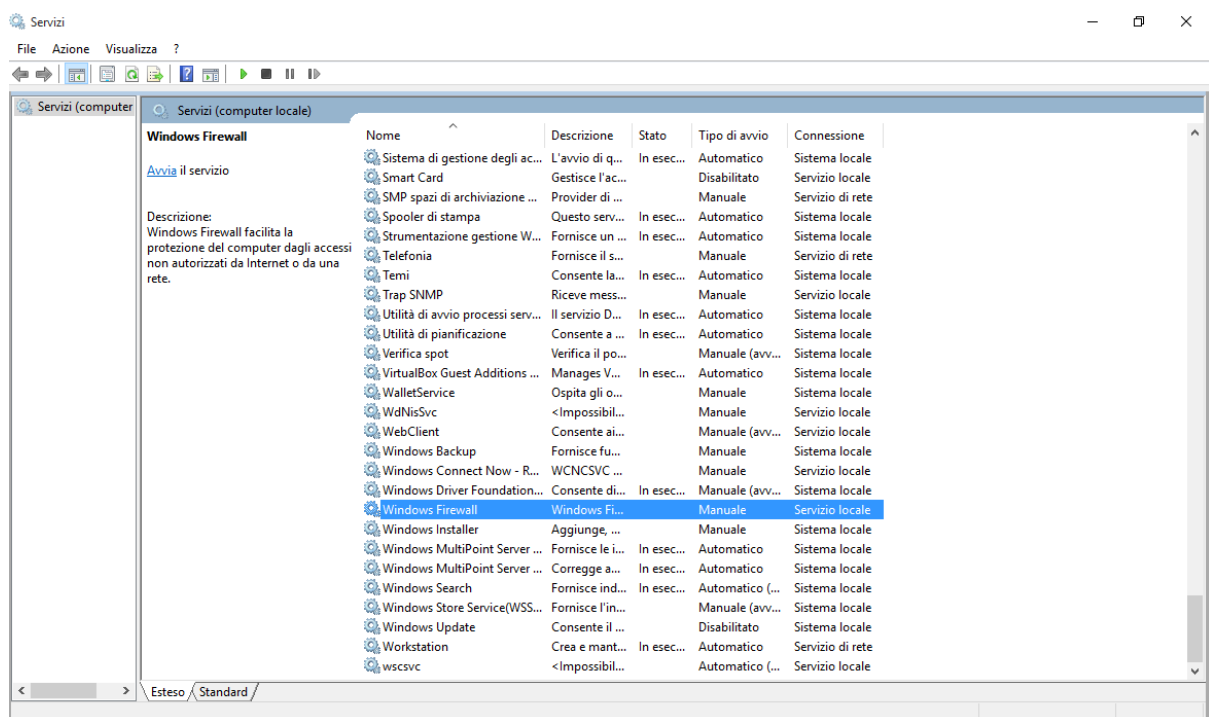


W3D4 - Configurazione di una policy sul firewall windows10

Esercizio: Configurare policy nel Windows Firewall per consentire il ping da macchina Linux a macchina Windows nel nostro laboratorio.
Dato che le macchine del nostro laboratorio sono già comunicanti, ho deciso invece di impostare una policy che bloccasse il ping da Kali a Windows 10.

