McAfee®

VirusScan® Plus

AntiVirus, Firewall & AntiSpyware

Manual do Utilizador

Índice

CAPÍTULO 1

Introdução

Equipe o seu computador com a segurança combinada da firewall, análise de vírus e tecnologias de protecção contra spyware da McAfee. Pode utilizar o VirusScan Plus para proteger o seu computador contra vírus, monitorizar o tráfego da Internet em relação a actividade suspeita e bloquear spyware para evitar pôr em perigo a integridade da suas informações pessoas.

Neste capítulo

CAPÍTULO 2

McAfee SecurityCenter

O McAfee SecurityCenter permite monitorizar o estado de segurança do computador, saber instantaneamente se os serviços de protecção antivírus, anti-spyware, de correio electrónico e de firewall estão actualizados e adoptar medidas sobre potenciais vulnerabilidades de segurança. Fornece os controlos e as ferramentas de navegação necessários para coordenar e gerir todas as áreas da protecção do computador.

Antes de começar a configurar e gerir a protecção do computador, analise a interface do SecurityCenter e certifique-se de que compreende a diferença entre estado de protecção, categorias de protecção e serviços de protecção. Em seguida, actualize o SecurityCenter para assegurar que possui a mais recente protecção disponível da McAfee.

Depois de concluir as tarefas de configuração iniciais, utilize o SecurityCenter para monitorizar o estado de protecção do computador. Se o SecurityCenter detectar um problema de protecção, apresenta um alerta para que possa corrigi-lo ou ignorá-lo (dependendo da gravidade). Também pode analisar eventos do SecurityCenter, tais como alterações à configuração da análise de vírus, num registo de eventos.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

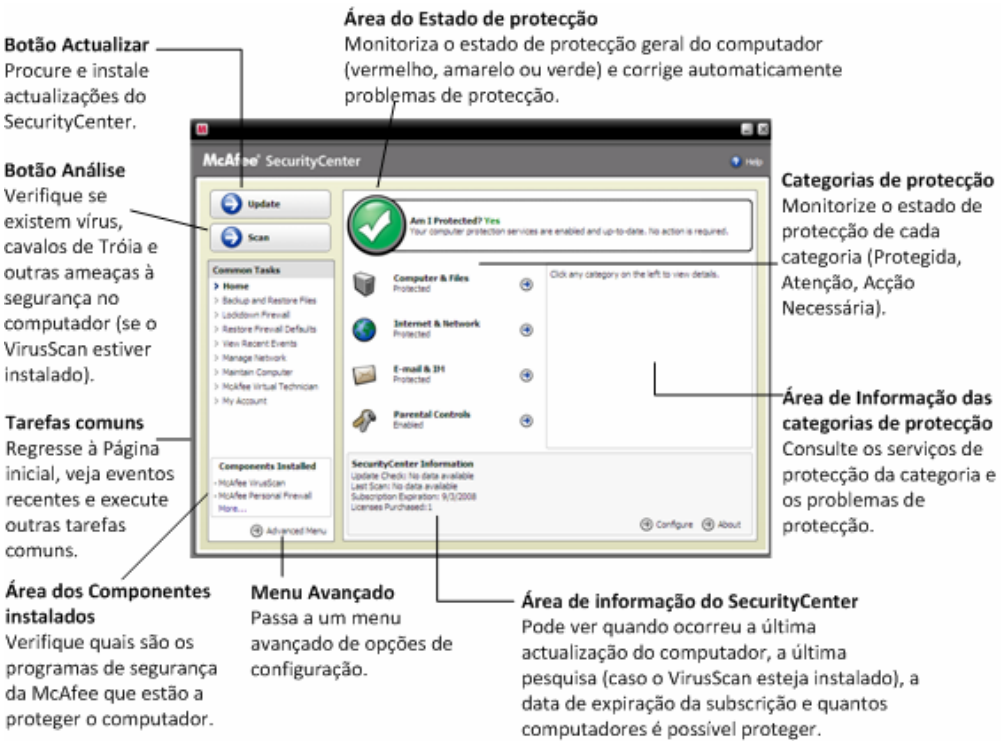
Funcionalidades do SecurityCenter

Estado de protecção simplificado	Analisa facilmente o estado de protecção do computador, procura actualizações e corrige problemas de protecção.
Actualizações automatizadas	O SecurityCenter transfere e instala automaticamente actualizações para os seus programas. Quando está disponível uma nova versão de um programa da McAfee, a mesma é fornecida automaticamente ao computador desde que a subscrição seja válida, garantindo sempre uma protecção actualizada.
Alertas em tempo real	Os alertas de segurança informam-no acerca de surtos de vírus de emergência e ameaças de segurança.

CAPÍTULO 3

Utilizar o SecurityCenter

Antes de começar a utilizar o SecurityCenter, analise os componentes e as áreas de configuração que utilizará para gerir o estado de protecção do computador. Para obter mais informações acerca da terminologia utilizada nesta imagem, consulte as secções Noções sobre o estado de protecção (página 8) e Noções sobre categorias de protecção (página 9). Em seguida, pode analisar a informação da sua conta McAfee e verificar a validade da subscrição.



Neste capítulo

Noções sobre o estado de protecção

O estado de protecção do computador é apresentado na área do estado de protecção no painel Página Inicial do SecurityCenter. O estado indica se o computador está totalmente protegido contra as mais recentes ameaças de segurança e pode ser influenciado por factores como ataques de segurança externos, outros programas de segurança e programas que acedem à Internet.

O estado de protecção do computador pode apresentar as cores vermelha, amarela ou verde.

Estado de protecção	Descrição
Vermelho	O computador não está protegido. A cor vermelha da área do estado de protecção no painel Página Inicial do SecurityCenter indica que não está protegido. O SecurityCenter comunica, pelo menos, um problema de segurança crítico. Para obter protecção total, deve corrigir todos os problemas de segurança críticos em cada categoria de protecção (o estado da categoria do problema é definido para **Acção Necessária**, também a vermelho). Para obter informações sobre como corrigir problemas de protecção, consulte a secção Corrigir problemas de protecção (página 18).
Amarelo	O computador está parcialmente protegido. A cor amarela da área do estado de protecção no painel Página Inicial do SecurityCenter indica que não está protegido. O SecurityCenter comunica, pelo menos, um problema de segurança não crítico. Para obter protecção total, deve corrigir ou ignorar os problemas de segurança não críticos associados a cada categoria de protecção. Para obter informações sobre como corrigir ou ignorar problemas de protecção, consulte a secção Corrigir ou ignorar problemas de protecção (página 17).
Verde	O computador está totalmente protegido. A cor verde da área do estado de protecção no painel Página Inicial do SecurityCenter indica que está protegido. O SecurityCenter não comunica quaisquer problemas de segurança críticos ou não críticos. Cada categoria de protecção lista os serviços que estão a proteger o computador.

Noções sobre categorias de protecção

Os serviços de protecção do SecurityCenter estão divididos em quatro categorias: Computador e Ficheiros, Internet e Rede, Correio Electrónico e Mensagens Instantâneas e Limitações de Acesso. Estas categorias ajudam-no a procurar e a configurar os serviços de segurança que protegem o computador.

Clique no nome de uma categoria para configurar os respectivos serviços de protecção e ver os problemas de segurança detectados para esses serviços. Se o estado de protecção do computador apresentar as cores vermelha ou amarela, uma ou mais categorias apresentam as mensagens *Acção Necessária* ou *Atenção* para indicar que o SecurityCenter detectou um problema na categoria. Para obter mais informações sobre o estado de protecção, consulte a secção Noções sobre o estado de protecção (página 8).

Categoria de Protecção	Descrição
Computador e Ficheiros	A categoria Computador e Ficheiros permite configurar os seguintes serviços de protecção: ▪ Protecção Antivírus ▪ Protecção Anti-Spyware ▪ Protecções do Sistema ▪ Protecção do Windows ▪ Saúde do PC
Internet e Rede	A categoria Internet e Rede permite configurar os seguintes serviços de protecção: ▪ Protecção por Firewall ▪ Protecção Contra Phishing ▪ Protecção de Identidade
Correio Electrónico e Mensagens Instantâneas	A categoria Correio Electrónico e Mensagens Instantâneas permite configurar os seguintes serviços de protecção: ▪ Protecção Antivírus do Correio Electrónico ▪ Protecção Antivírus das Mensagens Instantâneas ▪ Protecção Anti-Spyware do Correio Electrónico ▪ Protecção Anti-Spyware das Mensagens Instantâneas ▪ Protecção contra Correio Publicitário Não Solicitado

Categoria de Protecção	Descrição
Limitações de Acesso	A categoria Limitações de Acesso permite configurar os seguintes serviços de protecção: ▪ Bloqueio de Conteúdos

Noções sobre serviços de protecção

Os serviços de protecção correspondem aos vários componentes de segurança que deve configurar para proteger o computador e os ficheiros. Os serviços de protecção correspondem directamente a programas da McAfee. Por exemplo, com a instalação do VirusScan, ficam disponíveis os seguintes serviços de protecção: Protecção Antivírus, Protecção Anti-Spyware, Protecções do Sistema e Análise de Scripts. Para obter informações detalhadas sobre estes serviços de protecção específicos, consulte a ajuda do VirusScan.

Por predefinição, todos os serviços de protecção associados a um programa são activados quando o programa é instalado; no entanto, é possível desactivar um serviço de protecção em qualquer altura. Por exemplo, se instalar as Limitações de Acesso, tanto o Bloqueio de Conteúdos, como a Protecção de Identidade, são activados. Se não pretender utilizar o serviço de protecção Bloqueio de Conteúdos, pode desactivá-lo totalmente. Também pode desactivar temporariamente um serviço de protecção enquanto executa tarefas de configuração ou de manutenção.

Gerir as subscrições

Cada produto de protecção McAfee adquirido é fornecido com uma subscrição que permite a sua utilização num determinado número de computadores durante um determinado período de tempo. A duração da subscrição varia de acordo com a aquisição, mas normalmente tem início assim que activa o produto. A activação é simples e gratuita, necessitando apenas de uma ligação à Internet, mas é muito importante uma vez que permite receber actualizações do produto regulares e automáticas, que mantêm o computador protegido contra as mais recentes ameaças.

Normalmente, a activação ocorre quando o produto é instalado, mas se optar por esperar (por exemplo, se não tiver uma ligação à Internet), terá 15 dias para efectuar a activação. Se não activar durante os 15 dias, os seus produtos deixarão de receber actualizações críticas ou efectuar análises. Também será notificado periodicamente (através de mensagens apresentadas no ecrã) antes de a subscrição expirar. Dessa forma, poderá evitar interrupções na protecção renovando-a antecipadamente ou configurando a renovação automática no nosso Web site.

A presença de uma ligação no SecurityCenter solicitando a activação significa que a subscrição não foi activada. Para ver a data de validade da subscrição, pode consultar a página Conta.

Aceder à conta McAfee

Pode aceder facilmente às informações da sua conta McAfee (página Conta) a partir do SecurityCenter.

1. Em **Tarefas Comuns**, clique em **A Minha Conta**.
2. Inicie sessão na sua conta McAfee.

Activar os produtos

Normalmente, a activação ocorre quando instala o produto. Se tal não acontecer, aparecerá uma ligação no SecurityCenter solicitando que efectue a activação. Também será notificado periodicamente.

- No painel Página Inicial do SecurityCenter, em **Informações sobre o SecurityCenter**, clique em **Active a sua subscrição**.

Sugestão: Também pode efectuar a activação a partir do alerta apresentado periodicamente.

Verifique a subscrição

Deve verificar a sua subscrição para assegurar-se de que ainda não expirou.

- Clique com o botão direito do rato no ícone do SecurityCenter na área de notificação, na parte mais à direita da barra de tarefas e, em seguida, clique em **Verificar Subscrição**.

Renovar a subscrição

Pouco antes de a subscrição expirar, aparecerá uma ligação no SecurityCenter solicitando que efectue a renovação. Também será notificado periodicamente sobre a expiração pendente através de alertas.

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

Sugestão: Também pode renovar o produto a partir da mensagem de notificação apresentada periodicamente. Em alternativa, vá para a página Conta, na qual poderá efectuar a renovação ou configurar a renovação automática.

CAPÍTULO 4

Actualizar o SecurityCenter

O SecurityCenter assegura que os seus programas registados da McAfee estão actualizados ao procurar e instalar actualizações online de quatro em quatro horas. Dependendo dos programas que tiver instalado e activado, as actualizações online podem incluir as mais recentes definições de vírus e actualizações de protecção de privacidade, contra hackers, correio publicitário não solicitado ou spyware. Se pretender verificar a existência de actualizações durante o período predefinido de quatro horas, pode fazê-lo em qualquer altura. Enquanto o SecurityCenter verifica a existência de actualizações, pode continuar a executar outras tarefas.

Embora não seja recomendado, pode alterar a forma como o SecurityCenter verifica e instala as actualizações. Por exemplo, pode configurar o SecurityCenter para transferir e não instalar as actualizações ou para o notificar antes de transferir ou instalar as actualizações. Também pode desactivar a actualização automática.

Nota: Se tiver instalado o produto McAfee a partir de um CD, terá de efectuar a activação num prazo de 15 dias ou os produtos não receberão actualizações críticas nem efectuarão análises.

Neste capítulo

Verificar a existência de actualizações

Por predefinição, o SecurityCenter verifica automaticamente a existência de actualizações de quatro em quatro horas quando o computador está ligado à Internet; no entanto, se pretender verificar a existência de actualizações dentro do período de quatro horas, pode fazê-lo. Se tiver desactivado as actualizações automáticas, deve verificar regularmente se existem actualizações.

- No painel Página Inicial do SecurityCenter, clique em **Actualizar**.

Sugestão: Para verificar a existência de actualizações sem iniciar o SecurityCenter, clique com o botão direito do rato no ícone do SecurityCenter na área de notificação, na parte mais à direita da barra de tarefas e, em seguida, clique em **Actualizações**.

Configurar actualizações automáticas

Por predefinição, o SecurityCenter procura e instala automaticamente actualizações de quatro em quatro horas quando o computador está ligado à Internet. Se pretender alterar este comportamento predefinido, pode configurar o SecurityCenter para transferir automaticamente as actualizações e, em seguida, notificá-lo de que estas estão prontas para serem instaladas, ou notificá-lo antes de transferir as actualizações.

Nota: O SecurityCenter utiliza alertas para o notificar da existência de actualizações prontas para transferir ou instalar. A partir dos alertas, pode transferir ou instalar as actualizações ou adiar as actualizações. Ao actualizar os programas a partir de um alerta, poderá ser-lhe solicitado que verifique a sua subscrição antes de transferir e instalar. Para obter mais informações, consulte a secção Utilizar alertas (página 21).

1 Abra o painel de configuração do SecurityCenter.

   Como?

   1. Em **Tarefas Comuns**, clique em **Página Inicial**.
   2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.

2 No painel de configuração do SecurityCenter, em **As actualizações automáticas estão desactivadas**, clique em **Activar** e, em seguida, em **Avançadas**.

3 Clique num dos seguintes botões:

   - **Instalar as actualizações automaticamente e notificar-me quando os serviços forem actualizados (recomendado)**
   - **Transferir as actualizações automaticamente e notificar quando estiverem prontas para serem instaladas**
   - **Notificar antes de transferir quaisquer actualizações**

4 Clique em **OK**.

Desactivar as actualizações automáticas

Se desactivar as actualizações automáticas, passa a ser da sua responsabilidade verificar regularmente a existência de actualizações, caso contrário, o computador não terá a mais recente protecção de segurança. Para obter informações sobre a verificação manual de actualizações, consulte a secção Verificar a existência de actualizações (página 13).

1 Abra o painel de configuração do SecurityCenter.

   Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.

2 No painel de configuração do SecurityCenter, em **As actualizações automáticas estão activadas**, clique em **Desactivar**.

3 Na caixa de diálogo de confirmação, clique em **Sim**.

Sugestão: Para activar as actualizações automáticas, clique no botão **Activar** ou desmarque a opção **Desactivar as actualizações automáticas e deixar-me verificar manualmente se existem actualizações** no painel Opções de Actualização.

CAPÍTULO 5

Corrigir ou ignorar problemas de protecção

O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Os problemas críticos requerem uma acção imediata e comprometem o estado de protecção (a cor muda para vermelho) Os problemas de protecção não críticos não requerem uma acção imediata e podem ou não comprometer o estado de protecção (dependendo do tipo de problema). Para obter o estado de protecção verde, deve corrigir todos os problemas críticos e corrigir ou ignorar todos os problemas não críticos. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee. Para obter mais informações sobre o Técnico Virtual da McAfee, consulte a ajuda do Técnico Virtual da McAfee.

Neste capítulo

Resolução de problemas relacionados com protecção

A maioria dos problemas de segurança pode ser corrigida automaticamente; no entanto, alguns problemas poderão requerer a sua intervenção. Por exemplo, se a Protecção por Firewall estiver desactivada, o SecurityCenter pode activá-la automaticamente; no entanto, se não estiver instalada, terá de a instalar. A tabela seguinte descreve algumas acções que poderá ter de executar ao corrigir problemas de protecção manualmente:

Problema	Acção
Não foi executada uma análise completa do computador nos últimos 30 dias.	Analise o computador manualmente. Para obter mais informações, consulte a ajuda do VirusScan.
Os seus ficheiros de assinatura de detecção (DAT) estão desactualizados.	Actualize a protecção manualmente. Para obter mais informações, consulte a ajuda do VirusScan.
Um programa não está instalado.	Instale o programa a partir do Web site da McAfee ou de um CD.
Faltam componentes num programa.	Reinstale o programa a partir do Web site da McAfee ou de um CD.
Um programa não está activado e não pode receber protecção total.	Active o programa no Web site da McAfee.
A sua subscrição expirou.	Verifique o estado da sua conta no Web site da McAfee. Para mais informações, consulte Gerir as subscrições (página 11).

Nota: Muitas vezes, um único problema de protecção afecta mais do que uma categoria de protecção. Neste caso, a correcção do problema numa categoria resolve-o em todas as outras categorias de protecção.

Resolução automática de problemas de protecção

O SecurityCenter pode corrigir a maioria dos problemas de protecção automaticamente. As alterações de configuração efectuadas pelo SecurityCenter ao corrigir automaticamente problemas de protecção não são guardadas no registo de eventos. Para mais informações sobre eventos, consulte Ver Eventos (página 27).

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, na área do estado de protecção, clique em **Corrigir**.

Resolução manual de problemas de protecção

Se um ou mais problemas de protecção persistirem depois de tentar corrigi-los automaticamente, pode tentar corrigi-los manualmente.

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique na categoria de protecção em que o SecurityCenter comunica o problema.
3. Clique na ligação apresentada a seguir à descrição do problema.

Ignorar problemas de protecção

Se o SecurityCenter detectar um problema não crítico, pode optar por corrigi-lo ou ignorá-lo. Outros problemas não críticos (por exemplo, se os serviços de Anti-Spam ou Limitações de Acesso não estiverem instalados) são ignorados automaticamente. Os problemas ignorados não são apresentados na área de informação da categoria da protecção no painel Página Inicial do SecurityCenter, a menos que o estado de protecção do computador esteja verde. Se ignorar um problema e posteriormente decidir que pretende que o mesmo seja apresentado na área de informação da categoria de protecção mesmo que o estado de protecção do computador não esteja verde, pode mostrar o problema ignorado.

Ignorar um problema de protecção

É possível ignorar um problema não crítico detectado pelo SecurityCenter se não pretender corrigi-lo. Se ignorar o problema, este será removido da área de informação da categoria de protecção no SecurityCenter.

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique na categoria de protecção em que o problema é comunicado.
3. Clique na ligação **Ignorar** junto ao problema de protecção.

Mostrar ou ocultar problemas ignorados

Dependendo da gravidade, é possível mostrar ou ocultar um problema de protecção ignorado.

1. Abra o painel Opções de Alerta.

   Como?

   1. Em **Tarefas Comuns**, clique em **Página Inicial**.
   2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
   3. Em **Alertas**, clique em **Avançado**.

2. No painel Configuração do SecurityCenter, clique em **Problemas Ignorados**.
3. No painel Problemas Ignorados, proceda de um dos seguintes modos:
   - Para ignorar um problema, seleccione a caixa de verificação respectiva.
   - Para comunicar um problema na área de informação da categoria de protecção, desmarque a respectiva caixa de verificação.
4. Clique em **OK**.

Sugestão: Também pode clicar na ligação **Ignorar** junto ao problema comunicado na área de informação da categoria de protecção para o ignorar.

CAPÍTULO 6

Utilizar alertas

Os alertas são pequenas caixas de diálogo de pop-up que são apresentadas no canto inferior direito do ecrã quando ocorrem determinados eventos do SecurityCenter. Um alerta fornece informações detalhadas acerca de um evento, bem como recomendações e opções para a resolução de problemas que podem estar associados ao evento. Alguns alertas podem também conter ligações para informações adicionais acerca do evento. Essas ligações permitem aceder ao Web site global da McAfee ou enviar informações à McAfee para resolução de problemas.

Existem três tipos de alertas: vermelho, amarelo e verde.

Tipo de Alerta	Descrição
Vermelho	Um alerta vermelho é uma notificação crítica que requer uma resposta por parte do utilizador. Os alertas vermelhos ocorrem quando o SecurityCenter não consegue determinar a forma de corrigir automaticamente um problema de protecção.
Amarelo	Um alerta amarelo é uma notificação não crítica que, normalmente, requer uma resposta por parte do utilizador.
Verde	Um alerta vede é uma notificação não crítica que não requer uma resposta por parte do utilizador. Os alertas verdes fornecem informações básicas acerca de um evento.

Uma vez que os alertas desempenham um papel extremamente importante na monitorização e gestão do estado de protecção, não é possível desactivá-los. No entanto, é possível controlar se determinados tipos de alertas informativos são apresentados e configurar algumas opções de alerta (tais como se o SecurityCenter reproduz um som com o alerta ou se apresenta o ecrã inicial da McAfee no arranque).

Neste capítulo

Mostrar e ocultar alertas informativos

Os alertas informativos notificam-no quando ocorrem eventos que não constituem ameaças para a segurança do computador. Por exemplo, se tiver configurado a Protecção de Firewall, é apresentado um alerta informativo por predefinição sempre que um programa do computador for autorizado a aceder à Internet. Se não pretender que um determinado tipo de alerta informativo seja apresentado, pode ocultá-lo. Se não pretender visualizar quaisquer alertas informativos, pode ocultá-los todos. Também pode ocultar todos os alertas informativos quando está a jogar em modo de ecrã completo no computador. Quando terminar o jogo e sair do modo de ecrã completo, o SecurityCenter volta a apresentar os alertas informativos.

Se ocultar um alerta informativo acidentalmente, pode mostrá-lo novamente em qualquer altura. Por predefinição, o SecurityCenter mostra todos os alertas informativos.

Mostrar ou ocultar alertas informativos

É possível configurar o SecurityCenter para mostrar alguns alertas informativos e ocultar outros, bem como para ocultar todos os alertas informativos.

1 Abra o painel Opções de Alerta.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Configuração do SecurityCenter, clique em **Alertas Informativos**.

3 No painel Alertas Informativos, proceda de um dos seguintes modos:

- Para mostrar um alerta informativo, desmarque a respectiva caixa de verificação.
- Para ocultar um alerta informativo, seleccione a respectiva caixa de verificação.
- Para ocultar todos os alertas informativos, seleccione a caixa de verificação **Não mostrar alertas informativos**.

4 Clique em **OK**.

Sugestão: Também pode ocultar um alerta informativo seleccionando a caixa de verificação **Não mostrar este alerta novamente** no próprio alerta. Se o fizer, pode mostrar o alerta informativo novamente desmarcando a caixa de verificação adequada no painel Alertas Informativos.

Mostrar ou ocultar alertas informativos durante jogos

É possível ocultar todos os alertas informativos quando está a jogar em modo de ecrã completo no computador. Quando terminar o jogo e sair do modo de ecrã completo, o SecurityCenter volta a apresentar os alertas informativos.

1 Abra o painel Opções de Alerta.

   Como?

   1. Em **Tarefas Comuns**, clique em **Página Inicial**.
   2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
   3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de Alerta, seleccione ou desmarque a caixa de verificação **Mostrar alertas informativos quando o modo de jogo for detectado**.

