Using the Stormshield firewall

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

Cf. Book p.

Outline

- **LAB-0 : Preparing set-up : Firewall in router mode**
  - VMS
  - Initial state with basic router
  - Connectivity tests (see exercices on routing)

- **LAB-1 : Filtering**
  - Pass all
  - **Filters with a firewall**

- **MODBUS frames**
- **IDS/IPS with a Stormshield Firewall**
- **LAB-2 : Analysing frames with Wireshark and IPS**

- **Network address translation**
- **LAB-3 : NAT**

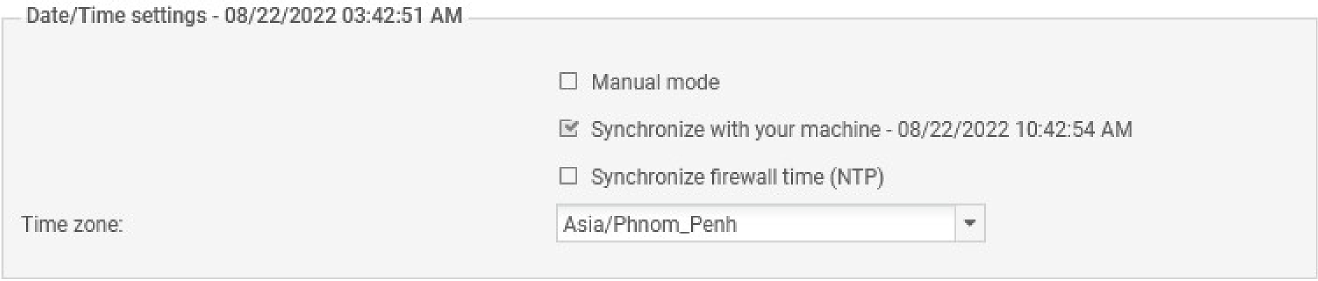
- **A word about UMAS**

- **Final : cybersecurity ?**

Cf. Book p.

LAB-0: Firewall Stormshield in router mode

- Get the stormshield VM
- Configure an internal network on VirtualBox (intnet5)
- Import Stormshield VM
- RUN PLC VM, run ControlExpertVM
- Import PCO – adapt the network configuration – Run PC0
- PC0 : Connect to the FW interface : https://10.0.0.254
- **SET TIME on ALL MACHINES**
  - **On FW :**



Date/Time settings - 08/22/2022 03:42:51 AM

☐ Manual mode

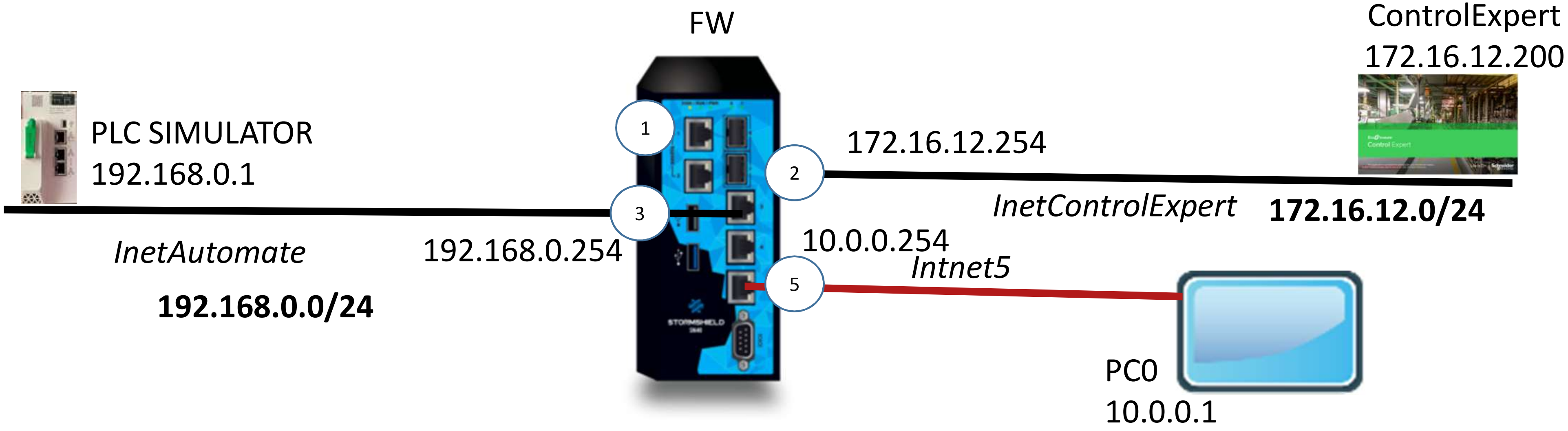
☑ Synchronize with your machine - 08/22/2022 10:42:54 AM

☐ Synchronize firewall time (NTP)

Time zone: Asia/Phnom_Penh

Cf. Book p.

Initial state :



FW

PLC SIMULATOR
192.168.0.1

InetAutomate

192.168.0.254

192.168.0.0/24

1

2

3

5

172.16.12.254

InetControlExpert

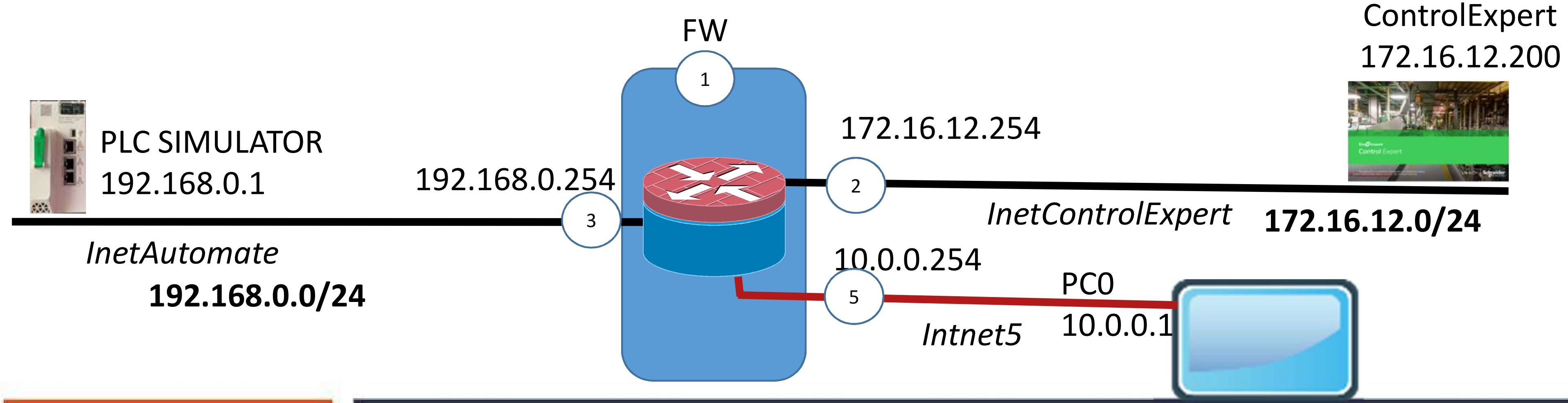
172.16.12.0/24

ControlExpert
172.16.12.200

10.0.0.254

Intnet5

PC0
10.0.0.1



FW

1

PLC SIMULATOR
192.168.0.1

192.168.0.254

3

InetAutomate

192.168.0.0/24

172.16.12.254

2

InetControlExpert

172.16.12.0/24

ControlExpert
172.16.12.200

10.0.0.254

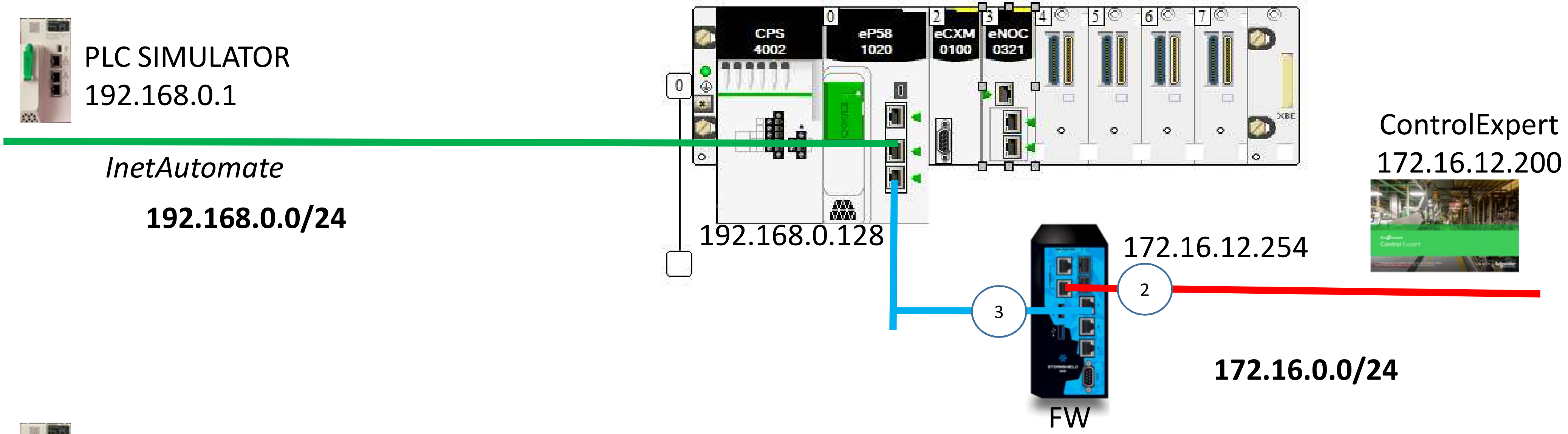
5

Intnet5

PC0
10.0.0.1

Cf. Book p.

remind: test routing with FW


PLC SIMULATOR
192.168.0.1

InetAutomate

192.168.0.0/24

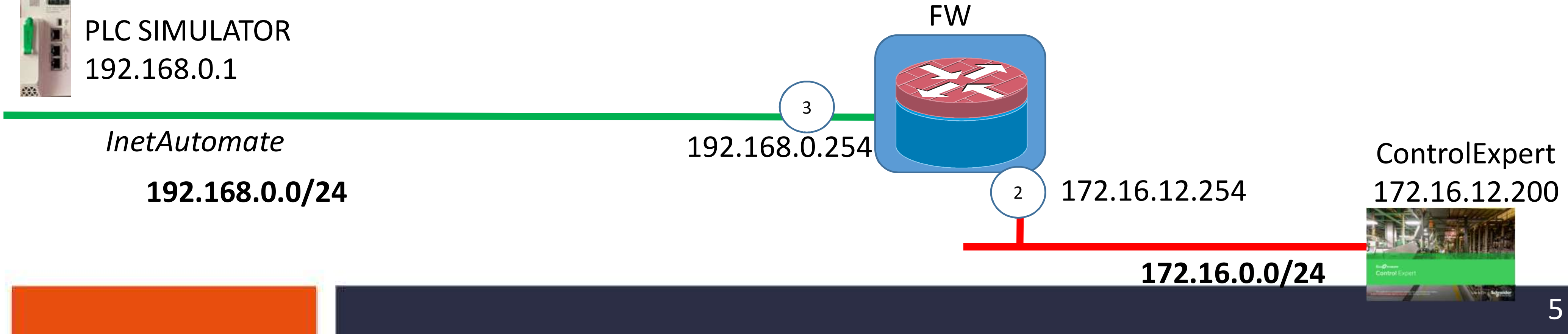
192.168.0.128

ControlExpert
172.16.12.200

172.16.12.254

172.16.0.0/24

FW


FW

PLC SIMULATOR
192.168.0.1

InetAutomate

192.168.0.0/24

192.168.0.254

172.16.12.254

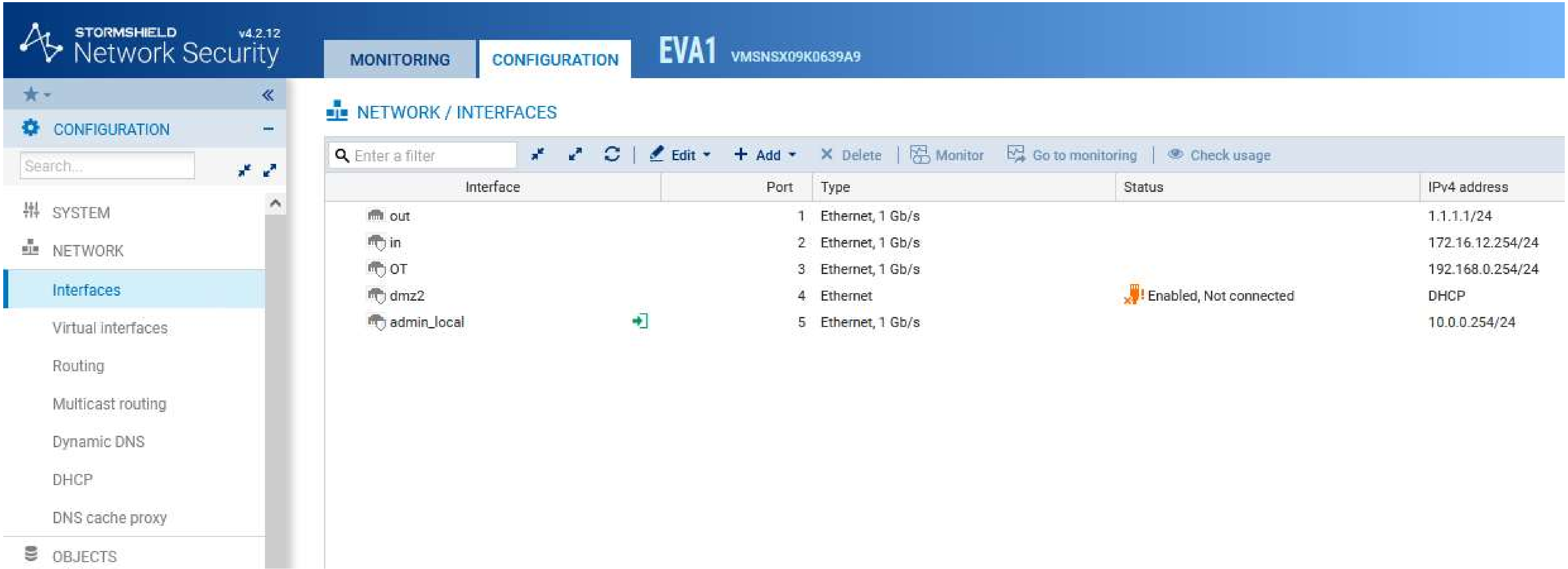
ControlExpert
172.16.12.200

172.16.0.0/24

Cf. Book p.

