TP3 - Cybersecurity - Protection by Custom Patterns

Operational objectives:

- Understand the concept of custom signature filtering on SNi40 firewalls
- Be able to configure an SNi40 firewall with a predefined signature
- Be able to define a new custom signature
- Be able to demonstrate the effectiveness of this type of filtering

Prerequisites :

- Master the basic operations of Control Expert
- Be able to launch Vijeo Designer in simulation mode
- Understand the basic structure of a Modbus frame and its main functions
- Have understood the main principles of SNi40 configuration

The problem posed:

Definition and implementation of a custom signature filtering on SNi40 firewall, in order to allow an automatic rejection of requests with content outside the admissible limits, as defined by the user.

Application example:

- Restrict the admissibility of a request to modify the speed setpoint to a minimum value of of 20% of its maximum speed
- Restrict the admissibility of a speed set point modification request to a maximum value of of 80% of its maximum speed

Resources :

- **Manufacturer documentation**
  - Schneider Electric
    - ➔ website
    - ➔ protocole-modbus.pdf
  - Stormshield :
    - ➔ SNS - User and Configuration Manual
    - ➔ sns-en-custom_context_based_protection_signatures_technical_note

- **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)
  - Custom signature file Prohibit50ormore_FC16.in

- **Software provided, to be installed on the working PC (console) for the realization of this TP:**
    - Control Expert (Schneider Electric): Programming 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
    - WinSCP/Putty: manipulation of Custom Patterns files on SNi40

Evaluation criteria :	😀	😐	😟
Interpreting a custom signature definition file			
Configuring an SNi40 firewall with predefined custom signature			
Definition of a custom signature file for SNi40 firewall			
Modifying a custom signature file for SNi40 firewall			
Creating a custom signature file for SNi40 firewall			
Demonstration of the effectiveness of filtering by Custom Patterns			
Autonomy - Quality of work/restitution			

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

TP3 - Protection by value limitation

Customized contextual protection signatures (Customs Patterns)

Custom contextual protection signatures (Customs Patterns) are intended for the analysis, by the firewall, of applications developed within the company or in addition to the signatures developed by the firewall manufacturer (Stormshield).

These signatures are based on regular expressions (called "variants"). These "variants" are used to analyze strings of characters in the data of exchanged network packets.

The associated alarms can then block or allow the detected flow to pass, depending on the settings made within the personalized signature (these settings can then be modified on each firewall, within the Application Protection > Applications and Protection module).

---

1. Review of the custom signature file provided

For the execution of this TP a .in file (Prohibit50ormore_FC16.in) is provided, which contains the definition of a "custom signature".

Provide a summary analysis of the contents of this file.

2. Setting up the configuration with Custom Patterns

Note: A pdf document entitled “sns-en-custom_context_based_protection_signatures_technical_note”.

This document deals specifically with custom signatures.It provides a number of guidelines that will be used in the execution of this tutorial.

A new configuration will be implemented on the SNi40 Firewall, initially to limit the fan speed to a maximum of 20% of its maximum speed, i.e. 50 Hz.

This will be done using a custom pattern, pre-configured and pre-mounted on the case.

By varying the speed on the customer, it will be seen that the fan speed set point is "limited".

With the available analysis tools, it will be verified that the client was trying to send values above this limit, but that they were blocked.

3. Use of Custom Signature Variants ('Custom Patterns')

We now wish to implement a variant of the previous filtering (which blocked setpoints above 50) by now blocking setpoints below 80% of the drive's maximum speed, i.e. 200 Hz.

In other words, we want to block the setpoints between 0 and 200.

By varying the speed on the customer, it will be seen that the fan speed set point is "limited".

With the available analysis tools, it will be verified that the client was trying to send values below this limit, but that they were blocked.

Note

This test sequence will be played by default according to the so-called Phase 2 architecture, i.e. integrating the SNi40 firewall, which is connected to an Ethernet port (DIO) of the M580 CPU.

It could just as easily be replayed according to the so-called Phase 4 architecture, i.e. the one involving a separation of networks: 'Control Network' vs 'Devices Network'. This time, the SNi40 firewall is not connected to an Ethernet DIO port on the CPU module, but to an Ethernet DIO port on the BME NOC 0321 module.

With this Phase 4 architecture, the elements present on the 'Control' network will register in the 172.16.12.0 addressing domain, while those present on the 'Equipment' network will persist in the 192.168.0.0 addressing domain (i.e. the same as before).

See TP2, Chapters 11 & 12, for cabling and initialization of routing on the Workstation

Details of expected operations

Important:

The **Web Gate** application, transposed into an Internet Browser of the HMI application running on the Magelis (HMI) terminal, connected locally by default, does not produce Modbus TCP requests as such, whether they correspond to reads or writes. It is in fact the HMI that ensures the Modbus TCP communication, and synchronizes its data with the image displayed in the browser.

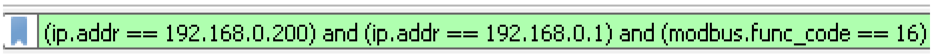
Consequently, the **Vijeo Designer** application, running in **Simulation** mode on the **Workstation**, will be used to produce Modbus TCP unit frames from the PC to the ePAC (PLC) for testing purposes, through the SNi40 Firewall if necessary.

That said, the **Web Gate** application (as well as the **Magelis** GUI) may be used concurrently to place the model in a given preliminary state.

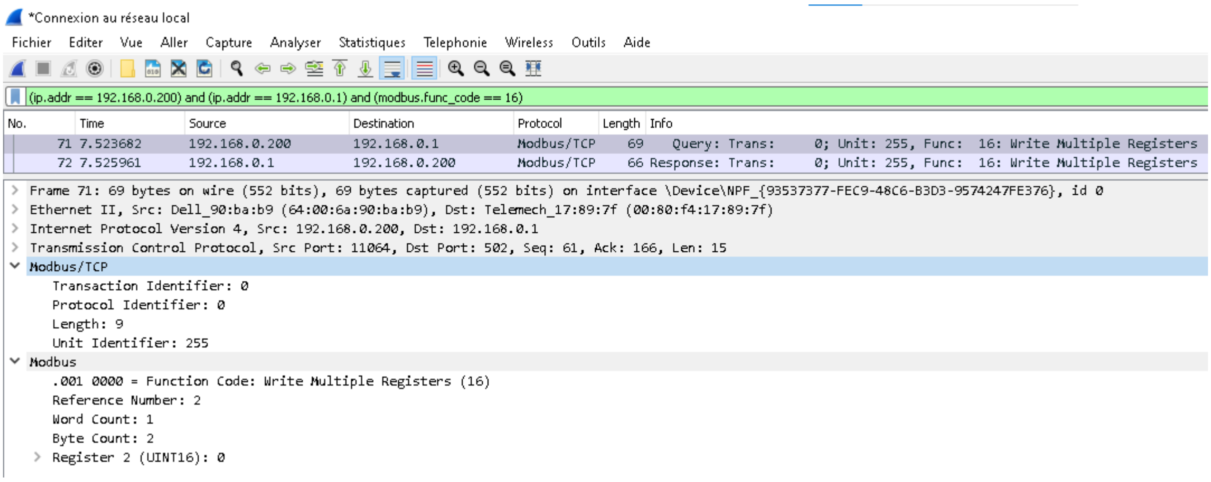
1. **Review of the custom signature file provided**
    - For the execution of this TP, a .in file (Prohibit50ormore_FC16.in) is provided, which contains the definition of a "custom signature". This signature can be compared with the captured packet corresponding to a requested frequency of 50 Hz via the **Vijeo Designer Simulation**.

      We will filter the Wireshark capture introducing the following:

(ip.addr == 192.168.0.200) and (ip.addr == 192.168.0.1) and (modbus.func_code == 16)

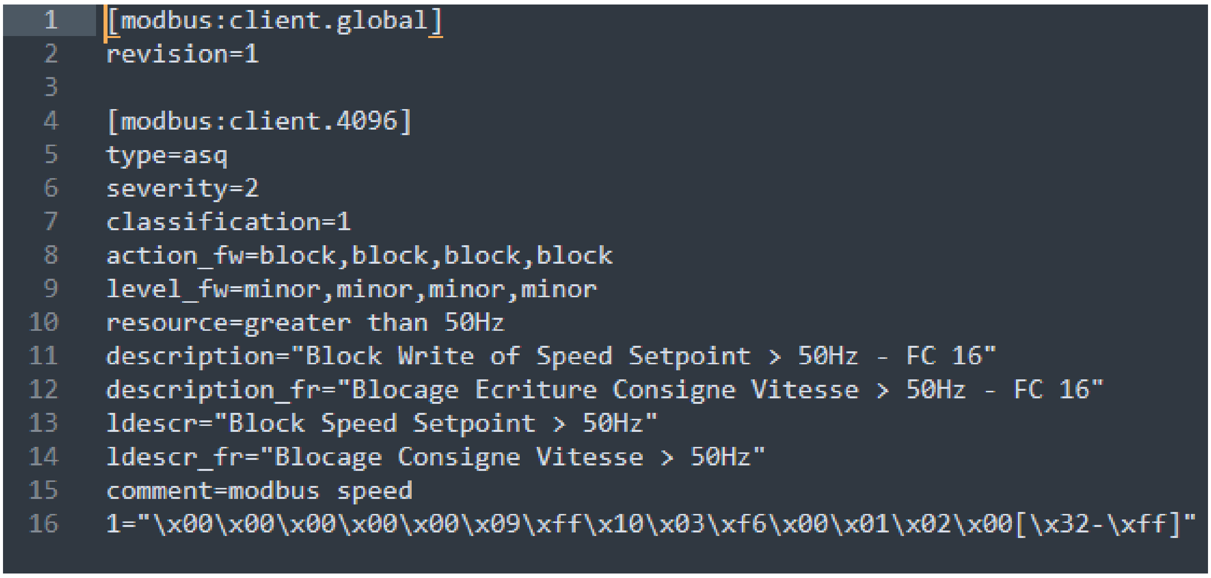


```
(ip.addr == 192.168.0.200) and (ip.addr == 192.168.0.1) and (modbus.func_code == 16)
```



```
(ip.addr == 192.168.0.200) and (ip.addr == 192.168.0.1) and (modbus.func_code == 16)

No.  Time      Source         Destination    Protocol    Length Info
  71 7.523682  192.168.0.200  192.168.0.1    Modbus/TCP    69   Query: Trans:     0; Unit: 255, Func:  16: Write Multiple Registers
  72 7.525961  192.168.0.1    192.168.0.200  Modbus/TCP    66 Response: Trans:     0; Unit: 255, Func:  16: Write Multiple Registers

> Frame 71: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{93537377-FEC9-48C6-B3D3-9574247FE376}, id 0
> Ethernet II, Src: Dell_90:ba:b9 (64:00:6a:90:ba:b9), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 11064, Dst Port: 502, Seq: 61, Ack: 166, Len: 15
v Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 9
    Unit Identifier: 255
v Modbus
    .001 0000 = Function Code: Write Multiple Registers (16)
    Reference Number: 2
    Word Count: 1
    Byte Count: 2
  > Register 2 (UINT16): 0
```

- The content of this file is pure ASCII. The details are given below:



```
[modbus:client.global]
revision=1

[modbus:client.4096]
type=asq
severity=2
classification=1
action_fw=block,block,block,block
level_fw=minor,minor,minor,minor
resource=greater than 50Hz
description="Block Write of Speed Setpoint > 50Hz - FC 16"
description_fr="Blocage Ecriture Consigne Vitesse > 50Hz - FC 16"
ldescr="Block Speed Setpoint > 50Hz"
ldescr_fr="Blocage Consigne Vitesse > 50Hz"
comment=modbus speed
1="\x00\x00\x00\x00\x00\x09\xff\x10\x03\xf6\x00\x01\x02\x00[\x32-\xff]"
```

The last line carries the Modbus encoding of a request that will send 9 bytes, indicating that a request will be made:

On the Modbus device N° 255 ($FF) (default device number, not significant in Modbus/TCP)

(This value may vary, however, depending on the sender of the request).

a multi-word write operation ($16) on address $03F6, i.e. 1014, i.e. the word of address %MW1014, carrying here the speed setpoint carrying in fact 1 word, i.e. two bytes

Note in particular the end of this last line, enclosed in square brackets

: [\x32-\xff]. These square brackets define the limits of the range of admissible values for the byte taking place on this position:

x32 (hexadecimal value) = 50 (decimal value)

xff (hexadecimal value) = 255 (decimal value)

In other words, the admissible values will be between 50 and 255

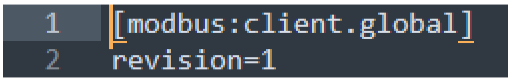
NB: In the conditions of use envisaged here, the SNi40 firewall will behave both as a recipe firewall and as a client firewall.