3 Clique em **OK**.

Configurar opções de alerta

O aspecto e a frequência dos alertas são configurados pelo SecurityCenter; no entanto, é possível ajustar opções básicas de alerta. Por exemplo, é possível reproduzir um som com os alertas ou ocultar a apresentação do alerta do ecrã inicial quando o Windows for iniciado. Também é possível ocultar alertas que notificam sobre surtos de vírus e outras ameaças de segurança na comunidade online.

Reproduzir um som com os alertas

Se pretender receber uma indicação audível de que ocorreu um alerta, pode configurar o SecurityCenter para reproduzir um som com cada alerta.

1 Abra o painel Opções de Alerta.

   Como?

   1. Em **Tarefas Comuns**, clique em **Página Inicial**.
   2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
   3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de Alertas, em **Som**, seleccione a caixa de verificação **Reproduzir um som quando ocorre um alerta**.

Ocultar o ecrã inicial no arranque

Por predefinição, o ecrã inicial da McAfee é apresentado brevemente quando o Windows é iniciado, para informar que o SecurityCenter está a proteger o computador. No entanto, é possível ocultar o ecrã inicial se não quiser que seja apresentado.

1 Abra o painel Opções de Alerta.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de Alerta, em **Ecrã Inicial**, desmarque a caixa de verificação **Mostrar o ecrã inicial da McAfee quando o Windows é iniciado**.

Sugestão: Para mostrar o ecrã inicial novamente em qualquer altura, seleccione a caixa de verificação **Mostrar o ecrã inicial da McAfee quando o Windows é iniciado**.

Ocultar alertas de surtos de vírus

É possível ocultar alertas que notificam sobre surtos de vírus e outras ameaças de segurança na comunidade online.

1 Abra o painel Opções de Alerta.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de Alerta, desmarque a caixa de verificação **Alertar-me quando ocorrer uma infecção por vírus ou uma ameaça de segurança**.

Sugestão: Para apresentar alertas de surtos de vírus em qualquer altura, seleccione a caixa de verificação **Alertar-me quando ocorrer uma infecção por vírus ou uma ameaça de segurança**.

Ocultar mensagens de segurança

É possível ocultar as notificações de segurança sobre como proteger mais computadores na sua rede doméstica. Estas mensagens fornecem informações sobre a subscrição, o número de computadores que pode proteger com a sua subscrição e como prolongar a subscrição para proteger ainda mais computadores.

1 Abra o painel Opções de Alerta.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de Alerta, desmarque a caixa de verificação **Mostrar avisos sobre vírus ou outras mensagens de segurança**.

Sugestão: Para apresentar estas mensagens de segurança em qualquer altura, seleccione a caixa de verificação **Mostrar avisos sobre vírus ou outras mensagens de segurança**.

CAPÍTULO 7

Ver eventos

Um evento é uma acção ou uma alteração de configuração que ocorre numa categoria de protecção e nos serviços de protecção relacionados. Serviços de protecção diferentes registam tipos de eventos diferentes. Por exemplo, o SecurityCenter regista um evento se um serviço de protecção for activado ou desactivado; a Protecção de Vírus regista um evento sempre que é detectado e removido um vírus; a Protecção de Firewall regista um evento sempre que é bloqueada uma tentativa de ligação à Internet. Para obter mais informações sobre categorias de protecção, consulte a secção Noções sobre categorias de protecção (página 9).

É possível visualizar eventos durante a resolução de problemas de configuração ou durante a análise de operações efectuadas por outros utilizadores. Muitos pais utilizam o registo de eventos para controlar o comportamento dos filhos na Internet. Para examinar apenas os últimos 30 eventos ocorridos, visualize eventos recentes. Para examinar uma lista completa de todos os eventos ocorridos, visualize todos os eventos. Quando um utilizador visualiza todos os eventos, o SecurityCenter inicia o registo de eventos, o qual ordena os eventos de acordo com a categoria de protecção em que ocorreram.

Neste capítulo

Ver eventos recentes

Para examinar apenas os últimos 30 eventos ocorridos, visualize eventos recentes.

- Em **Tarefas Comuns,** clique em **Ver Eventos Recentes**.

Ver todos os eventos

Para examinar uma lista completa de todos os eventos ocorridos, visualize todos os eventos.

1. Em **Tarefas Comuns,** clique em **Ver Eventos Recentes**.
2. No painel Eventos Recentes, clique em **Ver Registo**.
3. No painel esquerdo do registo de eventos, clique no tipo de eventos que pretende visualizar.

CAPÍTULO 8

McAfee VirusScan

Os serviços de protecção e detecção avançados do VirusScan protegem o utilizador e o computador contra as mais recentes ameaças de segurança, incluindo vírus, cavalos de Tróia, cookies de controlo, spyware, adware e outros programas potencialmente indesejados. A protecção não se limita aos ficheiros e pastas do computador de secretária, abrangendo também diferentes pontos de entrada de ameaças, entre os quais o correio electrónico, as mensagens instantâneas e a Web.

Com o VirusScan, a protecção do computador é imediata e contínua (sem necessidade de tarefas de administração fastidiosas). Enquanto trabalha, navega na Web ou verifica o correio electrónico, o VirusScan monitoriza, analisa e detecta perigos potenciais em tempo real, trabalhando em segundo plano. As análises completas são executadas de acordo com a agenda, utilizando um conjunto de opções mais sofisticado para verificar periodicamente o computador. O VirusScan proporciona-lhe flexibilidade para personalizar este comportamento, mas o computador continua protegido se não o fizer.

Durante a utilização normal do computador, podem infiltrar-se vírus, worms e outras ameaças potenciais. Se isso ocorrer, o VirusScan notifica-o sobre a ameaça mas trata-a automaticamente e limpa ou coloca em quarentena os itens infectados antes que ocorram danos. Por vezes, podem ser necessárias acções adicionais. Nesses casos, o VirusScan permite ao utilizador decidir o que fazer (voltar a analisar na próxima vez que iniciar o computador, manter o item detectado ou removê-lo).

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do VirusScan

Protecção antivírus completa	Defenda-se a si e ao seu computador das mais recentes ameaças de segurança, incluindo vírus, cavalos de Tróia, cookies de rastreio, spyware, adware e outros programas potencialmente indesejados. A protecção não se limita a ficheiros e pastas do computador de secretária, abrangendo também diferentes pontos de entrada de ameaças, entre os quais o correio electrónico, as mensagens instantâneas e a Web. Sem necessidade de tarefas de administração fastidiosas.
Opções de análise sensíveis aos recursos	Se pretender, pode personalizar opções de análise, mas, se não o fizer, o computador continua protegido. Se a velocidade de análise for lenta, pode desactivar a opção para utilizar recursos mínimos do computador, mas tenha em atenção que será dada uma prioridade mais elevada à protecção antivírus em detrimento de outras tarefas.
Reparações automáticas	Se o VirusScan detectar uma ameaça de segurança durante a execução de uma análise, tentará tratá-la automaticamente de acordo com o tipo de ameaça. Deste modo, a maioria das ameaças pode ser detectada e neutralizada sem interacção do utilizador. Por vezes, o VirusScan pode não conseguir neutralizar uma ameaça sozinho. Nesses casos, o VirusScan permite ao utilizador decidir o que fazer (voltar a analisar na próxima vez que iniciar o computador, manter o item detectado ou removê-lo).
Interromper tarefas em modo de ecrã completo	Quando estiver a ver filmes, a jogar no computador ou a realizar qualquer outra actividade que ocupe a totalidade do ecrã, o VirusScan interrompe diversas tarefas, como, por exemplo, as análises manuais.

CAPÍTULO 9

Analisar o computador

Antes de iniciar o SecurityCenter pela primeira vez, a protecção antivírus em tempo real do VirusScan começa a proteger o computador contra vírus, cavalos de Tróia e outras ameaças de segurança potencialmente prejudiciais. A menos que a protecção antivírus em tempo real seja desactivada, o VirusScan utiliza as opções de análise em tempo real configuradas pelo utilizador para monitorizar continuamente a existência de actividades de vírus no computador, analisando os ficheiros sempre que são acedidos pelo utilizador ou pelo computador. Para ter a certeza de que o computador está protegido contra as mais recentes ameaças de segurança, active a protecção antivírus em tempo real e agende análises manuais mais completas e regulares. Para mais informações sobre como configurar opções de análise, consulte Configurar a protecção antivírus (página 49).

O VirusScan fornece um conjunto de opções de análise mais detalhado para protecção antivírus, permitindo a execução periódica de análises mais completas. Pode executar uma análise completa, rápida, personalizada ou agendada a partir do SecurityCenter. Também pode executar análises manuais no Explorador do Windows enquanto trabalha. A análise no SecurityCenter oferece a vantagem de alterar as opções de análise instantaneamente. No entanto, a análise a partir do Explorador do Windows oferece uma abordagem adequada à segurança do computador.

Independentemente de executar uma análise a partir do SecurityCenter ou do Explorador do Windows, pode ver os resultados da análise depois de terminada. A visualização dos resultados de uma análise permite determinar se o VirusScan detectou, reparou ou colocou em quarentena vírus, cavalos de Tróia, spyware, adware, cookies e outros programas potencialmente indesejados. Os resultados de uma análise podem ser apresentados de diferentes formas. Por exemplo, é possível ver um resumo simples dos resultados da análise ou informações detalhadas, tais como o tipo e o estado da infecção. Também é possível ver estatísticas gerais de análise e detecção.

Neste capítulo

Analisar o computador

O VirusScan fornece um conjunto completo de opções de análise para protecção antivírus, incluindo análise em tempo real (que monitoriza constantemente o computador para detectar actividades de ameaça), análise manual a partir do Explorador do Windows e análise completa, rápida, personalizada ou agendada a partir do SecurityCenter.

Para...	Efectue o seguinte...
Iniciar a análise em tempo real para monitorizar continuamente a existência de actividades de vírus no computador, analisando os ficheiros sempre que são acedidos pelo utilizador ou pelo computador	1. Abra o painel Configuração de Computador e Ficheiros. Como? 1. No painel esquerdo, clique em **Menu Avançado**. 2. Clique em **Configurar**. 3. No painel Configurar, clique em **Computador & Ficheiros**. 2. Em **Protecção Antivírus**, clique em **Ligado**. **Nota**: A análise em tempo real está activada por predefinição.
Iniciar uma Análise Rápida para verificar rapidamente a existência de ameaças no computador	1. Clique em **Analisar** no menu Básico. 2. No painel Opções de Análise, em Análise Rápida, clique em **Iniciar**.
Iniciar uma Análise Completa para verificar exaustivamente a existência de ameaças no computador	1. Clique em **Analisar** no menu Básico. 2. No painel Opções de Análise, em Análise Completa, clique em **Iniciar**.

Para...	Efectue o seguinte...
Iniciar uma Análise Personalizada baseada em definições personalizadas	1. Clique em **Analisar** no menu Básico. 2. No painel Opções de Análise, em Deixar-me Escolher, clique em **Iniciar**. 3. Personalize uma análise desmarcando ou seleccionando: **Todas as Ameaças em Todos os Ficheiros** **Vírus Desconhecidos** **Ficheiros de Arquivo** **Spyware e Potenciais Ameaças** **Cookies de Rastreio** **Programas Furtivos** 4. Clique em **Iniciar**.
Iniciar uma Análise Manual para verificar a existência de ameaças em ficheiros, pastas ou unidades	1. Abra o Explorador do Windows. 2. Clique com o botão direito num ficheiro, pasta ou unidade e, em seguida, clique em **Analisar**.

Para...	Efectue o seguinte...
Iniciar uma Análise Agendada que verifica periodicamente a existência de ameaças no computador	1. Abra o painel Análise Agendada. Como? 1. Em **Tarefas Comuns**, clique em **Página Inicial**. 2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**. 3. Na área de informação Computador & Ficheiros, clique em **Configurar**. 4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**. 5. Clique em **Análise Agendada** no painel Protecção Antivírus. 2. Seleccione **Activar análise agendada**. 3. Para reduzir a capacidade do processador utilizada normalmente para as análises, seleccione **Analisar utilizando recursos mínimos do computador**. 4. Seleccione um ou mais dias. 5. Especifique uma hora de início. 6. Clique em **OK**.

Os resultados da análise são apresentados no alerta Análise concluída. Os resultados incluem o número de itens analisados, detectados, reparados, colocados em quarentena e removidos. Clique em **Ver detalhes da análise** para saber mais acerca dos resultados da análise ou tratar itens infectados.

Nota: Para obter mais informações sobre as opções de análise, consulte Tipos de Análise (página 42).

Ver resultados da análise

Depois de uma análise terminar, visualize os resultados para determinar o que foi encontrado e analisar o estado de protecção actual do computador. Os resultados da análise indicam se o VirusScan detectou, reparou ou colocou em quarentena vírus, cavalos de Tróia, spyware, adware, cookies e outros programas potencialmente indesejados.

Nos menus Básico ou Avançado, clique em **Analisar** e, em seguida, proceda de um dos seguintes modos:

Para...	Efectue o seguinte...
Ver os resultados da análise no alerta	Veja os resultados da análise no alerta de Análise concluída.
Ver mais informações sobre os resultados da análise	Clique em **Ver detalhes da análise** no alerta de Análise concluída.
Ver um breve resumo dos resultados da análise	Aponte para o ícone **Análise concluída** na área de notificação da barra de tarefas.
Ver estatísticas de análise e detecção	Faça duplo clique no ícone **Análise concluída** na área de notificação da barra de tarefas.
Ver detalhes sobre itens detectados, tipo e estado das infecções	1. Faça duplo clique no ícone **Análise concluída** na área de notificação da barra de tarefas. 2. Clique em **Detalhes** no painel Análise Completa, Análise Rápida, Análise Personalizada ou Análise Manual.
Ver detalhes sobre a análise mais recente	Faça duplo clique no ícone **Análise concluída** na área de notificação da barra de tarefas e veja os detalhes da análise mais recente em A Sua Análise no painel Análise Completa, Análise Rápida, Análise Personalizada ou Análise Manual.

CAPÍTULO 10

Utilizar os resultados da análise

Se o VirusScan detectar uma ameaça de segurança durante a execução de uma análise, tentará tratá-la automaticamente de acordo com o tipo de ameaça. Por exemplo, se o VirusScan detectar um vírus, um cavalo de Tróia ou um cookie de controlo no computador, tenta limpar o ficheiro infectado. O VirusScan coloca sempre um ficheiro em quarentena antes de o tentar limpar. Se não for limpo, o ficheiro fica em quarentena.

No que respeita a algumas ameaças de segurança, o VirusScan poderá não conseguir limpar ou colocar em quarentena um ficheiro com êxito. Nesse caso, o VirusScan solicita ao utilizador que trate a ameaça. É possível executar acções diferentes, dependendo do tipo de ameaça. Por exemplo, se for detectado um vírus num ficheiro e o VirusScan não conseguir limpar ou colocar em quarentena o ficheiro com êxito, nega qualquer acesso ao ficheiro. Se forem detectados cookies de controlo e o VirusScan não conseguir limpar ou colocar em quarentena os cookies com êxito, o utilizador pode decidir se confia nos cookies ou se os remove. Se forem detectados programas potencialmente indesejados, o VirusScan não executa nenhuma acção automática, permitindo ao utilizador decidir se confia no programa ou se o coloca em quarentena.

Quando o VirusScan coloca itens em quarentena, encripta-os e isola-os numa pasta para impedir que os ficheiros, programas ou cookies possam danificar o computador. É possível restaurar ou remover os itens em quarentena. Na maioria dos casos, pode eliminar um cookie colocado em quarentena sem afectar o sistema; no entanto, se o VirusScan tiver colocado em quarentena um programa que o utilizador reconhece e utiliza, pondere o seu restauro.

Neste capítulo

Tratar vírus e cavalos de Tróia

Se o VirusScan detectar um vírus ou um cavalo de Tróia num ficheiro do computador, tenta limpar o ficheiro. Se não conseguir limpar o ficheiro, o VirusScan tenta colocá-lo em quarentena. Se esta acção também falhar, o acesso ao ficheiro é negado (apenas em análises em tempo real).

1 Abra o painel Resultados da Análise.

   Como?

   1. Faça duplo clique no ícone **Análise concluída** na área de notificação, na parte mais à direita da barra de tarefas.
   2. No painel Progresso da Análise: Análise Manual, clique em **Ver Resultados**.

2 Na lista de resultados da análise, clique em **Vírus e Cavalos de Tróia**.

Nota: Para tratar os ficheiros colocados em quarentena pelo VirusScan, consulte a secção Tratar ficheiros em quarentena (página 41).

Tratar programas potencialmente indesejados

Se o VirusScan detectar um programa potencialmente indesejado no computador, o utilizador pode confiar no programa ou removê-lo. Se não conhecer o programa, recomendamos que considere a sua remoção. A remoção do programa potencialmente indesejado não o elimina realmente do sistema. Em vez disso, coloca o programa em quarentena para evitar que danifique o computador ou ficheiros.

1 Abra o painel Resultados da Análise.

   Como?

   1. Faça duplo clique no ícone **Análise concluída** na área de notificação, na parte mais à direita da barra de tarefas.
   2. No painel Progresso da Análise: Análise Manual, clique em **Ver Resultados**.

2 Na lista de resultados da análise, clique em **Programas Potencialmente Indesejados**.

3 Seleccione um programa potencialmente indesejado.

4 Em **Quero**, clique em **Remover** ou em **Confiar**.

5 Confirme a opção seleccionada.

Tratar ficheiros em quarentena

Quando o VirusScan coloca ficheiros infectados em quarentena, encripta-os e move-os para uma pasta para impedir que danifiquem o computador. Depois, é possível restaurar ou remover os itens em quarentena.

1 Abra o painel Ficheiros em Quarentena.

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Restaurar**.
3. Clique em **Ficheiros**.

2 Seleccione um ficheiro em quarentena.

3 Proceda de um dos seguintes modos:

- Para reparar um ficheiro infectado e devolvê-lo à sua localização original no computador, clique em **Restaurar**.
- Para remover o ficheiro infectado do computador, clique em **Remover**.

4 Clique em **Sim** para confirmar a opção seleccionada.

Sugestão: É possível restaurar ou remover vários ficheiros ao mesmo tempo.

Tratar programas e cookies em quarentena

Quando o VirusScan coloca programas potencialmente indesejados ou cookies de controlo em quarentena, encripta-os e move-os para uma pasta protegida para impedir que danifiquem o computador. Depois, é possível restaurar ou remover os itens em quarentena. Na maioria dos casos, é possível eliminar um item em quarentena sem provocar impacto no sistema.

1 Abra o painel Programas e Cookies de Controlo em Quarentena.

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Restaurar**.
3. Clique em **Programas e Cookies**.

2 Seleccione um programa ou um cookie em quarentena.

3 Proceda de um dos seguintes modos:

- Para reparar um ficheiro infectado e devolvê-lo à sua localização original no computador, clique em **Restaurar**.
- Para remover o ficheiro infectado do computador, clique em **Remover**.

4 Clique em **Sim** para confirmar a operação.

Sugestão: É possível restaurar ou remover vários programas e cookies ao mesmo tempo.

Tipos de análise

O VirusScan fornece um conjunto completo de opções de análise para protecção antivírus, incluindo análise em tempo real (que monitoriza constantemente o computador para detectar actividades de ameaça), análise manual a partir do Explorador do Windows e a possibilidade de executar uma análise completa, rápida ou personalizada a partir do SecurityCenter, bem como de personalizar quando deverão ocorrer as análises agendadas. A análise no SecurityCenter oferece a vantagem de alterar as opções de análise instantaneamente.

Análise em Tempo Real:

A protecção antivírus em tempo real monitoriza continuamente a existência de actividades de vírus no computador, analisando os ficheiros sempre que são acedidos pelo utilizador ou pelo computador. Para ter a certeza de que o computador está protegido contra as mais recentes ameaças de segurança, mantenha activada a protecção antivírus em tempo real e agende análises manuais mais completas e regulares.

Pode estabelecer opções predefinidas para análises em tempo real, que incluem análises de vírus desconhecidos e a verificação de existência de ameaças em cookies de rastreio e unidades de rede. Também pode tirar partido da protecção de sobrecarga da memória intermédia, que está activada por predefinição (excepto se estiver a utilizar um sistema operativo Windows Vista de 64 bits). Para mais informações, consulte Configurar opções de análise em tempo real (página 50).

Análise Rápida

A Análise Rápida permite verificar a existência de actividades de ameaça em processos, ficheiros críticos do Windows e outras áreas susceptíveis do computador.

Análise Completa

A Análise Completa permite verificar exaustivamente a existência de vírus, spyware e outras ameaças de segurança em qualquer parte do computador.

Análise Personalizada

A Análise Personalizada permite escolher definições de análise personalizadas para verificar a existência de actividades de ameaça no computador. As opções de análise personalizada incluem a verificação de existência de ameaças em todos os ficheiros, ficheiros de arquivo e cookies, bem como a análise de vírus desconhecidos, spyware e programas furtivos.

Pode estabelecer opções predefinidas para análises personalizadas, que incluem análises de vírus desconhecidos, ficheiros de arquivo, spyware e potenciais ameaças, cookies de rastreio e programas furtivos. Também pode efectuar a análise utilizando recursos mínimos do computador. Para mais informações, consulte Configurar opções de análise personalizada (página 52).

Análise Manual

A Análise Manual permite verificar rapidamente a existência de ameaças em ficheiros, pastas e unidades instantaneamente a partir do Explorador do Windows.

Análise agendada

As análises agendadas permitem verificar exaustivamente a existência de vírus e outras ameaças no computador em qualquer dia e hora da semana. As análises agendadas verificam sempre a totalidade do computador, utilizando as opções de análise predefinidas. Por predefinição, o VirusScan executa uma análise agendada uma vez por semana. Se achar que as velocidades de análise são lentas, pode desactivar a opção para utilizar recursos mínimos do computador, mas tenha em atenção que será dada uma prioridade mais elevada à protecção antivírus em detrimento de outras tarefas. Para mais informações, consulte Agendar uma análise (página 54)

Nota: Para obter informações sobre como iniciar a melhor opção de análise, consulte Analisar o computador (página 34)

CAPÍTULO 11

Utilizar protecção adicional

Além da protecção antivírus em tempo real, o VirusScan fornece protecção avançada contra scripts, spyware e anexos de correio electrónico e mensagens instantâneas potencialmente prejudiciais. Por predefinição, as protecções de análise de scripts, anti-spyware, de correio electrónico e de mensagens instantâneas estão activadas e a proteger o computador.

Protecção de análise de scripts

A protecção de análise de scripts detecta scripts potencialmente prejudiciais e impede que sejam executados no computador ou Web browser. A protecção monitoriza a existência de actividades de scripts suspeitas no computador, tais como um script que cria, copia ou elimina ficheiros, ou abre o registo do Windows e alerta-o antes que ocorram danos.

Protecção anti-spyware

A protecção anti-spyware detecta spyware, adware e outros programas potencialmente indesejados. Spyware é software que pode ser instalado secretamente no computador para monitorizar o seu comportamento, recolher informações pessoais e mesmo interferir no controlo do computador através da instalação de software adicional ou do redireccionamento da actividade do browser.

Protecção do correio electrónico

A protecção do correio electrónico detecta actividades suspeitas nas mensagens e anexos de correio electrónico enviados.

Protecção de mensagens instantâneas

A protecção de mensagens instantâneas detecta potenciais ameaças de segurança em anexos de mensagens instantâneas recebidas. De igual modo, impede que os programas de mensagens instantâneas partilhem informações pessoais.

Neste capítulo

Iniciar a protecção de análise de scripts

Active a protecção de análise de scripts para detectar scripts potencialmente prejudiciais e impedir que sejam executados no computador. A protecção de análise de scripts alerta o utilizador quando um script tenta criar, copiar ou eliminar ficheiros no computador ou alterar o registo do Windows.

1 Abra o painel de configuração Computador & Ficheiros.

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador & Ficheiros**.

2 Em **Protecção de análise de scripts**, clique em **Ligado**.

Nota: Embora seja possível desactivar a protecção de análise de scripts em qualquer altura, o computador ficará vulnerável a scripts prejudiciais.

