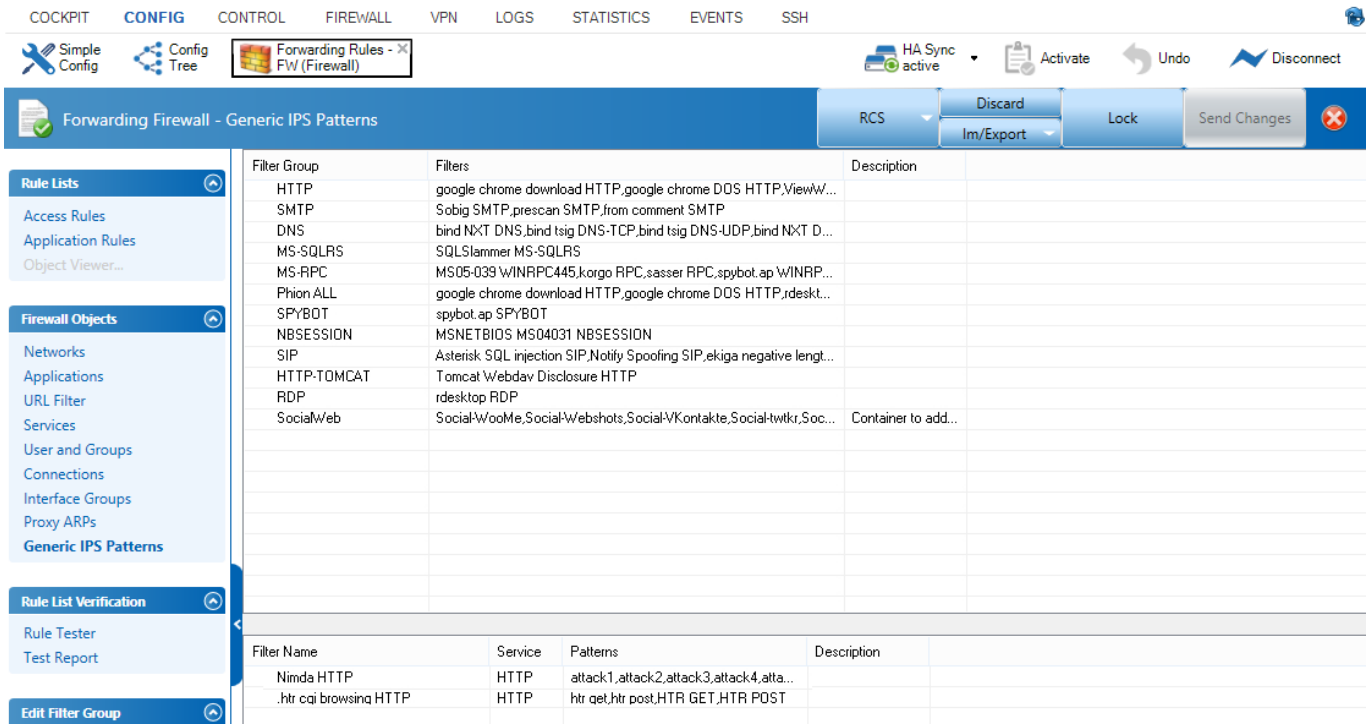
How to Define Generic IPS Patterns for Content Filtering

https://campus.barracuda.com/doc/41115742/

Barracuda Networks recommends using the Intrusion Prevention System (IPS) instead of the legacy generic IPS patterns.

Generic IPS Patterns do not work in combination with Application Control.

To block Internet worms and exploit attacks, configure a content filter. The Barracuda NG Firewall provides a set of predefined content filters that can be referenced by the firewall rule set. Network connection types (for example, SMTP) that are specified in the service or Service Object of firewall rules are checked for patterns that are configured in the content filters. Detected network attacks are logged in the <fw>_Content log file for later review. The source and destination address and the associated network interfaces or firewall rule actions are stored in the corresponding filter log (for example, [sqlslammer]).

