TP2 - IT Cybersecurity - Flow Analysis

Operational objectives :

- Understand the operational philosophy of the SNi40 Firewall, with the objective of analysing and identifying flows between the Supervisory Control Station and the Automation System.
- Be able to configure the SNi40 firewall in Block All vs Pass All + Analyse mode
- Be able to implement the RealTime Monitor software to render in Wireshark the details of the Modbus frames exchanged
- Be able to isolate and interpret the details of a Modbus read or write request

Prerequisites:

- Master the basic operations of Control Expert
- Be able to run Vijeo Designer in simulation mode
- Understand the basic structure of a Modbus frame and its main functions

The issue at hand:

- Configure an SNi40 Firewall to allow logging and analysis of data flows between the Control Station and the Automation System.

Resources :

- Manufacturer's documentation
  - Schneider Electric (site web)
  - Stormshield : SNS - User and Configuration Manual
- Specific documentation
  - Architectures Maquette Cybersec 28-05-2019.pptx
- Applications made available for this exercise:
  - M580 Application (Control Expert) : cybersec_M580 called md1ae58ecyb.stu
  - HMI application (Vijeo Designer) : cybersec_IHM called MD1AE58ECYB
  - Default SNi40 Firewall configuration file (SNI40-TP2-0.na)
- Software provided, to be installed on the working PC (console) for the realisation of this TP:
  - Control Expert (Schneider Electric) : Programmation Automate Schneider Electric M340, M580, …
  - Vijeo Designer V6.2 SP8: Magelis HMI Application Design (execution including in Simulation mode on the Workstation)
  - Web Gate Client (Schneider Electric): complement to Vijeo Designer [option]. (remote client of the Magelis HMI, running in an Internet browser)
  - Internet Explorer : Microsoft's 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
  - RealTime Monitor (Stormshield): redirection to Wireshark of frames captured by the SNi40

Evaluation criteria :

	😀	😐	😟
Connecting the SNi40			
Setting up a Block All security policy			
Configuration of a Pass All security policy			
Setting up a Pass All + Analyse security policy			
Handling the RealTime Monitor + Wireshark software			
Interpreting the details of a Modbus read or write request			
Autonomy - Quality of work/restitution			

Time spent :	2 h	**Objective(s) :**		Comment(s) :
Evaluation :	/ 20	Reached(s)	Not reached	

TP2 - Network flow analysis

The implementation of the Stormshield SNi40 is intended to increase the cyber security defence capabilities against external attacks on the automation system.

The course of this TP will involve successively :

- The SNi40 connection between the ePAC M580 (Ethernet DIO port of the CPU) and the Workstation.

  The latter will behave as a client towards the ePAC, in particular by displaying a supervision station by means of an Internet browser which allows the Webgate of the HMI.

  The SNi40 Firewall will first have a default filtering configuration, and it will be seen that all the exchanges are blocked, reads as well as writes of data on the ePAC: nothing will work any more. (This is intended to draw the user's attention to the fact that, by default, the behaviour of the platform is modified simply because of the insertion of the SNi40 Firewall)

- The configuration and adoption of a Security Policy (Block & Trace All) offering a first level of analysis (logging) will then take place, such that the entire flow emitted from the Control Network will be considered from the outset to be blocked, while maintaining the transit of the administration flow.
- The configuration and adoption of a new Security Policy (Pass & Trace All) offering a first level of analysis (logging) will then take place, such that the entire flow emitted from the Control Network will be considered from the outset to be authorised.
- This behaviour will then be modulated to allow detailed packet analysis of the frames targeting the M580 ePAC, e.g. those Modbus frames operating in write mode. This will require, in addition to maintaining the global authorisation previously given, specifically blocking these Modbus write functions. This will decide the production of as many events, whose packets will be requested to be captured. In the end, however, the transit authorisation of these targeted frames will be maintained.

  Thus, in the end, no request will be blocked, but we will have captured and archived in the firewall, for later analysis, the frame packets for which we wish to proceed with a detailed analysis.

- The behaviour of the motor controlled by the variable speed drive will be modified by changing the speed setpoint from the simulated HMI application on the Workstation. We will be particularly interested in the detail of the restitution of the exchanged frames - via the RealTime Monitor + Wireshark software - corresponding to these modifications of setpoint operated on the ePAC M580.
- This test sequence will be replayed with a separation of networks: Control Network vs Devices Network. This time the SNi40 firewall will not be connected to an Ethernet DIO port on the CPU module, but to an Ethernet DIO port on the BME NOC 0321 module. The elements present on the 'Control' network will be registered in the 172.16.12.0 addressing domain, while those present on the 'Devices' network will be registered in the 192.168.0.0 addressing domain (i.e. the same as before).

1. Using the documents provided (see Cybersec Model Architectures document), identify and comment on the various components of the target architecture, in accordance with the Phase 2 and Phase 4 architecture diagram, in comparison with the Phase 1 and Phase 3 architectures, respectively, discussed in TP1. In particular, identify and comment on the front panel ports of the SNi40 box.
2. First, install the Ethernet cables on the board in accordance with the Phase 1 architecture.
3. Load the M580 PLC with the default application program (cybersec_M580 called md1ae58ecyb.stu), which does not involve filtering on services or filtering on the IP addresses of accessors.

   NB: the HMI is loaded with the Vijeo Designer application (cybersec_IHM called MD1AE58ECYB)

   Check the access to the drive speed setpoint modification, first from the local HMI, then from an Internet Browser requesting the HMI IP address (Web Gate client), and then from Control Expert (address %MW1014).

4. Modify the placement of the Ethernet cables on the board to comply with the Phase 2 architecture.
5. The SNi40 Firewall must be configured as a bridge by default.

   We will first check the accessibility of the Firewall, and after connecting to it, we will proceed to the setting of the minimum authentication time.

   Check that the serial number of the unit matches and align the time with that of the workstation, in accordance with the Europe/Paris time zone. If the time zone is modified, the SNi40 will, after validation of this modification, start an automatic reboot sequence.

   In particular, check also that the SNi40 is allocated an IP address that corresponds to the cut-off network (i.e. the network on which this SNi40 is installed)

CAUTION: If the Ethernet cabling to the SNi40 is modified, it is advisable to turn off/on the test board. Indeed, connecting a machine on the external interface of the Firewall and then on an internal interface of the same Firewall will be interpreted by the latter as an attempt to usurp the IP address of the bridge and consequently, it will block all traffic generated by this machine. The firewall will then have to be restarted to unblock this situation.

6. The configuration considered at this stage for the SNi40 does not currently call for any specific filtering (security policy not including any particular filtering rule).

   Ensure that all exchanges through the SNi40 firewall are blocked.

   Result: Nothing works anymore in the relationship between the Workstation (PLC programming/loading applications, Webgate application on the HMI) and the Process Level (PLC and peripheral elements). This is intended to draw the user's attention to the fact that by default, the platform's behaviour is modified simply because of the insertion of the SNi40 firewall.

Demonstrate this by using the Wireshark utility, which can operate even from the Workstation, as well as on the Trace Station.

(As a reminder, both the CPU Service Port and the NOC 0321 BME Module Service Port mirror the flows on the other ports of the CPU vs NOC Module, respectively).

7. Modify the security policy in place in the SNi40 firewall configuration or adopt a new security policy for the SNi40 box, which continues to block exchanges (except for the admission of transit of administration flows), while logging events (blocking logging).

   Provide an assessment of the strategy used so far for the characterisation of exchanges.

8. Now adopt a new security policy for the SNi40 firewall configuration that allows the entire flow to pass. Check the effectiveness of this policy, for example by observing the behaviour of the Webgate application on the HMI.
9. Modify this security policy to require, in addition to the passage of the flow, the logging of exchanges with a view to their analysis.

   Provide an assessment of the strategy used so far for the characterisation of exchanges.

10. Complement the previous policy by ensuring that, with respect to the type of frames targeted (e.g. Modbus write functions) and for which a detailed analysis is desired, these are defined as prohibited, and therefore interpreted as events, but nevertheless allowed to transit.

    By configuring these event-generating frames as justifying the capture of their packets, the details of these frames will be available, which can be exploited by means of the Stormshield Real Time Monitor software, coupled with the Wireshark software.

11. To carry out now a test sequence identical to the sequence carried out until now (points 1 to 10) by considering specifically the Phase 4 Architecture, i.e. by accessing the ePAC - through the SNi40 firewall - not directly via an Ethernet CPU port (DIO), but via an Ethernet port (DIO) of the BME NOC 0321 coupler installed on the rack of this ePAC. (See document Architectures Cybersec model)

    (Focus on the transpose of step 11)

    Note: The workstation (as well as the observation station) will be assigned a new IP address - see document Architectures Cybersec Model.pptx - which is supposed to correspond to the addressing domain of the 'Control Network', while the 'devices' will remain in the previous addressing domain, supposed to be that of the 'Device Network'. Consequently, the workstation (as well as the observation station) will have to be initialised with a route command to designate the 'internal' IP address of the NOC coupler to the PC as the access point to the Device Network.

    Provide a short summary of the scope of the Modbus502, HTTP vs. FTP clients, depending on whether the target IP address is the main port of the M580 CPU or the external address of the BME NOC 0321 coupler.

Note: The BME coupler service port N0C 0321, as well as the M580 CPU service port, is configured in mirror mode by the M580 application program, to allow all traffic passing through the other coupler or CPU ports to be restored if required.

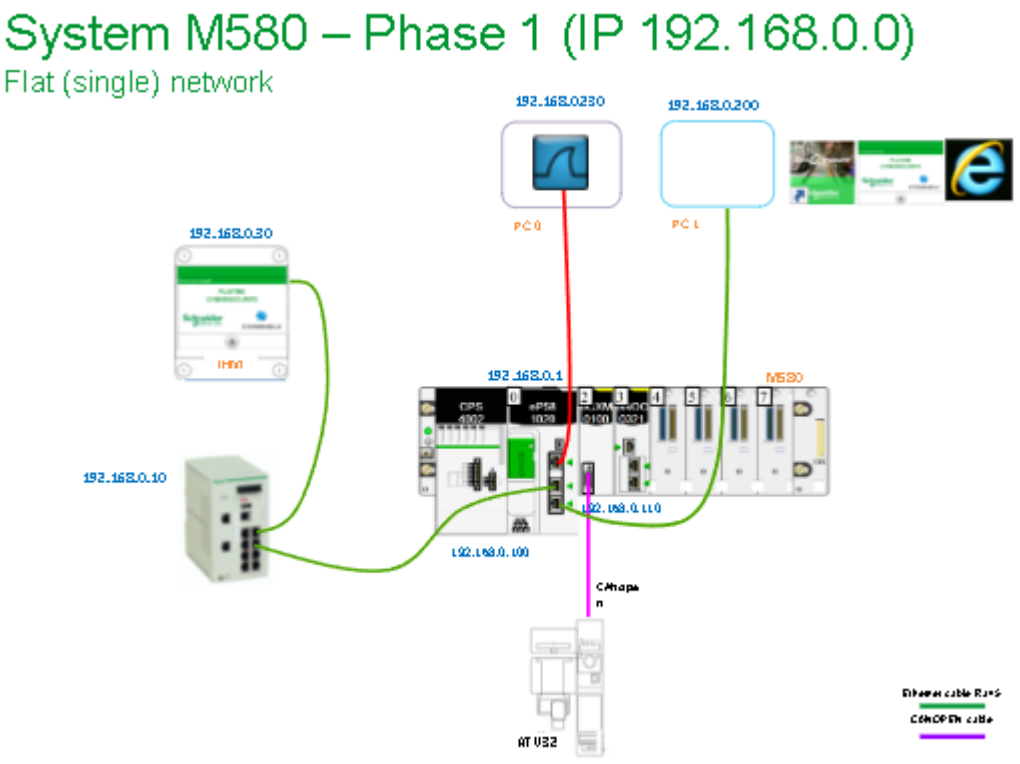
Details of expected operations

1. **Components of the target architectures / SNi40 front panel ports**

   (See document " Architectures Maquette Cybersec.pptx ")

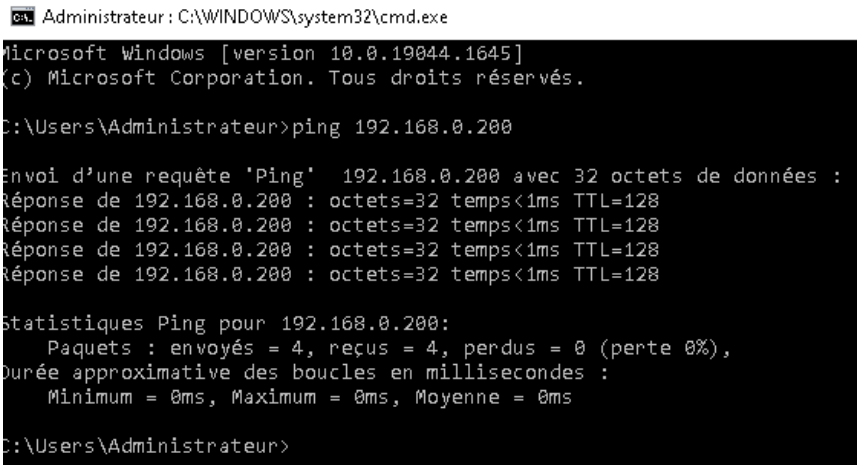
   - Identification and commentary on the components of the target architecture (Phases 1 / 2 / 3 / 4)
   - Identification and commentary on the Sni40 front panel ports

2. **Installation of Ethernet cables according to the Phase 1 architecture**



3. **Loading the program with the default application (cybersec_M580)**
   3.1. Checking the IP address of the workstation

Check the IP address of your workstation on your local (wired) network with a **PING: 192.168.0.200**



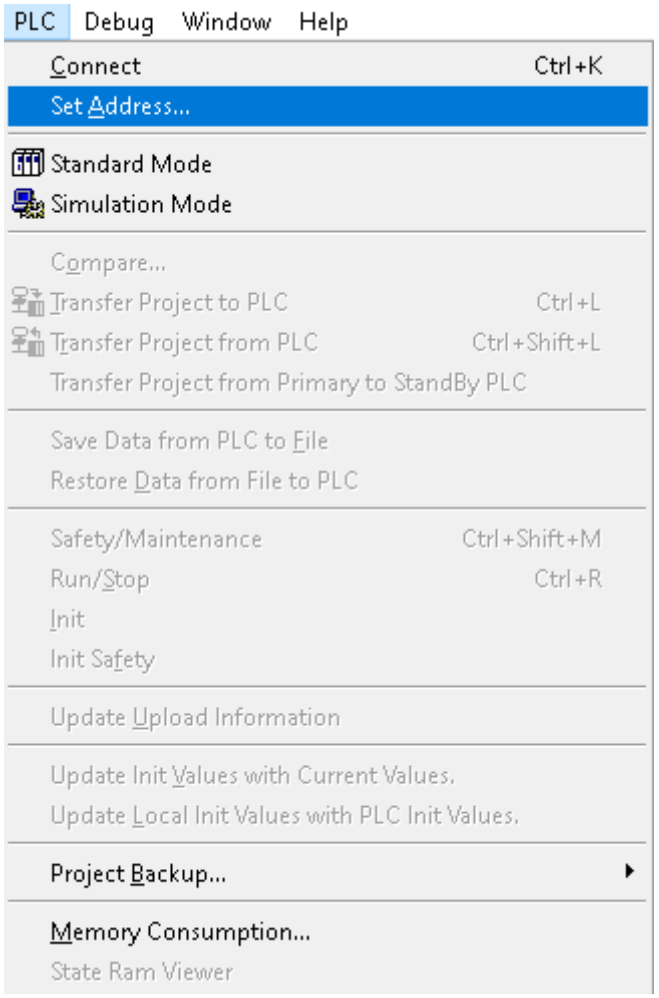
3.2. Checking the IP address of the M580 ePAC

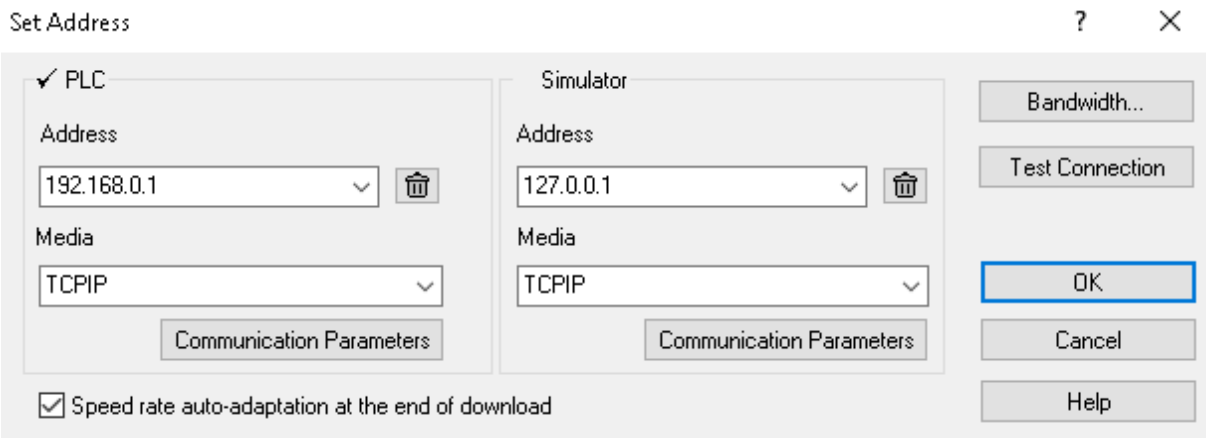
Before wiring the SNi40, make sure that the ePAC/M580 (main address **192.168.0.1**) is accessible by means of a **PING**

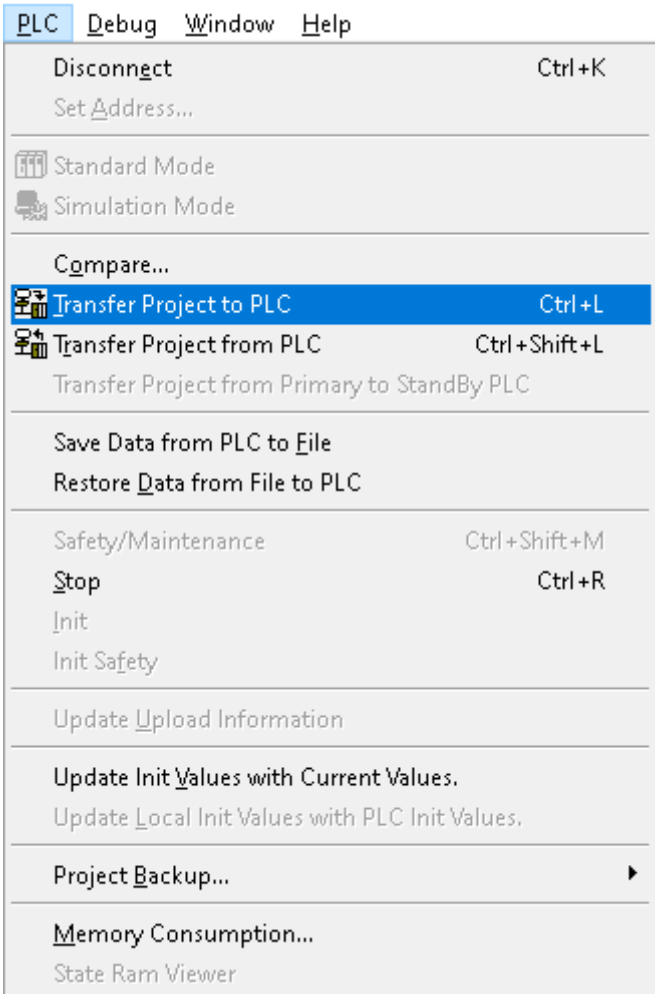
```
C:\Users\Administrateur>ping 192.168.0.1

Envoi d'une requête 'Ping'  192.168.0.1 avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps=4 ms TTL=64
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=64

Statistiques Ping pour 192.168.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 4ms, Moyenne = 2ms
```

3.3. Reloading the PLC program (optional)

Using the Control Expert software, reload (if necessary) the ePAC M580 with the application program (cybersec_M580 called md1ae58ecyb.stu), free of any protocol/service limitation and address filtering (using if possible the Ethernet link --- main address **192.168.0.1**) or alternatively the USB link


PLC
Debug
Window
Help
Connect Ctrl+K
Set Address...
Standard Mode
Simulation Mode
Compare...
Transfer Project to PLC Ctrl+L
Transfer Project from PLC Ctrl+Shift+L
Transfer Project from Primary to StandBy PLC
Save Data from PLC to File
Restore Data from File to PLC
Safety/Maintenance Ctrl+Shift+M
Run/Stop Ctrl+R
Init
Init Safety
Update Upload Information
Update Init Values with Current Values.
Update Local Init Values with PLC Init Values.
Project Backup...
Memory Consumption...
State Ram Viewer