Iniciar a protecção anti-spyware

Active a protecção anti-spyware para detectar e remover spyware, adware e outros programas potencialmente indesejados que recolhem e transmitem os seus dados privados sem o seu conhecimento ou permissão.

1 Abra o painel de configuração Computador & Ficheiros.

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador & Ficheiros**.

2 Em **Protecção de análise de scripts**, clique em **Ligado**.

Nota: Embora seja possível desactivar a protecção anti-spyware em qualquer altura, o computador ficará vulnerável a programas potencialmente indesejados.

Iniciar a protecção do correio electrónico

Active a protecção do correio electrónico para detectar worms e potenciais ameaças nas mensagens e anexos de correio electrónico a enviar (SMTP) e receber (POP3).

1 Abra o painel de configuração Correio Electrónico e Mensagens Instantâneas

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Correio electrónico & IM**.

2 Em **Protecção do correio electrónico**, clique em **Ligado**.

Nota: Embora seja possível desactivar a protecção de correio electrónico em qualquer altura, o computador ficará vulnerável a ameaças de correio electrónico.

Iniciar a protecção de mensagens instantâneas

Active a protecção de mensagens instantâneas para detectar ameaças de segurança que podem estar incluídas em anexos de mensagens instantâneas a receber.

1 Abra o painel de configuração Correio Electrónico e Mensagens Instantâneas

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Correio electrónico & IM**.

2 Em **Protecção de mensagens instantâneas**, clique em **Ligado**.

Nota: Embora seja possível desactivar a protecção de mensagens instantâneas em qualquer altura, o computador ficará vulnerável a anexos de mensagens instantâneas prejudiciais.

CAPÍTULO 12

Configurar a protecção antivírus

Pode definir diferentes opções de análise agendada, personalizada e em tempo real. Por exemplo, uma vez que a protecção em tempo real monitoriza continuamente o computador, pode seleccionar um conjunto específico de opções de análise básicas para esta protecção e reservar um conjunto mais abrangente de opções de análise para a protecção manual e a pedido.

Também pode decidir a forma como pretende que o VirusScan efectue a monitorização e gestão de alterações potencialmente não autorizadas ou indesejadas no computador utilizando as Protecções do Sistema e as Listas de Confiança. As Protecções do Sistema monitorizam, registam, comunicam e gerem eventuais alterações não autorizadas efectuadas no registo do Windows ou em ficheiros de sistema críticos no computador. As alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a sua segurança e danificar ficheiros de sistema valiosos. Pode utilizar Listas de Confiança para decidir se pretende confiar ou remover regras que detectem alterações de ficheiros ou do registo (Protecção do Sistema), sobrecargas da memória temporária ou programas. Se confiar no item e indicar que não pretende receber notificações futuras sobre a sua actividade, o item é adicionado a uma lista de confiança e o VirusScan deixa de o detectar ou de notificar o utilizador sobre a sua actividade.

Neste capítulo

Configurar opções de análise em tempo real

Quando a protecção antivírus em tempo real é iniciada, o VirusScan utiliza um conjunto de opções predefinido para analisar ficheiros; no entanto, é possível alterar as predefinições, se necessário.

Para alterar as opções de análise em tempo real, é necessário decidir o que o VirusScan deve inspeccionar durante uma análise, bem como as localizações e os tipos de ficheiros a analisar. Por exemplo, é possível especificar se o VirusScan analisa a existência de vírus desconhecidos ou cookies que podem ser utilizados por Web sites para registar o seu comportamento, ou se analisa unidades de rede mapeadas para o computador ou apenas unidades locais. Também é possível especificar os tipos de ficheiros a analisar (todos os ficheiros ou apenas ficheiros de programa e documentos, uma vez que a maioria dos vírus é detectada nestes tipos de ficheiros).

Ao alterar as opções de análise em tempo real, deve igualmente especificar se é importante que o computador possua protecção de sobrecarga da memória intermédia. Memória intermédia é uma parte da memória que é utilizada temporariamente para conter informações do computador. As sobrecargas da memória intermédia podem ocorrer quando a quantidade de informações que os programas ou processos suspeitos armazenam numa memória intermédia excede a capacidade da mesma. Quando esta situação ocorre, o computador fica mais vulnerável a ataques de segurança.

Configurar opções de análise em tempo real

A configuração de opções de análise em tempo real permite personalizar o que o VirusScan deve procurar durante uma análise em tempo real, bem como as localizações e os tipos de ficheiros a analisar. As opções incluem a análise de vírus desconhecidos e cookies de controlo, bem como a protecção contra sobrecarga da memória intermédia. Também é possível configurar a análise em tempo real para inspeccionar unidades de rede mapeadas para o computador.

1 Abra o painel Análise em Tempo Real.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.

2 Especifique as opções de análise em tempo real e, em seguida, clique em **OK**.

Para...	Efectue o seguinte...
Detectar vírus desconhecidos e novas variantes de vírus conhecidos	Seleccione **Analisar a existência de vírus desconhecidos**.
Detectar cookies	Seleccione **Analisar e remover cookies de registo**.
Detectar vírus e outras ameaças potenciais em unidades ligadas à rede	Seleccione **Analisar unidades de rede**.
Proteger o computador contra sobrecargas da memória intermédia	Seleccione **Activar protecção de sobrecarga da memória intermédia**.
Especificar os tipos de ficheiros a analisar	Clique em **Todos os ficheiros (recomendado)** ou **Apenas programas e documentos**.

Interromper a protecção antivírus em tempo real

Por vezes, poderá querer interromper temporariamente as análises em tempo real (por exemplo, para alterar algumas opções de análise ou resolver um problema de desempenho). Quando a protecção antivírus em tempo real está desactivada, o computador não está protegido e o estado de protecção do SecurityCenter fica vermelho. Para obter mais informações sobre o estado de protecção, consulte a secção "Noções sobre o estado de protecção" na ajuda do SecurityCenter.

É possível desactivar temporariamente a protecção antivírus em tempo real e especificar quando deve ser retomada. É possível retomar automaticamente a protecção após 15, 30, 45 ou 60 minutos, quando o computador é reiniciado ou nunca.

1 Abra o painel Configuração de Computador e Ficheiros.

   Como?

   1. No painel esquerdo, clique em **Menu Avançado**.
   2. Clique em **Configurar**.
   3. No painel Configurar, clique em **Computador & Ficheiros**.

2 Em **Protecção Antivírus**, clique em **Desligado**.

3 Na caixa de diálogo, seleccione quando deve ser retomada a análise em tempo real.

4 Clique em **OK**.

Configurar opções de análise personalizada

A protecção antivírus personalizada permite analisar ficheiros a pedido. Quando é iniciada uma análise personalizada, o VirusScan verifica a existência de vírus e outros itens potencialmente prejudiciais no computador, através de um conjunto mais abrangente de opções de análise. Para alterar as opções de análise personalizada, é necessário decidir o que o VirusScan deve inspeccionar durante uma análise. Por exemplo, é possível especificar se o VirusScan procura vírus desconhecidos, programas potencialmente indesejados, tais como spyware ou adware, programas furtivos, rootkits (que podem conceder acesso não autorizado ao computador) e cookies que podem ser utilizados por Web sites para registar o seu comportamento. É igualmente necessário decidir quais os tipos de ficheiros a analisar. Por exemplo, é possível especificar se o VirusScan verifica todos os ficheiros ou apenas ficheiros de programas e documentos (uma vez que é nestes tipos de ficheiros que é detectada a maioria dos vírus). Também é possível especificar se os ficheiros de arquivo (por exemplo, ficheiros .zip) são incluídos na análise.

Por predefinição, o VirusScan examina todas as unidades e pastas do computador, bem como todas as unidades de rede sempre que é executada uma análise personalizada; no entanto, é possível alterar as localizações predefinidas, se necessário. Por exemplo, é possível analisar apenas ficheiros críticos do computador, itens no ambiente de trabalho ou itens na pasta Programas. A menos que pretenda executar manualmente todas as análises personalizadas, pode configurar análises agendadas regulares. As análises agendadas verificam sempre a totalidade do computador, utilizando as opções de análise predefinidas. Por predefinição, o VirusScan executa uma análise agendada uma vez por semana.

Se concluir que as velocidades de análise são lentas, pode desactivar a opção para utilizar recursos mínimos do computador, mas tenha em atenção que será dada uma prioridade mais elevada à protecção antivírus do que a outras tarefas.

Nota: Quando está a ver filmes, a jogar no computador ou a realizar qualquer outra actividade que ocupe a totalidade do ecrã, o VirusScan interrompe diversas tarefas, incluindo actualizações automáticas e análises personalizadas.

Configurar opções de análise personalizada

A configuração de opções de análise personalizada permite personalizar o que o VirusScan deve procurar durante uma análise personalizada, bem como as localizações e os tipos de ficheiros a analisar. As opções incluem a análise de vírus desconhecidos, ficheiros de arquivo, spyware e programas potencialmente indesejados, cookies de controlo, rootkits e programas furtivos. Também pode configurar a localização de análise personalizada para determinar onde o VirusScan deve procurar vírus e outros itens prejudiciais durante uma análise personalizada. É possível analisar todos os ficheiros, pastas e unidades do computador ou restringir a análise a pastas e unidades específicas.

1 Abra o painel Análise Personalizada.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.
5. Clique em **Análise Manual** no painel Protecção Antivírus.

2 Especifique as opções de análise personalizada e, em seguida, clique em **OK**.

Para...	Efectue o seguinte...
Detectar vírus desconhecidos e novas variantes de vírus conhecidos	Seleccione **Analisar a existência de vírus desconhecidos**.
Detectar e remover vírus existentes em ficheiros .zip e noutros ficheiros de arquivo	Seleccione **Analisar ficheiros de arquivo**.
Detectar spyware, adware e outros programas potencialmente indesejados	Seleccione **Analisar a existência de spyware e de ameaças potenciais**.
Detectar cookies	Seleccione **Analisar e remover cookies de registo**.
Detectar rootkits e programas furtivos que podem alterar e explorar os ficheiros de sistema do Windows existentes	Seleccione **Analisar a existência de programas furtivos**.

Para...	Efectue o seguinte...
Utilizar menos capacidade do processador para as análises e dar uma prioridade mais elevada a outras tarefas (tais como navegar na Web ou abrir documentos)	Seleccione **Analisar utilizando recursos mínimos do computador**.
Especificar os tipos de ficheiros a analisar	Clique em **Todos os ficheiros (recomendado)** ou **Apenas programas e documentos**.

3 Clique em **Localização Predefinida a Analisar**, seleccione ou desmarque as localizações que pretende analisar ou ignorar e, em seguida, clique em **OK**:

Para...	Efectue o seguinte...
Analisar todos os ficheiros e pastas do computador	Seleccione **(O Meu) Computador**.
Analisar ficheiros, pastas e unidades específicas no computador	Desmarque a caixa de verificação **(O Meu) Computador** e seleccione uma ou mais pastas ou unidades.
Analisar ficheiros de sistema críticos	Desmarque a caixa de verificação **(O Meu) Computador** e seleccione a caixa de verificação **Ficheiros de Sistema Críticos**.

Agendar uma análise

As análises agendadas permitem analisar exaustivamente o computador para detectar vírus e outras ameaças em qualquer dia e hora da semana. As análises agendadas verificam sempre a totalidade do computador, utilizando as opções de análise predefinidas. Por predefinição, o VirusScan executa uma análise agendada uma vez por semana. Se concluir que as velocidades de análise são lentas, pode desactivar a opção para utilizar recursos mínimos do computador, mas tenha em atenção que será dada uma prioridade mais elevada à protecção antivírus do que a outras tarefas.

Análises agendadas que verificam exaustivamente a existência de vírus e outras ameaças no computador, utilizando as opções de análise predefinidas. Por predefinição, o VirusScan executa uma análise agendada uma vez por semana.

1 Abra o painel Análise Agendada.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.
5. Clique em **Análise Agendada** no painel Protecção Antivírus.

2 Seleccione **Activar análise agendada**.

3 Para reduzir a capacidade do processador utilizada normalmente para as análises, seleccione **Analisar utilizando recursos mínimos do computador**.

4 Seleccione um ou mais dias.

5 Especifique uma hora de início.

6 Clique em **OK**.

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

Utilizar opções das Protecções do Sistema

As Protecções do Sistema monitorizam, registam, comunicam e gerem eventuais alterações não autorizadas efectuadas no registo do Windows ou em ficheiros de sistema críticos no computador. As alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.

As alterações do registo e de ficheiros são frequentes e ocorrem com regularidade no computador. Uma vez que muitas dessas alterações são inofensivas, as predefinições das Protecções do Sistema são configuradas de modo a fornecer uma protecção fiável, inteligente e em tempo real contra alterações não autorizadas que podem representar danos potenciais significativos. Por exemplo, quando as Protecções do Sistema detectam alterações invulgares e que constituem uma ameaça significativa potencial, a actividade é imediatamente comunicada e registada. As alterações mais comuns que ainda representam alguns danos potenciais são apenas registadas. No entanto, a monitorização de alterações normais e de baixo risco está desactivada por predefinição. A tecnologia das Protecções do Sistema pode ser configurada para alargar o âmbito da protecção a qualquer ambiente.

Existem três tipos de Protecções do Sistema: Programa de Protecções do Sistema, Protecções do Sistema do Windows e Protecções do Sistema do Browser.

Programa de Protecções do Sistema

O Programa de Protecções do Sistema detecta eventuais alterações não autorizadas no registo do computador e noutros ficheiros críticos essenciais do Windows. Estes itens do registo e ficheiros importantes incluem instalações ActiveX, itens de arranque, hooks de execução da shell do Windows e dos carregamentos com atraso do objecto do serviço da shell. Através da monitorização destes itens, o Programa de Protecções do Sistema detém programas ActiveX suspeitos (transferidos da Internet), bem como spyware e programas potencialmente indesejados que podem ser iniciados automaticamente no arranque do Windows.

Protecções do Sistema do Windows

As Protecções do Sistema do Windows também detectam eventuais alterações não autorizadas no registo do computador e noutros ficheiros críticos essenciais do Windows. Estes itens do registo e ficheiros importantes incluem processadores de menus de contexto, appInit DLLs e o ficheiro hosts do Windows. Através da monitorização destes itens, a tecnologia das Protecções do Sistema do Windows ajuda a impedir que o computador envie ou receba informações pessoais ou não autorizadas através da Internet. De igual modo, ajuda a deter programas suspeitos que podem efectuar alterações indesejadas no aspecto e no comportamento de programas importantes para si e para a sua família.

Protecções do Sistema do Browser

À semelhança do Programa de Protecções do Sistema e das Protecções do Sistema do Windows, as Protecções do Sistema do Browser detectam eventuais alterações não autorizadas no registo do computador e noutros ficheiros críticos essenciais do Windows. No entanto, as Protecções do Sistema do Browser monitorizam as alterações de ficheiros e itens importantes do registo, tais como suplementos, URLs e zonas de segurança do Internet Explorer. Através da monitorização destes itens, a tecnologia das Protecções do Sistema do Browser ajuda a impedir actividades não autorizadas do browser, tais como o redireccionamento para Web sites suspeitos, alterações de definições e opções do browser sem o seu conhecimento e confiança não desejada em Web sites suspeitos.

Activar Protecções do Sistema

Active as Protecções do Sistema para detectar e alertar sobre eventuais alterações não autorizadas do registo do Windows e ficheiros no computador. As alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.

1 Abra o painel de configuração Computador & Ficheiros.

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador & Ficheiros**.

2 Em **Protecção do Sistema**, clique em **Ligado**.

Nota: Para desactivar a Protecção do Sistema, clique em **Desligado**.

Configurar opções das Protecções do Sistema

Utilize o painel das Protecções do Sistema para configurar as opções de protecção, início de sessão e alerta contra alterações não autorizadas do registo e de ficheiros associadas a ficheiros do Windows, programas e ao Internet Explorer. As alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.

1 Abra o painel das Protecções do Sistema.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a Protecção do Sistema está activada e, em seguida, clique em **Avançada**.

2 Seleccione um tipo de Protecção do Sistema na lista.

- **Programa de Protecções do Sistema**
- **Protecções do Sistema do Windows**
- **Protecções do Sistema do Browser**

3 Em **Quero**, proceda de um dos seguintes modos:

- Para detectar, registar e comunicar alterações não autorizadas do registo e de ficheiros associadas ao Programa de Protecções do Sistema e às Protecções do Sistema do Windows e dos Browsers, clique em **Mostrar alertas.**
- Para detectar e registar alterações não autorizadas do registo e de ficheiros associadas ao Programa de Protecções do Sistema e às Protecções do Sistema do Windows e dos Browsers, clique em **Registar apenas alterações.**
- Para desactivar a detecção de alterações não autorizadas do registo e de ficheiros associadas ao Programa de Protecções do Sistema e às Protecções do Sistema do Windows e dos Browsers, clique em **Desactivar a Protecção do Sistema.**

Nota: Para obter mais informações sobre os tipos de Protecções do Sistema, consulte a secção Acerca dos tipos de Protecções do Sistema (página 59).

Acerca dos tipos de Protecções do Sistema

As Protecções do Sistema detectam eventuais alterações não autorizadas no registo do computador e noutros ficheiros críticos essenciais do Windows. Existem três tipos de Protecções do Sistema: Programa de Protecções do Sistema, Protecções do Sistema do Windows e Protecções do Sistema do Browser

Programa de Protecções do Sistema

A tecnologia do Programa de Protecções do Sistema detém programas ActiveX suspeitos (transferidos da Internet), bem como spyware e programas potencialmente indesejados que podem ser iniciados automaticamente no arranque do Windows.

Protecção do Sistema	Detecta...
Instalações ActiveX	Alterações não autorizadas ao registo de instalações ActiveX que podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.
Itens de Arranque	Spyware, adware e outros programas potencialmente indesejados que podem instalar alterações a ficheiros dos itens de arranque, permitindo a execução de programas suspeitos quando o computador é iniciado.
Hooks de Execução da Shell do Windows	Spyware, adware e outros programas potencialmente indesejados que podem instalar hooks de execução da shell do Windows para evitar que os programas de segurança sejam executados correctamente.
Carregamento com Atraso do Objecto do Serviço da Shell	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo do carregamento com atraso do objecto do serviço da shell, permitindo a execução de ficheiros prejudiciais quando o computador é iniciado.

Protecções do Sistema do Windows

A tecnologia das Protecções do Sistema do Windows ajuda a impedir que o computador envie ou receba informações pessoais ou não autorizadas através da Internet. De igual modo, ajuda a deter programas suspeitos que podem efectuar alterações indesejadas no aspecto e no comportamento de programas importantes para si e para a sua família.

Protecção do Sistema	Detecta...
Processadores de Menus de Contexto	Alterações não autorizadas ao registo das rotinas de tratamento de menus de contexto do Windows que podem afectar o aspecto e o comportamento dos menus do Windows. Os menus de contexto permitem executar acções no computador, tais como clicar com o botão direito do rato em ficheiros.
AppInit DLLs	Alterações não autorizadas ao registo dos AppInit DLLs do Windows que podem permitir a execução de ficheiros potencialmente prejudiciais quando o computador é iniciado.
Ficheiro Hosts do Windows	Spyware, adware e programas potencialmente indesejados que podem efectuar alterações não autorizadas ao ficheiro hosts do Windows, permitindo o redireccionamento do browser para Web sites suspeitos e o bloqueio de actualizações de software.
Shell do Início de Sessão	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo da shell de Início de Sessão do Windows, permitindo a substituição do Explorador do Windows por outros programas.
Início de Sessão UserInit	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo da aplicação user init de Início de Sessão do Windows, permitindo a execução de programas suspeitos quando o utilizador inicia sessão no Windows.
Protocolos do Windows	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo dos protocolos do Windows, afectando a forma como o computador envia e recebe informação através da Internet.
Fornecedores de Serviços em Camadas do Winsock	Spyware, adware e outros programas potencialmente indesejados que podem instalar alterações ao registo dos Fornecedores de Serviços em Camadas (LSPs) do Winsock para interceptar e alterar informações enviadas e recebidas através da Internet.

Protecção do Sistema	Detecta...
Comandos Open da Shell do Windows	Alterações não autorizadas aos Open Commands da shell do Windows que podem permitir a execução de worms e de outros programas prejudiciais no computador.
Agendador de Tarefas Partilhado	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações a ficheiros e ao registo do agendador de tarefas partilhado, permitindo a execução de ficheiros potencialmente prejudiciais quando o computador é iniciado.
Windows Messenger Service	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo do serviço Windows Messenger, permitindo a existência de publicidade não solicitada e programas executados remotamente no computador.
Ficheiro Win.ini do Windows	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao ficheiro Win.ini, permitindo a execução de programas suspeitos quando o computador é iniciado.

Protecções do Sistema do Browser

A tecnologia das Protecções do Sistema do Browser ajuda a impedir actividades não autorizadas do browser, tais como o redireccionamento para Web sites suspeitos, alterações de definições e opções do browser sem o seu conhecimento e confiança não desejada em Web sites suspeitos.

Protecção do Sistema	Detecta...
Objectos de Auxiliares do Browser	Spyware, adware e outros programas potencialmente indesejados que podem utilizar os objectos auxiliares do browser para rastrear a navegação na Web e mostrar publicidade não solicitada.
Barras do Internet Explorer	Alterações não autorizadas ao registo dos programas da Barra do Internet Explorer, tais como Procurar ou Favoritos, que podem afectar o aspecto e o comportamento do Internet Explorer.
Suplementos do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem instalar suplementos do Internet Explorer para rastrear a navegação na Web e mostrar publicidade não solicitada.

Protecção do Sistema	Detecta...
Browser da Shell do Internet Explorer	Alterações não autorizadas ao registo do browser da shell do Internet Explorer que podem afectar o aspecto e o comportamento do Web browser.
Web Browser Internet Explorer	Alterações não autorizadas ao registo do Web browser Internet Explorer que podem afectar o aspecto e o comportamento do browser.
Hooks de Procura de URL do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo dos hooks de procura de URLs do Internet Explorer, permitindo o redireccionamento do browser para Web sites suspeitos ao efectuar procuras na Web.
URLs do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo dos URLs do Internet Explorer, afectando as definições do browser.
Restrições do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo das restrições do Internet Explorer, afectando as definições e as opções do browser.
Zonas de Segurança do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo das zonas de segurança do Internet Explorer, permitindo a execução de ficheiros potencialmente prejudiciais quando o computador é iniciado.
Sites Fidedignos do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo dos sites fidedignos do Internet Explorer, permitindo que o browser passe a confiar em Web sites suspeitos.
Política do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo das políticas do Internet Explorer, afectando o aspecto e o comportamento do browser.

Utilizar listas de confiança

Se o VirusScan detectar uma alteração ao registo ou ficheiro (Protecção do Sistema), programa ou sobrecarga da memória intermédia, solicita-lhe que confie ou remova o item detectado. Se confiar no item e indicar que não pretende receber notificações futuras sobre a respectiva actividade, o item é adicionado a uma lista de confiança e o VirusScan deixa de o detectar ou de notificar sobre a respectiva actividade. É possível bloquear a actividade de um item que tenha sido adicionado a uma lista de confiança. O bloqueio impede que o item seja executado ou que efectue alterações ao computador sem o notificar de todas as tentativas. Também é possível remover um item de uma lista de confiança. A remoção permite ao VirusScan detectar a actividade do item novamente.

Gerir listas de confiança

Utilize o painel Listas de Confiança para confiar ou bloquear itens que tenham sido detectados e confiados anteriormente. Também pode remover um item de uma lista de confiança para que o VirusScan o detecte novamente.

1 Abra o painel Listas de Confiança.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.
5. Clique em **Listas de Confiança** no painel Protecção Antivírus.

2 Seleccione um dos seguintes tipos de listas de confiança:

- **Programa de Protecções do Sistema**
- **Protecções do Sistema do Windows**
- **Protecções do Sistema do Browser**
- **Programas de Confiança**
- **Sobrecargas da Memória Intermédia de Confiança**

3 Em **Quero**, proceda de um dos seguintes modos:

- Para permitir que o item detectado efectue alterações ao registo do Windows ou a ficheiros do sistema críticos do computador sem o notificar, clique em **Confiar**.

