STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

IDENTIFYING INDUSTRIAL PROTOCOL COMMANDS GOING THROUGH THE FIREWALL

Product concerned: SNS 3.x, SNS 4.x

Document last updated: December 9, 2019

Reference: sns-en-identifying_industrial_protocol_commands_technical_note

Table of contents

Introduction 3
Requirements 3
Creating a customized inspection profile 4
Selecting the Modbus protocol profile 4
Prohibiting all public Modbus operations 4
Customizing the application inspection profile 5
Modifying the action of the "Function code denied" alarm 6
Creating a filter rule using the customized inspection profile 7
Viewing generated alarms 9
Viewing alarms in the dashboard 9
Viewing alarms in the log and activity report application 9
Building a customized security policy 10
Selecting the protocol inspection profile 10
Using this profile in the application inspection profile 10
Modifying the action of the "Function code denied" alarm 11
Modifying the filter rule dedicated to the industrial protocol 12
Further reading 13

Introduction

Most of the time, industrial protocols are designed for a functional purpose, without necessarily taking into account security aspects.

In general, they allow client machines to request actions from PLCs (Programmable Logic Controllers), expecting such actions to be run in return. Client workstations may as such ask a PLC to write data in memory or simply order it to shut down.

Such requests for action are defined in a particular field of the protocol called the "function code". As industrial protocols do not include any security mechanisms such as the verification of the message sender's identity, any machine on the network would then be able to request actions from the PLC.

The aim of this document is to set out a method that would allow identifying a protocol's various function codes exchanged over the corporate industrial network. After this capture, the administrator would be able to build up a security policy adapted to the function codes to be allowed or prohibited for each machine found on the network.

Therefore, suspicious machines located on the network would not be able to send messages to the PLC as the Stormshield Network Firewall would filter them.

Requirements

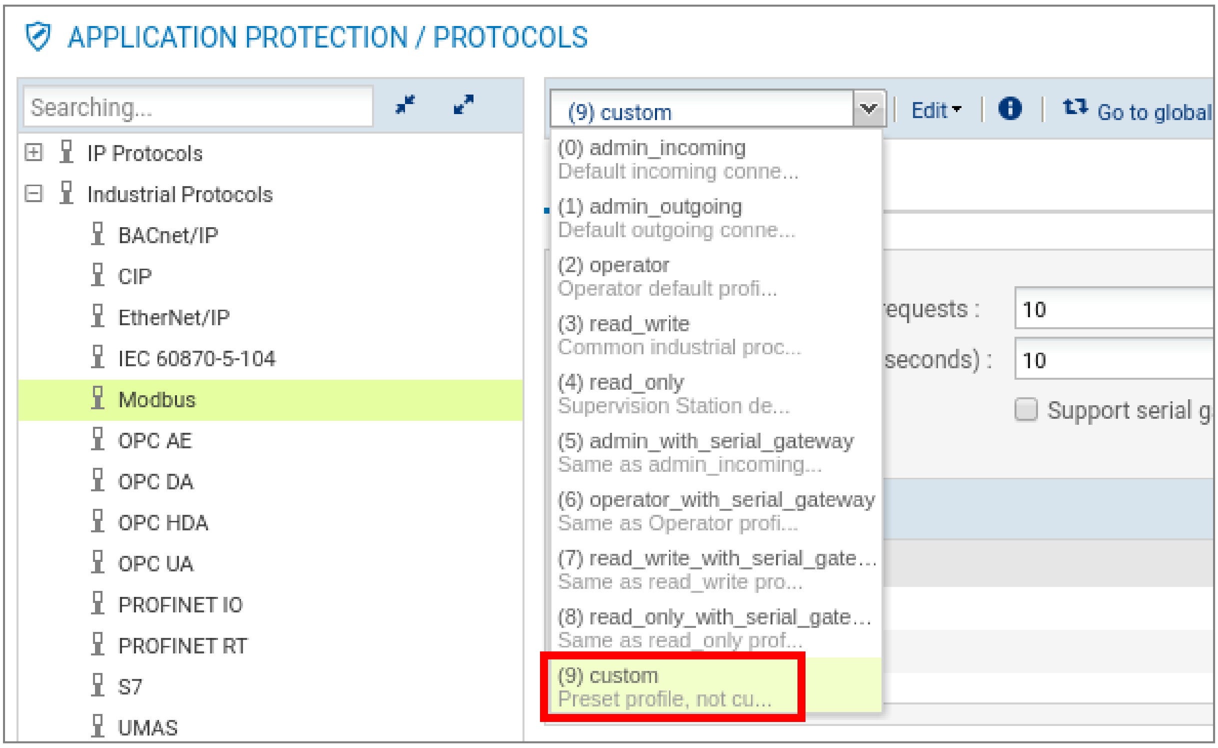
SNS firewall in version 2.3.4 or higher.