- **Reminder on the structure of a custom contextual signature file**

  The minimum structure of the custom context signature definition file is as follows:

  - A "[context.global]" section, unique for each context, in which the revision of signatures is specified.

    In our example, we have for example :



```
[modbus:client.global]
revision=1
```

*This means that the **context** referred to here as **modbus:client** and the **revision number of the associated signatures** is 1*

  - For each custom context signature, a section "[context.identifier]", containing the following mandatory fields (the order of the fields in the section is free):

type =	Clarifies the scope of the signature	Value: asq
classification =	Categorisation of the signature	Value: **0** (Protections) **1** (Applications) **2** (Malware)
action_fw =	Action applied by the associated alarm to the custom signature Field composed of 4 values, separated by a comma,	Value: **pass / block** Example : pass,pass,pass,pass pass,pass,block,block

	without space, corresponding to 4 predefined security models: Internet, Low, Medium and High	
level_fw =	Level assigned to the associated alarm Field composed of 4 values, separated by a comma, without space, corresponding to the 4 predefined security models: Internet, Low, Medium and High.	Value: **ignore / minor / major** Example : ignore,minor,major,major major,major,major
description =	Short description of the signature written in English. This text is displayed in the **Message** column of the **Applications and Protection** module	Value: Free text framed by Exemple "Access to perdu.org site"
ldescr =	Complément d'information sur la signature, rédigé en anglais. Ce texte est affiché dans une infobulle, lors du survol du descriptif de l'alarme (colonne **Message** du module **Applications et protection**).	Valeur : Texte libre encadré par des guillemets Exemple "This custom signature is able to detect when a computer tries to connect to the website perdu.org"
1 =	First regular expression used in the signature	Value: Regular expression enclosed in inverted commas

In our example, we have :

modbus: client. 4096

This means that the **context** designated here is still **modbus:client**

and that the **identifier** of this custom signature filtering is **4096**

We will insert as many "[context.identifier]" sections as we have to define custom signatures in the considered context (within the limit of 2048 possible signatures per context).

type = asq => Scope of the signature: **asq**

severity = 2 => Severity level assigned to the detected threat (optional): **2 = moderate**

classification = 1 => Category : **1 = Applications**

action_fw = block, block, block, block => Action applied by the associated alarm

level_fw = minor,minor, minor,minor => Level assigned to the associated alarm

Idescr => Additional information on the signature:

"speed command greater than 50Hz"

comment => ?! comment

1 => First regular expression: here: framed **Modbus frame**

"\x00\x00\x00\x00\x00\x09\xff\x10\x03\xf6\x00\x01\x02\x00[\x32-\xff]"

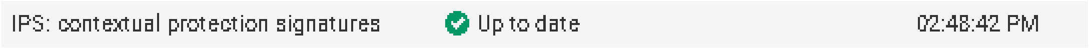
2. Setting up the configuration with Custom Signature ('Custom Pattern')

2.1. Custom Signatures and Active Update

- Initial context of the SNi40 Firewall configuration:

  Go to the part corresponding to the **CONFIGURATION > CONTROL PANEL** menu and look at the **ACTIVE UPDATE** section (lower right-hand part of the screen):

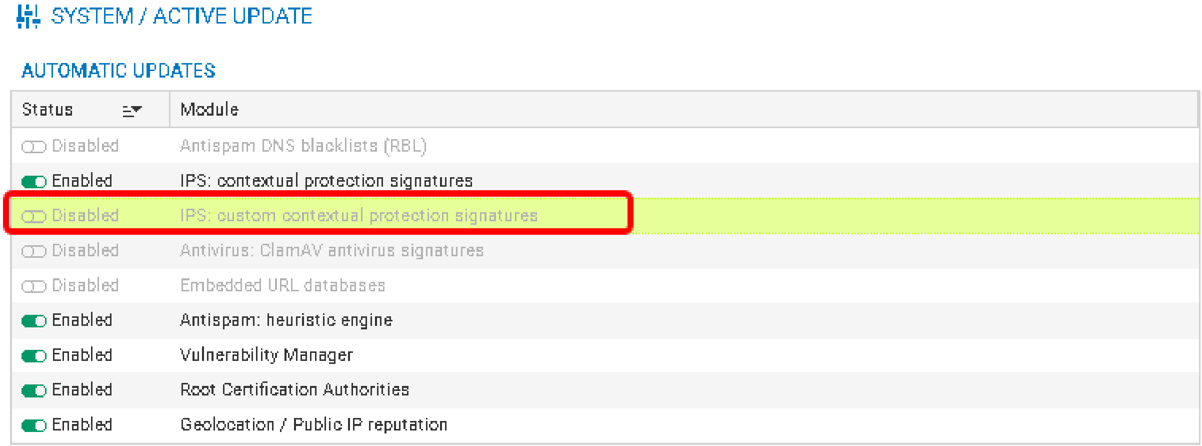
- Check that the **contextual protection IPS signatures** are **up to date**



IPS: contextual protection signatures ✓ Up to date 02:48:42 PM

- Check that **custom context signatures** are disabled, i.e. that custom signatures are excluded from the Auto Update mechanism

  Thus, in the **SYSTEM > Active Update > Automatic Updates module**, check that the line "IPS: custom contextual protection signatures" is disabled; this is to prevent custom signatures being overwritten by those retrieved from the Active Update server.

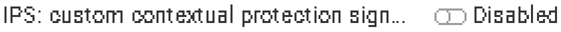


SYSTEM / ACTIVE UPDATE

AUTOMATIC UPDATES

Status	Module
Disabled	Antispam DNS blacklists (RBL)
Enabled	IPS: contextual protection signatures
Disabled	IPS: custom contextual protection signatures
Disabled	Antivirus: ClamAV antivirus signatures
Disabled	Embedded URL databases
Enabled	Antispam: heuristic engine
Enabled	Vulnerability Manager
Enabled	Root Certification Authorities
Enabled	Geolocation / Public IP reputation

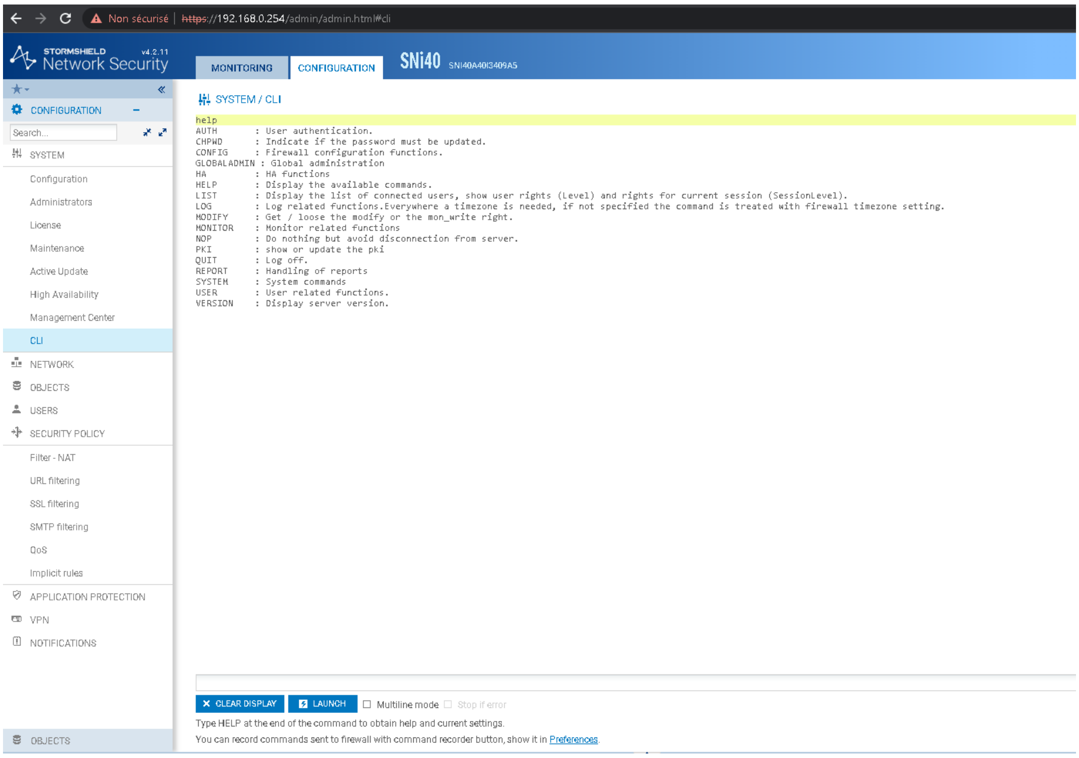
- As a result, the **DASHBOARD** in turn reflects the fact that these custom contextual protection signatures are disabled



IPS: custom contextual protection sign... Disabled

2.2. CLI Console: Enable custom signature support

- On the graphical interface, go to **CONFIGURATION > SYSTEM > CLI Console**



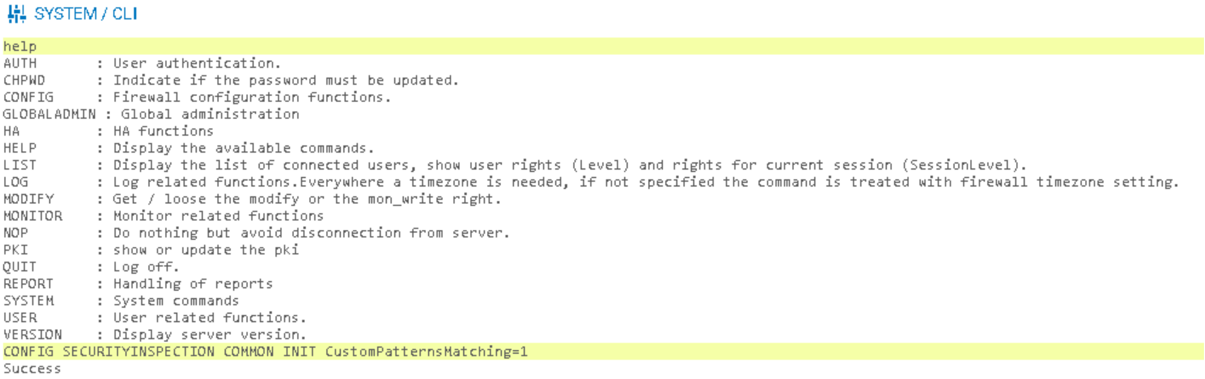
```
help
AUTH        : User authentication.
CHPWD       : Indicate if the password must be updated.
CONFIG      : Firewall configuration functions.
GLOBALADMIN : Global administration
HA          : HA functions
HELP        : Display the available commands.
LIST        : Display the list of connected users, show user rights (Level) and rights for current session (SessionLevel).
LOG         : Log related functions.Everywhere a timezone is needed, if not specified the command is treated with firewall timezone setting.
MODIFY      : Get / loose the modify or the mon_write right.
MONITOR     : Monitor related functions
NOP         : Do nothing but avoid disconnection from server.
PKI         : show or update the pki
QUIT        : Log off.
REPORT      : Handling of reports
SYSTEM      : System commands
USER        : User related functions.
VERSION     : Display server version.
```

Type HELP at the end of the command to obtain help and current settings.

You can record commands sent to firewall with command recorder button, show it in Preferences.

