McAfee®

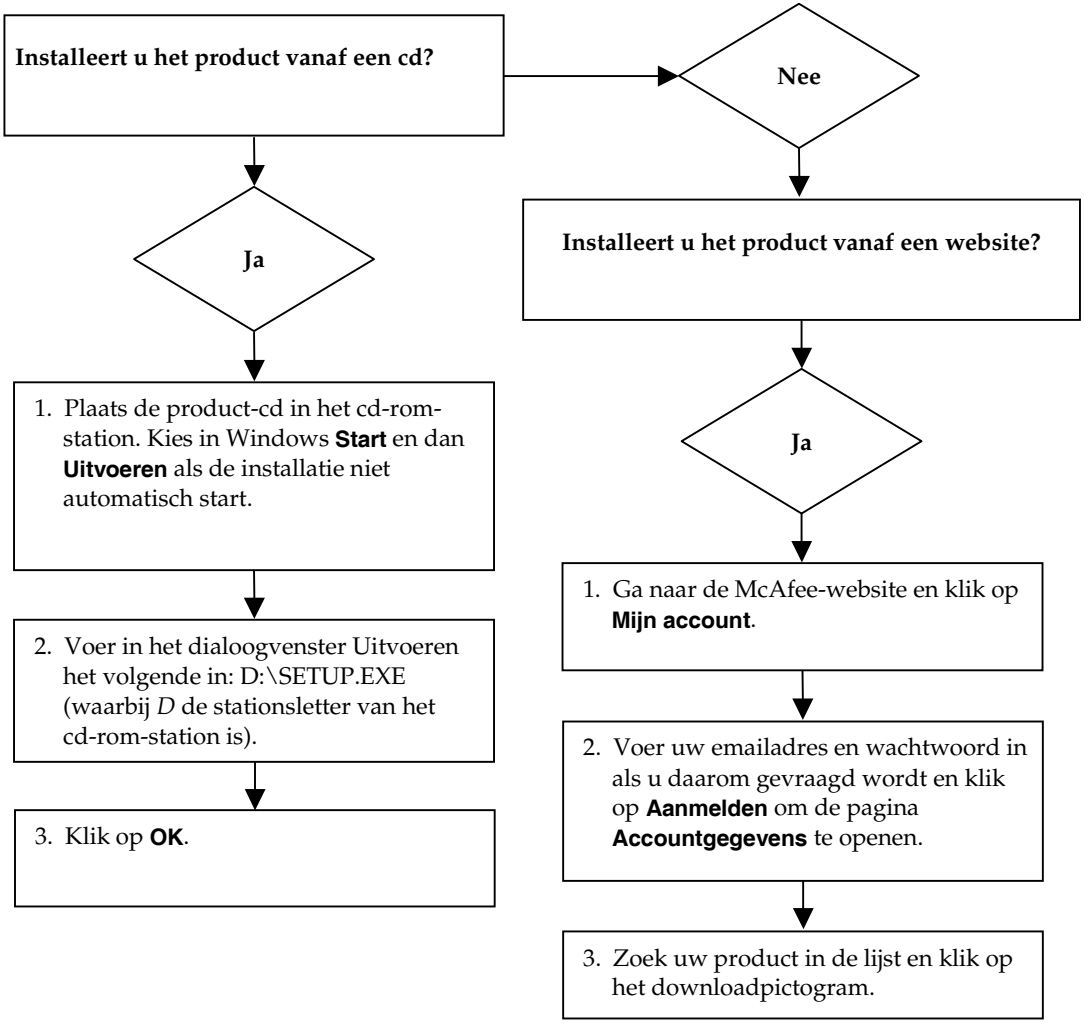
personalfirewallplus

Gebruikershandleiding

McAfee®

Aan de slag

Als u het product installeert vanaf een cd of een website, kunt u deze handige pagina afdrukken ter referentie.



Meer informatie

Als u de Gebruikershandleidingen op de product-cd wilt bekijken, moet Acrobat Reader zijn geïnstalleerd. Als dit niet het geval is, kunt u Adobe Acrobat Reader nu installeren vanaf de product-cd van McAfee.

1. Plaats de product-cd in het cd-rom-station.
2. Open de Verkenner: Klik op **Start** op het Windows-bureaublad en klik vervolgens op **Zoeken**.
3. Zoek naar de map Manuals en dubbelklik op het PDF-bestand van de gebruikershandleiding die u wilt openen.

Voordelen van registratie

McAfee raadt u aan om de eenvoudige registratiestappen in het product uit te voeren om uw registratiegegevens rechtstreeks naar ons te verzenden. Als u zich registreert, kunt u rechtstreeks contact opnemen met een medewerker van de technische ondersteuning. Daarnaast hebt u recht op:

- Gratis elektronische ondersteuning
- Updates voor virusdefinitiebestanden (.DAT) tot een jaar na installatie als u de VirusScan-software aanschaft

  Ga naar nl.mcafee.com om te zien wat u betaalt voor een extra jaar updates voor virusdefinitiebestanden.
- 60 dagen garantie: uw software-cd wordt vervangen bij een defect of beschadiging
- Als u SpamKiller aanschaft, ontvangt u een jaar lang filterupdates na installatie van SpamKiller

  Ga naar nl.mcafee.com om te zien wat u betaalt voor een extra jaar filterupdates.
- Updates voor McAfee Internet Security Suite tot een jaar na aanschaf van de MIS-software

  Ga naar nl.mcafee.com om te zien wat u betaalt voor een extra jaar updates voor inhoud.

Technische ondersteuning

Ga voor technische ondersteuning naar http://www.mcafeehulp.com/.

Via onze ondersteuningssite hebt u 24 uur per dag toegang tot de gebruiksvriendelijke antwoordwizard voor antwoorden op veelgestelde vragen.

Ervaren gebruikers kunnen ook gebruikmaken van onze geavanceerde opties, zoals een trefwoordenindex en Help-structuur. Als u geen oplossing vindt voor uw probleem, hebt u eveneens toegang tot de gratis chatvoorzieningen en E-mail Express! opties. Met behulp van deze voorzieningen kunt u via internet snel en gratis contact opnemen met onze ondersteuningsmedewerkers. U kunt echter ook telefonische ondersteuning krijgen. Voor de contactgegevens gaat u naar http://www.mcafeehulp.com/.

Inhoud

Aan de slag 1

Welkom bij McAfee Personal Firewall Plus.

De software van McAfee Personal Firewall Plus biedt geavanceerde beveiliging voor uw computer en uw persoonlijke gegevens. Personal Firewall vormt een barrière tussen uw computer en internet, waarbij het internetverkeer wordt gecontroleerd op verdachte activiteiten, zonder dat hiervan melding wordt gemaakt.

Als u zich op VirusScan abonneert, beschikt u over de volgende voorzieningen:

- Biedt bescherming tegen toegangspogingen en mogelijke aanvallen van hackers
- Vormt een aanvulling op uw antivirusprogramma´s
- Houdt internet- en netwerkactiviteiten in de gaten
- Waarschuwt u voor mogelijk vijandige gebeurtenissen
- Biedt gedetailleerde informatie over verdacht internetverkeer
- Integratie met de voorzieningen van Hackerwatch.org, waaronder gebeurtenisrapportage, automatische testprogramma's en de mogelijkheid om gerapporteerde gebeurtenissen via e-mail te verzenden naar andere online instanties
- Gedetailleerde functies voor het traceren en onderzoeken van gebeurtenissen

Nieuwe functies

- **Verbeterde ondersteuning van online spelletjes**
  McAfee Personal Firewall Plus beschermt uw computer tegen inbraakpogingen en verdachte activiteiten tijdens online spellen die u schermvullend speelt, maar kan waarschuwingen verbergen wanneer het een inbraakpoging of andere verdachte activiteiten aantreft. Rode waarschuwingen verschijnen pas nadat u het spel hebt afgesloten.
- **Verbeterde afhandeling van toegangsverzoeken**
  McAfee Personal Firewall Plus stelt gebruikers in staat dynamisch toepassingen tijdelijke toegang tot het internet te verlenen. De toegang wordt beperkt van de tijd dat de toepassing wordt gestart tot de tijd dat deze weer wordt afgesloten. Wanneer Personal Firewall een onbekend programma aantreft dat probeert te communiceren met het internet, wordt in een Rode waarschuwing de gelegenheid gegeven tijdelijk toegang te verlenen tot het internet.

- **Verbeterde beveiligingscontrole**
  Met de optie Vergrendelen in McAfee Personal Firewall Plus kunt u direct al het binnenkomend en uitgaand internetverkeer tussen een computer en het internet blokkeren. Gebruikers kunnen de optie Vergrendelen in- of uitschakelen vanaf drie plaatsen in Personal Firewall.

- **Verbeterde herstelopties**
  U kunt nu de functie Opties opnieuw instellen uitvoeren om automatisch de standaardinstellingen van de Personal Firewall te herstellen. Als de Personal Firewall ongewenst gedrag vertoont dat u niet kunt corrigeren, kunt u ervoor kiezen de huidige instellingen ongedaan te maken en terug te keren naar de standaardinstellingen van het product.

