McAfee®

VirusScan® Plus 2007

AntiVirus, Firewall & AntiSpyware

Manual do Utilizador

Índice

CAPÍTULO 1

Introdução

O McAfee VirusScan Plus Suite protege o computador e os ficheiros contra vírus, spyware e hackers. Pode navegar na Web e transferir ficheiros em segurança e com confiança, sabendo que a McAfee está sempre presente, sempre a actualizar e sempre a protegê-lo. A protecção de confiança da McAfee bloqueia ameaças e detém os hackers automaticamente, mantendo o computador estável e seguro. A McAfee também facilita as tarefas de visualizar o estado de segurança, analisar vírus e spyware e assegurar que os produtos estão actualizados, utilizando o renovado McAfee SecurityCenter. Além disso, receberá automaticamente o mais recente software e actualizações da McAfee com a sua subscrição.

O VirusScan Plus inclui os seguintes programas:

- SecurityCenter
- VirusScan
- Personal Firewall
- Network Manager
- EasyNetwork (licença apenas para 3 utilizadores)
- SiteAdvisor

CAPÍTULO 2

McAfee SecurityCenter

O McAfee SecurityCenter é um ambiente fácil de utilizar onde os utilizadores da McAfee podem criar, gerir e configurar as respectivas subscrições de segurança.

O SecurityCenter funciona também como uma fonte de informação de alertas contra vírus, informações sobre produtos, suporte, informações de subscrição e acesso de um clique a ferramentas e notícias incluídas no Web site da McAfee.

Neste capítulo

Funcionalidades

O McAfee SecurityCenter oferece as seguintes funcionalidades e benefícios novos:

Estado de protecção optimizado

Analisa facilmente o estado de segurança do computador, procura actualizações e corrige potenciais problemas de segurança.

Actualizações contínuas

Instala actualizações diárias automaticamente. Quando existe uma nova versão do software da McAfee disponível, esta pode ser obtida automaticamente e de forma gratuita durante a subscrição, garantindo sempre uma protecção actualizada.

Alerta em tempo real

Os alertas de segurança informam-no de surtos de vírus e ameaças de segurança, fornecendo opções de resposta para remover, neutralizar ou obter mais informações sobre a ameaça.

Protecção adequada

Existe uma grande variedade de opções de renovação que ajudam a manter a protecção da McAfee actualizada.

Ferramentas de desempenho

Removem ficheiros não utilizados, desfragmentam ficheiros utilizados e utilizam processos de restauro do sistema que maximizam o desempenho do computador.

Ajuda real online

Pode obter suporte de peritos na segurança do seu computador da McAfee através de chat, correio electrónico ou telefone.

Protecção de navegação segura

Se instalada, a extensão do browser McAfee SiteAdvisor protege-o contra spyware, correio publicitário não solicitado, vírus e fraudes online, classificando os Web sites que visita ou que aparecem nos resultados de procura na Web. Pode ver classificações de segurança detalhadas que reflectem os testes efectuados aos sites em termos de práticas de correio electrónico, transferências, filiações online e perturbações, tais como janelas de contexto e cookies de registo de terceiros.

CAPÍTULO 3

Utilizar o SecurityCenter

Pode executar o SecurityCenter a partir do ícone McAfee SecurityCenter na área de notificação do Windows na parte mais à direita da barra de tarefas ou no ambiente de trabalho do Windows.

Ao abrir o SecurityCenter, o painel Página Inicial apresenta o estado de segurança do computador e permite um acesso rápido a actualizações e pesquisas (se o McAfee VirusScan estiver instalado), bem como a outras tarefas comuns:

Cabeçalho

Ajuda

Veja o ficheiro de ajuda dos programas.

Coluna da esquerda

Actualizar

Actualize o seu produto para garantir protecção contra as mais recentes ameaças.

Analisar

Se o McAfee VirusScan estiver instalado, pode efectuar uma pesquisa manual do computador.

Tarefas comuns

Efectue tarefas comuns, que incluem voltar ao painel Página Inicial, ver eventos recentes, gerir a rede do computador (se trabalhar num computador com capacidade de gestão para este tipo de rede) e efectuar a manutenção do computador. Se o McAfee Data Backup estiver instalado, pode também criar uma cópia de segurança dos dados.

Componentes instalados

Veja quais são os serviços de segurança que estão a proteger a segurança do seu computador.

Painel principal

Estado de protecção

Em **Estou protegido?**, veja o nível geral do estado de protecção do seu computador. Abaixo desta opção, veja uma perturbação de estado por categoria e tipo de protecção.

Informações sobre o SecurityCenter

Pode ver quando ocorreu a última actualização do computador, a última pesquisa (caso o McAfee VirusScan esteja instalado), assim como a data de expiração da subscrição.

Neste capítulo

Noções sobre os ícones do SecurityCenter

Os ícones do SecurityCenter são apresentados na área de notificação do Windows, na parte mais à direita da barra de tarefas. Utilize os ícones para ver se o computador está totalmente protegido, ver o estado de uma pesquisa em curso (caso o McAfee VirusScan esteja instalado), verificar se existem actualizações, ver eventos recentes, efectuar a manutenção do computador e obter suporte do Web site da McAfee.

Abrir o SecurityCenter e utilizar funções adicionais

Quando o SecurityCenter estiver a funcionar, é apresentado o ícone M do SecurityCenter na área de notificação do Windows, na parte mais à direita da barra de tarefas.

Para abrir o SecurityCenter ou utilizar funções adicionais:

- Clique com o botão direito do rato no ícone do SecurityCenter e clique numa das seguintes opções:
  - Abrir o SecurityCenter
  - Actualizações
  - Ligações rápidas

    O submenu contém ligações a Página Inicial, Ver Eventos Recentes, Gerir Rede, Manter Computador e Cópia de Segurança de Dados (caso esteja instalada).
  - Verificar Subscrição

    (Esta opção é apresentada quando expira, pelo menos, uma subscrição de produtos.)
  - Centro de Actualizações
  - Suporte ao Cliente

Verificar o estado de protecção

Se o computador não estiver totalmente protegido, é apresentado o ícone de estado de protecção na área de notificação do Windows na parte mais à direita da barra de tarefas. O ícone pode aparecer a vermelho ou a amarelo, conforme o estado de protecção.

Para verificar o estado de protecção:

- Clique no ícone de estado de protecção para abrir o SecurityCenter e corrigir quaisquer problemas.

Verificar o estado das actualizações

Se estiver a verificar actualizações, é apresentado o ícone de actualizações na área de notificação do Windows, na parte mais à direita da barra de tarefas.

Para verificar o estado das actualizações:

- Clique no ícone de actualizações para ver o estado das actualizações numa sugestão.

Noções sobre o estado de protecção

O estado de protecção de segurança geral do computador é indicado em **Estou protegido?** no SecurityCenter.

O estado de protecção informa-o se o computador está totalmente protegido contra as mais recentes ameaças de segurança ou se os problemas requerem atenção e mostra-lhe como resolver esses problemas. Se um problema afectar mais de uma categoria de protecção, a resolução desse problema pode resultar na reposição de várias categorias para o estado de protecção total.

Alguns dos factores que influenciam o estado de protecção incluem ameaças de segurança externas, produtos de segurança instalados no computador, produtos que acedem à Internet e o tipo de configuração destes produtos de segurança e Internet.

Por predefinição, se as opções Protecção contra Correio Publicitário Não Solicitado ou Bloqueio de Conteúdos não estiverem instaladas, estes problemas de protecção não críticos serão automaticamente ignorados, não sendo registados no estado de protecção geral. No entanto, se for apresentada uma ligação **Ignorar** junto a um problema de protecção, pode ignorar o problema, caso tenha a certeza de que não quer resolvê-lo.

Estou protegido?

Verifique o nível geral do estado de protecção do computador em **Estou protegido?** no SecurityCenter:

- É apresentado **Sim** se o computador estiver totalmente protegido (verde).
- É apresentado **Não** se o computador estiver parcialmente protegido (amarelo) ou não protegido (vermelho).

Para resolver a maioria dos problemas de protecção automaticamente, clique em **Corrigir** junto do estado de protecção. No entanto, se continuarem a aparecer um ou mais problemas que exijam a sua resposta, clique na ligação junto do problema para realizar a acção sugerida.

Noções sobre tipos e categorias de protecção

Em **Estou protegido?** no SecurityCenter, pode ver uma perturbação de estado que inclui estes tipos e categorias de protecção:

- Computador e ficheiros
- Internet e rede
- Correio electrónico e mensagens instantâneas
- Limitações de acesso

Os tipos de protecção apresentados no SecurityCenter dependem dos produtos instalados. Por exemplo, é apresentado o tipo de protecção Monitorização do Estado do Sistema se o software Cópia de Segurança de Dados McAfee estiver instalado.

Se uma categoria não tiver quaisquer problemas de protecção, o estado é Verde. Se clicar numa categoria Verde, é apresentada no lado direito uma lista dos tipos de protecção activados, assim como uma lista dos problemas já ignorados. Se não houver nenhum problema, é apresentado um aviso de vírus em vez de quaisquer problemas. Pode também clicar em **Configurar** para alterar as opções dessa categoria.

Se todos os tipos de protecção de uma categoria tiverem o estado Verde, o estado dessa categoria é Verde. Do mesmo modo, se todas as categorias de protecção tiverem o estado Verde, o estado de protecção geral é Verde.

Se alguma das categorias de protecção tiver o estado Amarelo ou Vermelho, pode resolver os problemas de protecção corrigindo-os ou ignorando-os, mudando o estado para Verde.

Noções sobre protecção de computadores e ficheiros

A categoria de protecção Computador e Ficheiros inclui os seguintes tipos de protecção:

- **Protecção Antivírus** -- A protecção de pesquisa em tempo real protege o computador de vírus, worms, cavalos de Tróia, scripts suspeitos, ataques híbridos e outras ameaças. Efectua uma pesquisa automática e tenta limpar os ficheiros (incluindo ficheiros comprimidos .exe, sector de arranque, memória e ficheiros críticos) quando são utilizados pelo utilizador ou pelo computador.
- **Protecção Anti-Spyware** -- A protecção anti-spyware detecta, bloqueia e remove spyware, adware e outros programas potencialmente indesejados que possam recolher e transmitir dados privados sem a sua autorização.
- **Protecções do Sistema** -- As Protecções do Sistema detectam alterações no computador e avisam-no quando ocorrem. Pode, em seguida, analisar estas alterações e decidir se pretende autorizá-las.
- **Protecção do Windows** -- A protecção do Windows mostra o estado do Windows Update no computador. Se o McAfee VirusScan estiver instalado, a protecção contra sobrecargas da memória intermédia está também disponível.

Um dos factores que influenciam a protecção Computador e Ficheiros são as ameaças de vírus externos. Por exemplo, se ocorrer um surto de vírus, será que o software antivírus instalado pode protegê-lo? Além disso, outros factores incluem a configuração do software antivírus e se o software está a ser constantemente actualizado com os mais recentes ficheiros de assinatura de detecção que protegem o computador das mais recentes ameaças.

Abra o painel de configuração Computador e Ficheiros

Se não existirem problemas em **Computador e & Ficheiros**, pode abrir o painel de configuração no painel de informações.

Para abrir o painel de configuração Computador e Ficheiros:

1. No painel Página Inicial, clique em **Computador e & Ficheiros**.
2. No painel da direita, clique em **Configurar**.

Noções sobre protecção da Internet e da rede

A categoria de protecção Internet e Rede inclui os seguintes tipos de protecção:

- **Protecção por Firewall** -- A protecção por firewall protege o computador de intrusões e tráfego de rede indesejado. Ajuda-o a gerir as ligações de entrada e saída da Internet.
- **Wireless Protection** -- A protecção sem fios protege a rede doméstica sem fios de intrusões e intercepção de dados. Contudo, se tiver uma ligação a uma rede sem fios externa, a protecção varia consoante o nível de segurança dessa rede.
- **Protecção da Navegação na Web** -- A protecção de navegação na Web oculta anúncios, janelas de contexto e bugs da Web no computador quando se navega na Internet.
- **Protecção contra Phishing** -- A protecção contra Phishing permite bloquear Web sites fraudulentos que solicitam informações pessoais através de hiperligações em mensagens instantâneas e de correio electrónico, janelas de contexto e outros meios.
- **Protecção de Informações Pessoais** -- A protecção de informações pessoais impede a divulgação de informações sensíveis e confidenciais na Internet.

Abra o painel de configuração Internet e Rede

Se não existirem problemas em **Internet e & Rede**, pode abrir o painel de configuração no painel de informações.

Para abrir o painel de configuração Internet e Rede:

1. No painel Página Inicial, clique em **Internet e & Rede**.
2. No painel da direita, clique em **Configurar**.

Noções sobre protecção de correio electrónico e mensagens instantâneas

A categoria de protecção Correio Electrónico e Mensagens Instantâneas inclui os seguintes tipos de protecção:

- **Protecção do Correio Electrónico** -- A protecção do correio electrónico efectua pesquisas automáticas e tenta limpar vírus, spyware e ameaças potenciais em mensagens de correio electrónico e anexos enviados e recebidos.
- **Protecção contra Correio Publicitário Não Solicitado** -- A protecção contra correio publicitário não solicitado ajuda a impedir a entrada de mensagens de correio electrónico na caixa de correio.
- **Protecção do IM** -- A protecção de mensagens instantâneas (IM) efectua pesquisas automáticas e tenta limpar vírus, spyware e potenciais ameaças nos anexos de mensagens instantâneas recebidas. Além disso, impede que clientes de mensagens instantâneas troquem conteúdo ou informações pessoais indesejadas através da Internet.
- **Protecção de Navegação Segura** -- Se estiver instalado, o plug-in do browser McAfee SiteAdvisor ajuda a protegê-lo de spyware, correio electrónico não solicitado, vírus e fraudes online, classificando os Web sites visitados ou que são apresentados nos resultados de procura da Web. Pode ver classificações de segurança pormenorizadas que indicam o resultado do teste de um site no que respeita a práticas de correio electrónico, transferências, afiliações online e aspectos incómodos, como janelas de contexto e cookies de registo de terceiros.

Abra o painel de configuração Correio Electrónico e Mensagens Instantâneas

Se não existirem problemas em **Correio Electrónico e& Mensagens Instantâneas**, pode abrir o painel de configuração no painel de informações.

Para abrir o painel de configuração Correio Electrónico e Mensagens Instantâneas:

1. No painel Página Inicial, clique em **Correio Electrónico e& Mensagens Instantâneas**.
2. No painel da direita, clique em **Configurar**.

Noções sobre a protecção de limitação de acesso

A categoria de protecção Limitação de Acesso inclui o seguinte tipo de protecção:

- **Limitações de acesso** -- As limitações de acesso impedem que os utilizadores vejam conteúdo indesejado da Internet, bloqueando o acesso a Web sites potencialmente nocivos. É possível monitorizar e limitar a actividade e utilização da Internet.

Abra o painel de configuração Limitações de Acesso

Se não existirem problemas em **Limitações de Acesso**, pode abrir o painel de configuração no painel de informações.

Para abrir o painel de configuração Limitações de Acesso:

1. No painel Página Inicial, clique em **Limitações de Acesso**.
2. No painel da direita, clique em **Configurar**.

Resolução de problemas relacionados com protecção

A maioria dos problemas de protecção pode ser resolvida automaticamente. No entanto, se persistirem um ou mais problemas, deve resolvê-los manualmente.

Resolução automática de problemas de protecção

A maioria dos problemas de protecção pode ser resolvida automaticamente.

Para uma resolução automática de problemas de protecção:

- Clique em **Corrigir** junto ao estado de protecção.

Resolução manual de problemas de protecção

Se um ou mais problemas de protecção não forem resolvidos automaticamente, clique na ligação junto do problema para realizar a acção sugerida.

Para uma resolução manual de problemas de protecção:

- Efectue uma das seguintes acções:
  - Se não tiver efectuado uma pesquisa total do computador nos últimos 30 dias, clique em **Analisar** no lado esquerdo do estado de protecção principal para realizar uma pesquisa manual. (Esta opção é apresentada se o McAfee VirusScan estiver instalado.)
  - Se os ficheiros de assinatura de detecção (DAT) estiverem desactualizados, clique em **Actualizar** no lado esquerdo do estado de protecção geral para actualizar a protecção.
  - Se um programa não estiver instalado, clique em **Obter protecção total** para instalá-lo.
  - Se faltarem componentes no programa, reinstale-o.
  - Se for necessário registar um programa para receber protecção total, clique em **Registar agora** para o registar. (Esta opção é apresentada se um ou mais programas tiverem expirado.)
  - Se um programa tiver expirado, clique em **Verificar a minha subscrição agora** para ver o estado da conta. (Esta opção é apresentada se um ou mais programas tiverem expirado.)

Ver informações sobre o SecurityCenter

A opção Informações sobre o SecurityCenter, localizada na parte inferior do painel do estado de protecção, permite acesso a opções do SecurityCenter e mostra as mais recentes informações sobre actualizações, pesquisas (caso o McAfee VirusScan esteja instalado) e data de expiração da subscrição dos produtos McAfee.

Abra o painel de configuração SecurityCenter

Para sua comodidade, pode abrir o painel de configuração SecurityCenter para alterar as opções no painel Página Inicial.

Para abrir o painel de configuração SecurityCenter:

- No painel Página Inicial em **Informações sobre o SecurityCenter**, clique em **Configurar**.

Ver informações sobre os produtos instalados

Pode ver uma lista dos produtos instalados, onde é indicado o número da versão do produto e a data da última actualização.

Para ver as informações sobre o produto McAfee:

- No painel Página Inicial em **Informações sobre o SecurityCenter**, clique em **Ver Detalhes** para abrir a janela de informações sobre o produto.

Utilizar o Menu Avançado

Quando abre o SecurityCenter pela primeira vez, é apresentado o Menu Básico na coluna da esquerda. Se for um utilizador avançado, pode clicar em **Menu Avançado** para abrir um menu de comandos mais pormenorizado. Para sua comodidade, é apresentado o último menu que utilizou quando abrir novamente o SecurityCenter.

O Menu Avançado inclui as seguintes opções:

- Página inicial
- Relatórios e Registos (inclui a lista Eventos Recentes e registos por tipo relativos aos últimos 30, 60 e 90 dias)
- Configurar
- Restaurar
- Ferramentas

CAPÍTULO 4

Configurar as opções do SecurityCenter

O SecurityCenter mostra o estado geral de protecção do computador, permite-lhe criar contas de utilizador McAfee, instala automaticamente as mais recentes actualizações de produtos e notifica automaticamente o utilizador através de alertas e avisos sonoros de surtos de vírus públicos, ameaças de segurança e actualizações de produto.

No painel Configuração do SecurityCenter, pode alterar as opções do SecurityCenter para estas funções:

- Estado de protecção
- Utilizadores
- Actualizações automáticas
- Alertas

Neste capítulo

Configurar o estado de protecção

O estado de protecção de segurança geral do computador é indicado em **Estou protegido?** no SecurityCenter.

O estado de protecção informa-o se o computador está totalmente protegido contra as mais recentes ameaças de segurança ou se os problemas requerem atenção e mostra-lhe como resolver esses problemas.

Por predefinição, se as opções Protecção contra Correio Publicitário Não Solicitado ou Bloqueio de Conteúdos não estiverem instaladas, estes problemas de protecção não críticos serão automaticamente ignorados, não sendo registados no estado de protecção geral. No entanto, se for apresentada uma ligação **Ignorar** junto a um problema de protecção, pode ignorar o problema, caso tenha a certeza de que não quer resolvê-lo. Se decidir corrigir mais tarde um problema ignorado anteriormente, pode incluí-lo no estado de protecção para registo.

Configurar problemas ignorados

Pode incluir ou excluir o registo de problemas como parte do estado de protecção geral do computador. Se for apresentada uma ligação **Ignorar** junto a um problema de protecção, pode ignorar o problema, caso tenha a certeza de que não quer resolvê-lo. Se decidir corrigir mais tarde um problema ignorado anteriormente, pode incluí-lo no estado de protecção para registo.

Para configurar problemas ignorados:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Estado da Protecção** para aumentar o respectivo painel e depois clique em **Avançadas**.
3. Seleccione uma das seguintes opções no painel Problemas Ignorados:
   - Para incluir problemas ignorados anteriormente no estado da protecção, desmarque as respectivas caixas de verificação.
   - Para excluir problemas do estado da protecção, seleccione as respectivas caixas de verificação.
4. Clique em **OK**.

Configurar opções de utilizador

Se utilizar programas McAfee que requerem autorizações de utilizador, estas autorizações correspondem, por predefinição, às contas de utilizador do Windows no computador. Para facilitar a gestão destes programas pelos utilizadores, pode optar por utilizar as contas de utilizador McAfee em qualquer altura.

Se optar por utilizar contas de utilizador McAfee, quaisquer nomes de utilizador e autorizações existentes do programa Limitações de Acesso serão importados automaticamente. No entanto, quando mudar pela primeira vez, deve criar uma conta de administrador. Em seguida, pode criar e configurar outras contas de utilizador McAfee.

Mudar para contas de utilizador McAfee

Por predefinição, está a utilizar contas de utilizador do Windows. No entanto, se mudar para contas de utilizador da McAfee, já não é necessário criar contas adicionais do Windows.

Para mudar para contas de utilizador McAfee:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Utilizadores** para aumentar o respectivo painel e depois clique em **Avançadas**.
3. Para utilizar contas de utilizador McAfee, clique em **Mudar**.

Se mudar para contas de utilizador McAfee pela primeira vez, deve criar uma conta de administrador (página 23).

Criar uma conta de administrador

Quando muda pela primeira vez para utilizar utilizadores McAfee, é-lhe solicitado que crie uma conta de administrador.

Para criar uma conta de administrador:

1. Introduza uma palavra-passe na caixa **Palavra-passe** e introduza-a novamente na caixa **Confirmar Palavra-passe**.
2. Seleccione uma pergunta de recuperação de palavra-passe na lista e introduza a resposta à pergunta secreta na caixa **Resposta**.
3. Clique em **Aplicar**.

   Quando terminar, o tipo de conta de utilizador é actualizado no painel com os nomes de utilizador e autorizações existentes no programa Limitações de Acesso, caso existam. Quando configurar as contas de utilizador pela primeira vez, é apresentado o painel Gerir Utilizador.

Configurar opções de utilizador

Se optar por utilizar contas de utilizador McAfee, quaisquer nomes de utilizador e autorizações existentes do programa Limitações de Acesso são importados automaticamente. No entanto, quando mudar pela primeira vez, deve criar uma conta de administrador. Em seguida, pode criar e configurar outras contas de utilizador McAfee.

Para configurar opções de utilizador:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Utilizadores** para expandir o respectivo painel e, em seguida, clique em **Avançadas**.
3. Em **Contas de Utilizador**, clique em **Adicionar**.
4. Introduza um nome de utilizador na caixa **Nome de Utilizador**.
5. Introduza uma palavra-passe na caixa **Palavra-passe** e introduza-a novamente na caixa **Confirmar Palavra-passe**.
6. Seleccione a caixa de verificação **Utilizador de Arranque** se quiser que este novo utilizador inicie sessão automaticamente quando o SecurityCenter for iniciado.
7. Em **Tipo de Conta do Utilizador**, seleccione um tipo de conta para este utilizador e, em seguida, clique em **Criar**.

   Nota: Depois de criar a conta de utilizador, deve configurar as definições para um Utilizador Limitado em Limitações de Acesso.

8. Para editar a palavra-passe de um utilizador, início de sessão automático ou tipo de conta, seleccione um nome de utilizador na lista e clique em **Editar**.
9. Quando terminar, clique em **Aplicar**.

Obter a palavra-passe de administrador

Quando se esquecer da palavra-passe de administrador, pode obtê-la.

Para obter a palavra-passe de administrador:

1. Clique com o botão direito do rato no ícone M do SecurityCenter e depois clique em **Mudar de Utilizador**.
2. Na lista **Nome de Utilizador**, seleccione **Administrador** e clique em **Palavra-passe Esquecida**.
3. Introduza a resposta da pergunta secreta que seleccionou ao criar a conta de administrador.
4. Clique em **Submeter**.

   É apresentada a sua palavra-passe de administrador.

Alterar a palavra-passe de administrador

Se não se lembrar da palavra-passe de administrador ou se suspeitar que pode não ser seguro utilizá-la, pode alterá-la.

Para alterar a palavra-passe de administrador:

1. Clique com o botão direito do rato no ícone M do SecurityCenter e depois clique em **Mudar de Utilizador**.
2. Na lista **Nome de Utilizador**, seleccione **Administrador** e clique em **Alterar Palavra-passe**.
3. Introduza a palavra-passe existente na caixa **Palavra-passe Antiga**.
4. Introduza a nova palavra-passe na caixa **Palavra-passe** e introduza-a novamente na caixa **Confirmar Palavra-passe**.
5. Clique em **OK**.

Configurar opções de actualização

O SecurityCenter verifica automaticamente actualizações para todos os serviços McAfee de quatro em quatro horas quando se está ligado à Internet e depois instala automaticamente as mais recentes actualizações de produtos. No entanto, pode verificar manualmente em qualquer altura se existem actualizações, carregando no ícone do SecurityCenter na área de notificação, localizada na parte mais à direita da barra de tarefas.

Verificar actualizações automaticamente

O SecurityCenter verifica automaticamente se existem actualizações de quatro em quatro horas quando existe uma ligação à Internet. Contudo, pode configurar o SecurityCenter para notificá-lo antes de transferir ou instalar actualizações.

Para verificar actualizações automaticamente:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto do estado **As actualizações automáticas estão activadas** para expandir o respectivo painel e, em seguida, clique em **Avançadas**.
3. Seleccione uma das seguintes opções no painel Opções de Actualização:
   - Instalar as actualizações automaticamente e notificar quando o produto for actualizado (recomendado) (página 27)
   - Transferir as actualizações automaticamente e notificar quando estiverem prontas para serem instaladas (página 28)
   - Notificar antes de transferir quaisquer actualizações (página 28)
4. Clique em **OK**.

Nota: Para uma máxima protecção, a McAfee recomenda que permita ao SecurityCenter procurar e instalar automaticamente as actualizações. No entanto, se pretende actualizar apenas manualmente os serviços de segurança, pode desactivar a actualização automática (página 29).

Transferir e instalar actualizações automaticamente

Se seleccionar **Instalar as actualizações automaticamente e notificar quando o produto for actualizado (recomendado)** nas Opções de Actualização do SecurityCenter, este transfere e instala automaticamente as actualizações.

Transferência automática de actualizações

Se seleccionar **Transferir as actualizações automaticamente e notificar quando estiverem prontas para serem instaladas** nas Opções de Actualização, o SecurityCenter transfere actualizações automaticamente e depois notifica-o quando estão prontas a instalar. Em seguida, pode instalar a actualização ou adiá-la (página 29).

Para instalar uma actualização transferida automaticamente:

1. Clique em **Actualizar os meus produtos agora** no alerta e depois clique em **OK**.

   Se solicitado, deve iniciar sessão no Web site para verificar a subscrição antes de efectuar a transferência.

2. Depois de verificar a subscrição, clique em **Actualizar** no painel Actualizações para transferir e instalar a actualização. Se a subscrição tiver expirado, clique em **Renovar a minha subscrição** no alerta e siga as indicações.

Nota: Nalguns casos, ser-lhe-á solicitado para reiniciar o computador de modo a concluir a actualização. Guarde o trabalho que estiver a fazer e feche todos os programas antes de reiniciar o computador.

Notificar antes de transferir actualizações

Se seleccionar **Notificar antes de transferir quaisquer actualizações** no painel Opções de Actualização, o SecurityCenter notifica-o antes de transferir quaisquer actualizações. Em seguida, pode transferir e instalar uma actualização para que os serviços de segurança possam eliminar a ameaça de ataque.

Para transferir e instalar uma actualização:

1. Seleccione **Actualizar os meus produtos agora** no alerta e depois clique em **OK**.
2. Se solicitado, inicie sessão no Web site.

   A actualização é transferida automaticamente.
3. Clique em **OK** no alerta quando a instalação da actualização estiver concluída.

Nota: Nalguns casos, ser-lhe-á solicitado para reiniciar o computador de modo a concluir a actualização. Guarde o trabalho que estiver a fazer e feche todos os programas antes de reiniciar o computador.

Desactivar a actualização automática

Para uma máxima protecção, a McAfee recomenda que permita o SecurityCenter procurar e instalar automaticamente as actualizações. No entanto, se pretende actualizar apenas manualmente os serviços de segurança, pode desactivar a actualização automática.

Nota: Deve verificar manualmente as actualizações (página 30) pelo menos uma vez por semana. Se não verificar as actualizações, isso significa que o computador não está protegido com as mais recentes actualizações de segurança.

Para desactivar a actualização automática:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto do estado **As actualizações automáticas estão activadas** para aumentar o painel.
3. Clique em **Desligado**.
4. Clique em **Sim** para confirmar a alteração.

   O estado é actualizado no cabeçalho.

Se não verificar manualmente as actualizações durante sete dias, é apresentado um alerta a indicar-lhe para verificá-las.

Adiar actualizações

Se estiver demasiado ocupado para actualizar os serviços de segurança quando aparecer o alerta, pode ser avisado mais tarde ou pode ignorar o alerta.

Para adiar uma actualização:

- Efectue uma das seguintes acções:
  - Seleccione **Lembrar-me mais tarde** no alerta e clique em **OK**.
  - Seleccione **Fechar este alerta** e clique em **OK** para fechar o alerta sem efectuar qualquer acção.

Verificar actualizações manualmente

O SecurityCenter verifica automaticamente actualizações de quatro em quatro horas quando se está ligado à Internet e depois instala as mais recentes actualizações de produtos. No entanto, pode verificar manualmente em qualquer altura se existem actualizações, utilizando o ícone do SecurityCenter na área de notificação do Windows na parte mais à direita da barra de tarefas.

Nota: Para uma máxima protecção, a McAfee recomenda que permita ao SecurityCenter procurar e instalar automaticamente as actualizações. No entanto, se pretende actualizar apenas manualmente os serviços de segurança, pode desactivar a actualização automática (página 29).

Para verificar actualizações manualmente:

1. Certifique-se de que o computador está ligado à Internet.
2. Clique com o botão direito do rato no ícone M do SecurityCenter na área de notificação do Windows, na parte mais à direita da barra de tarefas e, em seguida, clique em **Actualizações**.

   Embora o SecurityCenter verifique as actualizações, pode continuar a executar outras tarefas com a referida aplicação.

   Para sua comodidade, é apresentado um ícone animado na área de notificação do Windows, na parte mais à direita da barra de tarefas. Quando o SecurityCenter terminar, o ícone desaparece automaticamente.
3. Se solicitado, inicie sessão no Web site para verificar a subscrição.

Nota: Em alguns casos, ser-lhe-á solicitado que reinicie o computador de modo a concluir a actualização. Guarde o trabalho e feche todos os programas antes de reiniciar o computador.

