Le reti

Sicurezza in rete

Tipi di reti

Con il termine *rete* si intende un insieme di componenti, sistemi o entità interconnessi tra loro. Nell'ambito dell'informatica, una rete è un complesso sistema di connessione di dispositivi informatici attraverso collegamenti fisici (linee telefoniche, cavi dedicati, onde radio, ecc.) al fine di utilizzare nel miglior modo possibile le risorse disponibili e di offrire vari servizi di comunicazione.
Il progetto di una rete copre ampie problematiche che vanno della sua architettura fisica alla codifica dei dati per facilitare la trasmissione, fino alla costruzione del software applicativo che mette a disposizione degli utenti i servizi di rete.
Negli ultimi due decenni, grazie alla rapida evoluzione delle tecnologie telematiche, c'è stata una espansione frenetica delle reti sia a livello locale (nelle aziende e negli uffici), sia a livello mondiale (Internet).
I principali vantaggi di una rete sono:

1. Condivisione risorse (file, periferiche…)
2. Indipendenza dei singoli elaboratori
3. Tolleranza ai guasti
4. Dischi e servizi di backup
5. Condivisione delle informazioni
6. Possibilità di lavoro di gruppo

In base all'estensione, geografica si possono identificare i seguenti tipi di reti.
Una rete locale o **LAN** (Local Area Network) è un gruppo di elaboratori e di altri dispositivi elettronici interconnessi che si trovano all'interno dello stesso edificio ed utilizzano mezzi trasmissivi dedicati e privati. Una normale LAN è quindi una *piccola* rete (da 2 a 30 utenti), che comunque non attraversa il suolo pubblico con i propri mezzi trasmissivi; ciò esonera il sistema dal puntuale rispetto degli standard della telefonia e della trasmissione dei dati pubblici.
Quando la rete locale diventa fisicamente molto grande e le distanze fra gli elaboratori aumentano considerevolmente, vengono inseriti nella struttura della rete dei dispositivi (quali *hub*, *bridge* o *switch*) che consentono di potenziare il segnale che fluisce attraverso i cavi in modo che raggiunga in maniera comprensibile il destinatario. Una rete formata da nodi che si trovano a notevoli distanze e che utilizzi canali trasmissivi che attraversano il suolo pubblico viene detta **WAN** (*Wide Area Network*): è una rete molto estesa a livello geografico, fino a livello mondiale come la rete internet.

Le problematiche di una WAN sono molto diverse di quelle di una LAN sia a causa dei vincoli imposti dagli enti preposti al controllo delle telecomunicazioni, sia per i diversi mezzi trasmissivi che il messaggio deve attraversare prima di giungere al destinatario.
Nelle reti geografiche vengono usati tutti i mezzi trasmissivi disponibili, dai doppini telefonici alle fibre ottiche, utilizzando anche le più moderne tecnologie satellitari.
A metà via tra LAN e WAN si trovano le reti **MAN** (*Metropolitan Area Network*) che utilizzano tecnologie simili a quelle delle reti locali, avendo però mezzi trasmissivi messi a disposizione da un gestore pubblico. In effetti una WAN è formata dalla connessione di un elevato numero di elaboratori singoli, reti locali e MAN e la sua efficienza si misura nel modo in cui permette la comunicazione fra le varie reti di base.
Un "ibrido" tra una Lan e una Man sono le reti **VPN** (Virtual Private Network). Una VPN è una rete privata (caratteristica della LAN) che sfrutta una rete pubblica (caratteristica della MAN e WAN), la rete internet, per permettere ai computer appartenenti alla rete di comunicare tra loro come se fossero collegati allo stesso server. Il termine "Virtuale" è dovuto al fatto che i computer non sono effettivamente collegati solo tra loro, non hanno delle linee dedicate, ma utilizzano una struttura pubblica quale, appunto, la rete internet. La rete VPN permette a computer ubicati in luoghi fisici diversi di stabilire un collegamento privato come se ci fosse un "tunnel" virtuale che corre tra i nodi pubblici di internet.
Dato che le connessioni a internet sono connessioni pubbliche, quindi con accesso non protetto, c'è il rischio che le informazioni trasmesse sul web attraverso una VPN possano essere intercettate. Per questo motivo con una rete VPN è possibile crittografare i dati e inviarli solo a un computer, o a gruppi di computer specifici. Inoltre i collegamenti attraverso le reti VPN necessitano di una *autenticazione* all'accesso, in modo che l'utilizzo sia concesso solo a utenti autorizzati. La sicurezza è quindi garantita dai protocolli di cifratura e dall'autenticazione.

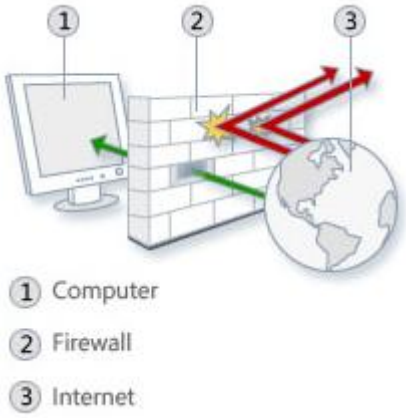
L'amministratore di rete

Abbiamo visto come, nell'utilizzo di una rete, sia di fondamentale importanza garantire la sicurezza dei dati e l'accesso ad essi solo da parte di utenti autorizzati.
L'*amministratore di rete* (o di sistema) è la figura professionale che, oltre ad occuparsi della gestione e della manutenzione della rete, deve garantire, anche per aspetti "legali", un'adeguata protezione dei dati. Non sono amministratori di sistema coloro che intervengono sugli elaboratori solo occasionalmente (per esempio, a scopo di manutenzione straordinaria).
L'individuazione precisa e responsabile di tali soggetti è una delle scelte fondamentali all'interno di un'azienda. Infatti, l'amministratore di sistema deve implementare, in raccordo con il titolare e/o eventuali altri responsabili delle informazioni, *politiche di accesso* alle risorse della rete, come documenti, cartelle, componenti hardware, ecc. Deve stabilire chi, e come, può accedere alle risorse del sistema informativo e a tutti i dati personali aziendali (anche sensibili): per tale motivo gli amministratori di sistema devono essere scelti con particolare attenzione, poiché i rischi che possono correre le banche dati o le reti informatiche sono sempre più elevati.
La gestione degli accesi avviene con l'assegnazione di *account*, composto da un nome utente e una password, agli utenti del sistema. Il nome utente serve a identificare l'utente, la password ad autenticare. Ad ogni account è associato il rispettivo livello di abilitazione per l'accesso alle risorse.

