

# Suggerimenti per l'installazione di Cisco QuickVPN per i sistemi operativi Windows

Per un video che mostra i suggerimenti per l'installazione su Quick VPN, visitare il sito <http://youtu.be/hHu2z6A78N8>

## Obiettivo

Cisco QuickVPN è un software gratuito progettato per l'accesso remoto a una rete. È facile da installare su un PC e da gestire. QuickVPN è compatibile con il sistema operativo Windows (versioni a 32 bit e a 64 bit). Affinché QuickVPN funzioni correttamente, è necessario verificare una serie di requisiti per garantire la connettività VPN con la rete.

Questo articolo spiega i requisiti e i suggerimenti per la corretta esecuzione di QuickVPN, nonché una spiegazione di come QuickVPN ottiene l'accesso alla rete.

## Dispositivi interessati

RV215W  
RV110W  
· RV180 / RV180W  
RV120W  
RV220W  
· RV016  
RV042/RV042G  
RV082  
· RVS4000  
· SA520/SA520W  
SA540  
WRV200  
WRV210  
WRVS4400N  
· Windows XP, Windows Vista, Windows 7

## Processo QuickVPN

Di seguito è riportata una spiegazione del funzionamento di QuickVPN nel computer e dei

motivi per cui è importante soddisfare i requisiti prima di eseguire QuickVPN.

1. Il client si connette al router utilizzando SSL (Secure Sockets Layer). La connessione utilizza il numero di porta 443 o 60443 (a seconda della configurazione VPN sul router) e cerca un certificato. Per ulteriori informazioni, fare riferimento alla sezione [Requisiti del router](#).

Nota: se si utilizza un certificato, verificare che sia stato salvato nel computer. In caso contrario, fare clic su No per non utilizzare un certificato quando viene visualizzato il messaggio di avviso del certificato.

2. Il nome utente e la password del client vengono autenticati dal router. Una volta autenticato l'utente, viene stabilito il tunnel IPsec.

Nota: se non è possibile accedere alla VPN, verrà visualizzato un messaggio di errore.

3. Il client invia un pacchetto di richiesta echo ICMP all'indirizzo IP interno del router. Il router risponde con un pacchetto di risposta echo ICMP. Lo scopo è quello di stabilire una connettività tra entrambe le estremità. Per questo motivo, è necessario accertarsi (a seconda del sistema operativo in uso) di impostare i requisiti appropriati per ICMP. Per ulteriori informazioni, fare riferimento alla sezione [Requisiti del sistema operativo Windows Vista/Windows 7](#).

Nota: se la connessione non riesce, viene visualizzato un messaggio di errore Gateway remoto che non risponde.

## Requisiti del router

Di seguito è riportato un elenco di requisiti che il router per piccole imprese deve soddisfare.

