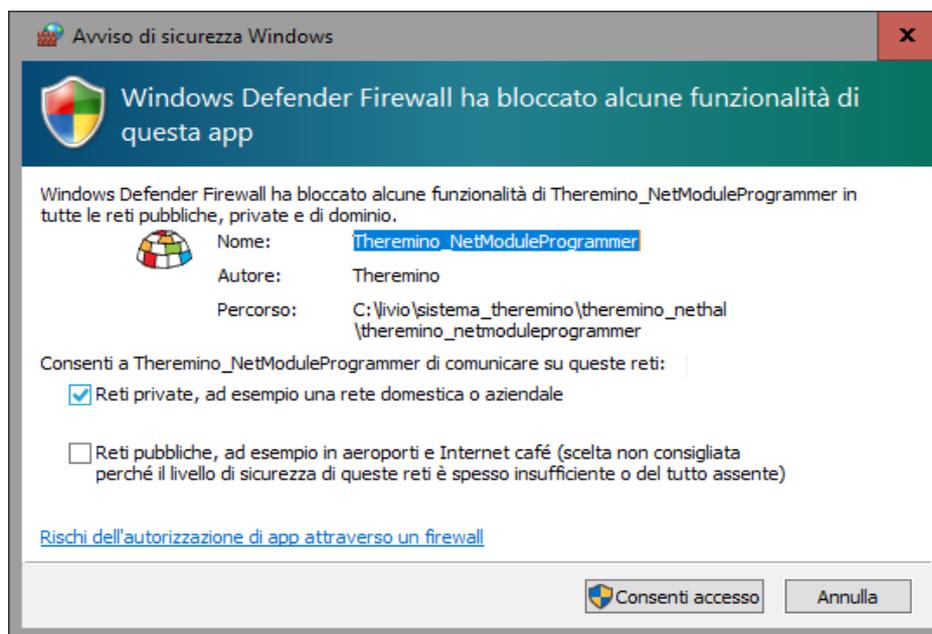


Theremino System

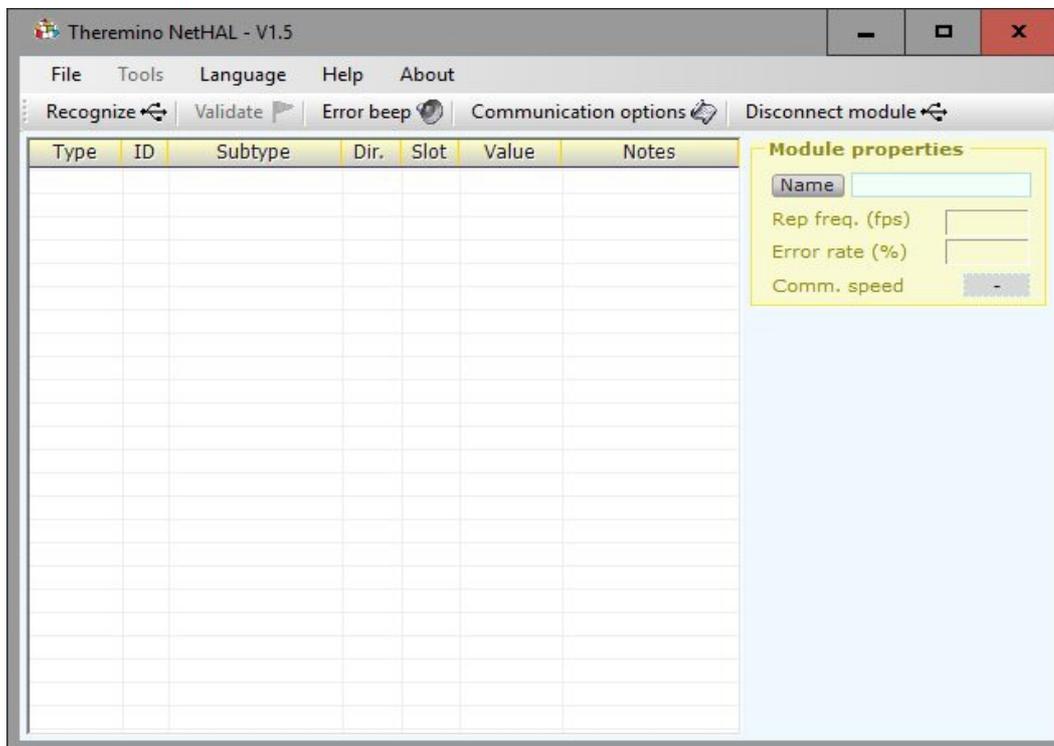


Theremino NetModule

Firewall Problems

Firewall problems

It may happen that NetHAL not be able to communicate with NetModules. In these cases the module list remains empty, as seen in this image.