L’amministratore deve aver cura di conservare l’elenco degli account in un luogo sicuro e richiedere la modifica periodica delle password da parte degli utenti.

Firewall

Un firewall (letteralmente, muro di fuoco) è un software, o un hardware, se non addirittura un computer o un insieme di computer posto sul “confine” telematico, ad esempio presso il modem o il router, tra un computer, o una rete locale, e il resto del mondo collegato alla rete. Serve per proteggere contro aggressioni provenienti dall’esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell’utente. Il firewall applica dei filtri software ai dati in entrata e in uscita, per bloccare gli attacchi via internet.



Configurare il firewall di Windows: consentire un programma

Per garantire il controllo in entrata e in uscita, un firewall deve essere ben configurato. La sua configurazione è un compromesso tra usabilità della rete, sicurezza e risorse disponibili per la manutenzione della configurazione stessa Le regole che si impostano per il firewall influenzano l’efficace funzionamento.

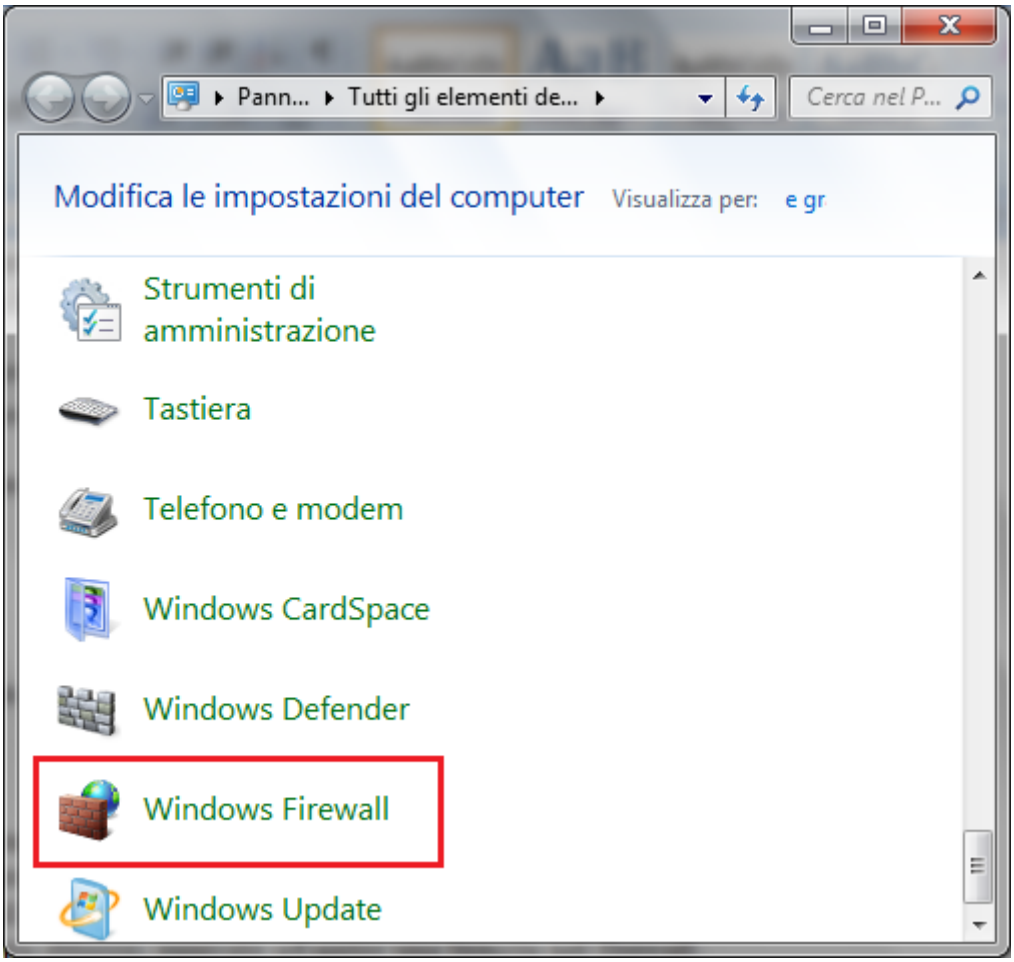
Il firewall presente in Windows consente di specificare quali programmi possono ricevere informazioni attraverso il firewall e di impostare regole per le connessioni in entrata e in uscita.

Per prima cosa vediamo come consentire ad un programma di inviare o ricevere informazioni attraverso il firewall.

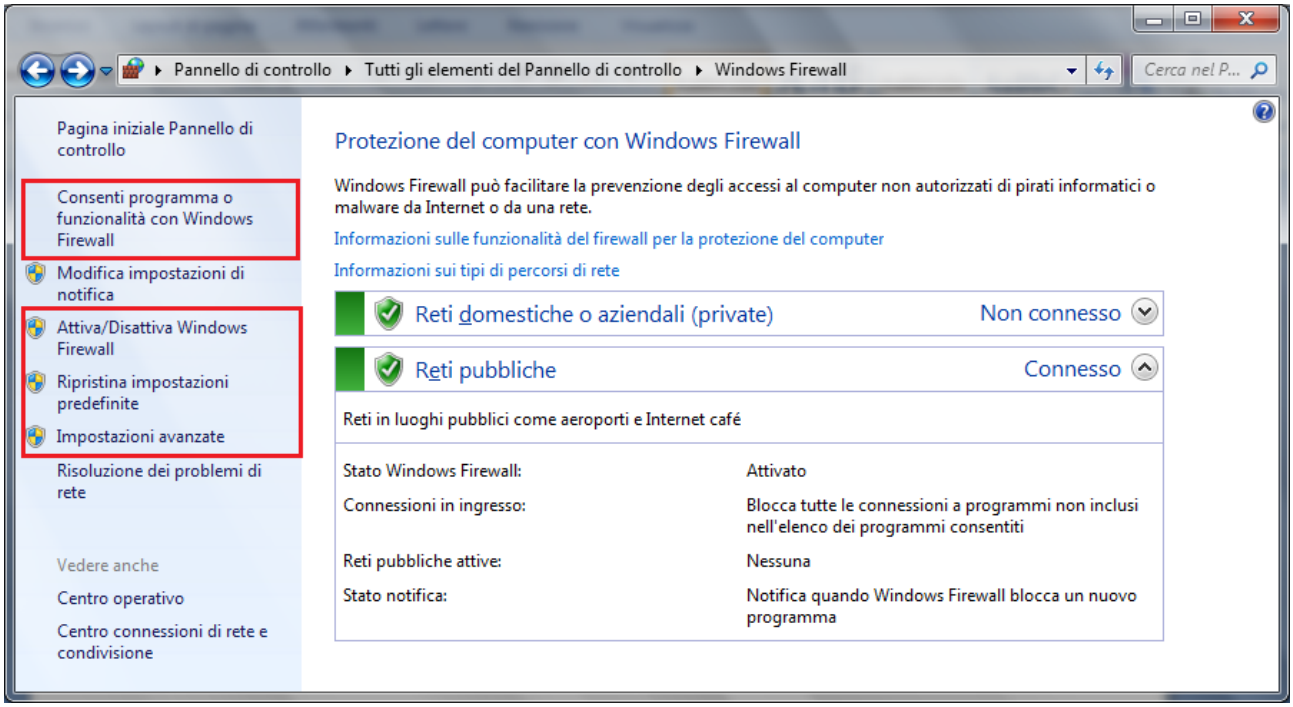
Per impostazione predefinita, la maggior parte dei programmi viene bloccata da Windows Firewall per garantire una maggiore sicurezza del computer. Ma potrebbe essere necessario consentire a tali programmi di comunicare attraverso il firewall.

