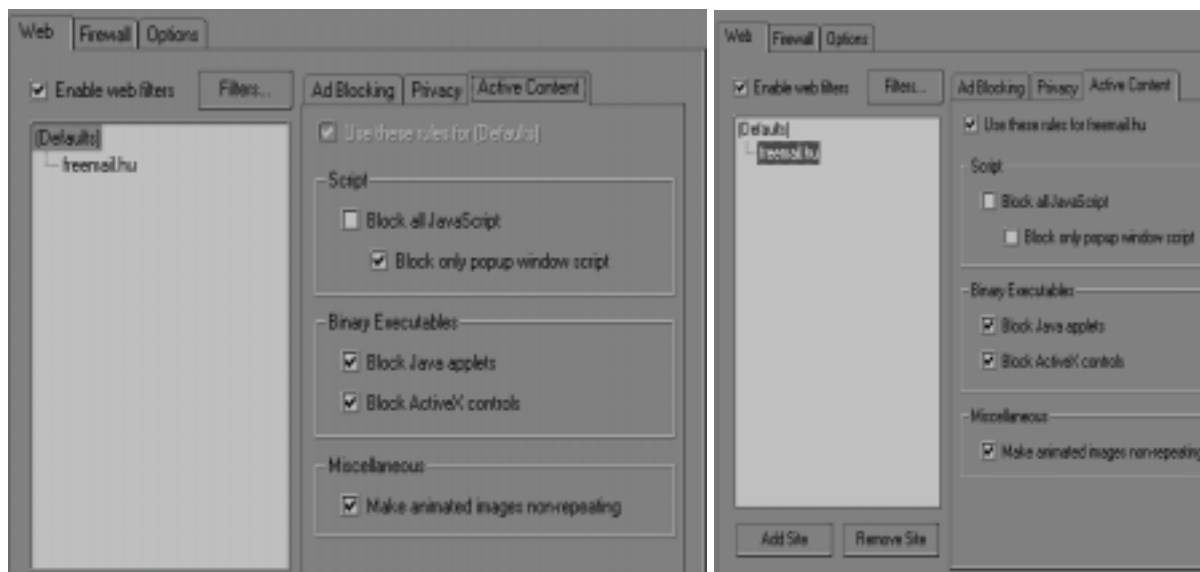
Az **Enable password protection**-nal jelszót állíthatunk be. Ilyenkor minden egyes művelethez, legyen az akár az eseménynapló megtekintése, vagy a tűzfal kikapcsolása, illetve az ÖNTANULÓ RENDSZER működése, mindig jelszót kell bepötyögni. A **Startup Options**- nál a tűzfal indítása állítható be. Win9X-nél célszerű a *Run at network startup*, Windows NT-nél a *Run at system startup*. Gyengébb gépek esetén, melyek csak ritkán kerülnek hálózati kapcsolatba, célszerű a *Manual Startup*.

Firewall



Ez csupán illusztráció, eszébe ne jusson senkinek ezt lemásolni!

Enable Rule Assistant: Ez az öntanuló rendszer beállítását jelenti. Minden előzőleg nem konfigurált hálózati eseményre rákérdez. Például a freemail-en az e-mail küldéséhez szükséges Javascript-re, vagy a Cookies fogadására (ez egyébként nem szükséges a freemail-en, viszont kell a netposta-n). Jellemző probléma, hogy a \Web\Active Content fülnél a felhasználó bejelöli a **Block only popup window script-t** default (alapértelmezett)-ként, és amikor a freemail rákérdez a Javascript-re azt elfogadja, és használat közben csodálkozik, hogy nem tud fájl mellékletet csatolni, vagy egy kapott e-mail forrását nem tudja megnézni. Tehát ha alapértelmezettként bejelöljük ezt az opciót, akkor figyelniünk kell az Öntanuló rendszer ugyanis erre nem vonatkozik, tehát „kézzel” kell módosítanunk a kérdéses címet. Ennek a problémának a felismerése „webhely válogatya kategória” vagyis némi gyakorlat szükséges hozzá. Csak az használja a **Block only popup window script-t** alapértelmezettként, aki felismeri, ha emiatt nem töltődik be egy weblap!



