2.1 Configurare il Firewall di Windows

Due o più computer possono scambiare dati, informazioni o servizi di tipo diverso utilizzando una **connessione**. Quindi, spesso, ad una **connessione fisica** corrispondono più **connessioni logiche**, una per ogni servizio attivo.

Per esempio attraverso un'unica connessione via cavo è possibile effettuare più connessioni logiche (al server di *Google*, *Skype*, *Facebook*, *eMule*).

Per distinguere le connessioni logiche si utilizza il concetto di *porta*. Una **porta** può essere pensata come un numero che permette di individuare il servizio. Quando si deve inviare un pacchetto di dati da un computer all'altro è possibile indicare l'**indirizzo IP** (per esempio 192.168.1.117), specificando il numero di porta (per esempio 8080) dopo il carattere due punti. Per esempio

192.168.1.117:8080

Quindi gli indirizzi:

192.168.1.117:4668 192.168.1.117:8080 192.168.1.117:4678

indicano tre connessioni logiche differenti (porte 4668, 8080 e 4678) destinate alla stessa interfaccia di rete (192.168.1.117).

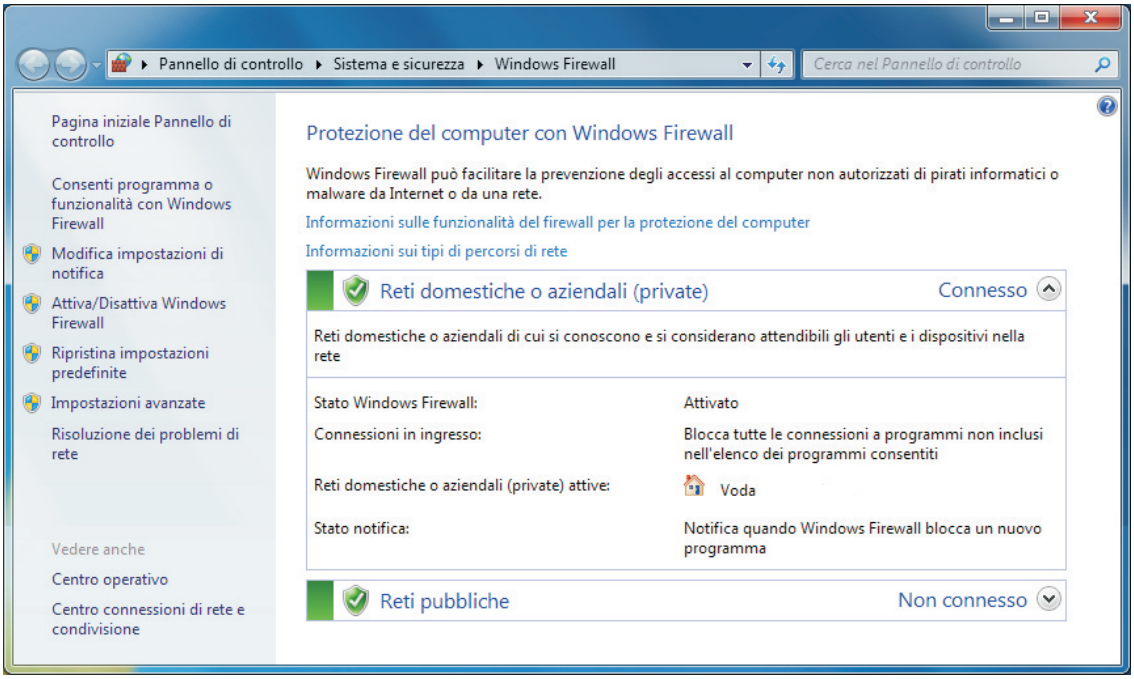
Molti servizi standard utilizzando sempre la stessa porta, per cui esiste un elenco, stabilito a livello internazionale, che ad ogni porta associa il servizio relativo (in inglese: *well-known port*). Per esempio:

Numero di porta	Nome del servizio	Descrizione del servizio
20 e 21	FTP	Trasferimento dati
22	SSH	Accesso remoto sicuro
23	TELNET	Accesso remoto
80, 8080	HTTP	Trasmissione di pagine Web
443	HTTPS	Trasmissione di pagine Web criptate
110, 995	POP3	Ricezione di posta elettronica
25, 465	SMTP	Invio di posta elettronica

Dunque qualsiasi computer, connesso ad una rete, effettua numerose connessioni. Alcune di queste connessioni potrebbero essere utilizzate da malintenzionati per scopi malevoli. Un **firewall** è un programma che controlla tutte le connessioni in entrata e in uscita e, in base a un elenco di regole predefinite, le autorizza o le blocca. Un *firewall* può essere sia *hardware* che *software*.