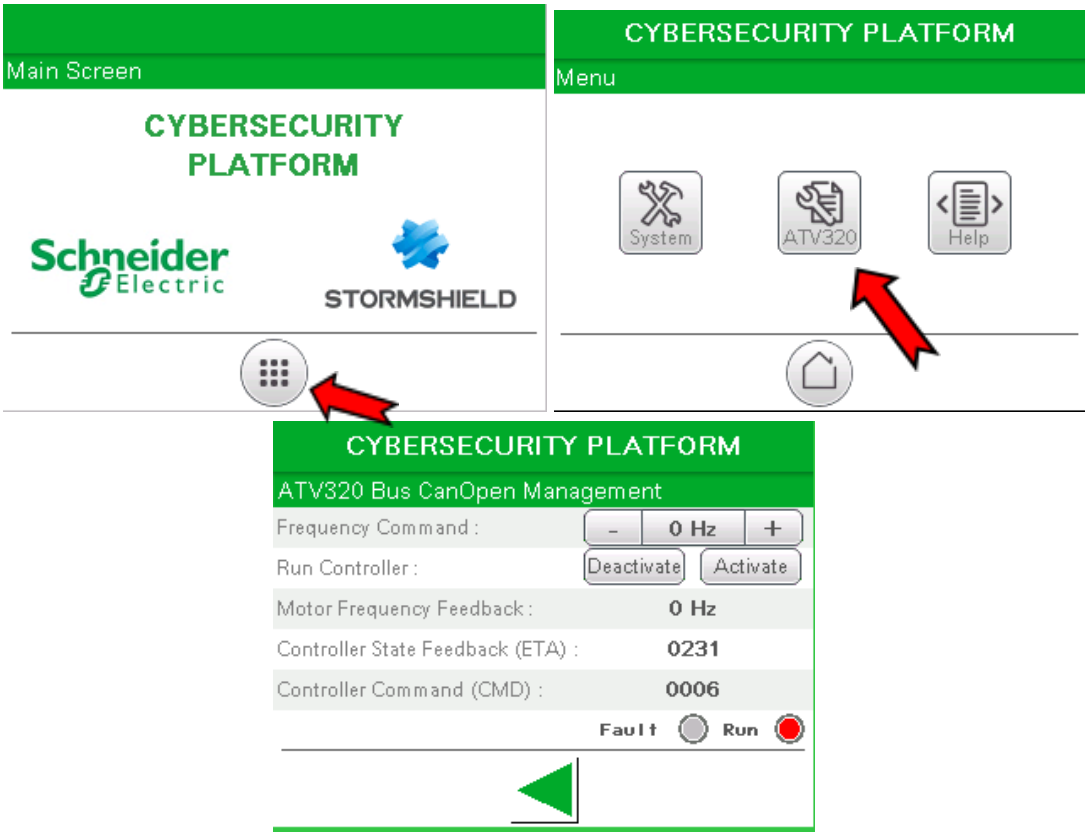

Set Address
PLC
Address
192.168.0.1
Media
TCPIP
Communication Parameters
Simulator
Address
127.0.0.1
Media
TCPIP
Communication Parameters
Bandwidth...
Test Connection
OK
Cancel
Help
Speed rate auto-adaptation at the end of download



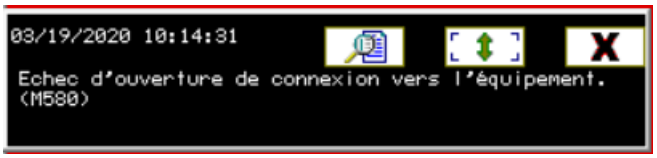
At the end of this loading, put the automaton in **RUN.**

3.4. Checking the accessibility of the ePAC for the HMI

- From the HMI, go to the drive control view

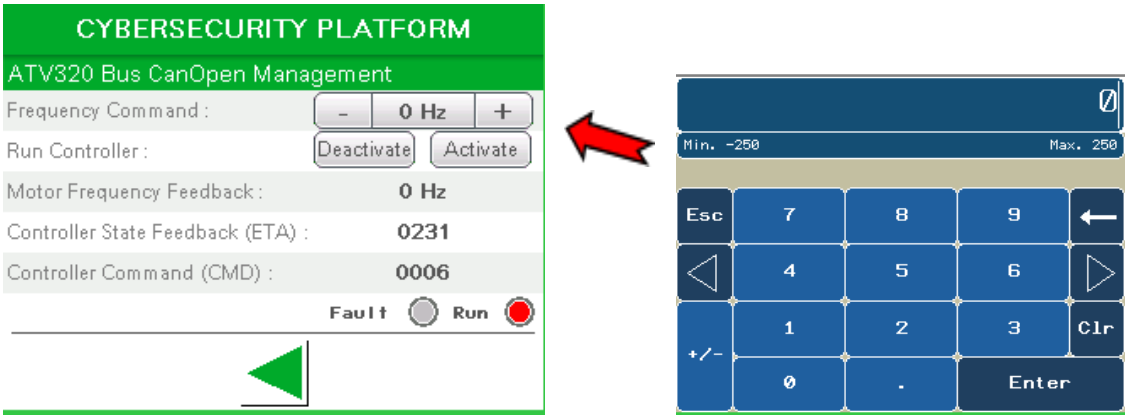


NOTE: If the ePAC is inaccessible, the base of the HMI display will show a message like :

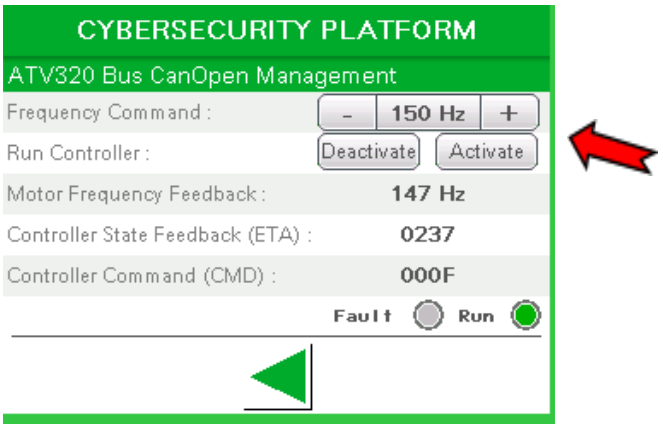


If this error occurs, check the wiring. If necessary, check the HMI and ePAC applications

- Changing the speed setpoint



- Start the engine by pressing the "Activate" button, and ensure that the engine is running.



Play with the speed setpoint and check that the motor speed matches the setpoint.

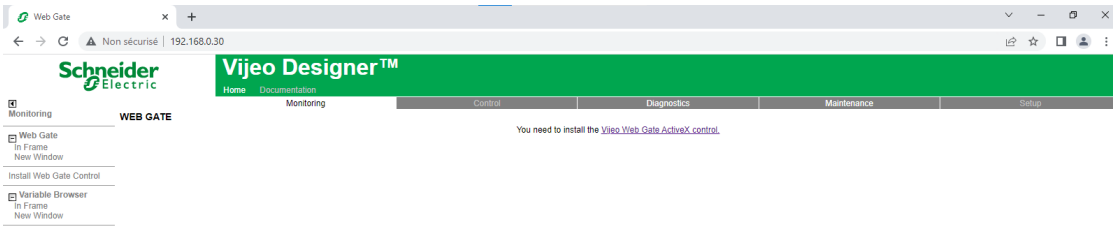
- Switch off the engine by pressing the "Disable" button, and ensure that the engine is stopped.

3.5. Verification of ePAC accessibility for the Web Gate replica of the HMI

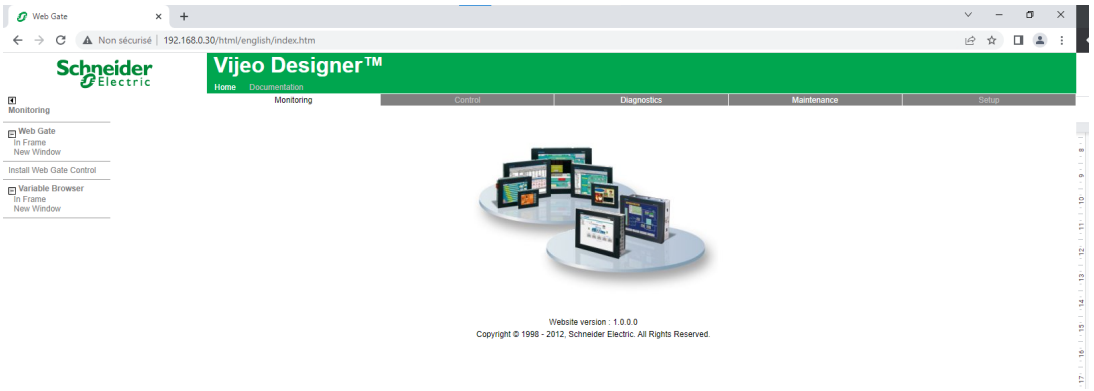
Proceed in the same way, using a Web Gate access of the HMI on the workstation through an Internet Browser (Internet Explorer).

- Change the PC screen resolution to 800x600
- Install "**Web_Gate_Client_Files_6.2_SP8**" available in the "Software" folder in “Web Gate”
- Open Internet Explorer (do not use another browser) and enter the address of the HMI (**192.168.0.30**) in the address bar.

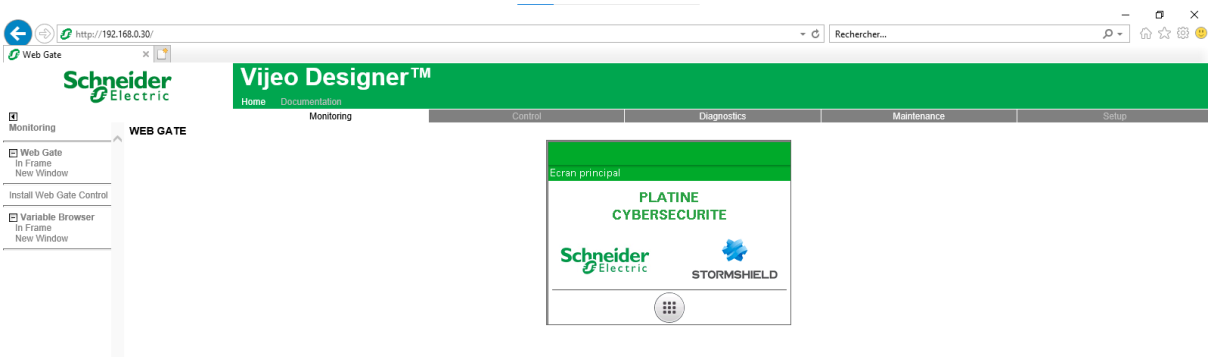
  Validate if necessary the Vijeo Web Gate add-on (Allow)



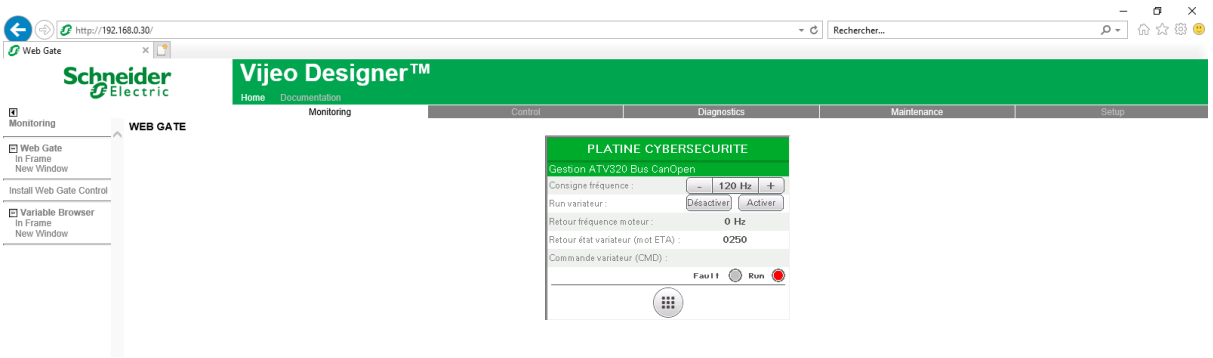
- Select the English language

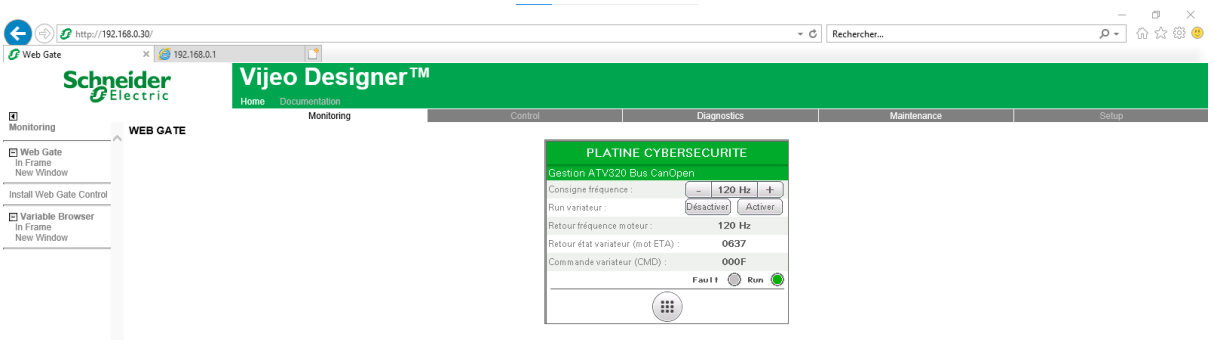


- Then click on the Visualization tab and then on the entry Webgate | In Frame to display the HMI screens.



- Proceed as on the HMI to reach the drive control screen

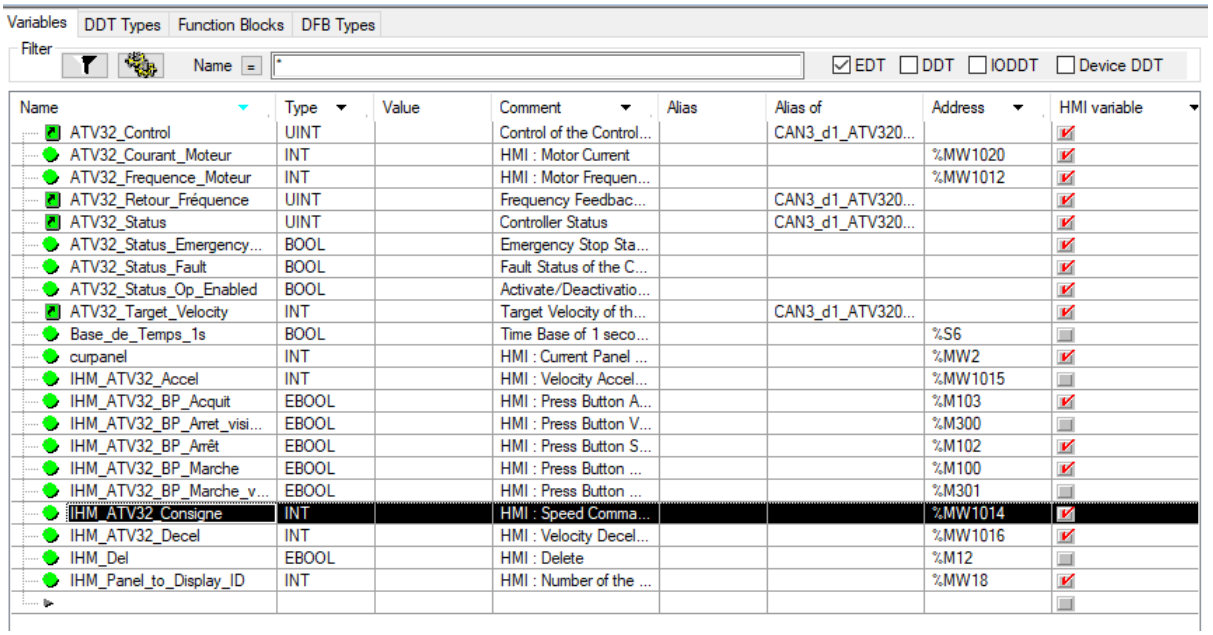




NOTE: the commands operated from WebGate will, within the framework of this practical work, only be effectively taken into account if this view is simultaneously displayed on the HMI

3.6. Verification of ePAC accessibility for Vijeo Designer in Simulation Mode

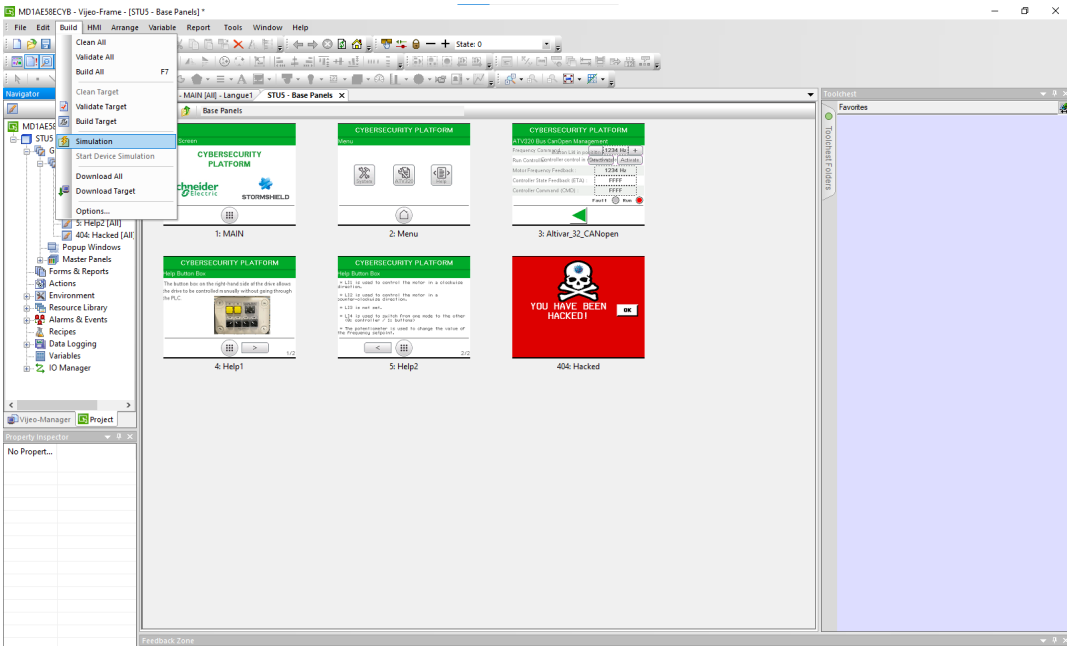
- First check with Control Expert, through an Animation Table, the possibility to read/write the speed setpoint value of the drive, i.e. the possibility to read/write the variable HMI_ATV32_Setpoint (%MW1014)



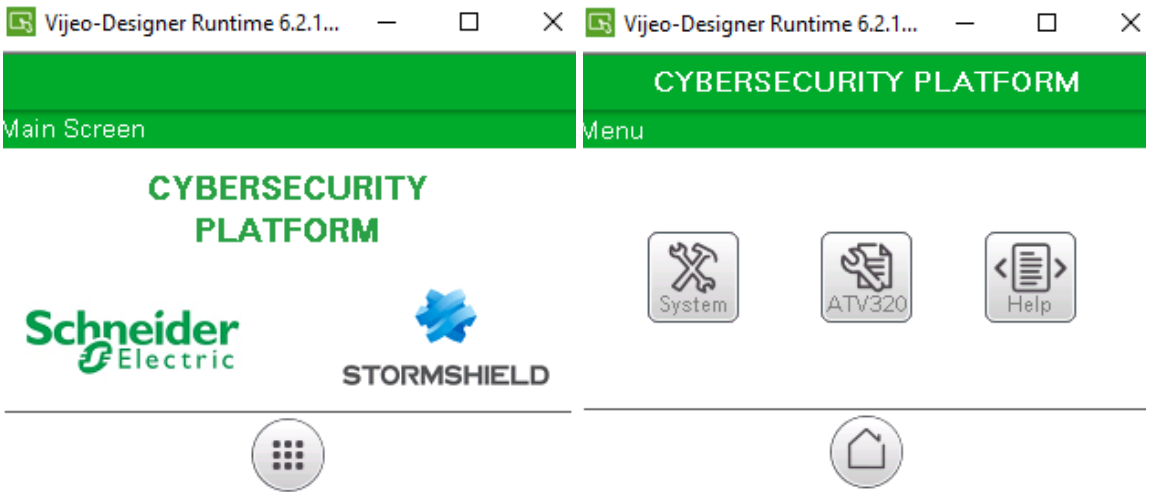
Name	Type	Value	Comment	Alias	Alias of	Address	HMI variable
ATV32_Control	UINT		Control of the Control...		CAN3_d1_ATV320...		
ATV32_Courant_Moteur	INT		HMI : Motor Current			%MW1020	
ATV32_Frequence_Moteur	INT		HMI : Motor Frequen...			%MW1012	
ATV32_Retour_Fréquence	UINT		Frequency Feedbac...		CAN3_d1_ATV320...		
ATV32_Status	UINT		Controller Status		CAN3_d1_ATV320...		
ATV32_Status_Emergency...	BOOL		Emergency Stop Sta...				
ATV32_Status_Fault	BOOL		Fault Status of the C...				
ATV32_Status_Op_Enabled	BOOL		Activate/Deactivatio...				
ATV32_Target_Velocity	INT		Target Velocity of th...		CAN3_d1_ATV320...		
Base_de_Temps_1s	BOOL		Time Base of 1 seco...			%S6	
curpanel	INT		HMI : Current Panel ...			%MW2	
IHM_ATV32_Accel	INT		HMI : Velocity Accel...			%MW1015	
IHM_ATV32_BP_Acquit	EBOOL		HMI : Press Button A...			%M103	
IHM_ATV32_BP_Arret_visi...	EBOOL		HMI : Press Button V...			%M300	
IHM_ATV32_BP_Arrêt	EBOOL		HMI : Press Button S...			%M102	
IHM_ATV32_BP_Marche	EBOOL		HMI : Press Button ...			%M100	
IHM_ATV32_BP_Marche_v...	EBOOL		HMI : Press Button ...			%M301	
IHM_ATV32_Consigne	INT		HMI : Speed Comma...			%MW1014	
IHM_ATV32_Decel	INT		HMI : Velocity Decel...			%MW1016	
IHM_Del	EBOOL		HMI : Delete			%M12	
IHM_Panel_to_Display_ID	INT		HMI : Number of the ...			%MW18	

- Also, ensure that the ePAC (main address 192.168.0.1) is accessible via a Modbus request. Check that a read access to the word %MW1014 (which corresponds to the drive speed setpoint address) gives the same value as the one identified via Control Expert.

