McAfee®

VirusScan® Plus 2007

AntiVirus, Firewall & AntiSpyware

Guida dell'utente

Sommario

CAPITOLO 1

Introduzione

McAfee VirusScan Plus Suite protegge il computer e i file da virus, spyware e hacker. La navigazione sul Web e il download di file non sono mai stati così sicuri, grazie alla protezione sempre attiva e agli aggiornamenti sempre disponibili offerti da McAfee. La protezione affidabile di McAfee consente di bloccare automaticamente le minacce e gli attacchi degli hacker, assicurando il buon rendimento e la protezione del computer. Con McAfee, non solo la visualizzazione dello stato della protezione e la ricerca di virus e spyware sono più semplici, ma il continuo aggiornamento dei prodotti è assicurato grazie a McAfee SecurityCenter, ora completamente riprogettato. In più, con l'abbonamento, è possibile ricevere il software e gli aggiornamenti di McAfee più recenti in modo automatico.

In VirusScan Plus sono inclusi i seguenti programmi:

- SecurityCenter
- VirusScan
- Personal Firewall
- Network Manager
- EasyNetwork (solo licenza per 3 utenti)
- SiteAdvisor

CAPITOLO 2

McAfee SecurityCenter

McAfee SecurityCenter è un ambiente di facile utilizzo, che consente agli utenti McAfee di avviare, gestire e configurare i propri abbonamenti ai prodotti di protezione.

SecurityCenter fornisce inoltre informazioni su avvisi relativi ai virus, prodotti, supporto tecnico e abbonamenti nonché un accesso rapido a strumenti e notizie presenti sul sito Web di McAfee.

In questo capitolo

Funzioni

McAfee SecurityCenter offre le nuove funzioni e i vantaggi riportati di seguito:

Stato di protezione riprogettato

Consente un controllo semplificato dello stato di protezione del computer, la verifica della disponibilità di aggiornamenti e la risoluzione dei potenziali problemi di protezione.

Aggiornamenti continui

L'installazione di aggiornamenti quotidiani avviene automaticamente. Quando una nuova versione di software McAfee è disponibile, verrà scaricata automaticamente senza alcun costo ulteriore nel corso dell'abbonamento, garantendo quindi una protezione sempre aggiornata.

Avvisi in tempo reale

Gli avvisi di protezione notificano all'utente la diffusione di virus e di minacce per la protezione e forniscono opzioni di risposta che consentono di rimuovere e neutralizzare la minaccia o di ottenere ulteriori informazioni su di essa.

Protezione conveniente

Un'ampia gamma di opzioni di rinnovo consente di mantenere aggiornata l'attuale protezione McAfee.

Strumenti per il rendimento

È possibile rimuovere i file inutilizzati, deframmentare quelli utilizzati e servirsi del ripristino della configurazione di sistema per ottenere sempre prestazioni ottimali dal proprio computer.

Guida in linea in tempo reale

Consente di ricevere assistenza tramite chat Internet, posta elettronica e telefono dagli esperti di protezione dei computer di McAfee.

Navigazione protetta e sicura

Se installato, il plug-in per browser McAfee SiteAdvisor consente di proteggere il computer da spyware, posta indesiderata, virus e frodi in linea tramite un sistema di classificazione dei siti Web visitati o riportati nei risultati delle ricerche effettuate sul Web. È possibile visualizzare una classificazione di sicurezza che indica in dettaglio la valutazione di un sito in relazione a gestione della posta elettronica, esecuzione dei download, iscrizioni online e disturbi quali popup e cookie traccianti di terze parti.

CAPITOLO 3

Utilizzo di SecurityCenter

È possibile avviare SecurityCenter dall'icona di McAfee SecurityCenter , situata nell'area di notifica di Windows all'estremità destra della barra delle applicazioni, oppure dal desktop di Windows.

Quando si apre SecurityCenter, il riquadro Home visualizza lo stato di protezione del computer e consente di accedere rapidamente alle funzioni di aggiornamento, alle scansioni (se è stato installato McAfee VirusScan) e ad altre attività comuni.

Intestazione

Guida in linea

Visualizza il file della guida in linea del programma.

Colonna di sinistra

Aggiorna

Aggiorna il prodotto per assicurare la protezione dalle minacce più recenti.

Scansione

Se è stato installato McAfee VirusScan, è possibile eseguire una scansione manuale del computer.

Attività comuni

Consente di eseguire le attività comuni, tra cui il ritorno al riquadro Home, la visualizzazione degli eventi più recenti, la gestione della rete di computer (nel caso in cui si tratti di un computer con capacità di gestione della rete), nonché la manutenzione del computer. Se è stato installato McAfee Data Backup, è anche possibile eseguire il backup dei dati.

Componenti installati

Consente di visualizzare i servizi di protezione attivi sul computer in uso.

Riquadro principale

Stato protezione

La sezione **Il computer è protetto?** indica il livello di protezione generale del computer. Nella sezione sottostante sono visualizzati i dettagli dello stato suddivisi per tipo e per categoria di protezione.

Informazioni su SecurityCenter

Consente di visualizzare la data dell'ultimo aggiornamento del computer, la data dell'ultima scansione (se è stato installato McAfee VirusScan) e la data di scadenza dell'abbonamento.

In questo capitolo

Informazioni sulle icone di SecurityCenter

Le icone di SecurityCenter vengono visualizzate nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni. È possibile utilizzarle per verificare se il computer è protetto, consultare lo stato di una scansione in corso (se è stato installato McAfee VirusScan), controllare la disponibilità di aggiornamenti, visualizzare gli eventi recenti, eseguire la manutenzione del computer e ottenere assistenza dal sito web di McAfee.

Apertura di SecurityCenter e utilizzo delle funzioni aggiuntive

Quando SecurityCenter è in esecuzione, l'icona M viene visualizzata nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni.

Per aprire SecurityCenter o utilizzare le funzioni aggiuntive

- Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, quindi selezionare uno dei seguenti comandi:
  - Apri SecurityCenter
  - Aggiornamenti
  - Collegamenti rapidi

    Il sottomenu contiene collegamenti a Home, Visualizza eventi recenti, Gestione rete, Manutenzione computer e Data Backup (se installato).
  - Verifica abbonamento

    Questa voce viene visualizzata quando l'abbonamento di almeno un prodotto è scaduto.
  - Centro aggiornamenti
  - Servizio clienti

Verifica dello stato di protezione

Se il computer non è completamente protetto, l'icona dello stato di protezione viene visualizzata nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni. L'icona può essere rossa o gialla in base allo stato di protezione.

Per verificare dello stato di protezione

- Fare clic sull'icona dello stato di protezione per aprire SecurityCenter e risolvere eventuali problemi.

Verifica dello stato degli aggiornamenti

Se è in corso la verifica della disponibilità degli aggiornamenti, l'icona  degli aggiornamenti viene visualizzata nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni.

Per verificare lo stato degli aggiornamenti

- Scegliere l'icona degli aggiornamenti per visualizzare una breve descrizione dello stato degli aggiornamenti.

Informazioni sullo stato della protezione

Lo stato di protezione generale del computer viene visualizzato nella sezione **Il computer è protetto?** di SecurityCenter.

Lo stato della protezione indica se il computer è protetto nei confronti delle più recenti minacce alla sicurezza, se permangono problemi che richiedono attenzione e il modo in cui affrontarli. Quando un problema interessa più di una categoria di protezione, la sua risoluzione può avere come effetto il ritorno allo stato di protezione completa di più categorie.

Lo stato della protezione è influenzato da alcuni fattori, tra cui le minacce esterne, i prodotti di protezione o di accesso a Internet installati nel computer e la configurazione di tali prodotti.

Per impostazione predefinita, se non sono installati prodotti di protezione dalla posta indesiderata o di blocco dei contenuti, i problemi di protezione secondari controllati da tali prodotti vengono automaticamente ignorati e non vengono considerati nello stato di protezione generale. Tuttavia, se un problema di protezione è seguito da un collegamento **Ignora** , è possibile scegliere di ignorare il problema se si è certi di non avere la necessità di risolverlo.

Il computer è protetto?

Il livello generale di protezione del computer può essere visualizzato nella sezione **Il computer è protetto?** di SecurityCenter:

- Se il computer è protetto, viene visualizzato **Sì** (in verde).
- Se il computer è parzialmente protetto o non protetto, viene visualizzato **No**, rispettivamente in giallo o in rosso.

Per risolvere automaticamente la maggior parte dei problemi di protezione, fare clic su **Correggi** accanto allo stato di protezione. Tuttavia, se uno o più problemi persistono e richiedono un intervento, fare clic sul collegamento visualizzato accanto al problema per intraprendere le azioni consigliate.

Informazioni sulle categorie e i tipi di protezione

Nella sezione **Il computer è protetto?** di SecurityCenter è possibile visualizzare i dettagli dello stato, costituito dai seguenti tipi e categorie di protezione:

- Computer e file
- Rete e Internet
- Posta elettronica e MI
- Controllo genitori

I tipi di protezione visualizzati da SecurityCenter dipendono dai prodotti installati. Ad esempio, il tipo di protezione Stato del computer viene visualizzato se è stato installato il software McAfee Data Backup.

Se una categoria non presenta alcun problema di protezione, lo stato è Verde. Se si fa clic su una categoria Verde, viene visualizzato a destra un elenco di tipi di protezione attivati, seguito da un elenco di problemi già ignorati. Se non esistono problemi, viene visualizzato un avviso virus. È inoltre possibile fare clic su **Configura** per modificare le opzioni relative a una determinata categoria.

Se lo stato è Verde per tutti i tipi di protezione di una stessa categoria, anche lo stato della categoria sarà Verde. Analogamente, se lo stato di tutte le categorie di protezione è Verde, lo Stato di protezione generale sarà Verde.

Se lo stato di alcune categorie di protezione è Giallo o Rosso, è possibile risolvere i problemi di protezione correggendoli o ignorandoli e in entrambi i casi lo stato diventerà Verde.

Informazioni sulla protezione di computer e file

La categoria di protezione Computer e file comprende i seguenti tipi di protezione:

- **Protezione da virus**: protezione con scansione in tempo reale che difende il computer da virus, worm, trojan horse, script sospetti, attacchi di vario genere e altre minacce. Analizza e automaticamente tenta di pulire i file, compresi file eseguibili compressi, settore di avvio, memoria e file essenziali, quando viene eseguito l'accesso dall'utente o dal computer.
- **Protezione da spyware**: rileva, blocca e rimuove rapidamente programmi spyware, adware e altri programmi potenzialmente indesiderati che potrebbero raccogliere e trasmettere i dati personali senza l'autorizzazione dell'utente.
- **SystemGuards**: moduli che rilevano le modifiche apportate al computer e le segnalano all'utente. È quindi possibile esaminare le modifiche e decidere se consentirle.
- **Protezione di Windows**: la protezione di Windows fornisce lo stato dell'aggiornamento di Windows sul computer. Se è stato installato McAfee VirusScan, è inoltre disponibile la protezione da sovraccarico del buffer.

Uno dei fattori che influenzano la protezione di computer e file è costituito dalle minacce esterne di virus. Ad esempio, in caso di diffusione di un virus, è opportuno verificare se il software antivirus in uso è in grado di proteggere il computer. Altri fattori possono essere la configurazione del software antivirus e la frequenza con cui il software viene aggiornato in base ai nuovi file delle firme per i rilevamenti, in modo da proteggere il computer dalle minacce più recenti.

Apertura del riquadro di configurazione File e computer

Se in **File & computer** non sono stati rilevati problemi, è possibile aprire il riquadro di configurazione dal riquadro di informazioni.

Per aprire il riquadro di configurazione File e computer

1. Nel riquadro Home, fare clic su **File & computer**.
2. Nel riquadro di destra, fare clic su **Configura**.

Informazioni sulla protezione di Internet e rete

La categoria di protezione Rete e Internet comprende i seguenti tipi di protezione:

- **Protezione firewall**: consente di difendere il computer da intrusioni e da traffico di rete indesiderato e agevola la gestione delle connessioni Internet in entrata e in uscita.
- **Wireless Protection**: consente di proteggere la rete wireless domestica da intrusioni e intercettazioni di dati. Tuttavia, se attualmente si è connessi a una rete wireless esterna, il livello di protezione varia a seconda del livello di sicurezza di quella rete.
- **Protezione navigazione Web**: la protezione della navigazione sul Web consente di nascondere pubblicità, popup e Web bug sul computer durante la navigazione su Internet.
- **Protezione da phishing**: consente di bloccare i siti Web fraudolenti che richiedono l'invio di dati personali tramite collegamenti ipertestuali visualizzati in messaggi di posta elettronica, messaggi immediati, popup e in altri elementi.
- **Protezione dei dati personali**: blocca la diffusione dei dati sensibili e riservati su Internet.

Apertura del riquadro di configurazione Internet e rete

Se in **Internet & rete** non sono stati rilevati problemi, è possibile aprire il riquadro di configurazione dal riquadro di informazioni.

Per aprire il riquadro di configurazione Internet e rete

1. Nel riquadro Home, fare clic su **Internet & rete**.
2. Nel riquadro di destra, fare clic su **Configura**.

Informazioni sulla protezione di posta elettronica e MI

La categoria di protezione Posta elettronica e MI comprende i seguenti tipi di protezione:

- **Protezione della posta elettronica**: analizza e automaticamente tenta di eliminare i virus, i programmi spyware e le minacce potenziali presenti nei messaggi e negli allegati di posta elettronica in ingresso e in uscita.
- **Protezione da posta indesiderata**: consente di bloccare l'accesso alla Posta in arrivo dei messaggi di posta elettronica indesiderati.
- **Protezione MI**: la protezione della messaggistica immediata (MI) esamina e automaticamente tenta di eliminare i virus, i programmi spyware e le minacce potenziali presenti negli allegati ai messaggi immediati in ingresso. Impedisce inoltre ai client di messaggistica immediata di scambiare contenuti indesiderati o informazioni personali su Internet.
- **Navigazione protetta e sicura**: se installato, il plug-in per browser McAfee SiteAdvisor consente di proteggere il computer da spyware, spam, virus e frodi in linea tramite un sistema di classificazione dei siti Web visitati o riportati nei risultati delle ricerche effettuate sul Web. È possibile visualizzare una classificazione di sicurezza che indica in dettaglio la valutazione di un sito in relazione a gestione della posta elettronica, esecuzione dei download, iscrizioni online e disturbi quali popup e tracking cookie di terze parti.

Apertura del riquadro di configurazione Posta elettronica e MI

Se in **Posta elettronica & MI** non sono stati rilevati problemi, è possibile aprire il riquadro di configurazione dal riquadro di informazioni.

Per aprire il riquadro di configurazione Posta elettronica e MI

1. Nel riquadro Home, fare clic su **Posta elettronica & MI**.
2. Nel riquadro di destra, fare clic su **Configura**.

Informazioni sulla protezione Controllo genitori

La categoria di protezione Controllo genitori comprende i seguenti tipi di protezione:

- **Controllo genitori**: la funzione di blocco dei contenuti impedisce agli utenti di visualizzare i contenuti Internet indesiderati bloccando i siti Web potenzialmente dannosi. È anche possibile monitorare e limitare l'attività degli utenti di Internet.

Apertura del riquadro di configurazione Controllo genitori

Se in **Controllo genitori** non sono stati rilevati problemi, è possibile aprire il riquadro di configurazione dal riquadro di informazioni.

Per aprire il riquadro di configurazione Controllo genitori

1. Nel riquadro Home, fare clic su **Controllo genitori**.
2. Nel riquadro di destra, fare clic su **Configura**.

Risoluzione dei problemi di protezione

La maggior parte dei problemi di protezione può essere risolta automaticamente. Tuttavia, se uno o più problemi persistono, è necessario risolverli.

Risoluzione automatica dei problemi di protezione

È possibile risolvere automaticamente la maggior parte dei problemi di protezione.

Per risolvere automaticamente i problemi di protezione

- Fare clic su **Correggi** accanto allo stato di protezione.

Risoluzione manuale dei problemi di protezione

Se uno o più problemi non vengono risolti automaticamente, fare clic sul collegamento accanto al problema e intraprendere le azioni consigliate.

Per risolvere manualmente i problemi di protezione

- Effettuare una delle seguenti operazioni:
  - Se non è stata eseguita una scansione completa del computer negli ultimi 30 giorni, fare clic su **Scansione** a sinistra dello stato di protezione principale, per eseguire una scansione manuale. Questa voce viene visualizzata solo se è installato McAfee VirusScan.
  - Se i file delle firme per i rilevamenti (DAT) non sono aggiornati, fare clic su **Aggiorna** a sinistra dello stato di protezione principale per aggiornare la protezione.
  - Se un programma non è installato, fare clic su **Protezione completa** per installarlo.
  - Se in un programma mancano alcuni componenti, sarà necessario reinstallarlo.
  - Nel caso in cui sia necessario registrare un programma per ottenere la protezione completa, fare clic su **Registra adesso** per effettuare la registrazione. Questa voce viene visualizzata se uno o più programmi sono scaduti.
  - Se un programma è scaduto, fare clic su **Verifica abbonamento** per controllare lo stato dell'account. Questa voce viene visualizzata se uno o più programmi sono scaduti.

Visualizzazione delle informazioni su SecurityCenter

Nella parte inferiore del riquadro dello stato della protezione, Informazioni su SecurityCenter consente di accedere alle opzioni di SecurityCenter e di visualizzare i dati relativi all'ultimo aggiornamento, all'ultima scansione eseguita (se è installato McAfee VirusScan) e alla scadenza dell'abbonamento dei prodotti McAfee installati.

Apertura del riquadro di configurazione di SecurityCenter

Per comodità, dal riquadro Home è possibile aprire il riquadro di configurazione di SecurityCenter per modificare le opzioni.

Per aprire il riquadro di configurazione di SecurityCenter

- Nel riquadro Home, in **Informazioni su SecurityCenter**, fare clic su **Configura**.

Visualizzazione delle informazioni sui prodotti installati

È possibile visualizzare un elenco dei prodotti installati che mostri il numero della versione di ogni prodotto e la data dell'ultimo aggiornamento.

Per visualizzare le informazioni sui prodotti McAfee

- Nel riquadro Home, in **Informazioni su SecurityCenter**, fare clic su **Visualizza dettagli** per aprire la finestra di informazioni sul prodotto.

Utilizzo del menu avanzato

Quando si apre per la prima volta SecurityCenter, nella colonna di sinistra viene visualizzato il menu standard. Gli utenti esperti possono accedere a un menu più dettagliato facendo clic su **Menu avanzato**. Per praticità, ogni volta che si apre SecurityCenter viene visualizzato il menu utilizzato la volta precedente.

Il menu avanzato contiene i seguenti elementi:

- Home
- Rapporti e registri (comprende l'elenco Eventi recenti e i registri ordinati per tipo per i 30, 60 e 90 giorni precedenti).
- Configura
- Ripristina
- Strumenti

CAPITOLO 4

Configurazione delle opzioni di SecurityCenter

SecurityCenter visualizza lo stato generale di protezione del computer, consente di creare gli account utente McAfee, installa automaticamente gli aggiornamenti più recenti dei prodotti e segnala automaticamente all'utente, mediante avvisi e segnali acustici, la diffusione di virus, il rilevamento di minacce e la disponibilità di aggiornamenti dei prodotti.

Nel riquadro Configurazione di SecurityCenter, è possibile modificare le opzioni per le seguenti funzioni:

- Stato protezione
- Utenti
- Aggiornamenti automatici
- Avvisi

In questo capitolo

Configurazione dello stato della protezione

Lo stato di protezione generale del computer viene visualizzato nella sezione **Il computer è protetto?** di SecurityCenter.

Lo stato della protezione indica se il computer è protetto nei confronti delle più recenti minacce alla sicurezza, se permangono problemi che richiedono attenzione e il modo in cui affrontarli.

Per impostazione predefinita, se non sono installati prodotti di protezione dalla posta indesiderata o di blocco dei contenuti, i problemi di protezione secondari controllati da tali prodotti vengono automaticamente ignorati e non vengono considerati nello stato di protezione generale. Tuttavia, se un problema di protezione è seguito da un collegamento **Ignora**, è possibile scegliere di ignorare il problema se si è certi di non avere la necessità di risolverlo. Se si decide in un secondo momento di risolvere un problema precedentemente ignorato, è possibile includerlo nello stato della protezione perché venga rilevato.

Configurazione dei problemi ignorati

È possibile indicare nello stato di protezione generale del computer di includere o escludere dal rilevamento determinati problemi. Se un problema di protezione è seguito da un collegamento **Ignora** , è possibile scegliere di ignorare il problema se si è certi di non avere la necessità di risolverlo. Se si decide in un secondo momento di risolvere un problema precedentemente ignorato, è possibile includerlo nello stato della protezione perché venga rilevato.

Per configurare i problemi ignorati

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto a **Stato della protezione** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. Nel riquadro Problemi ignorati, eseguire una delle seguenti operazioni:
   - Per includere problemi precedentemente ignorati nello stato della protezione, deselezionare le relative caselle di controllo.
   - Per escludere dei problemi dallo stato della protezione, selezionare le relative caselle di controllo.
4. Fare clic su **OK**.

Configurazione delle opzioni utente

Se si utilizzano programmi McAfee che richiedono autorizzazioni utente, tali autorizzazioni corrispondono per impostazione predefinita agli account utente di Windows del computer in uso. Per facilitare la gestione di questi programmi da parte degli utenti, è possibile decidere in qualsiasi momento di utilizzare gli account utente McAfee.

Se si decide di utilizzare gli account utente McAfee, eventuali nomi utente e autorizzazioni già esistenti nel programma per il controllo genitori in uso verranno importati automaticamente. Tuttavia, prima di utilizzare gli account utente McAfee, è necessario creare un account Amministratore. In seguito sarà possibile creare e configurare altri account utente McAfee.

Utilizzo degli account utente McAfee

Per impostazione predefinita, si utilizzano gli account utente di Windows. Tuttavia, l'utilizzo degli account utente McAfee rende superflua la creazione di nuovi account utente di Windows.

Per utilizzare gli account utente McAfee

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto a **Utenti** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. Per utilizzare gli account utente McAfee, fare clic su **Passa a**.

Se si utilizzano gli account utente McAfee per la prima volta, è necessario procedere alla creazione di un account Amministratore (pagina 23).

Creazione di un account Amministratore

La prima volta che si utilizzano gli account utente McAfee, viene richiesta la creazione di un account Amministratore.

Per creare un account Amministratore

1. Immettere una password nella casella **Password** e immetterla nuovamente nella casella **Conferma password**.
2. Selezionare una domanda per il recupero della password dall'elenco fornito e immettere la risposta nella casella **Risposta**.
3. Fare clic su **Applica**.

   Al termine della procedura, il tipo di account utente viene aggiornato nel riquadro in cui sono visualizzati gli account utente e le autorizzazioni del programma per il controllo genitori preesistente, se presenti. Se si configurano gli

account utente per la prima volta, verrà visualizzato il riquadro di gestione utente.

Configurazione delle opzioni utente

Se si decide di utilizzare gli account utente McAfee, eventuali nomi utente e autorizzazioni già esistenti nel programma per il controllo genitori in uso verranno importati automaticamente. Tuttavia, prima di utilizzare gli account utente McAfee, è necessario creare un account Amministratore. In seguito sarà possibile creare e configurare altri account utente McAfee.

Per configurare le opzioni utente

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto a **Utenti** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. In **Account utente** fare clic su **Aggiungi**.
4. Immettere un nome utente nella casella **Nome utente**.
5. Immettere una password nella casella **Password** e immetterla nuovamente nella casella **Conferma password**.
6. Selezionare la casella di controllo **Utente di avvio** se si desidera che il nuovo utente si colleghi automaticamente all'avvio di SecurityCenter.
7. In **Tipo account utente**, selezionare il tipo di account dell'utente e fare clic su **Crea**.

   Nota: dopo aver creato l'account utente, è necessario configurare le impostazioni di utente con limitazioni in Controllo genitori.

8. Per modificare la password, l'accesso automatico o il tipo di account di un utente, selezionare il nome dell'utente dall'elenco e fare clic su **Modifica**.
9. Al termine dell'operazione, fare clic su **Applica**.

Recupero della password di amministratore

Se si dimentica la password di amministratore, è possibile recuperarla.

Per recuperare la password di amministratore

1. Fare clic con il pulsante destro del mouse sull'icona M di SecurityCenter, quindi fare clic su **Cambia utente**.
2. Nell'elenco **Nome utente** selezionare **Amministratore**, quindi fare clic su **Password dimenticata**.
3. Immettere la risposta alla domanda segreta selezionata al momento della creazione dell'account Amministratore.
4. Fare clic su **Invia**.

   Verrà visualizzata la password di amministratore dimenticata.

Modifica della password di amministratore

Se si ritiene che la password di amministratore sia compromessa o si hanno difficoltà a ricordarla, è possibile modificarla.

Per modificare la password di amministratore

1. Fare clic con il pulsante destro del mouse sull'icona M di SecurityCenter, quindi fare clic su **Cambia utente**.
2. Nell'elenco **Nome utente** selezionare **Amministratore**, quindi fare clic su **Modifica password**.
3. Immettere la password in uso nella casella **Vecchia password** .
4. Immettere la nuova password nella casella **Password** e immetterla nuovamente nella casella **Conferma password**.
5. Fare clic su **OK**.

Configurazione delle opzioni di aggiornamento

Quando si è connessi a Internet, SecurityCenter verifica automaticamente ogni quattro ore la disponibilità di aggiornamenti per tutti i servizi McAfee in uso, quindi installa gli aggiornamenti più recenti dei prodotti. È tuttavia sempre possibile verificare manualmente la presenza di aggiornamenti mediante l'icona di SecurityCenter situata nell'area di notifica, all'estremità destra della barra delle applicazioni.

Verifica automatica degli aggiornamenti

Quando si è connessi a Internet, SecurityCenter verifica automaticamente la disponibilità di aggiornamenti ogni quattro ore. È tuttavia possibile configurare SecurityCenter in modo tale che visualizzi una notifica prima di scaricare o installare gli aggiornamenti.

Per verificare automaticamente la disponibilità di aggiornamenti

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto allo stato **Gli aggiornamenti automatici sono attivi** per ingrandire il riquadro, quindi fare clic su **Avanzate**.
3. Selezionare un'opzione nel riquadro Opzioni di aggiornamento:
   - Installa automaticamente gli aggiornamenti e avvisa quando il prodotto viene aggiornato (consigliato) (pagina 27)
   - Scarica automaticamente gli aggiornamenti e avvisa quando sono pronti per l'installazione (pagina 28)
   - Avvisa prima di scaricare aggiornamenti (pagina 28)
4. Fare clic su **OK**.

Nota: per una protezione ottimale, McAfee consiglia di configurare SecurityCenter in modo tale da eseguire automaticamente la ricerca e l'installazione degli aggiornamenti. Se tuttavia si desidera aggiornare manualmente i servizi di protezione, è possibile disattivare l'aggiornamento automatico (pagina 29).

Esecuzione automatica del download e dell'installazione degli aggiornamenti

Se si seleziona **Installa automaticamente gli aggiornamenti e avvisa quando i servizi vengono aggiornati (consigliato)** nel riquadro Opzioni di aggiornamento di SecurityCenter, il download e l'installazione degli aggiornamenti verranno eseguiti automaticamente.

Download automatico degli aggiornamenti

Se si seleziona **Scarica automaticamente gli aggiornamenti e avvisa quando sono pronti per l'installazione** nel riquadro Opzioni di aggiornamento, SecurityCenter scarica automaticamente gli aggiornamenti e avvisa quando un aggiornamento è pronto per l'installazione. È quindi possibile decidere di installare o posticipare l'aggiornamento (pagina 29).

Per installare un aggiornamento scaricato automaticamente

1. Fare clic su **Aggiorna i prodotti adesso** nella finestra dell'avviso e fare clic su **OK**.

   Se richiesto, è necessario connettersi al sito Web per verificare l'abbonamento prima di effettuare il download.

2. Una volta verificato l'abbonamento, fare clic su **Aggiorna** nel riquadro Aggiornamenti per scaricare e installare l'aggiornamento. Se l'abbonamento è scaduto, fare clic su **Rinnova abbonamento** nella finestra dell'avviso e attenersi alle istruzioni visualizzate.

Nota: in alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutti i programmi prima di riavviare.

Avvisa prima di scaricare aggiornamenti

Se si seleziona **Avvisa prima di scaricare aggiornamenti** nel riquadro Opzioni di aggiornamento, prima del download di eventuali aggiornamenti verrà visualizzato un avviso di SecurityCenter. Sarà quindi possibile decidere di scaricare e installare un aggiornamento dei servizi di protezione per rimuovere la minaccia di un attacco.

Per scaricare e installare un aggiornamento

1. Selezionare **Aggiorna i prodotti adesso** nella finestra dell'avviso e fare clic su **OK**.
2. Se richiesto, accedere al sito Web.

   L'aggiornamento viene scaricato automaticamente.
3. Al termine dell'installazione dell'aggiornamento fare clic su **OK**.

Nota: in alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutti i programmi prima di riavviare.

Disattivazione dell'aggiornamento automatico

Per una protezione ottimale, McAfee consiglia di configurare SecurityCenter in modo tale da eseguire automaticamente la ricerca e l'installazione degli aggiornamenti. Se tuttavia si desidera aggiornare manualmente i servizi di protezione, è possibile disattivare l'aggiornamento automatico.

Nota: è necessario ricordarsi di verificare manualmente la disponibilità di aggiornamenti (pagina 30) almeno una volta alla settimana. Se non si effettua tale verifica, il computer non disporrà degli aggiornamenti di protezione più recenti.

Per disattivare l'aggiornamento automatico

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto allo stato **Gli aggiornamenti automatici sono attivi** per ingrandire il riquadro.
3. Fare clic su **Disattiva**.
4. Fare clic su **Sì** per confermare la modifica.

   Lo stato viene aggiornato nell'intestazione.

Se per sette giorni non viene eseguita la ricerca manuale degli aggiornamenti, verrà visualizzato un avviso che ricorda di ricercare gli aggiornamenti.

Posticipazione degli aggiornamenti

Se non si ha tempo di aggiornare i servizi di protezione quando viene visualizzato l'avviso, è possibile decidere di visualizzare l'avviso in seguito o di ignorare l'avviso.

Per posticipare un aggiornamento

- Effettuare una delle seguenti operazioni:
  - Selezionare **Visualizza un promemoria in un secondo momento** nella finestra dell'avviso e fare clic su **OK**.
  - Selezionare **Chiudere l'avviso** e fare clic su **OK** per chiudere la finestra dell'avviso senza intraprendere alcuna azione.

Verifica manuale degli aggiornamenti

Quando si è connessi a Internet, SecurityCenter verifica automaticamente la disponibilità di aggiornamenti ogni quattro ore, quindi installa gli aggiornamenti dei prodotti più recenti. È tuttavia sempre possibile verificare manualmente la presenza di aggiornamenti mediante l'icona di SecurityCenter nell'area di notifica di Windows, posta all'estremità destra della barra delle applicazioni.

Nota: per una protezione ottimale, McAfee consiglia di configurare SecurityCenter in modo tale da eseguire automaticamente la ricerca e l'installazione degli aggiornamenti. Se tuttavia si desidera aggiornare manualmente i servizi di protezione, è possibile disattivare l'aggiornamento automatico (pagina 29).

Per verificare manualmente la disponibilità di aggiornamenti

1. Assicurarsi che il computer sia connesso a Internet.
2. Fare clic con il pulsante destro del mouse sull'icona M di SecurityCenter nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni, quindi scegliere **Aggiornamenti**.

   Mentre SecurityCenter verifica la disponibilità di aggiornamenti, è possibile proseguire con altre attività.

