TP5 - Cybersecurity - Network Segregated Firewall

Operational objectives :

- Understand the value of a network-separated firewall architecture
- To be able to define and implement a split network firewall architecture
- Be able to define and implement a filtering rule on a separate network
- Be able to demonstrate the effectiveness of this type of architecture

Prerequisites :

- Master the basic operations of Control Expert
- Be able to launch Vijeo Designer in simulation mode
- Have understood the main principles of SNi40 configuration

The problem :

To set up a firewall architecture with separate networks: Internet, industrial and administrator networks, and to limit access to the industrial network to members of the administrator network.

Resources :

- **Manufacturer documentation**
  - Schneider Electric
    - ➔ website
    - ➔ protocol-modbus.pdf
  - Stormshield :
    - ➔ SNS - User and Configuration Manual
- **Specific documentation**
  - Architectures Maquette Cybersec_anglais.pptx
- **Applications made available for the realization of this TP :**
  - M580 application (Control Expert): md1ae58ecyb.stu
  - HMI application (Vijeo Designer): MD1AE58ECYB
  - Default SNi40 Firewall configuration file (SNI40-TP2-0.na)
- **Software provided, to be installed on the work PC (console) for the realization of this TP:**
  - Control Expert (Schneider Electric) : Programming of Schneider Electric M340, M580, …
  - Vijeo Designer V6.2 SP8 : Design of Magelis HMI applications(execution including in Simulation mode on the Workstation)
  - Web Gate Client (Schneider Electric): complement to Vijeo Designer [option] (remote client of the Magelis HMI) (remote client of the Magelis HMI, running in an Internet Browser)
  - Internet Explorer : Microsoft Internet Browser
  - Angry IP Scanner (angryip.org): check for accessible IP addresses in a given range [option]
  - Wireshark (Wireshark Foundation): observation of Ethernet frame details

Critères d'évaluation :	😀	😐	😟
Understand the value of network separation at the firewall level			
Implementation of network separation with SNI40			
Setting up a filtering rule on a separate network			
Demonstrating the effectiveness of this type of architecture			
Autonomy - Quality of work/restitution			

Time spent :	1 h	**Objective(s) :**		Comment(s) :
Evaluation :	/ 20	Reached(s)	Not reached	

TP5 - Firewall with Separate Networks

1. Using the document provided "Architectures Maquette Cybersec_anglais.pptx", identify the different sub-networks to be set up on the Sni40 and explain the advantages of setting up such a separation of networks.
2. Define a port on the Sni40 for each subnet, set up the cabling and configure the Sni40 to separate the subnets. Validate the configuration by testing access to the Sni40 gateway for each subnet via a "ping" command. (N.B. You can add an additional test network in preparation for the following questions).

3. From the administrator's network, after establishing the correct routing on his PC and enabling the "pass all" security policy on the Sni40, ping the M580 NOC. Explain the result.

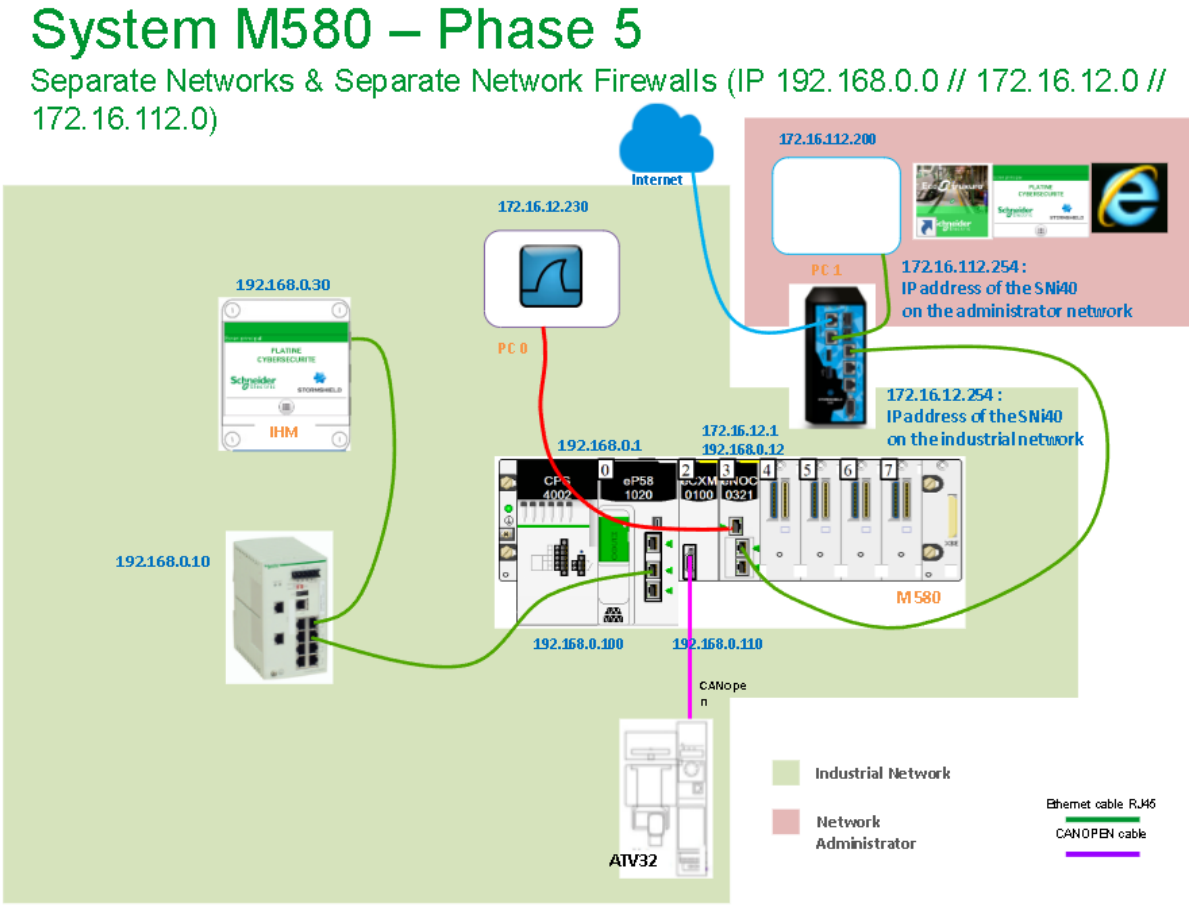
4. Configure the M580 NOC router to allow access from the industrial subnet to the Sni40 gateway, then check the accessibility of the NOC from the administrator network.

5. Set up the routing so that the M580 can be accessed from its NOC router gateway through the Sni40 and check that it is working correctly using Vijeo Designer.

6. Restrict access to the industrial network to the administrator network only. Validate the implementation of this filtering by trying to access the industrial network from another network (test network).

