

Uso di Windows Firewall

Che cos'è un firewall

Connettersi a Internet senza utilizzare un firewall, è come entrare in un negozio lasciando le chiavi nell'automobile e lo sportello aperto. Sebbene siate convinti di entrare e uscire dal negozio senza che nessuno lo noti, qualcuno invece potrebbe approfittarsi della situazione.

In Internet, gli hacker (sarebbe meglio dire i *malintenzionati*) utilizzano codice dannoso, ad esempio virus, worm e trojan, alla ricerca di computer non sufficientemente protetti. Un firewall può essere di aiuto per proteggere il computer da questi come da altri tipi di minacce.

Cosa può comportare l'attacco di un malintenzionato? Questo dipende dalla natura dell'attacco. Sebbene molti attacchi rappresentano solo una seccatura poiché si tratta spesso di hacker che si divertono a penetrare nei computer vulnerabili solo per gioco, in altri casi l'intento è effettivamente quello di creare danni, come eliminare dati dal computer o metterlo fuori uso, rubare informazioni personali, quali le password o i numeri delle carte di credito.

Fortunatamente, è possibile ridurre il rischio di infezioni utilizzando un firewall.

Esistono sia firewall hardware per l'utilizzo nelle reti LAN aziendali, sia software per uso personale a protezione di un singolo computer: Windows Vista offre una soluzione di quest'ultimo tipo che va sotto il nome di **Windows Firewall**

Una definizione generale di firewall software è: *programma che filtra tutti i pacchetti di dati in entrata e in uscita da un singolo computer applicando regole di controllo del traffico da e verso Internet che contribuiscono alla creazione di un ambiente sicuro*

Nell'ambito delle reti di computer, un firewall (termine inglese dal significato originario di *muro tagliafuoco*) è un componente passivo di difesa; il firewall filtra il traffico per i pacchetti di dati in transito e ne esegue il monitoraggio.

Un firewall personale effettua anche un controllo di tutti i programmi, installati sul pc, che tentano di accedere ad Internet, consentendo all'utente di impostare delle regole che possano concedere o negare l'accesso ad Internet a questi programmi, ciò per prevenire la possibilità che un software nocivo possa connettere il computer all'esterno minacciandone seriamente la sicurezza.

Quando accediamo ad Internet, per visitare un sito web o per scaricare la posta elettronica, Windows Vista apre delle porte di comunicazione attraverso le quali può contattare i server web o i servizi di posta elettronica richiesti dall'utente.

La funzionalità principale di un firewall, quindi, è quella di creare un filtro sulle connessioni in entrata ed in uscita dal computer, in questo modo il dispositivo innalza il livello di sicurezza del sistema e garantisce un sufficiente livello di sicurezza.

Windows Firewall è attivato per impostazione predefinita e agisce in modo che le porte di comunicazione del computer vengano aperte solamente quando l'utente decide di accedere ad Internet e che tali porte risultino invece chiuse qualora un malintenzionato tenti di accedere tramite Internet al nostro sistema.

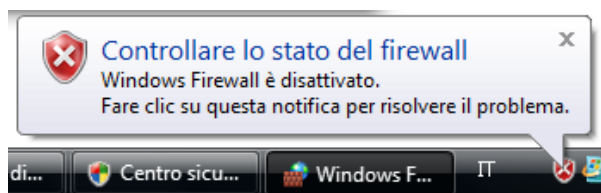
Windows Firewall è, tutto sommato, un buon prodotto, anche se sul mercato sono disponibili firewall software sicuramente migliori e più completi, sia fra quelli a pagamento che tra quelli gratuiti.

*Nel caso si decida di installare un firewall software diverso e più avanzato è buona norma disattivare **Windows Firewall** poichè i due software potrebbero presentare dei conflitti e dare dei problemi nelle connessioni in rete e, talvolta, pregiudicare la stabilità del sistema.*

Controllare lo stato di Windows Firewall

Per controllare lo stato di Windows Firewall sono disponibili sia il **Centro Sicurezza PC** all'interno del **Pannello di controllo**, sia i messaggi a forma di fumetto molto utili ed intuitivi collocati nell'area di sistema in basso a destra nello schermo.




