Configuration Editor - user manual

version 0.2.0 - 13 December 2013

PoSecCo

http://www.posecco.eu

Contents

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

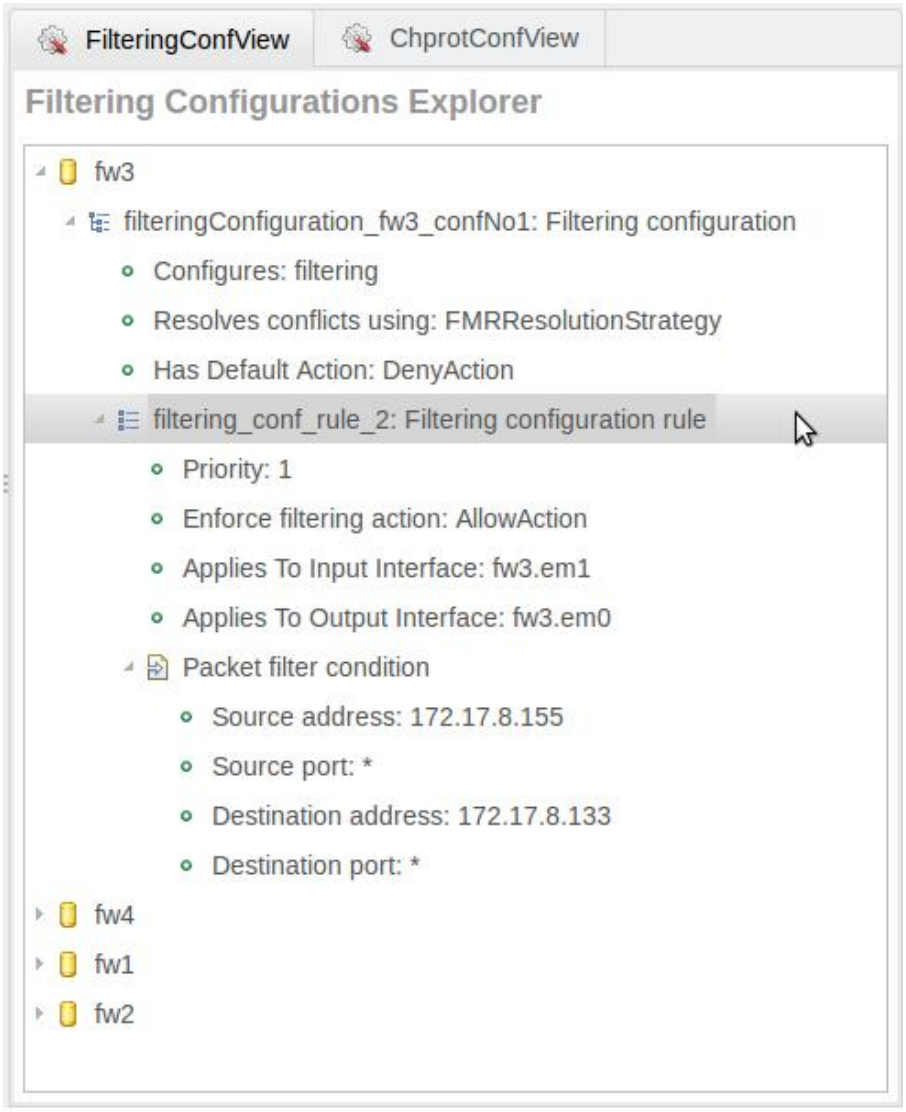

Figure 1: Filtering View

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

