# Sygate Personal Firewall 5.6


---

## INDEX:



---

## 1/ Het **wat**, **hoe** en **waarom** van een Firewall

***Wat is een firewall?***

Simpel uitgelegd is een firewall een programma dat je PC **beschermt** tegen ongewenste indringers.
Een firewall controleert, filtert en registreert (logt) het **netwerkverkeer** tussen jouw PC en de rest van de buitenwereld.
Verdere info kan je hier vinden: Microsoft - Firewalls

***Waarom heb je een firewall nodig ?***

Firewall > Engelstalige term uit de bouw. Betonnen "brandmuur" die het vuur tegenhoudt, zodat de rest van het gebouw gespaard blijft. De functie van een "firewall" op je pc kan hiermee vergeleken worden.

Het biedt **bescherming tegen bedreigingen via inkomend dataverkeer**, zoals: computerinbraak, hackers, trojans, ...
Goede firewalls controleren ook het **uitgaande verkeer**: hierdoor kan bijvoorbeeld voorkomen worden dat derden je PC gaan gebruiken om andere computers / websites aan te vallen zonder dat je er weet van hebt. (vb: DoS-aanval: je pc wordt buiten je weten om, door de hacker overgenomen om deel uit te maken van een netwerk van tienduizenden pc's die tegelijk een verzoek om info bij een bepaalde site gaat maken. Deze site kan al de aanvragen niet gelijktijdig verwerken en zal uiteindelijk crashen = "denial of service", dienstweigering.

***Hoe werkt een firewall***

Voor het inbreken op uw PC maken hackers meestal gebruik van programma's die, aan de hand van je IP-adres de diverse "**ports**" (= "deuren" die wordt gebruikt voor internetverkeer) op je PC beginnen te scannen op kwetsbaarheden / open ingangen. Wanneer iemand van buitenaf toegang probeert te krijgen tot jouw PC, dan maakt je firewall hier meteen melding van en houdt de poorten **gesloten** door ze te blokkeren of onzichtbaar te maken.

*Iets over "**Sygate Personal Firewall**"*

Sygate Personal Firewall (**Free**) is een voorbeeld van een goede firewall die zowel ingaand als uitgaand verkeer controleert en indien nodig blokkeert. Sygate Personal Firewall is gratis voor persoonlijk gebruik. Een "personal" firewall is een firewall die slechts **één** PC beveiligt.

Sygate is helaas overgenomen door Symantec (NORTON) en wordt niet meer ondersteund (bijgewerkt). Het programma voldoet echter nog uitstekend en wellicht nog voor meerdere jaren.

Er bestaat (bestond?) ook een **Pro** versie van Sygate. Deze is niet gratis. Het verschil zit 'm in een aantal extra services zoals bv de optie "enable stealth mode browsing" waardoor sites je browser(versie) niet kunnen zien ed..., maar voor de doorsnee gebruiker volstaat de gratis versie van Sygate ruimschoots.

De meeste functies / services die bij de gratis versie van Sygate uitgeschakeld zijn, zijn herkenbaar aan de grijze weergave in de (sub)menu's.

***Naar INDEX***

## 2/ Sygate Personal Firewall 5.6 downloaden

Sygate Personal Firewall 5.6 is gratis te downloaden (downloadgrootte = 8,8 MB) vanaf volgende locatie:

**Indirecte download**: Sygate 5.6 via Planet Internet

of: http://www.tucows.com/get/213160_90233?_mid=000002476

***Naar INDEX***

## 3/ Sygate installeren

De installatie van Sygate erg eenvoudig

Toch even de stappen op een rijtje:

**NA DE DOWNLOAD**

- Het is sterk aan te raden om tijdens de installatie van Sygate, de firewall van Windows (XP) uit te schakelen.
- Sluit best ook even de openstaande programma's op je taakbalk onderaan
- Ga naar de locatie waar je het gedownloade bestand hebt opgeslagen, bv het bureaublad, en

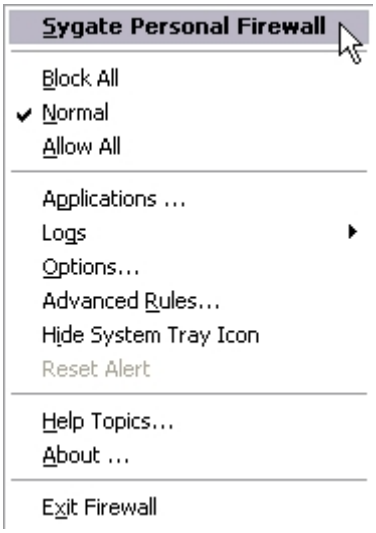

dubbelklik op het icoontje van het bestand: **Spf.exe**

- De welkom installation wizard wordt geopend ---> Klik "Next"
- "License Agreement" opent ---> Vink "I accept" aan ----> Klik "Next"
- Het volgende venster is dat van de "Destination Folder" of de map / locatie waar het programma geïnstalleerd moet worden. Dit is standaard de map "C:\Program Files\Sygate spf". Je kunt deze locatie eventueel veranderen dmv de "blader-knop", maar het is aan te raden deze gewoon zo te laten ---> Klik "Next"
- Klaar voor installatie ---> Klik "Next" (of "Back indien u eerdere instellingen nog wilt veranderen)
- De installatie vindt plaats. Wanneer u meldingen krijgt van andere (anti-malware) progjes bv van Microsoft Anti-Spyware, Spybot S&D, SpySweeper, ... : deze accepteren
- Installatie voltooid ---> Klik "Finish"
- Herstart de PC om de installatie van Sygate Personal Firewall helemaal te voltooien

**NA DE HERSTART**

In de systraybalk (rechts onderaan) bevindt zich nu een icoontje met 2 grijze pijlen. Je zult zien dat Sygate zelf op dit moment nog niet actief is

- Rechtermuisklik op dat icoontje en klik op "Sygate Personal Firewall".




- Je moet namelijk eerst nog een soort van **gebruikersregistratie** invullen: (een) naam + (geldig, eventueel tijdelijk) E-mailadres volstaat. Klik daarna op de knop "Register Now".

Nu is Sygate geactiveerd en wordt je pc beschermd tegen ongewenst inkomend en uitgaand netwerkverkeer. Omdat je nog geen richtlijnen  hebt gegeven aan Sygate over wat mag toegelaten worden en wat niet, heb je op dit moment nog geen netwerkverbinding. De toepassingen "Internet Explorer" moet eerst toegelaten worden. Je kunt Sygate namelijk toepassingen met het Internet laten toestaan(Allow) – blokkeren(Block) - laten vragen(Ask).