- **Bescherming van uw internetverbinding**
  Om te voorkomen dat een gebruiker per ongeluk zijn of haar internetverbinding uitschakelt, is de optie om een internetadres te blokkeren niet opgenomen in Blauwe waarschuwingen wanneer de Firewall waarneemt dat een internetverbinding afkomstig is van een DHCP- of DNS-server. Als het binnenkomende verkeer niet afkomstig is van een DHCP- of DNS-server, is de optie wel beschikbaar.

- **Verbeterde integratie met HackerWatch.org**
  Het aangeven van potentiële hackers is eenvoudiger dan ooit. McAfee Personal Firewall Plus verbetert de functionaliteit van HackerWatch.org, waarmee mogelijk schadelijke gebeurtenissen naar de database worden gestuurd.

- **Uitgebreid intelligent beheer van toepassingen**
  Wanneer een toepassing internettoegang wil, controleert Personal Firewall eerst of de toepassing kan worden vertrouwd of dat deze schadelijk is. Via Personal Firewall wordt automatisch toegang verleend tot internet als de toepassing vertrouwd is, zodat u dit niet zelf hoeft te doen.

- **Geavanceerde opsporing van Trojaanse paarden**
  In McAfee Personal Firewall Plus is het beheer van toepassingsverbindingen gecombineerd met een verbeterde database. Met behulp hiervan worden mogelijk schadelijke toepassingen, zoals Trojaanse paarden, opgespoord en wordt voorkomen dat ze toegang krijgen tot internet en uw persoonlijke gegevens doorgeven.

- **Verbeterde visuele tracering**
  Visual Trace bevat gemakkelijk leesbare grafische kaarten die de bron van vijandige aanvallen en verkeer wereldwijd aangeven, inclusief gedetailleerde contact- en eigenaargegevens van de bron-IP-adressen.

- **Verbeterde bruikbaarheid**
  McAfee Personal Firewall Plus bevat een Configuratieassistent en een zelfstudievoorziening om gebruikers te helpen bij de configuratie en het gebruik van de firewall. Hoewel het product moet kunnen worden gebruikt zonder tussenkomst van de gebruiker, biedt McAfee gebruikers een grote hoeveelheid informatie over de voorzieningen van de firewall.

- **Verbeterde inbraakdetectie**
  Met het inbraakdetectiesysteem (IDS) van Personal Firewall worden veelgebruikte aanvalspatronen en andere verdachte activiteiten gedetecteerd. Elk gegevenspakket wordt gecontroleerd op verdachte gegevensoverdracht of overdrachtmethoden en dit wordt vastgelegd in het gebeurtenislogboek.

- **Verbeterde verkeersanalyse**
  Met McAfee Personal Firewall Plus worden zowel de inkomende als de uitgaande gegevens van een computer weergegeven. Bovendien worden toepassingsverbindingen weergegeven, waaronder toepassingen die actief 'luisteren' naar geopende verbindingen. Gebruikers kunnen zo zien welke toepassingen kwetsbaar zijn voor inbraak en desgewenst actie ondernemen.

Systeemvereisten

- Microsoft® Windows 98, Windows ME, Windows 2000 of Windows XP
- Personal computer met Pentium-compatibele processor
  Windows 98, 2000: 133 MHz of hoger
  Windows Me: 150 MHz of hoger
  Windows XP (Home en Professional): 300 MHz of hoger
- RAM
  Windows 98, Me en 2000: 64 MB
  Windows XP (Home en Professional): 128 MB
- 40 MB aan ruimte op de vaste schijf
- Microsoft® Internet Explorer 5.5 of hoger

Opmerking
Als u een upgrade wilt uitvoeren naar de laatste versie van Internet Explorer, gaat u naar de Microsoft-website op http://www.microsoft.com.

Andere firewalls van de computer verwijderen

Voordat u McAfee Personal Firewall Plus installeert, moet u eventuele andere firewallprogramma's van de computer verwijderen. Volg hiervoor de instructies voor het verwijderen van het desbetreffende firewallprogramma.

Opmerking
Als u Windows XP gebruikt, is het niet nodig om de ingebouwde firewall uit te schakelen voordat u McAfee Personal Firewall Plus installeert. Het is echter aan te raden om de ingebouwde firewall toch uit te schakelen. Als u dit niet doet, ontvangt u geen gebeurtenissen in het logboek van inkomende gebeurtenissen in McAfee Personal Firewall Plus.

De standaardfirewall instellen

Met McAfee Personal Firewall kunt u machtigingen en verkeer voor de internettoepassingen op uw computer beheren, zelfs als Windows Firewall wordt uitgevoerd op uw computer.

Wanneer McAfee Personal Firewall is geïnstalleerd, wordt Windows Firewall automatisch uitgeschakeld door McAfee Personal Firewall en wordt Personal Firewall ingesteld als de standaardfirewall. Alleen McAfee Personal Firewall wordt dan uitgevoerd en u ontvangt alleen berichten van dit programma. Als u vervolgens Windows Firewall inschakelt via het Beveiligingscentrum van Windows of via het Configuratiescherm van Windows, zodat beide firewalls worden uitgevoerd op uw computer, kan dit resulteren in gedeeltelijke logboekregistraties in McAfee Firewall en dubbele status- en waarschuwingsberichten.

Opmerking
Als beide firewalls zijn ingeschakeld, worden niet alle geblokkeerde IP-adressen weergegeven op het tabblad Inkomende gebeurtenis van McAfee Personal Firewall. De meeste gebeurtenissen worden onderschept en geblokkeerd door Windows Firewall, waardoor McAfee Personal Firewall deze gebeurtenissen niet kan detecteren en registreren. McAfee Personal Firewall blokkeert en registreert mogelijk extra verkeer op basis van de beveiligingsinstellingen.

Standaard is de registratie in Windows Firewall uitgeschakeld, maar als u ervoor kiest beide firewalls in te schakelen, kunt de logboekregistratie voor Windows Firewall inschakelen. De standaardlocatie voor het logboek van Windows Firewall is C:\Windows\pfirewall.log

Om ervoor te zorgen dat uw computer is beveiligd met ten minste één firewall, wordt Windows Firewall automatisch opnieuw ingeschakeld als McAfee Personal Firewall wordt verwijderd.

Als u McAfee Personal Firewall uitschakelt of de beveiligingsinstelling **Open** opgeeft zonder dat u Windows Firewall inschakelt, wordt alle firewallbeveiliging verwijderd, behalve eerder geblokkeerde toepassingen.

Het beveiligingsniveau instellen

U kunt beveiligingsopties instellen voor de manier waarop Personal Firewall moet reageren wanneer ongewenst verkeer wordt gedetecteerd. Standaard is het beveiligingsniveau **Standaard** ingeschakeld. Wanneer u in het beveiligingsniveau **Standaard** een toepassing toegang geeft tot internet, geeft u de toepassing volledige toegang. Bij volledige toegang mag de toepassing zowel gegevens verzenden als ongevraagde gegevens ontvangen op niet-systeempoorten.

Beveiligingsinstellingen configureren:

1 Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Opties**.

2 Klik op het pictogram **Beveiligingsinstellingen**.

3 Stel het beveiligingsniveau in door de schuifregelaar naar het gewenste niveau te schuiven.

Het beveiligingsniveau varieert van Vergrendelen tot Open:

- **Vergrendelen —** Alle internetverbindingen van uw computer worden afgesloten. U kunt deze instelling gebruiken om poorten met een open configuratie voor de pagina Systeemservices te blokkeren.
- **Strikte beveiliging —** Wanneer een toepassing een bepaald type toegang vraagt tot het internet (bijvoorbeeld alleen uitgaand), kunt u dit deze toepassing toestaan of weigeren. Als de toepassing later volledige internettoegang vraagt, geeft u op dat moment de toepassing Volledige toegang of beperkt u de toegang tot Alleen uitgaande toegang.
- **Standaardbeveiliging (aanbevolen) —** Wanneer een toepassing toegang tot internet vraagt en deze ook krijgt, betreft het volledige toegang voor de afhandeling van zowel binnenkomend als uitgaand verkeer.
- **Vertrouwende beveiliging**: **—** alle toepassingen worden automatisch vertrouwd wanneer er verbinding met internet wordt gemaakt. U kunt Personal Firewal echter zo instellen dat u wordt gewaarschuwd wanneer er nieuwe toepassingen op uw computer worden aangetroffen. Gebruik deze instelling als bepaalde games of streaming media niet werken.
- **Open**: **—** uw firewall is uitgeschakeld. Bij deze instelling mag alle verkeer Personal Firewall passeren zonder dat er wordt gefilterd.

Opmerking
Voorheen geblokkeerde toepassingen blijven geblokkeerd wanneer voor de firewall de beveiligingsinstelling **Open** of **Vergrendelen** wordt gebruikt. Om dit te voorkomen, kunt u de machtigingen voor de toepassing wijzigen in **Volledige toegang toestaan** of verwijdert u de machtigingsregel **Geblokkeerd** in de lijst met **Internettoepassingen**.

4 Selecteer extra beveiligingsinstellingen:

Opmerking
Als op de computer Windows XP wordt uitgevoerd en er meerdere XP-gebruikers zijn toegevoegd, zijn deze opties alleen beschikbaar wanneer u als beheerder van deze computer bent aangemeld.