Details of expected operations

1. Interest of a separate network architecture

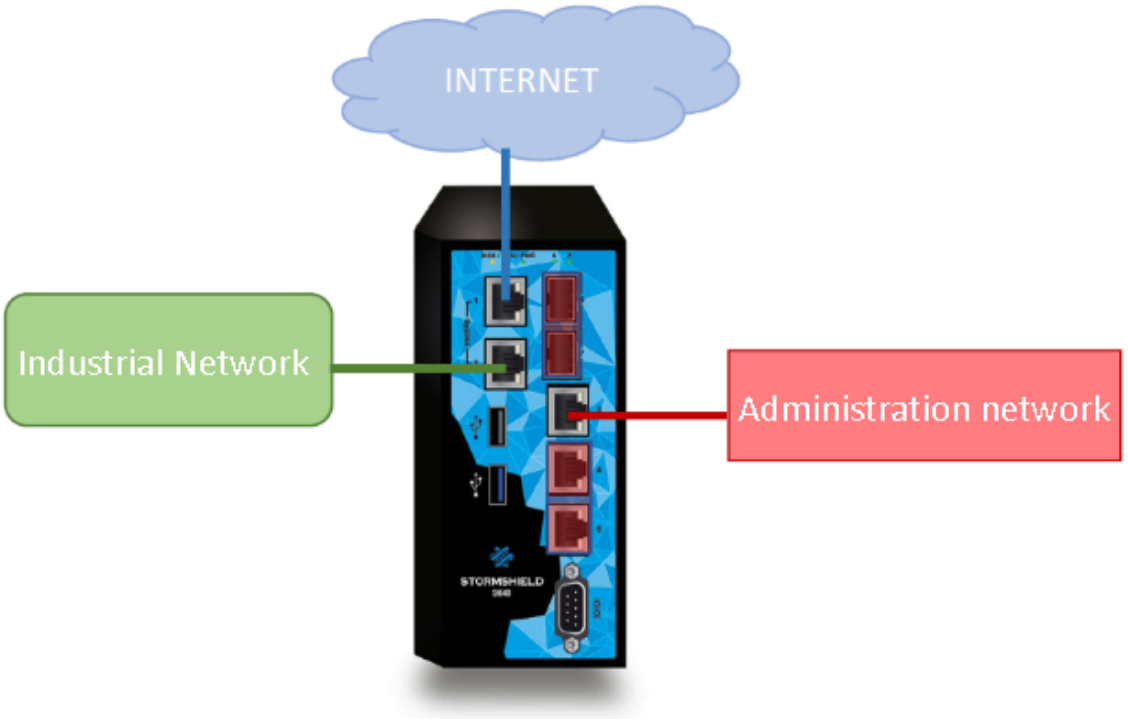


The network linked to the Sni40 is divided into 3 sub-networks: an industrial network which includes all the elements linked to the industry (PLC, etc.), an administrator network which allows the administration of the industrial network, the manipulation of the Sni40 (configuration modification, data analysis, etc.) and an internet network which allows the firewall to be updated.

There are many advantages to such a network architecture:

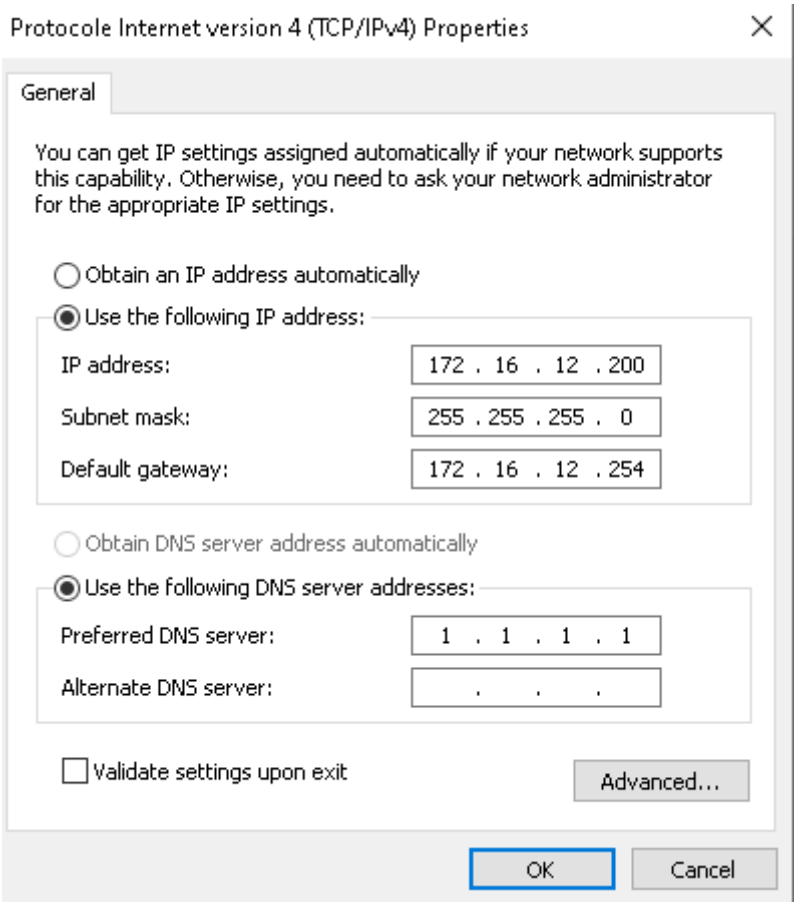
- Reduction of the network load (number of packets on the network) by distributing the devices on different broadcast domains (one for each subnet) and therefore also reduction of the number of (useless) packets received for each equipment.
- Improved security level: on the one hand by reducing the impact of certain cyber-attacks (attack via broadcasting, ...), on the other hand by offering the possibility of establishing specific security rules for each subnet.
- Improved quality of network monitoring: each subnet has its own role (easier to filter, analyze, etc.).

2. **Setting up the basic configuration**



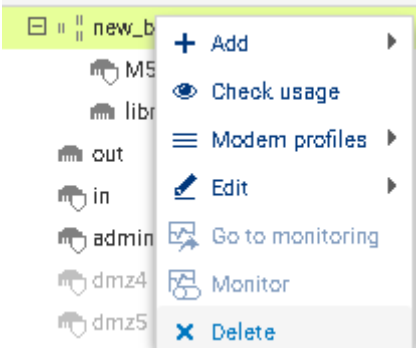
To answer this question, a possible proposal is to use port 2 of the Sni40 as an interface for the industrial network and port 3 as an interface for the administration network. Port 1 of the Sni40 is intended for the Internet network. The other interfaces (ports) will be disabled to improve security. However, a test subnet on port 4 can already be set up for the rest of the tutorial.

First, connect to the firewall by setting the IP configuration correctly:

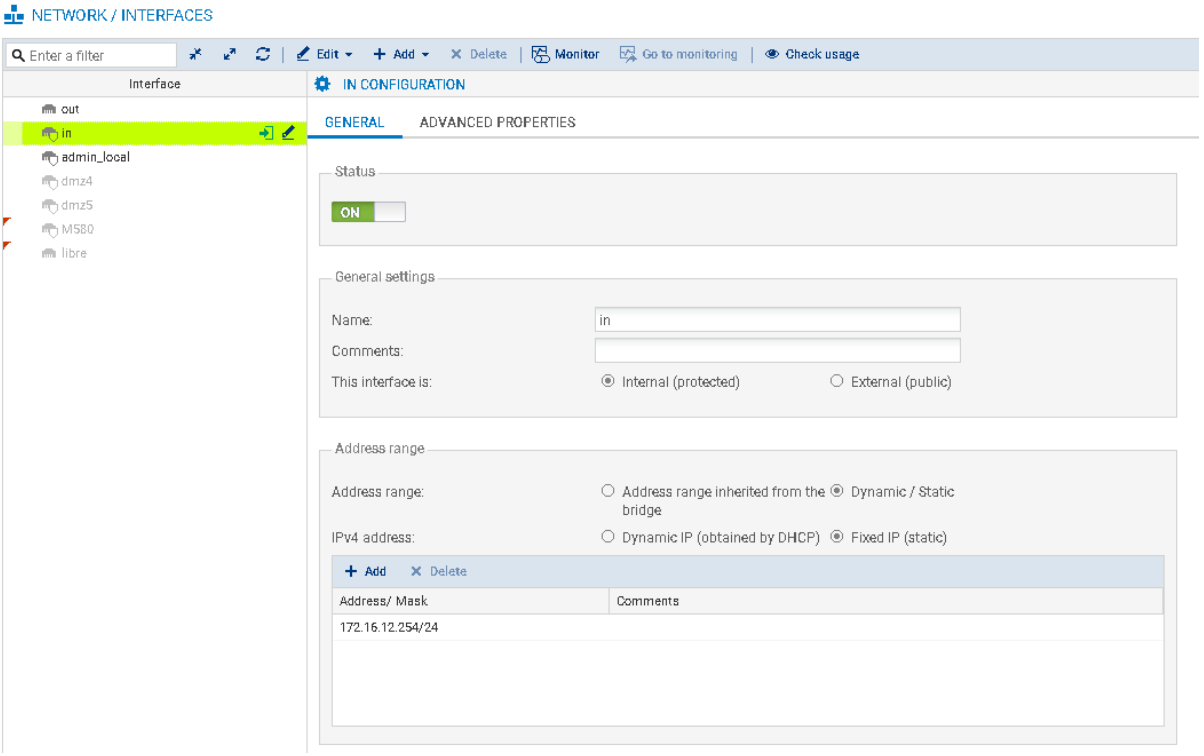


You can then connect to the firewall at https://172.16.12.254/admin and access the **Configuration > Network > Interfaces** panel to configure the network interfaces.