***Naar INDEX***

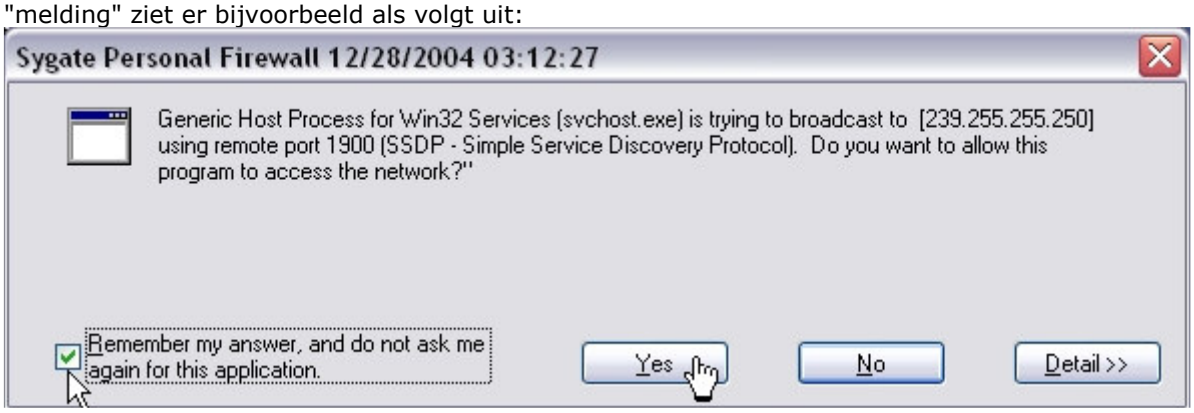
## 4/ Vriend en vijand onderscheiden: Toelaten of blokkeren ?

Bij het puntje over wat een firewall is, werd verwezen naar de oorspronkelijke betekenis van "brandmuur". Toch is er een belangrijk verschil. Waar een brandmuur in een gebouw een complete barrière moet vormen om het vuur volledig buiten te houden, moet er bij een PC-firewall wel een mogelijkheid zijn tot netwerk**verkeer**. Niet alles mag geblokkeerd worden, anders heb je natuurlijk niet veel aan een netwerkverbinding

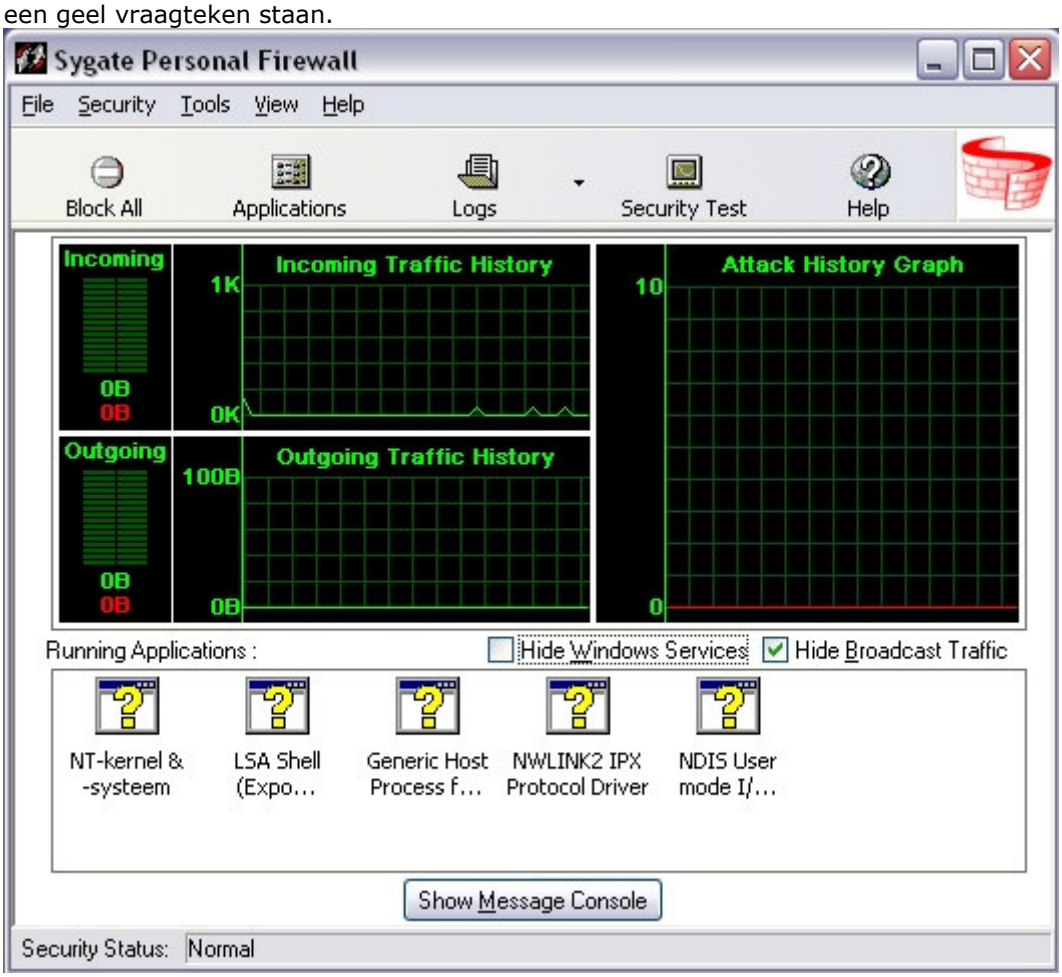
In een PC-firewall moet er dus een soort "**portier**"functie zijn => observatie en controle van binnenkomend en uitgaand "verkeer"

**Specifiek netwerkverkeer** moet doorgelaten kunnen worden. Dit gebeurt door de instellingen te configureren zonder de beveiliging van het netwerk aan te tasten. De firewall beslist, aan de hand van door de gebruiker opgestelde regels, welk netwerkverkeer toegelaten en welk geblokkeerd wordt.

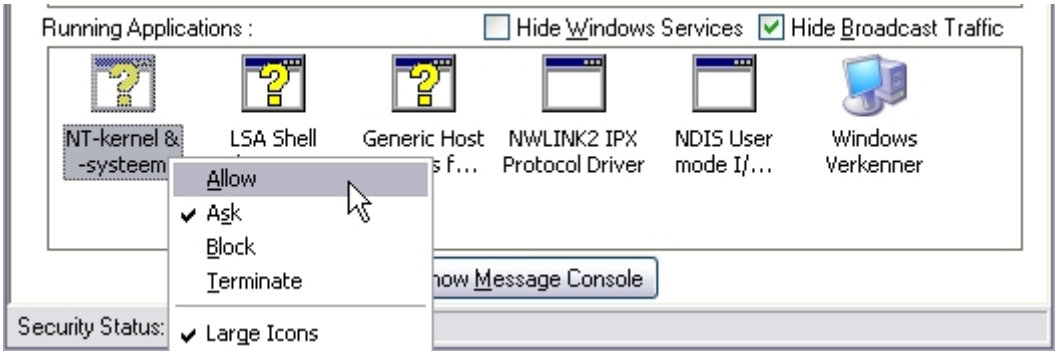
**Hoe ziet dat er concreet uit bij Sygate ?**
Vanaf het moment dat de pc voor de eerste keer sinds de installatie van Sygate opgestart is, ga je aanvankelijk een aantal "meldingen" krijgen van applicaties (toepassingen) die het net op willen en waarvoor je Sygate de toestemming moet geven om deze al dan niet "door te laten". Zo een "melding" ziet er bijvoorbeeld als volgt uit:




Ook zie je in het venster van Sygate, onderaan bij "Running Applications", een aantal items met een geel vraagteken staan.




