McAfee®

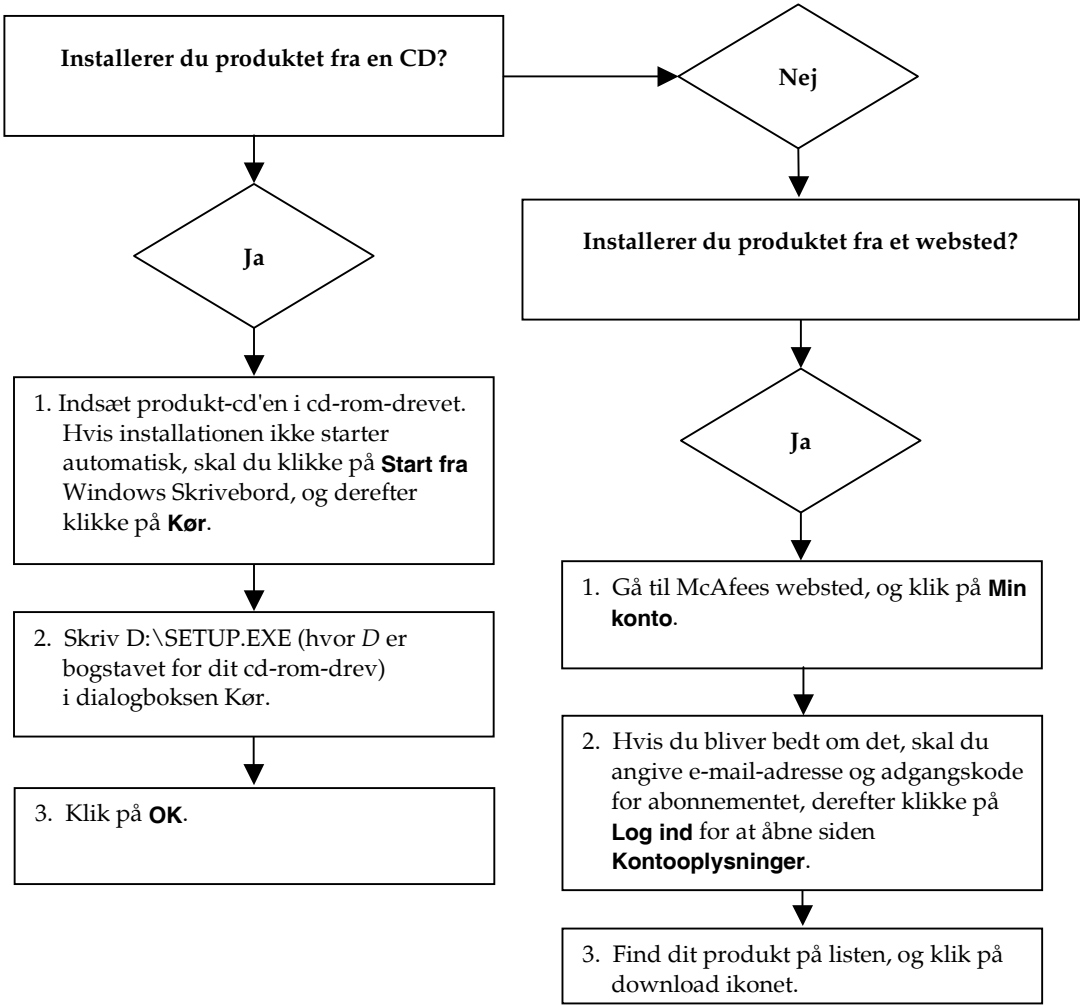
personalfirewallplus

Brugerhåndbog

McAfee®

Oversigtskort

Hvis du installerer produktet fra en cd eller et websted, kan du med fordel udskrive dette praktiske referenceark.



Få yderligere oplysninger

Hvis du vil kunne læse brugerhåndbøgerne på produkt-cd'en, skal du kontrollere, at Acrobat Reader er installeret på computeren, og hvis dette ikke er tilfældet, kan du installere den nu fra McAfee produkt-cd'en.

1. Indsæt produkt-cd'en i cd-rom-drevet.
2. Åbn Windows Stifinder: Klik på **Start** på Windows-skrivebordet, og klik på **Søg**.
3. Find mappen Manuals og dobbeltklik på den ønskede brugerhåndbog i.PDF-format.

Fordele ved registrering

McAfee anbefaler, at du følger den enkle fremgangsmåde, som produktet giver mulighed for, til at fremsende din registrering direkte til os. Registreringen sikrer, at du modtager rettidig teknisk ekspertbistand plus de følgende fordele:

- GRATIS elektronisk support
- Virusdefinitions (.DAT)-filopdateringer i et år efter installationen ved køb af VirusScan-software

  Gå til http://www.mcafee.com/ for at få oplyst prisen på yderligere et års abonnement på virussignaturer.
- 60-dages garanti, som garanterer erstatning af software-cd'en, hvis denne er fejlbehæftet eller beskadiget
- SpamKiller-filteropdateringer i et år efter installationen ved køb af SpamKiller-software

  Gå til http://www.mcafee.com/ for at få oplyst prisen på yderligere et års abonnement på filteropdateringer.
- McAfee Internet Security Suite-opdateringer i et år efter installationen ved køb af MIS-software

  Gå til http://www.mcafee.com/ for at få oplyst prisen på yderligere et års abonnement på indholdsopdateringer.

Teknisk support

Teknisk support fås på

http://www.mcafeehelp.com/.

Vores supportwebsted tilbyder 24-timers adgang til vores brugervenlige Svarguide, der rummer løsninger og svar på de mest almindelige supportspørgsmål.

Erfarne brugere kan også prøve vores mere avancerede muligheder, herunder Nøgleordssøgning og Hjælp-træ. Hvis du ikke kan finde en løsning, kan du også prøve vores GRATIS Chat Now!- og E-mail Express! -faciliteter. Via chat og e-mail kan du hurtigt kontakte vores kvalificerede supportteknikere via internettet uden omkostning. Ellers kan du finde oplysninger om telefonsupport på

http://www.mcafeehelp.com/.

Indhold

Introduktion 1

Velkommen til McAfee Personal Firewall Plus.

McAfee Personal Firewall Plus-software giver dig avanceret beskyttelse af din computer og dine personlige data. Personal Firewall opstiller en barriere mellem computeren og internettet og ligger i baggrunden og overvåger, om der foregår mistænkelige aktiviteter i internettrafikken.

Programmet giver dig følgende funktioner:

- Forsvarer dig mod potentielle hackerscanninger og -angreb
- Supplerer antivirusbeskyttelsen
- Overvåger internet- og netværksaktivitet
- Alarmerer dig om potentielt fjendtlige hændelser
- Giver dig detaljerede oplysninger om mistænkelig internettrafik
- Integrerer funktionalitet fra HackerWatch.org, herunder rapportering af hændelser, værktøj til selvtest og mulighed for at rapportere hændelser til andre myndigheder på internettet pr. e-mail
- Funktioner til omhyggelig sporing og undersøgelse af hændelser

Nye funktioner

- **Forbedret spilsupport**
  McAfee Personal Firewall Plus beskytter computeren mod forsøg på indtrængen og mistænkelige aktiviteter under spil med fuld skærm, men alarmerne kan skjules, hvis programmet registrerer forsøg på indtrængen eller mistænkelige aktiviteter. Røde alarmer vises, når du afslutter spillet.

- **Forbedret adgangshåndtering**
  McAfee Personal Firewall Plus lader dig i hvert enkelt tilfælde give programmer midlertidig adgang til internettet. Adgangen begrænses til perioden fra start til afslutning af programmet. Når Personal Firewall registrerer et ukendt program, der forsøger at kommunikere via internettet, vises en rød alarm, hvor du kan give programmet midlertidig adgang til internettet.

- **Forbedret sikkerhedskontrol**
  Ved hjælp af låsefunktionen i McAfee Personal Firewall Plus kan du øjeblikkeligt blokere al ind- og udgående trafik mellem computeren og internettet. Du kan aktivere og deaktivere låsning tre steder i Personal Firewall.

