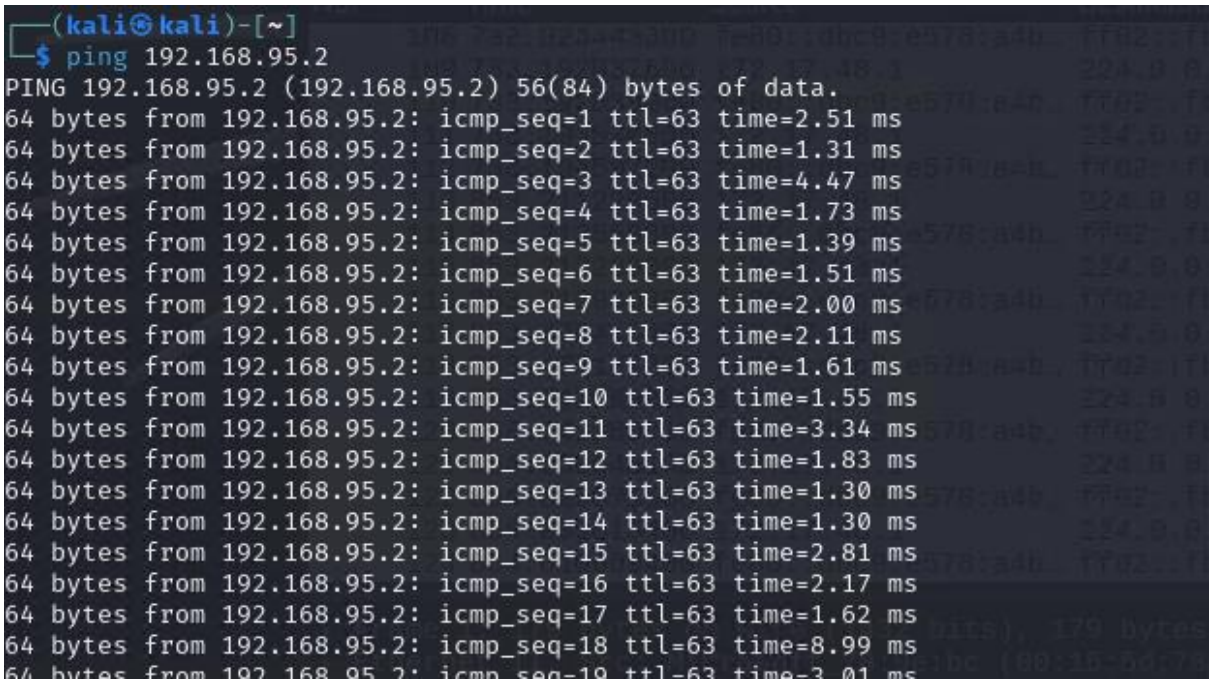
For enhanced security, configuring firewall rule is crucial

since there is no firewall rule attacking from kali vm to plc was successful, for example modifying the statue of coil 40 where affects hmi operation