**Je kunt die, en onderstaande applicaties, veilig toestaan** (rechtermuisklik op het icoontje ---> "Allow")




Kernel
LSA Shell
Generic Host Process
Application Layer Gateway Service (Windows XP)
NDIS User mode I/O Driver

Ook deze toepassingen mogen, indien aanwezig of bij vermelden in zo een kadertje, op "allow":

**Windows 98/ME:**

ICSHAREP.VXD
ICSMGR.EXE
NDIS
NetBeui
IPX
Kernel

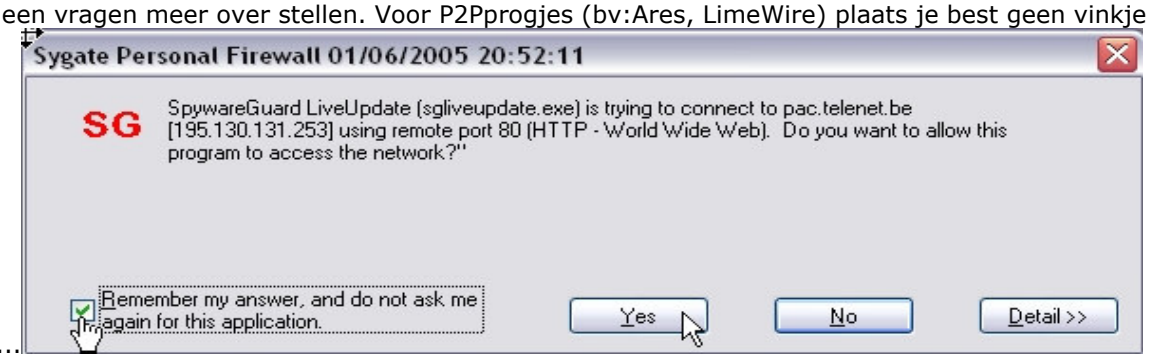
**Windows 2000:**

LSASS.EXE
TCP/IP
NDIS
NetBeui
IPX
Kernel

**Windows XP:**

LSASS.EXE
ALG.EXE
NDIS
Kernel

Telkens wanneer je vanaf nu een programma, dat gebruik maakt van het Internet, de eerste keer sinds de installatie van Sygate opstart, verschijnt er een venster met de vraag of toegang tot het Internet voor dat programma mag worden gegeven. (bv: Outlook, Messenger, enz.).
Je kunt je antwoord (Yes of No) een permanent karakter geven door eerst "remember my answer" aan te vinken. Sygate weet nu wat het in het vervolg met die toepassingen moet doen en zal je er geen vragen meer over stellen. Voor P2Pprogjes (bv:Ares, LimeWire) plaats je best geen vinkje ....



Wanneer je een programma / toepassing dat toegang vraagt tot het Internet, **niet (her)kent**, geef dan vooreerst **geen toestemming**: de kans bestaat dat je een trojan toestemming geeft om te verbinden met het Internet.

Je kunt wel ook eerst de "meer info" nalezen: deze krijg je door bij de betreffende melding, de knop "**Details**" te klikken, dat geeft meer info over de toepassing die het Internet op wil.

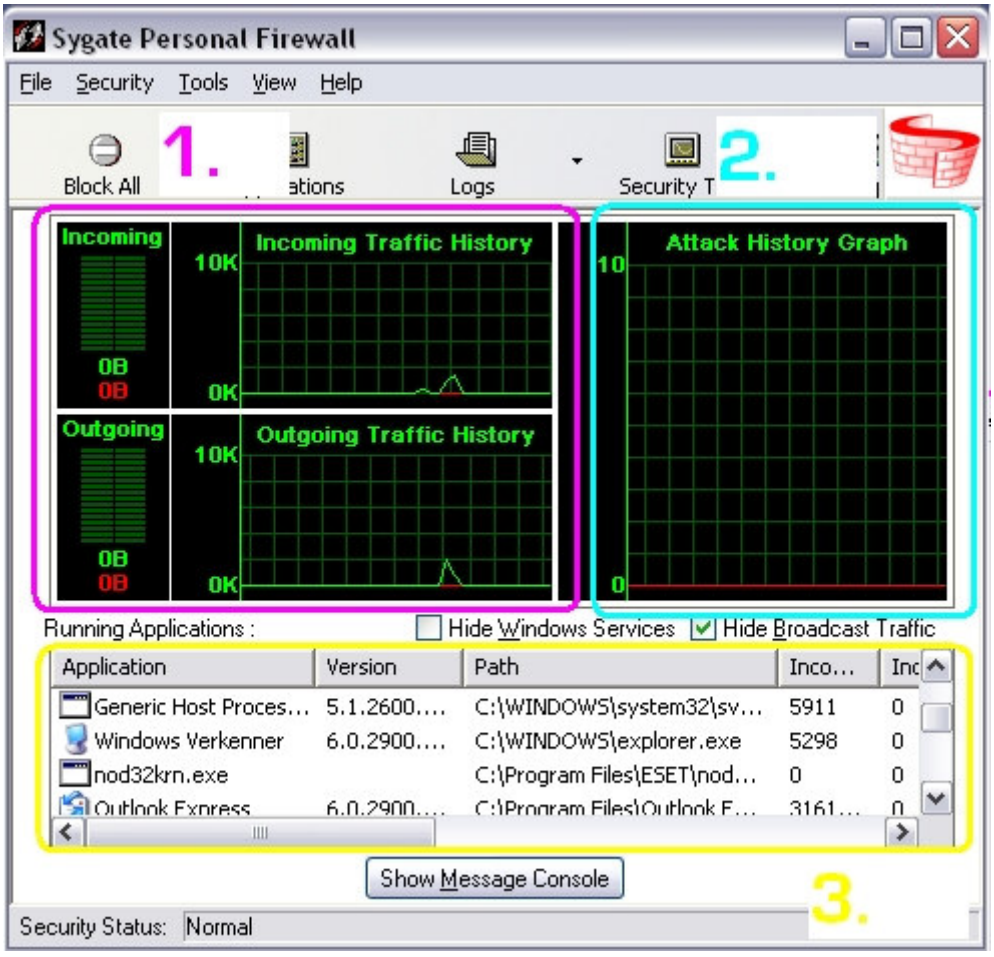
Wanneer je twijfelt, kun je best voor "**No**" kiezen, *zonder* "remember my answer ...." aan te vinken en kijken wat het resultaat daarvan is, of het betreffende bestand opzoeken op Internet (Google, forum, ...) of het te betrouwen is .

Ook niet alles wat om internettoegang vraagt heeft dat daadwerkelijk nodig, bv De Windows Mediaplayer.