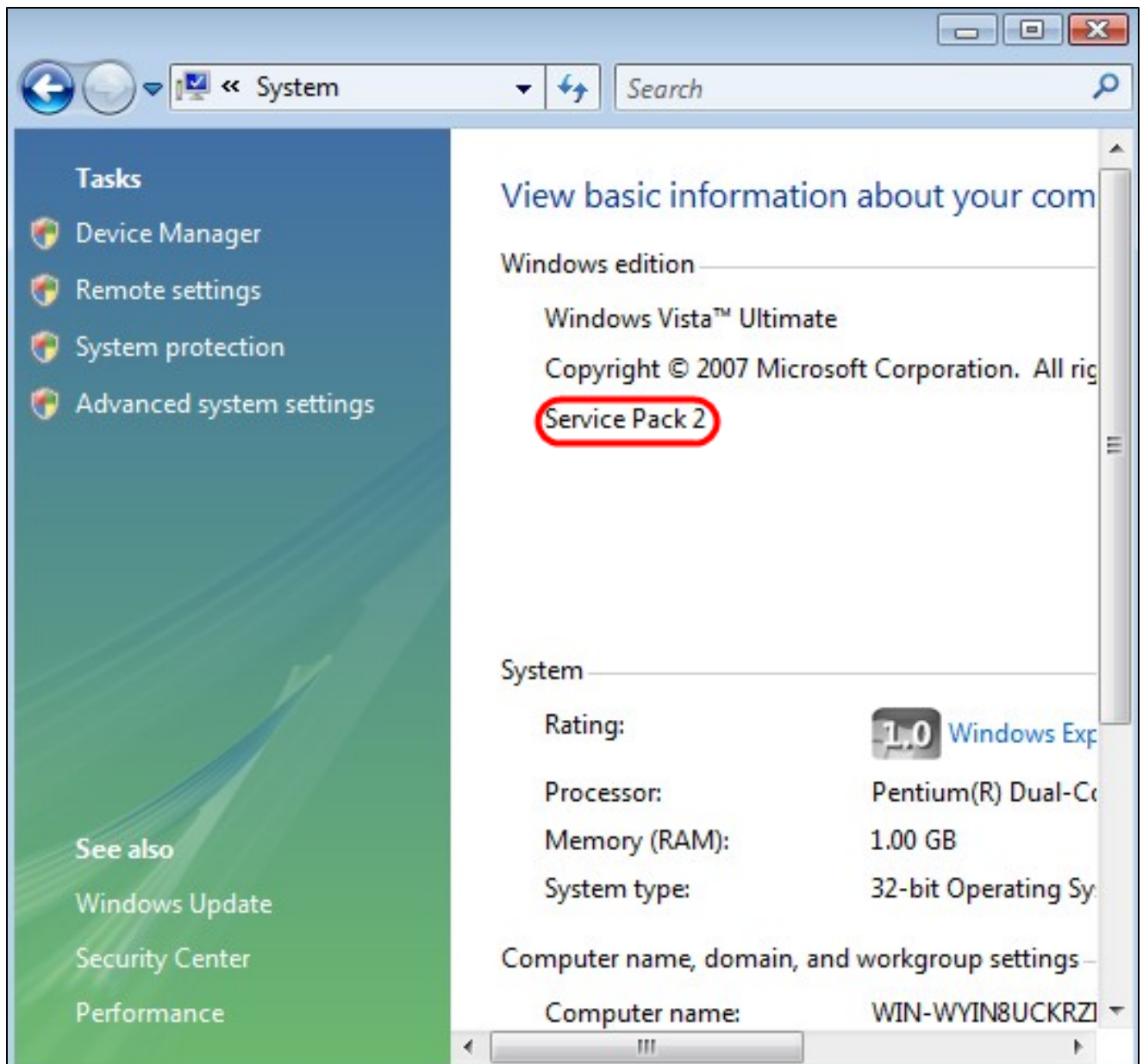
- La gestione remota deve essere abilitata per le porte 443 e 60443.
- Gli utenti devono creare e abilitare il tunnel VPN.
- Il nome utente e la password fanno distinzione tra maiuscole e minuscole e devono corrispondere in entrambe le estremità della connessione.
- È consentita una sola connessione per account utente.

- La subnet della rete locale deve essere diversa dalla subnet della rete remota.
- Se si utilizza un certificato, il file del certificato deve essere salvato nel computer nella cartella QuickVPN Client.