Creating a customized inspection profile

Create a customized inspection profile for the selected industrial protocol (Modbus in the example). In this profile, all function codes will be configured to generate an alarm allowing the identification of codes going through the network. This inspection profile will then be used in the filter policy.

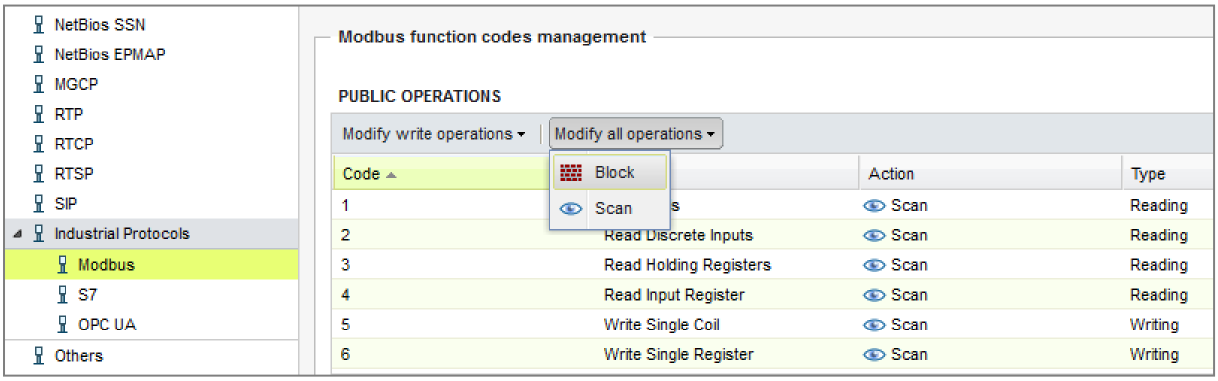
Selecting the Modbus protocol profile

1. In the **Configuration** > **Application protection** > **Protocols** menu, select the Modbus protocol (*Industrial protocols* section):
2. Select the protocol profile **(9) custom**:


APPLICATION PROTECTION / PROTOCOLS
Searching...
IP Protocols
Industrial Protocols
BACnet/IP
CIP
EtherNet/IP
IEC 60870-5-104
Modbus
OPC AE
OPC DA
OPC HDA
OPC UA
PROFINET IO
PROFINET RT
S7
UMAS
(9) custom
Edit
Go to global
(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_gateway
Same as admin_incoming...
(6) operator_with_serial_gateway
Same as Operator profi...
(7) read_write_with_serial_gate...
Same as read_write pro...
(8) read_only_with_serial_gate...
Same as read_only prof...
(9) custom
Preset profile, not cu...
equests : 10
seconds) : 10
Support serial g

Prohibiting all public Modbus operations

1. In the table lusting all public Modbus operations, browse the menu **Modify all operations**, and select **Block**. This action would result in an alarm being raised every time a Modbus function code is detected:

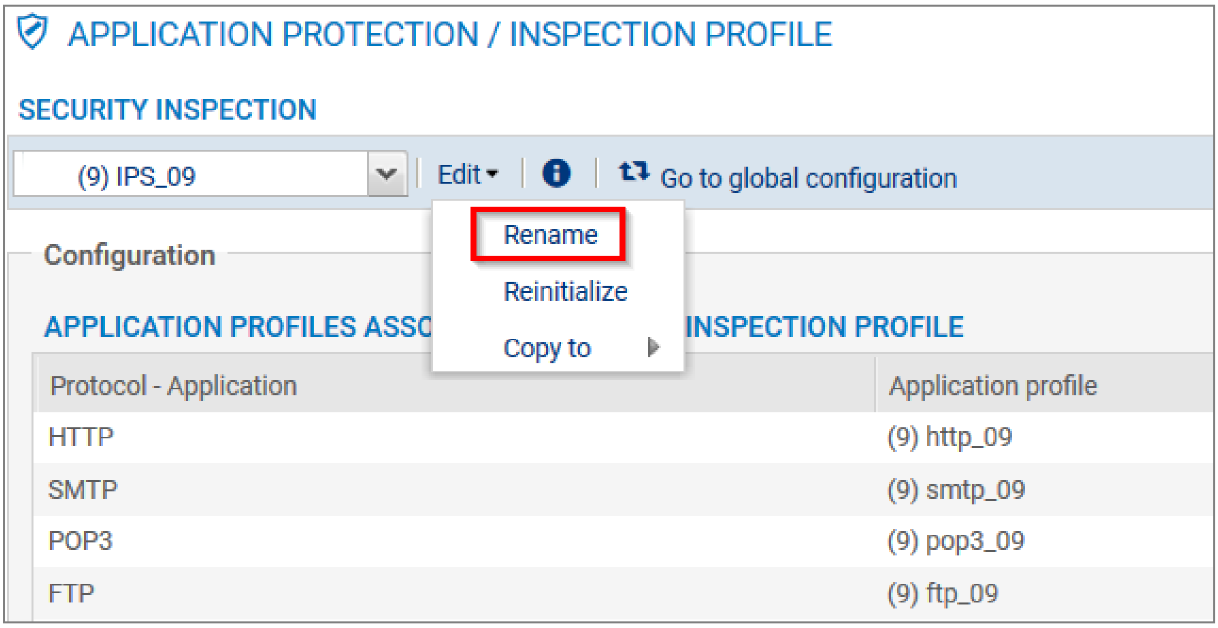


Code ▲		Action	Type
1	s	Scan	Reading
2	Read Discrete Inputs	Scan	Reading
3	Read Holding Registers	Scan	Reading
4	Read Input Register	Scan	Reading
5	Write Single Coil	Scan	Writing
6	Write Single Register	Scan	Writing

2. Confirm by clicking on **Apply**.

Customizing the application inspection profile

1. In the **Configuration** > **Application protection** > **Inspection profile** menu, click on **Go to profiles**.
2. Select the profile **(9) IPS_09** (by default, this inspection profile will use no. 9 protocol profiles):
3. Expand the **Edit** menu and select **Rename** in order to customize the name of this inspection profile:

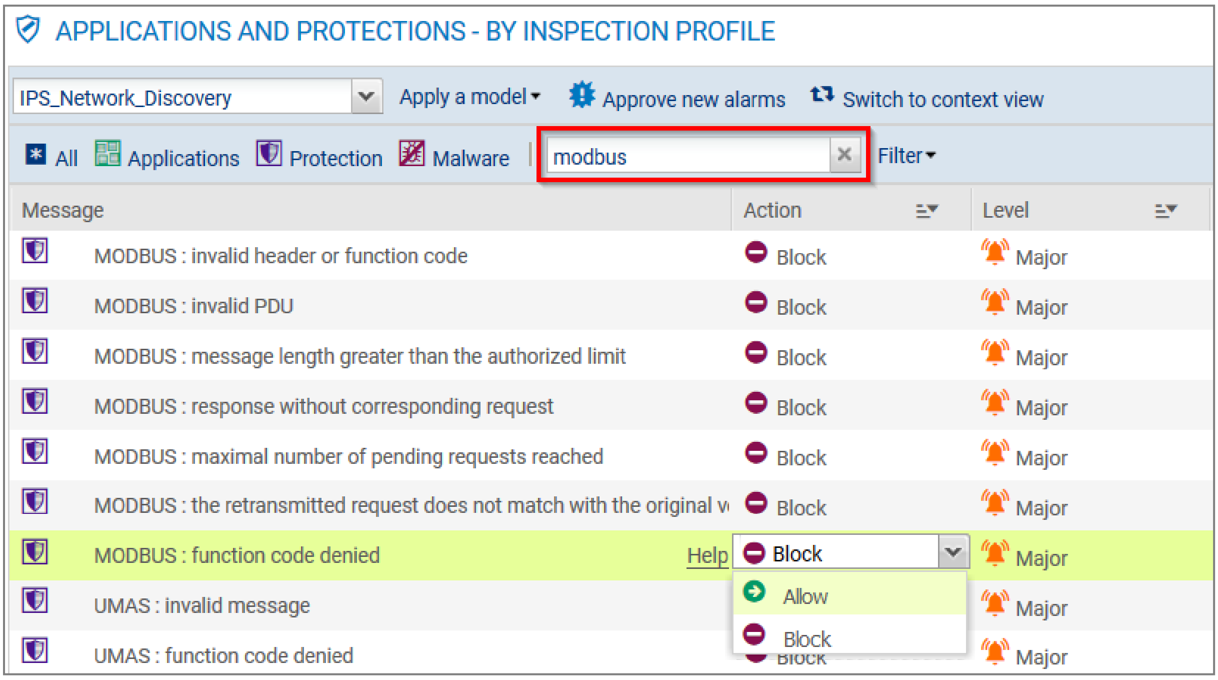

APPLICATION PROTECTION / INSPECTION PROFILE
SECURITY INSPECTION
(9) IPS_09
Edit ▾
Go to global configuration
Rename
Reinitialize
Copy to
Configuration
APPLICATION PROFILES ASSO
INSPECTION PROFILE

Protocol - Application	Application profile
HTTP	(9) http_09
SMTP	(9) smtp_09
POP3	(9) pop3_09
FTP	(9) ftp_09

4. Choose a representative name (*IPS_Network_Discovery* in the example) and confirm the change by clicking on **Update**.

Modifying the action of the "Function code denied" alarm

1. In the **Configuration** > **Application protection** > **Applications and protections** menu, select the customized inspection profile created earlier:
2. Enter the name of the industrial protocol to be filtered in the search field. All alarms relating to this protocol will appear:
3. Locate the "function code denied" alarm and modify its action by double-clicking on *Block*. Select *Allow*:
4. Confirm the change by clicking on **Apply**.



APPLICATIONS AND PROTECTIONS - BY INSPECTION PROFILE

IPS_Network_Discovery | Apply a model | Approve new alarms | Switch to context view

All | Applications | Protection | Malware | modbus | Filter

Message	Action	Level
MODBUS : invalid header or function code	Block	Major
MODBUS : invalid PDU	Block	Major
MODBUS : message length greater than the authorized limit	Block	Major
MODBUS : response without corresponding request	Block	Major
MODBUS : maximal number of pending requests reached	Block	Major
MODBUS : the retransmitted request does not match with the original v	Block	Major
MODBUS : function code denied Help	Block Allow Block	Major
UMAS : invalid message		Major
UMAS : function code denied	Block	Major

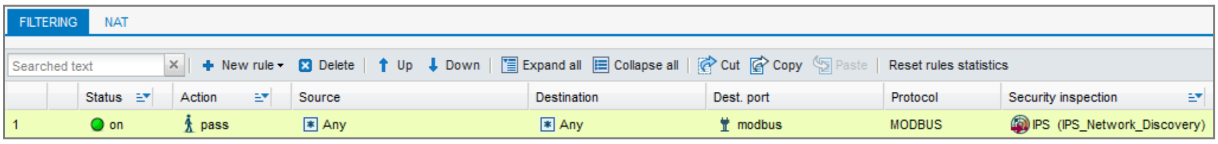
Creating a filter rule using the customized inspection profile

The aim of this rule is to allow all function codes from the selected industrial protocol (Modbus in this document) while systematicaly generating an alarm in order to identify them in the firewall's logs.

> **NOTE**
> While this rule is temporary, it needs to be placed at the top of the active filter policy.