- **Forbedrede gendannelsesindstillinger**
  Ved at klikke på Nulstil indstillinger kan du automatisk gendanne standardindstillingerne i Personal Firewall. Hvis Personal Firewall udviser uønsket adfærd, som du ikke kan ændre, kan du vælge at fortryde dine indstillinger og vende tilbage til produktets standardindstillinger.

- **Beskyttelse af internetforbindelse**
  For at forhindre utilsigtet lukning af internetforbindelsen fjerner Personal Firewall muligheden for at forbyde en internetadresse fra en blå alarm, hvis Personal Firewall registrerer, at en internetforbindelse stammer fra en DHCP- eller DNS-server. Hvis den indgående trafik ikke stammer fra en DHCP- eller DNS-server, vises muligheden.

- **Forbedret integration af HackerWatch.org**
  Det er nemmere end nogensinde før at indberette potentielle hackere. McAfee Personal Firewall Plus forbedrer HackerWatch.org's funktionalitet, som omfatter indsendelse af oplysninger om potentielt skadelige hændelser til databasen.

- **Udvidet intelligent programhåndtering**
  Når et program forsøger at opnå internetadgang, kontrollerer Personal Firewall først, om det er et program, der er tillid til, eller et potentielt ondsindet program. Hvis programmet genkendes som et, der er tillid til, giver Personal Firewall det automatisk adgang til internettet, så du ikke behøver at gøre det.

- **Avanceret registrering af trojanske heste**
  McAfee Personal Firewall Plus kombinerer håndtering af programmers forbindelse til internettet med en forbedret database, så det registrerer flere potentielt ondsindede programmer, såsom trojanske heste, og blokerer deres forsøg på at opnå adgang til internettet og videresende dine personlige data.

- **Forbedret visuel sporing**
  Den visuelle sporingsfunktion omfatter letlæselige grafiske kort, som viser, hvor i verden fjendtlige angreb og fjendtlig trafik stammer fra, og detaljerede oplysninger om kontakter og ejere fra den IP-adresse, som angrebene og trafikken stammer fra.

- **Øget brugervenlighed**
  McAfee Personal Firewall Plus omfatter en installationsassistent og en brugervejledning, som hjælper brugerne ved installation og brug af deres firewall. Selvom produktet er beregnet til at fungere uden indgriben, stiller McAfee en lang række ressourcer til rådighed for brugerne, som gør det lettere at forstå, hvad deres firewall gør for dem.

- **Forbedret registrering af indtrængen**
  Personal Firewall's system til registrering af indtrængen registrerer udbredte angrebsmønstre og andre mistænkelige aktiviteter. Systemet overvåger alle datapakker, holder øje med mistænkelige dataoverførsler og -overførselsmetoder og logfører disse i hændelseslogfilen.

- **Forbedret trafikanalyse**
  McAfee Personal Firewall Plus viser dig både indgående og udgående data til og fra computeren, ligesom det viser programforbindelser, herunder programmer der aktivt "lytter" efter åbne forbindelser. Herved kan du se og skride ind over for programmer, der kan være sårbare i forhold til indtrængen.

Systemkrav

- Microsoft® Windows 98, Windows Me, Windows 2000 eller Windows XP
- Pc med Pentium-kompatibel processor
  Windows 98, 2000: 133 MHz eller hurtigere
  Windows Me: 150 MHz eller hurtigere
  Windows XP (Home og Pro): 300 MHz eller hurtigere
- RAM
  Windows 98, Me, 2000: 64 MB
  Windows XP (Home og Pro): 128 MB
- 40 MB ledig plads på harddisken
- Microsoft® Internet Explorer 5.5 eller nyere

BEMÆRK
Besøg Microsofts websted på adressen http://www.microsoft.com/worldwide/ for at opgradere til den seneste version af Internet Explorer.

Afinstallation af andre firewalls

Før du installerer McAfee Personal Firewall Plus-software, skal du afinstallere eventuelle andre firewall-programmer på computeren. Følg dit nuværende firewall-programs vejledning til afinstallation.

BEMÆRK
Hvis du bruger Windows XP, behøver du ikke at deaktivere den indbyggede firewall, før du installerer McAfee Personal Firewall Plus. Vi anbefaler dog, at du deaktiverer den indbyggede firewall. Hvis du ikke gør det, modtager du ingen hændelser i logfilen over indgående hændelser i McAfee Personal Firewall Plus.

Angivelse af standard-firewall

McAfee Personal Firewall kan administrere tilladelser og trafik i forhold til internetprogrammer på computeren, selv om Windows Firewall kører på den.

Når McAfee Personal Firewall er installeret, deaktiverer den automatisk Windows Firewall og indstiller sig selv som standard-firewall. Derefter oplever du kun McAfee Personal Firewall-funktionalitet og -meddelelser. Hvis du senere aktiverer Windows Firewall i Windows Sikkerhedscenter eller Windows Kontrolpanel og lader begge firewalls køre på computeren, kan det medføre mangelfuld logføring i McAfee Firewall og dobbeltforekomster af status- og alarmmeddelelser.

BEMÆRK
Hvis begge firewalls er aktiveret, viser McAfee Personal Firewall ikke alle de blokerede IP-adresser under fanen Indgående hændelser. Windows Firewall opfanger og blokerer de fleste af disse hændelser, hvilket forhindrer McAfee Personal Firewall i at registrere og logføre dem. McAfee Personal Firewall kan dog blokere yderligere trafik på grundlag af andre sikkerhedsfaktorer, og denne trafik logføres.

Logføring er som standard deaktiveret i Windows Firewall, men hvis du vælger at aktivere begge firewalls, kan du aktivere Windows Firewall-logføring. Windows Firewall-logfilens standardplacering er C:\Windows\pfirewall.log

For at sikre, at computeren beskyttes af mindst én firewall, genaktiveres Windows Firewall automatisk, når McAfee Personal Firewall afinstalleres.

Hvis du deaktiverer McAfee Personal Firewall eller vælger sikkerhedsindstillingen **Åben** uden manuelt at aktivere Windows Firewall, fjerner du al firewall-beskyttelse, dog ikke hvad angår tidligere blokerede programmer.

Indstilling af sikkerhedsniveau

Du kan konfigurere sikkerhedsindstillingerne og angive, hvordan Personal Firewall skal reagere på uønsket trafik. Som udgangspunkt er sikkerhedsniveauet **Standard** aktiveret. Når et program anmoder om internetadgang, og du giver det adgang, på sikkerhedsniveauet **Standard**, giver du programmet fuld adgang. Ved fuld adgang får programmet lov til både at sende data og modtage uopfordrede data på ikke-systemporte.

Sådan konfigureres sikkerhedsindstillingerne:

1 Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indstillinger**.

2 Klik på ikonet **Sikkerhedsindstillinger**.

3 Indstil sikkerhedsniveauet ved at flytte skyderen til det ønskede niveau.

Sikkerhedsniveauet kan indstilles mellem Lockdown (Låst) og Open (Åben).

- **Lockdown** (Låst) **-** Alle internetforbindelser på computeren lukkes. Du kan bruge denne indstilling til at blokere porte, som du har konfigureret til at være åbne på siden Systemtjenester.
- **Høj sikkerhed -** Når et program anmoder om en bestemt form for internetadgang (f.eks. Kun udgående adgang), kan du enten give eller nægte programmet en internetforbindelse. Hvis programmet senere anmoder om fuld adgang, kan du enten give det fuld adgang eller bevare begrænsningen Kun udgående adgang.
- **Standardsikkerhed** (anbefales) **-** Når et program anmoder om og får internetadgang, får det fuld internetadgang til at håndtere ind- og udgående trafik.
- **Tillidssikkerhed -** Du har automatisk tillid til alle programmer, første gang de forsøger at få adgang til internettet. Du kan dog konfigurere Personal Firewall således, at der gives alarmer, som underretter dig om nye programmer på computeren. Brug denne indstilling, hvis du oplever, at visse spil eller streaming-medier ikke virker.
- **Open** (Åben) **-** Din firewall er deaktiveret. Denne indstilling tillader al trafik at passere gennem Personal Firewall uden filtrering.

