

# Configuration Editor - user manual

version 0.2.0 - 13 December 2013



<http://www.posecco.eu>

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>GUI</b>	<b>3</b>
	Filtering View . . . . .	3
	Data Protection View . . . . .	4
	Insert a new rule . . . . .	4
	New Filtering Rule . . . . .	4
	New IPsec Rule . . . . .	5
	New WS-Security Rule . . . . .	5
	New SSH Rule . . . . .	5
	Delete a configuration rule . . . . .	5

## **1 Introduction**

The role of this document is to provide an overview on how to use the configuration editor. The configuration editor can be used to remove and insert rules for filtering and data protection configurations. Currently only filtering configurations (packet filters, stateful firewalls and application layer firewalls) together with data protection rules (IPsec, WS-Security and SSH) are supported.

## 2 GUI

The main GUI of the Configuration Editor is divided into two views, the filtering view and the data protection view.

### Filtering View

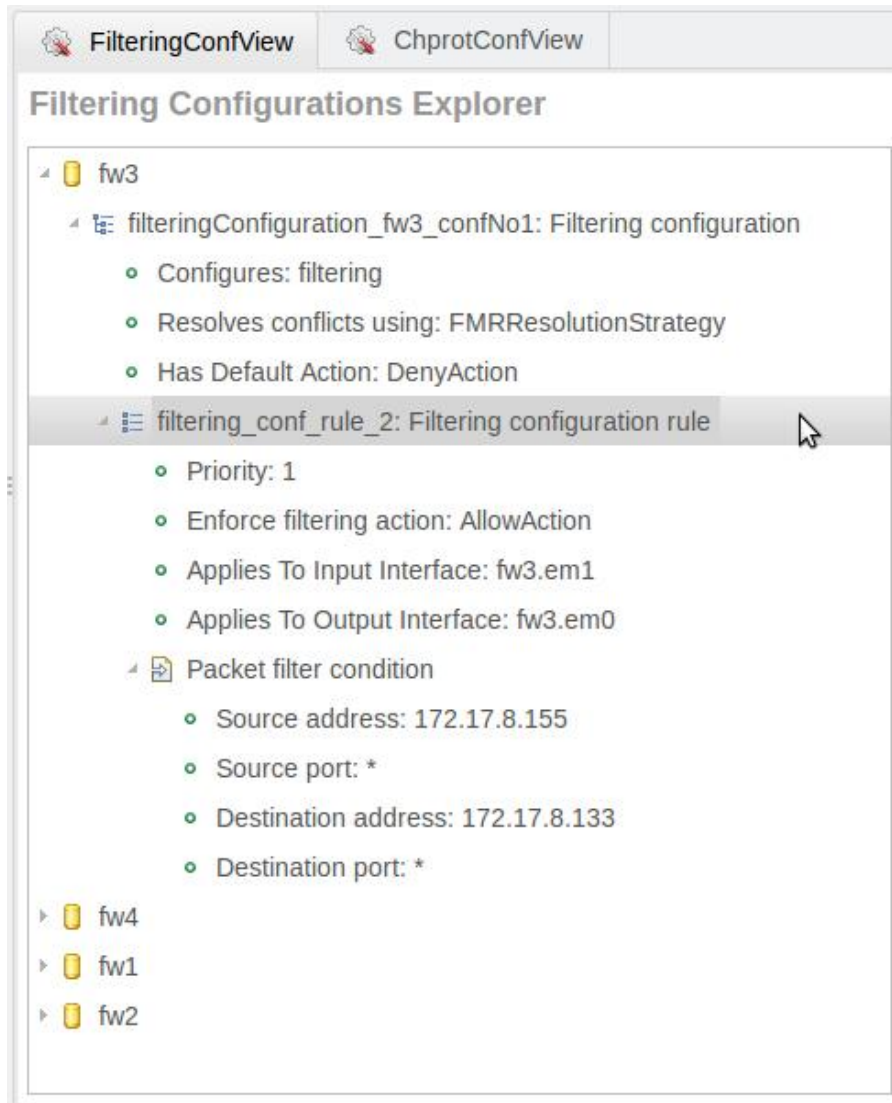


Figure 1: Filtering View

The filtering view Fig. 1 contains all filtering configurations, the view is structured as a tree in the following way:

- the first level contains the set of configured devices (e.g., fw1);
- the second level contains the set of Filtering Configurations (typically one for each firewall);
- the third level defines the configuration properties and the related rules. For example the Fig. 1 shows that we configure filtering capability on fw1.OS using a First Matching Rule strategy and a Deny All as default action.
- the fourth level defines the properties of a configuration rule. For example the Fig. 1 shows: the priority, the action (allow, deny), the input and output interfaces and the related packet filter conditions (source and destination IP address, direction, etc.).

## Data Protection View

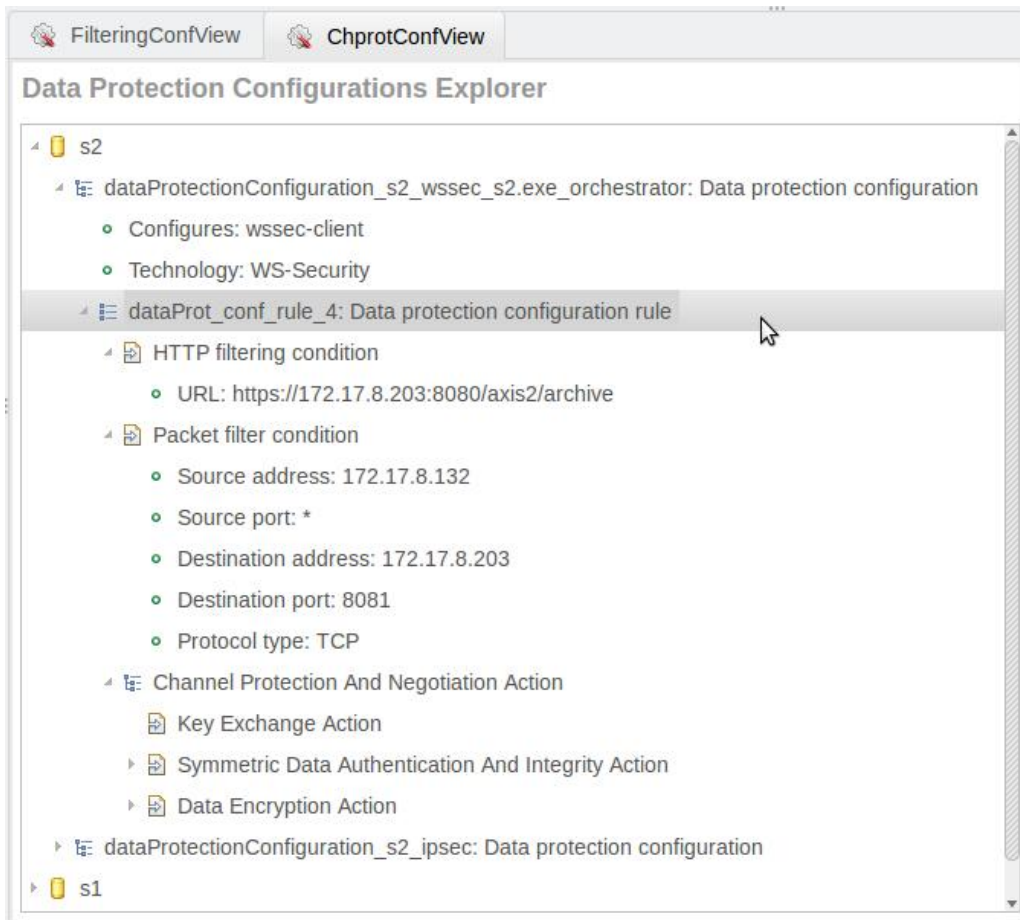


Figure 2: Data Protection View

The data protection view Fig. 2 contains all filtering configurations, the view is structured as a tree in the following way:

- the first level contains the set of configured devices (e.g., s1);
- the second level contains the set of Data Protection Configurations;
- the third level defines the configuration properties and the related rules. For example the Fig. 2 shows that we configure IPsec (end-to-end mode) on s1.os using a First Matching Rule strategy.
- the fourth level defines the properties of a configuration rule. For example the Fig. 2 shows the related packet filter conditions (source and destination IP address, direction, etc.).

### Insert a new rule

To insert a new rule in a configuration, the users performs a right click on the configuration to which he wants to add a new rule and than clicks on the appearing menu.

### New Filtering Rule

After clicking the “Add Rule” a wizard page open (see Fig. 3) where the user can insert all the properties of the new filtering rule.

**New Filtering Rule**

Priority: 1

Filtering Action: AllowAction

Input Interface: \*

Output Interface: \*

PacketFilterCondition

Source Address: 1.1.1.1

Source Port: 1

Destination address: 2.2.2.2

Destination Port: 2

Protocol Type: \*

Direction: \*

HTTPFilteringCondition

URL: www.posecco.eu

Method: GET

Finish Cancel

Figure 3: New Filtering Rule Wizard

### New IPsec Rule

After clicking the “Add Rule” a wizard page open (see Fig. 4) where the user can insert all the properties of the new IPsec rule.

### New WS-Security Rule

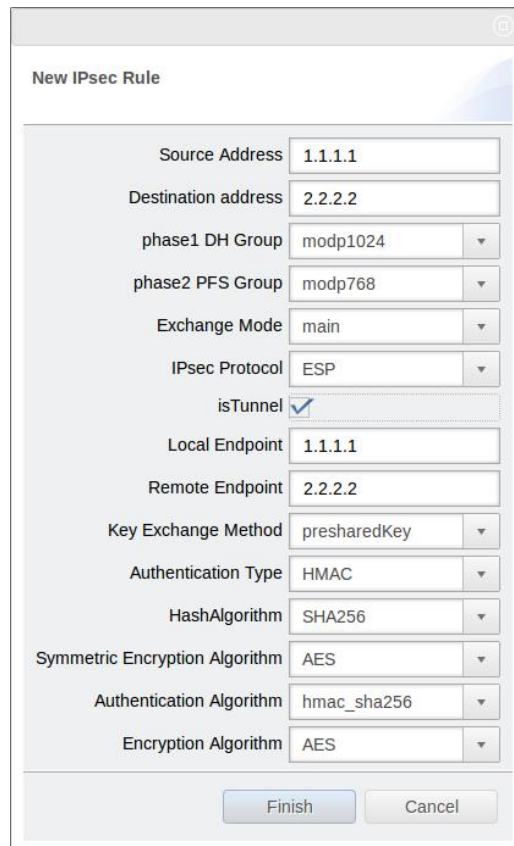
After clicking the “Add Rule” a wizard page open (see Fig. 6) where the user can insert all the properties of the new WS-Security rule.

### New SSH Rule

After clicking the “Add Rule” a wizard page open (see Fig. ??) where the user can insert all the properties of the new SSH rule.

### Delete a configuration rule

To delete a configuration rule, the users performs a right click on the rule which he wants to delete and than clicks on the appearing menu “Remove Rule”.