Initial state :

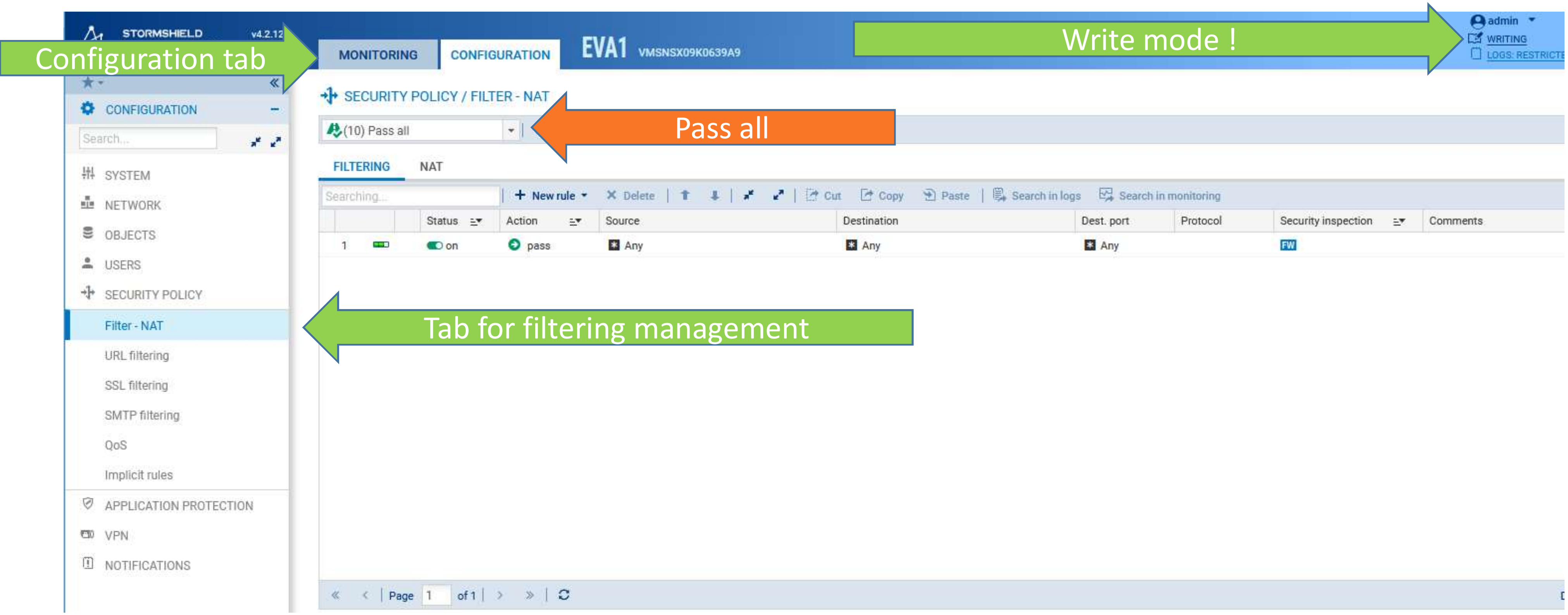
- Update OT IP address if necessary – Don’t mind about OUT



Interface	Port	Type	Status	IPv4 address
out	1	Ethernet, 1 Gb/s		1.1.1.1/24
in	2	Ethernet, 1 Gb/s		172.16.12.254/24
OT	3	Ethernet, 1 Gb/s		192.168.0.254/24
dmz2	4	Ethernet	Enabled, Not connected	DHCP
admin_local	5	Ethernet, 1 Gb/s		10.0.0.254/24

Cf. Book p.

Basic rules implementation
Initial state



Configuration tab

Write mode !

Pass all

Tab for filtering management

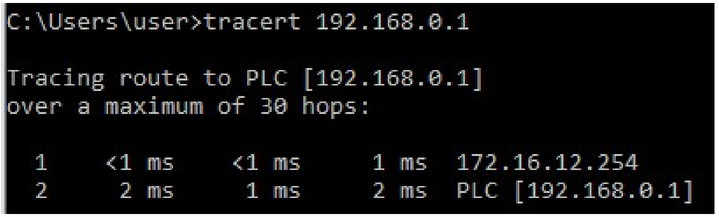
(10) Pass all

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
1		on	pass	Any	Any	Any		FW	

Cf. Book p.

Connectivity tests

- From ControlExpert

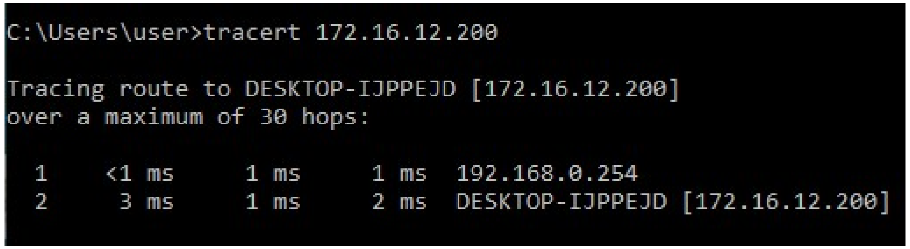


```
C:\Users\user>tracert 192.168.0.1

Tracing route to PLC [192.168.0.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms     1 ms  172.16.12.254
  2     2 ms     1 ms     2 ms  PLC [192.168.0.1]
```

- From PLC



```
C:\Users\user>tracert 172.16.12.200

Tracing route to DESKTOP-IJPPEJD [172.16.12.200]
over a maximum of 30 hops:

  1    <1 ms     1 ms     1 ms  192.168.0.254
  2     3 ms     1 ms     2 ms  DESKTOP-IJPPEJD [172.16.12.200]
```

Cf. Book p.

Outline

- LAB-0 : Preparing set-up
  - VMS
  - Initial state with basic router
  - Connectivity tests (see exercices on routing)

- **LAB-1 : Filtering**
  - Pass all
  - **Filters with a firewall**

- **MODBUS frames**
- **IDS/IPS with a Stormshield Firewall**
- **LAB-2 : Analysing frames with Wireshark and IPS**

- **Network address translation**
- **LAB-3 : NAT**

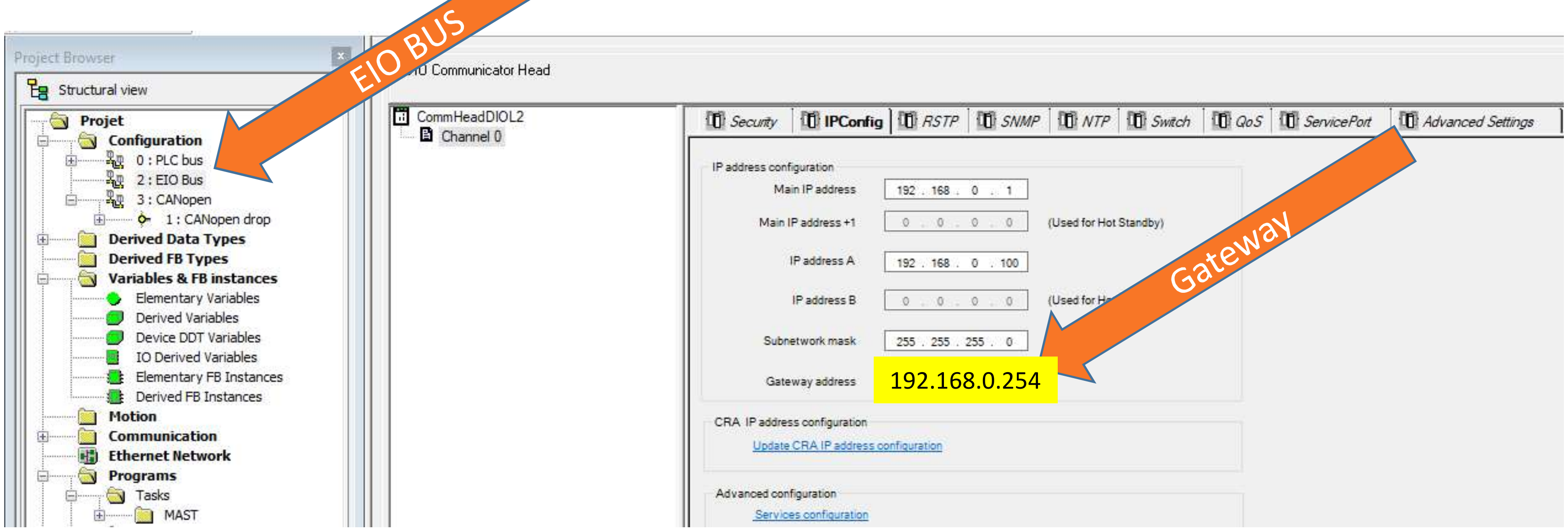
- **A word about UMAS**

- **Final : cybersecurity ?**

Cf. Book p.

Lab 1 : Basics filtering rules

- Prepare the PLC
  - Upload a configuration with the proper parameters



EIO BUS

Gateway

Project Browser

Structural view

- Projet
  - Configuration
    - 0 : PLC bus
    - 2 : EIO Bus
    - 3 : CANopen
      - 1 : CANopen drop
  - Derived Data Types
  - Derived FB Types
  - Variables & FB instances
    - Elementary Variables
    - Derived Variables
    - Device DDT Variables
    - IO Derived Variables
    - Elementary FB Instances
    - Derived FB Instances
  - Motion
  - Communication
  - Ethernet Network
  - Programs
    - Tasks
      - MAST

IO Communicator Head

CommHeadDIOL2
- Channel 0

IP address configuration

Main IP address 192 . 168 . 0 . 1

Main IP address +1 0 . 0 . 0 . 0 (Used for Hot Standby)

IP address A 192 . 168 . 0 . 100

IP address B 0 . 0 . 0 . 0 (Used for Ho

Subnetwork mask 255 . 255 . 255 . 0

Gateway address 192.168.0.254

CRA IP address configuration

Update CRA IP address configuration

Advanced configuration

Services configuration

Cf. Book p.

Lab 1 : Basics filtering rules

- Modify rules so that

Only CE VM (172.16.12.200) could access the 192.168.0.0/24 network

- pings allowed
- Modbus allowed
- http/https allowed (! cannot be tested in virtual env on PLC simulator)

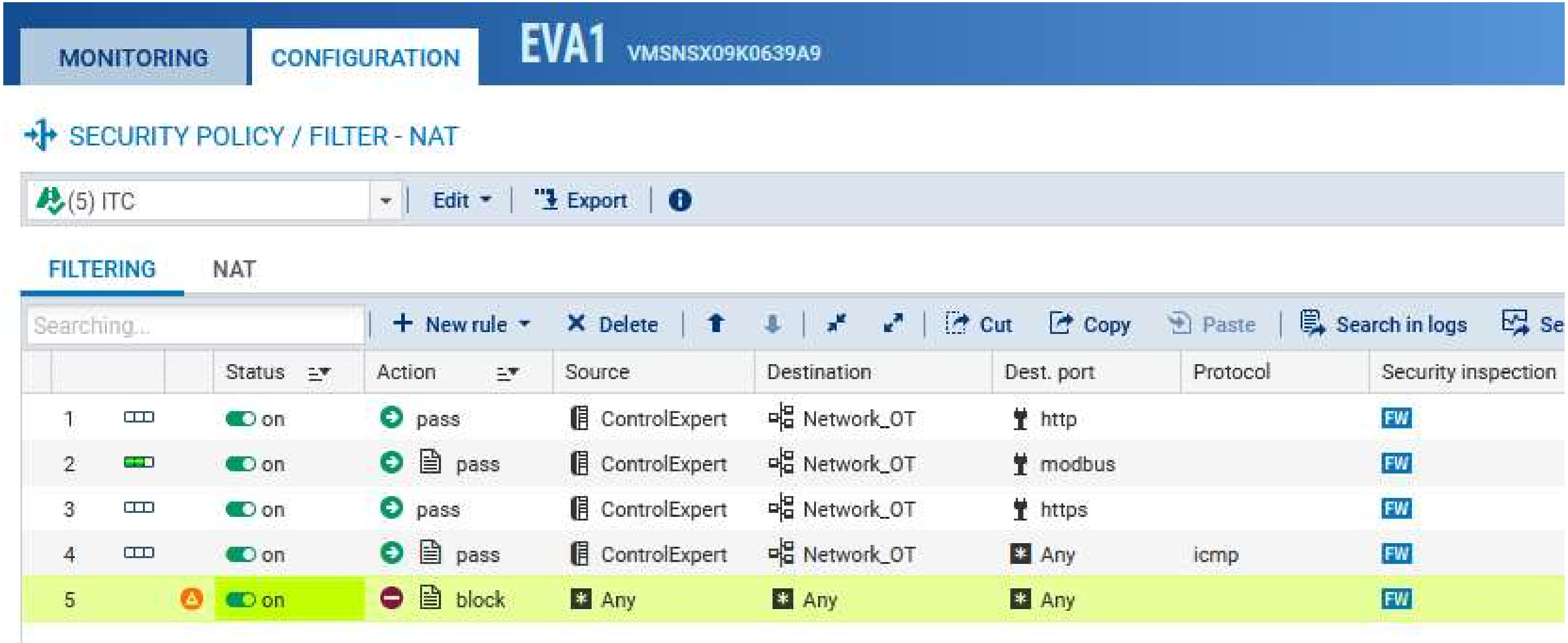
→Verify ControlExpert has the required access.

Change the IP of CE to 12.16.12.100

→Verify that no acces is possible any more

Solution

Cf. Book p.



		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	ControlExpert	Network_OT	http		FW
2		on	pass	ControlExpert	Network_OT	modbus		FW
3		on	pass	ControlExpert	Network_OT	https		FW
4		on	pass	ControlExpert	Network_OT	Any	icmp	FW
5		on	block	Any	Any	Any		FW

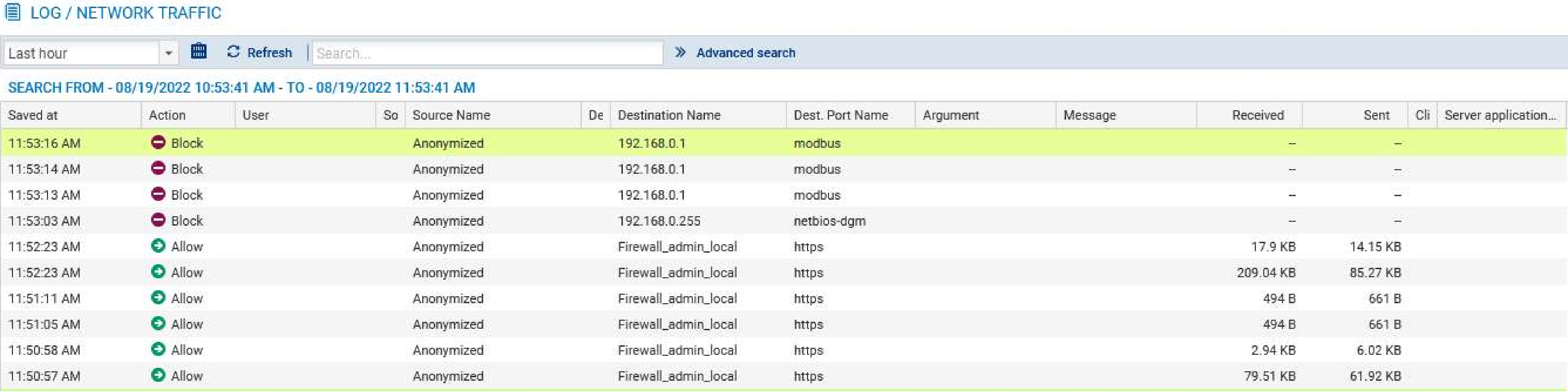
Cf. Book p.

About rules evaluation

- Rules evaluated one by one
- If a packet is matching a rule => Rule applied
- Otherwise, Go to next rule.
- When a rule is applied, stop evaluation (next rules not evaluated).
- If the packet is matcing no rule => destroyed

logs

Cf. Book p.