  Use the Vijeo designer application, running in Simulation mode on the working PC

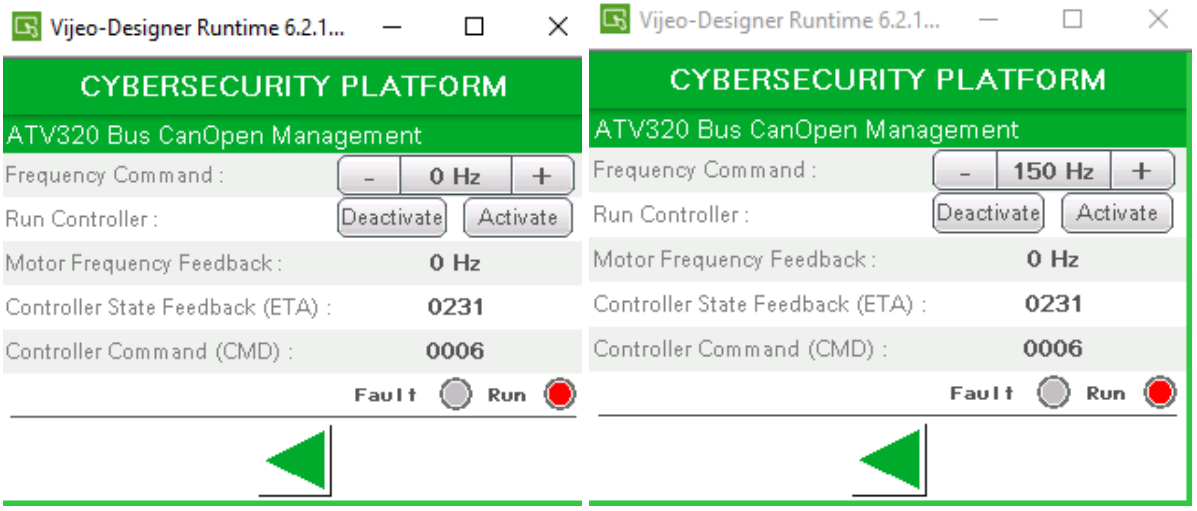


- The welcome screen displayed by the simulator is as follows:



- Click on the ATV32 button.

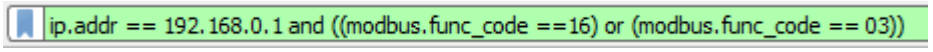
  Proceed as on the HMI to control the drive

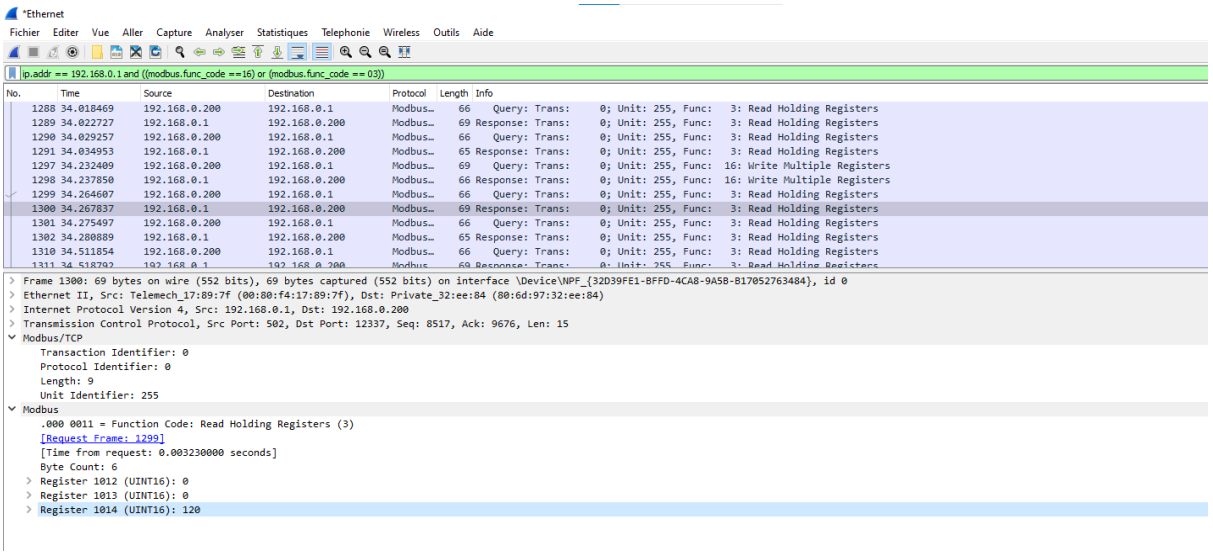


- Check via Wireshark, that Modbus/TCP frames are exchanged between the Workstation and the M580 CPU.

  We are going to filter all the frames captured by this expression:

  ip.addr == 192.168.0.1 and ((modbus.func_code ==16) or (modbus.func_code == 03))

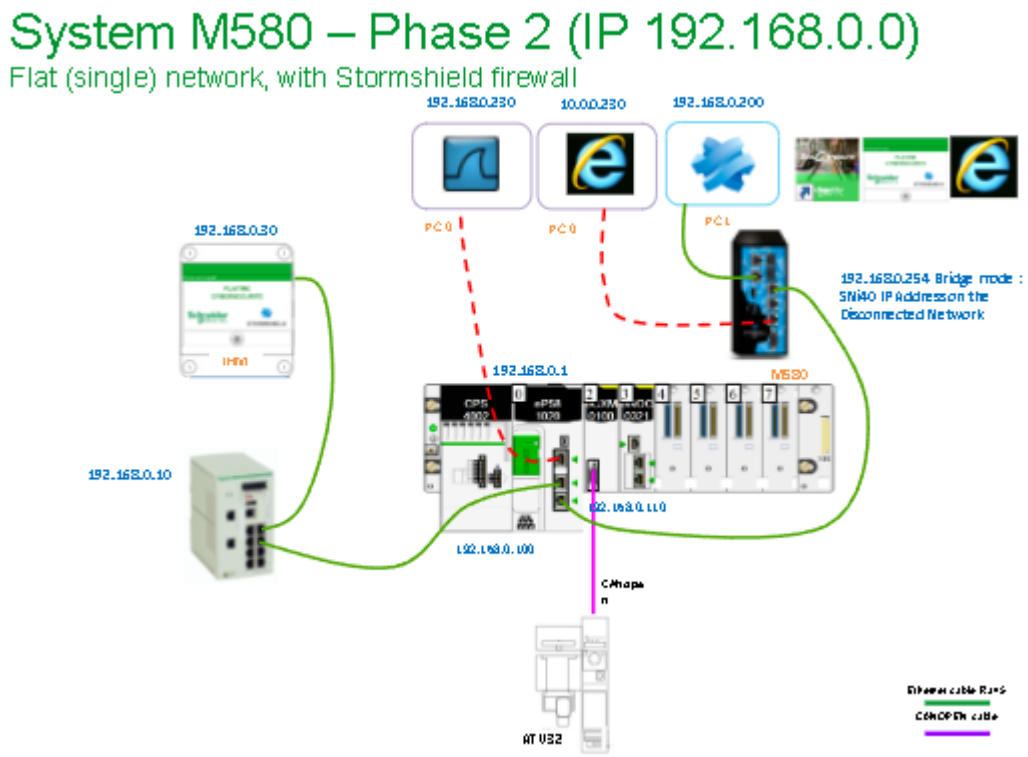




Example: cyclic multiple register read frames (function code 03) and specific multiple register write frames (function code 16)

- Discontinue the Vijeo Designer Simulation after use.

4. Installation of Ethernet cables according to the Phase 2 architecture



5. Configuring the Sni40 Firewall in Bridge Mode

5.1. Accessibility of the SNi40

On PC0, set the Ethernet port

IP address: **10.20.0.230**

Subnet mask: **255.255.255.0**

Connect PC0 to interface 5 of the Sni40 and check that the SNi40 is accessible by means of a PING

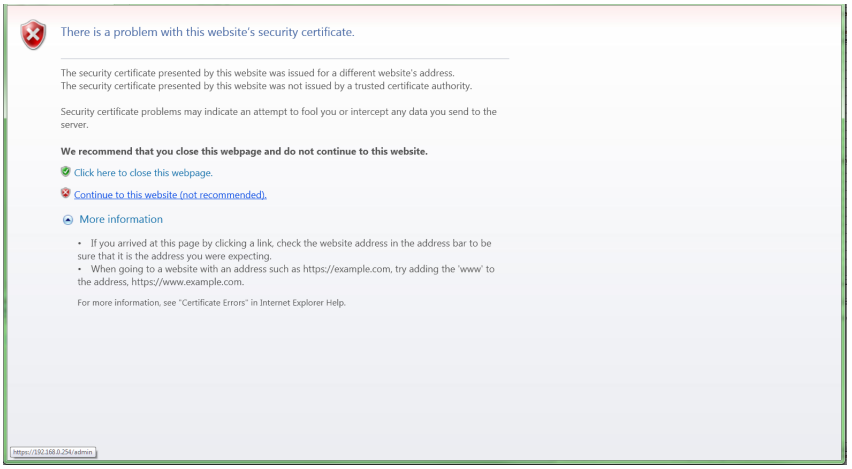
```
C:\Users\Administrateur>ping 10.20.0.254

Envoi d'une requête 'Ping'  10.20.0.254 avec 32 octets de données :
Réponse de 10.20.0.254 : octets=32 temps=2 ms TTL=64
Réponse de 10.20.0.254 : octets=32 temps=2 ms TTL=64
Réponse de 10.20.0.254 : octets=32 temps=2 ms TTL=64
Réponse de 10.20.0.254 : octets=32 temps=2 ms TTL=64

Statistiques Ping pour 10.20.0.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms

C:\Users\Administrateur>
```

5.2. Connection to the SNi40

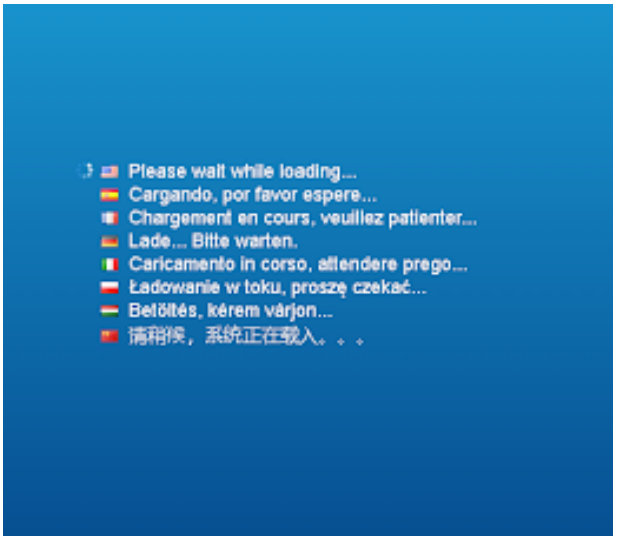
- Open an Internet Browser (e.g. Internet Explorer) and connect to the SNi40, address 10.0.0.254

  https://10.0.0.254/admin

  If necessary, override the reporting of a certificate problem

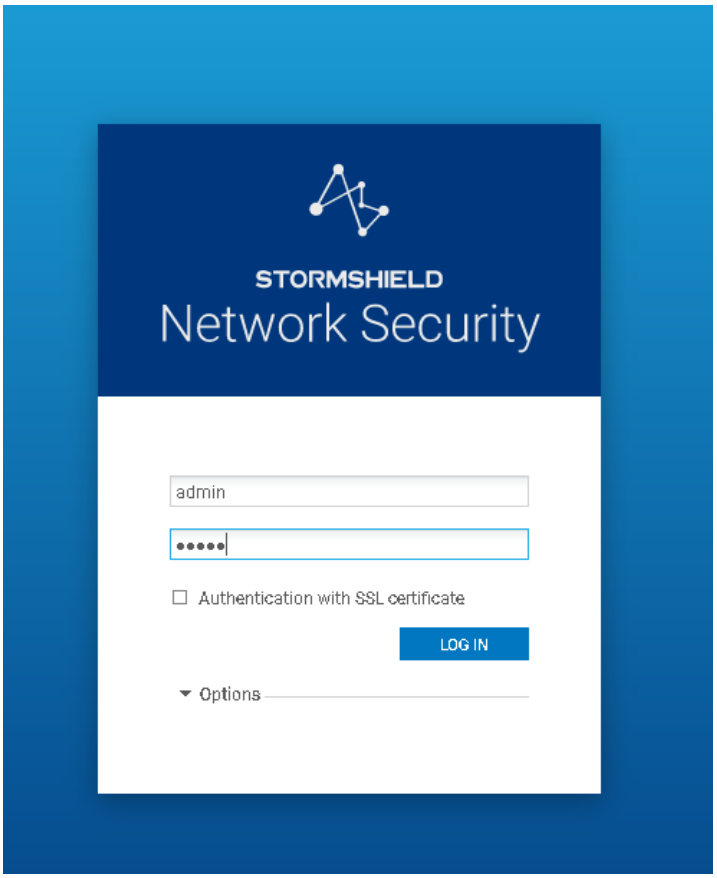


- The SNi40 Home screen is then automatically displayed



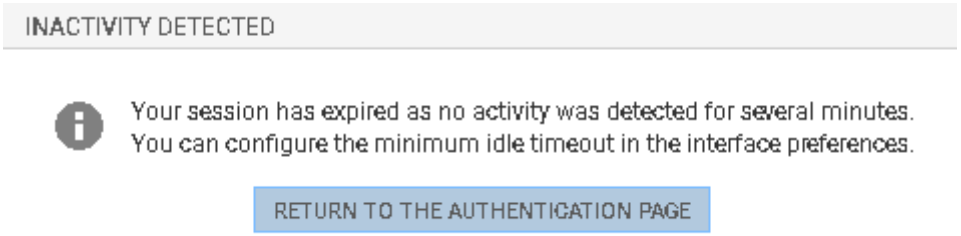
5.3. Authentication

- Authenticate with default ID and Password, i.e. admin and admin



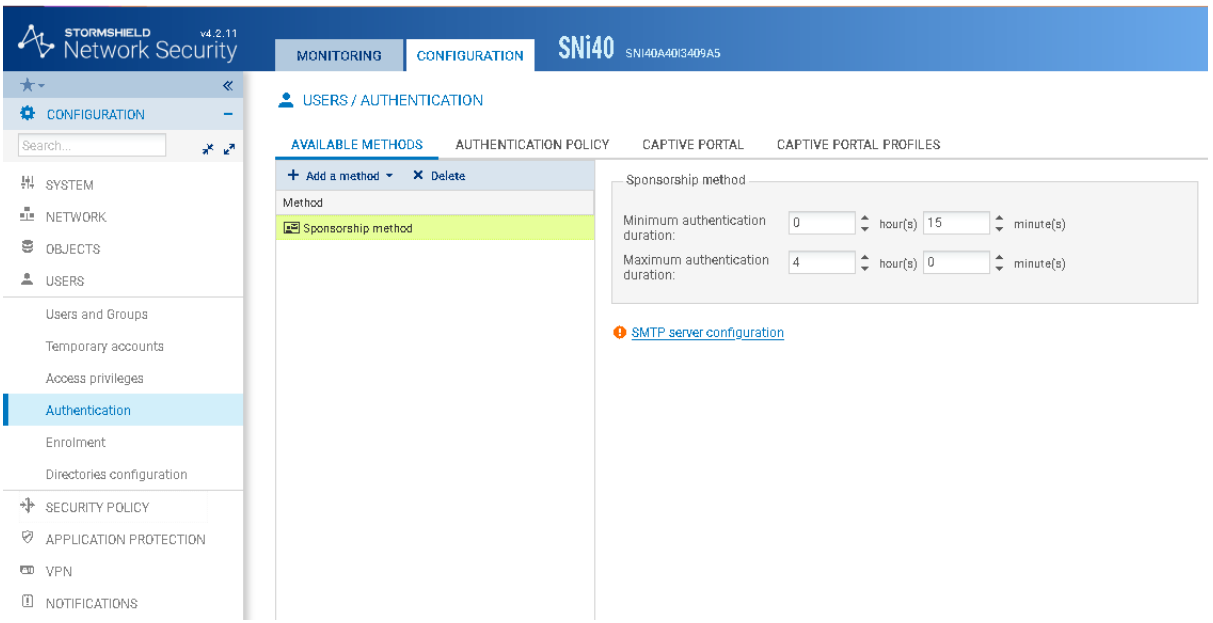
5.4. Setting the duration of a connection on the SNi40 before requesting confirmation (option)

For security purposes, the SNi40 GUI in the browser periodically returns to the identification screen.



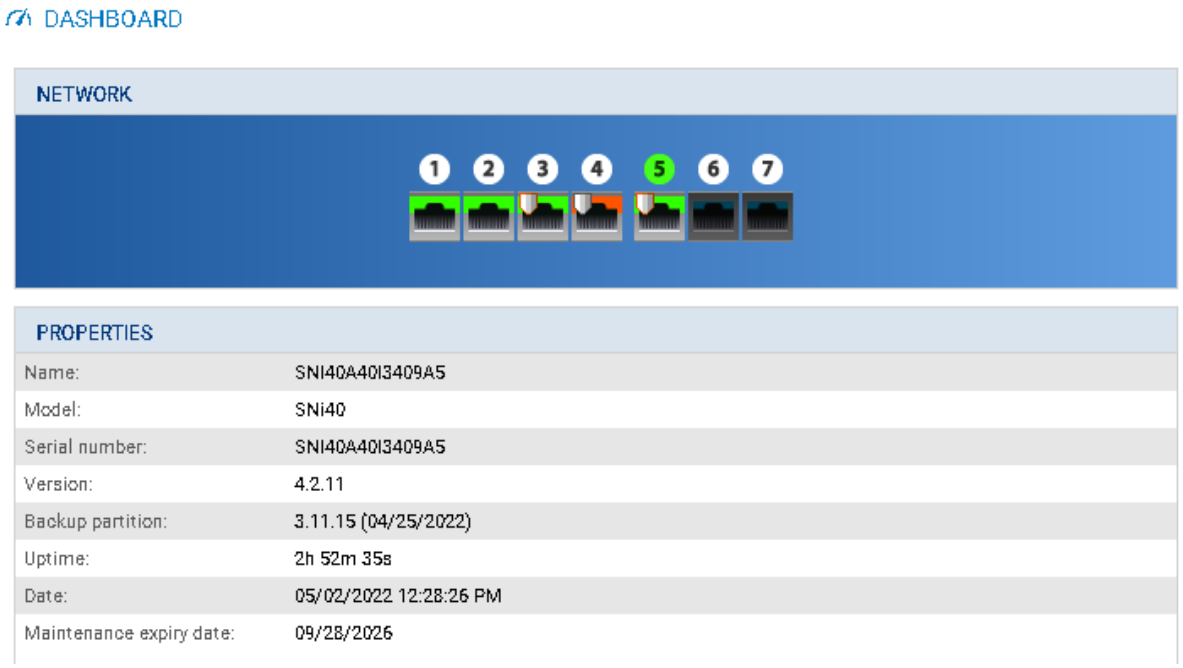
The method (by default, the so-called sponsorship method) dictating this identification and the associated renewal period can be decided.

- Go to the USERS sub-menu, Authentication section. Specify the minimum duration desired and validate.