   Per maggiore praticità, nell'area di notifica di Windows, all'estremità destra della barra delle applicazioni, viene visualizzata un'icona animata. Quando SecurityCenter ha terminato l'operazione di verifica, l'icona scompare automaticamente.
3. Se richiesto, accedere al sito Web per verificare il proprio abbonamento.

Nota: in alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutti i programmi prima di riavviare.

Configurazione delle opzioni di avviso

SecurityCenter informa automaticamente l'utente, mediante avvisi e riproduzione di suoni, della diffusione di virus, di minacce per la protezione e degli aggiornamenti dei prodotti. È tuttavia possibile configurare SecurityCenter in modo da visualizzare solo gli avvisi che richiedono un'attenzione immediata.

Configurazione delle opzioni di avviso

SecurityCenter informa automaticamente l'utente, mediante avvisi e riproduzione di suoni, della diffusione di virus, di minacce per la protezione e degli aggiornamenti dei prodotti. È tuttavia possibile configurare SecurityCenter in modo da visualizzare solo gli avvisi che richiedono un'attenzione immediata.

Per configurare le opzioni di avviso

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto ad **Avvisi** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. Selezionare una delle seguenti opzioni nel riquadro Opzioni di avviso:
   - **Avvisa quando si verifica la diffusione di un virus o una minaccia per la protezione**
   - **Visualizza avvisi informativi quando viene rilevata la modalità di gioco**
   - **Riproduci un suono quando si verifica un avviso.**
   - **Mostra schermata iniziale di McAfee all'avvio di Windows**
4. Fare clic su **OK**.

Nota: per disattivare gli avvisi informativi futuri dall'avviso visualizzato, selezionare la casella di controllo **Non visualizzare più questo messaggio**. Sarà possibile riattivare gli avvisi in un secondo tempo dal riquadro Avvisi informativi.

Configurazione degli avvisi informativi

Gli avvisi informativi avvertono l'utente del verificarsi di eventi che non richiedono una risposta immediata. Se si disattivano gli avvisi informativi futuri dall'avviso stesso, è possibile riattivarli in seguito dal riquadro degli avvisi informativi.

Per configurare gli avvisi informativi

1. In **Informazioni su SecurityCenter**, fare clic su **Configura**.
2. Fare clic sulla freccia accanto ad **Avvisi** per ingrandirne il riquadro, quindi fare clic su **Avanzate**.
3. In **Configurazione di SecurityCenter**, fare clic su **Avvisi informativi**.
4. Deselezionare la casella di controllo **Nascondi avvisi informativi**, quindi deselezionare le caselle di controllo corrispondenti agli avvisi che si desidera visualizzare.
5. Fare clic su **OK**.

CAPITOLO 5

Esecuzione delle attività comuni

È possibile eseguire attività comuni come il ritorno al riquadro Home, la visualizzazione degli eventi più recenti, la gestione della rete di computer (nel caso in cui si tratti di un computer con capacità di gestione della rete), nonché la manutenzione del computer. Se è stato installato McAfee Data Backup, è anche possibile eseguire il backup dei dati.

In questo capitolo

Esecuzione delle attività comuni

È possibile eseguire attività comuni come il ritorno al riquadro Home, la visualizzazione degli eventi più recenti, la manutenzione del computer, la gestione della rete (nel caso in cui si tratti di un computer con capacità di gestione della rete) e il backup dei dati, se è stato installato McAfee Data Backup.

Per eseguire le attività comuni

- In **Attività comuni** nel menu standard, eseguire una delle seguenti operazioni:
  - Per ritornare al riquadro Home, fare clic su **Home**.
  - Per visualizzare gli eventi recenti rilevati dal software di protezione, fare clic su **Eventi recenti**.
  - Per eliminare file inutilizzati, deframmentare i dati e ripristinare le impostazioni precedenti del computer, fare clic su **Manutenzione computer**.
  - Se il computer dispone di capacità di gestione delle reti, fare clic su **Gestione rete** per gestire la rete di computer.

    Network Manager esegue il monitoraggio dei computer in rete alla ricerca di possibili vulnerabilità nella protezione, consentendo di individuare eventuali problemi di protezione della rete.

- Per creare delle copie di backup dei file, se è stato installato McAfee Data Backup fare clic su **Backup dati**.

  Il backup automatizzato salva copie dei file più importanti nelle posizioni desiderate, crittografandoli e memorizzandoli su CD/DVD o su unità USB, esterne o di rete.

Suggerimento: per comodità, è possibile eseguire le attività comuni da altre due posizioni, da **Home** nel menu avanzato e dal menu **Collegamenti rapidi** dell'icona M di SecurityCenter all'estremità destra della barra delle applicazioni. È inoltre possibile visualizzare gli eventi recenti e i registri completi per tipo in **Rapporti e registri** nel menu avanzato.

Visualizzazione degli eventi recenti

Gli eventi recenti vengono registrati quando si verificano cambiamenti nel computer, ad esempio quando si attiva o disattiva un tipo di protezione, si rimuove una minaccia o viene bloccato un tentativo di connessione via Internet. È possibile visualizzare i 20 eventi più recenti con i relativi dettagli.

Per ulteriori dettagli sugli eventi relativi a un particolare prodotto, consultare la guida in linea del prodotto.

Per visualizzare gli eventi recenti

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Visualizza eventi recenti**.

   Gli eventi recenti vengono visualizzati nell'elenco, insieme alla data e a una breve descrizione.

2. Selezionare un evento da **Eventi recenti** per visualizzarne le informazioni nel riquadro dei dettagli.

   Le azioni consentite vengono visualizzate nella sezione **Desidero**.

3. Per visualizzare un elenco di eventi più completo, fare clic su **Visualizza registro**.

Manutenzione automatica del computer

Per liberare spazio su disco e ottimizzare le prestazioni del computer, è possibile programmare le attività di QuickClean o di deframmentazione dischi ad intervalli regolari. Queste attività comprendono l'eliminazione, la distruzione e la deframmentazione di file e cartelle.

Per eseguire la manutenzione automatica del computer:

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.
3. Nell'elenco delle operazioni, selezionare **QuickClean** o **Deframmentazione dischi**.
4. Effettuare una delle seguenti operazioni:
   - Per modificare un'attività esistente, selezionarla e fare clic su **Modifica**. Seguire le istruzioni riportate sullo schermo.
   - Per creare una nuova attività, immettere il nome nella casella **Nome attività**, quindi fare clic su **Crea**. Seguire le istruzioni riportate sullo schermo.
   - Per eliminare un'attività, selezionarla e fare clic su **Elimina**.
5. In **Riepilogo attività**, verificare la data dell'ultima esecuzione dell'attività, la data della prossima esecuzione e lo stato.

Manutenzione manuale del computer

È possibile eseguire manualmente le attività di manutenzione per eliminare i file inutilizzati, deframmentare i dati oppure per ripristinare le precedenti impostazioni del computer.

Per eseguire la manutenzione manuale del computer

- Effettuare una delle seguenti operazioni:
  - Per utilizzare QuickClean, fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi**, fare clic su **Manutenzione computer** e quindi su **Avvia**.
  - Per utilizzare Deframmentazione dischi, fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi**, fare clic su **Manutenzione computer** e quindi su **Analizza**.
  - Per utilizzare l'utilità di ripristino del sistema, selezionare **Strumenti** dal menu avanzato, fare clic su **Ripristino configurazione di sistema**, quindi su **Avvia**.

Rimozione di file e cartelle non utilizzati

Utilizzare QuickClean per liberare spazio su disco e ottimizzare le prestazioni del computer.

Per rimuovere file e cartelle non utilizzati

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Manutenzione computer**.
2. In **QuickClean** fare clic su **Avvia**.
3. Seguire le istruzioni riportate sullo schermo.

Deframmentazione di file e cartelle

La frammentazione dei file si verifica quando si eliminano file e cartelle e si aggiungono nuovi file. La frammentazione rallenta l'accesso al disco e riduce le prestazioni del computer, sebbene spesso non in modo significativo.

L'utilità di deframmentazione consente di riscrivere parti di un file in settori adiacenti del disco rigido per aumentare la velocità di accesso e di recupero.

Per deframmentare file e cartelle

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Manutenzione computer**.
2. In **Deframmentazione dischi**, fare clic su **Analizza**.
3. Seguire le istruzioni riportate sullo schermo.

Ripristino delle impostazioni precedenti del computer

I punti di ripristino sono istantanee del computer che Windows salva periodicamente e quando si verificano eventi importanti, ad esempio quando si installa un programma o un driver. È tuttavia possibile creare e denominare i propri punti di ripristino in qualsiasi momento.

Utilizzare i punti di ripristino per annullare modifiche potenzialmente pericolose per il computer e ritornare alle impostazioni precedenti.

Per ripristinare le impostazioni precedenti del computer

1. Nel menu avanzato, fare clic su **Strumenti**, quindi su **Ripristino configurazione di sistema**.
2. In **Ripristino configurazione di sistema**, fare clic su **Avvia**.
3. Seguire le istruzioni riportate sullo schermo.

Gestione della rete

Se il computer dispone delle capacità di gestione della rete di computer, è possibile utilizzare Network Manager per monitorare i computer in rete alla ricerca di eventuali vulnerabilità nella protezione, in modo tale da consentire l'identificazione dei problemi.

Se lo stato della protezione del computer non è monitorato sulla rete, ciò significa che il computer non fa parte della rete oppure è un membro non gestito della rete. Per ulteriori dettagli, consultare il file della guida in linea di Network Manager.

Per gestire la rete

1. Fare clic con il pulsante destro del mouse sull'icona principale di SecurityCenter, scegliere **Collegamenti rapidi** e fare clic su **Gestione rete**.
2. Fare clic sull'icona che rappresenta il computer nella mappa della rete.
3. Nella sezione **Desidero**, fare clic su **Monitorare il computer**.

Ulteriori informazioni sui virus

Utilizzare la Libreria di informazioni sui virus e la Virus Map per:

- Ottenere ulteriori informazioni su virus, messaggi di posta elettronica ingannevoli (hoax) e altre minacce più recenti.
- Ottenere strumenti gratuiti per la rimozione dei virus che facilitano la riparazione del computer.
- Ottenere una panoramica in tempo reale degli ultimi virus in circolazione a livello mondiale.

Per ottenere ulteriori informazioni sui virus

1. Nel menu avanzato, fare clic su **Strumenti**, quindi su **Informazioni sui virus**.
2. Effettuare una delle seguenti operazioni:
   - Ricercare i virus utilizzando la Libreria di informazioni sui virus gratuita di McAfee.
   - Ricercare i virus utilizzando la World Virus Map sul sito web di McAfee.

CAPITOLO 6

McAfee QuickClean

Durante la navigazione in Internet, sul computer si accumulano rapidamente file e dati inutili. QuickClean permette di proteggere la privacy e di eliminare i file superflui relativi a Internet e posta elettronica, identificando ed eliminando i file accumulati durante la navigazione, compresi i cookie, la posta elettronica, i download e la cronologia: file che possono contenere dati personali. QuickClean protegge la privacy assicurando l'eliminazione in modalità protetta delle informazioni riservate.

QuickClean consente inoltre di eliminare i programmi indesiderati, specificando i file da eliminare e rimuovendo i file non necessari, senza rimuovere le informazioni indispensabili.

In questo capitolo

Informazioni sulle funzioni di QuickClean

Questa sezione descrive le funzioni di QuickClean.

Funzioni

McAfee QuickClean fornisce un insieme di strumenti efficaci e facili da usare per rimuovere in modo sicuro i file non più necessari. È così possibile liberare prezioso spazio su disco e ottimizzare le prestazioni del computer.

CAPITOLO 7

Pulizia del computer

QuickClean consente di eliminare file e cartelle in tutta sicurezza.

Quando si naviga in Internet, il browser copia ciascuna pagina Internet e la grafica associata in una cartella cache sul disco, in modo da poterla poi caricare rapidamente in caso di nuova visita. La memorizzazione di file nella cache è utile se si visitano ripetutamente le stesse pagine Internet e il relativo contenuto non viene modificato di frequente. Quasi sempre, tuttavia, i file memorizzati nella cache sono inutili e quindi eliminabili.

È possibile eliminare diversi elementi mediante le operazioni di pulitura riportate di seguito.

- Pulitura del Cestino: esegue la pulitura del Cestino di Windows.
- Pulitura dei file temporanei: elimina i file memorizzati in cartelle temporanee.
- Pulitura dei collegamenti: elimina i collegamenti interrotti e quelli non associati a programmi.
- Pulitura dei frammenti di file persi: elimina dal computer i frammenti di file persi.
- Pulitura del registro di sistema: elimina le informazioni del registro di sistema di Windows relative ai programmi che non sono più installati nel computer.
- Pulitura della cache: elimina i file memorizzati nella cache accumulati durante la navigazione in Internet. I file di questo tipo vengono solitamente memorizzati come file temporanei di Internet.
- Pulitura dei cookie: elimina i cookie. I file di questo tipo vengono solitamente memorizzati come file temporanei di Internet.
  I cookie sono piccoli file che il browser Web registra sul computer in seguito alla richiesta di un server Web. Ogni volta che sul server Web viene visualizzata una pagina Web, il browser invia di nuovo il cookie al server. I cookie svolgono una funzione simile quella di un cartellino che consente al server Web di registrare quali pagine vengono visualizzate e con quale frequenza.
- Pulitura della cronologia del browser: elimina la cronologia del browser.
- Pulitura della posta di Outlook Express e Outlook (per posta eliminata e inviata): elimina la posta elettronica dalle cartelle Posta inviata e Posta eliminata di Outlook.

- Pulitura dei file utilizzati di recente: elimina i file utilizzati di recente e memorizzati sul computer, ad esempio i documenti di Microsoft Office.
- Pulitura di ActiveX e plug-in: elimina i controlli ActiveX e i plug-in.
  ActiveX è una tecnologia utilizzata per implementare controlli all'interno di un programma. Un controllo ActiveX è in grado di aggiungere un pulsante all'interfaccia di un programma. La maggior parte di questi controlli è innocua, tuttavia la tecnologia ActiveX potrebbe essere utilizzata per acquisire informazioni dal computer.
  I plug-in sono piccoli programmi software che si inseriscono in applicazioni di dimensioni maggiori per offrire ulteriori funzioni. I plug-in consentono al browser Web di accedere ai file incorporati nei documenti HTML il cui formato non verrebbe normalmente riconosciuto (ad esempio, file di animazione, audio e video) e, quindi, di eseguirli.
- Pulitura dei punti di ripristino configurazione di sistema: elimina dal computer i punti di ripristino configurazione di sistema obsoleti.

In questo capitolo

Uso di QuickClean

Questa sezione descrive come utilizzare QuickClean.

Pulitura del computer

È possibile eliminare file e cartelle inutilizzati, liberare spazio su disco e migliorare le prestazioni del computer.

Per eseguire la pulitura del computer:

1. Nel menu avanzato, fare clic su **Strumenti**.
2. Fare clic su **Manutenzione computer**, quindi su **Avvia** in **McAfee QuickClean**.
3. Effettuare una delle seguenti operazioni:
   - Scegliere **Avanti** per accettare le operazioni di pulitura predefinite visualizzate nell'elenco.
   - Selezionare o deselezionare le operazioni di pulitura appropriate e fare clic su **Avanti.** Per la pulitura dei file utilizzati di recente, è possibile fare clic su **Proprietà** per deselezionare i programmi i cui elenchi non verranno puliti.
   - Fare clic su **Ripristina impostazioni predefinite** per ripristinare le operazioni di pulitura predefinite, quindi su **Avanti**.
4. Al termine dell'analisi, scegliere **Avanti** per confermare l'eliminazione dei file. È possibile espandere questo elenco per visualizzare i file di cui verrà eseguita la pulitura con il relativo percorso.
5. Fare clic su **Avanti**.
6. Effettuare una delle seguenti operazioni:
   - Fare clic su **Avanti** per accettare l'opzione predefinita **Eliminare i file usando l'eliminazione standard di Windows**.
   - Fare clic su **Eliminare i file in modalità protetta utilizzando Shredder** e specificare il numero di tentativi. Non è possibile recuperare i file eliminati con Shredder.
7. Scegliere **Fine**.
8. In **Riepilogo di QuickClean**, è visualizzato il numero di file del registro di sistema eliminati e la quantità di spazio su disco recuperato dopo la pulitura Internet e del disco.

CAPITOLO 8

McAfee Shredder

I file eliminati possono essere recuperati dal computer anche dopo che il Cestino è stato svuotato. Quando si elimina un file, lo spazio occupato sull'unità disco viene contrassegnato da Windows come non più in uso, ma il file fisicamente esiste ancora. Grazie all'utilizzo di appositi strumenti informatici, è possibile recuperare dichiarazioni dei redditi, curricula professionali o altri documenti eliminati. Shredder protegge la privacy dell'utente eliminando in modo sicuro e definitivo i file indesiderati.

Per eliminare definitivamente un file, occorre sovrascriverlo ripetutamente con nuovi dati. Microsoft® Windows non elimina i file in modo sicuro in quanto ogni operazione sui file risulterebbe molto lenta. La distruzione di un documento non ne impedisce sempre il recupero poiché alcuni programmi creano copie temporanee nascoste dei documenti aperti. Se si distruggono solo i documenti visibili in Esplora risorse di Windows®, è possibile che ne esistano ancora delle copie temporanee.

Nota: il backup dei file distrutti non viene eseguito, pertanto non sarà possibile ripristinare i file eliminati da Shredder.

In questo capitolo

Informazioni sulle funzioni di Shredder

Questa sezione illustra le funzioni di Shredder.

Funzioni

Shredder consente di cancellare il contenuto del Cestino, i file temporanei di Internet, la cronologia dei siti Web, file, cartelle e dischi.

CAPITOLO 9

Cancellazione dei file indesiderati con Shredder

Shredder protegge la privacy del'utente eliminando in modo sicuro e definitivo i file indesiderati, ad esempio il contenuto del Cestino, i file temporanei di Internet e la cronologia dei siti Web. È possibile selezionare i file e le cartelle da distruggere oppure eseguire una ricerca.

In questo capitolo

Uso di Shredder

Questa sezione descrive le modalità di utilizzo di Shredder.

Distruzione di file, cartelle e dischi

I file possono continuare a risiedere nel computer anche dopo aver svuotato il Cestino. Tuttavia, una volta distrutti, i dati risultano definitivamente eliminati e gli hacker non possono accedervi.

Per distruggere file, cartelle e dischi:

1. Nel menu avanzato, fare clic su **Strumenti**, quindi su **Shredder**.
2. Effettuare una delle seguenti operazioni:
   - Fare clic su **Cancellare file e cartelle** per distruggere file e cartelle.
   - Fare clic su **Cancellare un intero disco** per distruggere il contenuto di un intero disco.
3. Selezionare uno dei seguenti livelli di distruzione:
   - **Rapido**: distrugge gli elementi selezionati utilizzando 1 solo passaggio.
   - **Completo**: distrugge gli elementi selezionati utilizzando 7 passaggi.
   - **Personalizzato**: distrugge gli elementi selezionati utilizzando 10 passaggi. Un numero più elevato di passaggi nel processo di distruzione rende più sicura l'eliminazione dei file.
4. Fare clic su **Avanti**.
5. Effettuare una delle seguenti operazioni:
   - Se si desidera distruggere file, fare clic su **Contenuto del Cestino**, **File temporanei Internet** o **Cronologia siti Web** nell'elenco **Selezionare i file da distruggere**. Se invece si desidera distruggere il contenuto di un disco, fare clic su di esso.
   - Fare clic su **Sfoglia**, individuare i file da distruggere e selezionarli.
   - Digitare il percorso dei file da distruggere nell'elenco **Selezionare i file da distruggere**.
6. Fare clic su **Avanti**.
7. Fare clic su **Fine** per completare l'operazione.
8. Fare clic su **Fine**.

CAPITOLO 10

McAfee Network Manager

McAfee® Network Manager rappresenta graficamente i computer e i componenti che costituiscono la rete domestica. Network Manager consente di eseguire il monitoraggio remoto dello stato di protezione di tutti i computer gestiti in rete e quindi di risolvere le vulnerabilità della protezione segnalate su di essi.

Prima di iniziare a utilizzare Network Manager, è possibile conoscerne alcune delle funzioni più comuni. La guida di Network Manager contiene dettagli sulla configurazione e sull'utilizzo di tali funzioni.

In questo capitolo

Funzioni

Network Manager offre le seguenti funzioni:

Mappa grafica della rete

La mappa della rete di Network Manager fornisce una panoramica grafica dello stato di protezione dei computer e dei componenti che costituiscono la rete domestica. Quando vengono apportate modifiche alla rete, ad esempio con l'aggiunta di un computer, la mappa della rete è in grado di riconoscerle. È possibile aggiornare la mappa della rete, rinominare la rete e mostrare o nascondere i componenti della mappa per personalizzare la visualizzazione. Possono inoltre essere visualizzati i dettagli associati a uno qualsiasi dei componenti mostrati sulla mappa della rete.

Gestione remota

Utilizzare la mappa della rete di Network Manager per gestire lo stato di protezione dei computer che costituiscono la rete domestica. È possibile invitare un computer a diventare membro della rete gestita, monitorare lo stato di protezione del computer gestito e risolvere le vulnerabilità conosciute della protezione da un computer remoto della rete.

Informazioni sulle icone di Network Manager

Nella seguente tabella sono descritte le icone di uso comune nella mappa della rete di Network Manager.

Icona	Descrizione
	Rappresenta un computer gestito in linea
	Rappresenta un computer gestito non in linea
	Rappresenta un computer non gestito su cui è installato il software di protezione McAfee 2007
	Rappresenta un computer non gestito e non in linea
	Rappresenta un computer in linea su cui non è installato il software di protezione McAfee 2007 oppure un dispositivo di rete sconosciuto
	Rappresenta un computer non in linea su cui non è installato il software di protezione McAfee 2007 oppure un dispositivo di rete sconosciuto e non in linea
	Indica che l'elemento corrispondente è protetto e connesso
	Indica che l'elemento corrispondente richiede l'attenzione dell'utente
	Indica che l'elemento corrispondente richiede l'attenzione dell'utente ed è disconnesso
	Rappresenta un router domestico senza fili
	Rappresenta un router domestico standard
	Rappresenta Internet, quando è stata effettuata la connessione
	Rappresenta Internet, quando non è stata effettuata la connessione

CAPITOLO 11

Impostazione di una rete gestita

Per impostare una rete gestita occorre organizzare gli elementi della mappa della rete e aggiungere membri (computer) alla rete.

In questo capitolo

Utilizzo della mappa della rete

Ogni volta che un computer si connette alla rete, Network Manager analizza lo stato della rete al fine di determinare se sono presenti eventuali membri (gestiti o non gestiti), gli attributi del router e lo stato di Internet. Se non viene rilevato alcun membro, Network Manager presume che il computer attualmente connesso sia il primo della rete, rendendolo automaticamente membro gestito con autorizzazioni di amministratore. Per impostazione predefinita, il nome della rete include il gruppo di lavoro o nome di dominio del primo computer che si connette alla rete e su cui è installato il software di protezione McAfee 2007. Tuttavia, è possibile rinominare la rete in qualsiasi momento.

Quando si apportano modifiche alla propria rete (ad esempio, mediante l'aggiunta di un computer), è possibile personalizzare la mappa della rete. Ad esempio, è possibile aggiornare la mappa della rete, rinominare la rete e mostrare o nascondere i componenti della mappa della rete per personalizzare la visualizzazione. Possono inoltre essere visualizzati i dettagli associati a uno qualsiasi dei componenti mostrati sulla mappa della rete.

Accesso alla mappa della rete

Per accedere alla mappa della propria rete occorre avviare Network Manager dall'elenco delle attività comuni di SecurityCenter. La mappa della rete rappresenta graficamente i computer e i componenti che costituiscono la rete domestica.

Per accedere alla mappa della rete:

- Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**.
  La mappa della rete viene visualizzata nel riquadro a destra.

Nota: Al primo accesso alla mappa della rete, prima della visualizzazione della mappa viene richiesto di impostare come affidabili gli altri computer della rete.

Aggiornamento della mappa della rete

È possibile aggiornare la mappa della rete in qualsiasi momento; ad esempio, dopo che un nuovo computer è diventato membro della rete gestita.

Per aggiornare la mappa della rete:

1. Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**.
   La mappa della rete viene visualizzata nel riquadro a destra.
2. Fare clic su **Aggiornare la mappa della rete** nella sezione **Desidero**.

Nota: il collegamento **Aggiornare la mappa della rete** è disponibile solo quando non è stato selezionato alcun elemento nella mappa della rete. Per deselezionare un elemento, fare clic sull'elemento selezionato oppure in un'area vuota della mappa della rete.

Ridenominazione della rete

Per impostazione predefinita, il nome della rete include il gruppo di lavoro o nome di dominio del primo computer che si connette alla rete e su cui è installato il software di protezione McAfee 2007. Se il nome non è appropriato è possibile modificarlo.

Per rinominare la rete:

1. Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**.
   La mappa della rete viene visualizzata nel riquadro a destra.
2. Fare clic su **Rinominare la rete** nella sezione **Desidero**.
3. Digitare il nome della rete nella casella **Rinomina rete**.
4. Fare clic su **OK**.

Nota: il collegamento **Rinomina rete** è disponibile solo quando non è stato selezionato alcun elemento nella mappa della rete. Per deselezionare un elemento, fare clic sull'elemento selezionato oppure in un'area vuota della mappa della rete.

Visualizzazione o non visualizzazione di elementi sulla mappa della rete

Per impostazione predefinita, nella mappa della rete sono visualizzati tutti i computer e i componenti della rete domestica. Tuttavia, se vi sono elementi nascosti, è possibile visualizzarli in qualsiasi momento. È possibile nascondere solo gli elementi non gestiti, ma non i computer gestiti.

Per...	Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**, quindi eseguire una delle seguenti operazioni.
Nascondere un elemento sulla mappa della rete	Fare clic su un elemento sulla mappa della rete, quindi su **Nascondere l'elemento** nella sezione **Desidero**. Nella finestra di dialogo di conferma, fare clic su **Sì**.
Mostrare elementi nascosti sulla mappa della rete	Nella sezione **Desidero**, fare clic su **Visualizzare gli elementi nascosti**.

Visualizzazione dei dettagli di un elemento

Per visualizzare informazioni dettagliate su qualsiasi componente in rete, selezionarne uno nella mappa della rete. Tra le informazioni disponibili sono inclusi il nome del componente, il relativo stato di protezione nonché altri dettagli richiesti per la gestione del componente.

Per visualizzare i dettagli di un elemento:

1. Fare clic sull'icona di un elemento sulla mappa della rete.
2. Nella sezione **Dettagli** è possibile visualizzare le informazioni sull'elemento.

Aggiunta alla rete gestita

Affinché un computer sia gestito in modalità remota oppure ottenga l'autorizzazione per la gestione remota di altri computer in rete, è necessario che diventi membro affidabile della rete. I nuovi computer vengono aggiunti alla rete dai membri della rete (computer) esistenti, dotati di autorizzazioni amministrative. Per garantire che vengano aggiunti alla rete solo i computer affidabili, gli utenti dei computer che concedono l'autorizzazione e quelli che la ricevono devono autenticarsi reciprocamente.

Quando un computer viene aggiunto alla rete, viene richiesto di esporne lo stato di protezione McAfee agli altri computer in rete. Se un computer accetta di esporre il proprio stato di protezione, esso diventerà un membro *gestito* della rete. Se un computer rifiuta di esporre il proprio stato di protezione, esso diventerà un membro *non gestito* della rete. I membri non gestiti della rete sono di solito computer guest che desiderano accedere ad altre funzioni della rete (ad esempio, la condivisione di file o stampanti).

Nota: se sono stati installati altri programmi di rete McAfee (ad esempio, McAfee Wireless Network Security o EasyNetwork), dopo l'aggiunta il computer verrà riconosciuto come computer gestito anche in tali programmi. Il livello di autorizzazione assegnato a un computer in Network Manager si applica a tutti i programmi di rete McAfee. Per ulteriori informazioni sul significato di autorizzazione guest, completa o con autorizzazioni amministrative in altri programmi di rete McAfee, consultare la relativa documentazione.

Aggiunta a una rete gestita

Quando si riceve un invito a diventare membro di una rete gestita, è possibile accettarlo o rifiutarlo. È anche possibile determinare se si desidera che il computer in uso e altri computer in rete eseguano il monitoraggio reciproco delle rispettive impostazioni di protezione (ad esempio, se i servizi di protezione da virus di un computer sono aggiornati).

Per diventare membro di una rete gestita:

1. Nella finestra di dialogo dell'invito, selezionare la casella di controllo **Consenti a questo e ad altri computer della rete di monitorare reciprocamente le rispettive impostazioni di protezione** per consentire ad altri computer della rete gestita di monitorare le impostazioni di protezione del proprio computer.
2. Fare clic su **Aggiungi**.
   Quando si accetta l'invito vengono visualizzate due carte da gioco.
3. Verificare che le carte da gioco siano uguali a quelle visualizzate sul computer che ha inviato l'invito a diventare membro della rete gestita.
4. Fare clic su **Conferma**.

Nota: se sul computer che ha inviato l'invito a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Diventare membro della rete può mettere a rischio il proprio computer; pertanto, fare clic su **Rifiuta** nella finestra di dialogo di conferma.

Invio a un computer di un invito a diventare membro della rete gestita

Se un computer viene aggiunto alla rete gestita oppure un altro computer non gestito è presente in rete, è possibile invitare tale computer a diventare membro della rete gestita. Solo i computer con autorizzazioni amministrative in rete possono invitare altri computer a diventare membri della rete. Quando si invia l'invito, occorre inoltre specificare il livello di autorizzazione che si desidera assegnare al computer aggiunto.

Per invitare un computer a diventare membro della rete gestita:

1. Fare clic sull'icona del computer non gestito nella mappa della rete.
2. Fare clic su **Monitorare il computer** nella sezione **Desidero**.
3. Nella finestra di dialogo Invita un computer a diventare membro della rete gestita, fare clic su una delle seguenti opzioni:
   - **Concedi accesso Guest**
     L'accesso Guest consente al computer di accedere alla rete.
   - **Concedi accesso completo a tutte le applicazioni della rete gestita**
     L'accesso completo (come l'accesso Guest) consente al computer di accedere alla rete.
   - **Concedi accesso con privilegi di amministratore a tutte le applicazioni della rete gestita**
     L'accesso con privilegi di amministratore consente al computer di accedere alla rete con privilegi di amministratore. Consente inoltre al computer di concedere l'accesso ad altri computer che desiderano diventare membri della rete gestita.

4 Fare clic su **Invita**.
Al computer viene inviato un invito a diventare membro della rete gestita. Quando il computer accetta l'invito vengono visualizzate due carte da gioco.

5 Verificare che le carte da gioco siano uguali a quelle visualizzate sul computer invitato a diventare membro della rete gestita.

6 Fare clic su **Consenti accesso**.

Nota: se sul computer invitato a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Consentire al computer di diventare membro della rete può mettere a rischio altri computer; pertanto, fare clic su **Rifiuta accesso** nella finestra di dialogo di conferma.

Impostazione di computer in rete come non affidabili

Se per errore si è accettato di considerare affidabili altri computer in rete, è possibile considerarli come non affidabili.

Per negare l'affidabilità a computer in rete:

- Fare clic su **Non considerare affidabili i computer su questa rete** nella sezione **Desidero**.

Nota: il collegamento **Non considerare affidabili i computer su questa rete** è disponibile solo quando nessun altro computer gestito è diventato membro della rete.

CAPITOLO 12

Gestione remota della rete

Dopo aver impostato la rete gestita, è possibile utilizzare Network Manager per la gestione remota dei computer e dei componenti che costituiscono la rete. È possibile eseguire il monitoraggio dello stato e dei livelli di autorizzazione del computer e dei componenti, nonché risolvere le vulnerabilità della protezione in modalità remota.