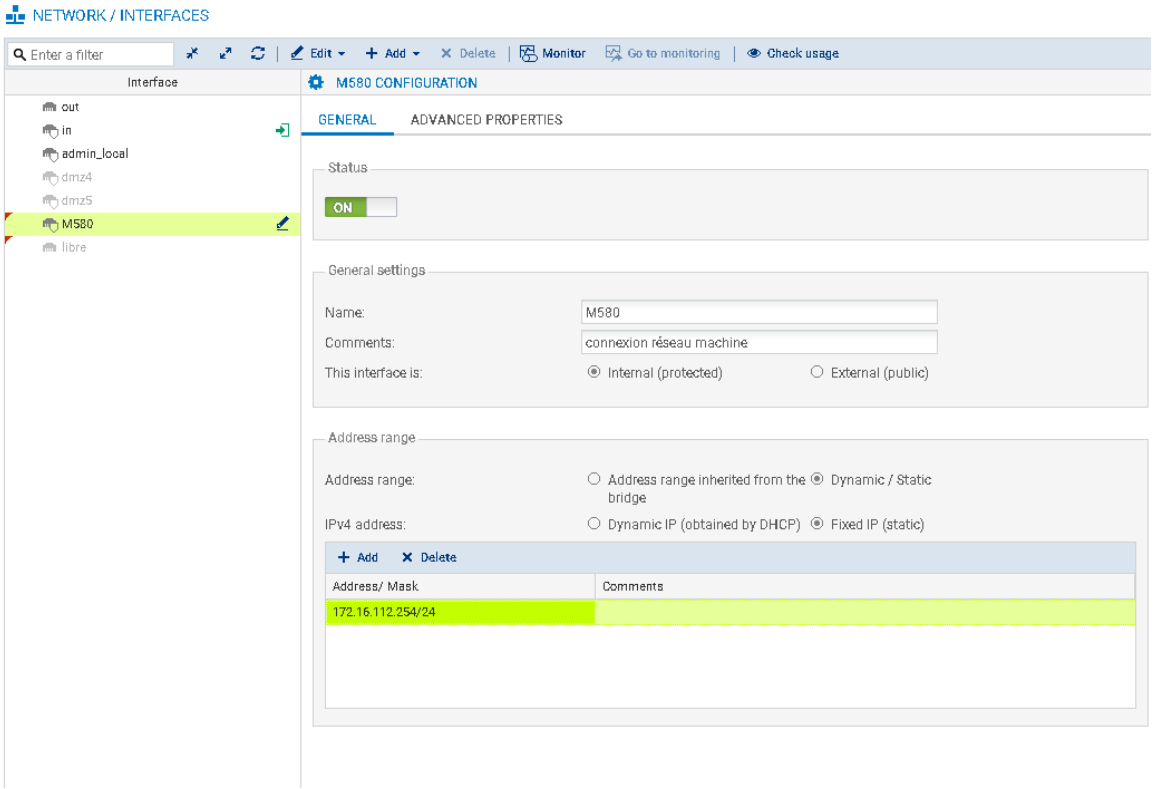
Then click on **bridge** and delete it. When requested, click on "Force Delete":



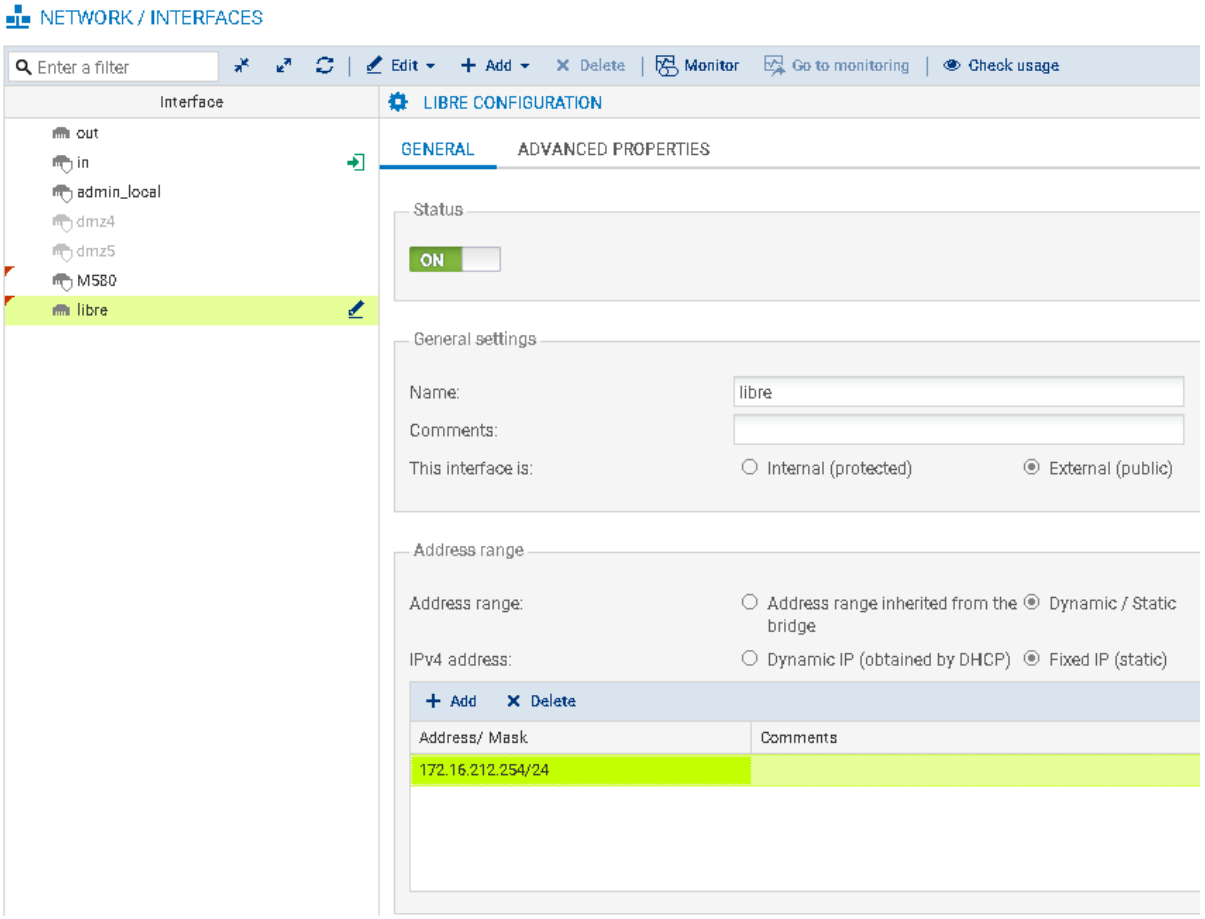
Enter **172.16.12.254/24** as the IPv4 address to “in” interface port 2:



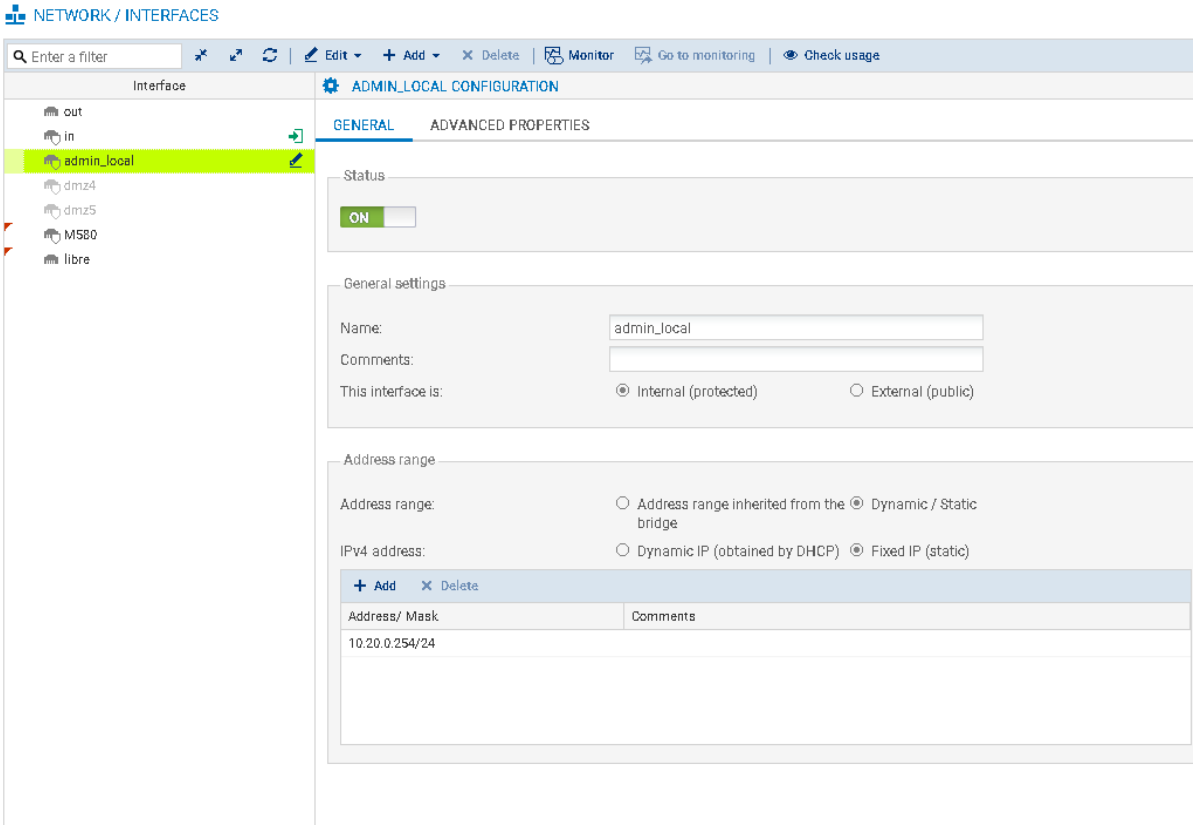
The same operation will be performed for **dmz1** (port 3), this time using the IPv4 address **172.16.112.254/24** :