Configurar opções de alerta

O SecurityCenter notifica-o automaticamente através de alertas e avisos sonoros para obter informações sobre surtos de vírus públicos, ameaças de segurança e actualizações de produtos. No entanto, pode configurar o SecurityCenter para apresentar apenas alertas que exijam a sua atenção imediata.

Configurar opções de alerta

O SecurityCenter notifica-o automaticamente através de alertas e avisos sonoros para obter informações sobre surtos de vírus públicos, ameaças de segurança e actualizações de produtos. No entanto, pode configurar o SecurityCenter para apresentar apenas alertas que exijam a sua atenção imediata.

Para configurar opções de alerta:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Alertas** para aumentar o respectivo painel e depois clique em **Avançadas**.
3. Seleccione uma das seguintes opções no painel Opções de Alerta:
   - **Alertar-me se ocorrer um surto de vírus público ou ameaças de segurança**
   - **Mostrar alertas informativos se for detectado um modo de jogo**
   - **Reproduzir um aviso sonoro se ocorrer um alerta**
   - **Mostrar o ecrã splash da McAfee no arranque do Windows**
4. Clique em **OK**.

Nota: Para desactivar futuros alertas informativos do respectivo alerta, seleccione a caixa de verificação **Não voltar a mostrar este alerta**. Pode activá-los de novo posteriormente no painel Alertas Informativos.

Configurar alertas informativos

Os alertas informativos notificam-no quando ocorrem eventos que não requerem a sua resposta imediata. Se desactivar futuros alertas informativos do próprio alerta, pode activá-los de novo posteriormente no painel Alertas Informativos.

Para configurar alertas informativos:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Alertas** para aumentar o respectivo painel e depois clique em **Avançadas**.
3. Em **Configuração do SecurityCenter**, clique em **Alertas Informativos**.
4. Desmarque a caixa de verificação **Ocultar alertas informativos** e depois desmarque as caixas de verificação dos alertas na lista que pretende mostrar.
5. Clique em **OK**.

CAPÍTULO 5

Efectuar tarefas comuns

Pode efectuar tarefas comuns, que incluem voltar ao painel Página inicial, ver eventos recentes, gerir a rede do computador (se estiver a trabalhar com um computador com capacidade de gestão para este tipo de rede) e efectuar a manutenção do computador. Se a opção Cópia de Segurança de Dados McAfee estiver instalada, pode também criar uma cópia de segurança dos dados.

Neste capítulo

Efectuar tarefas comuns

Pode efectuar tarefas comuns, que incluem voltar ao painel Página Inicial, ver eventos recentes, efectuar a manutenção do computador, gerir a rede do computador (se estiver ligada a um computador com capacidade de gestão para este tipo de rede) e criar cópias de segurança dos dados (se o software Cópia de Segurança de Dados McAfee estiver instalado).

Para efectuar tarefas comuns:

- Em **Tarefas Comuns** no Menu Básico, efectue uma das seguintes opções:
  - Para voltar ao painel Página Inicial, clique em **Página Inicial**.
  - Para ver eventos recentes detectados pelo software de segurança, clique em **Eventos Recentes**.
  - Para remover ficheiros não utilizados, desfragmente os dados e restaure o computador para as definições anteriores, clique em **Fazer Manutenção do Computador**.
  - Para efectuar a gestão da rede do computador, clique em **Gerir Rede** num computador com capacidade de gestão para esta rede.

    A opção Gestor de Rede monitoriza os computadores na rede no que respeita a falhas de segurança, para que possa facilmente identificar problemas de segurança na rede.

- Para criar cópias de segurança dos ficheiros, clique em **Cópia de Segurança de Dados** se o software Cópia de Segurança de Dados McAfee estiver instalado.

  A cópia de segurança automática guarda cópias dos ficheiros mais importantes num local à sua escolha, encriptando e armazenando os ficheiros num CD/DVD ou numa unidade USB, externa ou de rede.

Sugestão: Para sua comodidade, pode executar tarefas comuns a partir de dois locais adicionais (em **Página Inicial** no Menu Avançado e no menu **QuickLinks** do ícone M do SecurityCenter na parte mais à direita da barra de tarefas). Pode ver também eventos recentes e registos por tipo abrangentes em **Relatórios e Registos** no Menu Avançado.

Ver eventos recentes

Os eventos recentes são registados quando ocorrem alterações no computador. Isto verifica-se quando, por exemplo, um tipo de protecção é activado ou desactivado, quando uma ameaça é removida ou quando uma tentativa de ligação à Internet é bloqueada. Pode ver os 20 eventos mais recentes e os respectivos pormenores.

Consulte o ficheiro de ajuda do respectivo produto para obter informações detalhadas sobre os eventos.

Para ver eventos recentes:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e depois clique em **Ver Eventos Recentes**.

   São apresentados na lista quaisquer eventos recentes, mostrando a data e uma descrição resumida.

2. Em **Eventos Recentes**, seleccione um evento para ver as informações adicionais no painel Detalhes.

   Em **Pretendo**, são apresentadas as acções disponíveis.

3. Para ver uma lista mais abrangente de eventos, clique em **Ver Registo**.

Manutenção automática do computador

Para libertar espaço em disco importante e optimizar o desempenho do computador, pode agendar as tarefas QuickClean ou Desfragmentador de Disco para intervalos regulares. Estas tarefas incluem eliminar, apagar e desfragmentar ficheiros e pastas.

Para efectuar uma manutenção automática do computador:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e depois clique em **Fazer Manutenção do Computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.
3. Na lista de operações, seleccione **QuickClean** ou **Desfragmentador de Disco**.
4. Efectue uma das seguintes acções:
   - Para modificar uma tarefa existente, seleccione-a e depois clique em **Modificar**. Siga as instruções indicadas no ecrã.
   - Para criar uma nova tarefa, introduza o nome na caixa **Nome da Tarefa** e depois clique em **Criar**. Siga as instruções indicadas no ecrã.
   - Para eliminar uma tarefa, seleccione-a e depois clique em **Eliminar**.
5. Em **Resumo de Tarefas**, veja a data em que a tarefa foi executada pela última vez, a data da próxima execução e o respectivo estado.

Manutenção manual do computador

Pode efectuar tarefas de manutenção manual para remover ficheiros não utilizados, desfragmentar dados ou repor o computador para as definições anteriores.

Para efectuar uma manutenção manual do computador:

- Efectue uma das seguintes acções:
  - Para utilizar a opção QuickClean, clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks**, clique em **Fazer Manutenção do Computador** e depois clique em **Iniciar**.
  - Para utilizar a opção Desfragmentador de Disco, clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks**, clique em **Fazer Manutenção do Computador** e depois clique em **Analisar**.
  - Para utilizar a opção Restauro do Sistema, no Menu Avançado clique em **Ferramentas**, clique em **Restauro do Sistema** e depois clique em **Iniciar**.

Remover ficheiros e pastas não utilizados

Utilize a opção QuickClean para disponibilizar espaço em disco importante e optimizar o desempenho do computador.

Para remover ficheiros e pastas não utilizados:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e, em seguida, clique em **Fazer Manutenção do Computador**.
2. Em **QuickClean**, clique em **Iniciar**.
3. Siga as instruções indicadas no ecrã.

Desfragmentar ficheiros e pastas

A fragmentação de ficheiros ocorre quando os ficheiros e pastas são eliminados e são adicionados novos ficheiros. Esta fragmentação reduz o acesso ao disco e resulta numa deterioração geral do desempenho do computador, embora não seja normalmente grave.

Utilize a desfragmentação para gravar novamente partes de um ficheiro em sectores contíguos num disco rígido, de modo a aumentar a velocidade de acesso e obtenção.

Para desfragmentar ficheiros e pastas:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e depois clique em **Fazer Manutenção do Computador**.
2. Em **Desfragmentador de Disco**, clique em **Analisar**.
3. Siga as instruções indicadas no ecrã.

Restaurar o computador para as definições anteriores

Os pontos de restauro são instantâneos do computador guardados periodicamente pelo Windows e quando ocorrem eventos significativos (por exemplo, durante a instalação de um programa ou controlador). No entanto, pode criar e atribuir um nome aos seus pontos de restauro em qualquer altura.

Utilize os pontos de restauro para resolver alterações nocivas no computador e voltar às definições anteriores.

Para restaurar o computador para as definições anteriores:

1. No Menu Avançado, clique em **Ferramentas** e depois clique em **Restauro do Sistema**.
2. Em **Restauro do Sistema**, clique em **Iniciar**.
3. Siga as instruções indicadas no ecrã.

Gerir a sua rede

Se o computador dispuser de capacidade de gestão de rede, pode utilizar o Gestor de Rede para monitorizar computadores na rede no que respeita a falhas de segurança, para que possa identificar facilmente problemas de segurança.

Se o estado de protecção do computador não estiver a ser monitorizado nesta rede, isso significa que o computador não faz parte desta rede ou não está a ser gerido nesta rede. Para obter informações detalhadas, consulte o ficheiro de ajuda do Gestor de Rede.

Para gerir a sua rede:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e depois clique em **Gerir Rede**.
2. Clique no ícone que representa este computador no mapa de rede.
3. Em **Pretendo**, clique em **Monitorizar este computador**.

Obter mais informações sobre vírus

Utilize a Virus Information Library e o Virus Map para:

- Obter mais informações sobre os mais recentes vírus, logros de vírus por correio electrónico e outras ameaças.
- Obter ferramentas gratuitas de remoção de vírus para ajudar a reparar o computador.
- Obter uma visão de conjunto, em tempo real, do local onde os computadores mais recentes estão a infectar computadores a nível mundial.

Para obter mais informações sobre vírus:

1. No Menu Avançado, clique em **Ferramentas** e depois em **Informações sobre Vírus**.
2. Efectue uma das seguintes acções:
   - Efectue uma procura de vírus com o Virus Information Library gratuito da MacAfee.
   - Efectue uma procura de vírus com o World Virus Map no Web site da McAfee.

CAPÍTULO 6

McAfee QuickClean

Quando se navega na Internet, acumula-se rapidamente muito lixo no computador. Proteja a sua privacidade e elimine o correio electrónico indesejado, bem como os ficheiros da Internet de que já não precisa através do QuickClean. O QuickClean identifica e elimina os ficheiros que se acumulam enquanto utiliza a Internet, incluindo cookies, correio electrónico, conteúdos transferidos, ficheiros de histórico (dados que contêm informações pessoais). Protege a sua privacidade, proporcionando uma eliminação segura desta informação confidencial.

O QuickClean elimina também programas indesejados. Poderá especificar os ficheiros que pretende eliminar e destruir os ficheiros indesejados sem eliminar informações essenciais.

Neste capítulo

Noções básicas sobre as funcionalidades do QuickClean

Esta secção descreve as funcionalidades do QuickClean.

Funcionalidades

O QuickClean disponibiliza um conjunto de ferramentas eficientes e de fácil utilização para eliminar o lixo digital de uma forma segura. Pode libertar espaço em disco valioso e optimizar o desempenho do computador.

CAPÍTULO 7

Limpar o computador

O QuickClean permite-lhe eliminar ficheiros e pastas com segurança.

Quando navega na Internet, o browser copia cada página da Internet e respectivos gráficos para uma pasta de cache no disco. O browser pode assim carregar rapidamente a página se voltar novamente a essa página. Os ficheiros de cache são úteis se visitar constantemente as mesmas páginas da Internet e o seu conteúdo não mudar com frequência. Na maior parte dos casos, no entanto, os ficheiros de cache não são úteis e podem ser eliminados.

É possível eliminar vários itens com as seguintes funções de limpeza.

- Limpeza da Reciclagem: Limpa a reciclagem do Windows.
- Limpeza de Ficheiros Temporários: Elimina os ficheiros armazenados em pastas temporárias.
- Limpeza de Atalhos: Elimina atalhos quebrados e atalhos sem um programa associado.
- Limpeza de Fragmentos Perdidos de Ficheiros: Elimina fragmentos perdidos de ficheiros do computador.
- Limpeza do Registo: Elimina informações de registo do Windows relativas a programas que já não existem no computador.
- Limpeza da Cache: Elimina ficheiros de cache que se vão acumulando quando navega na Internet. Os ficheiros deste tipo são normalmente guardados como ficheiros temporários da Internet.
- Limpeza de Cookies: Elimina cookies. Os ficheiros deste tipo são normalmente guardados como ficheiros temporários da Internet.
  Os cookies são pequenos ficheiros que o Web browser guarda no computador a pedido de um servidor Web. Sempre que consulta uma página Web a partir do servidor Web, o browser envia o cookie para o servidor. Estes cookies podem funcionar como um código, que permite ao servidor Web registar as páginas que visita e a frequência com que as visita.
- Limpeza do Histórico do Browser: Elimina o histórico do browser.
- Limpeza de mensagens das pastas 'Itens enviados' e 'Itens eliminados' do Correio Electrónico do Outlook Express e do Outlook: Elimina as mensagens de correio electrónico das pastas 'Itens enviados' e 'Itens eliminados' do Outlook.

- Limpeza de Ficheiros Utilizados Recentemente: Elimina os itens recentemente utilizados que se encontram guardados no computador, como os documentos do Microsoft Office.
- Limpeza de ActiveX e Plug-in: Elimina controlos e extensões ActiveX.
  ActiveX é uma tecnologia utilizada para implementar controlos num programa. Um controlo ActiveX permite adicionar um botão à interface de um programa. A maioria destes controlos são inofensivos; no entanto, algumas pessoas podem utilizar a tecnologia ActiveX para capturar informações do computador.
  Extensões são pequenos programas de software que estabelecem ligação com aplicações mais abrangentes, com vista a proporcionar uma maior funcionalidade. As extensões permitem que o Web browser aceda a e execute ficheiros incorporados em documentos HTML em formatos que o browser normalmente não reconheceria (por exemplo, ficheiros de animação, vídeo e áudio).
- Limpeza de Pontos de Restauro do Sistema: Elimina do computador pontos de restauro do sistema antigos.

Neste capítulo

Utilizar o QuickClean

Esta secção descreve como utilizar o QuickClean.

Limpar o computador

Pode eliminar ficheiros e pastas não utilizados, libertar espaço em disco e tornar o computador mais eficiente.

Para limpar o computador:

1. No menu Avançado, clique em **Ferramentas**.
2. Clique em **Fazer Manutenção do Computador** e, em seguida, seleccione **Iniciar** em **McAfee QuickClean**.
3. Efectue um dos seguintes procedimentos:
   - Clique em **Seguinte** para aceitar as limpezas predefinidas na lista.
   - Seleccione ou desmarque as limpezas que considerar adequadas e, em seguida, clique em **Seguinte.** Para a Limpeza de Ficheiros Utilizados Recentemente, pode clicar em **Propriedades** para desmarcar os programas cujas listas não deseja limpar.
   - Clique em **Restaurar Predefinições** para repor as limpezas predefinidas e, em seguida, clique em **Seguinte.**
4. Depois de efectuada a análise, clique em **Seguinte** para confirmar a eliminação dos ficheiros. Pode expandir esta lista para ver os ficheiros que serão limpos e a sua localização.
5. Clique em **Seguinte**.
6. Efectue um dos seguintes procedimentos:
   - Clique em **Seguinte** para aceitar a opção predefinida **Não, quero eliminar os ficheiros utilizando o método padrão de eliminação do Windows**.
   - Clique em **Sim, pretendo apagar os ficheiros com segurança utilizando o Shredder** e especifique o número de passagens. Os ficheiros eliminados com o Shredder não podem ser recuperados.
7. Clique em **Concluir**.
8. Em **Resumo do QuickClean**, visualize o número de ficheiros de registo que foram eliminados e a quantidade de espaço em disco recuperada após a limpeza do disco e da Internet.

CAPÍTULO 8

McAfee Shredder

Os ficheiros eliminados podem ser recuperados a partir do computador mesmo depois de esvaziar a Reciclagem. Quando elimina um ficheiro, o Windows marca esse espaço na unidade de disco para indicar que já não está a ser utilizado, mas o ficheiro continua presente. Com ferramentas de peritagem informática, pode recuperar registos de impostos, currículos ou outros documentos que tenha eliminado. O Shredder protege a sua privacidade eliminando os ficheiros indesejados de forma segura e permanente.

Para eliminar um ficheiro de forma permanente, é necessário substituir várias vezes o ficheiro existente por novos dados. O Microsoft® Windows não elimina ficheiros com segurança, porque cada operação de ficheiro seria muito lenta. A destruição de um documento nem sempre impede que o documento seja recuperado, pois alguns programas fazem cópias ocultas temporárias de documentos abertos. Se destruir apenas os documentos apresentados no Explorador do Windows®, é possível que ainda tenha cópias temporárias desses documentos.

Nota: Não é efectuada cópia de segurança dos ficheiros destruídos. Não é possível recuperar ficheiros eliminados pelo Shredder.

Neste capítulo

Noções básicas das funcionalidades do Shredder

Esta secção descreve as funcionalidades do Shredder.

Funcionalidades

O Shredder permite apagar o conteúdo da Reciclagem, os ficheiros temporários da Internet, o histórico dos Web sites, ficheiros, pastas e discos.

CAPÍTULO 9

Apagar ficheiros indesejados com o Shredder

O Shredder protege a sua privacidade, eliminando, de forma segura e permanente, ficheiros indesejados, tais como o conteúdo da Reciclagem, os ficheiros temporários da Internet e o histórico dos Web sites. Pode seleccionar ou procurar os ficheiros e as pastas que pretende destruir.

Neste capítulo

Utilizar o Shredder

Esta secção descreve como utilizar o Shredder.

Destruir ficheiros, pastas e discos

Os ficheiros podem permanecer no computador, mesmo depois de esvaziar a Reciclagem. No entanto, quando destrói ficheiros, os dados são eliminados de forma permanente e os hackers não conseguem aceder aos mesmos.

Para destruir ficheiros, pastas e discos:

1. No menu Avançado, clique em **Ferramentas** e, em seguida, clique em **Shredder**.
2. Efectue um dos seguintes procedimentos:
   - Clique em **Apagar ficheiros e pastas** para destruir ficheiros e pastas.
   - Clique em **Apagar um disco inteiro** para destruir discos**.**
3. Seleccione um dos seguintes níveis de destruição:
   - **Rápido**: Destrói os itens seleccionados uma vez.
   - **Abrangente**: Destrói os itens seleccionados 7 vezes.
   - **Personalizar**: Destrói os itens seleccionados até 10 vezes. Um número maior de passagens de destruição aumenta o nível de eliminação segura dos ficheiros.
4. Clique em **Seguinte**.
5. Efectue um dos seguintes procedimentos:
   - Para destruir ficheiros, clique em **Conteúdo da Reciclagem**, **Ficheiros temporários da Internet** ou **Histórico dos Web sites** na lista **Seleccionar os ficheiros a destruir**. Para destruir um disco, clique no disco.
   - Clique em **Procurar**, procure os ficheiros que pretende destruir e seleccione-os.
   - Escreva o caminho para os ficheiros que pretende destruir na lista **Seleccionar os ficheiros a destruir**.
6. Clique em **Seguinte**.
7. Clique em **Terminar** para concluir a operação.
8. Clique em **Concluído**.

CAPÍTULO 10

McAfee Network Manager

O McAfee® Network Manager apresenta uma vista gráfica dos computadores e componentes que compõem a sua rede doméstica. Pode utilizar o Network Manager para monitorizar, de forma remota, o estado de protecção de cada computador gerido na sua rede e corrigir remotamente vulnerabilidades de segurança comunicadas nesses computadores geridos.

Antes de começar a utilizar o Network Manager, pode familiarizar-se com algumas das funcionalidades mais populares. A ajuda do Network Manager inclui detalhes sobre configuração e utilização destas funcionalidades.

Neste capítulo

Funcionalidades

O Network Manager oferece as seguintes funcionalidades:

Mapeamento de rede gráfico

O mapeamento de rede do Network Manager proporciona uma visão gráfica global do estado de segurança dos computadores e componentes que compõem a sua rede doméstica. Quando altera a rede (por exemplo, adicionando um computador), o mapeamento de rede reconhece essas alterações. Pode actualizar o mapeamento de rede, mudar o nome da rede e mostrar ou ocultar componentes do mapeamento de rede, para personalizar a visualização. Pode também ver as informações associadas aos componentes apresentados no mapeamento de rede.

Gestão remota

Utilize o mapeamento de rede do Network Manager para gerir o estado de segurança dos computadores que fazem parte da sua rede doméstica. Pode convidar um computador a aderir à rede gerida, monitorizar o estado de protecção do computador gerido e resolver problemas de vulnerabilidade de segurança detectados a partir de um computador remoto da rede.

Noções básicas sobre os ícones do Network Manager

A tabela seguinte descreve os ícones normalmente utilizados no mapeamento de rede do Network Manager.

Ícone	Descrição
	Representa um computador gerido e online
	Representa um computador gerido e offline
	Representa um computador não gerido com o software de segurança McAfee 2007 instalado
	Representa um computador não gerido e offline
	Representa um computador online que não tem o software de segurança McAfee 2007 instalado nem um dispositivo de rede desconhecido
	Representa um computador offline que não tem o software de segurança McAfee 2007 instalado nem um dispositivo de rede desconhecido offline
	Significa que o item correspondente está protegido e ligado
	Significa que o item correspondente requer a sua atenção
	Significa que o item correspondente requer a sua atenção e está desligado
	Representa um router de raiz sem fios
	Representa um router de raiz padrão
	Representa a Internet, quando está ligada
	Representa a Internet, quando está desligada

CAPÍTULO 11

Configurar uma rede gerida

Configurou uma rede gerida, utilizando os itens no mapeamento de rede e adicionando membros (computadores) à rede.

Neste capítulo

Utilizar o mapeamento de rede

Sempre que liga um computador à rede, o Network Manager analisa o estado da rede para determinar se existem membros (geridos ou não geridos), atributos de router e o estado da Internet. Se não forem encontrados membros, o Network Manager presume que o computador actualmente ligado é o primeiro computador na rede e torna-o automaticamente um membro gerido com permissões de administração. Por predefinição, o nome da rede inclui o nome do grupo de trabalho ou do domínio do primeiro computador que é ligado à rede com o software de segurança McAfee 2007 instalado; no entanto, é possível mudar o nome da rede a qualquer momento.

Se efectuar alterações na rede (por exemplo, adicionar um computador), pode personalizar o mapeamento de rede. Por exemplo, pode actualizar o mapeamento de rede, mudar o nome da rede, bem como mostrar ou ocultar componentes do mapeamento de rede para personalizar a sua vista. Pode também ver as informações associadas aos componentes apresentados no mapeamento de rede.

Aceder ao mapeamento de rede

Pode aceder ao mapa da sua rede, iniciando o Network Manager a partir da lista de tarefas comuns do SecurityCenter. O mapeamento de rede mostra uma representação gráfica dos computadores e componentes que compõem a sua rede doméstica.

Para aceder ao mapeamento de rede:

- No menu Básico ou Avançado, clique em **Gerir Rede**.
  O mapeamento de rede é apresentado no painel da direita.

Nota: A primeira vez que acede ao mapeamento de rede, é-lhe solicitado que confie nos outros computadores da rede antes de o mapeamento de rede ser apresentado.

Actualizar o mapeamento de rede

Pode actualizar o mapeamento de rede em qualquer altura; por exemplo, depois de adicionar outro computador à rede gerida.

Para actualizar o mapeamento de rede:

1. No menu Básico ou Avançado, clique em **Gerir Rede**.
   O mapeamento de rede é apresentado no painel da direita.
2. Clique em **Actualizar o mapeamento de rede** em **Quero**.

Nota: A lista **Actualizar o mapeamento de rede** só está disponível se não estiverem seleccionados itens no mapeamento de rede. Para desmarcar um item, clique no item seleccionado ou numa área em branco no mapeamento de rede.

Mudar o nome da rede

Por predefinição, o nome da rede inclui o nome do grupo de trabalho ou do domínio do primeiro computador que é ligado à rede com o software de segurança McAfee 2007 instalado. Se o nome não for adequado, pode alterá-lo.

Para mudar o nome da rede:

1. No menu Básico ou Avançado, clique em **Gerir Rede**.
   O mapeamento de rede é apresentado no painel da direita.
2. Clique em **Mudar o nome da rede** em **Quero**.
3. Introduza o nome da rede na caixa **Mudar o nome da rede**.
4. Clique em **OK**.

Nota: A ligação **Mudar o nome da rede** só está disponível se não estiverem seleccionados itens no mapeamento de rede. Para desmarcar um item, clique no item seleccionado ou numa área em branco no mapeamento de rede.

Mostrar ou ocultar itens no mapeamento de rede

Por predefinição, todos os computadores e componentes na sua rede doméstica são apresentados no mapeamento de rede. No entanto, se tiver itens ocultos, pode mostrá-los novamente em qualquer altura. Só é possível ocultar os itens não geridos; os computadores geridos não podem ser ocultos.

Para...	No menu Básico ou Avançado, clique em **Gerir Rede** e efectue o seguinte...
Ocultar um item no mapeamento de rede	Clique num item no mapeamento de rede e, em seguida, clique em **Ocultar este item** em **Quero**. Na caixa de diálogo de confirmação, clique em **Sim**.
Mostrar itens ocultos no mapeamento de rede	Em **Quero**, clique em **Mostrar itens ocultos**.

Ver detalhes do item

Pode ver informações detalhadas sobre qualquer componente na sua rede, seleccionando o componente no mapeamento de rede. Estas informações incluem o nome do componente, o respectivo estado de protecção e outras informações necessárias para gerir o componente.

Para ver os detalhes de um item:

1. Clique no ícone de um item no mapeamento de rede.
2. Em **Detalhes**, visualize a informação sobre o item.

Aderir à rede gerida

Antes de um computador poder ser gerido remotamente ou ser-lhe concedida permissão para gerir, de forma remota, outros computadores na rede, deve tornar-se um membro de confiança da rede. A confirmação de membro da rede é concedida a novos computadores através de membros de rede existentes (computadores) com permissões de administração. Para garantir que aderem apenas computadores de confiança à rede, os utilizadores dos computadores de concessão e adesão devem autenticar-se entre si.

Se um computador aderir à rede, ser-lhe-á solicitado para expor o respectivo estado de protecção McAfee a outros computadores na rede. Se um computador aceitar expor o respectivo estado de protecção, torna-se um membro *gerido* da rede. Se um computador recusar expor o respectivo estado de protecção, torna-se um membro *não gerido* da rede. Os membros não geridos da rede são normalmente computadores convidados que pretendem aceder a outras funções de rede (por exemplo, partilha de ficheiros ou impressoras).

Nota: Depois de aderir, se tiver outros programas de rede da McAfee instalados (por exemplo, o McAfee Wireless Network Security ou o EasyNetwork), o computador é igualmente reconhecido como um computador gerido nesses programas. O nível de permissão atribuído a um computador no Network Manager aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o significado das permissões de convidado, de acesso total ou administrativo noutros programas de rede da McAfee, consulte a documentação fornecida com o respectivo programa.

Aderir a uma rede gerida

Se receber um convite para aderir a uma rede gerida, pode aceitá-lo ou recusá-lo. Pode também determinar se pretende que este computador e outros computadores na rede monitorizem as definições de segurança de cada um (por exemplo, se os serviços de protecção antivírus de um computador estão actualizados).

Para aderir a uma rede gerida:

1. Na caixa de diálogo de convite, active a caixa de verificação **Permitir que este e outros computadores da rede monitorizem as definições de segurança de cada um** para permitir que outros computadores na rede gerida monitorizem as definições de segurança do seu computador.
2. Clique em **Aderir**.
   Se aceitar o convite, são apresentadas duas cartas de jogar.
3. Confirme se essas cartas de jogar são iguais às apresentadas no computador que o convidou para aderir à rede gerida.
4. Clique em **Confirmar**.

Nota: Se o computador que o convidou para aderir à rede gerida não apresentar as mesmas cartas de jogar apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. A adesão à rede pode colocar o computador em perigo; por conseguinte, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Convidar um computador para aderir à rede gerida

Se um computador for adicionado à rede gerida ou existir outro computador não gerido na rede, pode convidar esse computador para aderir à rede gerida. Apenas os computadores com permissões de administração na rede podem convidar outros computadores para aderir à rede. Se enviar o convite, pode também especificar o nível de permissão que pretende atribuir ao computador aderente.

Para convidar um computador para aderir à rede gerida:

1. Clique no ícone de um computador não gerido no mapeamento de rede.
2. Clique em **Monitorizar este computador** em **Quero**.
3. Na caixa de diálogo Convidar um computador a aderir a esta rede gerida, clique numa das seguintes opções:
   - **Conceder acesso de convidado**
     O acesso de convidado permite ao computador ter acesso à rede.

- **Conceder acesso total a todas as aplicações de rede geridas**
  Acesso total (tal como o acesso de convidado) permite o acesso do computador à rede.
- **Conceder acesso administrativo a todas as aplicações de rede geridas**
  O acesso administrativo permite ao computador aceder à rede com permissões de administração. Permite também ao computador conceder acesso a outros computadores que pretendam aderir à rede gerida.

4 Clique em **Convidar**.
É enviado ao computador um convite para aderir à rede gerida. Se o computador aceitar o convite, são apresentadas duas cartas de jogar.

5 Confirme se essas cartas de jogar são iguais às apresentadas no computador que convidou para aderir à rede gerida.

6 Clique em **Conceder Acesso**.

Nota: Se o computador que convidou para aderir à rede gerida não apresentar as mesmas cartas de jogar apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. Permitir a adesão de um computador à rede pode colocar outros computadores em risco; por conseguinte, clique em **Rejeitar Acesso** na caixa de diálogo de confirmação de segurança.

Parar de confiar nos computadores da rede

Se, por engano, concordar em confiar noutros computadores na rede, pode parar essa acção.

Para parar de confiar em computadores na rede:

- Clique em **Parar de confiar em computadores nesta rede** em **Quero**.

Nota: A ligação **Parar de confiar em computadores nesta rede** só está disponível se outros computadores geridos não tiverem aderido à rede.

CAPÍTULO 12

Gerir a rede de forma remota

Depois de configurar a rede gerida, pode utilizar o Network Manager para gerir remotamente os computadores e componentes que compõem a sua rede. Pode monitorizar o estado e os níveis de permissão dos computadores e componentes e corrigir vulnerabilidades de segurança de forma remota.

Neste capítulo

Monitorizar o estado e as permissões

Uma rede gerida dispõe de dois tipos de membros: membros geridos e membros não geridos. Os membros geridos permitem que outros computadores da rede monitorizem o respectivo estado de protecção McAfee; os membros não geridos não o permitem. Os membros não geridos são normalmente computadores convidados que pretendem aceder a outras funções de rede (por exemplo, partilha de ficheiros ou impressoras). Como computador não gerido, pode ser convidado a tornar-se um computador gerido em qualquer altura por outro computador gerido na rede. Do mesmo modo, um computador gerido pode tornar-se não gerido em qualquer altura.