- **Gebeurtenissen inbraakdetectie (IDS) vastleggen in logboek van inkomende gebeurtenissen —** Als u deze optie selecteert, worden gebeurtenissen die door IDS zijn gedetecteerd, in het logboek van inkomende gebeurtenissen weergegeven. Met het inbraakdetectiesysteem worden veelvoorkomende soorten aanvallen en andere verdachte activiteiten gedetecteerd. Met inbraakdetectie wordt elk inkomend en uitgaand gegevenspakket gecontroleerd op verdachte gegevensoverdracht of overdrachtsmethoden. Deze worden vergeleken met een database met 'handtekeningen' en de pakketten die van de verdachte computer afkomstig zijn, worden automatisch geblokkeerd.

  IDS zoekt naar specifieke patronen die door aanvallers worden gebruikt. IDS controleert elk pakket dat op de computer wordt ontvangen om verdacht verkeer of bekende aanvallen op te sporen. Als Personal Firewall bijvoorbeeld ICMP-pakketten ziet, worden deze pakketten geanalyseerd op verdachte patronen door het ICMP-verkeer te vergelijken met de patronen van bekende aanvallen.

- **ICMP-ping-aanvragen accepteren —** ICMP-verkeer wordt voornamelijk gebruikt voor het uitvoeren van traceerbewerkingen en pings. Pings worden vaak gebruikt als een snelle test voordat wordt geprobeerd communicatie tot stand te brengen. Als u een programma gebruikt waarmee peer-to-peer bestanden worden gedeeld, ontvangt u mogelijk erg vaak pings. Als u deze optie selecteert, staat Personal Firewall alle ping-aanvragen toe zonder dat de pings worden geregistreerd in het logboek van inkomende gebeurtenissen. Als u deze optie niet selecteert, worden alle ping-aanvragen geblokkeerd en worden de pings geregistreerd in het logboek van inkomende gebeurtenissen.

- **Beperkte gebruikers toestaan om instellingen Personal Firewall te wijzigen —** Als op uw computer Windows XP of Windows 200 Professional wordt uitgevoerd met meerdere gebruikers, moet u deze opties selecteren om XP-gebruikers met beperkte rechten in staat te stellen de instellingen van Personal Firewall te wijzigen.

5 Klik op **OK** als u klaar bent met het aanbrengen van wijzigingen.

McAfee Personal Firewall Plus testen

U kunt de installatie van uw Personal Firewall testen op eventuele zwakke plekken die gevoelig zijn voor aanvallen en verdachte activiteiten.

Als u de installatie van uw Personal Firewall wilt testen van uit het McAfee-pictogram in het systeemvak, gaat u als volgt te werk.

- Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Firewall testen**.

Internet Explorer wordt geopend en http://www.hackerwatch.org/ wordt opgezocht, een website die wordt onderhouden door McAfee. Volg de aanwijzingen op de pagina Probe van Hackerwatch.org om Personal Firewall te testen.

McAfee SecurityCenter gebruiken

McAfee SecurityCenter is de centrale plaats voor uw beveiliging, die u eenvoudig opent via het pictogram op de taakbalk of het bureaublad van Windows. Met SecurityCenter kunt u de volgende nuttige taken uitvoeren:

- Gratis beveiligingsanalyse voor uw computer.
- Al uw McAfee-abonnementen starten, beheren en configureren met één pictogram.
- Voortdurend bijgewerkte viruswaarschuwingen en de meest recente productinformatie bekijken.
- Snelkoppelingen naar veelgestelde vragen en accountgegevens op de McAfee-website.

> **Opmerking**
> Klik op **Help** in het dialoogvenster **SecurityCenter** voor meer informatie over de functies van deze toepassing.

Wanneer SecurityCenter actief is en alle op de computer geïnstalleerde McAfee-voorzieningen zijn ingeschakeld, wordt een rood M-pictogram weergegeven in het systeemvak van Windows. Het systeemvak is het gebied in de taakbalk waar u ook de tijd ziet.

Als één of meer op uw computer geïnstalleerde McAfee-toepassingen is uitgeschakeld, wordt het pictogram van McAfee zwart.

Ga als volgt te werk om McAfee SecurityCenter te starten:

1. Klik met de rechtermuisknop op het McAfee-pictogram en selecteer vervolgens **SecurityCenter openen**.

Ga als volgt te werk om Personal Firewall te starten vanuit het McAfee SecurityCenter:

1. Klik in het SecurityCenter op de tab **Personal Firewall Plus**.
2. Selecteer de taak uit het menu Ik wil.

Ga als volgt te werk om Personal Firewall te starten vanuit Windows:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, en wijs **Personal Firewall**.
2. Selecteer een taak.

McAfee Personal Firewall Plus gebruiken 2

Ga als volgt te werk om Personal Firewall te openen:

- Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall**, aan en selecteer een taak.

De pagina Overzicht

Het overzicht van Personal Firewall bevat vier pagina's:

- Hoofdoverzicht
- Overzicht van toepassingen
- Overzicht van gebeurtenissen
- Overzicht HackerWatch.org

De overzichtspagina's bevatten verschillende rapporten over recente inkomende gebeurtenissen, de status van toepassingen en wereldwijde inbraakactiviteiten die door HackerWatch.org zijn gerapporteerd. U vindt op deze pagina's ook koppelingen naar taken die vaak in Personal Firewall worden uitgevoerd.

Ga als volgt te werken om de pagina Hoofdoverzicht van Personal Firewall te openen:

- Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Overzicht weergeven** (Afbeelding 2-1).

Afbeelding 2-1. Pagina Hoofdoverzicht

Klik op de volgende items om naar verschillende overzichtspagina's te navigeren:

Item	Beschrijving
Weergave wijzigen	Klik op **Weergave wijzigen** om een lijst met overzichtspagina's te openen. Selecteer in de lijst een overzichtspagina die u wilt bekijken.
Pijltje naar rechts	Klik op het pijltje naar rechts om de volgende overzichtspagina te bekijken.
Pijltje naar links	Klik op het pijltje naar links om de vorige overzichtspagina te bekijken.
Begin	Klik op het pictogram van de beginpagina om terug te gaan naar de pagina **Hoofdoverzicht**.

Op de pagina Hoofdoverzicht wordt de volgende informatie weergegeven:

Item	Beschrijving
Beveiligingsinstelling	Het beveiligingsniveau van de firewall geeft aan hoe de beveiliging van de firewall is ingesteld. Klik op de koppeling om het beveiligingsniveau te wijzigen.
Geblokkeerde gebeurtenissen	Het aantal gebeurtenissen dat vandaag is geblokkeerd. Klik op de koppeling om gebeurtenisdetails te bekijken van de pagina met inkomende gebeurtenissen.
Gewijzigde toepassingsregels	Het aantal toepassingsregels dat de afgelopen tijd is gewijzigd. Klik op de koppeling om de lijst met toegestane en geblokkeerde toepassingen te bekijken en om toepassingsmachtigingen te wijzigen.
Wat is nieuw?	**Wat is nieuw?** toont de meest recente toepassing die toegang tot internet heeft gekregen.
Laatste gebeurtenis	Met **Laatste gebeurtenis** worden de laatste inkomende gebeurtenissen weergegeven. U kunt op een koppeling klikken om de gebeurtenis te traceren of het IP-adres te vertrouwen. Als u een IP-adres vertrouwt, geeft u alle verkeer van het desbetreffende IP-adres toegang tot uw computer.
Dagelijks rapport	Met **Dagelijks rapport** wordt het aantal inkomende gebeurtenissen weergegeven dat vandaag, deze week en deze maand door Personal Firewall is geblokkeerd. Klik op de koppeling om gebeurtenisdetails te bekijken van de pagina met inkomende gebeurtenissen.
Actieve toepassingen	De **Actieve toepassingen** zijn de toepassingen die momenteel op uw computer worden uitgevoerd en internettoegang hebben. Klik op een toepassing om na te gaan met welke IP-adressen de toepassing verbinding maakt.
Algemene taken	Als u op een koppeling in **Algemene taken** klikt, gaat u naar pagina's van Personal Firewall waarop u de firewallactiviteit kunt bekijken en taken kunt uitvoeren.

Als u de pagina Overzicht van toepassingen wilt bekijken:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Overzicht weergeven**.
2. Klik op **Weergave wijzigen** en selecteer vervolgens **Overzicht van toepassingen**.

Op de pagina Overzicht van toepassingen wordt de volgende informatie weergegeven:

Item	Beschrijving
Verkeersmonitor	De **Verkeersmonitor** geeft de inkomende en uitgaande internetverbindingen gedurende de afgelopen vijftien minuten weer. Klik op de grafiek om de bijbehorende details te bekijken.
Actieve toepassingen	**Actieve toepassingen** geeft aan hoeveel bandbreedte de meest actieve toepassingen op de computer hebben gebruikt gedurende de afgelopen 24 uur. **Toepassing**— De toepassing die toegang heeft gekregen tot internet. **%**— Het percentage bandbreedte dat door de toepassing is gebruikt. **Machtiging**— Het type internettoegang waarvoor de toepassing toestemming heeft. **Regel gemaakt**— Wanneer de toepassingsregel is gemaakt.
Wat is nieuw?	**Wat is nieuw?** toont de meest recente toepassing die toegang tot internet heeft gekregen.
Actieve toepassingen	De **Actieve toepassingen** zijn de toepassingen die momenteel op uw computer worden uitgevoerd en internettoegang hebben. Klik op een toepassing om na te gaan met welke IP-adressen de toepassing verbinding maakt.
Algemene taken	Klik op een koppeling in **Algemene taken** om naar pagina's van Personal Firewall te gaan waarop u de status van toepassingen kunt bekijken en taken kunt uitvoeren die met toepassingen verband houden.