***Naar INDEX***

## 5/ Algemene werking: Wat staat voor wat?

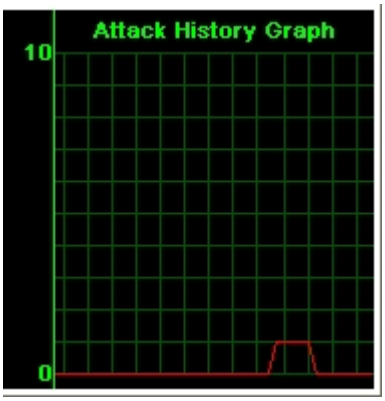
**## Het openingsvenster van Sygate**




* **1. Links** zie je 2 grafieken. Deze tonen het internetverkeer dat gedurende de 2 laatste minuten je PC binnenkomt en verlaat. De bovenste geeft een beeld weer van het verloop van het inkomende verkeer. De onderste toont het uitgaande verkeer. De horizontale as stelt de tijd voor in seconden. Links zie je wanneer er data uitgewisseld wordt, om "hoeveel" data het gaat.
Het gaat zowel om toegelaten, als om geblokkeerd verkeer.

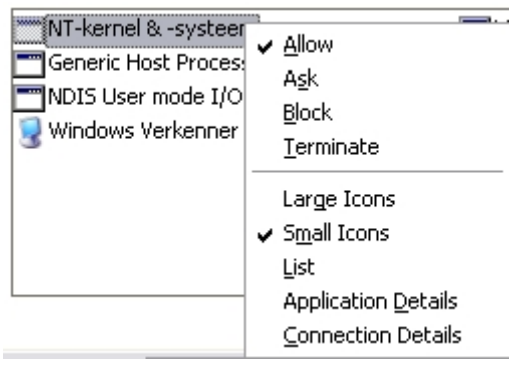
De groene lijnen en balken stellen het totale verkeer voor dat toegelaten wordt om de pc binnen te komen / te verlaten. De rode lijnen en balken wijzen op verkeer dat door Sygate geblokkeerd wordt.

* **2. Rechts** staat een grafiek die weergeeft op welke momenten en in welke mate je poorten aangevallen worden (pogingen tot) en Sygate de gegevensstromen tegengehouden heeft: de "Attack History Graph".
De horizontale as geeft de laatste 2 minuten tijd weer (in sec.) hoe verder af van de verticale as, hoe recenter de "aanval". De verticale as stelt de graad "ernst" van de aanval voor (minor - major - critical). Hoe hoger de amplitude van de rode lijn reikt, hoe ernstiger de aanval was.




* **3. Onderaan** staat een **weergave** van de actieve programma's en services die Internet nodig hebben. Je kunt via het menu "view" deze op verschillende manieren laten weergeven: enkel grote iconen, kleine iconen, als een lijst, met details over de beftreffende toepassing (vb) en met details over de verbinding

Rechtermuisklik op een programma in deze lijst geeft de mogelijkheid om de **status** van die toepassing (application) te wijzigen. De status die de toepassing heeft, is afhankelijk van of jij al dan niet internettoegang ("allow") eraan hebt gegeven. Dat kan hier uitgevoerd zijn, of via een opspringend venster wanneer het programma voor de eerste keer sinds de installatie van Sygate opgestart werd. Je kunt deze status te allen tijde veranderen dmv rechtermuisklik.



- **Allow** = toestaan

verkeer dat veilig beschouwd wordt, omdat je dat bij de meldingen zelf zo aangegeven hebt, bv Internet Explorer, Outlook, normale netwerk- en communicatiesoftware. Ken deze status alleen toe aan applicaties waarvan je zeker bent dat het verbinding mag / moet maken met het Internet (zie deel 1)

- **Ask**= vragen

Telkens wanneer dat programma toegang zoekt tot het Internet, zal het gekende venster verschijnen met de vraag om de toepassing toe te staan of te weigeren. Slechts wanneer je het vinkje bij "remember my answer ….." gezet hebt, zal je betreffende die toepassing niets meer gevraagd worden.

- **Block** = toegang tot Internet weigeren

Verkeer waarvan geweten is dat het gevaarlijk of onveilig is. Of bij twijfel.

- **Terminate** = programma uit de lijst van toepassingen verwijderen.


*Windows Media Player: allow - ask – block*

Verder zie je soms ook kleine blauwe hoekjes verschijnen bij de icoontjes in het onderste gedeelte van het hoofdscherm. Deze geven aan dat de toepassing data ontvangt (links) of verstuurt (rechts) via het net


**## Waarvoor staan de tabbladen in de menubalk ?**


- **File**

- **Close** ---> Sluit het hoofdvenstertje van Sygate

- **Exit Personal Firewall** ---> schakelt de firewall uit zodat je pc onbeschermd is.

- **Security**


Vink hier de optie "**Normal**" aan

Bij "**Block all**" wordt internetverkeer in beide richtingen geblokkeerd

Bij "**Allow all**" wordt aan alle toepassingen, zowel ingaand als uitgaand, internetverkeer toegelaten. Dit wordt afgeraden, want dan kun je net zo goed geen firewall gebruiken.

- **Tools** (deze worden in deel 3 verder uitgediept)


- **Applications** ---> opent de lijst met toepassingen

- **Logs** ---> Hiermee kun je de (4) verschillende logjes bekijken die Sygate opmaakt.
  - ***Security log***, belangrijkste log, toont de aanvallen, poortscans en dergelijke die op de firewall gebeukt zijn / tegengehouden werden.
  - ***Trafic log***. Telkens je pc verbinding maakt met een netwerk, wordt de transactie vermeld in dit logje.
  - ***Packet log***, kan elk data-paketjec dat een poort binnenkomt of uitgaat, loggen. Standaard staat deze logoptie echter uitgeschakeld om megasize-logs te voorkomen.
  - ***System log***. Hier wordt weergegeven wanneer Sygate gestart / beeindigd werd, errors in het progje zelf, veranderingen in de standaard regels (dus bv wanneer je zelf een geavanceerde regel instelt), ...

- **Options** ---> enkele extra security options, bv email alerts, Network Neighborhood browsing rights, log file configuratie, ...

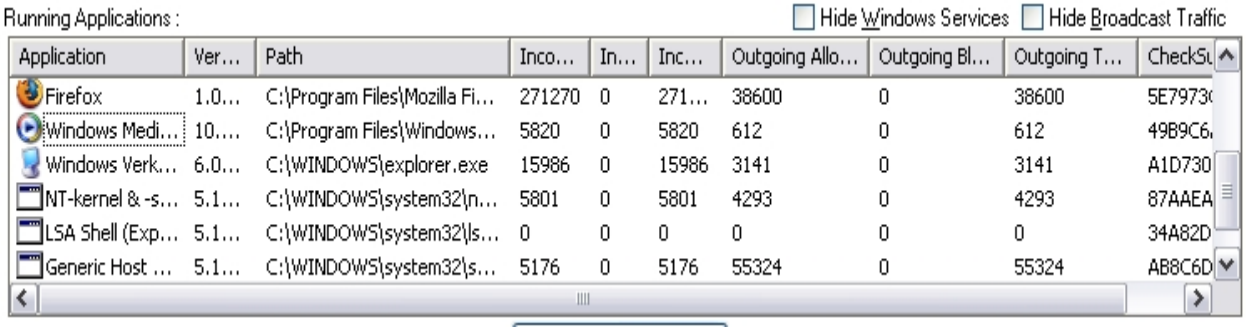
- **Advanced Rules**—> specifieke regels instellen voor de firewall