In questo capitolo

Monitoraggio dello stato e delle autorizzazioni

Una rete gestita prevede due tipi di membri: membri gestiti e membri non gestiti. I membri gestiti, diversamente da quelli non gestiti, consentono agli altri computer in rete di monitorare lo stato della protezione McAfee. I membri non gestiti sono di solito computer guest che desiderano accedere ad altre funzioni della rete (ad esempio, la condivisione di file o stampanti). Un computer gestito in rete può invitare un computer non gestito a diventare un computer gestito in qualsiasi momento. In maniera simile, un computer gestito può diventare non gestito in qualsiasi momento.

Ai computer gestiti sono associate autorizzazioni amministrative, complete o Guest. Le autorizzazioni amministrative consentono al computer gestito di amministrare lo stato di protezione di tutti gli altri computer gestiti in rete, nonché di concedere agli altri computer di diventare membri della rete. Le autorizzazioni complete e Guest consentono a un computer solo di accedere alla rete. È possibile modificare il livello di autorizzazione di un computer in qualsiasi momento.

Poiché una rete gestita può comprendere anche dei dispositivi (ad esempio i router), è possibile gestire anche questi ultimi mediante Network Manager. È inoltre possibile configurare e modificare le proprietà di visualizzazione di un dispositivo sulla mappa della rete.

Monitoraggio dello stato della protezione di un computer

Se lo stato della protezione del computer non è monitorato sulla rete (perché il computer non è membro della rete oppure è un membro non gestito della rete), è possibile inviare una richiesta di monitoraggio.

Per monitorare lo stato della protezione di un computer:

1. Fare clic sull'icona del computer non gestito nella mappa della rete.
2. Fare clic su **Monitorare il computer** nella sezione **Desidero**.

Interruzione del monitoraggio dello stato della protezione di un computer

È possibile interrompere il monitoraggio dello stato della protezione di un computer gestito nella rete privata, che diventa quindi un computer non gestito.

Per interrompere il monitoraggio dello stato della protezione di un computer:

1. Fare clic sull'icona del computer gestito nella mappa della rete.
2. Fare clic su **Interrompere il monitoraggio del computer** nella sezione **Desidero**.
3. Nella finestra di dialogo di conferma, fare clic su **Sì**.

Modifica delle autorizzazioni di un computer gestito

È possibile modificare le autorizzazioni di un computer gestito in qualsiasi momento. Ciò consente di stabilire quali computer possono monitorare lo stato della protezione (impostazioni di protezione) di altri computer della rete.

Per modificare le autorizzazioni di un computer gestito:

1. Fare clic sull'icona del computer gestito nella mappa della rete.
2. Fare clic su **Modificare i permessi per il computer** nella sezione **Desidero**.
3. Nella finestra di dialogo di modifica dei permessi, selezionare o deselezionare la casella di controllo per determinare se il computer selezionato e altri computer sulla rete gestita possono monitorare reciprocamente il rispettivo stato della protezione.
4. Fare clic su **OK**.

Gestione di una periferica

È possibile gestire una periferica eseguendo l'accesso alla relativa pagina Web di amministrazione in Network Manager.

Per gestire una periferica:

1. Fare clic sull'icona di una periferica nella mappa della rete.
2. Fare clic su **Gestire la periferica** nella sezione **Desidero**. Il browser Web verrà aperto e verrà visualizzata la pagina Web di amministrazione della periferica.
3. Nel browser Web, fornire i dati di accesso e configurare le impostazioni di protezione della periferica.

Nota: se la periferica è un router o un punto di accesso senza fili protetto con Wireless Network Security, per configurare le impostazioni di protezione della periferica è necessario utilizzare Wireless Network Security.

Modifica delle proprietà di visualizzazione di una periferica

Quando si modificano le proprietà di visualizzazione di una periferica è possibile modificare il nome della periferica visualizzato e specificare se si tratta di un router senza fili.

Per modificare le proprietà di visualizzazione di una periferica:

1. Fare clic sull'icona di una periferica nella mappa della rete.
2. Fare clic su **Modificare le proprietà della periferica** nella sezione **Desidero**.
3. Per specificare il nome della periferica visualizzato, digitare un nome nella casella **Nome**.
4. Per specificare il tipo di periferica, fare clic su una delle seguenti opzioni:
   - **Router**
     Rappresenta un router domestico standard.
   - **Router wireless**
     Rappresenta un router domestico senza fili.
5. Fare clic su **OK**.

Risoluzione delle vulnerabilità della protezione

I computer gestiti con autorizzazioni con privilegi di amministratore possono monitorare lo stato della protezione McAfee di altri computer gestiti sulla rete e risolvere eventuali vulnerabilità segnalate in modalità remota. Ad esempio, se lo stato della protezione McAfee di un computer gestito indica che VirusScan è disattivato, un altro computer gestito con autorizzazioni con privilegi di amministratore può *risolvere* la vulnerabilità della protezione attivando VirusScan in modalità remota.

Quando si risolvono le vulnerabilità della protezione in modalità remota, Network Manager ripara automaticamente gran parte dei problemi segnalati. Tuttavia, alcune vulnerabilità della protezione potrebbero richiedere un intervento manuale sul computer locale. In tal caso, Network Manager corregge i problemi che è possibile riparare in modalità remota, quindi richiede all'utente di risolvere i restanti problemi effettuando l'accesso a SecurityCenter sul computer vulnerabile e attenendosi ai suggerimenti forniti. In alcuni casi, per correggere il problema si suggerisce di installare il software di protezione McAfee 2007 sul computer remoto o sui computer in rete.

Risoluzione delle vulnerabilità della protezione

È possibile utilizzare Network Manager per risolvere automaticamente gran parte delle vulnerabilità della protezione sui computer gestiti remoti. Ad esempio, se VirusScan è disattivato su un computer remoto, è possibile utilizzare Network Manager per attivarlo automaticamente.

Per risolvere le vulnerabilità della protezione:

1. Fare clic sull'icona di un elemento sulla mappa della rete.
2. Visualizzare lo stato della protezione dell'elemento nella sezione **Dettagli**.
3. Fare clic su **Risolvere vulnerabilità della protezione** nella sezione **Desidero**.
4. Dopo aver risolto i problemi di protezione, fare clic su **OK**.

Nota: benché Network Manager risolva automaticamente gran parte delle vulnerabilità della protezione, per l'esecuzione di alcune operazioni potrebbe essere necessario avviare SecurityCenter sul computer vulnerabile e attenersi ai suggerimenti forniti.

Installazione del software di protezione McAfee sui computer remoti

Se su uno o più computer in rete non è in esecuzione il software di protezione McAfee 2007, non è possibile monitorare in modalità remota il rispettivo stato della protezione. Se si desidera monitorare questi computer in modalità remota, è necessario installare il software di protezione McAfee su ciascuno di essi.

Per installare il software di protezione McAfee su un computer remoto:

1. Nel browser del computer remoto andare all'indirizzo http://download.mcafee.com/us/.
2. Seguire le istruzioni visualizzate per installare il software di protezione McAfee 2007 sul computer.

CAPITOLO 13

McAfee VirusScan

VirusScan offre la protezione più completa, affidabile e aggiornata contro virus e spyware. Basato sulla notissima tecnologia di scansione di McAfee, VirusScan protegge da virus, worm, trojan horse, script sospetti, rootkit, sovraccarichi del buffer, attacchi ibridi, spyware, programmi potenzialmente indesiderati e altre minacce.

In questo capitolo

Funzioni

Nella presente versione di VirusScan sono disponibili le seguenti funzioni.

Protezione da virus

Analisi dei file in tempo reale quando l'utente o il computer vi accede.

Scansione

Ricerca di virus e altre minacce presenti nei dischi rigidi, nei dischi floppy e in singoli file e cartelle. Per eseguire la scansione di un elemento è anche possibile fare clic con il pulsante destro del mouse sull'elemento stesso.

Rilevamento di programmi spyware e adware

VirusScan identifica e rimuove spyware, adware e altri programmi che possono mettere a rischio la privacy e rallentare le prestazioni del computer.

Aggiornamenti automatici

Gli aggiornamenti automatici proteggono il computer dalle più recenti minacce identificate e non identificate.

Scansione rapida in background

Veloci scansioni identificano e distruggono in modalità silenziosa virus, trojan horse, worm, spyware, adware, dialer e altre minacce senza interrompere il lavoro dell'utente.

Avvisi di protezione in tempo reale

Gli avvisi di protezione avvertono l'utente della diffusione di virus e di minacce per la protezione, fornendo opzioni di risposta che consentono di rimuovere, neutralizzare o conoscere meglio la minaccia.

Rilevamento e pulizia in più punti di accesso

VirusScan esegue il monitoraggio e la pulizia nei principali punti di accesso del computer: messaggi di posta elettronica, allegati di messaggi immediati e download di Internet.

Monitoraggio della posta elettronica per attività di tipo worm

WormStopper™ impedisce ai trojan di diffondere i worm in altri computer tramite posta elettronica e avvisa l'utente prima che programmi di posta elettronica sconosciuti possano inviare messaggi ad altri computer.

Monitoraggio degli script per attività di tipo worm

ScriptStopper™ blocca l'esecuzione di script noti e dannosi sul computer.

McAfee X-Ray for Windows

McAfee X-Ray rileva ed elimina i rootkit e altri programmi non rilevati da Windows.

Protezione dal sovraccarico del buffer

Protegge contro i sovraccarichi del buffer. I sovraccarichi del buffer si verificano quando programmi o processi sospetti tentano di memorizzare in un buffer (area di memorizzazione temporanea dei dati) del computer una quantità di dati superiore al limite consentito, causando il danneggiamento o la sovrascrittura di dati validi presenti nei buffer adiacenti.

McAfee SystemGuards

I moduli SystemGuard esaminano comportamenti specifici del computer che possono segnalare la presenza di virus, spyware o attività di hacker.

CAPITOLO 14

Gestione della protezione da virus

È possibile gestire la protezione in tempo reale contro virus, spyware, e script nonché i moduli SystemGuard. Ad esempio, è possibile disattivare la scansione o specificare l'elemento di cui si desidera eseguire la scansione.

Solo gli utenti con privilegi di amministratore possono modificare le opzioni avanzate.

In questo capitolo

Uso della protezione da virus

Quando viene avviata, la protezione da virus (scansione in tempo reale) controlla costantemente il computer per rilevare eventuali attività di virus. La scansione in tempo reale sottopone a scansione i file ogni volta che l'utente o il computer vi accede. Quando la protezione da virus rileva un file infetto, tenta di pulirlo o di rimuovere l'infezione. Se risulta impossibile pulire o rimuovere un file, un avviso richiede all'utente di intraprendere ulteriori azioni.

Argomenti correlati

- Informazioni sugli avvisi di protezione (pagina 105)

Disattivazione della protezione da virus

Se si disattiva la protezione da virus, il computer non verrà più tenuto costantemente sotto controllo alla ricerca di eventuali attività di virus. Se è necessario arrestare la protezione da virus, accertarsi di non essere connessi a Internet.

Nota: la disattivazione della protezione da virus implica anche l'interruzione della protezione in tempo reale della posta elettronica, della messaggistica immediata e contro i programmi spyware.

Per disattivare la protezione da virus:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione da virus**, fare clic su **Disattiva**.
4. Nella finestra di dialogo di conferma, effettuare una delle seguenti operazioni:
   - Per riavviare la protezione da virus dopo un intervallo di tempo specificato, selezionare la casella di controllo **Riattiva la scansione in tempo reale dopo** e selezionare un intervallo dal menu.
   - Per impedire il riavvio della protezione da virus dopo un intervallo specificato, deselezionare la casella di controllo **Riattiva protezione da virus dopo**.

5 Fare clic su **OK**.

Se è stato configurato l'avvio della protezione in tempo reale all'avvio di Windows, il computer sarà protetto quando viene riavviato.

Argomenti correlati

- Configurazione della protezione in tempo reale (pagina 76)

Attivazione della protezione da virus

La protezione da virus controlla costantemente il computer per rilevare la presenza di eventuali attività di virus.

Per attivare la protezione da virus:

1 Nel menu avanzato, fare clic su **Configura**.

2 Nel riquadro Configura, fare clic su **Computer e file**.

3 In **Protezione da virus**, fare clic su **Attiva**.

Configurazione della protezione in tempo reale

È possibile modificare la protezione da virus in tempo reale. Ad esempio, è possibile eseguire la scansione solo di programmi e documenti oppure disattivare la scansione in tempo reale all'avvio di Windows (non consigliato).

Configurazione della protezione in tempo reale

È possibile modificare la protezione da virus in tempo reale. Ad esempio, è possibile eseguire la scansione solo di programmi e documenti oppure disattivare la scansione in tempo reale all'avvio di Windows (non consigliato).

Per configurare la protezione in tempo reale:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione da virus**, fare clic su **Avanzate**.
4. Selezionare o deselezionare le seguenti caselle di controllo:
   - **Ricerca di virus sconosciuti con tecnologia euristica**: i file vengono confrontati con le firme di virus noti allo scopo di rilevare tracce di virus non identificati. Questa opzione fornisce la scansione più accurata, ma in genere è più lenta di una scansione normale.
   - **Esegui scansione su unità floppy al momento dell'arresto**: quando si arresta il computer, viene eseguita la scansione dell'unità floppy.
   - **Ricerca di programmi spyware e programmi potenzialmente indesiderati**: vengono rilevati e rimossi spyware, adware e altri programmi che possono raccogliere e trasmettere dati senza l'autorizzazione dell'utente.
   - **Cerca e rimuovi cookie traccianti**: vengono rilevati e rimossi i cookie che possono raccogliere e trasmettere dati senza l'autorizzazione dell'utente. Un cookie identifica gli utenti quando visitano una pagina Web.
   - **Esegui scansione su unità di rete**: viene eseguita la scansione delle unità di rete connesse.
   - **Attiva protezione dal sovraccarico del buffer**: le attività di sovraccarico del buffer eventualmente rilevate vengono bloccate e l'utente viene avvisato.
   - **Avvio scansione in tempo reale all'avvio di Windows (consigliato)**: la protezione in tempo reale viene attivata ad ogni avvio del computer, anche quando viene spento per una sessione.

5 Fare clic su uno dei seguenti pulsanti:

- **Tutti i file (consigliato)**: viene eseguita la scansione di tutti i tipi di file utilizzati dal computer. Questa opzione offre la scansione più accurata.
- **Solo file di programma e documenti**: viene eseguita la scansione esclusivamente di file di programma e documenti.

6 Fare clic su **OK**.

Uso della protezione da spyware

La protezione da spyware rileva e rimuove spyware, adware e altri programmi potenzialmente indesiderati che raccolgono e trasmettono dati senza l'autorizzazione dell'utente.

Disattivazione della protezione da spyware

Se si disattiva la protezione da spyware, i programmi potenzialmente indesiderati che raccolgono e trasmettono dati senza l'autorizzazione dell'utente non verranno rilevati.

Per disattivare la protezione da spyware:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione da spyware**, fare clic su **Disattiva**.

Attivazione della protezione da spyware

La protezione da spyware rileva e rimuove spyware, adware e altri programmi potenzialmente indesiderati che raccolgono e trasmettono dati senza l'autorizzazione dell'utente.

Per attivare la protezione da spyware:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer & file**.
3. In **Protezione da spyware**, fare clic su **Attiva**.

Uso di SystemGuards

I moduli SystemGuard rilevano le modifiche potenzialmente non autorizzate apportate al computer e le segnalano all'utente. È quindi possibile esaminare le modifiche e decidere se consentirle.

La classificazione dei moduli SystemGuard è riportata di seguito.

Programmi

I SystemGuard programmi rilevano le modifiche apportate ai file di avvio, alle estensioni e ai file di configurazione.

Windows

I SystemGuard Windows rilevano le modifiche apportate alle impostazioni di Internet Explorer, inclusi gli attributi del browser e le impostazioni di protezione.

Browser

I SystemGuard browser rilevano le modifiche apportate a servizi, certificati e file di configurazione di Windows .

Disattivazione dei moduli SystemGuard

Se si disattivano i moduli SystemGuard, le modifiche al computer potenzialmente non autorizzate non verranno rilevate.

Per disattivare tutti i moduli SystemGuard:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione SystemGuard**, fare clic su **Disattiva**.

Attivazione dei moduli SystemGuard

I moduli SystemGuard rilevano le modifiche potenzialmente non autorizzate apportate al computer e le segnalano all'utente.

Per attivare i moduli SystemGuard:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione SystemGuard**, fare clic su **Attiva**.

Configurazione dei moduli SystemGuard

È possibile modificare i moduli SystemGuard. Per ciascuna modifica rilevata, è possibile decidere se ricevere avvisi e registrare l'evento, registrare solo l'evento o disattivare il modulo SystemGuard.

Configurazione dei moduli SystemGuard

È possibile modificare i moduli SystemGuard. Per ciascuna modifica rilevata, è possibile decidere se ricevere avvisi e registrare l'evento, registrare solo l'evento o disattivare il modulo SystemGuard.

Per configurare i moduli SystemGuard:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione SystemGuard**, fare clic su **Avanzate**.
4. Nell'elenco dei moduli SystemGuard, selezionare una categoria per visualizzare l'elenco dei moduli associati e il relativo stato.
5. Fare clic sul nome di un modulo SystemGuard.
6. Le informazioni sul modulo SystemGuard vengono visualizzate in **Dettagli**.
7. In **Desidero**, effettuare una delle seguenti operazioni:
   - Fare clic su **Mostra avvisi** se si desidera essere avvisati quando viene apportata una modifica e registrare un evento.
   - Fare clic su **Registra solo le modifiche** se non si desidera che sia intrapresa un'azione al rilevamento di una modifica. La modifica verrà solo registrata.
   - Fare clic su **Disattiva SystemGuard** per disattivare il modulo SystemGuard. Quando viene apportata una modifica, non verrà emesso alcun avviso e l'evento non verrà registrato.
8. Fare clic su **OK**.

Informazioni sui moduli SystemGuard

I moduli SystemGuard rilevano le modifiche potenzialmente non autorizzate apportate al computer e le segnalano all'utente. È quindi possibile esaminare le modifiche e decidere se consentirle.

La classificazione dei moduli SystemGuard è riportata di seguito.

Programmi

I SystemGuard programmi rilevano le modifiche apportate ai file di avvio, alle estensioni e ai file di configurazione.

Windows

I SystemGuard Windows rilevano le modifiche apportate alle impostazioni di Internet Explorer, inclusi gli attributi del browser e le impostazioni di protezione.

Browser

I SystemGuard browser rilevano le modifiche apportate a servizi, certificati e file di configurazione di Windows ∃.

Informazioni sui SystemGuard programmi

I SystemGuard programmi rilevano gli elementi riportati di seguito.

Installazione di ActiveX

Vengono rilevati i programmi ActiveX scaricati mediante Internet Explorer. I programmi ActiveX vengono scaricati dai siti Web e memorizzati sul computer in C:\Windows\Downloaded Program Files o in C:\Windows\Temp\Temporary Internet Files. Il CLSID (una stringa composta di numeri e lettere compresi fra parentesi graffe) di tali programmi viene inoltre memorizzato nel registro di sistema.

Internet Explorer utilizza molti programmi ActiveX legittimi. Se non si è certi di un programma ActiveX, è possibile eliminarlo senza danneggiare il computer. Nel caso in cui il programma sia nuovamente necessario, Internet Explorer lo scaricherà automaticamente al successivo accesso a un sito Web che lo richiede.

Elementi di avvio

Viene eseguito il monitoraggio delle modifiche apportate alle chiavi di avvio del registro di sistema e alle cartelle di avvio. Le chiavi di avvio del registro di sistema di Windows e le cartelle di avvio nel menu Start memorizzano i percorsi di programmi presenti sul computer. I programmi memorizzati in questi percorsi vengono caricati all'avvio di Windows. I programmi spyware o potenzialmente indesiderati tentano spesso di essere inclusi nell'elenco dei programmi caricati all'avvio di Windows.

Hook di esecuzione della shell di Windows

Viene eseguito il monitoraggio delle modifiche apportate all'elenco di programmi che vengono caricati in explorer.exe. Un hook di esecuzione della shell è un programma caricato nella shell Windows di explorer.exe. Un hook di esecuzione della shell riceve tutti i comandi di esecuzione utilizzati su un computer. I programmi caricati nella shell di explorer.exe sono in grado di eseguire operazioni aggiuntive prima dell'avvio di altri programmi. I programmi spyware o potenzialmente indesiderati possono utilizzare gli hook di esecuzione della shell per impedire l'esecuzione dei programmi di protezione.

Chiave ShellServiceObjectDelayLoad

Viene eseguito il monitoraggio dei file elencati nella chiave ShellServiceObjectDelayLoad, che vengono caricati da explorer.exe all'avvio del computer. Poiché explorer.exe è la shell del computer, esso viene sempre avviato e carica i file elencati in questa chiave. I file vengono caricati nella fase iniziale del processo di avvio, prima di qualsiasi intervento da parte dell'utente.

Informazioni sui SystemGuard Windows

I SystemGuard Windows rilevano gli elementi riportati di seguito.

Gestori dei menu di scelta rapida

Viene impedita la modifica non autorizzata ai menu di scelta rapida di Windows. I menu di scelta rapida consentono di fare clic su un file con il pulsante destro del mouse e di eseguire azioni specifiche in relazione a quel file.

DLL AppInit

Viene impedita la modifica o l'aggiunta non autorizzata di DLL AppInit di Windows. Il valore del registro AppInit_DLLs contiene un elenco di file che vengono caricati al momento del caricamento di user32.dll. I file presenti nel valore AppInit_DLLs vengono caricati nella fase iniziale della routine di avvio di Windows, quando è possibile che una DLL potenzialmente pericolosa si nasconda prima di qualsiasi intervento da parte dell'utente.

File Hosts di Windows

Viene eseguito il monitoraggio delle modifiche apportate al file Hosts del computer. Il file Hosts viene utilizzato per reindirizzare determinati nomi di dominio a indirizzi IP specifici. Ad esempio, se si desidera visitare il sito www.esempio.com, il browser controlla il file Hosts e, se individua una voce per il nome host www.esempio.com, stabilisce una connessione all'indirizzo IP ad esso associato. Alcuni programmi spyware tentano di modificare il file Hosts allo scopo di reindirizzare il browser a siti diversi da quelli desiderati o di impedire l'aggiornamento corretto del software.

Shell di Winlogon

Viene eseguito il monitoraggio della shell di Winlogon. La shell viene caricata quando un utente effettua l'accesso a Windows e costituisce l'interfaccia utente (UI, User Interface) principale utilizzata per la gestione di Windows. La shell corrisponde di solito a Esplora risorse di Windows (explorer.exe). Tuttavia, è possibile modificare facilmente il programma cui la shell di Windows fa riferimento. In questo caso, ad ogni accesso da parte di un utente verrà avviato un programma diverso dalla shell di Windows.

Chiave UserInit di Winlogon

Viene eseguito il monitoraggio delle modifiche apportate alle impostazioni utente relative all'accesso a Windows. Nella chiave HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit è specificato il programma da avviare in seguito all'accesso a Windows da parte di un un utente. Il programma predefinito ripristina il profilo, i caratteri, i colori e le altre impostazioni associate al proprio nome utente. I programmi spyware e altri programmi potenzialmente indesiderati possono tentare di avviarsi aggiungendosi a questa chiave.

Protocolli Windows

Viene eseguito il monitoraggio delle modifiche apportate ai protocolli di rete in uso. Alcuni programmi spyware o potenzialmente indesiderati assumono il controllo di alcune modalità di invio e ricezione di informazioni da parte del computer. Ciò avviene mediante filtri e gestori dei protocolli di Windows.

Layered Service Provider di Winsock

Viene eseguito il monitoraggio degli LSP (Layered Service Providers), che possono intercettare i dati sulla rete e modificarli o reindirizzarli. I Layered Service Provider legittimi includono il software del controllo genitori, i firewall e altri programmi di protezione. I programmi spyware possono utilizzare i Layered Service Provider per il monitoraggio dell'attività in Internet e la modifica dei dati dell'utente. Per evitare la reinstallazione del sistema operativo, utilizzare i programmi McAfee per rimuovere automaticamente i programmi spyware e gli Layered Service Provider compromessi.

Comandi Apri della shell di Windows

Viene impedita la modifica dei comandi Apri della shell di Windows (explorer.exe). Tali comandi consentono l'esecuzione di programmi specifici al momento dell'esecuzione di determinati tipi di file. Ad esempio, un worm può tentare di avviarsi ogni volta che viene eseguita un'applicazione con estensione exe.

Utilità di pianificazione condivisa

Viene eseguito il monitoraggio della chiave di registro SharedTaskScheduler, contenente un elenco di programmi che vengono eseguiti all'avvio di Windows. Alcuni programmi spyware o potenzialmente indesiderati modificano questa chiave e si aggiungono all'elenco senza autorizzazione.

Windows Messenger Service

Viene eseguito il monitoraggio di Windows Messenger Service, una funzionalità non documentata di Windows Messenger che consente l'invio di messaggi popup. Alcuni programmi spyware o potenzialmente indesiderati tentano di attivare il servizio e di inviare pubblicità non richieste. Il servizio può essere inoltre sfruttato per eseguire codice in remoto utilizzando una vulnerabilità conosciuta.

File Win.ini di Windows

Il file win.ini è un file di testo che fornisce un elenco di programmi da eseguire all'avvio di Windows. La sintassi di caricamento di tali programmi è specificata nel file allo scopo di supportare precedenti versioni di Windows. La maggior parte dei programmi non utilizza il file win.ini per caricare i programmi, tuttavia, alcuni programmi spyware o potenzialmente indesiderati sono progettati in modo tale da sfruttare tale sintassi e sono in grado di caricarsi durante l'avvio di Windows.

Informazioni sui SystemGuard browser

I SystemGuard browser rilevano gli elementi riportati di seguito.

Oggetti browser helper

Viene eseguito il monitoraggio delle aggiunte apportate agli oggetti browser helper. Gli oggetti browser helper sono programmi che si comportano come plug-in di Internet Explorer. I programmi spyware e gli hijacker spesso utilizzano tali oggetti per visualizzare pubblicità o monitorare le abitudini di navigazione. Gli oggetti browser helper vengono inoltre utilizzati da molti programmi legittimi, ad esempio dalle comuni barre degli strumenti di ricerca.

Barre di Internet Explorer

Vengono monitorate le modifiche apportate all'elenco dei programmi delle barre di Internet Explorer. Le barre di Explorer, ad esempio Cerca, Preferiti o Cronologia, sono riquadri visualizzati in Internet Explorer (IE) o Esplora risorse di Windows.

Plug-in di Internet Explorer

Viene impedito ai programmi spyware di installare plug-in di Internet Explorer, componenti software aggiuntivi che vengono caricati all'avvio di Internet Explorer. I programmi spyware utilizzano spesso i plug-in di Internet Explorer per visualizzare pubblicità o monitorare le abitudini di navigazione. I plug-in legittimi aggiungono funzionalità a Internet Explorer.

ShellBrowser di Internet Explorer

Viene eseguito il monitoraggio delle modifiche apportate all'istanza del componente ShellBrowser di Internet Explorer. Il componente ShellBrowser di Internet Explorer contiene informazioni e impostazioni relative a un'istanza di Internet Explorer. Se tali impostazioni vengono modificate o viene aggiunto un nuovo componente ShellBrowser, il componente ShellBrowser può assumere il controllo completo di Internet Explorer, aggiungendo funzionalità come barre degli strumenti, menu e pulsanti.

WebBrowser di Internet Explorer

Viene eseguito il monitoraggio delle modifiche apportate all'istanza del componente WebBrowser di Internet Explorer. Tale componente contiene informazioni e impostazioni relative a un'istanza di Internet Explorer. Se tali impostazioni vengono modificate o viene aggiunto un nuovo componente WebBrowser, il componente WebBrowser può assumere il controllo completo di Internet Explorer, aggiungendo funzionalità come barre degli strumenti, menu e pulsanti.

Hook di ricerca URL di Internet Explorer

Viene eseguito il monitoraggio delle modifiche apportate all'hook di ricerca degli URL di Internet Explorer. L'hook di ricerca degli URL viene utilizzato quando si digita un indirizzo nell'apposito campo del browser senza indicare un protocollo, ad esempio http:// o ftp://. Quando si immette un indirizzo di quel tipo, il browser può utilizzare l'hook di ricerca per individuare il percorso immesso su Internet.

URL di Internet Explorer

Viene eseguito il monitoraggio delle modifiche apportate agli URL preimpostati in Internet Explorer per impedire che programmi spyware o altri programmi potenzialmente indesiderati modifichino le impostazioni del browser senza autorizzazione.

Restrizioni di Internet Explorer

Viene eseguito il monitoraggio delle restrizioni di Internet Explorer, che consentono all'amministratore di un computer di impedire la modifica della home page o di altre opzioni in Internet Explorer. Tali opzioni appaiono solo per impostazione esplicita da parte dell'amministratore.

Aree di protezione di Internet Explorer

Viene eseguito il monitoraggio delle aree di protezione di Internet Explorer. Internet Explorer dispone di quattro aree di protezione predefinite: Internet, Intranet locale, Siti attendibili e Siti con restrizioni. A ciascuna area di protezione sono associate impostazioni di protezione specifiche, predefinite o personalizzate. Le aree di protezione costituiscono il bersaglio di alcuni programmi spyware o potenzialmente indesiderati perché l'abbassamento del livello di protezione consente a questi programmi di evitare la visualizzazione di avvisi di protezione e di agire senza essere rilevati.

Siti attendibili di Internet Explorer

Viene eseguito il monitoraggio dei siti attendibili di Internet Explorer. L'elenco dei siti attendibili è un elenco di siti Web che sono stati definiti tali. Alcuni programmi spyware o potenzialmente indesiderati utilizzano questo elenco poiché fornisce un metodo per impostare come attendibili siti sospetti senza l'autorizzazione dell'utente.

Criterio di Internet Explorer

Viene eseguito il monitoraggi dei criteri di Internet Explorer Le impostazioni dei criteri di Internet Explorer vengono in genere modificate dagli amministratori di sistema, ma possono essere sfruttate dai programmi spyware. Le modifiche possono impedire l'impostazione di una home page diversa o possono nascondere le schede nella finestra di dialogo Opzioni Internet del menu Strumenti.

Uso della scansione script

Uno script consente di creare, copiare o eliminare dei file, nonché di aprire il registro di sistema di Windows.

La scansione script blocca automaticamente l'esecuzione di script noti e dannosi sul computer.

Disattivazione della scansione script

Se si disattiva la scansione script, le operazioni sospette di esecuzione di script non verranno rilevate.

Per disattivare la scansione script:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione con scansione script**, fare clic su **Disattiva**.

Attivazione della scansione script

Durante la scansione script viene visualizzato un avviso quando l'esecuzione di uno script determina la creazione, la copia o l'eliminazione di file oppure l'apertura del registro di sistema di Windows.

Per attivare la scansione script:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione con scansione script**, fare clic su **Attiva**.

Uso della protezione della posta elettronica

La protezione della posta elettronica rileva e blocca le minacce contenute nei messaggi di posta elettronica in arrivo (POP3) e in uscita (SMTP) e negli allegati, tra cui virus, trojan, worm, spyware, adware e altre minacce.

Disattivazione della protezione della posta elettronica

Se si disattiva la protezione della posta elettronica, non verranno rilevate le potenziali minacce contenute nei messaggi di posta elettronica in arrivo (POP3) e in uscita (SMTP) e negli allegati.

Per disattivare la protezione della posta elettronica:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.
3. In **Protezione della posta elettronica**, fare clic su **Disattiva**.

Attivazione della protezione della posta elettronica

La protezione della posta elettronica rileva le minacce contenute nei messaggi di posta elettronica in arrivo (POP3) e in uscita (SMTP) e negli allegati.

Per attivare la protezione della posta elettronica:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.
3. In **Protezione della posta elettronica**, fare clic su **Attiva**.