LOG / NETWORK TRAFFIC

Last hour

SEARCH FROM - 08/19/2022 10:53:41 AM - TO - 08/19/2022 11:53:41 AM

Saved at	Action	User	So	Source Name	De	Destination Name	Dest. Port Name	Argument	Message	Received	Sent	Cli	Server application...
11:53:16 AM	Block			Anonymized		192.168.0.1	modbus			–	–		
11:53:14 AM	Block			Anonymized		192.168.0.1	modbus			–	–		
11:53:13 AM	Block			Anonymized		192.168.0.1	modbus			–	–		
11:53:03 AM	Block			Anonymized		192.168.0.255	netbios-dgm			–	–		
11:52:23 AM	Allow			Anonymized		Firewall_admin_local	https			17.9 KB	14.15 KB		
11:52:23 AM	Allow			Anonymized		Firewall_admin_local	https			209.04 KB	85.27 KB		
11:51:11 AM	Allow			Anonymized		Firewall_admin_local	https			494 B	661 B		
11:51:05 AM	Allow			Anonymized		Firewall_admin_local	https			494 B	661 B		
11:50:58 AM	Allow			Anonymized		Firewall_admin_local	https			2.94 KB	6.02 KB		
11:50:57 AM	Allow			Anonymized		Firewall_admin_local	https			79.51 KB	61.92 KB		

Outline

Cf. Book p.

- LAB-0 : Preparing set-up
  - VMS
  - Initial state with basic router
  - Connectivity tests (see exercices on routing)

- LAB-1 : Filtering
  - Pass all
  - **Filters with a firewall**

- **MODBUS frames**
- **IDS/IPS with a Stormshield Firewall**
- **LAB-2 : Analysing frames with Wireshark and IPS**

- **Network address translation**
- **LAB-3 : NAT**

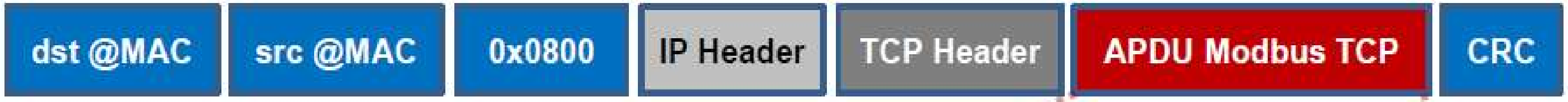
- **A word about UMAS**

- **Final : cybersecurity ?**

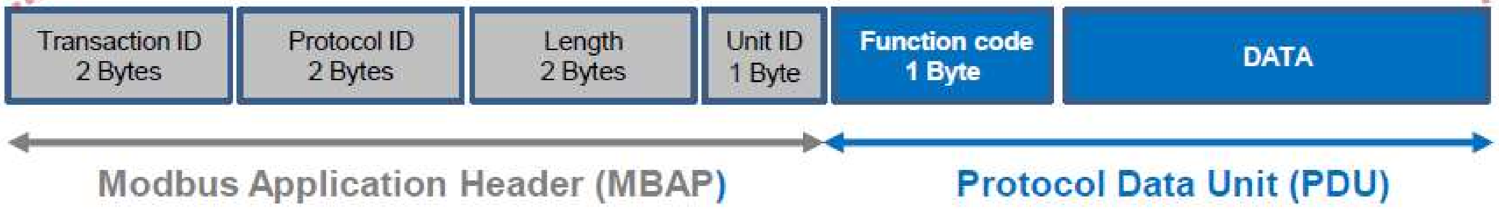
TCP/ModBus

Cf. Book p.

- Trame Ethernet



- Couche applicative Modbus TCP (Application Protocol Data Unit)



Cf. Book p.

ModBus Application Header (MBAP)

▪ Transaction id	: Transaction number
▪ Protocol Id	: 0 for MODBUS TCP
▪ Length	: nb of bytes after this field
▪ Unit ID	: Slave ID, usually 255 with modbus TCP

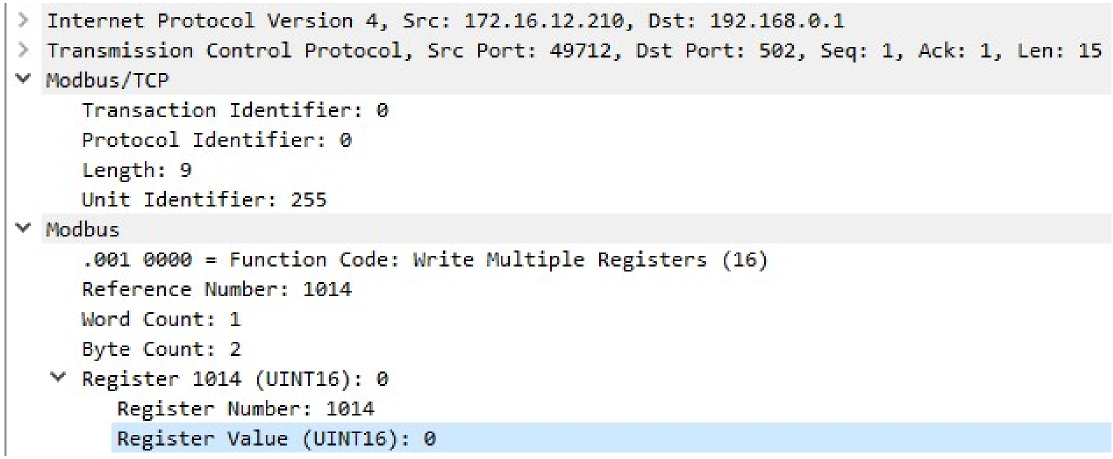
Protocol Data Unit

- Function code : role of the frame
- Data

- Example : FC=16

(Writing multiple registers)

FC	Ref Nb	Word Count	Byte Count	value
1 byte	2 bytes	2 bytes	1 byte	2 bytes
0x10	0x03F6	0x0001	0x02	0x0000



```
> Internet Protocol Version 4, Src: 172.16.12.210, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 49712, 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): 0
      Register Number: 1014
      Register Value (UINT16): 0
```

- FC : **Function code**
- Ref Nb: **starting adress**
- Word count = **Nb of registers**
- Byte count = **2 * nb of registers**
- Value = **Values for registers**

Cf. Book p.

MODBUS Data model

- In a MODBUS PDU each data is addressed from 0 to 65535.
- MODBUS data model composed of 4 blocks that comprises several elements numbered from 1 to n.

Data type	Format	Access
Discrete Inputs	Single bit	Read only
Coil	Single bit	Read / Write
Inputs Registers	16-bit word	Read only
Holding Registers	16-bit word	Read / Write

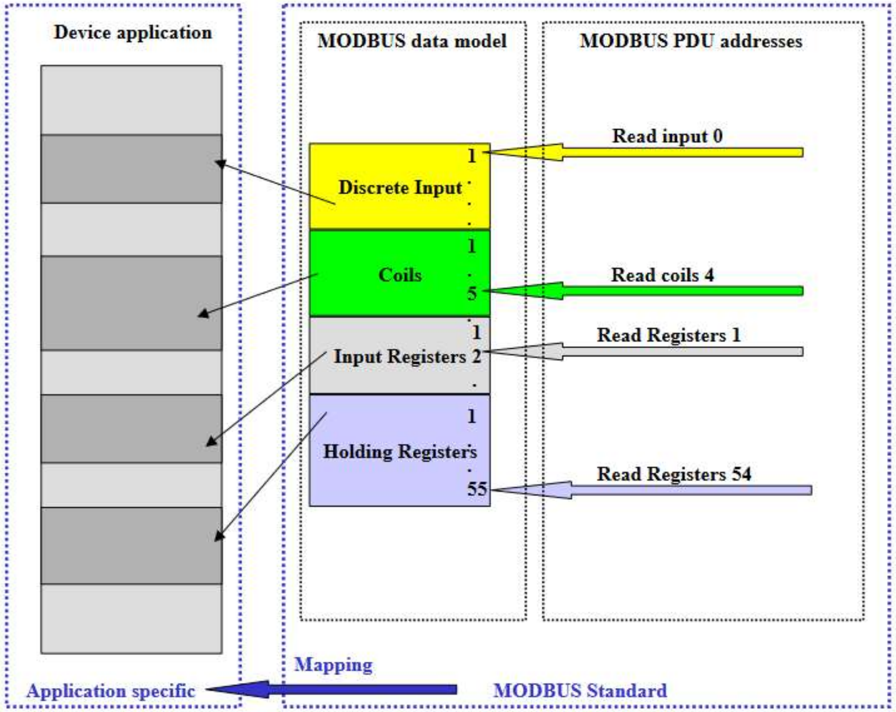


Figure 8 MODBUS Addressing model

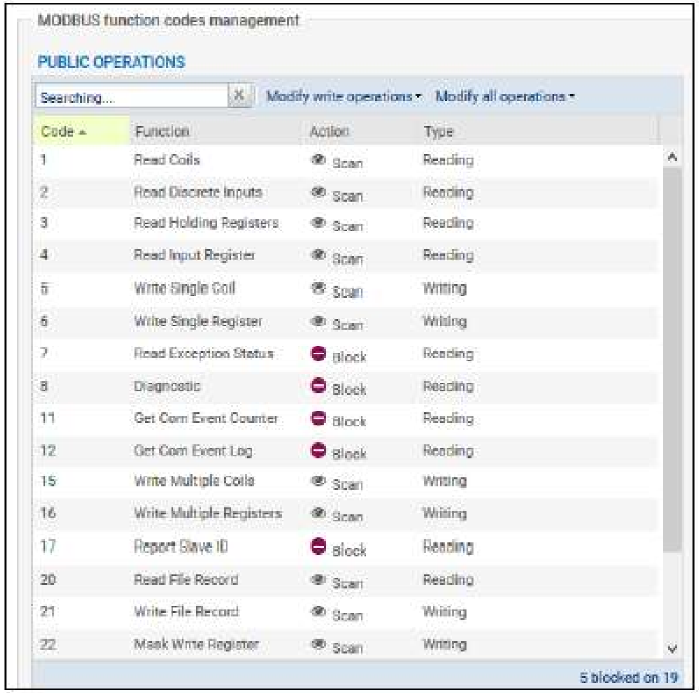
https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

Cf. Book p.

MODBUS function codes

- See also : https://www.youtube.com/watch?v=JBGaInI-TG4

Function code	Size	Description
01	1	Read coil
02	1	Read discrete inputs
05	1	Write single coil
15	1	Write multiple coils
03	16	Read holding registers
04	16	Read input registers
06	16	Write single registers
16	16	Write multiple registers
23	16	Read/Write multiple registers



MODBUS function codes management

PUBLIC OPERATIONS

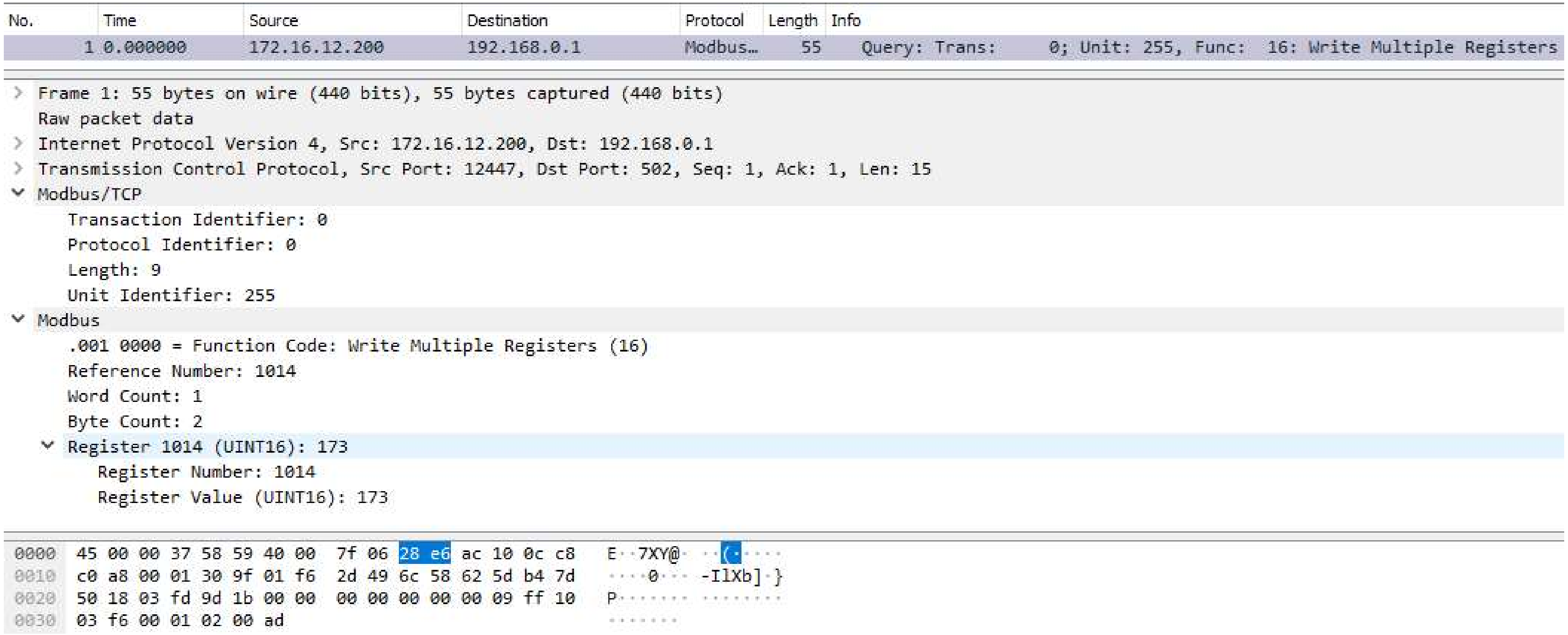
Searching...

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	Block	Reading
8	Diagnostic	Block	Reading
11	Get Com Event Counter	Block	Reading
12	Get Com Event Log	Block	Reading
15	Write Multiple Coils	Scan	Writing
16	Write Multiple Registers	Scan	Writing
17	Report Slave ID	Block	Reading
20	Read File Record	Scan	Reading
21	Write File Record	Scan	Writing
22	Mask Write Register	Scan	Writing

5 blocked on 19

Cf. Book p.

Modbus Frame Analysis



```
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
```

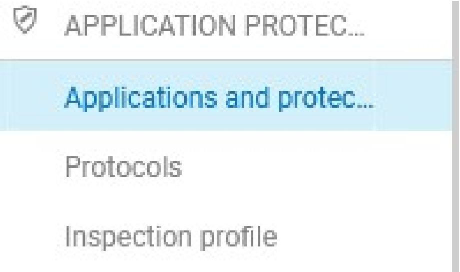
```
0000  45 00 00 37 58 59 40 00  7f 06 28 e6 ac 10 0c c8   E··7XY@·  ··(·····
0010  c0 a8 00 01 30 9f 01 f6  2d 49 6c 58 62 5d b4 7d   ····0···  -IlXb]·}
0020  50 18 03 fd 9d 1b 00 00  00 00 00 00 00 09 ff 10   P·······  ········
0030  03 f6 00 01 02 00 ad                               ·······
```

Cf. Book p.