- **Hide System Tray Icon** ---> als je deze optie aanvinkt, wordt er geen icoontje weergegeven in de systraybalk

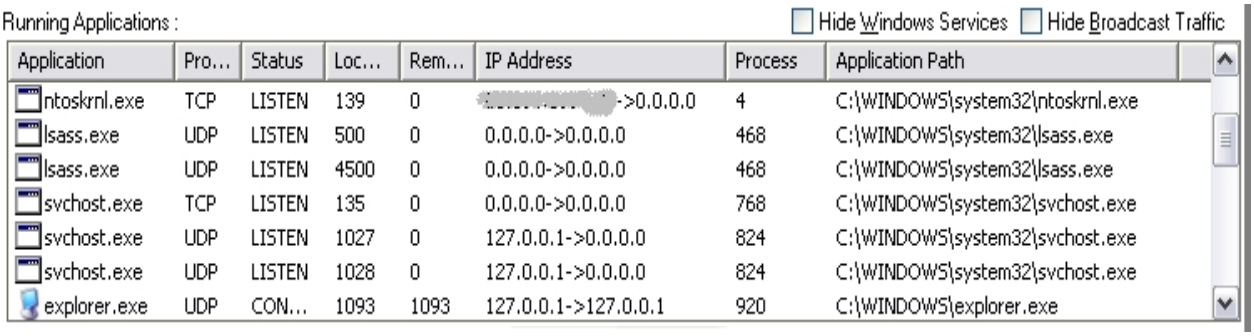
- **Test Your Firewall** ---> Opent de "Sygate Technologies scan site", poortscans en dergelijke, waarmee je de effectiviteit van je Firewall kunt testen.

- **View**

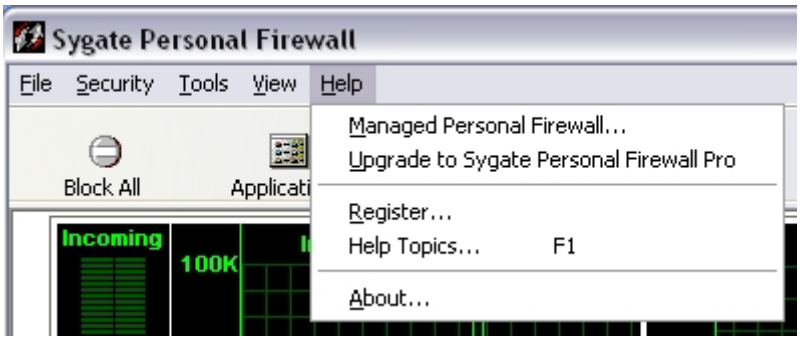

Hiermee kun je de weergave van de icoontjes in het onderste kadertje van het hoofdscherm veranderen : grote icoontjes (32x32), kleine icoontjes (16x16), weergave in een lijst, weergave waarbij details van de betr. toepassingen ("application details") getoond worden, zoals versie, pad, ...:




en weergave waarbij verbindingsdetails ("connection details"), zoals protocol, ip-adres, status, .... getoond worden:



- **Help**




Bevat de helpbestanden ("help topics). Deze zijn uitgebreid, maar wel Engelstalig.
Bij "About" kan je gegevens over je versie van Sygate terugvinden.
Er is ook een optie om je freeware Sygate te upgraden naar de Pro (betalend). De optie leidt je naar deze pagina van de Sygate-site (Nu, Symantec).
Wanneer je op de link "Managed Personal Firewall" klikt, wordt je naar deze pagina van de Sygate-site (Symantec) geleid, waar je en overzicht krijgt van de producten die Sygate aanbiedt.
Bij "Register..." kun je de registratiegegevens die je bij de installatie ingevuld hebt (zie deel 1), zoals naam en e-mail, veranderen.

***Naar INDEX***

## 6/ Systray-Icoontjes van Sygate

Is het icoontje in de balk rechts onderaan op het scherm, waarin zich ook de klok bevindt.
Dit systray-symbooltje is in al zijn weergaven een goede bron van directe informatie over de acties van de firewall.
Het icoontje van Sygate bestaat uit een **naar boven en naar onder wijzende pijl**
De neergaande pijl stelt het inkomend verkeer op de pc voor, terwijl de opgaande pijl het buitengaand verkeer symboliseert.
De pijltjes geven snelle informatie aan de hand van hun **kleur**.
Soms hebben beide pijltjes dezelfde kleur maar dit is niet altijd zo.

**QUOTE**

> **rood** => internetverkeer wordt door Sygate geblokkeerd
> **blauw** => verkeer verloopt zonder onderbroken te worden
> **grijs** => er is geen uitwisseling van gegevens via het net, geen verkeer

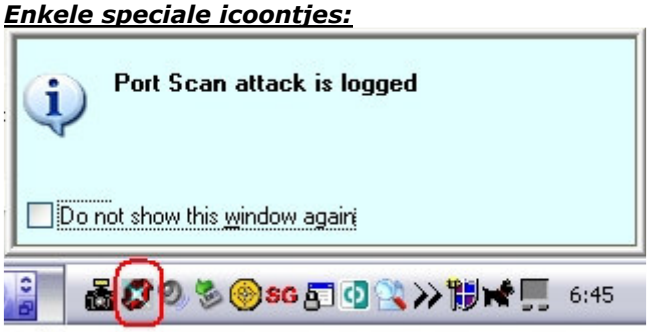
### *9 mogelijke combinaties*

Aan de hand van de betekenis van de kleuren van een pijl, kan je makkelijk de verschillende weergaven van het systray-icoontje van Sygate begrijpen, er zijn 9 "combinaties" mogelijk, waaronder deze:

 => het binnenkomend verkeer (pijltje naar beneden) wordt geblokkeerd (rood), er is geen uitgaand verkeer (grijs opwaarts pijltje)

 => er is ononderbroken (blauw)binnenkomend verkeer, het uitgaand verkeer wordt geblokkeerd (rood)
.... etc

***Enkele speciale icoontjes:***




**Alarm** : er werd bv. een portscan uitgevoerd / er werd gepoogd uw pc binnen te dringen, Sygate heeft hier verslag van gedaan in het security-log (te vinden onder: Tools ---> Logs ---> Security Log). Om het pinkende icoontje weer "normaal" te krijgen: rechtermuisklik op het systray-icoontje ---> "Reset Alert" (meer over "alarm" in deel 3 )

 : al het verkeer wordt door Sygate **geblokkeerd**. Er is geen inkomend en uitgaand verkeer mogelijk.

 : alle inkomend en uitgaand verkeer wordt **toegestaan**.