Configurazione della protezione della posta elettronica

Le opzioni di protezione dei messaggi di posta elettronica consentono di sottoporre a scansione i messaggi di posta in arrivo, in uscita e i worm. I worm si replicano e consumano risorse del sistema, rallentando le prestazioni o interrompendo le attività. I worm possono inviare copie di sé stessi mediante la posta elettronica. Ad esempio, possono tentare di inoltrare messaggi di posta elettronica agli utenti presenti nella rubrica.

Configurazione della protezione della posta elettronica

Le opzioni di protezione dei messaggi di posta elettronica consentono di sottoporre a scansione i messaggi di posta in arrivo, in uscita e i worm.

Per configurare la protezione della posta elettronica:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.
3. In **Protezione della posta elettronica**, fare clic su **Avanzate**.
4. Selezionare o deselezionare le seguenti caselle di controllo:
   - **Esegui scansione sui messaggi di posta elettronica in arrivo**: viene eseguita la scansione dei messaggi in arrivo (POP3) al fine di rilevare potenziali minacce.
   - **Esegui scansione sui messaggi di posta elettronica in uscita**: viene eseguita la scansione dei messaggi in uscita (SMTP) al fine di rilevare potenziali minacce.
   - **Attiva WormStopper**: WormStopper blocca i worm nei messaggi di posta elettronica.
5. Fare clic su **OK**.

Uso della protezione della messaggistica immediata

La protezione della messaggistica immediata consente di rilevare le minacce contenute negli allegati ai messaggi immediati in arrivo.

Disattivazione della protezione della messaggistica immediata

Se si disattiva la protezione della messaggistica immediata, non verranno rilevate le minacce contenute negli allegati ai messaggi immediati in arrivo.

Per disattivare la protezione della messaggistica immediata:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.
3. In **Protezione messaggistica immediata**, fare clic su **Disattiva**.

Attivazione della protezione della messaggistica immediata

La protezione della messaggistica immediata consente di rilevare le minacce contenute negli allegati ai messaggi immediati in arrivo.

Per attivare la protezione della messaggistica immediata:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.
3. In **Protezione messaggistica immediata**, fare clic su **Attiva**.

CAPITOLO 15

Scansione manuale del computer

È possibile eseguire la ricerca di virus e altre minacce in dischi rigidi, dischi floppy e in singoli file e cartelle. Quando viene individuato un file sospetto, viene eseguito un tentativo di pulitura del file, a meno che non si tratti di un programma potenzialmente indesiderato. Se questa operazione non riesce, il file verrà messo in quarantena o eliminato.

In questo capitolo

Scansione manuale

È possibile eseguire la scansione manuale in qualsiasi momento. Ad esempio, se VirusScan è stato appena installato, è possibile eseguire una scansione per verificare che sul computer non siano presenti virus o altre minacce. In alternativa, se è stata disattivata la scansione in tempo reale, è possibile eseguire una scansione per verificare che il computer sia ancora sicuro.

Scansione mediante le impostazioni di scansione manuale

Questo tipo di scansione utilizza le impostazioni di scansione manuale specificate dall'utente. VirusScan esegue la scansione di file compressi (.zip, .cab, ecc.), ma considera un file compresso come un solo file. Inoltre, il numero di file analizzati può variare se sono stati eliminati i file temporanei di Internet dopo l'ultima scansione.

Per eseguire la scansione in base alle impostazioni di scansione manuale personalizzate:

1. Nel menu standard, fare clic su **Esegui scansione**. Al termine della scansione, verranno visualizzati in un riepilogo il numero di elementi analizzati e rilevati, il numero elementi puliti e la data dell'ultima scansione eseguita.
2. Scegliere **Fine**.

Argomenti correlati

- Configurazione di scansioni manuali (pagina 96)

Scansione senza impostazioni di scansione manuale

Questo tipo di scansione non utilizza le impostazioni di scansione manuale specificate dall'utente. VirusScan esegue la scansione di file compressi (.zip, .cab, ecc.), ma considera un file compresso come un solo file. Inoltre, il numero di file analizzati può variare se sono stati eliminati i file temporanei di Internet dopo l'ultima scansione.

Per eseguire la scansione senza le impostazioni di scansione manuale personalizzate:

1. Nel menu avanzato, fare clic su **Home**.
2. Nel riquadro Home, fare clic su **Esegui scansione**.
3. In **Percorsi da sottoporre a scansione**, selezionare le caselle di controllo accanto a file, cartelle e unità che si desidera sottoporre a scansione.
4. Selezionare in **Opzioni** le caselle di controllo adiacenti al tipo di file che si desidera sottoporre a scansione.
5. Fare clic su **Esegui scansione**. Al termine della scansione, verranno visualizzati in un riepilogo il numero di elementi analizzati e rilevati, il numero elementi puliti e la data dell'ultima scansione eseguita.
6. Fare clic su **Fine**.

Nota: le opzioni selezionate non verranno salvate.

Scansione in Esplora risorse

È possibile eseguire la ricerca di virus e altre minacce nei file, nelle cartelle o nelle unità selezionate in Esplora risorse.

Per eseguire la scansione di file in Esplora risorse:

1. Aprire Esplora risorse.
2. Fare clic con il pulsante destro del mouse sul file, la cartella o l'unità da sottoporre a scansione, quindi scegliere **Esegui scansione**. Tutte le opzioni di scansione predefinite verranno selezionate per offrire la scansione più accurata possibile.

Configurazione di scansioni manuali

Quando si desidera eseguire una scansione manuale o pianificata, è possibile specificare i tipi di file e i percorsi da sottoporre a scansione, nonché l'ora e il giorno in cui si desidera eseguire la scansione.

Configurazione dei tipi di file da analizzare

È possibile configurare i tipi di file da sottoporre a scansione.

Per configurare i tipi di file da sottoporre a scansione:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione da virus**, fare clic su **Avanzate**.
4. Nel riquadro Protezione da virus, fare clic su **Scansione manuale**.
5. Selezionare o deselezionare le seguenti caselle di controllo:
   - **Ricerca di virus sconosciuti con tecnologia euristica**: i file vengono confrontati con le firme di virus noti allo scopo di rilevare tracce di virus non identificati. Questa opzione fornisce la scansione più accurata, ma in genere è più lenta di una scansione normale.
   - **Scansione di file .zip e altri file di archivio**: rileva e rimuove i virus nei file .zip e in altri file di archivio. Talvolta gli autori dei virus inseriscono i virus in un file .zip, quindi inseriscono il file .zip in un altro file .zip per tentare di superare le barriere dei programmi antivirus.
   - **Ricerca di programmi spyware e programmi potenzialmente indesiderati**: vengono rilevati e rimossi spyware, adware e altri programmi che possono raccogliere e trasmettere dati senza l'autorizzazione dell'utente.
   - **Cerca e rimuovi cookie traccianti**: vengono rilevati e rimossi i cookie che possono raccogliere e trasmettere dati senza l'autorizzazione dell'utente. Un cookie identifica gli utenti quando visitano una pagina Web.
   - **Ricerca di rootkit e altri programmi di mascheramento**: vengono rilevati e rimossi eventuali rootkit o altri programmi non identificati da Windows.
6. Fare clic su uno dei seguenti pulsanti:
   - **Tutti i file (consigliato)**: viene eseguita la scansione di tutti i tipi di file utilizzati dal computer. Questa opzione offre la scansione più accurata.
   - **Solo file di programma e documenti**: viene eseguita la scansione esclusivamente di file di programma e documenti.

7 Fare clic su **OK**.

Configurazione dei percorsi da sottoporre a scansione

È possibile configurare i percorsi da sottoporre a scansioni manuali o pianificate.

Per configurare i percorsi da sottoporre a scansione:

1 Nel menu avanzato, fare clic su **Configura**.

2 Nel riquadro Configura, fare clic su **Computer e file**.

3 In **Protezione da virus**, fare clic su **Avanzate**.

4 Nel riquadro Protezione da virus, fare clic su **Scansione manuale**.

5 In **Percorso predefinito da sottoporre a scansione**, selezionare i file, le cartelle e le unità che si desidera sottoporre a scansione.

Per eseguire la scansione più accurata possibile, verificare che l'opzione **File importanti** sia selezionata.

6 Fare clic su **OK**.

Pianificazione di scansioni

Per una ricerca accurata dei virus e di altre minacce nel computer, è possibile pianificare le scansioni a intervalli di tempo specificati.

Per pianificare una scansione:

1 Nel menu avanzato, fare clic su **Configura**.

2 Nel riquadro Configura, fare clic su **Computer e file**.

3 In **Protezione da virus**, fare clic su **Avanzate**.

4 Nel riquadro Protezione da virus, fare clic su **Scansione pianificata**.

5 Verificare che l'opzione **Attiva scansione pianificata** sia selezionata.

6 Selezionare la casella di controllo accanto al giorno della settimana in cui eseguire la scansione.

7 Fare clic sui valori negli elenchi dell'ora di inizio per specificare l'ora di inizio.

8 Fare clic su **OK**.

Suggerimento: per utilizzare la pianificazione predefinita, fare clic su **Ripristina**.

CAPITOLO 16

Amministrazione di VirusScan

È possibile rimuovere voci dagli elenchi di elementi affidabili, gestire programmi, cookie e file in quarantena, visualizzare eventi e registri, nonché segnalare attività sospette a McAfee.

In questo capitolo

Gestione degli elenchi di elementi affidabili

Quando si definisce come affidabile un modulo SystemGuard, un programma, un sovraccarico del buffer o un programma di posta elettronica, l'elemento viene aggiunto a un elenco di elementi affidabili in modo che non venga più rilevato in futuro.

Se per errore si definisce come affidabile un programma o se si desidera che il programma venga rilevato, è necessario rimuoverlo da questo elenco.

Gestione degli elenchi di elementi affidabili

Quando si definisce come affidabile un modulo SystemGuard, un programma, un sovraccarico del buffer o un programma di posta elettronica, l'elemento viene aggiunto a un elenco di elementi affidabili in modo che non venga più rilevato in futuro.

Se per errore si definisce come affidabile un programma o se si desidera che il programma venga rilevato, è necessario rimuoverlo da questo elenco.

Per rimuovere delle voci dall'elenco degli elementi affidabili:

1. Nel menu avanzato, fare clic su **Configura**.
2. Nel riquadro Configura, fare clic su **Computer e file**.
3. In **Protezione da virus**, fare clic su **Avanzate**.
4. Nel riquadro Protezione da virus, fare clic su **Elementi affidabili**.
5. Nell'elenco, selezionare un modulo SystemGuard, un programma, un sovraccarico del buffer o un programma di posta elettronica affidabili per visualizzarne i relativi dettagli e lo stato dell'affidabilità.
6. Le informazioni sull'elemento vengono visualizzate in **Dettagli**.
7. In **Desidero**, fare clic su una delle azioni elencate.
8. Fare clic su **OK**.

Gestione di programmi, cookie e file in quarantena

I programmi, cookie e file in quarantena possono essere ripristinati, eliminati o inviati a McAfee per l'analisi.

Ripristino di programmi, cookie e file in quarantena

Se necessario, è possibile ripristinare programmi, cookie e file messi in quarantena.

Per ripristinare programmi, cookie e file in quarantena:

1. Nel menu avanzato, fare clic su **Ripristina**.
2. Nel riquadro Ripristina, fare clic su **Programmi e cookie** o **File**, a seconda delle necessità.
3. Selezionare i programmi, cookie o file in quarantena che si desidera ripristinare.
4. Per ulteriori informazioni sui virus in quarantena, fare clic sul nome del rilevamento in **Dettagli**. Verrà visualizzata la descrizione del virus riportata nella Libreria di informazioni sui virus.
5. In **Desidero**, fare clic su **Ripristina**.

Rimozione di programmi, cookie e file in quarantena

È possibile rimuovere programmi, cookie e file messi in quarantena.

Per rimuovere programmi, cookie e file in quarantena:

1. Nel menu avanzato, fare clic su **Ripristina**.
2. Nel riquadro Ripristina, fare clic su **Programmi e cookie** o **File**, a seconda delle necessità.
3. Selezionare i programmi, cookie o file in quarantena che si desidera ripristinare.
4. Per ulteriori informazioni sui virus in quarantena, fare clic sul nome del rilevamento in **Dettagli**. Verrà visualizzata la descrizione del virus riportata nella Libreria di informazioni sui virus.
5. In **Desidero**, fare clic su **Rimuovi**.

Invio a McAfee di programmi, cookie e file in quarantena

È possibile inviare a McAfee programmi, cookie e file in quarantena per l'analisi.

Nota: se il file in quarantena inviato supera le dimensioni minime, è possibile che venga rifiutato. Nella maggior parte dei casi, ciò non si verifica.

Per inviare programmi, cookie e file in quarantena a McAfee:

1. Nel menu avanzato, fare clic su **Ripristina**.
2. Nel riquadro Ripristina, fare clic su **Programmi e cookie** o **File**, a seconda delle necessità.
3. Selezionare i programmi, cookie o file in quarantena che si desidera inviare a McAfee.
4. Per ulteriori informazioni sui virus in quarantena, fare clic sul nome del rilevamento in **Dettagli**. Verrà visualizzata la descrizione del virus riportata nella Libreria di informazioni sui virus.
5. In **Desidero**, fare clic su **Invia a McAfee**.

Visualizzazione di registri ed eventi recenti

I registri e gli eventi recenti visualizzano gli eventi relativi a tutti i prodotti McAfee installati.

In Eventi recenti è possibile visualizzare gli ultimi 30 eventi significativi verificatisi sul computer. È possibile ripristinare programmi bloccati, riattivare la scansione in tempo reale e ritenere affidabili sovraccarichi del buffer.

È inoltre possibile visualizzare i registri in cui sono memorizzati tutti gli eventi verificatisi negli ultimi 30 giorni.

Visualizzazione di eventi

In Eventi recenti è possibile visualizzare gli ultimi 30 eventi significativi verificatisi sul computer. È possibile ripristinare programmi bloccati, riattivare la scansione in tempo reale e definire come affidabili sovraccarichi del buffer.

Per visualizzare gli eventi:

1. Nel menu avanzato, fare clic su **Rapporti e registri**.
2. Nel riquadro Rapporti e registri, fare clic su **Eventi recenti**.
3. Selezionare l'evento da visualizzare.
4. Le informazioni sull'evento vengono visualizzate in **Dettagli**.
5. In **Desidero**, fare clic su una delle azioni elencate.

Visualizzazione di registri

Nei registri sono memorizzati tutti gli eventi verificatisi negli ultimi 30 giorni.

Per visualizzare i registri:

1. Nel menu avanzato, fare clic su **Rapporti e registri**.
2. Nel riquadro Rapporti e registri, fare clic su **Eventi recenti**.
3. Nel riquadro Eventi recenti, fare clic su **Visualizza registro**.
4. Selezionare il tipo di registro da visualizzare, quindi selezionare un registro.
5. Le informazioni sul registro vengono visualizzate in **Dettagli**.

Segnalazione automatica di informazioni anonime

È possibile inviare a McAfee informazioni su virus, programmi potenzialmente indesiderati e sul rintracciamento di hacker in modo anonimo. Questa opzione è disponibile solo durante l'installazione.

Non verranno raccolti dati personali che consentano l'identificazione.

Segnalazioni a McAfee

È possibile inviare a McAfee informazioni su virus, programmi potenzialmente indesiderati e sul rintracciamento di hacker. Questa opzione è disponibile solo durante l'installazione.

Per segnalare automaticamente informazioni anonime:

1. Durante l'installazione di VirusScan, confermare l'opzione predefinita **Invia informazioni anonime**.
2. Fare clic su **Avanti**.

Informazioni sugli avvisi di protezione

Se la scansione in tempo reale rileva una minaccia, viene visualizzato un avviso di protezione. Se la scansione in tempo reale rileva virus, trojan, script e worm, nella maggior parte dei casi viene eseguito un tentativo di pulitura automatica del file e l'utente viene avvisato. Nel caso di programmi potenzialmente indesiderati e moduli SystemGuard, la scansione in tempo reale rileva il file o la modifica e l'utente viene avvisato. La scansione in tempo reale blocca automaticamente le attività di sovraccarico del buffer, cookie traccianti ed esecuzione di script e e l'utente viene avvisato.

Gli avvisi possono essere raggruppati in tre tipi principali.

- Avviso rosso
- Avviso giallo
- Avviso verde

È possibile quindi scegliere come gestire i file e i messaggi di posta elettronica rilevati, gli script sospetti, i potenziali worm, i programmi potenzialmente indesiderati, i moduli SystemGuard o i sovraccarichi del buffer.

Gestione degli avvisi

Per agevolare la gestione della protezione, McAfee utilizza una serie di avvisi. Gli avvisi possono essere raggruppati in tre tipi principali.

- Avviso rosso
- Avviso giallo
- Avviso verde

Avviso rosso

Un avviso rosso richiede una risposta da parte dell'utente. In alcuni casi, McAfee non può determinare come rispondere automaticamente a una particolare attività. In questi casi, l'avviso rosso descrive l'attività in questione e offre all'utente una o più opzioni da selezionare.

Avviso giallo

Un avviso giallo è una notifica non critica che di solito richiede una risposta da parte dell'utente. L'avviso giallo descrive l'attività in questione e offre all'utente una o più opzioni da selezionare.

Avviso verde

Nella maggioranza dei casi, un avviso verde fornisce informazioni di base su un evento, senza richiedere la risposta da parte dell'utente.

Configurazione delle opzioni di avviso

Se si sceglie di non visualizzare nuovamente un avviso e in seguito si cambia idea, è possibile riconfigurare tale avviso in modo che sia visualizzato di nuovo. Per ulteriori informazioni sulla configurazione delle opzioni di avviso, vedere la documentazione di SecurityCenter.

CAPITOLO 17

Ulteriori informazioni

In questo capitolo sono riportate le domande frequenti e le procedure per la risoluzione dei problemi.

In questo capitolo

Domande frequenti

In questa sezione vengono fornite le risposte alle domande più frequenti.

Cosa occorre fare quando è stata rilevata una minaccia?

Per agevolare la gestione della protezione, McAfee utilizza gli avvisi. Gli avvisi possono essere raggruppati in tre tipi principali.

- Avviso rosso
- Avviso giallo
- Avviso verde

È possibile quindi scegliere come gestire i file e i messaggi di posta elettronica rilevati, gli script sospetti, i potenziali worm, i programmi potenzialmente indesiderati, i moduli SystemGuard o i sovraccarichi del buffer.

Per ulteriori informazioni sulla gestione di particolari minacce, consultare la Libreria di informazioni sui virus all'indirizzo: http://it.mcafee.com/virusInfo/default.asp?affid=.

Argomenti correlati

- Informazioni sugli avvisi di protezione (pagina 105)

È possibile utilizzare VirusScan con i browser Netscape, Firefox e Opera ?

È possibile utilizzare Netscape, Firefox e Opera come browser Internet predefiniti, ma è necessario che Microsoft ∃ Internet Explorer versione 6.0 o successiva sia installato sul computer.

Per eseguire una scansione è necessario essere connessi a Internet?

Non è necessario essere connessi a Internet per eseguire una scansione, ma occorre connettersi almeno una volta alla settimana per ricevere gli aggiornamenti di McAfee.

VirusScan esegue la scansione degli allegati dei messaggi di posta elettronica?

Se sono state attivate le funzioni di scansione in tempo reale e di protezione della posta elettronica, quando si riceve un messaggio di posta elettronica gli eventuali allegati vengono sottoposti a scansione.

VirusScan esegue la scansione dei file compressi?

VirusScan esegue la scansione di file .zip e di altri file di archivio.

Perché si verificano errori di scansione dei messaggi di posta elettronica in uscita?

Durante la scansione dei messaggi di posta elettronica in uscita possono verificarsi i seguenti tipi di errore:

- Errore di protocollo. Il server di posta elettronica ha rifiutato un messaggio di posta elettronica.
  Se si verifica un errore di protocollo o di sistema, i messaggi di posta elettronica rimanenti per quella sessione vengono elaborati e inviati al server.
- Errore di connessione. La connessione al server di posta elettronica si è interrotta.
  Se si verifica un errore di connessione, accertarsi che il computer sia connesso a Internet, quindi riprovare inviando il messaggio dall'elenco nella cartella **Posta inviata** del programma di posta elettronica.
- Errore di sistema. Si è verificato un errore di gestione dei file o un altro errore di sistema.
- Errore di connessione SMTP crittografata. Il programma di posta elettronica ha rilevato una connessione SMTP crittografata.
  Se si presenta un errore di connessione SMTP crittografata, per accertarsi che i messaggi di posta elettronica siano sottoposti a scansione, disattivare la connessione SMTP crittografata nel programma di posta elettronica.

Se si verificano dei timeout durante l'invio di messaggi di posta elettronica, disattivare la scansione della posta in uscita o disattivare la connessione SMTP crittografata nel programma di posta elettronica.

Argomenti correlati

- Configurazione della protezione della posta elettronica (pagina 90)

Risoluzione dei problemi

In questa sezione sono riportate informazioni utili in caso di problemi generali.

È impossibile rimuovere o eliminare un virus

Per alcuni virus, è necessario effettuare la pulizia manuale del computer. Riavviare il computer, quindi eseguire nuovamente la scansione.

Se il computer non è in grado di rimuovere o eliminare un virus, consultare la Libreria di informazioni sui virus all'indirizzo: http://it.mcafee.com/virusInfo/default.asp?affid=.

Per ulteriore assistenza, rivolgersi al Servizio clienti McAfee sul sito Web di McAfee.

Nota: non è possibile rimuovere virus da CD-ROM, DVD e dischi floppy protetti da scrittura.

Anche dopo il riavvio risulta impossibile rimuovere un elemento

Dopo la scansione e la rimozione di elementi, in alcuni casi è necessario riavviare il computer.

Se l'elemento non viene rimosso dopo il riavvio del computer, inviare il file a McAfee.

Nota: non è possibile rimuovere virus da CD-ROM, DVD e dischi floppy protetti da scrittura.

Argomenti correlati

- Gestione di programmi, cookie e file in quarantena (pagina 101)

Alcuni componenti risultano mancanti o danneggiati

Alcune situazioni possono causare un'installazione errata di VirusScan:

- Lo spazio su disco o la memoria del computer sono insufficienti. Verificare che il computer soddisfi i requisiti di sistema per l'esecuzione del software.
- Il browser Internet non è configurato correttamente.
- La connessione a Internet è difettosa. Verificare la connessione o tentare di riconnettersi in un secondo momento.
- File mancanti o installazione non riuscita.

La soluzione migliore consiste nel risolvere i potenziali problemi, quindi reinstallare VirusScan.

CAPITOLO 18

McAfee Personal Firewall

Personal Firewall offre una protezione avanzata per il computer e per i dati personali. Personal Firewall consente di stabilire una barriera tra il computer in uso e Internet, monitorando il traffico Internet alla ricerca di attività sospette, senza richiedere interazione da parte dell'utente.

In questo capitolo

Funzioni

Personal Firewall offre la completa protezione firewall in entrata e in uscita, considerando automaticamente come affidabili i programmi riconosciuti come tali e contribuendo a bloccare spyware, trojan e keylogger. Il firewall difende dagli attacchi degli hacker, controlla Internet e le attività della rete, segnala eventi dannosi o sospetti, fornisce informazioni dettagliate sul traffico Internet e completa la difesa antivirus.

Livelli di protezione standard e personalizzati

Le impostazioni di protezione predefinite del firewall consentono di salvaguardarsi da intrusioni e attività sospette, ma è anche possibile personalizzarle in base alle proprie esigenze.

Consigli in tempo reale

Il firewall offre l'opportunità di ricevere in maniera dinamica alcuni consigli che contribuiscono a determinare a quali programmi consentire l'accesso a Internet e se ritenere affidabile il traffico di rete.

Gestione intelligente dell'accesso per i programmi

Nel riquadro Autorizzazioni programmi del firewall è possibile gestire l'accesso a Internet per i programmi tramite avvisi e registri eventi, oppure configurare le autorizzazioni di accesso per programmi specifici.

Protezione durante l'esecuzione di giochi

Per non distrarsi durante l'esecuzione di giochi a schermo intero, è possibile configurare il firewall per la visualizzazione degli avvisi al termine della sessione di gioco qualora esso rilevi tentativi di intrusione o attività sospette.

Protezione all'avvio del computer

Il firewall protegge il computer da tentativi di intrusione, programmi e traffico di rete indesiderati già prima dell'avvio di Windows.

Controllo delle porte dei servizi di sistema

Le porte dei servizi di sistema potrebbero essere utilizzate come backdoor di accesso al computer. Il firewall consente di creare e gestire le porte dei servizi di sistema, aperte e chiuse, richieste da alcuni programmi.

Gestione delle connessioni del computer

Il firewall consente di ritenere affidabili o escludere le connessioni remote e gli indirizzi IP che possono stabilire connessioni al computer.

Integrazione delle informazioni di HackerWatch

HackerWatch è un hub con informazioni sulla protezione che rintraccia sequenze generali di attività di hacker e intrusioni, oltre a fornire informazioni aggiornatissime sui programmi installati sul computer. Consente di visualizzare statistiche globali sugli eventi di protezione e sulle porte Internet.

Blocca firewall

Consente di bloccare immediatamente tutto il traffico Internet in ingresso e in uscita tra il computer e Internet.

Ripristina firewall

Ripristina immediatamente le impostazioni di protezione originali del firewall. Se Personal Firewall mostra un comportamento diverso da quello previsto, è possibile ripristinare le impostazioni predefinite del firewall.

Rilevamento avanzato di trojan

Combina la gestione delle connessioni dei programmi con un database potenziato per rilevare e bloccare l'accesso a Internet e l'inoltro di dati personali da parte di applicazioni potenzialmente dannose, ad esempio i trojan.

Registrazione eventi

Specificare se si desidera attivare o disattivare la registrazione e, nel primo caso, quali tipi di eventi registrare. Grazie alla registrazione degli eventi è possibile visualizzare gli eventi recenti in ingresso e in uscita e anche quelli di rilevamento intrusioni.

Monitoraggio del traffico Internet

È possibile consultare mappe grafiche di facile lettura che mostrano l'origine del traffico e degli attacchi dannosi in tutto il mondo. Inoltre, è possibile individuare informazioni dettagliate sui proprietari e dati geografici relativi agli indirizzi IP di origine. Il firewall permette inoltre di analizzare il traffico in ingresso e in uscita, monitorare l'utilizzo della larghezza di banda dei programmi e le attività dei programmi.

Prevenzione delle intrusioni

Aumenta la protezione della privacy fornendo funzioni di prevenzione delle intrusioni contro possibili minacce Internet. Mediante una funzionalità di tipo euristico, McAfee offre un terzo livello di protezione bloccando gli elementi che presentano i sintomi di un attacco o le caratteristiche di un tentativo di intrusione.

Analisi complessa del traffico

Consente di analizzare il traffico Internet in ingresso e in uscita, nonché le connessioni dei programmi, compresi quelli attivamente in ascolto di connessioni aperte. In questo modo è possibile rilevare i programmi vulnerabili a un'eventuale intrusione e intervenire di conseguenza.

Avvio del firewall

Una volta installato il firewall, il computer è protetto da intrusioni e da traffico di rete indesiderato. Inoltre l'utente è pronto a gestire gli avvisi e l'accesso Internet in ingresso e in uscita di programmi noti e sconosciuti. L'attivazione dei suggerimenti intelligenti e del livello di protezione Standard avviene automaticamente.

È possibile disattivare il firewall dal riquadro Configurazione di Internet e rete ma, in questo caso, il computer non sarà più protetto da intrusioni e da traffico di rete indesiderato e l'utente non potrà gestire in maniera efficace le connessioni Internet in ingresso e in uscita. Pertanto, la protezione firewall deve essere disattivata solo temporaneamente e in caso di necessità. Il firewall può essere anche attivato dal pannello Configurazione di Internet e rete.

Personal Firewall disattiva automaticamente Windows® Firewall e imposta se stesso come firewall predefinito.

Nota: per configurare Personal Firewall, aprire il riquadro Configurazione di Internet & rete.

Avvio della protezione firewall

L'attivazione della protezione firewall consente di difendere il computer da intrusioni e da traffico di rete indesiderato e di gestire le connessioni Internet in ingresso e in uscita.

Per attivare la protezione firewall

1. Nel riquadro McAfee SecurityCenter, effettuare una delle seguenti operazioni:
   - Fare clic su **Internet e rete**, quindi su **Configura**.
   - Fare clic su **Menu avanzato**, quindi su **Configura** nel riquadro **Home** e selezionare **Internet e rete**.
2. Nel riquadro **Configurazione di Internet e rete**, in **Protezione firewall**, fare clic su **Attiva**.

Arresto della protezione firewall

La disattivazione della protezione firewall rende il computer vulnerabile alle intrusioni e al traffico di rete indesiderato e impedisce la gestione delle connessioni Internet in ingresso e in uscita.

Per disattivare la protezione firewall

1. Nel riquadro McAfee SecurityCenter, effettuare una delle seguenti operazioni:
   - Fare clic su **Internet e rete**, quindi su **Configura**.
   - Fare clic su **Menu avanzato**, quindi su **Configura** nel riquadro **Home** e selezionare **Internet e rete**.
2. Nel riquadro **Configurazione di Internet e rete**, in **Protezione firewall**, fare clic su **Disattiva**.

Utilizzo degli avvisi

Il firewall utilizza una serie di avvisi che facilitano la gestione della protezione da parte dell'utente, raggruppabili in quattro tipi principali.

- Avviso Trojan bloccato
- Avviso rosso
- Avviso giallo
- Avviso verde

Gli avvisi possono anche contenere informazioni utili all'utente per decidere come gestire gli avvisi o ottenere informazioni sui programmi in esecuzione sul computer.

Informazioni sugli avvisi

Il firewall prevede quattro tipi principali di avvisi. Alcuni avvisi, inoltre, includono informazioni utili all'apprendimento o al reperimento di informazioni relative ai programmi in esecuzione sul computer.

Avviso Trojan bloccato

Un trojan ha l'aspetto di un programma legittimo, ma può consentire l'accesso non autorizzato al computer, provocarne malfunzionamenti e danneggiarlo. L'avviso Trojan bloccato viene visualizzato quando il firewall rileva, e quindi blocca, un trojan sul computer e suggerisce una scansione alla ricerca di altre minacce. Questo avviso viene visualizzato in tutti i livelli di protezione, tranne Aperto, o quando Suggerimenti intelligenti è disattivato.

Avviso rosso

Si tratta del tipo più comune di avviso e in genere richiede una risposta da parte dell'utente. Poiché il firewall, in alcuni casi, non è in grado di stabilire automaticamente un'azione particolare da intraprendere per l'attività di un programma o un evento di rete, l'avviso per prima cosa descrive l'attività del programma o l'evento di rete in questione seguiti da una o più opzioni a cui l'utente deve rispondere. Quando Suggerimenti intelligenti è attivato, i programmi vengono aggiunti al riquadro Autorizzazioni programmi.

Di seguito sono riportate le descrizioni degli avvisi più comuni:

- **Il programma richiede l'accesso a Internet**: il firewall rileva un programma che tenta di accedere a Internet.
- **Il programma è stato modificato**: il firewall rileva un programma che risulta in qualche modo modificato, forse in seguito a un aggiornamento online.
- **Programma bloccato**: il firewall blocca un programma perché è elencato nel riquadro Autorizzazioni programmi.

In base alle impostazioni, all'attività del programma o all'evento di rete, le opzioni riportate di seguito sono le più frequenti:

- **Consenti accesso**: consente a un programma del computer di accedere a Internet. La regola viene aggiunta alla pagina Autorizzazioni programmi.
- **Consenti accesso solo una volta**: consente a un programma del computer di accedere temporaneamente a Internet. Ad esempio l'installazione di un nuovo programma potrebbe richiedere questo tipo di accesso.
- **Blocca accesso**: impedisce l'accesso di un programma a Internet.