Os computadores geridos têm permissões de administração, total ou de convidado associadas aos mesmos. As permissões de administração permitem ao computador gerido administrar o estado de protecção de todos os outros computadores geridos na rede e conceder aos computadores inscritos acesso à rede. As permissões de convidado e acesso total permitem que um computador aceda apenas à rede. Pode modificar o nível de permissão de um computador em qualquer altura.

Uma vez que a rede gerida é composta igualmente por dispositivos (por exemplo, routers), pode utilizar o Network Manager para geri-los também. Pode também configurar e modificar as propriedades de visualização de um dispositivo no mapeamento de rede.

Monitorizar o estado de protecção de um computador

Se o estado de protecção de um computador não estiver a ser monitorizado na rede (quer seja pelo facto do computador não ser um membro da rede ou pelo facto do computador ser um membro não gerido da rede), pode efectuar um pedido para monitorizá-lo.

Para monitorizar o estado de protecção de um computador:

1. Clique no ícone de um computador não gerido no mapeamento de rede.
2. Clique em **Monitorizar este computador** em **Quero**.

Parar de monitorizar o estado de protecção de um computador

Pode parar de monitorizar o estado de protecção de um computador gerido na sua rede privada. Em seguida, o computador torna-se um computador não gerido.

Para parar de monitorizar o estado de protecção de um computador:

1. Clique no ícone de um computador gerido no mapeamento de rede.
2. Clique em **Parar de monitorizar este computador** em **Quero**.
3. Na caixa de diálogo de confirmação, clique em **Sim**.

Modificar as permissões de um computador gerido

Pode modificar as permissões de um computador gerido em qualquer altura. Isto permite-lhe ajustar os computadores que podem monitorizar o estado de protecção (definições de segurança) de outros computadores na rede.

Para modificar as permissões de um computador gerido:

1. Clique no ícone de um computador gerido no mapeamento de rede.
2. Clique em **Modificar as permissões deste computador** em **Quero**.
3. Na caixa de diálogo para modificar as permissões, seleccione ou desmarque a caixa de verificação para determinar se este e outros computadores na rede gerida podem monitorizar o estado de protecção de cada um.
4. Clique em **OK**.

Gerir um dispositivo

Pode gerir um dispositivo, acedendo à respectiva página Web de administração a partir do Network Manager.

Para gerir um dispositivo:

1. Clique no ícone de um dispositivo no mapeamento de rede.
2. Clique em **Gerir este dispositivo** em **Quero**.
   É aberto um Web browser e aparece a página Web de administração do dispositivo.
3. No Web browser, introduza as informações de início de sessão e configure as definições de segurança do dispositivo.

Nota: Se o dispositivo for um router ou um ponto de acesso sem fios protegido pelo Wireless Network Security, deve utilizar o Wireless Network Security para configurar as definições de segurança do dispositivo.

Modificar as propriedades de visualização de um dispositivo

Se modificar as propriedades de visualização de um dispositivo, pode também alterar o nome de visualização do dispositivo no mapeamento de rede e especificar se o dispositivo é um router sem fios.

Para modificar as propriedades de visualização de um dispositivo:

1. Clique no ícone de um dispositivo no mapeamento de rede.
2. Clique em **Modificar as propriedades do dispositivo** em **Quero**.
3. Para especificar o nome de visualização do dispositivo, introduza um nome na caixa **Nome**.
4. Para especificar o tipo de dispositivo, clique numa das seguintes opções:
   - **Router**
     Isto representa um router de raiz padrão.
   - **Router sem fios**
     Isto representa um router de raiz sem fios.
5. Clique em **OK**.

Corrigir vulnerabilidades de segurança

Os computadores geridos com permissões de administração podem monitorizar o estado de protecção McAfee de outros computadores geridos na rede e corrigir remotamente quaisquer vulnerabilidades de segurança. Por exemplo, se o estado de protecção McAfee de um computador gerido indicar que o VirusScan está desactivado, outro computador gerido com permissões de administração pode *corrigir* esta vulnerabilidade de segurança, activando o VirusScan remotamente.

Se corrigir vulnerabilidades de segurança remotamente, o Network Manager repara automaticamente a maioria dos problemas comunicados. No entanto, algumas vulnerabilidades de segurança podem requerer intervenção manual no computador local. Neste caso, o Network Manager corrige esses problemas que podem ser reparados remotamente e depois pede-lhe para corrigir os problemas restantes, iniciando sessão no SecurityCenter no computador vulnerável e seguindo as recomendações fornecidas. Nalguns casos, a correcção sugerida é instalar o software de segurança McAfee 2007 no(s) computador(es) remoto(s) na sua rede.

Corrigir vulnerabilidades de segurança

Pode utilizar o Network Manager para corrigir automaticamente a maior parte das vulnerabilidades de segurança de computadores remotos geridos. Por exemplo, se o VirusScan estiver desactivado num computador remoto, pode utilizar o Network Manager para activá-lo automaticamente.

Para corrigir vulnerabilidades de segurança:

1. Clique no ícone de um item no mapeamento de rede.
2. Veja o estado de protecção do item em **Detalhes**.
3. Clique em **Corrigir vulnerabilidades de segurança** em **Quero**.
4. Quando os problemas tiverem sido corrigidos, clique em **OK**.

Nota: Embora o Network Manager corrija automaticamente a maioria das vulnerabilidades de segurança, algumas correcções podem exigir que inicie o SecurityCenter no computador vulnerável e siga as recomendações fornecidas.

Instalar o software de segurança McAfee em computadores remotos

Se um ou mais computadores na sua rede não utilizarem o software de segurança McAfee 2007, o estado de segurança não pode ser monitorizado remotamente. Se pretender monitorizar estes computadores remotamente, deve aceder a cada computador e instalar o software de segurança McAfee 2007.

Para instalar o software de segurança McAfee num computador remoto:

1. Num browser do computador remoto, vá para http://download.mcafee.com/us/.
2. Siga as instruções no ecrã para instalar o software de segurança McAfee 2007 no computador.

CAPÍTULO 13

McAfee VirusScan

O VirusScan oferece uma protecção completa, fiável e actualizada contra vírus e spyware. Controlado pela galardoada tecnologia de análise da McAfee, o VirusScan oferece protecção contra vírus, worms, cavalos de Tróia, scripts suspeitos, rootkits, capacidade da memória intermédia excedida, ataques híbridos, spyware, programas potencialmente indesejados e outras ameaças.

Neste capítulo

Funcionalidades

Esta versão do VirusScan oferece as seguintes funcionalidades.

Protecção antivírus

A análise em tempo real verifica os ficheiros quando o computador ou o utilizador acede aos ficheiros.

Analisar

Procura vírus e outras ameaças em unidades de disco rígido, disquetes e em ficheiros e pastas individuais. Pode também clicar com o botão direito do rato num item para o analisar.

Detecção de spyware e adware

O VirusScan identifica e remove spyware, adware e outros programas que possam pôr a sua privacidade em perigo e diminuir o desempenho do seu computador.

Actualizações automáticas

As actualizações automáticas protegem-no contra as mais recentes ameaças informáticas identificadas e não identificadas.

Análise rápida em segundo plano

As análises rápidas e discretas identificam e destroem vírus, cavalos de Tróia, worms, spyware, adware, marcadores e outras ameaças sem interromperem o seu trabalho.

Alertas de segurança em tempo real

Os alertas de segurança informam-no de surtos de vírus e ameaças de segurança, fornecendo opções de resposta para remover, neutralizar ou obter mais informações sobre a ameaça.

Detecção e limpeza em vários pontos de entrada

O VirusScan monitoriza e limpa os pontos de entrada principais do seu computador: correio electrónico, anexos de mensagens instantâneas e conteúdos transferidos da Internet.

Monitorização de actividades semelhantes a worms em correio electrónico

O WormStopper™ impede que os cavalos de Tróia enviem mensagens de correio electrónico com worms para outros computadores e avisa o utilizador antes de os programas de correio electrónico desconhecidos enviarem mensagens para outros computadores.

Monitorização de actividades semelhantes a worms em scripts

O ScriptStopper™ impede a execução de scripts conhecidos e prejudiciais no seu computador.

McAfee X-ray for Windows

O McAfee X-ray detecta e mata rootkits e outros programas que se escondem do Windows.

Protecção contra capacidade da memória intermédia excedida

A protecção contra capacidade da memória intermédia excedida evita que a memória intermédia fique sobrecarregada. A capacidade da memória intermédia excedida ocorre quando programas ou processos suspeitos tentam armazenar numa memória intermédia (área de armazenamento de dados temporário) mais dados do que o limite suportado, danificando ou substituindo dados válidos nas memórias intermédias adjacentes.

Protecção de Sistema da McAfee

As Protecções do Sistema procuram no computador comportamentos específicos que indiciem actividades relacionadas com vírus, spyware ou hackers.

CAPÍTULO 14

Gerir a Protecção Antivírus

Pode gerir a protecção em tempo real antivírus, contra spyware, Protecções do Sistema e scripts. Por exemplo, pode desactivar a análise ou indicar o que pretende analisar.

Apenas utilizadores com direitos de Administrador podem modificar opções avançadas.

Neste capítulo

Utilizar protecção antivírus

Quando inicia a protecção antivírus (análise em tempo real), o computador é constantemente monitorizado para detecção de actividades relacionadas com vírus. A análise em tempo real verifica os ficheiros sempre que o utilizador ou o computador acede aos mesmos. Quando a protecção antivírus detecta um ficheiro infectado, tenta limpar ou remover a infecção. Se não for possível limpar ou remover a infecção, o utilizador recebe um aviso para tomar medidas adicionais.

Tópicos relacionados

- Noções básicas sobre alertas de segurança (página 103)

Desactivar a protecção antivírus

Se desactivar a protecção antivírus, não será efectuada a monitorização contínua do computador para detecção de vírus. Se tiver de parar a protecção antivírus, certifique-se de que não está ligado à Internet.

Nota: Ao desactivar a protecção antivírus, desactiva igualmente a protecção em tempo real contra spyware, correio electrónico e mensagens instantâneas.

Para desactivar a protecção antivírus:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador e Ficheiros**.
3. Em **Protecção Antivírus**, clique em **Desligado**.
4. Na caixa de diálogo de confirmação, execute um dos seguintes procedimentos:
   - Para reiniciar a protecção antivírus após um determinado período de tempo, seleccione a caixa de verificação **Reactivar a análise em tempo real após** e seleccione um período de tempo no menu.
   - Para impedir que a protecção antivírus seja reiniciada após um determinado período de tempo, desmarque a caixa de verificação **Reactivar a protecção antivírus após**.

5 Clique em **OK**.

Se a protecção em tempo real estiver configurada para ser iniciada durante o arranque do Windows, o computador ficará protegido quando for reiniciado.

Tópicos relacionados

- Configurar protecção em tempo real (página 74)

Activar a protecção antivírus

A protecção antivírus efectua continuamente a monitorização do computador para detecção de actividades relacionadas com vírus.

Para activar a protecção antivírus:

1 No Menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador & Ficheiros**.

3 Em **Protecção Antivírus**, clique em **Ligado**.

Configurar protecção em tempo real

Pode modificar a protecção antivírus em tempo real. Por exemplo, pode analisar apenas documentos e ficheiros de programas ou desactivar a análise em tempo real aquando do arranque do Windows (não recomendado).

Configurar protecção em tempo real

Pode modificar a protecção antivírus em tempo real. Por exemplo, pode analisar apenas documentos e ficheiros de programas ou desactivar a análise em tempo real aquando do arranque do Windows (não recomendado).

Para configurar a protecção em tempo real:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador e Ficheiros**.
3. Em **Protecção Antivírus**, clique em **Avançado**.
4. Marque ou desmarque as seguintes caixas de verificação:
   - **Análise de vírus desconhecidos utilizando heurística**: É efectuada a correspondência entre os ficheiros e as assinaturas de vírus conhecidos, com vista à detecção de indícios de vírus não identificados. Esta opção fornece a análise mais completa, mas é geralmente mais lenta do que uma análise normal.
   - **Analisar a unidade de disquetes ao encerrar**: Quando encerra o computador, a unidade de disquetes é analisada.
   - **Analisar a existência de spyware e programas potencialmente indesejados**: Programas de spyware, adware e outros programas potencialmente susceptíveis de recolha e transmissão de dados sem permissão são detectados e removidos.
   - **Analisar e remover cookies de registo**: Os cookies potencialmente susceptíveis de recolha e transmissão de dados sem permissão são detectados e removidos. Um cookie identifica os utilizadores quando estes visitam uma página Web.
   - **Analisar unidades de rede**: As unidades ligadas à rede são analisadas.
   - **Activar a protecção contra capacidade da memória intermédia excedida**: Se for detectada actividade excessiva da memória intermédia, a memória é bloqueada e o utilizador recebe um aviso.
   - **Iniciar análise em tempo real no arranque do Windows (recomendado)**: A protecção em tempo real é activada sempre que inicia o computador, mesmo que encerre uma sessão.

5 Clique num dos seguintes botões:

- **Todos os ficheiros (recomendado)**: Todos os tipos de ficheiros utilizados pelo computador são analisados. Utilize esta opção para obter a análise mais completa.
- **Apenas ficheiros de programas e documentos**: Apenas são analisados documentos e ficheiros de programas.

6 Clique em **OK**.

Utilizar protecção contra spyware

A protecção contra spyware remove spyware, adware e outros programas potencialmente indesejados que recolham e transmitam dados sem permissão.

Desactivar a protecção contra spyware

Se desactivar a protecção contra spyware, os programas potencialmente indesejados que recolham e transmitam dados sem permissão não são detectados.

Para desactivar a protecção contra spyware:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção contra spyware**, clique em **Desligado**.

Activar a protecção contra spyware

A protecção contra spyware remove spyware, adware e outros programas potencialmente indesejados que recolham e transmitam dados sem permissão.

Para activar a protecção contra spyware:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção contra spyware**, clique em **Ligado**.

Utilizar Protecções do Sistema

As Protecções do Sistema detectam eventuais alterações não autorizadas no computador e alertam-no quando estas ocorrem. Pode, então, analisar essas alterações e decidir se as permite.

As Protecções do Sistema são categorizadas da seguinte forma.

Programa

O Programa de Protecções do Sistema detecta alterações nos ficheiros de arranque, nas extensões e nos ficheiros de configuração.

Windows

As Protecções do Sistema do Windows detectam as alterações efectuadas nas definições do Internet Explorer, incluindo os atributos do browser e as definições de segurança.

Browser

As Protecções do Sistema do Browser detectam as alterações efectuadas nos serviços, certificados e ficheiros de configuração do Windows ∃.

Desactivar Protecções do Sistema

Se desactivar as Protecções do Sistema, eventuais alterações não autorizadas que ocorram no computador não serão detectadas.

Para desactivar todas as Protecções do Sistema:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção do Sistema**, clique em **Desligado**.

Activar Protecções do Sistema

As Protecções do Sistema detectam eventuais alterações não autorizadas no computador e alertam-no quando estas ocorrem.

Para activar Protecções do Sistema:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção do Sistema**, clique em **Ligado**.

Configurar Protecções do Sistema

Pode modificar as Protecções do Sistema. Para cada alteração detectada, pode decidir se quer receber um aviso e registar o evento, apenas registar o evento ou desactivar as Protecções do Sistema.

Configurar Protecções do Sistema

Pode modificar as Protecções do Sistema. Para cada alteração detectada, pode decidir se quer receber um aviso e registar o evento, apenas registar o evento ou desactivar as Protecções do Sistema.

Para configurar Protecções do Sistema:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção do Sistema**, clique em **Avançado**.
4. Na lista de Protecções do Sistema, clique numa categoria para ver a lista de Protecções do Sistema associadas e o respectivo estado.
5. Clique no nome de uma Protecção do Sistema.
6. Em **Detalhes**, visualize informações sobre a Protecção do Sistema.
7. Em **Quero**, execute uma das seguintes operações:
   - Clique em **Mostrar avisos** se quiser receber um aviso quando ocorrer uma alteração e se quiser que o evento seja registado.
   - Clique em **Registar apenas alterações** se não quiser que seja executada qualquer acção quando for detectada uma alteração. A alteração será apenas registada.
   - Clique em **Desactivar esta Protecção do Sistema** para desligar a Protecção do Sistema. Quando ocorrer uma alteração, não receberá qualquer aviso, nem o evento será registado.
8. Clique em **OK**.

Noções Básicas de Protecções do Sistema

As Protecções do Sistema detectam eventuais alterações não autorizadas no computador e alertam-no quando estas ocorrem. Pode, então, analisar essas alterações e decidir se as permite.

As Protecções do Sistema são categorizadas da seguinte forma.

Programa

O Programa de Protecções do Sistema detecta alterações nos ficheiros de arranque, nas extensões e nos ficheiros de configuração.

Windows

As Protecções do Sistema do Windows detectam as alterações efectuadas nas definições do Internet Explorer, incluindo os atributos do browser e as definições de segurança.

Browser

As Protecções do Sistema do Browser detectam as alterações efectuadas nos serviços, certificados e ficheiros de configuração do Windows ∃.

Acerca do Programa de Protecções do Sistema

O Programa de Protecções do Sistema detecta os seguintes itens.

Instalações ActiveX

Detecta programas ActiveX transferidos através do Internet Explorer. Os programas ActiveX são transferidos de Web sites e armazenados no computador em C:\Windows\Downloaded Program Files ou em C:\Windows\Temp\Temporary Internet Files. Também estão referenciados no registo através do seu CLSID (a grande sequência de números entre chavetas).

O Internet Explorer utiliza muitos programas ActiveX legítimos. Se tiver dúvidas acerca de um programa ActiveX, pode eliminá-lo sem perigo para o computador. Se precisar desse programa mais tarde, o Internet Explorer transferi-lo-á na próxima vez que aceder a um Web site que necessite dele.

Itens de Arranque

Controlam as alterações efectuadas nas pastas e chaves de registo do arranque. As chaves de registo do arranque no registo do Windows e nas pastas de arranque do menu Iniciar guardam os caminhos para os programas existentes no computador. Os programas listados nessas localizações são carregados quando o Windows arranca. Os programas de spyware ou outros programas potencialmente indesejados procuram com frequência ser carregados quando o Windows arranca.

Rotinas de Execução da Shell do Windows

Controlam as alterações efectuadas na lista de programas que são carregados no ficheiro explorer.exe. Uma rotina de execução da shell é um programa que é carregado na shell do ficheiro explorer.exe do Windows. Uma rotina de execução da shell recebe todos os comandos de execução que são executados num computador. Qualquer programa carregado na shell do ficheiro explorer.exe pode executar uma tarefa adicional antes de outro programa ser iniciado. Os programas de spyware ou outros programas potencialmente indesejados podem utilizar as rotinas de execução da shell para impedir a execução de programas de segurança.

Shell Service Object Delay Load

Controla as alterações efectuadas nos ficheiros listados em Shell Service Object Delay Load. Estes ficheiros são carregados pelo ficheiro explorer.exe quando o computador arranca. Uma vez que o explore.exe é a shell do computador, é sempre iniciado e carrega os ficheiros existentes nesta chave. Estes ficheiros são carregados no início do processo de arranque, antes da ocorrência de qualquer intervenção humana.

Sobre as Protecções do Sistema do Windows

As Protecções do Sistema do Windows detectam os seguintes itens.

Processadores de Menus de Contexto

Evitam que sejam efectuadas alterações não autorizadas aos menus de contexto do Windows. Estes menus permitem clicar com o botão direito do rato num ficheiro e executar acções específicas relacionadas com esse ficheiro.

AppInit DLLs

Evitam que sejam efectuadas alterações ou adições não autorizadas às AppInit.DLLs do Windows. O valor do registo AppInit_DLLs contém uma lista de ficheiros que são carregados quando o ficheiro user32.dll é carregado. Os ficheiros do valor AppInit_DLLs são carregados inicialmente durante a rotina de arranque do Windows, permitindo que um ficheiro .DLL potencialmente perigoso se oculte antes de ocorrer qualquer intervenção humana.

Ficheiro Hosts do Windows

Controla as alterações efectuadas ao ficheiro Hosts do computador. O ficheiro Hosts do computador é utilizado para redireccionar determinados nomes de domínio para endereços IP específicos. Por exemplo, quando visita www.exemplo.com, o browser consulta o ficheiro Hosts, detecta uma entrada para exemplo.com e aponta para o endereço IP desse domínio. Alguns programas de spyware tentam alterar o ficheiro Hosts para redireccionar o browser para outro site ou para impedir que o software seja actualizado adequadamente.

Shell do Início de Sessão

Controle a Shell do Início de Sessão. Esta shell é carregada quando um utilizador inicia sessão no Windows. A shell é a principal Interface do Utilizador (UI) utilizada para gerir o Windows e, normalmente, é o Explorador do Windows (explore.exe). No entanto, a shell do Windows pode ser alterada facilmente para apontar para outro programa. Se isso acontecer, é iniciado um programa diferente da shell do Windows sempre que um utilizador inicia sessão.

Início de Sessão UserInit

Controle as alterações das definições do utilizador para início de sessão no Windows. A chave HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit indica qual o programa iniciado depois de um utilizador iniciar sessão no Windows. O programa predefinido repõe o perfil, os tipos de letra, as cores e outras definições do nome de utilizador. É possível que spyware e outros programas potencialmente indesejados tentem arrancar, adicionando-se a esta chave.

Protocolos do Windows

Controle as alterações aos protocolos de rede. Alguns programas de spyware e outros programas potencialmente indesejados assumem o controlo de determinadas formas utilizadas pelo computador para enviar e receber dados. Este controlo é conseguido através dos filtros e rotinas de tratamento de protocolos do Windows.

Fornecedores de Serviços em Camadas do Winsock

Controle os Fornecedores de Serviços em Camadas (LSPs) que podem interceptar os dados através da rede e alterá-los ou redireccioná-los. Os LSPs legítimos incluem software com controlos de acesso, firewalls e outros programas de segurança. Os programas de spyware podem utilizar os LSPs para controlar a sua actividade na Internet e alterar os seus dados. Para evitar a reinstalação do sistema operativo, utilize programas da McAfee para remover automaticamente spyware e LSPs duvidosos.

Comandos Open da Shell do Windows

Impeça alterações aos Comandos Open da Shell (explorer.exe) do Windows. Os Comandos Open da Shell permitem que um programa específico seja executado sempre que é executado um determinado tipo de ficheiro. Por exemplo, um worm pode tentar executar-se sempre que uma aplicação .exe é executada.

Programador de Tarefas Partilhado

Controle a chave de registo SharedTaskScheduler que contém uma lista dos programas que são executados quando o Windows arranca. Alguns programas de spyware ou outros programas potencialmente indesejados modificam esta chave e adicionam-se a si próprios à lista sem a sua permissão.

Windows Messenger Service

O Windows Messenger Service é uma funcionalidade não documentada do Windows Messenger, que permite aos utilizadores enviar mensagens de pop-up. Alguns programas de spyware ou outros programas potencialmente indesejados tentam activar o serviço e enviar publicidade não solicitada. O serviço pode ser explorado utilizando uma vulnerabilidade conhecida para executar remotamente o código.

Ficheiro Win.ini do Windows

O ficheiro win.ini é um ficheiro baseado em texto que contém uma lista dos programas a executar quando o Windows arranca. A sintaxe de carregamento destes programas existe no ficheiro utilizado para suportar versões mais antigas do Windows. A maioria dos programas não utiliza o ficheiro sin.ini para carregar programas: no entanto, alguns programas de spyware ou outros programas potencialmente indesejados são concebidos de forma a tirar partido desta sintaxe e carregar-se a si próprios durante o arranque do Windows.

Acerca das Protecções do Sistema do Browser

As Protecções do Sistema do Browser detectam os seguintes itens.

Browser Helper Objects

Controle as adições aos Browser Helper Objects (BHOs). Os BHOs são programas que actuam como extensões do Internet Explorer. Os programas de spyware e de utilização abusiva do browser utilizam com frequência BHOs para mostrar anúncios ou registar hábitos de navegação. Os BHOs são também utilizados por muitos programas legítimos, tais como barras de ferramentas de pesquisa comuns.

Barras do Internet Explorer

Controle as alterações efectuadas à lista de programas da barra do Internet Explorer. Uma barra de exploração é um painel idêntico aos painéis Procurar, Favoritos ou Histórico do Internet Explorer (IE) ou do Explorador do Windows.

Extensões do Internet Explorer

Evite que programas de spyware instalem extensões do Internet Explorer. As extensões do Internet Explorer são suplementos de software que são carregados quando o Internet Explorer é iniciado. Os programas de spyware utilizam frequentemente extensões do Internet Explorer para mostrar anúncios ou registar hábitos de navegação. As extensões legítimas proporcionam uma funcionalidade acrescida para o Internet Explorer.

ShellBrowser do Internet Explorer

Controle as alterações efectuadas à instância ShellBrowser do Internet Explorer. O ShellBrowser do Internet Explorer contém informações e definições sobre uma instância do Internet Explorer. Se essas definições forem alteradas ou se for adicionado um novo ShellBrowser, este ShellBrowser pode adquirir controlo total sobre o Internet Explorer, adicionando funcionalidades como, por exemplo, barras de ferramentas, menus e botões.

WebBrowser do Internet Explorer

Controle as alterações efectuadas à instância WebBrowser do Internet Explorer. O WebBrowser do Internet Explorer contém informações e definições sobre uma instância do Internet Explorer. Se essas definições forem alteradas ou se for adicionado um novo WebBrowser, este WebBrowser pode adquirir controlo total sobre o Internet Explorer, adicionando funcionalidades como, por exemplo, barras de ferramentas, menus e botões.

Rotinas de Pesquisa de URL do Internet Explorer

Controle as alterações efectuadas à Rotina de Pesquisa de URL do Internet Explorer. As Rotinas de Pesquisa de URL são utilizadas quando digita um endereço na área de endereço do browser sem um protocolo como http:// ou ftp:// no endereço. Quando é introduzido um desses endereços, o browser pode utilizar a função UrlSearchHook para pesquisar na Internet e encontrar a localização introduzida.

URLs do Internet Explorer

Controle as alterações aos URLs predefinidos do Internet Explorer. Isto impede que spyware ou outros programas potencialmente indesejados alterem as definições do browser sem a sua permissão.

Restrições do Internet Explorer

Controle as restrições do Internet Explorer, que permitem aos administradores dos sistemas impedir que um utilizador altere a home page ou outras opções do Internet Explorer. Estas opções só são apresentadas se forem definidas intencionalmente pelo administrador.

Zonas de Segurança do Internet Explorer

Controle as zonas de segurança do Internet Explorer. O Internet Explorer tem quatro zonas de segurança predefinidas: Internet, Intranet local, Sites fidedignos e Sites restritos. Cada zona de segurança tem a sua própria definição de segurança, que é predefinida ou personalizada. As zonas de segurança são um bom alvo para alguns programas de spyware ou outros programas potencialmente indesejados, uma vez que a redução do nível de segurança permite a esses programas ultrapassar os alertas de segurança e actuar sem serem detectados.

Sites Fidedignos do Internet Explorer

Controle os sites fidedignos do Internet Explorer. A lista de sites fidedignos é um directório que inclui os Web sites nos quais confia. Alguns programas de spyware ou outros programas potencialmente indesejados têm esta lista como alvo, uma vez que proporciona um método que permite confiar em sites suspeitos sem a permissão do utilizador.

Política do Internet Explorer

Controle as políticas do Internet Explorer. Estas definições são normalmente alteradas pelos administradores do sistema, mas podem ser exploradas por programas de spyware. As alterações podem evitar que defina uma Home page diferente ou podem ocultar a visualização de separadores na caixa de diálogo Opções da Internet do menu Ferramentas.

Utilizar a análise de scripts

Um script pode criar, copiar ou eliminar ficheiros. Pode também abrir o Registo do Windows.

A análise de scripts impede automaticamente a execução de scripts conhecidos e prejudiciais no seu computador.

Desactivar a análise de scripts

Se desactivar a análise de scripts, não serão detectadas quaisquer execuções de scripts suspeitas.

Para desactivar a análise de scripts:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção de análise de scripts**, clique em **Desligado**.

Permitir a análise de scripts

A análise de scripts avisa o utilizador se da execução de um script resultar a criação, cópia ou eliminação de ficheiros ou a abertura do Registo do Windows.

Para activar a análise de scripts:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção de análise de scripts**, clique em **Ligado**.

Utilizar a protecção do correio electrónico

A protecção de correio electrónico detecta e impede ameaças nas mensagens e anexos de correio de electrónico a receber (POP3) e a enviar (SMTP), incluindo vírus, Troianos, worms, spyware, adware e outra ameaças.

Desactivar a protecção do correio electrónico

Se desactivar a protecção do correio electrónico, as potenciais ameaças existentes nas mensagens e anexos de correio electrónico a receber (POP3) e a enviar (SMTP) não são detectadas.

Para desactivar a protecção do correio electrónico:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Correio electrónico & IM**.
3. Em **Protecção do correio electrónico**, clique em **Desligado**.

Activar a protecção do correio electrónico

A protecção do correio electrónico detecta ameaças em mensagens e anexos de correio electrónico a receber (POP3) e a enviar (SMTP).

Para activar a protecção do correio electrónico:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Correio electrónico & IM**.
3. Em **Protecção do correio electrónico**, clique em **Ligado**.

Configurar a protecção do correio electrónico

As opções de protecção do correio electrónico permitem analisar as mensagens de correio electrónico a receber, as mensagens de correio electrónico a enviar e worms. Os worms replicam-se e consomem recursos do sistema, diminuindo o desempenho ou parando tarefas. Os worms podem enviar cópias de si próprios através de mensagens de correio electrónico. Por exemplo, podem tentar encaminhar mensagens de correio electrónico para os contactos existentes no livro de endereços.

Configurar a protecção do correio electrónico

As opções de protecção do correio electrónico permitem analisar as mensagens de correio electrónico a receber, as mensagens de correio electrónico a enviar e worms.

Para configurar a protecção do correio electrónico:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Correio electrónico & IM**.
3. Em **Protecção do correio electrónico**, clique em **Avançado**.
4. Marque ou desmarque as seguintes caixas de verificação:
   - **Analisar mensagens de correio electrónico a receber**: As mensagens a receber (POP3) são analisadas para detecção de potenciais ameaças.
   - **Analisar mensagens de correio electrónico a enviar**: As mensagens a enviar (SMTP) são analisadas para detecção de potenciais ameaças.
   - **Active o WormStopper**. O WormStopper bloqueia worms em mensagens de correio electrónico.
5. Clique em **OK**.

Utilizar a protecção de mensagens instantâneas

A protecção de mensagens instantâneas detecta ameaças existentes nos anexos da mensagens instantâneas a receber.