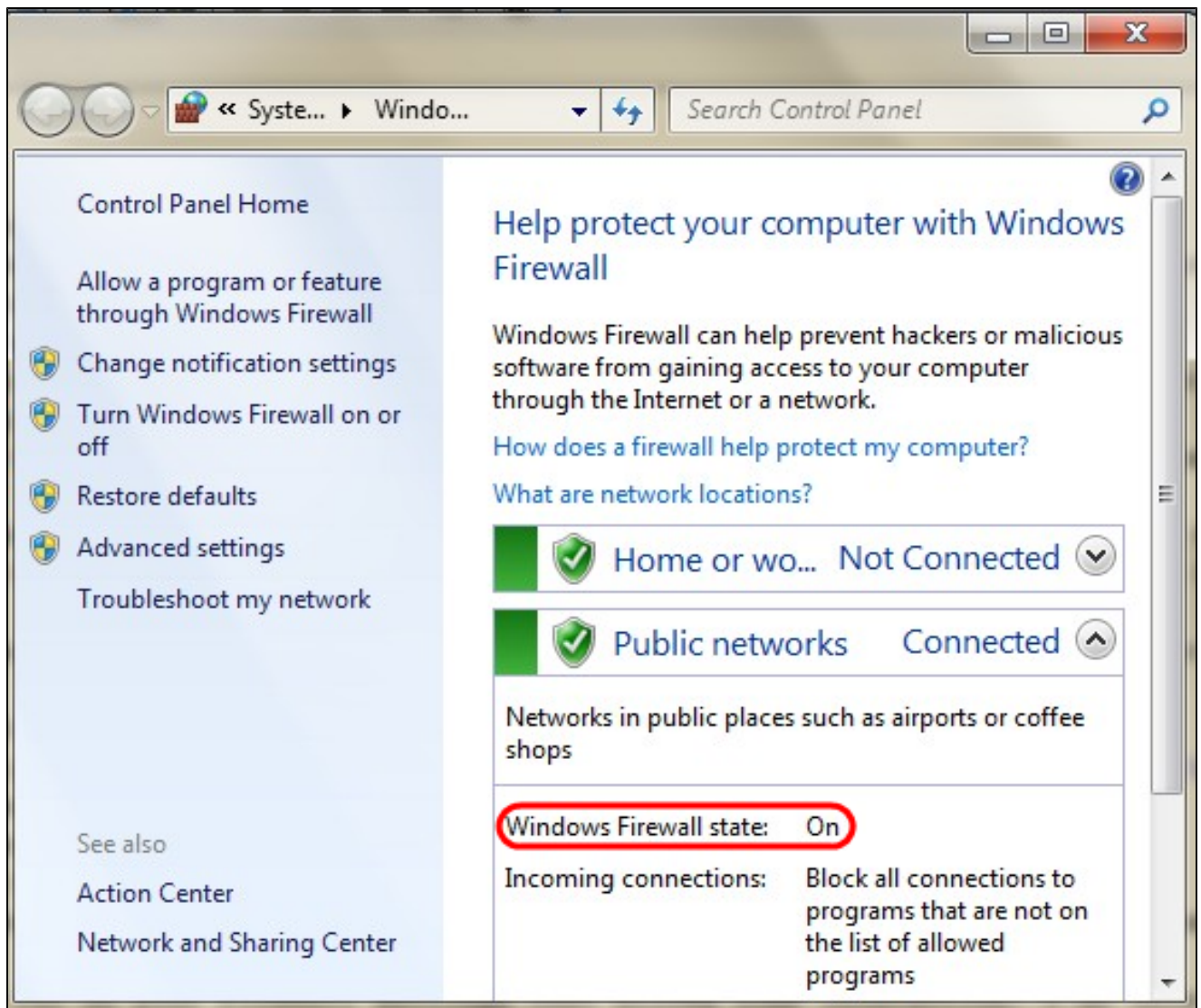
## Requisiti del sistema operativo Windows Vista / Windows 7

Passaggio 1. Se nel computer è installato Windows Vista, è necessario disporre della compatibilità con Service Pack 2 o Vista Service Pack 2 per Windows 7. Per verificare questa condizione, scegliere Start > Proprietà del computer. Se nel computer è installato Windows 7, ignorare questo passaggio.