BEMÆRK
Programmer, der tidligere er blevet blokeret, blokeres fortsat, når firewall'en indstilles til **Open** (Åben) eller **Lockdown** (Låst). Dette kan du undgå ved enten at ændre programmets tilladelse til **Tillad fuld adgang** eller slette tilladelsesreglen **Blokeret** på listen **Internetprogrammer**.

4 Du kan vælge yderligere sikkerhedsindstillinger:

BEMÆRK
Hvis computeren kører under Windows XP, og der er tilknyttet flere XP-brugere, kan du kun foretage disse indstillinger, hvis du er logget på computeren som administrator.

- **Registrer Registrering af indtrængen-hændelser i logfilen over indgående hændelser -** Hvis du vælger denne indstilling, vises hændelser, der registreres af systemet til registrering af indtrængen, i logfilen over indgående hændelser. Systemet til registrering af indtrængen registrerer almindelige former for angreb og andre mistænkelige aktiviteter. Systemet overvåger alle ind- og udgående datapakker og holder øje med mistænkelige dataoverførsler og -overførselsmetoder. Det sammenholder disse med en "signaturdatabase" og smider automatisk pakker fra angribende computere ud.

  Systemet til registrering af indtrængen overvåger bestemte trafikmønstre, som de uønskede gæster bruger. Det kontrollerer alle de pakker, som computeren modtager, for mistænkelig trafik og trafik, som med sikkerhed indebærer angreb. Hvis Personal Firewall f.eks. registrerer ICMP-pakker, analyserer det dem for at finde mistænkelige trafikmønstre ved at sammenholde ICMP-trafikken med kendte angrebsmønstre.

- **Accepter ICMP-ping-anmodninger** - ICMP-trafik bruges primært til at foretage sporinger og pings. Pings bruges ofte til at udføre en hurtig test, før der gøres forsøg på at oprette en kommunikationsforbindelse. Hvis du bruger eller har brugt et peer-to-peer-fildelingsprogram, modtager du sikkert mange pings. Hvis du vælger denne indstilling, imødekommer Personal Firewall alle ping-anmodninger uden at logføre de modtagne pings i logfilen over indgående hændelser. Hvis du ikke vælger denne indstilling, blokerer Personal Firewall alle ping-anmodninger og logfører de modtagne pings i logfilen over indgående hændelser.

- **Tillad bruger med begrænset adgang at ændre indstillinger for Personal Firewall** - Hvis du kører Windows XP eller Windows 2000 Professional med flere brugere, kan du vælge denne indstilling for at tillade XP-brugere med begrænset adgang at ændre indstillingerne i Personal Firewall.

5 Klik på **OK**, hvis du er færdig med at foretage ændringer.

Test af McAfee Personal Firewall Plus

Du kan teste, om din Personal Firewall er sårbar over for indtrængen og mistænkelig aktivitet.

Sådan testes Personal Firewall vha. McAfee-ikonet på proceslinjen:

- Højreklik på McAfee-ikonet på Windows-proceslinjen, og vælg **Test firewall**.

Personal Firewall åbner Internet Explorer og hjemmesiden http://www.hackerwatch.org/, som administreres af McAfee. Følg anvisningerne på scanningssiden hos HackerWatch.org for at teste Personal Firewall.

Brug af McAfee SecurityCenter

McAfee SecurityCenter er din "one-stop-shop" inden for sikkerhed, og du kan åbne det vha. dets ikon på Windows' proceslinje eller på Windows-skrivebordet. Med SecurityCenter kan du gøre følgende:

- Få en gratis sikkerhedsanalyse af computeren.
- Åbne, administrere og konfigurere alle dine McAfee-abonnementer vha. det samme ikon.
- Se konstant opdaterede virusalarmer og de seneste produktoplysninger.
- Finde hurtige links til ofte stillede spørgsmål og kontooplysninger på McAfees websted.

> **BEMÆRK**
> Klik på **Hjælp** i dialogboksen **SecurityCenter** for at få yderligere oplysninger om funktionerne.

Når SecurityCenter kører, og alle McAfee-funktionerne på din computer er aktiverede, vises et rødt M-ikon på Windows-proceslinjen. Dette område befinder sig normalt i nederste højre hjørne af dit Windows-skrivebord, hvor uret sidder.

Hvis et eller flere McAfee-programmer på din computer er deaktiverede, skifter McAfee-ikonet til sort.

Sådan åbnes McAfee SecurityCenter:

1. Højreklik på McAfee-ikonet, og vælg **Åbn SecurityCenter**.

Sådan åbnes Personal Firewall i McAfee SecurityCenter:

1. Klik på fanen **Personal Firewall Plus** i SecurityCenter.
2. Vælg en opgave i menuen Jeg ønsker at...

Sådan åbnes Personal Firewall fra Windows:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, og vælg **Personal Firewall**.
2. Vælg en opgave.

Brug af McAfee Personal Firewall Plus 2

Sådan åbnes Personal Firewall:

- Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg en opgave.

Om siden Resume

Resumefunktionen i Personal Firewall omfatter fire resumesider:

- Overordnet resume
- Programresume
- Hændelsesresume
- HackerWatch-resume

Resumesiderne indeholder en lang række forskellige rapporter om nylige indgående hændelser, programstatus og forsøg på indtrængen over hele verden, som er registreret hos HackerWatch.org. Du kan også finde links til oplysninger om udførelse af almindelige opgaver i Personal Firewall.

Sådan åbnes siden Overordnet resume i Personal Firewall:

- Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Vis resume** (Figur 2-1).

Figur 2-1. Siden Overordnet resume

Klik på følgende for at navigere rundt til forskellige resumesider:

Punkt	Beskrivelse
Skift visning	Klik på **Skift visning** for at åbne en liste over resumesider. På listen kan du vælge en resumeside, der skal vises.
Højre pil	Klik på ikonet med pilen, der peger mod højre, for at få vist den næste resumeside.
Venstre pil	Klik på ikonet med pilen, der peger mod venstre, for at få vist den foregående resumeside.
Start	Klik på start-ikonet for at vende tilbage til siden **Overordnet resume**.

Siden Overordnet resume rummer følgende oplysninger:

Punkt	Beskrivelse
Sikkerhedsindstilling	Her vises det sikkerhedsniveau, som firewall'en er indstillet til. Klik på linket for at ændre sikkerhedsniveauet.
Blokerede hændelser	Her vises antallet af hændelser, der er blevet blokeret i dag. Klik på linket for at få vist detaljer fra siden Indgående hændelser.

Punkt	Beskrivelse
Ændrede programregler	Her vises antallet af programregler, der er blevet ændret for nylig. Du kan klikke på linket og få vist listen over programmer, som har fået adgang eller er blevet blokeret, og ændre programtilladelser.
Nyheder	**Nyheder** viser det seneste program, der har fået fuld adgang til internettet.
Sidste hændelse	**Sidste hændelse** viser de seneste indgående hændelser. Du kan klikke på et link og spore hændelsen eller angive, at du har tillid til IP-adressen. Hvis du angiver, at du har tillid til en IP-adresse, giver du al trafik fra adressen adgang til computeren.
Dagsrapport	**Dagsrapport** viser det antal indgående hændelser, som Personal Firewall har blokeret i dag, i denne uge og i denne måned. Klik på linket for at få vist detaljer fra siden Indgående hændelser.
Aktive programmer	**Aktive programmer** viser de programmer, der kører på computeren og har adgang til internettet lige nu. Du kan klikke på et program og få vist de IP-adresser, som programmet har forbindelse til.
Almindelige opgaver	Ved at klikke på et link under **Almindelige opgaver** kan du gå videre til sider i Personal Firewall, hvor du kan få vist firewall-aktiviteter og udføre opgaver.

Sådan åbnes siden Programresume:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Vis resume.**
2. Klik på **Skift visning**, og vælg **Programresume**.

Siden Programresume rummer følgende oplysninger:

Punkt	Beskrivelse
Trafikovervågning	**Trafikovervågning** viser de ind- og udgående internetforbindelser i de seneste 15 minutter. Du kan klikke på grafen for at få vist nærmere oplysninger om trafikovervågningen.
Aktive programmer	**Aktive programmer** viser de mest aktive programmers forbrug af båndbredde i de seneste 24 timer. **Program** - det program, der har adgang til internettet. **%** - programmets forbrug af båndbredde i procent. **Tilladelse** - den type internetadgang, som programmet har tilladelse til. **Regel oprettet** - det tidspunkt, hvor programreglen blev oprettet.