Als u de pagina Overzicht van gebeurtenissen wilt bekijken:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Overzicht weergeven**.
2. Klik op **Weergave wijzigen** en selecteer vervolgens **Overzicht van gebeurtenissen**.

Op de pagina Overzicht van gebeurtenissen wordt de volgende informatie weergegeven:

Item	Beschrijving
Poortvergelijking	Met **Poortvergelijking** wordt een cirkeldiagram weergegeven met de poorten op uw computer die gedurende de afgelopen 30 dagen het meest zijn gebruikt. U kunt op een poortnaam klikken om details te bekijken van de pagina met inkomende gebeurtenissen. U kunt ook de muisaanwijzer bewegen boven het poortnummer om een beschrijving van de poort te bekijken.
Belangrijkste overtreders	Met **Belangrijkste overtreders** worden de IP-adressen weergegeven die het vaakst zijn geblokkeerd, wanneer de laatste inkomende gebeurtenis is opgetreden voor elk adres en hoeveel inkomende gebeurtenissen gedurende de laatste dertig dagen zijn opgetreden voor elk adres. Klik op een gebeurtenis om gebeurtenisdetails te bekijken van de pagina Inkomende gebeurtenissen.
Dagelijks rapport	Met **Dagelijks rapport** wordt het aantal inkomende gebeurtenissen weergegeven dat vandaag, deze week en deze maand door Personal Firewall is geblokkeerd. Klik op een aantal om de gebeurtenisdetails te bekijken uit het logboek Inkomende gebeurtenissen.
Laatste gebeurtenis	Met **Laatste gebeurtenis** worden de laatste inkomende gebeurtenissen weergegeven. U kunt op een koppeling klikken om de gebeurtenis te traceren of het IP-adres te vertrouwen. Als u een IP-adres vertrouwt, geeft u alle verkeer van het desbetreffende IP-adres toegang tot uw computer.
Algemene taken	Klik op een koppeling in **Algemene taken** om naar de pagina's in Personal Firewall te gaan waar u details van gebeurtenissen kunt bekijken en taken kunt uitvoeren die verband houden met gebeurtenissen.

Als u de pagina Overzicht van HackerWatch wilt bekijken:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Overzicht weergeven**.
2. Klik op **Weergave wijzigen** en selecteer vervolgens **Overzicht van HackerWatch**.

Op de pagina HackerWatch-overzicht wordt de volgende informatie weergegeven:

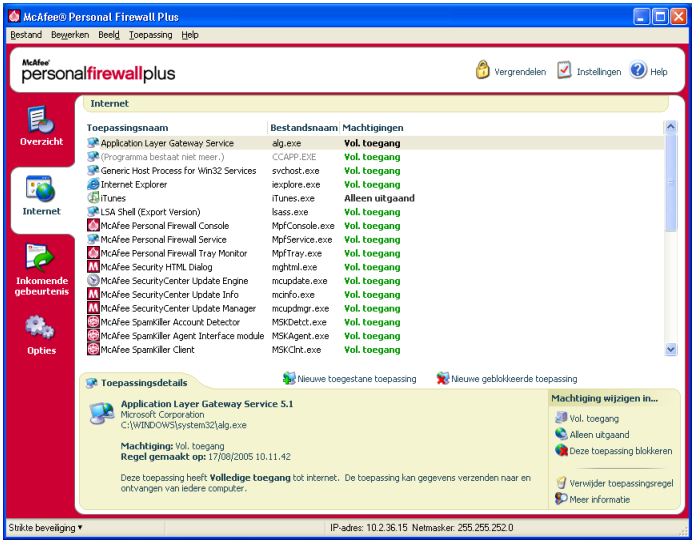
Item	Beschrijving
Activiteit in de wereld	Bij **Activiteit in de wereld** wordt een wereldkaart weergegeven met recentelijk geblokkeerde activiteiten die bij HackerWatch.org zijn gerapporteerd. Klik op de kaart om de Global Threat Analysis Map te openen in HackerWatch.org.
Tracering van gebeurtenissen	Bij **Tracering van gebeurtenissen** wordt het aantal inkomende gebeurtenissen aangegeven dat naar HackerWatch.org is verzonden.
Globale poortactiviteit	Bij **Globale poortactiviteit** worden de poorten aangegeven die de afgelopen vijf dagen de grootste bedreiging lijken te vormen. Klik op een poort om het poortnummer en de poortbeschrijving te bekijken.
Algemene taken	Klik op een koppeling onder **Algemene taken** om naar de pagina's van HackerWatch.org te gaan, waar u meer informatie kunt krijgen over wereldwijde hackersactiviteiten.

De pagina Internettoepassingen

Gebruik de pagina Internettoepassingen om de lijst met toegestane en geblokkeerde toepassingen te bekijken.

Ga als volgt te werk om de pagina Internettoepassingen te starten:

- Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Toepassingen** (Afbeelding 2-2).



Afbeelding 2-2. Pagina Internettoepassingen

Op de pagina Internettoepassingen worden de volgende gegevens weergegeven:

- Namen van toepassingen
- Bestandsnamen
- Huidige machtigingsniveaus
- Toepassingsdetails: Toepassingsnaam en -versie, bedrijfsnaam, padnaam, machtigingen tijdstempels en uitleg bij machtigingstypen.

Toepassingsregels wijzigen

Personal Firewall lets you change access rules for applications.

Ga als volgt te werk om een toepassingsregel te wijzigen:

1. Klik met de rechtermuisknop op het pictogram van McAfee, wijs **Personal Firewall** aan en selecteer vervolgens **Internettoepassingen**.
2. Klik in de lijst **Internettoepassingen** met de rechtermuisknop op de toepassingsregel voor een toepassing en selecteer een ander niveau:
   - **Volledige toegang toestaan —** Als u de toepassing wilt toestaan zowel uitgaande als binnenkomende internetverbindingen te openen.
   - **Alleen uitgaande toegang —** Als u de toepassing alleen wilt toestaan uitgaande internetverbindingen te openen.
   - **Deze toepassing blokkeren —** De toepassing toegang tot het internet weigeren.

     Opmerking
     Eerder geblokkeerde toepassingen blijven geblokkeerd wanneer de firewall is ingesteld op **Open** of **Vergrendelen**. Om dit te voorkomen, kunt u de toegangsregel voor de toepassing wijzigen in **Volledige toegang** of verwijdert u de toestemmingsregel **Geblokkeerd** in de lijst met **Internettoepassingen**.

Ga als volgt te werk om een toepassingsregel te verwijderen:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Internettoepassingen**.
2. Klik in de lijst **Internettoepassingen** met de rechtermuisknop op de toepassingsregel voor een toepassing en selecteer **Toepassingsregel verwijderen**

De volgende keer dat de toepassing internettoegang vraagt, kunt u het machtigingsniveau instellen om het machtigingsniveau weer aan de lijst toe te voegen.

Internettoepassingen toestaan en blokkeren

Ga als volgt te werk om de lijst met toegestane en geblokkeerde internettoepassingen te wijzigen:

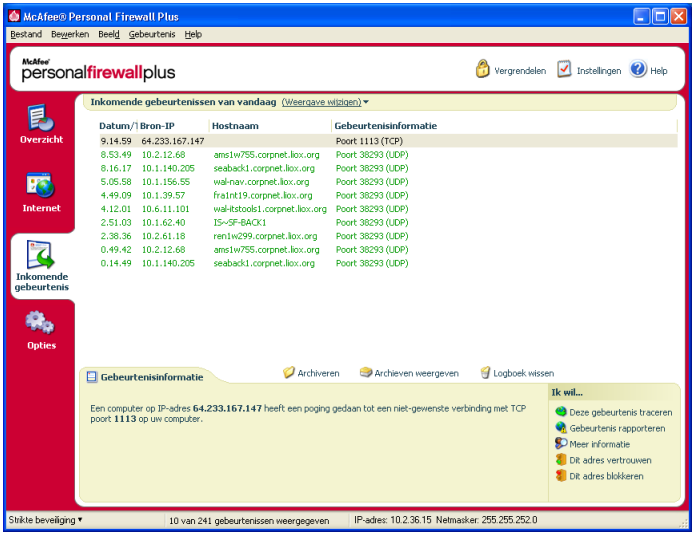
1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Internettoepassingen**.
2. Op de pagina Internettoepassingen klikt u op een van de volgende opties:
   - **Nieuwe toegestane toepassing** — De toepassing volledige toegang tot het internet geven.
   - **Nieuwe geblokkeerde toepassing** — Een toepassing toegang tot het internet weigeren.
   - **Toepassingsregel verwijderen** — Een toepassingsregel verwijderen.

