TP7 - Cybersecurity - Internet access through the SNi40

Operational objectives :

- Be able to configure Internet access from an SNi40 subnet
- Be able to define filtering rules to secure Internet access
- Be able to configure secure Internet access to an SNi40 subnet

Prerequisites :

- Be able to launch Vijeo Designer in simulation mode
- Understand the main principles of SNi40 configuration
- To have understood the principle of network separation on an SNi40

The problem :

- To set up secure Internet access from a subnet of the SNi40 and to a subnet of the SNi40.

Note :

This tutorial will be based on a split network configuration of the SNi40. An example configuration "SNi40 - Splitted Networks.na" is provided, the SNi40 can be accessed from port 3 dedicated to the administration network with the IP configuration 172.16.112.200/24 and the SNi40 gateway 172.16.112.254. Port 2 is dedicated to the industrial network 172.16.12.0/24 and port 1 must be connected to an Internet access. The correct functioning of the Internet access can be checked by updating the SNi40 via the Internet.

In addition, the part of the tutorial related to setting up a VPN tunnel to access the administrator's network from the Internet requires a compatible Internet router with VPN capabilities. If this is the case, it is quite possible that the VPN connections cannot pass through the NAT of the Internet router.

Resources :

- **Manufacturer documentation**
  - Schneider Electric
    - website
    - protocol-modbus.pdf
  - Stormshield :
    - SNS - User and Configuration Manual
- **Specific documentation**
  - Architectures Maquette Cybersec_anglais.pptx
- **Applications made available for the realization of this TP :**
  - M580 application (Control Expert): md1ae58ecyb.stu
  - HMI application (Vijeo Designer): MD1AE58ECYB
  - Default SNi40 Firewall configuration file (SNI40-TP2-0.na)
- **Software provided, to be installed on the work PC (console) for the realization of this TP:**
  - Control Expert (Schneider Electric) : Programming of Schneider Electric M340, M580, …
  - Vijeo Designer V6.2 SP8 : Design of Magelis HMI applications (execution including in Simulation mode on the Workstation)
  - Web Gate Client (Schneider Electric): complement to Vijeo Designer [option] (remote client of the Magelis HMI, 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

Evaluation criteria :	😄	😐	☹️
Be able to configure Internet access from an SNi40 subnet			
Be able to define filtering rules to secure Internet access			
Be able to configure an Internet access to an SNi40 subnet			
Autonomy - Quality of work/restitution			

Time spent :	30 m	**Objective(s) :**		Observation(s) :
Evaluation :	/ 20	Reached(s)	Not reached	

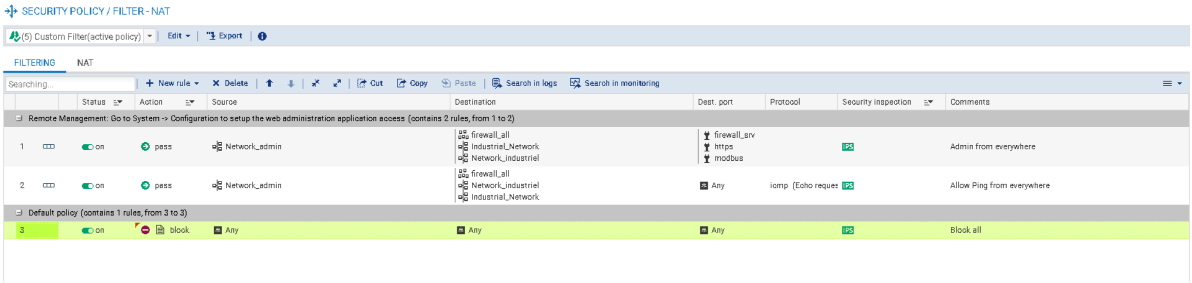
TP7 - Internet access through SNI40

1. You wish to give Internet access to the equipment on the administrator network through the Internet connection available on the firewall. Set the security policy to "pass all" and configure a NAT rule to allow Internet access from the administrator network. Check that Internet access from the administrator network is in place.
2. Configure access restrictions to allow Internet access from the administrator network only to the main services generally used: Web, Mail etc.

Details of expected operations

1. Setting up Internet access for the administrator network

In the **Configuration** > **Security Policy** > **Filtering and NAT** tab, start by enabling the security policy named "**Custom Filter**" if it is not already enabled:



SECURITY POLICY / FILTER - NAT

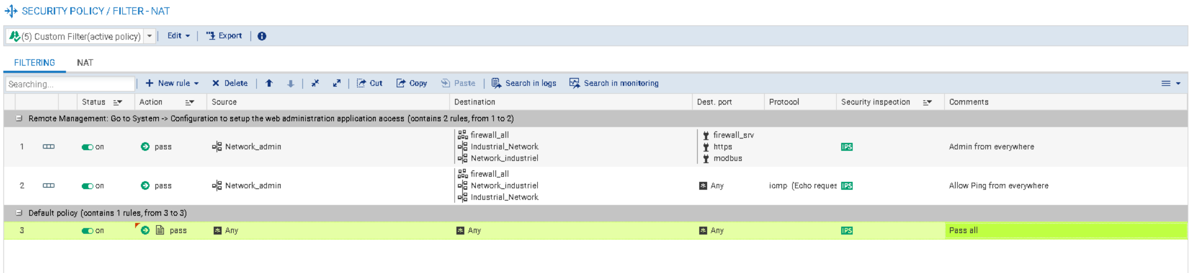
(5) Custom Filter(active policy) | Edit | Export

FILTERING | NAT

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Remote Management: Go to System -> Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)									
1		on	pass	Network_admin	firewall_all Industrial_Network Network_industriel	firewall_srv https modbus		IPS	Admin from everywhere
2		on	pass	Network_admin	firewall_all Network_industriel Industrial_Network	Any	icmp (Echo reques	IPS	Allow Ping from everywhere
Default policy (contains 1 rules, from 3 to 3)									
3		on	block	Any	Any	Any		IPS	Block all

The same logo to the left of the "Activate this policy" button should then appear to the left of the security policy name in the drop-down menu.