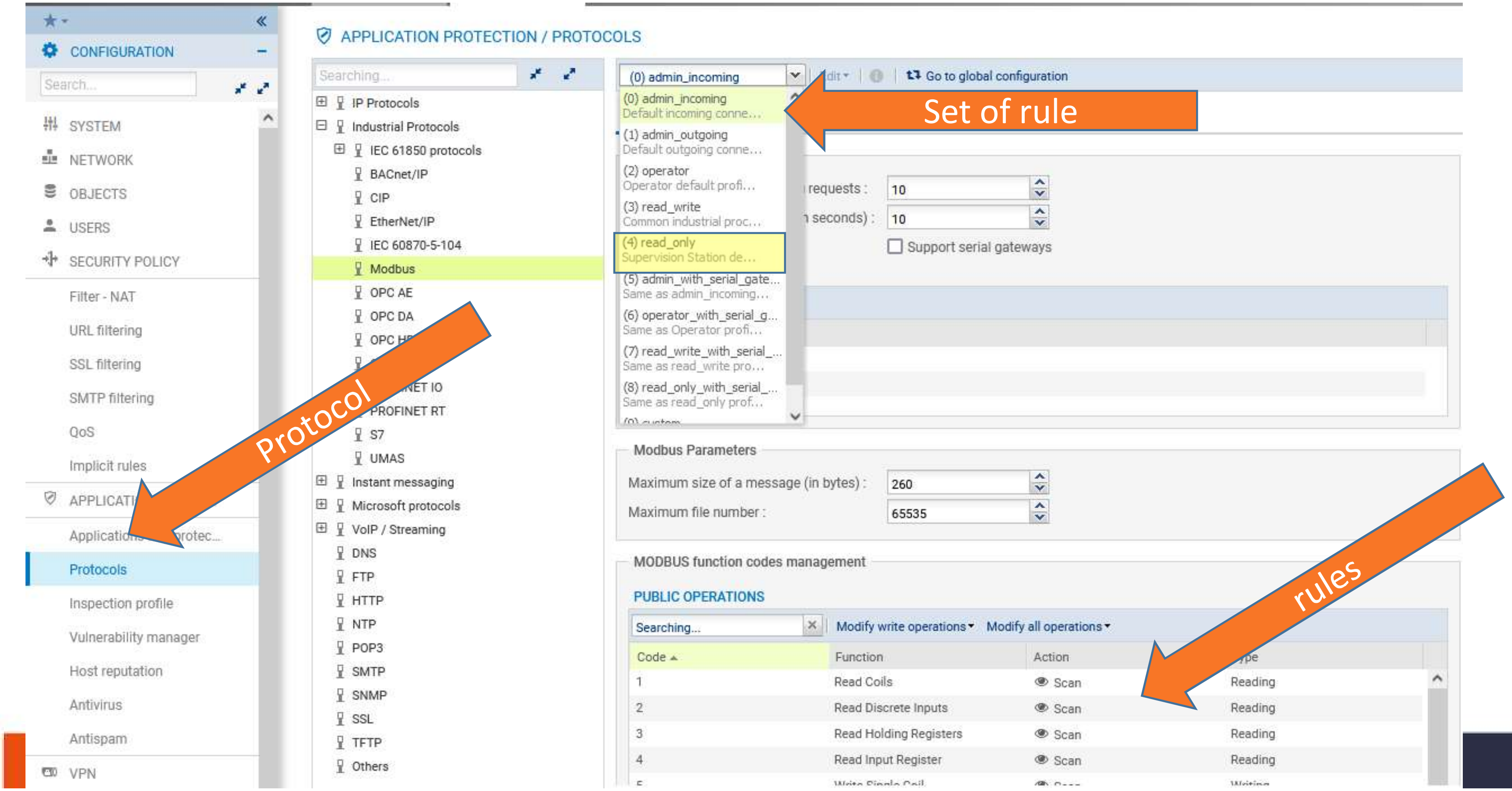
IDS/IPS

- **IDS** : Intrusion detection system
- **IPS** : Intrusion prévention system

- It is possible to configure the firewall to capture frames and to store them for further analysis
- Principle :
  - Block the frame
  - Transmit to the IPS system
    - Accept the frame
    - But capture it
- Requires configuring the IPS



- **Step 1 :**
- Configure or Verify sets of rules for a given protocol :



Set of rule

Protocol

rules

CONFIGURATION

Search...

- SYSTEM
- NETWORK
- OBJECTS
- USERS
- SECURITY POLICY
  - Filter - NAT
  - URL filtering
  - SSL filtering
  - SMTP filtering
  - QoS
  - Implicit rules
- APPLICATI...
  - Application protec...
  - Protocols
  - Inspection profile
  - Vulnerability manager
  - Host reputation
  - Antivirus
  - Antispam
- VPN

APPLICATION PROTECTION / PROTOCOLS

Searching...

- IP Protocols
- Industrial Protocols
  - IEC 61850 protocols
  - BACnet/IP
  - CIP
  - EtherNet/IP
  - IEC 60870-5-104
  - Modbus
  - OPC AE
  - OPC DA
  - OPC H...
  - ...NET IO
  - PROFINET RT
  - S7
  - UMAS
- Instant messaging
- Microsoft protocols
- VoIP / Streaming
- DNS
- FTP
- HTTP
- NTP
- POP3
- SMTP
- SNMP
- SSL
- TFTP
- Others

(0) admin_incoming | ...dit | Go to global configuration

- (0) admin_incoming
  Default incoming conne...
- (1) admin_outgoing
  Default outgoing conne...
- (2) operator
  Operator default profi...
- (3) read_write
  Common industrial proc...
- (4) read_only
  Supervision Station de...
- (5) admin_with_serial_gate...
  Same as admin_incoming...
- (6) operator_with_serial_g...
  Same as Operator profi...
- (7) read_write_with_serial_...
  Same as read_write pro...
- (8) read_only_with_serial_...
  Same as read_only prof...
- (9) custom

...requests : 10

...seconds) : 10

□ Support serial gateways

Modbus Parameters

Maximum size of a message (in bytes) : 260

Maximum file number : 65535

MODBUS function codes management

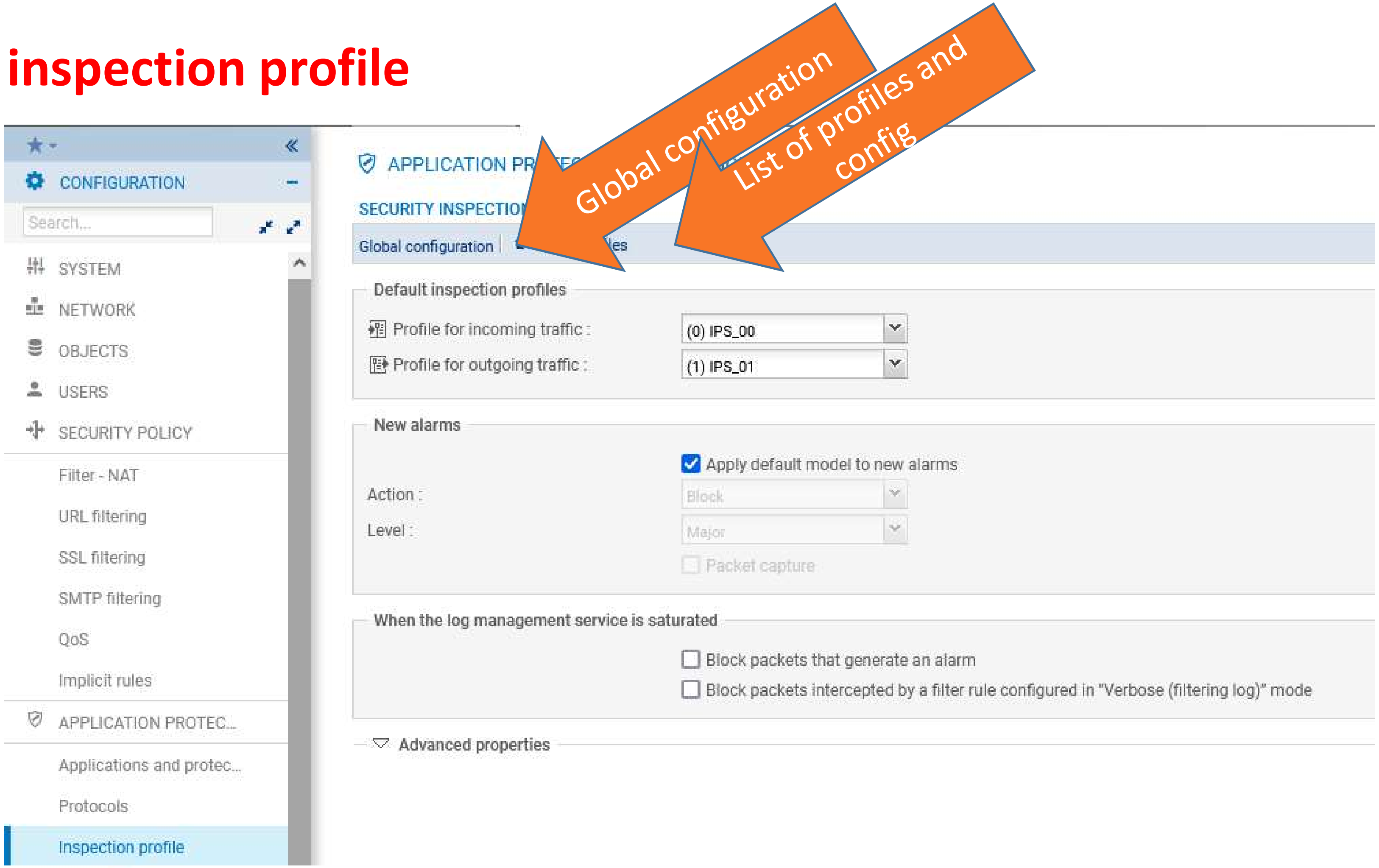
PUBLIC OPERATIONS

Searching... | Modify write operations | Modify all operations

Code	Function	Action	...ype
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

Cf. Book p.

- **Step 2 : inspection profile**



Global configuration

List of profiles and config

Default inspection profiles

Profile for incoming traffic : (0) IPS_00

Profile for outgoing traffic : (1) IPS_01

New alarms

☑ Apply default model to new alarms

Action : Block

Level : Major

□ Packet capture

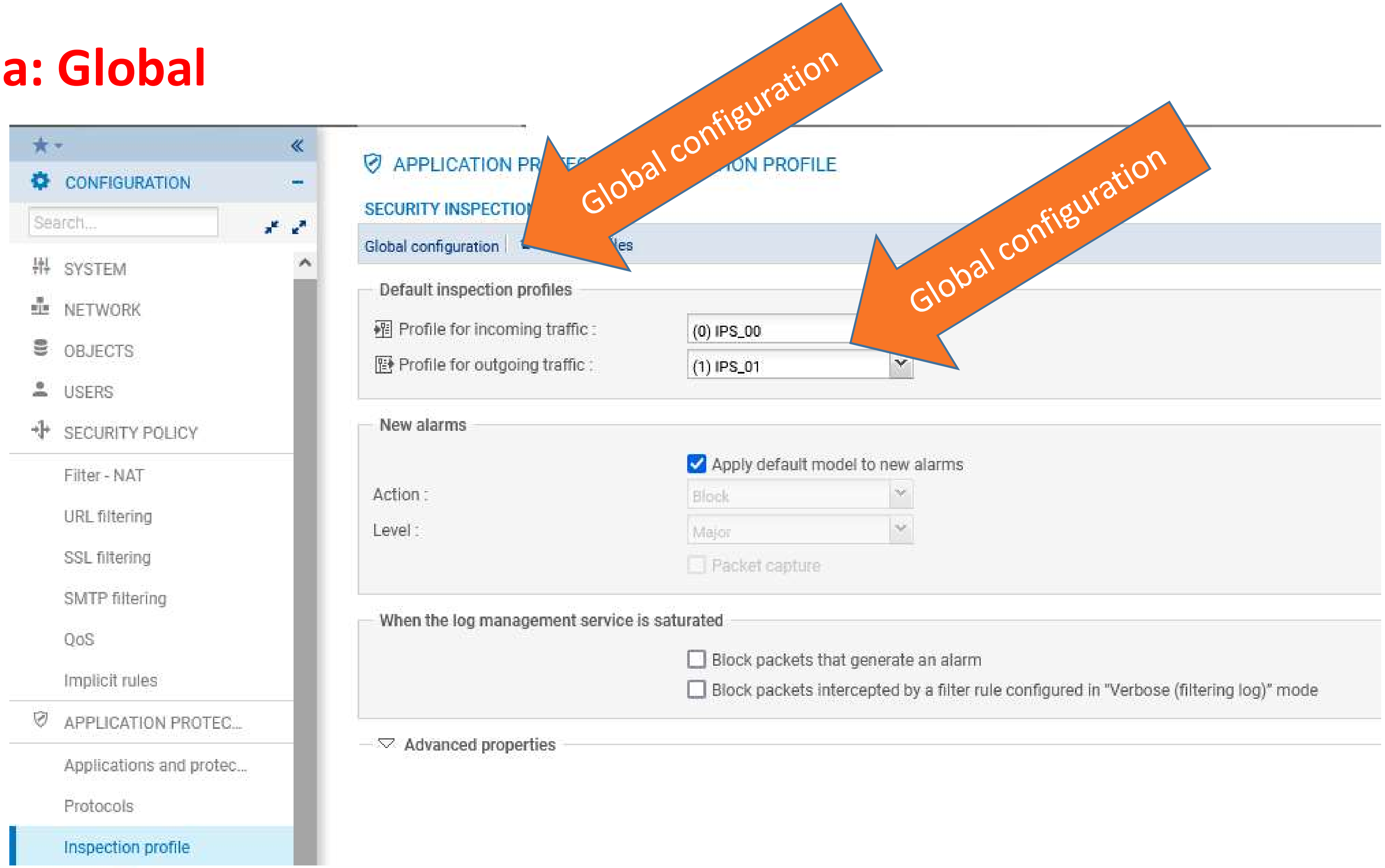
When the log management service is saturated

□ Block packets that generate an alarm

□ Block packets intercepted by a filter rule configured in "Verbose (filtering log)" mode

Advanced properties

- **Step 2 -a: Global**



Default inspection profiles

Profile for incoming traffic : (0) IPS_00

Profile for outgoing traffic : (1) IPS_01

New alarms

☑ Apply default model to new alarms

Action : Block

Level : Major

□ Packet capture

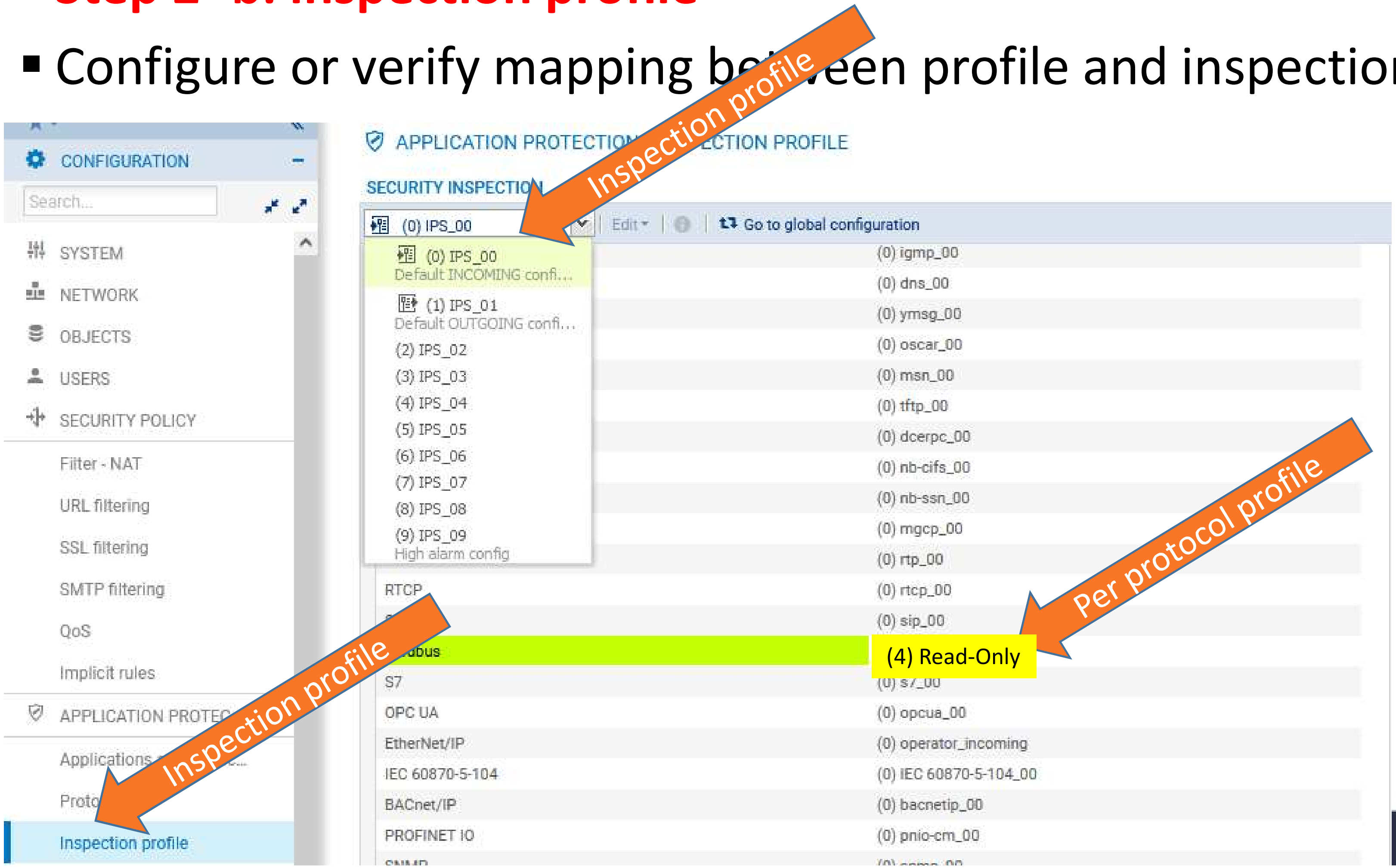
When the log management service is saturated