Inkomende gebeurtenissen

Gebruik de pagina Inkomende gebeurtenissen om het logboek van inkomende gebeurtenissen te bekijken dat wordt gegenereerd wanneer ongewenste internetverbindingen door Personal Firewall worden geblokkeerd.

Ga als volgt te werk om de pagina Inkomende gebeurtenissen te starten:

- Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen** (Afbeelding 2-3).



Afbeelding 2-3. Pagina Inkomende gebeurtenissen

Op de pagina Inkomende gebeurtenissen worden de volgende gegevens weergegeven:

- Tijdstempels
- Bron-IP's
- Hostnamen
- Namen van services of toepassingen
- Gebeurtenisdetails: verbindingstypen, verbindingspoorten, hostnamen of host-IP's en uitleg bij poortgebeurtenissen

Wat zijn gebeurtenissen

IP-adressen

IP-adressen zijn getallen: vier getallen tussen 0 en 255. Deze getallen geven een specifieke plek aan waar verkeer op internet naartoe kan worden gestuurd.

IP-adrestypen

Een aantal IP-adressen zijn om verschillende redenen ongebruikelijk:

Niet routeerbare IP-adressen — Deze worden ook wel aangeduid als 'Privé-IP-ruimte'. Deze IP-adressen kunnen niet worden gebruikt op internet. Privé-IP-adressen zijn 10.x.x.x, 172.16.x.x - 172.31.x.x en 192.168.x.x.

Loopback-IP-adressen — Loopback-adressen worden gebruikt voor testdoeleinden. Verkeer dat naar deze IP-adressen wordt verstuurd, komt weer terug naar het apparaat dat het pakket heeft gegenereerd. Het verkeer verlaat het apparaat niet en wordt alleen gebruikt voor het testen van de hardware en software. Het loopback-IP-adres is 127.x.x.x.

Null-IP-adres — Dit is een ongeldig adres. Personal Firewall geeft aan dat het verkeer een blanco IP-adres had. Dit is uiteraard niet normaal en het geeft meestal aan dat de afzender opzettelijk probeert de bron van het verkeer te maskeren. De afzender kan geen antwoord op het verkeer ontvangen, tenzij het pakket wordt ontvangen door een toepassing die de inhoud begrijpt van het pakket, dat specifieke instructies voor die toepassing bevat. Elk adres dat begint met 0 (0.x.x.x) is een null-adres. 0.0.0.0 is bijvoorbeeld een null-IP-adres.

Gebeurtenissen van 0.0.0.0

Als u gebeurtenissen ziet van IP-adres 0.0.0.0, zijn hier twee mogelijke oorzaken voor. De eerste en meest voorkomende oorzaak is dat uw computer een onjuist samengesteld pakket heeft ontvangen. Internet is niet altijd 100% betrouwbaar en er kunnen ongeldige pakketten voorkomen. Aangezien Personal Firewall de pakketten ziet voordat deze door TCP/IP kunnen worden gevalideerd, worden deze pakketten mogelijk gerapporteerd als een gebeurtenis.

De andere situatie treedt op wanneer het bron-IP-adres wordt vervalst. Vervalste pakketten duiden er meestal op dat er iemand op uw computer op zoek is naar Trojaanse paarden. Personal Firewall blokkeert dit soort pogingen, dus uw computer is veilig.

Gebeurtenissen van 127.0.0.1

Gebeurtenissen hebben soms als bron-IP 127.0.0.1. Dit is een zogenaamd loopback-adres of een localhost.

Veel legitieme programma's gebruiken het loopback-adres voor de communicatie tussen onderdelen. Zo kunt u bijvoorbeeld veel persoonlijke e-mail- of webservers configureren via een webinterface. Om toegang te krijgen tot de webinterface, typt u “http://localhost/” in uw webbrowser.

Personal Firewall staat verkeer van deze programma's toe, dus als u gebeurtenissen ziet van 127.0.0.1, betekent dit waarschijnlijk dat het bron-IP-adres is vervalst. Vervalste pakketten duiden er meestal op dat een andere computer die van u probeert te scannen. Personal Firewall blokkeert dit soort pogingen tot inbraak, dus uw computer is veilig.

Voor bepaalde programma's, met name Netscape 6.2 en hoger, moet u 127.0.0.1 echter aan de lijst met vertrouwde IP-adressen toevoegen. De onderdelen van deze programma's communiceren op een zodanige wijze met elkaar dat Personal Firewall niet kan bepalen of het verkeer lokaal is.

Als u bij Netscape 6.2 het adres 127.0.0.1 niet vertrouwt, kunt u de buddylijst niet gebruiken. Als u dus verkeer ziet van 127.0.0.1 en alle toepassingen op de computer werken op de normale wijze, dan is het veilig om dit verkeer te blokkeren. Als een programma (zoals Netscape) echter problemen heeft, voegt u 127.0.0.1 toe aan de lijst met vertrouwde IP-adressen in Personal Firewall en kijkt u of het probleem is opgelost.

Als het probleem is opgelost door 127.0.0.1 in de lijst met vertrouwde IP-adressen te plaatsen, moet u het volgende overwegen: als u 127.0.0.1 vertrouwt, werkt uw programma, maar bent u kwetsbaarder voor aanvallen met een vervalst IP-adres. Als u het adres niet vertrouwt, werkt het programma niet, maar bent u nog wel beveiligd tegen bepaald schadelijk verkeer.

Gebeurtenissen van computers op uw LAN

Vanaf computers op uw LAN (Local Area Network) kunnen gebeurtenissen worden gegenereerd. Om aan te geven dat gebeurtenissen afkomstig zijn van uw netwerk, worden ze door Personal Firewall groen weergegeven.

In de meeste bedrijfs-LAN's moet de optie **Alle computers op het LAN Vertrouwd maken** onder Vertrouwde IP-adressen worden ingeschakeld.

In sommige situaties kan uw 'lokale' netwerk echter net zo gevaarlijk of zelfs gevaarlijker zijn dan het internet, vooral wanneer uw computer verbonden is een netwerk op basis van DSL of een kabelmodem met een grote bandbreedte. In dit geval moet u niet kiezen voor **Alle computers op het LAN Vertrouwd maken**. In plaats daarvan kunt u beter de IP-adressen van al uw lokale computers toevoegen aan de lijst Vertrouwde IP-adressen.

Gebeurtenissen van privé-IP-adressen

IP-adressen met de indeling 192.168.xxx.xxx, 10.xxx.xxx.xxx en 172.16.0.0 - 172.31.255.255 worden niet-routeerbare of privé-IP-adressen genoemd. In principe mogen deze IP-adressen uw netwerk nooit verlaten en kunnen ze meestal worden vertrouwd.

Het blok 192.168.xxx.xxx wordt gebruikt voor de voorziening Internetverbinding delen van Microsoft. Als u gebruikmaakt van Internetverbinding delen en u gebeurtenissen ziet van dit IP-blok, kunt u het IP-adres 192.168.255.255 aan uw lijst met vertrouwde IP-adressen toevoegen. U vertrouwt dan het volledige blok 192.168.xxx.xxx.

Als u zich niet op een privé-netwerk bevindt en u gebeurtenissen ziet uit deze IP-bereiken, kan het bron-IP-adres vervalst zijn. Vervalste pakketten duiden er meestal op dat er iemand op zoek is naar Trojaanse paarden. Personal Firewall heeft deze poging geblokkeerd, dus uw computer is veilig.

Aangezien hetzelfde privé-IP-adres naar totaal verschillende computers kan verwijzen, afhankelijk van het netwerk waar u zich bevindt, heeft het geen zin om deze gebeurtenissen te rapporteren.

Gebeurtenissen weergeven in het logboek van inkomende gebeurtenissen

In het logboek van inkomende gebeurtenissen worden de gebeurtenissen op een aantal manieren weergeven. In de standaardweergave zijn er alleen gebeurtenissen van de huidige dag zichtbaar. U kunt ook gebeurtenissen van deze week bekijken of het volledige logboek.

Met Personal Firewall kunt u ook gebeurtenissen weergeven van specifieke dagen, specifieke internetadressen (IP-adressen) of gebeurtenissen die dezelfde gebeurtenisinformatie bevatten.

Als u meer informatie wenst over een gebeurtenis, klikt u op de desbetreffende gebeurtenis. De informatie wordt dan weergegeven in het vak **Gebeurtenisinformatie**.

Gebeurtenissen van vandaag weergeven

Gebruik deze optie om de gebeurtenissen van vandaag te bekijken.

Ga als volgt te werk om de gebeurtenissen van vandaag weer te geven:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop op een item in het logboek Inkomende gebeurtenissen en klik vervolgens op **Gebeurtenissen van vandaag weergeven**.

Gebeurtenissen van deze week weergeven

Gebruik deze optie om de gebeurtenissen van deze week te bekijken.

Ga als volgt te werk om de gebeurtenissen van deze week weer te geven:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop op een item in het logboek Inkomende gebeurtenissen en klik vervolgens op **Gebeurtenissen van deze week weergeven**.

Het volledige logboek Inkomende gebeurtenissen weergeven

Gebruik deze optie om alle gebeurtenissen van deze week te bekijken.