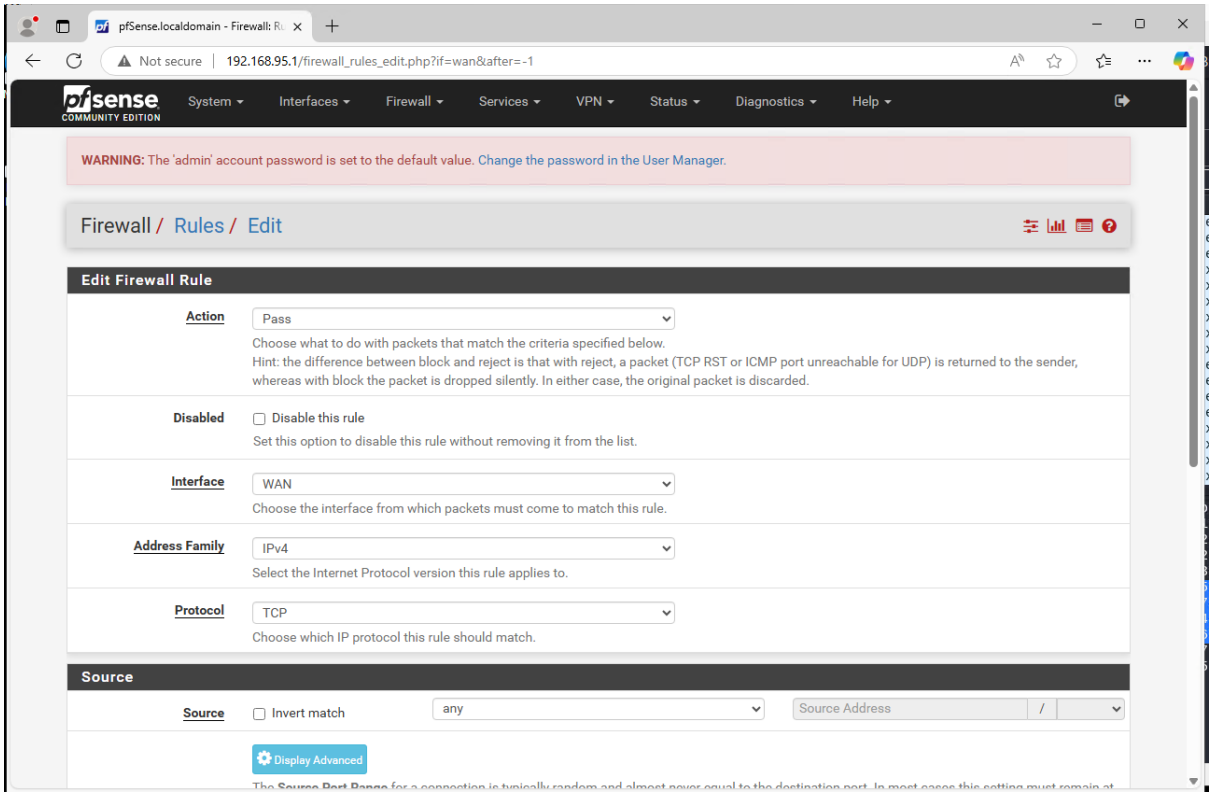
by configuring firewall rule, could prevent plc being detected and communicating from kali vm, blocking the