

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

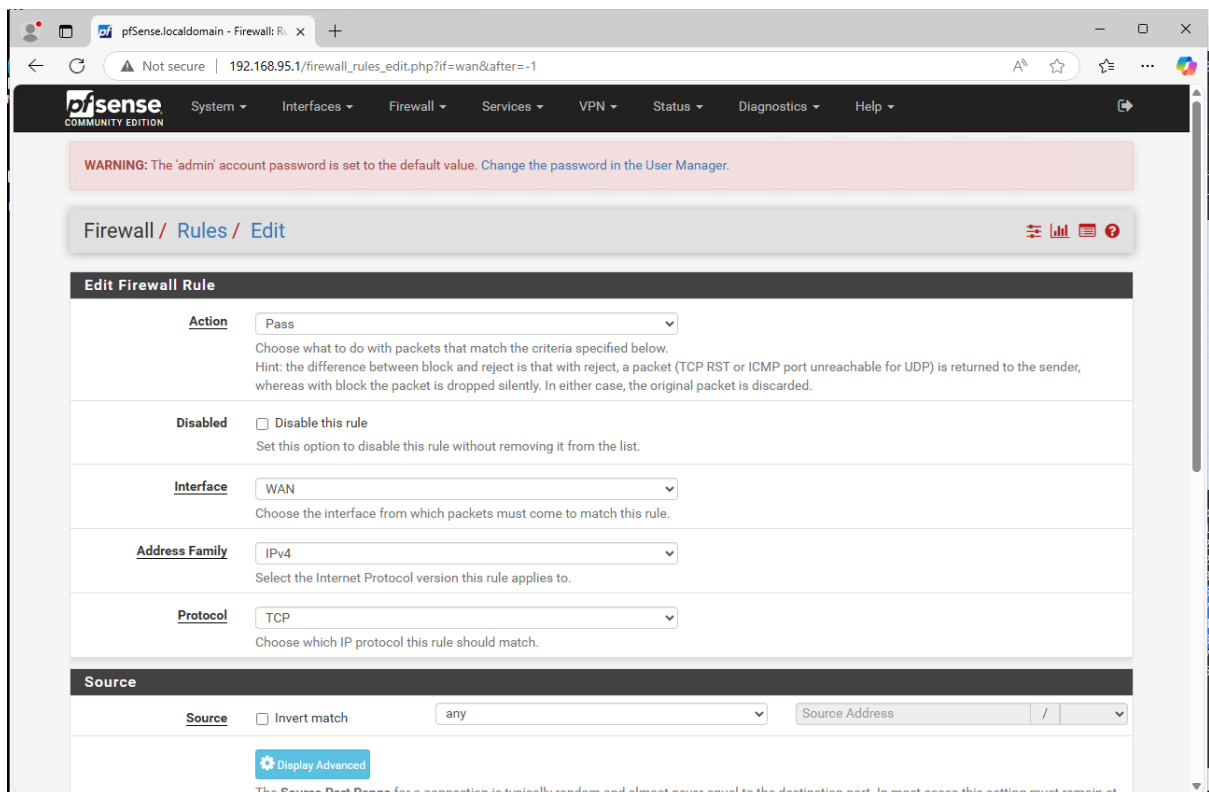
```
(kali@kali)-[~]
$ ping 192.168.95.2
PING 192.168.95.2 (192.168.95.2) 56(84) bytes of data.
64 bytes from 192.168.95.2: icmp_seq=1 ttl=63 time=2.51 ms
64 bytes from 192.168.95.2: icmp_seq=2 ttl=63 time=1.31 ms
64 bytes from 192.168.95.2: icmp_seq=3 ttl=63 time=4.47 ms
64 bytes from 192.168.95.2: icmp_seq=4 ttl=63 time=1.73 ms
64 bytes from 192.168.95.2: icmp_seq=5 ttl=63 time=1.39 ms
64 bytes from 192.168.95.2: icmp_seq=6 ttl=63 time=1.51 ms
64 bytes from 192.168.95.2: icmp_seq=7 ttl=63 time=2.00 ms
64 bytes from 192.168.95.2: icmp_seq=8 ttl=63 time=2.11 ms
64 bytes from 192.168.95.2: icmp_seq=9 ttl=63 time=1.61 ms
64 bytes from 192.168.95.2: icmp_seq=10 ttl=63 time=1.55 ms
64 bytes from 192.168.95.2: icmp_seq=11 ttl=63 time=3.34 ms
64 bytes from 192.168.95.2: icmp_seq=12 ttl=63 time=1.83 ms
64 bytes from 192.168.95.2: icmp_seq=13 ttl=63 time=1.30 ms
64 bytes from 192.168.95.2: icmp_seq=14 ttl=63 time=1.30 ms
64 bytes from 192.168.95.2: icmp_seq=15 ttl=63 time=2.81 ms
64 bytes from 192.168.95.2: icmp_seq=16 ttl=63 time=2.17 ms
64 bytes from 192.168.95.2: icmp_seq=17 ttl=63 time=1.62 ms
64 bytes from 192.168.95.2: icmp_seq=18 ttl=63 time=8.99 ms
64 bytes from 192.168.95.2: icmp_seq=19 ttl=63 time=3.01 ms
```