Desactivar a protecção de mensagens instantâneas

Se desactivar a protecção de mensagens instantâneas, as ameaças existentes em anexos de mensagens instantâneas não serão detectadas.

Para desactivar a protecção de mensagens instantâneas:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Correio electrónico & IM**.
3. Em **Protecção de mensagens instantâneas**, clique em **Desligado**.

Activar a protecção de mensagens instantâneas

A protecção de mensagens instantâneas detecta ameaças existentes nos anexos da mensagens instantâneas a receber.

Para activar a protecção de mensagens instantâneas:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Correio electrónico & IM**.
3. Em **Protecção de mensagens instantâneas**, clique em **Ligado**.

CAPÍTULO 15

Analisar o Computador Manualmente

Pode procurar vírus e outras ameaças em unidades de disco rígido, disquetes e em ficheiros e pastas individuais. Quando o VirusScan encontra um ficheiro suspeito, tenta limpá-lo, excepto se for um programa potencialmente indesejado. Se o VirusScan não conseguir limpar o ficheiro, poderá colocá-lo em quarentena ou eliminá-lo.

Neste capítulo

Análise manual

Pode efectuar manualmente uma análise a qualquer momento. Por exemplo, se acabou de instalar o VirusScan, pode executar uma análise para se certificar de que o seu computador não tem vírus ou outras ameaças. Se tiver desactivado a análise em tempo real, pode executar uma análise para se certificar de que o computador continua seguro.

Analisar com definições manuais de análise

Este tipo de análise utiliza as definições de análise manuais especificadas pelo utilizador. O VirusScan analisa ficheiros comprimidos no seu interior (.zip, .cab, etc.), mas considera um ficheiro comprimido como um ficheiro. Para além disso, o número de ficheiros analisado pode variar se tiver eliminado os ficheiros temporários da Internet desde a última análise.

Para analisar com as definições manuais de análise:

1. No Menu Básico, clique em **Analisar**. Quando a análise terminar, aparece um resumo que indica o número de itens analisados e detectados, o número de itens limpos e a data da última análise efectuada.
2. Clique em **Concluir**.

Tópicos relacionados

- Configurar análises manuais (página 94)

Analisar sem utilizar definições de análise manuais

Este tipo de análise não utiliza as definições de análise manuais especificadas pelo utilizador. O VirusScan analisa ficheiros comprimidos no seu interior (.zip, .cab, etc.), mas considera um ficheiro comprimido como um ficheiro. Para além disso, o número de ficheiros analisado pode variar se tiver eliminado os ficheiros temporários da Internet desde a última análise.

Para analisar sem as definições de análise manuais:

1. No Menu Avançado, clique em **Página Inicial**.
2. No painel Página Inicial, clique em **Analisar**.
3. Em **Localizações a analisar**, seleccione as caixas de verificação que se encontram junto dos ficheiros, pastas e unidades que pretende analisar.
4. Em **Opções**, seleccione as caixas de verificação que se encontram junto do tipo de ficheiros que pretende analisar.
5. Clique em **Analisar Agora**. Quando a análise terminar, aparece um resumo que indica o número de itens analisados

e detectados, o número de itens limpos e a data da última análise efectuada.

6 Clique em **Concluir**.

Nota: Estas opções não são guardadas.

Analisar no Explorador do Windows

Pode procurar vírus e outras ameaças em ficheiros, pastas ou unidades seleccionadas dentro do Explorador do Windows.

Para analisar ficheiros no Explorador do Windows:

1 Abra o Explorador do Windows.

2 Clique com o botão direito do rato na unidade, pasta ou ficheiro que pretende analisar e, em seguida, clique em **Analisar**. Todas as opções de análise predefinidas são seleccionadas para a execução de uma análise completa.

Configurar análises manuais

Quando efectuar uma análise manual ou agendada, pode especificar o tipo de ficheiros a analisar, as localizações a analisar e a data de execução da análise.

Configurar o tipo de ficheiros a analisar

Pode configurar o tipo de ficheiros a analisar.

Para configurar o tipo de ficheiros a analisar:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção Antivírus**, clique em **Avançado**.
4. No painel Protecção Antivírus, clique em **Análise Manual**.
5. Marque ou desmarque as seguintes caixas de verificação:
   - **Análise de vírus desconhecidos utilizando heurística**: É efectuada a correspondência entre os ficheiros se as assinaturas de vírus conhecidos, com vista à detecção de indícios de vírus não identificados. Esta opção fornece a análise mais completa, mas é geralmente mais lenta do que uma análise normal.
   - **Analisar ficheiros .zip e outros ficheiros de arquivo**: Detecta e remove vírus existentes em ficheiros .zip e noutros ficheiros de arquivo. Por vezes, os autores colocam os vírus num ficheiro .zip e depois inserem esse ficheiro .zip noutro ficheiro .zip, para tentarem enganar os programas antivírus.
   - **Analisar a existência de spyware e programas potencialmente indesejados**: Programas de spyware, adware e outros programas potencialmente susceptíveis de recolha e transmissão de dados sem permissão são detectados e removidos.
   - **Analisar e remover cookies de registo**: Os cookies potencialmente susceptíveis de recolha e transmissão de dados sem permissão são detectados e removidos. Um cookie identifica os utilizadores quando estes visitam uma página Web.
   - **Analisar a existência de rootkits e outros programas furtivos**: Detecta e remove qualquer rootkit ou outro programa que se esconda do Windows.
6. Clique num dos seguintes botões:
   - **Todos os ficheiros (recomendado)**: Todos os tipos de ficheiros utilizados pelo computador são analisados. Utilize esta opção para obter a análise mais completa.
   - **Apenas ficheiros de programas e documentos**: Apenas são analisados documentos e ficheiros de programas.

7 Clique em **OK**.

Configurar as localizações a analisar

Pode configurar as localizações a analisar para efectuar análises manuais ou agendadas.

Para configurar o local a analisar:

1 No Menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador & Ficheiros**.

3 Em **Protecção Antivírus**, clique em **Avançado**.

4 No painel Protecção Antivírus, clique em **Análise Manual**.

5 Em **Localização Predefinida a Analisar**, seleccione os ficheiros, pastas e unidades que pretende analisar.

Para obter uma análise o mais completa possível, assegure-se de que selecciona **Ficheiros críticos**.

6 Clique em **OK**.

Análises agendadas

Pode agendar análises para verificar exaustivamente a existência de vírus e outras ameaças no seu computador, em intervalos especificados.

Para agendar uma análise:

1 No Menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador & Ficheiros**.

3 Em **Protecção Antivírus**, clique em **Avançado**.

4 No painel Protecção Antivírus, clique em **Análise Agendada**.

5 Assegure-se de que a opção **Activar análise agendada** está seleccionada.

6 Seleccione a caixa de verificação situada junto do dia da semana em que será efectuada a análise.

7 Seleccione os valores nas listas de horas de início para especificar a hora de início.

8 Clique em **OK**.

Sugestão: Para utilizar a agenda predefinida, clique em **Repor**.

CAPÍTULO 16

Administrar o VirusScan

Pode remover itens das listas fidedignas, gerir programas, cookies e ficheiros em quarentena, visualizar eventos e registos e reportar actividades suspeitas à McAfee.

Neste capítulo

Gerir listas fidedignas

Quando confia numa Protecção do Sistema, num programa, num protecção de sobrecarga da memória temporária ou num programa de correio electrónico, o item é adicionado à lista fidedigna, para que não volte a ser detectado.

Se tiver confiado num programa por engano ou se quiser que o programa seja detectado, tem de o remover desta lista.

Gerir listas fidedignas

Quando confia numa Protecção do Sistema, num programa, num protecção de sobrecarga da memória temporária ou num programa de correio electrónico, o item é adicionado à lista fidedigna, para que não volte a ser detectado.

Se tiver confiado num programa por engano ou se quiser que o programa seja detectado, tem de o remover desta lista.

Para remover itens das listas fidedignas:

1. No Menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador & Ficheiros**.
3. Em **Protecção Antivírus**, clique em **Avançado**.
4. No painel Protecção Antivírus, clique em **Listas Fidedignas**.
5. Na lista, seleccione uma Protecção do Sistema, um programa, uma protecção de sobrecarga da memória temporária ou um programa de correio electrónico de confiança para visualizar os respectivos itens e estado de confiança.
6. Em **Detalhes**, visualize informações sobre o item.
7. Em **Quero**, clique numa acção.
8. Clique em **OK**.

Gerir programas, cookies e ficheiros em quarentena

Os programas, cookies e ficheiros em quarentena podem ser restaurados, eliminados ou enviados à McAfee para análise.

Restaurar programas, cookies e ficheiros em quarentena

Se necessário, pode restaurar programas, cookies e ficheiros em quarentena.

Para restaurar programas, cookies e ficheiros em quarentena:

1. No Menu Avançado, clique em **Restaurar**.
2. No painel Restaurar, clique em **Programas e Cookies** ou **Ficheiros**, consoante o que for adequado.
3. Seleccione os programas, cookies ou ficheiros em quarentena que pretende restaurar.
4. Para obter mais informações sobre o vírus em quarentena, clique no respectivo nome de detecção em **Detalhes**. Aparece a Biblioteca de Informações sobre Vírus com uma descrição do vírus.
5. Em **Quero**, clique em **Restaurar**.

Remover programas, cookies e ficheiros em quarentena

Pode remover programas, cookies e ficheiros em quarentena.

Para remover programas, cookies e ficheiros em quarentena:

1. No Menu Avançado, clique em **Restaurar**.
2. No painel Restaurar, clique em **Programas e Cookies** ou **Ficheiros**, consoante o que for adequado.
3. Seleccione os programas, cookies ou ficheiros em quarentena que pretende restaurar.
4. Para obter mais informações sobre o vírus em quarentena, clique no respectivo nome de detecção em **Detalhes**. Aparece a Biblioteca de Informações sobre Vírus com uma descrição do vírus.
5. Em **Quero**, clique em **Remover**.

Enviar programas, cookies e ficheiros em quarentena para a McAfee

Pode enviar programas, cookies e ficheiros em quarentena à McAfee para análise.

Nota: Se o ficheiro em quarentena que está a enviar exceder um tamanho máximo, pode ser rejeitado. Na maioria dos casos, isto não acontece.

Para enviar programas ou ficheiros em quarentena à McAfee:

1. No Menu Avançado, clique em **Restaurar**.
2. No painel Restaurar, clique em **Programas e Cookies** ou **Ficheiros**, consoante o que for adequado.
3. Seleccione os programas, cookies ou ficheiros em quarentena que pretende enviar à McAfee.
4. Para obter mais informações sobre o vírus em quarentena, clique no respectivo nome de detecção em **Detalhes**. Aparece a Biblioteca de Informações sobre Vírus com uma descrição do vírus.
5. Em **Quero**, clique em **Enviar à McAfee**.

Ver eventos e registos recentes

Os eventos e registos recentes apresentam eventos de todos os produtos da McAfee instalados.

Em Eventos Recentes, pode ver os últimos 30 eventos significativos que ocorreram no computador. Pode restaurar programas bloqueados, reactivar a análise em tempo real e confiar em protecções de sobrecarga da memória.

Pode também ver registos, que guardam todos os eventos ocorridos nos últimos 30 dias.

Ver eventos

Em Eventos Recentes, pode ver os últimos 30 eventos significativos que ocorreram no computador. Pode restaurar programas bloqueados, reactivar a análise em tempo real e confiar em protecções de sobrecarga da memória.

Para ver eventos:

1. No Menu Avançado, clique em **Relatórios & Registos**.
2. No painel Relatórios & Registos, clique em **Eventos Recentes**.
3. Seleccione o evento que pretende visualizar.
4. Em **Detalhes**, visualize informações sobre o evento.
5. Em **Quero**, clique numa acção.

Ver registos

Os registos guardam todos os eventos ocorridos nos últimos 30 dias.

Para ver registos:

1. No Menu Avançado, clique em **Relatórios & Registos**.
2. No painel Relatórios & Registos, clique em **Eventos Recentes**.
3. No painel Eventos Recentes, clique em **Ver Registo**.
4. Seleccione o tipo de registo que pretende visualizar e, em seguida, seleccione um registo.
5. Em **Detalhes**, visualize informações sobre o registo.

Reportar automaticamente informações anónimas

Pode enviar anonimamente informações de registo de vírus, programas potencialmente indesejados e hackers à McAfee. Esta opção só está disponível durante a instalação.

Não são recolhidas informações de identificação pessoal.

Comunicar à McAfee

Pode enviar informações de registo de vírus, programas potencialmente indesejados e hackers à McAfee. Esta opção só está disponível durante a instalação.

Para reportar automaticamente informações anónimas:

1. Durante a instalação do VirusScan, aceite a predefinição **Enviar informações anónimas**.
2. Clique em **Seguinte**.

Noções básicas sobre alertas de segurança

Se a análise em tempo real detectar uma ameaça, aparece um aviso. No caso da maioria dos vírus, Troianos, scripts e worms, a análise em tempo real tenta limpar o ficheiro e avisa o utilizador. Para Protecções do Sistema e programas potencialmente indesejados, a análise em tempo real detecta o ficheiro ou a alteração e avisa o utilizador. Para actividades de sobrecarga da memória temporária, registo de cookies e script, a análise em tempo real bloqueia automaticamente a actividade e avisa o utilizador.

Estes avisos podem ser agrupados em três tipos básicos:

- Alerta vermelho
- Alerta amarelo
- Alerta verde

Pode então escolher como pretende gerir ficheiros detectados, correio electrónico detectado, scripts suspeitos, worms potenciais, programas potencialmente indesejados, Protecções do Sistema e protecções de sobrecarga da memória.

Gerir avisos

A McAfee utiliza um conjunto de avisos para o ajudar a gerir a sua segurança. Estes avisos podem ser agrupados em três tipos básicos:

- Alerta vermelho
- Alerta amarelo
- Alerta verde

Alerta vermelho

Um alerta vermelho exige uma resposta por parte do utilizador. Em alguns casos, a McAfee não consegue determinar como responder automaticamente a uma actividade em particular. Nesses casos, o alerta vermelho descreve a actividade em questão e dá-lhe uma ou mais opções à escolha.

Alerta amarelo

Um alerta amarelo é uma notificação não crítica que, normalmente, requer uma resposta por parte do utilizador. O alerta amarelo descreve a actividade em questão e dá-lhe uma ou mais opções à escolha.

Alerta verde

Na maioria dos casos, um alerta verde inclui informações básicas sobre um evento e não requer qualquer resposta.

Configurar opções de alerta

Se optar por não mostrar novamente um aviso e, posteriormente, mudar de ideias, pode voltar atrás e configurar o aviso para ser novamente apresentado. Para obter mais informações sobre opções de configuração de alertas, consulte a sua documentação do SecurityCenter.

CAPÍTULO 17

Ajuda Adicional

Este capítulo apresenta perguntas frequentes e cenários de resolução de problemas.

Neste capítulo

Perguntas Mais Frequentes

Esta secção inclui respostas às perguntas mais frequentes.

Foi detectada uma ameaça, o que devo fazer?

A McAfee utiliza avisos para o ajudar a gerir a sua segurança. Estes avisos podem ser agrupados em três tipos básicos:

- Alerta vermelho
- Alerta amarelo
- Alerta verde

Pode então escolher como pretende gerir ficheiros detectados, correio electrónico detectado, scripts suspeitos, worms potenciais, programas potencialmente indesejados, Protecções do Sistema e protecções da capacidade da memória intermédia excedida.

Para obter mais informações sobre como gerir determinadas ameaças, consulte a Biblioteca de Informações sobre Vírus em: http://us.mcafee.com/virusInfo/default.asp?affid=.

Tópicos relacionados

- Noções básicas sobre alertas de segurança (página 103)

Posso utilizar o VirusScan com os browsers Netscape, Firefox e Opera?

Pode utilizar o Netscape, Firefox e Opera como browser da Internet predefinido, mas tem de ter o Microsoft ∃ Internet Explorer 6.0 ou posterior instalado no computador.

Preciso de estar ligado à Internet para executar uma análise?

Não tem de estar ligado à Internet para executar uma análise, mas deve fazê-lo pelo menos uma vez por semana para receber as actualizações da McAfee.

O VirusScan analisa os anexos do correio electrónico?

Se tiver a análise em tempo real e a protecção de correio electrónico activadas, todos os anexos são analisados quando a mensagem de correio electrónico chega.

O VirusScan analisa ficheiros comprimidos?

O VirusScan analisa ficheiros .zip e outros ficheiros de arquivo.

Porque é que ocorrem erros na análise do correio electrónico de saída?

Durante a análise do correio electrónico a enviar, podem ocorrer os seguintes tipos de erros:

- Erro de protocolo. O servidor de correio electrónico rejeitou uma mensagem.
  Se ocorrer um erro de protocolo ou de sistema, as restantes mensagens de correio electrónico da sessão actual serão processadas e enviadas para o servidor.
- Erro de ligação. A ligação ao servidor de correio electrónico foi interrompida.
  Se ocorrer um erro de ligação, certifique-se de que o computador está ligado à Internet e, em seguida, tente enviar novamente a mensagem a partir da lista de itens **Enviados** do seu programa de correio electrónico.
- Erro de sistema. Ocorreu uma falha no processamento de um ficheiro ou outro erro do sistema.
- Erro de ligação SMTP encriptada. Foi detectada uma ligação SMTP encriptada no seu programa de correio electrónico.
  Se ocorrer um erro de ligação SMTP encriptada, desactive essa ligação no seu programa de correio electrónico para garantir que as mensagens de correio electrónico são analisadas.

Se o tempo limite for excedido durante o envio de mensagens de correio electrónico, desactive a análise do correio electrónico a enviar ou desactive a ligação SMTP encriptada no seu programa de correio electrónico.

Tópicos relacionados

- Configurar a protecção do correio electrónico (página 88)

Resolução de problemas

Esta secção ajuda-o a resolver problemas gerais que podem ocorrer.

Impossível limpar ou eliminar um vírus

Para alguns vírus, tem de limpar manualmente o computador. Experimente reiniciar o computador e efectuar novamente a análise.

Se o computador não conseguir limpar ou eliminar um vírus, consulte a Biblioteca de Informações sobre Vírus em: http://us.mcafee.com/virusInfo/default.asp?affid=.

Para obter mais ajuda, consulte o Suporte a Clientes da McAfee no Web site da McAfee.

Nota: Não é possível limpar vírus de CD-ROMs, DVDs e disquetes protegidas contra escrita.

Depois de reiniciar, continua a não conseguir remover um item

Depois de analisar e remover itens, algumas situações exigem que reinicie o computador.

Se o item não for removido depois de reiniciar o computador, envie o ficheiro à McAfee.

Nota: Não é possível limpar vírus de CD-ROMs, DVDs e disquetes protegidas contra escrita.

Tópicos relacionados

- Gerir programas, cookies e ficheiros em quarentena (página 99)

Componentes em falta ou danificados

Algumas situações podem conduzir a uma instalação incorrecta do VirusScan:

- O seu computador não possui espaço em disco ou memória suficiente. Certifique-se de que o seu computador reúne os requisitos de sistema necessários para executar este software.
- O browser da Internet está configurado incorrectamente.
- A sua ligação à Internet tem falhas. Verifique a sua ligação ou tente ligar novamente mais tarde.
- Faltam ficheiros ou a instalação falhou.

A melhor solução será resolver estas questões potenciais e, em seguida, reinstalar o VirusScan.

CAPÍTULO 18

McAfee Personal Firewall

O Personal Firewall proporciona uma protecção avançada para o computador e dados pessoais. O Personal Firewall cria uma barreira entre o computador e a Internet, monitorizando discretamente actividades suspeitas no tráfego da Internet.

Neste capítulo

Funcionalidades

O Personal Firewall assegura uma protecção de entrada e de saída completa, confia automaticamente nos programas bem intencionados e ajuda a bloquear spyware, cavalos de Tróia e programas de registo da actividade do teclado. O Personal Firewall permite-lhe defender-se contra as pesquisas e os ataques dos hackers, monitoriza a actividade na rede e na Internet, alerta-o para eventos hostis e suspeitos, fornece informações detalhadas sobre o tráfego na Internet e complementa as defesas antivírus.

Níveis de protecção padrão e personalizados

Proteja-se contra intrusos e actividade suspeita, utilizando a protecção predefinida do Personal Firewall ou personalizando-a, de acordo com as suas necessidades em termos de segurança.

Recomendações em tempo real

Receba recomendações de uma forma dinâmica, que o ajudam a determinar se deve permitir o acesso de programas à Internet ou se deve confiar no tráfego da rede.

Gestão de acesso inteligente para programas

Pode gerir o acesso de programas à Internet através de alertas e registos de eventos ou configurar permissões de acesso para programas específicos a partir do painel Permissões do Programa da firewall.

Protecção de jogos

Evite que avisos relativos a tentativas de intrusão e actividades suspeitas o distraiam durante um jogo em ecrã inteiro e configure a firewall para apresentar os avisos quando o jogo terminar.

Protecção durante o arranque do computador

Antes de iniciar o Windows, a firewall protege o computador de tentativas de intrusão, programas indesejados e tráfego da rede.

Controlo da porta de serviço do sistema

As portas de serviço de sistema podem funcionar como uma backdoor para o computador. O Personal Firewall permite-lhe criar e gerir portas de serviço do sistema abertas e fechadas requeridas por alguns programas.

Gerir ligações do computador

Pode confiar ou banir ligações remotas e endereços IP de ligação ao seu computador

Integração de informações de HackerWatch

O HackerWatch é um centro de informações de segurança que regista padrões globais de invasão e intrusão e disponibiliza as informações mais actualizadas sobre os programas instalados no seu computador. Pode ver estatísticas globais de eventos de segurança e de portas da Internet.

Bloquear a firewall

Bloqueia instantaneamente todo o tráfego de entrada e saída da Internet entre o computador e a Internet.

Restaurar a firewall

Restaura instantaneamente as definições de protecção originais da firewall. Se o Personal Firewall manifestar um comportamento indesejável que não consegue corrigir, pode repor as suas predefinições.

Detecção avançada de cavalos de Tróia

Combina a gestão de ligações de programas com uma base de dados avançada para detectar e bloquear aplicações potencialmente maliciosas, tais como cavalos de Tróia, impedindo-as de aceder à Internet e transmitir dados pessoais.

Registo de eventos

Especifique se deseja activar ou desactivar o registo e, no caso de o activar, que tipo de eventos pretende registar. O registo de eventos permite ver os últimos eventos de entrada e de saída. Também pode ver eventos de intrusões detectados.

Monitorizar tráfego da Internet

Analisa mapas gráficos de fácil leitura que mostram a origem dos ataques hostis e o tráfego mundial. Além disso, localiza informações detalhadas do proprietário e dados geográficos dos endereços IP de origem. Analisa ainda o tráfego de entrada e de saída, monitoriza a largura de banda dos programas e a actividade dos programas.

Prevenção de intrusões

Proteja a sua privacidade precavendo-se contra a invasão de eventuais ameaças da Internet. Através de uma funcionalidade semelhante à heurística, a McAfee fornece uma camada de protecção terciária através do bloqueio de itens que apresentem sintomas de ataques ou características de tentativas de intrusão.

Análise de tráfego sofisticada

Analisa o tráfego de entrada e de saída da Internet, bem como as ligações dos programas, incluindo as que estão em processo de escuta activa à procura de ligações abertas. Desta forma, poderá ver e actuar sobre programas que possam estar vulneráveis a intrusões.

Iniciar a firewall

Assim que a firewall for instalada, o computador fica protegido contra intrusões e tráfego de rede indesejado. Além disso, está pronto para lidar com alertas e gerir o acesso de entrada e saída de programas conhecidos e desconhecidos da Internet. As opções Recomendações Inteligentes e nível de segurança Padrão são activadas automaticamente.

Embora possa desactivar a Firewall no painel Configuração de Internet & Rede, o computador deixa de estar protegido contra intrusões e tráfego de rede indesejado, não sendo possível poder gerir eficazmente as ligações de entrada e saída da Internet. Se tiver de desactivar a protecção por firewall, faça-o temporariamente e apenas quando necessário. Também pode activar a firewall no painel Configuração de Internet & Rede.

A firewall desactiva automaticamente a Firewall do Windows® e fica como firewall predefinida.

Nota: Para configurar a firewall, abra o painel Configuração de Internet e Rede.

Iniciar a protecção por firewall

A activação da protecção por firewall defende o computador de intrusões e de tráfego de rede indesejado e permite-lhe gerir ligações de entrada e saída da Internet.

Para activar a protecção por firewall:

1. No painel McAfee SecurityCenter, efectue uma das seguintes acções:
   - Clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
   - Clique em **Menu Avançado**, **Configurar** no painel **Página Inicial** e, em seguida, aponte para **Internet e Rede**.
2. No painel **Configuração de Internet e Rede**, em **Protecção de firewall**, clique em **Ligado**.

Parar a protecção por firewall

Ao desactivar a protecção por firewall, o computador fica vulnerável a intrusões e tráfego de rede indesejado. Se a protecção por firewall estiver desactivada, não pode gerir as ligações de entrada e saída da Internet.

Para desactivar a protecção por firewall:

1. No painel McAfee SecurityCenter, efectue uma das seguintes acções:
   - Clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
   - Clique em **Menu Avançado**, **Configurar** no painel **Página Inicial** e, em seguida, aponte para **Internet e Rede**.
2. No painel **Configuração de Internet e Rede**, em **Protecção de firewall**, clique em **Desligado**.

Utilizar alertas

A firewall utiliza uma série de alertas que o ajudam a gerir a segurança. Estes alertas podem ser agrupados em quatro tipos básicos.

- Alerta de Bloqueio de Cavalos de Tróia
- Alerta vermelho
- Alerta amarelo
- Alerta verde

Os alertas podem conter também informações que ajudam o utilizador a decidir como lidar com alertas ou obter informações sobre programas instalados no computador.

Acerca dos alertas

A firewall dispõe de quatro tipos básicos de alerta. Alguns alertas incluem também informações que o ajudam a conhecer ou obter informações sobre programas instalados no computador.

Alerta de Bloqueio de Cavalos de Tróia

Um cavalo de Tróia aparenta ser um programa legítimo, mas pode interromper, danificar e fornecer acesso não autorizado ao seu computador. O alerta de cavalos de Tróia é apresentado quando a firewall detecta, e depois bloqueia, um cavalo de Tróia e recomenda a pesquisa de outras ameaças. Este alerta ocorre em todos os níveis de segurança, excepto em Aberta ou quando a opção Recomendações Inteligentes está desactivada.

Alerta vermelho

O tipo mais comum de alerta é o vermelho, que normalmente requer uma resposta do utilizador. Uma vez que a firewall não consegue, nalguns casos, determinar automaticamente um processo específico para a actividade de um programa ou para um evento da rede, o alerta descreve primeiro a actividade do programa ou o evento de rede e depois apresenta uma ou mais opções que deve adoptar. Se a opção Recomendações Inteligentes estiver activada, os programas são adicionados no painel Permissões do Programa.

As seguintes descrições de alerta são, normalmente, as mais encontradas:

- **Programa requer acesso à Internet**: A firewall detecta um programa que tenta aceder à Internet.
- **O programa foi modificado**: A firewall detecta um programa que foi de algum modo alterado, provavelmente devido a uma actualização online.
- **Programa Bloqueado**: A firewall bloqueia um programa porque está indicado no painel Permissões do Programa.

Consoante as definições e a actividade do programa ou evento de rede, normalmente são encontradas as seguintes opções:

- **Conceder acesso**: Permite que um programa instalado no computador tenha acesso à Internet. A regra é adicionada à página Permissões do Programa.
- **Conceder acesso uma vez**: Permite que um programa instalado no computador tenha acesso temporário à Internet. Por exemplo, a instalação de um novo programa pode requerer apenas um acesso à Internet.
- **Bloquear acesso**: Impede o acesso de um programa à Internet.
- **Conceder acesso apenas de saída**: Permite apenas uma ligação de saída à Internet. Este alerta é normalmente apresentado quando estão definidos os níveis de segurança Apertada e Invisível.
- **Confiar nesta rede**: Permite o tráfego de entrada e saída a partir de uma rede. A rede é adicionada à secção Endereços IP de Confiança.
- **Não confiar agora nesta rede**: Bloqueia o tráfego de entrada e saída a partir de uma rede.

Alerta amarelo

O alerta amarelo é uma notificação não crítica que o informa sobre um evento de rede detectado pela firewall. Por exemplo, o alerta **Nova Rede Detectada** é apresentado quando a firewall é executada pela primeira vez ou quando um computador com uma firewall instalada é ligado a uma nova rede. Pode optar por confiar ou não na rede. Se a rede for de confiança, a firewall permite o tráfego a partir de outro computador na rede e é adicionado a Endereços IP de Confiança.

Alerta verde

Na maioria dos casos, um alerta verde fornece informações básicas sobre um evento, não sendo necessária uma resposta. Os alertas verdes normalmente ocorrem quando os níveis de segurança Padrão, Apertada, Invisível e Bloquear estão definidos. As descrições de alerta verde são as seguintes:

- **O programa foi Modificado**: Informa-o que um programa ao qual permitiu acesso à Internet anteriormente foi modificado. Pode bloquear o programa, mas se não o fizer, o alerta desaparece e o programa continua a dispor de acesso à Internet.
- **O Programa Concedeu Acesso à Internet**: Informa-o que foi concedido acesso à Internet a um programa. Pode bloquear o programa, mas se não o fizer, o alerta desaparece e o programa continua a aceder à Internet.

Assistência ao utilizador

Muitos alertas da firewall contêm informações adicionais que o ajudam a gerir a segurança do computador, que incluem:

- **Obter mais informações sobre este programa**: Inicie o Web site de segurança global da McAfee para obter informações sobre um programa detectado pela firewall no computador.
- **Informar a McAfee sobre este programa**: Enviar informações à McAfee sobre um ficheiro desconhecido detectado pela firewall no computador.
- **A McAfee recomenda**: Conselhos sobre como lidar com alertas. Por exemplo, um alerta pode recomendar que seja concedido acesso a um programa.

Gerir alertas informativos

A firewall permite-lhe mostrar ou ocultar alertas informativos durante determinados eventos.

Apresentar alertas durante jogos

Por predefinição, a firewall impede a presença de alertas informativos durante jogos em ecrã total. No entanto, pode configurar a firewall para apresentar alertas informativos durante jogos se forem detectadas tentativas de intrusão ou actividade suspeita.

Para mostrar alertas durante o jogo:

1. No painel Tarefas Comuns, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Alertas**.
4. Clique em **Avançadas**.
5. No painel **Opções de Alerta**, seleccione **Mostrar alertas informativos quando o modo de jogo for detectado**.

Ocultar alertas informativos

Os alertas informativos notificam-no sobre eventos que não requerem a sua resposta imediata.