Punkt	Beskrivelse
Nyheder	**Nyheder** viser det seneste program, der har fået fuld adgang til internettet.
Aktive programmer	**Aktive programmer** viser de programmer, der kører på computeren og har adgang til internettet lige nu. Du kan klikke på et program og få vist de IP-adresser, som programmet har forbindelse til.
Almindelige opgaver	Ved at klikke på et link under **Almindelige opgaver** kan du gå videre til sider i Personal Firewall, hvor du kan få vist programstatus og udføre programrelaterede opgaver.

Sådan åbnes siden Hændelsesresume:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Vis resume.**
2. Klik på **Skift visning**, og vælg **Hændelsesresume**.

Siden Hændelsesresume rummer følgende oplysninger:

Punkt	Beskrivelse
Portsammenligning	**Portsammenligning** viser et cirkeldiagram, som angiver de porte på computeren, der hyppigst er søgt adgang til i de seneste 30 dage. Du kan klikke på et portnavn og få vist detaljer fra siden Indgående hændelser. Du kan også anbringe musemarkøren over portnummeret og få vist en beskrivelse af porten.
Hyppigste angribere	**Hyppigste angribere** viser de hyppigst blokerede IP-adresser, hvornår den seneste indgående hændelse er forekommet for hver adresse, og det samlede antal indgående hændelser for hver adresse i de seneste 30 dage. Du kan klikke på en hændelse og få vist detaljer om den fra siden Indgående hændelser.
Dagsrapport	**Dagsrapport** viser det antal indgående hændelser, som Personal Firewall har blokeret i dag, i denne uge og i denne måned. Du kan klikke på et tal og få vist detaljer om hændelsen fra logfilen over indgående hændelser.
Sidste hændelse	**Sidste hændelse** viser de seneste indgående hændelser. Du kan klikke på et link og spore hændelsen eller angive, at du har tillid til IP-adressen. Hvis du angiver, at du har tillid til en IP-adresse, giver du al trafik fra adressen adgang til computeren.
Almindelige opgaver	Ved at klikke på et link under **Almindelige opgaver** kan du gå videre til sider i Personal Firewall, hvor du kan få vist detaljer om hændelser og udføre hændelsesrelaterede opgaver.

Sådan åbnes siden HackerWatch-resume:

1 Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Vis resume.**

2 Klik på **Skift visning**, og vælg **HackerWatch-resume**.

Siden HackerWatch-resume rummer følgende oplysninger**:**

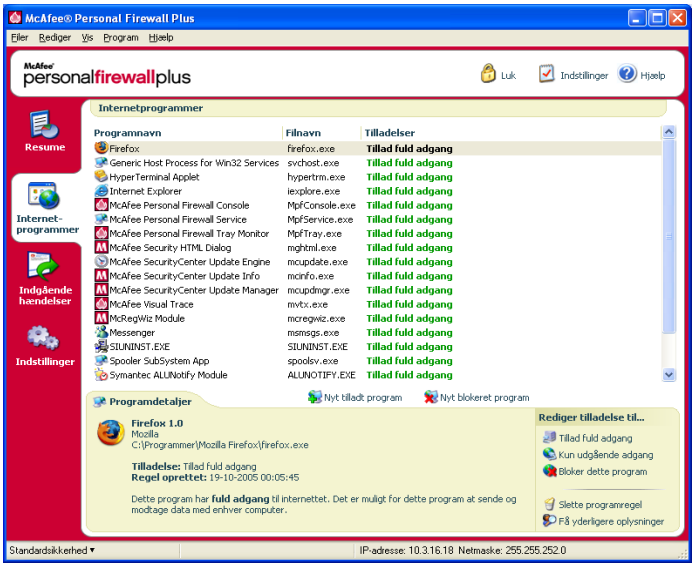
Punkt	Beskrivelse
World Activity (Aktiviteter på verdensplan)	**World Activity** (Aktiviteter på verdensplan) viser et verdenskort med angivelse af nyligt blokerede aktiviteter, som overvåges af HackerWatch.org. Du kan klikke på kortet og åbne verdenskortet til analyse af trusler Global Threat Analysis Map hos HackerWatch.org.
Event Tracking (Hændelsessporing)	**Event Tracking** (Hændelsessporing) viser antallet af indgående hændelser, der er sendt til HackerWatch.org.
Global Port Activity (Global portaktivitet)	**Global Port Activity** (Global portaktivitet) viser de porte, hvor der i de seneste 5 dage synes at have været flest trusler. Du kan klikke på en port for at få vist dens nummer og en beskrivelse af den.
Almindelige opgaver	Du kan klikke på et link i **Almindelige opgaver** og gå videre til sider hos HackerWatch.org, hvor du kan få yderligere oplysninger om hacker-aktivitet over hele verden.

Om siden Internetprogrammer

Du kan bruge siden Internetprogrammer til at få vist listen over programmer, som har fået adgang eller er blevet blokeret.

Sådan åbnes siden Internetprogrammer:

- Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Programmer** (Figur 2-2).



Figur 2-2. Siden Internetprogrammer

Siden Internetprogrammer rummer følgende oplysninger:

- Programnavne
- Filnavne
- Aktuelle tilladelsesniveauer
- Programdetaljer: programnavn og -version, selskabsnavn, stinavn, tilladelse, tidsstempler samt forklaringer af tilladelsestyper.

Ændring af regler for internetprogrammer

Med Personal Firewall kan du ændre adgangsregler for programmer.

Sådan ændres en programregel:

1. Højreklik på McAfee-ikonet, peg på **Personal Firewall**, og vælg **Internetprogrammer**.
2. Højreklik på reglen for programmet på listen **Internetprogrammer**, og vælg en indstilling:
   - **Tillad fuld adgang -** Programmet tillades at oprette udgående og indgående forbindelser.
   - **Kun udgående adgang -** Programmet tillades kun at oprette udgående internetforbindelser.
   - **Bloker dette program -** Programmet nægtes internetadgang.

     BEMÆRK
     Tidligere blokerede programmer blokeres fortsat, når firewall'en indstilles til **Open** (Åben) eller **Lockdown** (Låst). Dette kan du undgå ved enten at ændre programmets adgangsregel til **Fuld adgang** eller slette tilladelsesreglen **Blokeret** i listen over **Internetprogrammer**.

Sådan slettes en programregel:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Internetprogrammer**.
2. Højreklik på reglen for programmet på listen **Internetprogrammer**, og vælg **Slet programregel**.

Næste gang programmet anmoder om internetadgang, kan du indstille dets tilladelsesniveau og tilføje det til listen igen.

Tilladelse og blokering af internetprogrammer

Sådan foretages der ændringer i listen over internetprogrammer, som har fået adgang eller er blevet blokeret:

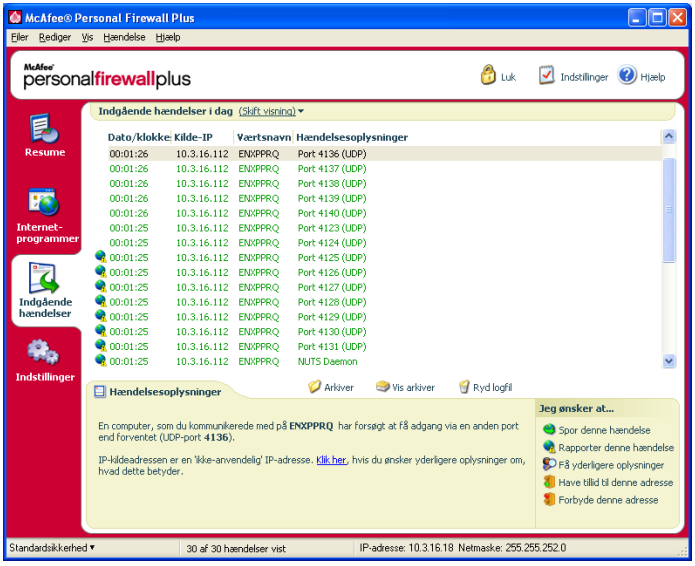
1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Internetprogrammer**.
2. Klik på en af følgende indstillinger på siden Internetprogrammer:
   - **Nyt tilladt program** - Programmet tillades fuld internetadgang.
   - **Nyt blokeret program** - Programmet nægtes internetadgang.
   - **Slet programregel** - Programreglen slettes.