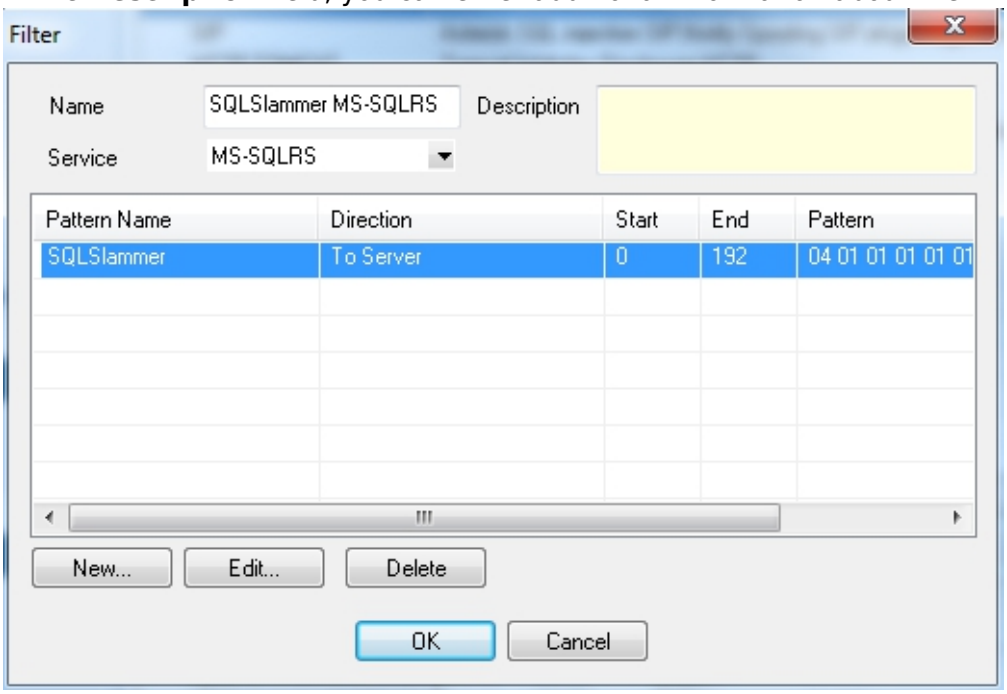


You can edit existing filters or add new filters. You can also create filter groups.

In this article:

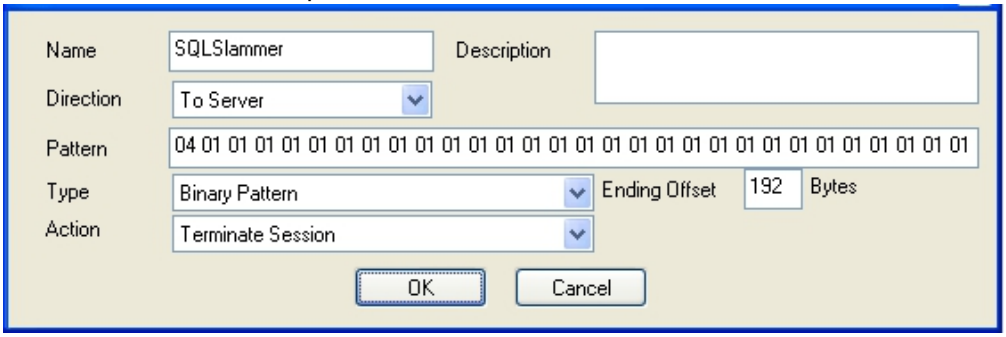
Configure a Filter

1. Open the **Forwarding Rules** page (**CONFIG > Full Config > Virtual Servers > *your virtual server*** **> Firewall**).
2. In the left navigation pane, click on **Generic IPS Patterns**.
3. Create a new filter or select an existing filter to edit:
   - To create a new filter, right-click the lower table and select **New**.
   - To edit an existing filter, double-click its name in the lower table.
4. Enter or edit the descriptive **Name** for the filter.
5. From the **Service** list, select the service to be filtered.
6. In the **Description** field, you can enter additional information about the filter.