Ad esempio, proviamo ad aggiungere ai programmi consentiti alla comunicazione il browser Mozilla Firefox. Può capitare che il firewall non consente la connessione con Firefox: in questo caso, il browser può riportare errori di tipo “Indirizzo non trovato” quando si cerca di accedere ad un sito web.

Per accedere al firewall aprire il **Pannello di controllo** di Windows.

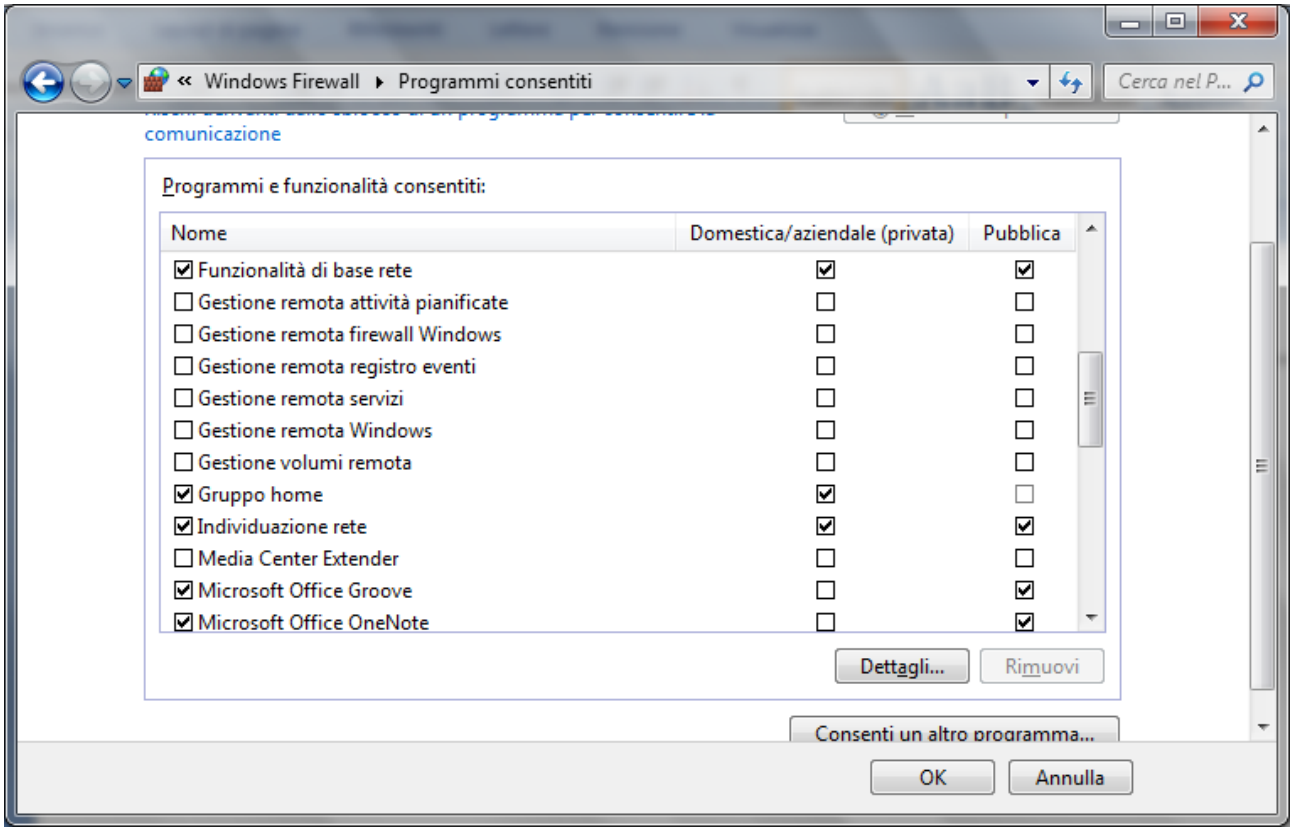


Con due clic sull'icona appare la finestra iniziale del firewall.