Om siden Indgående hændelser

Du kan bruge siden Indgående hændelser til at få vist den logfil over indgående hændelser, der genereres, når Personal Firewall blokerer uopfordrede internetforbindelser.

Sådan åbnes siden Indgående hændelser:

- Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser** (Figur 2-3).



Figur 2-3. Siden Indgående hændelser

Siden Indgående hændelser rummer følgende oplysninger:

- Tidsstempler
- Kilde-IP-adresser
- Værtsnavne
- Navne på tjenester og programmer
- Hændelsesdetaljer: forbindelsestyper, forbindelsesporte, værtsnavne eller IP-adresser samt forklaringer af hændelser på porte

Forklaring af hændelser

Om IP-adresser

IP-adresser består af tal: nærmere bestemt fire tal mellem 0 og 255. Disse tal identificerer et bestemt sted, som man kan dirigere trafik hen til på internettet.

IP-adressetyper

Der findes flere IP-adressetyper, som skiller sig ud af forskellige årsager:

Ikke-anvendelige IP-adresser - Disse kaldes også "Private IP-adresser". De kan ikke benyttes på internettet. De private IP-blokke er 10.x.x.x, 172.16.x.x - 172.31.x.x og 192.168.x.x.

Tilbagekoblings-IP-adresser - Tilbagekoblingsadresser anvendes til testformål. Trafik, der sendes til denne blok af IP-adresser, sendes direkte tilbage til den enhed, som genererede pakken. Den forlader aldrig enheden og anvendes primært til afprøvning af hardware og software. Tilbagekoblings-IP-blokken er 127.x.x.x.

Null-IP-adresser - Disse IP-adresser er ugyldige. Når en sådan adresse registreres, angiver Personal Firewall, at trafikken anvendte en tom IP-adresse. Dette er typisk et tegn på, at afsenderen bevidst forsøger at skjule, hvor trafikken kommer fra. Afsenderen vil ikke kunne modtage svar på det afsendte, medmindre pakken modtages af et program, der forstår pakkens indhold, som omfatter særlige instruktioner til netop dette program. Alle adresser, der starter med 0 (0.x.x.x), er null-adresser. For eksempel er 0.0.0.0 en ugyldig IP-adresse.

Hændelser fra 0.0.0.0

Hvis du oplever hændelser fra IP-adressen 0.0.0.0, er der to sandsynlige årsager. Den første og mest almindelige er, at computeren har modtaget en forkert udformet pakke. Internettet er ikke altid 100% pålideligt, og forkert udformede pakker kan forekomme. Da Personal Firewall opdager disse pakker, før TCP/IP-funktionen kan validere dem, rapporterer programmet muligvis pakkerne som en hændelse.

Den anden situation opstår, når kilde-IP-adressen er en fupadresse. Fuppakker kan være et tegn på, at der er nogen, der leder efter trojanske heste på computeren. Personal Firewall blokerer denne form for aktiviteter, så computeren er ikke i fare.

Hændelser fra 127.0.0.1

Ved hændelser anføres kilde-IP-adressen 127.0.0.1 af og til. Dette kaldes en tilbagekoblingsadresse eller localhost.

Mange legitime programmer bruger tilbagekoblingsadressen til kommunikation blandt komponenter. For eksempel kan du konfigurere mange personlige e-mail- og webservere via en webgrænseflade. For at få adgang til grænsefladen skal du skrive adressen "http://localhost/" i internetbrowseren.

Personal Firewall tillader trafik fra disse programmer, så hvis du bemærker hændelser fra 127.0.0.1, betyder det sandsynligvis, at kilde-IP-adressen er en fupadresse. Fuppakker er normalt et tegn på, at der er nogen, der leder efter trojanske heste på computeren. Personal Firewall blokerer disse forsøg på indtrængen, så computeren er ikke i fare.

Der er nogle programmer, navnlig Netscape 6.2 og nyere, der kræver, at du tilføjer 127.0.0.1 til listen over IP-adresser, der er tillid til. Disse programmers komponenter kommunikerer med hinanden på en måde, så Personal Firewall ikke kan afgøre, om trafikken er lokal eller ej.

I eksemplet med Netscape 6.2, vil du ikke kunne bruge din venneliste, hvis du ikke har tillid til 127.0.0.1. Hvis du oplever trafik fra 127.0.0.1, og alle programmer på computeren fungerer normalt, er det således sikkert at blokere denne trafik. Men hvis der er problemer med et program (såsom Netscape), kan du tilføje 127.0.0.1 til listen over IP-adresser, du har tillid til, i Personal Firewall.

Hvis det løser problemet at tilføje 127.0.0.1 til listen, bliver du nødt til at afveje fordele og ulemper: Hvis du har tillid til 127.0.0.1, fungerer programmet, men du bliver mere udsat for fupangreb. Hvis du ikke har tillid til adressen, fungerer programmet ikke, men du forbliver beskyttet mod visse former for ondartet trafik.

Hændelser fra computere på dit LAN

Hændelser kan genereres fra computere på det lokale netværk (LAN). For at fremhæve, at disse hændelser genereres af netværket, viser Personal Firewall dem med grønt.

På de fleste virksomhedsnetværk er det mest hensigtsmæssigt at vælge **Hav tillid til alle computere på dit LAN** i indstillingerne under IP-adresser, der er tillid til.

I nogle situationer kan et "lokalt" netværk dog være lige så farligt som internettet, især hvis computeren indgår i et bredbåndsnetværk, hvor der anvendes DSL- eller kabelmodem. I så fald skal du ikke vælge indstillingen **Hav tillid til alle computere på dit LAN**. Tilføj i stedet de lokale computeres IP-adresser til listen over IP-adresser, der er tillid til.

Hændelser fra private IP-adresser

IP-adresser med formatet 192.168.xxx.xxx, 10.xxx.xxx.xxx og 172.16.0.0 - 172.31.255.255 betegnes som ikke-anvendelige eller private IP-adresser. Disse IP-adresser bør aldrig forlade netværket, og man kan oftest have tillid til dem.

192.168.xxx.xxx-blokken anvendes i forbindelse med Microsoft ICS (Internet Connection Sharing). Hvis du bruger ICS og ser hændelser fra denne IP-blok, kan du eventuelt tilføje IP-adressen 192.168.255.255 til listen over IP-adresser, du har tillid til. Herved angiver du, at du har tillid til hele blokken 192.168.xxx.xxx.

Hvis du ikke befinder dig på et privat netværk, men ser hændelser fra IP-adresser i disse områder, er kilde-IP-adressen muligvis en fupadresse. Fuppakker er normalt et tegn på, at der er nogen, der scanner efter trojanske heste. Det er vigtigt at huske på, at Personal Firewall blokerer disse forsøg, så computeren er ikke i fare.

Da private IP-adresser henviser til forskellige computere, afhængigt af hvilket netværk du befinder dig på, nytter det ikke at indberette disse hændelser.

Visning af hændelser i logfilen over indgående hændelser

Logfilen over indgående hændelser viser hændelser på flere forskellige måder. Standardvisningen begrænses til at vise hændelser, der er forekommet i dag. Du kan også få vist hændelser, der er forekommet i den forløbne uge, eller hele logfilen.

Personal Firewall gør det også muligt at få vist indgående hændelser fra bestemte dage eller bestemte internetadresser (IP-adresser) eller hændelser, der indeholder de samme hændelsesoplysninger.

Hvis du ønsker oplysninger om en hændelse, kan du klikke på hændelsen og få vist oplysninger i ruden **Hændelsesoplysninger**.

Visning af hændelser fra i dag

Brug denne indstilling til at få vist dagens hændelser.