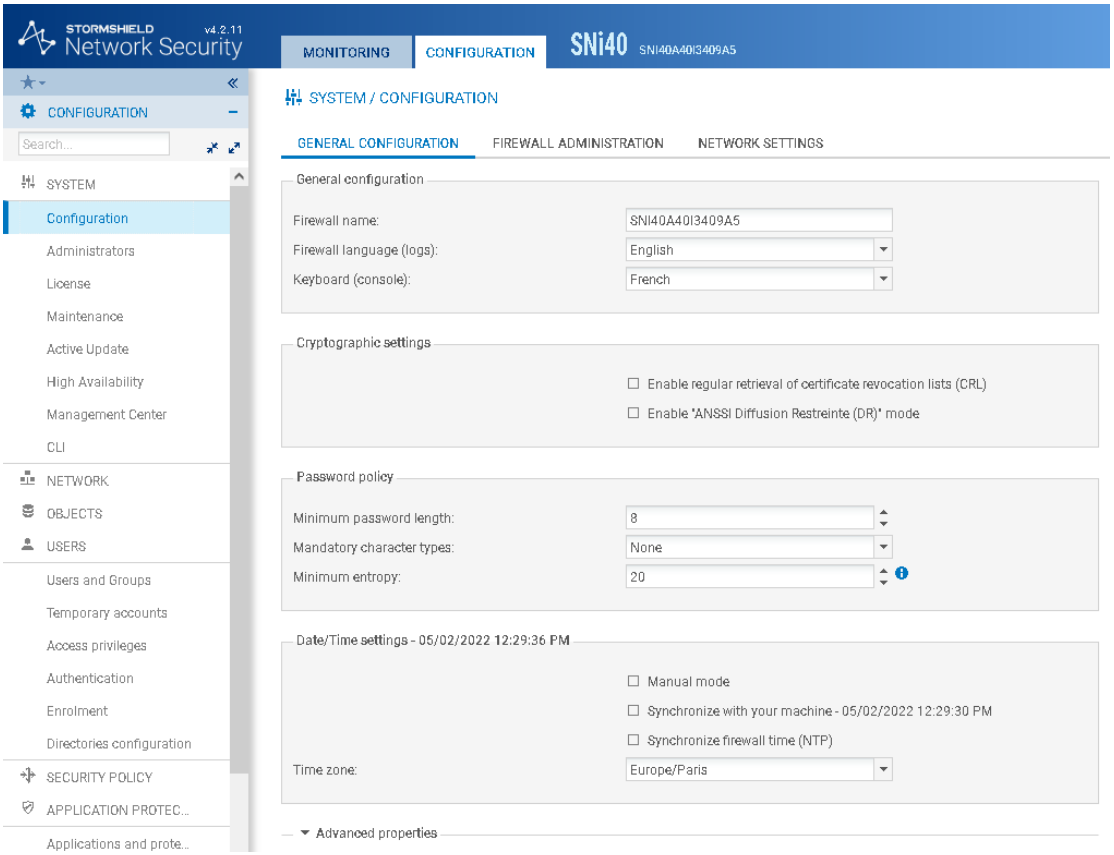
5.5. Checking the SNi40 Serial Number match (optional)

- Check that the serial number on the dashboard matches the one on the side of the Stormshield SNi40



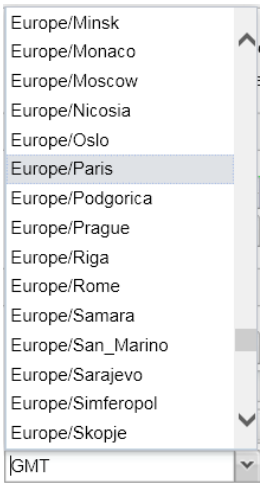
5.6. Aligning the SNi40 time stamp with the PC time stamp

- Expand the SYSTEM submenu and then click on the Configuration entry



- In the lower part of the screen, (data and time settings section), click on the Synchronise with your machine button (option)

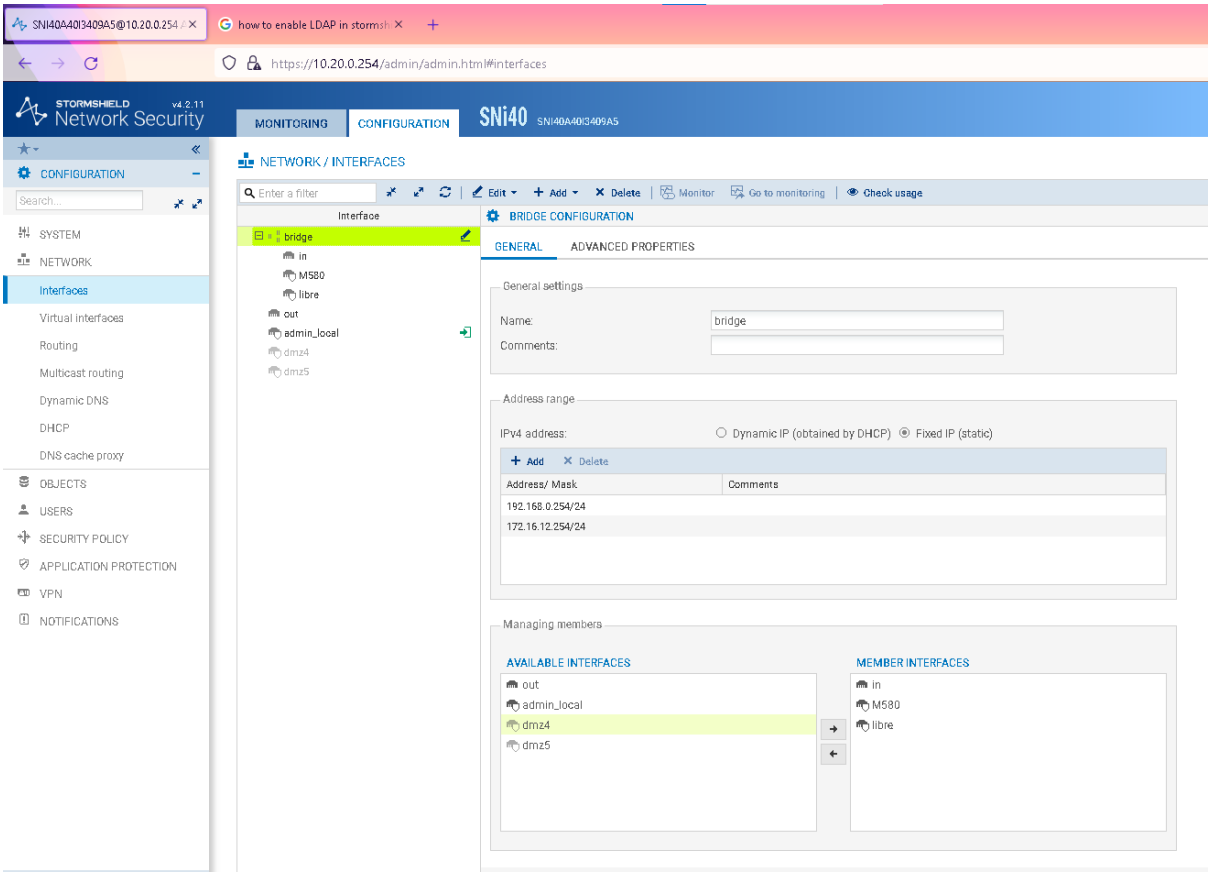
NB: it is preferable to select the time of the local time zone rather than GMT



5.7. Configuring the SNi40 as a Bridge

Here we will check that the SNi40 in question is configured as a Bridge (i.e. as an Intelligent Switch)

- Go to the CONFIGURATION menu and select the NETWORK sub-menu, heading Interfaces.

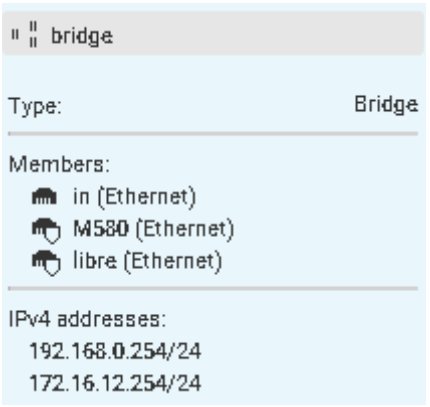


NB: check here that the IP address to which the SNi40 responds is compatible with the network currently cut by this SNi40.

Example: IP address 192.168.0.254 allocated to the network 192.168.0.0

- We can even anticipate here the cut-off of the 172.16.12.0 network, which will occur in Phase 4.

  To do this, we must add an IP address, in this case: 172.16.12.254

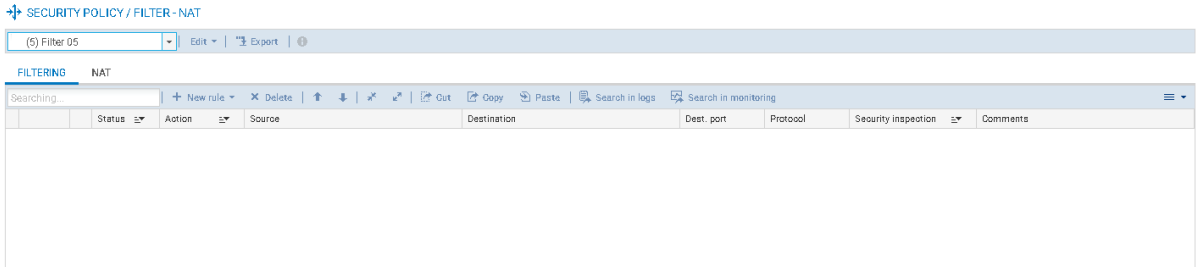


6. Configuration of SNi40 without a specific filtering rule

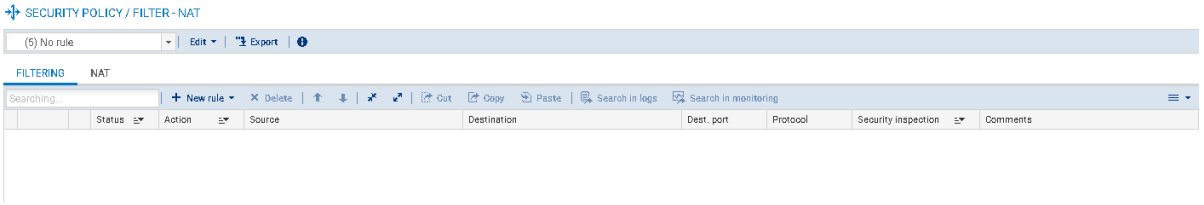
Here we are interested in whether the SNi40 in question complies with the "security policy" decided upon (SECURITY POLICY sub-menu, Filtering and NAT section)

The first step is to check that it is easy to block all the frames passing through the SNi40.

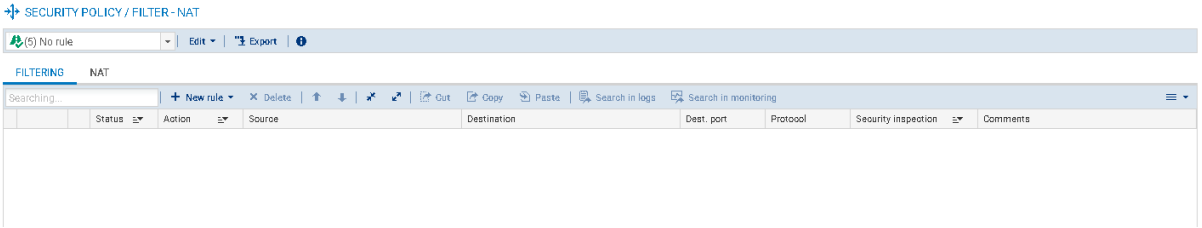
- Select an undefined policy (e.g. Policy Filter_05) from the list in the top left-hand corner of the central area of the screen.



- If necessary, rename this policy "No Rule", for example

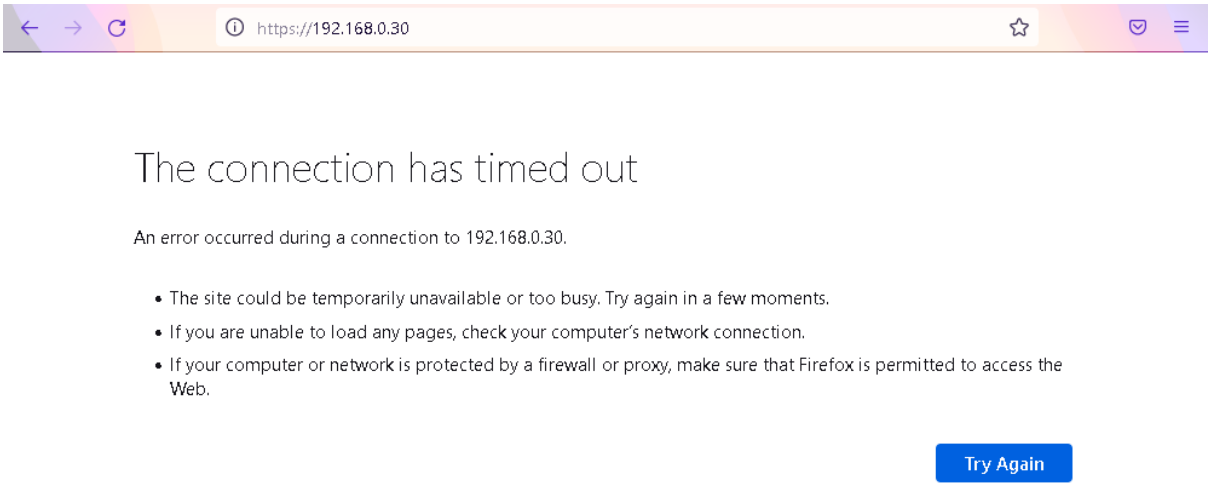


- Click on the Activate this policy command

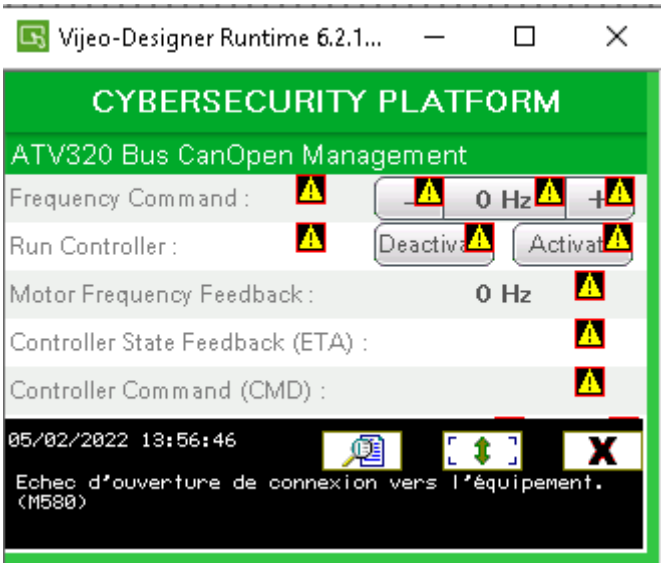


Note: The symbol  refers to the Active Security Policy

We will normally check that nothing is passing through the SNi40 and that, for example, the HMI Web Gate service cannot be accessed.



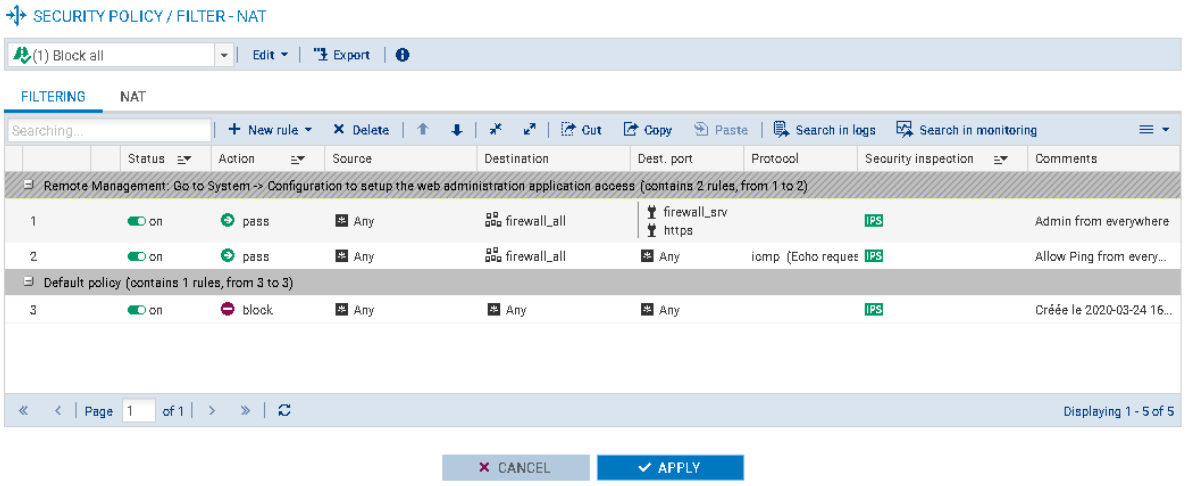
Similarly, we check that the Vijeo Designer Simulation is not able to access the M580 PLC.



7. Configuring the SNi40 in Block All mode with Logging

We will now reconsider the policy adopted, which, like the previous one, aims to block all traffic, except for administration traffic, but also to trace the frames blocked by the SNi40.

- Call the first policy "(1) Block All", in the list of available security policies, (CONFIGURATION menu, SECURITY POLICY sub-menu, Filtering and NAT section),



Note that this policy has 3 rules:

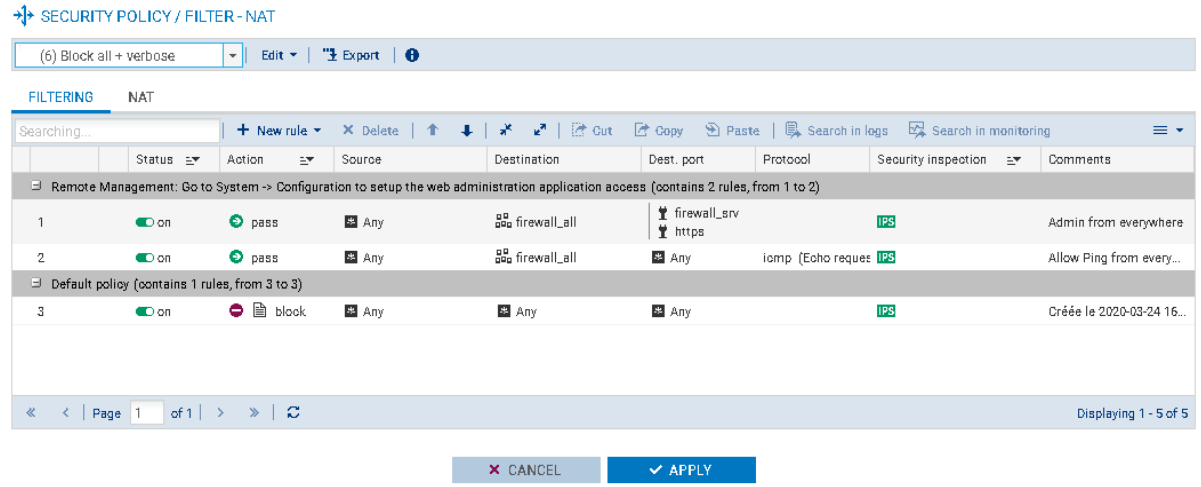
- The first two rules are derived from the SNi40 setup (see menu SYSTEM | Configuration)

  The first two rules are derived from the SNi40 setup (see SYSTEM menu | Configuration) and allow the reception/transit of requests dedicated to the Firewall Service as well as HTTPS frames to the Firewall, and ICMP requests (PING), all destinations.

- The third rule is the rule that will be applied by default, and will block all frames that escape the administration (see first 2 rules) but the exchanges are not recorded to be analysed.
  - ➢ Important note: for all the proposed exercises, the filtering policies "(1) Block all" and "(10) Pass all" must not be modified.

    In the drop-down list, policies 5 to 9 will be used for the exercises.

- Call policy "(6) Block All + verbose", from the list of available security policies



- Click on the "Activate this policy" button
- When you go, a moment after having validated this policy, to the menu LOGS AUDIT LOGS, submenu LOGS - LOGS, heading Filtering, you will see the logged exchanges
- When the Anonymized indication appears in the Source Name column, you can right click on the Restricted Access to Logs link in the top banner.

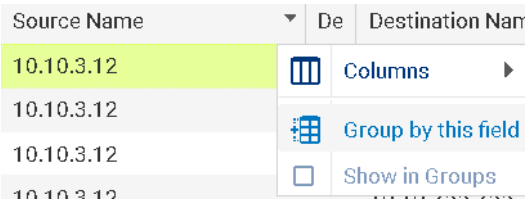
Then, after refreshing the screen (

), you get a screen like the following, which shows the IP addresses of the 'sources' in clear text

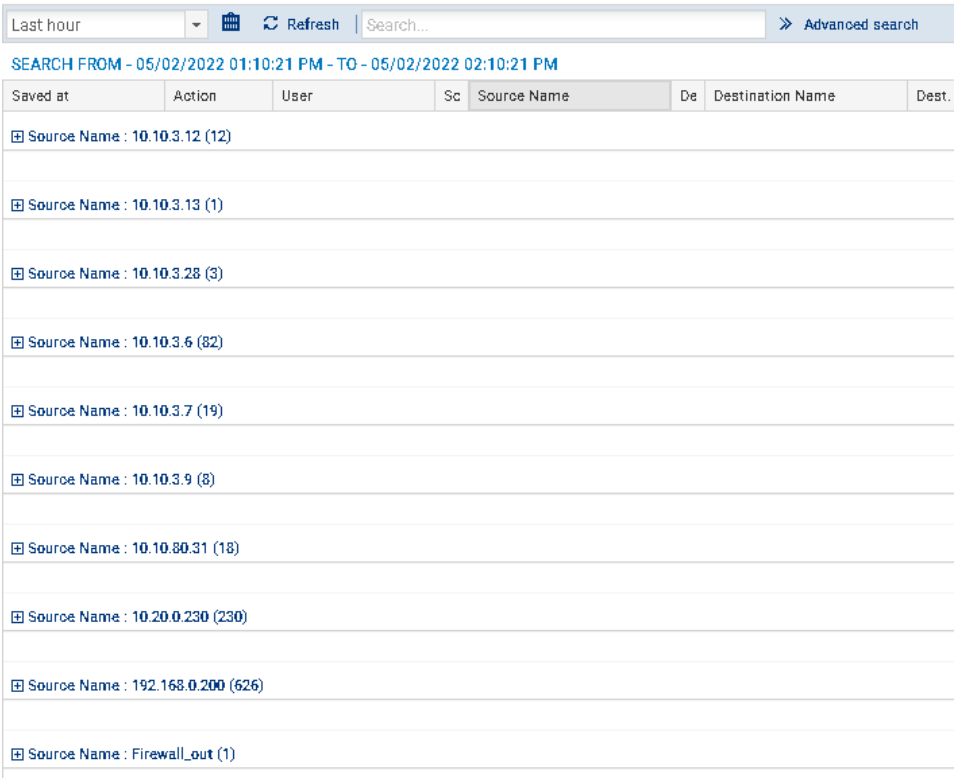
NB : 

As long as the indication of the possible stop (refresh) command in the upper banner is visible, this means that the screen refresh is in progress. Wait or stop.