Ga als volgt te werk om alle gebeurtenissen in het logboek Inkomende gebeurtenissen weer te geven:

1. Klik met de rechtermuisknop op het pictogram van McAfee, wijs **Personal Firewall** aan en klik vervolgens op **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop op een item in het logboek Inkomende gebeurtenissen en klik vervolgens op **Volledig logboek weergeven**.

   In het logboek Inkomende gebeurtenissen worden alle gebeurtenissen van het logboek Inkomende gebeurtenissen weergegeven.

Gebeurtenissen voor een bepaalde dag weergeven

Gebruik deze optie om de gebeurtenissen van een bepaalde dag te bekijken.

Ga als volgt te werk om de gebeurtenissen van een bepaalde dag weer te geven:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop op een item in het logboek Inkomende gebeurtenissen en klik vervolgens op **Alleen gebeurtenissen van deze dag weergeven**.

Gebeurtenissen voor een bepaald Internetadres weergeven

Gebruik deze optie om andere gebeurtenissen te bekijken die van een bepaald internetadres komen.

Ga als volgt te werk om de gebeurtenissen van een internetadres weer te geven:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop op een item in het logboek Inkomende gebeurtenissen en klik vervolgens op **Alleen gebeurtenissen van geselecteerd internetadres weergeven**.

Gebeurtenissen met dezelfde gebeurtenisinformatie weergeven

Deze optie gebruikt u wanneer u wilt zien of er andere gebeurtenissen in het logboek van inkomende gebeurtenissen zijn opgenomen die dezelfde informatie bevatten in de kolom Gebeurtenisinformatie als de gebeurtenis die u hebt geselecteerd. U kunt zien hoe vaak deze gebeurtenis voorkomt en of de bron overeenkomt. De kolom Gebeurtenisinformatie bevat een beschrijving van de gebeurtenis en, indien bekend, het overeenkomende programma of de overeenkomende service die de desbetreffende poort gebruikt.

Ga als volgt te werk om gebeurtenissen met dezelfde gebeurtenisinformatie weer te geven:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop op een item in het logboek Inkomende gebeurtenissen en klik vervolgens op **Alleen gebeurtenissen met dezelfde gebeurtenisinformatie weergeven**.

Reageren op inkomende gebeurtenissen

U kunt niet alleen informatie bekijken over gebeurtenissen in het logboek van inkomende gebeurtenissen, maar u kunt ook proberen een Visual Trace uit te voeren van de IP-adressen voor een gebeurtenis in het logboek van inkomende gebeurtenissen, of gebeurtenisdetails opvragen bij de website HackerWatch.org voor de bestrijding van hackers.

De geselecteerde gebeurtenis traceren

U kunt met Visual Trace proberen de IP-adressen te traceren voor een gebeurtenis in het logboek Inkomende gebeurtenissen.

Ga als volgt te werk om een geselecteerde gebeurtenis te traceren:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop in het logboek van inkomende gebeurtenissen op de gebeurtenis die u wilt traceren en klik vervolgens op **Geselecteerde gebeurtenis traceren**. U kunt ook dubbelklikken op en gebeurtenis die u wilt traceren.

Standaard begint Personal Firewall een traceerbewerking met het geïntegreerde programma Personal Firewall Visual Trace.

Advies opvragen bij HackerWatch.org

Ga als volgt te werk om advies te vragen bij HackerWatch.org:

1. Klik met de rechtermuisknop op het pictogram van McAfee, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Selecteer het item van de gebeurtenis op de pagina Inkomende gebeurtenissen, klik vervolgens op **Meer informatie** in het vak **Ik wil**.

De standaard webbrowser wordt geopend en de website HackerWatch.org op http://www.hackerwatch.org/ wordt opgezocht voor informatie over het gebeurtenistype en advies over het al dan niet rapporteren van de gebeurtenis.

Een gebeurtenis rapporteren

Ga als volgt te werk om een gebeurtenis te rapporteren waarvan u vermoedt dat het een aanval op uw computer was:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik op de gebeurtenis die u wilt rapporteren en klik vervolgens op **Deze gebeurtenis rapporteren** in het vak **Ik wil**.

De gebeurtenis wordt door Personal Firewall gerapporteerd bij HackerWatch.org met uw unieke id.

Aanmelden bij HackerWatch.org

Wanneer u de overzichtspagina van Personal Firewall voor het eerst opent, neemt Personal Firewall contact op met HackerWatch.org om een unieke gebruikers-id voor u te genereren. Als u een bestaande gebruiker bent, wordt uw aanmelding automatisch gevalideerd. Als u een nieuwe gebruiker bent, moet u een alias en een e-mailadres opgeven en vervolgens op de validatiekoppeling klikken in het bevestigingsbericht van HackerWatch.org. Daarna kunt u de voorzieningen voor het filteren en e-mailen van gebeurtenissen gebruiken op deze website.

U kunt gebeurtenissen rapporteren HackerWatch.org zonder uw gebruikers-ID te valideren. Wanneer u gebeurtenissen wilt filteren en deze naar een vriend wilt e-mailen, moet u zich echter aanmelden voor de service.

Als u zich bij de service aanmeldt, wordt alles dat u hebt verzonden, vastgelegd. U krijgt bericht als HackerWatch.org meer informatie van u nodig heeft of als is vastgesteld dat u nadere actie moet ondernemen. Aanmelding is ook vereist omdat de informatie die we ontvangen pas nuttig is als de informatie kan worden bevestigd.

Alle e-mailadressen die bij HackerWatch.org worden opgegeven, worden vertrouwelijk behandeld. Als een internetprovider om extra informatie vraagt, wordt die aanvraag via HackerWatch.org doorgestuurd. Uw e-mailadres wordt nooit bekendgemaakt.

Een adres vertrouwen

U kunt de pagina Inkomende gebeurtenissen gebruiken om een IP-adres toe te voegen aan de lijst Vertrouwde IP-adressen en zo een permanente verbinding toestaan.

Als u een gebeurtenis ziet op de pagina Inkomende gebeurtenissen die een IP-adres bevat dat u wilt toestaan, kunt u met Personal Firewall toestaan dat vanaf dit adres verbinding wordt gemaakt:

Ga als volgt te werk om een IP-adres toe te voegen de lijst Vertrouwde IP-adressen:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop op de gebeurtenis waarvan u het IP-adres wilt vertrouwen en klik op **Bron-IP-adres vertrouwen**.

Controleer of het IP-adres dat wordt weergegeven in het dialoogvenster 'Dit adres vertrouwen' juist is en klik op **OK**. Het IP-adres wordt toegevoegd aan de lijst Vertrouwde IP-adressen.

Ga als volgt te werk om te controleren of het IP-adres is toegevoegd:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer **Opties**.
2. Klik op het pictogram **Vertrouwde en verboden IP-adressen** en vervolgens op de tab **Vertrouwde IP-adressen**.

Het IP-adres verschijnt aangevinkt in de lijst Vertrouwde IP-adressen.

Een adres verbieden

Als een IP-adres is opgenomen in het logboek van inkomende gebeurtenissen, betekent dit dat verkeer van het desbetreffende adres is geblokkeerd. Het verbieden van een adres biedt dan ook geen aanvullende bescherming, tenzij uw computer poorten heeft die opzettelijk zijn geopend via de systeemservices of tenzij uw computer een toepassing heeft die is gemachtigd om verkeer te ontvangen.

Voeg alleen een IP-adres toe aan de lijst met verboden adressen als een of meer poorten opzettelijk zijn geopend en als er aanleiding is om te voorkomen dat het adres toegang krijgt

Als u op de pagina Inkomende gebeurtenissen een gebeurtenis ziet die een IP-adres bevat dat u wilt verbieden, kunt u Personal Firewall zo configureren dat vanaf dit adres nooit meer verbinding wordt gemaakt:.

U kunt de pagina Inkomende gebeurtenissen met daarop een lijst van al het inkomende internetverkeer gebruiken om een IP-adres te verbieden dat u ervan verdenkt de bron te zijn van verdachte of ongewenste internetactiviteit.

Ga als volgt te werk om een IP-adres toe te voegen de lijst Verboden IP-adres:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Op de pagina Inkomende gebeurtenissen vindt u de IP-adressen van al het inkomende internetverkeer. Selecteer een IP-adres en doe een van de volgende dingen:
   - Klik met de rechtermuisknop op het IP-adres en selecteer **Bron-IP-adres blokkeren**.
   - Klik in het menu **Ik wil** op **Dit adres blokkeren**.

3 In het dialoogvenster Regel verboden IP-adres toevoegen gebruikt u een of meer van de volgende instellingen op de regel voor het geblokkeerde IP-adres te configureren.

- **Eén IP-adres**: Het IP-adres dat moet worden geblokkeerd. De standaardinvoer is het IP-adres dat u hebt geselecteerd op de pagina Inkomende gebeurtenissen.
- **Een reeks IP-adressen**: De IP-adressen tussen het adres dat u opgeeft in Van IP-adres en het IP-adres dat u opgeeft in Naar IP-adres.
- **Deze regel vervalt op**: Datum en tijd waarop de Regel voor het verboden IP-adres vervalt. Selecteer in de keuzemenu's de datum en de tijd.
- **Beschrijving**: Geef eventueel een beschrijving van de nieuwe regel op.
- Klik op **OK**.