- Para impedir que o item detectado efectue alterações ao registo do Windows ou a ficheiros do sistema críticos do computador sem o notificar, clique em **Bloquear**.
- Para remover o item detectado das listas de confiança, clique em **Remover**.

4 Clique em **OK**.

Nota: Para obter mais informações sobre os tipos de listas de confiança, consulte a secção Acerca dos tipos de listas de confiança (página 64).

Acerca dos tipos de listas de confiança

As Protecções do Sistema no painel Listas de Confiança representam alterações não autorizadas do registo e de ficheiros detectadas anteriormente pelo VirusScan, mas que o utilizador optou por permitir a partir de um alerta ou do painel Resultados da Análise. Existem cinco tipos de listas de confiança que podem ser geridos no painel Listas de Confiança: Programa de Protecções do Sistema, Protecções do Sistema do Windows, Protecções do Sistema do Browser, Programas de Confiança e Sobrecargas da Memória Intermédia de Confiança.

Opção	Descrição
Programa de Protecções do Sistema	O Programa de Protecções do Sistema no painel Listas de Confiança representa alterações não autorizadas do registo e de ficheiros detectadas anteriormente pelo VirusScan, mas que o utilizador optou por permitir a partir de um alerta ou do painel Resultados da Análise. O Programa de Protecções do Sistema detecta alterações não autorizadas do registo e de ficheiros associados a instalações ActiveX, itens de arranque, hooks de execução da shell do Windows e actividade de carregamento com atraso do objecto do serviço da shell. Estes tipos de alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.

Opção	Descrição
Protecções do Sistema do Windows	As Protecções do Sistema do Windows no painel Listas de Confiança representam alterações não autorizadas do registo e de ficheiros detectadas anteriormente pelo VirusScan, mas que o utilizador optou por permitir a partir de um alerta ou do painel Resultados da Análise. As Protecções do Sistema do Windows detectam alterações não autorizadas do registo e de ficheiros associadas a processadores de menus de contexto, appInit DLLs, o ficheiro hosts do Windows, a shell de início de sessão do Windows e Fornecedores de Serviços em Camadas (LSPs) do Winsock, entre outros. Estes tipos de alterações não autorizadas do registo e de ficheiros podem afectar a forma como o computador envia e recebe informação através da Internet, alterar o aspecto e o comportamento de programas e permitir a execução de programas suspeitos no computador.
Protecções do Sistema do Browser	As Protecções do Sistema do Browser no painel Listas de Confiança representam alterações não autorizadas do registo e de ficheiros detectadas anteriormente pelo VirusScan, mas que o utilizador optou por permitir a partir de um alerta ou do painel Resultados da Análise. As Protecções do Sistema do Browser detectam alterações não autorizadas do registo e outros comportamentos indesejados associados a objectos auxiliares do Browser, suplementos, URLs e zonas de segurança do Internet Explorer, entre outros. Estes tipos de alterações não autorizadas do registo podem resultar em actividades indesejadas do browser, tais como o redireccionamento para Web sites suspeitos, alterações de definições e opções do browser e confiança em Web sites suspeitos.
Programas de Confiança	Os programas de confiança são programas potencialmente indesejados detectados anteriormente pelo VirusScan, mas que o utilizador optou por confiar a partir de um alerta ou do painel Resultados da Análise.

Opção	Descrição
Sobrecargas da Memória Intermédia de Confiança	As sobrecargas da memória intermédia de confiança representam actividades indesejadas detectadas anteriormente pelo VirusScan, mas que o utilizador optou por confiar a partir de um alerta ou do painel Resultados da Análise. As sobrecargas da memória intermédia podem danificar o computador e os respectivos ficheiros. As sobrecargas da memória intermédia ocorrem quando a quantidade de informações que os programas ou processos suspeitos armazenam numa memória intermédia excede a capacidade da mesma.

CAPÍTULO 13

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.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades da Firewall Pessoal

Níveis de protecção padrão e personalizados	Proteja-se contra intrusos e actividades suspeitas, utilizando as definições de protecção predefinidas ou personalizáveis da firewall.
Recomendações em tempo real	Receba recomendações de uma forma dinâmica, que o ajudam a decidir se deve permitir o acesso de programas à Internet ou se deve confiar no tráfego da rede.
Gestão de acesso inteligente para programas	Efectue a gestão do acesso dos programas à Internet através de alertas e registos de eventos e configure permissões de acesso para programas específicos.
Protecção de jogos	Evite que alertas relativos a tentativas de intrusão e actividades suspeitas o distraiam durante um jogo em ecrã inteiro.
Protecção durante o arranque do computador	Proteja o computador de tentativas de intrusão, programas indesejados e tráfego de rede logo que inicia o Windows®.
Controlo da porta de serviço do sistema	Efectue a gestão das portas de serviço do sistema abertas e fechadas requeridas por alguns programas.
Gerir ligações do computador	Permita e bloqueie ligações remotas entre outros computadores e o seu computador.
Integração de informações do HackerWatch	Registe padrões globais de invasão e intrusão através do Web site do HackerWatch, que também fornece informações de segurança actuais sobre os programas instalados no seu computador, bem como estatísticas globais de eventos de segurança e de portas da Internet.
Bloquear a firewall	Bloqueie instantaneamente todo o tráfego de entrada e saída entre o computador e a Internet.
Restaurar a firewall	Restaure instantaneamente as definições de protecção originais da Firewall.
Detecção avançada de cavalos de Tróia	Detecte e impeça que aplicações potencialmente maliciosas, tais como cavalos de Tróia, enviem os seus dados pessoais para a Internet.
Registo de eventos	Rastreie eventos recentes de entrada, de saída e intrusões.
Monitorizar tráfego da Internet	Analise mapas à escala mundial que mostram a origem do tráfego e dos ataques hostis. Além disso, localize informações detalhadas do proprietário e dados geográficos dos endereços IP de origem. Analise ainda o tráfego de entrada e de saída, monitorize a largura de banda dos programas e a actividade dos programas.
Prevenção de intrusões	Proteja a sua privacidade de possíveis ameaças da Internet. Através de uma funcionalidade semelhante à heurística, fornecemos 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	Analise 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.

CAPÍTULO 14

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 Recomendações Inteligentes e o nível de segurança Automático (com a opção seleccionada para permitir apenas acesso de saída da Internet aos programas) são activados automaticamente.

Embora possa desactivar a Firewall no painel Configuração de Internet e Rede, o computador deixa de estar protegido contra intrusões e tráfego de rede indesejado, não sendo possível 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 e 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 & Rede.

Neste capítulo

Iniciar a protecção por firewall

Pode activar a firewall para proteger o computador contra intrusões e tráfego de rede indesejado, bem como gerir as ligações de entrada e saída da Internet.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está desactivada**, clique em **Activada**.

Parar a protecção por firewall

Pode desactivar a firewall se não pretender proteger o computador contra intrusões e tráfego de rede indesejado. Se a firewall estiver desactivada, não poderá gerir as ligações de entrada e saída da Internet.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Desactivada**.

CAPÍTULO 15

Utilizar alertas

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

- Alerta vermelho
- Alerta amarelo
- Alerta verde

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

Neste capítulo

Acerca dos alertas

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

Alerta vermelho

O alerta vermelho é apresentado quando a Firewall detecta, e depois bloqueia, um cavalo de Tróia no computador e recomenda a análise de outras ameaças. Um cavalo de Tróia aparenta ser um programa legítimo, mas pode interromper, danificar e conceder acesso não autorizado ao seu computador. Este alerta ocorre em todos os níveis de segurança.

Alerta amarelo

O tipo mais frequente de alerta é o alerta amarelo, que informa sobre a actividade de um programa ou um evento de rede detectados pela Firewall. Quando esta situação ocorre, o alerta descreve a actividade do programa ou o evento de rede e, em seguida, apresenta uma ou mais opções que requerem a sua resposta. Por exemplo, o alerta **Nova Ligação de Rede** é apresentado quando um computador com uma Firewall instalada é ligado a uma nova rede. Pode especificar o nível de confiança que pretende atribuir a esta nova rede sendo, em seguida, apresentada na lista de Redes. Se a opção Recomendações Inteligentes estiver activada, os programas conhecidos são adicionados automaticamente ao painel Permissões do Programa.

Alerta verde

Na maioria dos casos, um alerta verde inclui informações básicas sobre um evento e não requer qualquer resposta. Por predefinição, os alertas verdes estão desactivados.

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 permitido acesso a um programa.

CAPÍTULO 16

Gerir alertas informativos

A firewall permite mostrar ou ocultar alertas informativos quando detecta tentativas de intrusão ou actividades suspeitas durante determinados eventos, por exemplo, durante jogos em ecrã inteiro.

Neste capítulo

Apresentar alertas durante jogos

Pode permitir que os alertas informativos sejam mostrados quando a firewall detecta tentativas de intrusão ou actividades suspeitas durante jogos em ecrã inteiro.

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

Ocultar alertas informativos

Pode impedir que os alertas informativos sejam mostrados quando a firewall detectar tentativas de intrusão ou actividades suspeitas.

1. No painel do McAfee SecurityCenter, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configuração do SecurityCenter, em **Alertas** clique em **Avançada**.
4. No painel Configuração do SecurityCenter, clique em **Alertas Informativos**.
5. No painel Alertas Informativos, proceda de um dos seguintes modos:
   - Seleccione **Não mostrar alertas informativos** para ocultar todos os alertas informativos.
   - Desmarque um alerta para o ocultar.
6. Clique em **OK**.

CAPÍTULO 17

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 da segurança da protecção do computador é definido como Automático e é permitido apenas acesso de saída da Internet aos programas. 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 acesso dos programas à Internet.

Neste capítulo

Gerir os níveis de segurança da Firewall

Os níveis de segurança da Firewall controlam o grau de gestão e resposta a alertas. Esses alertas são apresentados quando a firewall detecta tráfego de rede indesejado e ligações de entrada e saída da Internet. Por predefinição, o nível de segurança da Firewall está definido como Automático, com acesso apenas de saída.

Se o nível de segurança Automático estiver definido e a opção Recomendações Inteligentes estiver activada, os alertas amarelos disponibilizam a opção de permitir ou bloquear o acesso a programas desconhecidos que requeiram acesso de entrada. Apesar de os alertas verdes estarem desactivados por predefinição, estes serão apresentados quando forem detectados programas conhecidos e o acesso será permitido automaticamente. A concessão de acesso 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 Padrão), maior será o número de opções e alertas apresentados e que, por sua vez, devem ser geridos pelo utilizador.

A tabela seguinte descreve os três níveis de segurança da Firewall, do nível mais restritivo para o menos restritivo:

Nível	Descrição
Invisível	Bloqueia todas as ligações de entrada da Internet, excepto as portas abertas, ocultando a presença do computador na Internet. A firewall alerta o utilizador quando novos programas tentam estabelecer ligações de saída para a Internet ou quando recebe pedidos de ligação de entrada. Os programas bloqueados e adicionados são apresentados no painel Permissões do Programa.
Padrão	Monitoriza as ligações de entrada e saída e alerta-o quando novos programas tentam aceder à Internet. Os programas bloqueados e adicionados são apresentados no painel Permissões do Programa.

Nível	Descrição
Automática	Permite aos programas ter acesso de entrada e saída (total) ou apenas de saída da Internet. O nível de segurança predefinido é Automático, com a opção seleccionada para permitir apenas acesso de saída aos programas. Se for permitido acesso total a um programa, a Firewall confia automaticamente nesse programa e adiciona-o à lista de programas permitidos no painel Permissões do Programa. Se for permitido apenas acesso de saída a um programa, a Firewall confia automaticamente nesse programa apenas quando este estabelece uma ligação de saída da Internet. Uma ligação de entrada não é considerada fidedigna automaticamente.

A Firewall permite também repor de imediato o nível de segurança para Automático (e permitir apenas acesso de saída) no painel Restaurar Predefinições da Firewall.

Definir o nível de segurança para Invisível

É possível definir o nível de segurança da Firewall para Invisível para bloquear todas as ligações de entrada na rede, excepto as portas abertas, a fim de ocultar a presença do computador na Internet.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Nível de Segurança, mova a barra de deslocamento para que **Invisível** seja apresentado como o nível activado.
4. Clique em **OK**.

Nota: No modo Invisível, a Firewall alerta-o quando novos programas solicitarem ligações de saída para a Internet ou receberem pedidos de ligação de entrada.

Definir o nível de segurança para Padrão

É possível definir o nível de segurança para Padrão para monitorizar as ligações de entrada e saída e alertar se novos programas tentarem aceder à Internet.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Nível de Segurança, mova o controlo de deslize para que **Padrão** seja apresentado como o nível activado.
4. Clique em **OK**.

Definir o nível de segurança para Automático

É possível definir o nível de segurança da Firewall como Automático, a fim de permitir acesso total ou apenas de saída na rede.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Nível de Segurança, mova a barra de deslocamento para que **Automático** seja apresentado como o nível activado.
4. Proceda de um dos seguintes modos:
   - Para permitir acesso total de entrada e saída na rede, seleccione **Permitir Acesso Total**.
   - Para permitir apenas acesso de saída da rede, seleccione **Permitir Apenas Acesso de Saída**.
5. Clique em **OK**.

Nota: A opção **Permitir Apenas Acesso de Saída** é a opção predefinida.

Configurar Recomendações Inteligentes para alertas

Pode configurar a Firewall para incluir, excluir ou apresentar recomendações em alertas quando qualquer programa tentar aceder à Internet. A activação de Recomendações Inteligentes ajuda-o a lidar com alertas.

Se a opção Recomendações Inteligentes estiver aplicada (e o nível de segurança for Automático com acesso apenas de saída activado), a Firewall permite automaticamente o acesso a programas conhecidos e bloqueia programas potencialmente perigosos.

Se a opção Recomendações Inteligentes não estiver aplicada, a Firewall não permite nem bloqueia o acesso à Internet e também não fornece nenhuma recomendação no alerta.

Se a opção Recomendações Inteligentes estiver definida para Mostrar, um alerta solicita-lhe que permita ou bloqueie o acesso e a Firewall fornece uma recomendação no alerta.

Activar Recomendações Inteligentes

É possível activar as Recomendações Inteligentes para que a Firewall permita ou bloqueie automaticamente programas e alerte o utilizador sobre programas desconhecidos e potencialmente perigosos.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Nível de Segurança, em **Recomendações Inteligentes**, seleccione **Aplicar Recomendações Inteligentes**.
4. Clique em **OK**.

Desactivar Recomendações Inteligentes

É possível desactivar as Recomendações Inteligentes para que a firewall permita ou bloqueie programas e alerte o utilizador sobre programas desconhecidos e potencialmente perigosos. No entanto, os alertas deixam de apresentar recomendações sobre como gerir o acesso dos programas. Se a Firewall detectar um novo programa considerado suspeito ou uma possível ameaça, bloqueia automaticamente o acesso do programa à Internet.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Nível de Segurança, em **Recomendações Inteligentes**, seleccione **Não Aplicar Recomendações Inteligentes**.
4. Clique em **OK**.

Mostrar Recomendações Inteligentes

É possível mostrar as Recomendações Inteligentes para que apresentem apenas uma recomendação nos alertas que possibilite ao utilizador decidir se permite ou bloqueia programas desconhecidos e potencialmente perigosos.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Nível de Segurança, em **Recomendações Inteligentes**, seleccione **Mostrar Recomendações Inteligentes**.
4. 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 quando o Windows® é iniciado. Os utilizadores experientes também podem rastrear (ou enviar ping) ao seu computador para verificar se está ligado a uma rede. Além disso, podem enviar informações para o seu computador utilizando o protocolo UDP, sob a forma de unidades de mensagens (datagramas). A Firewall protege o computador contra estes tipos de intrusão permitindo bloquear o acesso de programas à Internet quando o Windows é iniciado, bloquear os pedidos de ping que ajudam outros utilizadores a detectar o computador numa rede e não permitindo que outros utilizadores enviem informações para o computador sob a forma de unidades de mensagens (datagramas).

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

É possível proteger o computador quando o Windows é iniciado, a fim de bloquear novos programas que não tinham, e agora necessitam, de acesso à Internet durante o arranque. A Firewall apresenta alertas relevantes sobre os programas que tenham solicitado acesso à Internet, o qual pode ser permitido ou bloqueado.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Nível de Segurança, em **Definições de Segurança**, seleccione **Activar protecção durante o arranque do Windows**.
4. Clique em **OK**.

Nota: As ligações e as intrusões bloqueadas não são registadas quando a protecção no arranque está activada.

Configurar definições de pedidos de ping

É possível permitir ou impedir a detecção do seu computador na rede por outros utilizadores.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. 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.
4. Clique em **OK**.

Configurar definições UDP

Pode permitir que outros utilizadores do computador de rede enviem unidades de mensagens (datagramas) para o computador, utilizando o protocolo UDP. No entanto, só poderá fazê-lo se tiver fechado uma porta de serviço do sistema para bloquear este protocolo.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Nível de Segurança, em **Definições de Segurança**, efectue um dos seguintes passos:
   - Seleccione **Activar rastreio UDP** para permitir que outros utilizadores enviem unidades de mensagens (datagramas) para o seu computador.
   - Desmarque **Activar rastreio UDP** para impedir que outros utilizadores enviem unidades de mensagens (datagramas) para o seu computador.
4. Clique em **OK**.

Configurar a detecção de intrusões

É possível detectar tentativas de intrusão para proteger o computador contra ataques e análises não autorizadas. A definição padrão da firewall inclui a detecção automática das tentativas de intrusão mais frequentes, tais como ataques de Recusa de Serviço ou explorações; no entanto, é possível desactivar a detecção automática para um ou mais ataques ou análises.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Detecção de Intrusões**.
4. 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.
5. Clique em **OK**.

Configurar as definições de Estado de Protecção por Firewall

É possível configurar a Firewall para ignorar que problemas específicos do computador não são comunicados ao SecurityCenter.

1. No painel direito do McAfee SecurityCenter, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. No painel Configuração do SecurityCenter, em **Estado da Protecção** clique em **Avançada**.
3. No painel Problemas Ignorados, seleccione uma ou mais das seguintes opções:
   - **A protecção por firewall está desactivada.**
   - **O serviço Firewall não está a funcionar.**
   - **A protecção por firewall não está instalada no computador.**
   - **A Firewall do Windows está desactivada.**
   - **A firewall de saída não está instalada no computador.**
4. Clique em **OK**.

Bloquear e restaurar a Firewall

A opção Bloquear impede instantaneamente todas as ligações de rede de entrada e saída, incluindo o acesso a Web sites, correio electrónico e actualizações de segurança. A opção Bloquear produz o mesmo resultado que desligar os cabos de rede do computador. Pode utilizar esta definição para bloquear portas abertas no painel Serviços do Sistema, bem como ajudar a isolar e a resolver problemas no computador.

Bloquear a Firewall instantaneamente

É possível bloquear a Firewall para impedir instantaneamente todo o tráfego de rede entre o computador e qualquer rede, incluindo a Internet.

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Bloquear Firewall**.
2. No painel Bloquear Firewall, clique em **Activar Bloqueio da Firewall**.
3. Clique em **Sim** para confirmar.

Sugestão: Também pode bloquear a Firewall clicando com o botão direito do rato no ícone do SecurityCenter na área de notificação situada na extremidade direita da barra de tarefas, clicando em **Ligações Rápidas** e, em seguida, clicando em **Bloquear Firewall**.

Desbloquear a Firewall de imediato

É possível desbloquear a Firewall para permitir instantaneamente todo o tráfego de rede entre o computador e qualquer rede, incluindo a Internet.

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Bloquear Firewall**.
2. No painel Bloqueio Activado, clique em **Desactivar Bloqueio da Firewall**.
3. Clique em **Sim** para confirmar.

Restaurar definições da Firewall

Pode restaurar rapidamente a Firewall para as definições originais de protecção. Deste modo, repõe o nível de segurança para Automático e permite apenas acesso de saída da rede, activa as Recomendações Inteligentes, restaura a lista de programas predefinidos e as respectivas permissões no painel Permissões do Programa, remove os endereços IP de confiança e banidos e restaura os serviços do sistema, as definições do registo de eventos e a detecção de intrusões.

1. No painel do McAfee SecurityCenter, clique em **Restaurar Predefinições da Firewall**.
2. No painel Restaurar Predefinições de Protecção por Firewall, clique em **Restaurar Predefinições**.
3. Clique em **Sim** para confirmar.
4. Clique em **OK**.

CAPÍTULO 18

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 controlar o acesso total ou apenas de saída a programas. Pode também bloquear o acesso a programas.

Neste capítulo

Permitir 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:

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

Também é possível permitir acesso total e apenas de saída para a Internet a programas, a partir dos registos Eventos de Saída e Eventos Recentes.

Permitir acesso total a um programa

É possível permitir que um programa bloqueado no computador tenha acesso total de entrada e saída da Internet.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Permissões do Programa**.
4. Em **Permissões do Programa**, seleccione um programa que esteja definido como **Bloqueado** ou **Apenas Acesso de Saída**.
5. Em **Acção**, clique em **Permitir Acesso**.
6. Clique em **OK**.

Permitir acesso total a um novo programa

É possível permitir que um novo programa no computador tenha acesso total de entrada e saída da Internet.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Permissões do Programa**.
4. Em **Permissões do Programa**, clique em **Adicionar Programa Permitido**.
5. Na caixa de diálogo **Adicionar Programa**, procure e seleccione o programa que pretende adicionar e clique em **Abrir**.

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 **Permitir Apenas Acesso de Saída** ou em **Bloquear Acesso** em **Acção**.

Permitir acesso total a partir do registo Eventos Recentes

É possível permitir que um programa bloqueado apresentado no registo de Eventos Recentes tenha acesso total de entrada e saída da Internet.

1. No painel do McAfee SecurityCenter, clique em **Menu Avançado**.
2. Clique em **Relatórios & Registos**.
3. Em **Eventos Recentes**, seleccione a descrição do evento e clique em **Permitir Acesso**.
4. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar.

Tópicos relacionados

- Ver eventos de saída (página 111)

Permitir acesso total a partir do registo Eventos de Saída

É possível permitir que um programa bloqueado apresentado no registo de Eventos de Saída tenha acesso total de entrada e saída da Internet.

1. No painel do McAfee SecurityCenter, clique em **Menu Avançado**.
2. Clique em **Relatórios & Registos**.
3. Em **Eventos Recentes**, clique em **Ver Registo**.
4. Clique em **Internet & Rede** e depois clique em **Eventos de Saída**.
5. Seleccione um programa e, em **Quero**, clique em **Permitir Acesso**.
6. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar.

Permitir apenas acesso de saída a programas

Alguns programas no computador requerem acesso de saída para a Internet. A firewall permite configurar as permissões do programa para permitir apenas acesso de saída para a Internet.

Permitir apenas acesso de saída a um programa

É possível permitir que um programa tenha apenas acesso de saída para a Internet.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Permissões do Programa**.
4. Em **Permissões do Programa**, seleccione um programa que esteja definido como **Bloqueado** ou **Acesso Total**.
5. Em **Acção**, clique em **Permitir Apenas Acesso de Saída**.
6. Clique em **OK**.

Permitir apenas acesso de saída a partir do registo Eventos Recentes

É possível permitir que um programa bloqueado apresentado no registo de Eventos Recentes tenha apenas acesso de saída para a Internet.

1. No painel do McAfee SecurityCenter, clique em **Menu Avançado**.
2. Clique em **Relatórios & Registos**.
3. Em **Eventos Recentes**, seleccione a descrição do evento e clique em **Permitir Apenas Acesso de Saída**.
4. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar.

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

É possível permitir que um programa bloqueado apresentado no registo de Eventos de Saída tenha apenas acesso de saída para a Internet.

1. No painel do McAfee SecurityCenter, clique em **Menu Avançado**.
2. Clique em **Relatórios & Registos**.
3. Em **Eventos Recentes**, clique em **Ver Registo**.
4. Clique em **Internet & Rede** e depois clique em **Eventos de Saída**.
5. Seleccione um programa e, em **Quero**, clique em **Permitir Apenas Acesso de Saída**.
6. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar.