1. In the **Configuration** > **Security policy** > **Filter - NAT** menu, select the active filter slot (slot (9) Filter 09 in the example), then click on **New rule** and select **Simple rule.**
2. In the Status column, double-click on **Off** to enable the rule (the status of the rule becomes **On**).
3. In the **Action** column, double-click on *block* then select the value *pass* for the **Action** field:
4. In the **Port - Protocol** section located to the left of the rule editing window, assign the following values to the various fields:
    - **Destination port**: modbus
    - **Protocol type**: Application protocol,
    - **Application protocol**: modbus
5. In the **Inspection** section, select the inspection profile that was renamed earlier (*(9)IPS_Network_Discovery* in the example):
6. Confirm the changes by clicking on **OK**.

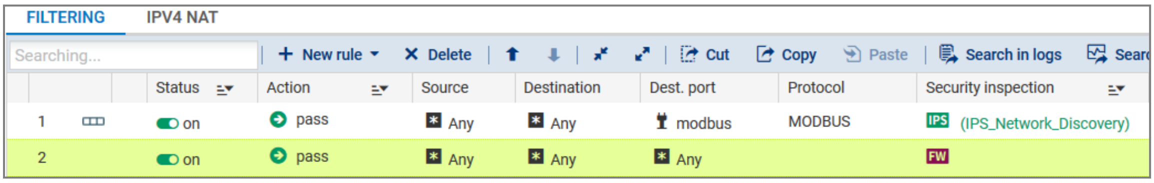
The filter rule will then look like this:



	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	● on	pass	Any	Any	modbus	MODBUS	IPS (IPS_Network_Discovery)

> **IMPORTANT**
> If none of the security policies were enabled on the firewall, a second filter rule must be created to ensure that no traffic outside the Modbus protocol is blocked. This rule will be the last in the filter slot and will have the following values:
>
> - **Status**: On,
> - **Action**: pass,
> - **Source**: Any,
> - **Destination**: Any,
> - **Destination port**: Any,
> - **Protocol**: leave the field blank,
> - **Security inspection**: select the *Firewall* mode.

The filter policy will then become:



		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	Any	Any	modbus	MODBUS	IPS (IPS_Network_Discovery)
2		on	pass	Any	Any	Any		FW

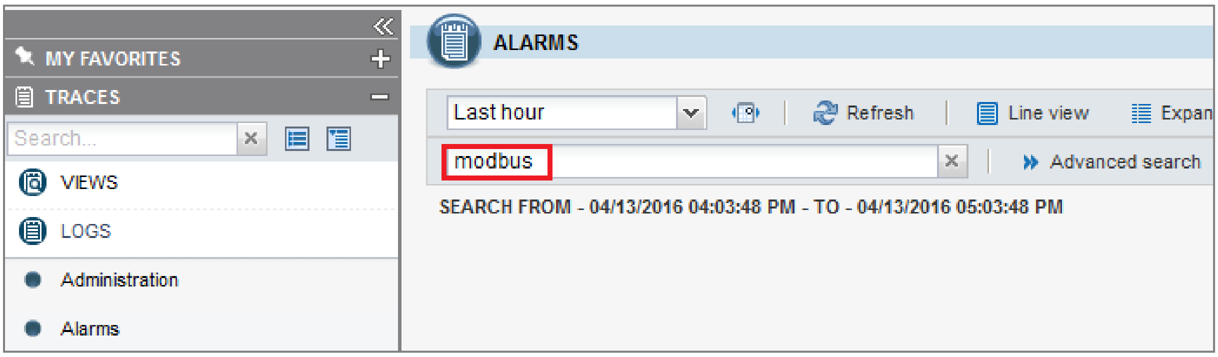
7. Enable the filter policy by clicking on **Save and apply**.

Viewing generated alarms

Viewing alarms in the dashboard

In the **Dashboard** menu, the **Protection** window will display in real time alarms that were raised when network packets from the industrial protocol go through the firewall.