4 Klik in het dialoogvenster op **Ja** om uw instellingen te bevestigen. Klik op **Nee** om terug te keren naar het dialoogvenster Regel verboden IP-adres toevoegen.

Wanneer Personal Firewall een gebeurtenis op het spoor komt van een verboden internetverbinding, wordt u gewaarschuwd volgens de methode die u hebt opgegeven op de pagina Instellingen waarschuwing.

Ga als volgt te werk om te controleren of het IP-adres is toegevoegd:

1 Klik op de tab **Opties**.

2 Klik op het pictogram **Vertrouwde en verboden IP-adressen** en klik vervolgens op de tab **Verboden IP-adressen**.

Het IP-adres verschijnt aangevinkt in de lijst Verboden IP-adressen.

Het logboek Inkomende gebeurtenissen beheren

U kunt de pagina Inkomende gebeurtenissen gebruiken om de gebeurtenissen te beheren in het logboek van inkomende gebeurtenissen dat wordt gegenereerd wanneer met Personal Firewall ongewenst internetverkeer wordt geblokkeerd.

Het logboek van inkomende gebeurtenissen archiveren

U kunt het huidige logboek Inkomende gebeurtenissen archiveren om alle inkomende gebeurtenissen te bewaren met datum en tijd, bron-IP's, hostnamen, poorten en gebeurtenisinformatie. U kunt het logboek Inkomende gebeurtenissen het beste regelmatig archiveren om te voorkomen dat het te groot wordt.

Ga als volgt te werk om het logboek Inkomende gebeurtenissen te archiveren:

1 Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.

2 Klik op de pagina Inkomende gebeurtenissen op **Archiveren**.

3 Klik in het dialoogvenster Logboek archiveren op **Ja** om door te gaan met de bewerking.

4 Klik op **Opslaan** om het archief op de standaardlocatie op te slaan of ga naar een locatie waar u het archief wilt opslaan.

Opmerking: Personal Firewall archiveert standaard automatisch het logboek Inkomende gebeurtenissen. Selecteer of deselecteer de optie **Geregistreerde gebeurtenissen automatisch archiveren** op de pagina Instellingen gebeurtenislogboek om de opties in- of uit te schakelen.

Gearchiveerde logboeken van inkomende gebeurtenissen bekijken

U kunt gearchiveerde logboeken van inkomende gebeurtenissen bekijken. Het opgeslagen archief bevat data en tijden, bron-IP's, hostnamen, poorten en gebeurtenisinformatie voor de gebeurtenissen.

Ga als volgt te werk als u een gearchiveerd logboek Inkomende gebeurtenissen wilt bekijken:

1 Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.

2 Klik op de pagina Inkomende gebeurtenissen op **Archieven weergeven**.

3 Selecteer of zoek de naam van het archiefbestand en klik op **Openen**.

Het logboek van inkomende gebeurtenissen wissen

U kunt alle informatie uit het logboek Inkomende gebeurtenissen wissen.

Waarschuwing: Wanneer u het logboek Inkomende gebeurtenissen wist, gaat de informatie definitief verloren. Als u verwacht dat u het logboek Gebeurtenissen in de toekomst nog nodig hebt, kunt u het beter archiveren.

U wist het logboek Inkomende gebeurtenissen als volgt:

1 Klik met de rechtermuisknop op het pictogram van McAfee, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.

2 Klik op de pagina Inkomende gebeurtenissen op **Logboek wissen**.

3 Klik op **Ja** in het dialoogvenster om het logboek te wissen.

Een gebeurtenis naar het klembord kopiëren

U kunt een gebeurtenis naar het klembord kopiëren, waarna u het in een tekstbestand kunt plakken met Kladblok.

Ga als volgt te werk om een gebeurtenis naar het klembord te kopiëren:

1. Klik met de rechtermuisknop op het pictogram van McAfee, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik met de rechtermuisknop op in het logboek Inkomende gebeurtenissen op de gebeurtenis.
3. Klik op **Geselecteerde gebeurtenis kopiëren naar klembord**.
4. Kladblok starten.
   - Typ `notepad` op de opdrachtregel of klik op de Windows **Start**-knop en kies voor **Programma's** en vervolgens **Accessoires**. Selecteer **Kladblok**.
5. Klik op **Bewerken** en vervolgens op Plakken. De tekst van de gebeurtenis wordt weergegeven in Kladblok. Herhaal deze stap tot alle gewenste gebeurtenissen zijn gekopieerd.
6. Sla het tekstbestand op een veilige plek op.

De geselecteerde gebeurtenis verwijderen

U kunt gebeurtenissen verwijderen uit het logboek Inkomende gebeurtenissen.

Ga als volgt te werk om gebeurtenissen te verwijderen uit het logboek Inkomende gebeurtenissen:

1. Klik met de rechtermuisknop op het pictogram van McAfee in het Windows-systeemvak, wijs **Personal Firewall** aan en selecteer vervolgens **Inkomende gebeurtenissen**.
2. Klik in het logboek Inkomende gebeurtenissen op de gebeurtenis die u wilt verwijderen.
3. Klik in het menu Bewerken op **Geselecteerde gebeurtenis verwijderen**. De gebeurtenis wordt verwijderd uit het logboek Inkomende gebeurtenissen.

Waarschuwingen

Zorg ervoor dat u bekend bent met het type waarschuwingen dat u kunt krijgen wanneer u Personal Firewall gebruikt. Bekijk de volgende typen waarschuwingen die kunnen verschijnen en de mogelijke reacties waaruit u kunt kiezen, zodat u weet wat u doet wanneer u op een waarschuwing reageert.

Opmerking
Aan de hand van aanbevelingen bij waarschuwingen kunt u bepalen hoe u op een waarschuwing moet reageren. Als u aanbevelingen wilt laten weergeven bij waarschuwingen, klikt u op de tab **Opties.**, klikt u op het pictogram **Instellingen voor waarschuwingen** en selecteert u vervolgens **Slimme aanbevelingen gebruiken** (de standaardoptie) of **Alleen Slimme aanbevelingen weergeven** in de lijst **Slimme aanbevelingen**.

Rode waarschuwingen

Rode waarschuwingen bevatten belangrijke informatie die uw onmiddellijke aandacht vereist:

- **Internettoepassing geblokkeerd —** Deze waarschuwing verschijnt als Personal Firewall de internettoegang van een toepassing blokkeert. Als bijvoorbeeld een waarschuwing verschijnt voor een Trojaans paard, wordt de internettoegang voor dit programma automatisch geblokkeerd en wordt u aangeraden de computer op virussen te scannen.
- **Toepassing verzoekt om toegang tot internet —** Deze waarschuwing verschijnt wanneer Personal Firewall internet- of netwerkverkeer detecteert voor nieuwe toepassingen.
- **Toepassing is gewijzigd —** deze waarschuwing verschijnt wanneer Personal Firewall detecteert dat een toepassing die u voorheen internettoegang hebt verleend, is gewijzigd. Als u deze toepassing niet onlangs hebt bijgewerkt, moet u voorzichtig zijn wanneer u de gewijzigde toepassing opnieuw toegang verleent tot internet.
- **Toepassing verzoekt om servertoegang —** Deze waarschuwing verschijnt wanneer Personal Firewall detecteert dat een toepassing die u eerder internettoegang hebt verleend, internettoegang heeft gevraagd als server.

  Opmerking
  Met de standaardinstelling voor Windows XP SP2, Automatische updates, worden updates voor het Windows-besturingssysteem en andere Microsoft-programma's automatisch gedownload en geïnstalleerd zonder dat u hierover bericht ontvangt. Als een toepassing is bijgewerkt via een op de achtergrond uitgevoerde Windows-update, verschijnen er McAfee Personal Firewall-waarschuwingen wanneer het Microsoft-programma wordt uitgevoerd.

  BELANGRIJK
  U moet toegang verlenen aan toepassingen die internettoegang nodig hebben voor online productupdates (zoals McAfee-services) om deze toepassingen up-to-date te houden.

Waarschuwing Internettoepassing geblokkeerd

Als een waarschuwing verschijnt voor een Trojaans paard (Afbeelding 2-4), wordt de internettoegang voor dit programma automatisch geblokkeerd en wordt u aangeraden de computer op virussen te scannen. Als McAfee VirusScan niet geïnstalleerd is, kunt u het McAfee SecurityCenter starten:

Afbeelding 2-4. Waarschuwing Internettoepassing geblokkeerd

Bekijk een korte beschrijving van de gebeurtenis en kies een van de volgende opties:

- Klik op **Meer informatie** om informatie over de gebeurtenis op te halen via het logboek van inkomende gebeurtenissen (zie *Inkomende gebeurtenissen* op pagina 22 voor meer informatie).
- Klik op **McAfee VirusScan Online starten** om de computer op virussen te scannen.
- Klik op **Doorgaan met waar ik mee bezig was** als u geen verdere actie wilt ondernemen buiten wat Personal Firewall al heeft gedaan.
- Klik op **Uitgaande toegang verlenen** om een uitgaande verbinding toe te staan (**Strikte** beveiliging).