attempt to attack such as previous practical examples



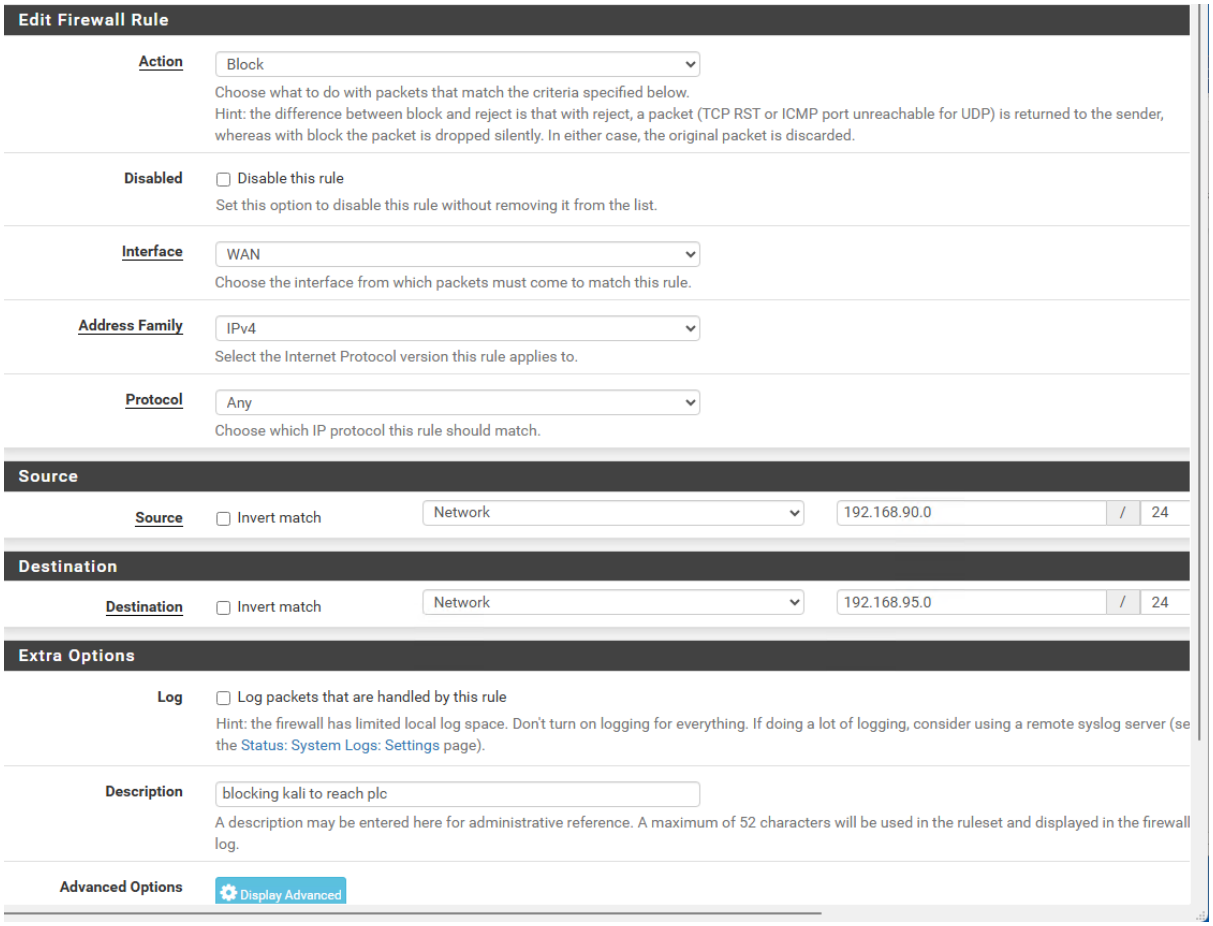
Currently plc is being pinged from kali and it responds