- Activation of personalized signatures.
  Type and validate the following two commands successively, in the lower input field. First enter the command below:

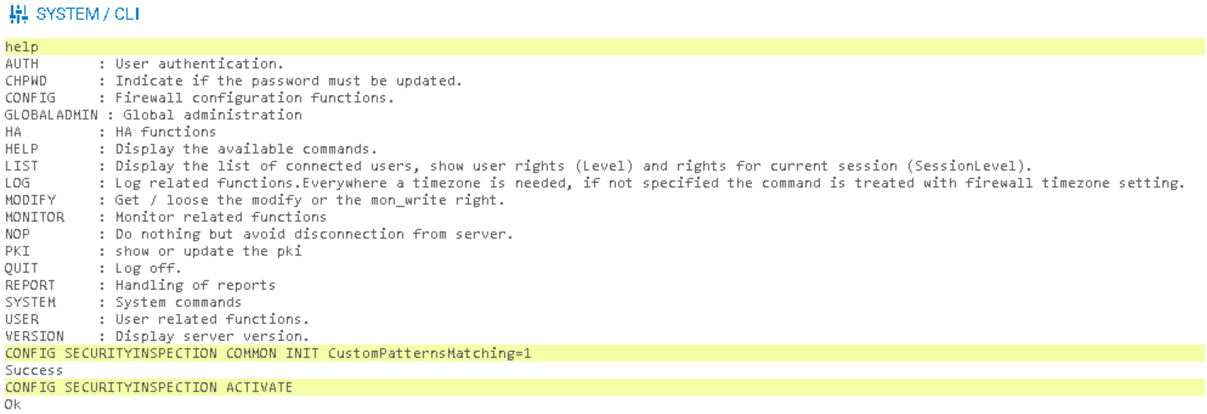
  CONFIG SECURITYINSPECTION COMMON INIT CustomPatternsMatching=1



```
help
AUTH        : User authentication.
CHPWD       : Indicate if the password must be updated.
CONFIG      : Firewall configuration functions.
GLOBALADMIN : Global administration
HA          : HA functions
HELP        : Display the available commands.
LIST        : Display the list of connected users, show user rights (Level) and rights for current session (SessionLevel).
LOG         : Log related functions.Everywhere a timezone is needed, if not specified the command is treated with firewall timezone setting.
MODIFY      : Get / loose the modify or the mon_write right.
MONITOR     : Monitor related functions
NOP         : Do nothing but avoid disconnection from server.
PKI         : show or update the pki
QUIT        : Log off.
REPORT      : Handling of reports
SYSTEM      : System commands
USER        : User related functions.
VERSION     : Display server version.
CONFIG SECURITYINSPECTION COMMON INIT CustomPatternsMatching=1
Success
```

Then enter the command below:

CONFIG SECURITYINSPECTION ACTIVATE

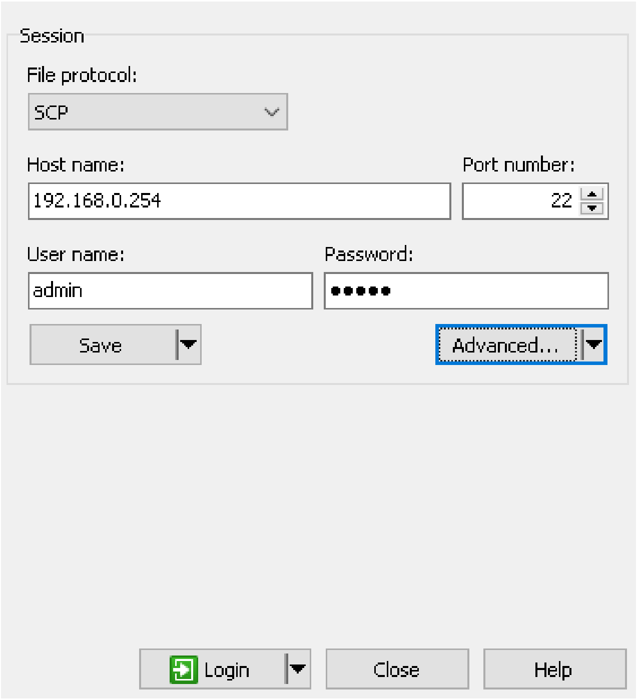


SYSTEM / CLI

```
help
AUTH        : User authentication.
CHPWD       : Indicate if the password must be updated.
CONFIG      : Firewall configuration functions.
GLOBALADMIN : Global administration
HA          : HA functions
HELP        : Display the available commands.
LIST        : Display the list of connected users, show user rights (Level) and rights for current session (SessionLevel).
LOG         : Log related functions.Everywhere a timezone is needed, if not specified the command is treated with firewall timezone setting.
MODIFY      : Get / loose the modify or the mon_write right.
MONITOR     : Monitor related functions
NOP         : Do nothing but avoid disconnection from server.
PKI         : show or update the pki
QUIT        : Log off.
REPORT      : Handling of reports
SYSTEM      : System commands
USER        : User related functions.
VERSION     : Display server version.
CONFIG SECURITYINSPECTION COMMON INIT CustomPatternsMatching=1
Success
CONFIG SECURITYINSPECTION ACTIVATE
Ok
```

2.3. Installing the custom signature file on the SNi40 with WinSCP

- Using the WinSCP utility, copy the file Prohibit50ormore_FC16.in (supplied) to the /usr/Firewall/ConfigFiles folder of the SNi40
- When using **WinSCP** for the first time, enter the host name (at most the IP address of the SNi40 Firewall) and the ID and password used to enter the configuration of the Firewall.



Session

File protocol: SCP

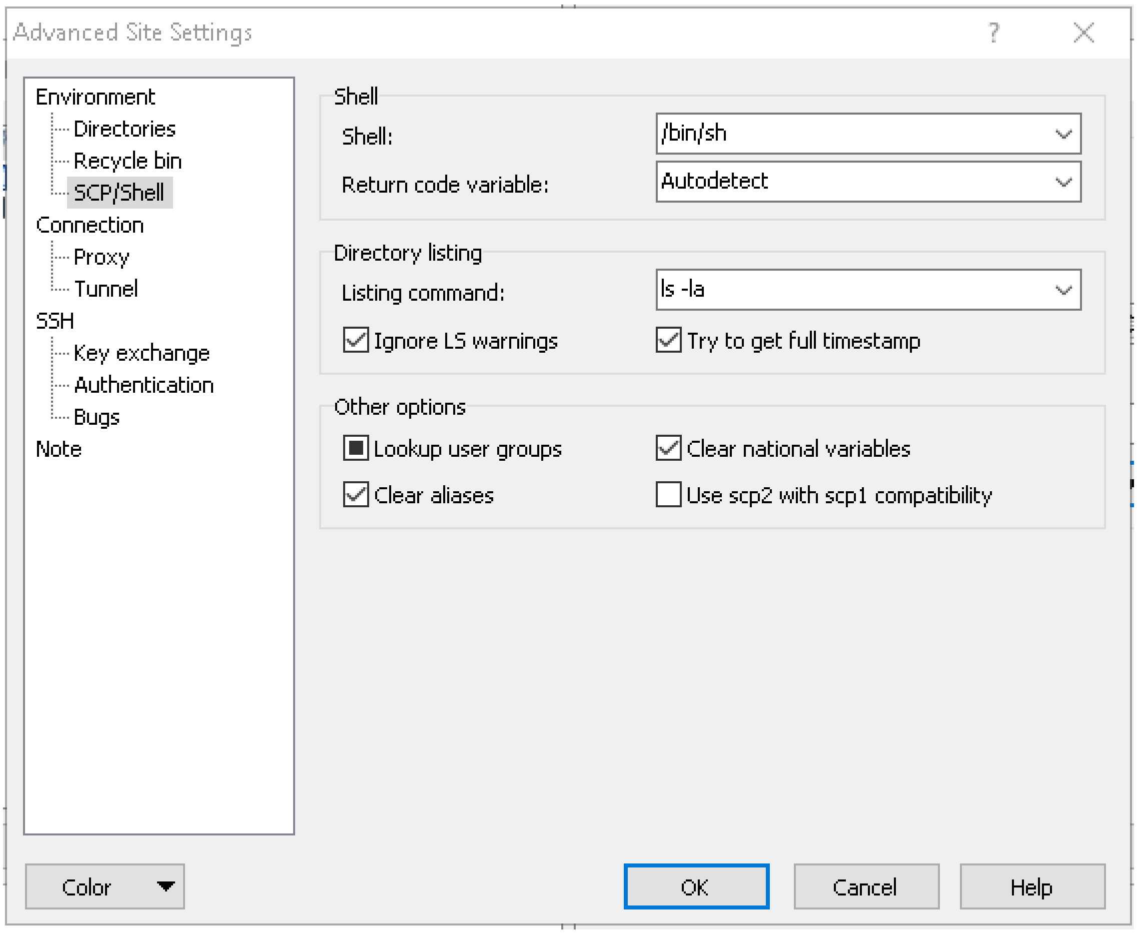
Host name: 192.168.0.254

Port number: 22

User name: admin

Password: ●●●●●

- Click on the **Advanced** button and after selecting the **SCP/Shell** entry, enter and validate **/bin/sh** in the **Shell** field :



Shell

Shell: /bin/sh

Return code variable: Autodetect

Directory listing

Listing command: ls -la

☑ Ignore LS warnings ☑ Try to get full timestamp

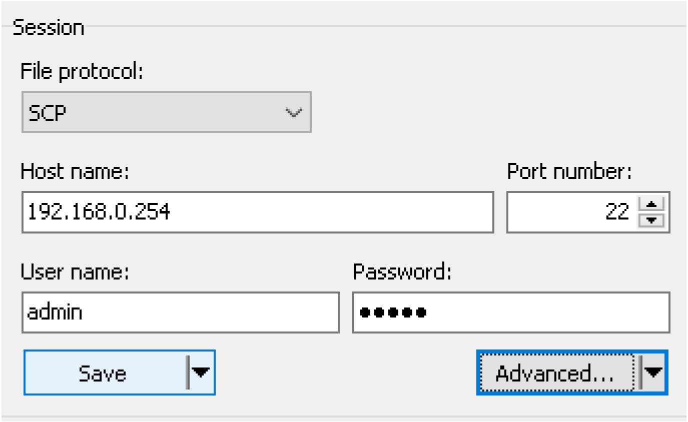
Other options

■ Lookup user groups ☑ Clear national variables

☑ Clear aliases □ Use scp2 with scp1 compatibility

The result will be that you will see the development of directory trees on the display

- If necessary, save the settings for this session for later use (Save button ...)



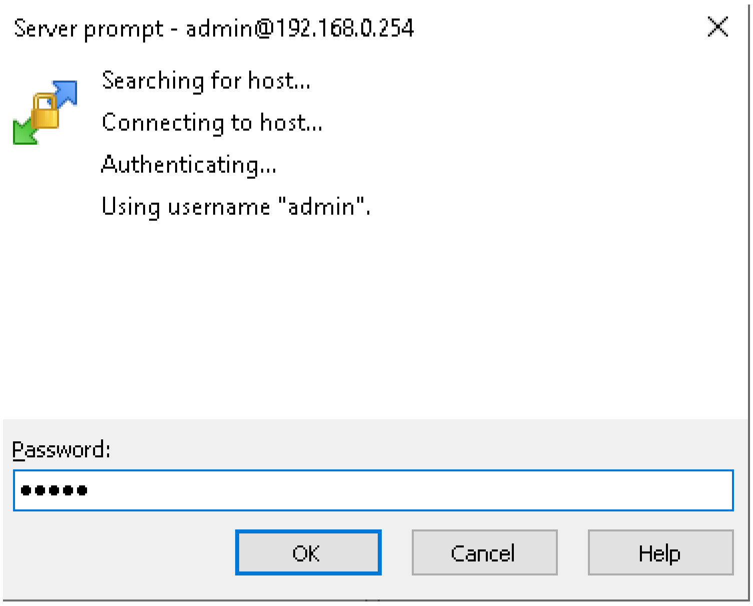
Session

File protocol: SCP

Host name: 192.168.0.254 Port number: 22

User name: admin Password: ●●●●●

in which case you will be asked to enter the password on the keyboard to access the SNi40

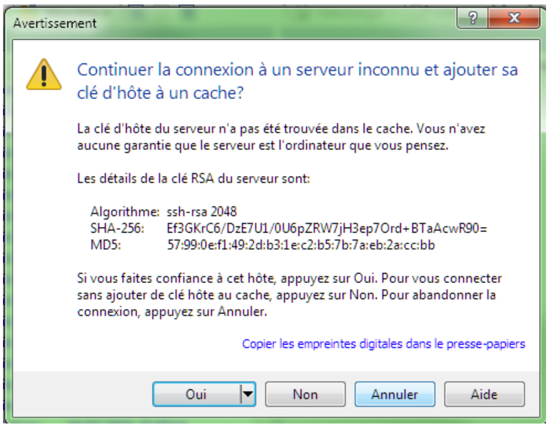


Server prompt - admin@192.168.0.254

Searching for host...
Connecting to host...
Authenticating...
Using username "admin".