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

É possível bloquear a permissão de acesso de entrada e saída da Internet a um programa.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Permissões do Programa**.
4. Em **Permissões do Programa**, seleccione um programa que esteja definido como **Acesso Total** ou **Acesso Apenas de Saída**.
5. Em **Acção**, clique em **Bloquear Acesso**.
6. Clique em **OK**.

Bloquear o acesso a um novo programa

É possível bloquear a permissão de acesso de entrada e saída da Internet a um novo programa.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Permissões do Programa**.
4. Em **Permissões do Programa**, clique em **Adicionar Programa Bloqueado**.
5. Na caixa de diálogo Adicionar Programa, procure e seleccione o programa que pretende adicionar e clique em **Abrir**.

Nota: Pode alterar as permissões de um novo programa adicionado, seleccionando e clicando em **Permitir Apenas Acesso de Saída** ou em **Bloquear Acesso** em **Acção**.

Bloquear o acesso a partir do registo Eventos Recentes

É possível bloquear a permissão de acesso de entrada e saída da Internet a um programa apresentado no registo de Eventos Recentes.

1. No painel do McAfee SecurityCenter, clique em **Menu Avançado**.
2. Clique em **Relatórios & Registos**.
3. Em **Eventos Recentes**, seleccione a descrição do evento e clique em **Bloquear Acesso**.
4. Na caixa de diálogo Permissões do Programa, clique em **Sim** para confirmar.

Remover as permissões de acesso dos programas

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

Remover uma permissão de programa

É possível remover a permissão de acesso de entrada e saída da Internet de um programa.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Permissões do Programa**.
4. Em **Permissões do Programa**, seleccione um programa.
5. Em **Acção**, clique em **Remover Permissão do Programa**.
6. Clique em **OK**.

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

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.

Obter informações sobre programas

Pode obter informações sobre o programa no Web site HackerWatch da McAfee para decidir se permite ou bloqueia o acesso de entrada e saída da Internet.

Nota: Certifique-se de que está ligado à Internet para que o browser inicie o Web site HackerWatch da McAfee, o qual fornece informações actualizadas sobre programas, requisitos de acesso à Internet e ameaças de segurança.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Permissões do Programa**.
4. Em **Permissões do Programa**, seleccione um programa.
5. Em **Acção**, clique em **Mais Informações**.

Obter informações sobre programas a partir do registo Eventos de Saída

A partir do Registo de Eventos de Saída, pode obter informações sobre o programa no Web site HackerWatch da McAfee para decidir se permite ou bloqueia o acesso de entrada e saída da Internet.

Nota: Certifique-se de que está ligado à Internet para que o browser inicie o Web site HackerWatch da McAfee, o qual fornece informações actualizadas sobre programas, requisitos de acesso à Internet e ameaças de segurança.

1. No painel do McAfee SecurityCenter, clique em **Menu Avançado**.
2. Clique em **Relatórios & Registos**.
3. Em Eventos Recentes, seleccione um evento e clique em **Ver Registo**.
4. Clique em **Internet & Rede** e depois clique em **Eventos de Saída**.
5. Seleccione um endereço IP e clique em **Mais informações**.

CAPÍTULO 19

Gerir ligações a computadores

Pode configurar a Firewall para gerir ligações remotas específicas ao computador, criando regras baseadas em endereços Protocolo Internet (IP), associados a computadores remotos. Os computadores associados a endereços IP de confiança podem estabelecer ligação 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 de confiança for infectado por um worm ou outro mecanismo, o seu computador poderá ficar vulnerável à infecção. Além disso, a McAfee recomenda que o computador de confiança esteja protegido por uma firewall e um programa antivírus actualizado. A Firewall não regista tráfego nem gera alertas de eventos a partir de endereços IP de confiança na lista **Redes**.

Pode banir computadores associados a endereços IP desconhecidos, suspeitos ou duvidosos, impedindo assim que estabeleçam ligação ao 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. 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.

Neste capítulo

Acerca de ligações do computador

As ligações do computador são ligações que este estabelece com outros computadores de qualquer rede e dentro da sua própria rede. Pode adicionar, editar e remover endereços IP na lista **Redes**. Estes endereços IP estão associados a redes às quais pretende atribuir um nível de confiança quando estabelecerem ligação ao computador: De Confiança, Padrão e Público.

Nível	Descrição
De Confiança	A Firewall permite que o computador receba tráfego de um IP através de qualquer porta. A actividade entre o computador associado a um endereço IP de confiança e o seu computador não é filtrada nem analisada pela Firewall. Por predefinição, a primeira rede privada que a Firewall encontra é apresentada como De Confiança na lista **Redes**. Um exemplo de uma rede De Confiança é um computador ou computadores na sua rede local ou doméstica.
Padrão	A Firewall controla o tráfego de um IP (mas não de qualquer outro computador nessa rede) quando estabelece ligação ao computador e permite-o ou bloqueia-o de acordo com as regras na lista **Serviços do Sistema**. A Firewall regista o tráfego e gera alertas de eventos a partir dos endereços IP Padrão. Um exemplo de uma rede Padrão é um computador ou computadores numa rede empresarial.
Público	A Firewall controla o tráfego a partir de uma rede pública de acordo com as regras na lista **Serviços do Sistema**. Um exemplo de uma rede Pública é uma rede Internet num café, hotel ou aeroporto.

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

Adicionar uma ligação de computador

É possível adicionar uma ligação de computador de confiança, padrão ou pública e o endereço IP associado.

1 No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.

2 No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.

3 No painel Firewall, clique em **Redes**.

4 No painel Redes, clique em **Adicionar**.

5 Se a ligação de computador estiver numa rede IPv6, seleccione a caixa de verificação **IPv6**.

6 Em **Adicionar Regra**, proceda de um dos seguintes modos:

- Seleccione **Único** e, em seguida, introduza o endereço IP na caixa **Endereço IP**.
- Seleccione **Intervalo** e, em seguida, introduza os endereços IP inicial e final nas caixas **Do Endereço IP** e **Até ao Endereço IP**. Se a ligação de computador estiver numa rede IPv6, introduza o endereço IP inicial e o comprimento do prefixo nas caixas **Do Endereço IP** e **Comprimento do Prefixo**.

7 Em **Tipo**, proceda de um dos seguintes modos:

- Seleccione **De Confiança** para especificar que esta ligação de computador é de confiança (por exemplo, um computador numa rede doméstica).
- Seleccione **Padrão** para especificar que a ligação deste computador (e não dos outros computadores na respectiva rede) é de confiança (por exemplo, um computador numa rede empresarial).
- Seleccione **Público** para especificar que esta ligação de computador é pública (por exemplo, um computador num cibercafé, hotel ou aeroporto).

8 Se um serviço do sistema utilizar a Partilha de Ligação à Internet (ICS), é possível adicionar o seguinte intervalo de endereços IP: 192.168.0.1 a 192.168.0.255.

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

10 Pode ainda introduzir uma descrição para a regra.

11 Clique em **OK**.

Nota: Para obter mais informações sobre a Partilha de Ligação à Internet (ICS), consulte a secção Configurar um novo serviço do sistema.

Adicionar um computador do registo Eventos de Entrada

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

1. No painel Tarefas Comuns do painel do McAfee SecurityCenter, clique em **Menu Avançado**.
2. Clique em **Relatórios e Registos**.
3. Em **Eventos Recentes**, clique em **Ver Registo**.
4. Clique em **Internet e Rede** e depois clique em **Eventos de Entrada**.
5. Seleccione um endereço IP de origem e, em **Quero**, proceda de um dos seguintes modos:
   - Clique em **Adicionar este IP como De Confiança** para adicionar este computador como De Confiança na lista **Redes**.
   - Clique em **Adicionar este IP como Padrão** para adicionar esta ligação de computador como Padrão na lista **Redes**.
6. Clique em **Sim** para confirmar.

Editar uma ligação de computador

É possível editar uma ligação de computador de confiança, padrão ou pública e o respectivo endereço IP associado.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Redes**.
4. No painel Redes, seleccione um endereço IP e, em seguida, clique em **Editar**.
5. Se a ligação de computador estiver numa rede IPv6, seleccione a caixa de verificação **IPv6**.
6. Em **Editar Regra**, proceda de um dos seguintes modos:
   - Seleccione **Único** e, em seguida, introduza o endereço IP na caixa **Endereço IP**.
   - Seleccione **Intervalo** e, em seguida, introduza os endereços IP inicial e final nas caixas **Do Endereço IP** e **Até ao Endereço IP**. Se a ligação de computador estiver numa rede IPv6, introduza o endereço IP inicial e o comprimento do prefixo nas caixas **Do Endereço IP** e **Comprimento do Prefixo**.

7 Em **Tipo**, proceda de um dos seguintes modos:
   - Seleccione **De Confiança** para especificar que esta ligação de computador é de confiança (por exemplo, um computador numa rede doméstica).
   - Seleccione **Padrão** para especificar que a ligação deste computador (e não dos outros computadores na respectiva rede) é de confiança (por exemplo, um computador numa rede empresarial).
   - Seleccione **Público** para especificar que esta ligação de computador é pública (por exemplo, um computador num cibercafé, hotel ou aeroporto).
8 Também pode seleccionar **Regra expira em** e introduzir o número de dias para aplicar a regra.
9 Pode ainda introduzir uma descrição para a regra.
10 Clique em **OK**.

Nota: Não é possível editar a ligação de computador predefinida que a Firewall adicionou automaticamente a partir de uma rede privada fidedigna.

Remover uma ligação de computador

É possível remover uma ligação de computador de confiança, padrão ou pública e o respectivo endereço IP associado.

1 No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2 No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3 No painel Firewall, clique em **Redes**.
4 No painel Redes, seleccione um endereço IP e, em seguida, clique em **Remover**.
5 Clique em **Sim** para confirmar.

Banir ligações de computadores

É possível adicionar, editar e remover endereços IP banidos no painel IPs Banidos.

Pode banir computadores associados a endereços IP desconhecidos, suspeitos ou duvidosos, impedindo assim que estabeleçam ligação ao 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. 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.

Adicionar uma ligação de computador banida

É possível adicionar uma ligação de computador banida e o endereço IP associado.

Nota: 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.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **IPs Banidos**.
4. No painel IPs Banidos, clique em **Adicionar**.
5. Se a ligação de computador estiver numa rede IPv6, seleccione a caixa de verificação **IPv6**.
6. Em **Adicionar Regra**, proceda de um dos seguintes modos:
   - Seleccione **Único** e, em seguida, introduza o endereço IP na caixa **Endereço IP**.
   - Seleccione **Intervalo** e, em seguida, introduza os endereços IP inicial e final nas caixas **Do Endereço IP** e **Até ao Endereço IP**. Se a ligação de computador estiver numa rede IPv6, introduza o endereço IP inicial e o comprimento do prefixo nas caixas **Do Endereço IP** e **Comprimento do Prefixo**.
7. Também pode seleccionar **Regra expira em** e introduzir o número de dias para aplicar a regra.
8. Pode ainda introduzir uma descrição para a regra.
9. Clique em **OK**.
10. Clique em **Sim** para confirmar.

Editar uma ligação de computador banida

É possível editar uma ligação de computador banida e o endereço IP associado.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **IPs Banidos**.
4. No painel IPs Banidos, clique em **Editar**.
5. Se a ligação de computador estiver numa rede IPv6, seleccione a caixa de verificação **IPv6**.
6. Em **Editar Regra**, proceda de um dos seguintes modos:
   - Seleccione **Único** e, em seguida, introduza o endereço IP na caixa **Endereço IP**.
   - Seleccione **Intervalo** e, em seguida, introduza os endereços IP inicial e final nas caixas **Do Endereço IP** e **Até ao Endereço IP**. Se a ligação de computador estiver numa rede IPv6, introduza o endereço IP inicial e o comprimento do prefixo nas caixas **Do Endereço IP** e **Comprimento do Prefixo**.
7. Também pode seleccionar **Regra expira em** e introduzir o número de dias para aplicar a regra.
8. Pode ainda introduzir uma descrição para a regra.
9. Clique em **OK**.

Remover uma ligação de computador banida

É possível remover uma ligação de computador banida e o endereço IP associado.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **IPs Banidos**.
4. No painel IPs Banidos, seleccione um endereço IP e, em seguida, clique em **Remover**.
5. Clique em **Sim** para confirmar.

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. Utilize este registo, 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.

Adicione um endereço IP à lista **IPs Banidos** se pretender bloquear todo o tráfego de entrada da Internet desse endereço IP, independentemente de as portas dos Serviços do Sistema estarem abertas ou fechadas.

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Menu Avançado**.
2. Clique em **Relatórios e Registos**.
3. Em **Eventos Recentes**, clique em **Ver Registo**.
4. Clique em **Internet e Rede** e depois clique em **Eventos de Entrada**.
5. Seleccione um endereço IP de origem e, em **Quero**, clique em **Banir este IP**.
6. Clique em **Sim** para confirmar.

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.

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Menu Avançado**.
2. Clique em **Relatórios e Registos**.
3. Em **Eventos Recentes**, clique em **Ver Registo**.
4. Clique em **Internet e Rede** e depois clique em **Eventos de Detecção de Intrusões**.
5. Seleccione um endereço IP de origem e, em **Quero**, clique em **Banir este IP**.
6. Clique em **Sim** para confirmar.

CAPÍTULO 20

Gerir serviços do sistema

Para um funcionamento adequado, determinados programas (incluindo servidores Web e programas de servidores de partilha de ficheiros) têm de 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 têm de estar abertas.

Neste capítulo

Configurar portas do serviço do sistema

As portas de serviços do sistema podem ser configuradas para permitir ou bloquear o acesso remoto à rede a serviços do computador. Estas portas do serviço do sistema podem ser abertas ou fechadas para os computadores apresentados como De Confiança, Padrão ou Públicos na lista **Redes**.

A lista seguinte apresenta os serviços do sistema comuns e as respectivas portas associadas:

- Porta 5357 Comum do Sistema Operativo
- 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
- Protocolo de Hora de Rede - Porta 123
- Ambiente de Trabalho Remoto / 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

As portas de serviços do sistema também podem ser configuradas para permitir que um computador partilhe a sua ligação à Internet com outros computadores ligados a este através da mesma rede. Esta ligação, conhecida como Partilha de Ligação à Internet (ICS), permite que o computador que está a partilhar a ligação actue como gateway para a Internet para os outros computadores ligados em rede.

Nota: Se o computador tiver uma aplicação que aceite ligações a servidores FTP ou Web, o computador que partilha a ligação poderá necessitar de abrir a porta do serviço do sistema associado e permitir o reencaminhamento de ligações de entrada para essas portas.

Permitir acesso a uma porta de serviço do sistema existente

É possível abrir uma porta existente para permitir o acesso remoto a um serviço do sistema no computador.

Nota: 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.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Serviços do Sistema**.
4. Em **Abrir Porta de Serviços do Sistema**, seleccione um serviço do sistema para abrir a respectiva porta.
5. Clique em **Editar**.
6. Proceda de um dos seguintes modos:
   - Para abrir a porta a qualquer computador numa rede de confiança, padrão ou pública (por exemplo, uma rede doméstica, empresarial ou da Internet), seleccione **De Confiança, Padrão e Público**.
   - Para abrir a porta a qualquer computador numa rede padrão (por exemplo, uma rede empresarial), seleccione **Padrão (inclui De Confiança)**.
7. Clique em **OK**.

Bloquear o acesso a uma porta de serviço do sistema existente

É possível fechar uma porta existente para bloquear o acesso remoto a um serviço do sistema no computador.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Serviços do Sistema**.
4. Em **Abrir Porta de Serviços do Sistema**, desmarque a caixa de verificação junto à porta do serviço do sistema que pretende fechar.
5. Clique em **OK**.

Configurar uma nova porta do serviço do sistema

É possível configurar uma nova porta de serviço de rede no computador que poderá ser aberta ou fechada para permitir ou bloquear o acesso remoto ao computador.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Serviços do Sistema**.
4. Clique em **Adicionar**.
5. No painel Serviços do Sistema, em **Adicionar Regra de Serviço do Sistema**, introduza as seguintes informações:
   - Nome do Serviço do Sistema
   - Categoria de Serviço do Sistema
   - Portas TCP/IP locais
   - Portas UDP locais
6. Proceda de um dos seguintes modos:
   - Para abrir a porta a qualquer computador numa rede de confiança, padrão ou pública (por exemplo, uma rede doméstica, empresarial ou da Internet), seleccione **De Confiança, Padrão e Público**.
   - Para abrir a porta a qualquer computador numa rede padrão (por exemplo, uma rede empresarial), seleccione **Padrão (inclui De Confiança)**.
7. Se pretender enviar informações sobre a actividade nesta porta para outro computador da rede Windows que partilhe a ligação à Internet, seleccione **Reencaminhar a actividade da rede desta porta para os computadores da rede que utilizam a Partilha de Ligação à Internet**.
8. Opcionalmente, pode descrever a nova configuração.
9. Clique em **OK**.

Nota: Se o computador tiver um programa que aceite ligações a servidores FTP ou Web, o computador que partilha a ligação poderá necessitar de abrir a porta do serviço do sistema associado e permitir o reencaminhamento de ligações de entrada para essas portas. Se utiliza a Partilha de Ligação à Internet, deve também adicionar uma ligação de computador de confiança à lista **Redes**. Para mais informações, consulte Adicionar uma ligação de computador.

Modificar uma porta do serviço do sistema

É possível modificar a informação sobre o acesso de entrada e saída da rede relativa a uma porta de serviço do sistema existente.

Nota: Se as informações da porta forem introduzidas incorrectamente, ocorre uma falha no serviço do sistema.

1. No painel McAfee SecurityCenter, clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet e Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Serviços do Sistema**.
4. Clique na caixa de verificação junto a um serviço do sistema e, em seguida, clique em **Editar**.
5. No painel Serviços do Sistema, em **Adicionar Regra de Serviço do Sistema**, modifique as seguintes informações:
   - Nome do serviço do sistema
   - Portas TCP/IP locais
   - Portas UDP locais
6. Proceda de um dos seguintes modos:
   - Para abrir a porta a qualquer computador numa rede de confiança, padrão ou pública (por exemplo, uma rede doméstica, empresarial ou da Internet), seleccione **De Confiança, Padrão e Público**.
   - Para abrir a porta a qualquer computador numa rede padrão (por exemplo, uma rede empresarial), seleccione **Padrão (inclui De Confiança)**.
7. Se pretender enviar informações sobre a actividade nesta porta para outro computador da rede Windows que partilhe a ligação à Internet, seleccione **Reencaminhar a actividade da rede desta porta para os computadores da rede que utilizam a Partilha de Ligação à Internet**.
8. Opcionalmente, pode descrever a configuração modificada.
9. Clique em **OK**.

Remover uma porta do serviço do sistema

É possível remover do computador uma porta de serviço do sistema existente. Após a remoção, os computadores remotos deixam de ter acesso ao serviço de rede no seu computador.

1. No painel McAfee SecurityCenter, clique em **Internet & Rede** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
3. No painel Firewall, clique em **Serviços do Sistema**.
4. Seleccione um serviço do sistema e clique em **Remover**.
5. Na solicitação, clique em **Sim** para confirmar.

CAPÍTULO 21

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 activar ou desactivar o registo de eventos e, no caso de o activar, que tipo de eventos pretende registar. O registo de eventos permite-lhe ver os eventos de entrada e saída recentes e os eventos de intrusão.

Configurar as definições do registo de eventos

É possível especificar e configurar os tipos de eventos de firewall a registar. Por predefinição, o registo de eventos está activado para todos os eventos e actividades.

1. No painel Configuração de Internet & Rede, em **A protecção de firewall está activada**, clique em **Avançada**.
2. No painel Firewall, clique em **Definições de Registo de Eventos**.
3. Se ainda não estiver seleccionada, seleccione a opção **Activar Registo de Eventos**.
4. Em **Activar Registo de Eventos**, seleccione ou desmarque os tipos de eventos que pretende ou não registar. Os tipos de eventos incluem:
   - Programas Bloqueados
   - 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. Mostra a actividade dos programas cujo acesso à Internet foi bloqueado explicitamente.

- 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 eventos de entrada. Os Eventos de Entrada incluem a data e a hora, o endereço IP de origem, o nome do anfitrião e tipo de evento e de informação.

1. Certifique-se de que o menu Avançado está activado. 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 Entrada**.

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

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.

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 Saída**.

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

Ver eventos de detecção de intrusões

Se a opção de registo estiver activada, pode ver eventos de entrada de intrusão. Os eventos de Detecção de Intrusões apresentam a data e a hora, o IP de origem, o nome do anfitrião do evento e o tipo de evento.

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.

Trabalhar com estatísticas

A Firewall optimiza o Web site de segurança HackerWatch 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.

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

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.

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.

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.

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.

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.

1. Certifique-se de que o menu Avançado está activado. 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 Entrada**.
4. No painel Eventos de Entrada, seleccione um endereço IP de origem e, em seguida, clique em **Rastrear este IP**.
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**.

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.

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**. No painel Eventos de Detecção de Intrusões, seleccione um endereço IP de origem e, em seguida. clique em **Rastrear este IP**.
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**.

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 até ao seu computador. Além disso, pode obter informações de registo e rede sobre o endereço IP.

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 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**.

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 de entrada e saída da Internet. Além disso, o Monitor de Tráfego apresenta os programas que utilizam o maior número de ligações de rede no computador, assim como os endereços IP a que 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.

Analisar tráfego de entrada e saída

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

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**.

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.

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.

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 22

Obter informações sobre segurança da Internet

A Firewall optimiza o HackerWatch, o Web site de segurança da McAfee, para fornecer 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.

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 23

McAfee QuickClean

O QuickClean melhora o desempenho do computador através da eliminação de ficheiros desnecessários no computador. Esvazia a Reciclagem e elimina ficheiros temporários, atalhos, fragmentos perdidos de ficheiros, ficheiros de registo, ficheiros em cache, cookies, ficheiros do histórico do browser, correio electrónico enviado e recebido, ficheiros usados recentemente, ficheiros ActiveX e ficheiros de ponto de restauro do sistema. O QuickClean protege igualmente a sua privacidade através da utilização do componente McAfee Shredder para eliminar, de forma permanente e segura, itens que possam conter informações pessoais e confidenciais, tais como o seu nome e endereço. Para informações acerca da destruição de ficheiros, consulte o McAfee Shredder.

O Desfragmentador de Disco dispõe os ficheiros e as pastas no computador de modo a assegurar que não fiquem dispersos (ou seja, fragmentados) quando são guardados no disco rígido do computador. Através da desfragmentação periódica do disco rígido, é possível assegurar que esses ficheiros e pastas fragmentados são consolidados para rápida obtenção posterior.

Se não pretender efectuar manualmente a manutenção do computador, pode programar o QuickClean e o Desfragmentador de Disco para serem executados automaticamente, como tarefas independentes, com qualquer frequência.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do QuickClean

Limpeza de Ficheiros	Elimine ficheiros desnecessários de forma segura e eficaz utilizando vários tipos de limpeza. Através da eliminação desses ficheiros, é possível aumentar o espaço livre no disco rígido do computador e melhorar o seu desempenho.

CAPÍTULO 24

Limpar o computador

O QuickClean elimina ficheiros desnecessários no computador. Esvazia a Reciclagem e elimina ficheiros temporários, atalhos, fragmentos perdidos de ficheiros, ficheiros de registo, ficheiros em cache, cookies, ficheiros do histórico do browser, correio electrónico enviado e recebido, ficheiros utilizados recentemente, ficheiros ActiveX e ficheiros de ponto de restauro do sistema. O QuickClean elimina estes itens sem afectar outras informações essenciais.

É possível utilizar qualquer uma das limpezas do QuickClean para eliminar ficheiros desnecessários do computador. A tabela seguinte descreve as limpezas do QuickClean:

Nome	Função
Limpeza da Reciclagem	Elimina ficheiros na Reciclagem.
Limpeza de Ficheiros Temporários	Elimina ficheiros armazenados em pastas temporárias.
Limpeza de Atalhos	Elimina atalhos quebrados e atalhos que não têm um programa associado.
Limpeza de Fragmentos de Ficheiros Perdidos	Elimina fragmentos de ficheiros perdidos no computador.
Limpeza do Registo	Elimina informações de registo do Windows® relativas a programas que já não existem no computador. O registo é uma base de dados na qual o Windows armazena a sua informação de configuração. O registo contém os perfis de cada utilizador do computador e informações acerca do hardware do sistema, dos programas instalados e de definições de propriedade. O Windows consulta continuamente estas informações durante o seu funcionamento.
Limpeza da Cache	Elimina ficheiros de cache que se vão acumulando quando navega em páginas Web. Esses ficheiros são normalmente armazenados como ficheiros temporários numa pasta cache. Uma pasta cache é uma área de armazenamento temporário no computador. Para aumentar a velocidade e a eficiência da navegação na Web, o browser pode obter uma página Web a partir da cache (em vez de recorrer a um servidor remoto) na próxima vez que a visualizar.