Általános érvényű Tűzfalszabályok beállítása

Az interneteléréshez böngészésre minimálisan az alábbi dolgok szükségesek:

- Rá tudjunk csatlakozni az Internet szolgáltató ún. Domain Name Serverére. Ez gyakorlatilag minden esetben egy oda/vissza irányuló kapcsolatot jelent a számítógépünk, és az ISP Domain Name Server-e között – tehát csak e között – mégpedig az **UDP Protocol 53-as (domain)** portján. Ez egyfajta szabvány.
- Az „internetcímeket” pl. freemail, stb. el tudjuk érni az ún. **web-protollokon a webböngészővel (http, https, ftp, stb.)**

Ennek megfelelően kell beállítani az AtGuard-ot, vagyis gyakorlatilag a teljes telepítés utáni „kezdő” konfigurációt ki lehet törölni kímélet nélkül. A tűzfalszabályok kialakításánál a legfontosabb, amit szem előtt kell tartani!

Az AtGuard FELŐRŐL LEFELÉ halad a szabályokon! Ez azt jelenti, ha már az első sorban minden alkalmazásnak engedélyeztünk mindenféle kommunikációt, akkor a végén semmit nem ér, ha tiltjuk, annyira mintha a tűzfalat kikapcsolnánk. Természetesen ez fordítva is igaz, vagyis ha az elején mindenkinek mindent megtiltunk, akkor a második sorban engedélyezhetünk akármit, nem fog történni semmi.

Akkor nézzük a tippeket:

- **Default Block ICMP** (az icmp továbbítja a ping –csomagokat, és egyéb a hálózati kapcsolat tulajdonságaira vonatkozó információkat, egyáltalán nem nélkülözhetetlen, illetve ismert probléma, hogy ezen a protokollon ún. DoS támadásokat lehet indítani a hálózati forgalom leterheltsége céljából). Az Iránya legyen **Either** (mindkét), és vonatkozzon **Any Adress-re**, mind a local, mind a remote irányban.

Name:

Action:

Direction:

Protocol:

Type Address Time Active Logging

Write an event log entry when this rule is matched.
 Log event after: matches.

Show notification in the dashboard when this rule is logged.

Type: Any Type, Logging/ , vagyis minden 5. után jegyezze fel a naplófile-ba. Ugyanis az ICMP csupán egymás utáni sokszorososa veszélyes. Így ezek az oldalak kerülnek naplózásra. Ettől még az összes ICMP csomagot vissza fogja utasítani a gép, csupán akkor naplóz, ha egymás után 5.-et észlelte. Ha csak egyet észlel azt sem fogadja be, de nem szemeteli tele a naplófile-t. Paranoiások az 5-t egy-re javíthatják, A **SHOW notification in the dashboard when this rule is logged** pedig egy kis piros jegyzetömböt helyez el a megfelelő helyen.☺

- Engedélyezzük a Domain name server-t!:

Modify Firewall Rule

Name:

Action:

Direction:

Protocol:

Application Service Address Time Active Logging

Remote Service

Single service
 Service range
 List of services
 Any service

Service name or port:

Local Service

Single service
 Service range
 List of services
 Any service

First port number:

Last port number:

Az Adress-hez a 10.0.0.2- helyett az ISP domain name serverét kell belőni.
 Ez is szükséges még:

Modify Firewall Rule [?] [X]

Name:

Action:

Direction:

Protocol:

Application Service Address Time Active Logging

Remote Service

- Single service
- Service range
- List of services
- Any service

Service name or port:

Local Service

- Single service
- Service range
- List of services
- Any service

First port number:

Last port number:

Az Application pedig legyen a System!