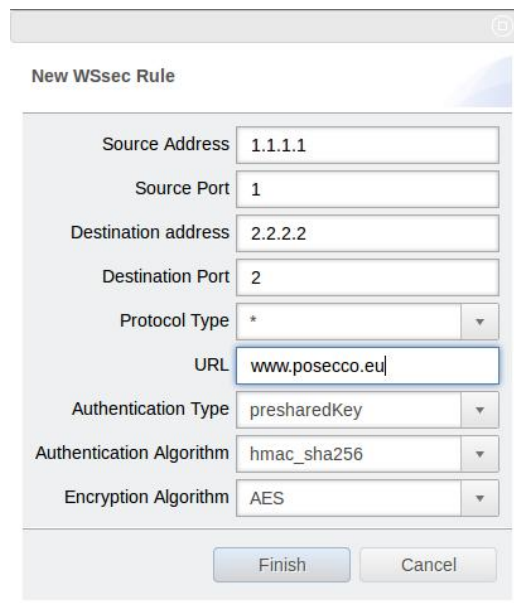


The 'New IPsec Rule' wizard window contains the following configuration fields:

Source Address	1.1.1.1
Destination address	2.2.2.2
phase1 DH Group	modp1024
phase2 PFS Group	modp768
Exchange Mode	main
IPsec Protocol	ESP
isTunnel	<input checked="" type="checkbox"/>
Local Endpoint	1.1.1.1
Remote Endpoint	2.2.2.2
Key Exchange Method	presharedKey
Authentication Type	HMAC
HashAlgorithm	SHA256
Symmetric Encryption Algorithm	AES
Authentication Algorithm	hmac_sha256
Encryption Algorithm	AES

Buttons: Finish, Cancel

Figure 4: New IPsec Rule Wizard

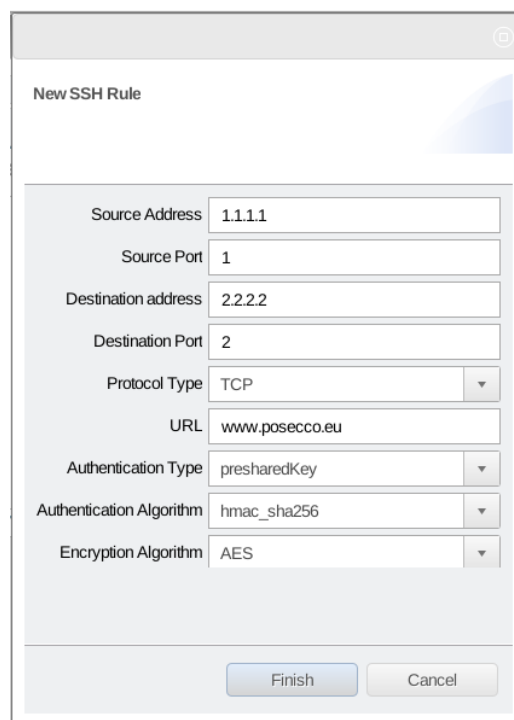


The 'New WSsec Rule' wizard window contains the following configuration fields:

Source Address	1.1.1.1
Source Port	1
Destination address	2.2.2.2
Destination Port	2
Protocol Type	*
URL	www.posecco.eu
Authentication Type	presharedKey
Authentication Algorithm	hmac_sha256
Encryption Algorithm	AES

Buttons: Finish, Cancel

Figure 5: New WS-Security Rule Wizard



The image shows a 'New SSH Rule' wizard dialog box. It contains several input fields and dropdown menus for configuring an SSH rule. The fields are: Source Address (1.1.1.1), Source Port (1), Destination address (2.2.2.2), Destination Port (2), Protocol Type (TCP), URL (www.posecco.eu), Authentication Type (presharedKey), Authentication Algorithm (hmac\_sha256), and Encryption Algorithm (AES). At the bottom, there are 'Finish' and 'Cancel' buttons.

Source Address	1.1.1.1
Source Port	1
Destination address	2.2.2.2
Destination Port	2
Protocol Type	TCP
URL	www.posecco.eu
Authentication Type	presharedKey
Authentication Algorithm	hmac_sha256
Encryption Algorithm	AES

Figure 6: New SSH Rule Wizard