Para ocultar alertas informativos:

1. No painel Tarefas Comuns, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Alertas**.
4. Clique em **Avançadas**.
5. No painel **Configuração do SecurityCenter**, clique em **Alertas Informativos**.
6. No painel **Alertas Informativos**, efectue uma das seguintes acções:
   - Seleccione o tipo de alerta que pretende ocultar.
   - Seleccione **Ocultar alertas informativos** para ocultar todos os alertas informativos.
7. Clique em **OK**.

CAPÍTULO 19

Configurar a protecção por firewall

A firewall dispõe de vários métodos que permitem gerir a segurança e personalizar a maneira como pretende responder a eventos e alertas de segurança.

Depois de instalar a firewall pela primeira vez, o nível de protecção é definido para a segurança Padrão. Para a maior parte dos utilizadores, esta definição vai ao encontro de todas as necessidades de segurança. Contudo, a firewall inclui outros níveis, que vão desde o nível mais restritivo até ao mais permissivo.

A firewall permite também receber recomendações sobre alertas e o acesso dos programas à Internet.

Neste capítulo

Gerir os níveis de segurança da firewall

Pode configurar os níveis de segurança para controlar o grau com que pretende gerir e responder a alertas, quando a firewall detecta tráfego de rede indesejado e ligações de entrada e saída da Internet. Por predefinição, o nível de segurança Padrão está activado.

Se o nível de segurança Padrão estiver definido e a opção Recomendações Inteligentes activada, os alertas vermelhos permitem conceder ou bloquear acesso a programas desconhecidos ou modificados. Quando forem detectados programas conhecidos, são apresentados alertas informativos verdes e o acesso é automático. Ao conceder acesso, isso permite a um programa criar ligações de saída e controlar ligações de entrada não solicitadas.

Normalmente, quanto mais restrito for um nível de segurança (Invisível e Apertada), maior será o número de opções e alertas apresentados e que, por sua vez, devem ser geridos pelo utilizador.

A firewall dispõe de seis níveis de segurança. Começando pelo nível mais restritivo até ao mais permissivo, estes níveis incluem:

- **Bloquear**: Bloqueia todas as ligações à Internet.
- **Invisível**: Bloqueia todas as ligações de entrada da Internet.
- **Apertada**: Os alertas requerem a sua resposta a todos os pedidos de ligação de entrada e saída da Internet.
- **Padrão**: Os alertas notificam-no quando programas novos ou desconhecidos solicitam acesso à Internet.
- **Confiante**: Concede acesso a todas as ligações de entrada e de saída da Internet e adiciona-as automaticamente ao painel Permissões do Programa.
- **Aberta**: Concede acesso a todas as ligações de entrada e saída à Internet.

A firewall permite também repor de imediato o nível de segurança em Padrão no painel Restaurar Predefinições de Protecção por Firewall.

Definir o nível de segurança para Bloquear

Ao definir o nível de segurança da firewall para Bloquear, todas as ligações de entrada e saída são bloqueadas, incluindo o acesso a Web sites, correio electrónico e actualizações de segurança. Este nível de segurança é o mesmo que remover a ligação à Internet. Pode utilizar esta definição para bloquear as portas que definiu como abertas no painel Serviços do Sistema. Se a opção Bloquear estiver activada, os alertas podem continuar a solicitar-lhe que bloqueie programas.

Para definir o nível de segurança da firewall para Bloquear:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, mova a barra de deslocamento para que **Bloquear** seja apresentado como o nível activado.
3. Clique em **OK**.

Definir o nível de segurança para Invisível

Se definir o nível de segurança da firewall para Invisível, todas as ligações de rede de entrada são bloqueadas, excepto portas abertas. Esta definição oculta por completo a presença do computador na Internet. Se o nível de segurança estiver definido para Invisível, a firewall alerta-o quando novos programas tentarem efectuar ligações de saída para a Internet ou receberem pedidos de ligação de entrada. Os programas bloqueados e adicionados são apresentados no painel Permissões do Programa.

Para definir o nível de segurança da firewall para Invisível:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, mova a barra de deslocamento para que **Invisível** seja apresentado como o nível activado.
3. Clique em **OK**.

Definir o nível de segurança para Apertada

Se tiver definido o nível de segurança para Apertada, a firewall informa-o se novos programas tentarem efectuar ligações de saída à Internet ou receberem pedidos de ligação de entrada. Os programas bloqueados e adicionados são apresentados no painel Permissões do Programa. Se o nível de segurança estiver definido para Apertada, um programa solicita apenas o tipo de acesso necessário nesse momento, por exemplo, acesso apenas de saída, que pode ser concedido ou bloqueado pelo utilizador. Se o programa solicitar, posteriormente, uma ligação de entrada e saída, o utilizador pode conceder acesso total ao programa a partir do painel Permissões do Programa.

Para definir o nível de segurança da firewall para Apertada:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, mova a barra de deslocamento para que **Apertada** seja apresentado como o nível activado.
3. Clique em **OK**.

Definir o nível de segurança para Padrão

Padrão é o nível de segurança predefinido e recomendado.

Se especificar o nível de segurança da firewall para Padrão, a firewall monitoriza as ligações de entrada e saída e informa-o se novos programas tentarem aceder à Internet. Os programas bloqueados e adicionados são apresentados no painel Permissões do Programa.

Para definir o nível de segurança da firewall para Padrão:

1. No painel Configuração de Internet e Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, mova o controlo de deslize para que **Padrão** seja apresentado como o nível activado.
3. Clique em **OK**.

Definir o nível de segurança para Confiante

Se definir o nível de segurança da firewall para Confiante, todas as ligações de entrada e saída são permitidas. Na opção de segurança Confiante, a firewall concede um acesso automático a todos os programas e adiciona-os à lista de programas permitidos no painel Permissões do Programa.

Para definir o nível de segurança da firewall para Confiante:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, mova a barra de deslocamento para que **Confiante** seja apresentado como o nível activado.
3. Clique em **OK**.

Configurar recomendações inteligentes para alertas

Pode configurar a firewall para incluir, excluir ou apresentar recomendações em alertas relativamente a programas que tentem aceder à Internet.

A activação de recomendações inteligentes ajuda-o a lidar com alertas. Se a opção Recomendações Inteligentes estiver activada (e o nível de segurança for Padrão), a firewall concede ou bloqueia automaticamente o acesso a programas conhecidos, informando-o e recomendando um procedimento quando detecta programas desconhecidos e potencialmente perigosos.

Se a opção Recomendações Inteligentes estiver desactivada, a firewall não concede nem bloqueia automaticamente o acesso à Internet e também não recomenda um procedimento.

Quando a firewall estiver configurada para apresentar apenas Recomendações Inteligentes, é apresentado um alerta para conceder ou bloquear o acesso, mas sugere um procedimento.

Activar recomendações inteligentes

A activação da opção Recomendações Inteligentes ajuda-o a decidir como lidar com alertas. Se a opção Recomendações Inteligentes estiver activada, a firewall concede ou bloqueia automaticamente os programas e informa-o sobre programas não reconhecidos e potencialmente perigosos.

Para activar a opção Recomendações Inteligentes:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, em **Recomendações Inteligentes**, seleccione **Activar Recomendações Inteligentes**.
3. Clique em **OK**.

Desactivar recomendações inteligentes

Se desactivar a opção Recomendações Inteligentes, os alertas deixam de apresentar ajuda sobre como lidar com alertas e como gerir o acesso a programas. Se a opção Recomendações Inteligentes estiver desactivada, a firewall continua a conceder ou bloquear acesso a programas e informa-o sobre programas não reconhecidos e potencialmente perigosos. E se detectar um novo programa que seja suspeito ou uma possível ameaça, a firewall bloqueia automaticamente o acesso do programa à Internet.

Para desactivar a opção Recomendações Inteligentes:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, em **Recomendações Inteligentes**, seleccione **Desactivar Recomendações Inteligentes**.
3. Clique em **OK**.

Apresentar apenas recomendações inteligentes

Ao activar a opção Recomendações Inteligentes, isso ajuda-o a decidir como lidar com alertas relacionados com programas não reconhecidos e potencialmente perigosos. Se a opção Recomendações Inteligentes estiver definida como **Apresentar apenas**, são apresentadas informações sobre como lidar com alertas, mas ao contrário da opção **Activar Recomendações Inteligentes**, as recomendações apresentadas não são aplicadas automaticamente e o acesso aos programas não é concedido nem bloqueado de modo automático. Em vez disso, os alertas fornecem recomendações que o ajudam a decidir se deve conceder acesso ou bloquear programas.

Para apresentar apenas a opção Recomendações Inteligentes:

1. No painel Configuração de Internet e Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, em **Recomendações Inteligentes**, seleccione **Apresentar apenas**.
3. Clique em **OK**.

Optimizar a segurança da firewall

A segurança do computador pode ser comprometida de várias maneiras. Por exemplo, alguns programas podem tentar estabelecer ligação à Internet antes do Windows® ser iniciado. Além disso, os utilizadores experientes podem tentar aceder ao seu computador para verificar se está ligado a uma rede. A firewall permite-lhe defender-se contra ambos os tipos de intrusão, permitindo-lhe activar a protecção durante o arranque e bloquear os pedidos de ping de ICMP. A primeira definição impede que os programas acedam à Internet quando o Windows é iniciado e a segunda definição bloqueia os pedidos de ping que ajudam outros utilizadores a detectarem o computador do utilizador numa rede.

As definições de instalação padrão incluem a detecção automática das tentativas de intrusão mais comuns, tais como explorações ou ataques por Recusa de Serviço. A utilização das definições de instalação padrão garante-lhe protecção contra estes ataques e análises; no entanto, pode desactivar a detecção automática para um ou mais ataques ou análises, no painel Detecção de Intrusões.

Proteger o computador durante o arranque

A firewall pode proteger o computador durante o arranque do Windows. A protecção durante o arranque bloqueia todos os novos programas cujo acesso não tinha sido ainda concedido e que solicitam acesso à Internet. Depois da firewall ser iniciada, apresenta alertas relevantes sobre os programas que tenham solicitado acesso à Internet durante o arranque, podendo conceder ou bloquear o acesso. Para utilizar esta opção, o nível de segurança não deve estar definido para Aberta nem Bloquear.

Para proteger o computador durante o arranque:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, em Definições de Segurança, seleccione **Activar protecção durante o arranque**.
3. Clique em **OK**.

Nota: As ligações e as intrusões bloqueadas não são registadas durante a activação da protecção no arranque.

Configurar definições de pedidos de ping

Os utilizadores informáticos podem utilizar uma ferramenta de ping, que envia e recebe mensagens de ICMP Echo Request, para verificar se um determinado computador está ligado à rede. Pode configurar a firewall para impedir ou permitir que os utilizadores efectuem pedidos de ping ao seu computador.

Para configurar a definição dos pedidos de ping de ICMP:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, em **Definições de Segurança**, efectue um dos seguintes passos:
   - Seleccione **Permitir pedidos de ping de ICMP** para permitir a detecção do computador na rede através de pedidos de ping.
   - Desmarque **Permitir pedidos de ping de ICMP** para impedir a detecção do computador na rede através de pedidos de ping.
3. Clique em **OK**.

Configurar a detecção de intrusões

A Detecção de Intrusões (IDS) monitoriza os pacotes de dados de transferências de dados ou métodos de transferência suspeitos. A IDS analisa o tráfego e os pacotes de dados relativamente a padrões de tráfego específico utilizado por atacantes. Por exemplo, se a firewall detectar pacotes ICMP, esta analisa-os para verificar se existem padrões de tráfego suspeitos, comparando o tráfego ICMP com padrões de ataque conhecidos. A firewall compara os pacotes com uma base de dados de assinaturas e, se encontrar algo de suspeito ou nocivo, rejeita os pacotes do computador que os enviou e, em seguida, regista opcionalmente o evento.

As definições de instalação padrão incluem a detecção automática das tentativas de intrusão mais comuns, tais como explorações ou ataques por Recusa de Serviço. A utilização das definições de instalação padrão garante-lhe protecção contra estes ataques e análises; no entanto, pode desactivar a detecção automática para um ou mais ataques ou análises, no painel Detecção de Intrusões.

Para configurar a detecção de intrusões:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Detecção de Intrusões**.
3. Em **Detectar Tentativas de Intrusão**, efectue um dos seguintes passos:
   - Seleccione um nome para detectar automaticamente o ataque ou pesquisa.
   - Apague um nome para desactivar a detecção automática do ataque ou pesquisa.
4. Clique em **OK**.

Configurar as definições Estado de Protecção por Firewall

O SecurityCenter regista problemas que pertencem ao Estado de Protecção geral do computador. No entanto, pode configurar a firewall para ignorar problemas específicos no computador que possam afectar o Estado de Protecção. Pode configurar o SecurityCenter para ignorar problemas se a firewall estiver definida para o nível de segurança Aberta, se o serviço Firewall não estiver a funcionar e se não estiver instalada uma firewall apenas de saída no computador.

Para configurar as definições Estado de Protecção por Firewall:

1. No painel Tarefas Comuns, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Alertas**.
4. Clique em **Avançadas**.
5. No painel Tarefas Comuns, clique em **Menu Avançado**.
6. Clique em **Configurar**.
7. No painel Configuração do SecurityCenter, clique em **Estado da Protecção**.
8. Clique em Avançadas.
9. No painel Problemas Ignorados, seleccione uma ou mais das seguintes opções:
   - **A firewall está definida para o nível de segurança Aberta.**
   - **O serviço Firewall não está a funcionar.**
   - **A firewall de saída não está instalada no computador.**
10. Clique em **OK**.

Bloquear e restaurar a firewall

A opção de bloqueio é útil quando se trata de emergências relacionadas com o computador, utilizadores que necessitem de bloquear todo o tráfego para isolar e resolver problemas no computador ou para aqueles que não tenham a certeza e necessitem de saber como gerir o acesso de um programa à Internet.

Bloquear a firewall de imediato

O bloqueio da firewall impede, imediatamente, todo o tráfego de rede de entrada e saída entre o computador e a Internet. Impede que todas as ligações remotas acedam ao computador e bloqueia o acesso de todos os programas à Internet.

Para bloquear de imediato a firewall e impedir todo o tráfego de rede:

1. Nos painéis Página Inicial e Tarefas Comuns, com a opção **Básico** ou **Menu Avançado** activada, clique em **Bloquear Firewall**.
2. No painel Bloquear Firewall, clique em **Bloquear**.
3. Na caixa de diálogo, clique em **Sim** para confirmar que pretende bloquear de imediato todo o tráfego de entrada e saída.

Desbloquear a firewall de imediato

O bloqueio da firewall impede, imediatamente, todo o tráfego de rede de entrada e saída entre o computador e a Internet. Impede que todas as ligações remotas acedam ao computador e bloqueia o acesso de todos os programas à Internet. Depois de seleccionar a opção Bloquear Firewall, pode desbloqueá-la para permitir o tráfego de rede.

Para desbloquear de imediato a firewall e permitir o tráfego de rede:

1. Nos painéis Página Inicial e Tarefas Comuns, com a opção **Básico** ou **Menu Avançado** activada, clique em **Bloquear Firewall**.
2. No painel Bloqueio Activado, clique em **Desbloquear**.
3. Na caixa de diálogo, clique em **Sim** para confirmar que pretende desbloquear a firewall e permitir o tráfego de rede.

Restaurar definições da firewall

Pode restaurar rapidamente a firewall para as definições originais de protecção. Isto define o nível de segurança para o valor padrão, activa a opção Recomendações Inteligentes, restaura endereços IP de confiança e banidos e remove todos os programas do painel Permissões do Programa.

Para restaurar a firewall para as definições originais:

1. Nos painéis Página Inicial e Tarefas Comuns, com a opção **Básico** ou **Menu Avançado** activada, clique em **Restaurar Predefinições da Firewall**.
2. No painel Restaurar Predefinições de Protecção por Firewall, clique em **Restaurar Predefinições**.
3. Na caixa de diálogo Restaurar Predefinições de Protecção por Firewall, clique em **Sim** para confirmar que pretende restaurar a configuração da firewall para os valores predefinidos.

Definir o nível de segurança para Aberta

Se especificar o nível de segurança da firewall para Aberta, a firewall concede acesso a todas as ligações de rede de entrada e saída. Para conceder acesso a programas bloqueados anteriormente, utilize o painel Permissões do Programa.

Para definir o nível de segurança da firewall para Aberta:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Nível de Segurança, mova a barra de deslocamento para que **Aberta** seja apresentado como o nível activado.
3. Clique em **OK**.

Nota: Os programas bloqueados anteriormente continuam a ser bloqueados se o nível de segurança da firewall estiver definido como **Aberta**. Para evitar isto, pode alterar a regra do programa para **Acesso Total**.

CAPÍTULO 20

Gerir programas e permissões

A firewall permite gerir e criar permissões de acesso para programas novos e existentes que requerem acesso de entrada e saída à Internet. A firewall permite-lhe conceder acesso total ou apenas de saída a programas. Pode também bloquear o acesso a programas.

Neste capítulo

Conceder o acesso de programas à Internet

Alguns programas, tais como browsers da Internet, necessitam do acesso à Internet para funcionarem correctamente.

A firewall permite-lhe utilizar a página Permissões do Programa para:

- Conceder acesso a programas
- Conceder acesso apenas de saída a programas
- Bloquear o acesso a programas

Pode também conceder um acesso total ou apenas de saída a partir dos registos Eventos de Saída e Eventos Recentes.

Conceder acesso total a um programa

Muitos programas no computador requerem um acesso de entrada e saída à Internet. O Personal Firewall inclui uma lista de programas com acesso total automático à Internet, mas o utilizador pode modificar estas permissões.

Para conceder o acesso total de um programa à Internet:

1. No painel Configuração de Internet e Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Permissões do Programa**.
3. Em **Permissões do Programa**, seleccione um programa que esteja definido como **Bloqueado** ou **Acesso Apenas de Saída**.
4. Em **Acção**, clique em **Conceder Acesso Total**.
5. Clique em **OK**.

Conceder acesso total a um novo programa

Muitos programas no computador requerem um acesso de entrada e saída à Internet. A firewall inclui uma lista de programas com acesso total automático à Internet, mas pode adicionar um novo programa e alterar as permissões.

Para conceder o acesso total de um novo programa à Internet:

1. No painel Configuração de Internet e Rede, clique em **Avançadas**.
2. No painel **Firewall**, clique em **Permissões do Programa**.
3. Em **Permissões do Programa**, clique em **Adicionar Programa Permitido**.
4. Na caixa de diálogo **Adicionar Programa**, procure e seleccione o programa que pretende adicionar.
5. Clique em **Abrir**.
6. Clique em **OK**.

   O novo programa adicionado é apresentado em **Permissões do Programa**.

Nota: Pode alterar as permissões de um novo programa adicionado, tal como faria com um programa já existente, seleccionando o programa e, em seguida, clicando em **Conceder Acesso Apenas de Saída** ou em **Bloquear Acesso** em **Acção**.

Conceder acesso total a partir do registo Eventos Recentes

Muitos programas no computador requerem um acesso de entrada e saída à Internet. Pode seleccionar um programa a partir do registo Eventos Recentes e conceder-lhe acesso total à Internet.

Para conceder o acesso total a um programa a partir do registo Eventos Recentes:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em Eventos Recentes, seleccione a descrição do evento e depois clique em **Conceder Acesso Total**.
3. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar que pretende conceder acesso total ao programa.

Tópicos relacionados

- Ver eventos de saída (página 166)

Conceder acesso total a partir do registo Eventos de Saída

Muitos programas no computador requerem um acesso de entrada e saída à Internet. Pode seleccionar um programa a partir do registo Eventos de Saída e conceder-lhe acesso total à Internet.

Para conceder o acesso total de um programa à Internet a partir do registo Eventos de Saída:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Seleccione **Internet e Rede** e, em seguida, seleccione **Eventos de Saída**.
4. No painel Eventos de Saída, seleccione um endereço IP de origem e depois clique em **Conceder acesso**.
5. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar que pretende conceder acesso total à Internet ao programa.

Tópicos relacionados

- Ver eventos de saída (página 166)

Conceder acesso apenas de saída a programas

Alguns programas no computador requerem apenas acesso de saída à Internet. A firewall permite-lhe conceder acesso apenas de saída à Internet a programas.

Conceder acesso apenas de saída a um programa

Muitos programas no computador requerem um acesso de entrada e saída à Internet. O Personal Firewall inclui uma lista de programas com acesso total automático à Internet, mas o utilizador pode modificar estas permissões.

Para conceder a um programa acesso apenas de saída:

1. No painel Configuração de Internet e Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Permissões do Programa**.
3. Em **Permissões do Programa**, seleccione um programa que esteja definido como **Bloqueado** ou **Acesso Total**.
4. Em **Acção**, clique em **Conceder Acesso Apenas de Saída**.
5. Clique em **OK**.

Conceder acesso apenas de saída a partir do registo Eventos Recentes

Muitos programas no computador requerem um acesso de entrada e saída à Internet. Pode seleccionar um programa a partir do registo Eventos Recentes e conceder-lhe acesso apenas de saída à Internet.

Para conceder o acesso apenas de saída a um programa a partir do registo Eventos Recentes:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em Eventos Recentes, seleccione a descrição do evento e depois clique em **Conceder Acesso Apenas de Saída**.
3. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar que pretende conceder acesso apenas de saída ao programa.

Tópicos relacionados

- Ver eventos de saída (página 166)

Conceder acesso apenas de saída a partir do registo Eventos de Saída

Muitos programas no computador requerem um acesso de entrada e saída à Internet. Pode seleccionar um programa a partir do registo Eventos de Saída e conceder-lhe acesso apenas de saída à Internet.

Para conceder o acesso apenas de saída a um programa a partir do registo Eventos de Saída:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Seleccione **Internet e Rede** e, em seguida, seleccione **Eventos de Saída**.
4. No painel Eventos de Saída, seleccione um endereço IP de origem e depois clique em **Conceder Acesso Apenas de Saída**.
5. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar que pretende conceder acesso apenas de saída ao programa.

Tópicos relacionados

- Ver eventos de saída (página 166)

Bloquear o acesso de programas à Internet

A firewall permite-lhe bloquear o acesso de programas à Internet. Certifique-se de que o bloqueio de um programa não interrompe a ligação à rede ou a outro programa que necessite do acesso à Internet para funcionar correctamente.

Bloquear o acesso a um programa

Muitos programas no computador requerem um acesso de entrada e saída à Internet. O Personal Firewall inclui uma lista de programas com acesso total automático à Internet, mas pode bloquear estas permissões.

Para bloquear o acesso de um programa à Internet:

1. No painel Configuração de Internet e Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Permissões do Programa**.
3. Em **Permissões do Programa**, seleccione um programa que esteja definido como **Acesso Total** ou **Acesso Apenas de Saída**.
4. Em **Acção**, clique em **Bloquear Acesso**.
5. Clique em **OK**.

Bloquear o acesso a um novo programa

Muitos programas no computador requerem um acesso de entrada e saída à Internet. O Personal Firewall inclui uma lista de programas com acesso total automático, mas o utilizador pode adicionar um novo programa e bloquear o respectivo acesso à Internet.

Para bloquear o acesso de um novo programa à Internet:

1. No painel Configuração de Internet e Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Permissões do Programa**.
3. Em **Permissões do Programa**, clique em **Adicionar Programa Bloqueado**.
4. Na caixa de diálogo **Adicionar Programa**, procure e seleccione o programa que pretende adicionar.
5. Clique em **Abrir**.
6. Clique em **OK**.

   O novo programa adicionado é apresentado em **Permissões do Programa**.

Nota: Pode alterar as permissões de um novo programa adicionado, tal como faria com um programa existente, seleccionando o programa e, em seguida, clicando em **Conceder Acesso Apenas de Saída** ou **Conceder Acesso Total** em **Acção**.

Bloquear o acesso a partir do registo Eventos Recentes

Muitos programas no computador requerem um acesso de entrada e saída à Internet. No entanto, pode também bloquear o acesso de programas à Internet a partir do registo Eventos Recentes.

Para bloquear o acesso de um programa a partir do registo Eventos Recentes:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em Eventos Recentes, seleccione a descrição do evento e depois clique em **Bloquear Acesso**.
3. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar que pretende bloquear o programa.

Tópicos relacionados

- Ver eventos de saída (página 166)

Remover as permissões de acesso dos programas

Antes de remover a permissão para um programa, certifique-se de que não é indispensável para o funcionamento do computador ou para a ligação à rede.

Remover uma permissão de programa

Muitos programas no computador requerem um acesso de entrada e saída à Internet. A Personal Firewall inclui uma lista de programas com acesso total automático, mas pode remover programas que tenham sido adicionados manual e automaticamente.

Para remover uma permissão de um novo programa:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Permissões do Programa**.
3. Em **Permissões do Programa**, seleccione um programa.
4. Em **Acção**, clique em **Eliminar Permissão do Programa**.
5. Clique em **OK**.

   O programa é removido do painel Permissões do Programa.

Nota: A firewall impede que o utilizador modifique alguns programas, esbatendo e desactivando acções.

Obter informações sobre programas

Se não tiver a certeza sobre a permissão de programa a utilizar, pode obter informações sobre o programa no Web site HackerWatch da McAfee para ajudá-lo a decidir

Obter informações sobre programas

Muitos programas no computador requerem um acesso de entrada e saída à Internet. A Personal Firewall inclui uma lista de programas com acesso total automático à Internet, mas pode modificar estas permissões.

A firewall pode ajudá-lo a decidir se deve conceder ou bloquear o acesso de um programa à Internet. Certifique-se de que está ligado à Internet para que o browser inicie com êxito o Web site HackerWatch da McAfee, que fornece informações actualizadas sobre programas, requisitos de acesso à Internet e ameaças de segurança.

Para obter informações sobre programas:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Permissões do Programa**.
3. Em **Permissões do Programa**, seleccione um programa.
4. Em **Acção**, clique em **Mais Informações**.

Obter informações sobre programas a partir do registo Eventos de Saída

A Personal Firewall permite-lhe obter informações sobre os programas apresentados no registo Eventos de Saída.

Antes de obter informações sobre um programa, certifique-se de que tem uma ligação à Internet e um browser da Internet.

Para obter informações sobre programas a partir do registo Eventos de Saída:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Seleccione **Internet e Rede** e, em seguida, seleccione **Eventos de Saída**.
4. No painel Eventos de Saída, seleccione um endereço IP de origem e depois clique em **Mais Informações**.

   Pode ver informações sobre o programa no Web site HackerWatch. O HackerWatch fornece informações actualizadas sobre programas, requisitos de acesso à Internet e ameaças de segurança.

Tópicos relacionados

- Ver eventos de saída (página 166)

CAPÍTULO 21

Gerir serviços do sistema

Para um funcionamento adequado, determinados programas (incluindo servidores Web e programas de servidores de partilha de ficheiros) devem aceitar ligações não solicitadas de outros computadores através de portas específicas do serviço do sistema. Normalmente, a firewall fecha estas portas do serviço do sistema porque representam a fonte mais provável de inseguranças no sistema. No entanto, para aceitarem ligações de computadores remotos, as portas do serviço do sistema devem estar abertas.

Esta lista mostra as portas padrão dos serviços comuns.

- Protocolo de Transferência de Ficheiros (FTP) - Portas 20 e 21
- Servidor de Correio (IMAP) - Porta 143
- Servidor de Correio (POP3) - Porta 110
- Servidor de Correio (SMTP) - Porta 25
- Microsoft Directory Server (MSFT DS) - Porta 445
- Microsoft SQL Server (MSFT SQL) - Porta 1433
- Assistência Remota / Servidor de Terminais (RDP) - Porta 3389
- Chamadas de Procedimentos Remotas (RPC) - Porta 135
- Servidor Web Seguro (HTTPS) - Porta 443
- Universal Plug and Play (UPNP) - Porta 5000
- Servidor Web (HTTP) - Porta 80
- Windows File Sharing (NETBIOS) - Portas 137 a 139

Neste capítulo

Configurar portas do serviço do sistema

Para permitir o acesso remoto a um serviço num computador, deve especificar o serviço e a porta associada que pretende abrir. Seleccione apenas um serviço e uma porta se tiver a certeza que devem ser abertos. Não é normalmente necessário abrir uma porta.

Permitir acesso a uma porta de serviço do sistema existente

A partir do painel Serviços do Sistema, pode abrir ou fechar uma porta existente para permitir ou recusar o acesso remoto a um serviço de rede no seu computador. Uma porta de serviço do sistema aberta pode tornar o computador vulnerável a ameaças de segurança da Internet, pelo que só deve abrir uma porta caso seja necessário.

Para permitir acesso a uma porta de serviço do sistema:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Serviços do Sistema**.
3. Em **Abrir Porta de Serviços do Sistema**, seleccione um serviço do sistema para abrir uma porta.
4. Clique em **OK**.

Bloquear o acesso a uma porta de serviço do sistema existente

A partir do painel Serviços do Sistema, pode abrir ou fechar uma porta existente para permitir ou recusar o acesso remoto a um serviço de rede no seu computador. Uma porta de serviço do sistema aberta pode tornar o computador vulnerável a ameaças de segurança da Internet, pelo que só deve abrir uma porta caso seja necessário.

Para bloquear o acesso a uma porta de serviço do sistema:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Serviços do Sistema**.
3. Em **Abrir Porta de Serviços do Sistema**, retire um serviço do sistema para fechar uma porta.
4. Clique em **OK**.

Configurar uma nova porta do serviço do sistema

No painel Serviços do Sistema, pode adicionar uma nova porta de serviço do sistema que, por sua vez, pode abrir ou fechar para permitir ou recusar o acesso remoto a um serviço de rede no computador do utilizador. Uma porta aberta do serviço do sistema pode tornar o computador vulnerável a ameaças de segurança na Internet, devendo apenas abrir uma porta quando for necessário.

Para criar e configurar uma nova porta do serviço do sistema:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Serviços do Sistema**.
3. Clique em **Adicionar**.
4. Em **Adicionar Configuração da Porta**, especifique as seguintes opções:
   - Nome do programa
   - Portas TCP/IP de entrada
   - Portas TCP/IP de saída
   - Portas UDP de entrada
   - Portas UDP de saída
5. Pode também descrever a nova configuração.
6. Clique em **OK**.

   A nova porta configurada do serviço do sistema é apresentada em **Abrir Porta do Serviço de Sistema**.

Modificar uma porta do serviço do sistema

Uma porta aberta e fechada permite e nega acesso a um serviço de rede no computador. No painel Serviços do Sistema, pode modificar as informações de entrada e saída de uma determinada porta. Se as informações da porta forem introduzidas incorrectamente, ocorre uma falha no serviço do sistema.

Para modificar uma porta do serviço do sistema:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Serviços do Sistema**.
3. Seleccione um serviço do sistema e clique em **Editar**.
4. Em **Adicionar Configuração da Porta**, especifique as seguintes opções:
   - Nome do programa

- Portas TCP/IP de entrada
- Portas TCP/IP de saída
- Portas UDP de entrada
- Portas UDP de saída

5 Pode também descrever a configuração modificada.

6 Clique em **OK**.

A porta modificada do serviço do sistema configurado é apresentada em **Abrir Serviço do Sistema**.