- Right-click on the selection list at the top of the Source Name column and click on the Group this field choice

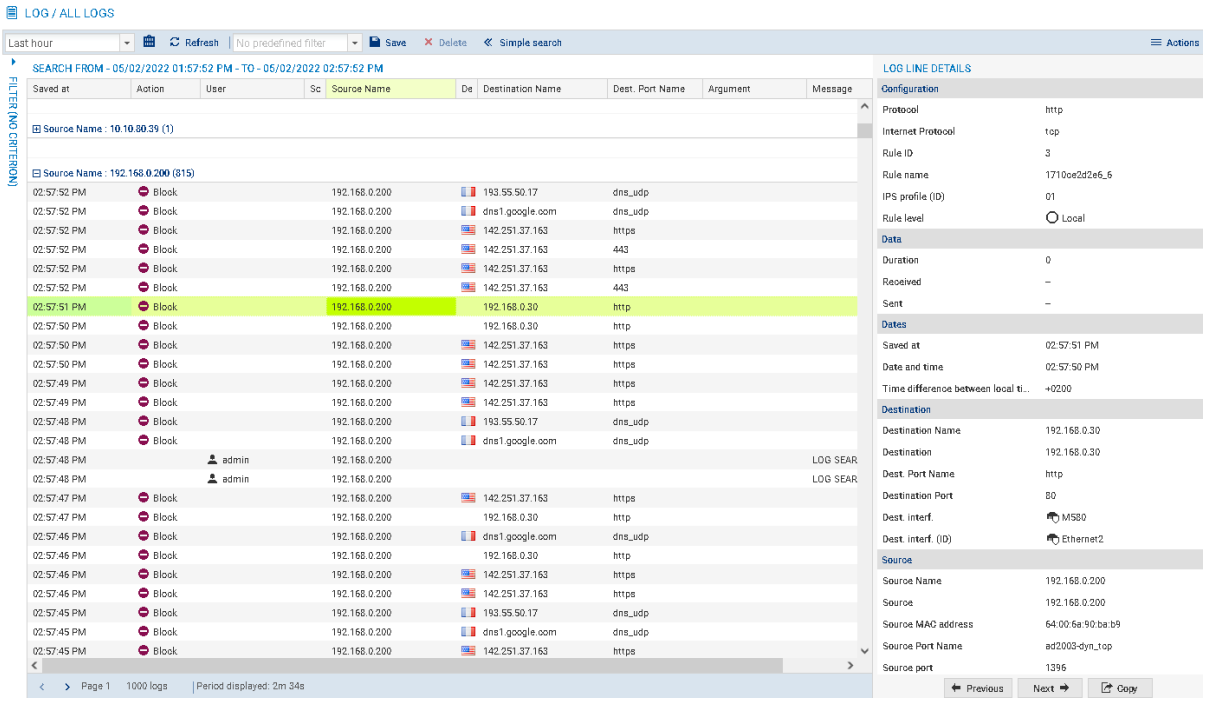


The display then shows the result of a group sort



- We can 'unfold' this or that group to look at its contents.

  For example, the snapshot below shows the characterisation of a frame passed between the 192.168.0.200 device (the PC) and the 192.168.0.30 device (the HMI) (traffic a priori produced by the Web Gate application)



The result of this manipulation is that, due to the (almost) complete blocking of traffic, no application exchange flow transits through the SNi40 firewall. However, the firewall, with regard to this configuration (Block & Trace All), records these blockages and provides a summary report.

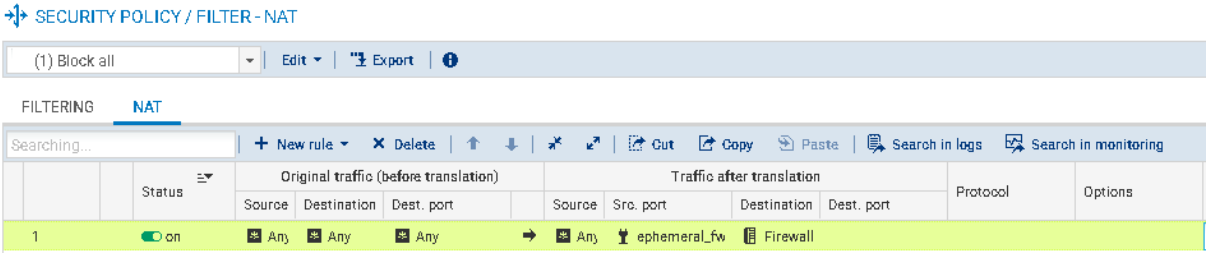
However, in order to have a mode of restitution likely to lend itself to an analysis of the details of the frames, it will be necessary to seek another strategy.

8. Configuring the SNi40 in Pass All mode

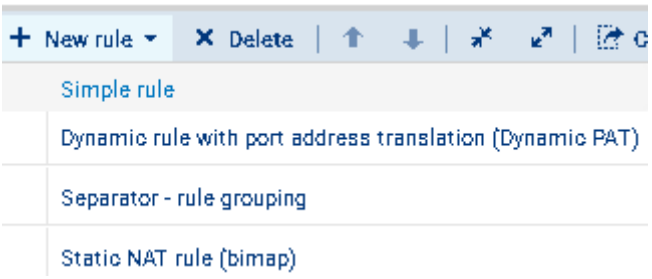
Following the conclusions of the previous manipulations, we will now try to consider a new policy, conforming to the basic rule of letting all traffic pass through the SNi40.

- Call the policy "(7) Pass All", from the list of available security policies,

To delete a rule, select it (the background will change to pale green) and press the Delete key



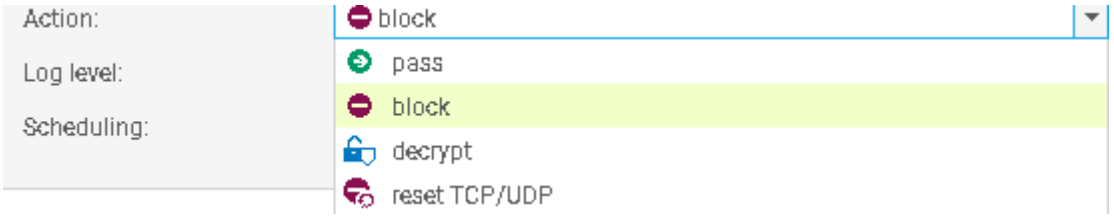
- If you have a policy without any rules, click on the New Rule command on the menu visible under the FILTERING tab.



- Then click on Simple Rule

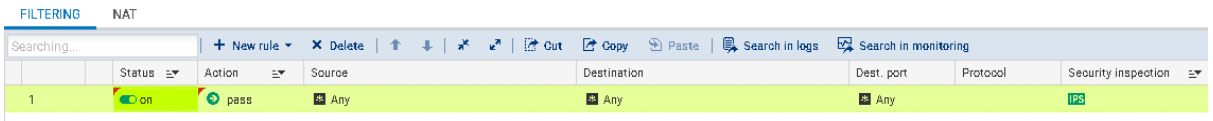
  This install a new default rule, where all exchanges are blocked

- We now need to refine this rule. Since we want to let everything through, we will modify the desired action via the selector accessible at the top of the Action column. Select Set pass action



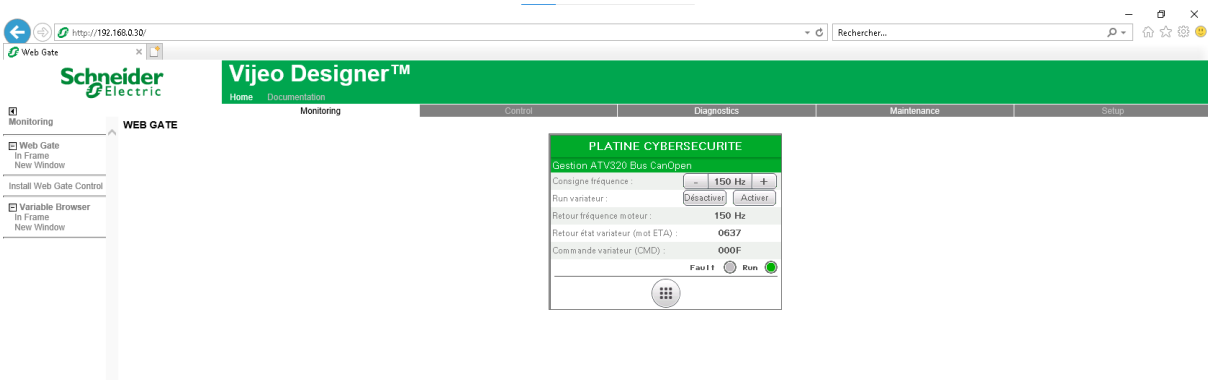
- Set the activity status of this rule to On

  (at its simplest, click on the status cell to switch it on)

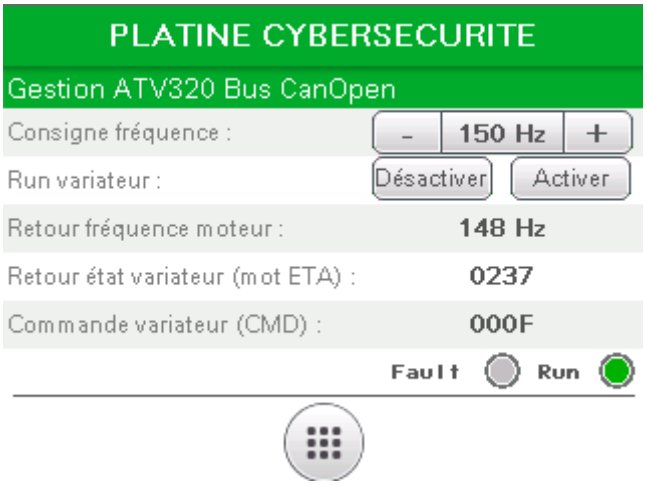


- Finally, click on the Activate this policy command, 

  Check that the flows resume through the SNi40 and that, for example, the HTTP exchanges between Web Gate and HMI are effectively served...



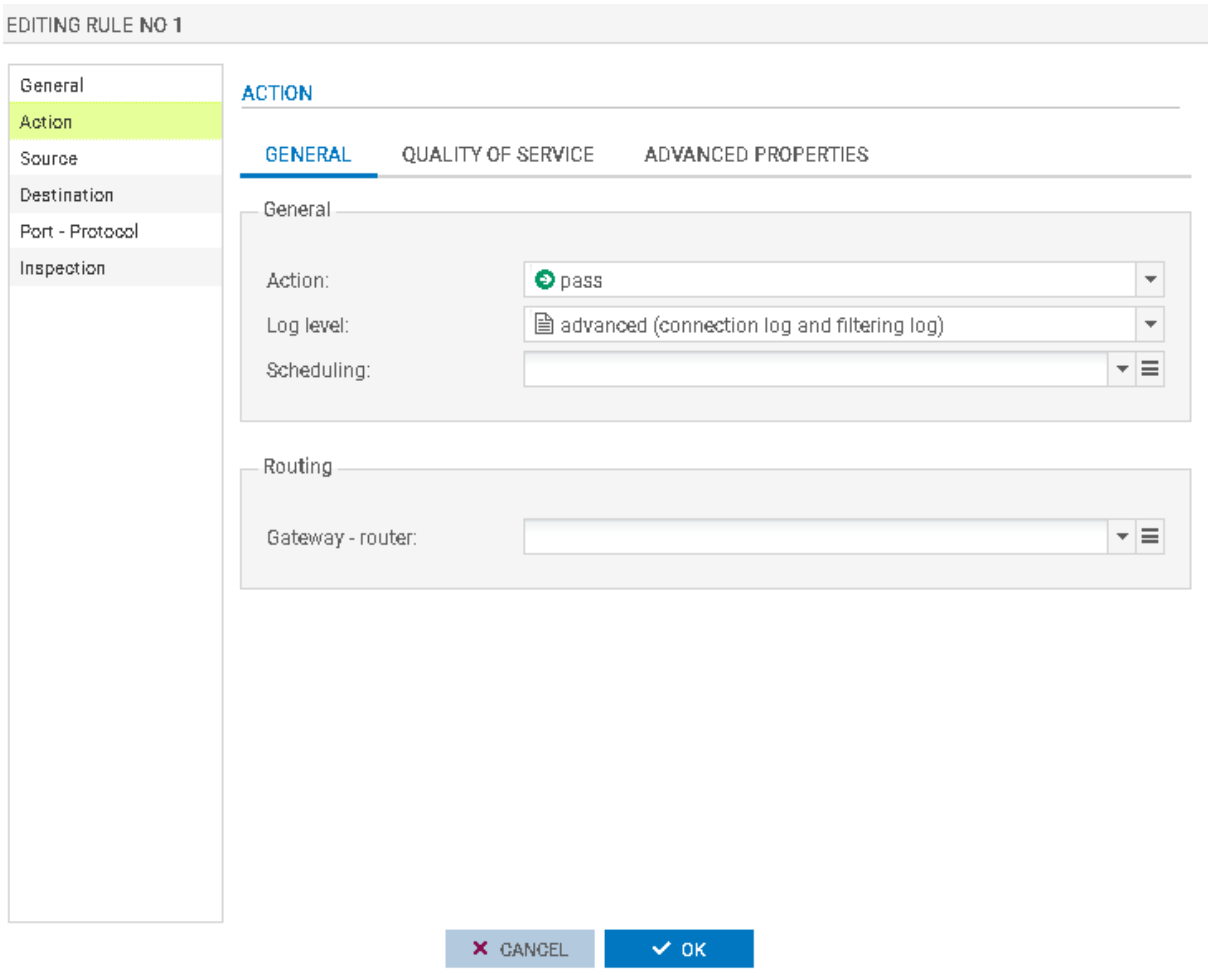
... as well as the Modbus Read/Write requests presented by the **Vijeo Designer Simulation** to the ePAC



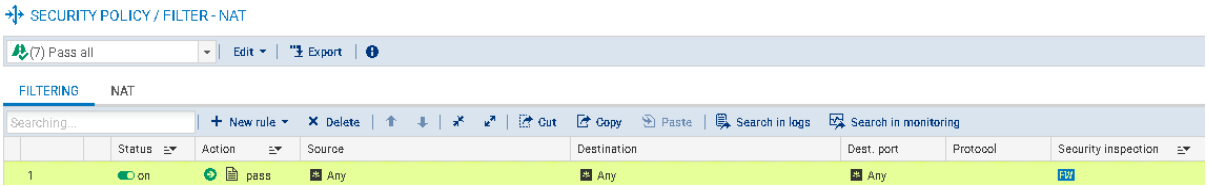
9. Configuring the SNi40 in Pass & Trace All mode

At this stage we can see that, from the applications and in particular from the **Vijeo Designer Simulation**, the flow of exchanges passes through the SNi40. But until now, we have no trace that allows us to analyse these flows. We will therefore try to reconsider the policy adopted, by adding to the rule which indicates that all traffic should be allowed to pass through the SNi40 an attribute which requires the logging of these exchanges (**Trace level: verbose**)

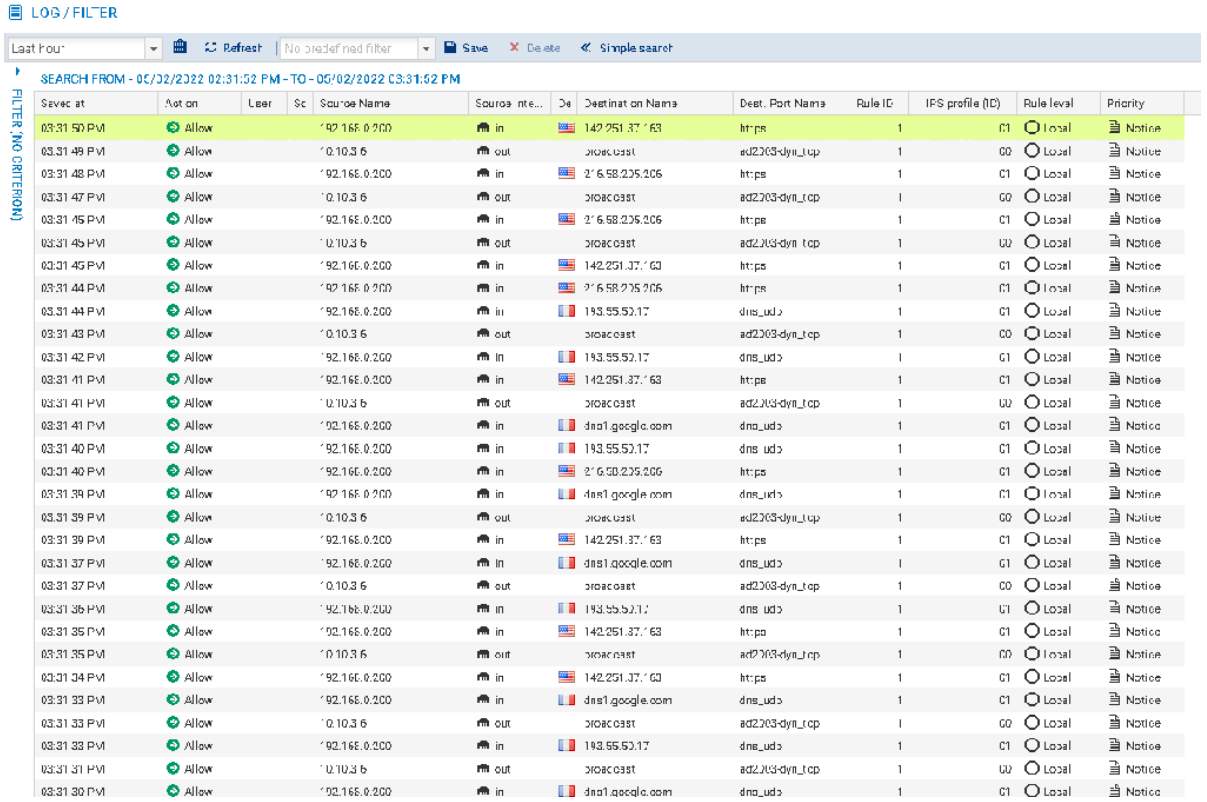
Double click on the "pass" field of the rule previously established.

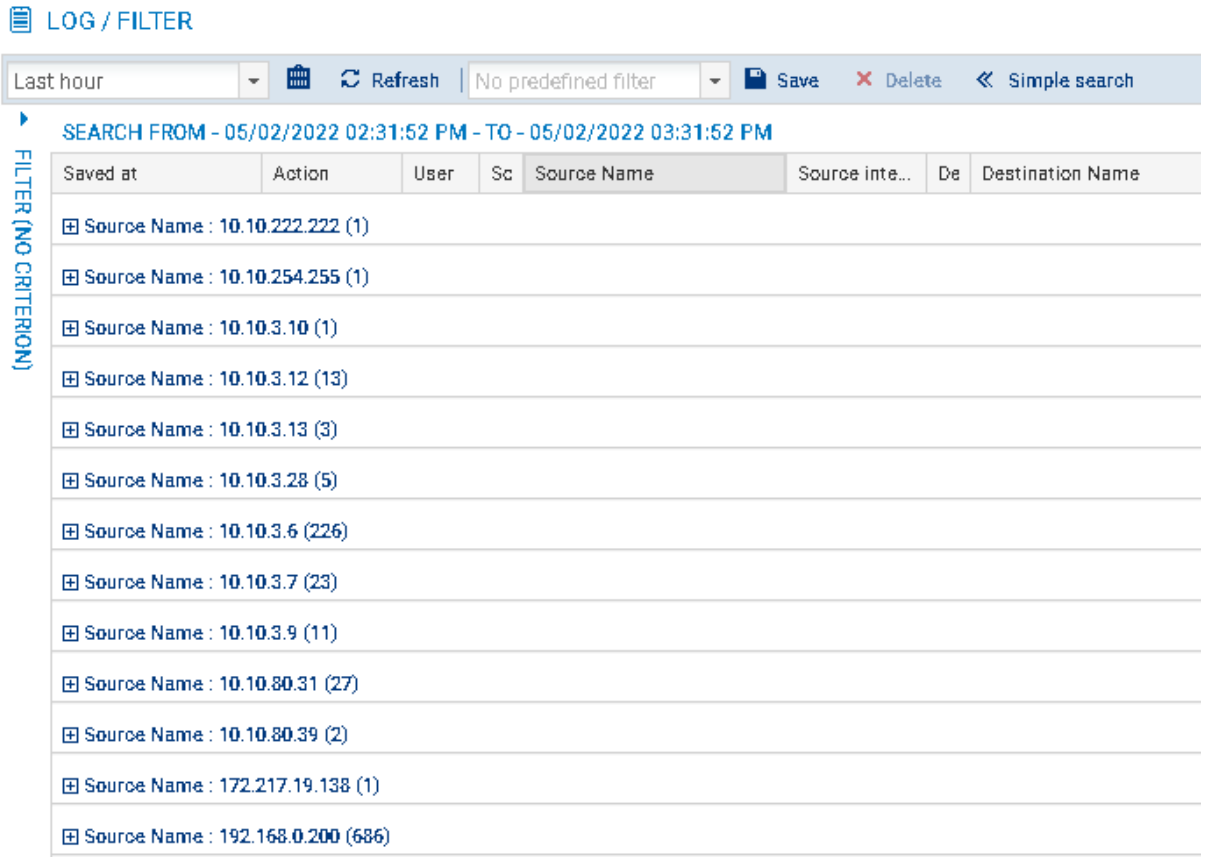


- Validate this modification of the rule and rename the policy "(7) Pass & Trace All".
- Activate this policy



- After validating this policy, go to the menu LOGS AUDIT LOGS, submenu LOGS - LOGS, heading Filtering, and you will see the logged exchanges (proceed as previously explained, when working in Block & Trace All)


LOG / FILTER
Last hour
Refresh
No predefined filter
Save
Delete
Simple search
FILTER (NO CRITERION)
SEARCH FROM - 05/02/2022 02:31:52 PM - TO - 05/02/2022 03:31:52 PM
Saved at
Action
User
Sc
Source Name
Source inte...
De
Destination Name
Dest. Port Name
Rule ID
IPS profile (ID)
Rule level
Priority


LOG / FILTER
Last hour
Refresh
No predefined filter
Save
Delete
Simple search
FILTER (NO CRITERION)
SEARCH FROM - 05/02/2022 02:31:52 PM - TO - 05/02/2022 03:31:52 PM
Saved at
Action
User
Sc
Source Name
Source inte...
De
Destination Name
Source Name : 10.10.222.222 (1)
Source Name : 10.10.254.255 (1)
Source Name : 10.10.3.10 (1)
Source Name : 10.10.3.12 (13)
Source Name : 10.10.3.13 (3)
Source Name : 10.10.3.28 (5)
Source Name : 10.10.3.6 (226)
Source Name : 10.10.3.7 (23)
Source Name : 10.10.3.9 (11)
Source Name : 10.10.80.31 (27)
Source Name : 10.10.80.39 (2)
Source Name : 172.217.19.138 (1)
Source Name : 192.168.0.200 (686)

⊟ Source Name : 192.168.0.200 (559)

03:40:36 PM	Allow	192.168.0.200	in	192.168.0.1	http	1	01	Local	Notice
03:40:36 PM	Allow	192.168.0.200	in	192.168.0.1	http	1	01	Local	Notice
03:40:36 PM	Allow	192.168.0.200	in	192.168.0.1	http	1	01	Local	Notice
03:40:36 PM	Allow	192.168.0.200	in	192.168.0.1	http	1	01	Local	Notice
03:40:36 PM	Allow	192.168.0.200	in	192.168.0.1	http	1	01	Local	Notice
03:40:36 PM	Allow	192.168.0.200	in	192.168.0.1	http	1	01	Local	Notice

The result of this manipulation is that, due to the global passage authorisation allocated to the traffic, all the application exchanges now transit through the SNi40 firewall. Furthermore, with regard to this configuration (Pass & Trace All), the firewall records these blockages and provides a summary report.