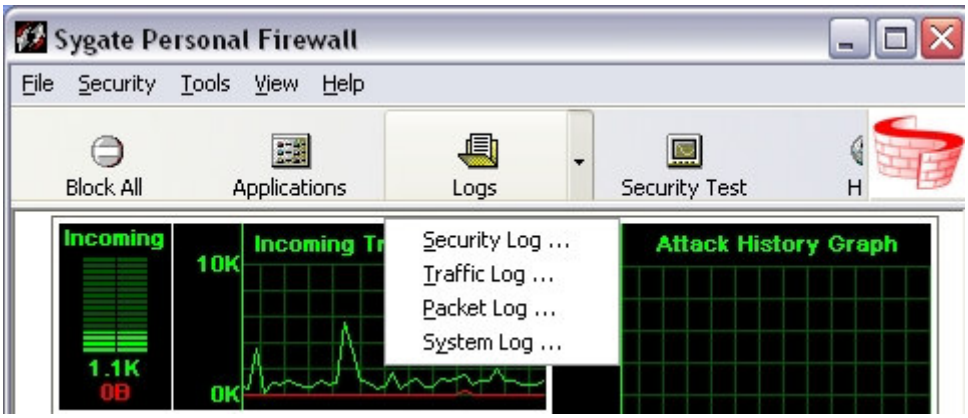
## 7/ Testje

Via Tools (menubalk) ---> **Test Your Firewall** (of simpeler: via de knop "**Security Test**") kun je een aantal scans laten doen om na te gaan of je Sygate wel goed geconfigureerd is en de nodige poorten bij scans/aanvalllen wel degelijk gesloten (closed) of onzichtbaar (stealthed) voor de buitenwereld houdt. Het gaat om de degelijke scans van Sygate zelf die hier terug te vinden zijn.
http://scan.sygatetech.com/

Daarnaast kun je ook bij deze **sites** laten controleren of je firewall z'n werk wel goed doet:
Hackerwatch.org/
PcFlank.com
Shields Up!
Dslreports Portscan
Symantec Security Check (bij deze moet u een active-x element toelaten)
(Opm: *Tijdens* deze scans is het mogelijk dat je Sygate een alarmvenstertje "portscan" geeft, dat is normaal want je poorten worden door de tests gescand of ze al dan niet gesloten zijn )
a² Online Check

***Naar INDEX***

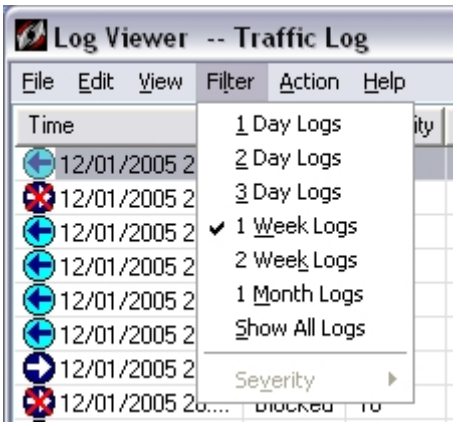
## 8/ Hoe lees je de logs van Sygate ? (basis)



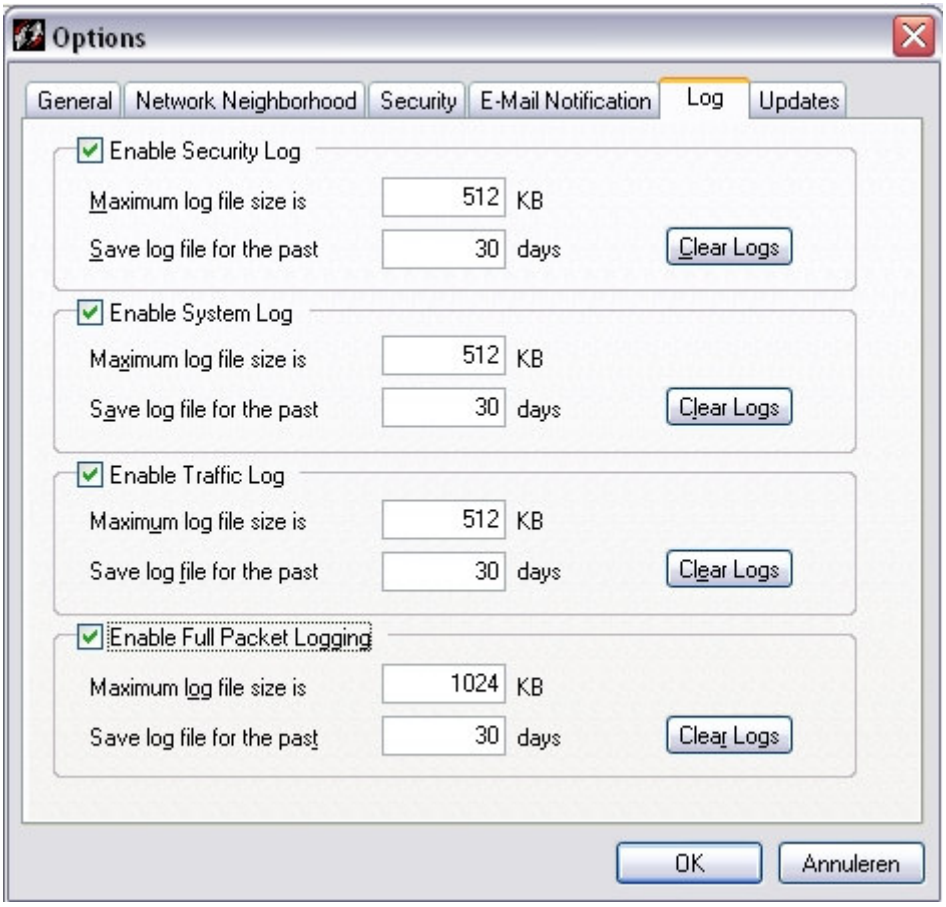

Sygate maakt **4 verschillende** logs op:

Security log - Traffic log - Packet log - System log

Met de **logfilter**, stel je de termijn van de log in:




Voor de instellingen betreffende de **Log-weergave** moet je naar **Opties.**
Klik, hiervoor, in de **Log Viewer** op "File" ---> Options --> Tabblad "Log".



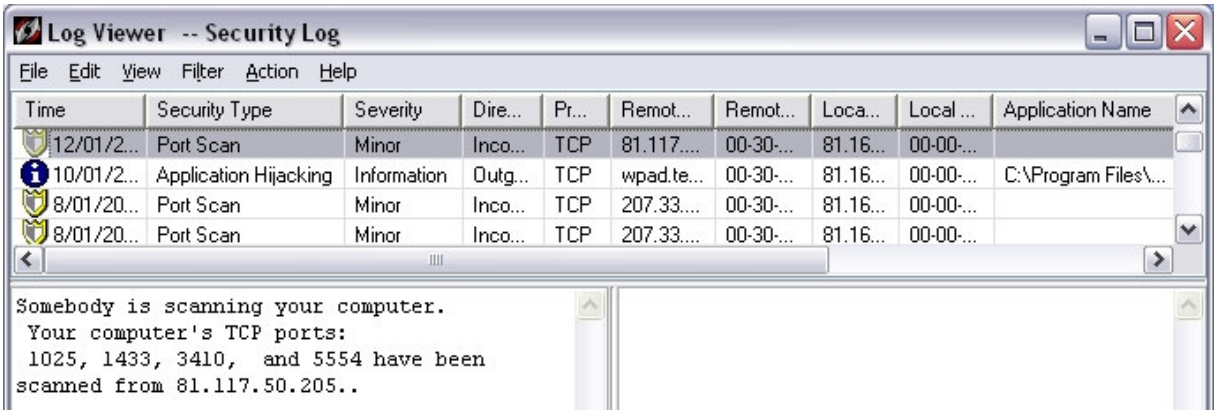

Je kunt aangeven hoe groot elk afzonderlijk logbestand mag worden, hoe lang het bijgehouden moet worden, welke van de 4 mogelijke logs weergegeven worden,...