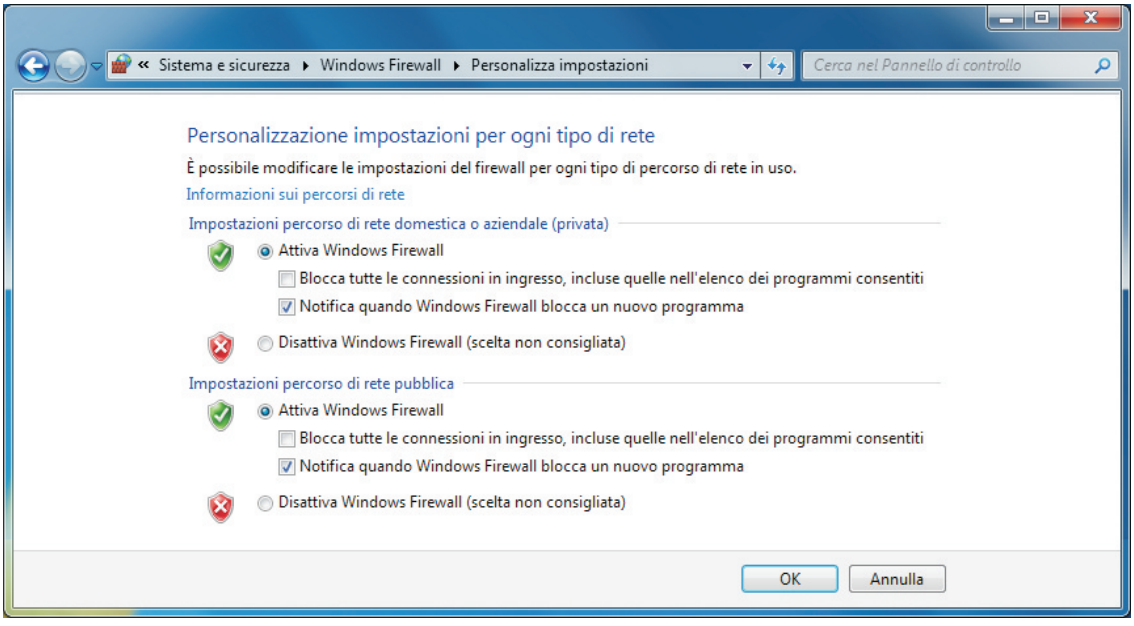
Il sistema operativo *Windows*, a partire dalla versione Windows XP, integra un *firewall* che, nonostante sia molto semplice, permette di aumentare notevolmente il grado di sicurezza del sistema.

Dal pulsante *Start*, fare clic su *Pannello di controllo*: selezionare *Sistema e sicurezza* e poi *Windows Firewall*.



Attivando il firewall (con un clic su Attiva/Disattiva Windows Firewall nel riquadro a sinistra) vengono utilizzate delle regole standard. In alcuni casi, per esempio durante l'installazione di un programma o quando un software tenta di accedere alla rete, viene richiesto all'utente come comportarsi. Se l'utente ritiene che il software non sia malevolo può autorizzare la connessione. Da quel momento il firewall permetterà automaticamente di effettuare la connessione. In caso contrario il programma viene bloccato e non potrà accedere alla rete.