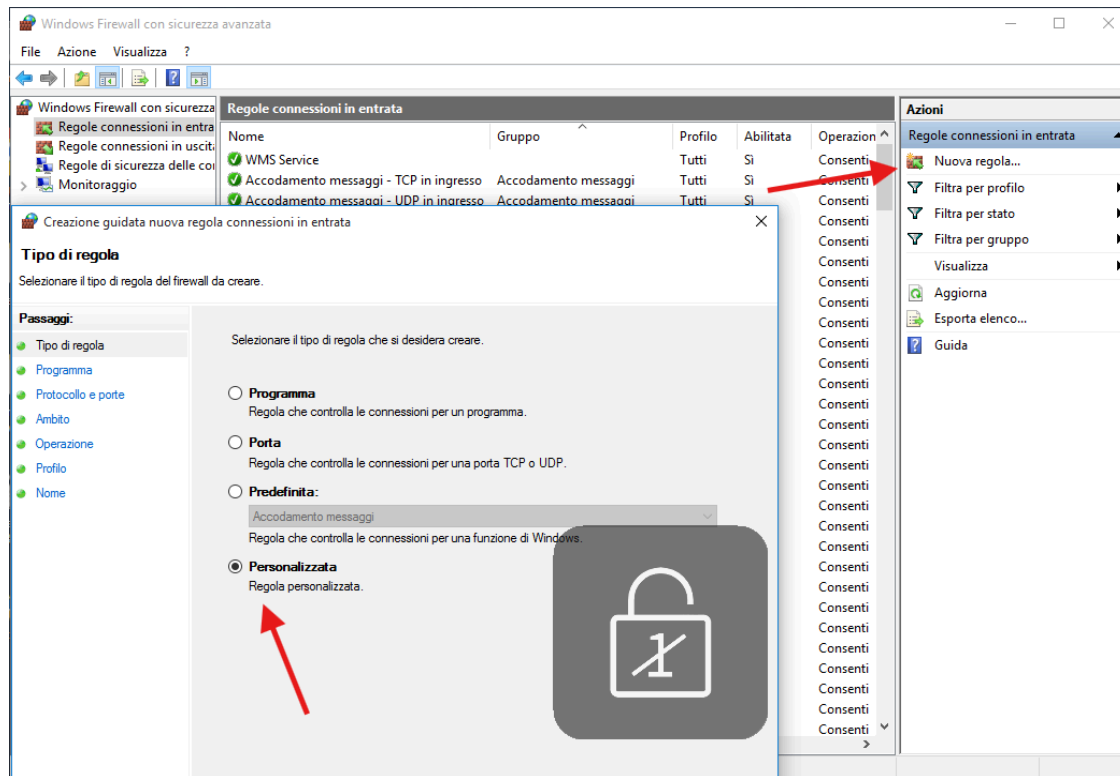
Soluzione:

Accedendo ai servizi ho attivato Windows Firewall con avvio “manuale”.



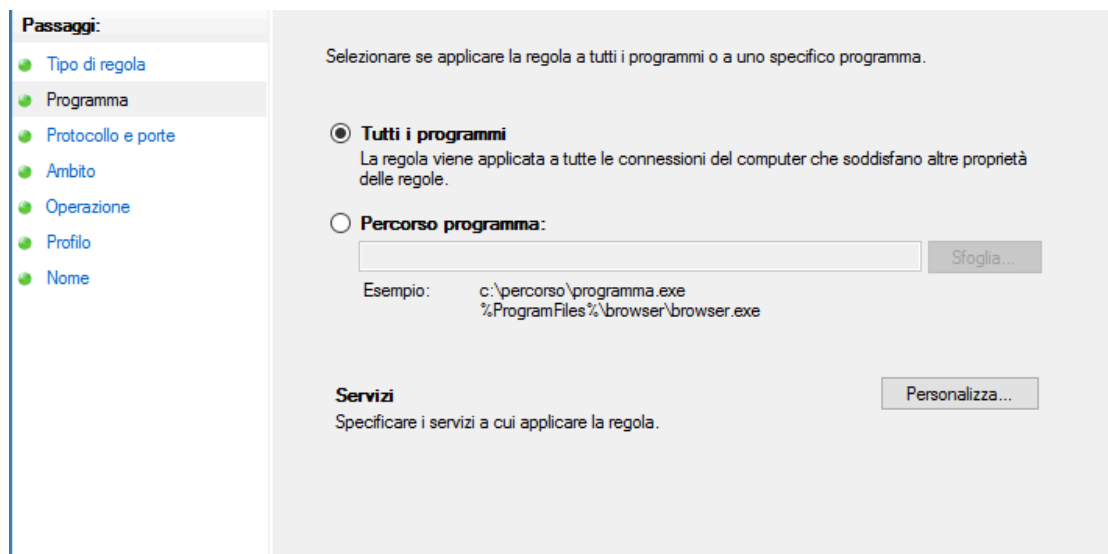
Per la configurazione della policy che blocca il ping proveniente dalla MV Kali (192.168.50.100), ho provveduto alla creazione di una nuova regola di connessione in “entrata”.

Una volta cliccato su “Nuova Regola” (in alto a dx), ho scelto la tipologia “personalizzata”.



In seguito:

- nella sezione Programma, ho scelto “tutti i programmi”.



- nella sezione Protocollo e Porte, ho impostato il protocollo ICMP poiché è il protocollo che si occupa di verificare la raggiungibilità di un host.

The screenshot shows the 'Protocollo e porte' (Protocol and Ports) configuration window. On the left, a sidebar titled 'Passaggi:' (Steps) lists: Tipo di regola, Programma, Protocollo e porte (selected), Ambito, Operazione, Profilo, and Nome. The main area is titled 'Selezionare le porte e i protocolli a cui applicare la regola.' (Select the ports and protocols to which the rule will be applied). It contains the following fields: 'Tipo di protocollo:' (Protocol type) set to 'ICMPv4'; 'Numero protocollo:' (Protocol number) set to '1'; 'Porta locale:' (Local port) set to 'Tutte le porte' (All ports); and 'Porta remota:' (Remote port) also set to 'Tutte le porte'. Below these, an example is given: 'Esempio: 80, 443, 5000-5010'. At the bottom, there is a section for 'Impostazioni ICMP (Internet Control Message Protocol):' with a 'Personalizza...' (Customize...) button.