Remover uma porta do serviço do sistema

Uma porta aberta ou fechada permite ou nega acesso a um serviço de rede no computador. No painel Serviços do Sistema, pode remover uma porta existente e o serviço do sistema associado. Depois de remover uma porta e o serviço do sistema do painel Serviços do Sistema, os computadores remotos deixam de ter acesso ao serviço de rede no computador.

Para remover uma porta do serviço do sistema:

1 No painel Configuração de Internet & Rede, clique em **Avançadas**.

2 No painel Firewall, clique em **Serviços do Sistema**.

3 Seleccione um serviço do sistema e clique em **Remover**.

4 Na caixa de diálogo **Serviços do Sistema**, clique em **Sim** para confirmar se pretende eliminar o serviço de sistema.

A porta do serviço do sistema deixa de aparecer no painel Serviços do Sistema.

CAPÍTULO 22

Gerir ligações a computadores

Pode configurar a firewall para gerir ligações remotas específicas ao computador, criando regras baseadas em endereços Protocolo Internet (IPs), associados a computadores remotos. Os computadores associados a endereços IP de confiança podem ser ligados ao seu computador e os IPs desconhecidos, suspeitos ou que não sejam de confiança podem ser impedidos de estabelecer ligação ao computador.

Quando autoriza uma ligação, certifique-se de que o computador no qual está a confiar é seguro. Se um computador considerado de confiança for infectado por um worm ou outro mecanismo, o seu computador poderá também ficar vulnerável à infecção. Além disso, a McAfee recomenda que os computadores de confiança estejam protegidos por uma firewall e um programa antivírus devidamente actualizado. A firewall não regista tráfego nem gera alertas de eventos a partir de endereços IP na lista Endereços IP de Confiança.

Os computadores associados a endereços IP desconhecidos, suspeitos ou duvidosos podem ser banidos, impedindo assim que estabeleçam ligação com o seu computador.

Uma vez que a firewall bloqueia todo o tráfego indesejado, normalmente, não será necessário banir um endereço IP. Só deverá banir um endereço IP quando tiver a certeza de que uma ligação à Internet representa uma ameaça específica. Certifique-se de que não são bloqueados endereços IP importantes, tais como o servidor de DNS ou DHCP, nem outros servidores relacionados com o ISP. Dependendo das definições de segurança, a firewall pode avisar o utilizador quando for detectado um evento proveniente de um computador banido.

Neste capítulo

Ligações de confiança a um computador

Pode adicionar, editar e remover endereços IP de confiança no painel IPs de Confiança e Banidos, em **Endereços IP de Confiança**.

A lista **Endereços IP de Confiança** do painel IPs de Confiança e Banidos permite-lhe autorizar que todo o tráfego proveniente de um computador específico chegue ao seu computador. A firewall não regista tráfego nem gera alertas de eventos de endereços IP que constam da lista **Endereços IP de Confiança**.

A firewall confia em todos os endereços IP presentes na lista e permite sempre o tráfego de um IP de confiança através da firewall em qualquer porta. A firewall não regista quaisquer eventos de endereços IP de confiança. A actividade entre o computador associado a um endereço IP de confiança e o seu computador não é filtrada nem analisada pela firewall.

Quando autoriza uma ligação, certifique-se de que o computador no qual está a confiar é seguro. Se um computador considerado de confiança for infectado por um worm ou outro mecanismo, o seu computador poderá também ficar vulnerável à infecção. Além disso, a McAfee recomenda que os computadores de confiança estejam protegidos por uma firewall e um programa antivírus devidamente actualizado.

Adicionar uma ligação de confiança ao computador

Pode utilizar a firewall para adicionar uma ligação de confiança ao computador e ao endereço IP associado.

A lista **Endereços IP de Confiança** do painel IPs de Confiança e Banidos permite-lhe autorizar que todo o tráfego proveniente de um computador específico chegue ao seu computador. A firewall não regista tráfego nem gera alertas de eventos de endereços IP que constam da lista **Endereços IP de Confiança**.

Os computadores associados a endereços IP de confiança podem ligar sempre ao seu computador. Antes de adicionar, editar ou remover um endereço IP de confiança, certifique-se de que a comunicação com esse endereço ou a sua remoção são seguras.

Para adicionar uma ligação de confiança ao computador:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **IPs de Confiança e Banidos**.
3. No painel IPs de Confiança e Banidos, seleccione **Endereços IP de Confiança**.
4. Clique em **Adicionar**.
5. Em **Adicionar Regra de Endereço IP de Confiança**, efectue um dos seguintes passos:
   - Seleccione um **Endereço IP Simples** e depois introduza o endereço IP.
   - Seleccione um **Intervalo do Endereço IP** e depois introduza os endereços IP inicial e final nas caixas **Do Endereço IP** e **Para o Endereço IP**.
6. Também pode seleccionar **Regra expira em** e introduzir o número de dias para aplicar a regra.
7. Pode ainda introduzir uma descrição para a regra.
8. Clique em **OK**.
9. Na caixa de diálogo Adicionar Regra de Endereço IP de Confiança, clique em **Sim** para confirmar se pretende adicionar a ligação de confiança ao computador.

   O novo endereço IP adicionado é apresentado em **Endereços IP de Confiança**.

Adicionar um computador de confiança a partir do registo Eventos de Entrada

Pode adicionar uma ligação de confiança a um computador e o respectivo endereço IP associado a partir do registo Eventos de Entrada.

Os computadores associados a endereços IP de confiança podem ligar sempre ao seu computador. Antes de adicionar, editar ou remover um endereço IP de confiança, certifique-se de que a comunicação com esse endereço ou a sua remoção são seguras.

Para adicionar uma ligação de confiança a um computador a partir do registo Eventos de Entrada:

1. Certifique-se de que o menu Avançado está activado. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Clique em **Internet e Rede** e, em seguida, clique em **Eventos de Entrada**.
4. No painel Eventos de Entrada, seleccione um endereço IP de origem e depois clique em **Confiar Neste Endereço**.
5. Na caixa de diálogo Adicionar Regra de Endereço IP de Confiança, clique em **Sim** para confirmar se pretende confiar no endereço IP.

   O novo endereço IP adicionado é apresentado em **Endereços IP de Confiança**.

Tópicos relacionados

- Registo de eventos (página 164)

Editar uma ligação de confiança a um computador

Pode utilizar a firewall para editar uma ligação de confiança ao computador e ao endereço IP associado.

Os computadores associados a endereços IP de confiança podem ligar sempre ao seu computador. Antes de adicionar, editar ou remover um endereço IP de confiança, certifique-se de que a comunicação com esse endereço ou a sua remoção são seguras.

Para editar uma ligação de confiança ao computador:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **IPs de Confiança e Banidos**.
3. No painel IPs de Confiança e Banidos, seleccione **Endereços IP de Confiança**.
4. Seleccione um endereço IP e depois clique em **Editar**.
5. Em **Adicionar Regra de Endereço IP de Confiança**, efectue um dos seguintes passos:
   - Seleccione um **Endereço IP Simples** e depois introduza o endereço IP.
   - Seleccione um **Intervalo do Endereço IP** e depois introduza os endereços IP inicial e final nas caixas **Do Endereço IP** e **Para o Endereço IP**.
6. Também pode seleccionar **Regra expira em** e introduzir o número de dias para aplicar a regra.
7. Pode ainda introduzir uma descrição para a regra.
8. Clique em **OK**.

   O endereço IP modificado é apresentado em **Endereços IP de Confiança**.

Remover uma ligação de confiança ao computador

Pode utilizar a firewall para remover uma ligação de confiança ao computador e ao endereço IP associado.

Os computadores associados a endereços IP de confiança podem ligar sempre ao seu computador. Antes de adicionar, editar ou remover um endereço IP de confiança, certifique-se de que a comunicação com esse endereço ou a sua remoção são seguras.

Para remover uma ligação de confiança ao computador:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **IPs de Confiança e Banidos**.
3. No painel IPs de Confiança e Banidos, seleccione **Endereços IP de Confiança**.
4. Seleccione um endereço IP e depois clique em **Remover**.
5. Na caixa de diálogo **IPs de Confiança e Banidos**, clique em **Sim** para confirmar se pretende remover o endereço IP de confiança em **Endereços IP de Confiança**.

Banir ligações a computadores

Pode adicionar, editar e remover endereços IP de confiança no painel IPs de Confiança e Banidos, em **Endereços IP Banidos**.

Os computadores associados a endereços IP desconhecidos, suspeitos ou duvidosos podem ser banidos, impedindo assim que estabeleçam ligação com o seu computador.

Uma vez que a firewall bloqueia todo o tráfego indesejado, normalmente, não será necessário banir um endereço IP. Só deverá banir um endereço IP quando tiver a certeza de que uma ligação à Internet representa uma ameaça específica. Certifique-se de que não são bloqueados endereços IP importantes, tais como o servidor de DNS ou DHCP, nem outros servidores relacionados com o ISP. Dependendo das definições de segurança, a firewall pode avisar o utilizador quando for detectado um evento proveniente de um computador banido.

Adicionar uma ligação banida a um computador

Pode utilizar a firewall para adicionar uma ligação de computadores banidos e endereços IP associados.

Os computadores associados a endereços IP desconhecidos, suspeitos ou duvidosos podem ser banidos, impedindo assim que estabeleçam ligação com o seu computador.

Uma vez que a firewall bloqueia todo o tráfego indesejado, normalmente, não será necessário banir um endereço IP. Só deverá banir um endereço IP quando tiver a certeza de que uma ligação à Internet representa uma ameaça específica. Certifique-se de que não são bloqueados endereços IP importantes, tais como o servidor de DNS ou DHCP, nem outros servidores relacionados com o ISP. Dependendo das definições de segurança, a firewall pode avisar o utilizador quando for detectado um evento proveniente de um computador banido.

Para adicionar uma ligação de computadores banidos:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **IPs de Confiança e Banidos**.
3. No painel IPs de Confiança e Banidos, seleccione **Endereços IP Banidos**.
4. Clique em **Adicionar**.
5. Em Adicionar Regra de Endereço IP Banido, efectue um dos seguintes passos:
   - Seleccione um **Endereço IP Simples** e depois introduza o endereço IP.

- Seleccione um **Intervalo do Endereço IP** e depois introduza os endereços IP inicial e final nos campos **Do Endereço IP** e **Para o Endereço IP**.

6 Também pode seleccionar **Regra expira em** e introduzir o número de dias para aplicar a regra.

7 Pode ainda introduzir uma descrição para a regra.

8 Clique em **OK**.

9 Na caixa de diálogo **Adicionar Regra de Endereço IP Banido**, clique em **Sim** para confirmar se pretende adicionar a ligação banida ao computador.

O novo endereço IP adicionado é apresentado em **Endereços IP Banidos**.

Editar uma ligação banida ao computador

Pode utilizar a firewall para editar uma ligação banida ao computador e ao endereço IP associado.

Os computadores associados a endereços IP desconhecidos, suspeitos ou duvidosos podem ser banidos, impedindo assim que estabeleçam ligação com o seu computador.

Uma vez que a firewall bloqueia todo o tráfego indesejado, normalmente, não será necessário banir um endereço IP. Só deverá banir um endereço IP quando tiver a certeza de que uma ligação à Internet representa uma ameaça específica. Certifique-se de que não são bloqueados endereços IP importantes, tais como o servidor de DNS ou DHCP, nem outros servidores relacionados com o ISP. Dependendo das definições de segurança, a firewall pode avisar o utilizador quando for detectado um evento proveniente de um computador banido.

Para editar uma ligação banida ao computador:

1 No painel Configuração de Internet & Rede, clique em **Avançadas**.

2 No painel Firewall, clique em **IPs de Confiança e Banidos**.

3 No painel IPs de Confiança e Banidos, seleccione **Endereços IP Banidos**.

4 Seleccione um endereço IP e depois clique em **Editar**.

5 Em **Adicionar Regra de Endereço IP de Confiança**, efectue um dos seguintes passos:

- Seleccione um **Endereço IP Simples** e depois introduza o endereço IP.
- Seleccione um **Intervalo do Endereço IP** e depois introduza os endereços IP inicial e final nos campos **Do Endereço IP** e **Para o Endereço IP**.

6 Também pode seleccionar **Regra expira em** e introduzir o número de dias para aplicar a regra.

7 Pode ainda introduzir uma descrição para a regra.

Clique em **OK**. O endereço IP modificado é apresentado em **Endereços IP Banidos**.

Remover uma ligação banida ao computador

Pode utilizar a firewall para remover uma lista banida ao computador e ao endereço IP associado.

Os computadores associados a endereços IP desconhecidos, suspeitos ou duvidosos podem ser banidos, impedindo assim que estabeleçam ligação com o seu computador.

Uma vez que a firewall bloqueia todo o tráfego indesejado, normalmente, não será necessário banir um endereço IP. Só deverá banir um endereço IP quando tiver a certeza de que uma ligação à Internet representa uma ameaça específica. Certifique-se de que não são bloqueados endereços IP importantes, tais como o servidor de DNS ou DHCP, nem outros servidores relacionados com o ISP. Dependendo das definições de segurança, a firewall pode avisar o utilizador quando for detectado um evento proveniente de um computador banido.

Para remover uma ligação banida ao computador:

1 No painel Configuração de Internet & Rede, clique em **Avançadas**.

2 No painel Firewall, clique em **IPs de Confiança e Banidos**.

3 No painel IPs de Confiança e Banidos, seleccione **Endereços IP Banidos**.

4 Seleccione um endereço IP e clique em **Remover**.

5 Na caixa de diálogo **IPs de Confiança e Banidos**, clique em **Sim** para confirmar se pretende remover o endereço IP de confiança em **Endereços IP Banidos**.

Banir um computador do registo Eventos de Entrada

Pode banir uma ligação a um computador e o respectivo endereço IP associado a partir do registo Eventos de Entrada.

Os endereços IP apresentados no registo Eventos de Entrada são bloqueados. Por conseguinte, banir um endereço não confere protecção adicional, excepto se o computador utilizar portas que estejam propositadamente abertas ou se o computador tiver um programa instalado ao qual tenha sido concedido acesso à Internet.

Só deve adicionar um endereço IP à lista **Endereços IP e Banidos** se tiver uma ou mais portas que estejam deliberadamente abertas e se quiser impedir o acesso desse endereço a portas abertas.

Pode utilizar a página Eventos de Entrada, onde são indicados os endereços IP de todo o tráfego de entrada da Internet, para banir um endereço IP que possa ser responsável por actividade suspeita e não desejável na Internet.

Para banir uma ligação de confiança a um computador a partir do registo Eventos de Entrada:

1. Certifique-se de que o menu Avançado está activado. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Clique em **Internet e Rede** e, em seguida, clique em **Eventos de Entrada**.
4. No painel Eventos de Entrada, seleccione um endereço IP de origem e depois clique em **Banir este endereço**.
5. Na caixa de diálogo **Adicionar Regra de Endereço IP Banido**, clique em **Sim** para confirmar se pretende banir o endereço IP.

   O novo endereço IP adicionado é apresentado em **Endereços IP Banidos**.

Tópicos relacionados

- Registo de eventos (página 164)

Banir um computador do registo Eventos de Detecção de Intrusões

Pode banir uma ligação a um computador e o respectivo endereço IP associado a partir do registo Eventos de Detecção de Intrusões.

Os computadores associados a endereços IP desconhecidos, suspeitos ou duvidosos podem ser banidos, impedindo assim que estabeleçam ligação com o seu computador.

Uma vez que a firewall bloqueia todo o tráfego indesejado, normalmente, não será necessário banir um endereço IP. Só deverá banir um endereço IP quando tiver a certeza de que uma ligação à Internet representa uma ameaça específica. Certifique-se de que não são bloqueados endereços IP importantes, tais como o servidor de DNS ou DHCP, nem outros servidores relacionados com o ISP. Dependendo das definições de segurança, a firewall pode avisar o utilizador quando for detectado um evento proveniente de um computador banido.

Para banir uma ligação a um computador do registo Eventos de Detecção de Intrusões:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Clique em **Internet e Rede** e, em seguida, clique em **Eventos de Detecção de Intrusões**.
4. No painel Eventos de Detecção de Intrusões, seleccione um endereço IP de origem e depois clique em **Banir este endereço**.
5. Na caixa de diálogo **Adicionar Regra de Endereço IP Banido**, clique em **Sim** para confirmar se pretende banir o endereço IP.

   O novo endereço IP adicionado é apresentado em **Endereços IP Banidos**.

Tópicos relacionados

- Registo de eventos (página 164)

CAPÍTULO 23

Registo, monitorização e análise

A firewall fornece registo, monitorização e análise abrangentes e fáceis de utilizar para eventos e tráfego da Internet. A compreensão do tráfego e dos eventos da Internet ajudam a gerir as ligações à Internet.

Neste capítulo

Registo de eventos

A firewall permite-lhe especificar se pretende activar ou desactivar a opção de registo e, se estiver activada, quais os tipos de eventos a registar. O registo de eventos permite-lhe ver os eventos de entrada e saída recentes. Pode ver igualmente os eventos de intrusões detectados.

Configurar as definições do registo de eventos

Para registar os eventos e a actividade da firewall, pode especificar e configurar os tipos de eventos que pretende ver.

Para configurar o registo de eventos:

1. No painel Configuração de Internet & Rede, clique em **Avançadas**.
2. No painel Firewall, clique em **Definições de Registo de Eventos**.
3. No painel Definições de Registo de Eventos, efectue uma das seguintes acções:
   - Seleccione **Registar o Evento** para activar o registo de eventos.
   - Seleccione **Não registar o evento** para desactivar o registo de eventos.
4. Em **Definições de Registo de Eventos**, especifique os tipos de eventos a registar. Os tipos de eventos incluem:
   - Pings de ICMP
   - Tráfego de endereços IP banidos
   - Eventos nas portas do serviço de sistemas
   - Eventos em portas desconhecidas
   - Eventos de Detecção de intrusões (IDS)
5. Para impedir o registo em portas específicas, seleccione **Não registar eventos na(s) seguinte(s) porta(s)** e depois introduza números de portas individuais separados por vírgulas ou intervalos de portas com travessões. Por exemplo, `137-139, 445, 400-5000`.
6. Clique em **OK**.

Ver eventos recentes

Se a opção de registo estiver activada, pode ver eventos recentes. O painel Eventos Recentes mostra a data e a descrição do evento. O painel Eventos Recentes apresenta apenas a actividade dos programas que tenham sido explicitamente bloqueados de aceder à Internet.

Para ver eventos recentes da firewall:

- No **Menu Avançado**, no painel Tarefas Comuns, clique em **Relatórios & Registos** ou em **Ver Eventos Recentes**. Como alternativa, clique em **Ver Eventos Recentes** no painel Tarefas Comuns no Menu Básico.

Ver eventos de entrada

Se a opção de registo estiver activada, pode ver e ordenar eventos de entrada.

O registo Eventos de Entrada inclui as seguintes categorias de registo:

- Data e hora
- Endereço IP de origem
- Nome anfitrião
- Tipo de eventos e informações

Para ver os eventos de entrada da firewall:

1. Certifique-se de que o menu Avançado está activado. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Clique em **Internet e Rede** e, em seguida, clique em **Eventos de Entrada**.

Nota: Pode confiar, banir e rastrear um endereço IP a partir do registo Evento de Entrada.

Tópicos relacionados

- Adicionar um computador de confiança a partir do registo Eventos de Entrada (página 154)
- Banir um computador do registo Eventos de Entrada (página 160)
- Rastrear um computador a partir do registo Eventos de Entrada (página 169)

Ver eventos de saída

Se a opção de registo estiver activada, pode ver eventos de saída. Eventos de Saída inclui o nome do programa que tenta efectuar o acesso de saída, a data e hora do evento e a localização do programa no computador.

Para ver os eventos de saída da firewall:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Seleccione **Internet e Rede** e, em seguida, seleccione **Eventos de Saída**.

Nota: Pode conceder um acesso total e apenas de saída a um programa a partir do registo Eventos de Saída. Pode também localizar informações adicionais sobre o programa.

Tópicos relacionados

- Conceder acesso total a partir do registo Eventos de Saída (página 138)
- Conceder acesso apenas de saída a partir do registo Eventos de Saída (página 140)
- Obter informações sobre programas a partir do registo Eventos de Saída (página 145)

Ver eventos de detecção de intrusões

Se a opção de registo estiver activada, pode ver eventos de entrada. A Detecção de Intrusões apresenta a data e a hora, o IP de origem e o nome anfitrião do evento. O registo descreve também o tipo de evento.

Para ver os eventos de detecção de intrusões:

1. No painel Tarefas Comuns, clique em **Relatórios & Registos**.
2. Em Eventos Recentes, clique em **Ver Registo**.
3. Clique em **Internet & Rede** e depois clique em **Eventos de Detecção de Intrusões**.

Nota: Pode banir e rastrear um endereço IP a partir do registo Eventos de Detecção de Intrusões.

Tópicos relacionados

- Banir um computador do registo Eventos de Detecção de Intrusões (página 161)
- Rastrear um computador a partir do registo Eventos de Detecção de Intrusões (página 170)

Trabalhar com estatísticas

A Firewall optimiza o HackerWatch, o Web site de segurança da McAfee, para fornecer ao utilizador estatísticas sobre eventos de segurança global da Internet e actividade das portas.

Ver estatísticas globais de eventos de segurança

O HackerWatch regista eventos de segurança da Internet a nível mundial, que podem ser vistos a partir do SecurityCenter. As informações recolhidas incluem os incidentes enviados para o HackerWatch nas últimas 24 horas, 7 dias e 30 dias.

Para ver as estatísticas globais de segurança:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **HackerWatch**.
3. Veja as estatísticas de eventos de segurança em **Registo de Eventos**.

Ver a actividade global das portas da Internet

O HackerWatch regista eventos de segurança da Internet a nível mundial, que podem ser vistos a partir do SecurityCenter. As informações apresentadas incluem as principais portas de eventos registadas no HackerWatch durante os últimos sete dias. Normalmente, são apresentadas informações sobre as portas HTTP, TCP e UDP.

Para ver a actividade das portas a nível mundial:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **HackerWatch**.
3. Veja os principais eventos da porta de eventos em **Actividade Recente das Portas**.

Registar tráfego na Internet

A firewall dispõe de várias opções de registo do tráfego na Internet. Estas opções permitem rastrear, geograficamente, um computador em rede, obter informações de rede e domínio e rastrear computadores a partir dos registos Eventos de Entrada e Eventos de Detecção de Intrusões.

Rastrear geograficamente um computador em rede

Pode utilizar o Visual Tracer para localizar, geograficamente, um computador que esteja a efectuar ou a tentar uma ligação ao seu computador, utilizando o respectivo nome ou um endereço IP. Pode também utilizar o Visual Tracer para aceder a informações de rede e registo. O Visual Tracer permite visualizar um mapa mundial que apresenta o percurso mais provável dos dados, desde o computador de origem até ao seu computador.

Para localizar geograficamente um computador:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Visual Tracer**.
3. Introduza o endereço IP do computador e clique em **Rastrear**.
4. Em **Visual Tracer**, seleccione **Vista de Mapa**.

Nota: Não pode rastrear eventos de endereços IP em ciclo, privados ou inválidos.

Obter informações sobre o registo de computadores

Pode obter as informações de registo de um computador no SecurityCenter com a opção Visual Trace. As informações incluem o nome de domínio, o nome e endereço do inscrito e o contacto administrativo.

Para obter informações de domínio de um computador:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Visual Tracer**.
3. Introduza o endereço IP do computador e clique em **Rastrear**.
4. Em **Visual Tracer**, seleccione **Vista do Inscrito**.

Obter informações de rede sobre computadores

Pode obter as informações de rede de um computador no SecurityCenter com a opção Visual Trace. As informações de rede incluem pormenores sobre a rede na qual está instalado o domínio.

Para obter informações de rede de um computador:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Visual Tracer**.
3. Introduza o endereço IP do computador e clique em **Rastrear**.
4. Em **Visual Tracer**, seleccione **Vista de Rede**.

Rastrear um computador a partir do registo Eventos de Entrada

No painel Eventos de Entrada, pode rastrear um endereço IP apresentado no registo Eventos de Entrada.

Para rastrear o endereço IP de um computador a partir do registo Eventos de Entrada:

1. Certifique-se de que o menu Avançado está activado. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Clique em **Internet e Rede** e, em seguida, clique em **Eventos de Entrada**.
4. No painel Eventos de Entrada, seleccione um endereço IP de origem e depois clique em **Rastrear Este Endereço**.
5. No painel Visual Tracer, clique numa das seguintes acções:
   - **Vista de Mapa**: Localize geograficamente um computador com o endereço IP seleccionado.
   - **Vista do Inscrito**: Localize as informações de domínio com o endereço IP seleccionado.
   - **Vista de Rede**: Localize as informações de rede com o endereço IP seleccionado.
6. Clique em **Concluído**.

Tópicos relacionados

- Registar tráfego na Internet (página 168)
- Ver eventos de entrada (página 165)

Rastrear um computador a partir do registo Eventos de Detecção de Intrusões

No painel Eventos de Detecção de Intrusões, pode rastrear um endereço IP apresentado no registo Eventos de Detecção de Intrusões.

Para rastrear o endereço IP de um computador a partir do registo Eventos de Detecção de Intrusões:

1. No painel Tarefas Comuns, clique em **Relatórios e Registos**.
2. Em **Eventos Recentes**, clique em **Ver Registo**.
3. Clique em **Internet e Rede** e, em seguida, clique em **Eventos de Detecção de Intrusões**. No painel Eventos de Detecção de Intrusões, seleccione um endereço IP de origem e depois clique em **Rastrear este endereço**.
4. No painel Visual Tracer, clique numa das seguintes acções:
   - **Vista de Mapa**: Localize geograficamente um computador com o endereço IP seleccionado.
   - **Vista do Inscrito**: Localize as informações de domínio com o endereço IP seleccionado.
   - **Vista de Rede**: Localize as informações de rede com o endereço IP seleccionado.
5. Clique em **Concluído**.

Tópicos relacionados

- Registar tráfego na Internet (página 168)
- Registo, monitorização e análise (página 163)

Rastrear um endereço IP monitorizado

Pode rastrear um endereço IP monitorizado para obter uma perspectiva geográfica, que apresenta o percurso mais provável dos dados, desde o computador de origem ao seu computador. Além disso, pode obter informações de registo e rede sobre o endereço IP.

Para monitorizar a utilização da largura de banda dos programas:

1. Certifique-se de que o Menu Avançado está activado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Monitor de Tráfego**.
3. Em **Monitor de Tráfego**, clique em **Programas Activos**.
4. Seleccione um programa e, em seguida, o endereço IP indicado abaixo do nome do programa.
5. Em **Actividade do Programa**, clique em **Rastrear este IP**.
6. Em **Visual Tracer**, pode visualizar um mapa mundial que apresenta o percurso mais provável dos dados, desde o computador de origem até ao seu computador. Além disso, pode obter informações de registo e rede sobre o endereço IP.

Nota: Para ver as estatísticas mais recentes, clique em **Actualizar** em **Visual Tracer**.

Tópicos relacionados

- Monitorizar o tráfego na Internet (página 172)

Monitorizar o tráfego na Internet

A firewall dispõe de vários métodos para monitorizar o tráfego na Internet, incluindo:

- **Gráfico Análise de Tráfego**: Apresenta o tráfego recente de entrada e saída da Internet.
- **Gráfico Utilização de Tráfego**: Apresenta a percentagem de largura de banda utilizada pelos programas mais activos durante as últimas 24 horas.
- **Programas Activos**: Apresenta os programas que normalmente utilizam o maior número de ligações de rede no computador, assim como os endereços IP a que os programas acedem.

Acerca do gráfico Análise de Tráfego

O gráfico da Análise de Tráfego é uma representação numérica e gráfica do tráfego da Internet de entrada e saída. Além disso, o Monitor de Tráfego mostra os programas que utilizam o maior número de ligações de rede no computador, bem como os endereços IP aos quais os programas acedem.

No painel Análise de Tráfego, pode ver tráfego recente de entrada e saída da Internet, assim como as velocidades actuais, médias e máximas de transferência. Pode ver também o volume de tráfego, incluindo o volume desde que iniciou a firewall, bem como o tráfego total do mês actual e de meses anteriores.

O painel Análise de Tráfego apresenta a actividade da Internet em tempo real no computador, incluindo o volume e a velocidade do tráfego recente de entrada e saída da Internet no computador, a velocidade de ligação e o número total de bytes transferidos na Internet.

A linha verde sólida representa a velocidade actual de transferência do tráfego de entrada. A linha verde ponteada representa a velocidade média de transferência de tráfego de entrada. Se a velocidade actual de transferência e a velocidade média de transferência forem iguais, a linha ponteada não aparece no gráfico. A linha sólida representa tanto a velocidade média como a velocidade actual da transferência.

A linha vermelha sólida representa a velocidade actual de transferência do tráfego de saída. A linha vermelha ponteada representa a velocidade média de transferência do tráfego de saída. Se a velocidade actual de transferência e a velocidade média de transferência forem iguais, a linha ponteada não aparece no gráfico. A linha sólida representa tanto a velocidade média como a velocidade actual da transferência.

Tópicos relacionados

- Analisar tráfego de entrada e saída (página 174)

Analisar tráfego de entrada e saída

O gráfico da Análise de Tráfego é uma representação numérica e gráfica do tráfego da Internet de entrada e saída. Além disso, o Monitor de Tráfego mostra os programas que utilizam o maior número de ligações de rede no computador, bem como os endereços IP aos quais os programas acedem.

Para analisar o tráfego de entrada e saída:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Monitor de Tráfego**.
3. Em **Monitor de Tráfego**, clique em **Análise de Tráfego**.

Sugestão: Para ver as estatísticas mais recentes, clique em **Actualizar** em **Análise de Tráfego**.

Tópicos relacionados

- Acerca do gráfico Análise de Tráfego (página 173)

Monitorizar a largura de bandas dos programas

Pode ver o gráfico circular, que apresenta a percentagem aproximada de largura de banda utilizada pela maioria dos programas activos no computador durante as últimas vinte e quatro horas. O gráfico circular apresenta uma representação visual dos valores relativos de largura de banda utilizados pelos programas.

Para monitorizar a utilização da largura de banda dos programas:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Monitor de Tráfego**.
3. Em **Monitor de Tráfego**, clique em **Utilização de Tráfego**.

Sugestão: Para ver as estatísticas mais recentes, clique em **Actualizar** em **Utilização de Tráfego**.

Monitorizar a actividade dos programas

Pode ver a actividade de entrada e saída dos programas, apresentando as ligações e portas do computador remoto.