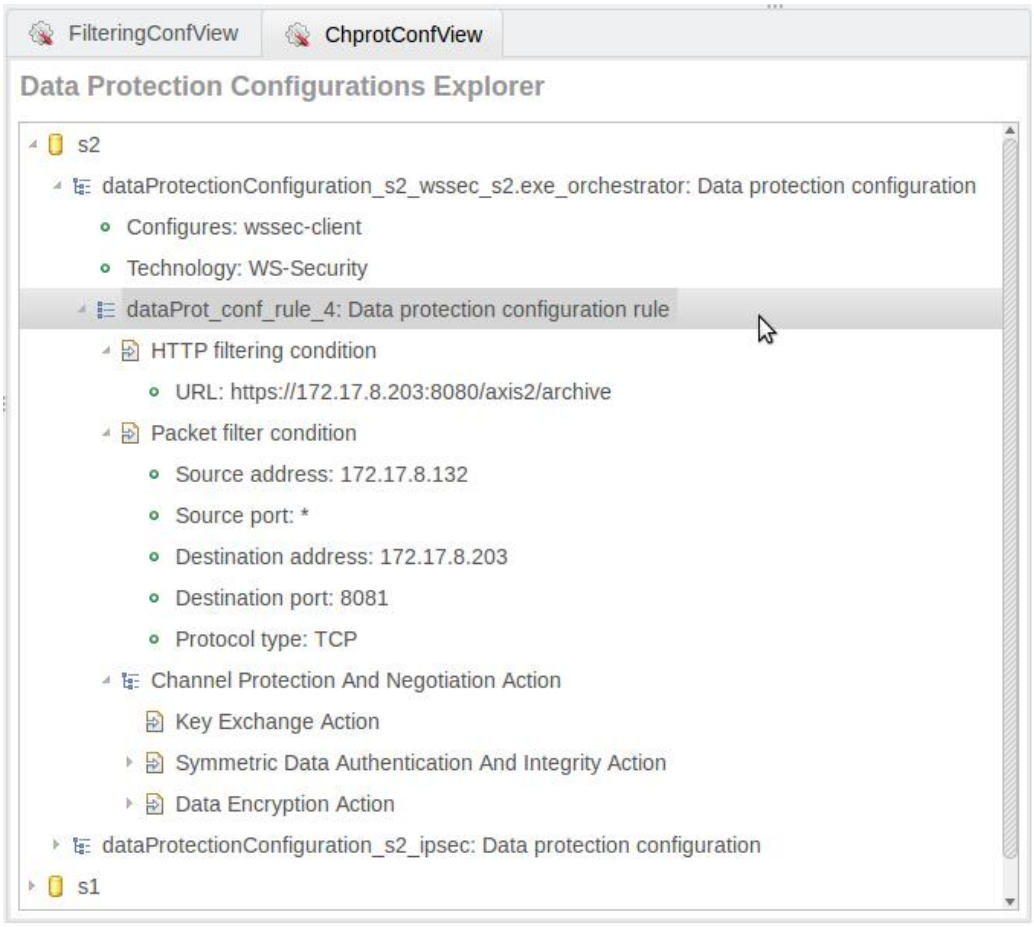

Figure 2: Data Protection View

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.

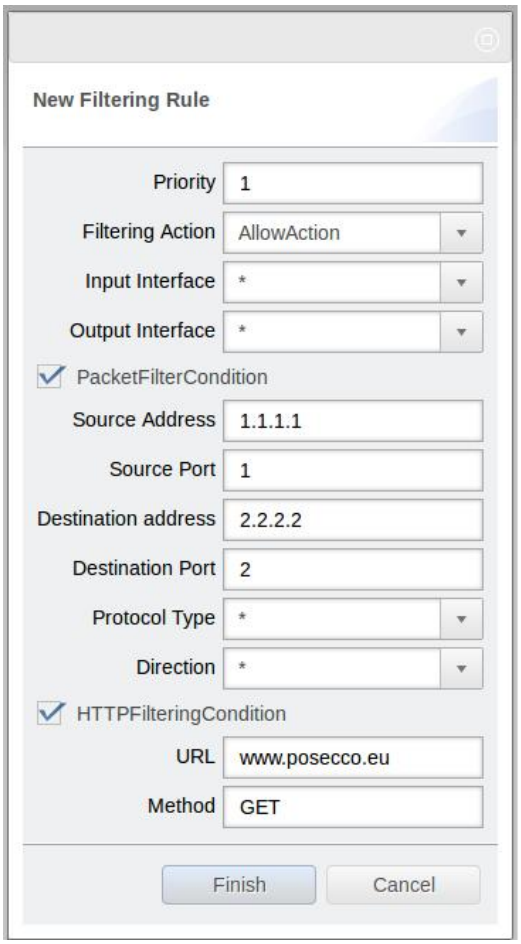

Figure 3: New Filtering Rule Wizard

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”.