Nevertheless, for analysis purposes, we may want to have the actual details of the exchanged frames (Modbus frames for example). We will therefore have to consider another logging strategy, and therefore implement another security policy.

10. SNi40 configuration in Pass All & Analyse mode

The aim here is to provide the means to investigate the details of the frames in transit.

The configuration of the SNi40 is then quite specific:

Synopsis of the manipulations

1) Invocation of a security policy involving the passage of ALL the frames passing through the SNi40 (Pass All), with Trace

2) Adoption of an IPS (Contextual Protection Signature) by default

We will complete the SNi40 configuration by playing with the PROTECTION & APPLICATION 'module'.

1. With regard to the protection profile used by the policy in place, we will first indicate that we are blocking this or that type of request, Modbus and/or UMAS (these types of requests correspond to those we wish to examine).

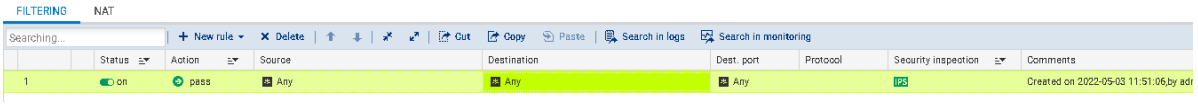
   The modulated policy will then allow all frames to pass except those designated, whose blocking will cause an event. In addition, we will specifically request packet capture for these frames, which we will ultimately exploit.

2. For these event-producing (and previously blocked) frames, we will nevertheless bypass the blocking and explicitly declare that their transit is nevertheless allowed.

In order to exploit these frames that justify our interest, we can use the Stormshield Real Time Monitor tool. RTM will indeed allow the extraction of SNi40 from the box; and coupled with the Wireshark analysis tool, it will allow the examination of its content.

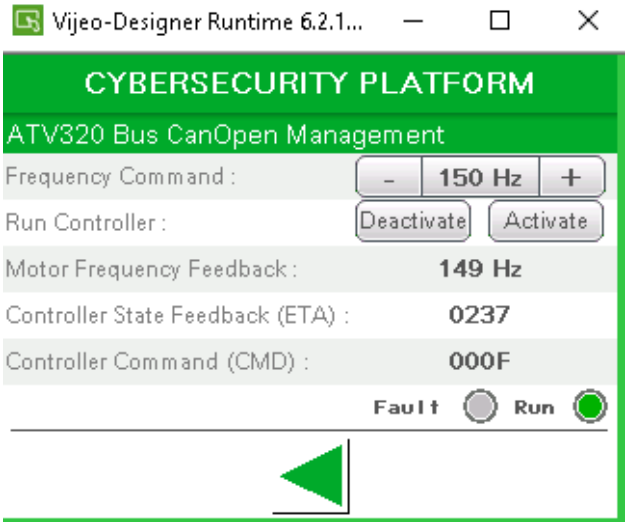
Details of the manipulations

- Security Policy: We will rename the policy defined until now " (7) Pass & Trace All " as " (7) Pass All & Analyse ".



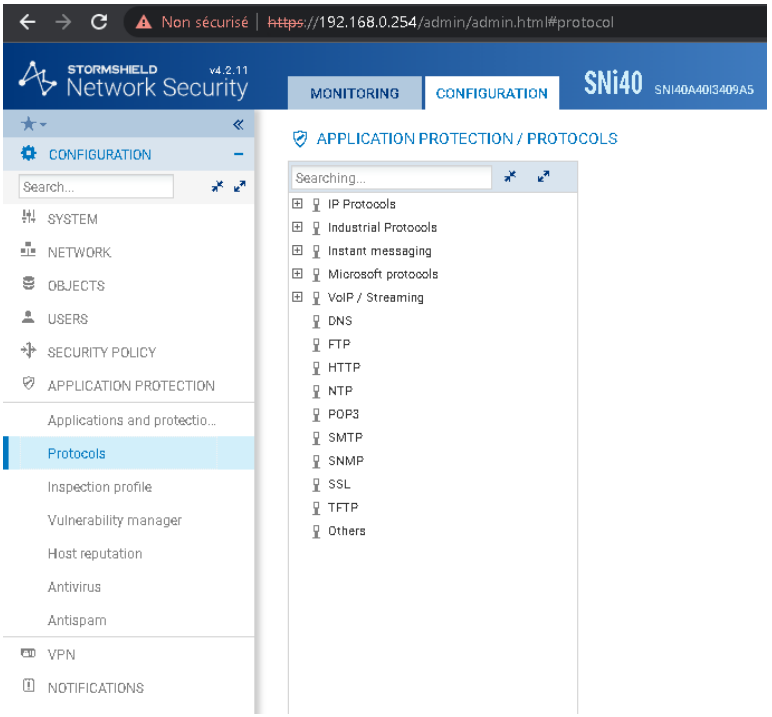
- Click on the Activate this policy command, 

Check that the exchanges resume through the SNi40 and that, for example, the Read requests presented by the HMI substitute running on the Workstation (Vijeo Designer in Simulation mode) to the ePAC are effectively served (see more yellow triangle)

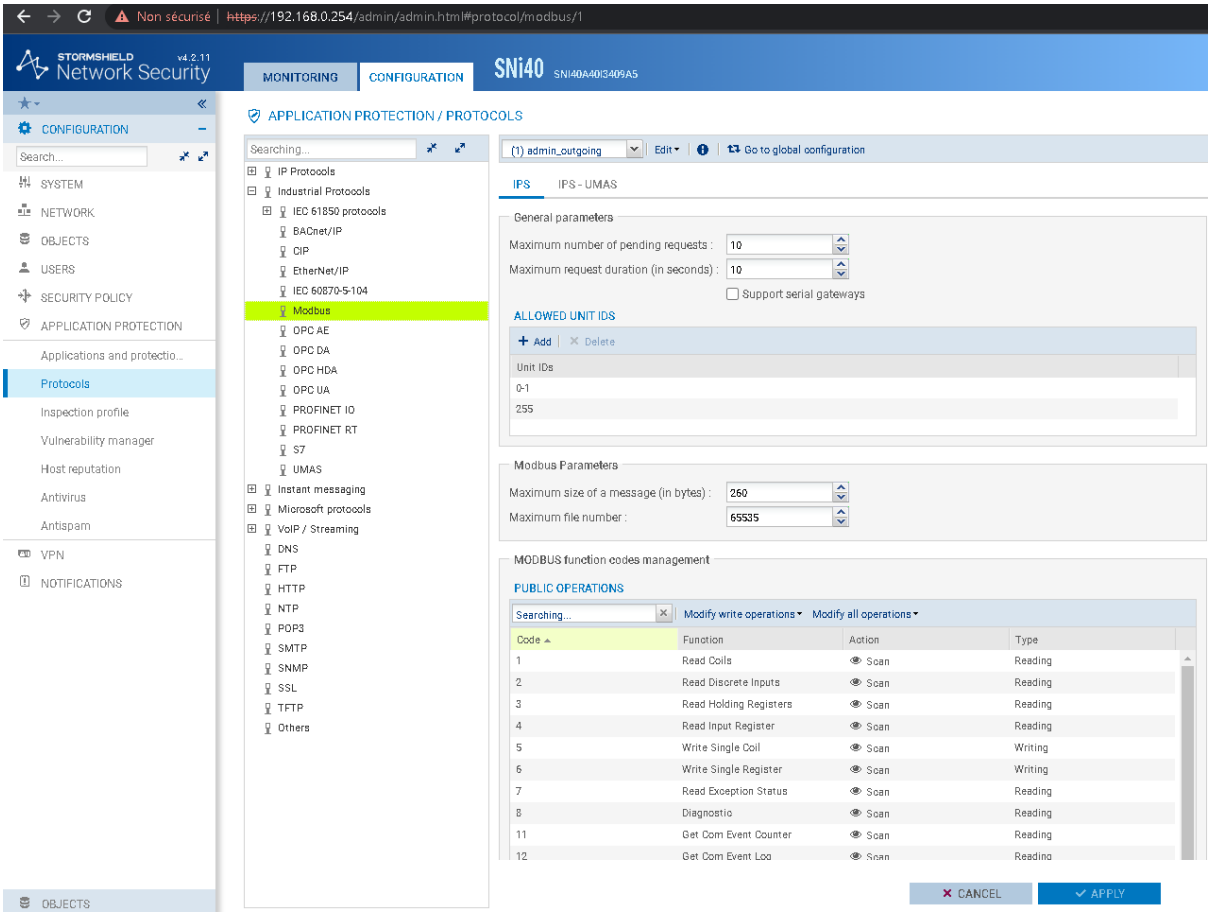


NB: Make sure that the view displayed on the HMI is that of the drive control, so that the commands/writings issued from Web Gate are effectively taken into account.

- Now go to the CONFIGURATION menu, APPLICATION PROTECTION submenu, Protocols section



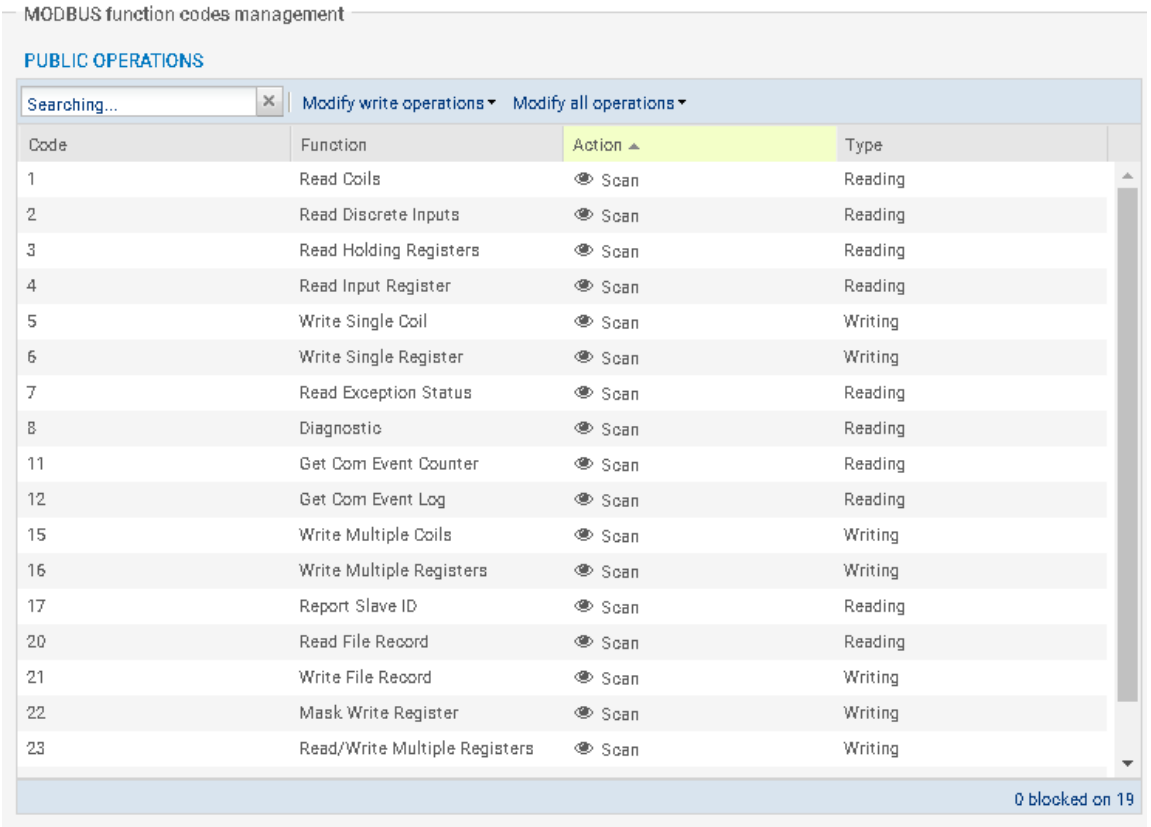
- In the middle section of the screen, expand the Industrial Protocols entry and select Modbus

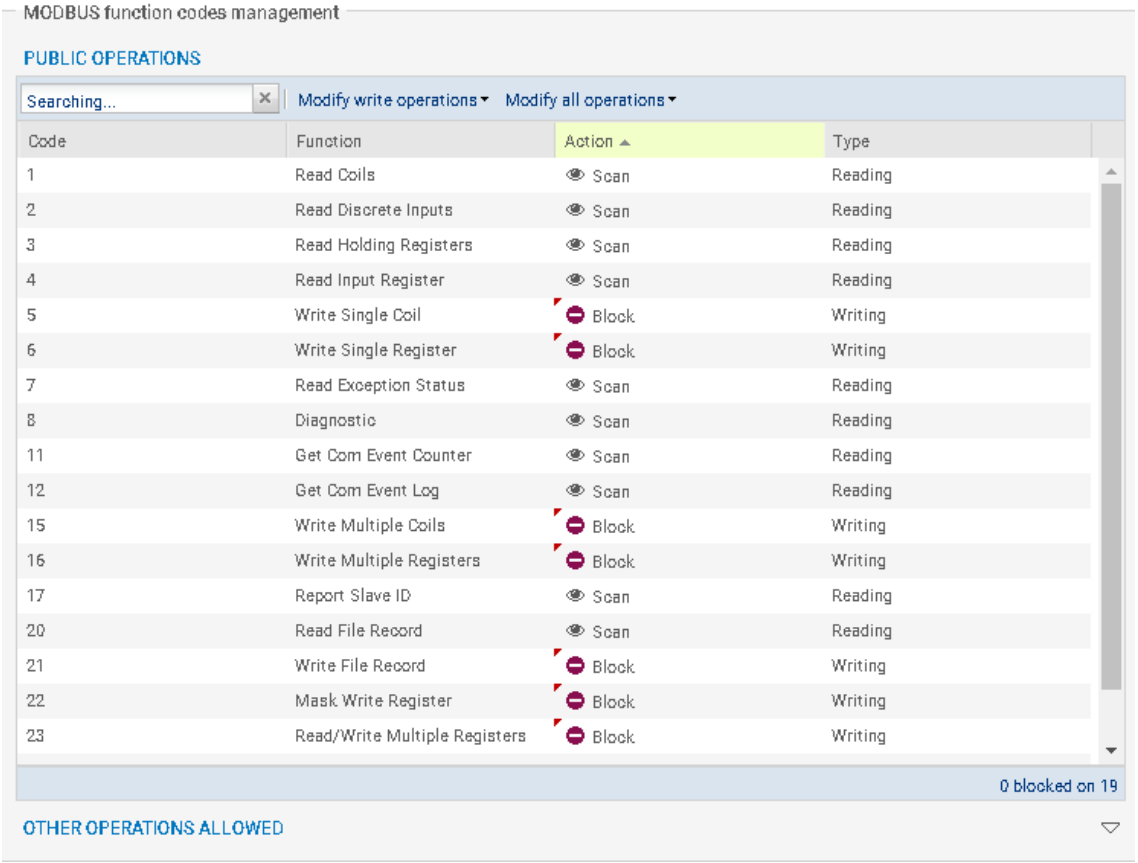


- Firstly, by looking at the IPS tab, which relates to Modbus frames, decide on the actions to be taken against the different types of frame: Analyse (the frame is allowed to pass) vs Block (the frame is blocked and produces an alarm)

  The buttons Modify write operations vs Modify all operations are available to make a global or group selection.

  For this exercise, we will consider wishing to alarm (which implies the choice Block) for all the traditional Modbus operations of writing on bit(s) or word(s) variables


MODBUS function codes management
PUBLIC OPERATIONS
Searching...
Modify write operations
Modify all operations
Code
Function
Action
Type
1 Read Coils Scan Reading
2 Read Discrete Inputs Scan Reading
3 Read Holding Registers Scan Reading
4 Read Input Register Scan Reading
5 Write Single Coil Scan Writing
6 Write Single Register Scan Writing
7 Read Exception Status Scan Reading
8 Diagnostic Scan Reading
11 Get Com Event Counter Scan Reading
12 Get Com Event Log Scan Reading
15 Write Multiple Coils Scan Writing
16 Write Multiple Registers Scan Writing
17 Report Slave ID Scan Reading
20 Read File Record Scan Reading
21 Write File Record Scan Writing
22 Mask Write Register Scan Writing
23 Read/Write Multiple Registers Scan Writing
0 blocked on 19



NB: The configuration manipulations operated until now decide :

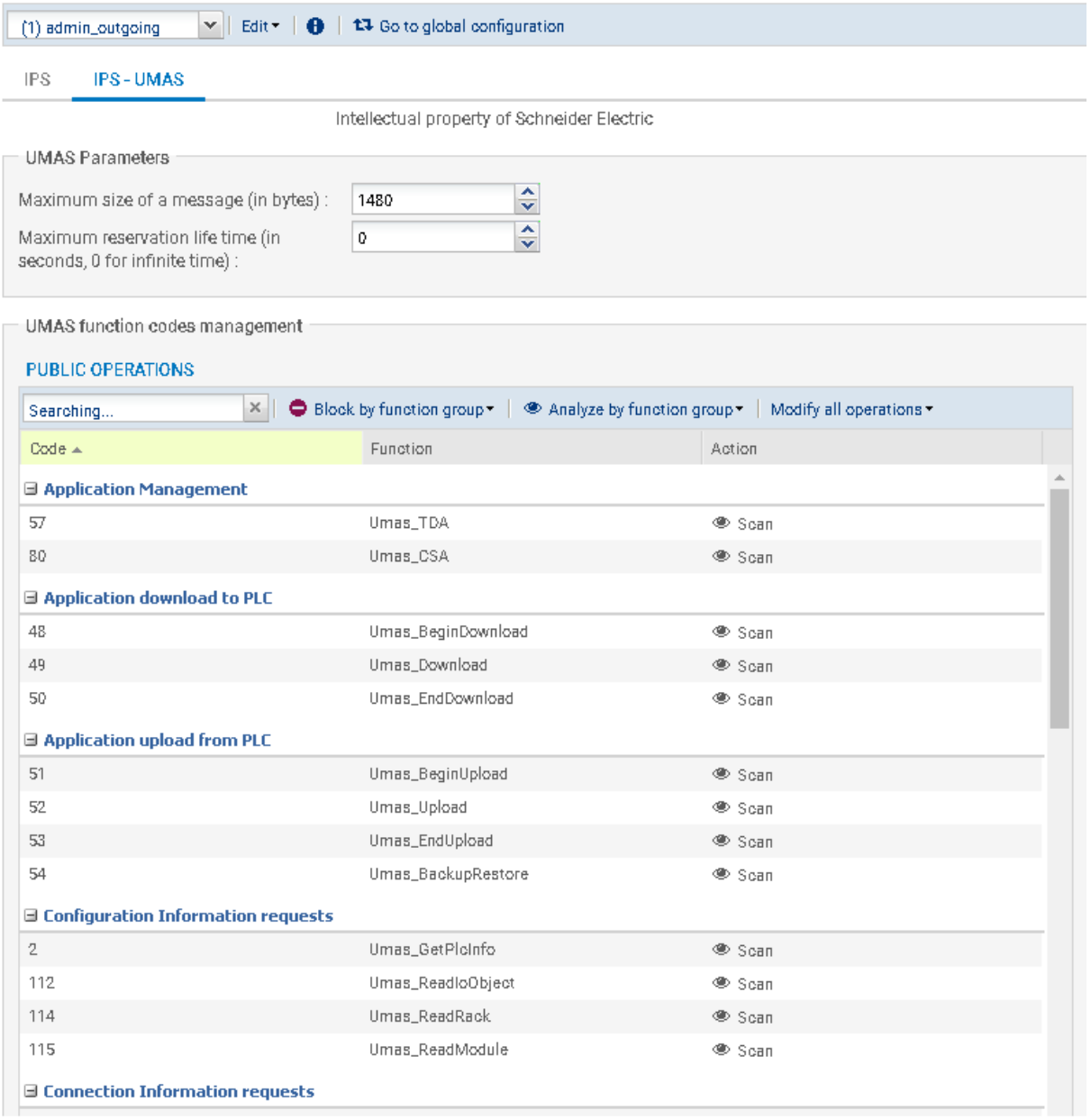
- to forbid (Block) the Modbus function codes of writing

- to allow (Analyse) the Modbus function codes of reading

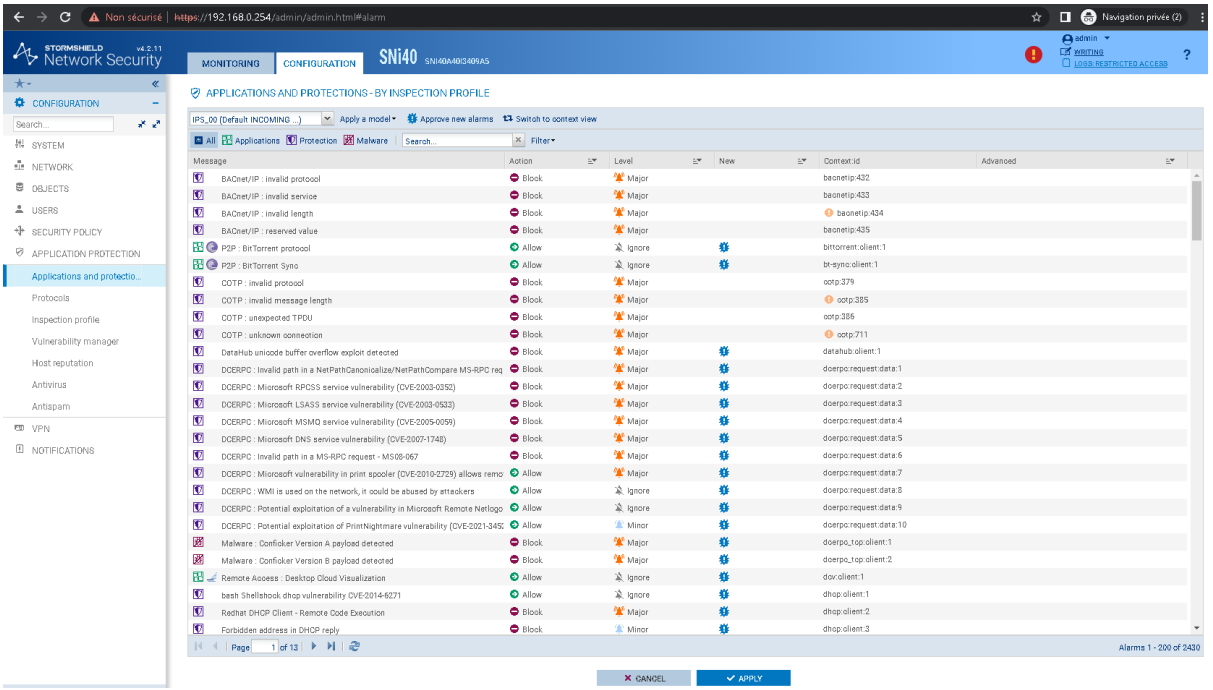
- The same type of work could be done concurrently for the IPS-UMAS tab, which relates to UMAS frames, to decide on the actions to be taken against the different types of frames: Analyse (the frame is allowed to pass) vs Block (the frame is blocked and produces an alarm)

  The buttons Analyse by function group vs Group by function group are available to decide which action to take, by group.