Sådan vises hændelserne fra i dag:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Højreklik på en post i logfilen over indgående hændelser, og klik på **Vis hændelser fra i dag**.

Visning af denne uges hændelser

Brug denne indstilling til at få vist ugens hændelser.

Sådan vises denne uges hændelser:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Højreklik på en post i logfilen over indgående hændelser, og klik på **Vis denne uges hændelser**.

Visning af hele logfilen over indgående hændelser

Brug denne indstilling til at få alle hændelser.

Sådan vises alle hændelser i logfilen over indgående hændelser:

1. Højreklik på McAfee-ikonet, peg på **Personal Firewall**, og klik på **Indgående hændelser**.
2. Højreklik på en post i logfilen over indgående hændelser, og klik på **Vis fuld logfil**.

   Alle hændelser fra logfilen over indgående hændelser vises.

Visning af hændelser fra en bestemt dag

Brug denne indstilling til at få vist hændelser fra en bestemt dag.

Sådan vises en bestemt dags hændelser:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Højreklik på en post i logfilen over indgående hændelser, og klik på **Vis kun hændelser fra den markerede dag**.

Visning af hændelser fra en bestemt internetadresse

Brug denne indstilling til at få vist andre hændelser, der stammer fra en bestemt internetadresse.

Sådan vises hændelser fra en bestemt internetadresse:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og klik på **Indgående hændelser**.
2. Højreklik på en post i logfilen over indgående hændelser, og klik på **Vis kun hændelser fra den markerede internetadresse**.

Visning af hændelser med samme hændelsesoplysninger

Brug denne indstilling til at få vist andre hændelser i logfilen over indgående hændelser, der har de samme oplysninger i kolonnen Hændelsesoplysninger som den hændelse, du har valgt. Du kan finde ud af, hvor mange gange hændelsen er forekommet, og om den stammer fra den samme kilde. Kolonnen Hændelsesoplysninger indeholder en beskrivelse af hændelsen og det program eller den tjeneste, der bruger den pågældende port, hvis programmet eller tjenesten er kendt.

Sådan vises hændelser med samme hændelsesoplysninger:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og klik på **Indgående hændelser**.
2. Højreklik på en post i logfilen over indgående hændelser, og klik på **Vis kun hændelser med samme hændelsesoplysninger**.

Reaktioner på indgående hændelser

Ud over at få vist oplysninger om hændelser i logfilen over indgående hændelser kan du foretage en visuel sporing af de IP-adresser, der vedrører en hændelse i logfilen, eller få oplysninger om hændelsen hos antihacker-specialisterne på webstedet HackerWatch.org.

Sporing af den markerede hændelse

Du kan forsøge at foretage en visuel sporing af IP-adresser vedrørende en hændelse i logfilen over indgående hændelser.

Sådan spores en markeret hændelse:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Højreklik på den hændelse, du vil spore, i logfilen over indgående hændelser, og klik på **Spor markeret hændelse**. Du kan også dobbeltklikke på en hændelse for at spore den.

Som standard er Personal Firewall indstillet til at indlede en visuel sporing vha. det program til visuel sporing, der er integreret i Personal Firewall.

Få råd fra HackerWatch.org

Sådan får du råd fra HackerWatch.org:

1. Højreklik på McAfee-ikonet, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Vælg hændelsesposten på siden Indgående hændelser, og klik på **Få yderligere oplysninger** i ruden **Jeg ønsker at...**.

I din standardinternetbrowser åbnes webstedet HackerWatch.org for at hente oplysninger om hændelsestypen og råd om, hvorvidt hændelsen skal rapporteres.

Rapportering af en hændelse

Sådan rapporteres en hændelse, som du tror, var et angreb på computeren:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Klik på den hændelse, du vil rapportere, og klik på **Rapporter denne hændelse** i ruden **Jeg ønsker at...**.

Personal Firewall rapporterer hændelsen til HackerWatch.org vha. dit unikke bruger-id.

Tilmelding til HackerWatch.org

Første gang du åbner siden Resume, kontakter Personal Firewall HackerWatch.org for at generere et unikt bruger-id til dig. Hvis du allerede bruger tjenesten, valideres din tilmelding automatisk. Hvis du er ny bruger, skal du angive et kaldenavn og en e-mail-adresse og derefter klikke på valideringslinket i den bekræftelses-e-mail, som HackerWatch.org sender, for at kunne bruge de hændelsesrelaterede filtrerings-/e-mail-funktioner på webstedet.

Du kan indberette hændelser til HackerWatch.org uden at validere dit bruger-id. Men hvis du vil filtrere hændelser og sende e-mails om dem til en ven, skal du tilmelde dig tjenesten.

Når du tilmelder dig tjenesten, bliver det muligt at spore dine indberetninger, og vi kan underrette dig, hvis HackerWatch.org behøver flere oplysninger, eller hvis du skal foretage dig yderligere. Vi forudsætter også, at du tilmelder dig, da vi skal bekræfte de oplysninger, vi modtager, for at de kan være til gavn.

Alle e-mail-adresser, der stilles til rådighed for HackerWatch.org, holdes fortrolige. Hvis en internetudbyder anmoder om yderligere oplysninger, sendes denne anmodning via HackerWatch.org. Din e-mail-adresse afsløres aldrig.

Angivelse af tillid til en adresse

Du kan bruge siden Indgående hændelser til at tilføje en IP-adresse til listen over IP-adresser, der er tillid til, for at give den permanent forbindelse.

Hvis du ser en hændelse på siden Indgående hændelser, der indeholder en IP-adresse, som du ønsker at give adgang, kan du få Personal Firewall til at tillade forbindelser fra den til enhver tid.

Sådan tilføjes en IP-adresse til listen over IP-adresser, der er tillid til:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Højreklik på den hændelse, hvis IP-adresse du vil angive tillid til, og klik på **Hav tillid til IP-kildeadressen**.

Kontroller, at den IP-adresse, der vises i dialogboksen Hav tillid til denne adresse, er korrekt, og klik på **OK**. IP-adressen tilføjes til listen over IP-adresser, der er tillid til.

Sådan kontrolleres det, at IP-adressen er tilføjet:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indstillinger**.
2. Klik på ikonet **IP-adresser, der er tillid til / forbudte**, og klik på fanen **IP-adresser, der er tillid til**.

IP-adressen er nu markeret på listen over IP-adresser, der er tillid til.

Blokering af en adresse

Hvis en IP-adresse vises i logfilen over indgående hændelser, betyder det, at trafikken fra den pågældende adresse er blevet blokeret. Derfor øger det ikke beskyttelsen at forbyde en adresse, medmindre computeren har porte, der åbnes forsætligt vha. funktionen Systemtjenester, eller medmindre computeren har et program, der har tilladelse til at modtage trafik.

Tilføj kun en IP-adresse på listen over forbudte IP-adresser, hvis du har en eller flere porte, der åbnes forsætligt, og hvis du har grund til at mene, at du bør nægte den pågældende adresse adgang til åbne porte.

Hvis du ser en hændelse på siden Indgående hændelser, der indeholder en IP-adresse, som du ønsker at forbyde, kan du konfigurere Personal Firewall til at forhindre forbindelser fra den til enhver tid.

Du kan bruge siden Indgående hændelser, der indeholder IP-adresserne til al indgående internettrafik, til at forbyde en IP-adresse, som du mener er kilden til mistænkelig eller uønsket internetaktivitet.

Sådan tilføjes en IP-adresse til listen over forbudte IP-adresser:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. På siden Indgående hændelser vises IP-adresserne til al indgående internettrafik. Marker en IP-adresse, og benyt derefter en af følgende fremgangsmåder:
   - Højreklik på IP-adressen, og marker derefter **Forbyd IP-kildeadresse**.
   - Klik på **Forbyd denne adresse** i menuen **Jeg ønsker at**.
3. Brug en eller flere af følgende indstillinger til at konfigurere reglen for den forbudte IP-adresse i dialogboksen Tilføj regel for forbudt IP-adresse:
   - **En enkelt IP-adresse**: Den IP-adresse, der skal forbydes. Standardadressen er den IP-adresse, du har valgt på siden Indgående hændelser.
   - **Et IP-adresseområde**: De IP-adresser, der ligger mellem den, du angiver i feltet Fra IP-adresse, og den, du angiver i feltet Til IP-adresse.
   - **Lad denne regel udløbe den**: Den dato og det tidspunkt, hvor reglen for IP-adressen skal udløbe. Vælg den ønskede rullemenu for at vælge datoen og tidspunktet.
   - **Beskrivelse**: Du kan også beskrive den nye regel.
   - Klik på **OK**.
4. Klik på **Ja** i dialogboksen for at bekræfte indstillingen. Klik på **Nej** for at vende tilbage til dialogboksen Tilføj regel for forbudt IP-adresse.