In these cases, the first advice is:

- ◆ Check that the NetModule are powered, optionally reset them and see if their LED flashes normally and then turns off.
- ◆ If necessary, connect the USB NetModule and see what is sent to the app. Theremino Terminal when you press the Reset (if something is sent).
- ◆ Press the Communication Options button in the NetHAL and control at the end of the file that: "LanIpList All", "LanPort 49152" and "Names All".

In case nothing works and the list continues to remain white then it could be a firewall configuration problem.

The simplest method to solve these problems is explained on the next page.

If the module does not appear in the lists

The method of this page is the simplest but also the most rough and drastic (it makes a total reset of the network and the firewall). Experts may therefore prefer to skip it and use the following pages.

Symptoms

1. The module appears in the list of networks, but then does not appear in the lists of NetHal and NetModuleProgrammer
2. The module connects to the WiFi network, but then does not appear in the lists of NetHal and NetModuleProgrammer.

Sometimes the network may be in an abnormal state, some say it is due to the Proxy, or it could be due to misconfiguration of the firewall rules.

We recommend that you perform the following sequence:

- ◆ Click on the Windows Search box (bottom left).
- ◆ Write CMD and wait for it to appear "Command Prompt".
- ◆ Click it with the right mouse button and choose "Run as administrator."
- ◆ Copy the following two commands one by one and give ENTER to all them
netsh int ip reset
netsh winsock reset
- ◆ Try again if the modules appear on NetHAL (starting it, or by pressing "Recognize").
- ◆ If they do not yet appear, try to make a restart
- ◆ If they do not yet appear, try also the following command (that completely reset the firewall and therefore may block some programs).

netsh advfirewall reset

Delete firewall rules and recreate them

- ◆ Open the Control Panel
- ◆ Choose "Windows Defender Firewall"
- ◆ Click "Allow app or feature through Windows Firewall Defender"
- ◆ Scroll down the list until "Theremino"
- ◆ Press the "Change settings"
- ◆ Select "Theremino NetHAL" press "Remove" and then "Yes"
- ◆ Select "Theremino NetModuleProgrammer" press "Remove" and "Yes"

Consenti alle app di comunicare attraverso Windows Defender Firewall

Per aggiungere, modificare o rimuovere le app e le porte consentite, fare clic su Modifica impostazioni.

Rischi derivanti dallo sblocco di un'app per consentire la comunicazione

Modifica impostazioni

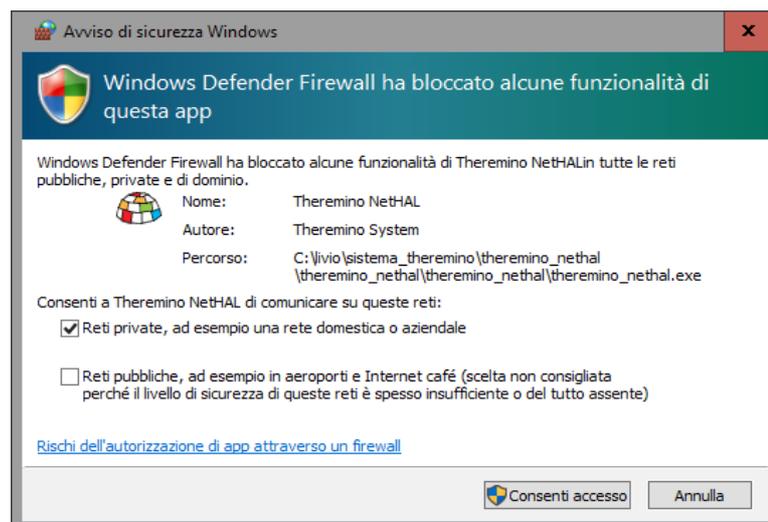
App e funzionalità consentite:

Nome	Privata	Pubblica	
<input checked="" type="checkbox"/> Theremino NetHAL	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Theremino NetModuleProgrammer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Trap SNMP	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Visualizzatore realtà mista	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> vshost32.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Windows Defender Security Center	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Once deleted, the next time the rules NetHAL applications and NetModuleProgrammer Firewall should ask permission again.

When you launch the applications you should give permission for private networks, but then the applications might not see the modules if by chance the first connection of the Access Point network had not chosen "YES".