Password:
●●●●●

- Connect to the firewall (if necessary, override a security warning)



Avertissement

Continuer la connexion à un serveur inconnu et ajouter sa clé d'hôte à un cache?

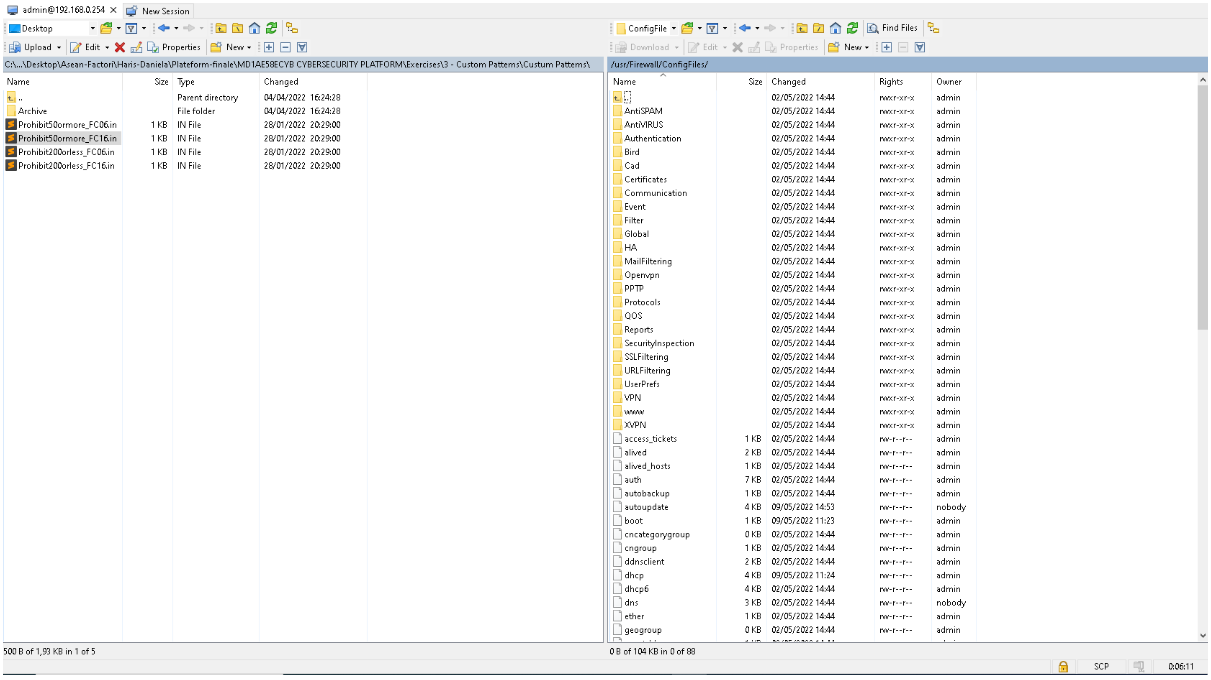
La clé d'hôte du serveur n'a pas été trouvée dans le cache. Vous n'avez aucune garantie que le serveur est l'ordinateur que vous pensez.

Les détails de la clé RSA du serveur sont:

```
Algorithme:  ssh-rsa 2048
SHA-256:     Ef3GKrC6/DzE7U1/0U6pZRW7jH3ep7Ord+BTaAcwR90=
MD5:         57:99:0e:f1:49:2d:b3:1e:c2:b5:7b:7a:eb:2a:cc:bb
```

Si vous faites confiance à cet hôte, appuyez sur Oui. Pour vous connecter sans ajouter de clé hôte au cache, appuyez sur Non. Pour abandonner la connexion, appuyez sur Annuler.

- Make sure that the left-hand side of the display shows the disk directory where the .in file to be copied is located, and that the right-hand side of the display shows the target directory on the SNi40 :



C:\...\Desktop\Asean-Factori\Haris-Daniela\Plateform-finale\MD1AE58ECYB CYBERSECURITY PLATFORM\Exercises\3 - Custom Patterns\Custum Patterns\

Name	Size	Type	Changed
..		Parent directory	04/04/2022 16:24:28
Archive		File folder	04/04/2022 16:24:28
Prohibit50ormore_FC06.in	1 KB	IN File	28/01/2022 20:29:00
Prohibit50ormore_FC16.in	1 KB	IN File	28/01/2022 20:29:00
Prohibit200orless_FC06.in	1 KB	IN File	28/01/2022 20:29:00
Prohibit200orless_FC16.in	1 KB	IN File	28/01/2022 20:29:00

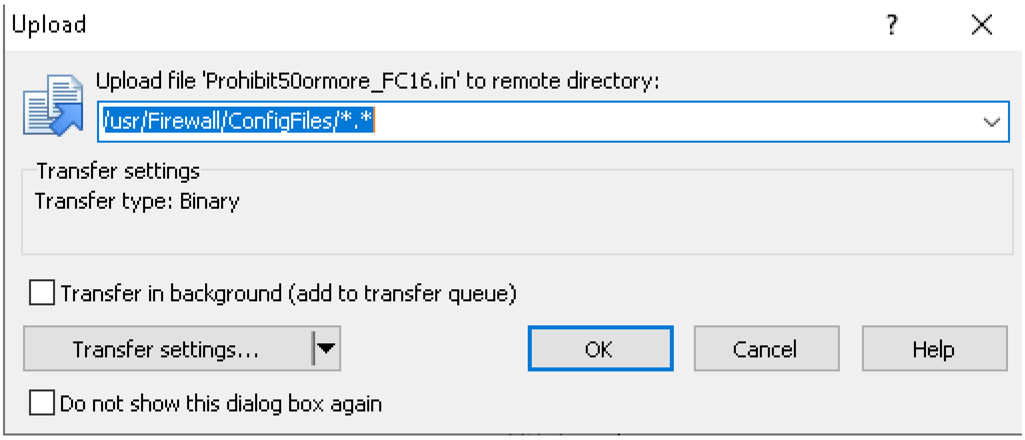
500 B of 1,93 KB in 1 of 5

/usr/Firewall/ConfigFiles/

Name	Size	Changed	Rights	Owner
..		02/05/2022 14:44	rwxr-xr-x	admin
AntiSPAM		02/05/2022 14:44	rwxr-xr-x	admin
AntiVIRUS		02/05/2022 14:44	rwxr-xr-x	admin
Authentication		02/05/2022 14:44	rwxr-xr-x	admin
Bird		02/05/2022 14:44	rwxr-xr-x	admin
Cad		02/05/2022 14:44	rwxr-xr-x	admin
Certificates		02/05/2022 14:44	rwxr-xr-x	admin
Communication		02/05/2022 14:44	rwxr-xr-x	admin
Event		02/05/2022 14:44	rwxr-xr-x	admin
Filter		02/05/2022 14:44	rwxr-xr-x	admin
Global		02/05/2022 14:44	rwxr-xr-x	admin
HA		02/05/2022 14:44	rwxr-xr-x	admin
MailFiltering		02/05/2022 14:44	rwxr-xr-x	admin
Openvpn		02/05/2022 14:44	rwxr-xr-x	admin
PPTP		02/05/2022 14:44	rwxr-xr-x	admin
Protocols		02/05/2022 14:44	rwxr-xr-x	admin
QOS		02/05/2022 14:44	rwxr-xr-x	admin
Reports		02/05/2022 14:44	rwxr-xr-x	admin
SecurityInspection		02/05/2022 14:44	rwxr-xr-x	admin
SSLFiltering		02/05/2022 14:44	rwxr-xr-x	admin
URLFiltering		02/05/2022 14:44	rwxr-xr-x	admin
UserPrefs		02/05/2022 14:44	rwxr-xr-x	admin
VPN		02/05/2022 14:44	rwxr-xr-x	admin
www		02/05/2022 14:44	rwxr-xr-x	admin
XVPN		02/05/2022 14:44	rwxr-xr-x	admin
access_tickets	1 KB	02/05/2022 14:44	rw-r--r--	admin
alived	2 KB	02/05/2022 14:44	rw-r--r--	admin
alived_hosts	1 KB	02/05/2022 14:44	rw-r--r--	admin
auth	7 KB	02/05/2022 14:44	rw-r--r--	admin
autobackup	1 KB	02/05/2022 14:44	rw-r--r--	admin
autoupdate	4 KB	09/05/2022 14:53	rw-r--r--	nobody
boot	1 KB	09/05/2022 11:23	rw-r--r--	admin
cncategorygroup	0 KB	02/05/2022 14:44	rw-r--r--	admin
cngroup	1 KB	02/05/2022 14:44	rw-r--r--	admin
ddnsclient	2 KB	02/05/2022 14:44	rw-r--r--	admin
dhcp	4 KB	09/05/2022 11:24	rw-r--r--	admin
dhcp6	4 KB	02/05/2022 14:44	rw-r--r--	admin
dns	3 KB	02/05/2022 14:44	rw-r--r--	nobody
ether	1 KB	02/05/2022 14:44	rw-r--r--	admin
geogroup	0 KB	02/05/2022 14:44	rw-r--r--	admin

0 B of 104 KB in 0 of 88

- Copy via SCP (by drag'n drop using the WinSCP utility) the custom signature definition file Prohibit50ormore_FC16.in to the /usr/Firewall/ConfigFiles directory of the SNi40 firewall



Upload file 'Prohibit50ormore_FC16.in' to remote directory:

/usr/Firewall/ConfigFiles/*.*

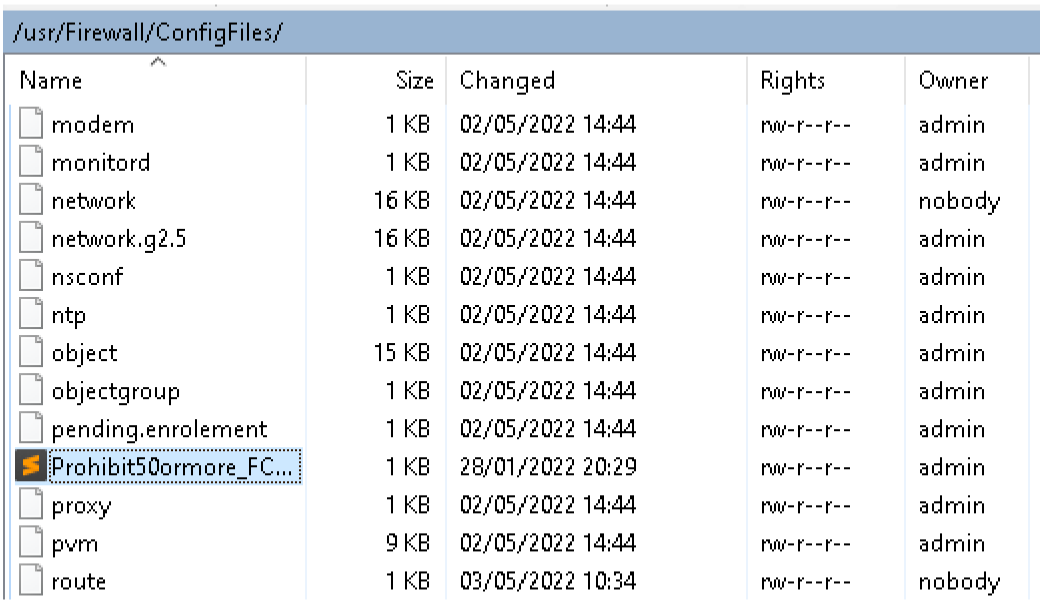
Transfer settings

Transfer type: Binary

☐ Transfer in background (add to transfer queue)