Para monitorizar a utilização da largura de banda dos programas:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Monitor de Tráfego**.
3. Em **Monitor de Tráfego**, clique em **Programas Activos**.
4. Pode ver as seguintes informações:
   - Gráfico Actividade de Programas: Seleccione um programa para visualizar um gráfico da respectiva actividade.
   - Ligação de controlo: Seleccione uma opção de escuta sob o nome do programa.
   - Ligação a computadores: Seleccione um endereço IP abaixo do nome do programa, processo ou serviço do sistema.

Nota: Para ver as estatísticas mais recentes, clique em **Actualizar** em **Programas Activos**.

CAPÍTULO 24

Obter informações sobre segurança da Internet

A Firewall optimiza o HackerWatch, o Web site de segurança da McAfee, para fornecer-lhe informações actualizadas sobre programas e actividade global da Internet. O HackerWatch inclui também uma apresentação em HTML sobre a firewall.

Neste capítulo

Iniciar a apresentação do HackerWatch

Para obter mais informações sobre a firewall, pode aceder à apresentação do HackerWatch no SecurityCenter.

Para iniciar a apresentação do HackerWatch:

1. Certifique-se de que o Menu Avançado está activado e depois clique em **Ferramentas**.
2. No painel Ferramentas, clique em **HackerWatch**.
3. Em **Recursos do HackerWatch**, clique em **Ver Apresentação**.

CAPÍTULO 25

McAfee EasyNetwork

O McAfee® EasyNetwork permite a partilha segura de ficheiros, simplifica as transferências de ficheiros e torna a partilha de impressoras automática entre os computadores da sua rede doméstica.

Antes de começar a utilizar o EasyNetwork, pode familiarizar-se com algumas das funcionalidades mais conhecidas. Na ajuda do EasyNetwork, encontrará informações pormenorizadas sobre como configurar e utilizar essas funcionalidades.

Neste capítulo

Funcionalidades

O EasyNetwork oferece as seguintes funcionalidades.

Partilha de ficheiros

O EasyNetwork facilita a partilha de ficheiros entre o seu computador e outros computadores da rede. Ao partilhar ficheiros, está a conceder aos outros computadores acesso apenas de leitura aos ficheiros. Apenas os computadores que são membros da rede gerida (isto é, que têm acesso total ou administrativo) podem partilhar ficheiros ou aceder a ficheiros partilhados por outros membros.

Transferência de ficheiros

Pode enviar ficheiros para outros computadores que sejam membros da rede gerida. Quando recebe um ficheiro, este aparece na pasta A receber do EasyNetwork. A pasta A receber é um local de armazenamento temporário para todos os ficheiros que lhe são enviados por outros computadores da rede.

Partilha de impressoras automática

Depois de aderir a uma rede gerida, o EasyNetwork partilha automaticamente todas as impressoras locais ligadas ao seu computador, utilizando o nome actual da impressora como nome de impressora partilhada. Detecta ainda impressoras partilhadas por outros computadores na rede e permite-lhe configurar e utilizar essas impressoras.

CAPÍTULO 26

Configurar o EasyNetwork

Antes de utilizar as funcionalidades do EasyNetwork, tem de iniciar o programa e aderir à rede gerida. Uma vez efectuada a adesão, pode abandonar a rede em qualquer altura.

Neste capítulo

Iniciar o EasyNetwork

Por predefinição, é-lhe solicitado que inicie o EasyNetwork imediatamente após a instalação; no entanto, pode também fazê-lo posteriormente.

Iniciar o EasyNetwork

Por predefinição, é-lhe solicitado que inicie o EasyNetwork imediatamente após a instalação; no entanto, pode também fazê-lo posteriormente.

Para iniciar o EasyNetwork:

- No menu **Iniciar**, seleccione **Programas**, seleccione **McAfee** e, em seguida, clique em **McAfee EasyNetwork**.

Sugestão: Se aceitou criar ícones no ambiente de trabalho e de início rápido durante a instalação, pode igualmente iniciar o EasyNetwork fazendo duplo clique no ícone McAfee EasyNetwork no ambiente de trabalho ou clicando no ícone McAfee EasyNetwork na área de notificação situada à direita da barra de tarefas.

Aderir a uma rede gerida

Depois de instalar o SecurityCenter, é adicionado um agente de rede ao computador que funciona em segundo plano. No EasyNetwork, o agente de rede é responsável por detectar uma ligação de rede válida e impressoras locais para partilhar, bem como por monitorizar o estado da rede.

Se não for encontrado outro computador com o agente de rede na rede à qual está ligado, fica automaticamente membro da rede e é-lhe solicitado que identifique se a rede é fidedigna. Sendo o primeiro computador a aderir à rede, o nome do seu computador é incluído no nome da rede; no entanto, pode alterar o nome da rede em qualquer altura.

Quando um computador acede à rede, é enviado um pedido de adesão a todos os outros computadores actualmente ligados à rede. O pedido pode ser concedido por qualquer computador com permissões administrativas na rede. O concessor pode também determinar o nível de permissão do computador que está a aderir à rede; por exemplo, direitos de convidado (permite apenas a transferências de ficheiros) ou acesso total/administrativo (transferência e partilha de ficheiros). No EasyNetwork, os computadores com acesso administrativo podem conceder acesso a outros computadores e gerir permissões (isto é, promover ou despromover computadores); os computadores com acesso total não podem executar estas tarefas administrativas. Antes de o computador poder efectuar a adesão, é efectuada uma verificação de segurança.

Nota: Depois da adesão, se tiver outros programas de rede da McAfee instalados (por exemplo, McAfee Wireless Network Security ou Network Manager), o computador é reconhecido como um computador gerido nesses programas. O nível de permissão atribuído a um computador aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o significado das permissões de convidado, de acesso total ou administrativo noutros programas de rede da McAfee, consulte a documentação fornecida com o respectivo programa.

Aderir à rede

Quando um computador acede a uma rede fidedigna pela primeira vez depois de instalar o EasyNetwork, é apresentada uma mensagem a perguntar se pretende aderir à rede gerida. Quando o computador aceita aderir, é enviado um pedido a todos os computadores da rede que têm acesso administrativo. Este pedido tem de ser aceite para que o computador possa partilhar impressoras ou ficheiros, enviar e copiar ficheiros da rede. Se o computador for o primeiro computador da rede, adquire automaticamente permissões de administração na rede.

Para aderir à rede:

1. Na janela Ficheiros Partilhados, clique em **Sim, quero aderir à rede agora**.
   Quando um computador com direitos administrativos na rede aceita o pedido, é apresentada uma mensagem a perguntar se este computador e outros computadores da rede estão autorizados a gerir as definições de segurança uns dos outros.
2. Para autorizar este e outros computadores da rede a gerir as definições de segurança uns dos outros, clique em **Sim**; caso contrário, clique em **Não**.
3. Confirme se o computador concessor apresenta as cartas de jogar actualmente apresentadas na caixa de diálogo de confirmação de segurança e, em seguida, clique em **Confirmar**.

Nota: Se o computador concessor não apresentar as mesmas cartas apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. A adesão à rede pode colocar o computador em perigo; por conseguinte, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Conceder acesso à rede

Quando um computador pede para aderir à rede gerida, é enviada uma mensagem aos outros computadores da rede que têm acesso administrativo. O primeiro computador a responder à mensagem passa a ser o concessor. Como concessor, esse computador é responsável por determinar o tipo de acesso a conceder ao computador: convidado, total ou administrativo.

Para conceder acesso à rede:

1. No aviso, seleccione uma das seguintes caixas de verificação:
   - **Conceder acesso de convidado**: Permite que o utilizador envie ficheiros para outros computadores, mas não permite a partilha de ficheiros.

- **Conceder acesso total a todas as aplicações da rede gerida**: Permite que o utilizador envie e partilhe ficheiros.
- **Conceder acesso administrativo a todas as aplicações da rede gerida**: Permite que o utilizador envie e partilhe ficheiros, conceda acesso a outros computadores e ajuste os níveis de permissão de outros computadores.

2 Clique em **Conceder Acesso**.

3 Confirme se o computador apresenta as cartas de jogar actualmente apresentadas na caixa de diálogo de confirmação de segurança e, em seguida, clique em **Confirmar**.

Nota: Se o computador não apresentar as mesmas cartas apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. Permitir o acesso deste computador à rede pode colocar o seu computador em perigo; por conseguinte, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Mudar o nome da rede

Por predefinição, o nome da rede inclui o nome do primeiro computador que aderiu à rede; no entanto, pode mudar o nome da rede em qualquer altura. Ao mudar o nome da rede, altera a descrição da rede apresentada no EasyNetwork.

Para mudar o nome da rede:

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, introduza o nome da rede na caixa **Nome da Rede**.
3. Clique em **OK**.

Abandonar uma rede gerida

Se aderir a uma rede gerida e, posteriormente, decidir que quer deixar de ser membro da rede, pode abandonar a rede. Depois de anular a sua subscrição, pode voltar a aderir à rede em qualquer altura; no entanto, tem novamente de obter permissão para aderir e efectuar a verificação de segurança. Para obter mais informações, consulte Aderir a uma rede gerida (página 183).

Abandonar uma rede gerida

Pode abandonar uma rede gerida à qual anteriormente aderiu.

Para abandonar uma rede gerida:

1. No menu **Ferramentas**, clique em **Abandonar Rede**.
2. Na caixa de diálogo Abandonar Rede, seleccione o nome da rede que pretende abandonar.
3. Clique em **Abandonar Rede**.

CAPÍTULO 27

Partilhar e enviar ficheiros

O EasyNetwork permite que ficheiros do seu computador sejam facilmente partilhados e enviados para outros computadores da rede. Ao partilhar ficheiros, está a conceder aos outros computadores acesso apenas de leitura aos ficheiros. Apenas os computadores que são membros da rede gerida (isto é, que têm acesso total ou administrativo) podem partilhar ficheiros ou aceder a ficheiros partilhados por outros membros.

Neste capítulo

Partilhar ficheiros

O EasyNetwork facilita a partilha de ficheiros entre o seu computador e outros computadores da rede. Ao partilhar ficheiros, está a conceder aos outros computadores acesso apenas de leitura aos ficheiros. Apenas os computadores que são membros da rede gerida (isto é, que têm acesso total ou administrativo) podem partilhar ficheiros ou aceder a ficheiros partilhados por outros membros. Se partilhar uma pasta, todos os ficheiros contidos nessa pasta e respectivas subpastas são partilhados; no entanto, os ficheiros posteriormente adicionados à pasta não são automaticamente partilhados. Se um ficheiro ou uma pasta partilhados forem eliminados, são automaticamente removidos da janela Ficheiros Partilhados. Pode deixar de partilhar um ficheiro em qualquer altura.

Pode aceder a um ficheiro partilhado de duas formas: abrindo o ficheiro directamente a partir do EasyNetwork ou copiando o ficheiro para o seu computador para depois o abrir. Se a sua lista de ficheiros partilhados ficar muito extensa, pode procurar os ficheiros partilhados aos quais pretende aceder.

Nota: Os ficheiros partilhados através do EasyNetwork não podem ser acedidos a partir de outros computadores através do Explorador do Windows. A partilha de ficheiros no EasyNetwork é efectuada com base em ligações seguras.

Partilhar um ficheiro

Quando partilha um ficheiro, este fica automaticamente disponível para todos os outros membros da rede gerida que tenham acesso total ou administrativo.

Para partilhar um ficheiro:

1. No Explorador do Windows, localize o ficheiro que pretende partilhar.
2. Arraste o ficheiro do Explorador do Windows para a janela Ficheiros Partilhados do EasyNetwork.

Sugestão: Pode igualmente partilhar um ficheiro, clicando em **Partilhar Ficheiros** no menu **Ferramentas**. Na caixa de diálogo Partilhar, percorra a pasta onde está guardado o ficheiro que pretende partilhar, seleccione o ficheiro e clique em **Partilhar**.

Interromper a partilha de um ficheiro

Se estiver a partilhar um ficheiro na rede gerida, pode interromper a partilha desse ficheiro em qualquer altura. Quando interrompe a partilha de um ficheiro, os outros membros da rede gerida deixam de ter acesso ao mesmo.

Para interromper a partilha de um ficheiro:

1. No menu **Ferramentas**, seleccione **Parar Partilha de Ficheiros**.
2. Na caixa de diálogo Parar Partilha de Ficheiros, seleccione o ficheiro que já não pretende partilhar.
3. Clique em **Não Partilhar**.

Copiar um ficheiro partilhado

Pode copiar ficheiros partilhados para o seu computador, a partir de qualquer computador da rede gerida. Se o computador interromper a partilha do ficheiro, continua a ter a cópia.

Para copiar um ficheiro:

- Arraste o ficheiro da janela Ficheiros Partilhados do EasyNetwork para uma localização no Explorador do Windows ou para o ambiente de trabalho do Windows.

Sugestão: Pode também copiar um ficheiro partilhado, seleccionando o ficheiro no EasyNetwork e clicando em **Copiar para** no menu **Ferramentas**. Na caixa de diálogo Copiar para a pasta, percorra a pasta até ao local para onde pretende copiar o ficheiro, seleccione-o e clique em **Guardar**.

Procurar um ficheiro partilhado

Pode procurar um ficheiro que tenha sido partilhado por si ou por qualquer outro membro da rede. À medida que digita os seus critérios de procura, o EasyNetwork apresenta automaticamente os resultados correspondentes na janela Ficheiros Partilhados.

Para procurar um ficheiro partilhado:

1. Na janela Ficheiros Partilhados, clique em **Procurar**.
2. Clique numa das seguintes opções da lista **Contém**:
   - **Contém todas as palavras**: Procura nomes de ficheiros ou caminhos que contenham todas as palavras especificadas na lista **Nome do Caminho ou Ficheiro**, por qualquer ordem.

- **Contém qualquer das palavras**: Procura nomes de ficheiros ou caminhos que contenham qualquer uma das palavras especificadas na lista **Nome do Caminho ou Ficheiro**.
- **Contém a cadeia exacta**: Procura nomes de ficheiros ou caminhos que contenham a frase exacta que especificou na lista **Nome do Caminho ou Ficheiro**.

3 Introduza o nome parcial ou completo do ficheiro ou do caminho na lista **Nome do Caminho ou Ficheiro**.

4 Clique num dos seguintes tipos de ficheiro da lista **Tipo**:

- **Qualquer**: Procura todos os tipos de ficheiros partilhados.
- **Documento**: Procura todos os documentos partilhados.
- **Imagem**: Procura todos os ficheiros de imagem partilhados.
- **Vídeo**: Procura todos os ficheiros de vídeo partilhados.
- **Áudio**: Procura todos os ficheiros de som partilhados.

5 Na listas **De** e **Até**, seleccione as datas correspondentes ao intervalo de datas em que o ficheiro foi criado.

Enviar ficheiros para outros computadores

Pode enviar ficheiros para outros computadores que sejam membros da rede gerida. Antes de enviar um ficheiro, o EasyNetwork confirma se o computador de destino tem espaço em disco suficiente.

Quando recebe um ficheiro, este aparece na pasta A receber do EasyNetwork. A pasta A receber é um local de armazenamento temporário para todos os ficheiros que lhe são enviados por outros computadores da rede. Se tiver o EasyNetwork aberto quando receber um ficheiro, o ficheiro aparece de imediato na pasta A receber; caso contrário, aparece uma mensagem na área de notificação situada à direita da barra de tarefas do Windows. Se não quiser receber mensagens de aviso, pode desactivá-las. Se já existir um ficheiro com o mesmo nome na pasta A receber, é acrescentado um sufixo numérico ao nome do novo ficheiro. O ficheiros permanecem na pasta A receber até que os aceite (isto é, até que os copie para uma localização no seu computador).

Enviar um ficheiro para outro computador

Pode enviar um ficheiro directamente para outro computador da rede gerida, sem o partilhar. Para que o utilizador do computador de destino possa ver o ficheiro, tem de o guardar localmente. Para mais informações, consulte Aceitar um ficheiro de outro computador (página 194).

Para enviar um ficheiro para outro computador:

1. No Explorador do Windows, localize o ficheiro que pretende enviar.
2. Arraste o ficheiro do Explorador do Windows para o ícone de um computador activo do EasyNetwork.

Sugestão: Pode enviar vários ficheiros para um computador, premindo CTRL quando selecciona os ficheiros. Em alternativa, pode clicar em **Enviar** no menu **Ferramentas**, seleccionar os ficheiros e clicar em **Enviar** para enviar ficheiros.

Aceitar um ficheiro de outro computador

Se outro computador da rede gerida lhe enviar um ficheiro, tem de o aceitar (guardando-o numa pasta do seu computador). Se não tiver o EasyNetwork aberto ou em primeiro plano quando o ficheiro for enviado para o seu computador, receberá uma mensagem de aviso na área de notificação situada à direita da barra de tarefas. Clique na mensagem de aviso para abrir o EasyNetwork e aceder ao ficheiro.

Para receber um ficheiro de outro computador:

- Clique em **Recebidos** e, em seguida, arraste um ficheiro da pasta A receber do EasyNetwork para uma pasta do Explorador do Windows.

Sugestão: Pode também receber um ficheiro de outro computador, seleccionando o ficheiro na pasta A receber do EasyNetwork e clicando em **Aceitar** no menu **Ferramentas**. Na caixa de diálogo Aceitar para a pasta, percorra a pasta até ao local onde pretende guardar os ficheiros recebidos, seleccione-o e clique em **Guardar**.

Receber um aviso de envio de ficheiro

Pode receber um aviso quando outro computador da rede gerida lhe envia um ficheiro. Se o EasyNetwork não estiver aberto nem a funcionar em primeiro plano no ambiente de trabalho, aparece uma mensagem de aviso na área de notificação situada à direita da barra de tarefas do Windows.

Para receber um aviso de envio de ficheiro:

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, seleccione a caixa de verificação **Notificar-me quando outro computador me enviar ficheiros**.
3. Clique em **OK**.

CAPÍTULO 28

Partilhar impressoras

Depois de aderir a uma rede gerida, o EasyNetwork partilha automaticamente todas as impressoras locais ligadas ao seu computador. Detecta ainda impressoras partilhadas por outros computadores na rede e permite-lhe configurar e utilizar essas impressoras.

Neste capítulo

Trabalhar com impressoras partilhadas

Depois de aderir a uma rede gerida, o EasyNetwork partilha automaticamente todas as impressoras locais ligadas ao seu computador, utilizando o nome actual da impressora como nome de impressora partilhada. Detecta ainda impressoras partilhadas por outros computadores na rede e permite-lhe configurar e utilizar essas impressoras. Se tiver configurado um controlador de impressão para imprimir através de um servidor de impressão de rede (por exemplo, um servidor de impressão USB sem fios), o EasyNetwork considera a impressora como uma impressora local e partilha-a automaticamente na rede. Pode deixar de partilhar uma impressora em qualquer altura.

O EasyNetwork detecta ainda as impressoras partilhadas por todos os outros computadores da rede. Se for detectada uma impressora remota que ainda não esteja ligada ao seu computador, aparecerá a hiperligação **Impressoras de rede disponíveis** na janela Ficheiros Partilhados, quando abrir o EasyNetwork pela primeira vez. Desta forma, poderá instalar impressoras disponíveis ou desinstalar impressoras que já estejam ligadas ao seu computador. Pode também actualizar a lista de impressoras detectadas na rede.

Se ainda não aderiu à rede gerida, mas estiver ligado a ela, pode aceder às impressoras partilhadas a partir do painel de controlo de impressoras padrão do Windows.

Interromper a partilha de uma impressora

Pode deixar de partilhar uma impressora em qualquer altura. Os membros que instalaram a impressora deixarão de conseguir imprimir através dessa impressora.

Para interromper a partilha de uma impressora:

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Gerir Impressoras de Rede, clique no nome da impressora que já não pretende partilhar.
3. Clique em **Não Partilhar**.

Instalar uma impressora de rede disponível

Como membro de uma rede gerida, pode aceder às impressoras partilhadas na rede. Para isso, tem de instalar o controlador de impressora utilizado pela impressora. Se, depois de ter instalado uma impressora, o seu proprietário interromper a partilha, deixa de poder imprimir com essa impressora.

Para instalar uma impressora de rede disponível:

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Impressoras de Rede Disponíveis, clique no nome de uma impressora.
3. Clique em **Instalar**.

CAPÍTULO 29

Referência

O Glossário de Termos apresenta e define a terminologia de segurança mais utilizada que pode encontrar nos produtos da McAfee.

Acerca da McAfee fornece informações jurídicas sobre a McAfee Corporation.

Glossário

8

802.11

Um conjunto de normas da IEEE para a tecnologia de LAN sem fios. A 802.11 especifica uma interface via rádio entre um cliente sem fios e uma estação base ou entre dois clientes sem fios. As várias especificações da 802.11 incluem a 802.11a, uma norma para redes até 54 Mbps na banda de frequências dos 5 Ghz, a 802.11b, uma norma para redes até 11 Mbps na banda de frequências dos 2,4 Ghz, a 802.11g, uma norma para redes até 54 Mbps na banda de frequências dos 2,4 Ghz, e a 802.11i, um conjunto de normas de segurança para todas as Ethernets sem fios.

802.11a

Uma extensão da 802.11 aplicável a LANs sem fios e que envia dados até 54 Mbps na banda de frequências dos 5 GHz. Apesar da velocidade de transmissão ser superior à da 802.11b, a distância abrangida é muito menor.

802.11b

Uma extensão da 802.11 aplicável a LANs sem fios e que permite a transmissão a 11 Mbps na banda de frequências dos 2,4 GHz. A 802.11b é actualmente considerada a norma das redes sem fios.

802.11g

Uma extensão da 802.11 aplicável a LANs sem fios e que permite a transmissão até 54 Mbps na banda de frequências dos 2,4 GHz.

802.1x

Não suportada pelo Wireless Home Network Security. Uma norma da IEEE para autenticação em redes com e sem fios, mas mais frequentemente utilizada em redes sem fios 802.11. Esta norma fornece uma autenticação forte e mútua entre um cliente e um servidor de autenticação. Para além disso, a 802.1x fornece chaves WEP dinâmicas por utilizador e por sessão, diminuindo o trabalho administrativo e os riscos de segurança associados às chaves WEP estáticas.

A

adaptador sem fios

Adaptador que contém os circuitos necessários para permitir que um computador ou outro dispositivo comunique com um router sem fios (ou seja, que aceda a uma rede sem fios). Os adaptadores sem fios podem estar incorporados nos circuitos principais de um dispositivo de hardware ou constituir um periférico separado, que pode ser inserido num dispositivo através da porta adequada.

Adaptadores sem fios PCI

Permitem ligar um computador de secretária a uma rede. A placa é ligada a uma ranhura de expansão PCI existente no interior do computador.

Adaptadores sem fios USB

Fornecem uma interface série Plug and Play expansível. Esta interface fornece uma ligação sem fios padrão, de baixo custo, para dispositivos periféricos tais como teclados, ratos, joysticks, impressoras, digitalizadores, dispositivos de memória e câmaras de videoconferência.

análise de imagens

Bloqueia a apresentação de imagens potencialmente inapropriadas. As imagens são bloqueadas para todos os utilizadores, excepto para os membros do grupo dos adultos.

análise em tempo real

Quando o utilizador ou o computador acede aos ficheiros, estes são analisados para detecção de vírus e outras actividades.

arquivo

Para criar uma cópia dos seus ficheiros de monitorização localmente na unidade de CD, DVD, USB, na unidade de disco externo ou na unidade de rede.

arquivo

Para criar uma cópia dos seus ficheiros de monitorização localmente na unidade de CD, DVD, USB, na unidade de disco externo ou na unidade de rede.

arquivo integral

Para arquivar um conjunto completo de dados baseado nas localizações e nos tipos de ficheiros monitorizados que definiu.

arquivo rápido

Para arquivar apenas os ficheiros monitorizados que foram alterados desde o último arquivo completo ou rápido.

ataque de dicionário

Estes ataques envolvem a utilização de um conjunto de palavras existente numa lista para identificar a palavra-passe de um utilizador. Os atacantes não experimentam manualmente todas as combinações, dispondo de ferramentas que tentam automaticamente identificar a palavra-passe de um utilizador.

ataque de força bruta

Trata-se de um método de tentativa e erro utilizado pelas aplicações para descodificarem dados encriptados, tais como palavras-passe, através do esforço exaustivo (utilizando a força bruta) em vez da utilização de estratégias intelectuais. Tal como um criminoso pode conseguir abrir um cofre tentando as várias combinações possíveis, uma aplicação de ataque de força bruta tenta sequencialmente todas as combinações possíveis de caracteres legais. A força bruta é considerada uma abordagem infalível, se bem que demorada.

ataque de intermediário (man-in-the-middle)

O atacante intercepta as mensagens numa troca de chaves públicas e, em seguida, retransmite-as, substituindo a chave pedida pela sua própria chave pública de modo a que pareça que os dois interlocutores originais continuam a comunicar directamente. O atacante utiliza um programa que aparenta ser o servidor ao cliente e que aparenta ser o cliente ao servidor. O ataque pode ser utilizado apenas para obter acesso às mensagens ou para permitir que o atacante modifique as mensagens antes de as retransmitir. O termo deriva do facto do atacante agir como "intermediário" da comunicação.

autenticação

O processo de identificação de um indivíduo, normalmente baseado num nome de utilizador e palavra-passe. A autenticação assegura que esse indivíduo é realmente quem afirma ser, mas não contém quaisquer informações sobre os direitos de acesso desse indivíduo.

B

biblioteca

Área de armazenamento online para ficheiros publicados por utilizadores do Data Backup. A biblioteca é um Web site da Internet, que está acessível a todos os que tiverem acesso à Internet.

browser

Um programa cliente que utiliza o Hypertext Transfer Protocol (HTTP) para efectuar pedidos de servidores Web na Internet. Um Web browser apresenta o conteúdo graficamente ao utilizador.

C

cabeçalho

Um cabeçalho são informações adicionadas a uma parte da mensagem durante o seu ciclo de vida. O cabeçalho indica ao software da Internet como enviar a mensagem, para onde as respostas da mensagem devem ser enviadas, um identificador exclusivo para a mensagem de correio electrónico e outras informações administrativas. Exemplos de campos de cabeçalho: Para, De, CC, Data, Assunto, ID da Mensagem e Recebido.

Cavalo de Tróia

Os Cavalos de Tróia são programas que aparentam ser aplicações benignas. Os cavalos de Tróia não são considerados vírus porque não se replicam, mas podem ser tão destrutivos como estes.

chave

Uma série de letras e/ou números utilizada por dois dispositivos para autenticação da respectiva comunicação. Ambos os dispositivos têm de possuir a chave. Consulte também WEP, WPA, WPA2, WPA-PSK e WPA2- PSK.

cliente

Uma aplicação, em execução num computador pessoal ou estação de trabalho, que depende de um servidor para efectuar algumas operações. Por exemplo, um cliente de correio electrónico é uma aplicação que lhe permite enviar e receber correio electrónico.

cliente de correio electrónico

Uma conta de correio electrónico. Por exemplo, Microsoft Outlook ou Eudora.

Cofre de Palavras-passe

Área de armazenamento seguro para palavras-passe pessoais. Permite guardar palavras-passe com a certeza de que nenhum outro utilizador (nem mesmo um Administrador da McAfee ou um administrador do sistema) terá acesso às mesmas.

compressão

Processo pelo qual os dados (ficheiros) são comprimidos num formato que reduz o espaço necessário para os armazenar ou transmitir.

conta de correio electrónico padrão

A maioria dos utilizadores domésticos possui este tipo de conta. Consulte também Conta POP3.

Conta MAPI

Acrónimo de Messaging Application Programming Interface, interface de programação de aplicações de mensagens. Especificação de interface Microsoft que permite que diferentes aplicações de mensagens e de grupos de trabalho (incluindo correio electrónico, correio de voz e fax) funcionem através de um único cliente, como o cliente Exchange. Por este motivo, o MAPI é utilizado frequentemente em ambientes empresariais quando a empresa utiliza o Microsoft® Exchange Server. No entanto, muitas pessoas utilizam o Microsoft Outlook para o correio electrónico da Internet pessoal.

conta MSN

Abreviatura de Rede Microsoft. Um serviço online e um portal da Internet. Trata-se de uma conta baseada em ambiente Web.

Conta POP3

Acrónimo de Post Office Protocol 3. A maioria dos utilizadores domésticos possuem este tipo de conta. Trata-se da versão actual do protocolo de postos de correio utilizado na maioria das redes TCP/IP. Também conhecida como conta de correio electrónico padrão.

cookie

Na World Wide Web, um bloco de dados que um servidor Web guarda num sistema cliente. Quando um utilizador regressa ao mesmo Web site, o browser envia uma cópia do cookie para o servidor. Os cookies são utilizados para identificar utilizadores, para dar indicação ao servidor para enviar uma versão personalizada da página Web solicitada, para enviar informações de conta ao utilizador e para outros efeitos administrativos.

Os cookies permitem que o Web site memorize a identificação do utilizador e rastreie o número de pessoas que o visitaram, quando o visitaram e que páginas foram visualizadas. Os cookies também ajudam uma empresa a personalizar o respectivo Web site em função do utilizador. Um grande número de Web sites requer um nome de utilizador e uma palavra-passe para permitir o acesso a determinadas páginas, enviando um cookie ao computador para que não seja necessário iniciar sessão sempre que a página é visitada. No entanto, os cookies podem ser utilizados por motivos maliciosos. As empresas de publicidade online utilizam frequentemente os cookies para determinarem os sites que o utilizador visita com mais frequência, colocando anúncios nos Web site favoritos do utilizador. Antes de aceitar os cookies de um site, verifique se os cookies são fidedignos.

Embora sejam uma fonte de informações para empresas legítimas, os cookies podem também ser uma fonte de informações para hackers. Um grande número de Web sites com lojas online armazenam informações de cartões de crédito e outras informações pessoais em cookies para simplificar o processo de compra. Infelizmente, podem existir erros de segurança que permitem aos hackers aceder às informações dos cookies armazenados nos computadores dos clientes.

cópia de segurança

Para criar uma cópia dos ficheiros de monitorização num servidor online seguro.

correio electrónico

Correio Electrónico, mensagens enviadas através da Internet ou por uma rede local ou alargada empresarial. Os anexos de correio electrónico no formato de ficheiros EXE (executáveis) ou VBS (scripts do Visual Basic) tornaram-se muito populares como forma de transmissão de vírus e Troianos.

D

Denial-of-Service

Na Internet, um ataque Denial-of-Service (DoS) é um incidente no qual um utilizador ou organização fica privado dos serviços de um recurso que normalmente esperaria ter. Normalmente, a perda de serviço é a indisponibilidade de um serviço de rede específico, tal como o correio electrónico, ou a perda temporária de toda a conectividade e serviços de rede. Por exemplo, nos piores casos, um Web site acedido por milhões de pessoas pode ocasionalmente ser forçado a interromper temporariamente o funcionamento. Um ataque Denial-of-Service também poderá destruir a programação e os ficheiros num sistema informático. Apesar de ser normalmente intencional e malicioso, um ataque Denial-of-Service também pode por vezes ocorrer acidentalmente. Um ataque Denial-of-Service é um tipo de falha de segurança de um sistema informático que não resulta normalmente no furto de informações ou na perda de outros serviços. No entanto, estes ataques podem causar à vítima uma grande perda de tempo e dinheiro.