Enabling "Private Networks", "Public Networks" and "Domain Networks" (if any), then press the "Allow Access button."



Eliminate networks and reopen

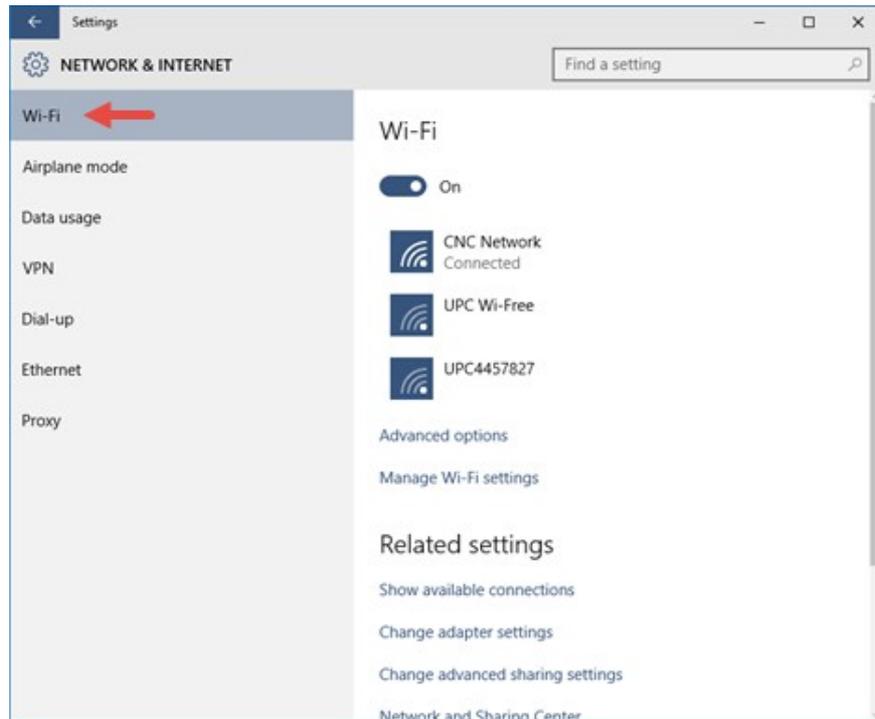
Eliminate Known Networks

To open:

- *Start*
- *Settings*
- *Network and Internet*
- *Wifi*

Then, in the list of Wi-Fi networks, click the link "Manage known networks".

Click the network of the access point and press the "Forget" button.

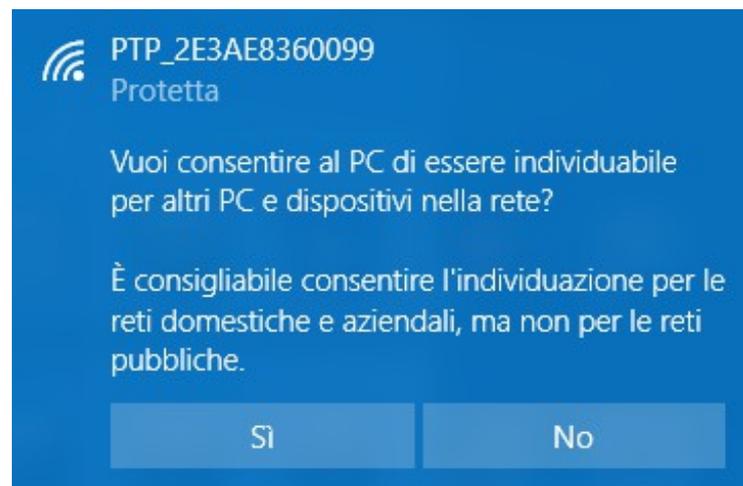
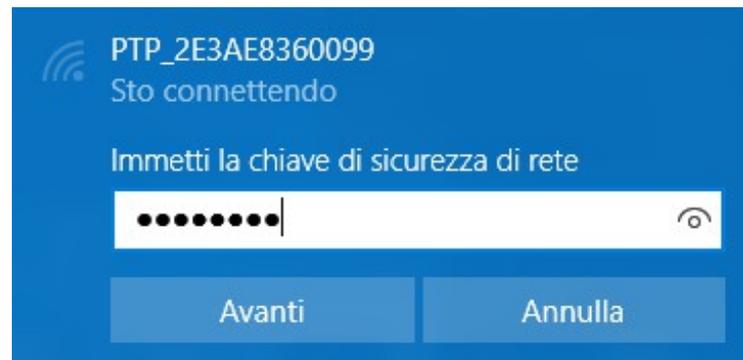