Viewing alarms in the log and activity report application



Last hour

modbus

SEARCH FROM - 04/13/2016 04:03:48 PM - TO - 04/13/2016 05:03:48 PM

Building a customized security policy

After having highlighted the function codes of the industrial protocol circulating on your network, you will now be able to implement an adapted security policy. The various steps that you need to follow are:

1. Choose a predefined protocol inspection profile or build a customized profile for the industrial protocol being considered.
2. Associate this protocol profile with an application inspection profile.
3. Modify the action associated with the "*function code denied*" alert to make it block such traffic.
4. Modify the filter rule dedicated to the industrial protocol in order to call up this application inspection profile.

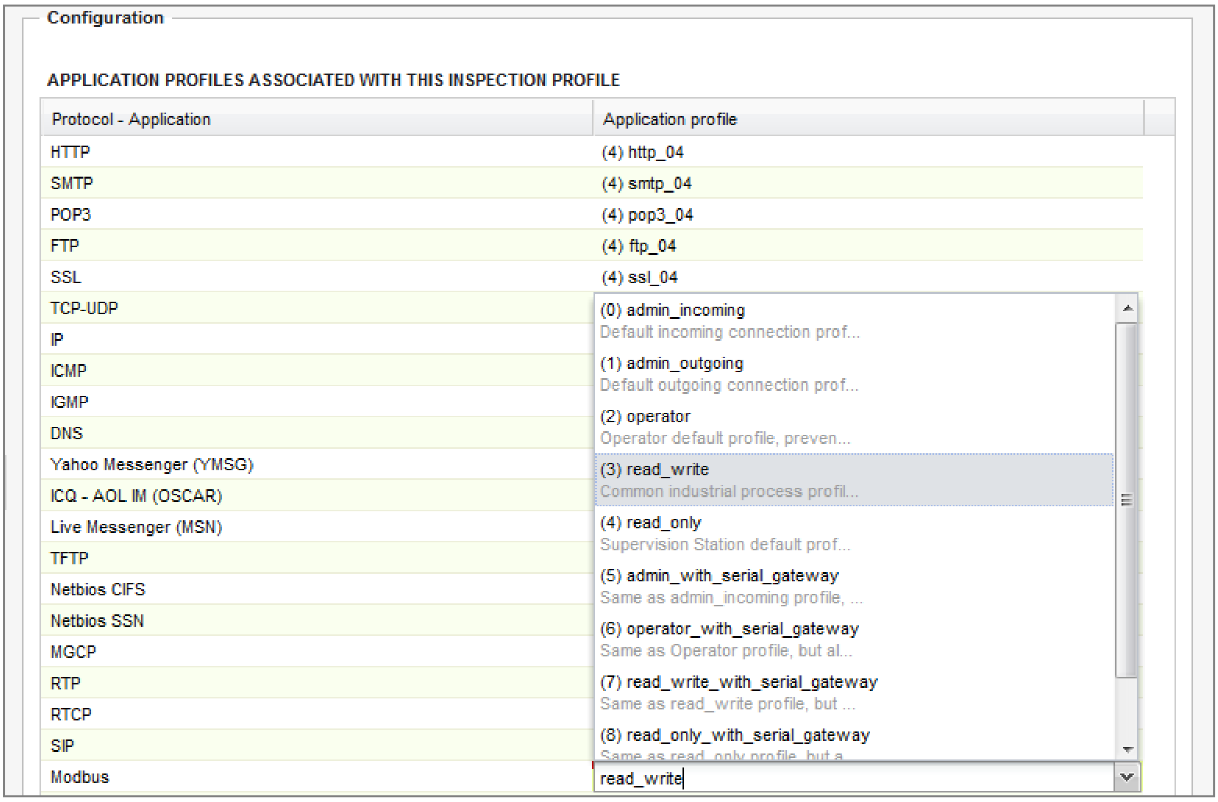
Selecting the protocol inspection profile

1. In the **Configuration** > **Application protection** > **Protocols** menu, click on **Industrial protocols**, then click on the industrial protocol to be configured (*Modbus* in the example). The menu for selecting protocol profiles offers 9 predefined profiles (numbered from 0 to 8) and a customized profile (9),
2. By clicking on each of these profiles, view the prohibited or allowed public operations and locate the profile corresponding to the configuration you wish to set up.
3. If none of the predefined profiles meet your needs, choose profile "(9)" which will be used during the analysis. Select the action *Scan* for each public operation to allow. Click on **Apply**.