Also change the default rule to a "pass all" rule as follows:



SECURITY POLICY / FILTER - NAT

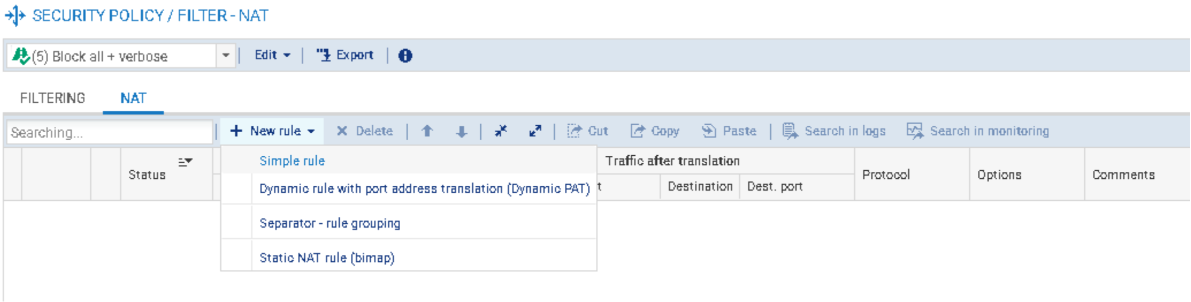
(5) Custom Filter(active policy) | Edit | Export

FILTERING | NAT

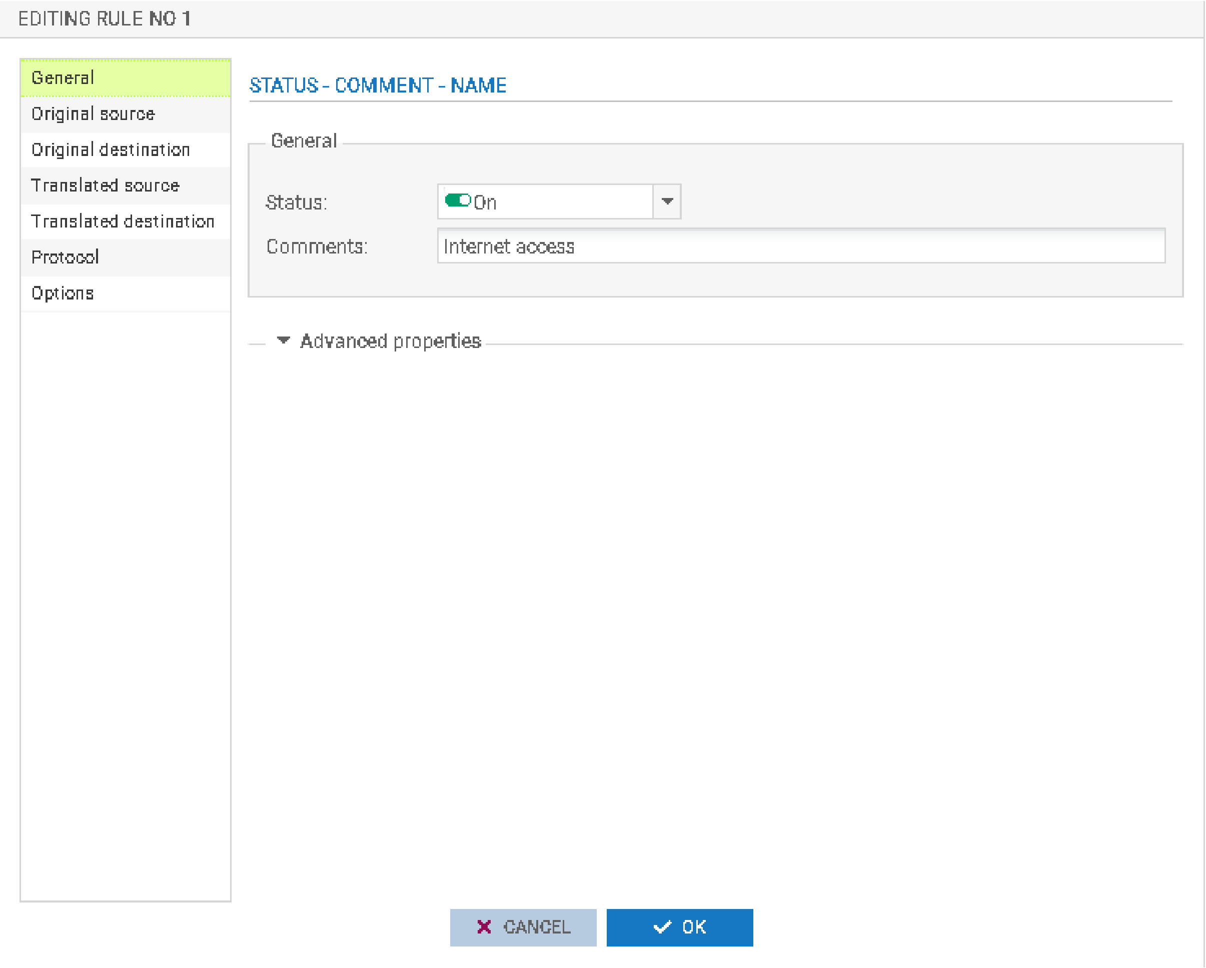
		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Remote Management: Go to System -> Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)									
1		on	pass	Network_admin	firewall_all Industrial_Network Network_industriel	firewall_srv https modbus		IPS	Admin from everywhere
2		on	pass	Network_admin	firewall_all Network_industriel Industrial_Network	Any	icmp (Echo reques	IPS	Allow Ping from everywhere
Default policy (contains 1 rules, from 3 to 3)									
3		on	pass	Any	Any	Any		IPS	Pass all