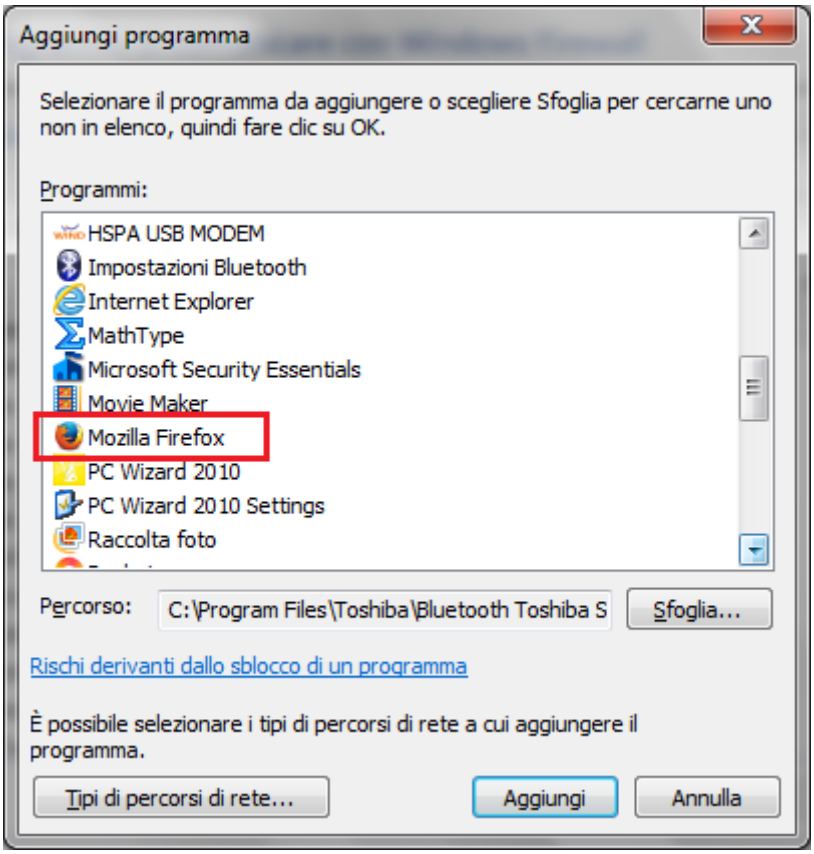


Da questa finestra è possibile Disattivare o attivare il firewall con il comando **Attiva/Disattiva Windows Firewall**.

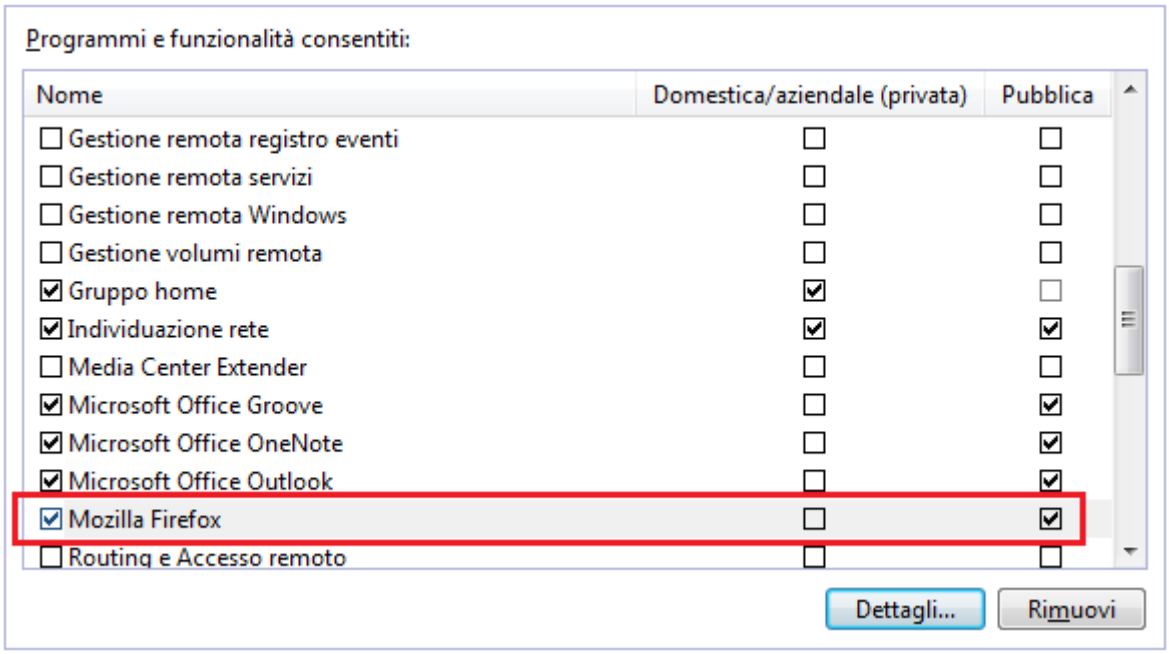
Per aggiungere un programma fare clic su Consenti programma o funzionalità con Windows Firewall.



A questo punto, basta selezionare la casella di controllo accanto al programma che si desidera abilitare. Se il programma non appare nell'elenco, come nel nostro caso, si può aggiungerlo con il comando **Consenti un altro programma**. Verrà visualizzata la finestra **Aggiungi programma**.



Se non appare il programma nella lista, con un clic sul pulsante **Sfoglia** si può navigare fino alla cartella di installazione di Firefox (cioè C:\Program Files\Mozilla Firefox\) e scegliere firefox.exe.
A questo punto, fare clic sul pulsante **Aggiungi** e sul pulsante **OK** per chiudere la finestra dei programmi consentiti.