- **Consenti solo accesso in uscita**: consente solo una connessione in uscita a Internet. Si tratta di un avviso che in genere si visualizza quando sono impostati i livelli di protezione Elevato e Mascheramento.
- **Imposta la rete come affidabile**: consente il traffico in ingresso e in uscita da una rete. La rete viene aggiunta alla sezione Indirizzi IP affidabili.
- **Non impostare la rete come affidabile adesso**: blocca il traffico in ingresso e in uscita da una rete.

Avviso giallo

L'avviso giallo rappresenta una notifica non critica che informa l'utente su un evento di rete rilevato dal firewall. Ad esempio, l'avviso **Rilevata nuova rete** viene visualizzato quando si esegue il firewall per la prima volta o quando un computer con firewall installato è connesso a una nuova rete. È possibile scegliere se impostare o non impostare come affidabile la rete. Nel primo caso, il firewall consente il traffico da qualsiasi altro computer in rete e viene aggiunto agli indirizzi IP affidabili.

Avviso verde

Nella maggior parte dei casi, l'avviso verde fornisce informazioni di base relative a un evento e non richiede una risposta. Gli avvisi verdi solitamente vengono visualizzati quando sono impostati i livelli di protezione Standard, Elevato, Mascheramento e Blocco. Di seguito sono elencate le descrizioni di tali avvisi:

- **Il programma è stato modificato**: informa l'utente della modifica avvenuta in un programma a cui precedentemente è stato consentito l'accesso a Internet. È possibile scegliere di bloccarlo, tuttavia in caso di mancata risposta, l'avviso scompare dal desktop e il programma continua ad avere accesso.
- **Accesso a Internet consentito al programma**: informa l'utente che un programma è stato autorizzato ad accedere a Internet. È possibile scegliere di bloccarlo, tuttavia in caso di mancata risposta, l'avviso scompare e il programma continua ad accedere a Internet.

Assistenza per l'utente

Molti avvisi firewall contengono ulteriori informazioni che consentono di gestire con facilità la protezione del computer, tra cui:

- **Ulteriori informazioni su questo programma**: avviare il sito Web di protezione globale di McAfee per ottenere informazioni su un programma che il firewall ha rilevato sul computer.

- **Informa McAfee di questo programma**: inviare informazioni a McAfee su un file sconosciuto rilevato sul computer dal firewall.
- **McAfee suggerisce**: vengono forniti suggerimenti per la gestione degli avvisi. Ad esempio, un avviso può suggerire di consentire l'accesso a un programma.

Gestione degli avvisi informativi

Il firewall consente di visualizzare o di nascondere gli avvisi informativi durante determinati eventi.

Visualizzazione degli avvisi durante l'esecuzione di giochi

Per impostazione predefinita, il firewall impedisce la visualizzazione degli avvisi informativi durante l'esecuzione di giochi a schermo intero. Tuttavia è possibile configurare il firewall per la visualizzazione di tali avvisi anche durante l'esecuzione di giochi qualora esso rilevi tentativi di intrusione o attività sospette.

Per visualizzare gli avvisi durante l'esecuzione di giochi

1. Nel riquadro Attività comuni, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avvisi**.
4. Fare clic su **Avanzate**.
5. Nel riquadro **Opzioni di avviso**, selezionare **Visualizza avvisi informativi quando viene rilevata la modalità di gioco**.

Procedura per nascondere gli avvisi informativi

Gli avvisi informativi informano l'utente su eventi che non richiedono attenzione immediata.

Per nascondere gli avvisi informativi

1. Nel riquadro Attività comuni, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avvisi**.
4. Fare clic su **Avanzate**.
5. Nel riquadro **Configurazione di SecurityCenter**, fare clic su **Avvisi informativi**.
6. Nel riquadro **Avvisi informativi**, effettuare una delle seguenti operazioni:
   - Selezionare il tipo di avviso da nascondere.

- Selezionare **Nascondi avvisi informativi** per nascondere tutti gli avvisi informativi.

7 Fare clic su **OK**.

CAPITOLO 19

Configurazione della protezione del firewall

Il firewall prevede alcuni metodi per gestire la protezione e personalizzare la modalità di risposta agli eventi e agli avvisi relativi alla protezione.

Dopo la prima installazione, il livello di protezione è impostato su Standard. Nella maggior parte dei casi questa impostazione soddisfa tutte le esigenze di protezione. Il firewall comunque fornisce altri livelli, a partire da quelli maggiormente restrittivi per arrivare a quelli più permissivi.

Offre inoltre l'opportunità di ricevere suggerimenti concernenti gli avvisi e l'accesso Internet dei programmi.

In questo capitolo

Gestione dei livelli di protezione del firewall

È possibile configurare i livelli di protezione per controllare in che misura si desidera gestire gli avvisi e rispondere quando il firewall rileva traffico di rete indesiderato e connessioni Internet in ingresso e in uscita. Per impostazione predefinita, viene attivato il livello di protezione Standard.

Quando il livello di protezione è impostato su Standard e i suggerimenti intelligenti sono attivati, gli avvisi rossi offrono la possibilità di autorizzare o bloccare l'accesso ai programmi sconosciuti o modificati. Al rilevamento di programmi noti, viene visualizzato un avviso informativo di colore verde e l'accesso è automaticamente consentito. Ottenuto l'accesso, un programma sarà in grado di creare connessioni in uscita e di ascoltare connessioni in ingresso non richieste.

In genere, più il livello di protezione è restrittivo (Mascheramento ed Elevato), maggiore sarà il numero di opzioni e avvisi visualizzati che, a loro volta, dovranno essere gestiti dall'utente.

Personal Firewall utilizza sei livelli di protezione, riportati di seguito a cominciare dal più restrittivo:

- **Blocco**: blocca tutte le connessioni Internet.
- **Mascheramento**: blocca tutte le connessioni Internet in ingresso.
- **Elevato**: gli avvisi esigono una risposta per ogni richiesta di connessione Internet in ingresso e in uscita.
- **Standard**: gli avvisi avvertono l'utente quando programmi sconosciuti o nuovi richiedono di accedere a Internet.
- **Basato sull'affidabilità**: consente tutte le connessioni Internet, sia in ingresso che in uscita, e le aggiunge automaticamente al riquadro Autorizzazioni programmi.
- **Aperto**: consente tutte le connessioni Internet, sia in ingresso che in uscita.

Il firewall offre inoltre la possibilità di reimpostare immediatamente il livello di protezione su Standard dal riquadro Ripristina le impostazioni predefinite della protezione firewall.

Impostazione del livello di protezione su Blocco

L'impostazione del livello di protezione su Blocco consente di bloccare tutte le connessioni di rete, sia in ingresso che in uscita, compreso l'accesso a siti Web, posta elettronica e aggiornamenti della protezione. Il risultato offerto da questo livello di protezione equivale a quello che si otterrebbe rimuovendo la connessione a Internet. È possibile utilizzare questa impostazione per bloccare porte configurate come aperte nel riquadro Servizi di sistema. Durante il blocco, gli avvisi possono continuare a richiedere il blocco dei programmi.

Per impostare il livello di protezione del firewall su Blocco

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Blocco** venga visualizzato come livello corrente.
3. Fare clic su **OK**.

Impostazione del livello di protezione su Mascheramento

L'impostazione del livello di protezione su Mascheramento consente di bloccare tutte le connessioni di rete in ingresso, porte aperte escluse, e nasconde completamente la presenza del computer su Internet. Quando il livello di protezione è impostato su Mascheramento, il firewall avvisa l'utente se un nuovo programma tenta di stabilire una connessione in uscita a Internet oppure riceve una richiesta di connessione in ingresso. I programmi bloccati e aggiunti sono visualizzati nel riquadro Autorizzazioni programmi.

Per impostare il livello di protezione del firewall su Mascheramento

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Mascheramento** venga visualizzato come livello corrente.
3. Fare clic su **OK**.

Impostazione del livello di protezione su Elevato

Quando il livello di protezione è impostato su Elevato, il firewall informa l'utente se un nuovo programma tenta di stabilire una connessione in uscita a Internet oppure riceve una richiesta di connessione in ingresso. I programmi bloccati e aggiunti sono visualizzati nel riquadro Autorizzazioni programmi. Quando il livello di protezione è impostato su Elevato, un programma richiede solo il tipo di accesso necessario in quel momento, ad esempio l'accesso solo in uscita, che l'utente può consentire o bloccare. In seguito, qualora il programma richieda una connessione sia in ingresso che in uscita, è possibile consentire l'accesso completo al programma dal riquadro Autorizzazioni programmi.

Per impostare il livello di protezione del firewall su Elevato

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Elevato** venga visualizzato come livello corrente.
3. Fare clic su **OK**.

Impostazione del livello di protezione su Standard

Standard è il livello di protezione predefinito e consigliato.

Quando il livello di protezione del firewall è impostato su Standard, il firewall monitora le connessioni in ingresso e in uscita e avvisa nel momento in cui nuovi programmi tentano di accedere a Internet. I programmi bloccati e aggiunti sono visualizzati nel riquadro Autorizzazioni programmi.

Per impostare il livello di protezione del firewall su Standard

1. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Standard** venga visualizzato come livello corrente.
3. Fare clic su **OK**.

Impostazione del livello di protezione su Basato sull'affidabilità

L'impostazione del livello di protezione del firewall su Basato sull'affidabilità consente tutte le connessioni in ingresso e in uscita. Se viene utilizzato questo tipo di protezione, il firewall consente automaticamente l'accesso a tutti i programmi e li aggiunge all'elenco dei programmi consentiti nel riquadro Autorizzazioni programmi.

Per impostare il livello di protezione del firewall su Basato sull'affidabilità

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Basato sull'affidabilità** venga visualizzato come livello corrente.
3. Fare clic su **OK**.

Configurazione dei suggerimenti intelligenti per gli avvisi

È possibile configurare il firewall in modo tale da includere, escludere o visualizzare i suggerimenti in avvisi concernenti i programmi che tentano di accedere a Internet.

L'attivazione dei suggerimenti intelligenti aiuta a decidere la modalità di gestione degli avvisi. Se i suggerimenti intelligenti sono attivati (livello di protezione impostato su Standard), il firewall consente o blocca automaticamente i programmi noti, inoltre avvisa l'utente e gli suggerisce l'azione da intraprendere in caso di rilevamento di programmi sconosciuti e potenzialmente pericolosi.

Se invece sono disattivati, il firewall non consente né blocca automaticamente l'accesso a Internet e neppure suggerisce un'azione da intraprendere.

Nel caso in cui il firewall sia configurato per impostare la sola visualizzazione dei suggerimenti intelligenti, un avviso chiede all'utente di consentire o bloccare l'accesso e consiglia un'azione da intraprendere.

Attivazione dei suggerimenti intelligenti

L'attivazione dei suggerimenti intelligenti aiuta a decidere la modalità di gestione degli avvisi. Se i suggerimenti intelligenti sono attivati, il firewall automaticamente consente o blocca l'accesso ai programmi e avvisa l'utente nel caso in cui rilevi programmi sconosciuti e potenzialmente pericolosi.

Per attivare i suggerimenti intelligenti

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Attiva suggerimenti intelligenti**.
3. Fare clic su **OK**.

Disattivazione dei suggerimenti intelligenti

Con la disattivazione dei suggerimenti intelligenti, viene esclusa l'assistenza sulla gestione degli avvisi e dell'accesso ai programmi. Se tali suggerimenti sono disattivati, il firewall continua a consentire o bloccare l'accesso ai programmi e avvisa l'utente nel caso in cui rilevi programmi sconosciuti e potenzialmente pericolosi. Se viene rilevato un nuovo programma sospetto o noto come potenziale minaccia, il firewall impedisce automaticamente al programma di accedere a Internet.

Per disattivare i suggerimenti intelligenti

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Disattiva suggerimenti intelligenti**.
3. Fare clic su **OK**.

Impostazione dei suggerimenti intelligenti per la sola visualizzazione

La visualizzazione dei suggerimenti intelligenti aiuta a decidere la modalità di gestione degli avvisi per quanto concerne i programmi sconosciuti e potenzialmente pericolosi. Se i suggerimenti intelligenti sono impostati su **Solo visualizzazione**, vengono mostrate le informazioni sulla gestione degli avvisi ma, a differenza di quanto accade con l'opzione **Attiva suggerimenti intelligenti**, l'applicazione dei suggerimenti visualizzati non è automatica e neppure l'accesso dei programmi viene consentito o bloccato automaticamente. Gli avvisi continuano comunque a fornire suggerimenti utili per decidere se consentire o bloccare l'accesso a un programma.

Per impostare la sola visualizzazione dei suggerimenti intelligenti

1. Nel riquadro Configurazione Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Solo visualizzazione**.
3. Fare clic su **OK**.

Ottimizzazione della protezione firewall

La protezione di un computer può risultare compromessa per diverse ragioni. Ad esempio, alcuni programmi potrebbero tentare di connettersi a Internet prima dell'avvio di Windows®. Inoltre, utenti particolarmente esperti potrebbero inviare un ping al computer per stabilire se è connesso a una rete. Grazie al firewall è possibile difendersi contro questi due tipi di intrusione consentendo l'attivazione della protezione all'avvio e il blocco delle richieste ping ICMP. La prima impostazione impedisce ai programmi di accedere a Internet all'avvio di Windows mentre la seconda blocca le richieste ping che consentono ad altri utenti di individuare il computer su una rete.

Le impostazioni di installazione standard includono il rilevamento automatico dei tentativi di intrusione più comuni, ad esempio attacchi o vulnerabilità che causano negazioni del servizio (DoS, Denial of Service). L'utilizzo di tali impostazioni garantisce la protezione dell'utente contro attacchi e scansioni, tuttavia è possibile disattivare il rilevamento automatico per uno o più attacchi o scansioni nel riquadro Rilevamento delle intrusioni.

Protezione del computer durante l'avvio

Personal Firewall è in grado di proteggere il computer all'avvio di Windows. La protezione all'avvio blocca tutti i nuovi programmi precedentemente non autorizzati e che richiedono accesso a Internet. Una volta avviato, il firewall visualizza gli avvisi relativi ai programmi che avevano richiesto l'accesso a Internet durante l'avvio, da consentire oppure bloccare a discrezione dell'utente. Per utilizzare questa opzione, è necessario che il livello di protezione non sia impostato su Aperto o su Blocco.

Per proteggere il computer durante l'avvio

1. Nel riquadro Configurazione Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, in Impostazioni protezione, selezionare **Attiva protezione all'avvio**.
3. Fare clic su **OK**.

Nota: finché è abilitata la protezione all'avvio le connessioni risultano bloccate e non viene registrata alcuna intrusione.

Configurazione delle impostazioni di richieste ping

Gli utenti di computer possono utilizzare uno strumento ping, che invia e riceve messaggi di richiesta Echo ICMP, per stabilire se un determinato computer è connesso alla rete. È possibile configurare il firewall per impedire o consentire agli utenti di inviare ping al computer.

Per configurare l'impostazione delle richieste ping ICMP

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, in **Impostazioni protezione**, effettuare una delle seguenti operazioni:
   - Selezionare **Consenti richieste ping ICMP** per consentire il rilevamento del computer sulla rete mediante richieste ping.
   - Deselezionare **Consenti richieste ping ICMP** per impedire il rilevamento del computer sulla rete mediante richieste ping.
3. Fare clic su **OK**.

Configurazione del rilevamento intrusioni

Il sistema di rilevamento intrusioni (IDS) controlla i pacchetti di dati per rilevare eventuali trasferimenti di dati o metodi di trasferimento sospetti. IDS analizza il traffico e i pacchetti di dati alla ricerca di modelli di traffico sospetti utilizzati dai pirati informatici. Ad esempio, se il firewall rileva i pacchetti ICMP, li analizza alla ricerca di modelli di traffico sospetti confrontando il traffico ICMP con modelli di attacco noti. Il firewall confronta i pacchetti in un database di firme e, nel caso li ritenga sospetti o dannosi, esclude quelli provenienti dal computer che ha generato l'attacco ed eventualmente registra l'evento.

Le impostazioni di installazione standard includono il rilevamento automatico dei tentativi di intrusione più comuni, ad esempio attacchi o vulnerabilità che causano negazioni del servizio (DoS, Denial of Service). L'utilizzo di tali impostazioni garantisce la protezione dell'utente contro attacchi e scansioni, tuttavia è possibile disattivare il rilevamento automatico per uno o più attacchi o scansioni nel riquadro Rilevamento delle intrusioni.

Per configurare il rilevamento delle intrusioni

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Rilevamento delle intrusioni**.
3. In **Rileva tentativi di intrusione**, effettuare una delle seguenti operazioni:
   - Selezionare un nome per rilevare automaticamente l'attacco o la scansione.
   - Deselezionare un nome per disattivare il rilevamento automatico dell'attacco o della scansione.
4. Fare clic su **OK**.

Configurazione delle impostazioni relative allo stato della protezione firewall

SecurityCenter monitora i problemi facenti parte dello stato generale della protezione del computer. Tuttavia il firewall può anche essere configurato per ignorare determinati problemi del computer in uso che possono influire sullo stato della protezione. È possibile configurare SecurityCenter in modo tale che ignori quando il firewall è impostato sul livello di protezione Aperto, quando il servizio firewall non è in funzione e quando un firewall solo in uscita non è installato sul computer.

Per configurare le impostazioni relative allo stato della protezione firewall

1. Nel riquadro Attività comuni, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avvisi**.
4. Fare clic su **Avanzate**.
5. Nel riquadro Attività comuni, fare clic su **Menu avanzato**.
6. Fare clic su **Configura**.
7. Nel riquadro Configurazione di SecurityCenter, fare clic su **Stato protezione**.
8. Fare clic su Avanzate.
9. Nel riquadro Problemi ignorati, selezionare una o più delle seguenti opzioni:
   - **Il firewall è impostato sul livello di protezione Aperto.**
   - **Il servizio firewall non è in esecuzione.**
   - **Il firewall in uscita non è installato nel computer.**
10. Fare clic su **OK**.

Blocco e ripristino del firewall

La modalità di blocco è utile nella gestione delle situazioni di emergenza correlate al computer, per gli utenti che devono bloccare il traffico per isolare e risolvere un problema del computer o per coloro che non sono sicuri e devono stabilire il modo in cui gestire l'accesso di un programma a Internet.

Blocco immediato del firewall

Il blocco del firewall consente di bloccare immediatamente tutto il traffico di rete in ingresso e in uscita tra il computer e Internet. In tale modalità, l'accesso al computer da parte di tutte le connessioni remote e l'accesso a Internet da parte di tutti i programmi sono bloccati.

Per bloccare immediatamente il firewall e tutto il traffico di rete

1. Nei riquadri Home o Attività comuni con il **Menu standard** o il **Menu avanzato** attivato, fare clic su **Blocca firewall**.
2. Nel riquadro Blocca firewall, fare clic su **Blocco**.
3. Nella finestra di dialogo, fare clic su **Sì** per confermare che si desidera bloccare immediatamente tutto il traffico in ingresso e in uscita.

Sblocco immediato del firewall

Il blocco del firewall consente di bloccare immediatamente tutto il traffico di rete in ingresso e in uscita tra il computer e Internet. In tale modalità, l'accesso al computer da parte di tutte le connessioni remote e l'accesso a Internet da parte di tutti i programmi sono bloccati. Una volta bloccato il firewall, è possibile sbloccarlo per consentire il traffico di rete.

Per sbloccare immediatamente il firewall e consentire il traffico di rete

1. Nei riquadri Home o Attività comuni con il **Menu standard** o il **Menu avanzato** attivato, fare clic su **Blocca firewall**.
2. Nel riquadro Blocco attivato, fare clic su **Sblocca**.
3. Nella finestra di dialogo, fare clic su **Sì** per confermare che si desidera sbloccare il firewall e consentire il traffico di rete.

Ripristino delle impostazioni del firewall

È possibile ripristinare rapidamente le impostazioni di protezione originali del firewall, ossia: livello di protezione impostato su Standard, suggerimenti intelligenti attivati, indirizzi IP affidabili ed esclusi reimpostati e tutti i programmi rimossi dal riquadro Autorizzazioni programmi.

Per ripristinare le impostazioni originali del firewall

1. Nei riquadri Home o Attività comuni con il **Menu standard** o il **Menu avanzato** attivato, fare clic su **Ripristina le impostazioni predefinite del firewall**.
2. Nel riquadro Ripristina le impostazioni predefinite della protezione firewall, fare clic su **Ripristina impostazioni predefinite**.
3. Nella finestra di dialogo Ripristina le impostazioni predefinite della protezione firewall, fare clic su **Sì** per confermare che si desidera ripristinare le impostazioni predefinite del firewall.

Impostazione del livello di protezione su Aperto

Quando il livello di protezione del firewall è impostato su Aperto, il firewall può consentire l'accesso a tutte le connessioni di rete in ingresso e in uscita. Per consentire l'accesso a programmi in precedenza bloccati, utilizzare il riquadro Autorizzazioni programmi.

Per impostare il livello di protezione del firewall su Aperto

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Aperto** venga visualizzato come livello corrente.
3. Fare clic su **OK**.

Nota: i programmi bloccati in precedenza rimangono tali quando il livello di protezione del firewall è impostato su **Aperto**. Per evitare che questo accada è possibile modificare la regola del programma in **Accesso completo**.

CAPITOLO 20

Gestione dei programmi e delle autorizzazioni

Personal Firewall consente di gestire e di creare autorizzazioni di accesso per programmi già esistenti e nuovi che richiedono accesso a Internet in ingresso e in uscita. Il firewall offre all'utente la possibilità di consentire ai programmi l'accesso completo o solo in uscita, ma anche di bloccare qualsiasi tipo di accesso.

In questo capitolo

Autorizzazione dell'accesso a Internet ai programmi

Alcuni programmi, quali i browser Internet, devono necessariamente accedere a Internet per funzionare in modo corretto.

Personal Firewall consente di utilizzare la pagina Autorizzazioni programmi per:

- Consentire l'accesso ai programmi
- Consentire solo l'accesso in uscita ai programmi
- Bloccare l'accesso ai programmi

È anche possibile consentire l'accesso completo e solo in uscita dal registro Eventi in uscita ed Eventi recenti

Autorizzazione dell'accesso completo per un programma

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. In Personal Firewall è incluso un elenco di programmi a cui viene automaticamente consentito l'accesso, tuttavia è possibile modificare tali autorizzazioni.

Per consentire a un programma l'accesso completo a Internet

1. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
3. In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Bloccato** o **Solo accesso in uscita**.
4. In **Azione**, fare clic su **Consenti accesso completo**.
5. Fare clic su **OK**.

Autorizzazione dell'accesso completo per un nuovo programma

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. In Personal Firewall è incluso un elenco di programmi a cui viene automaticamente consentito l'accesso completo, ma è possibile aggiungere un nuovo programma e modificare le relative autorizzazioni.

Per consentire a un nuovo programma l'accesso completo a Internet

1. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate**.
2. Nel riquadro **Firewall**, fare clic su **Autorizzazioni programmi**.
3. In **Autorizzazioni programmi**, fare clic su **Aggiungi programma autorizzato**.
4. Nella finestra di dialogo **Aggiungi programma** cercare e selezionare il programma che si desidera aggiungere.
5. Fare clic su **Apri**.
6. Fare clic su **OK**.

   Il programma appena aggiunto viene visualizzato in **Autorizzazioni programmi**.

Nota: è possibile modificare le autorizzazioni di un programma appena aggiunto in modo analogo a quello di un programma esistente, selezionandolo e quindi facendo clic su **Consenti solo accesso in uscita** o su **Blocca accesso** in **Azione**.

Autorizzazione dell'accesso completo dal registro Eventi recenti

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. È possibile selezionare un programma dal registro Eventi recenti e consentire ad esso l'accesso completo a Internet.

Per consentire a un programma l'accesso completo dal registro Eventi recenti

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In Eventi recenti, selezionare la descrizione dell'evento, quindi fare clic su **Consenti accesso completo**.
3. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare che si desidera consentire al programma l'accesso completo.

Argomenti correlati

- Visualizzazione degli eventi in uscita (pagina 170)

Autorizzazione dell'accesso completo dal registro Eventi in uscita

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. È possibile selezionare un programma dal registro Eventi in uscita e consentire ad esso l'accesso completo a Internet.

Per consentire a un programma l'accesso completo a Internet dal registro Eventi in uscita

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Selezionare **Rete & Internet**, quindi **Eventi in uscita**.
4. Nel riquadro Eventi in uscita, selezionare un indirizzo IP di origine, quindi fare clic su **Consenti accesso**.
5. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare che si desidera consentire al programma l'accesso completo a Internet.

Argomenti correlati

- Visualizzazione degli eventi in uscita (pagina 170)

Autorizzazione dell'accesso solo in uscita ai programmi

Alcuni programmi del computer richiedono l'accesso a Internet solo in uscita. Il firewall consente di autorizzare l'accesso a Internet solo in uscita per i programmi.

Autorizzazione dell'accesso solo in uscita per un programma

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. In Personal Firewall è incluso un elenco di programmi a cui viene automaticamente consentito l'accesso, tuttavia è possibile modificare tali autorizzazioni.

Per consentire a un programma l'accesso solo in uscita:

1. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
3. In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Bloccato** o **Accesso completo**.
4. In **Azione**, fare clic su **Consenti solo accesso in uscita**.
5. Fare clic su **OK**.

Autorizzazione dell'accesso solo in uscita dal registro Eventi recenti

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. È possibile selezionare un programma dal registro Eventi recenti e consentire ad esso l'accesso a Internet solo in uscita.

Per consentire a un programma l'accesso solo in uscita dal registro Eventi recenti

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In Eventi recenti, selezionare la descrizione dell'evento, quindi fare clic su **Consenti solo accesso in uscita**.
3. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare che si desidera consentire al programma l'accesso solo in uscita.

Argomenti correlati

- Visualizzazione degli eventi in uscita (pagina 170)

Autorizzazione dell'accesso solo in uscita dal registro Eventi in uscita

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. È possibile selezionare un programma dal registro Eventi in uscita e consentire ad esso l'accesso a Internet solo in uscita.

Per consentire a un programma l'accesso solo in uscita dal registro Eventi in uscita

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Selezionare **Rete & Internet**, quindi **Eventi in uscita**.
4. Nel riquadro Eventi in uscita, selezionare un indirizzo IP di origine, quindi fare clic su **Consenti solo accesso in uscita**.
5. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare che si desidera consentire al programma l'accesso solo in uscita.

Argomenti correlati

- Visualizzazione degli eventi in uscita (pagina 170)

Blocco dell'accesso a Internet per i programmi

Personal Firewall consente di impedire ai programmi l'accesso a Internet. Accertarsi che il blocco di un programma non interrompa la connessione di rete o non impedisca a un altro programma che richiede l'accesso a Internet di funzionare in modo corretto.

Blocco dell'accesso per un programma

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. In Personal Firewall è incluso un elenco di programmi a cui viene automaticamente consentito l'accesso, tuttavia è possibile bloccare tali autorizzazioni.

Per bloccare l'accesso a Internet per un programma

1. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
3. In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Accesso completo** o **Solo accesso in uscita**.
4. In **Azione**, fare clic su **Blocca accesso**.
5. Fare clic su **OK**.

Blocco dell'accesso per un nuovo programma

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. Personal Firewall comprende un elenco di programmi a cui è automaticamente consentito l'accesso completo, ma è comunque possibile aggiungere un nuovo programma e bloccarne l'accesso a Internet.

Per impedire a un nuovo programma di accedere a Internet

1. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
3. In **Autorizzazioni programmi**, fare clic su **Aggiungi programma bloccato**.
4. Nella finestra di dialogo **Aggiungi programma** cercare e selezionare il programma che si desidera aggiungere.
5. Fare clic su **Apri**.
6. Fare clic su **OK**.

   Il programma appena aggiunto viene visualizzato in **Autorizzazioni programmi**.

Nota: è possibile modificare le autorizzazioni di un programma appena aggiunto in modo analogo a quello di un programma esistente, selezionandolo e quindi facendo clic su **Consenti solo accesso in uscita** o su **Consenti accesso completo** in **Azione**.

Blocco dell'accesso dal registro Eventi recenti

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. È tuttavia possibile scegliere di impedire ai programmi di accedere a Internet dal registro Eventi recenti.

Per bloccare l'accesso a un programma dal registro Eventi recenti

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In Eventi recenti, selezionare la descrizione dell'evento, quindi fare clic su **Blocca accesso**.
3. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare che si desidera bloccare il programma.

Argomenti correlati

- Visualizzazione degli eventi in uscita (pagina 170)

Rimozione delle autorizzazioni di accesso per i programmi

Prima di rimuovere un'autorizzazione per un programma, accertarsi che l'eliminazione non influisca sulla funzionalità del computer o della connessione di rete.

Rimozione di un'autorizzazione per un programma

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. Personal Firewall comprende un elenco di programmi a cui è automaticamente consentito l'accesso completo, ma è comunque possibile rimuovere quelli aggiunti automaticamente e manualmente.

Per rimuovere un'autorizzazione per un nuovo programma

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
3. Selezionare un programma in **Autorizzazioni programmi**.
4. In **Azione**, fare clic su **Elimina autorizzazione programma**.
5. Fare clic su **OK**.

   Il programma viene rimosso dal riquadro Autorizzazioni programmi.

Nota: Personal Firewall impedisce all'utente di modificare alcuni programmi visualizzando in grigio e disattivando le relative azioni.

Informazioni sui programmi

Se non si è certi dell'autorizzazione da applicare per un programma, è possibile reperire informazioni utili sul sito Web HackerWatch di McAfee.

Reperimento delle informazioni sui programmi

Molti programmi del computer richiedono l'accesso a Internet in ingresso e in uscita. In Personal Firewall è incluso un elenco di programmi a cui viene automaticamente consentito l'accesso, tuttavia l'utente è in grado di modificare tali autorizzazioni.

Il firewall può aiutare a decidere se consentire o impedire a un programma di accedere a Internet. Accertarsi di essere connessi a Internet affinché il browser possa avviare senza problemi il sito Web HackerWatch di McAfee che fornisce informazioni aggiornate su programmi, requisiti di accesso a Internet e minacce per la protezione.

Per ottenere informazioni sui programmi

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
3. Selezionare un programma in **Autorizzazioni programmi**.
4. In **Azione**, fare clic su **Ulteriori informazioni**.

Reperimento delle informazioni sul programma dal registro Eventi in uscita

Personal Firewall consente di ottenere informazioni sui programmi che vengono visualizzate nel registro Eventi in uscita.

Prima di ottenere informazioni su un programma, accertarsi di disporre di una connessione e un browser Internet.

Per reperire informazioni sul programma dal registro Eventi in uscita

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Selezionare **Rete & Internet**, quindi **Eventi in uscita**.
4. Nel riquadro Eventi in uscita, selezionare un indirizzo IP di origine, quindi fare clic su **Ulteriori informazioni**.

   È possibile visualizzare le informazioni sul programma sul sito Web HackerWatch. HackerWatch fornisce informazioni

aggiornate su programmi, requisiti di accesso a Internet e minacce per la protezione.

Argomenti correlati

- Visualizzazione degli eventi in uscita (pagina 170)

CAPITOLO 21

Gestione dei servizi di sistema

Per funzionare correttamente, alcuni programmi, tra cui i server Web o i programmi server di condivisione dei file, devono accettare connessioni non richieste da altri computer attraverso porte progettate per i servizi di sistema. In genere il firewall chiude le porte dei servizi di sistema poiché rappresentano l'origine più probabile dei problemi di protezione del sistema. Per accettare le connessioni dai computer remoti è comunque necessario aprire tali porte.

Di seguito sono elencate le porte standard per servizi comuni.