In order to block traffic from kali to plc to prevent attacks

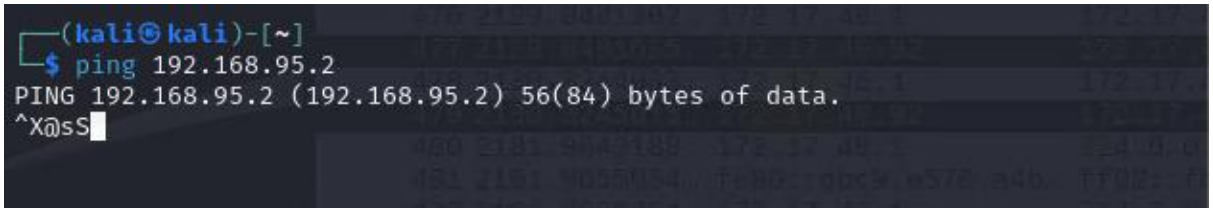
When traceroute done, it passes trough 192.168.90.100 and reaches plc



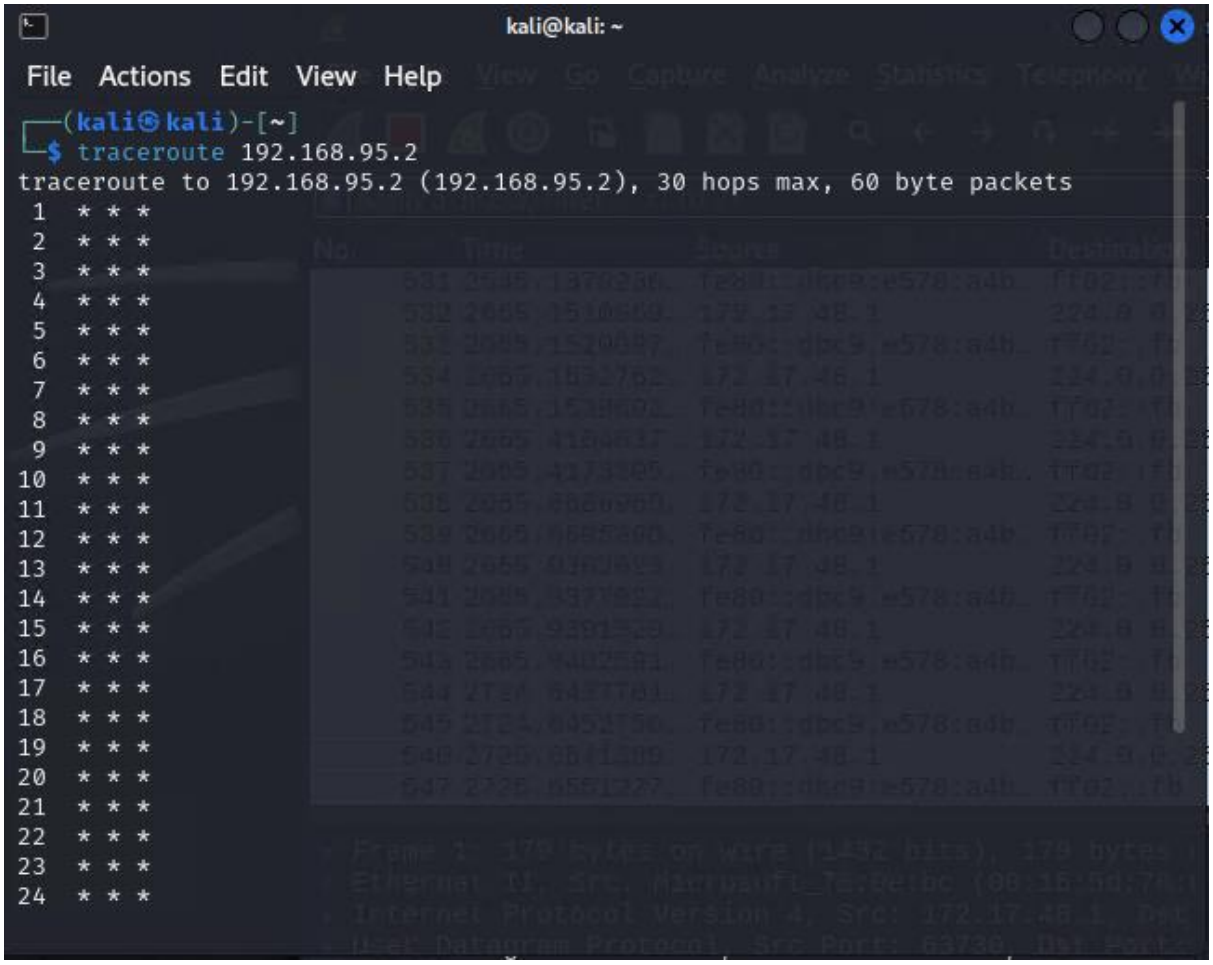
Go to pfsense firewall rule



Configure a firewall rule to block kali to interact with plc



after the configuration pinging the plc does not respond back, because the firewall blocks traffic from subnet 195.168.90.0/24 to plc subnet

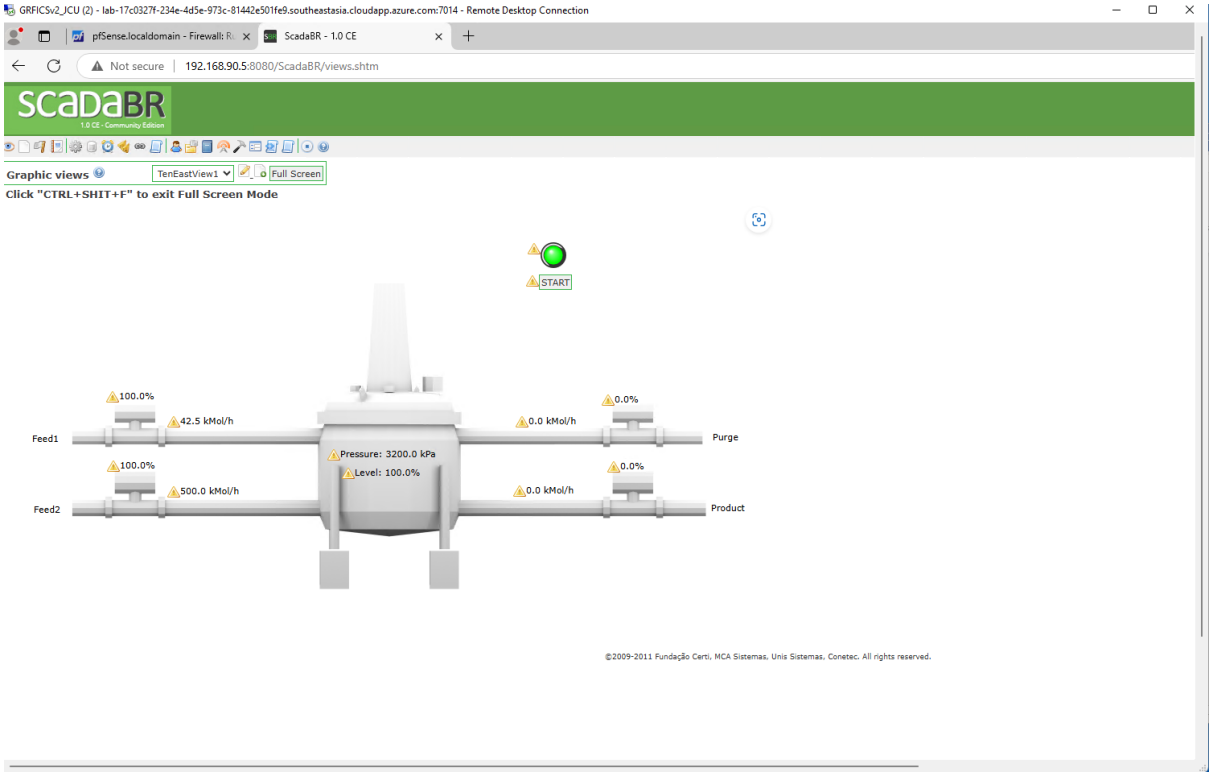


Traceroute does not show any result as well

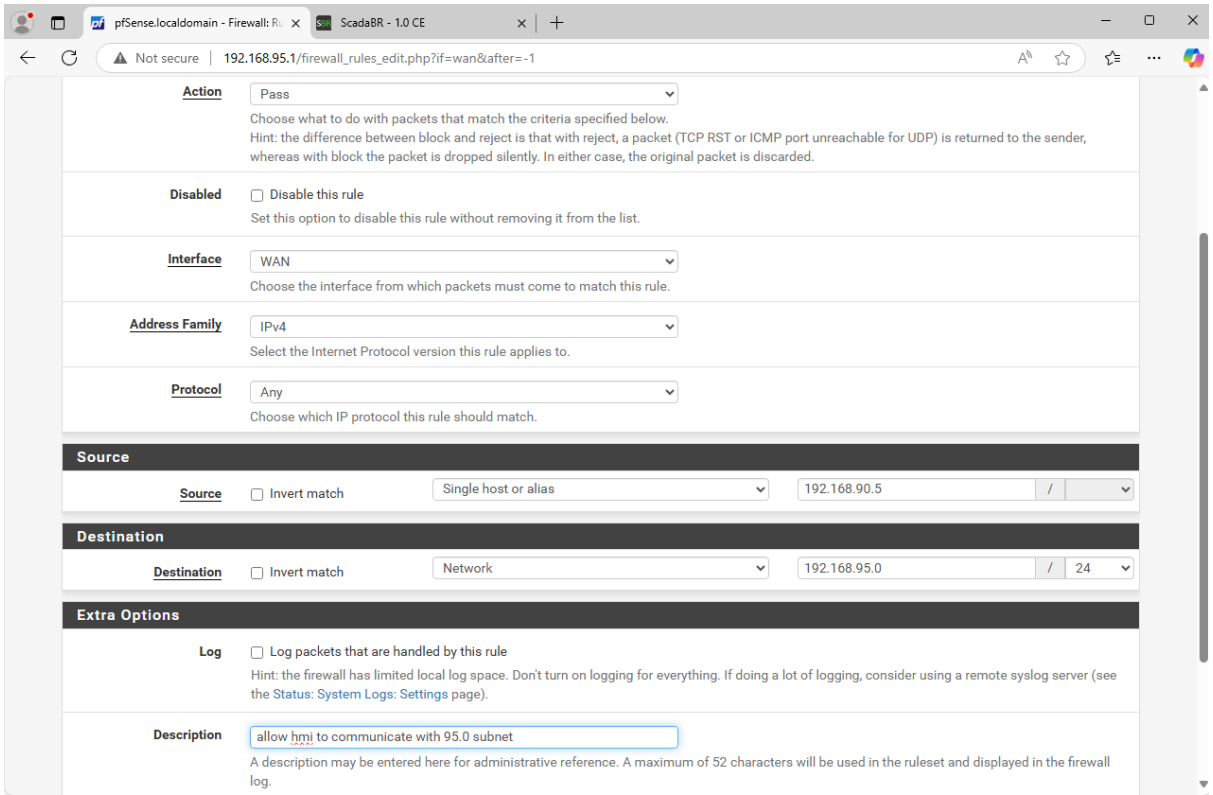
These results show that the configuration of new firewall rule blocking attempt from kali to plc was successful