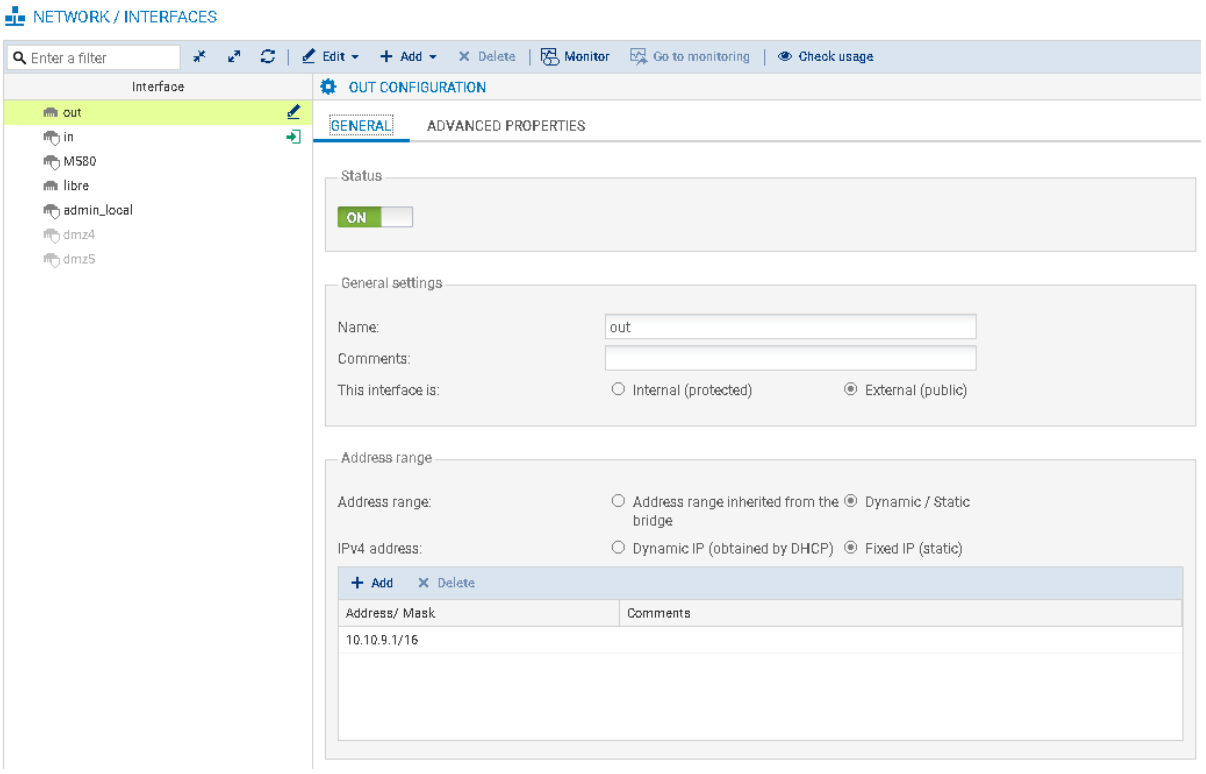
In anticipation of the rest of the tutorial, we will also perform this operation on **dmz2** (port 4) with the IPv4 address **172.16.212.254/24**, this will be the test network:



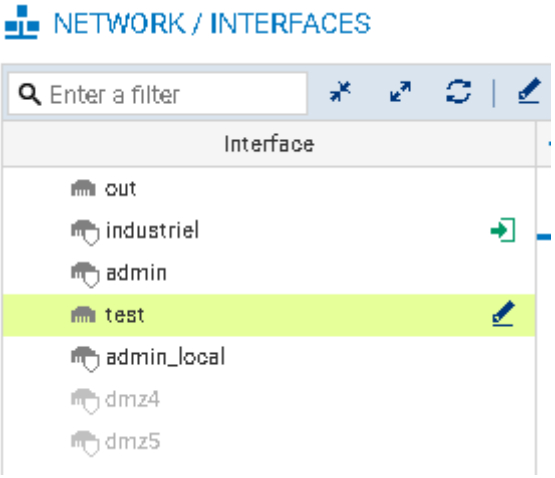
As for the other interfaces, by the same procedure, they are deactivated:



This results in the following configuration, which can be applied by ignoring the message warning that the connection will be interrupted:



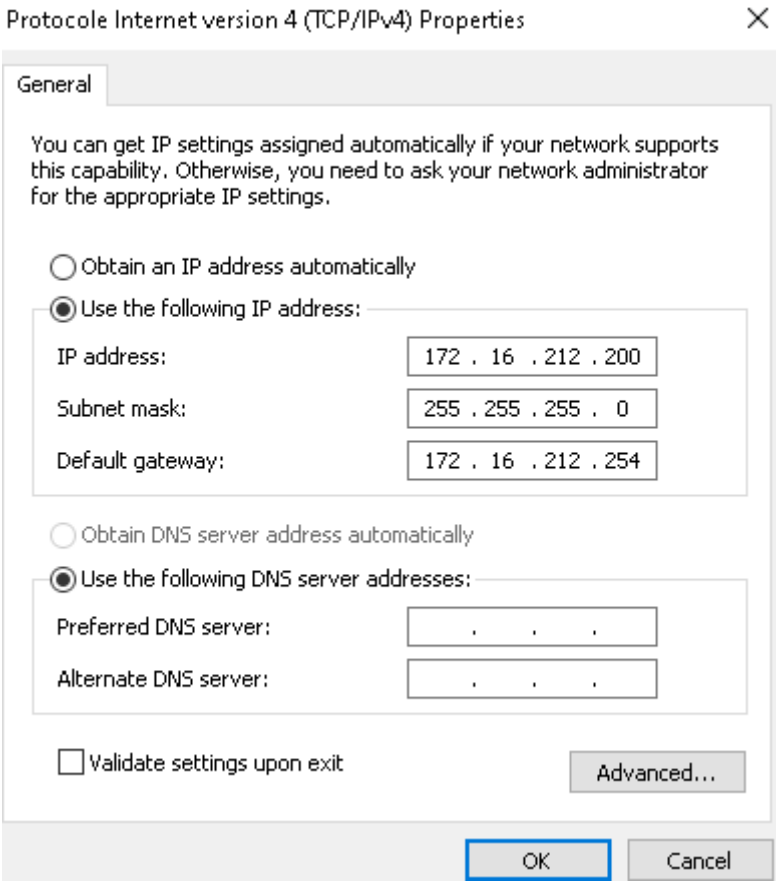
The names of the interfaces can then be changed as follows to make them easier to understand:



By going to port 2 of the firewall and without changing the IPv4 settings of the PC, we can then check on the command line that the configuration of this port works:

```
C:\Users\Administrateur>ping 172.16.12.254

Pinging 172.16.12.254 with 32 bytes of data:
Reply from 172.16.12.254: bytes=32 time=2ms TTL=64
Reply from 172.16.12.254: bytes=32 time=2ms TTL=64
Reply from 172.16.12.254: bytes=32 time=2ms TTL=64
Reply from 172.16.12.254: bytes=32 time=2ms TTL=64

Ping statistics for 172.16.12.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

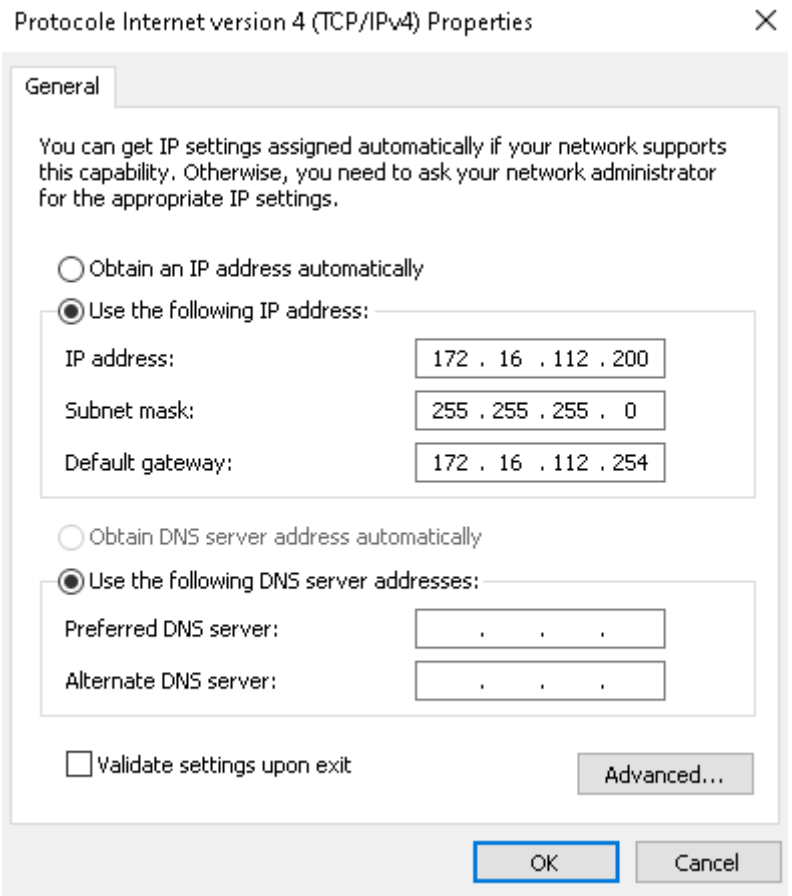
Then move to port 4 of the firewall with the following IPv4 configuration:



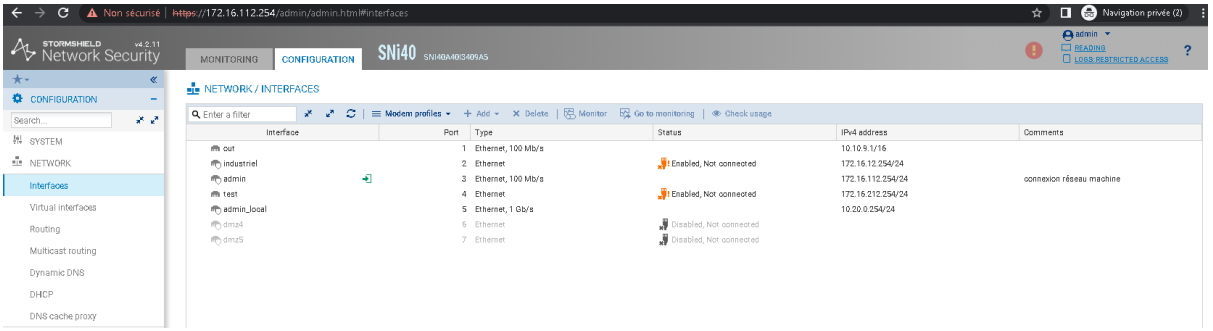
Then test that the configuration of this interface is correctly set up:

```
C:\Users\Administrateur>ping 172.16.212.254

Pinging 172.16.212.254 with 32 bytes of data:
Reply from 172.16.212.254: bytes=32 time=2ms TTL=64
Reply from 172.16.212.254: bytes=32 time=2ms TTL=64
Reply from 172.16.212.254: bytes=32 time=2ms TTL=64
Reply from 172.16.212.254: bytes=32 time=2ms TTL=64

Ping statistics for 172.16.212.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Finally, using the appropriate configuration, we move to port 3:



For the rest of the tutorial, we will remain on this port, so we can simply access the address https://172.16.112.254/admin and connect to verify the correct configuration of the port.

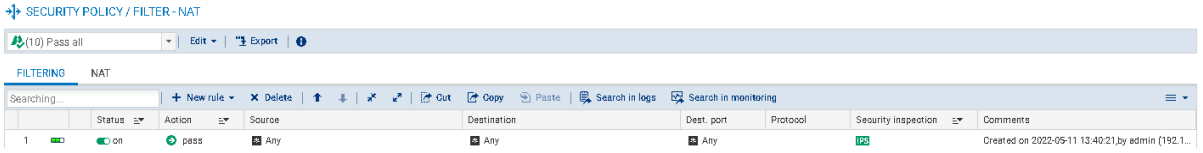


3. Configuring the M580 NOC Router

Before you can check the accessibility of the NOC via the administrator network, you need to set up the correct routing on the PC using the command "**route add 172.16.12.0 mask 255.255.255.0 172.16.112.254**":

```
C:\Users\Administrateur>route add 172.16.12.0 mask 255.255.255.0 172.16.112.254
 OK!
```

Also go to **Configuration > Security Policy > Filtering and NAT** to enable the **"(10) Pass All+Analysis"** security policy:



Check if the NOC is reachable from the administrator network (still on port 3) by pinging:

ping 172.16.12.1

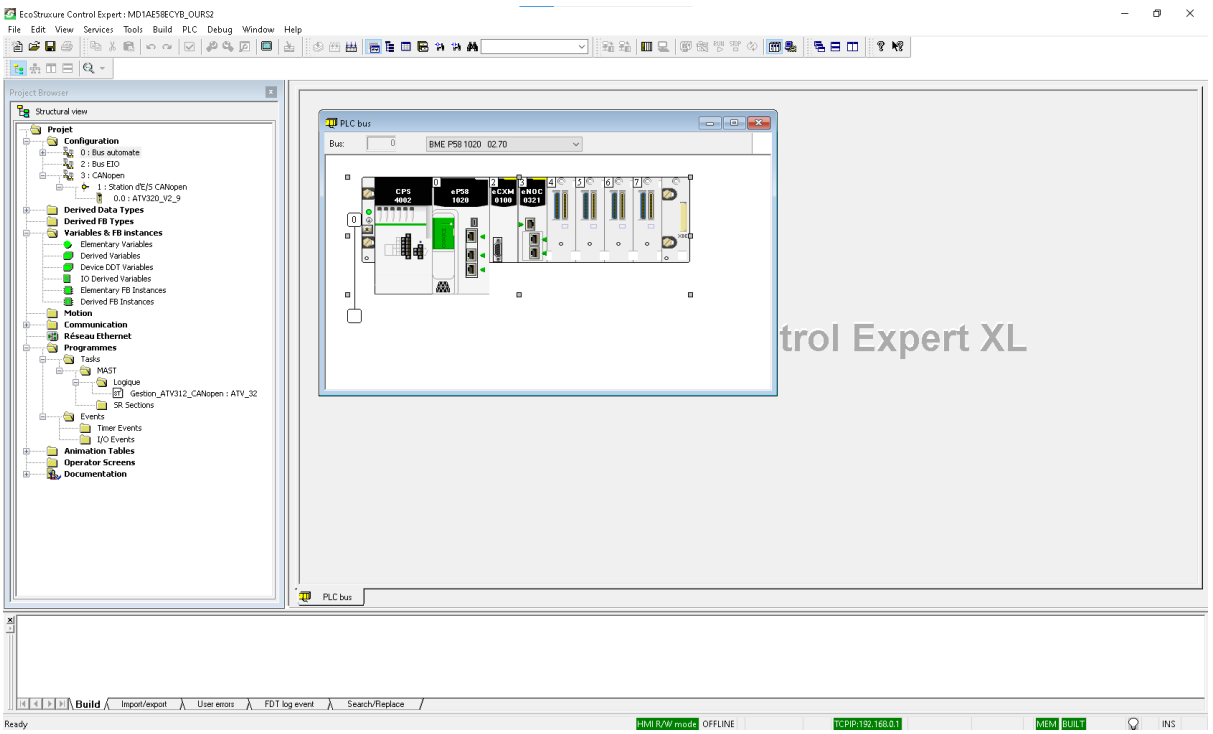
```
C:\Users\Administrateur>ping 172.16.12.1

Pinging 172.16.12.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.12.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Explanation: The packets sent by the PC on the administrator network are received by the Sni40 (this can be checked via Wireshark) and are also transmitted by the Sni40 to the industrial network (this can be checked via the command tcpdump -i igb1 -s 65535 port not 22 in ssh on the Sni40). However, with the current configuration of the M580, the NOC does not have the gateway address of the Sni40 in its IPv4 configuration, so it is impossible for the NOC to transmit the response packets to the Sni40 and therefore to the PC in the administrator network.

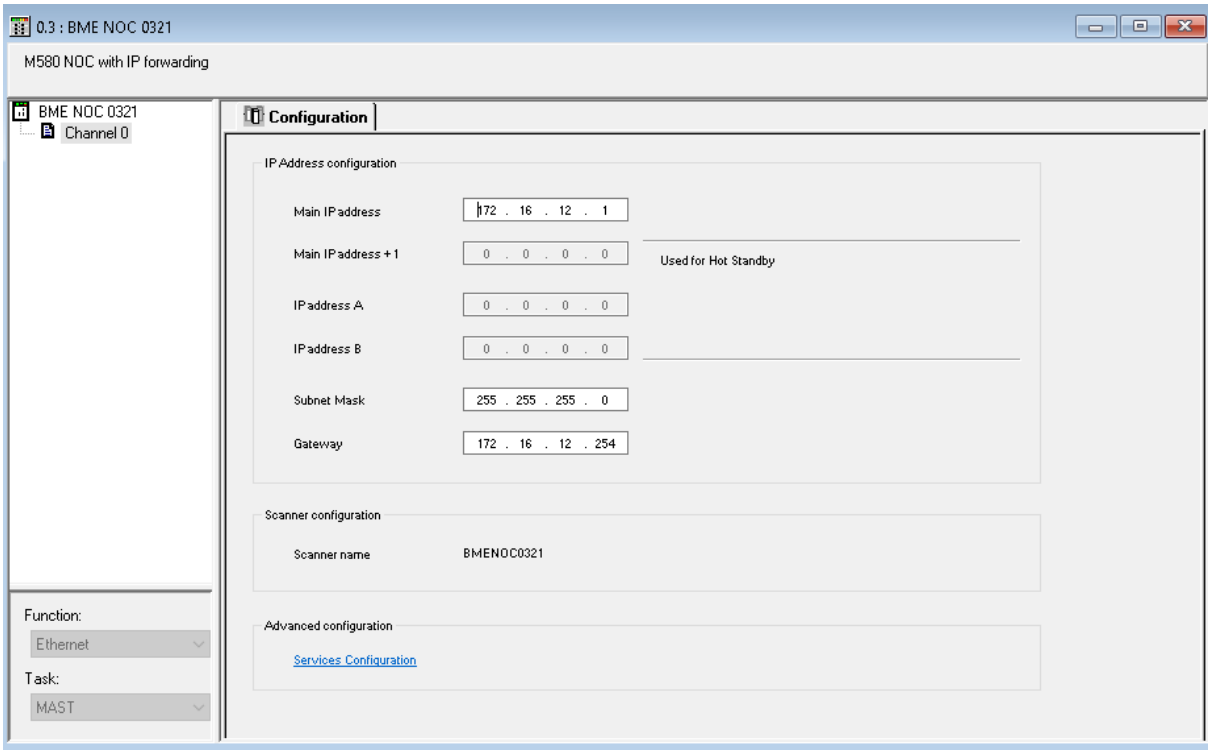
4. Configuring the M580 NOC Router

In order to access the M580 from the administrator network, open the md1ae58ecyb.stu program using Control Expert.

Double click on **PLC Bus (bus automate)** to open the M580 component map:



Then open the NOC router settings by double-clicking on the NOC and set the gateway value to **172.16.12.254** :



Close the window and validate the modifications when requested, then regenerate the project using the menu **Generation > Generate project** (or the shortcut Ctrl + B).

Then connect to the M580 via Ethernet or USB as seen in the previous tutorials, and transfer the project to the PLC (**PLC > Transfer project to PLC**). Do not forget to run the program once the transfer is complete.

N.B.: If the PLC fails, the model must be completely powered down and the PLC restarted.

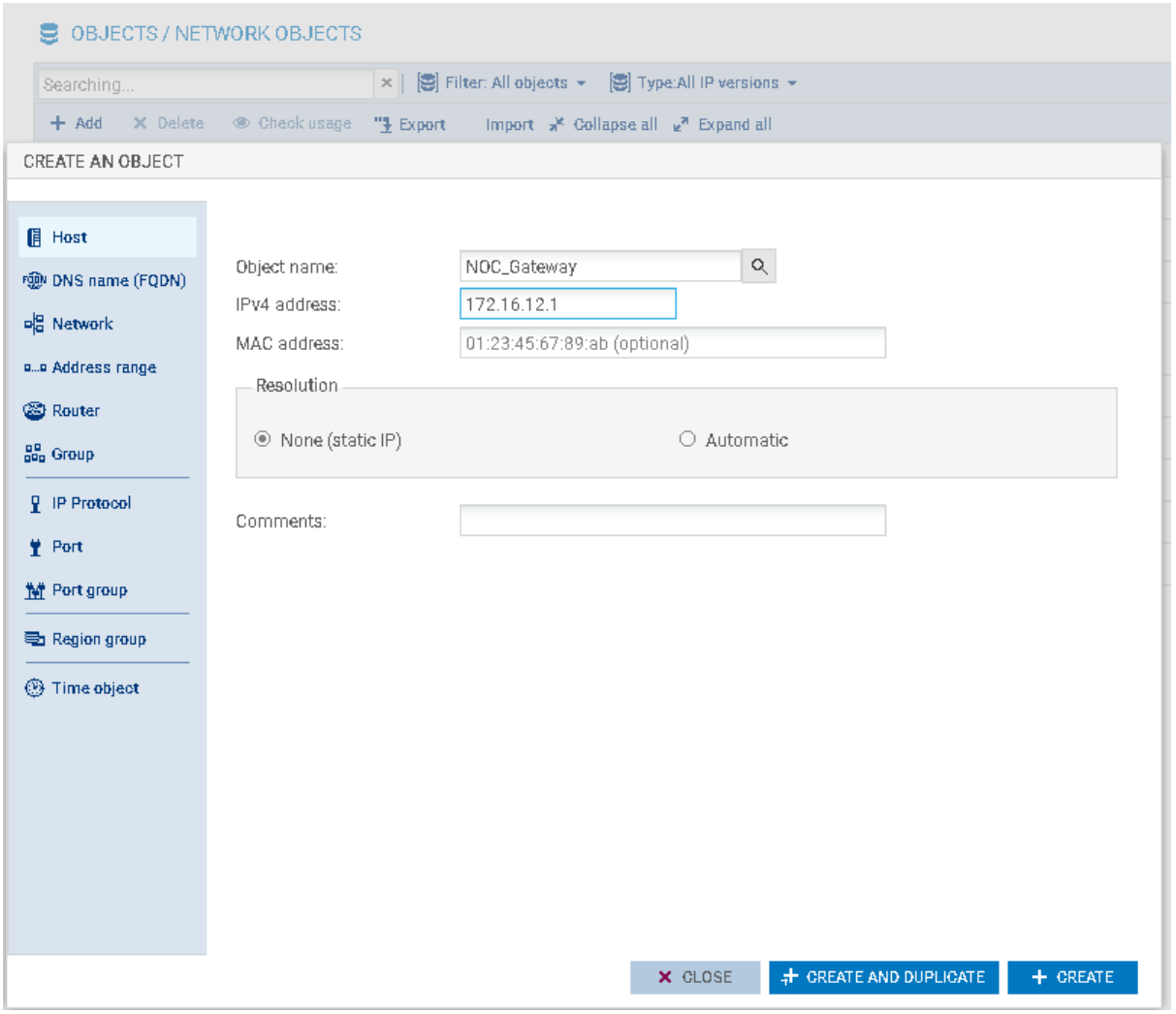
Check that the M580 NOC is accessible from the administrator network (port 3):