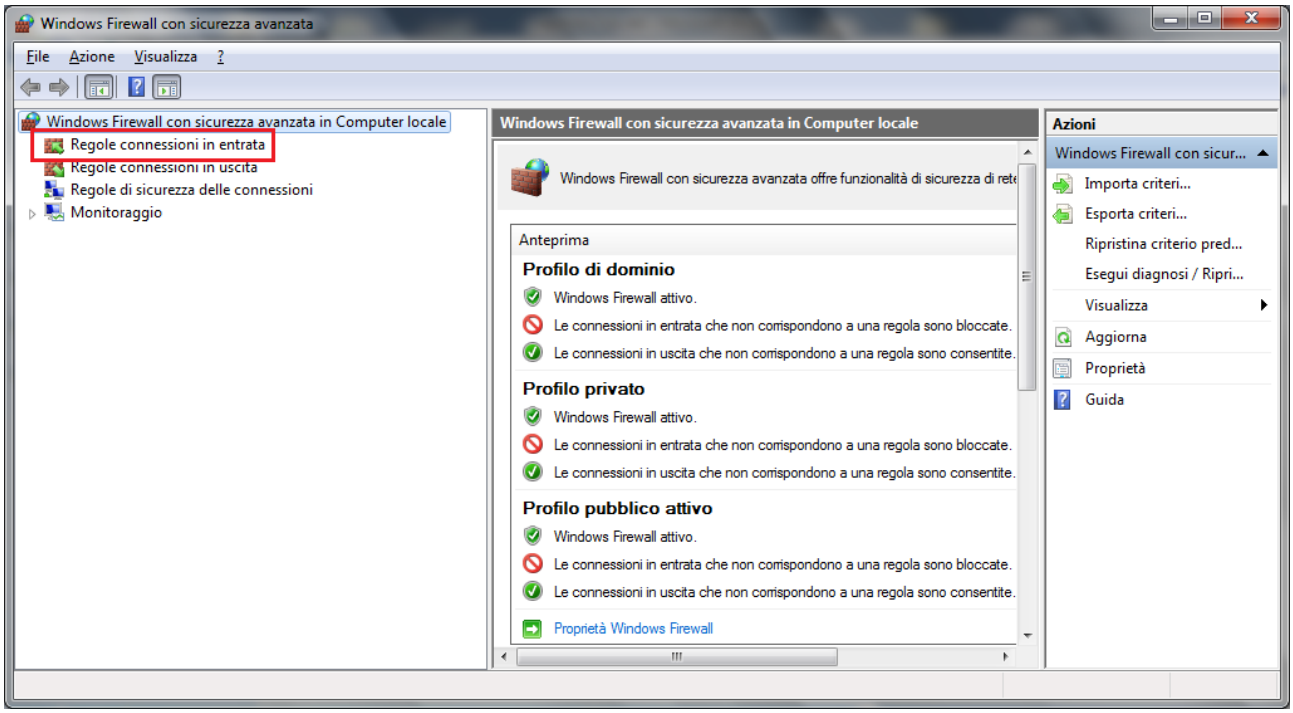


Ad ogni programma consentito si possono associare due tipologie di rete:

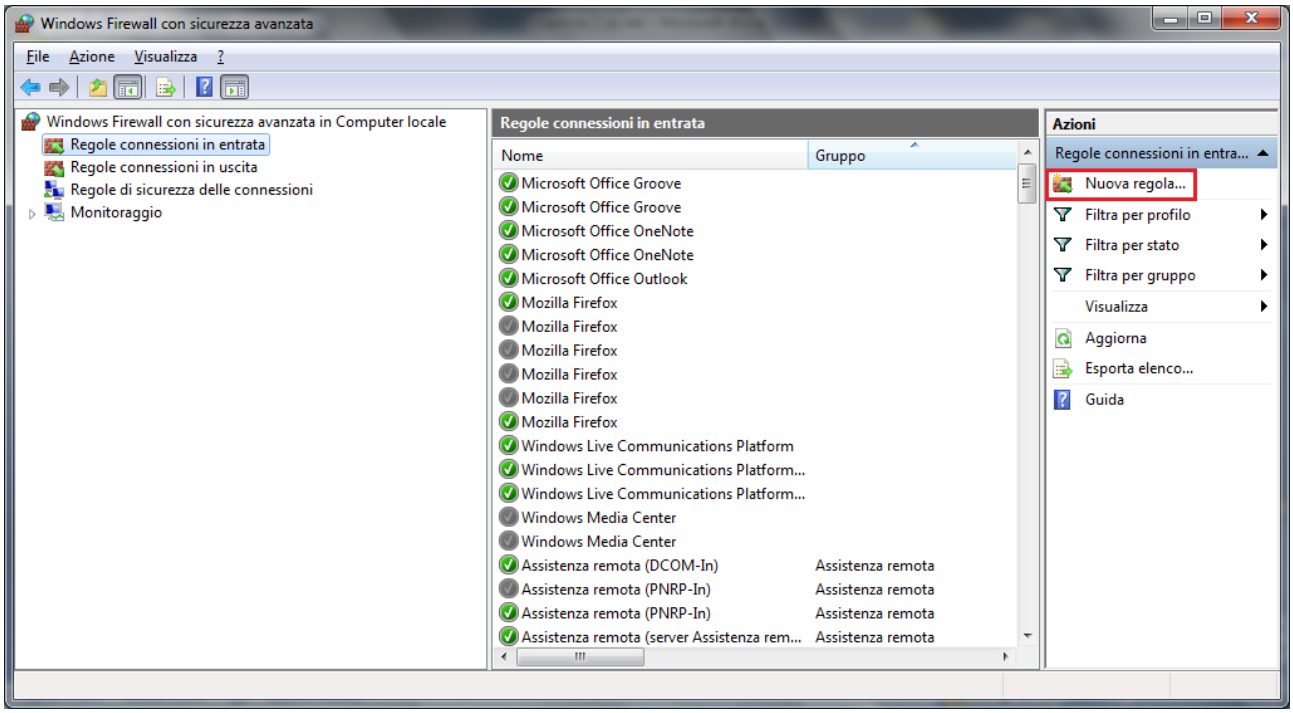
Domestica/aziendale (privata): sono le reti interne al proprio domicilio o azienda. In generale le reti dove i computer collegati si considerano attendibili e "sicuri".
Pubblica: sono reti in luoghi pubblici, quali Internet café o aeroporti. Se questo percorso è disabilitato si impedisce agli altri computer nelle vicinanze la visualizzazione del computer in uso, in modo da proteggerlo da qualsiasi software dannoso proveniente da internet.