Currently plc is being pinged from kali and it responds

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

```
kali@kali: ~
File Actions Edit View Help View Go Capture Analyze Statistics Telephony W
(kali@kali)-[~]
$ traceroute 192.168.95.2
traceroute to 192.168.95.2 (192.168.95.2), 30 hops max, 60 byte packets
 1  192.168.90.100 (192.168.90.100)  2.647 ms  2.734 ms  1.674 ms
 2  192.168.95.2 (192.168.95.2)  6.703 ms  6.845 ms  7.010 ms
(kali@kali)-[~]
$
```

When traceroute done, it passes trough 192.168.90.100 and reaches plc



Go to pfSense firewall rule

**Edit Firewall Rule**

**Action**

Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface**

WAN

Choose the interface from which packets must come to match this rule.

**Address Family**

IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**

Any

Choose which IP protocol this rule should match.

**Source**

**Source**

☐ Invert match

Network

192.168.90.0

/

24

**Destination**

**Destination**

☐ Invert match

Network

192.168.95.0

/

24

**Extra Options**

**Log**

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**

blocking kali to reach plc

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options**

[Display Advanced](#)

Configure a firewall rule to block kali to interact with plc

```
(kali@kali)-[~]
$ ping 192.168.95.2
PING 192.168.95.2 (192.168.95.2) 56(84) bytes of data.
^X@sS
```

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

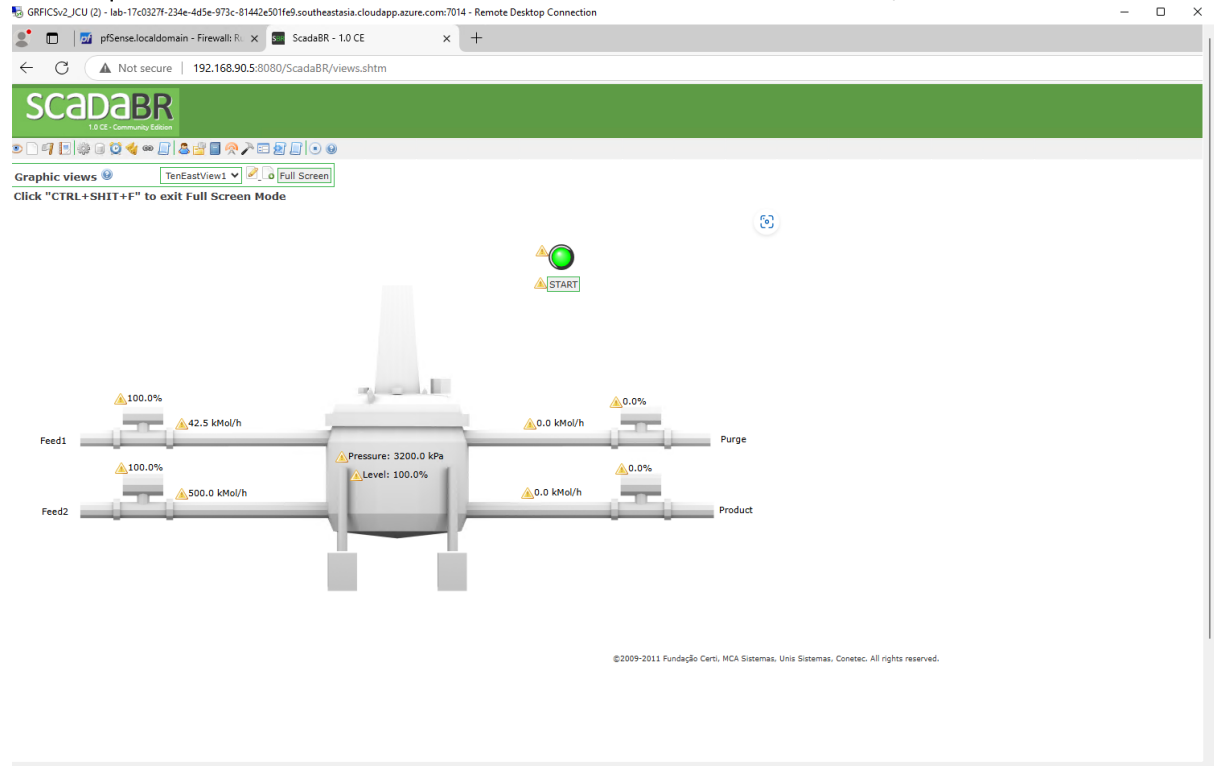
```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ traceroute 192.168.95.2
traceroute to 192.168.95.2 (192.168.95.2), 30 hops max, 60 byte packets
 1 * * *
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
```