- Porte 20-21 di File Transfer Protocol (FTP)
- Porta 143 del server di posta (IMAP)
- Porta 110 del server di posta (POP3)
- Porta 25 del server di posta (SMTP)
- Porta 445 di Microsoft Directory Server (MSFT DS)
- Porta 1433 di Microsoft SQL Server (MSFT SQL)
- Porta 3389 di Assistenza remota / Terminal Server (RDP)
- Porta 135 per chiamate di procedura remota (RPC)
- Porta 443 del server Web protetto (HTTPS)
- Porta 5000 di Universal Plug and Play (UPNP)
- Porta 80 del server Web (HTTP)
- Porte 137-139 per la condivisione file in Windows (NETBIOS)

In questo capitolo

Configurazione delle porte di servizio del sistema

Per consentire l'accesso remoto a un servizio sul computer occorre specificare il servizio e la porta associata da aprire. Selezionare un servizio e la relativa porta solo se si è certi di aprirla, il che non accade frequentemente.

Concessione dell'accesso alla porta di un servizio di sistema esistente

Dal riquadro Servizi di sistema è possibile aprire o chiudere una porta esistente per consentire o negare l'accesso a un servizio di rete del computer. Le porte dei servizi di sistema aperte possono rendere il computer vulnerabile a minacce per la protezione, pertanto devono essere aperte solo in caso di necessità.

Per consentire l'accesso alla porta di un servizio di sistema

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
3. Selezionare in **Apri porta del servizio di sistema** un servizio di sistema per aprire una porta.
4. Fare clic su **OK**.

Blocco dell'accesso a una porta dei servizi di sistema esistente

Dal riquadro Servizi di sistema è possibile aprire o chiudere una porta esistente per consentire o negare l'accesso a un servizio di rete del computer. Le porte dei servizi di sistema aperte possono rendere il computer vulnerabile a minacce per la protezione, pertanto devono essere aperte solo in caso di necessità.

Per bloccare l'accesso alla porta di un servizio di sistema

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
3. In **Apri porta del servizio di sistema**, deselezionare un servizio di sistema per chiudere una porta.
4. Fare clic su **OK**.

Configurazione di una nuova porta del servizio di sistema

Dal riquadro Servizi di sistema è possibile aggiungere una nuova porta del servizio che, a sua volta, può essere aperta o chiusa per consentire o negare l'accesso remoto a un servizio di rete nel computer. Le porte dei servizi di sistema aperte possono rendere il computer vulnerabile a minacce per la protezione, pertanto devono essere aperte solo in caso di necessità.

Per creare e configurare una nuova porta del servizio di sistema

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
3. Fare clic su **Aggiungi**.
4. In **Aggiungi configurazione porte**, specificare quanto segue:
   - Nome programma
   - Porte TCP/IP in ingresso
   - Porte TCP/IP in uscita
   - Porte UDP in ingresso
   - Porte UDP in uscita
5. Se lo si desidera, descrivere la nuova configurazione.
6. Fare clic su **OK**.

   La porta del servizio di sistema appena configurato viene visualizzata in **Apri porta del servizio di sistema**.

Modifica delle porte di servizi di sistema

Le porte aperte e chiuse consentono e negano l'accesso a un servizio di rete del computer. Dal riquadro Servizi di sistema, è possibile modificare le informazioni in ingresso e in uscita relative a una porta esistente. Se le informazioni sulla porta non vengono inserite in modo corrette, il servizio di sistema non funziona.

Per modificare una porta del servizio di sistema

1. Nel riquadro Configurazione Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
3. Selezionare un servizio di sistema e fare clic su **Modifica**.
4. In **Aggiungi configurazione porte**, specificare quanto segue:
   - Nome programma

- Porte TCP/IP in ingresso
- Porte TCP/IP in uscita
- Porte UDP in ingresso
- Porte UDP in uscita

5 Se lo si desidera, descrivere la configurazione modificata.

6 Fare clic su **OK**.

La porta del servizio di sistema appena modificata viene visualizzata in **Apri porta del servizio di sistema**.

Rimozione delle porte di servizi di sistema

Le porte aperte o chiuse consentono o negano l'accesso a un servizio di rete del computer. Nel riquadro Servizi di sistema è possibile rimuovere una porta esistente e il servizio di sistema associato. Dopo che una porta e il relativo servizio di sistema vengono rimossi dal riquadro Servizi di sistema, i computer remoti non sono più in grado di accedere al servizio di rete del computer.

Per rimuovere una porta del servizio di sistema

1 Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.

2 Nel riquadro Firewall, fare clic su **Servizi di sistema**.

3 Selezionare un servizio di sistema e fare clic su **Rimuovi**.

4 Nella finestra di dialogo **Servizi di sistema**, fare clic su **Sì** per confermare che si desidera eliminare il servizio di sistema.

La porta del servizio di sistema non viene più visualizzata nel riquadro Servizi di sistema.

CAPITOLO 22

Gestione delle connessioni al computer

È possibile configurare il firewall in modo tale da gestire connessioni remote specifiche al computer mediante la creazione di regole, basate sugli indirizzi IP, associate ai computer remoti. I computer associati a indirizzi IP affidabili si possono considerare ideonei alla connessione al computer in uso mentre gli indirizzi IP sconosciuti, sospetti o inattendibili, possono essere esclusi dalla connessione al computer.

Quando si consente una connessione, accertarsi che il computer considerato affidabile sia protetto. Se infatti tale computer fosse infetto per la presenza di un worm o di un altro meccanismo, il computer in uso potrebbe essere vulnerabile all'infezione. McAfee consiglia inoltre di proteggere con un firewall e un programma antivirus aggiornato anche i computer considerati affidabili. Il firewall non registra il traffico né genera avvisi relativi a eventi provenienti da indirizzi IP inclusi nell'elenco Indirizzi IP affidabili.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché Personal Firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione Internet comporti una specifica minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet. In base alle impostazioni di protezione, Personal Firewall avvisa l'utente nel momento in cui rileva un evento proveniente da un computer escluso.

In questo capitolo

Impostazione di una connessione come affidabile

È possibile aggiungere, modificare e rimuovere indirizzi IP affidabili nel riquadro IP affidabili ed esclusi nella sezione **Indirizzi IP affidabili**.

L'elenco **Indirizzi IP affidabili** nel riquadro IP affidabili ed esclusi consente a tutto il traffico proveniente da un determinato computer di raggiungere il computer in uso. Personal Firewall non registra il traffico né genera avvisi relativi a eventi provenienti da indirizzi IP inclusi nell'elenco **Indirizzi IP affidabili**.

Il firewall imposta come affidabili tutti gli indirizzi IP selezionati in elenco e consente sempre il traffico proveniente dagli stessi attraverso il firewall su qualsiasi porta. Gli eventi provenienti da indirizzi IP affidabili non vengono mai registrati dal firewall. L'attività intercorrente tra il computer associato a un indirizzo IP affidabile e quello in uso non viene filltrata o analizzata dal firewall.

Quando si consente una connessione, accertarsi che il computer considerato affidabile sia protetto. Se infatti tale computer fosse infetto per la presenza di un worm o di un altro meccanismo, il computer in uso potrebbe essere vulnerabile all'infezione. McAfee consiglia inoltre di proteggere con un firewall e un programma antivirus aggiornato anche i computer considerati affidabili.

Aggiunta di una connessione a un computer affidabile

Il firewall può essere utilizzato per aggiungere una connessione a un computer affidabile con i relativi indirizzi IP.

L'elenco **Indirizzi IP affidabili** nel riquadro IP affidabili ed esclusi consente a tutto il traffico proveniente da un determinato computer di raggiungere il computer in uso. Personal Firewall non registra il traffico né genera avvisi relativi a eventi provenienti da indirizzi IP inclusi nell'elenco **Indirizzi IP affidabili**.

I computer associati a indirizzi IP affidabili possono sempre stabilire connessioni al computer. Prima di aggiungere, modificare o rimuovere un indirizzo IP affidabile, assicurarsi che sia un indirizzo con il quale è sicuro comunicare.

Per aggiungere una connessione a un computer affidabile

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.
3. Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP affidabili**.
4. Fare clic su **Aggiungi**.
5. In **Aggiungi regola indirizzi IP affidabili**, effettuare una delle seguenti operazioni:
   - Selezionare un **Indirizzo IP singolo** e immettere l'indirizzo IP.
   - Selezionare un **Intervallo di indirizzi IP** e immettere gli indirizzi IP iniziali e finali nelle caselle **Da indirizzo IP** e **A indirizzo IP**.
6. Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.
7. Se lo si desidera, digitare una descrizione della regola.
8. Fare clic su **OK**.
9. Nella finestra di dialogo Aggiungi regola indirizzi IP affidabili, fare clic su **Sì** per confermare che si desidera aggiungere la connessione al computer affidabile.

   L'indirizzo IP appena aggiunto viene visualizzato in **Indirizzi IP affidabili**.

Aggiunta di un computer affidabile dal registro Eventi in ingresso

È possibile aggiungere una connessione a un computer affidabile con il relativo indirizzo IP dal registro Eventi in ingresso.

I computer associati a indirizzi IP affidabili possono sempre stabilire connessioni al computer. Prima di aggiungere, modificare o rimuovere un indirizzo IP affidabile, assicurarsi che sia un indirizzo con il quale è sicuro comunicare.

Per aggiungere una connessione a un computer affidabile dal registro Eventi in ingresso

1. Assicurarsi che il menu avanzato sia attivato. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Rete & Internet**, quindi su **Eventi in ingresso**.
4. Nel riquadro Eventi in ingresso, selezionare un indirizzo IP di origine, quindi fare clic su **Imposta indirizzo come affidabile**.
5. Nella finestra di dialogo Aggiungi regola indirizzi IP affidabili, fare clic su **Sì** per confermare che si desidera impostare l'indirizzo IP come affidabile.

   L'indirizzo IP appena aggiunto viene visualizzato in **Indirizzi IP affidabili**.

Argomenti correlati

- Registrazione eventi (pagina 168)

Modifica di una connessione a un computer affidabile

Il firewall può essere utilizzato per modificare una connessione a un computer affidabile con i relativi indirizzi IP.

I computer associati a indirizzi IP affidabili possono sempre stabilire connessioni al computer. Prima di aggiungere, modificare o rimuovere un indirizzo IP affidabile, assicurarsi che sia un indirizzo con il quale è sicuro comunicare.

Per modificare una connessione a un computer affidabile

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.
3. Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP affidabili**.
4. Selezionare un indirizzo IP, quindi fare clic su **Modifica**.
5. In **Aggiungi regola indirizzi IP affidabili**, effettuare una delle seguenti operazioni:
   - Selezionare un **Indirizzo IP singolo** e immettere l'indirizzo IP.
   - Selezionare un **Intervallo di indirizzi IP** e immettere gli indirizzi IP iniziali e finali nelle caselle **Da indirizzo IP** e **A indirizzo IP**.
6. Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.
7. Se lo si desidera, digitare una descrizione della regola.
8. Fare clic su **OK**.

   L'indirizzo IP modificato viene visualizzato in **Indirizzi IP affidabili**.

Rimozione di una connessione a un computer affidabile

Il firewall può essere utilizzato per rimuovere una connessione a un computer affidabile con i relativi indirizzi IP.

I computer associati a indirizzi IP affidabili possono sempre stabilire connessioni al computer. Prima di aggiungere, modificare o rimuovere un indirizzo IP affidabile, assicurarsi che sia un indirizzo con il quale è sicuro comunicare.

Per rimuovere una connessione a un computer affidabile

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.
3. Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP affidabili**.
4. Selezionare un indirizzo IP, quindi fare clic su **Rimuovi**.
5. Nella finestra di dialogo **IP affidabili ed esclusi**, fare clic su **Sì** per confermare che si desidera rimuovere l'indirizzo IP affidabile in **Indirizzi IP affidabili**.

Esclusione delle connessioni a computer

È possibile aggiungere, modificare e rimuovere indirizzi IP affidabili nel riquadro IP affidabili ed esclusi nella sezione **Indirizzi IP esclusi**.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché Personal Firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione Internet comporti una specifica minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet. In base alle impostazioni di protezione, Personal Firewall avvisa l'utente nel momento in cui rileva un evento proveniente da un computer escluso.

Aggiunta di una connessione a un computer escluso

Il firewall può essere utilizzato per aggiungere una connessione a un computer escluso con i relativi indirizzi IP.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché Personal Firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione Internet comporti una specifica minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet. In base alle impostazioni di protezione, Personal Firewall avvisa l'utente nel momento in cui rileva un evento proveniente da un computer escluso.

Per aggiungere una connessione a un computer escluso

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.
3. Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP esclusi**.
4. Fare clic su **Aggiungi**.
5. In Aggiungi regola indirizzi IP esclusi, effettuare una delle seguenti operazioni:
   - Selezionare un **Indirizzo IP singolo** e immettere l'indirizzo IP.

- Selezionare un **Intervallo di indirizzi IP** e immettere gli indirizzi IP iniziali e finali nei campi **Da indirizzo IP** e **A indirizzo IP**.

6 Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.

7 Se lo si desidera, digitare una descrizione della regola.

8 Fare clic su **OK**.

9 Nella finestra di dialogo **Aggiungi regola indirizzi IP esclusi**, fare clic su **Sì** per confermare che si desidera aggiungere la connessione al computer escluso.

L'indirizzo IP appena aggiunto viene visualizzato in **Indirizzi IP esclusi**.

Modifica di una connessione a un computer escluso

Il firewall può essere utilizzato per modificare una connessione a un computer escluso con i relativi indirizzi IP.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché Personal Firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione Internet comporti una specifica minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet. In base alle impostazioni di protezione, Personal Firewall avvisa l'utente nel momento in cui rileva un evento proveniente da un computer escluso.

Per modificare una connessione a un computer escluso

1 Nel riquadro Configurazione Internet & rete, fare clic su **Avanzate**.

2 Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.

3 Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP esclusi**.

4 Selezionare un indirizzo IP, quindi fare clic su **Modifica**.

5 In **Aggiungi regola indirizzi IP affidabili**, effettuare una delle seguenti operazioni:

- Selezionare un **Indirizzo IP singolo** e digitare l'indirizzo IP.
- Selezionare un **Intervallo di indirizzi IP**, quindi digitare gli indirizzi IP iniziali e finali nei campi **Da indirizzo IP** e **A indirizzo IP**.

6 Facoltativamente, selezionare **La regola scade tra** e digitare il numero di giorni in cui applicare la regola.

7 Se lo si desidera, digitare una descrizione della regola.

Fare clic su **OK**. L'indirizzo IP modificato viene visualizzato in **Indirizzi IP esclusi**.

Rimozione di una connessione a un computer escluso

Il firewall può essere utilizzato per rimuovere una connessione a un computer escluso con i relativi indirizzi IP.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché Personal Firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione Internet comporti una specifica minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet. In base alle impostazioni di protezione, Personal Firewall avvisa l'utente nel momento in cui rileva un evento proveniente da un computer escluso.

Per rimuovere una connessione a un computer escluso

1 Nel riquadro Configurazione Internet & rete, fare clic su **Avanzate**.

2 Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.

3 Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP esclusi**.

4 Selezionare un indirizzo IP, quindi fare clic su **Rimuovi**.

5 Nella finestra di dialogo **IP affidabili ed esclusi**, fare clic su **Sì** per confermare che si desidera rimuovere l'indirizzo IP da **Indirizzi IP esclusi**.

Esclusione di un computer dal registro Eventi in ingresso

È possibile escludere una connessione a un computer con il relativo indirizzo IP dal registro Eventi in ingresso.

Poiché gli indirizzi IP visualizzati nel registro Eventi in ingresso sono bloccati l'esclusione di un indirizzo non aggiunge nessuna ulteriore protezione a meno che il computer non utilizzi delle porte deliberatamente aperte o non includa un programma a cui è stato consentito l'accesso a Internet.

Aggiungere un indirizzo IP all'elenco **Indirizzi IP esclusi** solo se si dispone di una o più porte deliberatamente aperte e se si ha motivo di credere che sia necessario bloccare l'accesso di tale indirizzo alle porte aperte..

È possibile utilizzare la pagina Eventi in ingresso, che elenca gli indirizzi IP del traffico Internet in ingresso, per escludere un indirizzo IP che sembra essere l'origine di attività Internet sospette o indesiderate.

Per escludere una connessione a un computer affidabile dal registro Eventi in ingresso

1. Assicurarsi che il menu avanzato sia attivato. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Rete & Internet**, quindi su **Eventi in ingresso**.
4. Nel riquadro Eventi in ingresso, selezionare un indirizzo IP di origine, quindi fare clic su **Escludi questo indirizzo**.
5. Nella finestra di dialogo **Aggiungi regola indirizzi IP esclusi**, fare clic su **Sì** per confermare che si desidera escludere l'indirizzo IP.

   L'indirizzo IP appena aggiunto viene visualizzato in **Indirizzi IP esclusi**.

Argomenti correlati

- Registrazione eventi (pagina 168)

Esclusione di un computer dal registro Eventi Sistema rilevamento intrusioni

È possibile escludere una connessione a un computer e il relativo indirizzo IP dal registro Eventi Sistema rilevamento intrusioni.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché Personal Firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione Internet comporti una specifica minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet. In base alle impostazioni di protezione, Personal Firewall avvisa l'utente nel momento in cui rileva un evento proveniente da un computer escluso.

Per escludere una connessione a un computer dal registro Eventi Sistema rilevamento intrusioni

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Rete& Internet**, quindi su **Eventi Sistema rilevamento intrusioni**.
4. Nel riquadro Eventi Sistema rilevamento intrusioni, selezionare un indirizzo IP di origine, quindi fare clic su **Escludi questo indirizzo**.
5. Nella finestra di dialogo **Aggiungi regola indirizzi IP esclusi**, fare clic su **Sì** per confermare che si desidera escludere l'indirizzo IP.

   L'indirizzo IP appena aggiunto viene visualizzato in **Indirizzi IP esclusi**.

Argomenti correlati

- Registrazione eventi (pagina 168)

CAPITOLO 23

Registrazione, monitoraggio e analisi

Il firewall fornisce registrazione, monitoraggio e analisi estesi e di facile lettura relativi a eventi e traffico Internet. La comprensione di tali argomenti agevola la gestione delle connessioni Internet.

In questo capitolo

Registrazione eventi

Il firewall consente di specificare se si desidera attivare o disattivare la registrazione e, nel primo caso, quali tipi di eventi registrare. Grazie alla registrazione degli eventi è possibile visualizzare gli eventi recenti in ingresso e in uscita e anche quelli di rilevamento intrusioni.

Configurazione delle impostazioni del registro eventi

Per tenere traccia di eventi e attività del firewall, è possibile specificare e configurare i tipi di eventi da visualizzare.

Per configurare la registrazione degli eventi

1. Nel riquadro Configurazione di Internet & rete, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Impostazioni registro eventi**.
3. Nel riquadro Impostazioni registro eventi, effettuare una delle seguenti operazioni:
   - Selezionare **Registra evento** per attivare la registrazione degli eventi.
   - Selezionare **Non registrare l'evento** per disattivare la registrazione degli eventi.
4. Specificare in **Impostazioni registro eventi** i tipi di eventi da registrare. Tra i tipi di eventi sono inclusi:
   - Ping ICMP
   - Traffico da indirizzi IP esclusi
   - Eventi su porte dei servizi di sistema
   - Eventi su porte sconosciute
   - Eventi del Sistema di rilevamento intrusioni (IDS, Intrusion Detection System)
5. Per impedire la registrazione su determinate porte, selezionare **Non registrare gli eventi sulle porte seguenti**, quindi immettere i singoli numeri di porta separati da virgole o intervalli separati da trattini, ad esempio: `137-139, 445, 400-5000`.
6. Fare clic su **OK**.

Visualizzazione degli eventi recenti

Quando l'accesso è attivato, è possibile visualizzare gli eventi recenti. Nel riquadro Eventi recenti sono visualizzate la data e la descrizione dell'evento. Il riquadro visualizza solo l'attività dei programmi a cui è stato esplicitamente impedito l'accesso a Internet.

Per visualizzare gli eventi recenti del firewall

- Nel riquadro Attività comuni del **Menu avanzato**, fare clic su **Rapporti e registri** o su **Visualizza eventi recenti**. In alternativa, fare clic su **Visualizza eventi recenti** nel riquadro Attività comuni dal menu standard.

Visualizzazione degli eventi in ingresso

Quando l'accesso è attivato, è possibile visualizzare e ordinare gli eventi in ingresso.

Il registro Eventi in ingresso include le seguenti categorie di registrazione:

- Data e ora
- Indirizzo IP di origine
- Nome host
- Informazioni e tipi di eventi

Per visualizzare gli eventi in ingresso del firewall

1. Assicurarsi che il menu avanzato sia attivato. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Rete & Internet**, quindi su **Eventi in ingresso**.

Nota: un indirizzo IP può essere impostato come affidabile, escluso e rintracciato dal registro Eventi in ingresso.

Argomenti correlati

- Aggiunta di un computer affidabile dal registro Eventi in ingresso (pagina 158)
- Esclusione di un computer dal registro Eventi in ingresso (pagina 164)
- Rintracciamento di un computer dal registro Eventi in ingresso (pagina 174)

Visualizzazione degli eventi in uscita

Quando l'accesso è attivato, è possibile visualizzare gli eventi in uscita. Gli eventi in uscita includono il nome del programma che tenta l'accesso in uscita, la data e l'ora dell'evento e il percorso del programma sul computer.

Per visualizzare gli eventi in uscita del firewall

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Selezionare **Rete & Internet**, quindi **Eventi in uscita**.

Nota: è possibile consentire l'accesso completo e solo in uscita a un programma dal registro Eventi in uscita, nonché individuare ulteriori informazioni relative al programma.

Argomenti correlati

- Autorizzazione dell'accesso completo dal registro Eventi in uscita (pagina 142)
- Autorizzazione dell'accesso solo in uscita dal registro Eventi in uscita (pagina 144)
- Reperimento delle informazioni sul programma dal registro Eventi in uscita (pagina 148)

Visualizzazione degli eventi di rilevamento intrusioni

Quando l'accesso è attivato, è possibile visualizzare gli eventi in ingresso. Gli eventi di rilevamento intrusioni visualizzano la data e l'ora, l'IP di origine e il nome host dell'evento. Nel registro viene inoltre descritto il tipo di evento.

Per visualizzare gli eventi di rilevamento intrusioni

1. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2. In Eventi recenti, fare clic su **Visualizza registro**.
3. Fare clic su **Retee Internet**, quindi su **Eventi Sistema rilevamento intrusioni**.

Nota: un indirizzo IP può essere escluso e rintracciato dal registro Eventi Sistema rilevamento intrusioni.

Argomenti correlati

- Esclusione di un computer dal registro Eventi Sistema rilevamento intrusioni (pagina 165)
- Rintracciamento di un computer dal registro Eventi Sistema rilevamento intrusioni (pagina 175)

Utilizzo delle statistiche

Il firewall sfrutta il sito Web della protezione HackerWatch di McAfee per fornire statistiche sugli eventi di protezione e l'attività delle porte Internet globali.

Visualizzazione delle statistiche globali sugli eventi di protezione

HackerWatch tiene traccia degli eventi di protezione Internet a livello mondiale, visualizzabili da SecurityCenter. Le informazioni registrate elencano gli incidenti segnalati a HackerWatch nel corso delle ultime 24 ore, degli ultimi 7 giorni e degli ultimi 30 giorni.

Per visualizzare le statistiche globali sulla protezione

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **HackerWatch**.
3. Visualizzare le statistiche sugli eventi di protezione in **Traccia degli eventi**.

Visualizzazione dell'attività globale delle porte Internet

HackerWatch tiene traccia degli eventi di protezione Internet a livello mondiale, visualizzabili da SecurityCenter. Le informazioni visualizzate includono gli eventi principali relativi alle porte segnalati in HackerWatch durante gli ultimi sette giorni. In genere vengono visualizzate le informazioni sulle porte HTTP, TCP e UDP.

Per visualizzare l'attività delle porte a livello mondiale

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **HackerWatch**.
3. Visualizzare gli eventi principali relativi alle porte in **Attività recente sulle porte**.

Rintracciamento del traffico Internet

Il firewall prevede alcune opzioni per rintracciare il traffico Internet, che consentono di rintracciare geograficamente un computer di rete, ottenere informazioni relative a dominio e rete e rintracciare i computer dai registri Eventi in ingresso ed Eventi Sistema di rilevamento intrusioni.

Rintracciamento geografico di un computer di rete

È possibile utilizzare il tracciato visivo per individuare geograficamente un computer che è connesso o tenta di connettersi al computer in uso, tramite il nome o l'indirizzo IP, nonché per accedere alle informazioni sulla rete e ai dati per la registrazione. L'esecuzione del tracciato visivo consente di visualizzare il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione.

Per individuare geograficamente un computer

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3. Digitare l'indirizzo IP del computer e fare clic su **Rintraccia**.
4. In **Tracciato visivo**, selezionare **Visualizzazione mappa**.

Nota: non è possibile registrare eventi da indirizzi IP di loopback, privati o non validi.

Dati per la registrazione del computer

È possibile ottenere i dati per la registrazione di un computer da SecurityCenter tramite Tracciato visivo. Le informazioni includono il nome del dominio, il nome e l'indirizzo dell'intestatario e il contatto amministrativo.

Per ottenere le informazioni sul dominio di un computer

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3. Digitare l'indirizzo IP del computer, quindi fare clic su **Rintraccia**.
4. In **Tracciato visivo**, selezionare **Visualizzazione intestatario dominio**.

Informazioni sulla rete del computer

È possibile ottenere informazioni sulla rete di un computer da SecurityCenter tramite Tracciato visivo. Tali informazioni includono dettagli sulla rete in cui risiede il dominio in questione.

Per ottenere informazioni sulla rete di un computer

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3. Digitare l'indirizzo IP del computer, quindi fare clic su **Rintraccia**.
4. In **Tracciato visivo**, selezionare **Visualizzazione rete**.

Rintracciamento di un computer dal registro Eventi in ingresso

Dal riquadro Eventi in ingresso, è possibile rintracciare un indirizzo IP visualizzato nel registro Eventi in ingresso.

Per rintracciare l'indirizzo IP del computer dal registro Eventi in ingresso

1. Assicurarsi che il menu avanzato sia attivato. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Rete & Internet**, quindi su **Eventi in ingresso**.
4. Nel riquadro Eventi in ingresso, selezionare un indirizzo IP di origine, quindi fare clic su **Rintraccia questo indirizzo**.
5. Nel riquadro Tracciato visivo, fare clic su una delle seguenti opzioni:
   - **Visualizzazione mappa**: consente di individuare geograficamente un computer mediante l'indirizzo IP selezionato.
   - **Visualizzazione intestatario dominio**: consente di individuare le informazioni sul dominio mediante l'indirizzo IP selezionato.
   - **Visualizzazione rete**: consente di individuare le informazioni sulla rete mediante l'indirizzo IP selezionato.
6. Fare clic su **Fine**.

Argomenti correlati

- Rintracciamento del traffico Internet (pagina 173)
- Visualizzazione degli eventi in ingresso (pagina 169)

Rintracciamento di un computer dal registro Eventi Sistema rilevamento intrusioni

Dal riquadro Eventi Sistema rilevamento intrusioni, è possibile rintracciare un indirizzo IP visualizzato nell'omonimo registro.

Per rintracciare l'indirizzo IP del computer dal registro Eventi Sistema rilevamento intrusioni

1. Nel riquadro Attività comuni, fare clic su **Rapporti & registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Rete& Internet**, quindi su **Eventi Sistema rilevamento intrusioni**.Nel riquadro Eventi Sistema rilevamento intrusioni, selezionare un indirizzo IP di origine, quindi fare clic su **Rintraccia questo indirizzo**.
4. Nel riquadro Tracciato visivo, fare clic su una delle seguenti opzioni:
   - **Visualizzazione mappa**: consente di individuare geograficamente un computer mediante l'indirizzo IP selezionato.
   - **Visualizzazione intestatario dominio**: consente di individuare le informazioni sul dominio mediante l'indirizzo IP selezionato.
   - **Visualizzazione rete**: consente di individuare le informazioni sulla rete mediante l'indirizzo IP selezionato.
5. Fare clic su **Fine**.

Argomenti correlati

- Rintracciamento del traffico Internet (pagina 173)
- Registrazione, monitoraggio e analisi (pagina 167)

Rintracciamento di un indirizzo IP monitorato

È possibile rintracciare un indirizzo IP monitorato per ottenere una visualizzazione geografica indicante il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione. Sono inoltre reperibili i dati per la registrazione e le informazioni sulla rete relative all'indirizzo IP.

Per monitorare l'utilizzo della larghezza di banda dei programmi

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Programmi attivi**.
4. Selezionare un programma e l'indirizzo IP visualizzato sotto il nome del programma.
5. In **Attività programmi**, fare clic su **Rintraccia questo indirizzo IP**.
6. Nella sezione **Tracciato visivo** è possibile visualizzare una mappa che indica il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione. Sono inoltre reperibili i dati per la registrazione e le informazioni sulla rete relative all'indirizzo IP.

Nota: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Tracciato visivo**.

Argomenti correlati

- Monitoraggio del traffico Internet (pagina 177)

Monitoraggio del traffico Internet

Personal Firewall prevede alcuni metodi di monitoraggio del traffico Internet, tra cui:

- **Grafico analisi traffico**: visualizza il traffico Internet recente in entrata e in uscita.
- **Grafico utilizzo traffico**: visualizza la percentuale di larghezza di banda utilizzata dalle applicazioni maggiormente attive durante le ultime 24 ore.
- **Programmi attivi**: visualizza i programmi attualmente utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

Informazioni sul grafico analisi traffico

Il grafico Analisi traffico è una rappresentazione numerica e grafica del traffico Internet, sia in ingresso che in uscita. Inoltre, la funzione Controllo traffico visualizza i programmi attualmente utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

Dal riquadro Analisi traffico è possibile visualizzare il traffico Internet, in ingresso e in uscita, con velocità di trasferimento corrente, media e massima. È inoltre possibile visualizzare il volume del traffico, compresi la quantità di traffico dall'avvio del firewall e il traffico complessivo relativo al mese in corso e ai precedenti.

Il riquadro Analisi traffico mostra l'attività Internet in tempo reale nel computer in uso, inclusi il volume e la velocità di traffico Internet recente, in ingresso e in uscita, la velocità di connessione e i byte totali trasferiti attraverso Internet.

La linea verde continua rappresenta la velocità di trasferimento corrente del traffico in ingresso. La linea verde tratteggiata rappresenta la velocità di trasferimento media del traffico in ingresso. Se la velocità di trasferimento corrente e la velocità di trasferimento media sono identiche, la linea tratteggiata non viene visualizzata sul grafico e la linea continua rappresenta entrambe le velocità.

La linea rossa continua rappresenta la velocità di trasferimento corrente del traffico in uscita. La linea rossa tratteggiata rappresenta la velocità di trasferimento media del traffico in uscita. Se la velocità di trasferimento corrente e la velocità di trasferimento media sono identiche, la linea tratteggiata non viene visualizzata sul grafico e la linea continua rappresenta entrambe le velocità.

Argomenti correlati

- Analisi del traffico in ingresso e in uscita (pagina 178)

Analisi del traffico in ingresso e in uscita

Il grafico Analisi traffico è una rappresentazione numerica e grafica del traffico Internet, sia in ingresso che in uscita. Inoltre, la funzione Controllo traffico visualizza i programmi attualmente utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

Per analizzare il traffico in ingresso e in uscita

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Analisi traffico**.

Suggerimento: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Analisi traffico**.

Argomenti correlati

- Informazioni sul grafico analisi traffico (pagina 177)

Monitoraggio della larghezza di banda dei programmi

È possibile visualizzare il grafico a torta che mostra la percentuale approssimativa di larghezza di banda utilizzata dai programmi più attivi presenti nel computer durante le ultime ventiquattro ore. Il grafico a torta fornisce la rappresentazione visiva delle quantità di larghezza di banda relative utilizzate dai programmi.