- nella sezione Ambito è possibile specificare host locali e remoti a cui applicare la regola. Qui avrei potuto impostare l'indirizzo IP sorgente della MV Kali (remoto) ma ho scelto di lasciare l'impostazione predefinita che interessa tutti gli indirizzi, ovvero "qualsiasi indirizzo".

The screenshot shows the 'Ambito' (Scope) configuration window. The sidebar 'Passaggi:' now has 'Ambito' selected. The main area is titled 'Selezionare gli indirizzi IP locali a cui applicare la regola.' (Select the local IP addresses to which the rule will be applied). It has two radio buttons: 'Qualsiasi indirizzo IP' (Any IP address) which is selected, and 'Questi indirizzi IP:' (These IP addresses:). Below the second option is a large empty text box and three buttons: 'Aggiungi...' (Add...), 'Modifica...' (Modify...), and 'Rimuovi' (Remove). Below this is a section 'Personalizzare i tipi di interfaccia a cui applicare la regola:' (Customize the types of interfaces to which the rule will be applied) with a 'Personalizza...' button. The bottom section is titled 'Selezionare gli indirizzi IP remoti a cui applicare la regola.' (Select the remote IP addresses to which the rule will be applied). It also has two radio buttons: 'Qualsiasi indirizzo IP' (Any IP address) which is selected, and 'Questi indirizzi IP:' (These IP addresses:). Below the second option is another large empty text box and three buttons: 'Aggiungi...', 'Modifica...', and 'Rimuovi'.

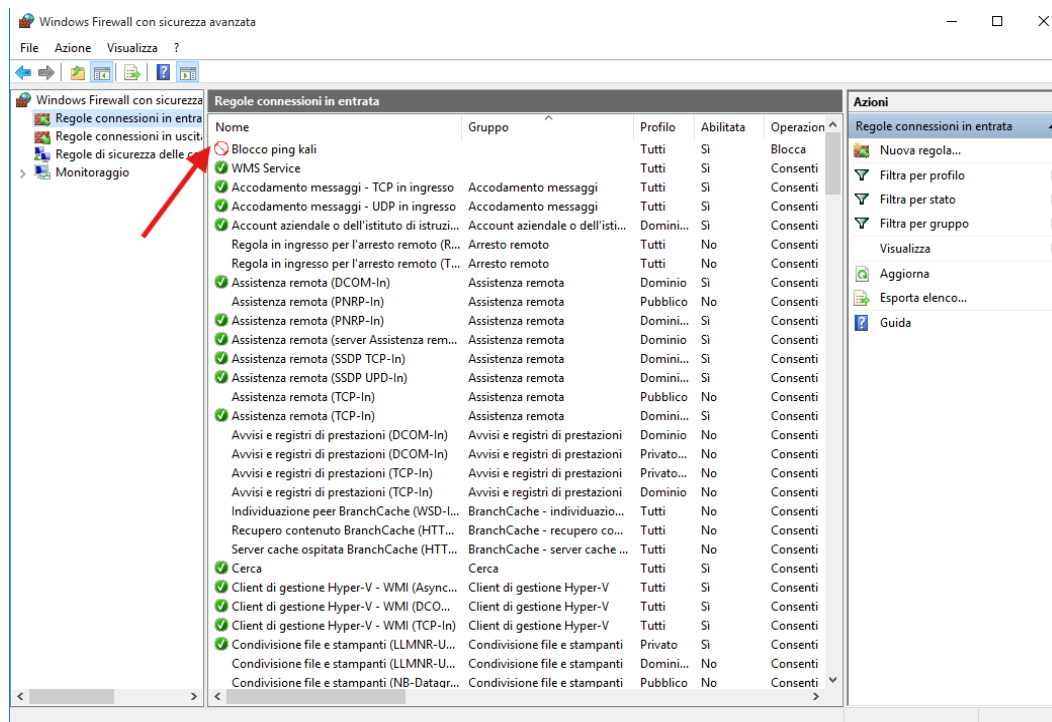
- nella sezione Operazione, dovendo bloccare il ping, ho impostato “Blocca connessione”.

