

Reti e risorse Web

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*.



Pannello di cont	trollo ► Sistema e sicurezza ► Windows Firewall	✓ 44 Cerca nel Pannello di controllo
Pagina iniziale Pannello di controllo Consenti programma o funzionalità con Windows Firewall Image: Straight of the straigh	Protezione del computer con Window Windows Firewall può facilitare la prevenzione de malware da Internet o da una rete. Informazioni sulle funzionalità del firewall per la p Informazioni sui tipi di percorsi di rete Reti domestiche o aziendali (p Reti domestiche o aziendali (p rete	e si considerano attendibili gli utenti e i dispositivi nella
Impostazioni avanzate Risoluzione dei problemi di rete	Stato Windows Firewall: Connessioni in ingresso: Reti domestiche o aziendali (private) attive: Stato notifica:	Attivato Blocca tutte le connessioni a programmi non inclusi nell'elenco dei programmi consentiti M Voda Notifica quando Windows Firewall blocca un nuovo
Vedere anche Centro operativo Centro connessioni di rete e condivisione	Reti pubbliche	programma Non connesso 📎

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.



LORENZI, GIUPPONI SCIENZE E TECNOLOGIE APPLICATE - INFORMATICA - © ATLAS



PARTE

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.

Windows Firewall con sicurezza avanzata		
File Azione Visualizza ?		
🔗 Windows Firewall con sicurezza avanzata	Windows Firewall con sicurezza avanzata in Computer locale	Azioni
 Regole connessioni in entrata Regole connessioni in uscita Regole di sicurezza delle connessioni Monitoraggio 	Windows Firewall con sicurezza avanzata offre funzionalità di sicurezza di rete per i computer Windows.	Windows Firewall con sicurezza avanzata in Windows Firewall con sicurezza avanzata in Second criteri
	Anteprima	Ripristina criterio predefinito
	Profilo di dominio	Esegui diagnosi / Ripristina
	Windows Firewall attivo.	Visualizza
	S Le connessioni in entrata che non corrispondono a una regola sono bloccate.	G Aggiorna
	Le connessioni in uscita che non corrispondono a una regola sono consentite.	Proprietà
	Profilo privato attivo Windows Firewall attivo. Le connessioni in entrata che non contispondono a una regola sono bloccate. Le connessioni in uscita che non contispondono a una regola sono bloccate. Windows Firewall attivo. Windows Firewall attivo. Windows Firewall attivo. Windows Firewall attivo. Le connessioni in entrata che non contispondono a una regola sono bloccate. Windows Firewall Proprietà Windows Firewall Attività iniziali Attenticare le comunicazioni tra computer Creare regole di sicurezza delle connessioni per specificare come e quando le connessioni tra computer vengono auteriticate e protette mediante l'Pece (Internet Protocol Security). Regole di sicurezza delle connessioni e connessioni a porte o programmi specifici. È inoltre possibile consertine una connessione solo se auteriticato se proventente da un uterte, un gruppo o un computer autorizato. Primpostazione predefinita, le connessioni in entrata vengono bloccate a meno che non esista una regola componderie che le connessioni in entrata vengono bloccate a meno che non esista una regola componderie che le connessioni in uscita vengono bloccate a meno che non siano bloccate da una regola.	Guida
« III)	Regole connessioni in entrata Regole connessioni in uscita Visualizzare criteri e attività l'Psec e del firewall correnti Visualizzare informazioni sulle regole di sicurezza delle connessioni e del firewall applicate, nonché sulle associazioni di sicurezza per le connessioni di rete attive. Montoraggio	

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".

Tipo di regola Selezionare il tipo di regola del firew	rall da creare.	
Passaggi: Tipo di regola Programma Operazione Profilo Nome	Selezionare il tipo di regola che si desidera creare. Programma Regola che controlla le connessioni per un programma. Prodefinita: Assistenza remota Regola che controlla le connessioni per una funzione di Windows. Personalizzata Regola personalizzata. Utteriori informazioni sui tipi di regole	

LORENZI, GIUPPONI SCIENZE E TECNOLOGIE APPLICATE - INFORMATICA - © ATLAS

Reti e risorse Web

PARTE

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.

Creazione guidata nuova regola connessioni in entrata Operazione Specificare l'operazione da eseguire quando una connessione corrisponde alle condizioni specificate nella regola.		
	< Indietro Avanti > Annulla	

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.