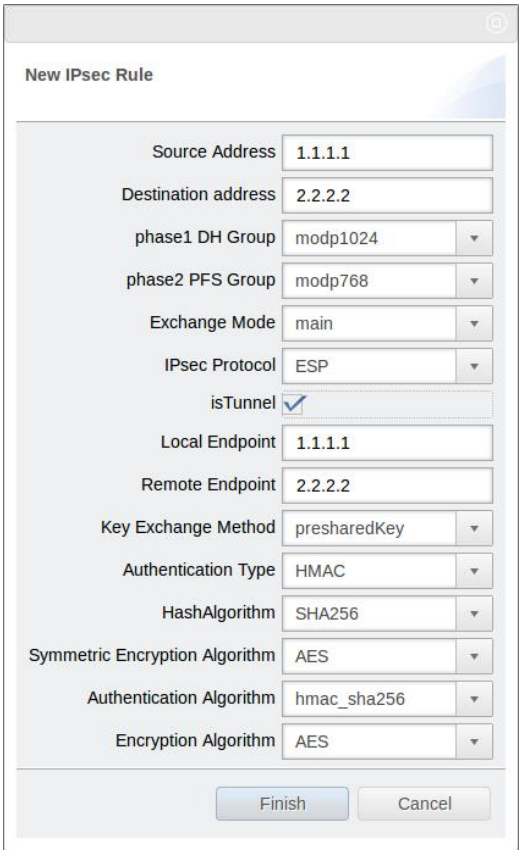

Figure 4: New IPsec Rule Wizard

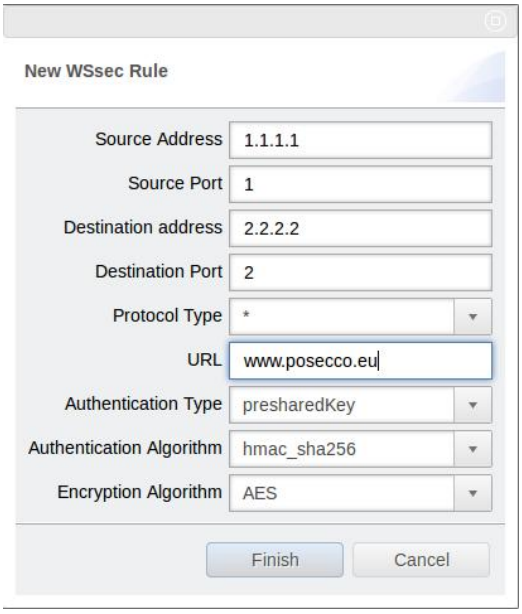

Figure 5: New WS-Security Rule Wizard

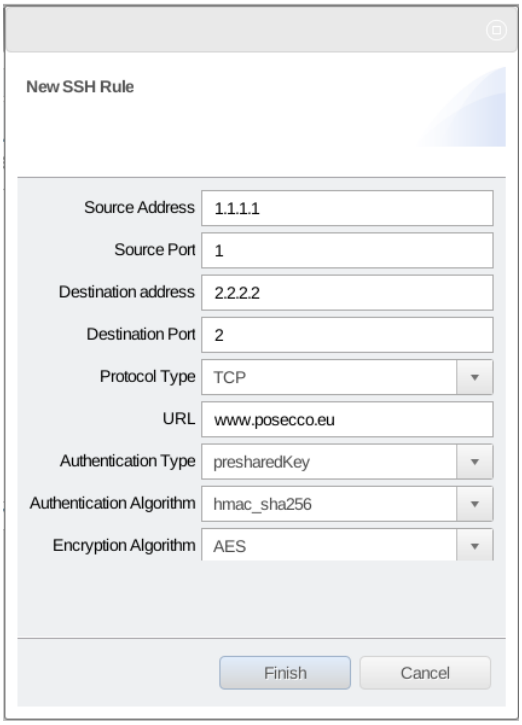

Figure 6: New SSH Rule Wizard