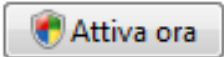






Il messaggio mostrato dallo scudetto rosso qui a fianco ci segnala che **Windows Firewall** è disattivato e che quindi il nostro computer è a rischio di intrusioni. Per risolvere il problema è sufficiente fare clic sul fumetto per aprire il **Centro Sicurezza PC**. Anche qui ci viene ribadita, con l'uso di una banda di colore rosso con la scritta **Disattivato**, la situazione di potenziale pericolo, per cui la soluzione migliore è quella di attivare **Windows Firewall**. E' sufficiente fare clic sul pulsante **Attiva ora** nella sezione **Firewall**. La barra della sezione **Firewall** ritorna verde con la scritta **Attivato**, a significare che il firewall è stato riattivato ed il computer è ora protetto.



Funzionalità fondamentali per la sicurezza

Per migliorare la protezione del computer, verificare che le quattro funzionalità fondamentali per la sicurezza siano contrassegnate come Attivato o OK.

Utilizzo di Centro sicurezza PC

Firewall	Disattivato 	
 Windows Firewall è disattivato. Mostra le opzioni disponibili.		
Nota: due o più firewall in esecuzione contemporaneamente possono entrare in conflitto. In che modo un firewall facilita la protezione del computer		
Aggiornamenti automatici	Non automatico 	
Protezione da malware	Attivato 	
Altre impostazioni di protezione	OK 	

Gestire le impostazioni di Windows Firewall

Per aprire **Windows Firewall** è sufficiente: fare clic su **Start** -> clic sulla voce **Pannello di controllo** -> clic sulla voce **Protezione** -> clic sulla voce **Windows Firewall**. Qui vediamo la schermata principale del programma: per modificarne le impostazioni -> clic sulla voce **Modifica impostazioni**

La finestra che si apre consente di visualizzare le impostazioni di **Windows Firewall**

Windows Firewall

Windows Firewall può facilitare la prevenzione degli accessi al computer non autorizzati di malintenzionati o malware da Internet o da una rete.

[In che modo un firewall facilita la protezione del computer?](#)

Windows Firewall sta facilitando la protezione del computer

Windows Firewall attivo. [Modifica impostazioni](#)

Le connessioni in ingresso per cui non è definita alcuna eccezione sono bloccate.

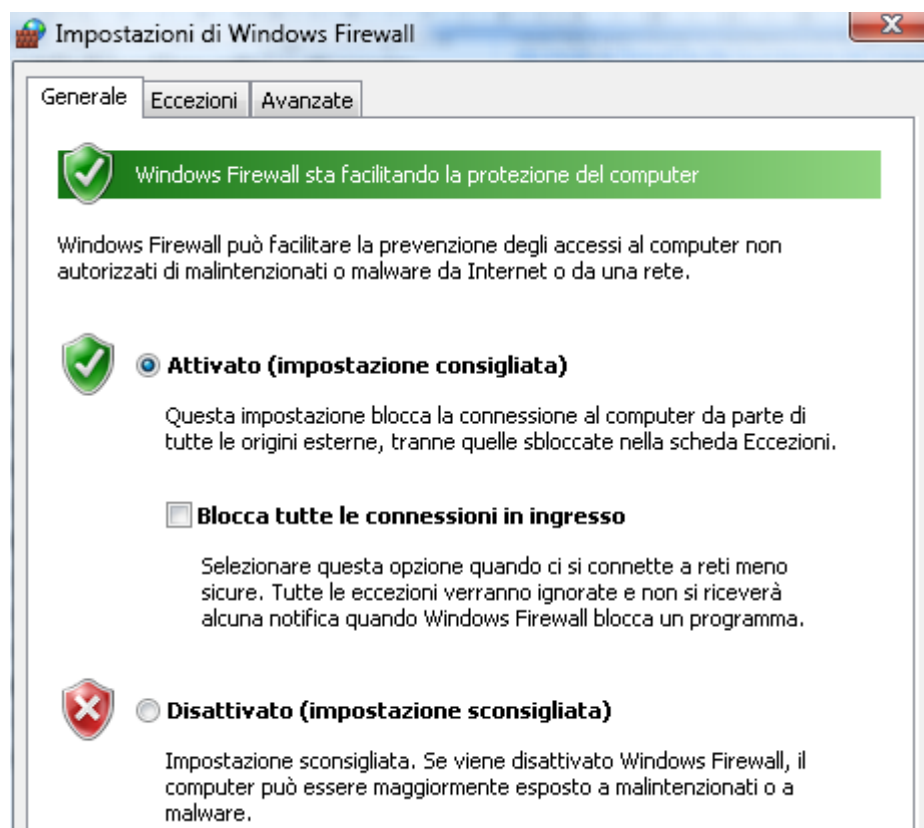
Visualizza notifica per il blocco di un programma: Sì