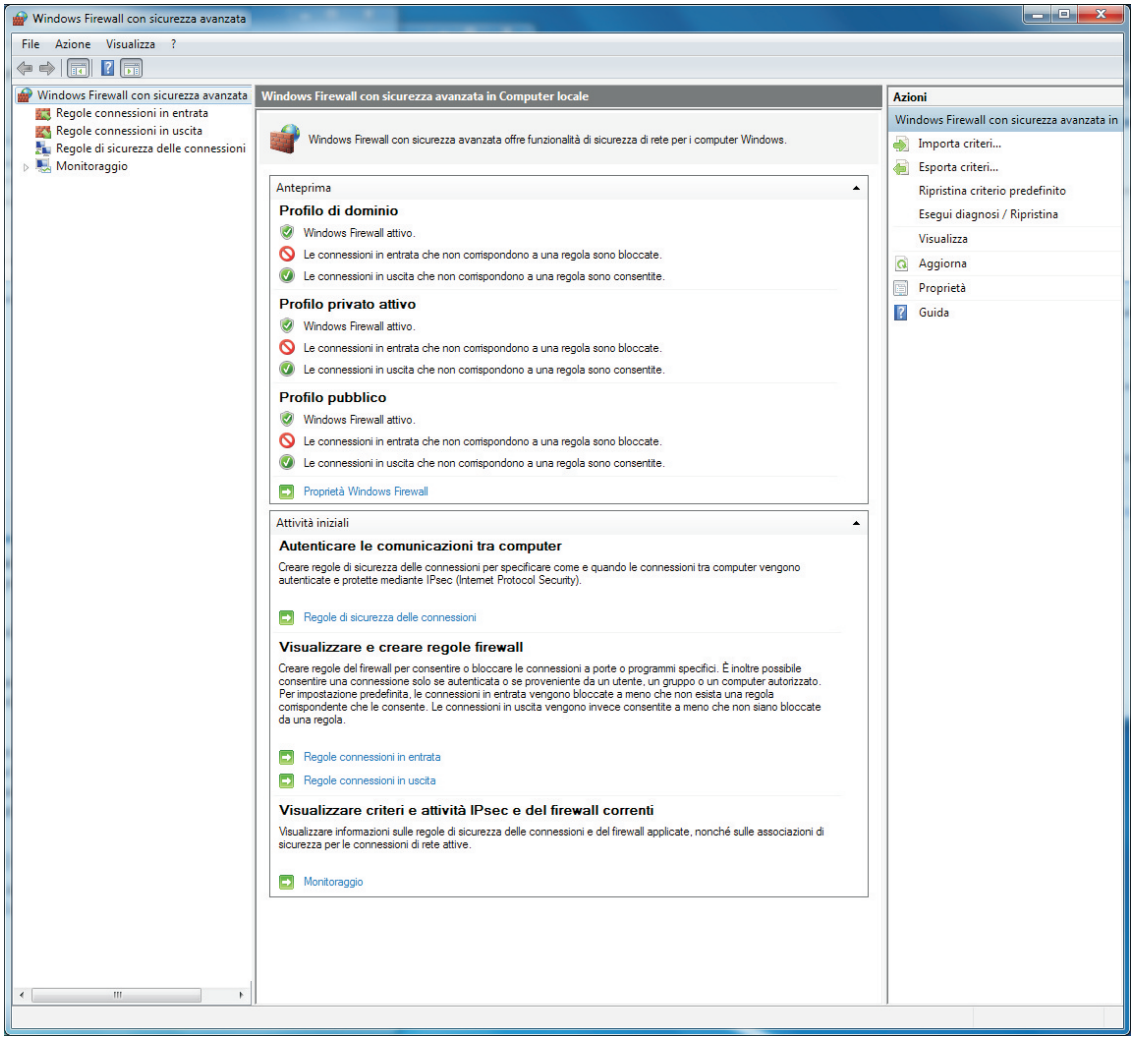
La scelta Modifica impostazioni di notifica consente di personalizzare il comportamento del firewall.