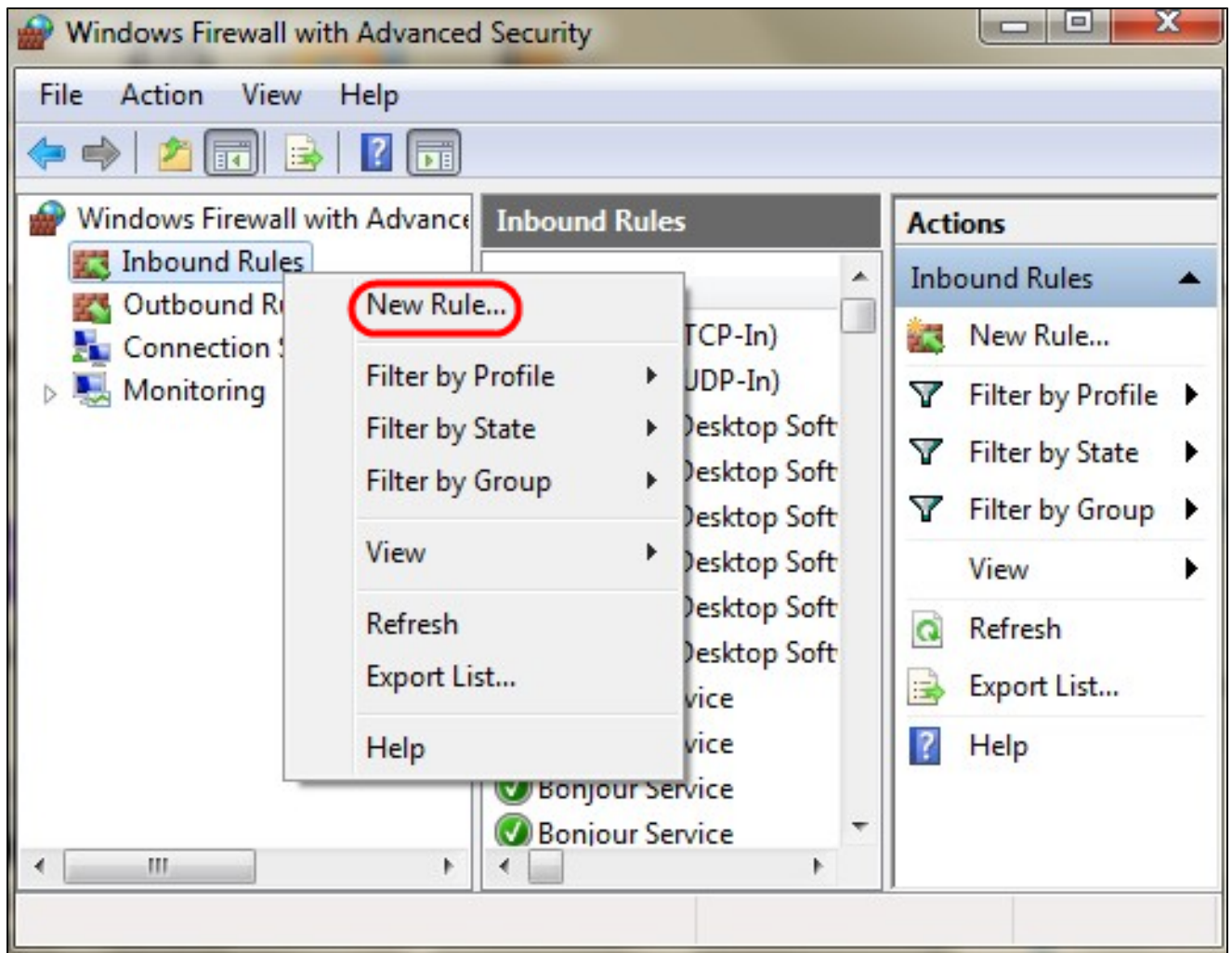
Nota: se in Windows Vista non è installato il Service Pack, scegliere Start > Tutti i programmi > Windows Update per aggiornare il sistema.