DNS

Sigla de Domain Name System, sistema de nomes de domínios. Sistema hierárquico através do qual os anfitriões na Internet possuem endereços de nome de domínio (como bluestem.prairienet.org) e endereço IP (como 192.17.3.4). O endereço do nome de domínio é utilizado pelas pessoas e é automaticamente convertido no endereço IP numérico, que é utilizado pelo software de encaminhamento de pacotes. Os nomes DNS são constituídos por um domínio de nível superior (como .com, .org e .net), um domínio de nível secundário (o nome do site de uma empresa, de uma organização ou de um indivíduo) e, possivelmente, um ou mais subdomínios (servidores dentro do domínio de nível secundário). Consulte também Servidor DNS e Endereço IP.

domínio

Um endereço de uma ligação de rede que identifica o proprietário desse endereço num formato hierárquico: servidor.organização.tipo. Por exemplo, www.whitehouse.gov identifica o servidor Web da Casa Branca, que faz parte do governo dos E.U.A.

E

encriptação

Processo pelo qual os dados passam de texto a código, ocultando as informações para impedir que sejam lidas por pessoas que não sabem como as desencriptar.

endereço IP

O endereço de protocolo Internet, ou endereço IP, é um número exclusivo composto por quatro partes separadas por pontos (por exemplo, 63.227.89.66). Todos os computadores na Internet, do maior servidor a um computador portátil, que comunicam através de um telemóvel, têm um número IP exclusivo. Nem todos os computadores têm um nome de domínio, mas todos têm um IP.

Lista de alguns tipos de endereços IP pouco frequentes:

- Endereços IP Não Encaminháveis: São igualmente designados por Espaço IP Privado. São endereços IP que não podem ser utilizados na Internet. Os blocos de endereços IP privados são 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.
- Endereços IP de Loop-Back**:** Os endereços de loop-back são utilizados para testes. O tráfego enviado para este bloco de endereços IP volta para o dispositivo que gerou o pacote. Nunca sai do dispositivo e é utilizado principalmente para testes de hardware e software. O bloco de endereços IP de Loopback é 127.x.x.x.

Endereço IP Nulo: É um endereço IP inválido. Quando for apresentado, indica que o tráfego tem um endereço IP nulo. Não é normal e geralmente indica que o remetente está deliberadamente a ocultar a origem do tráfego. O remetente não poderá receber nenhuma resposta para o tráfego, a não ser que o pacote seja recebido por uma aplicação que compreenda o respectivo conteúdo, o qual incluirá instruções específicas para essa aplicação. Qualquer endereço que comece por 0 (0.x.x.x) é um endereço nulo. Por exemplo, 0.0.0.0 é um endereço IP nulo.

Endereço MAC (Endereço de Controlo de Acesso a Suportes de Dados)

Um endereço de baixo nível atribuído a um dispositivo físico que acede à rede.

Erros de Web

Pequenos ficheiros gráficos que podem incorporar-se nas páginas HTML e permitir que uma fonte não autorizada instale cookies no computador. Estes cookies podem depois transmitir informações à fonte não autorizada. Erros de Web são também designados sinalizadores Web, pixel tags, GIFs limpos ou GIFs invisíveis.

ESS (Extended Service Set)

Um conjunto de duas ou mais redes que constituem uma única sub-rede.

evento

Eventos de 0.0.0.0

Se vir eventos com o endereço IP 0.0.0.0, existem duas causas prováveis. A primeira, e mais comum, é que, por algum motivo, o computador recebeu um pacote inválido. A Internet nem sempre é 100% fiável e poderão surgir pacotes danificados. Uma vez que o Firewall vê os pacotes antes de o TCP/IP os poder validar, poderá comunicar estes pacotes como um evento.

A segunda situação ocorre quando o IP de origem é alvo de fraude ou é falso. Os pacotes alvo de fraudes podem ser indícios de que alguém anda à procura de Troianos e tentou procurar no seu computador. É importante lembrar que o Firewall bloqueia a tentativa.

Eventos de 127.0.0.1

Por vezes, os eventos listam o respectivo endereço IP de origem como 127.0.0.1. É importante referir que este IP é especial e é designado como o endereço de loopback.

Independentemente do computador que está a utilizar, 127.0.0.1 designa sempre o seu computador local. Este endereço também é denominado localhost, visto que o localhost do nome do computador será sempre convertido no endereço IP 127.0.0.1. Isto significa que o computador está a tentar atacar-se a si mesmo? Estará algum Troiano ou spyware a tentar controlar o computador? Provavelmente não. Muitos programas legítimos utilizam o endereço de loopback para comunicação entre componentes. Por exemplo, muitos servidores de correio electrónico pessoal ou servidores Web podem ser configurados através de uma interface Web que normalmente é acedida através de um endereço semelhante a http://localhost/.

No entanto, o Firewall permite tráfego desses programas, pelo que, se forem apresentados eventos de 127.0.0.1, isso significa que o endereço IP de origem é fraudulento ou falso. Normalmente, os pacotes falsificados são um sinal de que alguém está a procurar Troianos. É importante lembrar que o Firewall bloqueia esta tentativa. Obviamente que reportar eventos a partir de 127.0.0.1 não tem qualquer utilidade, pelo que é desnecessário fazê-lo.

Assim sendo, alguns programas, nomeadamente o Netscape 6.2 e posterior, requerem que o endereço 127.0.0.1 seja adicionado à lista **Endereços IP de Confiança**. Os componentes destes programas comunicam entre si de um modo que o Firewall não consegue determinar se o tráfego é local ou não.

No exemplo do Netscape 6.2, se não considerar o endereço 127.0.0.1 fidedigno, não poderá utilizar a sua lista de amigos. Desta forma, se receber tráfego de 127.0.0.1 e todos os programas do computador funcionarem normalmente, então é seguro bloquear esse tráfego. No entanto, se um programa (como o Netscape) estiver com problemas, adicione 127.0.0.1 à lista **Endereços IP de Confiança** do Firewall e, em seguida, verifique se o problema ficou resolvido.

Se a introdução de 127.0.0.1 na lista **Endereços IP de Confiança** resolver o problema, será necessário analisar as opções: se considerar o endereço 127.0.0.1 fidedigno, o programa funcionará, mas estará mais vulnerável a ataques fraudulentos. Se não confiar no endereço, o programa não funcionará, mas continuará protegido contra qualquer tráfego malicioso.

Eventos de computadores na rede local

Para a maioria das definições de LAN empresarial, pode confiar em todos os computadores da rede local.

Eventos de endereços IP privados

Os endereços IP no formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 são referidos como endereços IP privados ou não encaminháveis. Estes endereços IP nunca devem sair da rede e, na maioria das vezes, podem ser considerados fidedignos.

O bloco 192.168 é usado com o Microsoft Internet Connection Sharing (ICS). Se estiver a utilizar o ICS e vir eventos deste bloco de IPs, poderá pretender adicionar o endereço IP 192.168.255.255 à respectiva lista de **Endereços IP de Confiança**. Isto tornará todo o bloco 192.168.xxx.xxx de confiança.

Se não estiver numa rede privada e receber eventos destes intervalos de endereços IP, é possível que o endereço IP de origem seja fraudulento ou falso. Normalmente, os pacotes falsificados são um sinal de que alguém está a procurar Troianos. É importante lembrar que o Firewall bloqueia esta tentativa.

Uma vez que os endereços IP privados estão separados dos endereços IP na Internet, a comunicação destes eventos não terá qualquer efeito.

Falsificação de IP

Falsificação dos endereços IP existentes num pacote IP. Esta técnica é utilizada em vários tipos de ataques, incluindo a utilização indevida de sessões. Esta técnica é também frequentemente utilizada para falsificar os cabeçalhos de correio publicitário não solicitado, para impedir que estes sejam correctamente rastreados.

firewall

Um sistema concebido para impedir o acesso não autorizado a uma rede privada. As firewalls podem ser implementadas em hardware, software, ou numa combinação dos dois. As firewalls são frequentemente utilizadas para impedir que utilizadores não autorizados acedam a redes privadas ligadas à Internet, especialmente a uma intranet. Todas as mensagens enviadas e recebidas pela intranet passam pela firewall. A firewall examina todas as mensagens e bloqueia as mensagens que não correspondem aos critérios de segurança especificados. As firewalls são consideradas a primeira linha de defesa na protecção das informações privadas. Para maior segurança, os dados podem ser encriptados.

Gateway integrado

Um dispositivo que combina as funções de um ponto de acesso (AP), de um router e de um firewall. Alguns dispositivos também podem incluir melhoramentos de segurança e funcionalidades de bridging.

grupos de classificação de conteúdos

Escalões etários a que um utilizador pertence O conteúdo é classificado (isto é, disponibilizado ou bloqueado), com base no grupo de classificação de conteúdos ao qual o utilizador pertence. Os grupos de classificação de conteúdos incluem: criança pequena, criança, adolescente mais novo, adolescente mais velho e adulto.

hotspot

Uma localização geográfica especifica em que um ponto de acesso (AP) fornece serviços públicos de banda larga aos utilizadores móveis através de uma rede sem fios. Os hotspots encontram-se frequentemente localizados em áreas de grande movimento, tais como aeroportos, estações ferroviárias, bibliotecas, marinas, centros de convenções e hotéis. Os hotspots dispõem normalmente de um alcance reduzido.

Internet

A Internet é composta por um grande número de redes interligadas que utilizam protocolos TCP/IP para localização e transferência de dados. A Internet surgiu a partir de uma rede criada para ligar computadores de universidades e faculdades (no fim da década de 60 e início de 70), fundada pelo Departamento de Defesa dos E.U.A. e era denominada ARPANET. Actualmente, a Internet é uma rede global de aproximadamente 100.000 redes independentes.

intranet

Rede privada, normalmente dentro de uma organização, que funciona da mesma maneira que a Internet. Tornou-se prática comum permitir o acesso a Intranets a partir de computadores autónomos utilizados por alunos ou funcionários remotos. As firewalls, os procedimentos de início de sessão e as palavras-passe são utilizados para proporcionar segurança.

LAN (Rede Local)

Uma rede de computadores que abrange uma área relativamente pequena. A maior parte das LANs estão confinadas a um só edifício ou a um grupo de edifícios. No entanto, uma LAN pode estar ligada a outras LANs através de linhas telefónicas e ondas de rádio. Um sistema de LANs interligado deste modo é chamado uma rede alargada (WAN). A maior parte das LANs interligam estações de trabalho e computadores pessoais através de concentradores ou comutadores simples. Cada nó (computador individual) existente numa LAN tem uma CPU própria com a qual executa programas, mas também pode aceder a dados e dispositivos (por ex.: impressoras) localizados em qualquer ponto da LAN. Isto permite que os utilizadores partilhem dispositivos dispendiosos, tais como impressoras laser, bem como dados. Os utilizadores também podem utilizar a LAN para comunicarem entre si (por exemplo, enviando mensagens de correio electrónico ou participando em sessões de conversação).

largura de banda

A quantidade de dados que pode ser transmitida num período de tempo fixo. Nos dispositivos digitais, a largura de banda é normalmente indicada em bits por segundo (bps) ou em bytes por segundo. Nos dispositivos analógicos, a largura de banda é indicada em ciclos por segundo, ou Hertz (Hz).

limitações de acesso

Definições que permitem configurar classificações de conteúdos que restringem o acesso a Web sites e conteúdos a utilizadores, bem como tempos limite da Internet que especificam o período e a duração do acesso dos utilizadores à Internet. As limitações de acesso também permitem restringir universalmente o acesso a Web sites específicos e conceder e bloquear acesso com base em permissões e palavras-chave por grupos etários.

lista de sites bloqueados

Uma lista de Web sites considerados maliciosos. Um Web site pode ser colocado numa lista negra, por actuação fraudulenta ou por explorar a vulnerabilidade do browser para enviar ao utilizador programas potencialmente indesejados.

lista de sites seguros

Lista de sites Web cujo acesso é permitido por não serem considerados fraudulentos.

localização com monitorização abrangente

Uma pasta (e todas as subpastas) do computador sujeita a monitorização para detecção de alterações pela Cópia de Segurança de Dados. Se tiver definido uma localização de monitorização abrangente, a Cópia de Segurança de Dados efectua a cópia de segurança dos tipos de ficheiros monitorizados dentro da pasta e respectivas subpastas.

localizações com monitorização superficial

Uma pasta do computador sujeita a monitorização para detecção de alterações efectuadas pelo Data Backup. Se tiver definido uma localização para monitorização superficial, o Data Backup efectua a cópia de segurança dos tipos de ficheiros monitorizados dentro da pasta, mas não inclui as respectivas subpastas.

localizações monitorizadas

Pastas do computador monitorizadas pelo Data Backup.

MAC (Controlo de Acesso a Suportes de Dados ou Código de Autenticação da Mensagem)

Para o primeiro, consulte Endereço MAC. O último é um código utilizado para identificar uma mensagem específica (por ex.: uma mensagem RADIUS). O código é, geralmente, um hash criptograficamente forte do conteúdo da mensagem, que inclui um valor exclusivo de protecção contra a reprodução.

mapeamento de rede

No Network Manager, corresponde a uma representação gráfica dos computadores e dos componentes que fazem parte de uma rede doméstica.

nó

Um único computador ligado a uma rede.

palavra-chave

Palavra que pode atribuir a um ficheiro do qual foi efectuada uma cópia de segurança para estabelecer uma relação ou uma ligação com outros ficheiros aos quais foi atribuída a mesma palavra-chave. A atribuição de palavras-chave a ficheiros facilita a procura de ficheiros publicados na Internet.

palavra-passe

Código (normalmente alfanumérico) utilizado para obter acesso ao computador ou a um determinado programa ou Web site.

partilha

Operação que permite que os destinatários do correio electrónico tenham acesso a ficheiros com cópia de segurança durante um período de tempo limitado. Quando partilha um ficheiro, envia uma cópia de segurança do ficheiro para os destinatários do correio electrónico que especificar. Os destinatários recebem a mensagem de correio electrónico a partir do Data Backup, com a indicação de que os ficheiros foram partilhados com os mesmos. A mensagem de correio electrónico inclui ainda uma ligação para os ficheiros partilhados.

phishing

Pronuncia-se como "fishing" e é um esquema fraudulento para obter ilicitamente informações valiosas, tais como números de cartões de crédito e de segurança social, IDs de utilizador e palavras-passe. Uma mensagem de correio electrónico com um aspecto aparentemente oficial é enviada para as potenciais vítimas, alegadamente como sendo proveniente do seu fornecedor de serviços Internet, banco ou revendedor. As mensagens de correio electrónico podem ser enviadas para pessoas constantes em listas seleccionadas ou em qualquer lista, na expectativa de que uma parte dos destinatários tenha realmente uma conta na verdadeira organização.

Placa de Rede

Uma placa que é ligada a um computador portátil ou outro dispositivo, permitindo-lhe aceder à LAN.

Ponto de Acesso (AP)

Um dispositivo de rede que permite que os clientes 802.11 acedam a uma rede local (LAN). Os APs aumentam o alcance físico dos utilizadores sem fios. Por vezes são chamados routers sem fios.

pontos de acesso não autorizados

Um ponto de acesso cujo funcionamento não seja autorizado por uma empresa. O problema é que os pontos de acesso não autorizados não respeitam, de uma maneira geral, as políticas de segurança das LANs sem fios (WLANs). Um ponto de acesso não autorizado constitui uma interface aberta e não protegida para a rede empresarial a partir do exterior das respectivas instalações.

Numa WLAN devidamente protegida, os pontos de acesso não autorizados são mais prejudiciais do que os utilizadores não autorizados. Os utilizadores não autorizados que tentem aceder a uma WLAN terão poucas hipóteses de alcançar recursos empresariais valiosos se os mecanismos de autenticação adequados estiverem activos. No entanto, a ligação de um ponto de acesso não autorizado por um funcionário ou um hacker origina problemas muito mais graves. Estes pontos de acesso não autorizados permitem que praticamente qualquer pessoa com um dispositivo compatível com 802.11 aceda à rede empresarial. Isto coloca qualquer pessoa muito perto dos recursos críticos.

pop-ups

Pequenas janelas que aparecem por cima de outras janelas no ecrã do computador. As janelas de pop-up são frequentemente utilizadas em Web browsers para apresentação de anúncios. A McAfee bloqueia as janelas de pop-up que são automaticamente transferidas quando abre uma página Web no browser. As janelas de pop-up que são transferidas quando clica numa ligação não são bloqueadas pela McAfee.

porta

Local por onde as informações passam para entrar ou sair de um computador; por exemplo, um modem analógico convencional está ligado a uma porta série. Os números de porta em comunicações TCP/IP são valores virtuais utilizados para separar tráfego em fluxos específicos de aplicações. As portas são atribuídas a protocolos padrão como SMTP ou HTTP para que os programas saibam quais as portas a utilizar para tentar estabelecer uma ligação. A porta de destino para pacotes TCP indica a aplicação ou o servidor procurado.

PPPoE

Point-to-Point Protocol Over Ethernet. Utilizado por muitos fornecedores de DSL, o PPPoE suporta as camadas de protocolo e a autenticação utilizadas no PPP, permitindo o estabelecimento de uma ligação ponto-a-ponto na arquitectura multiponto da Ethernet.

programa potencialmente indesejado

Os programas potencialmente indesejados incluem spyware, adware e outros programas que recolhem e transmitem dados do utilizador sem a sua permissão.

Protecções do Sistema

As Protecções do Sistema detectam alterações não autorizadas no computador e alertam-no quando estas ocorrem.

protocolo

Um formato acordado para a transmissão de dados entre dois dispositivos. Do ponto de vista do utilizador, o único aspecto interessante dos protocolos é que o respectivo computador ou dispositivo tem de suportar os protocolos adequados para comunicar com outros computadores. O protocolo pode ser implementado por hardware ou software.

proxy

Computador (ou software executado no mesmo) que funciona como barreira entre uma rede e a Internet, apresentando apenas um endereço de rede para sites externos. Ao agir como intermediário representando todos os computadores internos, o proxy protege identidades de rede ao mesmo tempo que fornece acesso à Internet. Consulte também Servidor Proxy.

publicar

Disponibilizar publicamente na Internet um ficheiro do qual foi efectuada uma cópia de segurança.

quarentena

Quando são detectados ficheiros suspeitos, estes são colocados em quarentena. Pode então tomar as medidas apropriadas.

RADIUS (Remote Access Dial-In User Service)

Um protocolo que permite a autenticação de utilizadores, normalmente no contexto do acesso remoto. Originalmente definido para utilização com servidores de acesso telefónico remoto, o protocolo é agora utilizado numa vasta gama de ambientes de autenticação, incluindo a autenticação 802.1x do Segredo Partilhado dos utilizadores de uma WLAN.

rede

Quando liga dois ou mais computadores, cria uma rede.

rede gerida

Uma rede doméstica com dois tipos de membros: membros geridos e membros não geridos. Os membros geridos permitem que outros computadores da rede monitorizem o respectivo estado de protecção McAfee; os membros não geridos não o permitem.

repositório de cópia de segurança online

Localização do servidor online onde os ficheiros monitorizados são guardados depois de ter sido efectuada a cópia de segurança.

restaurar

Para repor uma cópia de um ficheiro a partir de um arquivo ou do repositório de cópias de segurança online.

roaming

A capacidade de passar da área de cobertura de um ponto de acesso para outra sem interrupção do serviço ou perda de conectividade.

router

Um dispositivo de rede que encaminha pacotes entre redes. Com base nas tabelas de encaminhamento internas, os routers lêem cada pacote recebido e decidem como o devem encaminhar. A interface de destino dos pacotes enviados pelo router pode ser determinada por qualquer combinação de endereços de origem e destino, bem como pelas condições actuais de tráfego, tal como a carga, os custos das linhas e a existência de linhas danificadas. Por vezes é referido como ponto de acesso.

script

Os scripts podem criar, copiar ou eliminar ficheiros. Podem também abrir o Registo do Windows.

segredo partilhado

Consulte também RADIUS. Protege partes sensíveis de mensagens RADIUS. Este segredo partilhado é uma palavra-passe que é partilhada entre o autenticador e o servidor de autenticação de modo seguro.

servidor

Computador ou software que fornece serviços específicos ao software em execução noutros computadores. O "servidor de correio" no ISP é um software que processa todas as mensagens enviadas e recebidas dos utilizadores. Um servidor numa rede local é um hardware que constitui o nó principal da rede. Também poderá conter software que forneça serviços específicos, dados ou outros recursos a todos os computadores clientes ligados ao mesmo.

Servidor DNS

Versão abreviada do servidor de sistema de nomes de domínios. Um computador capaz de responder a consultas do sistema de nomes de domínios (DNS). O servidor DNS dispõe de uma base de dados de computadores anfitriões e respectivos endereços IP. Confrontado com o nome apex.com, por exemplo, o servidor DNS devolve o endereço IP da empresa hipotética Apex. Também designado: servidor de nomes. Consulte também DNS e Endereço IP.

servidor proxy

Componente de firewall que gere o tráfego de Internet de e para uma rede local. Um servidor proxy pode melhorar o desempenho ao fornecer dados pedidos com frequência, como, por exemplo, uma página Web popular, e consegue filtrar e ignorar pedidos que o proprietário não considera adequados, como pedidos de acesso não autorizado a ficheiros de propriedade.

Servidor SMTP

Sigla do protocolo de transferência de correio simples, Simple Mail Transfer Protocol. Um protocolo TCP/IP para o envio de mensagens de um computador para outro numa rede. Este protocolo é utilizado na Internet para encaminhamento de correio electrónico.

sincronizar

Permite resolver problemas de inconsistência entre ficheiros com cópia de segurança e ficheiros guardados no computador local. Sincroniza-se ficheiros quando a versão do ficheiro no repositório de cópias de segurança online é mais recente do que a versão do ficheiro existente nos outros computadores. A sincronização actualiza a cópia do ficheiro nos computadores com a versão do ficheiro existente no repositório de cópias de segurança online.

sobrecarga da memória temporária

As sobrecargas da memória temporária ocorrem quando programas ou processos suspeitos tentam armazenar numa memória temporária (área de armazenamento de dados temporário) mais dados do que o limite suportado, danificando ou substituindo dados válidos nas memórias temporárias adjacentes.

SSID (Identificador do Conjunto de Serviços)

Nome da rede para os dispositivos num subsistema de LAN sem fios. Trata-se de uma cadeia de 32 caracteres, em texto limpo, adicionada ao cabeçalho de cada pacote de uma WLAN. O SSID diferencia as WLANs, pelo que todos os utilizadores de uma rede têm de fornecer o mesmo SSID para acederem a um determinado ponto de acesso. Um SSID impede o acesso a qualquer dispositivo cliente que não possua o SSID. No entanto, por predefinição, os pontos de acesso difundem o respectivo SSID no sinalizador. Mesmo que a difusão do SSID esteja desactivada, um hacker poderá detectar o SSID utilizando aplicações de intercepção (sniffing).

SSL (Secure Sockets Layer)

Protocolo desenvolvido pela Netscape para a transmissão de documentos privados através da Internet. O SSL funciona através da utilização de uma chave pública para encriptar os dados que são transferidos através da ligação SSL. O Netscape Navigator e o Internet Explorer utilizam e suportam o SSL e muitos Web sites utilizam o protocolo para obterem informações confidenciais dos utilizadores, tais como números de cartões de crédito. Por convenção, os URLs que requerem uma ligação SSL começam com https: em vez de http:

texto cifrado

Dados que foram encriptados. O texto cifrado não é legível até ser convertido em texto simples (desencriptado) com uma chave.

texto simples

Qualquer mensagem que não está encriptada.

tipos de ficheiros monitorizados

Tipos de ficheiros (por exemplo, .doc, .xls, etc.) que o Data Backup copia ou arquiva nas localizações de monitorização.

TKIP (Temporal Key Integrity Protocol)

Um método de resolução dos pontos fracos inerentes à segurança WEP, especialmente a reutilização de chaves de encriptação. O TKIP altera as chaves temporais a cada 10.000 pacotes, proporcionando um método de distribuição dinâmica que melhora significativamente a segurança da rede. O processo de segurança do TKIP começa com uma chave temporal de 128 bits que é partilhada entre os clientes e os pontos de acesso. O TKIP combina a chave temporal com o endereço MAC das máquinas clientes e, em seguida, adiciona um vector de inicialização de 16 octetos, relativamente grande, para produzir a chave que encripta os dados. Este procedimento assegura que cada estação utiliza sequências de chaves diferentes para encriptar os dados. O TKIP utiliza o RC4 para a encriptação. O WEP também utiliza o RC4.

unidade de disco rígido externa

Disco instalado fora da caixa do computador.

unidade de rede

Uma unidade de disco ou uma unidade de banda que está ligada a um servidor de uma rede e que é partilhada por vários utilizadores. As unidades de rede são por vezes designadas unidades remotas.

URL

Uniform Resource Locator. É o formato padrão para endereços da Internet.

VPN (Rede Privada Virtual)

Uma rede criada através da utilização de cablagem pública para a interligação de nós. Por exemplo, existem vários sistemas que lhe permitem criar redes utilizando a Internet como meio de transporte dos dados. Estes sistemas utilizam encriptação e outros mecanismos de segurança para garantir que apenas os utilizadores autorizados podem aceder à rede e que os dados não podem ser interceptados.

wardriver

Hackers móveis, equipados com computadores portáteis, software especial e algum hardware alterado, que viajam de automóvel pelas cidades, subúrbios e parques de estacionamento para interceptarem o tráfego de LANs sem fios.

WEP (Wired Equivalent Privacy)

Um protocolo de encriptação e autenticação definido como parte da norma 802.11. As versões iniciais são baseadas em cifras RC4 e têm vários pontos fracos. O WEP tenta proporcionar segurança, encriptando os dados transmitidos através das ondas de rádio, de modo a que estes estejam protegidos enquanto viajam entre dois pontos. No entanto, chegou-se à conclusão que o WEP não é tão seguro como se pensava inicialmente.

Wi-Fi (Wireless Fidelity)

Termo utilizado genericamente para referir qualquer tipo de rede 802.11, quer seja 802.11b, 802.11a, banda dupla, etc. Este termo é utilizado pela Wi-Fi Alliance.

Wi-Fi Alliance

Uma organização composta pelos principais fabricantes de equipamento e software sem fios, tendo em vista (1) certificar a interoperacionalidade de todos os produtos baseados na norma 802.11 e (2) promover o termo Wi-Fi, como marca global, para qualquer produto de LAN sem fios baseado na norma 802.11. Esta organização age como um consórcio, laboratório de testes e ponto de encontro para todos os fabricantes que pretendam promover a interoperacionalidade e o crescimento da indústria.

Apesar de todos os produtos 802.11a/b/g serem denominados Wi-Fi, apenas os produtos que passaram os testes da Wi-Fi Alliance estão autorizados a ser referenciados como Wi-Fi Certified (uma marca registada). As embalagens dos produtos que passaram estes testes têm de apresentar um selo identificativo com a marca Wi-Fi Certified e a banda de frequências de rádio utilizada. Este grupo chamava-se anteriormente Wireless Ethernet Compatibility Alliance (WECA), mas mudou o respectivo nome em Outubro de 2002 para melhor reflectir a marca Wi-Fi que pretende criar.

Wi-Fi Certified

Quaisquer produtos testados e aprovados como Wi-Fi Certified (uma marca registada) pela Wi-Fi Alliance têm a garantia de serem interoperacionais entre si, mesmo que provenham de fabricantes diferentes. Um utilizador com um produto Wi-Fi Certified pode utilizar qualquer marca de ponto de acesso com qualquer outra marca de hardware cliente que também seja certificado. No entanto, normalmente, qualquer produto Wi-Fi que utilize a mesma frequência de rádio (por exemplo: 2,4 GHz para a 802.11b ou 11g, 5 GHz para a 802.11a) funciona com outro produto que utilize a mesma frequência de rádio, mesmo que este não seja Wi-Fi Certified.

WLAN (Rede Local sem Fios)

Consulte também LAN. Uma rede local que utiliza um suporte sem fios como ligação. Uma WLAN utiliza ondas de rádio de alta frequência para comunicar entre os nós, em vez de fios.

worm

Um worm é um vírus de replicação automática que reside na memória activa e que pode enviar cópias de si próprio através de mensagens de correio electrónico. Os worms replicam-se e consomem recursos do sistema, diminuindo o desempenho ou parando tarefas.

WPA (Wi-Fi Protected Access)

Uma norma que aumenta o nível de protecção de dados e controlo de acesso para os sistemas de LAN sem fios actuais e futuros. Concebido para funcionar no hardware existente, sob a forma de uma actualização de software, o WPA deriva e é compatível com a norma IEEE 802.11i. Quando instalado de modo correcto, fornece aos utilizadores da LAN sem fios um elevado grau de confiança em que os respectivos dados permanecem protegidos e que apenas os utilizadores autorizados da rede podem aceder a esta.

WPA-PSK

Um modo especial do WPA concebido para utilizadores domésticos que não requerem segurança de nível empresarial e que não dispõem de acesso a servidores de autenticação. Neste modo, o utilizador doméstico introduz manualmente a palavra-passe inicial para activar o Wi-Fi Protected Access no modo de Chave Pré-Partilhada, devendo alterar a frase-passe em cada computador e ponto de acesso sem fios regularmente. Consulte também WPA2-PSK e TKIP.

WPA2

Consulte também WPA. WPA2 é uma actualização da norma de segurança WPA e baseia-se na norma IEEE 802.11i.

WPA2-PSK

Consulte também WPA-PSK e WPA2. O WPA2-PSK é semelhante ao WPA-PSK e baseia-se na norma WPA2. Uma funcionalidade comum do WPA2-PSK é o facto de os dispositivos normalmente suportarem vários modos de encriptação (ex.: AES, TKIP) em simultâneo, enquanto que os dispositivos mais antigos, geralmente, suportavam apenas um único modo de encriptação de cada vez (isto é, todos os clientes teriam de utilizar o mesmo modo de encriptação).

Acerca da McAfee

A McAfee, Inc., com sede em Santa Clara, Califórnia (EUA), é o líder global em Prevenção de Intrusões e Gestão de Riscos de Segurança, fornecendo soluções e serviços preventivos e comprovados destinados a proteger sistemas e redes em todo o mundo. Graças aos seus conhecimentos ímpares na área da segurança e ao compromisso de inovação, a McAfee permite que utilizadores domésticos, empresas, o sector público e fornecedores de serviços possam bloquear ataques, impedir interrupções e controlar e melhorar continuamente a respectiva segurança.

Copyright

Índice remissivo

C

Ch

C

D

N

O

P

V

W