Hvis Personal Firewall registrerer en hændelse fra en forbudt internetforbindelse, får du besked om det på den måde, du har angivet på siden Alarmindstillinger.

Sådan kontrolleres det, at IP-adressen er tilføjet:

1. Klik på fanen **Indstillinger**.
2. Klik på ikonet **IP-adresser, der er tillid til / forbudte**, og klik derefter på fanen **Forbudte IP-adresser**.

IP-adressen er nu markeret på listen Forbudte IP-adresser.

Administration af logfilen over indgående hændelser

Du kan bruge siden Indgående hændelser til at administrere de hændelser i logfilen over indgående hændelser, der genereres, når Personal Firewall blokerer uopfordret internettrafik.

Arkivering af logfilen over indgående hændelser

Du kan arkivere den aktuelle logfil over indgående hændelser og gemme alle de logførte indgående hændelser, herunder oplysninger om dato og tidspunkt, IP-kildeadresser, værtsnavne, porte og hændelsesoplysninger. Du bør arkivere logfilen over indgående hændelser jævnligt for at forhindre, at den bliver for stor.

Sådan arkiveres logfilen over indgående hændelser:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Klik på **Arkiver** på siden Indgående hændelser.
3. Klik på **Ja** i dialogboksen Arkiver logfil for at fortsætte handlingen.
4. Klik på **Gem** for at gemme arkivet på standardplaceringen, eller find en ny placering, hvor du vil gemme arkivet.

Bemærk! Personal Firewall arkiverer automatisk logfilen over indgående hændelser som standard. Marker eller fjern markeringen i afkrydsningsfeltet **Arkiver automatisk logførte hændelser** på siden Indstillinger for hændelseslogfil for at aktivere eller deaktivere indstillingen.

Visning af en arkiveret logfil over indgående hændelser

Du kan få vist alle de logfiler over indgående hændelser, som du har arkiveret. De arkiverede filer rummer oplysninger om dato og tidspunkt, IP-kildeadresser, værtsnavne, porte og hændelsesoplysninger.

Sådan vises en arkiveret logfil over indgående hændelser:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Klik på **Vis arkiver** på siden Indgående hændelser.
3. Vælg arkivnavnet, eller find det ved gennemsyn, og klik på **Åbn**.

Rydning af logfilen over indgående hændelser

Du kan rydde alle oplysninger i logfilen over indgående hændelser.

ADVARSEL: Når du har ryddet logfilen over indgående hændelser, kan du ikke gendanne den. Hvis du regner med at få brug for hændelseslogfilen på et senere tidspunkt, anbefales det at arkivere den i stedet for.

Sådan ryddes logfilen over indgående hændelser:

1. Højreklik på McAfee-ikonet, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Klik på **Ryd logfil** på siden Indgående hændelser.
3. Klik på **Ja** i dialogboksen for at rydde logfilen.

Kopiering af en hændelse til Udklipsholder

Du kan kopiere en hændelse til Udklipsholder, så du kan indsætte den i en tekstfil ved hjælp af Notesblok.

Sådan kopieres hændelser til Udklipsholder:

1. Højreklik på McAfee-ikonet, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Højreklik på hændelsen i logfilen over indgående hændelser.
3. Klik på **Kopier markeret hændelse til Udklipsholder**.
4. Åbn Notesblok.
   - Skriv `notepad` på kommandolinjen, eller klik på knappen **Start** i Windows, peg på **Programmer** og derefter på **Tilbehør**. Vælg **Notesblok**.
5. Klik på **Rediger** og derefter på Sæt ind. Hændelsesteksten vises i Notesblok. Gentag dette trin, indtil du har alle de nødvendige hændelser.
6. Gem Notesblok-filen et sikkert sted.

Sletning af den markerede hændelse

Du kan slette hændelser i logfilen over indgående hændelser.

Sådan slettes hændelser i logfilen over indgående hændelser:

1. Højreklik på McAfee-ikonet på Windows-proceslinjen, peg på **Personal Firewall**, og vælg **Indgående hændelser**.
2. Klik på den hændelse, du vil slette, på siden Indgående hændelser.
3. Klik på **Slet markeret hændelse** i menuen Rediger. Hændelsen slettes i logfilen over indgående hændelser.

Om alarmer

Vi anbefaler kraftigt, at du gør dig bekendt med de former for alarmer, som du vil møde, når du bruger Personal Firewall. Gennemse følgende alarmtyper, som kan forekomme, og de svarmuligheder, du har, så du trygt kan reagere på alarmerne.

BEMÆRK
Anbefalingerne vedrørende alarmer hjælper dig med at afgøre, hvordan du skal håndtere en alarm. Hvis du vil have anbefalingerne vist i alarmerne, skal du klikke på fanen **Indstillinger**, klikke på ikonet **Alarmindstillinger** og vælge enten **Brug smarte anbefalinger** (standardindstillingen) eller **Vis kun smarte anbefalinger** på listen **Smarte anbefalinger**.

Røde alarmer

Røde alarmer indeholder vigtige oplysninger, der kræver øjeblikkelig opmærksomhed:

- **Internetprogram blokeret** - Denne alarm vises, hvis Personal Firewall blokerer et programs forsøg på at få adgang til internettet. Hvis der f.eks. vises en alarm vedrørende en trojansk hest, nægter McAfee automatisk dette program adgang til internettet, idet det anbefaler, at du scanner computeren for virus.
- **Program ønsker adgang til internettet -** Denne alarm vises, hvis Personal Firewall registrerer internet- eller netværkstrafik i forhold til nye programmer.
- **Program er blevet ændret -**Denne alarm vises, hvis Personal Firewall registrerer, at et program, som du tidligere har givet internetadgang, er blevet ændret. Hvis du ikke har opgraderet programmet for nylig, skal du være forsigtig med at give det ændrede program adgang til internettet.
- **Program anmoder om serveradgang -** Denne alarm vises, hvis Personal Firewall registrerer, at et program, som du tidligere har givet internetadgang, har anmodet om internetadgang som server.

  BEMÆRK
  Den automatiske opdateringsfunktion i Windows XP SP2 henter og installerer som standard opdateringer til Windows-operativsystemet og andre Microsoft-programmer på computeren uden at give dig besked. Hvis et Microsoft-program er blevet ændret ved en af disse Windows-opdateringer, viser McAfee Personal Firewall alarmer, næste gang programmet åbnes.

  VIGTIGT
  Du skal give adgang til programmer, som kræver internetadgang for at udføre produktopdateringer via internettet (såsom McAfee-tjenester) for at holde dem opdateret.

Alarmen Internetprogram blokeret

Hvis der vises en alarm vedrørende en trojansk hest (Figur 2-4), nægter Personal Firewall automatisk dette program adgang til internettet, idet det anbefaler, at du scanner computeren for virus. Hvis McAfee VirusScan ikke er installeret, kan du åbne McAfee SecurityCenter.

Figur 2-4. Alarmen Internetprogram blokeret

Du kan få vist en kort beskrivelse af hændelsen og derefter vælge mellem følgende:

- Klik på **Yderligere oplysninger** for at få nærmere oplysninger om hændelsen fra logfilen over indgående hændelser (se yderligere oplysninger under *Om siden Indgående hændelser* på side 22).
- Klik på **Start McAfee VirusScan** for at scanne computeren for virus.
- Klik på **Fortsæt mit arbejde**, hvis du ikke ønsker at gøre noget ud over det, Personal Firewall allerede har gjort.
- Klik på **Tildel udgående adgang**, hvis du vil tillade en udgående forbindelse (**Høj** sikkerhed).