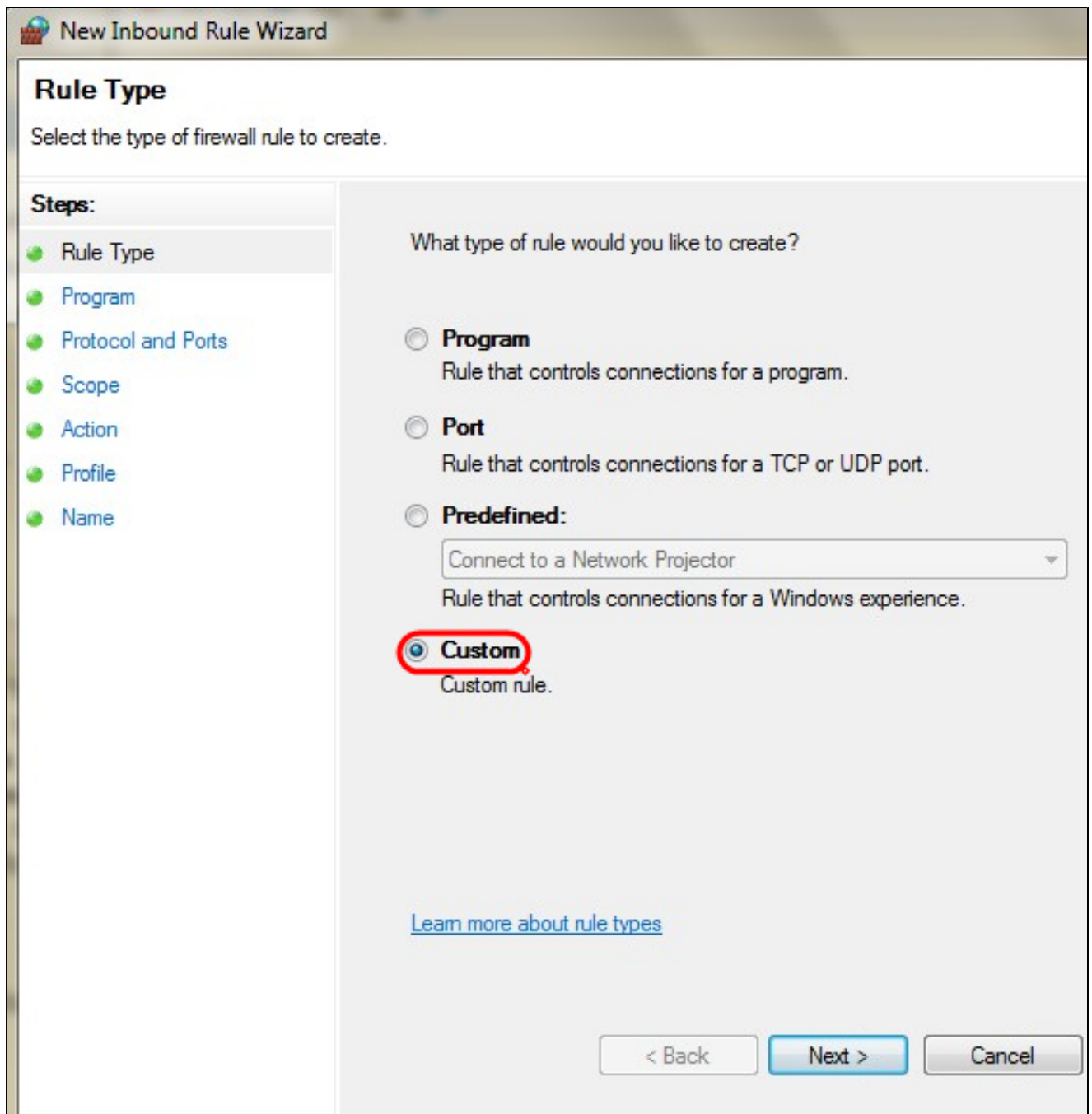
Passaggio 2. Windows Firewall deve essere attivato. Per verificare questa condizione, scegliere Start > Pannello di controllo > Sistema e sicurezza > Windows Firewall.



Passaggio 3. È necessario creare una regola per consentire le trasmissioni di pacchetti ICMP (Internet Control Message Protocol). A tale scopo, scegliere Start > Pannello di controllo > Sistema e sicurezza > Windows Firewall > Impostazioni avanzate. Verrà visualizzata la finestra Windows Firewall con protezione avanzata:

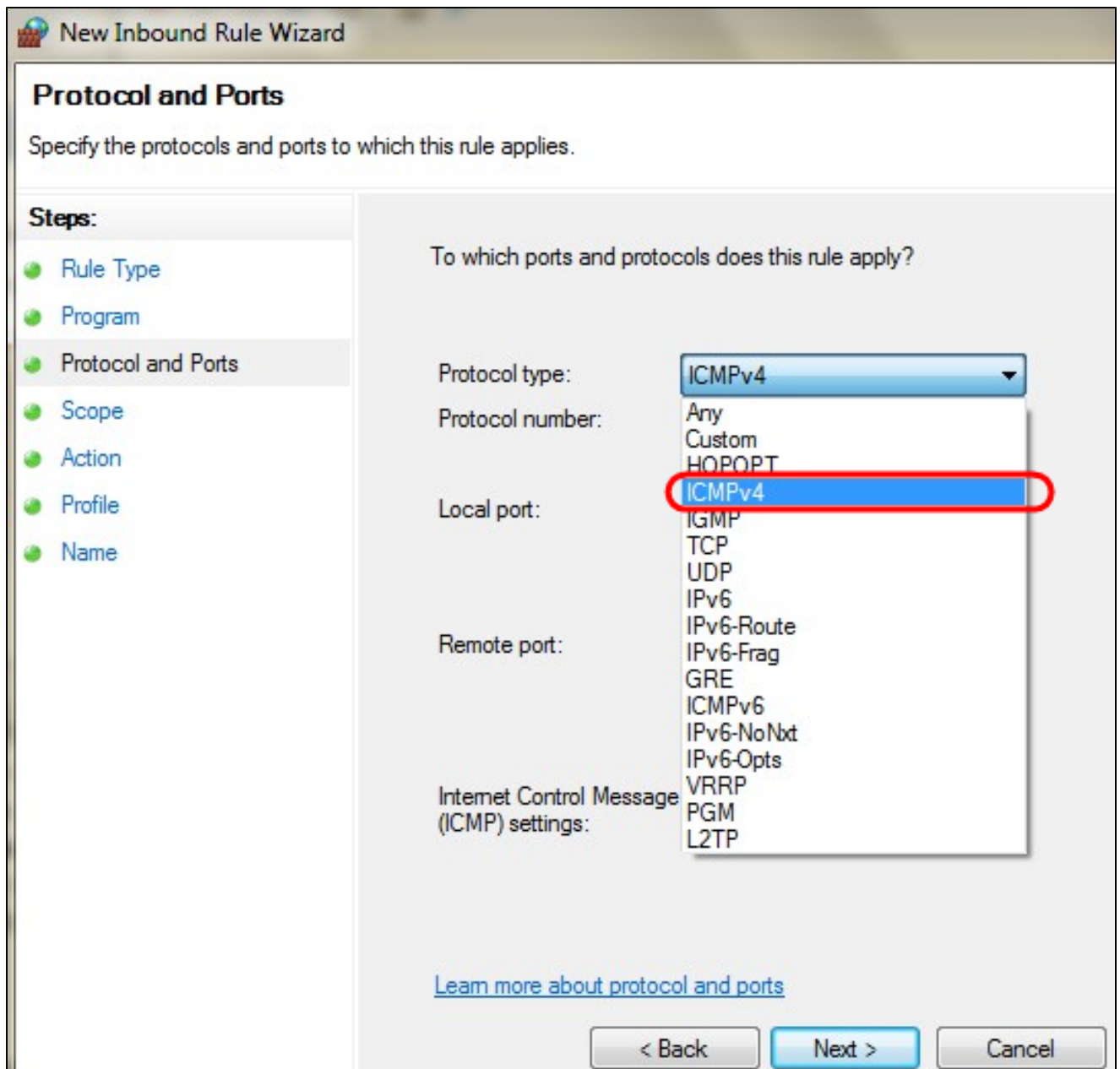


Passaggio 4. Fare clic con il pulsante destro del mouse su Regole in entrata e scegliere Nuova regola. Verrà visualizzata la pagina Creazione guidata nuova regola connessioni in entrata:



Passaggio 5. Fare clic su Personalizzato per creare una regola personalizzata.





Passaggio 6. Nell'elenco a discesa Protocol Type (Tipo di protocollo), selezionare ICMPv4.

Nota: gli altri campi possono rimanere nella configurazione predefinita.