Connect networks

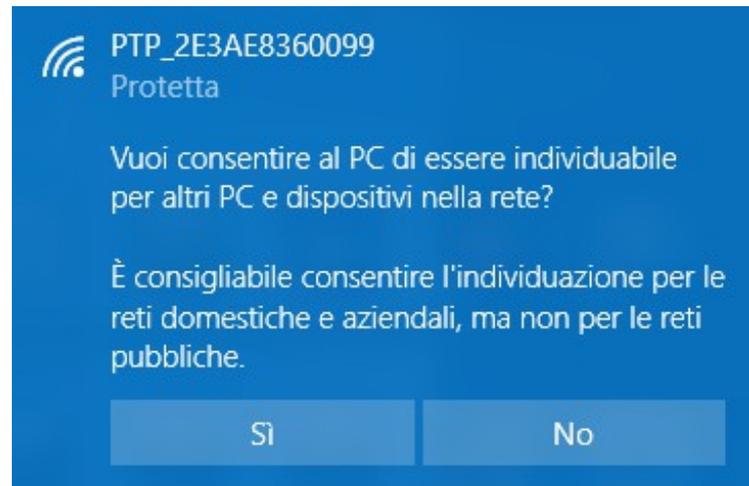
When the list of networks you connect to PTP_xxxxxxxxxxxx you must enter the password, which initially is "password"

This panel is particularly poorly written and confusing. Reading it you might think to get more security by choosing NO, but in reality the NO setting the network within the public, and at the same time freezes the ability to locate it.

So: consent by pressing "YES".



If by chance you are wrong to give No in this panel, the network has become public and the applications will not connect to NetModule.



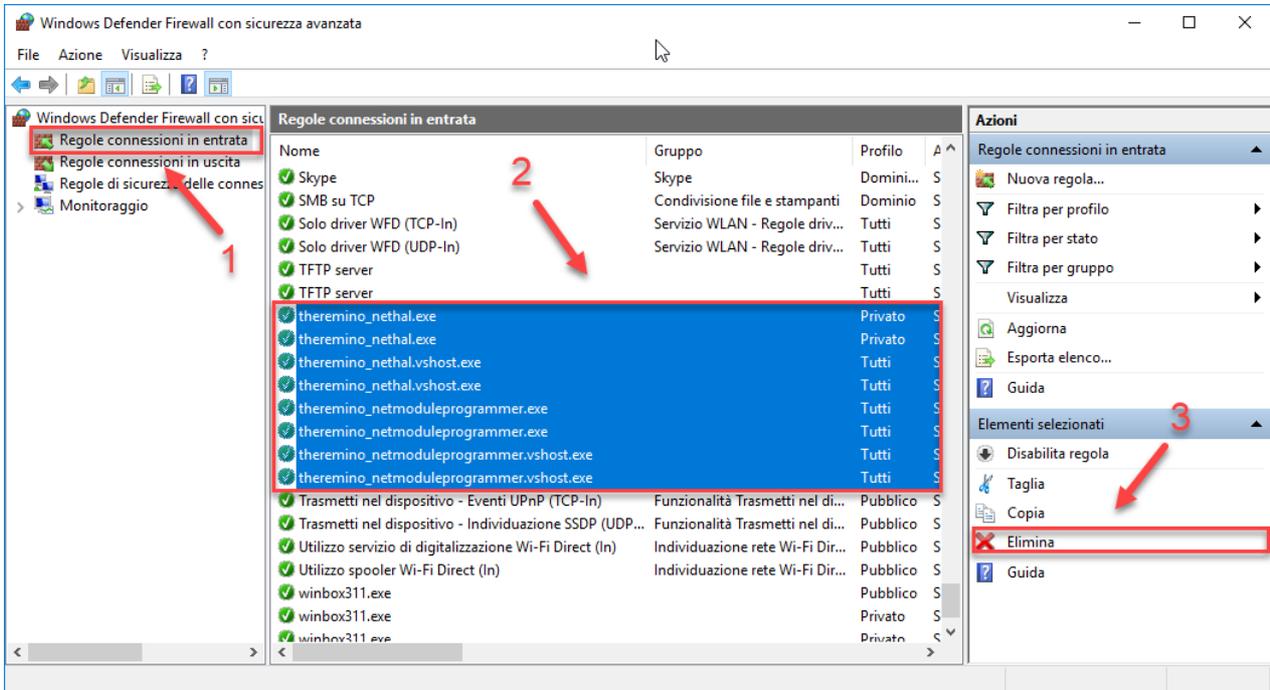
In order to make the private network:

- Click the symbol of the networks in the TaskBar
- Click the Network of the AccessPoint
- Click the word Properties
- It opens a page of options
- Put in "On" under "Make this PC discoverable"

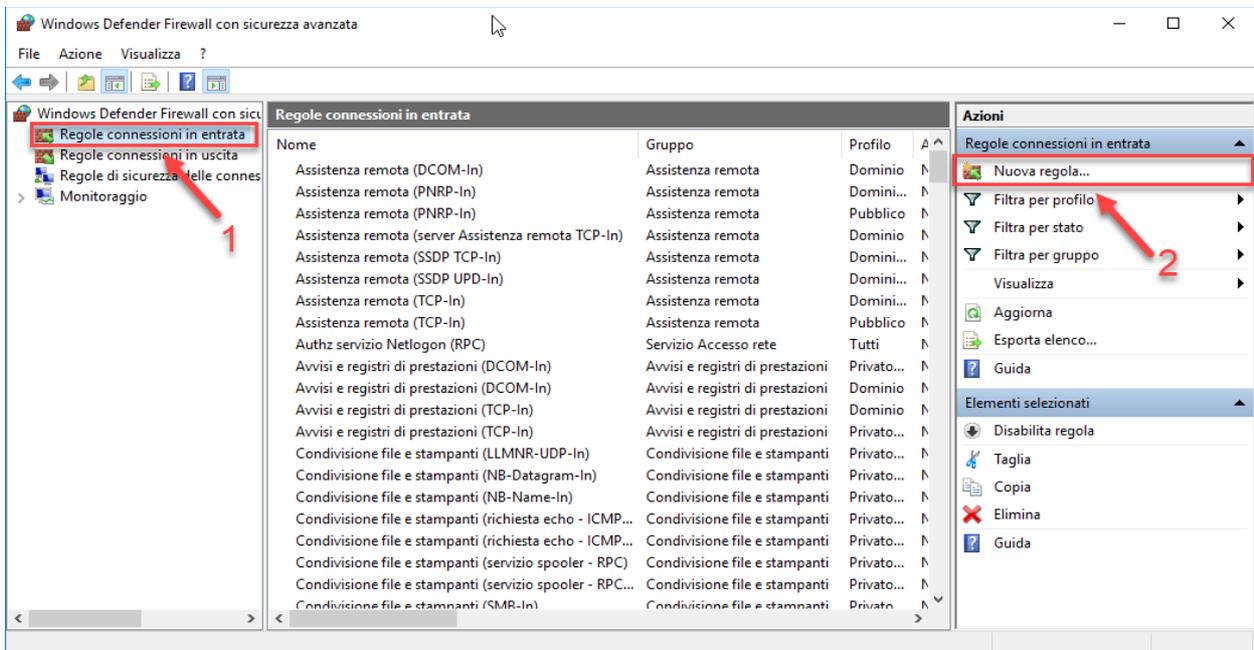
Manual adjustment of the rules

(These are complex operations, preferably use the previous pages)

1) Clean the rules that have been added automatically by the system



2) Add a rule



This applies wherever the executables are placed "NetHAL.exe" and "NetModuleProgrammer.exe".

3) Follow the Wizard, inputting these data, add UDP port 49152

Wizard (3a) - Rule Type

Creazione guidata nuova regola connessioni in entrata

Tipo di regola
Selezionare il tipo di regola del firewall da creare.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome

Selezionare il tipo di regola che si desidera creare.

Programma
Regola che controlla le connessioni per un programma.

Porta
Regola che controlla le connessioni per una porta TCP o UDP.

Predefinita:
Arresto remoto
Regola che controlla le connessioni per una funzione di Windows.

Personalizzata
Regola personalizzata.

< Indietro Avanti > Annulla

Wizard (3b) - Protocol and Ports

Creazione guidata nuova regola connessioni in entrata

Protocollo e porte
Specificare i protocolli e le porte a cui applicare la regola.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome

Selezionare se applicare la regola al protocollo TCP o UDP.

TCP

UDP

Selezionare se applicare la regola a tutte le porte locali o a porte locali specifiche.

Tutte le porte locali

Porte locali specifiche: 49152
Esempio: 80, 443, 5000-5010

< Indietro Avanti > Annulla

Wizard (3c) - Operation

Creazione guidata nuova regola connessioni in entrata

Operazione

Specificare l'operazione da eseguire quando una connessione corrisponde alle condizioni specificate nella regola.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome

Selezionare l'azione desiderata per le connessioni che soddisfano le condizioni specificate.