Nome	Função
Limpeza de Cookies	Elimina cookies. Esses ficheiros são normalmente armazenados como ficheiros temporários. Um cookie é um pequeno ficheiro que contém informações, incluindo normalmente um nome de utilizador e a data e hora actuais, armazenadas no computador de uma pessoa que navega na Web. Os cookies são utilizados principalmente por Web sites para identificar utilizadores que tenham efectuado previamente um registo ou visitado o site; no entanto, também podem constituir uma fonte de informação para hackers.
Limpeza do Histórico do Browser	Elimina o histórico do browser.
Limpeza de Correio Electrónico do Outlook Express e do Outlook (itens enviados e eliminados)	Elimina o correio electrónico enviado e eliminado do Outlook® e do Outlook Express.
Limpeza de Ficheiros Utilizados Recentemente	Elimina ficheiros utilizados recentemente que tenham sido criados com qualquer um dos seguintes programas: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
Limpeza de ActiveX	Elimina controlos ActiveX. O ActiveX é um componente de software utilizado por programas ou páginas Web para adicionar funcionalidades que actuam dissimuladas e aparecem como uma parte normal do programa ou da página Web. A maioria dos controlos ActiveX são inofensivos; no entanto, alguns podem capturar informações do computador.

Nome	Função
Limpeza de Pontos de Restauro do Sistema	Elimina pontos de restauro do sistema antigos (excepto o mais recente) do computador. Os pontos de restauro do sistema são criados pelo Windows para assinalar alterações efectuadas no computador a fim de que seja possível repor um estado anterior se ocorrerem problemas.

Neste capítulo

Limpar o computador

É possível utilizar qualquer uma das limpezas do QuickClean para eliminar ficheiros desnecessários do computador. Quando terminar, em **Resumo do QuickClean**, é possível ver a quantidade de espaço de disco recuperada após a limpeza, o número de ficheiros eliminados e a data e a hora em que foi executada a última operação do QuickClean no computador.

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
2. Em **McAfee QuickClean**, clique em **Iniciar**.
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**. Se seleccionar a Limpeza de Ficheiros Utilizados Recentemente, pode clicar em **Propriedades** para seleccionar ou limpar os ficheiros que foram criados recentemente com os programas da lista e, em seguida, clicar em **OK**.
   - Clique em **Restaurar Predefinições** para repor as limpezas predefinidas e, em seguida, clique em **Seguinte**.

4 Depois de executada a análise, clique em **Seguinte**.

5 Clique em **Seguinte** para confirmar a eliminação dos ficheiros.

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**, especifique o número de passagens, até 10, e clique em **Seguinte**. A destruição de ficheiros pode tornar-se um processo demorado se existir uma grande quantidade de informação a apagar.

7 Se existirem ficheiros ou itens bloqueados durante a limpeza, poderá ser-lhe solicitado que reinicie o computador. Clique em **OK** para fechar o pedido.

8 Clique em **Concluir**.

Nota: Os ficheiros eliminados com o Shredder não podem ser recuperados. Para informações acerca da destruição de ficheiros, consulte o McAfee Shredder.

CAPÍTULO 25

Desfragmentar o computador

O Desfragmentador de Disco dispõe os ficheiros e as pastas no computador de modo a que não fiquem dispersos (ou seja, fragmentados) quando são guardados no disco rígido do computador. Através da desfragmentação periódica do disco rígido, é possível assegurar que esses ficheiros e pastas fragmentados são consolidados para rápida obtenção posterior.

Desfragmentar o computador

É possível desfragmentar o computador para melhorar o acesso e a obtenção de ficheiros e pastas.

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
2. Em **Desfragmentador de Disco**, clique em **Analisar**.
3. Siga as instruções indicadas no ecrã.

Nota: Para obter mais informações acerca do Desfragmentador de Disco, consulte a Ajuda do Windows.

CAPÍTULO 26

Programar uma tarefa

O Programador de Tarefas automatiza a frequência com que o QuickClean ou o Desfragmentador de Disco são executados no computador. Por exemplo, é possível programar uma tarefa do QuickClean para esvaziar a Reciclagem todos os Domingos, às 21:00 ou uma tarefa do Desfragmentador de Disco para desfragmentar o disco rígido do computador no último dia de cada mês. É possível criar, modificar ou eliminar uma tarefa em qualquer altura. É necessário ter sessão iniciada no computador para que uma tarefa programada seja executada. Se uma tarefa não for executada por qualquer motivo, será reprogramada para cinco minutos depois de ter iniciado sessão novamente.

Programar uma tarefa do QuickClean

É possível programar uma tarefa do QuickClean para limpar automaticamente o computador utilizando uma ou mais limpezas. Quando terminar, em **Resumo do QuickClean**, é possível ver a data e a hora em que a tarefa será executada novamente.

1 Abra o painel Programador de Tarefas.

   Como?

   1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
   2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Seleccione a operação a programar**, clique em **McAfee QuickClean**.

3 Digite um nome para a tarefa na caixa **Nome da tarefa** e clique em **Criar.**

4 Efectue um dos seguintes procedimentos:

   - Clique em **Seguinte** para aceitar as limpezas da lista.
   - Seleccione ou desmarque as limpezas que considerar adequadas e, em seguida, clique em **Seguinte**. Se seleccionar a Limpeza de Ficheiros Utilizados Recentemente, pode clicar em **Propriedades** para seleccionar ou limpar os ficheiros que foram criados recentemente com os programas da lista e, em seguida, clicar em **OK**.
   - Clique em **Restaurar Predefinições** para repor as limpezas predefinidas e, em seguida, clique em **Seguinte**.

5 Efectue um dos seguintes procedimentos:

- Clique em **Programar** 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**, especifique o número de passagens, até 10, e clique em **Programar**.

6 Na caixa de diálogo **Programar**, seleccione a frequência de execução da tarefa e clique em **OK**.

7 Se tiver alterado as propriedades da Limpeza de Ficheiros Utilizados Recentemente, poderá ser-lhe solicitado que reinicie o computador. Clique em **OK** para fechar o pedido.

8 Clique em **Concluir**.

Nota: Os ficheiros eliminados com o Shredder não podem ser recuperados. Para informações acerca da destruição de ficheiros, consulte o McAfee Shredder.

Modificar uma tarefa do QuickClean

É possível modificar uma tarefa programada do QuickClean para alterar as limpezas utilizadas ou a frequência com que a mesma é executada no computador. Quando terminar, em **Resumo do QuickClean**, é possível ver a data e a hora em que a tarefa será executada novamente.

1 Abra o painel Programador de Tarefas.

Como?

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.

2. Na lista **Seleccione a operação a programar**, clique em **McAfee QuickClean**.
3. Seleccione a tarefa na lista **Seleccione uma tarefa existente** e clique em **Modificar**.
4. Efectue um dos seguintes procedimentos:
   - Clique em **Seguinte** para aceitar as limpezas seleccionadas para a tarefa.
   - Seleccione ou desmarque as limpezas que considerar adequadas e, em seguida, clique em **Seguinte**. Se seleccionar a Limpeza de Ficheiros Utilizados Recentemente, clique em **Propriedades** para seleccionar ou limpar os ficheiros que foram criados recentemente com os programas da lista e, em seguida, clique em **OK**.
   - Clique em **Restaurar Predefinições** para repor as limpezas predefinidas e, em seguida, clique em **Seguinte.**
5. Efectue um dos seguintes procedimentos:
   - Clique em **Programar** 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**, especifique o número de passagens, até 10, e clique em **Programar**.
6. Na caixa de diálogo **Programar**, seleccione a frequência de execução da tarefa e clique em **OK**.
7. Se tiver alterado as propriedades da Limpeza de Ficheiros Utilizados Recentemente, poderá ser-lhe solicitado que reinicie o computador. Clique em **OK** para fechar o pedido.
8. Clique em **Concluir**.

Nota: Os ficheiros eliminados com o Shredder não podem ser recuperados. Para informações acerca da destruição de ficheiros, consulte o McAfee Shredder.

Eliminar uma tarefa do QuickClean

É possível eliminar uma tarefa programada do QuickClean que já não pretende que seja executada automaticamente.

1 Abra o painel Programador de Tarefas.

   Como?

   1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
   2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Seleccione a operação a programar**, clique em **McAfee QuickClean**.

3 Seleccione a tarefa na lista **Seleccione uma tarefa existente**.

4 Clique em **Eliminar** e, em seguida, clique em **Sim** para confirmar a eliminação.

5 Clique em **Concluir**.

Programar uma tarefa do Desfragmentador de Disco

É possível programar uma tarefa do Desfragmentador de Disco para programar a frequência com que o disco rígido do computador é desfragmentado automaticamente. Quando terminar, em **Desfragmentador de Disco**, é possível ver a data e a hora em que a tarefa será executada novamente.

1 Abra o painel Programador de Tarefas.

   Como?

   1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
   2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Seleccione a operação a programar**, clique em **Desfragmentador de Disco**.

3 Digite um nome para a tarefa na caixa **Nome da tarefa** e clique em **Criar**.

4 Efectue um dos seguintes procedimentos:
   - Clique em **Programar** para aceitar a opção predefinida **Executar a defragmentação mesmo que exista pouco espaço livre em disco**.
   - Desmarque a opção **Executar a defragmentação mesmo que exista pouco espaço livre em disco** e clique em **Programar.**

5 Na caixa de diálogo **Programar**, seleccione a frequência de execução da tarefa e clique em **OK**.

6 Clique em **Concluir**.

Modificar uma tarefa do Desfragmentador de Disco

É possível modificar uma tarefa programada do Desfragmentador de Disco para alterar a frequência com que é executada automaticamente no computador. Quando terminar, em **Desfragmentador de Disco**, é possível ver a data e a hora em que a tarefa será executada novamente.

1 Abra o painel Programador de Tarefas.

   Como?

   1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
   2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Seleccione a operação a programar**, clique em **Desfragmentador de Disco**.

3 Seleccione a tarefa na lista **Seleccione uma tarefa existente** e clique em **Modificar**.

4 Efectue um dos seguintes procedimentos:
   - Clique em **Programar** para aceitar a opção predefinida **Executar a defragmentação mesmo que exista pouco espaço livre em disco**.
   - Desmarque a opção **Executar a defragmentação mesmo que exista pouco espaço livre em disco** e clique em **Programar.**

5 Na caixa de diálogo **Programar**, seleccione a frequência de execução da tarefa e clique em **OK**.

6 Clique em **Concluir**.

Eliminar uma tarefa do Desfragmentador de Disco

É possível eliminar uma tarefa programada do Desfragmentador de Disco que já não pretende que seja executada automaticamente.

1 Abra o painel Programador de Tarefas.

Como?

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Seleccione a operação a programar**, clique em **Desfragmentador de Disco**.

3 Seleccione a tarefa na lista **Seleccione uma tarefa existente**.

4 Clique em **Eliminar** e, em seguida, clique em **Sim** para confirmar a eliminação.

5 Clique em **Concluir**.

CAPÍTULO 27

McAfee Shredder

O McAfee Shredder elimina (ou destrói) itens do disco rígido do computador de forma permanente. Mesmo quando apaga ficheiros e pastas manualmente, esvazia a Reciclagem ou elimina a pasta Temporary Internet Files, ainda é possível recuperar estas informações utilizando ferramentas informáticas forenses. De igual modo, um ficheiro eliminado pode ser recuperado porque alguns programas criam temporariamente cópias ocultas de ficheiros abertos. O Shredder protege a sua privacidade eliminando os ficheiros indesejados de forma segura e permanente. É importante ter em conta que os ficheiros destruídos não podem ser restaurados.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do Shredder

Eliminar ficheiros e pastas permanentemente

Remove itens do disco rígido do computador de modo a que as respectivas informações associadas não possam ser recuperadas. Protege a sua privacidade eliminando, de forma permanente e segura, ficheiros e pastas, itens na Reciclagem e na pasta de Ficheiros Temporários da Internet e o conteúdo integral de discos de computador, tais como CDs regraváveis, unidades de disco externas e unidades de disquetes.

Destruir ficheiros, pastas e discos

O Shredder garante que as informações contidas nos ficheiros e pastas eliminados da Reciclagem e da pasta Temporary Internet Files não podem ser recuperadas, mesmo com ferramentas especiais. Com o Shredder, é possível especificar o número de vezes (até 10) que pretende que um item seja destruído. Um número maior de passagens de destruição aumenta o nível de eliminação segura dos ficheiros.

Destruir ficheiros e pastas

É possível destruir ficheiros e pastas do disco rígido do computador, incluindo itens da Reciclagem e da pasta Temporary Internet Files.

1 Abrir o **Shredder**.

   Como?

   1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Menu Avançado**.
   2. No painel esquerdo, clique em **Ferramentas**.
   3. Clique em **Shredder**.

2 No painel Destruir ficheiros e pastas, em **Quero**, clique em **Apagar ficheiros e pastas**.

3 Em **Nível de Destruição**, clique num dos níveis de destruição seguintes:

   - **Rápido**: Destrói os itens seleccionados uma vez.
   - **Abrangente**: Destrói os itens seleccionados 7 vezes.
   - **Personalizado**: Destrói os itens seleccionados até 10 vezes.

4 Clique em **Seguinte**.

5 Efectue um dos seguintes procedimentos:

- Na lista **Seleccione os ficheiros a destruir**, clique em **Conteúdo da Reciclagem** ou em **Ficheiros Temporários da Internet**.
- Clique em **Procurar**, procure o ficheiro que pretende destruir, seleccione-o e, em seguida, clique em **Abrir**.

6 Clique em **Seguinte**.

7 Clique em **Iniciar**.

8 Quanto o Shredder terminar, clique em **Concluído**.

Nota: Não trabalhe com nenhum ficheiro até o Shredder concluir esta tarefa.

Destruir todo o disco

É possível apagar todo o conteúdo de um disco de uma vez. Apenas podem ser destruídas unidades amovíveis, tais como unidades de disco externas, CDs graváveis e unidades de disquete.

1 Abrir o **Shredder**.

Como?

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Menu Avançado**.
2. No painel esquerdo, clique em **Ferramentas**.
3. Clique em **Shredder**.

2 No painel Destruir ficheiros e pastas, em **Quero**, clique em **Apagar um disco inteiro**.

3 Em **Nível de Destruição**, clique num dos níveis de destruição seguintes:

- **Rápido**: Destrói a unidade seleccionada uma vez.
- **Abrangente**: Destrói a unidade seleccionada 7 vezes.
- **Personalizado**: Destrói a unidade seleccionada até 10 vezes.

4 Clique em **Seguinte**.

5 Na lista **Seleccione o disco**, clique na unidade que pretende destruir.

6 Clique em **Seguinte** e, em seguida, clique em **Sim** para confirmar.

7 Clique em **Iniciar**.

8 Quanto o Shredder terminar, clique em **Concluído**.

Nota: Não trabalhe com nenhum ficheiro até que o McAfee Shredder tenha concluído esta tarefa.

CAPÍTULO 28

McAfee Network Manager

O Gestor de Rede apresenta uma vista gráfica dos computadores e outros dispositivos que compõem a sua rede doméstica. Pode utilizar o Gestor de Rede para gerir, de forma remota, o estado de protecção de cada computador gerido na sua rede e corrigir remotamente vulnerabilidades de segurança comunicadas nesses computadores. Se tiver instalado o McAfee Total Protection, o Gestor de Rede também poderá monitorizar a rede para detectar Intrusos (computadores ou dispositivos que não reconhece nem confia) que tentem estabelecer ligação à mesma.

Antes de utilizar o Gestor de Rede, pode familiarizar-se com algumas das funcionalidades. A ajuda do Gestor de Rede inclui detalhes sobre configuração e utilização dessas funcionalidades.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do Network Manager

Mapa de rede gráfico	Visualize uma descrição geral gráfica do estado de protecção dos computadores e dispositivos que compõem a sua rede doméstica. Quando efectua alterações à rede (por exemplo, adiciona um computador), o mapa de rede reconhece essas alterações. Pode actualizar o mapa de rede, mudar o nome da rede e mostrar ou ocultar componentes do mapa de rede, para personalizar a visualização. Pode também ver os detalhes de qualquer um dos dispositivos apresentados no mapa de rede.
Gestão remota	Efectue a gestão do estado de protecção dos computadores que compõem a sua rede doméstica. Pode convidar um computador para aderir à rede gerida, monitorizar o estado de protecção do computador gerido e corrigir vulnerabilidades de segurança conhecidas para um computador remoto na rede.
Monitorização da rede	Se estiver disponível, permita que o Gestor de Rede monitorize as redes e o notifique quando Amigos ou Intrusos estabelecerem ligação. A monitorização da rede só está disponível se tiver adquirido o McAfee Total Protection.

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 que tem o SecurityCenter instalado
	Representa um computador não gerido e offline
	Representa um computador online que não tem o SecurityCenter instalado ou um dispositivo de rede desconhecido
	Representa um computador offline que não tem o SecurityCenter instalado ou um dispositivo de rede desconhecido offline
	Significa que o item correspondente está protegido e ligado
	Significa que o item correspondente pode requerer a sua atenção
	Significa que o item correspondente requer a sua atenção imediata
	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 29

Configurar uma rede gerida

Para configurar uma rede gerida, considere a rede de confiança (caso ainda não o tenha feito) e adicione membros (computadores) à rede. Antes de um computador poder ser gerido remotamente ou de lhe ser concedida permissão para gerir, de forma remota, outros computadores na rede, deve tornar-se um membro de confiança da rede. A condição de membro da rede é concedida a novos computadores pelos membros de rede existentes (computadores) com permissões administrativas.

Pode ver os detalhes associados a qualquer um dos itens apresentados no mapa de rede, mesmo depois de efectuar alterações à rede (por exemplo, adicionar um computador).

Neste capítulo

Utilizar o mapa de rede

Quando um computador é ligado à rede, o Gestor de Rede analisa a rede para determinar se existem membros geridos ou não geridos, quais são os atributos do router e o estado da Internet. Se não forem encontrados membros, o Gestor de Rede presume que o computador actualmente ligado é o primeiro computador na rede e torna-o um membro gerido com permissões administrativas. Por predefinição, o nome da rede inclui o nome do primeiro computador que é ligado à rede e que possui o SecurityCenter 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 mapa de rede, mudar o nome da rede, bem como mostrar ou ocultar itens do mapa de rede para personalizar a vista. Pode, também, ver os detalhes associados aos itens apresentados no mapa de rede.

Aceder ao mapa de rede

O mapa de rede mostra uma representação gráfica dos computadores e dispositivos que compõem a sua rede doméstica.

- Nos Menus Básico ou Avançado, clique em **Gerir Rede**.

Nota: Caso ainda não tenha considerado a rede de confiança (utilizando o McAfee Personal Firewall), ser-lhe-á solicitado que o faça quando aceder ao mapa de rede pela primeira vez.

Actualizar o mapa de rede

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

1. Nos Menus Básico ou Avançado, clique em **Gerir Rede**.
2. Clique em **Actualizar mapa de rede** em **Quero**.

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

Mudar o nome da rede

Por predefinição, o nome da rede inclui o nome do primeiro computador que é ligado à rede e possui o SecurityCenter instalado. Se preferir utilizar um nome diferente, pode alterá-lo.

1 Nos Menus Básico ou Avançado, clique em **Gerir Rede**.

2 Clique em **Mudar o nome da rede** em **Quero**.

3 Introduza o nome da rede na caixa **Nome da rede**.

4 Clique em **OK**.

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

Mostrar ou ocultar um item no mapa de rede

Por predefinição, todos os computadores e dispositivos na sua rede doméstica são apresentados no mapa 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 ocultados

Para...	No menu Básico ou Avançado, clique em Gerir Rede e efectue o seguinte...
Ocultar um item no mapa de rede	Clique num item no mapa 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 mapa de rede	Em **Quero**, clique em **Mostrar itens ocultos**.

Ver os detalhes de um item

Pode ver informações detalhadas sobre qualquer item na rede se o seleccionar no mapa de rede. Estas informações incluem o nome do item, o respectivo estado de protecção e outras informações necessárias para gerir o item.

1 Clique no ícone de um item no mapa 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 administrativas. 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, enviar ficheiros ou partilhar impressoras).

Nota: Depois de aderir, se tiver outros programas de rede da McAfee instalados (por exemplo, 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. Também pode determinar se pretende que os outros computadores na rede efectuem a gestão destas definições de segurança do computador.

1. Na caixa de diálogo Rede Gerida, certifique-se de que a caixa de verificação **Permitir que todos os computadores desta rede giram definições de segurança** está seleccionada.
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 **OK**.

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 risco; por conseguinte, clique em **Cancelar** na caixa de diálogo Rede Gerida.

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 administrativas na rede podem convidar outros computadores para aderir. Ao enviar o convite, pode também especificar o nível de permissão que pretende atribuir ao computador aderente.

1. Clique no ícone de um computador não gerido no mapa de rede.
2. Clique em **Gerir este computador** em **Quero**.
3. Na caixa de diálogo Convidar um computador a aderir à rede gerida, clique numa das seguintes opções:
   - Clique em **Permitir acesso de convidado a programas da rede gerida** para permitir que o computador aceda à rede (pode utilizar esta opção para utilizadores temporários em casa).
   - Clique em **Permitir acesso total a programas da rede gerida** para permitir que o computador aceda à rede.
   - Clique em **Permitir acesso administrativo a programas da rede gerida** para permitir que o computador aceda à rede com permissões administrativas. Permite também ao computador conceder acesso a outros computadores que pretendam aderir à rede gerida.

4 Clique em **OK**.
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 a 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 do 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 confiou noutros computadores na rede inadvertidamente, pode parar de confiar neles.

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

Nota: A ligação **Parar de confiar em computadores nesta rede** não está disponível se possuir direitos administrativos e existirem outros computadores geridos na rede.

CAPÍTULO 30

Gerir a rede de forma remota

Depois de configurar a rede gerida, pode gerir remotamente os computadores e dispositivos que compõem a sua rede. Pode gerir o estado e os níveis de permissão dos computadores e dispositivos e corrigir a maioria das vulnerabilidades de segurança de forma remota.

Neste capítulo

Gerir estado e permissões

Uma rede gerida possui membros geridos e membros não geridos. Os membros geridos permitem que outros computadores da rede efectuem a gestão do seu estado de protecção McAfee, o que não acontece com os membros não geridos. Os membros não geridos são normalmente computadores convidados que pretendem aceder a outras funções de rede (por exemplo, enviar ficheiros ou partilhar impressoras). Um computador não gerido pode ser convidado a tornar-se um computador gerido em qualquer altura por outro computador gerido com permissões administrativas na rede. Do mesmo modo, um computador gerido com permissões administrativas pode tornar outro computador gerido não gerido a qualquer altura.

Os computadores geridos têm permissões administrativas, totais ou de convidado. As permissões administrativas permitem ao computador gerido administrar o estado de protecção de todos os outros computadores geridos na rede e permitir que outros computadores se tornem membros da 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 também pode ter dispositivos (por exemplo, routers), pode utilizar o Gestor de Rede para os gerir. Pode também configurar e modificar as propriedades de visualização de um dispositivo no mapa de rede.

Gerir o estado de protecção de um computador

Se o estado de protecção de um computador não estiver a ser gerido na rede (o computador não é um membro ou é um membro não gerido), pode efectuar um pedido para o gerir.

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

Parar de gerir o estado de protecção de um computador

Pode parar de gerir o estado de protecção de um computador gerido na rede; no entanto, o computador torna-se não gerido e não pode gerir o seu estado de protecção de forma remota.

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

Modificar as permissões de um computador gerido

Pode alterar as permissões de um computador gerido em qualquer altura. Isto permite-lhe modificar os computadores que podem gerir o estado de protecção de outros computadores na rede.