- *Böngészőprogram engedélyezése:*

Name:

Action:

Direction:

Protocol:

Application Service Address Time Active Logging

Application:

Application shown above
 Any application

Modify Firewall Rule ? x

Name:

Action:

Direction:

Protocol:

Application Service Address Time Active Logging

Remote Service
 Single service
 Service range
 List of services
 Any service

Local Service
 Single service
 Service range
 List of services
 Any service

First port number:
 Last port number:

Name:

Action:

Direction:

Protocol:

Application Service Address Time Active Logging

Remote Address
 Host address
 Network address
 Address range
 Any address

Local Address
 Host address
 Any address

Az általunk megtekinteni nem kívánt webhelyek „Block”-olását célszerűbb a /Web/Ad-fül alatt „hirdetésként” block-olni. Amennyiben a Firewall-nál állítgatjuk be, vagyis minden címre külön külön. Akkor egyrészt mazochisták vagyunk, másrészt a böngészőprogram minden nem kívánt címnél elsőszmötöl egy jó fél percig, megpróbálva a kapcsolatteremtést. Ha viszont a hirdetések között tartjuk nyilván mint nemkívánatos, akkor ez a szöszmötölés nem zajlik le, betölteni meg úgysem fogja.

- Egyéb hálózati címek blokkolása EZ LEGYEN AZ UTOLSÓ ELŐTTI SZABÁLY:

Modify Firewall Rule [?] [X]

Name: [OK]

Action: [Cancel]

Direction:

Protocol:

Application | **Service** | Address | Time Active | Logging

Application: [Browse...]

Application shown above

Any application

Name: [OK]

Action: [Cancel]

Direction:

Protocol:

Application | **Service** | Address | Time Active | Logging

<p>Remote Service</p> <p><input type="radio"/> Single service</p> <p><input type="radio"/> Service range</p> <p><input type="radio"/> List of services</p> <p><input checked="" type="radio"/> Any service</p>	<p>Local Service</p> <p><input type="radio"/> Single service</p> <p><input type="radio"/> Service range</p> <p><input type="radio"/> List of services</p> <p><input checked="" type="radio"/> Any service</p>
--	---

Modify Firewall Rule [?] [X]

Name: [OK]

Action: [Cancel]

Direction:

Protocol:

Application | **Service** | **Address** | Time Active | Logging

<p>Remote Address</p> <p><input type="radio"/> Host address</p> <p><input type="radio"/> Network address</p> <p><input type="radio"/> Address range</p> <p><input checked="" type="radio"/> Any address</p>	<p>Local Address</p> <p><input type="radio"/> Host address</p> <p><input checked="" type="radio"/> Any address</p>
---	--

Modify Firewall Rule [?] [X]

Name: [OK]

Action: [Cancel]

Direction:

Protocol:

Application | **Service** | **Address** | Time Active | **Logging**

Write an event log entry when this rule is matched.

Log event after: matches.

Show notification in the dashboard when this rule is logged.

*Ez a szabály az összes számítógépünk elleni támadást regisztrálni fogja!
Sokszerencsét az eseménynapló böngészéséhez!*

- Ez legyen szabályaink között az utolsó, mely az előzőtől csupán 2 helyen tér el:

Modify Firewall Rule [?] [X]

Name: OK

Action: Cancel

Direction:

Protocol:

Application Service Address Time Active Logging

Application:
 Browse...

Application shown above
 Any application

Modify Firewall Rule [?] [X]

Name: OK

Action: Cancel

Direction:

Protocol:

Application Service Address Time Active Logging

Write an event log entry when this rule is matched.
 Log event after: matches.
 Show notification in the dashboard when this rule is logged.

Ezt elsősorban az FTP letöltések, illetve az ICQ, és egyéb opcionális hálózati kapcsolat miatt nem érdemes naplózni, ugyanis ezek a fenti beállításokkal nem fognak működni!

Ez meggátolja a tudtukon kívüli internetes kapcsolatokat, vagyis hogy rávegyék gépünket arra, hogy különféle kapcsolatokat bonyolítsanak mindenféle.

F. A. Q!

K: Nem működik a fenti beállításoknál az FTP, nem tudok letölteni, és az ftp.xxxx.xxx-en a könyvtárat sem tudom beolvasni.

V: Így van. a Teendő a következő! Az utolsó szabály elől vegyük ki a pipát, majd menj ki az ftp –s címre a böngészővel öntanuló módban. Ekkor az AtGuard rákérdez, hogy a pl. "netscape.exe" kifelé irányuló kapcsolatot kezdeményezett ftp.akarmi.akarhova . Ezt engedélyezni kell a netscape számára , csak az adott ftp-s helyre és kész, az utolsó szabályt ezt követően vissza kell állítani!