**New Inbound Rule Wizard**

**Name**

Specify the name and description of this rule.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Name:  
ICMP Echo Request

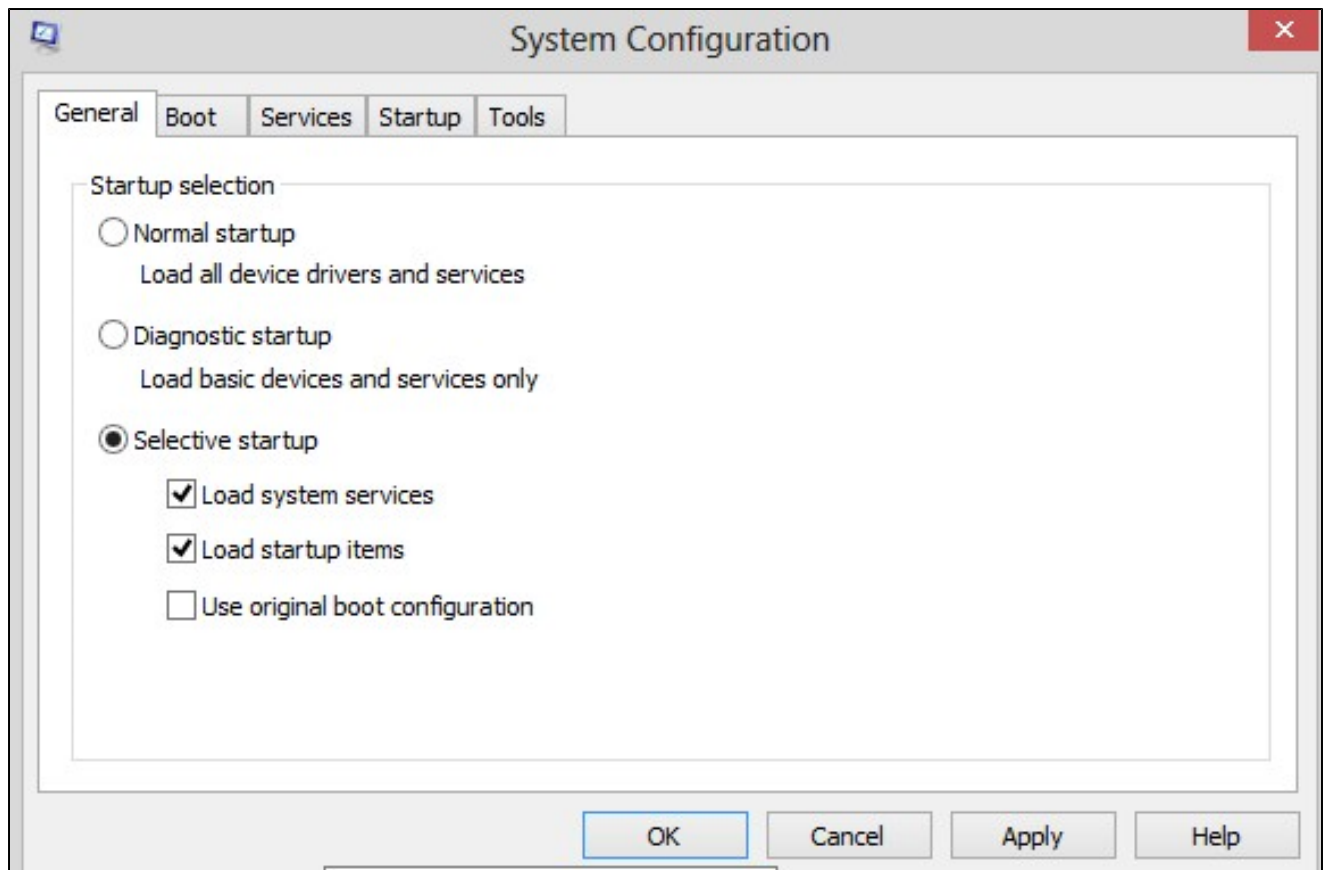
Description (optional):