Using this profile in the application inspection profile

1. In the **Configuration** > **Application protection** > **Inspection profiles** menu, click on **Go to profiles**.
2. For a more legible configuration, select the IPS profile bearing the same number as the selected protocol profile. For example, if you have chosen to apply the protocol profile titled "Read_write" (profil no. 3) for the industrial protocol being considered (Modbus in the example), select the IPS profile named "(3) IPS_03" which will apply this protocol profile by default.

NOTE
If this profile is unavailable, select an unused IPS profile, then double-click on the application profile applied by default for the industrial protocol and select the profile to use:



Configuration

APPLICATION PROFILES ASSOCIATED WITH THIS INSPECTION PROFILE

Protocol - Application	Application profile
HTTP	(4) http_04
SMTP	(4) smtp_04
POP3	(4) pop3_04
FTP	(4) ftp_04
SSL	(4) ssl_04
TCP-UDP	
IP	
ICMP	
IGMP	
DNS	
Yahoo Messenger (YMSG)	
ICQ - AOL IM (OSCAR)	
Live Messenger (MSN)	
TFTP	
Netbios CIFS	
Netbios SSN	
MGCP	
RTP	
RTCP	
SIP	
Modbus	read_write

(0) admin_incoming
Default incoming connection prof...
(1) admin_outgoing
Default outgoing connection prof...
(2) operator
Operator default profile, preven...
(3) read_write
Common industrial process profil...
(4) read_only
Supervision Station default prof...
(5) admin_with_serial_gateway
Same as admin_incoming profile, ...
(6) operator_with_serial_gateway
Same as Operator profile, but al...
(7) read_write_with_serial_gateway
Same as read_write profile, but ...
(8) read_only_with_serial_gateway
Same as read_only profile, but a

3. You can rename this profile in order to give it a more representative name (**Edit** > **Rename** menu). **Example**: "*IPS_Modbus_Protocol*".

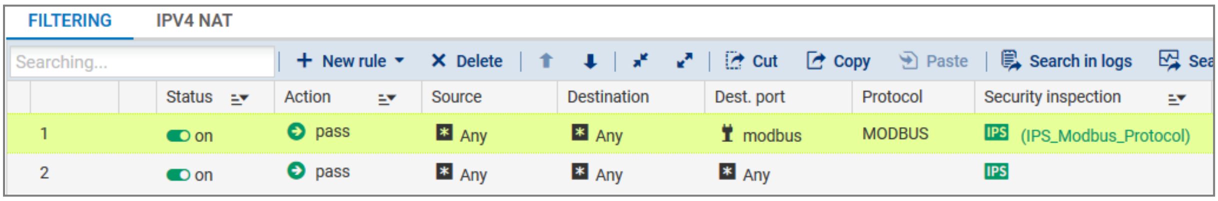
Modifying the action of the "Function code denied" alarm

1. In the **Configuration** > **Application protection** > **Applications and protections** menu, select the customized inspection profile used in the filter rule (*IPS_Modbus_Protocol* in the example).
2. Enter the name of the industrial protocol to be filtered in the search field. All alarms relating to this protocol will appear.
3. Locate the "function code denied" alarm and modify its action by double-clicking on *Allow*. Select *Block*.
4. Click on **Apply**.

Modifying the filter rule dedicated to the industrial protocol

1. In the **Configuration** > **Security policy** > **Filter - NAT** menu, select the filter rule created to discover industrial traffic going through the network.
2. Double-click on the inspection profile (*Security inspection* column) and choose the profile selected for the industrial protocol analysis (*IPS_Modbus_Protocol* in the example).
3. Click on **Save and apply**.

The filter rule will then look like this:



		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	Any	Any	modbus	MODBUS	IPS (IPS_Modbus_Protocol)
2		on	pass	Any	Any	Any		IPS

Further reading

Additional information and responses to questions you may have are available in the **Stormshield knowledge base** (authentication required).

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.