Configurare il firewall di Windows: aggiungere o togliere regole

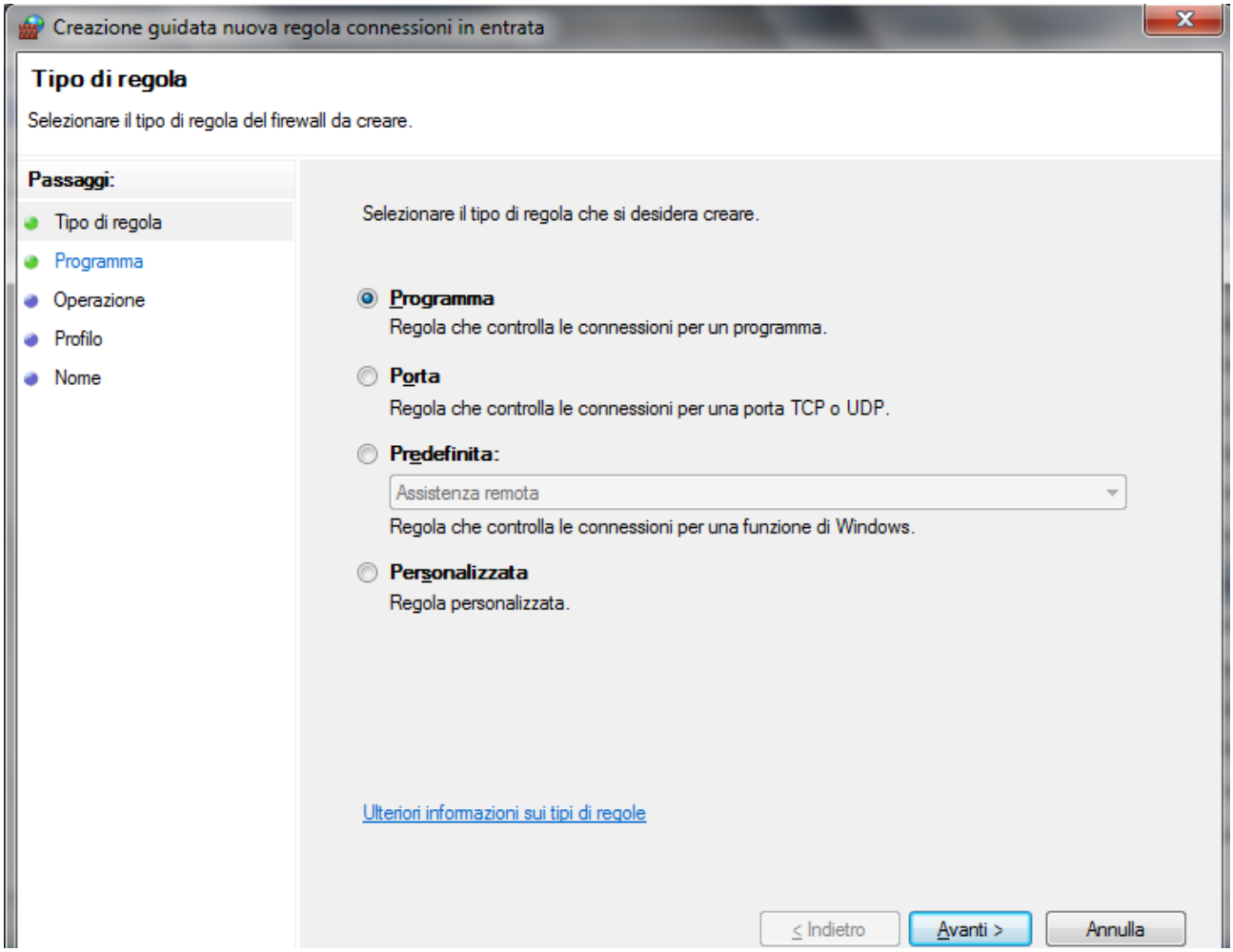
Aggiungendo un programma si apre un ulteriore accesso attraverso il firewall solo quando il programma è in esecuzione.
Ci possono essere dei casi in cui si preferisce aprire una **porta** di comunicazione, ad esempio se si desidera rendere disponibile un programma su un computer ad altri utenti tramite internet. Una porta è un numero che va da 0 a 65535 e serve ai computer per capire a che programma devono essere deviati i dati che arrivano. Possiamo pensare che se il computer fosse un condominio, il numero di IP (numero che identifica il computer nella rete) sarebbe l'indirizzo dell'edificio. La porta possiamo immaginarla come uno degli appartamenti interni al condominio, in cui ogni appartamento è un programma che vuole comunicare con internet.
Nel caso precedente abbiamo visto come consentire (o non consentire) ad un programma di ricevere o inviare dati attraverso il firewall. In questo caso siamo ad un livello più dettagliato: si specifica *attraverso quale porta* un programma può ricevere o inviare i dati o, viceversa, quale porta non deve usare per queste operazioni.
Di norma, un firewall blocca preventivamente qualsiasi tentativo proveniente dalla rete di accedere alle applicazioni installate sul sistema o alle funzionalità del sistema operativo. Ma, in talune circostanze, consentire l'accesso da remoto a certi programmi in esecuzione sul PC può essere una azione desiderata. Facciamo il caso che ci sia un programma che debba condividere file e cartelle con alcuni utenti remoti, cioè si comporti comporta come una sorta di server web. In questo caso si deve creare una specifica regola in entrata. Oppure se si desidera partecipare con gli amici a un gioco di gruppo su internet, potrebbe essere necessario aprire una specifica porta per il gioco in modo che il firewall consenta alle informazioni relative al gioco di raggiungere il computer. Altri esempi possono essere software per il peer-to-peer, le chat, la videoconferenza, ecc.
In questo caso la porta rimarrà sempre aperta: bisogna ricordarsi di chiuderla quando non sarà più necessario tenerla aperta.
Dalla finestra iniziale di Microsoft Firewall scegliere **Impostazioni avanzate**. Appare la finestra **Windows Firewall con sicurezza avanzata**.