  This exercise will stick to the classic Modbus operations: the UMAS functions will thus be limited to actions of type Analyse, rather than Block, and will thus not produce an alarm

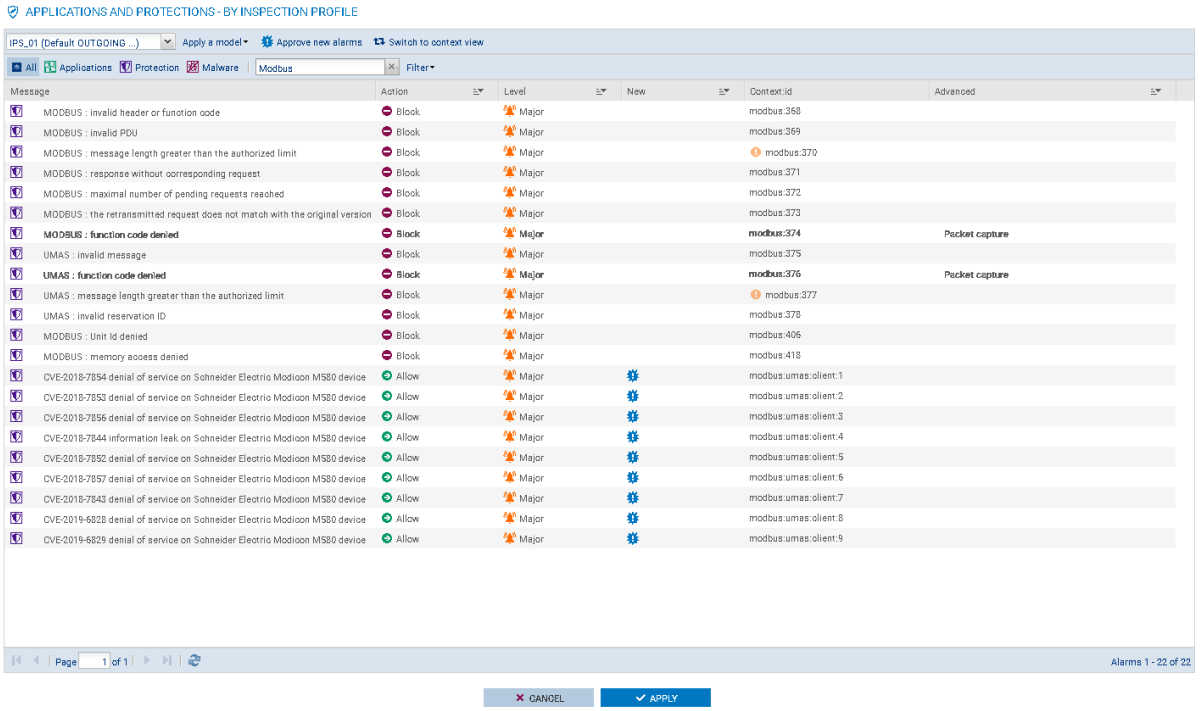


- Now go to the **CONFIGURATION** menu, **APPLICATION PROTECTION** sub-menu, **Applications and Protection** section



NB: check that the IPS selected refers to IPS_01 (Default Outgoing Config) by default

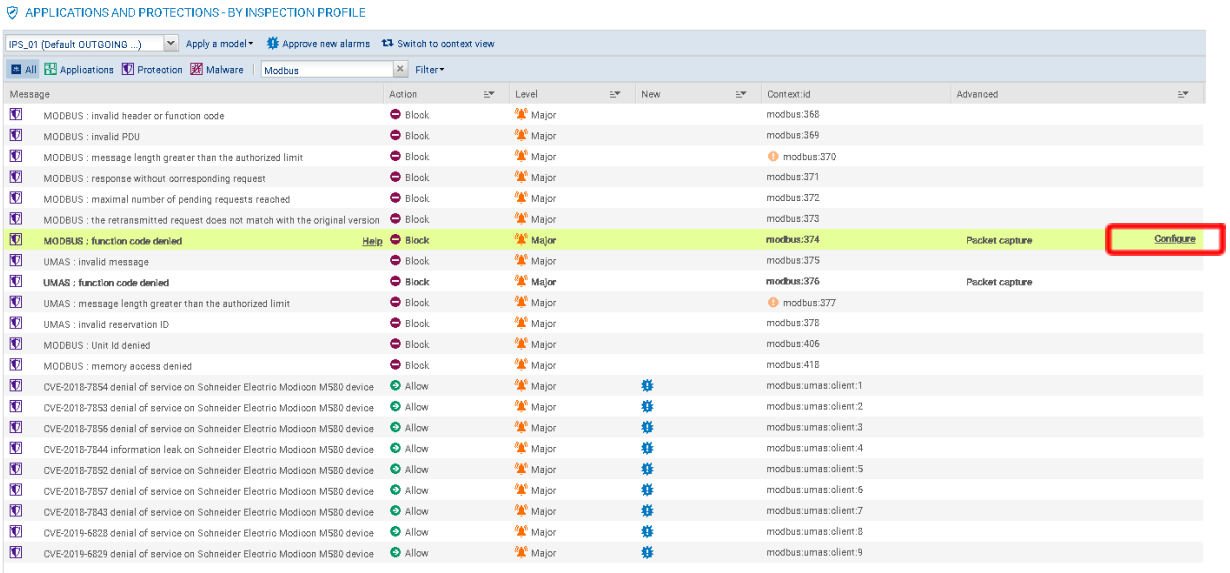
- Enter the Modbus keyword in the search field to identify the types of messages that must justify an alarm and that are linked to the Modbus (and/or UMAS) protocol



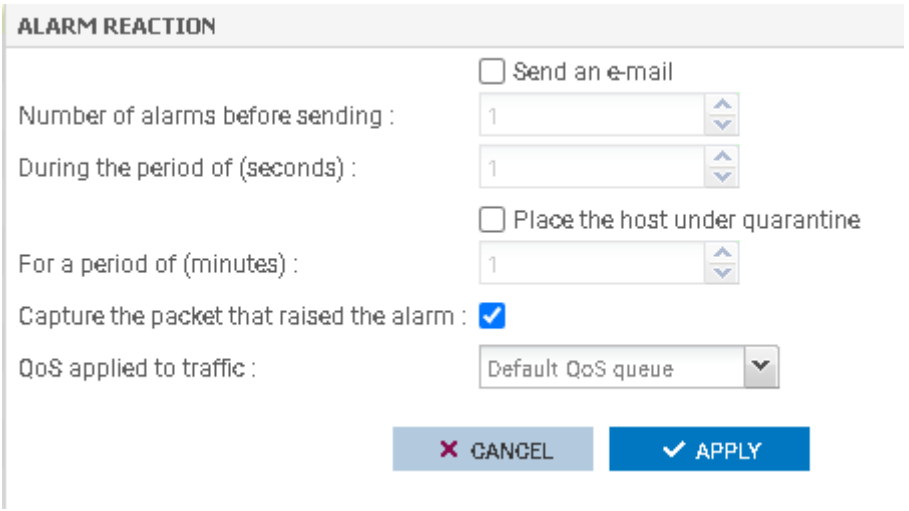
- For Modbus or UMAS frames that warrant a forbidden code (in terms of the frame types that the previous configuration step had set as Block), if necessary, change the action to be initiated for these exchanges from Forbid to Allow.

  In other words, we will explicitly decide here to override the blocking instruction for frames that we had previously decided should warrant an alarm. As a result, these frames, now authorised, will finally be allowed to transit through the SNi40.

- Select successively these types of frames to be authorised, and then click on the **Configure** button located on the right of the selected line, in the **Advanced** column.



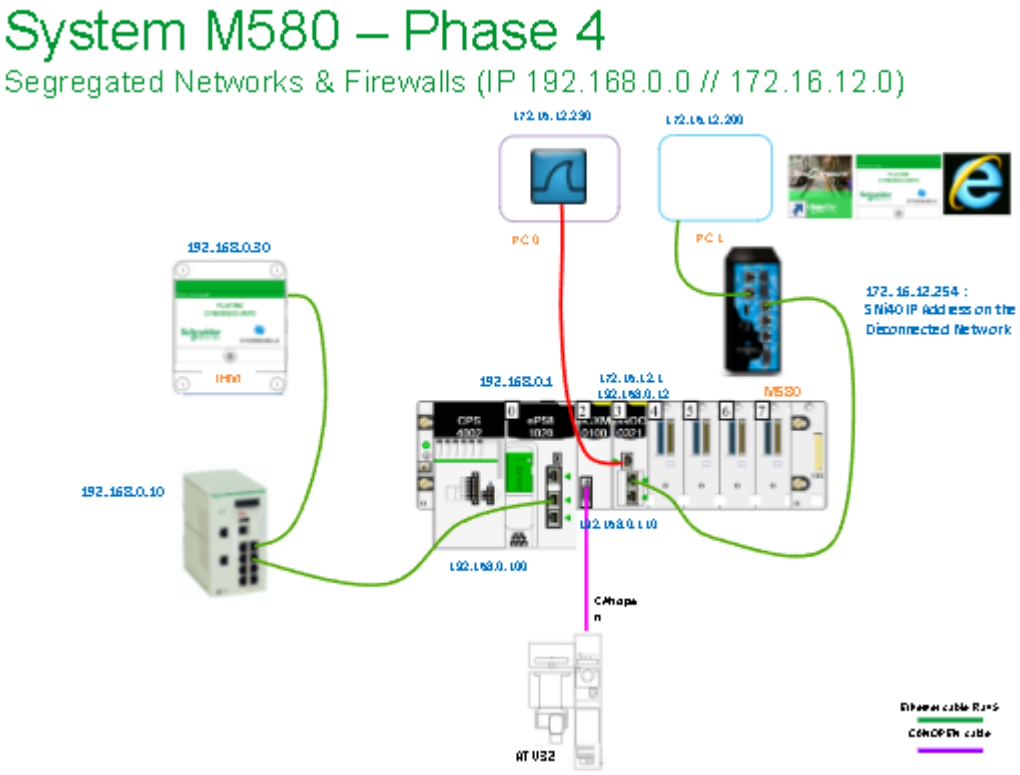
- This will then open the following dialog box, where we will ensure that the Capture the packet responsible for the alarm escalation selection is checked, to capture the packet responsible for the alarm escalation,



At this point, you realise that this progression - which is admittedly a little tortuous - is only intended to allow the capture for analysis of packets corresponding to the frames in which

the user is particularly interested (in this example, the Modbus data write frames), while ultimately allowing the entire flow to pass.

11. Installation of Ethernet cables according to the Phase 4 architecture



12. Modification and verification of new IP addresses

12.1. Workstation

- To find out which routes, if any, have been previously defined on the Workstation, view them using a route PRINT command
- If necessary, execute a route DELETE command to delete the routing used until now, before changing the IP address of the PC, and declaring a new routing

  e.g.: route DELETE 192.168.0.0

- Record the new address of the Workstation (172.16.12.200)

  Check via IPCONFIG

- Issue a route command designating the 'external' address of the NOC coupler (172.16.12.1) as the entry point for accessing the Device Network (192.168.0.0)

  Route ADD 192.168.0.0 mask 255.255.255.0 172.168.12.1

  Check the accessibility of the main address of the M580 CPU (PING)

12.2. Observation Station (frame capture)

- Record the new address of the Observation Station (172.16.12.230)

Verification via IPCONFIG

13. Configuration of the Sni40 Firewall in Bridge mode

13.1. Checking the accessibility of the SNi40

Check the accessibility of this SNi40 (address on the current cut network: 172.16.12.254) by means of (at most) a PING

https://172.16.12.254/admin

13.2. Checking the reachability of the ePAC for Vijeo Designer in Simulation Mode

Verify the accessibility of the ePAC (main address 192.168.0.1, routed by the BME NOC 0321 coupler) via a Modbus request: check under Control Expert that a read/write access on the word %MW1014 (which corresponds to the speed setpoint address of the drive) gives the same value as the one identified via Control Expert or the Magelis HMI for example

14. Configuring the SNi40 in Pass All & Analyze mode

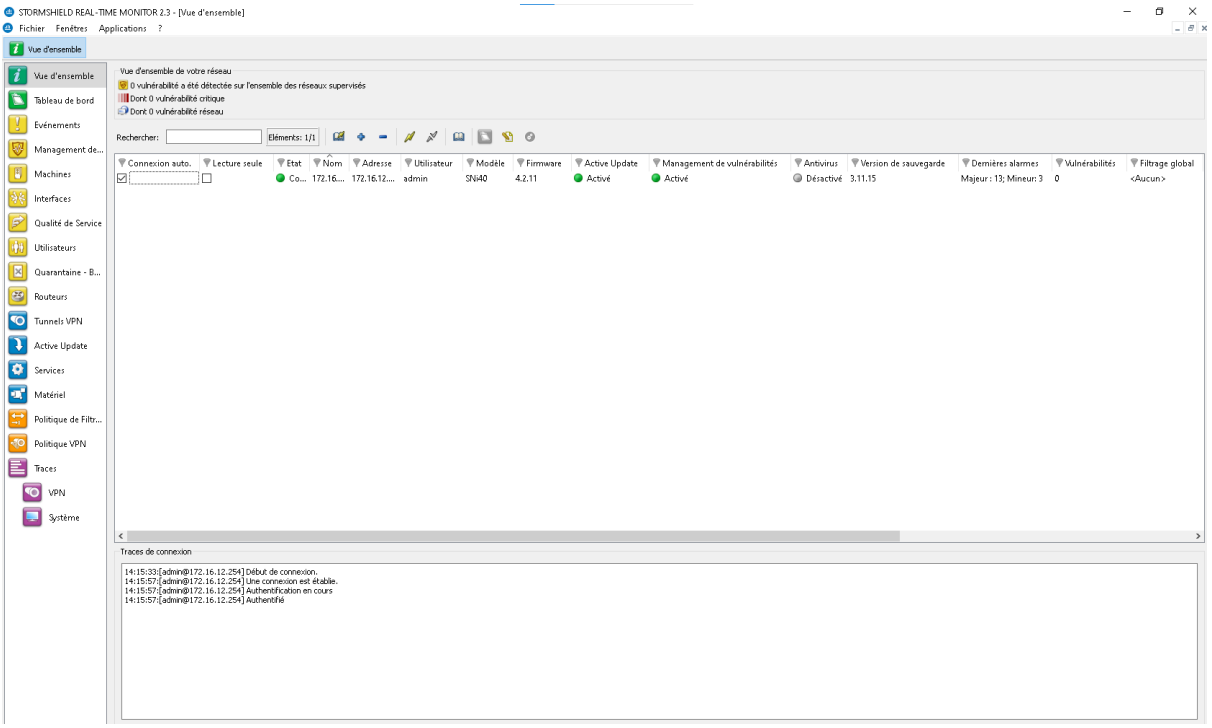
This is simply a matter of maintaining the SNi40 firewall configuration, as defined in the previous chapter (Pass All & Analyze)

Validate the effectiveness of the dialogue by observing the behaviour, for example, of the Vijeo Designer application running on the Workstation in Simulation mode

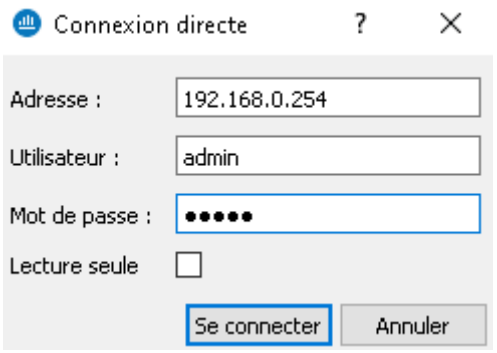
Annexe : Stormshield Real Time Monitor & Wireshark

This "companion" tool to Stormshield allows you to extract packets (e.g. Modbus/TCP exchanges) archived in the SNi40 firewall, and to sort/interpret them via Wireshark.

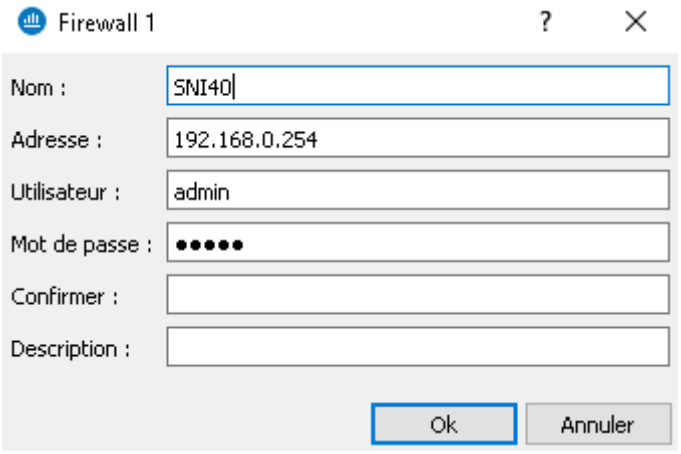
- Install Wireshark on the workstation if it is not already installed
- Ditto install Stormshield RealTime Monitor on the workstation if it does not already reside there
- Launch Stormshield Realtime Monitor by running the monitor.exe executable



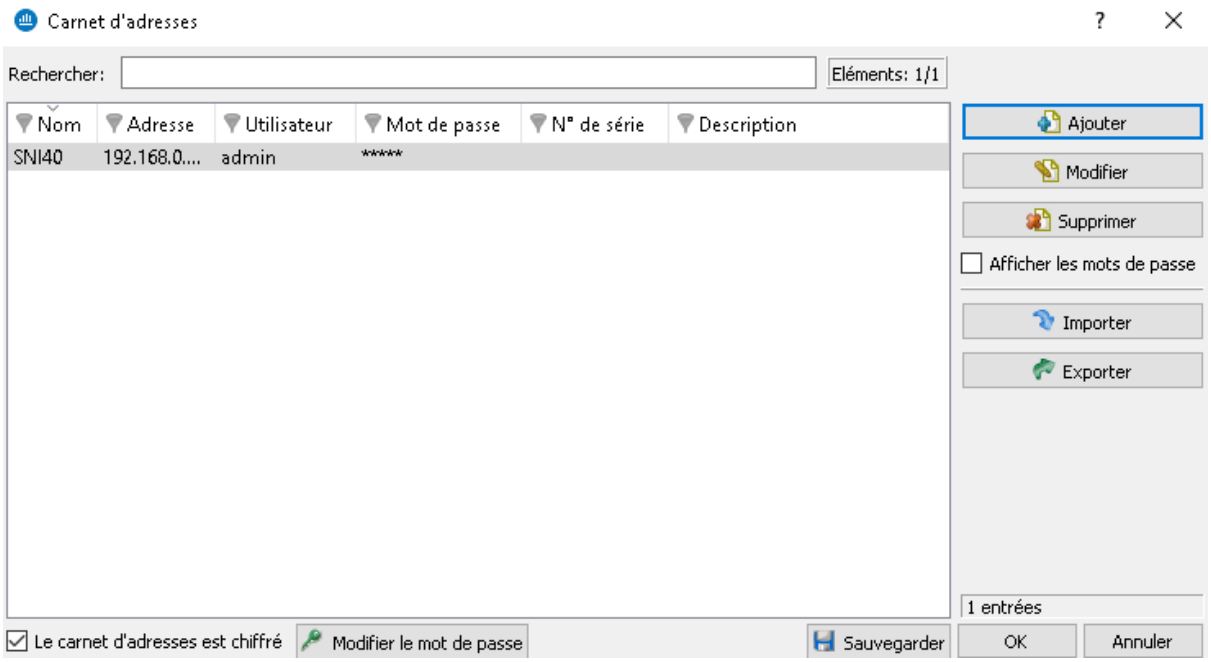
- For a first connection of RealTime Monitor to the target SNi40, we will either decide on a direct connection,