< Back   Finish   Cancel

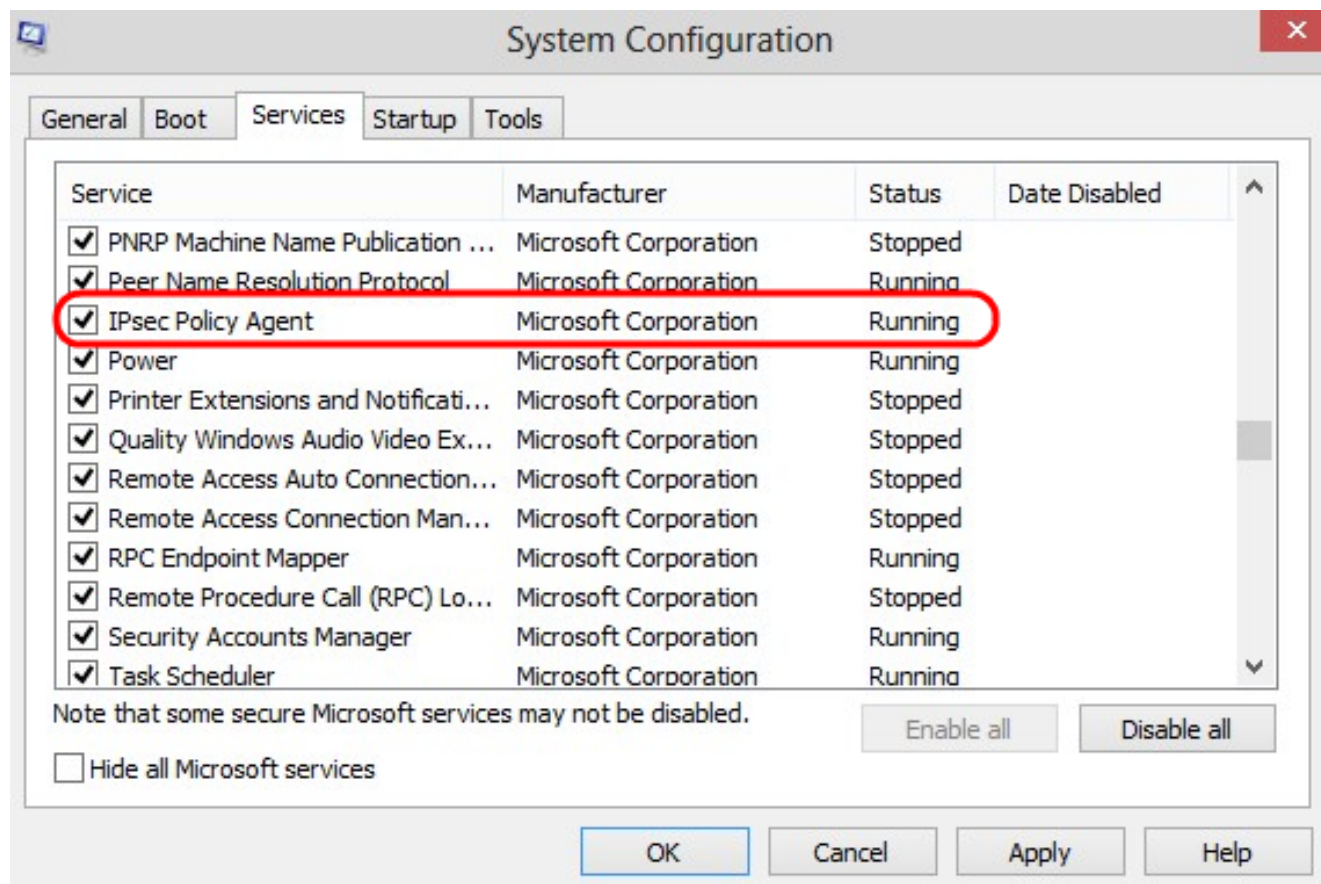
Passaggio 7. Nel campo Nome immettere un nome che descriva questa regola.

Passaggio 8. Fare clic su Finish (Fine).

Passaggio 9. Il servizio IPsec deve essere in esecuzione. Per verificare questa condizione, fare clic su Start e nel campo Cerca programmi e file, immettere msconfig. Viene visualizzata la finestra Configurazione di sistema:



Passaggio 10. Fare clic sulla scheda Servizi per verificare che l'Agente criteri IPsec sia abilitato. Se non è attivato, selezionare la casella di controllo Agente criteri IPsec per consentire il servizio IPsec.



Passaggio 11. Fare clic su Apply (Applica) per salvare le impostazioni.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).