```
C:\Users\Administrateur>ping 172.16.12.1

Pinging 172.16.12.1 with 32 bytes of data:
Reply from 172.16.12.1: bytes=32 time=5ms TTL=64
Reply from 172.16.12.1: bytes=32 time=3ms TTL=64
Reply from 172.16.12.1: bytes=32 time=3ms TTL=64
Reply from 172.16.12.1: bytes=32 time=3ms TTL=64

Ping statistics for 172.16.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

5. Setting up routing on the Sni40

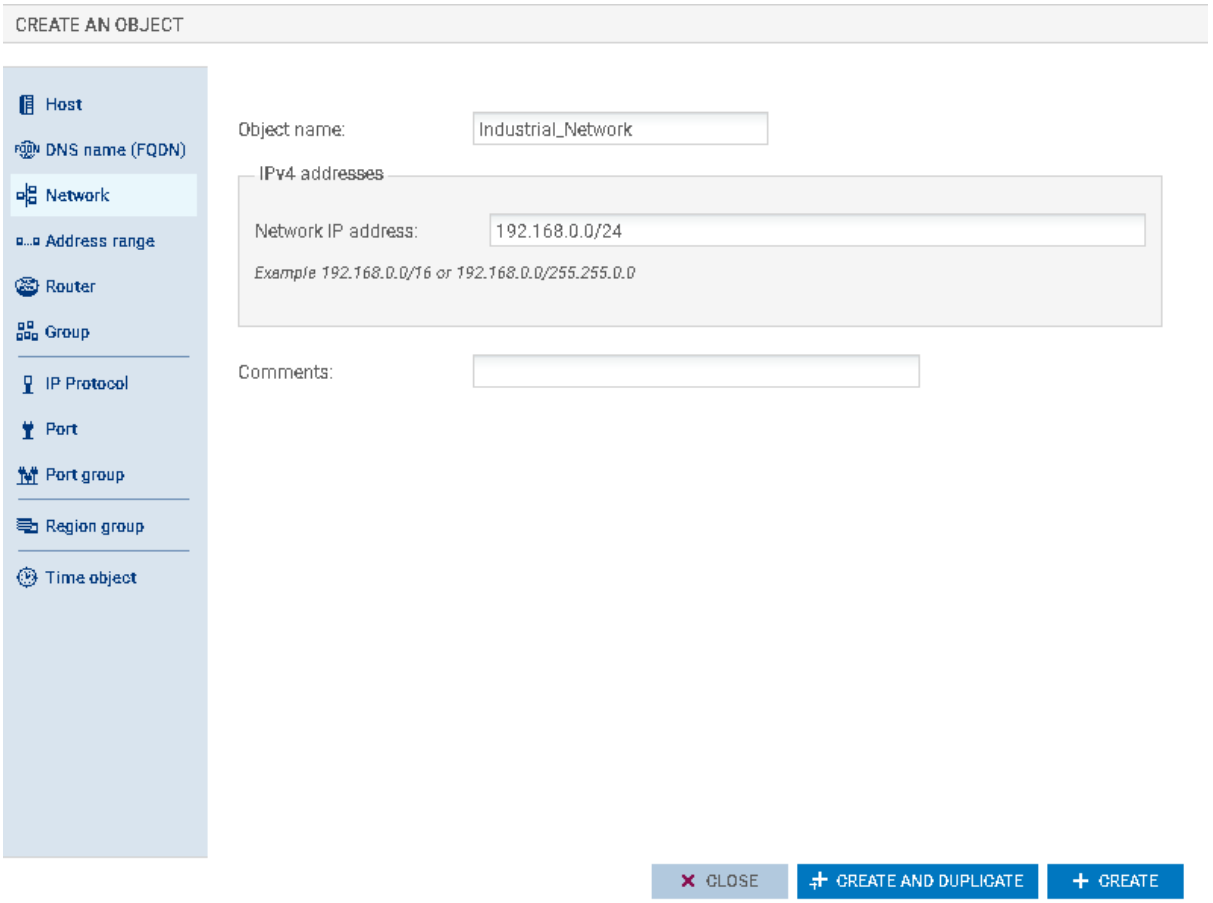
In order to access the M580 through the NOC accessible via the Sni40, a routing rule must be set up to route the addresses of the industrial LAN (**192.168.0.0/24**) through the NOC gateway (**172.16.12.1)**.

On the Sni40, from the **Configuration > Objects > Network Objects** menu, add a new **Host** object as follows:

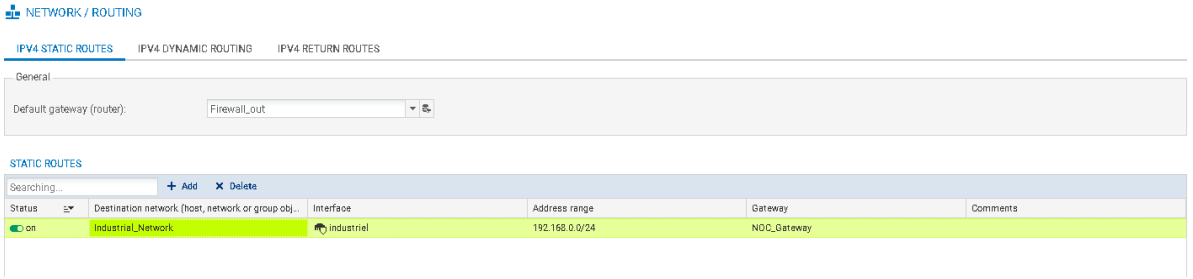


N.B.: For more security, the MAC address of the NOC router could also be specified.

Also add another object of type **Network** as defined below:



Then go to **Configuration > Network > Routing**, to define a new route as below, and apply the changes:



On the network administrator's PC, define the new route via the command line:

route add 192.168.0.0 mask 255.255.255.0 172.16.112.254

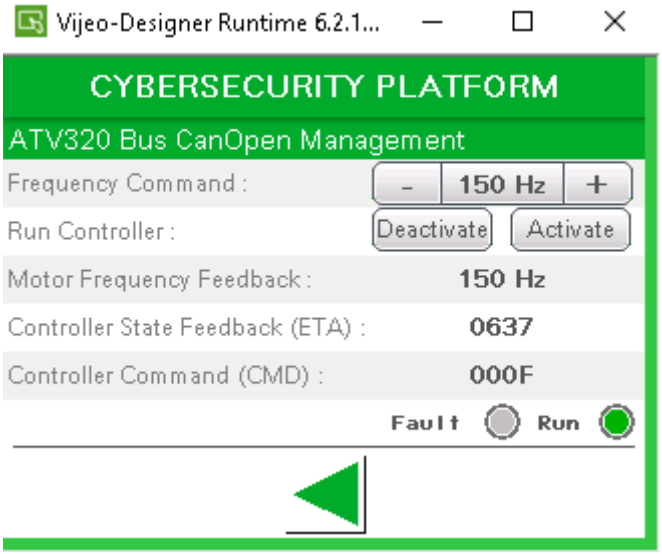
```
C:\Users\Administrateur>route add 192.168.0.0 mask 255.255.255.0 172.16.112.254
 OK!
```