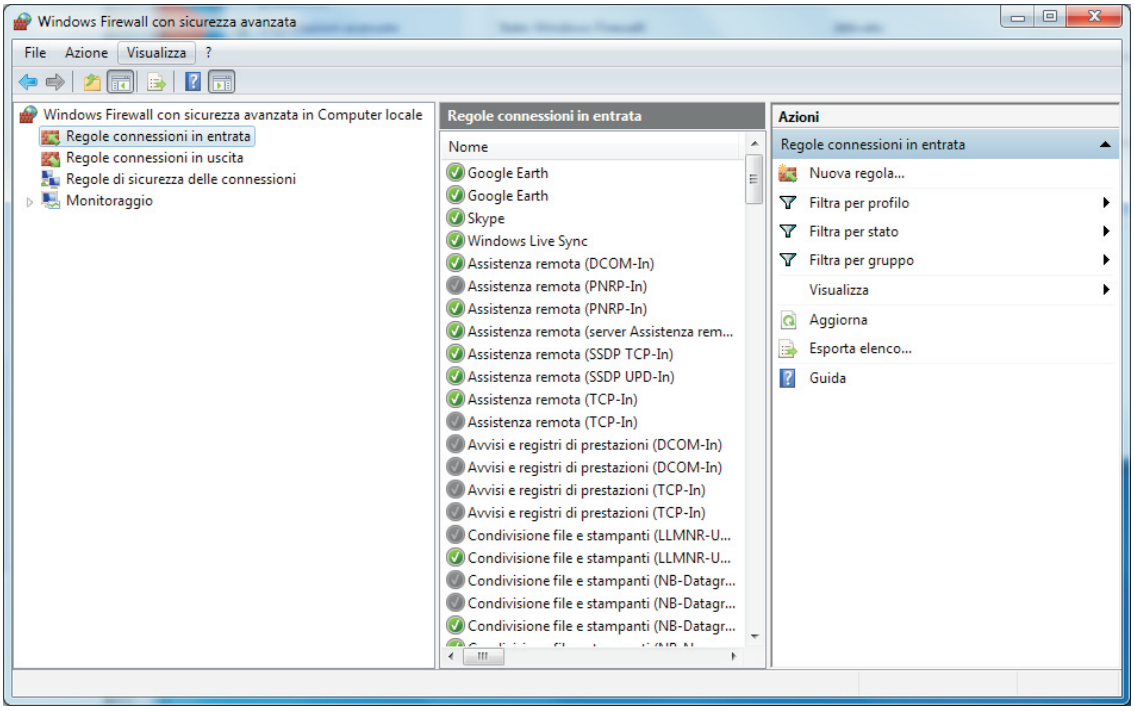
Le reti vengono divise in due categorie: **reti domestiche** (cioè reti locali nelle quali l'utente stesso è amministratore del computer) e **reti pubbliche** (per esempio una rete *wi-fi* pubblica in un aeroporto).
È possibile scegliere se **attivare o disattivare** il firewall. Se il firewall viene attivato si può scegliere tra due comportamenti:

- "*Blocca tutte le connessioni in ingresso, incluse quelle nell'elenco dei programmi consentiti*": è la scelta più sicura, ma potrebbe impedire il funzionamento corretto di alcuni programmi che devono utilizzare la rete.
- "*Notifica quando Windows Firewall blocca un nuovo programma*": richiede all'utente cosa fare ogni volta che un nuovo programma tenta di effettuare una connessione. Questa opzione è meno sicura, ma ci potrebbero essere numerose richieste all'utente; tuttavia permette ai programmi di funzionare correttamente.

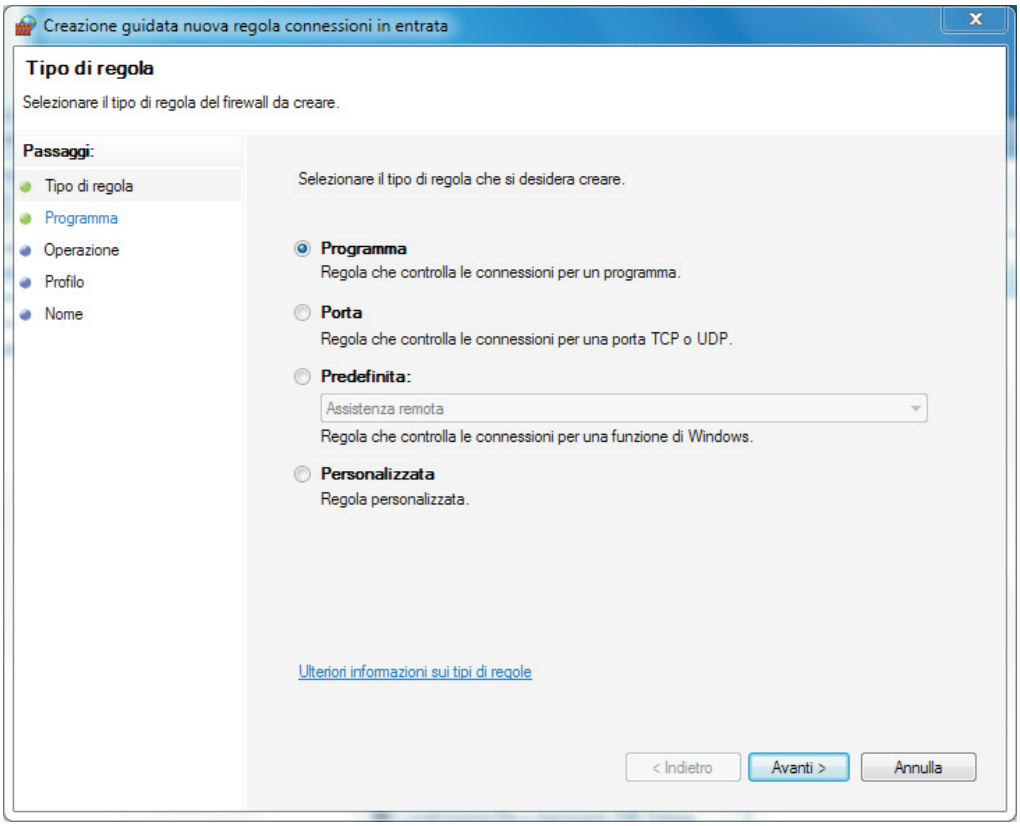
Con la scelta Impostazioni avanzate è possibile creare delle regole personali.