Save and activate the security policy when requested.

Still in the same tab, go to the page called "**NAT**", and create a new simple rule:



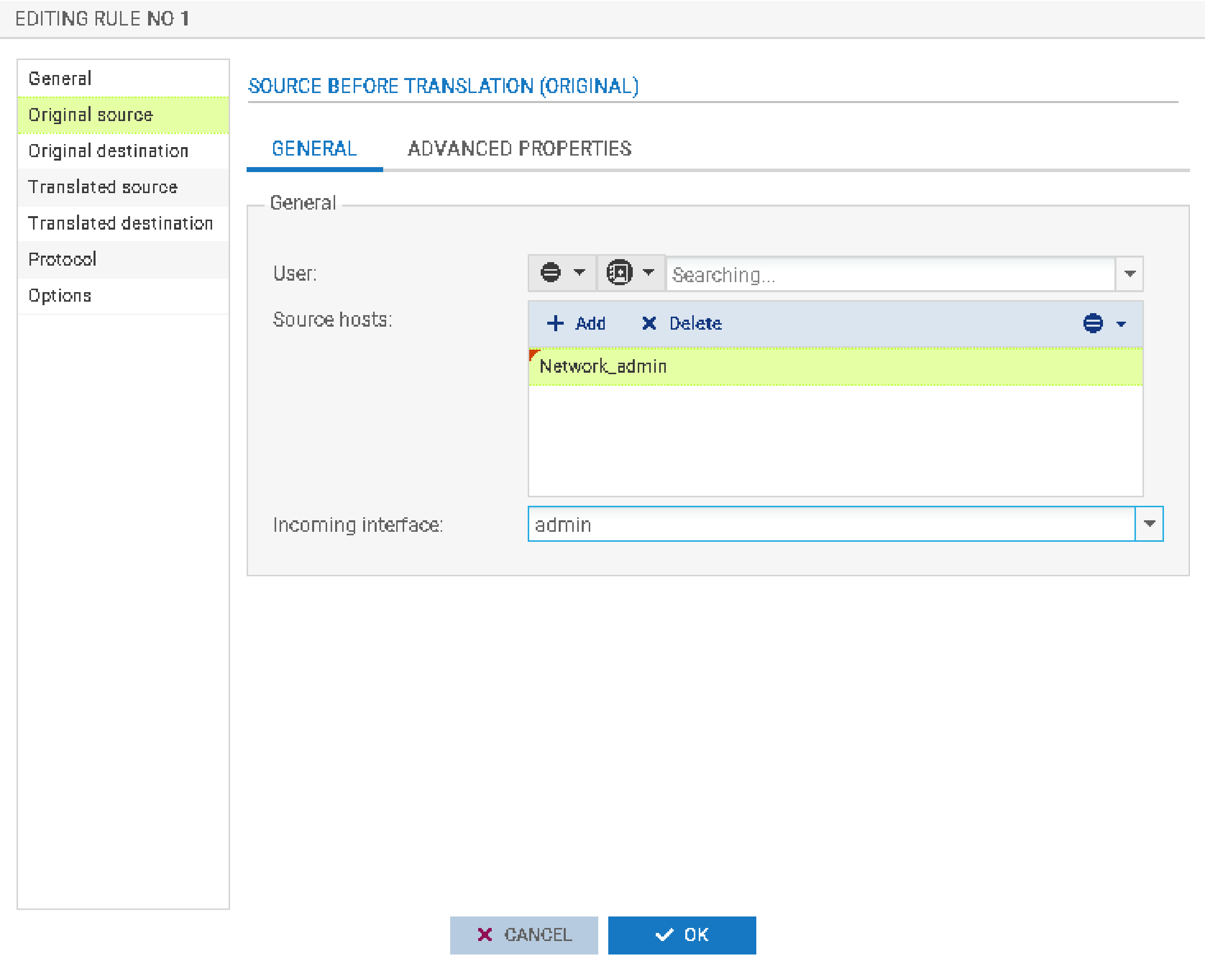
Double click on the rule that appears to modify it, in **General** set the status to **On** and modify the comment if desired:



Status: On

Comments: Internet access

In **Original Source**, change "**Any**" to "**Network_admin**" and select "admin" as the input interface:

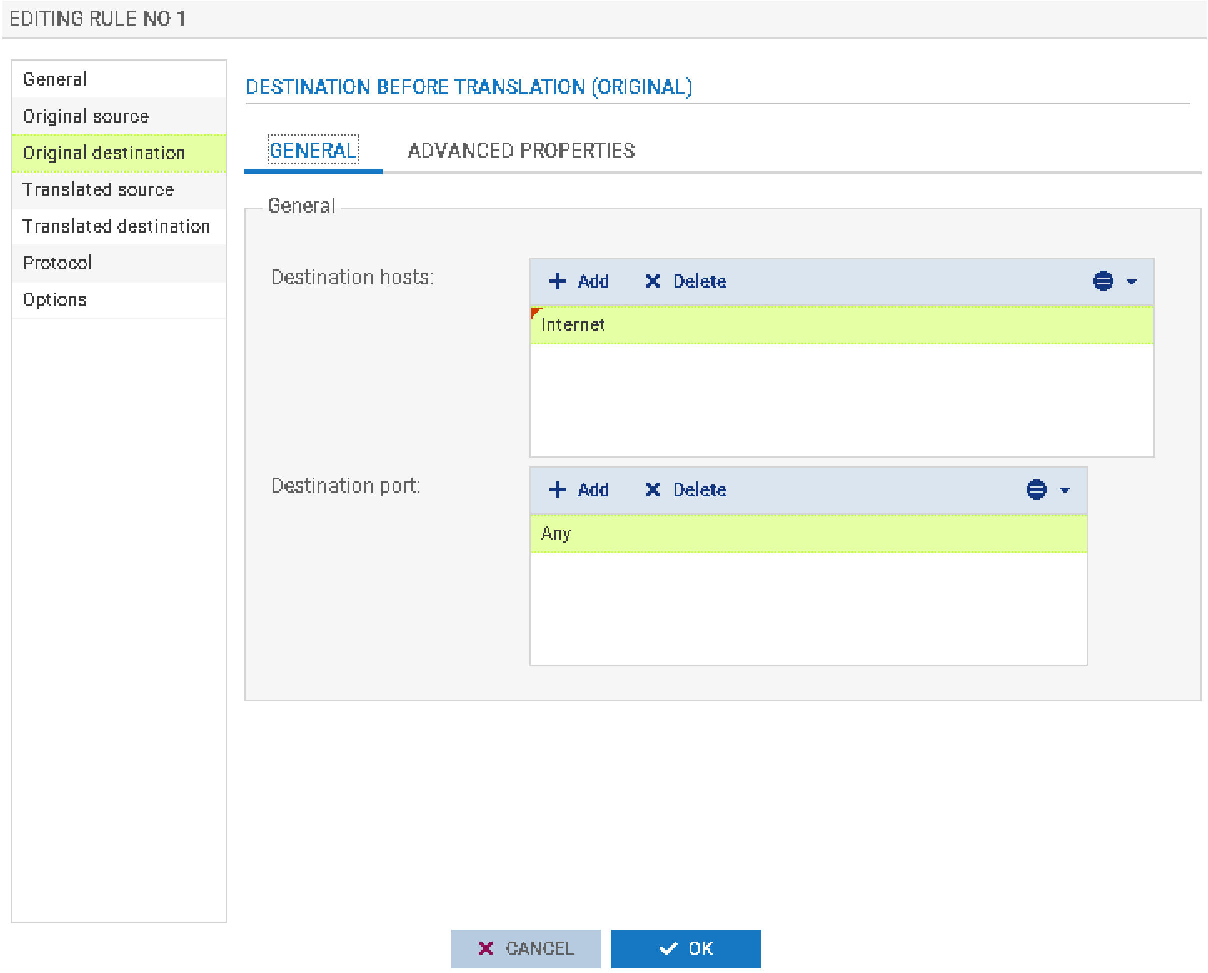


User: Searching...

Source hosts: Network_admin

Incoming interface: admin

In Original Destination choose "Internet" and in the advanced configuration the "out" interface:



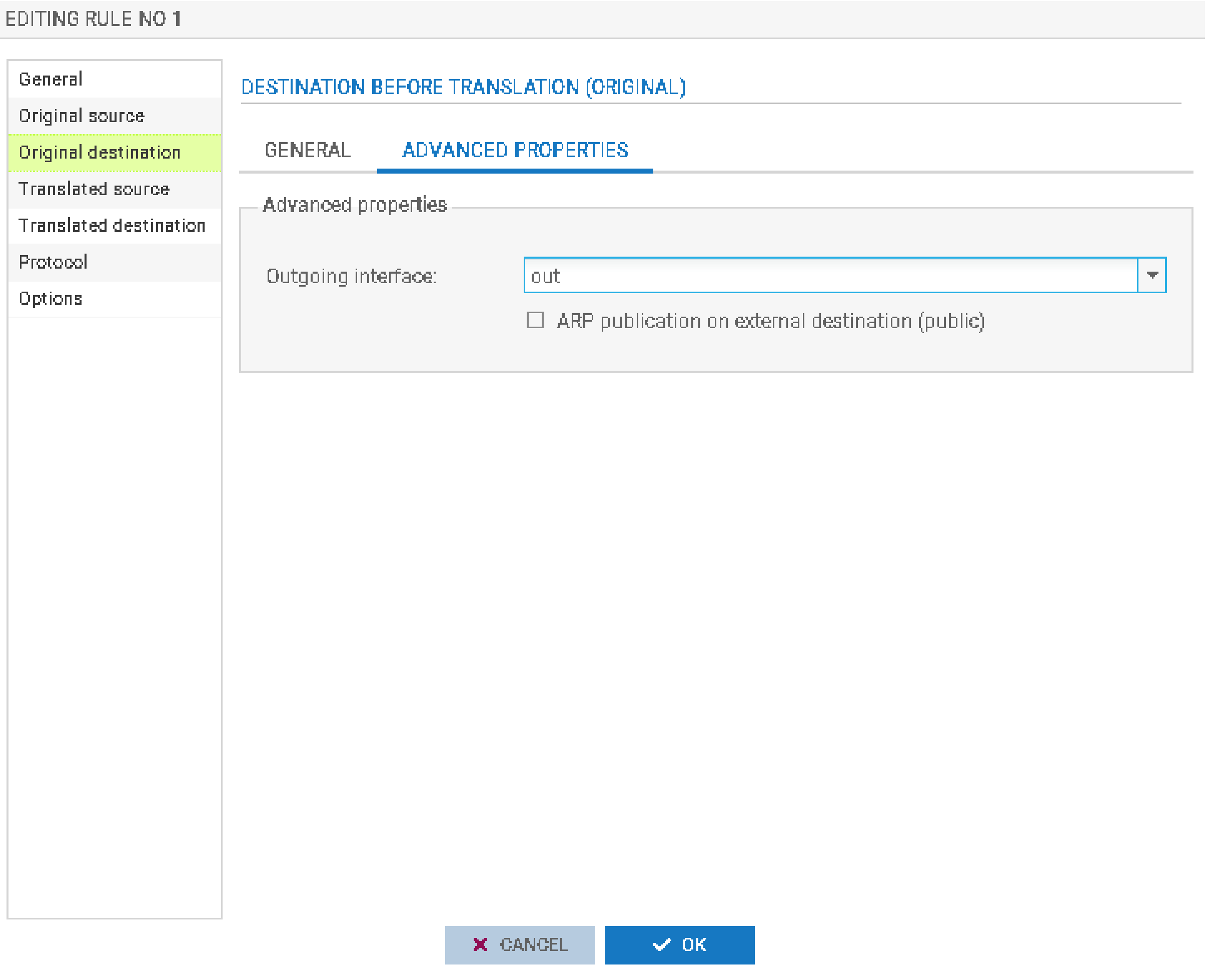
EDITING RULE NO 1

DESTINATION BEFORE TRANSLATION (ORIGINAL)

General

Destination hosts: Internet

Destination port: Any


EDITING RULE NO 1

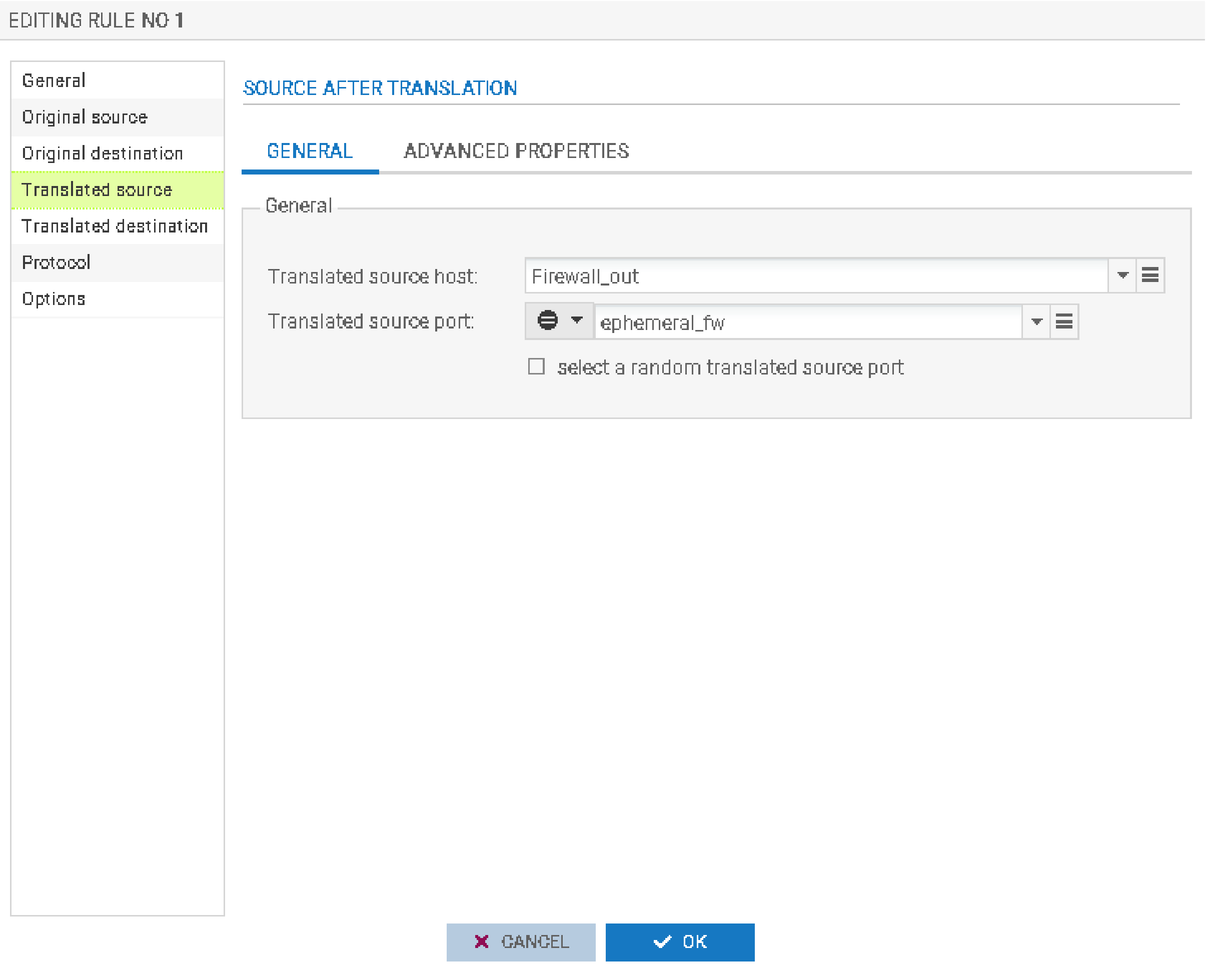
DESTINATION BEFORE TRANSLATION (ORIGINAL)