□ Block packets that generate an alarm

□ Block packets intercepted by a filter rule configured in "Verbose (filtering log)" mode

▪ Step 2 -b: inspection profile

- Configure or verify mapping between profile and inspection profile

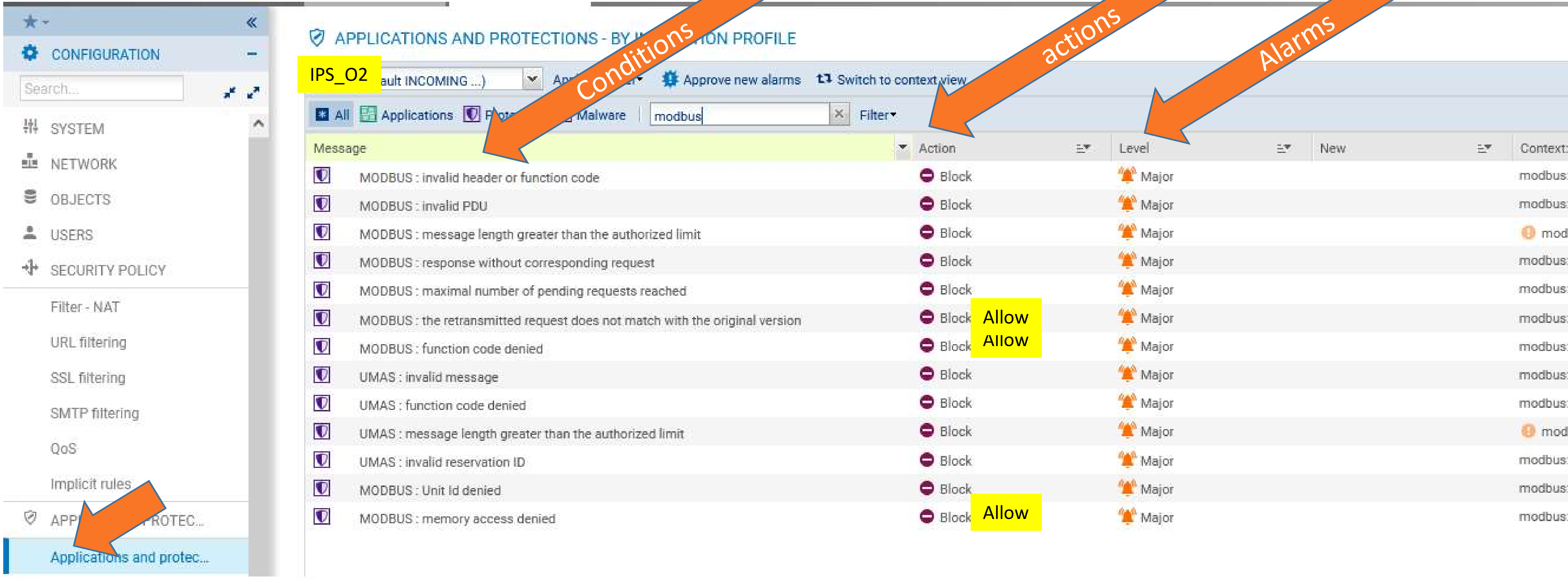


	(0) igmp_00
	(0) dns_00
	(0) ymsg_00
	(0) oscar_00
	(0) msn_00
	(0) tftp_00
	(0) dcerpc_00
	(0) nb-cifs_00
	(0) nb-ssn_00
	(0) mgcp_00
	(0) rtp_00
RTCP	(0) rtcp_00
	(0) sip_00
ubus	(4) Read-Only
S7	(0) s7_00
OPC UA	(0) opcua_00
EtherNet/IP	(0) operator_incoming
IEC 60870-5-104	(0) IEC 60870-5-104_00
BACnet/IP	(0) bacnetip_00
PROFINET IO	(0) pnio-cm_00

Cf. Book p.

▪ Step 3: alarms

▪ Configure or verify mapping between profile and inspection profile



Message	Action	Level	New	Context:
MODBUS : invalid header or function code	Block	Major		modbus:
MODBUS : invalid PDU	Block	Major		modbus:
MODBUS : message length greater than the authorized limit	Block	Major		mod
MODBUS : response without corresponding request	Block	Major		modbus:
MODBUS : maximal number of pending requests reached	Block	Major		modbus:
MODBUS : the retransmitted request does not match with the original version	Block Allow	Major		modbus:
MODBUS : function code denied	Block Allow	Major		modbus:
UMAS : invalid message	Block	Major		modbus:
UMAS : function code denied	Block	Major		modbus:
UMAS : message length greater than the authorized limit	Block	Major		mod
UMAS : invalid reservation ID	Block	Major		modbus:
MODBUS : Unit Id denied	Block	Major		modbus:
MODBUS : memory access denied	Block Allow	Major		modbus:

Cf. Book p.

Lab 2 : Using IPS to capture packet

- The IDS will allow packets but will capture each packet

1. Protocol/modbus

   Verify properties of the application profile «**(4) READ ONLY** »

2. Inspection profile :

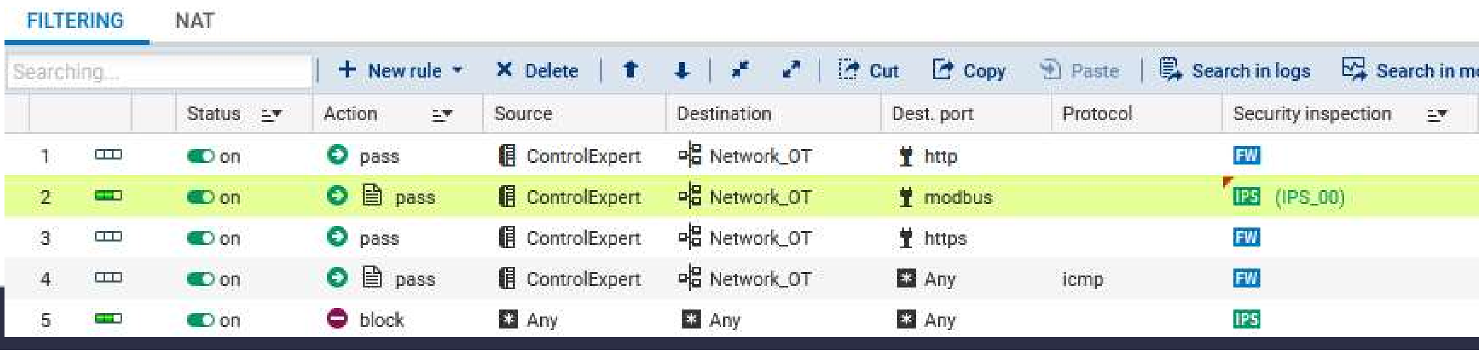
   IPS_02 =>ModBus => (4) **READ_ONLY**

3. Verify Global configuration (IPS_00 for input packets)

4. Set alarms and allow packets (see screen next page)
   - Function code denied
   - Memory access denied

5. Modify the filter rule

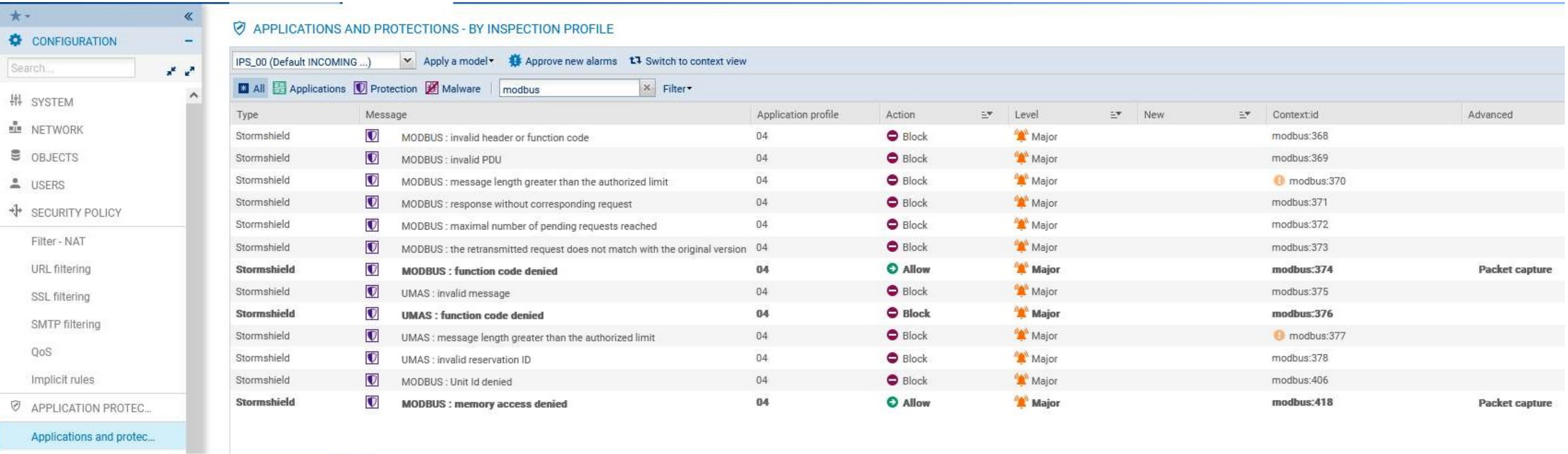
   IPS (IPS__02)



		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	ControlExpert	Network_OT	http		FW
2		on	pass	ControlExpert	Network_OT	modbus		IPS (IPS_00)
3		on	pass	ControlExpert	Network_OT	https		FW
4		on	pass	ControlExpert	Network_OT	Any	icmp	FW
5		on	block	Any	Any	Any		IPS

Cf. Book p.

- Allow packets
  - Function code denied
  - Modbus memory access denied
- Set packet capture



IPS_00 (Default INCOMING ...)

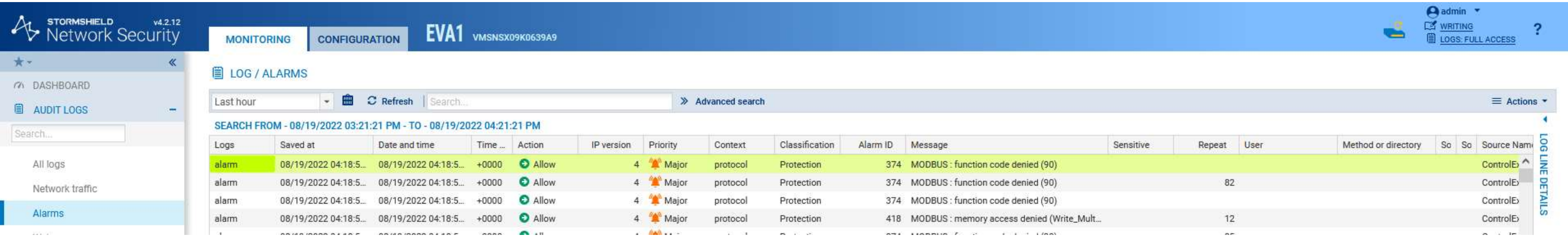
modbus

Type	Message	Application profile	Action	Level	New	Context:id	Advanced
Stormshield	MODBUS : invalid header or function code	04	Block	Major		modbus:368	
Stormshield	MODBUS : invalid PDU	04	Block	Major		modbus:369	
Stormshield	MODBUS : message length greater than the authorized limit	04	Block	Major		modbus:370	
Stormshield	MODBUS : response without corresponding request	04	Block	Major		modbus:371	
Stormshield	MODBUS : maximal number of pending requests reached	04	Block	Major		modbus:372	
Stormshield	MODBUS : the retransmitted request does not match with the original version	04	Block	Major		modbus:373	
Stormshield	**MODBUS : function code denied**	**04**	**Allow**	**Major**		**modbus:374**	**Packet capture**
Stormshield	UMAS : invalid message	04	Block	Major		modbus:375	
Stormshield	**UMAS : function code denied**	**04**	**Block**	**Major**		**modbus:376**	
Stormshield	UMAS : message length greater than the authorized limit	04	Block	Major		modbus:377	
Stormshield	UMAS : invalid reservation ID	04	Block	Major		modbus:378	
Stormshield	MODBUS : Unit Id denied	04	Block	Major		modbus:406	
Stormshield	**MODBUS : memory access denied**	**04**	**Allow**	**Major**		**modbus:418**	**Packet capture**

Cf. Book p.