7. Configure the patterns for the filter:
   - To edit an existing pattern, select it from the table and click **Edit**.
   - To create a new pattern, click **New**.

   The **Pattern** window opens.



8. You can edit the following pattern settings:

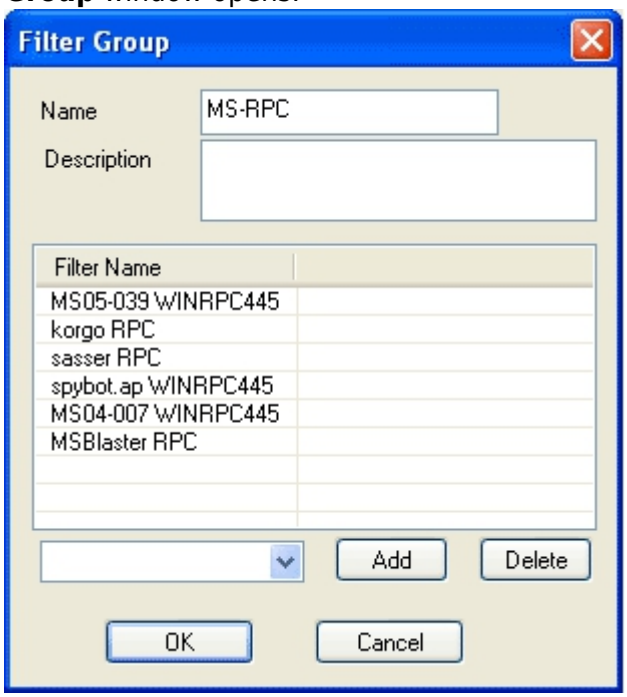
Setting	Description

Name	The pattern name.		
Direction	Which direction of traffic/stream is affected. You can select one of the following directions: ◦ **To Server** – Incoming traffic/stream. ◦ **To Client** – Outgoing traffic/stream.		
Description	Any additional information about the pattern.		
Pattern	The search pattern for the object that the stream is scanned for.		
Type	The pattern type. You can select any of the following pattern types:	**Binary Pattern**	List of hexadecimal digit pairs separated with a space. The above screenshot of the **Pattern** window displays an example for a binary pattern (SQL slammer).
		ASCII Pattern + Wildcards(*,?,[])	* – represents a variable number of characters including an empty string (space)
			? – matches exactly one character.
			[…] – matches only the characters that are enclosed within the brackets.
			Example pattern: [123]??attack*## Match on the following: 200attacking## 321attacker## 1stattack## Mismatch on the following: 500attackers## 1million attackers## 123ata# The patterns are detected at any offset in the traffic flow unless the sequence of matching characters exceeds the boundary that is specified by the **Ending Offset** setting.
Action	Enables a reporting only mode for individual patterns. You can select one of the following actions: ◦ **Terminate Session** – Causes session termination when the pattern matches. ◦ **Create Log Entry** – Triggers log entry generation only.		
Ending Offset	The number of bytes from the connection start that are scanned to find the pattern.		

9. Click **OK**.

Configure a Filter Group

1. Open the **Forwarding Rules** page (**CONFIG > Full Config > Virtual Servers > *your virtual server*** **> Firewall**).
2. In the left navigation pane click on **Generic IPS Patterns**.
3. Click **Lock**.
4. Create a new group or select an existing group to edit:
   - To create a new filter, right-click the upper table and select **New**.
   - To edit an existing group, double-click its name in the upper table. The **Filter Group** window opens:



5. You can edit the following group settings:
   - **Name** – The group name.
   - **Description** – Any additional information about the filter group.
   - **Filter Name** – Table that lists each filter that is included in the group. You can add or delete filters.
     - To add a filter, select it from the filter list and click **Add**.
     - To delete a filter, select it and click the **Delete**.
6. Click **OK**.

Referencing within the Corresponding Rules

When a pattern for content filtering was successfully applied to a service, the service, when selected in context with a firewall rule, will now automatically apply this pattern to the rule.

Figures

1. ct_filter.png
2. gen_filter_new.png
3. gen_pattern.png
4. f_group.png