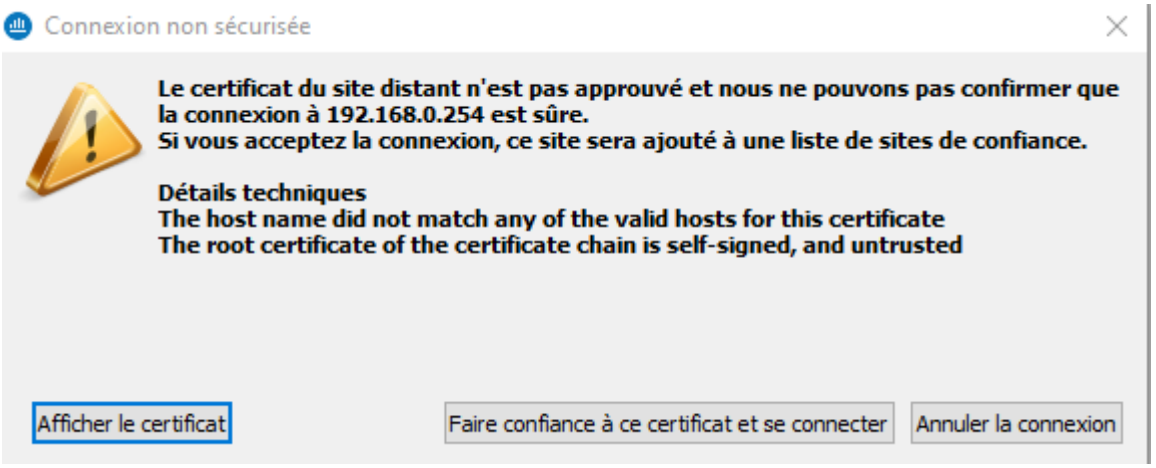
or we will anticipate and create a (new) entry



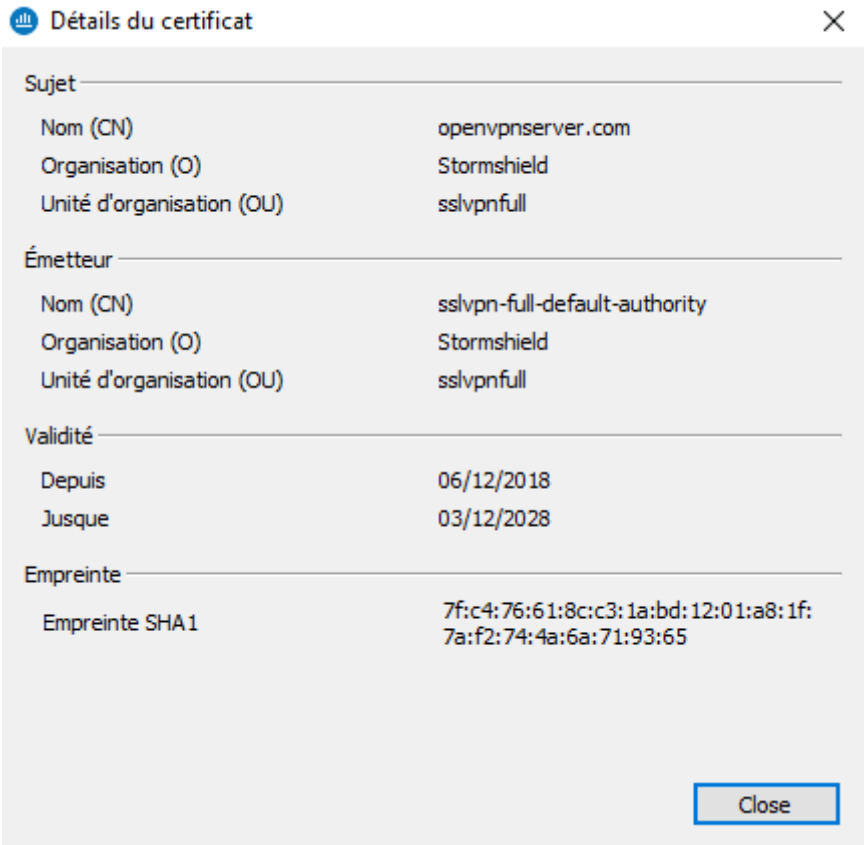
in the address book



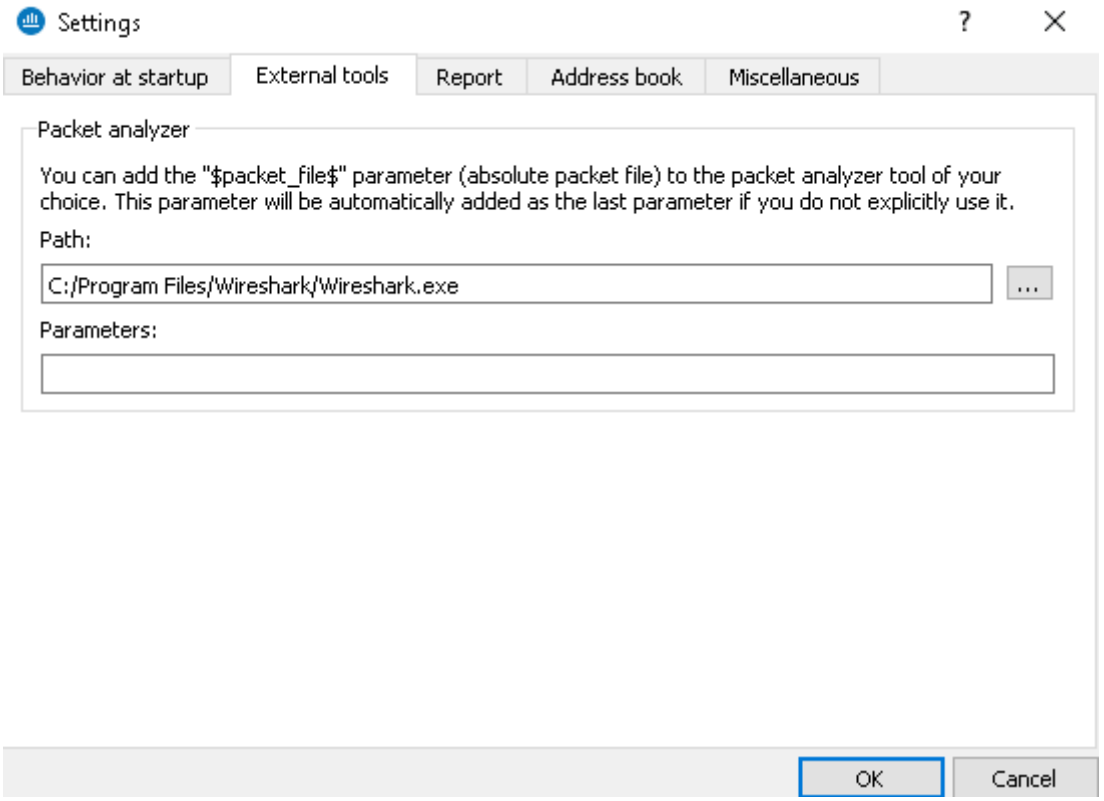
Note: It is possible that the first time you connect to the SNi40, the workstation browser may be prompted to authorise the certificate associated with that SNi40



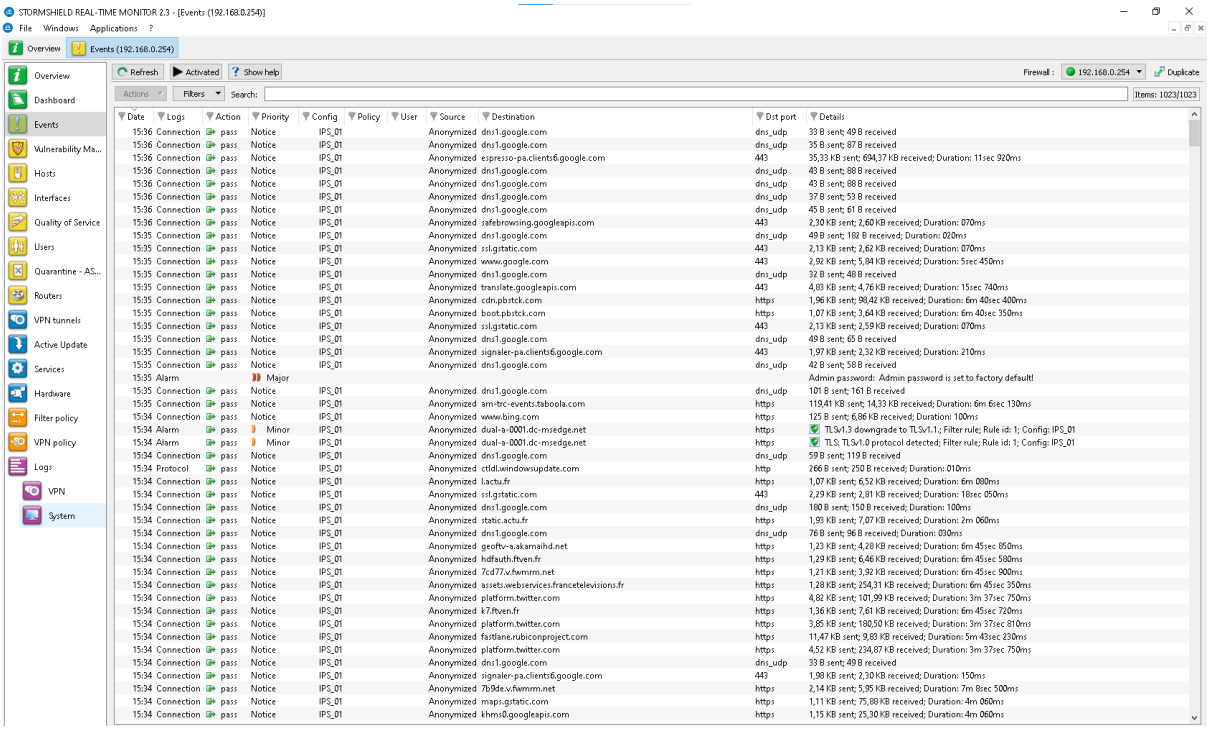
Incriminated certificate



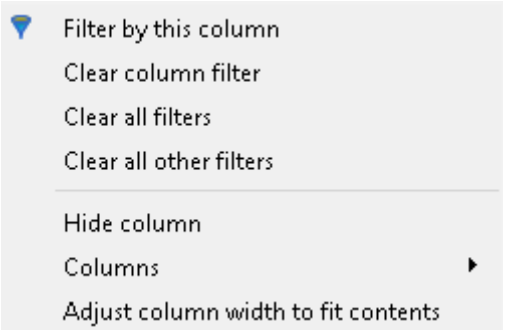
- As a further precaution, we should ensure that RTM can be automatically coupled to Wireshark



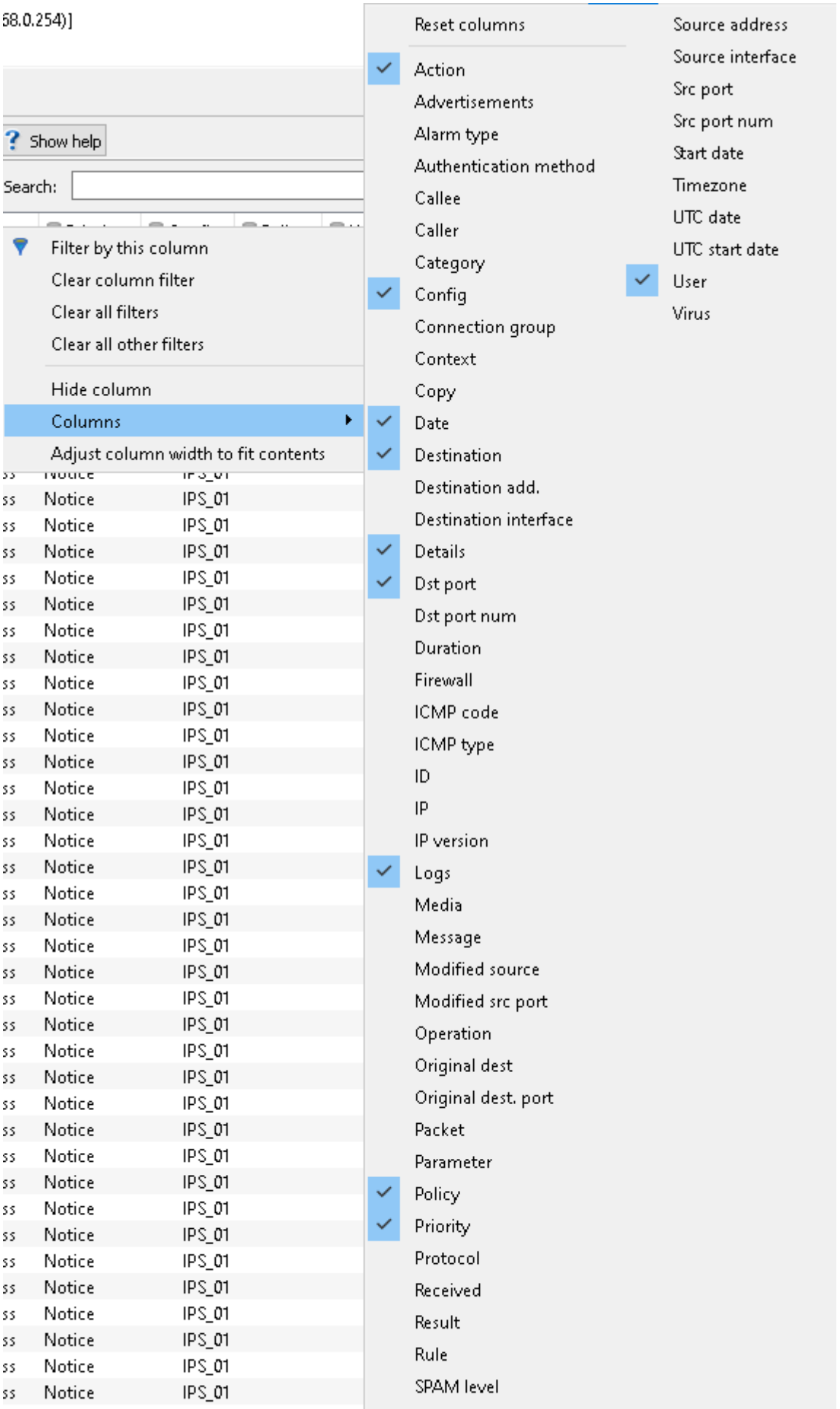
- Once these preliminaries are set, and having clicked on the address selection corresponding to the SNi40 Firewall used, we will click on the Events entry. This will display any events captured by the SNi40 and extracted by RTM.



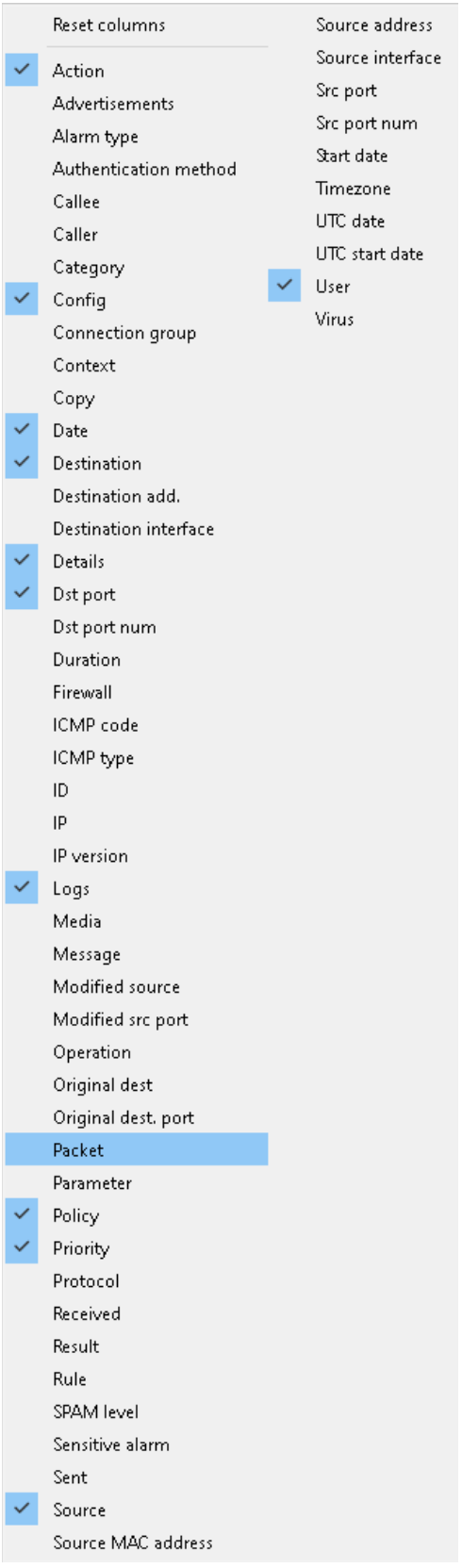
To display the content of the **Packet** column, if it is not already the case, a left click on the top banner of the columns displays the following dialog box:



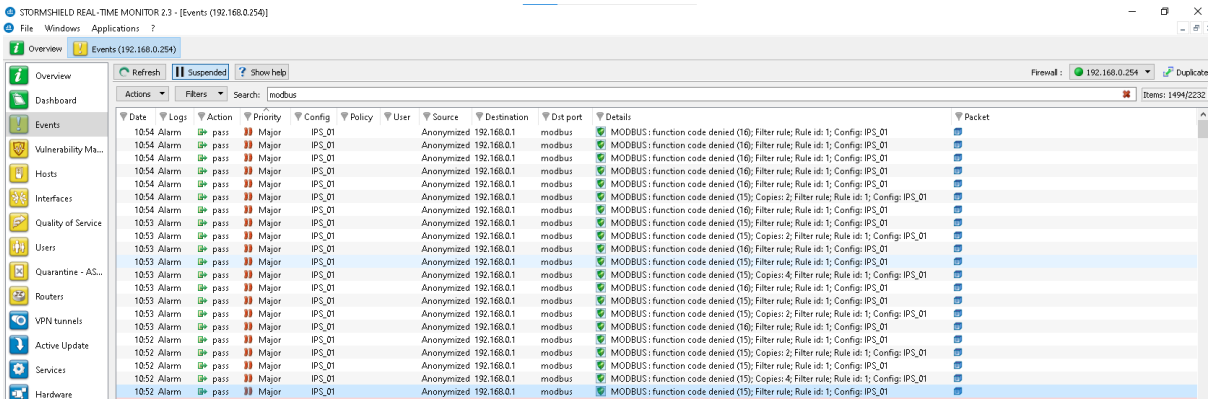
- This will allow you to click on the Columns entry to display the following dialogue box which allows you to set the details of what you want to be displayed


58.0.254)]
Show help
Search:
Filter by this column
Clear column filter
Clear all filters
Clear all other filters
Hide column
Columns
Adjust column width to fit contents
Reset columns
Action
Advertisements
Alarm type
Authentication method
Callee
Caller
Category
Config
Connection group
Context
Copy
Date
Destination
Destination add.
Destination interface
Details
Dst port
Dst port num
Duration
Firewall
ICMP code
ICMP type
ID
IP
IP version
Logs
Media
Message
Modified source
Modified src port
Operation
Original dest
Original dest. port
Packet
Parameter
Policy
Priority
Protocol
Received
Result
Rule
SPAM level
Source address
Source interface
Src port
Src port num
Start date
Timezone
UTC date
UTC start date
User
Virus
ss Notice IPS_01

- Click on **Package** if necessary to have this column **Package**

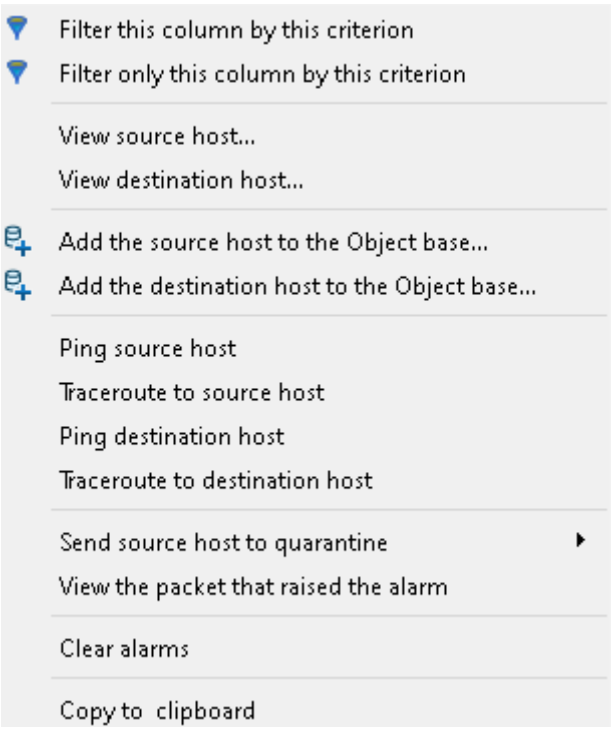


- To more easily isolate alarm-producing frames, you can enter the **prohibited** keyword (found in the labels displayed in the Details column)



- Once you have identified a frame for which you wish to see the details, a right click on the annunciating line opens a dialog box where you can select the command

  See the packet that triggered the alarm



- This opens the **Wireshark** tool, which points directly to the selected frame:

  The detail provided shows the nesting of the different layers, the application layer corresponding here to the Modbus protocol.

FOTO