Logs (Alarms) and packet capture

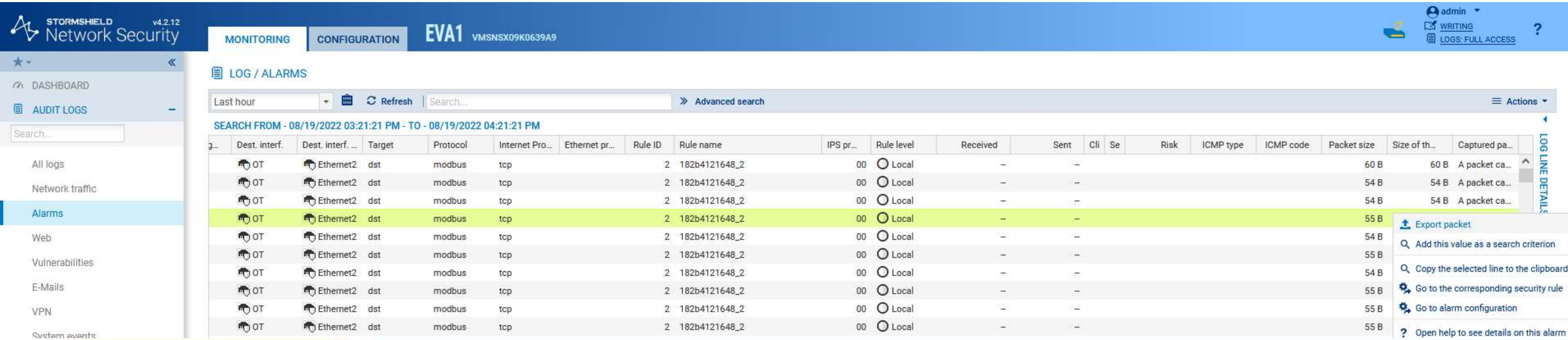
- Expand all the elements (actions dropdown button)



SEARCH FROM - 08/19/2022 03:21:21 PM - TO - 08/19/2022 04:21:21 PM

Logs	Saved at	Date and time	Time ...	Action	IP version	Priority	Context	Classification	Alarm ID	Message	Sensitive	Repeat	User	Method or directory	So	So	Source Nam
alarm	08/19/2022 04:18:5...	08/19/2022 04:18:5...	+0000	Allow	4	Major	protocol	Protection	374	MODBUS : function code denied (90)							ControlE
alarm	08/19/2022 04:18:5...	08/19/2022 04:18:5...	+0000	Allow	4	Major	protocol	Protection	374	MODBUS : function code denied (90)		82					ControlE
alarm	08/19/2022 04:18:5...	08/19/2022 04:18:5...	+0000	Allow	4	Major	protocol	Protection	374	MODBUS : function code denied (90)							ControlE
alarm	08/19/2022 04:18:5...	08/19/2022 04:18:5...	+0000	Allow	4	Major	protocol	Protection	418	MODBUS : memory access denied (Write_Mult...		12					ControlE

- At the end of rows :

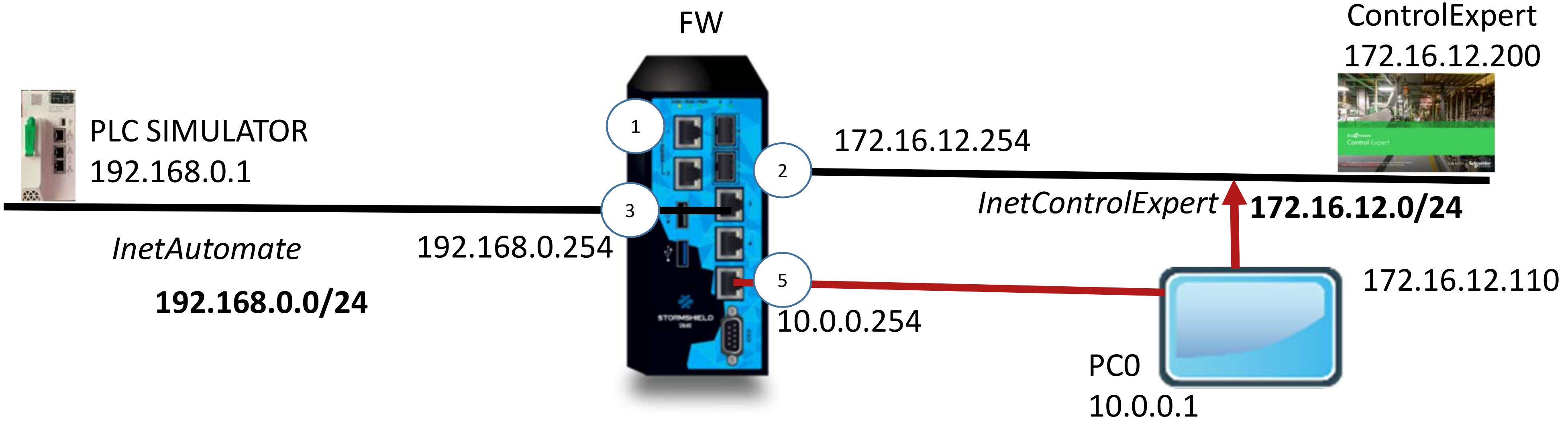


SEARCH FROM - 08/19/2022 03:21:21 PM - TO - 08/19/2022 04:21:21 PM

g...	Dest. interf.	Dest. interf. ...	Target	Protocol	Internet Pro...	Ethernet pr...	Rule ID	Rule name	IPS pr...	Rule level	Received	Sent	Cli	Se	Risk	ICMP type	ICMP code	Packet size	Size of th...	Captured pa...
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						60 B	60 B	A packet ca...
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						54 B	54 B	A packet ca...
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						54 B	54 B	A packet ca...
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						55 B		
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						54 B		
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						55 B		
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						54 B		
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						55 B		
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						55 B		
	OT	Ethernet2	dst	modbus	tcp		2	182b4121648_2	00	○ Local	–	–						55 B		

How to test

Cf. Book p.



FW

PLC SIMULATOR
192.168.0.1

1

2

3

5

ControlExpert
172.16.12.200

172.16.12.254

InetControlExpert

172.16.12.0/24

InetAutomate

192.168.0.254

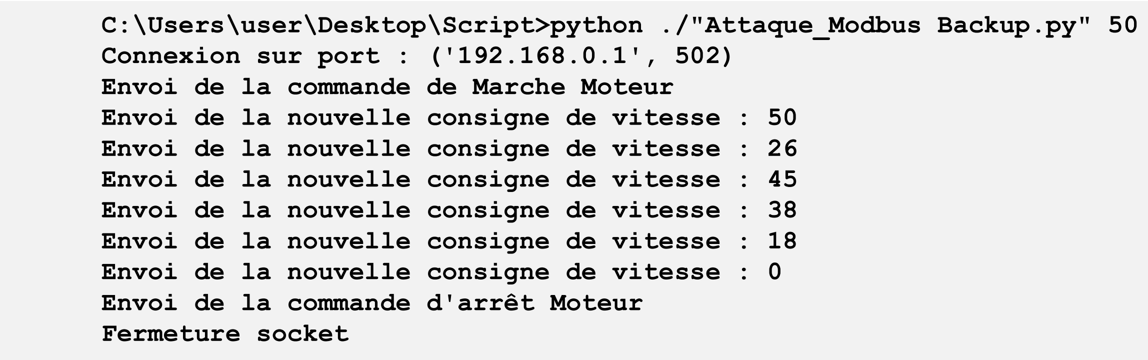
192.168.0.0/24

10.0.0.254

172.16.12.110

PC0
10.0.0.1

- PC0 (3rd card Connected to InetControlExpert)
  - IP = 172.16.12.110 (for example)
  - Open cmd in c:\users\Deskop\Scripts



```
C:\Users\user\Desktop\Script>python ./"Attaque_Modbus Backup.py" 50
Connexion sur port : ('192.168.0.1', 502)
Envoi de la commande de Marche Moteur
Envoi de la nouvelle consigne de vitesse : 50
Envoi de la nouvelle consigne de vitesse : 26
Envoi de la nouvelle consigne de vitesse : 45
Envoi de la nouvelle consigne de vitesse : 38
Envoi de la nouvelle consigne de vitesse : 18
Envoi de la nouvelle consigne de vitesse : 0
Envoi de la commande d'arrêt Moteur
Fermeture socket
```

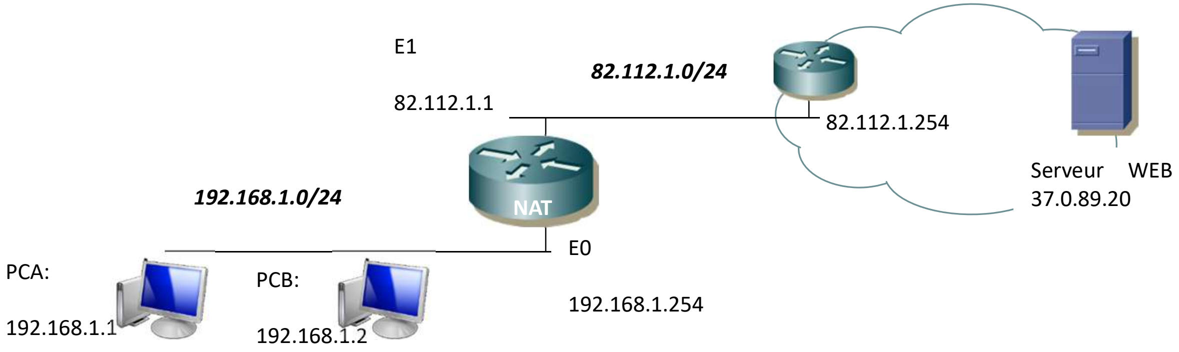
Cf. Book p.

Outline

- LAB-0 : Preparing set-up
  - VMS
  - Initial state with basic router
  - Connectivity tests (see exercises on routing)
- LAB-1 : Filtering
  - Pass all
  - Filters with a firewall
- MODBUS frames
- IDS/IPS with a Stormshield Firewall
- LAB-2 : Analysing frames with Wireshark and IPS
- **Network address translation**
- **LAB-3 : NAT**
- **A word about UMAS**
- **Final : cybersecurity ?**

Cf. Book p.

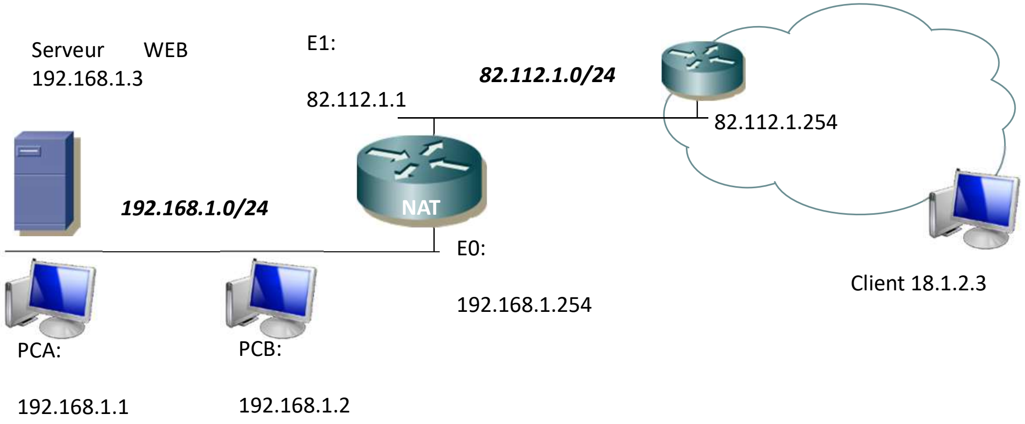
Network adress translation (SNAT)



Internal parameters (local)		Internal parameters (global)		External parameters (global)		Comments
IP	port	IP	port	IP	port	

Cf. Book p.

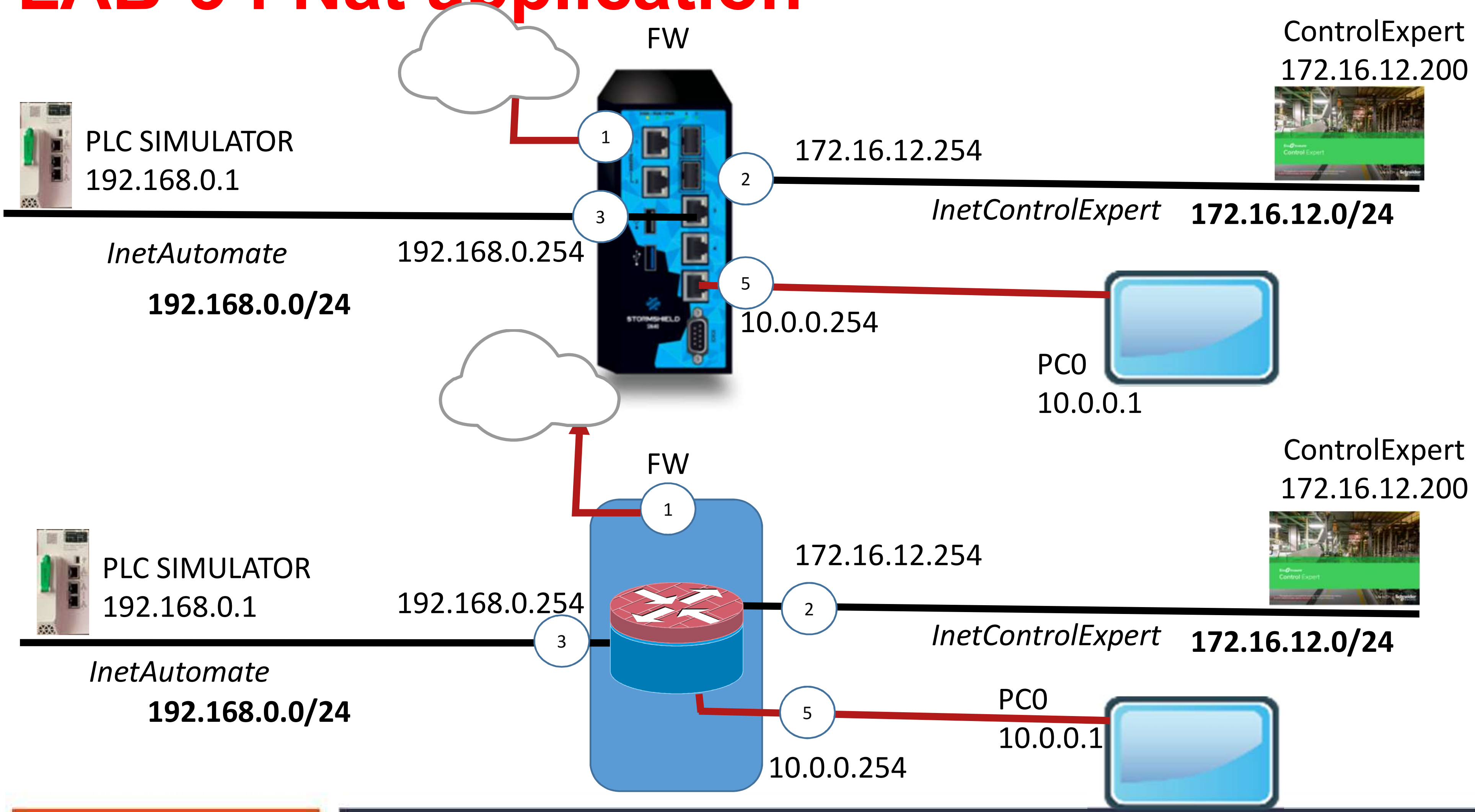
Network Address translation (DNAT)



	Internal parameters (local)		Internal parameters (global)		External parameters (global)		Comments
	IP	port	IP	port	IP	port	
L1							
L2							