Waarschuwing Toepassing verzoekt om toegang tot internet

Als u de beveiligingsinstelling **Standaard** of **Strikt** hebt gekozen, wordt er een waarschuwing (Afbeelding 2-5) weergegeven wanneer internet- of netwerkverbindingen worden gedetecteerd voor nieuwe of aangepaste toepassingen.

Afbeelding 2-5. Waarschuwing Toepassing verzoekt om toegang tot internet

Als er een waarschuwing wordt weergegeven waarin u wordt aangeraden voorzichtig te zijn bij het toestaan van internettoegang voor de toepassing, kunt u klikken op **Klik hier voor meer informatie** voor meer informatie over de toepassing. Deze optie wordt alleen in de waarschuwing weergegeven als is ingesteld dat slimme aanbevelingen moeten worden gebruikt in Personal Firewall.

Het is mogelijk dat McAfee de toepassing die probeert internettoegang te verkrijgen, niet herkent (Afbeelding 2-6).

Afbeelding 2-6. Waarschuwing Niet-herkende toepassing

McAfee kan u daarom geen aanbevelingen geven over de manier waarop u de toepassing moet behandelen. Verder is het mogelijk de toepassing bij McAfee te rapporteren door op **McAfee op de hoogte stellen van dit programma** te klikken. Er wordt een webpagina afgebeeld waarop waar u informatie over de toepassing kunt invoeren. Geef zoveel mogelijk informatie op.

De informatie die u verstuurt, wordt gebruikt samen met andere onderzoeksprogramma's van onze HackerWatch-medewerkers om te bepalen of er gronden zijn om een toepassing op te nemen in de database met bekende toepassingen en, indien dit het geval is, hoe deze toepassing door Personal Firewall moet worden behandeld.

Bekijk een korte beschrijving van de gebeurtenis en kies een van de volgende opties:

- Klik op **Toegang verlenen** om de toepassing een uitgaande en een inkomende verbinding toe te staan.
- Klik op **Eenmalig toegang verlenen** om de toepassing een tijdelijke verbinding toe te staan. De toegang wordt beperkt van de tijd dat de toepassing wordt gestart tot de tijd dat deze weer wordt afgesloten.
- Klik op **Alle toegang blokkeren** om een internetverbinding te verbieden.
- Klik op **Uitgaande toegang verlenen** om een uitgaande verbinding toe te staan (**Strikte** beveiliging).
- Klik op **Help mij kiezen** om de online Help over de toegangstoestemmingen voor toepassingen te bekijken.

Waarschuwing Toepassing is gewijzigd

Als u de beveiligingsinstelling **Vertrouwend**, **Standaard** of **Strikt** hebt gekozen, wordt een waarschuwing (Afbeelding 2-7) weergegeven wanneer Personal Firewall detecteert dat een toepassing die u eerder internettoegang hebt verleend, is gewijzigd. Als u de toepassing in kwestie niet onlangs hebt bijgewerkt, moet u voorzichtig zijn wanneer u de gewijzigde toepassing opnieuw toegang verleent tot internet.

Afbeelding 2-7. Waarschuwing Toepassing is gewijzigd

Bekijk een korte beschrijving van de gebeurtenis en kies een van de volgende opties:

- Klik op **Toegang verlenen** om de toepassing een uitgaande en een inkomende verbinding toe te staan.
- Klik op **Eenmalig toegang verlenen** om de toepassing een tijdelijke verbinding toe te staan. De toegang wordt beperkt van de tijd dat de toepassing wordt gestart tot de tijd dat deze weer wordt afgesloten.
- Klik op **Alle toegang blokkeren** om een internetverbinding te verbieden.
- Klik op **Uitgaande toegang verlenen** om een uitgaande verbinding toe te staan (**Strikte** beveiliging).
- Klik op **Help mij kiezen** om de online Help over de toegangstoestemmingen voor toepassingen te bekijken.

Waarschuwing Toepassing verzoekt om servertoegang

Als u de beveiligingsinstelling **Strikt** hebt gekozen, verschijnt er een waarschuwing (Afbeelding 2-8) wanneer er een toepassing wordt gedetecteerd die internettoegang als server heeft gevraagd en u die toepassing eerder internettoegang hebt verleend.

Afbeelding 2-8. Waarschuwing Toepassing verzoekt om servertoegang

Er verschijnt bijvoorbeeld een waarschuwing als MSN Messenger toegang tot de server wil hebben om tijdens het chatten een bestand te verzenden.

Bekijk een korte beschrijving van de gebeurtenis en kies een van de volgende opties:

- Klik op **Eenmalig toegang verlenen** om de toepassing een tijdelijke verbinding toe te staan. De toegang wordt beperkt van de tijd dat de toepassing wordt gestart tot de tijd dat deze weer wordt afgesloten.
- Klik op **Servertoegang verlenen** om de toepassing een inkomende en een uitgaande internetverbinding toe te staan.
- Klik op **Beperken tot uitgaande toegang** om een inkomende internetverbinding te verbieden.
- Klik op **Alle toegang blokkeren** om een internetverbinding te verbieden.
- Klik op **Help mij kiezen** om de online Help over de toegangstoestemmingen voor toepassingen te bekijken. Groene waarschuwingen

Groene waarschuwingen

Groen waarschuwingen verschijnen wanneer Personal Firewall automatisch internettoegang verleend aan toepassingen.

Programma krijgt toegang tot internet — Deze waarschuwing verschijnt wanneer Personal Firewall automatisch internettoegang verleent aan alle nieuwe toepassingen en hiervan vervolgens melding maakt (**Vertrouwende** beveiliging). Een voorbeeld van een gewijzigde toepassing is een toepassing met gewijzigde regels waarbij de toepassing automatisch internettoegang krijgt.

Waarschuwing Programma krijgt toegang tot internet

Als u de beveiligingsinstelling **Vertrouwend** hebt gekozen, geeft Personal Firewall automatisch alle nieuwe toepassingen toegang tot internet en krijgt u vervolgens een waarschuwing (Afbeelding 2-9).

Afbeelding 2-9. Programma krijgt toegang tot internet

Bekijk een korte beschrijving van de gebeurtenis en kies een van de volgende opties:

- Klik op **Het toepassingslogboek weergeven** als u meer informatie wilt over de gebeurtenis via het logboek Internettoepassingen (zie *De pagina Internettoepassingen* op pagina 20 voor meer informatie).
- Klik op **Dit type waarschuwing uitschakelen** om te voorkomen dat dit type waarschuwingen wordt weergegeven.
- Klik op **Doorgaan met waar ik mee bezig was** als u geen verdere actie wilt ondernemen buiten wat Personal Firewall al heeft gedaan.
- Klik op **Alle toegang blokkeren** om een internetverbinding te verbieden.

Waarschuwing Toepassing is gewijzigd

Als u de beveiligingsinstelling **Vertrouwend** hebt gekozen, geeft Personal Firewall automatisch alle gewijzigde toepassingen toegang tot internet. Bekijk een korte beschrijving van de gebeurtenis en kies een van de volgende opties:

- Klik op **Het toepassingslogboek weergeven** als u meer informatie wilt over de gebeurtenis via het logboek Internettoepassingen (zie *De pagina Internettoepassingen* op pagina 20 voor meer informatie).
- Klik op **Dit type waarschuwing uitschakelen** om te voorkomen dat dit type waarschuwingen wordt weergegeven.
- Klik op **Doorgaan met waar ik mee bezig was** als u geen verdere actie wilt ondernemen buiten wat Personal Firewall al heeft gedaan.
- Klik op **Alle toegang blokkeren** om een internetverbinding te verbieden.

Blauwe waarschuwingen

Blauwe waarschuwingen bevatten informatie, maar u hoeft hier niet op te reageren.

- **Verbindingspoging geblokkeerd:** deze waarschuwing verschijnt wanneer Personal Firewall ongewenst internet- of netwerkverkeer blokkeert. (Vertrouwende beveiliging, Standaardbeveiliging of Strikte beveiliging)

Waarschuwing Verbindingspoging geblokkeerd

Als u de beveiligingsinstelling **Vertrouwend**, **Standaard** of **Strikt** hebt geselecteerd, geeft Personal Firewall een waarschuwing (Afbeelding 2-10) weer wanneer ongewenst internet- of netwerkverkeer wordt geblokkeerd.

Afbeelding 2-10. Waarschuwing Verbindingspoging geblokkeerd

Bekijk een korte beschrijving van de gebeurtenis en kies een van de volgende opties:

- Klik op **Het gebeurtenislogboek weergeven** als u meer informatie wilt over de gebeurtenis via het logboek van inkomende gebeurtenissen van Personal Firewall (zie *Inkomende gebeurtenissen* op pagina 22 voor meer informatie).
- Klik op **Dit adres traceren** om de adressen voor deze gebeurtenissen te traceren met Visual Trace.
- Klik op **Dit adres blokkeren** om te voorkomen dat dit adres toegang krijgt tot uw computer. Het adres wordt toegevoegd aan de lijst Verboden IP-adressen.
- Klik op **Dit adres vertrouwen** om dit IP-adres toegang tot uw computer te verlenen.
- Klik op **Doorgaan met waar ik mee bezig was** als u geen verdere actie wilt ondernemen buiten wat Personal Firewall al heeft gedaan

Index

T

V

W