The screenshot shows the 'Operation' tab of a Windows Firewall rule configuration. On the left, a sidebar titled 'Passaggi:' (Steps) lists: Tipo di regola, Programma, Protocollo e porte, Ambito, Operazione (highlighted), Profilo, and Nome. The main area contains the instruction: 'Selezionare l'azione desiderata per le connessioni che soddisfano le condizioni specificate.' (Select the desired action for connections that meet the specified conditions). There are three radio button options: 1. 'Consenti la connessione' (Allow the connection) with the description 'Include le connessioni protette con IPsec e quelle non protette.' 2. 'Consenti solo connessioni protette' (Allow only protected connections) with the description '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.' 3. 'Blocca la connessione' (Block the connection), which is selected with a filled radio button. A 'Personalizza...' (Customize...) button is located between the second and third options.

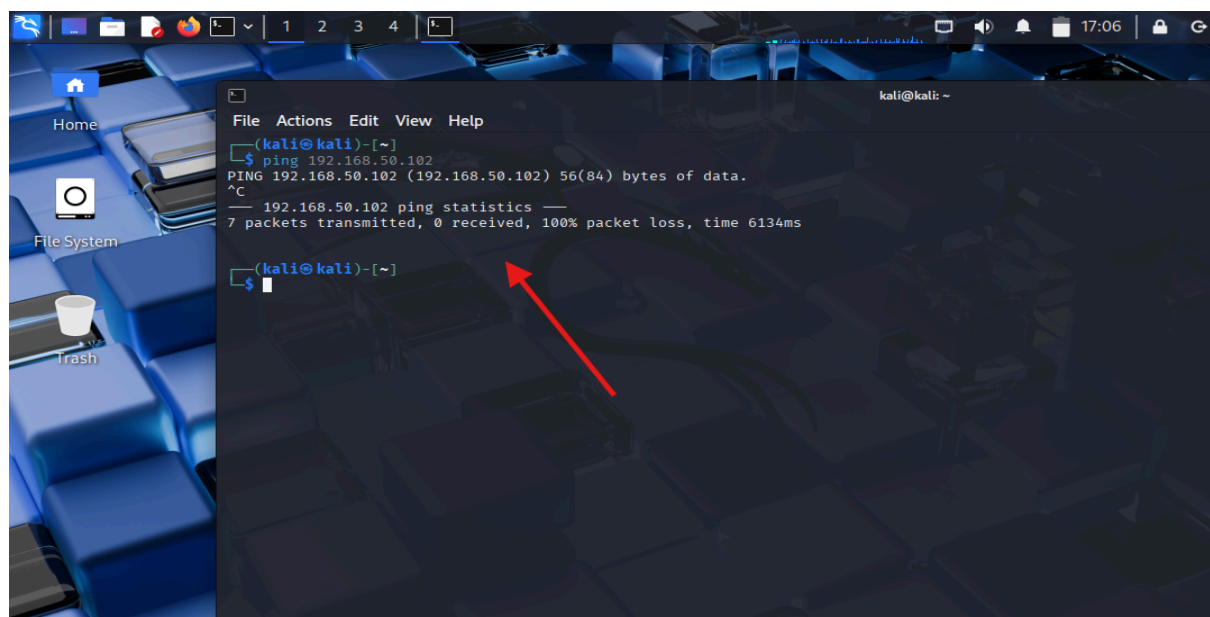
- nella sezione Profilo, ho spuntato tutti i profili di applicazione: Dominio, Privato e Pubblico.

The screenshot shows the 'Profile' tab of the same Windows Firewall rule configuration window. The 'Passaggi:' sidebar remains the same, with 'Profilo' (Profile) now highlighted. The main area contains the instruction: 'Selezionare il tipo di applicazione della regola.' (Select the type of application of the rule). There are three checked checkbox options: 1. 'Dominio' (Domain) with the description 'Regola applicabile ai computer connessi al rispettivo dominio aziendale.' 2. 'Privato' (Private) with the description 'Regola applicabile ai computer connessi a un percorso di rete privato, come una rete domestica o la rete di un ufficio.' 3. 'Pubblico' (Public) with the description 'Regola applicabile ai computer connessi ad un percorso di rete pubblico.'

Al termine di questa procedura, cliccando su “Fine”, possiamo trovare la nostra nuova policy in cima alla lista di regole delle connessioni in entrata.



Per verificare il corretto funzionamento della nuova policy, occorre adesso spostarci sulla MV Kali e provare un ping verso la MV Windows.



Nell' ultima foto si evince dunque che la policy creata sul Firewall Windows è stata correttamente inserita in quanto nessun pacchetto partito dalla MV Kali è riuscito ad arrivare alla MV Windows 10.

Ricci Riccardo

Roma, 11/10/2025