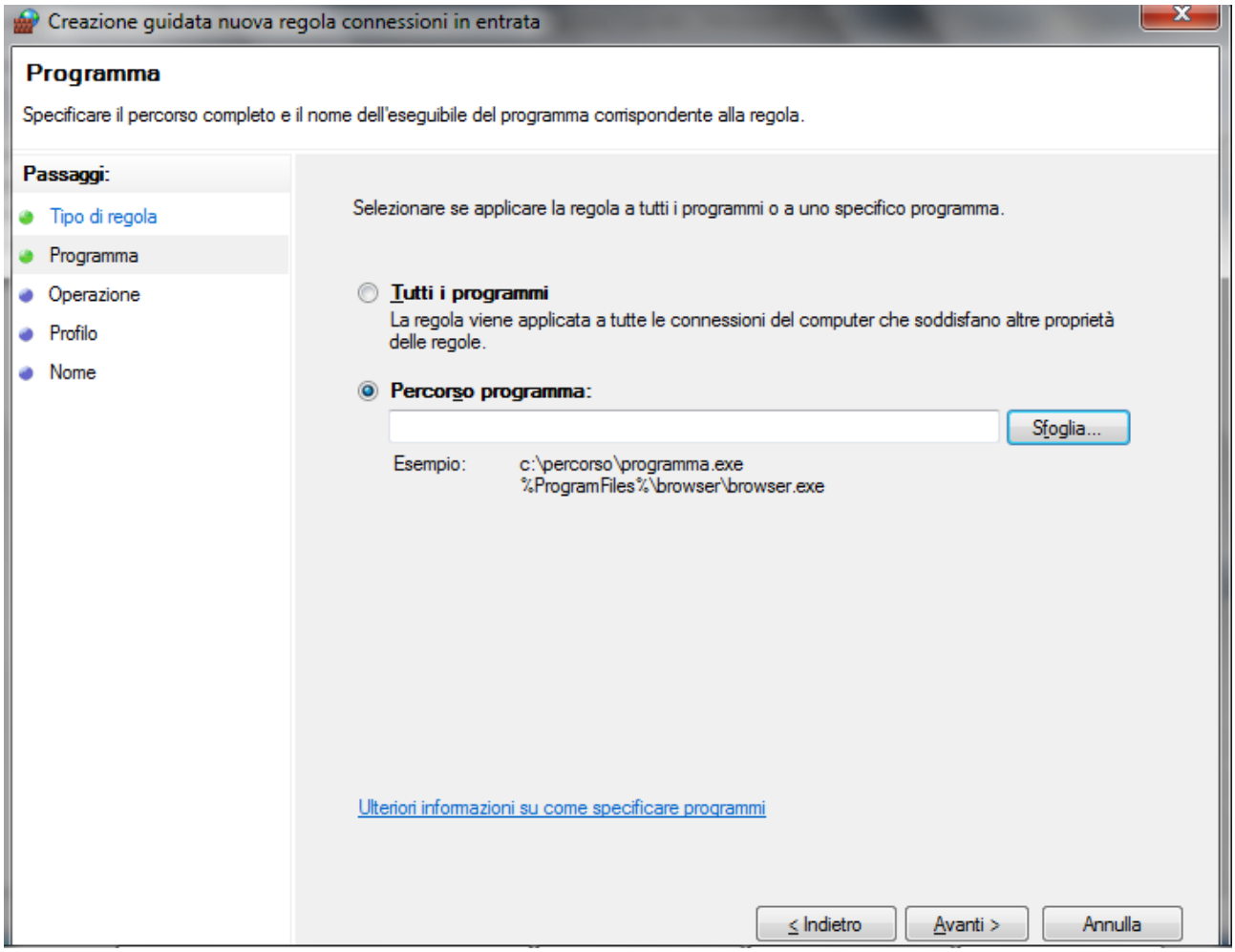
I comandi presenti in questa finestra sono molto specifici ed è preferibile che siano utilizzati solo da utenti esperti. Ci limitiamo a trattare solo un esempio di aggiunta di una regola di connessione in entrata, che poi elimineremo.
Nella colonna di sinistra scegliere **Regole connessioni in entrata**.



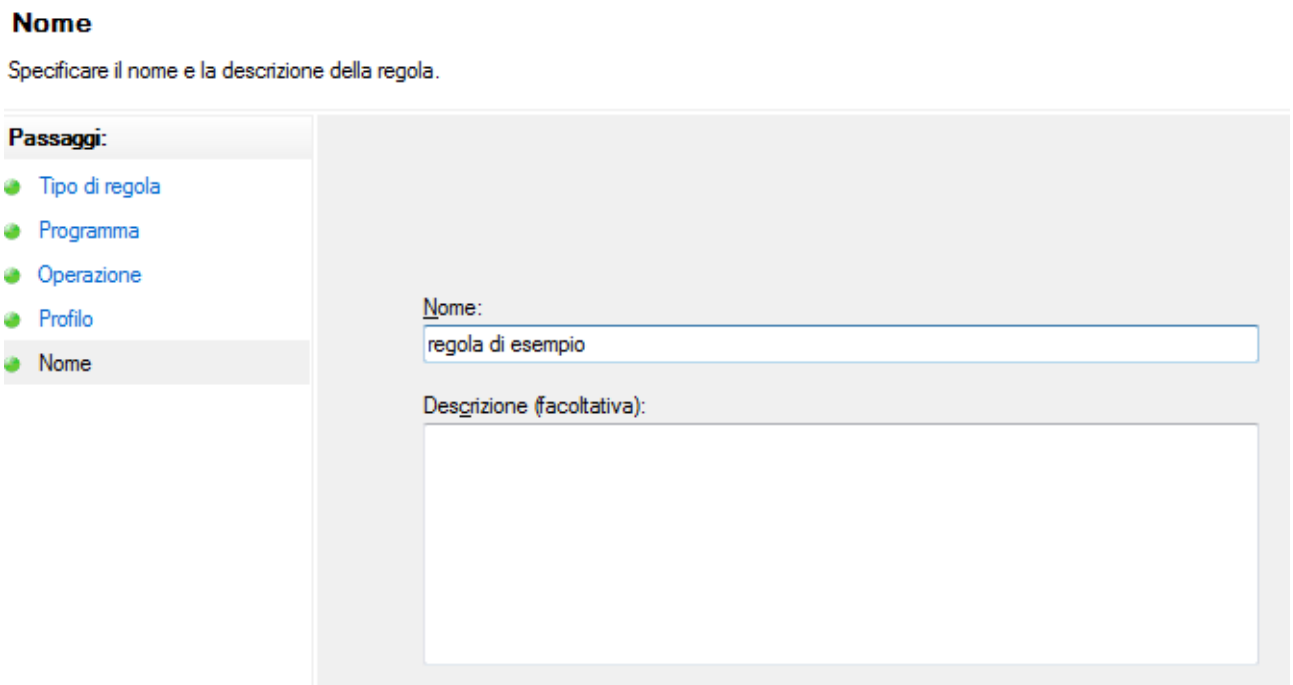
Appare l'elenco delle regole abilitate (icona verde) e disabilitate (icona grigia). Fare clic su **Nuova regola** (riquadro di destra) per iniziare la procedura guidata di creazione di una regola.