Percorso di rete: Rete privata

[Che cosa sono i percorsi di rete](#)

Come si può vedere dalla schermata qui sotto, in una situazione di uso normale è selezionata la prima opzione **Attivato (impostazione consigliata)**. Conviene lasciare selezionata questa opzione, poiché la seconda **Blocca tutte le connessioni in ingresso**, è molto restrittiva e potrebbe impedire il corretto funzionamento ad alcuni programmi che usano Internet o la rete locale.

Sconsigliamo assolutamente di disattivarlo usando la terza opzione **Disattivato (impostazione sconsigliata)** a meno che sul computer non si sia installato un'altro firewall software più evoluto.

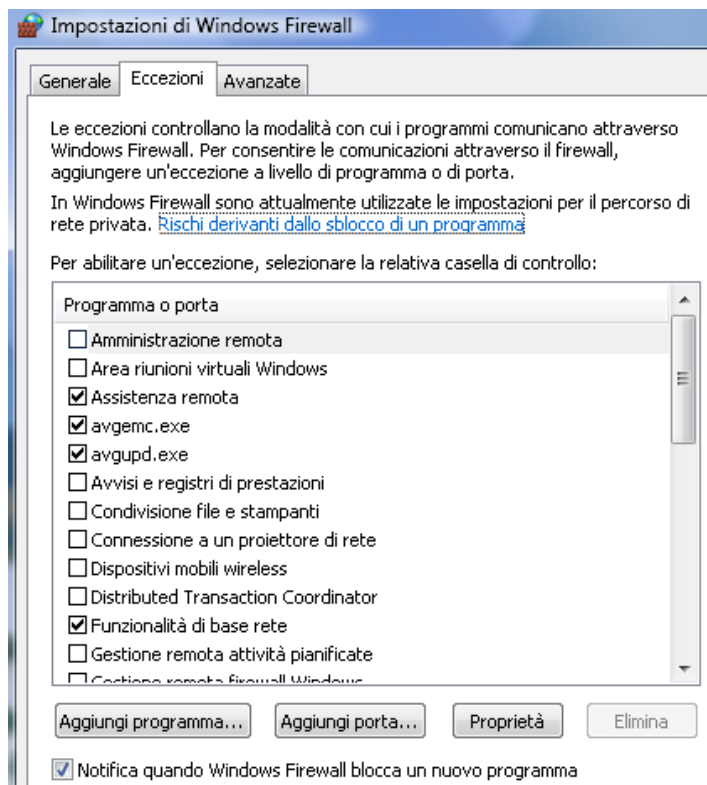


Creare un'eccezione in Windows Firewall

Nel caso si utilizzi un programma che per funzionare correttamente ha bisogno di accedere ad Internet (es. i programmi P2P di file sharing come e-mule o come i software per il controllo remoto in rete) è necessario configurare **Windows Firewall** in modo che lasci passare senza impedimenti questo programma.

Nella scheda **Eccezioni** è possibile aggiungere i programmi e i servizi che vogliamo abilitare per non essere bloccati da **Windows Firewall**. Fare clic sul pulsante **Aggiungi Programma**: compare una finestra in cui vengono visualizzati alcuni dei programmi installati sul computer.

Se il programma desiderato è presente in questo elenco, è sufficiente farvi un doppio clic sopra per inserirlo nella lista dei software che hanno pieno accesso a Internet. Se il programma non figura nell'elenco -> clic sul pulsante **Sfoglia** -> navigare nelle cartelle fino a trovare il software desiderato -> clic sul nome del programma -> clic sul pulsante **Apri** -> clic sul pulsante **OK**



Bloccare o sbloccare un programma

Quando **Windows Firewall** blocca un programma che richiede la ricezione di connessioni da Internet o dalla rete LAN aziendale, il sistema visualizzerà la schermata riportata qui sotto.

Se si vuole che il programma in questione acceda completamente ad Internet fare clic sul pulsante **Sblocca**, altrimenti fare clic sul pulsante **Continua a bloccare**