☐ Do not show this dialog box again

- Result:



/usr/Firewall/ConfigFiles/

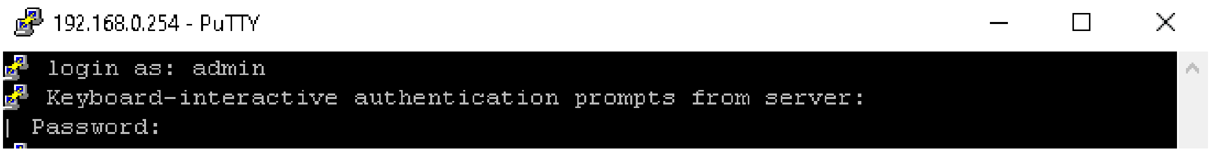
Name	Size	Changed	Rights	Owner
modem	1 KB	02/05/2022 14:44	rw-r--r--	admin
monitord	1 KB	02/05/2022 14:44	rw-r--r--	admin
network	16 KB	02/05/2022 14:44	rw-r--r--	nobody
network.g2.5	16 KB	02/05/2022 14:44	rw-r--r--	admin
nsconf	1 KB	02/05/2022 14:44	rw-r--r--	admin
ntp	1 KB	02/05/2022 14:44	rw-r--r--	admin
object	15 KB	02/05/2022 14:44	rw-r--r--	admin
objectgroup	1 KB	02/05/2022 14:44	rw-r--r--	admin
pending.enrolement	1 KB	02/05/2022 14:44	rw-r--r--	admin
Prohibit50ormore_FC...	1 KB	28/01/2022 20:29	rw-r--r--	admin
proxy	1 KB	02/05/2022 14:44	rw-r--r--	admin
pvm	9 KB	02/05/2022 14:44	rw-r--r--	admin
route	1 KB	03/05/2022 10:34	rw-r--r--	nobody

Note: The **ConfigFiles** directory is actually a link under the **Firewall** directory, which leads to the **/data/Main/ConfigFiles** directory

Note: with **WinSCP**, if by any chance you want to delete a directory created inadvertently on the SNi40 Firewall, you must first translate it to the local disk.

2.4. Enabling custom signature file support with Putty

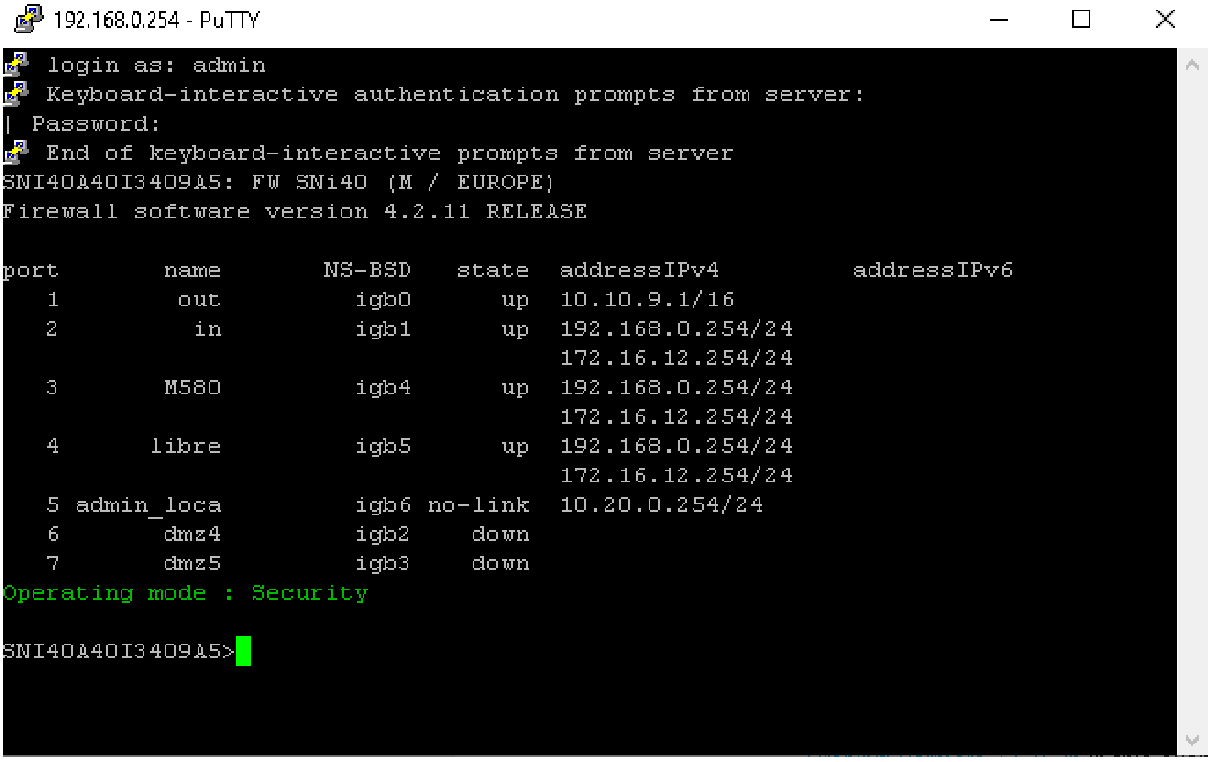
- Now check the validity of the custom signature definition file, in this case the file Prohibit50ormore_FC16.in in this example. To do this, we will use the **Putty** utility, which can be requested through WinSCP



192.168.0.254 - PuTTY

```
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
```

- Blindly enter the password (admin) and validate (Enter)

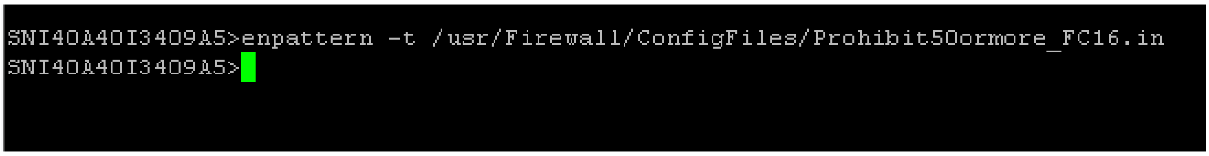


192.168.0.254 - PuTTY

```
 login as: admin
 Keyboard-interactive authentication prompts from server:
| Password:
 End of keyboard-interactive prompts from server
SNI40A40I3409A5: FW SNi40 (M / EUROPE)
Firewall software version 4.2.11 RELEASE

port       name       NS-BSD   state  addressIPv4         addressIPv6
   1        out         igb0      up  10.10.9.1/16
   2         in         igb1      up  192.168.0.254/24
                                      172.16.12.254/24
   3       M580         igb4      up  192.168.0.254/24
                                      172.16.12.254/24
   4      libre         igb5      up  192.168.0.254/24
                                      172.16.12.254/24
   5 admin_loca         igb6 no-link  10.20.0.254/24
   6       dmz4         igb2    down
   7       dmz5         igb3    down
Operating mode : Security

SNI40A40I3409A5>
```

- Enter and validate the following command line:

enpattern -t /usr/Firewall/ConfigFiles/Prohibit50ormore_FC16.in



```
SNI40A40I3409A5>enpattern -t /usr/Firewall/ConfigFiles/Prohibit50ormore_FC16.in
SNI40A40I3409A5>
```

Note: once the command string has been copied, right-clicking on **Putty** allows it to be pasted

If this signature definition file is invalid, one or more messages are displayed indicating the type of errors detected.

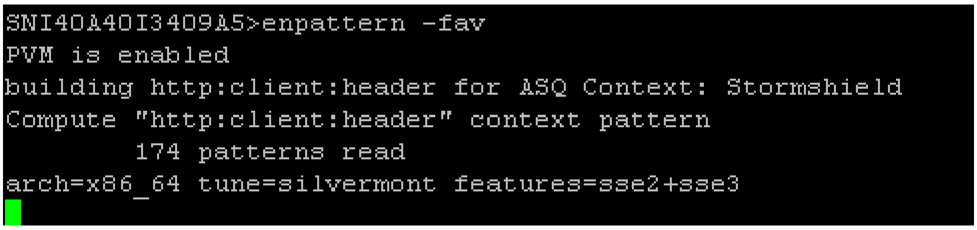
- Compile custom signatures :

  After correcting any anomalies detected in the custom signature definition file, run the command: enpattern -fav

  This command starts the compilation of all signatures (options -f and -a).

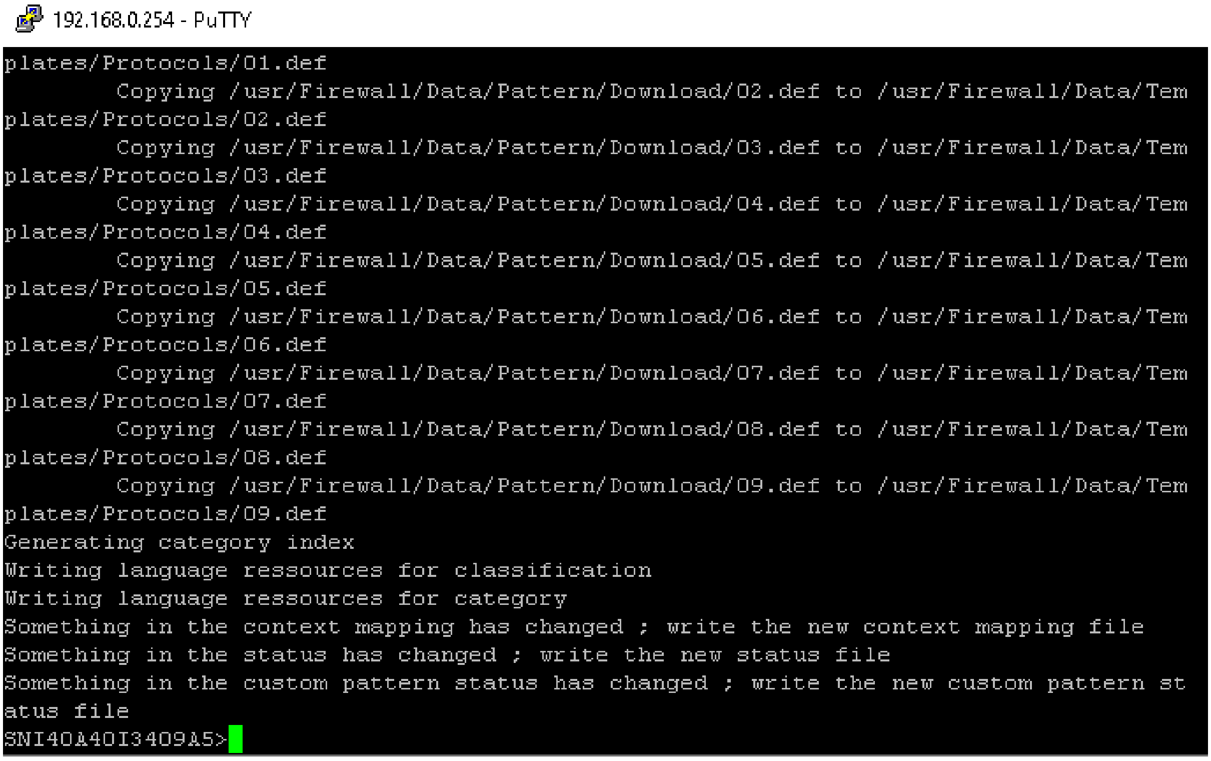
  (the -v option activates the verbose mode of the command).

- This translates into the following display event:



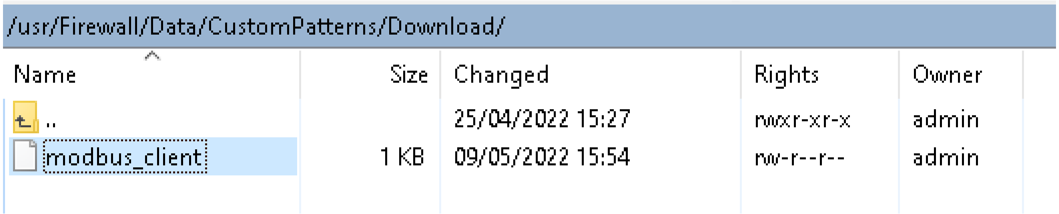
```
SNI40A40I3409A5>enpattern -fav
PVM is enabled
building http:client:header for ASQ Context: Stormshield
Compute "http:client:header" context pattern
        174 patterns read
arch=x86_64 tune=silvermont features=sse2+sse3

```

The execution continues for a good minute and results in the following display:



```
plates/Protocols/01.def
        Copying /usr/Firewall/Data/Pattern/Download/02.def to /usr/Firewall/Data/Tem
plates/Protocols/02.def
        Copying /usr/Firewall/Data/Pattern/Download/03.def to /usr/Firewall/Data/Tem
plates/Protocols/03.def
        Copying /usr/Firewall/Data/Pattern/Download/04.def to /usr/Firewall/Data/Tem
plates/Protocols/04.def
        Copying /usr/Firewall/Data/Pattern/Download/05.def to /usr/Firewall/Data/Tem
plates/Protocols/05.def
        Copying /usr/Firewall/Data/Pattern/Download/06.def to /usr/Firewall/Data/Tem
plates/Protocols/06.def
        Copying /usr/Firewall/Data/Pattern/Download/07.def to /usr/Firewall/Data/Tem
plates/Protocols/07.def
        Copying /usr/Firewall/Data/Pattern/Download/08.def to /usr/Firewall/Data/Tem
plates/Protocols/08.def
        Copying /usr/Firewall/Data/Pattern/Download/09.def to /usr/Firewall/Data/Tem
plates/Protocols/09.def
Generating category index
Writing language ressources for classification
Writing language ressources for category
Something in the context mapping has changed ; write the new context mapping file
Something in the status has changed ; write the new status file
Something in the custom pattern status has changed ; write the new custom pattern st
atus file
SNI40A40I3409A5>
```

*Note: The directory **/usr/Firewall/Data/CustomPatterns/Download** contains one file per context, containing all signatures specific to that context (example: **modbus_client**)*



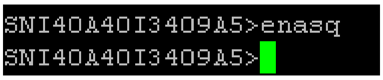
/usr/Firewall/Data/CustomPatterns/Download/

Name	Size	Changed	Rights	Owner
..		25/04/2022 15:27	rwxr-xr-x	admin
modbus_client	1 KB	09/05/2022 15:54	rw-r--r--	admin

- Enable custom signatures in the intrusion prevention engine

  Finally, enter and execute the following command line: enasq

  This is reflected in the following display event:



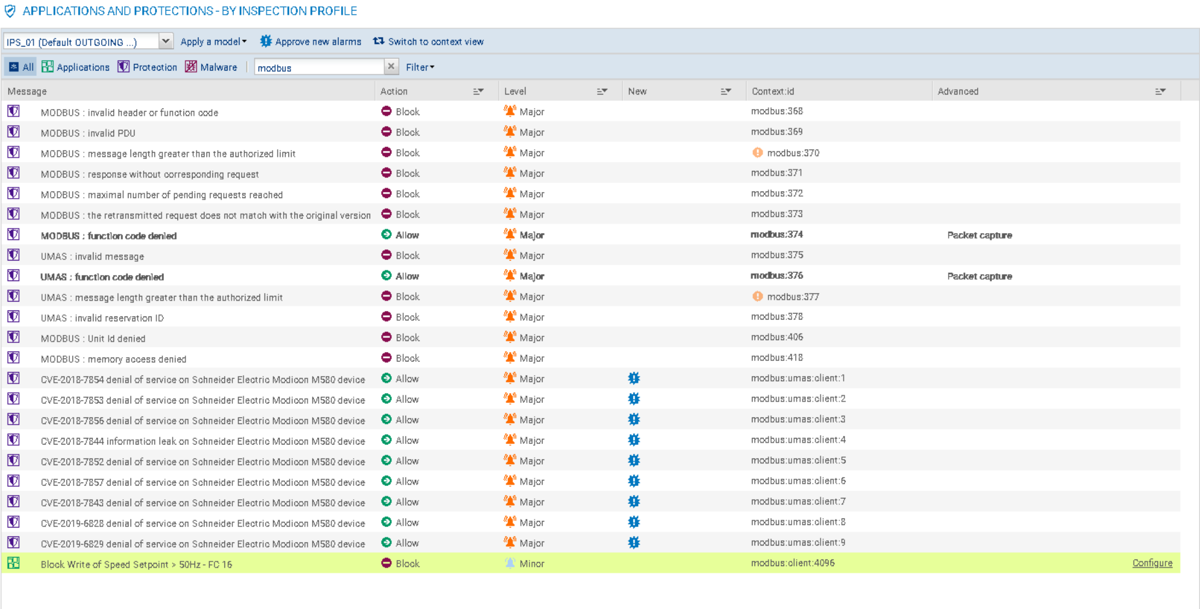
```
SNI40A40I3409A5>enasq
SNI40A40I3409A5>
```

This command forces the intrusion prevention engine to take into account previously compiled custom signatures.

2.5. Checking the presence of the personalized signature as protection

Now check that the added signature now appears in the **CONFIGURATION > APPLICATION PROTECTION > APPLICATIONS AND PROTECTIONS** menu:

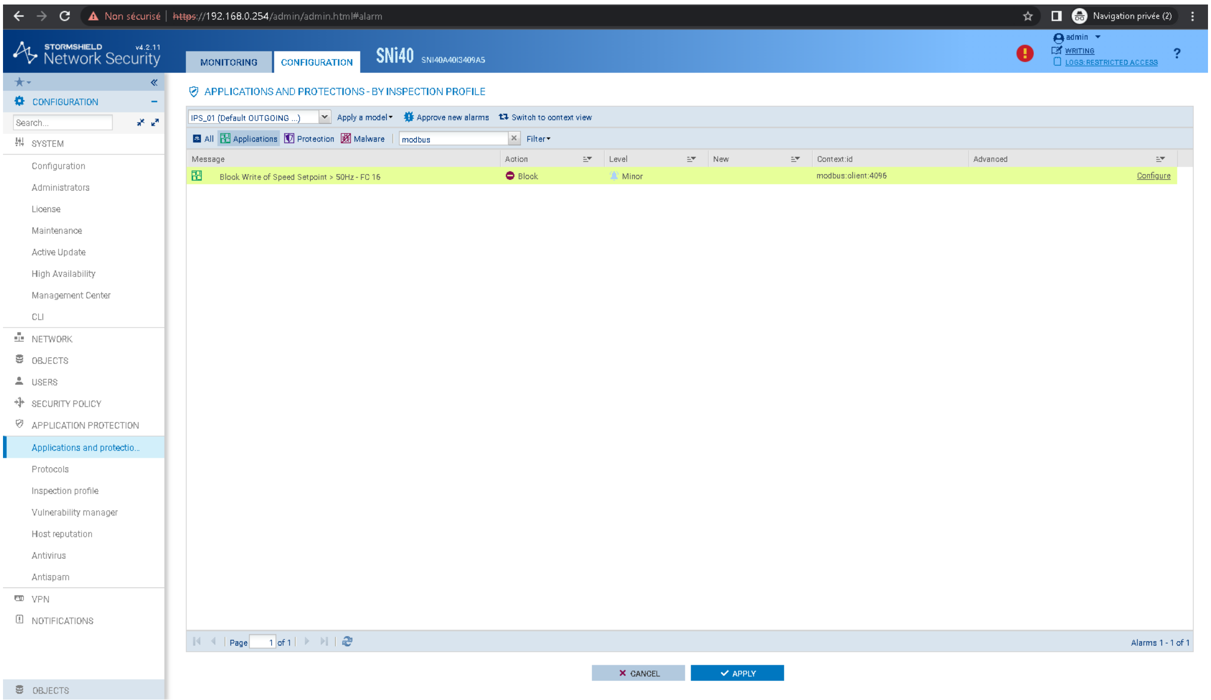
- Enter **modbus** in the filter field to restrict the scope of the displayed application protections



Message	Action	Level	New	Context:id	Advanced
MODBUS : invalid header or function code	Block	Major		modbus:368	
MODBUS : invalid PDU	Block	Major		modbus:369	
MODBUS : message length greater than the authorized limit	Block	Major		modbus:370	
MODBUS : response without corresponding request	Block	Major		modbus:371	
MODBUS : maximal number of pending requests reached	Block	Major		modbus:372	
MODBUS : the retransmitted request does not match with the original version	Block	Major		modbus:373	
MODBUS : function code denied	**Allow**	**Major**		**modbus:374**	**Packet capture**
UMAS : invalid message	Block	Major		modbus:375	
UMAS : function code denied	**Allow**	**Major**		**modbus:376**	**Packet capture**
UMAS : message length greater than the authorized limit	Block	Major		modbus:377	
UMAS : invalid reservation ID	Block	Major		modbus:378	
MODBUS : Unit Id denied	Block	Major		modbus:406	
MODBUS : memory access denied	Block	Major		modbus:418	
CVE-2018-7854 denial of service on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:1	
CVE-2018-7853 denial of service on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:2	
CVE-2018-7856 denial of service on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:3	
CVE-2018-7844 information leak on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:4	
CVE-2018-7852 denial of service on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:5	
CVE-2018-7857 denial of service on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:6	
CVE-2018-7843 denial of service on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:7	
CVE-2019-6828 denial of service on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:8	
CVE-2019-6829 denial of service on Schneider Electric Modicon M580 device	Allow	Major	✱	modbus:umas:client:9	
Block Write of Speed Setpoint > 50Hz - FC 16	Block	Minor		modbus:client:4096	Configure

NB: Click on the selector on the right-hand side of the screen to open the dialogue box for customizing the columns to be displayed.

- Click once on **Applications** to restrict to that category, then click on that column heading to display the custom signatures first:

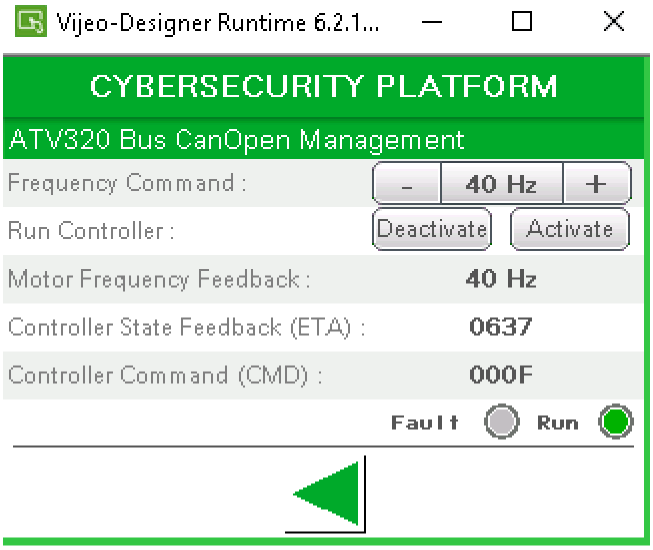


Message	Action	Level	New	Context:id	Advanced
Block Write of Speed Setpoint > 50Hz - FC 16	Block	Minor		modbus:client:4096	Configure

2.6. Test via Vijeo Designer in Simulation mode

It is checked that it is not possible to set as a new speed setpoint a value greater than 50 (i.e. values between 50 Hz and 250 Hz are rejected)

- Change the speed setpoint (%MW1014) to 40 :
  request accepted by filtering via Custom Pattern (because less than or equal to 50)



Vijeo-Designer Runtime 6.2.1...
CYBERSECURITY PLATFORM
ATV320 Bus CanOpen Management
-
+
Deactivate
Activate
Fault
Run

Frequency Command : 40 Hz

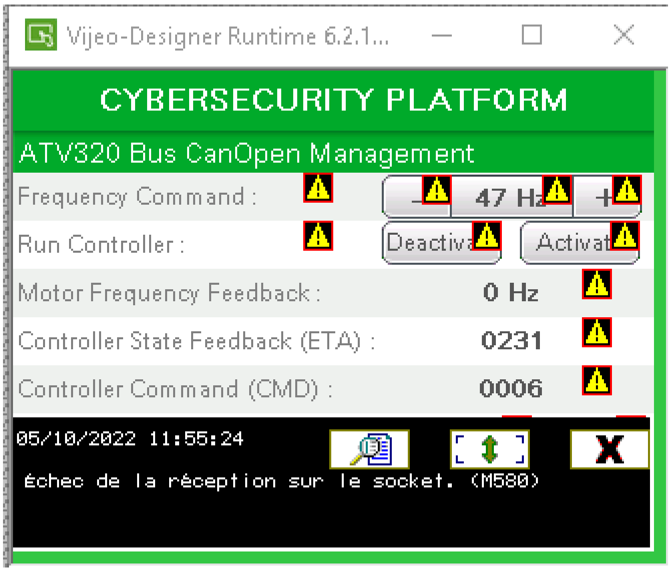
Run Controller :

Motor Frequency Feedback : 40 Hz

Controller State Feedback (ETA) : 0637

Controller Command (CMD) : 000F

- Change the speed setpoint (%MW1014) to 60 :
  request rejected by filtering via Custom Pattern (because greater than 50)



Vijeo-Designer Runtime 6.2.1...
CYBERSECURITY PLATFORM
ATV320 Bus CanOpen Management
-
+
Deactiva
Activat
X

Frequency Command : 47 Hz

Run Controller :

Motor Frequency Feedback : 0 Hz

Controller State Feedback (ETA) : 0231

Controller Command (CMD) : 0006

05/10/2022 11:55:24

Échec de la réception sur le socket. (M580)

The request is rejected. The old setpoint is retained

3. Changing values in custom patterns

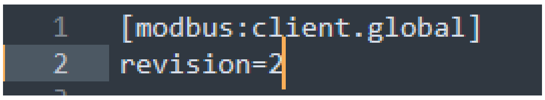
The modification of values in custom patterns is done in 2 steps:

(Follow this description carefully).

3.1. Step 1: Delete the previous signature file

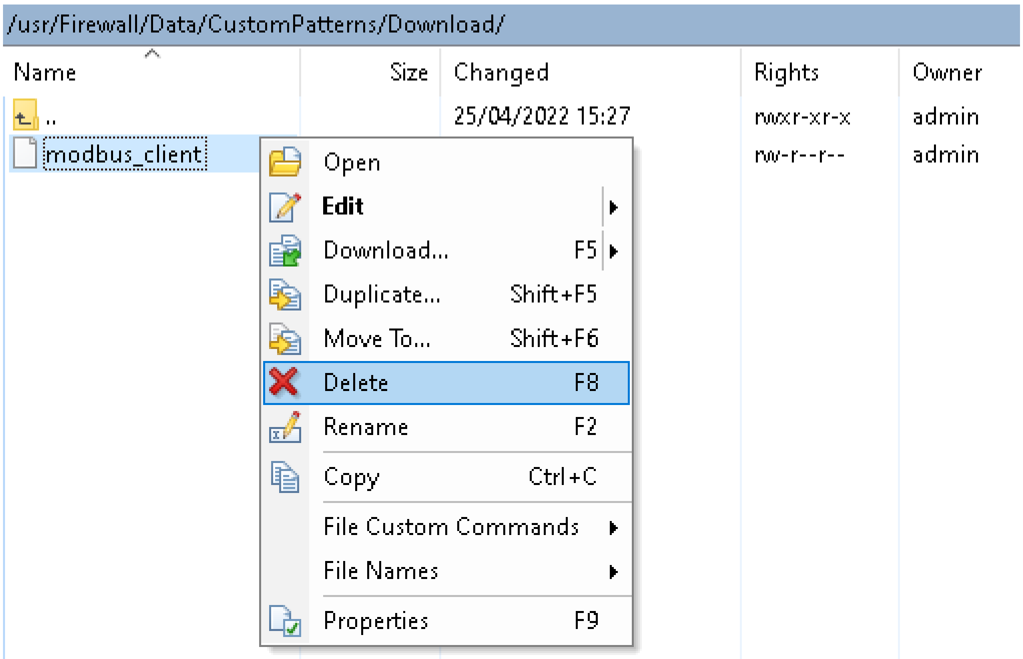
This first step is equivalent to the elimination of the previous signature file, and the deletion of its recognition.

- On the Development Station, return to the previously used custom signature definition file (in) previously used:
  a) increment the revision number
  b) Delete the previous signature definition



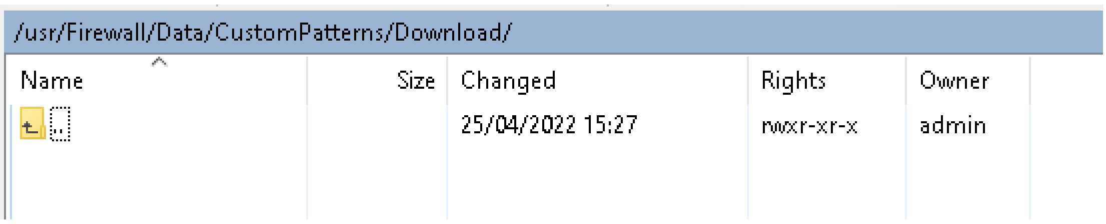
```
[modbus:client.global]
revision=2
```

- On the Firewall (recipe), delete the 'unit' file (example: **modbus_client**) which is located in the directory **/usr/Firewall/Data/CustomPatterns/Download**



/usr/Firewall/Data/CustomPatterns/Download/

Name	Size	Changed	Rights	Owner
..		25/04/2022 15:27	rwxr-xr-x	admin
modbus_client			rw-r--r--	admin



/usr/Firewall/Data/CustomPatterns/Download/

Name	Size	Changed	Rights	Owner
..		25/04/2022 15:27	rwxr-xr-x	admin

- Then enter the commands previously used in SSH (see previous manipulations via WinSCP/Putty), in order to make the previously created application alarm disappear: (the 'cleared' file will have been substituted for the previously used in file, [Prohibit50ormore_FC16.in], to be modified).

enpattern -t /usr/Firewall/ConfigFiles/Prohibit50ormore_FC16.in

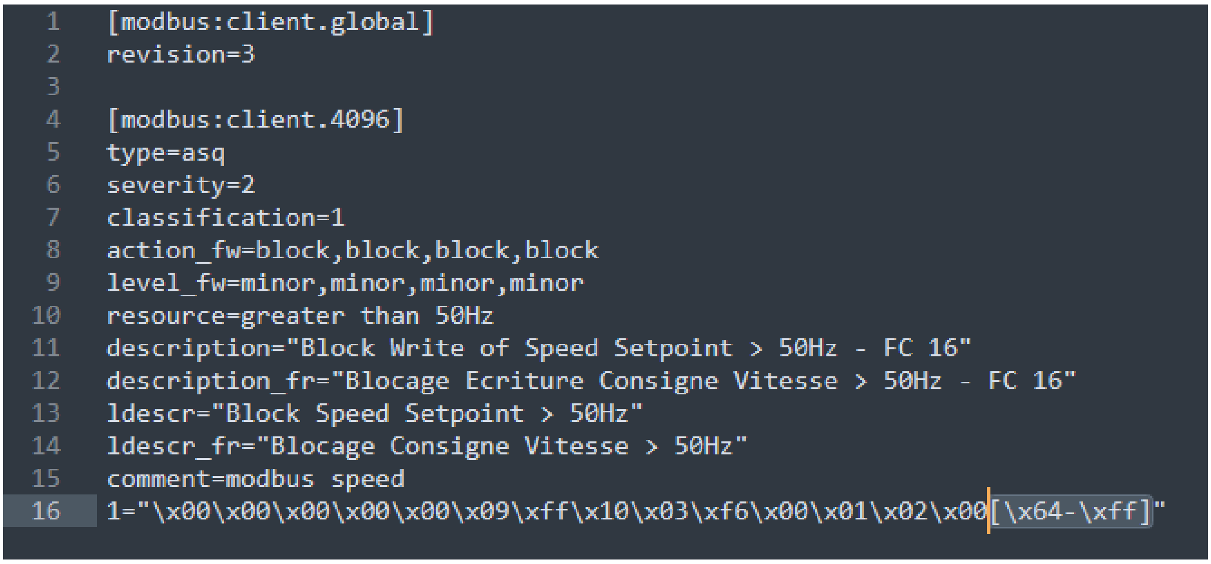
enpattern –fav

enasq

3.2. Step 2: Making changes to the signature file

This second step involves :

- Edit the target in-file again (Prohibit50ormore_FC16.in)
  Example: change the range of valid values
- At the same time perform a new increment of its revision number



```
[modbus:client.global]
revision=3

[modbus:client.4096]
type=asq
severity=2
classification=1
action_fw=block,block,block,block
level_fw=minor,minor,minor,minor
resource=greater than 50Hz
description="Block Write of Speed Setpoint > 50Hz - FC 16"
description_fr="Blocage Ecriture Consigne Vitesse > 50Hz - FC 16"
ldescr="Block Speed Setpoint > 50Hz"
ldescr_fr="Blocage Consigne Vitesse > 50Hz"
comment=modbus speed
1="\x00\x00\x00\x00\x00\x09\xff\x10\x03\xf6\x00\x01\x02\x00[\x64-\xff]"
```

- Redo the operation to add the application signatures on the firewall
  > copy the modified .in file to ConfigFiles
  (new increment + new or modified analysis)
  > SSH sequence execution

  enpattern -t /usr/Firewall/ConfigFiles/Prohibit50ormore_FC06.in

  enpattern –fav

  enasq

4. Use of Custom Signature Variants ('Custom Patterns')

We now wish, for example, to implement a variant of the previous filtering (which blocked setpoints above 50) by now blocking setpoints below 200 Hz (80% of the drive's maximum speed).

In other words, we want to block the setpoints between 0 and 200.

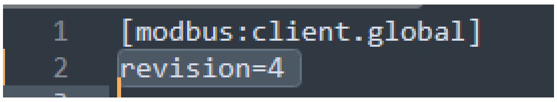
To do this, we will create a new in file (Prohibit200orless_FC16.in), based on the previous file (Prohibit50ormore_FC16.in)

4.1. Step 1: Delete the previous signature file

> Modification of the description lines of the previous file in

- incrementing the revision number

- deletion of the definition of the previous signature



```
[modbus:client.global]
revision=4
```

> Delete (if it exists) the '**unit**' file (example: **modbus_client**) present on the directory **/usr/Firewall/Data/CustomPatterns/Download**

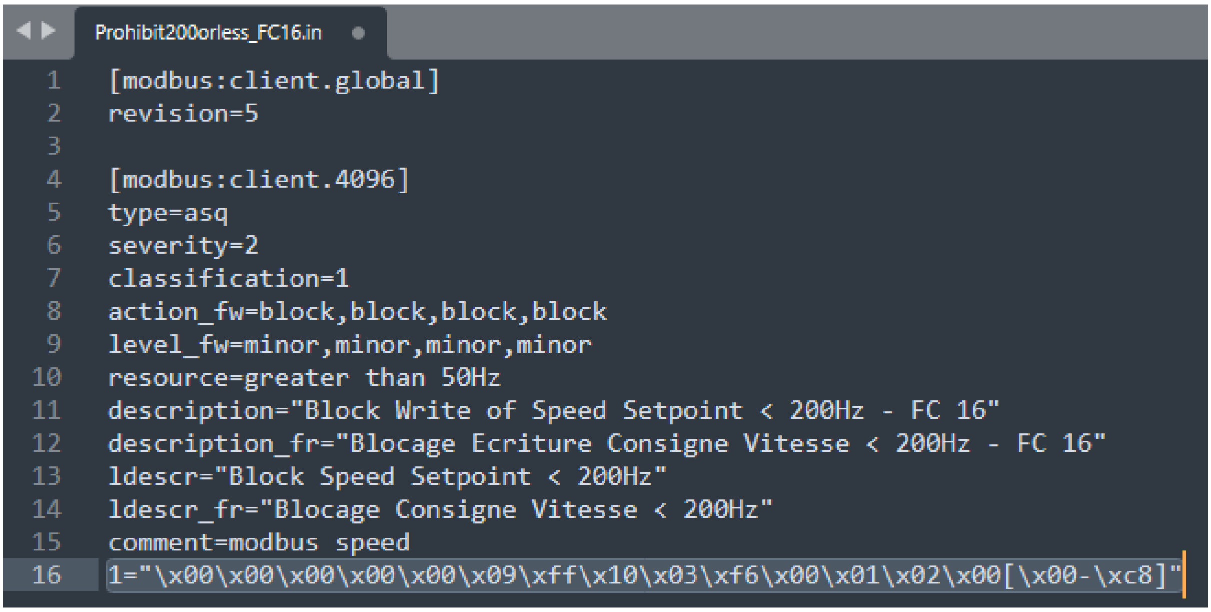
> **SSH** sequence execution

```
enpattern -t /usr/Firewall/ConfigFiles/Prohibit50ormore_FC06.in

enpattern –fav

enasq
```

4.2. Step 2: Editing / Integrating the new signature file

> Editing the description lines of the new in file (**Prohibit200orless_FC16.in**), derived from the previous one), installed on **ConfigFiles**

- New revision number increment
- Last line: c8 (hexadecimal value) = 200 (decimal value)



```
[modbus:client.global]
revision=5

[modbus:client.4096]
type=asq
severity=2
classification=1
action_fw=block,block,block,block
level_fw=minor,minor,minor,minor
resource=greater than 50Hz
description="Block Write of Speed Setpoint < 200Hz - FC 16"
description_fr="Blocage Ecriture Consigne Vitesse < 200Hz - FC 16"
ldescr="Block Speed Setpoint < 200Hz"
ldescr_fr="Blocage Consigne Vitesse < 200Hz"
comment=modbus speed
1="\x00\x00\x00\x00\x00\x09\xff\x10\x03\xf6\x00\x01\x02\x00[\x00-\xc8]"
```

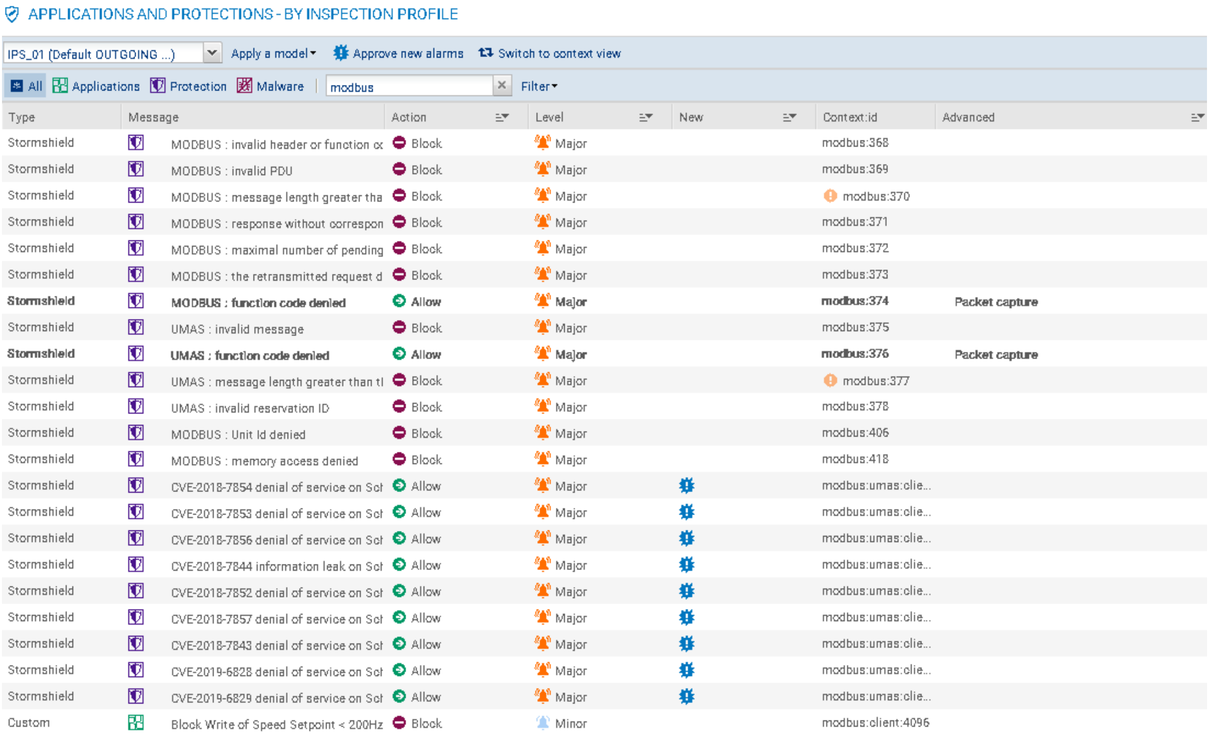
> SSH sequence execution

```
enpattern -t /usr/Firewall/ConfigFiles/Prohibit200orless_FC16.in

enpattern –fav

enasq
```

4.3. Checking the presence of the personalized signature as protection

Now check that the added signature now appears in the **CONFIGURATION > APPLICATION PROTECTION > Applications and protections** menu:

- Enter **modbus** in the filter field to restrict the scope of of the displayed application protections



APPLICATIONS AND PROTECTIONS - BY INSPECTION PROFILE

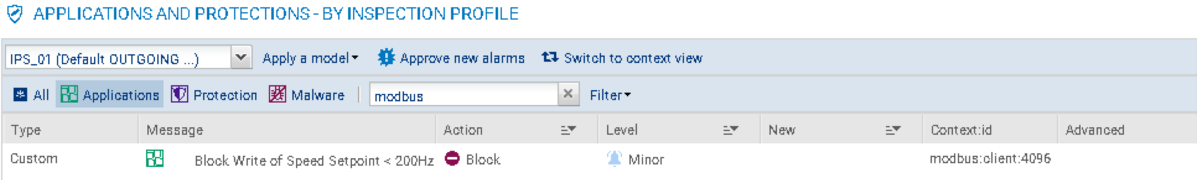
IPS_01 (Default OUTGOING ...)

Filter: modbus

Type	Message	Action	Level	New	Context:id	Advanced
Stormshield	MODBUS : invalid header or function cc	Block	Major		modbus:368	
Stormshield	MODBUS : invalid PDU	Block	Major		modbus:369	
Stormshield	MODBUS : message length greater tha	Block	Major		⚠ modbus:370	
Stormshield	MODBUS : response without correspon	Block	Major		modbus:371	
Stormshield	MODBUS : maximal number of pending	Block	Major		modbus:372	
Stormshield	MODBUS : the retransmitted request d	Block	Major		modbus:373	
Stormshield	**MODBUS : function code denied**	**Allow**	**Major**		**modbus:374**	**Packet capture**
Stormshield	UMAS : invalid message	Block	Major		modbus:375	
Stormshield	**UMAS : function code denied**	**Allow**	**Major**		**modbus:376**	**Packet capture**
Stormshield	UMAS : message length greater than tl	Block	Major		⚠ modbus:377	
Stormshield	UMAS : invalid reservation ID	Block	Major		modbus:378	
Stormshield	MODBUS : Unit Id denied	Block	Major		modbus:406	
Stormshield	MODBUS : memory access denied	Block	Major		modbus:418	
Stormshield	CVE-2018-7854 denial of service on Sct	Allow	Major	✱	modbus:umas:clie...	
Stormshield	CVE-2018-7853 denial of service on Sct	Allow	Major	✱	modbus:umas:clie...	
Stormshield	CVE-2018-7856 denial of service on Sct	Allow	Major	✱	modbus:umas:clie...	
Stormshield	CVE-2018-7844 information leak on Sct	Allow	Major	✱	modbus:umas:clie...	
Stormshield	CVE-2018-7852 denial of service on Sct	Allow	Major	✱	modbus:umas:clie...	
Stormshield	CVE-2018-7857 denial of service on Sct	Allow	Major	✱	modbus:umas:clie...	
Stormshield	CVE-2018-7843 denial of service on Sct	Allow	Major	✱	modbus:umas:clie...	
Stormshield	CVE-2019-6828 denial of service on Sct	Allow	Major	✱	modbus:umas:clie...	
Stormshield	CVE-2019-6829 denial of service on Sct	Allow	Major	✱	modbus:umas:clie...	
Custom	Block Write of Speed Setpoint < 200Hz	Block	Minor		modbus:client:4096	

NB: Click on the selector on the right-hand side of the screen to open the dialogue box for customizing the columns to be displayed.

- Click once on **Applications** to restrict to that category, then click on that column heading to display the custom signatures first:



APPLICATIONS AND PROTECTIONS - BY INSPECTION PROFILE

IPS_01 (Default OUTGOING ...)

Filter: modbus

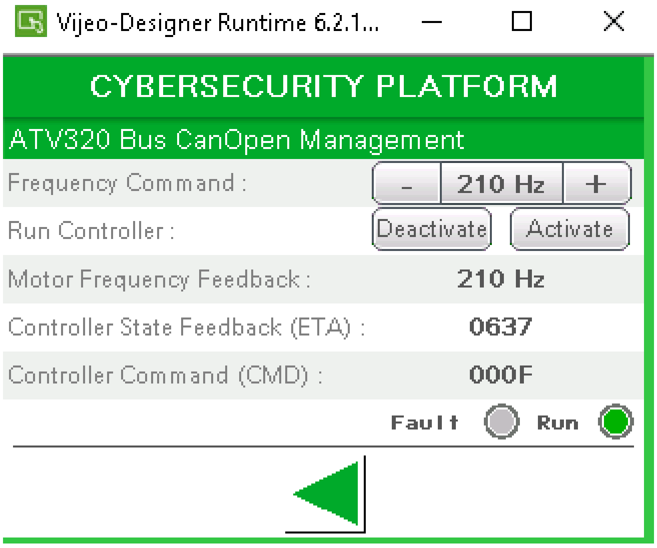
Type	Message	Action	Level	New	Context:id	Advanced
Custom	Block Write of Speed Setpoint < 200Hz	Block	Minor		modbus:client:4096	

4.4. Test via Vijeo Designer in Simulation mode

It is checked that it is not possible to set as a new speed setpoint a value lower than 200 (i.e. values between 0 Hz and 200 Hz are rejected)

- Change the speed setpoint (%MW1014) to 210 :

request accepted by filtering via Custom Pattern (because greater than or equal to 200)



CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : 210 Hz

Run Controller :

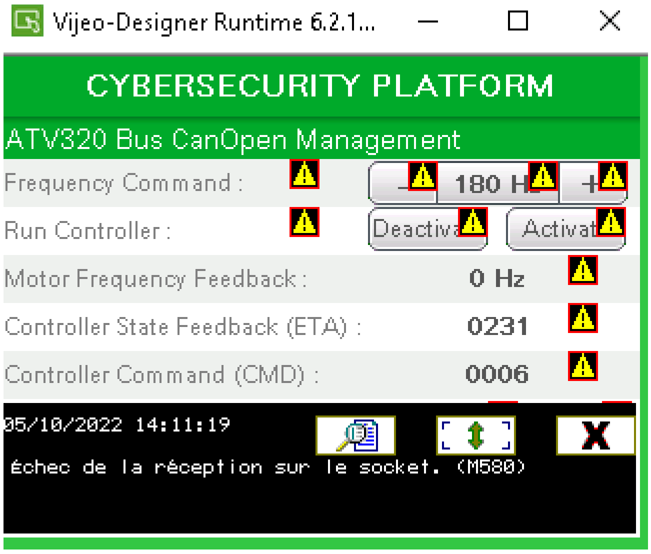
Motor Frequency Feedback : 210 Hz

Controller State Feedback (ETA) : 0637

Controller Command (CMD) : 000F

- Change the speed setpoint (%MW1014) to 180 :

  request rejected by filtering via Custom Pattern (because lower than 200)



CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : 180 H

Run Controller :

Motor Frequency Feedback : 0 Hz

Controller State Feedback (ETA) : 0231

Controller Command (CMD) : 0006

```
05/10/2022 14:11:19
échec de la réception sur le socket. (M580)
```

The request is rejected. The old setpoint is retained