1. Clique no ícone de um computador gerido no mapa 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 gerir 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 mapa de rede.

1. Clique no ícone de um dispositivo no mapa 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, tem de utilizar o McAfee 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.

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 em **Router Padrão** se não for um router sem fios, ou em **Router Sem Fios** se for o caso.
5. Clique em **OK**.

Corrigir vulnerabilidades de segurança

Os computadores geridos com permissões administrativas podem gerir o estado de protecção McAfee de outros computadores geridos na rede e corrigir remotamente as vulnerabilidades de segurança comunicadas. Por exemplo, se o estado de protecção McAfee de um computador gerido indicar que o VirusScan está desactivado, outro computador gerido com permissões administrativas pode activar o VirusScan remotamente.

Quando corrige vulnerabilidades de segurança remotamente, o Gestor de Rede repara a maioria dos problemas comunicados. No entanto, algumas vulnerabilidades de segurança podem requerer intervenção manual no computador local. Neste caso, o Gestor de Rede corrige os problemas que podem ser reparados remotamente e, em seguida, pede-lhe para corrigir os problemas restantes, iniciando sessão no SecurityCenter no computador vulnerável e seguindo as recomendações fornecidas. Nalguns casos, a resolução sugerida consiste em instalar a versão mais recente do SecurityCenter no(s) computador(es) remoto(s) da sua rede.

Corrigir vulnerabilidades de segurança

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

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 rede não utilizarem uma versão recente do SecurityCenter, o seu estado de protecção não pode ser gerido remotamente. Se pretender gerir esses computadores remotamente, deve aceder a cada computador e instalar uma versão recente do SecurityCenter.

1. Certifique-se de que segue estas instruções no computador que pretende gerir remotamente.
2. Tenha as informações de início de sessão da McAfee à mão; estas consistem no endereço de correio electrónico e palavra-passe utilizados ao activar o software da McAfee pela primeira vez.
3. Num browser, aceda ao Web site da McAfee, inicie sessão e clique em **A Minha Conta**.
4. Localize o produto que pretende instalar, clique no respectivo botão **Transferir** e, em seguida, siga as instruções apresentadas no ecrã.

Sugestão: Também pode obter informações sobre como instalar o software de segurança McAfee em computadores remotos abrindo o mapa de rede e clicando em **Proteger os meus computadores** em **Quero**.

CAPÍTULO 31

Monitorizar redes

Se tiver o McAfee Total Protection instalado, o Gestor de Rede também monitorizará as redes para detectar intrusos. Sempre que um computador ou dispositivo desconhecido estabelecer ligação à rede, será notificado sobre esta situação para que possa decidir se esse computador ou dispositivo é um Amigo ou um Intruso. Um Amigo é um computador ou dispositivo que reconhece e no qual confia; um Intruso é um computador ou dispositivo que não reconhece e no qual não confia. Se marcar um computador ou dispositivo como Amigo, poderá decidir se pretende ser notificado sempre que esse Amigo estabelecer ligação à rede. Se marcar um computador ou dispositivo como Intruso, será alertado automaticamente sempre que o mesmo tentar estabelecer ligação à rede.

A primeira vez que estabelecer ligação a uma rede depois de instalar ou actualizar esta versão do Total Protection, cada computador ou dispositivo será marcado automaticamente como Amigo e não será notificado quando estes estabelecerem ligação à rede no futuro. Após três dias, começará a ser notificado sobre cada computador ou dispositivo desconhecido que estabelecer ligação para que possa marcá-los manualmente.

Nota: A monitorização da rede é uma funcionalidade do Gestor de Rede apenas disponível com o McAfee Total Protection. Para mais informações sobre o Total Protection, visite o nosso Web site.

Neste capítulo

Parar monitorização de redes

Se desactivar a monitorização da rede, deixará de ser alertado quando intrusos estabelecerem ligação à sua rede doméstica ou a qualquer outra rede à qual esteja ligado.

1 Abra o painel Configuração de Internet e Rede.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Internet e Rede**.
3. Na secção Informações sobre Internet e Rede, clique em **Configurar**.

2 Em **Monitorização da rede**, clique em **Desligado**.

Reactivar notificações de monitorização de rede

Apesar de poder desactivar as notificações de monitorização de rede, não é recomendável que o faça. Se o fizer, deixará de ser notificado quando computadores desconhecidos ou Intrusos estabelecerem ligação à rede. Se desactivar inadvertidamente estas notificações (por exemplo, se seleccionar a caixa de verificação **Não mostrar este alerta novamente** num alerta), poderá reactivá-las a qualquer altura.

1 Abra o painel Opções de Alerta.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Configuração do SecurityCenter, clique em **Alertas Informativos**.

3 No painel Alertas Informativos, certifique-se de que as seguintes caixas de verificação estão desmarcadas:

- **Não mostrar alertas quando novos computadores ou dispositivos estabelecerem ligação à rede**
- **Não mostrar alertas quando Intrusos estabelecerem ligação à rede**
- **Não mostrar alertas para Amigos sobre os quais pretendo normalmente ser notificado**

- **Não me lembrar quando forem detectados computadores ou dispositivos desconhecidos**
- **Não me alertar quando o McAfee terminar a detecção de novos Amigos**

4 Clique em **OK**.

Marcar como Intruso

Marque um computador ou dispositivo na rede como Intruso se não o reconhecer nem confiar nele. Será alertado automaticamente sempre que o mesmo estabelecer ligação à rede.

1 Nos Menus Básico ou Avançado, clique em **Gerir Rede**.
2 No mapa de rede, clique num item.
3 Em **Quero**, clique em **Marcar como Amigo ou Intruso**.
4 Na caixa de diálogo, clique em **Intruso**.

Marcar como Amigo

Marque um computador ou dispositivo na rede como Amigo apenas se o reconhecer e confiar nele. Quando marca um computador ou dispositivo como Amigo, também poderá decidir se pretende ser notificado sempre que este estabelecer ligação à rede.

1 Nos Menus Básico ou Avançado, clique em **Gerir Rede**.
2 No mapa de rede, clique num item.
3 Em **Quero**, clique em **Marcar como Amigo ou Intruso**.
4 Na caixa de diálogo, clique em **Amigo**.
5 Para ser notificado sempre que este Amigo estabelecer ligação à rede, seleccione a caixa de verificação **Notificar-me quando este computador ou dispositivo estabelecer ligação à rede**.

Interromper detecção de novos Amigos

Durante os três primeiros dias depois de estabelecer ligação a uma rede com esta versão do Total Protection instalada, cada computador ou dispositivo sobre o qual não pretende ser notificado será automaticamente marcado como Amigo. Pode parar esta marcação automática a qualquer altura durante esses três dias, mas não poderá reiniciá-la mais tarde.

1 Nos Menus Básico ou Avançado, clique em **Gerir Rede**.
2 Em **Quero**, clique em **Interromper detecção de novos Amigos**.

CAPÍTULO 32

McAfee EasyNetwork

O EasyNetwork permite partilhar ficheiros em segurança, simplificar as transferências de ficheiros e partilhar impressoras entre os computadores da sua rede doméstica. No entanto, os computadores da rede devem ter o EasyNetwork instalado para aceder às suas funcionalidades.

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

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do EasyNetwork

O EasyNetwork oferece as seguintes funcionalidades.

Partilha de ficheiros

O EasyNetwork facilita a partilha de ficheiros com outros computadores da rede. Ao partilhar ficheiros, está a conceder aos outros computadores acesso apenas de leitura aos ficheiros. Apenas os computadores que possuem acesso administrativo ou total à rede gerida (membros) podem partilhar ou aceder a ficheiros partilhados por outros membros.

Transferência de ficheiros

Pode enviar ficheiros a outros computadores que possuem acesso administrativo ou total à rede gerida (membros). 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 os outros computadores da rede lhe enviam.

Partilha de impressoras automática

Depois de aderir a uma rede gerida, pode partilhar todas as impressoras locais ligadas ao seu computador com outros membros, 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 33

Configurar o EasyNetwork

Para poder utilizar o EasyNetwork, deve iniciar o programa e aderir a uma rede gerida. Depois de efectuar a adesão, pode partilhar, procurar e enviar ficheiros para outros computadores na rede. Também pode partilhar impressoras. Se decidir abandonar a rede, pode fazê-lo em qualquer altura.

Neste capítulo

Abrir o EasyNetwork

Pode abrir o EasyNetwork a partir do menu Iniciar do Windows ou clicando no respectivo ícone do ambiente de trabalho.

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

Sugestão: Também pode abrir o EasyNetwork fazendo duplo clique no ícone do McAfee EasyNetwork no ambiente de trabalho.

Aderir a uma rede gerida

Se nenhum dos computadores da rede a que está ligado possuir o SecurityCenter, torna-se 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, envia um pedido de adesão aos outros computadores da 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 adere à rede; por exemplo, acesso de convidado (apenas 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 (promover ou despromover computadores); os computadores com acesso total não podem executar estas tarefas administrativas.

Nota: Depois de aderir, se tiver outros programas de rede da McAfee instalados (por exemplo, o Network Manager), o computador é igualmente reconhecido como um computador gerido nesses programas. O nível de permissão atribuído a um computador no EasyNetwork 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. Se o computador aceitar 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. São concedidas automaticamente permissões administrativas ao primeiro computador da rede.

1. Na janela Ficheiros Partilhados, clique em **Aderir a esta rede**. 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 **OK**; caso contrário, clique em **Cancelar**.

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

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 risco; por conseguinte, clique em **Cancelar** 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 que responder ao pedido torna-se o concessor. Como concessor, esse computador é responsável por determinar o tipo de acesso a conceder ao computador: convidado, total ou administrativo.

1 No alerta, clique no nível de acesso adequado.

2 Na caixa de diálogo Convidar um computador a aderir à rede gerida, clique numa das seguintes opções:

- Clique em **Permitir acesso de convidado a programas da rede gerida** para permitir que o computador aceda à rede (pode utilizar esta opção para utilizadores temporários em casa).
- Clique em **Permitir acesso total a programas da rede gerida** para permitir que o computador aceda à rede.
- Clique em **Permitir acesso administrativo a programas da rede gerida** para permitir que o computador aceda à rede com permissões administrativas. Permite também ao computador conceder acesso a outros computadores que pretendam aderir à rede gerida.

3 Clique em **OK**.

4 Confirme se o computador apresenta as mesmas cartas de jogar apresentadas na caixa de diálogo de confirmação de segurança e, em seguida, clique em **Conceder Acesso**.

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 risco; por conseguinte, clique em **Rejeitar Acesso** 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; 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.

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, pode abandonar a rede. Depois de abandonar a rede gerida, pode voltar a aderir em qualquer altura; no entanto, deverá ser-lhe concedida permissão novamente. Para obter mais informações acerca da adesão, consulte a secção Aderir a uma rede gerida (página 162).

Abandonar uma rede gerida

Pode abandonar uma rede gerida à qual anteriormente aderiu.

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

CAPÍTULO 34

Partilhar e enviar ficheiros

O EasyNetwork facilita a partilha e o envio de ficheiros para outros computadores da rede. Ao partilhar ficheiros, concede aos outros computadores acesso apenas de leitura aos ficheiros. Apenas os computadores que são membros da rede gerida (acesso total ou administrativo) podem partilhar ficheiros ou aceder a ficheiros partilhados por outros membros.

Nota: Se partilhar um número elevado de ficheiros, os recursos do seu computador podem ser afectados.

Neste capítulo

Partilhar ficheiros

Apenas os computadores que são membros da rede gerida (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 removidos da janela Ficheiros Partilhados. Pode deixar de partilhar um ficheiro em qualquer altura.

Para aceder a um ficheiro partilhado, abra o ficheiro directamente a partir do EasyNetwork ou copie-o para o computador e abra-o localmente. Se a sua lista de ficheiros partilhados for extensa e for difícil ver onde o ficheiro se encontra, pode procurá-lo.

Nota: Os ficheiros partilhados com o EasyNetwork não podem ser acedidos a partir de outros computadores através do Explorador do Windows, uma vez que a partilha de ficheiros no EasyNetwork deve ser efectuada com base em ligações seguras.

Partilhar um ficheiro

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

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: Também pode 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 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 não podem aceder-lhe.

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 **OK**.

Copiar um ficheiro partilhado

Pode copiar um ficheiro partilhado para manter uma cópia quando este deixar de ser partilhado. Pode copiar um ficheiro partilhado de qualquer computador da rede gerida.

- 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: Também pode copiar um ficheiro partilhado, seleccionando-o 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 introduz os seus critérios de procura, o EasyNetwork apresenta os resultados correspondentes na janela Ficheiros Partilhados.

1. Na janela Ficheiros Partilhados, clique em **Procurar**.
2. Clique na opção adequada (página 167) na lista **Contém**.
3. Introduza o nome parcial ou completo do ficheiro ou do caminho na lista **Nome do Caminho ou Ficheiro**.
4. Clique no tipo de ficheiro (página 167) adequado na lista **Tipo**.
5. Na listas **De** e **Até**, seleccione as datas correspondentes ao intervalo de datas em que o ficheiro foi criado.

Critérios de procura

A tabela seguinte descreve os critérios de procura que pode especificar ao procurar ficheiros partilhados.

Nome do ficheiro ou caminho

Contém	Descrição
Contém todas as palavras	Procura um nome de ficheiro ou caminho que contenha todas as palavras especificadas na lista **Nome do Caminho ou Ficheiro**, por qualquer ordem.
Contém qualquer das palavras	Procura um nome de ficheiro ou caminho que contenha qualquer uma das palavras especificadas na lista **Nome do Caminho ou Ficheiro**.
Contém a cadeia exacta	Procura um nome de ficheiro ou caminho que contenha a frase exacta que especificou na lista **Nome do Caminho ou Ficheiro**.

Tipo de ficheiro

Tipo	Descrição
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 áudio partilhados.
Comprimidos	Procura todos os ficheiros comprimidos (por exemplo, ficheiros .zip).

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 os ficheiros que os outros computadores da rede lhe enviam. Se tiver o EasyNetwork aberto quando receber um ficheiro, o ficheiro é apresentado na pasta A receber; caso contrário, aparece uma mensagem na área de notificação situada na parte mais à direita da barra de tarefas. Se não quiser receber mensagens de aviso (por exemplo, estão a interromper o que está a fazer), pode desactivar esta funcionalidade. Se já existir um ficheiro com o mesmo nome na pasta A receber, é acrescentado um sufixo numérico ao nome do novo ficheiro. Os ficheiros permanecem na pasta A receber até que os aceite (os copie para o seu computador).

Enviar um ficheiro para outro computador

Pode enviar um ficheiro 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 169).

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: Para enviar vários ficheiros para um computador, prima 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 o EasyNetwork não estiver em execução quando for enviado um ficheiro para o seu computador, recebe uma mensagem de notificação na área de notificação na área mais à direita da barra de tarefas. Clique na mensagem de aviso para abrir o EasyNetwork e aceder ao ficheiro.

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

Sugestão: Também pode 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 uma mensagem de notificação quando outro computador da rede gerida lhe envia um ficheiro. Se o EasyNetwork não estiver em execução, a mensagem de notificação é apresentada na área de notificação mais à direita na barra de tarefas.

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 35

Partilhar impressoras

Depois de aderir a uma rede gerida, o EasyNetwork partilha as impressoras locais ligadas ao seu computador e utiliza o nome da impressora como nome de impressora partilhada. O EasyNetwork também detecta as 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 na rede. Pode deixar de partilhar uma impressora em qualquer altura.

Neste capítulo

Trabalhar com impressoras partilhadas

O EasyNetwork detecta as impressoras partilhadas por todos os outros computadores da rede. Se o EasyNetwork detectar uma impressora remota que não esteja ligada ao seu computador, a hiperligação **Impressoras de rede disponíveis** é apresentada na janela Ficheiros Partilhados quando abrir o EasyNetwork pela primeira vez. Depois, poderá instalar impressoras disponíveis ou desinstalar impressoras que já estejam ligadas ao seu computador. Também pode actualizar a lista de impressoras para garantir que está a ver informações actualizadas.

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 do Windows.

Interromper a partilha de uma impressora

Se interromper a partilha de uma impressora, os membros não podem utilizá-la.

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

Se é membro de uma rede gerida, pode aceder às impressoras partilhadas; deve instalar o controlador de impressora utilizado pela impressora. Se o proprietário da impressora interromper a partilha, não poderá utilizá-la.

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**.

Referência

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

Glossário

8

802.11

Um conjunto de normas para transmissão de dados através de uma rede sem fios. A norma 802.11 é normalmente conhecida como Wi-Fi.

802.11a

Uma extensão da norma 802.11 que transmite dados até 54 Mbps na banda de frequências dos 5 GHz. Embora a velocidade de transmissão seja superior à da norma 802.11b, a distância abrangida é muito menor.

802.11b

Uma extensão da norma 802.11 que transmite dados até 11 Mbps na banda de frequências dos 2,4 GHz. Embora a velocidade de transmissão seja inferior à da norma 802.11a, a distância abrangida é maior.

802.1x

Uma norma para autenticação em redes com fios e sem fios. A norma 802.1x é normalmente utilizada em redes sem fios 802.11. Ver também autenticação (página 175).

A

adaptador de rede sem fios PCI

Peripheral Component Interconnect. Um adaptador sem fios que é ligado a uma ranhura de expansão existente no interior do computador.

adaptador de rede sem fios USB

Um adaptador de rede sem fios ligado a uma porta USB do computador.

adaptador sem fios

Um dispositivo que proporciona capacidades sem fios a um computador ou PDA. É ligado através de uma porta USB, ranhura PC Card (CardBus), ranhura de cartão de memória ou internamente no barramento PCI.

análise a pedido

Uma análise agendada de ficheiros, aplicações ou dispositivos de rede seleccionados para localizar uma ameaça, uma vulnerabilidade ou outro código potencialmente indesejado. Pode ser efectuada de imediato, numa hora programada ou a intervalos agendados regularmente. Comparar com análise no acesso. Ver também vulnerabilidade.

análise em tempo real

O processo de verificar a existência de vírus e outras actividades em ficheiros e pastas quando estes são acedidos pelo utilizador ou pelo computador.

arquivo

Para criar uma cópia dos seus ficheiros importantes em CD, DVD, unidade USB, unidade de disco externa ou unidade de rede. Comparar com cópia de segurança (página 176).

atalho

Um ficheiro que contém apenas a localização de outro ficheiro no computador.

ataque de dicionário

Um tipo de ataque de força bruta que utiliza palavras comuns para tentar descobrir uma palavra-passe.

ataque de força bruta

Um método de hacking utilizado para localizar palavras-passe ou chaves de encriptação experimentando todas as combinações possíveis até abrir a encriptação.

ataque de intermediário

Um método para interceptar e possivelmente modificar mensagens trocadas entre dois utilizadores sem que estes saibam que a ligação de comunicação foi violada.

ataque denial-of-service (DOS)

Um tipo de ataque contra um computador, servidor ou rede que torna lento ou interrompe o tráfego numa rede. Ocorre quando uma rede é inundada com um número demasiado elevado de pedidos adicionais que provocam a lentidão ou a paragem total do tráfego normal. Um ataque denial-of-service sobrecarrega o alvo com falsos pedidos de ligação de modo a que ignore os pedidos legítimos.

autenticação

O processo de verificação da identidade digital do remetente de uma comunicação electrónica.

B

browser

Um programa utilizado para ver páginas Web na Internet. Os Web browsers mais conhecidos incluem o Microsoft Internet Explorer e o Mozilla Firefox.

C

cache

Uma área de armazenamento temporário no computador para dados acedidos com frequência ou recentemente. Por exemplo, para aumentar a velocidade e a eficiência da navegação na Web, o browser pode obter uma página Web da cache, em vez de um servidor remoto, na próxima vez que a visualizar.

capacidade da memória intermédia excedida

Uma condição que ocorre num sistema operativo ou numa aplicação quando programas ou processos suspeitos tentam armazenar numa memória intermédia (área de armazenamento temporário) mais dados do que esta pode suportar. A ocorrência da capacidade de memória intermédia excedida danifica a memória ou substitui dados em memórias intermédias adjacentes.

chave

Uma série de letras e números utilizada por dois dispositivos para autenticação da respectiva comunicação. Ambos os dispositivos têm de possuir a chave. Ver também WEP (página 186), WPA (página 187), WPA2 (página 187), WPA2-PSK (página 187), WPA-PSK (página 187).

cliente

Um programa que é executado num computador pessoal ou numa estação de trabalho e depende de um servidor para executar algumas operações. Por exemplo, um cliente de correio electrónico é uma aplicação que permite enviar e receber correio electrónico.

cliente de correio electrónico

Um programa executado no computador para enviar e receber correio electrónico (por exemplo, o Microsoft Outlook).

cofre de palavras-passe

Uma área de armazenamento segura para palavras-passe pessoais. Permite guardar palavras-passe com a certeza de que nenhum outro utilizador (nem mesmo um administrador) terá acesso às mesmas.

compressão

Um processo que comprime ficheiros para um formato que minimiza o espaço necessário para armazenamento ou transmissão.

conta de correio electrónico padrão

Ver POP3 (página 181).

controlo ActiveX

Um componente de software utilizado por programas ou páginas Web para adicionar funcionalidades que aparecem como uma parte normal do programa ou da página Web. A maioria dos controlos ActiveX são inofensivos; no entanto, alguns podem capturar informações do computador.

cookie

Um pequeno ficheiro de texto utilizado por muitos Web sites para armazenar informações sobre as páginas visitadas e que é armazenado no computador de uma pessoa que navega na Web. Pode conter informações de início de sessão ou de registo, informações de carrinhos de compras ou preferências de utilizadores. Os cookies são utilizados principalmente por Web sites para identificar utilizadores que tenham efectuado previamente um registo ou visitado o Web site; no entanto, também podem constituir uma fonte de informação para hackers.

cópia de segurança

Para criar uma cópia de ficheiros importantes, normalmente num servidor online seguro. Comparar com arquivo (página 174).

correio electrónico

Correio electrónico. Mensagens enviadas e recebidas electronicamente através de uma rede de computadores. Ver também webmail (página 186).

D

DAT

Ficheiros de definições de detecção, também denominados ficheiros de assinaturas, que contêm as definições que identificam, detectam e reparam vírus, cavalos de Tróia, spyware, adware e outros programas potencialmente indesejados (PUP).

DNS

Sistema de Nomes de Domínio. Um sistema de base de dados que traduz um endereço IP, por exemplo, 11.2.3.44, num nome de domínio, por exemplo, www.mcafee.com.

domínio

Uma sub-rede local ou um descritor de sites na Internet. Numa rede de área local (LAN), um domínio é uma sub-rede constituída por computadores clientes e servidores controlados por uma base de dados de segurança. Na Internet, o domínio faz parte de qualquer endereço Web. Por exemplo, em www.mcafee.com, mcafee é o domínio.

E

encriptação

Um método de encriptar informação para impedir o acesso de terceiros não autorizados. Na codificação dos dados utiliza-se uma "chave" e algoritmos matemáticos. As informações encriptadas não podem ser desencriptadas sem a chave adequada. Por vezes, os vírus utilizam encriptação para tentar escapar a detecções.

endereço IP

Endereço de protocolo Internet. Um endereço utilizado para identificar um computador ou um dispositivo numa rede TCP/IP. O formato de um endereço IP é um endereço numérico de 32 bits escrito como quatro números separados por pontos. Cada número deve estar compreendido entre 0 e 255 (por exemplo, 192.168.1.100).

endereço MAC

Endereço de Controlo de Acesso a Suportes de Dados. Um número de série exclusivo atribuído a um dispositivo físico (NIC, placa de rede) que acede à rede.

erros da Web

Pequenos ficheiros de gráficos que se introduzem em páginas HTML e permitem que uma fonte não autorizada defina cookies no seu computador. Estes cookies podem depois transmitir informações à fonte não autorizada. Os erros da Web são também conhecidos como “sinalizadores Web”, “pixel tags”, “GIFs limpos” ou “GIFs invisíveis”.

ESS

Extended service set. Duas ou mais redes que constituem uma única sub-rede.

evento

Num programa ou sistema informático, um incidente ou ocorrência passível de detecção por software de segurança, de acordo com critérios predefinidos. Normalmente, um evento desencadeia uma acção, por exemplo, o envio de uma notificação ou a adição de uma entrada num registo de eventos.

F

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. É também utilizada frequentemente para falsificar os cabeçalhos de correio publicitário não solicitado, para impedir que estes sejam correctamente rastreados.

ficheiro temporário

Um ficheiro, criado na memória ou no disco pelo sistema operativo ou outro programa, para ser utilizado durante uma sessão e, em seguida, eliminado.

firewall

Um sistema (de hardware, software ou ambos) concebido para impedir o acesso não autorizado a uma rede privada. 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, que as examina e bloqueia as que não correspondem aos critérios de segurança especificados.

fragmentos de ficheiros

Vestígios de ficheiros dispersos num disco. A fragmentação de ficheiros ocorre à medida que os ficheiros são adicionados ou eliminados e pode diminuir o desempenho do computador.

G

gateway integrado

Um dispositivo que combina as funções de um ponto de acesso (AP), de um router e de uma firewall. Alguns dispositivos também podem incluir melhoramentos de segurança e funcionalidades de bridging.

grupo de classificação de conteúdos

Nas Limitações de Acesso, um grupo etário a que um utilizador pertence. O conteúdo 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.

H

hotspot

Uma área geográfica abrangida por um ponto de acesso (AP) Wi-Fi (802.11). Os utilizadores que entram num hotspot através de um portátil sem fios podem estabelecer ligação à Internet, desde que o hotspot esteja a sinalizar (a divulgar a sua presença) e não seja exigida autenticação. Os hotspots encontram-se frequentemente localizados em áreas muito movimentadas, tais como aeroportos.

I

intranet

Uma rede de computadores privada, normalmente dentro de uma organização, que apenas pode ser acedida por utilizadores autorizados.

L

LAN

Rede de Área Local. Uma rede de computadores que abrange uma área relativamente pequena (por exemplo, um edifício). Os computadores existentes numa LAN podem comunicar entre si e partilhar recursos, tais como impressoras e ficheiros.

largura de banda

A quantidade de dados (débito) que pode ser transmitida num período de tempo fixo.

launchpad

Um componente da interface U3 que actua como um ponto de arranque para o início e a gestão de programas U3 USB.

lista de confiança

Uma lista de itens nos quais confia e que não estão a ser detectados. Se tiver confiado num item inadvertidamente (por exemplo, um programa potencialmente indesejado ou uma alteração do registo) ou pretender que o item seja detectado novamente, deve removê-lo desta lista.

lista de sites bloqueados

No Anti-Spam, uma lista de endereços de correio electrónico dos quais não pretende receber mensagens por considerar que as mesmas serão correio publicitário não solicitado. No antiphishing, uma lista de Web sites considerados fraudulentos. Comparar com lista de sites seguros (página 179).

lista de sites seguros

Uma lista de Web sites ou endereços de correio electrónico considerados seguros. Os Web sites existentes numa lista de sites seguros são aqueles aos quais os utilizadores estão autorizados a aceder. Os endereços de correio electrónico existentes numa lista de sites seguros provêm de origens fidedignas cujas mensagens pretende receber. Comparar com lista de sites bloqueados (página 179).

localizações de monitorização

As pastas do computador monitorizadas pela Cópia de Segurança e Restauro.

M

mapa de rede

Uma representação gráfica dos computadores e dos componentes que fazem parte de uma rede doméstica.

MAPI

Interface de Programação de Aplicações de Mensagens. Uma especificação de interface da 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.

marcadores

Software que redirecciona as ligações à Internet para um fornecedor diferente do ISP (fornecedor de serviços Internet) predefinido do utilizador, de modo a criar custos de ligação adicionais para fornecedores de conteúdo, fornecedores ou terceiros.

message authentication code (MAC)

Um código de segurança utilizado para encriptar mensagens transmitidas entre computadores. A mensagem é aceite se o computador reconhecer o código desencriptado como válido.

MSN

Rede Microsoft. Um grupo de serviços baseados na Web oferecido pela Microsoft Corporation, que inclui um motor de procura, correio electrónico, mensagens instantâneas e portal.

N

NIC

Placa de Rede. Uma placa que é ligada a um computador portátil ou outro dispositivo, permitindo-lhe aceder à LAN.

nó

Um único computador ligado a uma rede.

P

palavra-passe

Um código (normalmente constituído por letras e números) utilizado para obter acesso a um computador, programa ou Web site.

partilhar

Permitir 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 de correio electrónico que especificar. Os destinatários recebem uma mensagem de correio electrónico a partir da Cópia de Segurança e Restauro, com a indicação de que os ficheiros foram partilhados com os mesmos. A mensagem de correio electrónico contém igualmente uma ligação para os ficheiros partilhados.

phishing

Um método para obter informações pessoais, como palavras-passe, números da segurança social e detalhes de cartões de crédito de modo fraudulento, através do envio de mensagens de correio electrónico falsas que parecem enviadas por fontes fidedignas, como bancos ou empresas legítimas. Normalmente, as mensagens de phishing solicitam aos destinatários que cliquem na hiperligação incluída na mensagem ou que actualizem os detalhes de contacto ou as informações do cartão de crédito.

plug-in, extensão

Um pequeno programa de software que adiciona funcionalidades a ou melhora um programa de maiores dimensões. Por exemplo, permite que um 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.

ponto de acesso (AP)

Um dispositivo de rede (frequentemente designado por router sem fios) ligado a um concentrador ou comutador Ethernet para aumentar o alcance físico do serviço para os utilizadores sem fios. Quando os utilizadores sem fios se deslocam com os seus dispositivos móveis, a transmissão passa de um ponto de acesso para outro para manter a conectividade.

ponto de acesso não autorizado

Um ponto de acesso não autorizado. Os pontos de acesso não autorizados podem ser instalados numa rede empresarial protegida para conceder acesso à rede a pessoas não autorizadas. Também podem ser criados para permitir a um atacante executar um ataque de intermediário.

ponto de restauro do sistema

Um instantâneo (imagem) do conteúdo da memória ou de uma base de dados do computador. O Windows cria pontos de restauro periodicamente quando ocorrem eventos de sistema significativos, como, por exemplo, quando é instalado um programa ou um controlador. Também pode criar e atribuir um nome aos seus pontos de restauro em qualquer altura.

POP3

Post Office Protocol 3. Uma interface entre um programa de correio electrónico cliente e o servidor de correio electrónico. A maioria dos utilizadores domésticos possui uma conta de correio electrónico POP3, também conhecida como conta de correio electrónico padrão.

popups

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.

porta

Uma localização de hardware para passagem de dados de e para um dispositivo informático. Os computadores pessoais possuem vários tipos de portas, incluindo portas internas para ligar unidades de disco, monitores e teclados, bem como portas externas para ligar modems, impressoras, ratos e outros periféricos.

PPPoE

Point-to-Point Protocol Over Ethernet. Um método de utilização do protocolo de acesso telefónico Point-to-Point Protocol (PPP) com a Ethernet como transporte.

programa potencialmente indesejado (PUP)

Um programa de software que pode ser indesejado, independentemente de os utilizadores terem consentido a sua transferência. Pode alterar as definições de segurança ou de privacidade no computador onde é instalado. Os PUP podem — mas não necessariamente — incluir spyware, adware e marcadores e podem ser transferidos com um programa que o utilizador pretende.

protocolo

Um conjunto de regras que permite aos computadores ou dispositivos efectuarem permuta de dados. Numa arquitectura de rede por camadas (Open System Interconnection), cada camada possui os seus próprios protocolos que especificam a forma como as comunicações se processam a esse nível. O computador ou dispositivo deve suportar o protocolo correcto para comunicar com outros computadores. Ver também Open Systems Interconnection (OSI).

proxy

Um 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 representante de todos os computadores internos, o proxy protege identidades de rede ao mesmo tempo que fornece acesso à Internet. Ver também servidor proxy (página 183).

publicar

O processo de disponibilizar publicamente um ficheiro com cópia de segurança na Internet. É possível aceder a ficheiros publicados, pesquisando a biblioteca de Cópia de Segurança e Restauro.

Q

quarentena

Isolamento forçado de um ficheiro ou pasta suspeitos de conter vírus, correio publicitário não solicitado, conteúdo suspeito ou programas potencialmente indesejados (PUP), de modo a que os ficheiros ou pastas não possam ser executados ou abertos.

R

RADIUS

Remote Access Dial-In User Service. Um protocolo que permite a autenticação de utilizadores, normalmente no contexto de acesso remoto. Originalmente definido para utilização com servidores de acesso telefónico remoto, é agora utilizado numa vasta gama de ambientes de autenticação, incluindo a autenticação 802.1x do segredo partilhado dos utilizadores de uma WLAN. Ver também segredo partilhado.

Reciclagem

Um recipiente de lixo simulado para ficheiros e pastas eliminados no Windows.

rede

Um conjunto de sistemas baseados em IP (tais como routers, comutadores, servidores e firewalls) agrupados como uma unidade lógica. Por exemplo, uma “Rede Financeira” pode incluir todos os servidores, routers e sistemas que operam num departamento financeiro. Ver também rede doméstica (página 182).

rede doméstica

Dois ou mais computadores ligados entre si numa casa particular para partilharem ficheiros e o acesso à Internet. Ver também LAN (página 178).

registo

Uma base de dados utilizada pelo Windows para armazenar a informação de configuração para cada utilizador do computador, hardware do sistema, programas instalados e definições de propriedade. A base de dados está dividida em chaves, para as quais são definidos valores. Os programas indesejados podem alterar o valor de chaves do registo ou criar novas chaves para executar código malicioso.

roaming

Passar de uma área de cobertura de um Ponto de Acesso (AP) para outra sem interrupção do serviço ou perda de conectividade.

rootkit

Um conjunto de ferramentas (programas) que concede acesso de administrador a um computador ou rede de computadores. Os rootkits podem incluir spyware e outros programas potencialmente indesejados passíveis de gerar riscos adicionais para a segurança ou privacidade dos dados do computador e das informações pessoais.

router

Um dispositivo de rede que encaminha pacotes de dados entre redes. Os routers lêem cada pacote recebido e decidem como o devem reencaminhar a partir de qualquer combinação de endereços de origem e destino, bem como das condições actuais de tráfego. Por vezes, um router é referido como Ponto de Acesso (AP).

S

script

Uma sequência de comandos que pode ser executada automaticamente (ou seja, sem interacção do utilizador). Ao contrário dos programas, os scripts são normalmente armazenados em formato de texto simples e compilados sempre que são executados. As macros e os ficheiros batch também são referidos como scripts.

segredo partilhado

Uma sequência ou chave (normalmente uma palavra-passe) que foi partilhada entre duas partes antes de iniciarem uma comunicação entre si. É utilizado para proteger partes sensíveis de mensagens RADIUS. Ver também RADIUS (página 182).

servidor

Um computador ou programa que aceita ligações de outros computadores ou programas e devolve respostas adequadas. Por exemplo, o seu programa de correio electrónico estabelece ligação a um servidor de correio electrónico sempre que envia ou recebe mensagens de correio electrónico.

servidor proxy

Componente de firewall que gere o tráfego de Internet de e para uma rede de área 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 proprietários.

sincronizar

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.

SMTP

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.

SSID

Identificador do Conjunto de Serviços. Um token (chave secreta) que identifica uma rede Wi-Fi (802.11). O SSID é definido pelo administrador da rede e tem de ser fornecido a todos os utilizadores que pretendem estabelecer ligação à rede.

SSL

Secure Sockets Layer. Protocolo desenvolvido pela Netscape para a transmissão de documentos privados na Internet. O SSL funciona através da utilização de uma chave pública para encriptar os dados que são transferidos através da ligação SSL. Os URL que requerem uma ligação SSL começam por HTTPS em vez de HTTP.

SystemGuard

Alertas da McAfee que detectam alterações não autorizadas ao computador e o notificam quando as mesmas ocorrem.

T

texto cifrado

Texto encriptado. O texto cifrado não é legível até ser convertido em texto simples (ou seja, desencriptado). Ver também encriptação (página 177).

texto simples

Texto que não está encriptado. Ver também encriptação (página 177).

tipos de ficheiros monitorizados

Tipos de ficheiros (por exemplo, .doc, .xls) que a Cópia de Segurança e Restauro arquiva ou copia para as localizações de monitorização.

TKIP

Temporal Key Integrity Protocol (pronunciado tikip). Parte da norma de encriptação 802.11i para redes locais sem fios. O TKIP é a próxima geração do WEP, que é utilizado para proteger redes locais sem fios 802.11. O TKIP proporciona mistura de chaves por pacote, um mecanismo de recriação de chaves e verificação de integridade de mensagens, corrigindo assim as falhas do WEP.

Trojan, cavalo de Tróia

Um programa que não se replica mas provoca danos ou compromete a segurança do computador. Normalmente, os cavalos de Tróia são enviados por correio electrónico por alguém, não se enviam eles próprios. Também pode transferir inadvertidamente um cavalo de Tróia de um Web site ou através de uma rede ponto a ponto.

U

U3

Unidade: Simplificada, Inteligente, Portátil. Uma plataforma para executar programas do Windows 2000 ou do Windows XP directamente a partir de um dispositivo USB. A iniciativa U3 foi fundada em 2004 pela M-Systems e pela SanDisk e permite aos utilizadores executarem programas U3 num computador Windows sem instalarem ou armazenarem dados ou definições no computador.

unidade de disco rígido externa

Uma unidade de disco rígido armazenada no exterior do computador.

unidade de rede

Uma unidade de disco ou uma unidade de banda magnética que está ligada a um servidor de uma rede e que é partilhada por vários utilizadores. As unidades de rede são por vezes designadas por “unidades remotas”.

unidade inteligente

Ver unidade USB (página 185).

unidade USB

Uma pequena unidade de memória ligada à porta USB do computador. Uma unidade USB funciona como uma pequena unidade de disco, simplificando a transferência de ficheiros entre computadores.

URL

Uniform Resource Locator. O formato padrão para endereços da Internet.

USB

Universal Serial Bus. Um conector padrão da indústria existente na maior parte dos computadores modernos que liga vários dispositivos, desde teclados e ratos a câmaras Web, digitalizadores e impressoras.

V

vírus

Um programa de computador que pode copiar-se a si próprio e infectar o computador sem permissão ou consentimento do utilizador.

VPN

Rede Privada Virtual. Uma rede de comunicações privada que é configurada através de uma rede anfitriã, como a Internet. Os dados que viajam através de uma ligação VPN são encriptados e possuem sólidas características de segurança.

W

wardriver

Uma pessoa equipada com um computador Wi-Fi e algum hardware ou software especial e que percorre cidades para interceptar redes Wi-Fi (802.11).

webmail

Correio electrónico baseado na Web. Serviço de correio electrónico acedido normalmente através de um Web browser em vez de um cliente de correio electrónico instalado no computador, como o Microsoft Outlook. Ver também correio electrónico (página 176).

WEP

Wired Equivalent Privacy. Um protocolo de encriptação e autenticação definido como parte da norma Wi-Fi (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. Um termo utilizado genericamente pela Wi-Fi Alliance para referir qualquer tipo de rede 802.11.

Wi-Fi Alliance

Uma organização composta pelos principais fabricantes de equipamentos de hardware e software sem fios. A Wi-Fi Alliance visa certificar a interoperacionalidade de todos os produtos baseados na norma 802.11 e promover o termo Wi-Fi como marca global em todos os mercados para todos os produtos sem fios baseados na norma 802.11. A organização funciona como um consórcio, laboratório de testes e ponto de encontro para todos os fabricantes que pretendam promover o crescimento da indústria.

Wi-Fi Certified

Produtos testados e aprovados pela Wi-Fi Alliance. Os produtos aprovados como Wi-Fi Certified oferecem garantia de interoperacionalidade, mesmo que sejam provenientes 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.

WLAN

Rede Local sem Fios. Uma rede local (LAN) que utiliza uma ligação sem fios. Uma WLAN utiliza ondas de rádio de alta frequência para a comunicação entre computadores, em vez de fios.

worm

Um vírus que se propaga através da criação de duplicados de si próprio noutras unidades, sistemas ou redes. Um worm de propagação em massa por correio electrónico é um worm que necessita da intervenção do utilizador para se propagar, por exemplo, abrir um ficheiro ou executar um ficheiro transferido. A maioria dos vírus de correio electrónico actuais são worms. Um worm de auto-propagação não necessita da intervenção de um utilizador para se propagar. Os worms Blaster e Sasser são exemplos de worms de auto-propagação.

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 da e é compatível com a norma 802.11i. Quando instalado correctamente, fornece aos utilizadores da LAN sem fios um elevado grau de confiança de 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. Ver também WPA2-PSK (página 187), TKIP (página 184).

WPA2

Uma actualização da norma de segurança WPA, baseada na norma IEEE 802.11i.

WPA2-PSK

Um modo WPA especial idêntico ao modo WPA-PSK e baseado na norma WPA2. Uma funcionalidade comum do WPA2-PSK é o facto de os dispositivos suportarem normalmente vários modos de encriptação (por exemplo, AES, TKIP) em simultâneo, enquanto que os dispositivos mais antigos, geralmente, suportam apenas um único modo de encriptação de cada vez (ou seja, 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 proactivos 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.

Licença

Copyright

CAPÍTULO 36

Suporte a Clientes e Suporte Técnico

O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Os problemas críticos requerem uma acção imediata e comprometem o estado de protecção (a cor muda para vermelho) Os problemas de protecção não críticos não requerem uma acção imediata e podem ou não comprometer o estado de protecção (dependendo do tipo de problema). Para obter o estado de protecção verde, deve corrigir todos os problemas críticos e corrigir ou ignorar todos os problemas não críticos. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee. Para obter mais informações sobre o Técnico Virtual da McAfee, consulte a ajuda do Técnico Virtual da McAfee.

Se tiver adquirido o software de segurança num parceiro ou fornecedor da McAfee, abra um Web browser e aceda a www.mcafeeajuda.com. Em seguida, em Ligações de Parceiros, seleccione o parceiro ou fornecedor para aceder ao Técnico Virtual da McAfee.

Nota: Para instalar e executar o Técnico Virtual da McAfee, é necessário iniciar sessão no computador como Administrador do Windows. Caso contrário, o MVT poderá não conseguir resolver os seus problemas. Para obter informações sobre o início de sessão como Administrador do Windows, consulte a Ajuda do Windows. No Windows Vista™, é-lhe solicitado quando executar o MVT. Clique em **Aceitar**. O Técnico Virtual não é compatível com o Mozilla® Firefox.

Neste capítulo

Utilizar o Técnico Virtual da McAfee

À semelhança de um representante físico do suporte técnico, o Técnico Virtual recolhe informações sobre os programas do SecurityCenter para resolver os problemas de protecção do computador. Quando é executado, o Técnico Virtual verifica se os programas do SecurityCenter estão a funcionar correctamente. Se encontrar problemas, o Técnico Virtual pode solucioná-los ou fornecer-lhe informações mais detalhadas sobre os mesmos. Quando termina, o Técnico Virtual apresenta os resultados da análise que efectuou e permite-lhe procurar suporte técnico adicional da McAfee, se necessário.

Para manter a segurança e a integridade do computador e dos ficheiros, o Técnico Virtual não recolhe informações de identificação pessoal.

Nota: Para obter mais informações sobre o Técnico Virtual, clique no ícone da **Ajuda** no Técnico Virtual.

Iniciar o Técnico Virtual

O Técnico Virtual recolhe informações sobre os programas do SecurityCenter para resolver os seus problemas de protecção. Para salvaguardar a sua privacidade, estas informações não incluem informações de identificação pessoal.

1. Em **Tarefas Comuns**, clique em **Técnico Virtual da McAfee**.
2. Siga as instruções apresentadas no ecrã para transferir e executar o Técnico Virtual.

Consulte as tabelas seguintes para conhecer os sites de Suporte e Transferência da McAfee no seu país ou região, incluindo Manuais do Utilizador.

Suporte e Transferências

País/Região	Suporte McAfee	Transferências McAfee
Alemanha	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Austrália	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canadá (Francês)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
Canadá (Inglês)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp

China (Chinês Simplificado)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Coreia	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Dinamarca	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Eslováquia	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Espanha	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Estados Unidos	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp
Finlândia	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
França	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Grécia	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
Hungria	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp
Itália	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japão	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
México	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Noruega	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polónia	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Reino Unido	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
República Checa	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Rússia	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Suécia	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Taiwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Turquia	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp

Manuais do Utilizador do McAfee Total Protection

País/Região	Manuais do Utilizador da McAfee
Alemanha	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Austrália	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canadá (Francês)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Canadá (Inglês)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
China (Chinês Simplificado)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Coreia	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Eslováquia	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Grécia	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Hungria	http://download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Países Baixos	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf

Polónia	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Reino Unido	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Rússia	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf

Manuais do Utilizador do McAfee Internet Security

País/Região	Manuais do Utilizador da McAfee
Alemanha	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Austrália	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canadá (Francês)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Canadá (Inglês)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
China (Chinês Simplificado)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Coreia	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Eslováquia	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf

França	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Grécia	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Hungria	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Países Baixos	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Polónia	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Reino Unido	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Rússia	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf

Manuais do Utilizador do McAfee VirusScan Plus

País/Região	Manuais do Utilizador da McAfee
Alemanha	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Austrália	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canadá (Francês)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf

Canadá (Inglês)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
China (Chinês Simplificado)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Coreia	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Eslováquia	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Grécia	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Hungria	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Países Baixos	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Polónia	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Reino Unido	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Rússia	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf

Taiwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf

Manuais do Utilizador do McAfee VirusScan

País/Região	Manuais do Utilizador da McAfee
Alemanha	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Austrália	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canadá (Francês)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Canadá (Inglês)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
China (Chinês Simplificado)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Coreia	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Eslováquia	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Grécia	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Hungria	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
Itália	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf

Noruega	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Países Baixos	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Polónia	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Reino Unido	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Rússia	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf

Consulte a tabela seguinte para conhecer os sites do Centro de Ameaças e Informação de Vírus da McAfee no seu país ou região.

País/Região	Sede de Segurança	Informações sobre Vírus
Alemanha	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Austrália	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canadá (Francês)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canadá (Inglês)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
China (Chinês Simplificado)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Coreia	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Dinamarca	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo

Eslováquia	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Espanha	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Estados Unidos	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo
Finlândia	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
França	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Grécia	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Hungria	www.mcafee.com/us/threat_center www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
Itália	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japão	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
México	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Noruega	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Países Baixos	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Polónia	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Reino Unido	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
República Checa	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Rússia	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Suécia	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Taiwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Turquia	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo

Consulte a tabela seguinte para conhecer os sites do HackerWatch no seu país ou região.

País/Região	HackerWatch
Alemanha	www.hackerwatch.org/?lang=de
Austrália	www.hackerwatch.org
Brasil	www.hackerwatch.org/?lang=pt-br
Canadá (Francês)	www.hackerwatch.org/?lang=fr-ca
Canadá (Inglês)	www.hackerwatch.org
China (Chinês Simplificado)	www.hackerwatch.org/?lang=zh-cn
Coreia	www.hackerwatch.org/?lang=ko
Dinamarca	www.hackerwatch.org/?lang=da
Eslováquia	www.hackerwatch.org/?lang=sk
Espanha	www.hackerwatch.org/?lang=es
Estados Unidos	www.hackerwatch.org
Finlândia	www.hackerwatch.org/?lang=fi
França	www.hackerwatch.org/?lang=fr
Grécia	www.hackerwatch.org/?lang=el
Hungria	www.hackerwatch.org/?lang=hu
Itália	www.hackerwatch.org/?lang=it
Japão	www.hackerwatch.org/?lang=jp
México	www.hackerwatch.org/?lang=es-mx
Noruega	www.hackerwatch.org/?lang=no
Países Baixos	www.hackerwatch.org/?lang=nl
Polónia	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Reino Unido	www.hackerwatch.org
República Checa	www.hackerwatch.org/?lang=cs
Rússia	www.hackerwatch.org/?lang=ru
Suécia	www.hackerwatch.org/?lang=sv
Taiwan	www.hackerwatch.org/?lang=zh-tw
Turquia	www.hackerwatch.org/?lang=tr

Índice remissivo

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W