Advanced properties

Outgoing interface: out

□ ARP publication on external destination (public)

In **Translate Source** set the source to "**Firewall_out**" and the source port to "**ephemeral_fw**":



EDITING RULE NO 1

SOURCE AFTER TRANSLATION

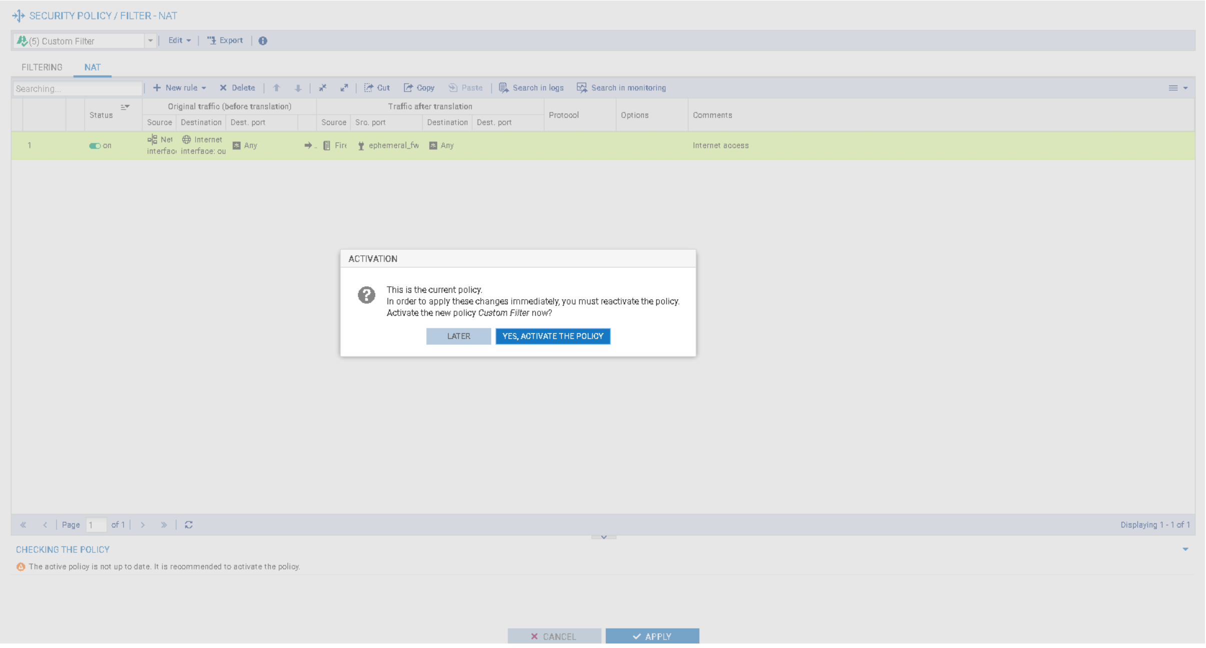
General

Translated source host: Firewall_out

Translated source port: ephemeral_fw

□ select a random translated source port

Leave the other tabs as they are, then save and activate the new policy:



SECURITY POLICY / FILTER - NAT

	Status	Original traffic (before translation)				Traffic after translation				Protocol	Options	Comments
		Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port			
1	on	Net interfac	Internet interface: ou	Any	→ ..	Fire	ephemeral_fw	Any				Internet access