Per monitorare l'utilizzo della larghezza di banda dei programmi

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Utilizzo traffico**.

Suggerimento: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Utilizzo traffico**.

Monitoraggio dell'attività dei programmi

È possibile visualizzare l'attività dei programmi in ingresso e in uscita in cui vengono mostrate le connessioni e le porte del computer remoto.

Per monitorare l'utilizzo della larghezza di banda dei programmi

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Programmi attivi**.
4. È possibile visualizzare le seguenti informazioni:
   - Grafico attività programmi: selezionare un programma per visualizzare il grafico della relativa attività.
   - Connessione in ascolto: selezionare un elemento in ascolto sotto il nome del programma.
   - Connessione al computer: selezionare un indirizzo IP sotto il nome del programma, il processo di sistema o il servizio.

Nota: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Programmi attivi**.

CAPITOLO 24

Informazioni sulla protezione Internet

Il firewall utilizza il sito Web della protezione di McAfee, HackerWatch, per fornire informazioni aggiornate sui programmi e sull'attività Internet globale. HackerWatch prevede inoltre un'esercitazione HTML relativa al firewall.

In questo capitolo

Avvio dell'esercitazione HackerWatch

Per ottenere ulteriori informazioni sul firewall, è possibile accedere all'esercitazione HackerWatch da SecurityCenter.

Per avviare l'esercitazione HackerWatch

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **HackerWatch**.
3. In **Risorse di HackerWatch**, fare clic su **Visualizza esercitazione**.

CAPITOLO 25

McAfee EasyNetwork

McAfee® EasyNetwork consente la condivisione protetta di file, semplifica i trasferimenti di file e automatizza la condivisione delle stampanti tra computer della rete domestica.

Prima di iniziare a utilizzare EasyNetwork, è opportuno acquisire dimestichezza con alcune delle funzioni più comuni. I dettagli relativi alla configurazione e all'utilizzo di queste funzioni sono reperibili nella Guida in linea di EasyNetwork.

In questo capitolo

Funzioni

EasyNetwork fornisce le funzioni riportate di seguito.

Condivisione di file

EasyNetwork semplifica la condivisione dei file tra il computer in uso e gli altri computer della rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer membri della rete gestita (cioè che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri membri.

Trasferimento di file

È possibile inviare file ad altri computer purché siano membri della rete gestita. Nel momento in cui si riceve un file, esso viene visualizzato nella casella di EasyNetwork, un percorso di archiviazione temporaneo per tutti i file ricevuti da altri computer della rete.

Condivisione automatica di stampanti

Dopo che l'utente è diventato membro di una rete gestita, EasyNetwork condivide automaticamente tutte le stampanti locali collegate al computer in uso, utilizzando il nome corrente della stampante come nome della stampante condivisa, rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso.

CAPITOLO 26

Impostazione di EasyNetwork

Prima di poter utilizzare le funzioni di EasyNetwork è necessario avviare il programma e diventare membro della rete gestita. Successivamente, sarà possibile abbandonare la rete in qualsiasi momento.

In questo capitolo

Avvio di EasyNetwork

Per impostazione predefinita viene richiesto di avviare EasyNetwork immediatamente dopo l'installazione, per quanto sia anche possibile avviarlo in un secondo momento.

Avvio di EasyNetwork

Per impostazione predefinita viene richiesto di avviare EasyNetwork immediatamente dopo l'installazione, benché sia anche possibile avviarlo in un secondo momento.

Per avviare EasyNetwork:

- Nel menu **Start**, scegliere **Programmi**, quindi **McAfee** e fare clic su **McAfee EasyNetwork**.

Suggerimento: se si decide di creare icone sul desktop e icone di avvio rapido durante l'installazione, è anche possibile avviare EasyNetwork facendo doppio clic sulla relativa icona sul desktop oppure, facendo un solo clic sull'icona McAfee EasyNetwork nell'area di notifica sulla destra della barra delle applicazioni.

Aggiunta di un membro alla rete gestita

Dopo aver installato SecurityCenter, un agente di rete viene aggiunto al computer ed eseguito in background. In EasyNetwork, l'agente di rete è responsabile del rilevamento di una connessione di rete valida, delle stampanti locali da condividere e del monitoraggio dello stato di rete.

Se non viene trovato nessun altro computer che esegue l'agente sulla rete a cui è connesso l'utente, quest'ultimo diventerà automaticamente membro della rete e gli verrà chiesto di stabilire se si tratta di rete affidabile. Poiché è il primo computer a diventare membro della rete, il nome del computer in uso viene incluso nel nome della rete, che potrà tuttavia essere rinominata in qualsiasi momento.

Quando un computer stabilisce una connessione alla rete, richiede agli altri computer attualmente in rete l'autorizzazione a diventarne membro. Alla richiesta è possibile acconsentire da qualsiasi computer con autorizzazioni amministrative in rete. La persona che concede le autorizzazioni può inoltre determinare il livello di autorizzazione del computer attualmente membro della rete, ad esempio, Guest (solo capacità di trasferimento file) oppure completo/con privilegi di amministratore (capacità di trasferimento e di condivisione file). In EasyNetwork, i computer che dispongono di accesso con privilegi di amministratore possono consentire l'accesso ad altri computer e gestire autorizzazioni (vale a dire, alzare o abbassare il livello dei computer) mentre i computer con accesso completo non sono in grado di eseguire attività amministrative di questo tipo. Prima di consentire al computer di diventare membro, viene anche eseguito un controllo di protezione.

Nota: una volta diventato membro di una rete, se sono stati installati altri programmi di rete McAfee (ad esempio, McAfee Wireless Network Security o Network Manager), il computer verrà anche riconosciuto come computer gestito in quei programmi. Il livello di autorizzazione assegnato al computer viene applicato a tutti i programmi di rete McAfee. Per ulteriori informazioni sul significato di autorizzazione guest, completa o con autorizzazioni amministrative in altri programmi di rete McAfee, consultare la relativa documentazione.

Aggiunta di un membro alla rete

Quando un computer si connette a una rete affidabile per la prima volta dopo l'installazione di EasyNetwork, viene visualizzato un messaggio che chiede al computer se intende diventare membro di una rete gestita. Se il computer accetta di diventarlo, verrà inviata una richiesta a tutti gli altri computer in rete che dispongono di accesso con privilegi di amministratore. Tale richiesta deve essere accettata prima che il computer possa condividere stampanti o file oppure inviare e copiare file in rete. Al primo computer della rete vengono automaticamente fornite autorizzazioni amministrative in rete.

Per diventare membro di una rete:

1. Nella finestra File condivisi, fare clic su **Sì, aggiungi il computer alla rete adesso**.
   Quando un computer con privilegi di amministratore in rete acconsente alla richiesta, viene visualizzato un messaggio in cui viene chiesto se si intende consentire al computer in uso e agli altri della rete di gestire le impostazioni di protezione reciproche.
2. Per consentire al computer in uso e agli altri computer di rete di gestire le reciproche impostazioni di protezione, fare clic su **Sì**, altrimenti fare clic su **No**.
3. Verificare che le carte da gioco visualizzate nella finestra di dialogo di conferma della protezione siano visualizzate anche sul computer a partire dal quale sono state concesse le autorizzazioni, quindi fare clic su **Conferma**.

Nota: se le stesse carte da gioco visualizzate nella finestra di dialogo di conferma della protezione non vengono visualizzate anche sul computer a partire dal quale sono state concesse le autorizzazioni, significa che si è verificata una violazione della protezione sulla rete gestita. Diventare membro della rete può mettere a rischio il proprio computer; pertanto, fare clic su **Rifiuta** nella finestra di dialogo di conferma.

Autorizzazione di accesso alla rete

Quando un computer chiede di diventare membro di una rete gestita, viene inviato un messaggio agli altri computer in rete che dispongono di accesso con privilegi di amministratore. Il primo computer a rispondere al messaggio diventa quello dell'utente che concede le autorizzazioni e, come tale, l'utente di questo computer sarà responsabile della scelta del tipo di accesso: Guest, completo o con privilegi di amministratore.

Per autorizzare l'accesso alla rete:

1. Nel messaggio di avviso, selezionare una delle seguenti caselle di controllo:
   - **Concedi accesso Guest**: consente all'utente di inviare file ad altri computer, ma non di condividerli.
   - **Concedi accesso completo a tutte le applicazioni della rete gestita**: consente all'utente di inviare e di condividere file.
   - **Concedi accesso con privilegi di amministratore a tutte le applicazioni della rete gestita**: consente all'utente di inviare e condividere file, autorizzare l'accesso ad altri computer e regolarne i livelli di autorizzazione.
2. Fare clic su **Consenti accesso**.
3. Verificare che le carte da gioco visualizzate nella finestra di dialogo di conferma della protezione siano visualizzate anche sul computer, quindi fare clic su **Conferma**.

Nota: se le stesse carte da gioco visualizzate nella finestra di dialogo di conferma della protezione non vengono visualizzate anche sul computer, significa che si è verificata una violazione della protezione sulla rete gestita. Poiché concedere a questo computer l'accesso alla rete potrebbe mettere a rischio il computer in uso, fare clic su **Rifiuta** nella finestra di dialogo di conferma della protezione.

Ridenominazione della rete

Per impostazione predefinita, il nome della rete include il nome del primo computer diventato membro della rete, tuttavia è possibile cambiarlo in qualsiasi momento. Quando si rinomina la rete, è possibile modificare la relativa descrizione visualizzata in EasyNetwork.

Per rinominare la rete:

1. Nel menu **Opzioni**, scegliere **Configura**.
2. Nella finestra di dialogo Configura, digitare il nome della rete nella casella **Nome di rete**.
3. Fare clic su **OK**.

Abbandono della rete gestita

Se l'utente diventato membro di una rete non intende più essere tale, può abbandonare la rete. Una volta che si è optato per l'abbandono è comunque possibile ridiventare membro della rete in qualsiasi momento, purché a tale scopo venga concessa l'autorizzazione e venga nuovamente effettuato un controllo di protezione. Per ulteriori informazioni, vedere Aggiunta di un membro alla rete gestita (pagina 187).

Abbandono della rete gestita

È possibile abbandonare una rete gestita di cui si è membri.

Per abbandonare una rete gestita:

1. Nel menu **Strumenti**, scegliere **Abbandona rete**.
2. Nella finestra di dialogo Abbandona rete, selezionare il nome della rete che si desidera abbandonare.
3. Fare clic su **Abbandona rete**.

CAPITOLO 27

Condivisione e invio di file

EasyNetwork semplifica la condivisione e l'invio di file sul computer in uso tra gli altri computer presenti in rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer membri della rete gestita (cioè che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri computer membri.

In questo capitolo

Condivisione di file

EasyNetwork semplifica la condivisione dei file tra il computer in uso e gli altri computer della rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer membri della rete gestita (cioè che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri computer membri. Se si condivide una cartella, vengono condivisi tutti i file in essa contenuti e le relative sottocartelle, tuttavia la condivisione delle cartelle aggiunte successivamente non avviene automaticamente. Una volta eliminati, file e cartelle condivisi vengono automaticamente rimossi dalla finestra File condivisi. È possibile interrompere la condivisione di un file in qualsiasi momento.

L'accesso a un file condiviso avviene in due modi: aprendo il file direttamente da EasyNetwork oppure copiandolo in una cartella del computer e quindi aprendolo. Se l'elenco dei file condivisi è troppo lungo, è possibile effettuare la ricerca dei file a cui si desidera accedere.

Nota: i file condivisi tramite EasyNetwork non sono accessibili da altri computer mediante Esplora risorse. La condivisione dei file EasyNetwork viene eseguita mediante connessioni protette.

Condivisione di un file

Quando si condivide un file, questo viene reso automaticamente disponibile a tutti gli altri membri che dispongono di accesso alla rete gestita, sia esso completo o con privilegi di amministratore.

Per condividere un file:

1. In Esplora risorse, individuare il file che si desidera condividere.
2. Trascinare il file dal percorso in Esplora risorse nella finestra File condivisi in EasyNetwork.

Suggerimento: è anche possibile condividere un file facendo clic su **Condividi file** nel menu **Strumenti**. Nella finestra di diaIogo Condividi, passare alla cartella in cui è memorizzato il file che si desidera condividere, selezionarlo e fare clic su **Condividi**.

Interruzione della condivisione di un file

Se un file viene condiviso sulla rete gestita, è possibile interrompere la condivisione in qualsiasi momento. Quando si interrompe la condivisione di un file, gli altri membri della rete gestita non possono più accedervi.

Per interrompere la condivisione di un file:

1. Nel menu **Strumenti**, scegliere **Interrompi condivisione file**.
2. Nella finestra di dialogo Interrompi condivisione file, selezionare il file che non si desidera più condividere.
3. Fare clic su **Non condividere**.

Copia di un file condiviso

È possibile copiare nel computer in uso i file condivisi provenienti da un qualsiasi computer della rete gestita. Si disporrà quindi ancora di una copia anche nel caso in cui il computer interrompa la condivisione del file.

Per copiare un file:

- Trascinare un file dalla finestra File condivisi di EasyNetwork in un percorso di Esplora risorse o sul desktop di Windows.

Suggerimento: è anche possibile copiare un file condiviso selezionandolo in EasyNetwork, quindi facendo clic su **Copia in** nel menu **Strumenti**. Nella finestra di dialogo Copia in, passare alla cartella in cui si desidera copiare il file, selezionarlo e fare clic su **Salva**.

Ricerca di un file condiviso

È possibile ricercare un file di cui si è eseguita la condivisione oppure che è stato condiviso da qualsiasi altro membro della rete. Nel momento in cui vengono digitati i criteri di ricerca, EasyNetwork visualizza automaticamente i risultati corrispondenti nella finestra File condivisi.

Per cercare un file condiviso:

1. Nella finestra File condivisi, fare clic su **Cerca**.
2. Scegliere una delle seguenti opzioni nell'elenco **Contiene**:
   - **Contiene tutte le parole**: consente di cercare i nomi di file o di percorso contenenti tutte le parole specificate nell'elenco **Nome file o percorso**, in qualsiasi ordine.

- **Contiene una qualsiasi delle parole**: consente di cercare i nomi di file o di percorso contenenti una qualsiasi delle parole specificate nell'elenco **Nome file o percorso**.
- **Contiene la stringa esatta**: consente di cercare i nomi di file o di percorso contenenti esattamente la stringa specificata nell'elenco **Nome file o percorso**.

3 Digitare, tutto o in parte, il nome del file o del percorso nell'elenco **Nome file o percorso**.

4 Scegliere una delle seguenti opzioni nell'elenco **Tipo**:

- **Qualsiasi**: consente di cercare tutti i tipi di file condivisi.
- **Documento**: consente di cercare tutti i documenti condivisi.
- **Immagine**: consente di cercare tutti i file di immagine condivisi.
- **Video**: consente di cercare tutti i file video condivisi.
- **Audio**: consente di cercare tutti i file audio condivisi.

5 Negli elenchi **Da** e **A** , fare clic sulle date che rappresentano l'intervallo temporale in cui è stato creato il file.

Invio di file ad altri computer

È possibile inviare file ad altri computer purché siano membri della rete gestita. Prima di inviare un file, EasyNetwork verifica che il computer che lo riceve abbia sufficiente spazio su disco.

Nel momento in cui si riceve un file, esso viene visualizzato nella casella dei file in arrivo di EasyNetwork, un percorso di archiviazione temporaneo per tutti i file ricevuti da altri computer della rete. Se durante la ricezione EasyNetwork è aperto, il file viene immediatamente visualizzato nella casella dei file in arrivo, in caso contrario viene visualizzato un messaggio nell'area di notifica a destra della barra delle applicazioni di Windows. Se non si desidera ricevere messaggi di notifica è possibile disattivarli. Qualora nella casella dei file in arrivo esista già un file con lo stesso nome, il nuovo file viene rinominato con un suffisso numerico. I file restano nella casella finché l'utente li accetta, vale a dire finché vengono copiati in un percorso sul computer in uso.

Invio di un file a un altro computer

È possibile inviare un file direttamente a un altro computer della rete gestita senza condividerlo. Prima che un utente del computer destinatario possa visualizzare il file, sarà necessario salvarlo in un percorso locale. Per ulteriori informazioni, vedere Accettazione di un file da un altro computer (pagina 198).

Per inviare un file a un altro computer:

1. In Esplora risorse, individuare il file che si desidera inviare.
2. In EasyNetwork, trascinare il file dal percorso in Esplora risorse sull'icona di un computer attivo.

Suggerimento: è possibile inviare più file a un computer premendo CTRL mentre li si seleziona. Per inviare i file è inoltre possibile fare clic su **Invia** nel menu **Strumenti**, selezionare i file e fare clic su **Invia**.

Accettazione di un file proveniente da un altro computer

Se un altro computer della rete gestita invia un file all'utente, è necessario accettarlo (salvandolo in una cartella del computer). Se durante l'invio del file al computer in uso EasyNetwork non è aperto o non è in primo piano, l'utente riceverà un messaggio nell'area di notifica a destra della barra delle applicazioni. Fare clic sul messaggio di notifica per aprire EasyNetwork e accedere al file.

Per ricevere un file da un altro computer:

- Fare clic su **Ricevuto**, quindi trascinare il file dalla casella dei file in arrivo di EasyNetwork in una cartella di Esplora risorse.

Suggerimento: è anche possibile ricevere un file da un altro computer selezionandolo nella casella dei file in arrivo di EasyNetwork e facendo clic su **Accetta** nel menu **Strumenti**. Nella finestra di dialogo Accetta nella cartella, passare alla cartella in cui si desidera salvare i file in ricezione, effettuare la selezione e fare clic su **Salva**.

Ricezione di una notifica all'invio di un file

È possibile ricevere una notifica quando un altro computer della rete gestita invia un file. Se EasyNetwork al momento non è aperto o non è in primo piano sul desktop, verrà visualizzato un messaggio nell'area di notifica sulla destra della barra delle applicazioni.

Per ricevere una notifica all'invio di un file:

1. Nel menu **Opzioni**, scegliere **Configura**.
2. Nella finestra di dialogo Configura, selezionare la casella di controllo **Avvisa quando è in corso l'invio di file da altri computer**.
3. Fare clic su **OK**.

CAPITOLO 28

Condivisione di stampanti

Una volta che l'utente è diventato membro di una rete gestita, EasyNetwork condivide automaticamente qualsiasi stampante locale collegata al computer, rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso.

In questo capitolo

Uso delle stampanti condivise

Una volta che l'utente è diventato membro di una rete gestita, EasyNetwork condivide automaticamente tutte le stampanti locali collegate al computer in uso, utilizzando il nome corrente della stampante come nome della stampante condivisa, rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso. Se è stato configurato un driver per stampare mediante un server di stampa di rete (ad esempio, un server di stampa USB senza fili), EasyNetwork considera la stampante come locale e la condivide automaticamente in rete. È anche possibile interrompere la condivisione di una stampante in qualsiasi momento.

EasyNetwork rileva inoltre le stampanti condivise da tutti gli altri computer della rete. Se viene rilevata una stampante remota non ancora connessa al computer, quando EasyNetwork viene aperto per la prima volta, nella finestra File condivisi viene visualizzato il collegamento **Stampanti di rete disponibili**. In questo modo l'utente potrà installare le stampanti disponibili o disinstallare quelle già connesse al computer nonché aggiornare l'elenco delle stampanti rilevate sulla rete.

Se invece è connesso alla rete gestita ma non ne è ancora diventato membro, l'utente potrà accedere alle stampanti condivise mediante il normale pannello di controllo delle stampanti di Windows.

Interruzione della condivisione di una stampante

È possibile interrompere la condivisione di una stampante in qualsiasi momento. I membri che hanno già installato la stampante non potranno più stampare su di essa.

Per interrompere la condivisione di una stampante:

1. Nel menu **Strumenti**, scegliere **Stampanti**.
2. Nella finestra di dialogo Gestione stampanti di rete, fare clic sul nome della stampante che non si desidera più condividere.
3. Fare clic su **Non condividere**.

Installazione di una stampante di rete disponibile

Come membro di una rete gestita, è possibile accedere alle stampanti condivise in rete purché vengano installati i driver appropriati. Se il proprietario della stampante interrompe la condivisione dopo che l'utente ha effettuato l'installazione, non sarà più possibile stampare su quella stampante.

Per installare una stampante di rete disponibile:

1. Nel menu **Strumenti**, scegliere **Stampanti**.
2. Nella finestra di dialogo Stampanti di rete disponibili, fare clic sul nome di una stampante.
3. Fare clic su **Installa**.

CAPITOLO 29

Riferimento

Nel Glossario dei termini sono elencati e illustrati i termini relativi alla protezione più comunemente utilizzati nei prodotti McAfee.

In Informazioni su McAfee vengono fornite informazioni legali riguardanti McAfee Corporation.

Glossario

8

802.11

Insieme di standard IEEE per la tecnologia LAN senza fili. 802.11 specifica un'interfaccia over-the-air tra un client senza fili e una stazione di base o tra due client senza fili. Diverse specifiche di 802.11 includono 802.11a, uno standard per connessioni di rete fino a 54 Mbps nella banda dei 5 Ghz, 802.11b, uno standard per connessioni di rete fino a 11 Mbps nella banda dei 2,4 Ghz, 802.11g, uno standard per connessioni di rete fino a 54 Mbps nella banda dei 2,4 Ghz e 802.11i, una suite di standard di protezione per tutte le reti Ethernet senza fili.

802.11a

Estensione di 802.11 che si applica alle LAN senza fili e consente la trasmissione di dati fino a 54 Mbps nella banda dei 5 GHz. Nonostante la velocità di trasmissione sia superiore rispetto a 802.11b, la distanza coperta è di gran lunga inferiore.

802.11b

Estensione di 802.11 che si applica alle LAN senza fili e fornisce una velocità di trasmissione di 11 Mbps nella banda dei 2,4 GHz. 802.11b è attualmente considerato lo standard senza fili.

802.11g

Estensione di 802.11 che si applica alle LAN senza fili e fornisce fino a 54 Mbps nella banda dei 2,4 GHz.

802.1x

Non supportato da Wireless Home Network Security. Si tratta di uno standard IEEE per l'autenticazione su reti cablate e senza fili, ma viene utilizzato soprattutto per le reti senza fili basate su 802.11. Questo standard consente l'autenticazione avanzata reciproca fra i client e un server di autenticazione. Inoltre, 802.1x può fornire chiavi WEP dinamiche per utente e per sessione, diminuendo il carico amministrativo e i rischi per la protezione legati alle chiavi WEP statiche.

A

account di posta elettronica standard

La maggior parte degli utenti privati dispone di questo tipo di account. Vedere anche account POP3.

account MAPI

Acronimo di Messaging Application Programming Interface. Specifica di interfaccia di Microsoft che consente a differenti applicazioni di workgroup e messaggistica (tra cui posta elettronica, casella vocale e fax) di collaborare attraverso un singolo client, ad esempio il client di Exchange. Per questo motivo, il sistema MAPI è spesso utilizzato in ambienti aziendali in cui su utilizza Microsoft® Exchange Server. Molti utenti utilizzano tuttavia Microsoft Outlook per la posta elettronica Internet personale.

account MSN

Acronimo di Microsoft Network. Servizio online e portale Internet. Si tratta di un account basato sul Web.

account POP3

Acronimo di Post Office Protocol 3. La maggior parte degli utenti privati utilizza questo tipo di account. Si tratta della versione corrente dello standard Post Office Protocol utilizzato comunemente sulle reti TCP/IP. Anche noto come account di posta elettronica standard.

analisi immagini

Blocco della visualizzazione di immagini potenzialmente inappropriate. Le immagini sono bloccate per tutti gli utenti, ad eccezione dei membri appartenenti al gruppo di età dei maggiori di 18 anni.

archiviazione

Creazione di una copia dei file monitorati a livello locale su CD, DVD, unità USB, disco rigido esterno o unità di rete.

archiviazione

Creazione di una copia dei file monitorati a livello locale su CD, DVD, unità USB, disco rigido esterno o unità di rete.

archiviazione completa

Archiviazione completa di un set di dati in base ai tipi di file e ai percorsi monitorati impostati.

archiviazione rapida

Archiviazione solo dei file monitorati che sono cambiati dopo l'ultima archiviazione completa o rapida.

archivio del backup in linea

Percorso del server online dove sono memorizzati i file monitorati dopo che ne è stato eseguito il backup.

Archivio protetto password

Area di memorizzazione protetta per le password personali. che consente di memorizzare le password in modo tale che nessun altro utente, compreso un amministratore di McAfee o un amministratore di sistema, possa accedervi.

attacco brute force

Noto anche come brute force cracking. Si tratta di un metodo basato su tentativi ed errori utilizzato da applicazioni per decodificare dati crittografati come le password, applicando un grande dispendio di energie (mediante la forza bruta) anziché impiegare strategie mirate. Proprio come un criminale potrebbe forzare una cassaforte tentando tutte le combinazioni possibili, un'applicazione che utilizza la forza bruta procede attraverso la sequenza di tutte le possibili combinazioni di caratteri consentiti. L'uso della forza bruta è considerato un approccio infallibile anche se richiede tempi piuttosto lunghi.

attacco di tipo dictionary

Tipo di attacco in cui si tenta di individuare una password utilizzando una grande quantità di parole contenute in un elenco. I tentativi non vengono effettuati manualmente, ma mediante strumenti che tentano automaticamente di identificare la password.

attacco di tipo man-in-the-middle

L'autore dell'attacco intercetta i messaggi in uno scambio di chiavi pubbliche e li ritrasmette sostituendo la propria chiave pubblica a quella richiesta, in modo che le due parti originarie risultino ancora in comunicazione diretta tra loro. L'autore dell'attacco utilizza un programma che al client sembra il server e al server sembra il client. L'attacco può essere utilizzato semplicemente per ottenere accesso ai messaggi o per consentirne la modifica prima che siano ritrasmessi. Il termine deriva da un gioco in cui i partecipanti tentano di lanciarsi una palla mentre un altro giocatore nel mezzo tenta di afferrarla.

autenticazione

Processo di identificazione di un individuo, di solito basato su un nome utente e una password. L'autenticazione consente di verificare la veridicità dell'identità dichiarata dall'utente, ma non fornisce informazioni sui suoi diritti di accesso.

B

backup

Creazione di una copia dei file monitorati su un server online protetto.

browser

Programma client che utilizza il protocollo HTTP (Hypertext Transfer Protocol) per inviare richieste a server Web attraverso Internet. Un browser Web consente di rappresentare graficamente i contenuti.

C

chiave

Serie di lettere e/o numeri utilizzata da due dispositivi per autenticarne la comunicazione. Entrambi i dispositivi devono disporre della chiave. Vedere anche WEP, WPA, WPA2, WPA-PSK e WPA2- PSK.

client

Applicazione eseguita su PC o workstation che richiede un un server per l'esecuzione di alcune operazioni. Ad esempio, un client di posta elettronica è un'applicazione che consente l'invio e la ricezione di messaggi di posta elettronica.

client di posta elettronica

Account di posta elettronica. Ad esempio, Microsoft Outlook o Eudora.

compressione

Processo mediante il quale i dati (file) vengono compressi in un formato tale da ridurre al minimo lo spazio richiesto per memorizzarli o trasmetterli.

condivisione

Operazione che consente ai destinatari del messaggio di posta elettronica di accedere ai file di backup selezionati per un periodo limitato di tempo. Quando si condivide un file, la copia di backup del file viene inviata ai destinatari del messaggio di posta elettronica specificati. I destinatari ricevono un messaggio di posta elettronica da Data Backup in cui viene segnalato che i file sono stati condivisi. Nel messaggio di posta elettronica è riportato anche un collegamento ai file condivisi.

Controllo genitori

Impostazioni che permettono di configurare classificazioni dei contenuti, che limitano i siti Web e i contenuti visualizzabili da determinati utenti, e di impostare limiti temporali per l'accesso a Internet, che consentono di determinare i periodi in cui Internet sarà accessibile e la durata consentita della navigazione. Il controllo genitori consente inoltre di limitare l'accesso a siti Web specifici da parte di tutti gli utenti e di consentire o bloccare l'accesso in base a gruppi di età e a parole chiave ad essi associate.

cookie

Sul World Wide Web, un blocco di dati memorizzato su un client da un server Web. Quando l'utente visita nuovamente lo stesso sito Web, il browser invia una copia del cookie al server. I cookie vengono utilizzati per identificare gli utenti, richiedere al server l'invio di versioni personalizzate di determinate pagine Web, inviare informazioni sull'account dell'utente e per altri scopi di natura amministrativa.

I cookie consentono ai siti Web di memorizzare dati relativi agli utenti e di tenere traccia del numero di visite ricevute, dell'orario in cui le visite si sono verificate e delle pagine visualizzate. I cookie consentono inoltre agli utenti di personalizzare i siti Web. Molti siti Web richiedono un nome utente e una password per consentire l'accesso a determinate pagine e inviano un cookie al computer in modo che l'utente non debba effettuare l'accesso ogni volta. Tuttavia, i cookie possono essere utilizzati per attività dannose. Le società pubblicitarie online utilizzano spesso i cookie per determinare quali sono i siti più visitati da determinati utenti in modo da visualizzare informazioni pubblicitarie sui loro siti Web preferiti. Prima di consentire l'invio di cookie da parte di un sito, è consigliabile assicurarsi della sua affidabilità.

Benché siano una fonte di informazioni legittima, i cookie possono anche essere una fonte di informazioni per gli hacker. Molti siti Web per gli acquisti online memorizzano i dati relativi a carte di credito e altri dati personali nei cookie, in modo da facilitare le operazioni di acquisto dei clienti. Purtroppo possono verificarsi vulnerabilità della protezione che consentono agli hacker di accedere ai dati presenti nei cookie memorizzati nei computer dei clienti.

crittografia

Processo mediante il quale i dati vengono trasformati da testo in codice, oscurando le informazioni per renderle illeggibili agli utenti che non sanno come decifrarle.

D

Denial of Service (Negazione del servizio)

Su Internet, un attacco DoS (Denial of Service, Negazione del servizio) è un incidente durante il quale un utente o un'organizzazione vengono privati dei servizi di una risorsa solitamente disponibile. Di solito, la negazione di un servizio è costituita dalla mancata disponibilità di un particolare servizio di rete, ad esempio la posta elettronica, oppure dalla perdita temporanea di tutti i servizi e della connettività di rete. Nei casi peggiori, ad esempio, un sito Web a cui accedono milioni di persone può essere occasionalmente forzato a interrompere temporaneamente il funzionamento. Un attacco DoS può anche provocare la distruzione di programmi e di file in un sistema informatico. Per quanto di solito siano intenzionali e pericolosi, gli attacchi DoS possono talvolta verificarsi accidentalmente. Un attacco DoS è un tipo di violazione della protezione di un sistema informatico che di solito non comporta il furto di informazioni o altre perdite di protezione. Tuttavia, questi attacchi possono costare alla persona o all'azienda che li riceve una gran quantità di tempo e denaro.

disco rigido esterno

Disco rigido collegato all'esterno del computer .

DNS

Acronimo di Domain Name System. Sistema gerarchico che consente agli host presenti su Internet di disporre sia di indirizzi del nome di dominio (ad esempio bluestem.prairienet.org) che di indirizzi IP (ad esempio 192.17.3.4). L'utente utilizza l'indirizzo del nome del dominio, il quale viene tradotto automaticamente nell'indirizzo IP numerico, il quale viene a sua volta utilizzato dal software di instradamento dei pacchetti. I nomi DNS sono costituiti da un dominio di primo livello (ad esempio .com, .org e .net), un dominio di livello secondario (il nome del sito di un'azienda, di un'organizzazione o di un privato) ed eventualmente da uno o più sottodomini (server all'interno di un dominio di secondo livello). Vedere anche server DNS e indirizzo IP.

dominio

Indirizzo di una connessione di rete che consente l'identificazione del titolare dell'indirizzo in un formato gerarchico: server.organizzazione.tipo. Ad esempio, www.whitehouse.gov identifica il server Web della Casa bianca (White House), che fa parte del governo degli Stati Uniti.