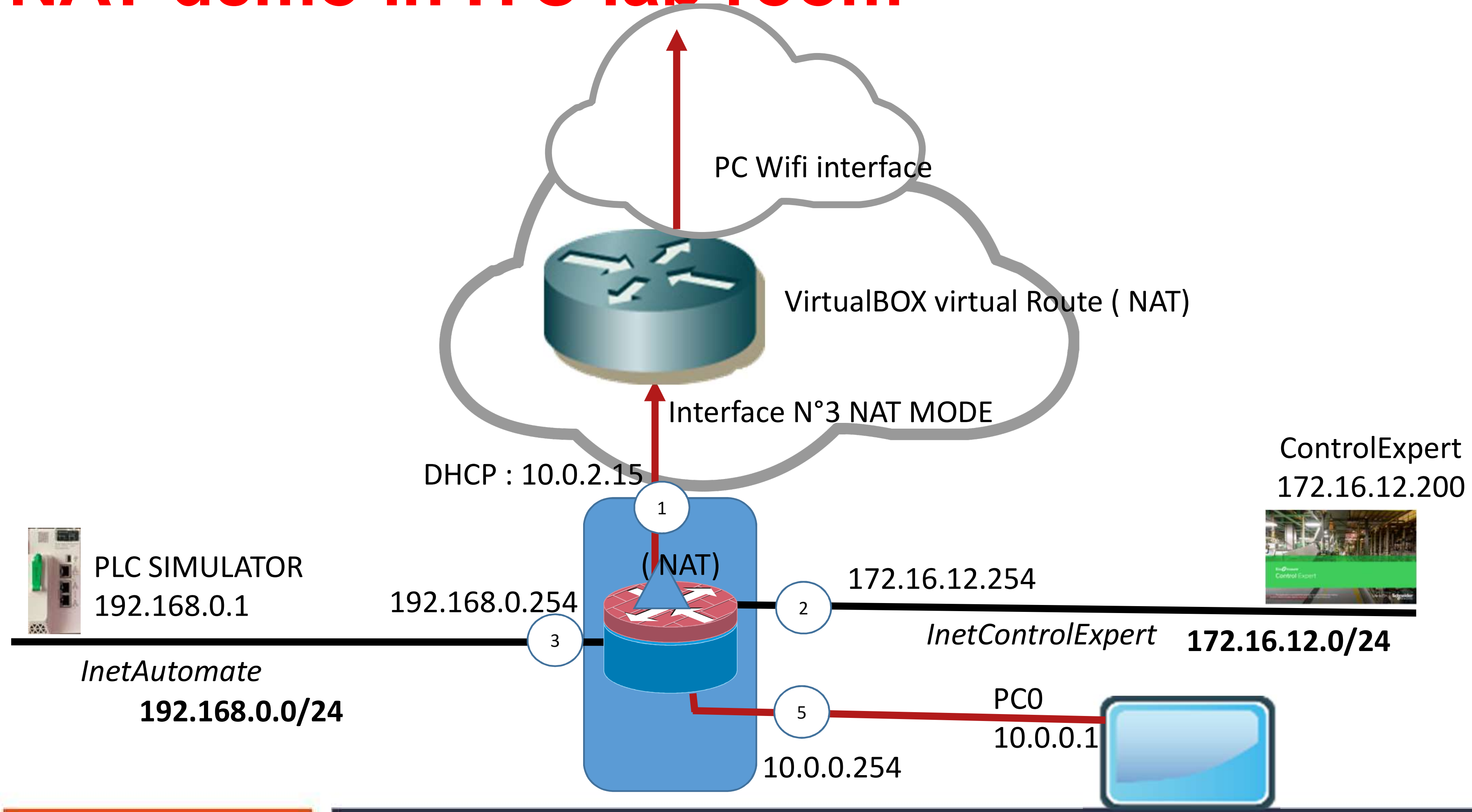
Cf. Book p.

LAB-3 : Nat application



Cf. Book p.

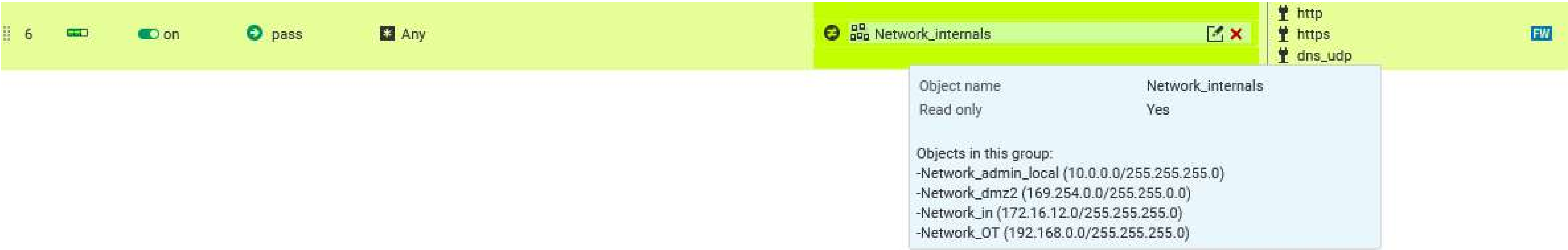
NAT demo in ITC lab room



Cf. Book p.

Rules

- New rules to allow traffic towards internet
  - Traffic HTTP and HTTPS allowed
  - DNS allowed : google DNS : 8.8.8.8

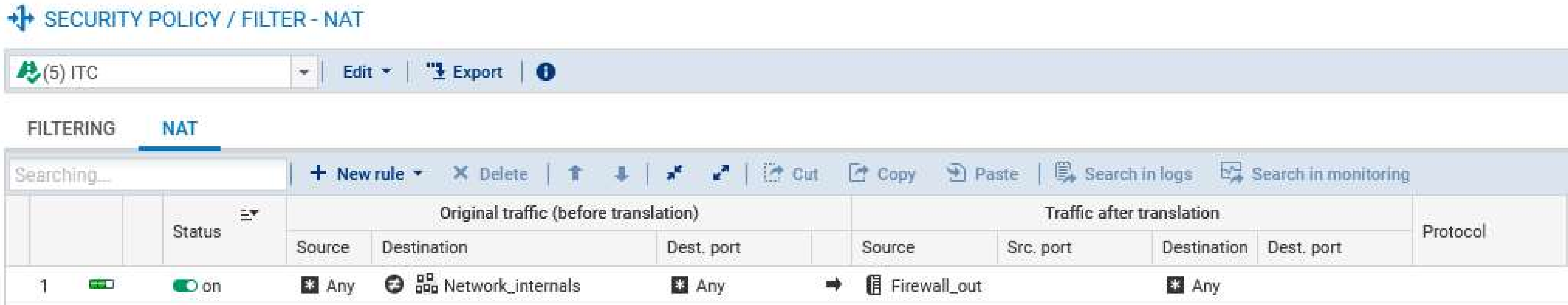


6		on	pass	Any	Network_internals	http https dns_udp	FW

Object name Network_internals
Read only Yes

Objects in this group:
-Network_admin_local (10.0.0.0/255.255.255.0)
-Network_dmz2 (169.254.0.0/255.255.0.0)
-Network_in (172.16.12.0/255.255.255.0)
-Network_OT (192.168.0.0/255.255.255.0)

- NAT RULE



SECURITY POLICY / FILTER - NAT

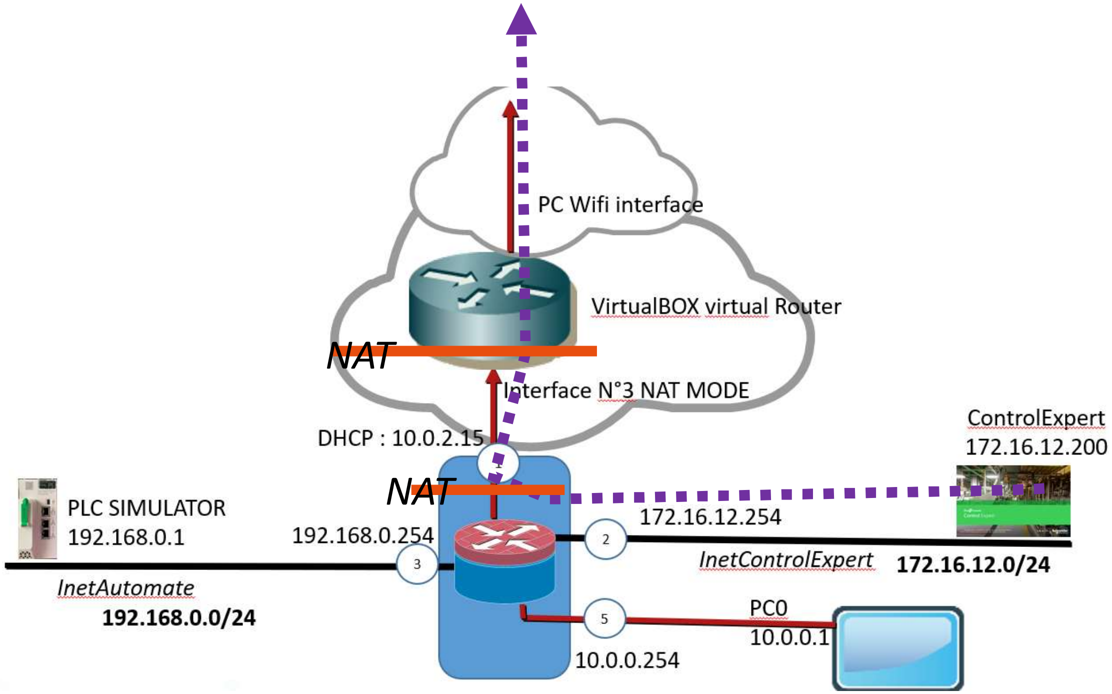
(5) ITC | Edit | Export

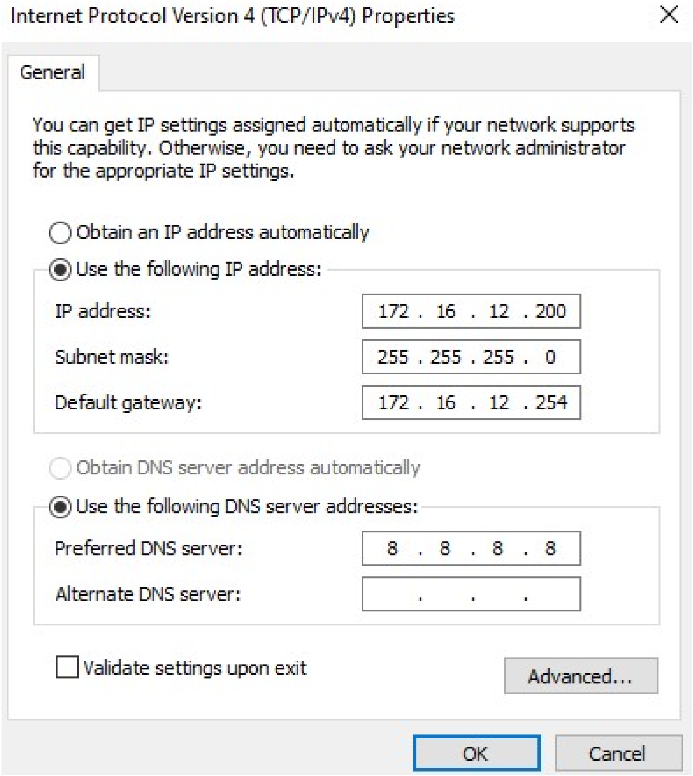
FILTERING | NAT

		Status	Original traffic (before translation)				Traffic after translation				Protocol
			Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port	
1		on	Any	Network_internals	Any	➡	Firewall_out		Any		

Cf. Book p.

Control Expert access to internet




Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	172 . 16 . 12 . 200
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	172 . 16 . 12 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	. . .

□ Validate settings upon exit

Cf. Book p.

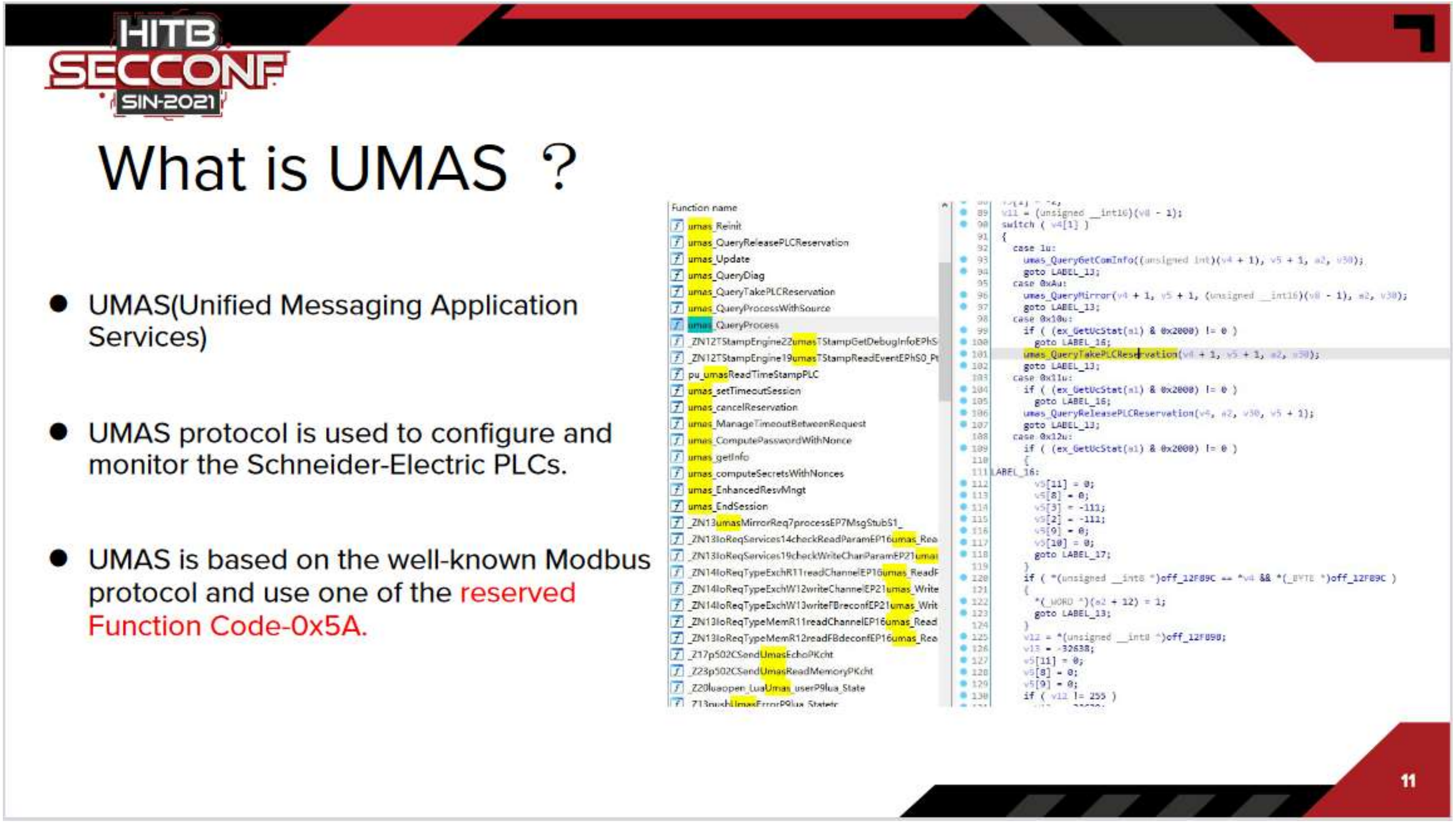
Outline

- LAB-0 : Preparing set-up
  - VMS
  - Initial state with basic router
  - Connectivity tests (see exercices on routing)
- LAB-1 : Filtering
  - Pass all
  - Filters with a firewall
- MODBUS frames
- IDS/IPS with a Stormshield Firewall
- LAB-2 : Analysing frames with Wireshark and IPS
- Network address translation
- LAB-3 : NAT
- **A word about UMAS**
- **Final : cybersecurity ?**

Cf. Book p.

A word about UMAS

- An extended protocol used by Control Expert (function code 90=0x5a)



HITB SECCONF SIN-2021

What is UMAS ?