Traceroute does not show any result as well

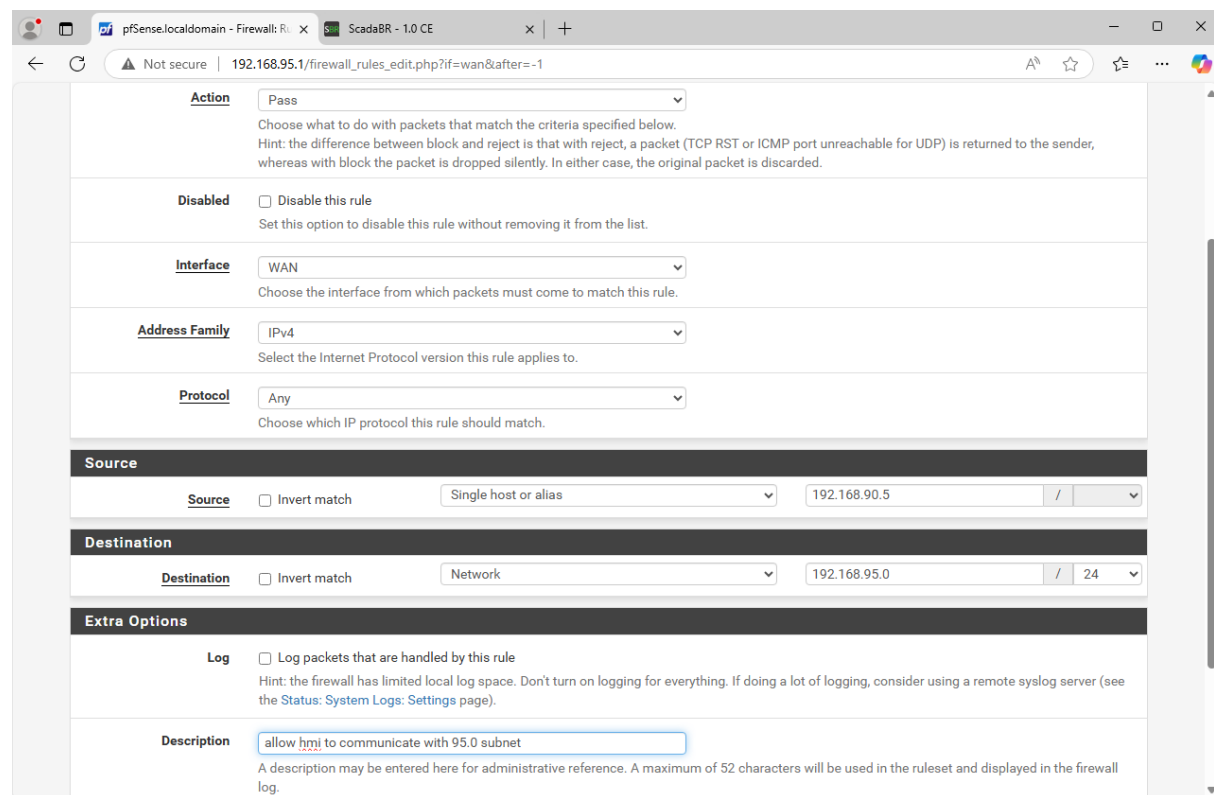
These results show that the configuration of new firewall rule blocking attempt from kali to plc was successful