Standaard staat de weergave van het **Packet log** NIET ingeschakeld, dit omdat deze log snel een enorme bestandgrootte kan aannemen.

Als je deze toch wil weergeven moet deze dus eerst aanvinken in bovenstaand kader

## 8.1. Security log

- **Welke info verschaft deze log ?**




In de Security Log ("beveiligings"-log) worden acties en verkeer genoteerd die schadelijk (hadden) kunnen zijn voor je systeem / netwerk. Zo wordt bv. melding gemaakt van:

**- DoS-attacks**("Denial of Service", weigering van diensten) is een aanval op jouw computer om die van internet af te gooien of hem te gebruiken om een website of ander netwerk te "overbelasten".
Meer info overDoS-aanvallen

- **Port scans**: techniek waarbij men erachter probeert te komen welke "poorten" open staan met als doel op een geopende poort een aanval uit te voeren.
Meer info over portscans

- **Trojan horse attacks** en activiteiten van op de pc aanwezige trojans.
Meer info over trojans

- **Application hijacking** waarschuwing wanneer een programma door andere programma's gestart wordt (bv. Internet Explorer door een kwaadwillend progje)

- **Hack pogingen** in het algemeen.
Meer info over hacken

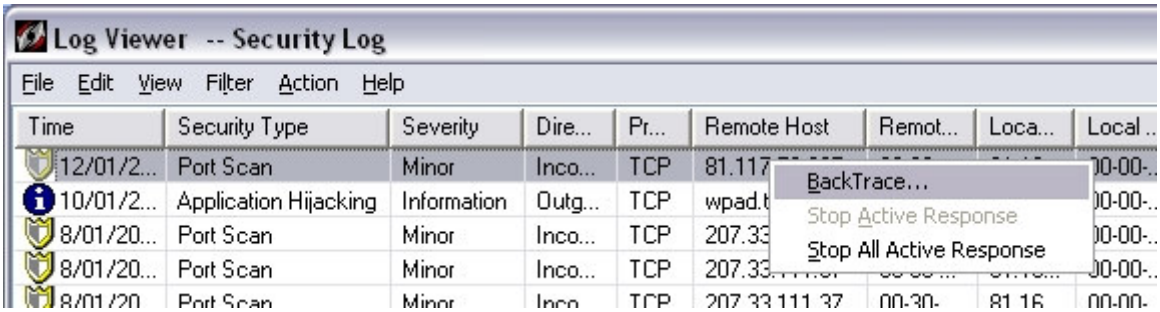
- **Opmerking:** Panikeer niet te snel bij alarmen.

  * Ook poortscans die je bewust laat uitvoeren door firewall-testsites worden hier vermeld.

  * "Application hijacking" is ook niet noodzakelijk kwaadaardig, vaak gaat het om (live-)updates die uitgevoerd worden, patches van progjes die opgehaald worden, ... Kijk bij alarm meldingen eerst even of je het betr. progje *herkent*, vb: bij het prentje hieronder gaat het om het checken voor / ophalen van de updates van het progje SpywareGuard via de live-update functie. Je kan ook uit het door Sygate voor die gebeurtenis gebruikte icoontje afleiden of het om een ernstig voorval gaat of niet.

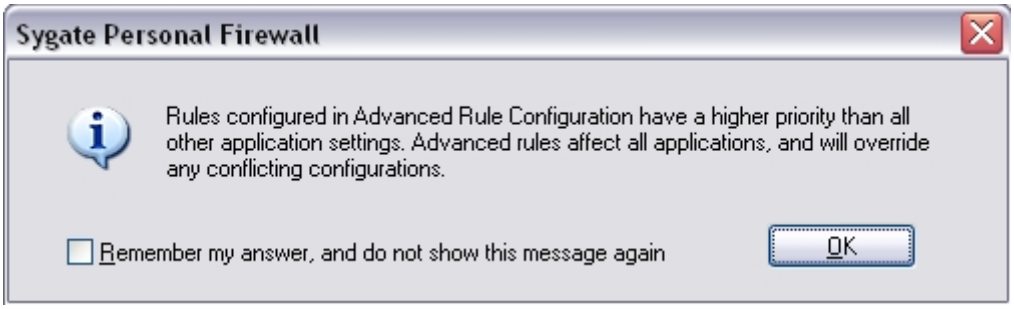
## • Hoe reageren ?

In het menuitem "**Actions**" vind je een aantal mogelijkheden om eventueel "actief" iets met de gegevens van de log te doen.




Met Sygate heb je de mogelijkheid tot een **BackTrace** (opsporing) van bv een IP-adres dat een poortscan of attack uitgevoerd heeft ( => rechtermuis-klik op het betreffende item).
Daarmee kun je via de knop "**Whois**" nagaan, waar de scan vandaan kwam.
Meestal ben je met deze info echter niet zo veel, omdat een hacker deze toch 'wijzigt'.
Het is niet altijd het adres van de oorspronkelijke afzender (= **IP-Spoofing**, vervalsing van een IP-adres). Meestal heeft backtracen dan ook weinig zin.
Backtracen kan wel nut hebben wanneer je, regelmatig, aanvallen van hetzelfde IP-adres ziet terugkeren in de security log. bv om de "abuse" aan te geven, of bv om een **geavanceerde regel** op te stellen waarbij een bepaald IP-adres geblokkeerd wordt ( => Tools --> Advanced Rules)