Alarmen Program ønsker adgang til internettet

Hvis du har valgt **Standard** eller **Høj** sikkerhed under Sikkerhedsindstillinger, viser Personal Firewall en alarm (Figur 2-5), når firewall'en registrerer internet- eller netværksforbindelser til nye eller ændrede programmer.

Figur 2-5. Alarmen Program ønsker adgang til internettet

Hvis der vises en alarm, der anbefaler forsigtighed med hensyn til at give programmet internetadgang, kan du klikke på **Klik her for at få mere at vide** for at få flere oplysninger om programmet. Denne mulighed vises kun i alarmen, hvis Personal Firewall er konfigureret til at bruge Smarte anbefalinger.

McAfee genkender muligvis ikke det program, der forsøger at få internetadgang (Figur 2-6).

Figur 2-6. Alarm om ikke-genkendt program

Derfor kan McAfee ikke fremsætte anbefalinger vedrørende håndtering af programmet. Du kan indberette programmet til McAfee ved at klikke på **Fortæl McAfee om dette program**. Der vises en webside, hvor du bedes om oplysninger om programmet. Angiv så mange oplysninger som muligt.

De oplysninger, du indsender, anvendes sammen med andre undersøgelsesværktøjer af vore HackerWatch-eksperter til at afgøre, om et program er berettiget til at stå opført i vores database over kendte programmer, og - i bekræftende fald - hvordan Personal Firewall skal håndtere det.

Du kan få vist en kort beskrivelse af hændelsen og derefter vælge mellem følgende:

- Klik på **Tildel adgang**, hvis du vil give programmet en udgående og indgående internetforbindelse.
- Klik på **Tildel adgang denne gang**, hvis du give programmet en midlertidig internetforbindelse. Adgangen begrænses til perioden fra start til afslutning af programmet.
- Klik på **Bloker al adgang** for at forbyde internetadgang.
- Klik på **Tildel udgående adgang**, hvis du vil tillade en udgående forbindelse (**Høj** sikkerhed).
- Klik på **Hjælp mig med at vælge** for at få vist onlinehjælp om programmers adgangstilladelser.

Alarmen Program er blevet ændret

Hvis du har valgt **Tillidssikkerhed**, **Standard** eller **Høj** sikkerhed under Sikkerhedsindstillinger, viser Personal Firewall en alarm (Figur 2-7), hvis Personal Firewall registrerer, at et program, som du tidligere har givet internetadgang, er blevet ændret. Hvis du ikke har opgraderet programmet for nylig, skal du være forsigtig med at give det ændrede program adgang til internettet.

Figur 2-7. Alarmen Program er blevet ændret

Du kan få vist en kort beskrivelse af hændelsen og derefter vælge mellem følgende:

- Klik på **Tildel adgang**, hvis du vil give programmet en udgående og indgående internetforbindelse.
- Klik på **Tildel adgang denne gang**, hvis du give programmet en midlertidig internetforbindelse. Adgangen begrænses til perioden fra start til afslutning af programmet.
- Klik på **Bloker al adgang** for at forbyde internetadgang.
- Klik på **Tildel udgående adgang**, hvis du vil tillade en udgående forbindelse (**Høj** sikkerhed).
- Klik på **Hjælp mig med at vælge** for at få vist onlinehjælp om programmers adgangstilladelser.

Alarmen Program anmoder om serveradgang

Hvis du har valgt **Høj** sikkerhed under sikkerhedsindstillingerne, viser Personal Firewall en alarm (Figur 2-8), når den registrerer, at et program, som du tidligere har givet internetadgang, har anmodet om internetadgang som server.

Figur 2-8. Alarmen Program anmoder om serveradgang

For eksempel vises der en alarm, hvis MSN Messenger anmoder om serveradgang for at sende en fil under en chat.

Du kan få vist en kort beskrivelse af hændelsen og derefter vælge mellem følgende:

- Klik på **Tildel adgang denne gang**, hvis du give programmet midlertidig internetadgang. Adgangen begrænses til perioden fra start til afslutning af programmet.
- Klik på **Tildel serveradgang**, hvis du vil give programmet en udgående og indgående internetforbindelse.

- Klik på **Begræns til udgående adgang**, hvis du vil forbyde en indgående internetforbindelse.
- Klik på **Bloker al adgang** for at forbyde internetadgang.
- Klik på **Hjælp mig med at vælge** for at få vist onlinehjælp om programmers adgangstilladelser. Grønne alarmer

Grønne alarmer

Grønne alarmer underretter dig om hændelser i Personal Firewall, f.eks. programmer, som automatisk har fået internetadgang.

Program tilladt adgang til internettet - Denne alarm vises, når Personal Firewall automatisk giver alle nye programmer internetadgang og derefter underretter dig (**Tillidssikkerhed**). Et eksempel på et ændret program er et program, hvis regler er blevet ændret, så det automatisk får internetadgang.

Alarmen Program tilladt adgang til internettet

Hvis du har valgt **Tillidssikkerhed** under sikkerhedsindstillingerne, giver Personal Firewall automatisk internetadgang til alle nye programmer, hvorefter den underretter dig med en alarm (Figur 2-9).

Figur 2-9. Program tilladt adgang til internettet

Du kan få vist en kort beskrivelse af hændelsen og derefter vælge mellem følgende:

- Klik på **Vis programlogfilen** for at få nærmere oplysninger om hændelsen fra internetprogramlogfilen (se yderligere oplysninger under *Om siden Internetprogrammer* på side 20).
- Klik på **Deaktiver denne alarmtype** for at undgå visning af disse alarmtyper.

- Klik på **Fortsætte mit arbejde**, hvis du ikke ønsker at gøre noget ud over det, Personal Firewall allerede har gjort.
- Klik på **Bloker al adgang** for at forbyde internetadgang.

Alarmen Program er blevet ændret

Hvis du har valgt **Tillidssikkerhed** under sikkerhedsindstillingerne, giver Personal Firewall automatisk internetadgang til alle ændrede programmer. Du kan få vist en kort beskrivelse af hændelsen og derefter vælge mellem følgende:

- Klik på **Vis programlogfilen** for at få nærmere oplysninger om hændelsen fra internetprogramlogfilen (se yderligere oplysninger under *Om siden Internetprogrammer* på side 20).
- Klik på **Deaktiver denne alarmtype** for at undgå visning af disse alarmtyper.
- Klik på **Fortsæt mit arbejde**, hvis du ikke ønsker at gøre noget ud over det, Personal Firewall allerede har gjort.
- Klik på **Bloker al adgang** for at forbyde internetadgang.

Blå alarmer

Blå alarmer indeholder oplysninger, men kræver ikke, at du reagerer.

- **Forbindelsesforsøg blokeret -** Denne alarm vises, hvis Personal Firewall blokerer uønsket internet- eller netværkstrafik. (Tillidssikkerhed, Standard eller Høj sikkerhed)

Alarmen Forbindelsesforsøg blokeret

Hvis du har markeret sikkerhedsindstillingen **Tillidssikkerhed**, **Standard** eller **Høj**, viser Personal Firewall en alarm (Figur 2-10), når den blokerer uønsket internet- eller netværkstrafik.

Figur 2-10. Alarmen Forbindelsesforsøg blokeret

Du kan få vist en kort beskrivelse af hændelsen og derefter vælge mellem følgende:

- Klik på **Vis hændelseslogfilen** for at få nærmere oplysninger om hændelsen fra logfilen over indgående hændelser i Personal Firewall (se yderligere oplysninger under *Om siden Indgående hændelser* på side 22).
- Klik på **Spore denne adresse** for at udføre en visuel sporing af IP-adresserne vedrørende denne hændelse.
- Klik på **Forbyd denne adresse** for at nægte adressen adgang til computeren. Adressen tilføjes til listen over forbudte IP-adresser.
- Klik på **Hav tillid til denne adresse** for at give IP-adressen adgang til computeren.
- Klik på **Fortsætte mit arbejde**, hvis du ikke ønsker at gøre noget ud over det, Personal Firewall allerede har gjort.

Stikordsregister

P

R

S

T

V

W