E

elenco indirizzi autorizzati

Elenco di siti Web a cui è consentito l'accesso perché non considerati dannosi.

elenco indirizzi bloccati

Elenco di siti Web considerati dannosi. Un sito Web può essere inserito in un elenco di indirizzi bloccati perché su di esso vengono eseguite operazioni fraudolente o perché sfrutta vulnerabilità del browser per inviare all'utente programmi potenzialmente indesiderati.

ESS (Extended Service Set)

Insieme di una o più reti che formano un'unica sottorete.

evento

Eventi provenienti da 0.0.0.0

Due sono le cause più probabili per il rilevamento di eventi provenienti dall'indirizzo IP 0.0.0.0. La prima causa, quella più comune, è che per qualche motivo il computer ha ricevuto un pacchetto non valido. Internet non è sempre affidabile al 100% ed è quindi possibile che vengano inoltrati pacchetti non validi. Poiché i pacchetti vengono esaminati da Firewall prima della convalida da parte di TCP/IP, è possibile che questi pacchetti vengano segnalati come evento.

In altri casi è possibile che sia stato effettuato lo spoofing dell'indirizzo IP di origine, ossia che quest'ultimo sia stato contraffatto. I pacchetti contraffatti potrebbero indicare che è in corso una scansione per la ricerca di Trojan e che è stato effettuato un tentativo sul computer in uso. È importante ricordare che Firewall blocca tali tentativi.

Eventi provenienti da 127.0.0.1

Alcuni eventi vengono generati dall'indirizzo IP 127.0.0.1. Si tratta di un indirizzo IP speciale, noto come indirizzo di loopback.

Indipendentemente dal computer in uso, 127.0.0.1 si riferisce sempre al computer locale. È anche possibile fare riferimento a tale indirizzo come localhost, poiché il nome di computer localhost viene sempre risolto nell'indirizzo IP 127.0.0.1. È comunque poco probabile che il computer stia tentando di attaccare se stesso oppure sia controllato da un Trojan o da spyware. Molti programmi legittimi utilizzano infatti l'indirizzo di loopback per la comunicazione fra i componenti. Ad esempio, molti server di posta o server Web personali possono essere configurati utilizzando un'interfaccia Web in genere accessibile mediante l'indirizzo http://localhost/.

Il traffico proveniente da tali programmi viene tuttavia autorizzato da Firewall. Quindi, se si rilevano eventi provenienti dall'indirizzo 127.0.0.1, è probabile che sia stato effettuato lo spoofing dell'indirizzo IP di origine, ossia che questo sia stato contraffatto. I pacchetti contraffatti indicano che è in corso una scansione per la ricerca di Trojan. È importante ricordare che Firewall blocca tali tentativi. È evidente che la segnalazione di eventi provenienti da 127.0.0.1 non è di alcuna utilità e, pertanto, non viene eseguita.

Esistono tuttavia programmi, come Netscape 6.2 e versioni successive, che richiedono l'aggiunta di 127.0.0.1 all'elenco degli **indirizzi IP affidabili**. La modalità di comunicazione tra i componenti di tali programmi non consente a Firewall di determinare se si tratti di traffico locale.

Nel caso di Netscape 6.2, se non si imposta 127.0.0.1 come affidabile, non sarà possibile utilizzare l'elenco degli amici. Se si rileva quindi traffico proveniente da 127.0.0.1 e tutti i programmi del computer funzionano normalmente, è possibile bloccare tale traffico senza che si verifichino problemi. Se, tuttavia, in un programma, ad esempio Netscape, si verificano problemi, aggiungere 127.0.0.1 all'elenco degli **indirizzi IP affidabili** di Firewall, quindi verificare se i problemi sono stati risolti.

Se l'inserimento di 127.0.0.1 nell'elenco degli **indirizzi IP affidabili** consente di risolvere il problema, è necessario valutare le opzioni disponibili: se si imposta 127.0.0.1 come affidabile, il programma funzionerà correttamente, ma il sistema sarà più vulnerabile ad attacchi di spoofing. Se non si imposta l'indirizzo come affidabile, il programma non funzionerà correttamente, ma si sarà protetti dal traffico dannoso.

Eventi proveninenti dai computer della LAN

Per la maggior parte delle impostazioni LAN in uso nelle aziende, è possibile considerare come affidabili tutti i computer presenti sulla LAN.

Eventi provenienti da indirizzi IP privati

Gli indirizzi IP con formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 sono detti non instradabili o privati. Tali indirizzi IP non dovrebbero mai lasciare la rete e possono essere considerati quasi sempre affidabili.

Il blocco 192.168 viene utilizzato con Condivisione connessione Internet di Microsoft. Se si utilizza Condivisione connessione Internet e si rilevano eventi provenienti da tale blocco di indirizzi IP, è possibile aggiungere l'indirizzo IP 192.168.255.255 all'elenco degli **indirizzi IP affidabili**. In tal modo verrà impostato come affidabile l'intero blocco 192.168.xxx.xxx.

Se non si è connessi a una rete privata e si rilevano eventi provenienti da questi intervalli di indirizzi IP, è possibile che gli indirizzi IP di origine siano stati sottoposti a spoofing, ovvero che siano stati contraffatti. I pacchetti contraffatti indicano solitamente che è in corso una scansione per la ricerca di Trojan. È importante ricordare che Firewall blocca tali tentativi.

Poiché gli indirizzi IP privati sono separati dagli indirizzi IP in Internet, la segnalazione di tali eventi risulta inutile, quindi non viene effettuata.

firewall

Sistema progettato per impedire l'accesso non autorizzato a o da una rete privata. I firewall possono essere implementati sia nell'hardware che nel software o con una combinazione di entrambi. I firewall vengono utilizzati di frequente per impedire a utenti di Internet non autorizzati di accedere a reti private connesse a Internet, specialmente a una rete Intranet. Tutti i messaggi in ingresso o in uscita da una rete Intranet passano attraverso il firewall. Il firewall esamina tutti i messaggi e blocca quelli non conformi ai criteri di protezione specificati. Un firewall è considerato la prima linea di difesa nella protezione delle informazioni private. Per una maggiore protezione, è possibile crittografare i dati.

gateway integrato

Dispositivo che combina le funzioni di punto di accesso, router e firewall. Alcuni dispositivi possono persino includere funzionalità avanzate di protezione e bridging.

gruppi di classificazione del contenuto

Gruppi di età a cui appartiene un utente. Il contenuto viene classificato (ossia, reso disponibile o bloccato) in base al gruppo di classificazione del contenuto al quale appartiene l'utente. I gruppi di classificazione del contenuto comprendono: minori di 6 anni, 6 - 9 anni, 10 - 13 anni, 14 - 18 anni, maggiori di 18 anni.

hotspot

Specifico luogo geografico in cui un punto di accesso fornisce a visitatori che dispongono di dispositivi portatili servizi pubblici di rete a banda larga attraverso una rete senza fili. Gli hotspot si trovano spesso in luoghi particolarmente affollati come gli aeroporti, le stazioni ferroviarie, le biblioteche, i porti marittimi, i centri congressuali e gli alberghi. Di solito la loro portata di accesso è limitata.

Indirizzo IP

L'indirizzo del protocollo Internet, o indirizzo IP, è un numero univoco costituito da quattro parti separate da punti, ad esempio 63.227.89.66. In Internet, a ogni computer, dal server più grande a un portatile che comunica attraverso un telefono cellulare, è assegnato un indirizzo IP univoco. Non tutti i computer dispongono di un nome di dominio, ma tutti dispongono di un indirizzo IP.

Di seguito sono elencati alcuni tipi di indirizzi IP speciali:

- Indirizzi IP non instradabili. Tali indirizzi sono noti anche come spazi IP privati e non possono essere utilizzati su Internet. I blocchi privati sono 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.
- Indirizzi IP di loopback**:** gli indirizzi di loopback vengono utilizzati a scopo di test. Il traffico inviato a questo blocco di indirizzi IP torna subito al dispositivo che genera il pacchetto, non lascia mai il dispositivo e viene utilizzato principalmente per test di hardware e software. Il blocco degli indirizzi IP di loopback è 127.x.x.x.

Indirizzo IP nullo: si tratta di un indirizzo non valido. Se risulta visibile, ciò indica che l'indirizzo IP da cui proveniva o a cui era destinato il traffico era vuoto. Ovviamente, tale situazione non è normale e indica spesso che l'origine del traffico viene deliberatamente nascosta dal mittente. Il mittente non sarà in grado di ricevere risposte, a meno che il pacchetto non venga ricevuto da un'applicazione in grado di comprenderne i contenuti, in cui devono essere incluse istruzioni specifiche per tale applicazione. Qualsiasi indirizzo che inizi per 0 (0.x.x.x) è un indirizzo nullo. Ad esempio, 0.0.0.0 è un indirizzo IP nullo.

Indirizzo MAC (Media Access Control Address)

Indirizzo di basso livello assegnato al dispositivo fisico che accede alla rete.

Internet

Internet è un sistema costituito da un numero elevatissimo di reti interconnesse che utilizzano i protocolli TCP/IP per individuare e trasferire dati. Internet è l'evoluzione di una rete di computer di università e college creata tra la fine degli anni '60 e l'inizio degli annu '70 dal Dipartimento della difesa degli Stati Uniti e denominata ARPANET. Internet è oggi una rete globale costituita da circa 100.000 reti indipendenti.

intestazione

Informazioni aggiunte a una porzione di un messaggio nel corso del ciclo di vita del messaggio stesso. L'intestazione contiene indicazioni relative alla modalità di consegna del messaggio da parte del software Internet, all'indirizzo cui inviare la risposta, un identificatore univoco per il messaggio di posta elettronica e altre informazioni amministrative. Esempi dei campi dell'intestazione sono: To, From, Cc, Date, Subject, Message-ID e Received.

intranet

Rete privata, situata in genere all'interno di un'organizzazione, il cui funzionamento è molto simile a quello di Internet. È divenuto abituale consentire l'accesso alle reti Intranet da computer autonomi utilizzati da studenti o dipendenti dall'esterno dell'università o del luogo di lavoro. Firewall, procedure di accesso e password hanno lo scopo di garantirne la protezione.

LAN (Local Area Network)

Rete di computer che si estende in un'area relativamente ridotta. Molte LAN sono ristrette a un solo edificio o gruppo di edifici. Tuttavia, una LAN può essere connessa ad altre LAN a qualunque distanza tramite telefono e onde radio. Un sistema di LAN connesse in questo modo è detto WAN (Wide-Area Network). Nella maggior parte delle LAN, workstation e PC sono connessi fra di loro, di solito mediante semplici hub o switch. Ciascun nodo (singolo computer) in una LAN dispone della propria CPU che utilizza per l'esecuzione di programmi, ma è anche in grado di accedere a dati e a dispositivi (ad esempio le stampanti) presenti in qualsiasi punto della LAN. In tal modo, molti utenti possono condividere dispositivi costosi, come le stampanti laser, nonché i dati. Gli utenti, inoltre, possono utilizzare la LAN per comunicare tra di loro, ad esempio inviando messaggi di posta elettronica o avviando sessioni di chat.

larghezza di banda

Quantità di dati trasmettibili in un determinato lasso di tempo. Per i dispositivi digitali, la larghezza di banda di solito viene espressa in bit per secondo (bps) o byte per secondo. Per i dispositivi analogici, la larghezza di banda viene espressa in cicli per secondo o Hertz (Hz).

libreria

Area di memorizzazione online per i file pubblicati dagli utenti di Data Backup. La libreria è un sito Web su Internet, accessibile a chiunque disponga di un accesso a Internet.

MAC (Media Access Control o Message Authenticator Code)

Per il primo significato, vedere Indirizzo MAC. Il secondo è un codice utilizzato per identificare un determinato messaggio (ad esempio, un messaggio RADIUS). Il codice generalmente è un hash dei contenuti del messaggio ottenuto mediante crittografia avanzata, che include un valore univoco per garantire una protezione contro la riproduzione.

mappa di rete

In Network Manager, rappresentazione grafica dei computer e dei componenti che costituiscono la rete domestica.

NIC (Network Interface Card)

Scheda che si inserisce in un laptop o in altro dispositivo e consente la connessione del dispositivo alla LAN.

nodo

Singolo computer connesso a una rete.

parola chiave

Parola che è possibile assegnare a un file di backup per stabilire un rapporto o una connessione con altri file a cui è stata assegnata la stessa parola chiave. L'assegnazione di parole chiave ai file agevola la ricerca dei file che sono stati pubblicati su Internet.

password

Codice, in genere alfanumerico, utilizzato per ottenere l'accesso a un computer, a un determinato programma o a un sito Web.

percorsi monitorati

Cartelle sul computer monitorate da Data Backup.

percorso di monitoraggio approfondito

Una cartella sul computer sottoposta, insieme a tutte le sue sottocartelle, al monitoraggio delle modifiche da parte di Data Backup. Se si imposta un percorso di monitoraggio approfondito, Data Backup esegue il backup dei tipi di file monitorati in tale cartella e nelle relative sottocartelle.

percorso di monitoraggio rapido

Cartella sul computer sottoposta al monitoraggio delle modifiche da parte di Data Backup. Se si imposta un percorso di monitoraggio rapido, Data Backup esegue il backup dei tipi di file monitorati all'interno della cartella, ignorando il contenuto delle sottocartelle.

phishing

Il termine, che si pronuncia "fishing", si riferisce a sistemi ingannevoli utilizzati per il furto di dati riservati quali il numero della carta di credito e del codice fiscale, l'ID utente e le password. Le potenziali vittime ricevono un messaggio di posta elettronica che ha l'aspetto di un messaggio inviato dal loro provider di servizi Internet, dalla loro banca o da un loro rivenditore di fiducia. I messaggi di posta elettronica possono essere inviati a utenti selezionati da un elenco o scelti in maniera casuale, nel tentativo di individuare una percentuale di essi che disponga effettivamente di un account presso l'organizzazione legittima.

popup

Piccole finestre che vengono visualizzate davanti ad altre finestre sullo schermo del computer. Le finestre popup sono spesso utilizzate nei browser Web per visualizzare annunci pubblicitari. McAfee blocca le finestre popup caricate automaticamente sul browser insieme a una pagina Web, ma non blocca le finestre popup che vengono caricate quando si seleziona un collegamento.

porta

Punto in cui i dati entrano e/o escono dal computer. Ad esempio, il tradizionale modem analogico viene connesso alla porta seriale. Nelle comunicazioni TCP/IP i numeri di porta sono valori virtuali utilizzati per suddividere il traffico in flussi associati ad applicazioni specifiche. Le porte sono assegnate a protocolli standard, quali SMTP o HTTP, in modo che ai programmi sia nota la porta sulla quale tentare di stabilire una connessione. La porta di destinazione per i pacchetti TCP indica l'applicazione o il server desiderato.

posta elettronica

Posta elettronica, messaggi inviati tramite Internet o all'interno della rete LAN o WAN di un'azienda. Gli allegati di posta elettronica sotto forma di file EXE (eseguibili) o file VBS (script di Visual Basic) sono diventati un mezzo sempre più diffuso per la trasmissione di virus e Trojan.

PPPoE

Point-to-Point Protocol Over Ethernet (Protocollo punto a punto su Ethernet). Utilizzato da molti provider DSL, PPPoE supporta i livelli di protocollo e l'autenticazione ampiamente utilizzati in PPP e consente di stabilire connessioni punto-punto nell'architettura Ethernet, solitamente multipunto.

programma potenzialmente indesiderato

I programmi potenzialmente indesiderati comprendono spyware, adware e altri programmi che raccolgono e trasmettono dati personali senza autorizzazione.

protocollo

Formato concordato per la trasmissione di dati tra due dispositivi. Dal punto di vista di un utente, l'unico aspetto rilevante dei protocolli è che il computer o il dispositivo deve supportare quelli appropriati, se desidera comunicare con altri computer. Il protocollo può essere implementato nell'hardware o nel software.

proxy

Computer o software che separa una rete da Internet, presentando un solo indirizzo di rete ai siti esterni. Agendo come intermediario per tutti i computer interni, il proxy protegge le identità di rete pur continuando a fornire l'accesso a Internet. Vedere anche Server proxy.

pubblicazione

Operazione il cui scopo è rendere un file di backup disponibile a tutti su Internet.

Punto di accesso (AP, Access Point)

Dispositivo di rete che consente ai client 802.11 di connettersi a una rete locale (LAN). I punti di accesso estendono la gamma fisica di servizi per gli utenti di dispositivi senza fili. Talvolta sono denominati router senza fili.

Punto di accesso pericoloso

Punto di accesso di cui un'azienda non autorizza il funzionamento. Questo tipo di punto di accesso spesso non è conforme ai criteri di protezione della LAN senza fili (WLAN). Un punto di accesso pericoloso attiva un'interfaccia alla rete aziendale non protetta e aperta accessibile dall'esterno della struttura fisicamente controllata.

All'interno di una WLAN correttamente protetta, i punti di accesso pericolosi sono più dannosi degli utenti non autorizzati. Se sono attivi dei meccanismi di autenticazione efficaci, è improbabile che utenti non autorizzati che tentano l'accesso a una WLAN riescano a raggiungere importanti risorse aziendali. Maggiori problemi sorgono, tuttavia, quando un dipendente o un hacker si collegano utilizzando un punto di accesso pericoloso. Questo, infatti, consente l'accesso alla rete aziendale a chiunque disponga di un dispositivo dotato di 802.11, consentendogli di avvicinarsi a risorse critiche.

quarantena

Se vengono rilevati file sospetti, essi vengono messi in quarantena. È quindi possibile intraprendere le opportune azioni in un secondo momento.

RADIUS (Remote Access Dial-In User Service)

Protocollo che fornisce l'autenticazione degli utenti, di solito in un contesto di accesso remoto. Inizialmente definito per l'uso con i server di accesso remoto dial-in, il protocollo viene ora utilizzato in un'ampia gamma di ambienti di autenticazione, inclusa l'autenticazione 802.1x del segreto condiviso di un utente di una WLAN.

rete

Quando si connettono due o più computer, si crea una rete.

rete gestita

Rete domestica con due tipi di membri: membri gestiti e membri non gestiti. I membri gestiti, diversamente da quelli non gestiti, consentono agli altri computer in rete di monitorare lo stato delle protezione McAfee.

ripristino

Recupero di una copia di un file dall'archivio del backup in linea o da un archivio.

roaming

Capacità di spostarsi da un'area coperta da un punto di accesso a un'altra senza interruzione di servizio o perdita di connettività.

router

Dispositivo di rete che inoltra pacchetti da una rete all'altra. Sulla base di tabelle di instradamento interne, i router leggono ogni pacchetto in ingresso e decidono come inoltrarlo. L'interfaccia del router alla quale i pacchetti in uscita vengono inviati può essere determinata dalla combinazione dell'indirizzo di origine e di destinazione, nonché dalle attuali condizioni di traffico, qiali il carico, i costi della linea e il cattivo stato della linea. Talvolta sono denominati punti di accesso.

scansione in tempo reale

Scansione dei file alla ricerca di virus o altre attività quando vengono aperti dall'utente o dal computer.

scheda di rete senza fili

Contiene i circuiti che consentono a un computer o altri dispositivi di comunicare con un router senza fili (collegamento a una rete senza fili). Le schede di rete senza fili possono essere incorporate nei circuiti principali di un dispositivo hardware oppure essere costituite da un componente aggiuntivo a parte da inserire nel dispositivo mediante un'apposita porta.

schede senza fili PCI

Consentono di connettere un computer desktop a una rete. La scheda si inserisce in uno slot di espansione PCI all'interno del computer.

schede senza fili USB

Forniscono un'interfaccia seriale Plug and Play espandibile. Questa interfaccia fornisce una connessione senza fili standard e a basso costo per periferiche come tastiere, mouse, joystick, stampanti, scanner, dispositivi di archiviazione e videocamere per conferenze.

script

Gli script possono creare, copiare o eliminare file. Sono anche i grado di aprire il registro di sistema di Windows.

segreto condiviso

Vedere anche RADIUS. Protegge parti riservate dei messaggi RADIUS. Il segreto condiviso è una password che può essere condivisa dall'autenticatore e dal server di autenticazione in maniera protetta.

server

Computer o software che fornisce servizi specifici al software in esecuzione su altri computer. Il "server di posta" presso il provider di servizi Internet è il software che gestisce tutta la posta in arrivo e in uscita per tutti gli utenti del provider. Un server in una LAN è l'hardware che costituisce il nodo primario della rete. Può anche disporre di software che fornisce servizi specifici, dati o altre funzionalità a tutti i computer client collegati.

server DNS

Abbreviazione per server Domain Name System. Computer in grado di rispondere a query DNS (Domain Name System). Sul server DNS è presente un database in cui sono memorizzati i computer host e i corrispondenti indirizzi IP. Se, ad esempio, al server DNS viene inviato il nome apex.com, esso restituirà l'indirizzo IP della società ipotetica Apex. Chiamato anche: server dei nomi. Vedere anche DNS e indirizzo IP.

server proxy

Componente del firewall che gestisce il traffico Internet da e verso una LAN (Local Area Network). Un server proxy consente di migliorare le prestazioni fornendo i dati richiesti frequentemente, ad esempio una pagina Web, e di filtrare ed eliminare le richieste non considerate appropriate, quali le richieste di accesso non autorizzato ai file proprietari.

server SMTP

Acronimo di Simple Mail Transfer Protocol. Protocollo TCP/IP per l'invio di messaggi da un computer a un altro su una rete. Questo protocollo è utilizzato su Internet per instradare i messaggi di posta elettronica.

sincronizzazione

Risoluzione di eventuali incoerenze tra i file di backup e quelli memorizzati sul computer locale. La sincronizzazione è necessaria quando la versione di un file presente nell'archivio del backup in linea è più recente rispetto a quella del file memorizzato negli altri computer. Mediante la sincronizzazione, la copia del file memorizzata sui computer viene aggiornata con la versione del file presente nell'archivio del backup in linea.

sovraccarico del buffer

I sovraccarichi del buffer si verificano quando programmi o processi sospetti tentano di memorizzare in un buffer (area di memorizzazione temporanea dei dati) del computer una quantità di dati superiore al limite consentito, causando il danneggiamento o la sovrascrittura di dati validi presenti nei buffer adiacenti.

spoofing degli indirizzi IP

Contraffazione di indirizzi IP in un pacchetto IP. Viene utilizzato in molti tipi di attacchi, inclusa la presa di controllo della sessione. Viene inoltre impiegato per contraffare le intestazioni dei messaggi di posta indesiderati in modo da impedire la corretta individuazione dei mittenti.

SSID (Service Set Identifier)

Nome di rete per i dispositivi in un sottosistema LAN senza fili. Si tratta di una stringa di testo non crittografata, contenente 32 caratteri, aggiunta all'inizio di ogni pacchetto WLAN. L'SSID differenzia una WLAN dall'altra, per cui tutti gli utenti di una rete devono fornire lo stesso SSID per accedere a un determinato punto di accesso. L'SSID impedisce l'accesso a qualsiasi dispositivo client che non disponga di dello stesso SSID. Tuttavia, per impostazione predefinita un punto di accesso trasmette il proprio SSID nel proprio beacon. Anche se la trasmissione dell'SSID è disattivata, un hacker può rilevare l'SSID attraverso lo sniffing.

SSL (Secure Sockets Layer)

Protocollo sviluppato da Netscape per la trasmissione di documenti privati tramite Internet. L'SSL funziona utilizzando una chiave pubblica per crittografare i dati trasferiti sulla connessione SSL. Sia Netscape Navigator che Internet Explorer utilizzano e supportano SSL e molti siti Web utilizzano il protocollo per ottenere informazioni riservate dagli utenti, come i numeri di carta di credito. Per convenzione, gli URL che richiedono una connessione SSL iniziano con https: invece di http:.

SystemGuard

I moduli SystemGuard rilevano le modifiche non autorizzate subite dal computer e visualizzano un messaggio quando tali modifiche vengono apportate.

testo crittografato

Dati crittografati. Il testo crittografato è illeggibile finché non viene convertito in testo normale (decrittografato) mediante una chiave.

testo normale

Qualsiasi messaggio non crittografato.

tipi di file monitorati

Tipi di file, ad esempio DOC, XLS e così via, di cui Data Backup esegue il backup o memorizza negli archivi all'interno dei percorsi monitorati.

TKIP (Temporal Key Integrity Protocol)

Metodo di correzione rapida per superare la debolezza inerente alla protezione WEP, in particolare il riutilizzo delle chiavi crittografiche. TKIP modifica le chiavi temporali ogni 10.000 pacchetti, fornendo un metodo di distribuzione dinamica che migliora notevolmente la protezione della rete. Il processo (di protezione) TKIP inizia con una chiave temporale da 128 bit condivisa tra client e punti di accesso. TKIP combina la chiave temporale con l'indirizzo MAC (del computer client) e aggiunge un vettore di inizializzazione da 16 ottetti, relativamente grande, per produrre la chiave utilizzata per la crittografia dei dati. Questa procedura assicura che ogni stazione utilizzi flussi di chiavi differenti per crittografare i dati. TKIP utilizza RC4 per eseguire la crittografia. Anche WEP utilizza RC4.

Trojan horse

I Trojan horse sono programmi che si presentano sotto forma di applicazioni innocue. I Trojan horse non sono virus in quanto non duplicano se stessi, ma possono essere altrettanto distruttivi.

unità di rete

Unità disco o nastro collegata a un server su una rete e condivisa da più utenti. Le unità di rete sono spesso chiamate unità remote.

URL

Uniform Resource Locator. Formato standard degli indirizzi Internet.

VPN (Virtual Private Network)

Rete costruita utilizzando cavi pubblici per l'unione di nodi. Ad esempio, esistono molti sistemi che consentono di creare reti utilizzando Internet come mezzo di trasmissione dei dati. Tali sistemi utilizzano la crittografia e altri meccanismi di protezione per garantire che solo gli utenti autorizzati possano accedere alla rete e che i dati non possano essere intercettati.

wardriver

Intrusi armati di laptop, software speciale e hardware di fortuna che girano per città, sobborghi e zone industriali per intercettare il traffico di LAN senza fili.

Web bug

Piccoli file grafici che si incorporano autonomamente nelle pagine HTML e consentono a un'origine non autorizzata di impostare cookie sul computer dell'utente. I cookie possono quindi trasmettere dati all'origine non autorizzata. I Web bug sono anche chiamati Web beacon, pixel tag, GIF trasparenti o GIF invisibili.

WEP (Wired Equivalent Privacy)

Protocollo di crittografia e autenticazione definito come parte dello standard 802.11. Le versioni iniziali sono basate su crittografia RC4 e sono caratterizzate da una notevole vulnerabilità. WEP tenta di fornire la protezione crittografando i dati su onde radio, in modo che siano protetti durante la trasmissione fra due punti. Tuttavia, si è scoperto che WEP non è tanto sicuro come si credeva.

Wi-Fi (Wireless Fidelity)

Utilizzato genericamente quando ci si riferisce a qualunque tipo di rete 802.11, che sia 802.11b, 802.11a, dual-band, ecc. Il termine è utilizzato da Wi-Fi Alliance.

Wi-Fi Alliance

Organizzazione costituita da fornitori leader di software e dispositivi senza fili con la missione di (1) certificare l'interoperabilità di tutti i prodotti basati su 802.11 e di (2) promuovere il termine Wi-Fi come nome di marchio globale in tutti i mercati per qualsiasi prodotto LAN senza fili basato su 802.11. L'organizzazione funge da consorzio, laboratorio di collaudo e centro di raccolta e smistamento per i fornitori che desiderano promuovere l'interoperabilità e lo sviluppo di questo settore.

Mentre tutti i prodotti 802.11a/b/g sono detti Wi-Fi, solo i prodotti che hanno superato la verifica Wi-Fi Alliance possono essere definiti Wi-Fi Certified (un marchio registrato). I prodotti che hanno superato la verifica sono contrassegnati da un sigillo di identificazione sulla confezione che segnala il prodotto come Wi-Fi Certified e che indica la banda di frequenza radio utilizzata. Questo gruppo prima era noto con il nome di Wireless Ethernet Compatibility Alliance (WECA), ma ha modificato il nome nell'ottobre 2002 per rispecchiare meglio il marchio Wi-Fi che desidera costruire.

Wi-Fi Certified

Tutti i prodotti collaudati e approvati come Wi-Fi Certified (un marchio registrato) da Wi-Fi Alliance sono reciprocamente iteroperativi, anche se realizzati da produttori diversi. Un utente che dispone di un prodotto Wi-Fi Certified può utilizzare un punto di accesso di qualunque marca con hardware client di qualsiasi altra marca, purché siano certificati. Tuttavia, in genere, tutti i prodotti Wi-Fi che utilizzano la stessa frequenza radio (ad esempio, 2,4 GHz per 802.11b o 11g, 5 GHz per 802.11a) di altri prodotti funzionano senza problemi, anche se non sono Wi-Fi Certified.

WLAN (Wireless Local Area Network)

Vedere anche LAN. Rete locale che utilizza supporto senza fili per le connessioni. In una WLAN, per la comunicazione tra nodi, vengono utilizzate onde radio ad alta frequenza anziché cavi.

worm

Un worm è un virus in grado di autoreplicarsi; esso risiede nella memoria attiva e può inviare copie di sé stesso attraverso la posta elettronica. I worm si replicano e utilizzano le risorse di sistema, rallentando o bloccando i programmi.

WPA (Wi-Fi Protected Access)

Standard di specifiche che aumenta notevolmente il livello di protezione dei dati e il controllo dell'accesso dei sistemi LAN senza fili, esistenti e futuri. Progettato per funzionare sull'hardware esistente come upgrade software, WPA è derivato dallo standard IEEE 802.11i ed è compatibile con esso. Se correttamente installato, garantisce agli utenti della LAN senza fili un elevato livello di protezione dei dati e che l'accesso alla rete venga effettuato solo da utenti autorizzati.

WPA-PSK

Una speciale modalità WPA progettata per gli utenti privati che non richiedono una protezione avanzata a livello enterprise e non hanno accesso a server di autenticazione. Utilizzando questa modalità, l'utente privato inserisce manualmente la password iniziale per attivare l'accesso protetto Wi-Fi in modalità PSK (Pre-Shared Key, Chiave già condivisa) e deve cambiare regolarmente la passphrase su ciascun punto di accesso e computer senza fili. Vedere anche WPA2-PSK e TKIP.

WPA2

Vedere anche WPA. WPA2 è un aggiornamento dello standard di protezione WPA e si basa sullo standard IEEE 802.11i.

WPA2-PSK

Vedere anche WPA-PSK e WPA2. WPA2-PSK è simile al WPA-PSK e si basa sullo standard WPA2. Una funzione comune di WPA2-PSK è che i dispositivi spesso supportano più modalità di crittografia (ad esempio AES, TKIP) contemporaneamente, mentre i dispositivi più obsoleti supportano generalmente solo una singola modalità di crittografia alla volta (ossia, tutti i client devono utilizzare la stessa modalità di crittografia).

Informazioni su McAfee

McAfee, Inc., con sede centrale a Santa Clara, California, e leader globale nella gestione dei rischi legati alla prevenzione delle intrusioni e alla protezione, offre soluzioni e servizi dinamici e affidabili che proteggono sistemi e reti di tutto il mondo. Grazie alla sua insuperata esperienza in materia di protezione e al suo impegno in termini di innovazione, McAfee offre agli utenti privati, alle aziende, al settore pubblico e ai provider di servizi la capacità di bloccare gli attacchi, di impedire le interruzioni e di controllare e migliorare continuamente la protezione dei loro computer.

Copyright

Indice

L

M

N

O

P

V

W