Meer info over de Advanced Rules




## • Gebruikte symbooltjes bij de Security-log

= Informatie

= Minor attack : kleinere aanval

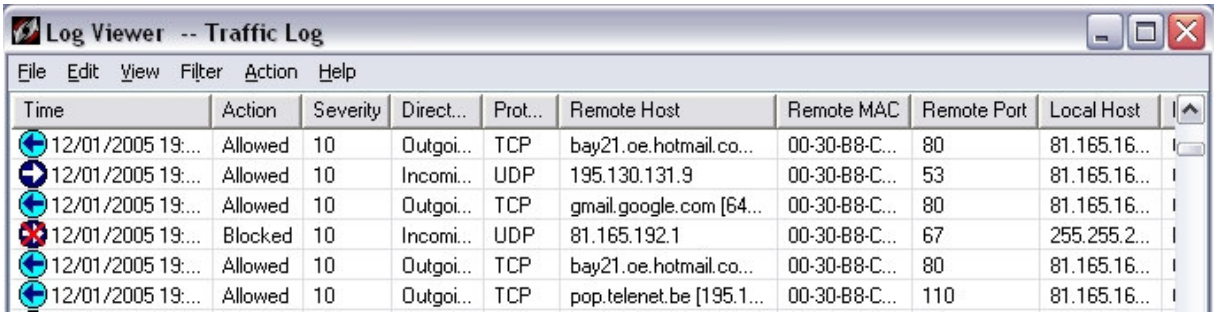
= Major attack : grotere aanval

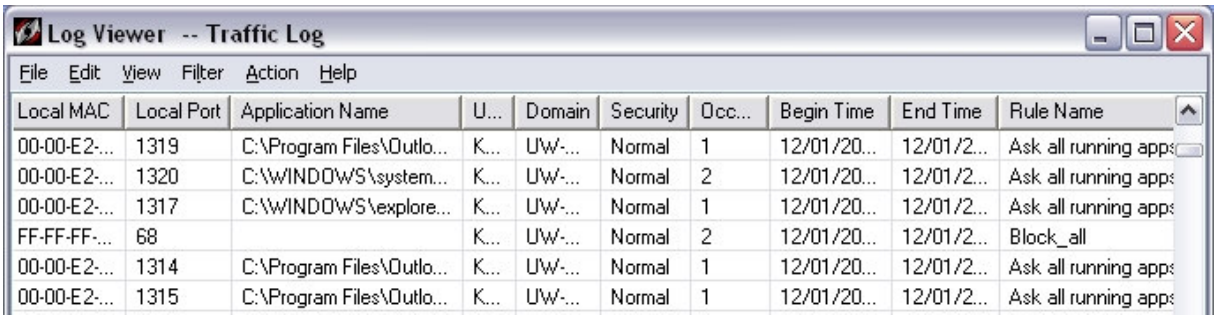
= Severe attack: zware aanval

## 8.2. Traffic log

De Trafic log somt alle transacties op die tussen je PC en het net plaatsvinden en geeft daarbij ook allerlei connectiegegevens weer, of het geblocked of toegestaan werd, ... ed

Ook hier kun je "backtracen"



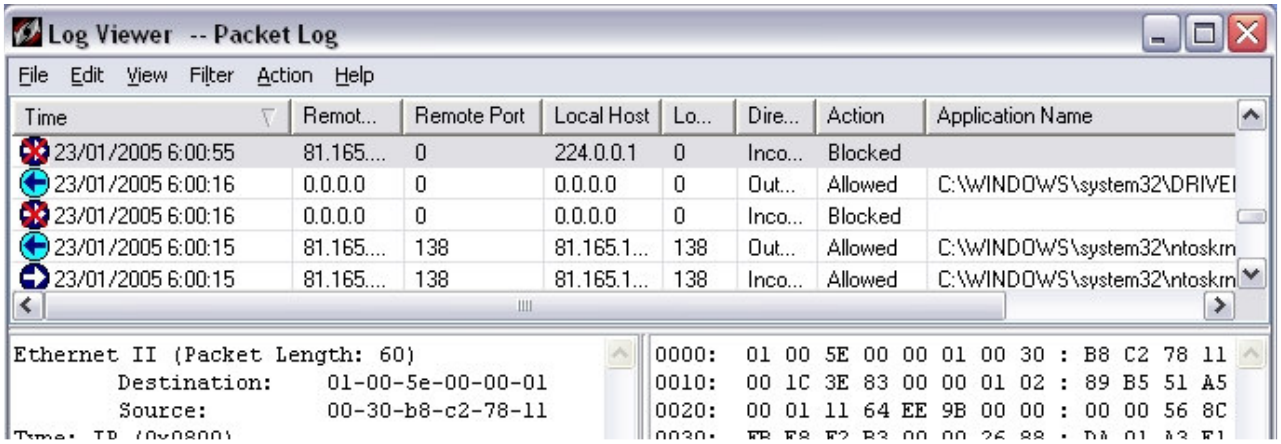




**De betekenis van de verschillende iconen:**

= Toegestaan inkomend verkeer
= Niet Toegestaan en door Sygate tegengehouden / geblokkeerd inkomend verkeer
= Toegestaan uitgaand verkeer
= Niet Toegestaan en geblokkeerd uitgaand verkeer
= Onbekend verkeer dat toegelaten werd.
= Onbekend verkeer dat geblokkeerd werd door Sygate

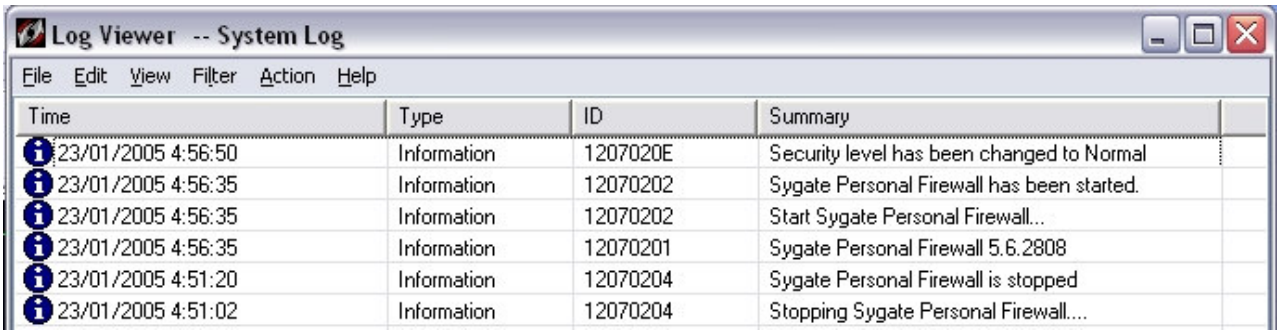
## 8.3. Packet log

Hier wordt alle inkomende en uitgaande verkeer, dat door het systeem / netwerk stroomt, weergegeven. Deze vermeldingen lopen bij even surfen al snel op, vandaar dat de weergave van deze log standaard niet ingeschakeld staat .




## 8.4. System log

De System log toont gegevens betreffende de status van de firewall, zoals wanneer de firewall opgestart werd, uitgeschakeld werd ....




**De betekenis van de verschillende icoontjes van de System log:**

= Informatie over de commando's van de firewall zoals wanneer Sygate opgestart werd, in welk security level, ... (niet te verwarren met hetzelfde icoontje bij Security log)

= Waarschuwing (warning) : geeft aan dat er mogelijk een probleem is met de firewall zelf, of componenten daarvan.

= Foutmelding (error) : toepassingsfouten van Sygate zelf (waardoor wschl de firewall uitgeschakeld is geworden)

# 9/ Nog wat algemene info ivm poorten, firewalls, Sygate

**Poorten**

Bij het lezen en analyseren van de logs kan het wel eens handig zijn om te weten waarvoor de poort-nummers staan. Sites waarin een overzicht gegeven wordt :

http://www.glocksoft.com/trojan_port.htm
http://www.iss.net/security_center/advice/...rts/default.htm
http://www.sans.org/resources/idfaq/oddports.php
http://www.nsc.gr/tcp_ports_used_by_viruses.htm
http://www.microsoft.com/netherlands/bevei...ll/poorten.aspx

***Naar INDEX***