The correct functioning of the route can then be checked through the Sni40 and the NOC gateway:

```
C:\Users\Administrateur>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=63
Reply from 192.168.0.1: bytes=32 time=2ms TTL=63
Reply from 192.168.0.1: bytes=32 time=2ms TTL=63
Reply from 192.168.0.1: bytes=32 time=3ms TTL=63

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

N.B.: The first ping may fail while the routing tables are being updated.

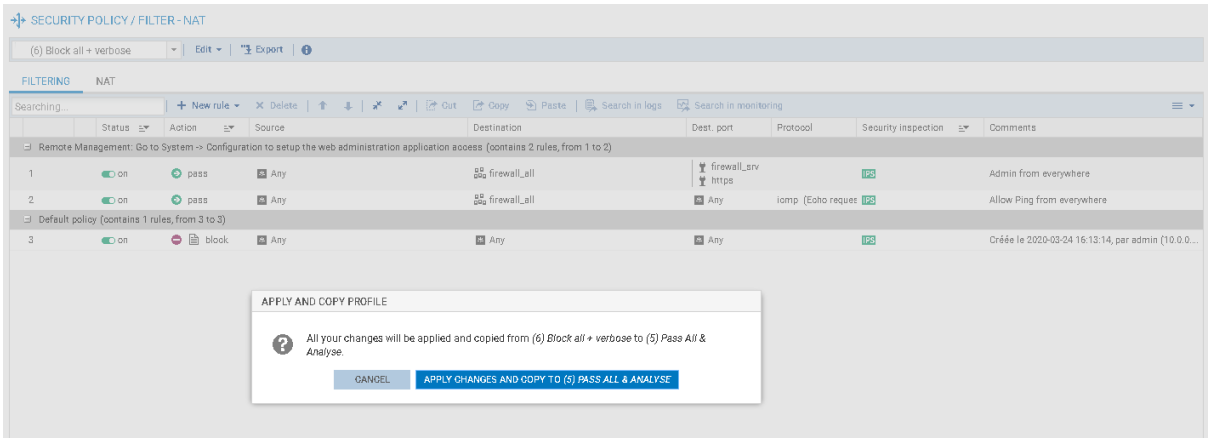
Using Vijeo Designer and the MD1AE58ECYB program, check that the current configuration is working properly by running a simulation:



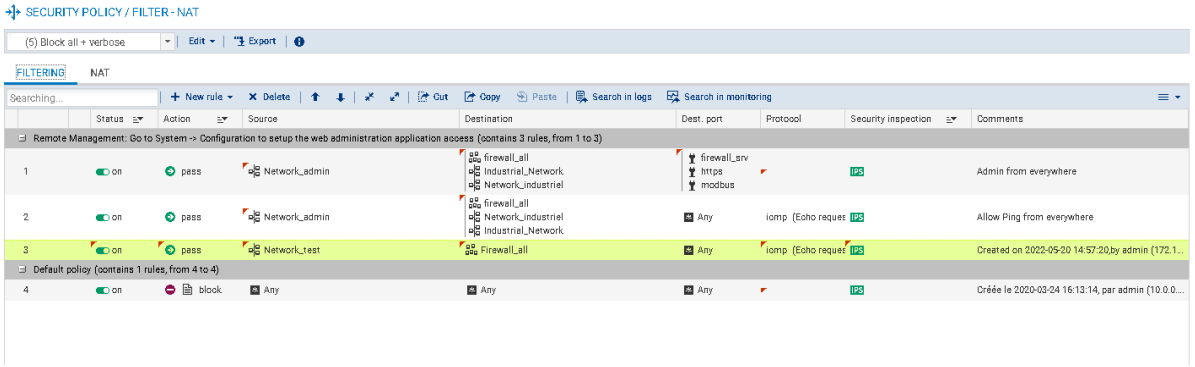
6. Setting up security filtering

At the beginning of the tutorial, the security policy was set to a "pass all" policy which allows all packets to pass. Now that the established configuration is functional, we wish to reinforce security by defining an effective security policy.

To do this, go to the **Configuration > Security Policy > Filter NAT** menu, and select the **(6) Block all+Verbose** policy and then, via the **Edit > Copy to** menu, copy this policy to an available policy (here **(5) Pass All & Analyse.).**



We then go to this policy using the drop-down menu, which is exactly the same as the previous one. The following changes are then made:

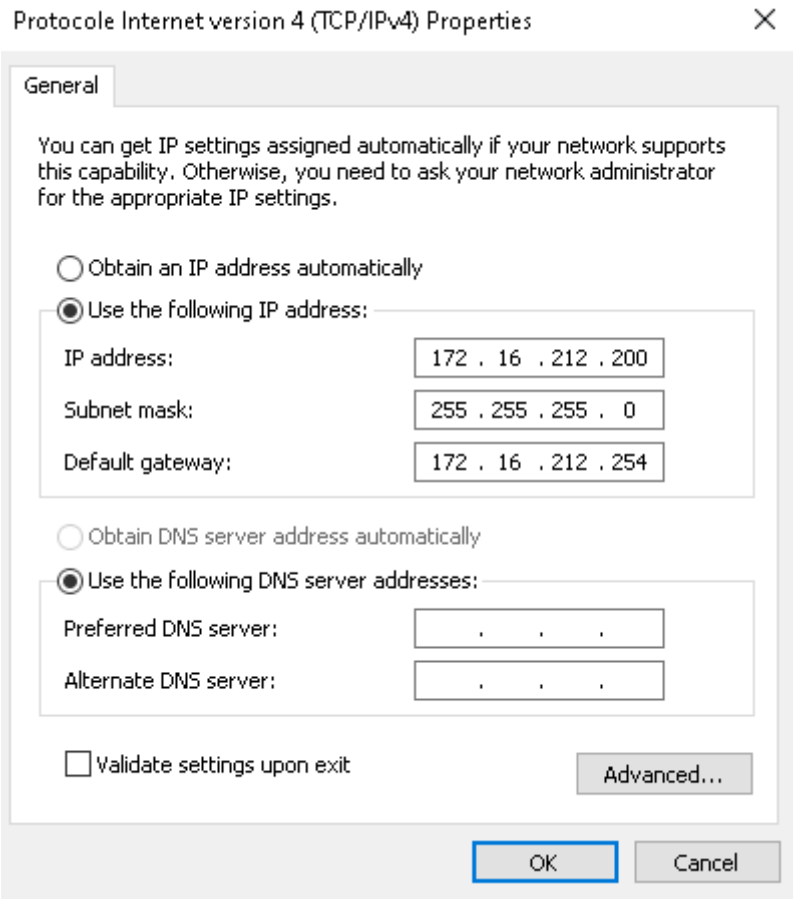


Save and apply this security policy, which establishes the following access rules:

- **Rule 1:** Allow connections from the administrator network to the different gateways of the firewall, as well as to the industrial network, only on the firewall_srv (1300), https (443) and modbus (502) ports.
- **Rule 2:** Allows connections from the administrator network to the various firewall gateways, as well as to the industrial network, for the ICMP request protocol only (protocol used for pings).
- **Rule 3 (optional)**: Allows connections from the test network to the various gateways of the firewall, as well as to the industrial network, for the ICMP request protocol only (protocol used for pings).
- **Rule 4:** Blocks all packets that have not been intercepted by the previous rules.

All rules have an inspection rule set on **IPS**, indicating that every packet passing through these rules will be analysed by the firewall and blocked in case of a security problem.

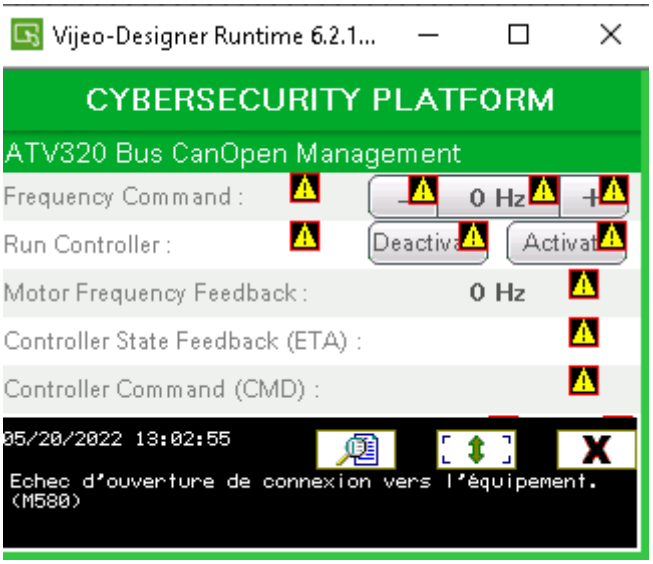
Then connect to port 4 of the firewall corresponding to the previously defined test network, using the following IPv4 configuration:



To verify that the security policy is working, we can start by sending a ping request to the firewall gateway, which is supposed to respond:

```
Pinging 172.16.212.254 with 32 bytes of data:
Reply from 172.16.212.254: bytes=32 time=2ms TTL=64
Reply from 172.16.212.254: bytes=32 time=2ms TTL=64
Reply from 172.16.212.254: bytes=32 time=2ms TTL=64
Reply from 172.16.212.254: bytes=32 time=2ms TTL=64

Ping statistics for 172.16.212.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

However, if you try to connect to the M580 via Vijeo Designer, the connection is refused, showing the effectiveness of the security policy in place:


Vijeo-Designer Runtime 6.2.1...
CYBERSECURITY PLATFORM
ATV320 Bus CanOpen Management
Frequency Command :
0 Hz
Run Controller :
Deactiva
Activat
Motor Frequency Feedback :
0 Hz
Controller State Feedback (ETA) :
Controller Command (CMD) :
05/20/2022 13:02:55
Echec d'ouverture de connexion vers l'équipement.
(M580)