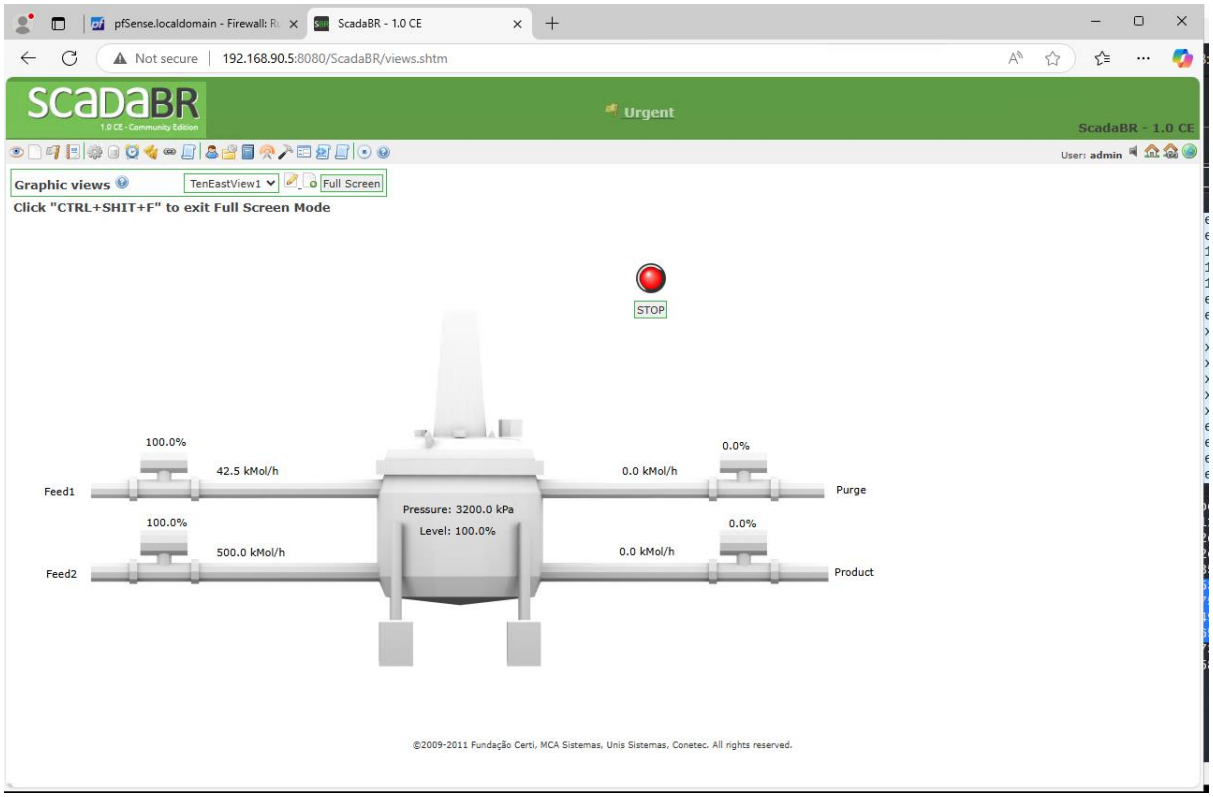
This could prevent attack attempt from kali vm to plc however this rule also impacts hmi

Thus requires another firewall rule for hmi to allow traffic to 192.168.95.0/24 subnet



the hmi operation is paused because traffic is blocked, there is no response when clicked on start button





After this new rule added, the hmi is back to its original operation

Firewall is essential in regulating traffic and preventing unauthorised access, in the example of our chemical plant OT, plc and hmi works as sensitive component of chemical plant proper configuration of firewall is critical in securing from any cyber threats also shown in practical 4 example of modifying coil 40 component affecting hmi operation statue

When configuring, remaining trusted devices being connected and taking out untrusted device is crucial, such as blocking kali and allowing hmi in this practical's example