- Consenti la connessione**
Include le connessioni protette con IPsec e quelle non protette.
- Consenti solo connessioni protette**
Include solo le connessioni autenticate mediante IPsec. Le connessioni saranno protette con le impostazioni delle regole e proprietà IPsec nel nodo Regole di sicurezza delle connessioni.
- Blocca la connessione**

Personalizza...

< Indietro Avanti > Annulla

Wizard (3d) - Profile:

Creazione guidata nuova regola connessioni in entrata

Profilo

Specificare i profili a cui si applica la regola.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome

Selezionare il tipo di applicazione della regola.

- Dominio**
Regola applicabile ai computer connessi al rispettivo dominio aziendale.
- Privato**
Regola applicabile ai computer connessi a un percorso di rete privato, come una rete domestica o la rete di un ufficio.
- Pubblico**
Regola applicabile ai computer connessi ad un percorso di rete pubblico.

< Indietro Avanti > Annulla

Wizard (3e) - First name

The screenshot shows a wizard window titled "Creazione guidata nuova regola connessioni in entrata" with a close button (X) in the top right corner. The main heading is "Nome" and the instruction is "Specificare il nome e la descrizione della regola." On the left, a "Passaggi:" sidebar lists five steps: "Tipo di regola", "Protocollo e porte", "Operazione", "Profilo", and "Nome", with "Nome" selected. The main area contains a "Nome:" label above a text input field containing "_Theremino-UDP", and a "Descrizione (facoltativa):" label above a larger empty text area. At the bottom right, there are three buttons: "< Indietro", "Fine" (highlighted with a blue border), and "Annulla".

(4) Follow the Wizard, inputting these data, add TCP port 8080

Wizard (4a) - Rule Type:

Creazione guidata nuova regola connessioni in entrata

Tipo di regola
Selezionare il tipo di regola del firewall da creare.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome

Selezionare il tipo di regola che si desidera creare.

Programma
Regola che controlla le connessioni per un programma.

Porta
Regola che controlla le connessioni per una porta TCP o UDP.

Predefinita:
Arresto remoto
Regola che controlla le connessioni per una funzione di Windows.

Personalizzata
Regola personalizzata.

< Indietro Avanti > Annulla

Wizard (4b) - Protocol and Ports:

Creazione guidata nuova regola connessioni in entrata

Protocollo e porte
Specificare i protocolli e le porte a cui applicare la regola.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome

Selezionare se applicare la regola al protocollo TCP o UDP.

TCP
 UDP

Selezionare se applicare la regola a tutte le porte locali o a porte locali specifiche.

Tutte le porte locali
 Porte locali specifiche: 8080
Esempio: 80, 443, 5000-5010

< Indietro Avanti > Annulla

Wizard (4c) - Operation:

Creazione guidata nuova regola connessioni in entrata

Operazione

Specificare l'operazione da eseguire quando una connessione corrisponde alle condizioni specificate nella regola.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome

Selezionare l'azione desiderata per le connessioni che soddisfano le condizioni specificate.

Consenti la connessione
Include le connessioni protette con IPsec e quelle non protette.

Consenti solo connessioni protette
Include solo le connessioni autenticate mediante IPsec. Le connessioni saranno protette con le impostazioni delle regole e proprietà IPsec nel nodo Regole di sicurezza delle connessioni.

Personalizza...

Blocca la connessione

< Indietro Avanti > Annulla

Wizard (4d) - Profile

Creazione guidata nuova regola connessioni in entrata

Profilo

Specificare i profili a cui si applica la regola.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome

Selezionare il tipo di applicazione della regola.

Dominio
Regola applicabile ai computer connessi al rispettivo dominio aziendale.

Privato
Regola applicabile ai computer connessi a un percorso di rete privato, come una rete domestica o la rete di un ufficio.

Pubblico
Regola applicabile ai computer connessi ad un percorso di rete pubblico.

< Indietro Avanti > Annulla

Wizard (4e) - First name

Creazione guidata nuova regola connessioni in entrata

Nome

Specificare il nome e la descrizione della regola.

Passaggi:

- Tipo di regola
- Protocollo e porte
- Operazione
- Profilo
- Nome**

Nome:

Descrizione (facoltativa):

< Indietro Fine Annulla

The two new rules in the rules list

By ordering the list by name, the two additions rules appear first:

