Using the Stormshield firewall

Denis Lubineau – denis.lubineau@univ-grenoble-alpes.fr

Cf. Book p.

Outline

Firewall reinitialization

- **LAB-1 : Reinitialising The Hardware Firewall**

- **LAB-2 : Configuring a Firewall as a split Firewall (Bridge mode)**

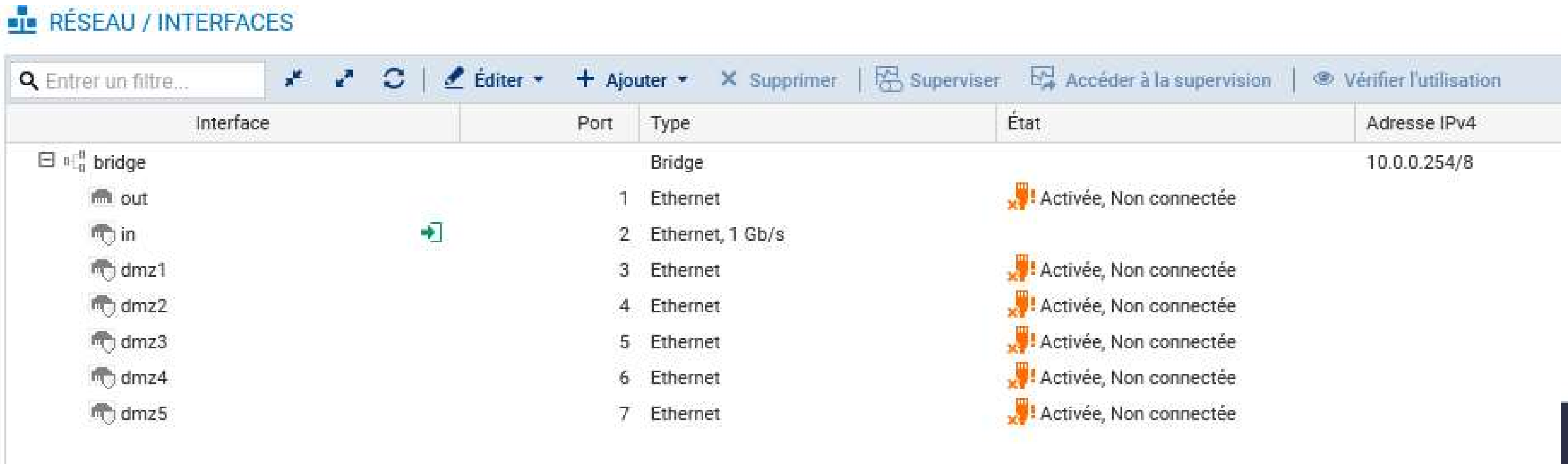
CUSTOMS patterns

- **LAB-3 : Custom patterns**

Cf. Book p.

Firewall réinitialisation

- Connect the serial console
  - Parameters : 115200 8N1 no XON/OFF
- Login as admin
- Reset the configuration :
  - defaultconfig -f -r -p
  - After reboot, the following configuration is available for interfaces :
    - Default access : admin/admin

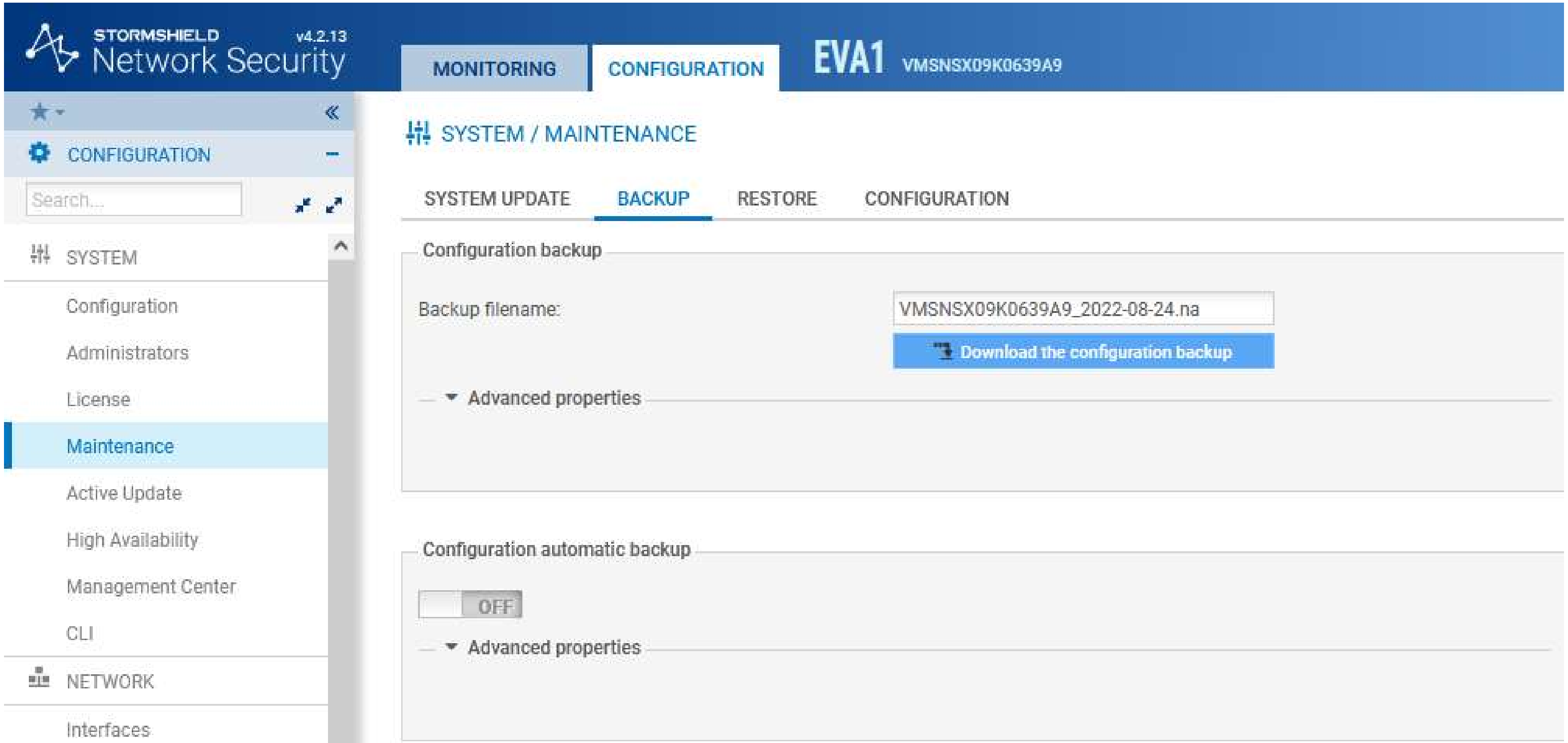


Interface	Port	Type	État	Adresse IPv4
bridge		Bridge		10.0.0.254/8
out	1	Ethernet	Activée, Non connectée	
in	2	Ethernet, 1 Gb/s		
dmz1	3	Ethernet	Activée, Non connectée	
dmz2	4	Ethernet	Activée, Non connectée	
dmz3	5	Ethernet	Activée, Non connectée	
dmz4	6	Ethernet	Activée, Non connectée	
dmz5	7	Ethernet	Activée, Non connectée	

Cf. Book p.

LAB-1 (Hardware Stormshield only)

- Save your config



Configuration backup

Backup filename: VMSNSX09K0639A9_2022-08-24.na

Configuration automatic backup

OFF

- Connect to the console
  - (use serial line if firewall = a real device)

- Login as admin
  - Reset the configuration with defaultconfig -f -r -p

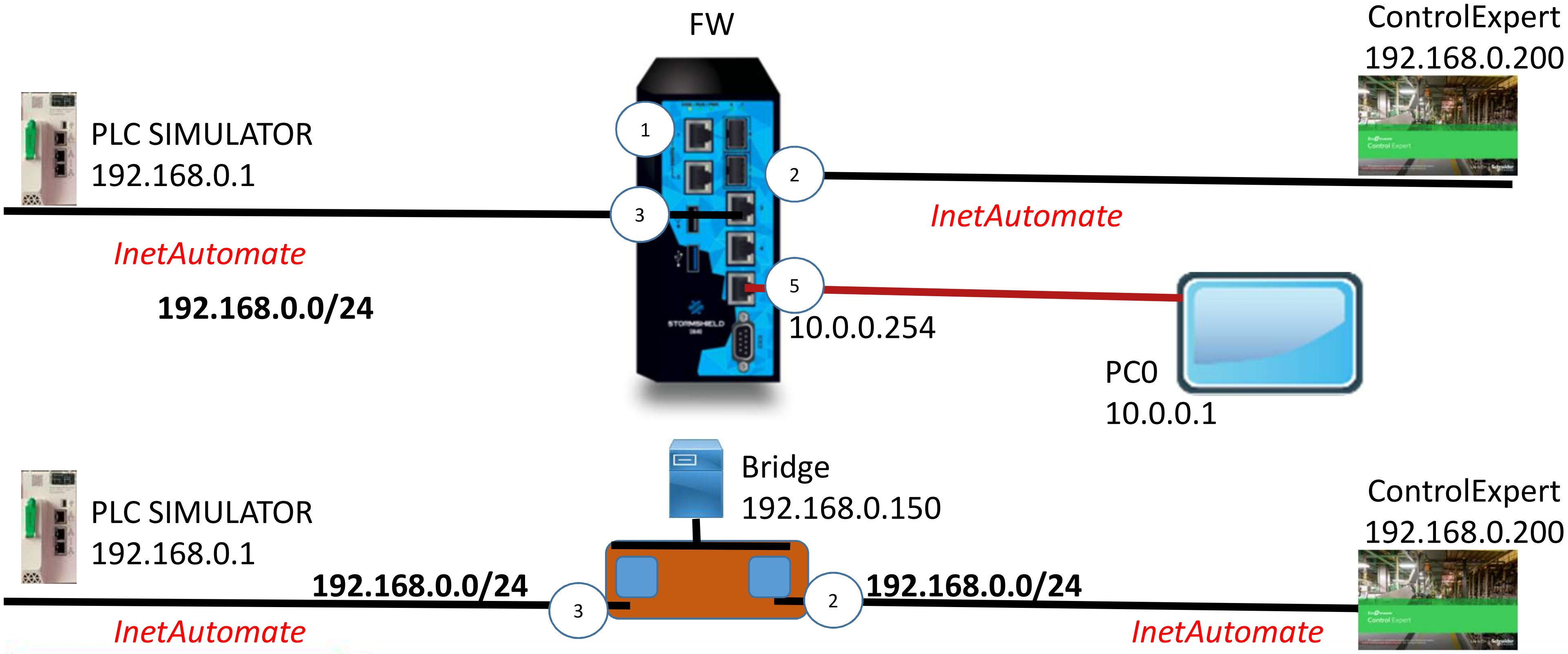
- After Reboot
  - The default address is now 10.0.0254
  - You can now login with admin/admin
  - The FW is in BLOCK ALL state by default

Cf. Book p.

LAB-2 : split mode

+ : You can use it on an existig network

- : Architecture less easy to interpret.



FW

ControlExpert
192.168.0.200

PLC SIMULATOR
192.168.0.1

1

2

3

InetAutomate

InetAutomate

192.168.0.0/24

5

10.0.0.254

PC0
10.0.0.1

Bridge
192.168.0.150

PLC SIMULATOR
192.168.0.1

ControlExpert
192.168.0.200

192.168.0.0/24

3

2

192.168.0.0/24

InetAutomate

InetAutomate

Cf. Book p.

LAB-2 : (On VM)

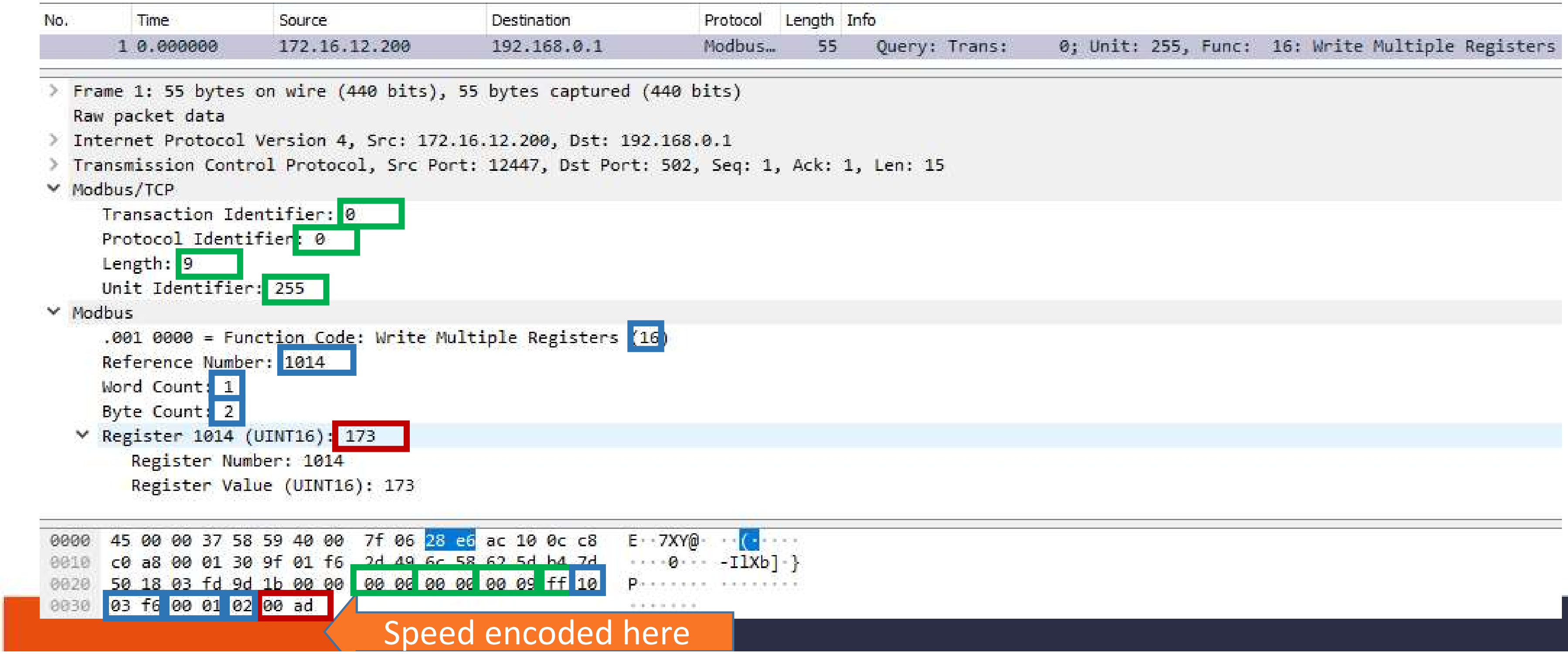
- Backup your configuration
- Restore the initial VirtualBox Snapshot
- load the configuration file : SNI40-TP2-0.na
  - Now you are working with a bridge mode
- Verify your configuration – choose the « pass all » filtering slot.
  - Adapt the configuration of ControlExpert VM.

- Create a new filtering SLOT so that :
  - Anybody can ping anybody
  - Modbus is allowed from anywhere but the IPS will capture the frames
    - (see previous labs)

Cf. Book p.

Custom patterns

- Goal
  - Filter some packets with bad characteristics
  - Can we filter speed commands so to accept only some defined values for speed ?



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.12.200	192.168.0.1	Modbus…	55	Query: Trans: 0; Unit: 255, Func: 16: Write Multiple Registers

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 172.16.12.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 12447, Dst Port: 502, Seq: 1, Ack: 1, 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: 1014
    Word Count: 1
    Byte Count: 2
  v Register 1014 (UINT16): 173
      Register Number: 1014
      Register Value (UINT16): 173
```

```
0000  45 00 00 37 58 59 40 00  7f 06 28 e6 ac 10 0c c8   E··7XY@· ··(·····
0010  c0 a8 00 01 30 9f 01 f6  2d 49 6c 58 62 5d b4 7d   ····0··· -IlXb]·}
0020  50 18 03 fd 9d 1b 00 00  00 00 00 00 00 09 ff 10   P······· ········
0030  03 f6 00 01 02 00 ad                               ·······
```

Speed encoded here

Cf. Book p.

Example of Custom pattern definition file

- What is the meaning of this expression ?

```
[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]"
```

Cf. Book p.

Outline

Firewall reinitialization

- LAB-1 : Reinitialising The Hardware Firewall

- LAB-2 : Configuring a Firewall as a split Firewall (Bridge mode)

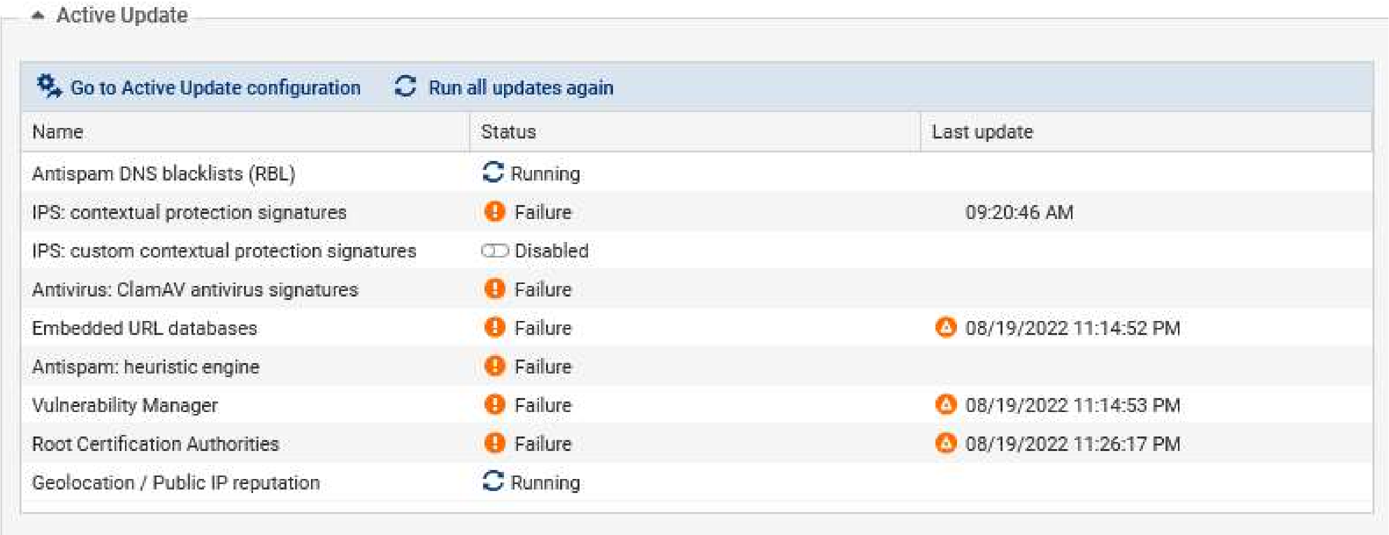
CUSTOMS patterns

- LAB-3 : Custom patterns

Cf. Book p.

LAB-3 : Custom patterns (1)

- Active update should work with last versions
  - OUT should be connected to Internet



Active Update

Name	Status	Last update
Antispam DNS blacklists (RBL)	Running	
IPS: contextual protection signatures	Failure	09:20:46 AM
IPS: custom contextual protection signatures	Disabled	
Antivirus: ClamAV antivirus signatures	Failure	
Embedded URL databases	Failure	08/19/2022 11:14:52 PM
Antispam: heuristic engine	Failure	
Vulnerability Manager	Failure	08/19/2022 11:14:53 PM
Root Certification Authorities	Failure	08/19/2022 11:26:17 PM
Geolocation / Public IP reputation	Running	

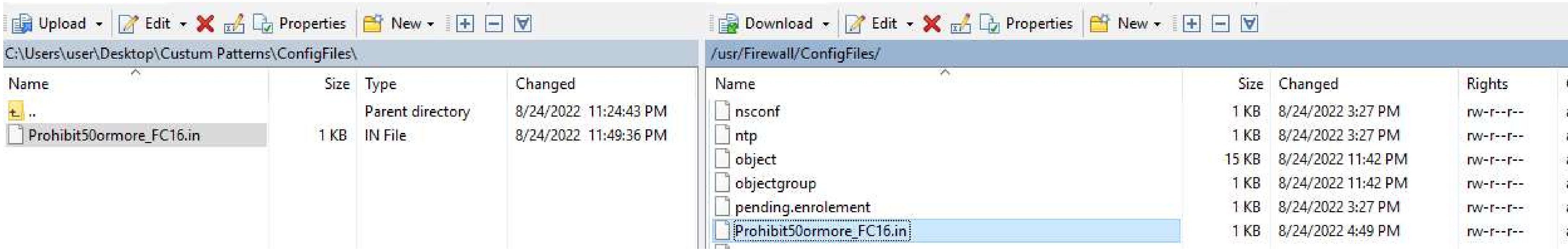
- In CLI

```
CONFIG SECURITYINSPECTION COMMON INIT CustomPatternMatching=1
CONFIG SECURITYINSPECTION ACTIVATE
```

Cf. Book p.

LAB-3 : Custom patterns (2)

- With SCP, copy the custom pattern in /usr/Firewall/ConfigFiles



C:\Users\user\Desktop\Custum Patterns\ConfigFiles\

Name	Size	Type	Changed
..		Parent directory	8/24/2022 11:24:43 PM
Prohibit50ormore_FC16.in	1 KB	IN File	8/24/2022 11:49:36 PM

/usr/Firewall/ConfigFiles/

Name	Size	Changed	Rights
nsconf	1 KB	8/24/2022 3:27 PM	rw-r--r--
ntp	1 KB	8/24/2022 3:27 PM	rw-r--r--
object	15 KB	8/24/2022 11:42 PM	rw-r--r--
objectgroup	1 KB	8/24/2022 11:42 PM	rw-r--r--
pending.enrolement	1 KB	8/24/2022 3:27 PM	rw-r--r--
Prohibit50ormore_FC16.in	1 KB	8/24/2022 4:49 PM	rw-r--r--

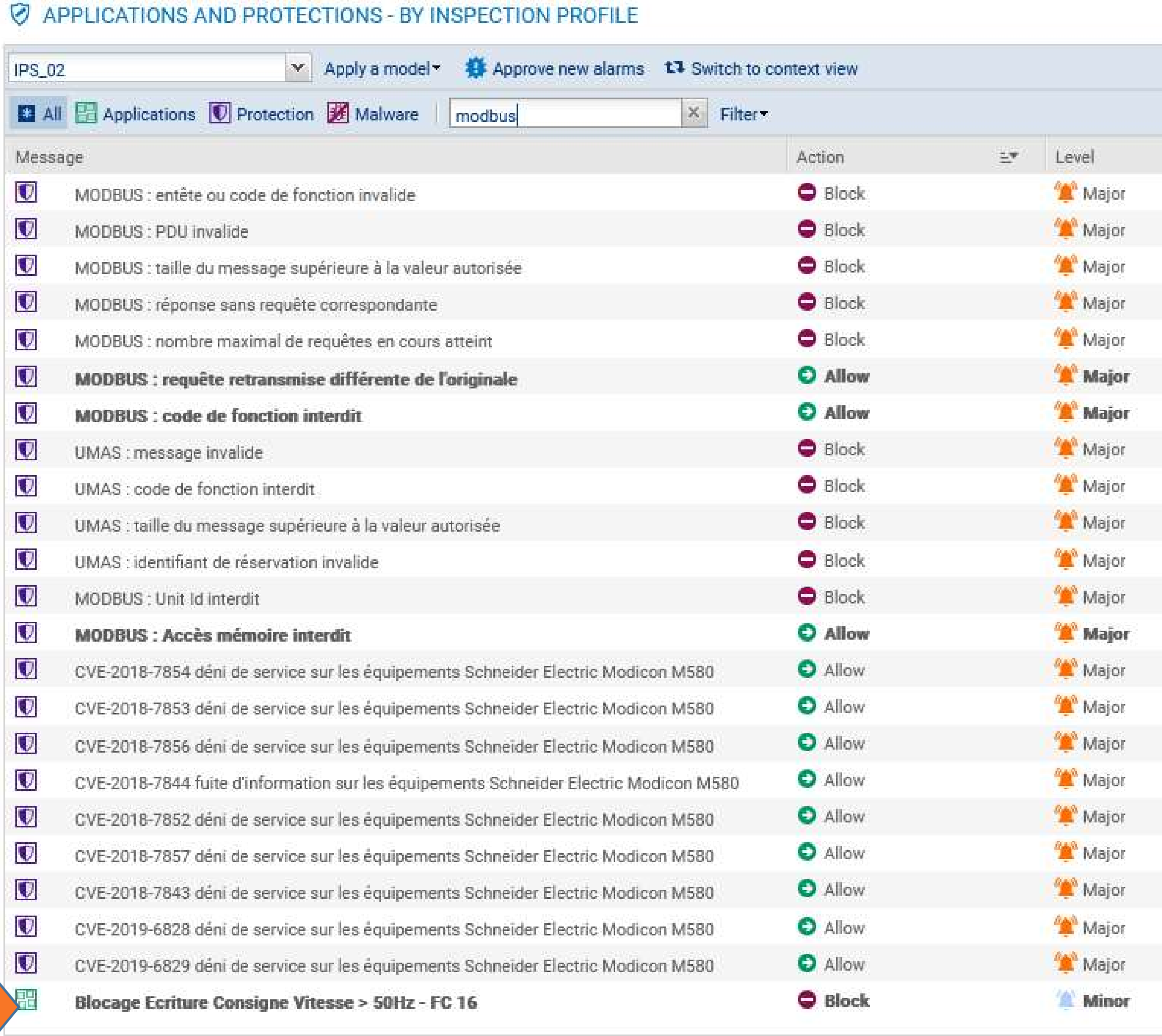
- On the firewall console (Connect first with SSH to the Firewall)

```
enpattern -t /usr/Firewall/ConfigFiles/Prohibit50ormore_FC16.in
enpattern –afv
enasq
```

Cf. Book p.

LAB-3 : Custom patterns (3)

- Now an additional rule !



APPLICATIONS AND PROTECTIONS - BY INSPECTION PROFILE

Message	Action	Level
MODBUS : entête ou code de fonction invalide	Block	Major
MODBUS : PDU invalide	Block	Major
MODBUS : taille du message supérieure à la valeur autorisée	Block	Major
MODBUS : réponse sans requête correspondante	Block	Major
MODBUS : nombre maximal de requêtes en cours atteint	Block	Major
MODBUS : requête retransmise différente de l'originale	**Allow**	**Major**
MODBUS : code de fonction interdit	**Allow**	**Major**
UMAS : message invalide	Block	Major
UMAS : code de fonction interdit	Block	Major
UMAS : taille du message supérieure à la valeur autorisée	Block	Major
UMAS : identifiant de réservation invalide	Block	Major
MODBUS : Unit Id interdit	Block	Major
MODBUS : Accès mémoire interdit	**Allow**	**Major**
CVE-2018-7854 déni de service sur les équipements Schneider Electric Modicon M580	Allow	Major
CVE-2018-7853 déni de service sur les équipements Schneider Electric Modicon M580	Allow	Major
CVE-2018-7856 déni de service sur les équipements Schneider Electric Modicon M580	Allow	Major
CVE-2018-7844 fuite d'information sur les équipements Schneider Electric Modicon M580	Allow	Major
CVE-2018-7852 déni de service sur les équipements Schneider Electric Modicon M580	Allow	Major
CVE-2018-7857 déni de service sur les équipements Schneider Electric Modicon M580	Allow	Major
CVE-2018-7843 déni de service sur les équipements Schneider Electric Modicon M580	Allow	Major
CVE-2019-6828 déni de service sur les équipements Schneider Electric Modicon M580	Allow	Major
CVE-2019-6829 déni de service sur les équipements Schneider Electric Modicon M580	Allow	Major
Blocage Ecriture Consigne Vitesse > 50Hz - FC 16	**Block**	**Minor**

Cf. Book p.

ConneXium Switch

- The effective IP on the set-up is 192.168.0.10
- The login is **admin** password **private**
- **Web Access: ! Old browser with JAVA support !**
- **SSH access with putty**

Stormshield Firewall labs : Balance

TP0 : return to initial conditions

Initialization – Hardware connections – Virtual environments

TP1 : inherent PLC protections

Enforced security, access control

TP2 : Flow Analysis

IDS/IPS – Use IPS to capture frames – Frame Analysis

TP3 : Protection by Custom Patterns

TP4 : Attack script

TP5 : Network Segregated Firewall

Routing, gateways, using the FW as a router

TP6 : Setting up an Manageable Switch

TP7 : Internet access through the SNi40

NAT setup, OUT interface configuration, filtering

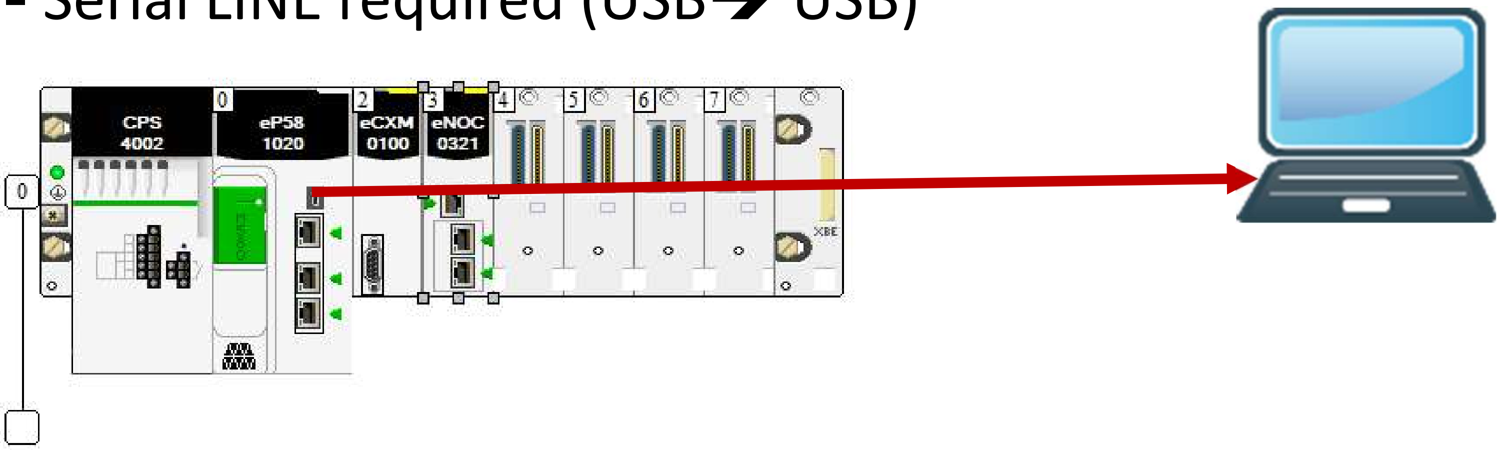
TP8 : Attacks and Protection

Cf. Book p.

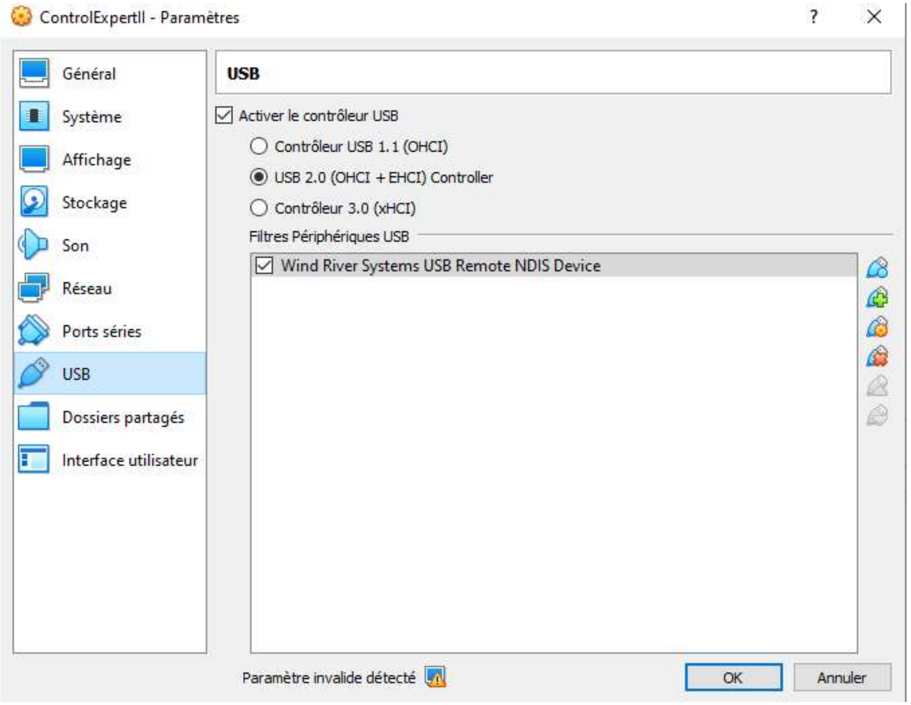
PLC serial connection

- If a WRONG configuration is uploaded to the PLC
  - May loose contact with PLC
  - No further connection possible

- Serial LINE required (USB➔ USB)



- If COntrolExpert in a VM
  - Associate the USB connection to your VM



ControlExpertII - Paramètres

USB

☑ Activer le contrôleur USB

○ Contrôleur USB 1.1 (OHCI)

● USB 2.0 (OHCI + EHCI) Controller

○ Contrôleur 3.0 (xHCI)

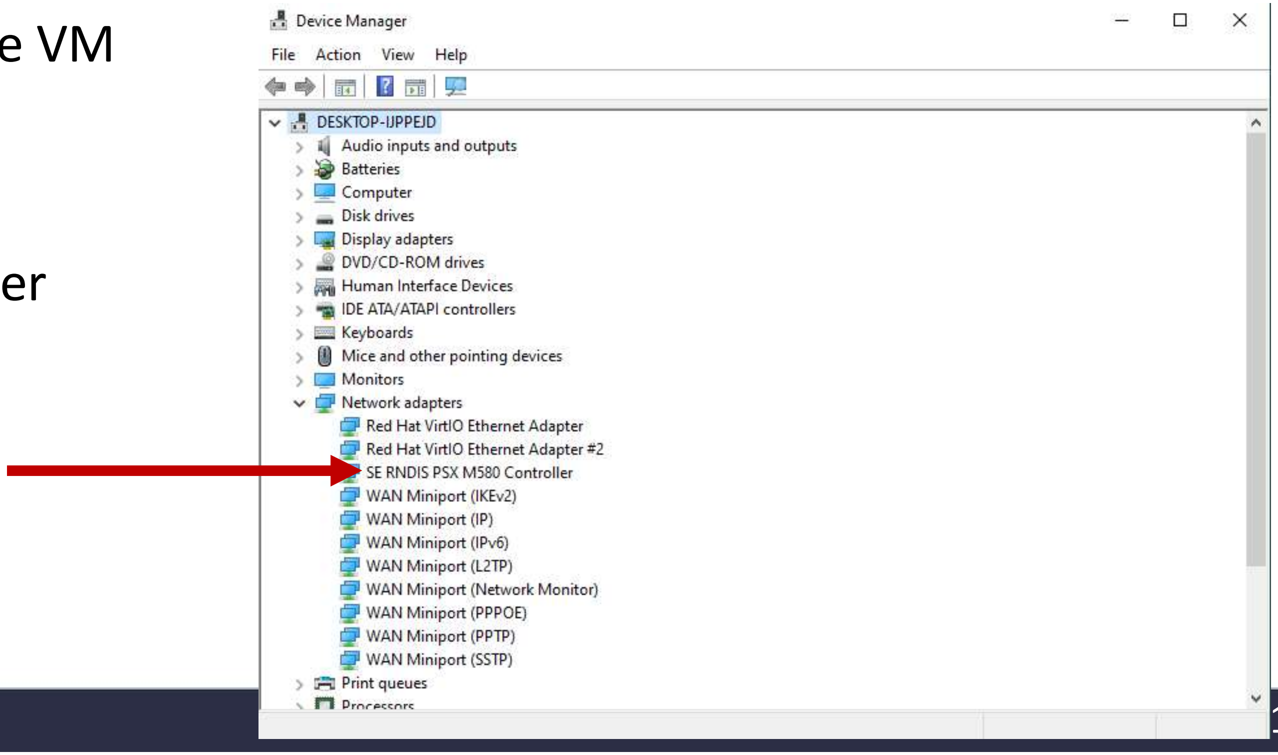
Filtres Périphériques USB

☑ Wind River Systems USB Remote NDIS Device

Paramètre invalide détecté

Cf. Book p.

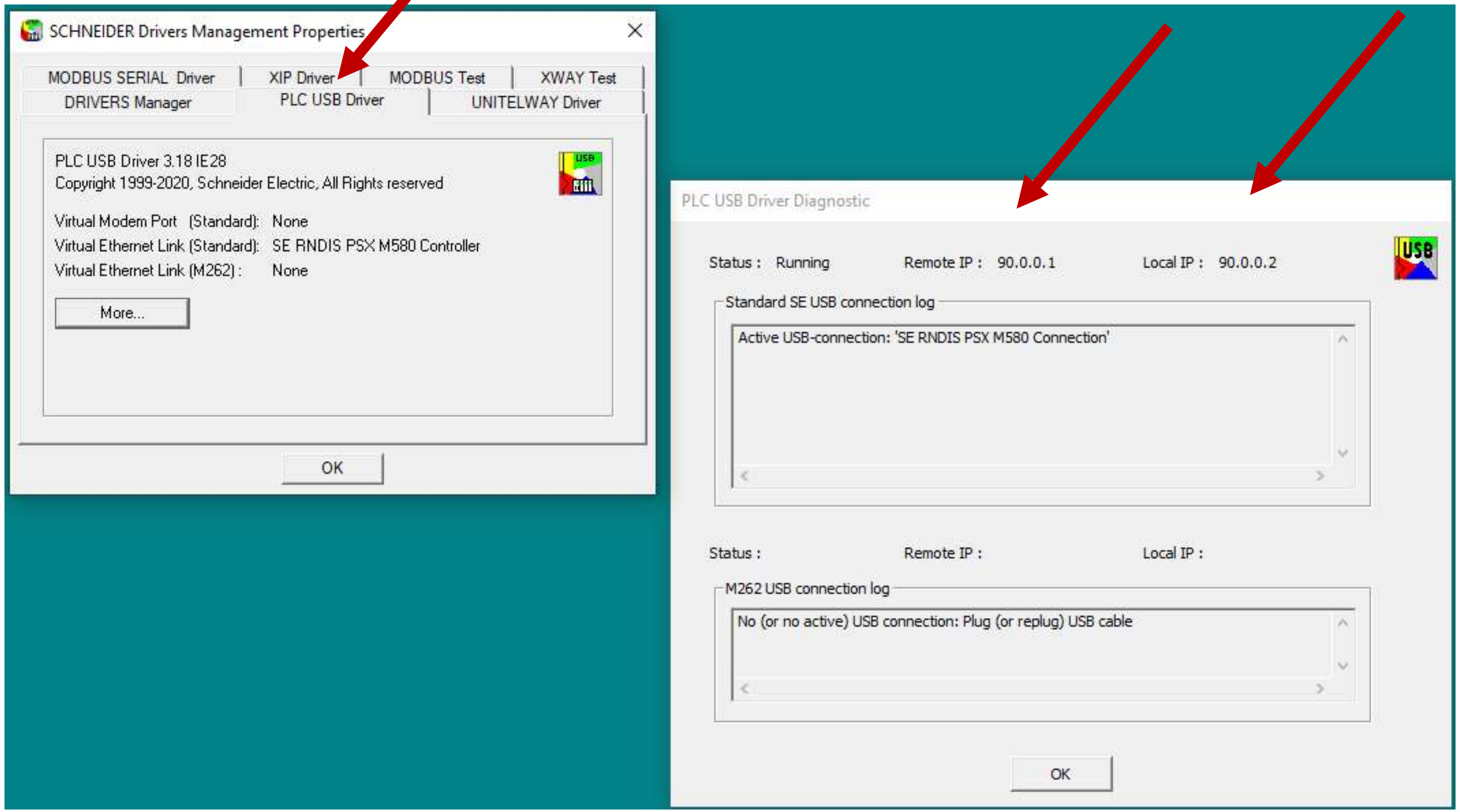
- ON the VM carying ControlExpert (or on real OS if ControlExpert on the real machine)
- A specific driver is required
  - Install SchneiderPLCUSBDriverSuite.exe
  - You may have to reboot the VM
- In device manager :
  - SERNDISPSXM580 Controller



- DESKTOP-IJPPEJD
  - Audio inputs and outputs
  - Batteries
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
    - Red Hat VirtIO Ethernet Adapter
    - Red Hat VirtIO Ethernet Adapter #2
    - SE RNDIS PSX M580 Controller
    - WAN Miniport (IKEv2)
    - WAN Miniport (IP)
    - WAN Miniport (IPv6)
    - WAN Miniport (L2TP)
    - WAN Miniport (Network Monitor)
    - WAN Miniport (PPPOE)
    - WAN Miniport (PPTP)
    - WAN Miniport (SSTP)
  - Print queues
  - Processors

Cf. Book p.

- In Schneider Driver manager
- IP defined for client and server



PLC USB Driver 3.18 IE28
Copyright 1999-2020, Schneider Electric, All Rights reserved

Virtual Modem Port (Standard): None
Virtual Ethernet Link (Standard): SE RNDIS PSX M580 Controller
Virtual Ethernet Link (M262) : None

Status : Running Remote IP : 90.0.0.1 Local IP : 90.0.0.2

Standard SE USB connection log

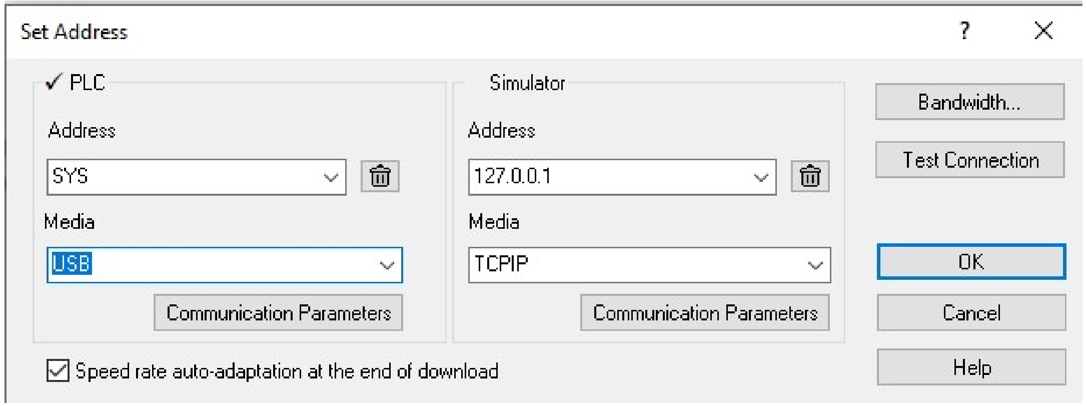
```
Active USB-connection: 'SE RNDIS PSX M580 Connection'
```

Status : Remote IP : Local IP :

M262 USB connection log

```
No (or no active) USB connection: Plug (or replug) USB cable
```

- Control Expert can now communicate other the USB line



PLC Address: SYS

PLC Media: USB

Simulator Address: 127.0.0.1

Simulator Media: TCPIP

☑ Speed rate auto-adaptation at the end of download

Cf. Book p.

Some other tools

- IP ANGRY SCANNER (IP Scanner)
  - https://angryip.org/
- TFTPD64 (DHCP server and some other small services)
  - https://www.intel.com/content/www/us/en/docs/programmable/683536/current/tftpd64-by-ph-jounin-installation.html
- Connexium Switch Management
  - Ethernet switch Configurator
- General Network Discovery and Management
  - Connexium Network Manager