K: AZ FTP könyvtárat be tudtam olvasni, a letölteni szándékozott fájlt kiválasztottam, azonban letölteni nem tudom.

V: Az utolsó szabályt ki kell venni, és az előzőhöz hasonlóan kell cselekedni, és engedélyezni kell a netscape.exe számára a befelé irányú hálózati kapcsolatot valószínűleg az „ftp-data” porton. Utolsó szabályt visszakapcsolni!

K: Nem működik a letöltésvezérlőm. (Pl: Download Accelerator).

V: Nyitni kell egy újabb szabályt! Gyakorlatilag a böngészőprogram szabályát kell egy az egyben lemásolni, csupán az alkalmazás neve ne netscape.exe legyen, hanem pl. dap.exe (getright.exe, stb.). Ilyen esetekben külön célszerű ügyelni arra, hogy a letöltésvezérlő melyik honlapra szeretne még ellátogatni engedély nélkül. Ezeket célszerű felvenni a hirdetésblokkoló listára. pl:(downloadaccelerator.com, speedbit.com, stb)

K: A fenti beállításokkal nem tudok internetezni, és Internet explorer-t használok,

V: Az internet Explorernek egy külön szabály kell még : TCP EITHER (Remote Adress: LOCALHOST) Az Internet Explorer ún. localhost-os program, vagyis működéséhez szükséges hogy el tudja érni a 127.0.0.1-es IP címet. Ami gyakorlatilag a Sajátgép. Ne kérdezzétek miért! Nem én írtam ☺!

K: Nem tudok E-mail-t küldeni, fogadni a levelezőprogramommal a saját mail-boxomon.

V: Engedélyezni kell a levelezőprogramot !(Pl. netscape.exe.)

2 szabállyal: TCP Outbound (Remote Adress: mail.mailbox.mailbox) Remote Port: pop3 /ezzel fogadjuk/ és TCP Outbound (Remote Adress: mail.mailbox.mailbox) Remote Port: smtp) /Ezzel küldünk/ Természetesen az utolsó 2 szabály előtt!. Naplózni ezeket felesleges.

K: Windows Nt-t használok, és az RPCSS.exe állandóan ki akar menni a localhostra, nem tudom mit tegyek ..

V: Nem szükséges engedélyezni, megvan anélkül is. Nem kell törödni vele. Ne kérdezzétek miért csinálja! A windows nt-t sem én írtam ☺!

K: Windows Nt-t használok, és az alertsvc.exe állandóan ki akar menni a localhostra...

V: Nem szükséges engedélyezni, megvan anélkül is. Nem kell törödni vele. Ne kérdezzétek miért csinálja! A Norton AntiVirust sem én írtam ☺!

K: Rendszeresen kapok UDP nbname, és nbsession befele irányuló kéréseket. Mit tegyek?

V: Ne ereszd be őket, de – sajnos – célszerű nem naplóztatni, mert tele lenne vele 10 perc alatt.

Célszerű egy új szabályt alkotni (UDP Inbound local port: nbname, nbdatagram Remote Adress Any, és nem naplózni) Jellemzően Windows NT alatt fordul elő.

K: Windows Nt-t használok, és az iexplore.exe állandóan ki akar menni a localhostra, nem tudom mit tegyek ..

V: Engedélyezni kell, ugyanis enélkül nem fogsz tudni netezni. Ne kérdezzétek miért csinálja! Sem a windows nt-t sem az Internet Explorer-t nem én írtam ☺!

Hát nagyjából ennyi így otthoni használat céljából első megközelítésben!

Az AtGuardtól ne várjátok, hogy minden port láthatatlan lesz, viszont stabil, megbízható, széles körűen konfigurálható – gondolok itt a hirdetések, stb. Javascript, stb. szűrésre , amit más tűzfalak nem nyújtanak. Viszont el kell hozzá némi gyakorlat, és hozzáértés. Na de mihez nem ??

További jó netezést!