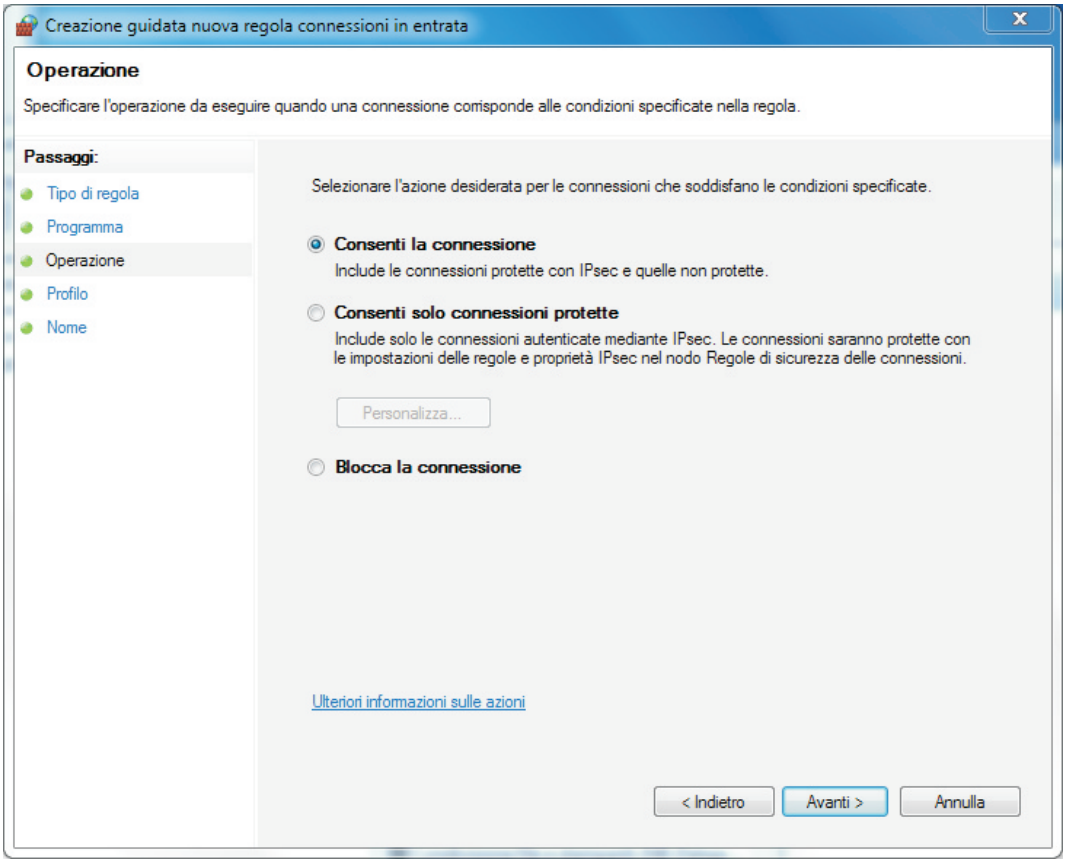
Supponiamo di voler consentire a un programma di accettare connessioni da Internet. Visto che si tratta di un programma che risiede sul nostro computer occorre andare in "*Regole di connessioni in entrata*".



Si deve fare clic su "*Nuova regola...*" in alto a destra.
Selezionare "*Programma*" e poi fare clic sul pulsante "*Avanti*".



Nella schermata successiva occorre selezionare il nome del programma eseguibile e poi fare clic sul pulsante "*Avanti*". A questo punto è possibile impostare "*Consenti la connessione*" e dare un nome alla regola.



Occorre ricordare che un firewall non è un antivirus, in quanto non modifica i dati presenti sul computer. Il firewall si limita a impedire che il software malevolo possa eseguire una connessione. Se però un virus è presente nel computer e non effettua connessioni verso l'esterno, esso non può essere individuato dal firewall e quindi può arrecare danni al sistema.