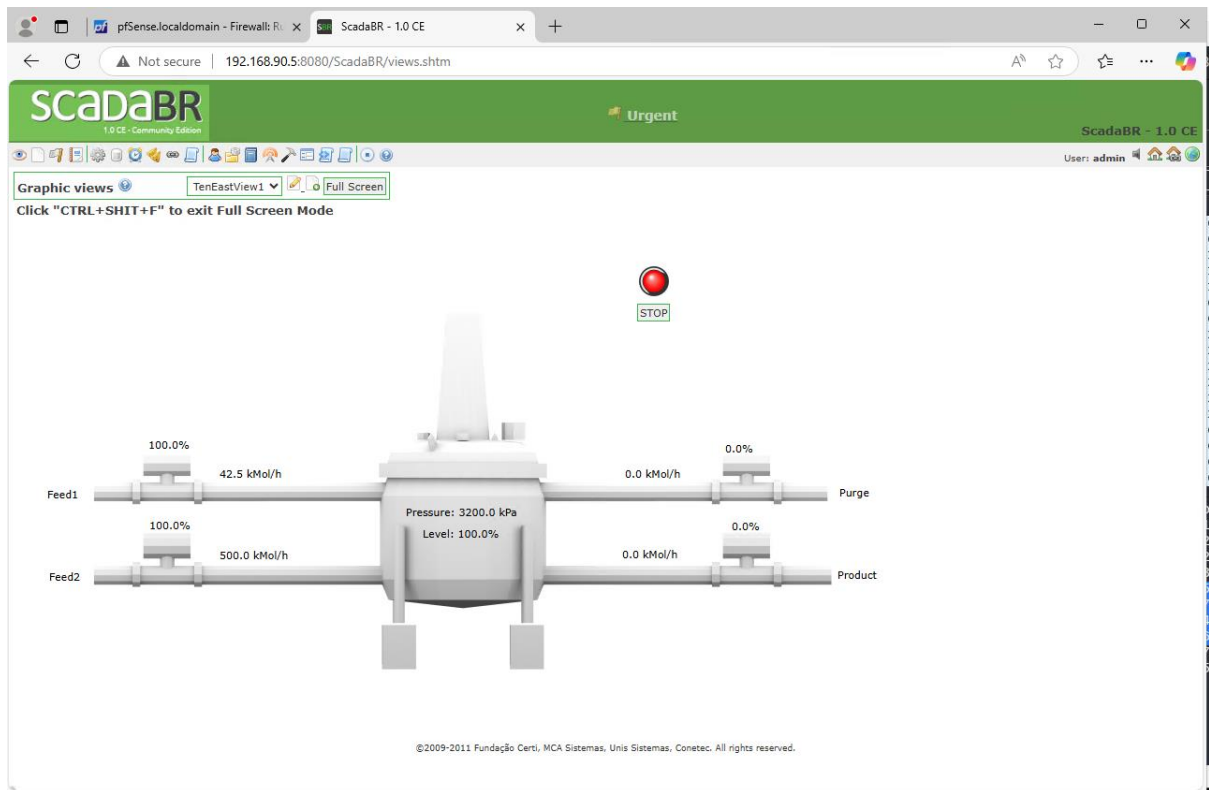
This could prevent attack attempt from kali vm to plc however this rule also impacts hmi

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