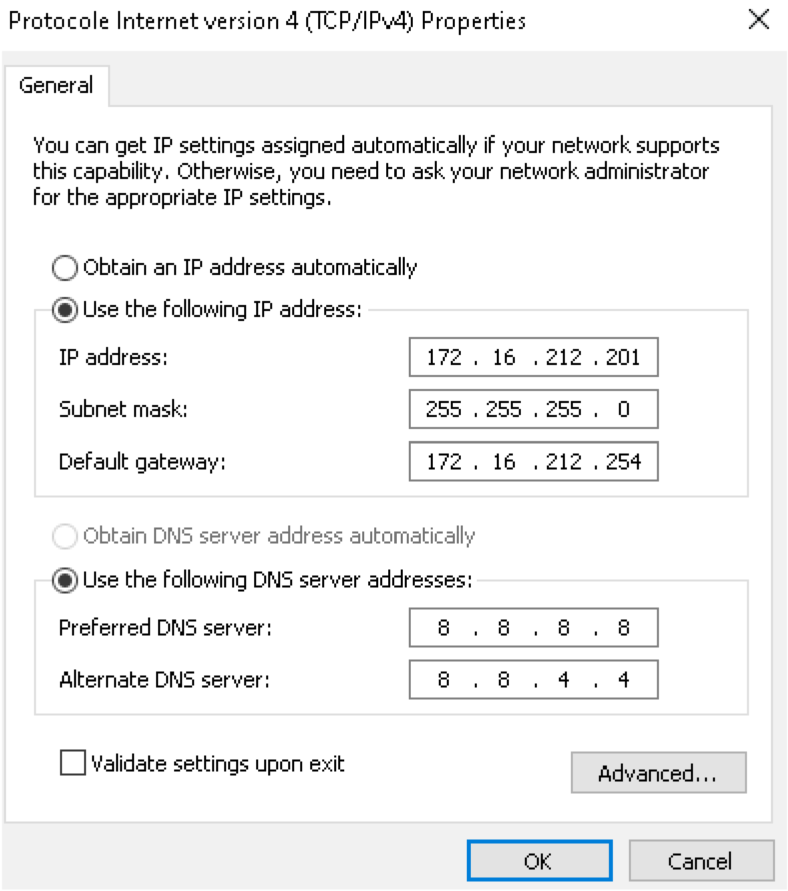
ACTIVATION

This is the current policy.
In order to apply these changes immediately, you must reactivate the policy.
Activate the new policy *Custom Filter* now?

CHECKING THE POLICY

The active policy is not up to date. It is recommended to activate the policy.

Then reconfigure your IPv4 settings to add DNS servers for domain name resolution (here we'll use Google's):



Protocole Internet 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 . 212 . 201

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 172 . 16 . 212 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

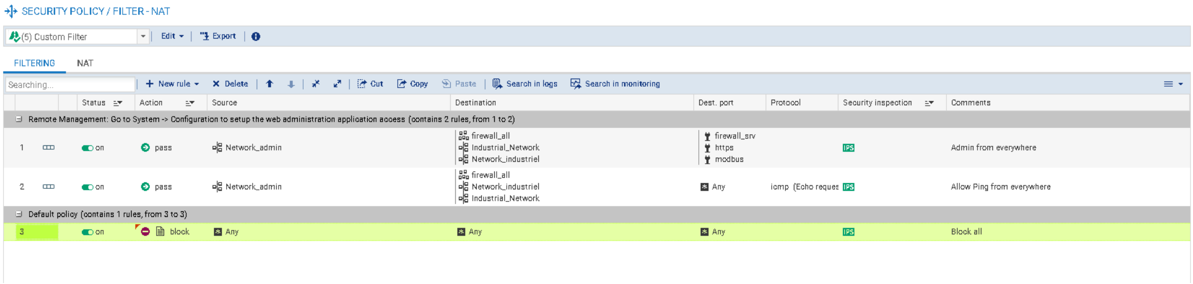
Alternate DNS server: 8 . 8 . 4 . 4

□ Validate settings upon exit

Then try to access a web page such as https://schneider-electric.com/ to check that the Internet access is working.

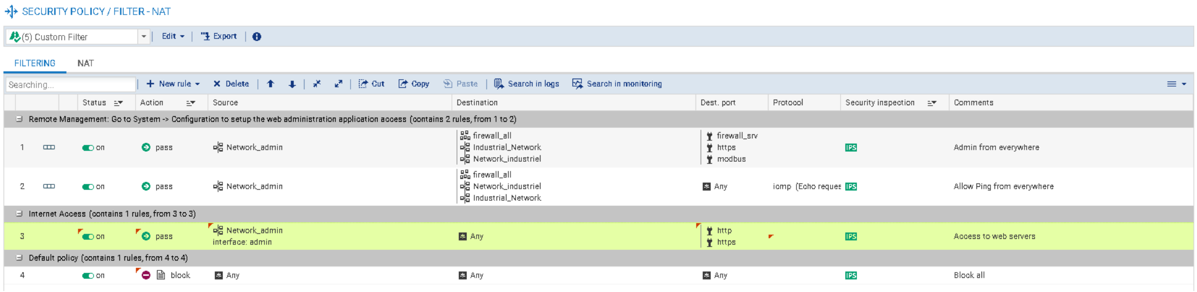
2. Setting a filter for Internet access

Start by restoring the default rule of blocking all connections:



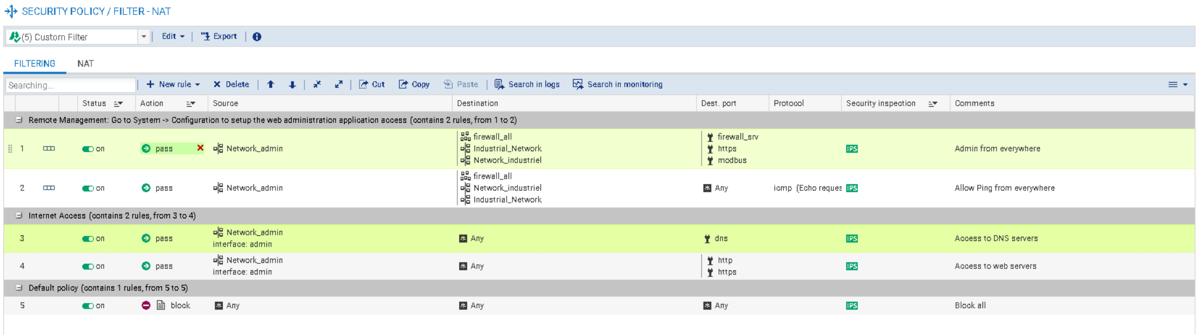
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Remote Management: Go to System -> Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)								
1	on	pass	Network_admin	firewall_all Industrial_Network Network_industriel	firewall_srv https modbus		IPS	Admin from everywhere
2	on	pass	Network_admin	firewall_all Network_industriel Industrial_Network	Any	icmp (Echo reques	IPS	Allow Ping from everywhere
Default policy (contains 1 rules, from 3 to 3)								
3	on	block	Any	Any	Any		IPS	Block all

Create a new rule allowing the network administrator to access the web servers :



	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
⊟ Remote Management: Go to System -> Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)								
1	on	pass	Network_admin	firewall_all Industrial_Network Network_industriel	firewall_srv https modbus		IPS	Admin from everywhere
2	on	pass	Network_admin	firewall_all Network_industriel Industrial_Network	Any	icmp (Echo reques	IPS	Allow Ping from everywhere
⊟ Internet Access (contains 1 rules, from 3 to 3)								
3	on	pass	Network_admin interface: admin	Any	http https		IPS	Access to web servers
⊟ Default policy (contains 1 rules, from 4 to 4)								
4	on	block	Any	Any	Any		IPS	Block all

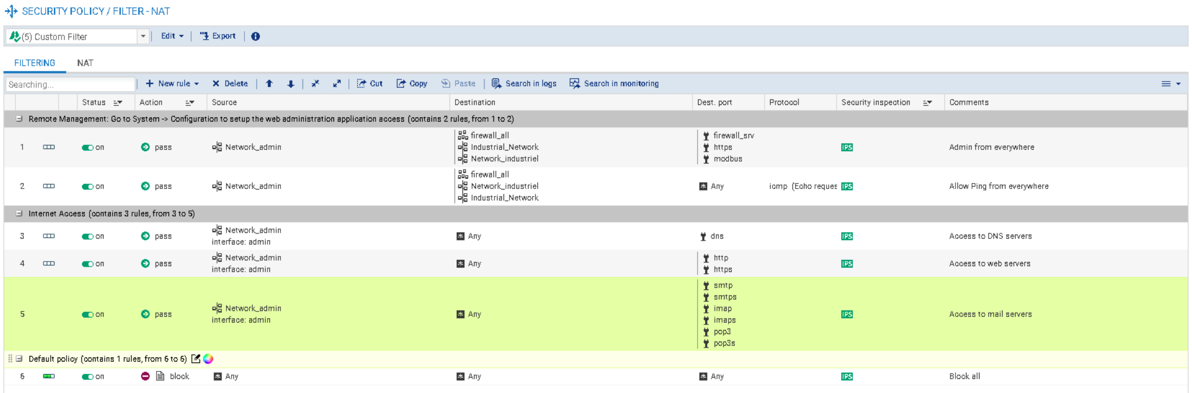
At this stage, it will still not be possible to access a website such as https://schneider-electric.com/, to do this it is necessary to allow access to DNS requests:



	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
⊟ Remote Management: Go to System -> Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)								
1	on	pass	Network_admin	firewall_all Industrial_Network Network_industriel	firewall_srv https modbus		IPS	Admin from everywhere
2	on	pass	Network_admin	firewall_all Network_industriel Industrial_Network	Any	icmp (Echo reques	IPS	Allow Ping from everywhere
⊟ Internet Access (contains 2 rules, from 3 to 4)								
3	on	pass	Network_admin interface: admin	Any	dns		IPS	Access to DNS servers
4	on	pass	Network_admin interface: admin	Any	http https		IPS	Access to web servers
⊟ Default policy (contains 1 rules, from 5 to 5)								
5	on	block	Any	Any	Any		IPS	Block all

Now check the accessibility of https://schneider-electric.com/.

Add a rule to allow Internet traffic using standard email protocols:



	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
⊟ Remote Management: Go to System -> Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)								
1	on	pass	Network_admin	firewall_all Industrial_Network Network_industriel	firewall_srv https modbus		IPS	Admin from everywhere
2	on	pass	Network_admin	firewall_all Network_industriel Industrial_Network	Any	icmp (Echo reques	IPS	Allow Ping from everywhere
⊟ Internet Access (contains 3 rules, from 3 to 5)								
3	on	pass	Network_admin interface: admin	Any	dns		IPS	Access to DNS servers
4	on	pass	Network_admin interface: admin	Any	http https		IPS	Access to web servers
5	on	pass	Network_admin interface: admin	Any	smtp smtps imap imaps pop3 pop3s		IPS	Access to mail servers
⊟ Default policy (contains 1 rules, from 6 to 6)								
6	on	block	Any	Any	Any		IPS	Block all

N.B.: It should be noted that all these protocols are not mandatory. To further improve security, only the protocols that are actually used can be kept, depending on the mail servers from which you wish to retrieve the mails.