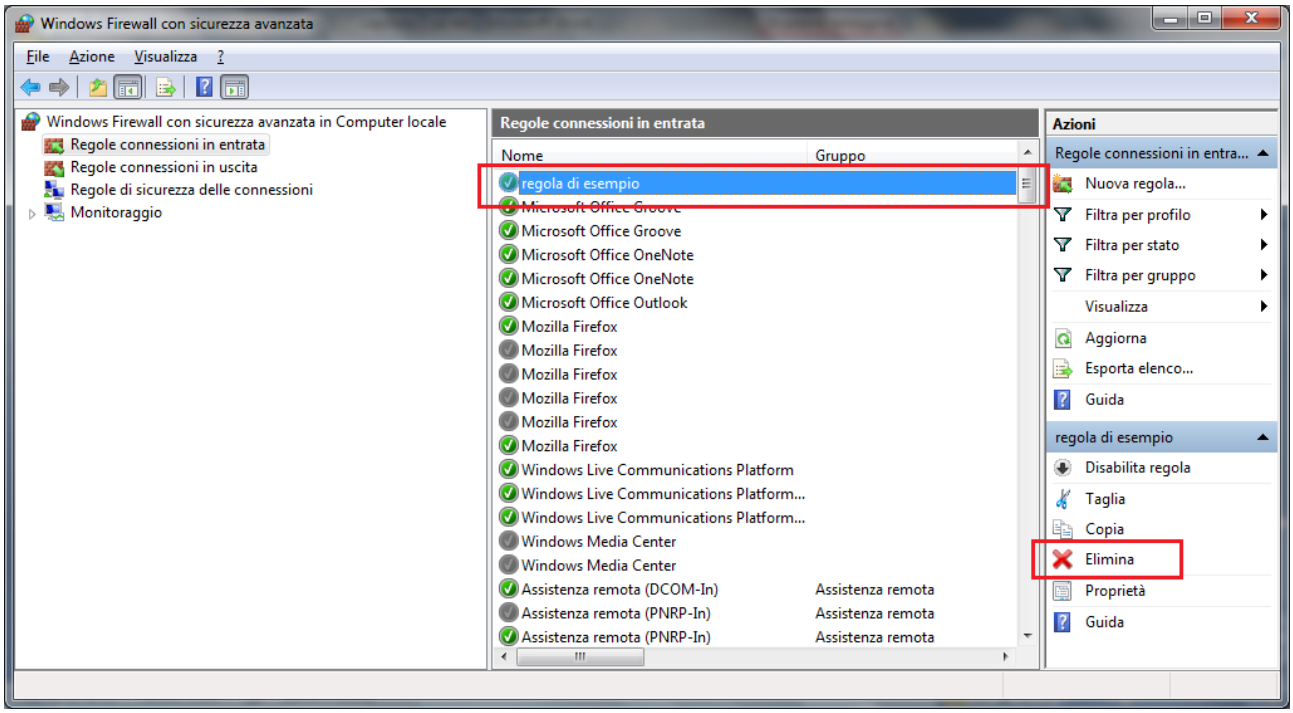
Windows Firewall con sicurezza avanzata offre quattro tipi di base di regole firewall. Utilizzando uno di questi tipi di regole firewall, è possibile creare eccezioni per consentire o negare in modo esplicito una connessione attraverso Windows Firewall.
Vediamo solo il caso di regola di **Programma** per autorizzare una connessione a seconda del programma che tenta di stabilirla.
Fare clic su **Avanti** per specificare il percorso del file del programma.



Scegliere un programma qualunque. Nel nostro esempio abbiamo scelto CCleaner. I passaggi successivi riguardano la scelta della porta per la connessione e del dominio e sono troppo tecnici: fare ripetutamente clic su **Avanti**, fino ad arrivare al nome della regola.



Inserire un nome fittizio e fare clic su **Fine**. La nuova regola appare nell'elenco delle regole.



Cancella la regola dall'elenco con il comando **Elimina**.

Configurare il firewall di Windows: considerazioni conclusive

Quando si aggiunge un programma all'elenco dei programmi consentiti in un firewall o si apre una porta di un firewall, si consente a un programma specifico di inviare o ricevere informazioni nel computer attraverso il firewall. Consentire a un programma di comunicare attraverso un firewall, operazione denominata talvolta **sblocco**, equivale ad aprire una breccia nel firewall.

Ogni volta che si apre una porta o si consente a un programma di comunicare attraverso un firewall, si riduce leggermente la sicurezza del computer. Maggiore è il numero di programmi consentiti o di porte aperte nel firewall, maggiori sono le opportunità per i pirati informatici o per il software dannoso di utilizzare una di tali aperture per diffondere un worm, accedere ai file o utilizzare il computer per diffondere software dannoso ad altri utenti.

È più sicuro, in genere, aggiungere un programma all'elenco dei programmi consentiti anziché aprire una porta. Una porta rimane aperta finché non viene chiusa, indipendentemente dal fatto che venga utilizzata o meno da un programma. Se si aggiunge un programma all'elenco dei programmi consentiti, la "breccia" viene aperta solo quando richiesto per una particolare comunicazione.

Per ridurre i rischi relativi alla sicurezza:

1. Consentire un programma o aprire una porta solo se strettamente necessario e rimuovere programmi dall'elenco dei programmi consentiti oppure chiudere le porte quando queste configurazioni non sono più necessarie. Come regola generale, si concede l'accesso a internet solo ai programmi che conosciuti e solo se la loro richiesta ha un senso. Per esempio, è ovvio che il browser (che sia Internet Explorer, Firefox, Chrome o quant'altro) avrà bisogno di accedere a internet, se vogliamo usarlo: il compito di un browser è appunto quello di navigare nei siti internet, per cui gli dovremo concedere il permesso di collegarsi a internet. Allo stesso modo, se

utilizziamo un programma per scaricare le e-mail sul nostro computer, avrà bisogno del permesso di collegarsi sia in entrata (per ricevere le e-mail), sia in uscita (per spedire le e-mail). Altri programmi, invece, avranno bisogno di poter accedere a internet solo per eventuali aggiornamenti. Se un programma cerca di collegarsi a internet in un momento in cui, apparentemente, non ha alcun bisogno di collegarsi, allora è sempre meglio negargli il permesso.

2. Non consentire mai a un programma sconosciuto di comunicare attraverso il firewall. Infatti, esiste sempre la possibilità che questo programma sia un virus, che abbiamo preso senza accorgercene, oppure che sia un programma infettato da un virus: in questo caso, l'accesso a internet gli servirà per comunicare con il creatore del virus, passargli le nostre informazioni, oppure aprirgli la porta e farlo entrare nel nostro computer.

Per ritornare alla configurazione iniziale fare clic su **Ripristina impostazioni predefinite**.