Fast Update Filters Overview

The dynamic firewall feature supports classic filters and fast update filters. Fast update filters support subscriber-specific filter values, as opposed to classic filters, which are interface-specific. Fast update filters allow individual filter terms, or rules, to be added or removed from filters without requiring that you recompile the filter after each modification—terms are added and removed when subscriber services are added and removed.

Using the fast update filters feature involves three distinct operations:

1. Creating the filter—You define fast update filters under the [edit dynamic-profiles *profile-name* firewall family *family*] hierarchy. The dynamic-profiles stanza enables you to use dynamic variables to create subscriber-specific configurations for the filter's match terms. See Configuring Fast Update Filters.
2. Associating the filter to a dynamic profile—You use the [edit dynamic-profiles *profile-name* interface *interface-name* unit *unit-number* family *family* hierarchy to associate the filter to a dynamic profile. This is the same procedure used for classic filters. See Associating Fast Update Filters to Interfaces in a Dynamic Profile.
3. Attaching the filter to an interface—When a subscriber logs in, the dynamic profile instantiates the subscriber session and applies the properties of the profile, including the fast update filter, to the session interface. This is the same procedure used for classic filters. Also, similar to classic filters, the name of fast update filters can be provided in a user's RADIUS file.

When a dynamic profile instantiates a subscriber session and applies a fast update filter, the router verifies that the filter is not already present on the session interface. If the filter is not present, the router adds the filter. If the filter is already present on the interface, the router simply adds any new terms that are not in the existing filter. This procedure is reversed when subscriber sessions are deleted. Any terms that were added by a session are then removed when the session is deleted. The filter is deleted when the last subscriber session is deleted.

NOTE: You can optionally specify that a term can be added only once and cannot be modified. See Match Conditions and Actions in Fast Update Filters.

This overview covers:

Fast Update Filter Components

When creating a fast update filter, you define one or more terms that specify the filtering criteria and the action to take when a match occurs.

Each term consists of the following components:

- Match condition—Specifies values or fields that the packet must contain. You can match a maximum of five fields in a fast update filter. A match condition can contain a single value or range. This differs from classic filters, in which terms can have multiple values. However, you can use additional terms to specify multiple ranges. Fast Update Filter Match Conditions lists the supported match conditions for fast update filters. The order in which the terms appear in a fast update filter is not important, because the router examines the most specific term first. (Classic filters examine the terms in the order in which the terms are listed.)
- Action—Specifies what to do when a packet matches the match condition. If no action is specified for a term, the default action is to accept the packet. Fast Update Filter Actions and Action Modifiers lists the supported actions for fast update filters.

Terms that are added to the filter during session instantiation must have a unique set of match conditions. Two terms overlap, or conflict, if a packet can match both sets of conditions—as a result, there are two different actions for the packet. You can ensure that terms are unique by using the $junos-subscriber-ip-address variable as the source-address (for an input filter) or destination-address (for an output filter) in the from statement. You must then supply the source-address or destination-address condition, as appropriate, as the first condition in the match-order statement.

Related Topics

- Fast Update Filter Actions and Action Modifiers
- Fast Update Filter Match Conditions
- Avoiding Conflicts When Terms Are Matched

Fast Update Filter Processing

You must use the match-order statement to explicitly specify the order in which the router examines filter match conditions. Also, the router examines only those conditions that you include in the match-order statement. When a fast update filter contains multiple terms, the router compares a packet against the terms starting with the most specific condition first. When the packet first matches a condition, the router performs the action defined in the term to either permit or deny the packet, and then no other terms are evaluated. If the router does not find a match between the packet and first term, it then compares the packet to the next term in the filter. The router continues to compare the packet to the next specified term until a match is found. If there is no match after all terms have been examined, the router silently drops the packet.

You can specify a precedence (from 0 through 255) for input and output filters within a dynamic profile to force filter processing in a particular order. Setting a lower

precedence value for a filter gives it a higher precedence within the dynamic profile. In other words, filters with lower precedence values are applied to interfaces before filters with higher precedence values. A precedence of zero (the default) gives the filter the highest precedence. If no precedence is specified, the filter receives a precedence of zero (highest precedence). Filters with matching precedence (zero or otherwise) are applied in random order.

Fast Update Filter Names

When a filter is attached to an interface, the router first searches for a classic filter with the specified name, and then uses the classic filter. If no classic filter exists with that name, the router then searches in the dynamic-profile for a fast update filter with the specified name, and uses that filter.

If two different dynamic-profiles include a fast update filter with the same name, the match-order specification of the two filters must be identical. If the two filters are activated on the same interface, the terms are added together.

The router includes the filter name in show firewall command results. The router also creates unique names for filter terms and counters for show firewall command.

When a fast update filter is created by the activation of a dynamic profile, the router creates an interface-specific name for the filter. The name uses the following format, which is also used for classic filters:

<filter-name>-<interface-name>.<subunit>-<direction>

For example, an input filter named httpFilter on interface ge-1/0/0.5 is named as follows (**in**indicates an input filter and **out**indicates an output filter):

http-filter-ge-1/0/0.5–in

The router creates unique names for the filter terms and counters by appending the session ID to all term and counter names. Terms that use the only-at-create statement have a session-id of 0. Terms and counters use the following format:

<term-name>-<session-id>

<counter-name>-<session-id>

Guidelines for Creating and Applying Fast Update Filters

Fast update filters enable you to create subscriber-specific firewall filters and dynamically apply these filters to statically created interfaces using dynamic profiles. Individual terms can be added to, or removed from, a filter without requiring that the entire filter be recompiled.

When creating and applying fast update filters, keep the following in mind:

- This release supports dynamic application of input and output filters.
- Fast update filters must always include terms that permit DHCP traffic to pass. See Configuring Filters to Permit Expected Traffic.

- The interface-specific statement is required for all fast update filters.
- The match-order statement is required—you must explicitly state the order of the match fields in a fast update filter. See Configuring the Match Order for Fast Update Filters
- The match-order statement uses an implied wildcard for conditions that you specify in the statement. If you specify a condition that is not also configured in the from specification of a filter term, the router considers that a wildcard for that condition.
- A filter term can have only a single value or range; however, you can configure multiple terms to specify multiple ranges.
- You can match a maximum of five match conditions in a filter.

Related Topics

- Dynamic Firewall Filters Overview
- Classic Filters Overview
- Dynamically Attaching Statically Created Filters
- Verifying and Managing Firewall Filter Configuration

Published: 2009-07-16