- UMAS(Unified Messaging Application Services)
- UMAS protocol is used to configure and monitor the Schneider-Electric PLCs.
- UMAS is based on the well-known Modbus protocol and use one of the reserved Function Code-0x5A.

```
Function name
umas_Reinit
umas_QueryReleasePLCReservation
umas_Update
umas_QueryDiag
umas_QueryTakePLCReservation
umas_QueryProcessWithSource
umas_QueryProcess
_ZN12TStampEngine22umasTStampGetDebugInfoEPhS
_ZN12TStampEngine19umasTStampReadEventEPhS0_Pt
pu_umasReadTimeStampPLC
umas_setTimeoutSession
umas_cancelReservation
umas_ManageTimeoutBetweenRequest
umas_ComputePasswordWithNonce
umas_getInfo
umas_computeSecretsWithNonces
umas_EnhancedResvMngt
umas_EndSession
_ZN13umasMirrorReq7processEP7MsgStubS1_
_ZN13IoReqServices14checkReadParamEP16umas_Rea
_ZN13IoReqServices19checkWriteCharParamEP21umas
_ZN14IoReqTypeExchR11readChannelEP16umas_ReadF
_ZN14IoReqTypeExchW12writeChannelEP21umas_Write
_ZN14IoReqTypeExchW13writeFBreconfEP21umas_Writ
_ZN13IoReqTypeMemR11readChannelEP16umas_Read
_ZN13IoReqTypeMemR12readFBdeconfEP16umas_Rea
_Z17p502CSendUmasEchoPKcht
_Z23p502CSendUmasReadMemoryPKcht
_Z20luaopen_LuaUmas_userP9lua_State
_Z13pushUmasErrorP9lua_Statetc
```

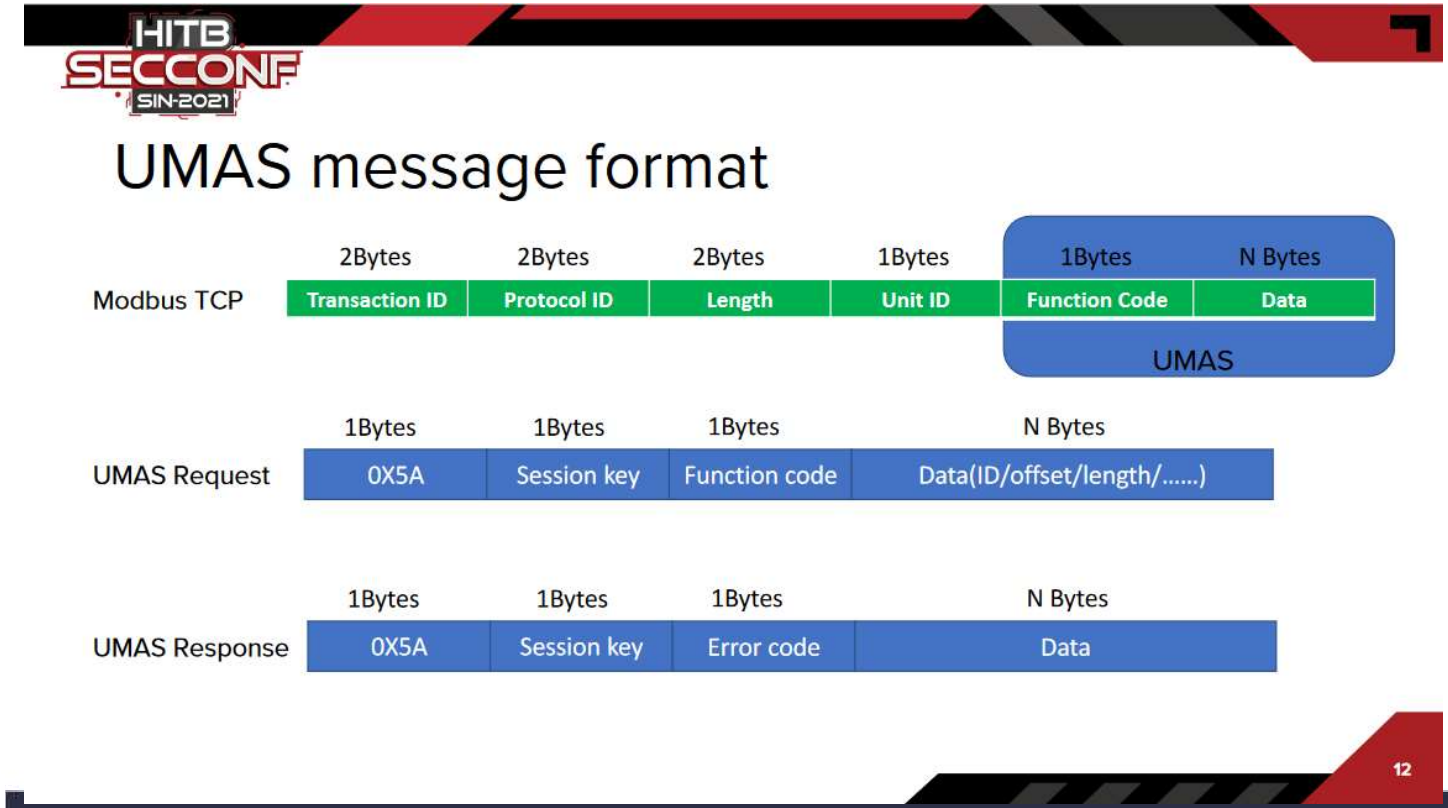
```
  v11 = (unsigned __int16)(v8 - 1);
  switch ( v4[1] )
  {
    case 1u:
      umas_QueryGetComInfo((unsigned int)(v4 + 1), v5 + 1, a2, v30);
      goto LABEL_13;
    case 0xAu:
      umas_QueryMirror(v4 + 1, v5 + 1, (unsigned __int16)(v8 - 1), a2, v30);
      goto LABEL_13;
    case 0x10u:
      if ( (ex_GetUcStat(a1) & 0x2000) != 0 )
        goto LABEL_16;
      umas_QueryTakePLCReservation(v4 + 1, v5 + 1, a2, v30);
      goto LABEL_13;
    case 0x11u:
      if ( (ex_GetUcStat(a1) & 0x2000) != 0 )
        goto LABEL_16;
      umas_QueryReleasePLCReservation(v4, a2, v30, v5 + 1);
      goto LABEL_13;
    case 0x12u:
      if ( (ex_GetUcStat(a1) & 0x2000) != 0 )
      {
LABEL_16:
        v5[11] = 0;
        v5[8] = 0;
        v5[3] = -111;
        v5[2] = -111;
        v5[9] = 0;
        v5[10] = 0;
        goto LABEL_17;
      }
      if ( *(unsigned __int8 *)off_12F89C == *v4 && *(_BYTE *)off_12F89C )
      {
        *(_WORD *)(a2 + 12) = 1;
        goto LABEL_13;
      }
      v12 = *(unsigned __int8 *)off_12F898;
      v13 = -32638;
      v5[11] = 0;
      v5[8] = 0;
      v5[9] = 0;
      if ( v12 != 255 )
```

11

https://conference.hitb.org/hitbsecconf2021sin/sessions/going-deeper-into-schneider-modicon-pac-security/

Cf. Book p.

- Session key required for some operations (Not ALL)
- Some attacks are however possible to break the key ?



HITB SECCONF SIN-2021

UMAS message format

	2Bytes	2Bytes	2Bytes	1Bytes	1Bytes	N Bytes
Modbus TCP	Transaction ID	Protocol ID	Length	Unit ID	Function Code	Data
					UMAS	

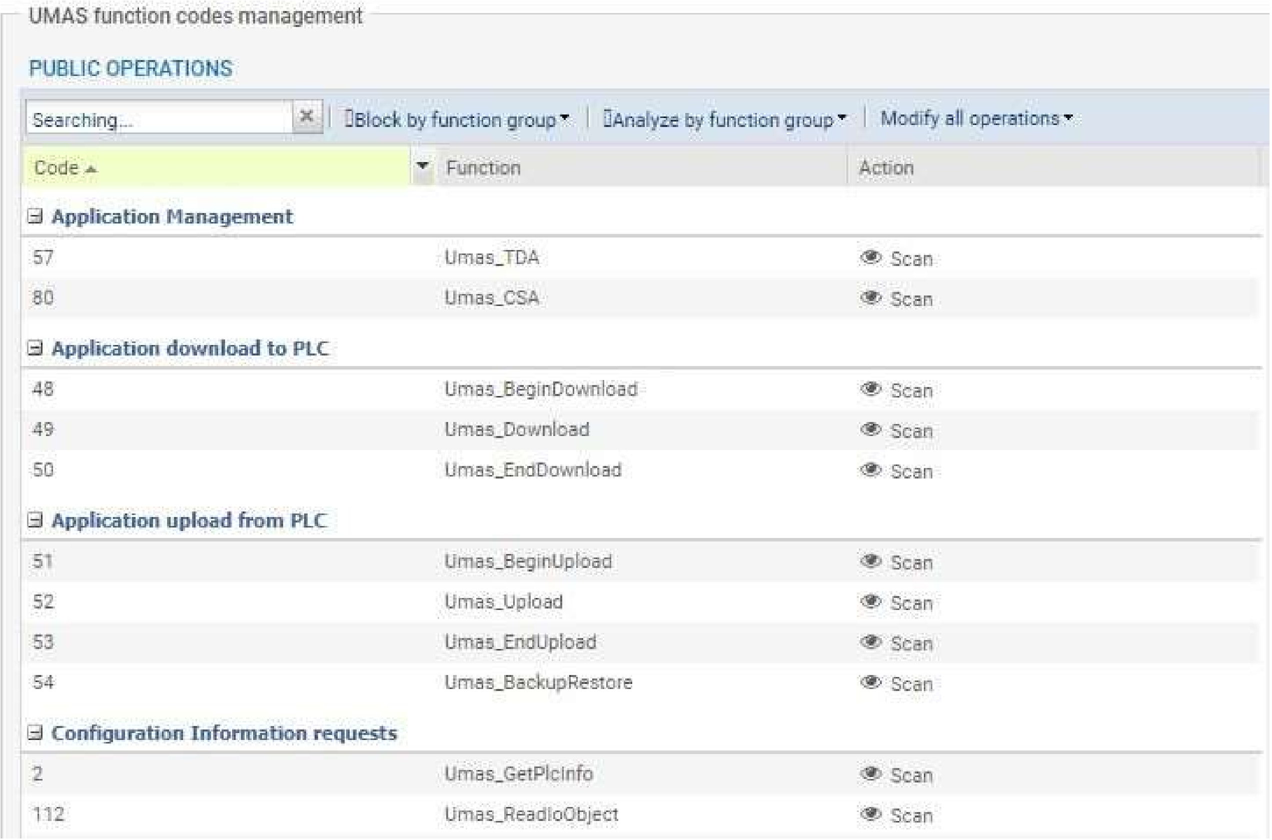
	1Bytes	1Bytes	1Bytes	N Bytes
UMAS Request	0X5A	Session key	Function code	Data(ID/offset/length/......)

	1Bytes	1Bytes	1Bytes	N Bytes
UMAS Response	0X5A	Session key	Error code	Data

12

Cf. Book p.

Some UMAS function codes



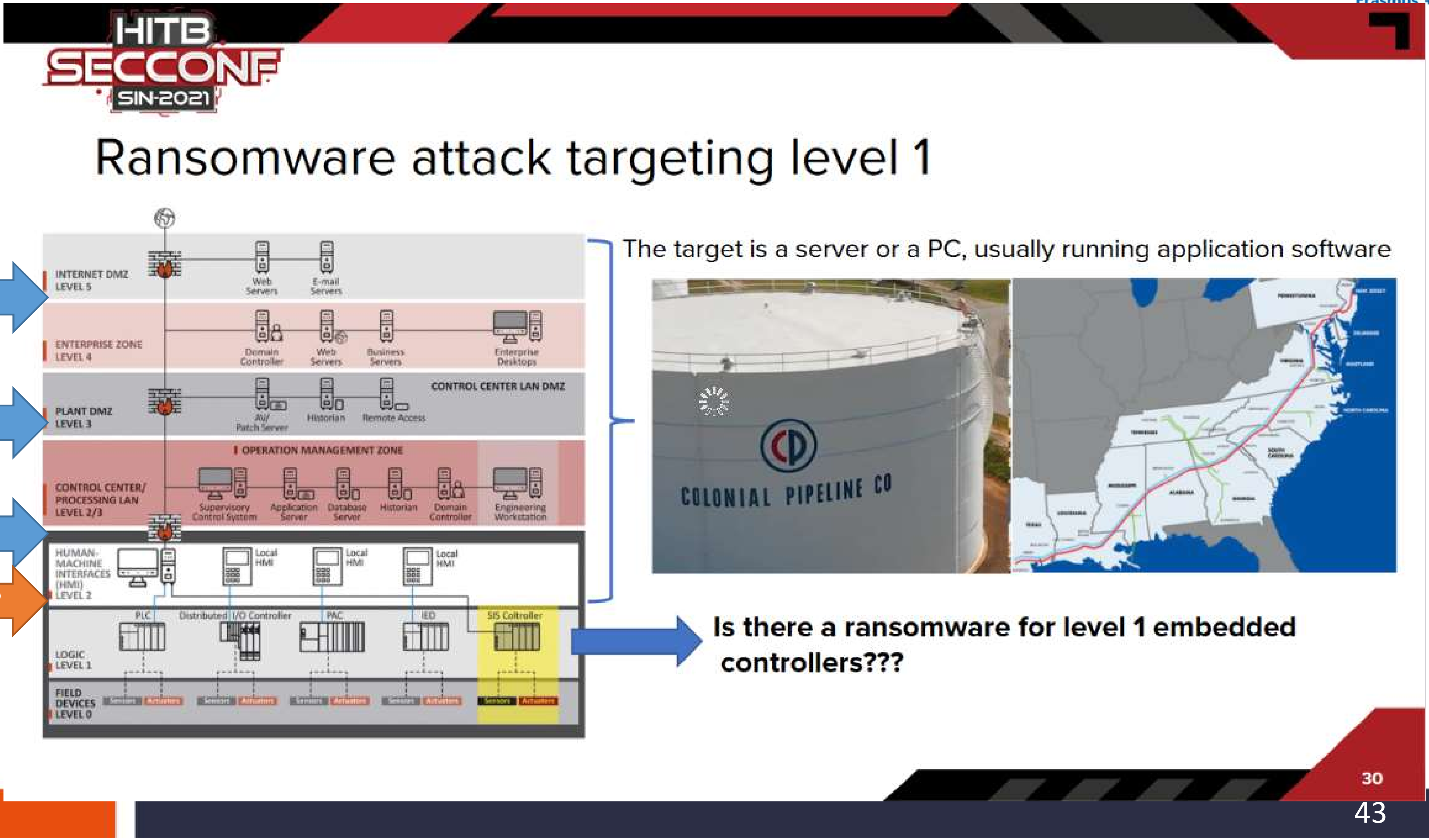
UMAS function codes management

PUBLIC OPERATIONS

Code	Function	Action
Application Management		
57	Umas_TDA	Scan
80	Umas_CSA	Scan
Application download to PLC		
48	Umas_BeginDownload	Scan
49	Umas_Download	Scan
50	Umas_EndDownload	Scan
Application upload from PLC		
51	Umas_BeginUpload	Scan
52	Umas_Upload	Scan
53	Umas_EndUpload	Scan
54	Umas_BackupRestore	Scan
Configuration Information requests		
2	Umas_GetPlcInfo	Scan
112	Umas_ReadIoObject	Scan

Cf. Book p.

Cybersecurity on industrial systems



HITB SECCONF SIN-2021

Ransomware attack targeting level 1

The target is a server or a PC, usually running application software

Is there a ransomware for level 1 embedded controllers???

FW

FW

FW

FW ?